nanoX-EL

User's Guide

intel

COM Express®

Revision: Rev. 1.2
Date: 2024-06-18
Part Number: 50M-72307-1020

ADLINK
LEADING EDGE COMPUTING

Revision History

Revision	Description	Date	Author
1.0	Initial release	2021-11-24	JC
1.1	BIOS tables added	2023-08-21	CC
1.2	DDI0 port spec updated	2024-06-18	AL

Preface

Disclaimer

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

Environmental Responsibility

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

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

Trademarks

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

Copyright © 2024 ADLINK Technology Incorporated

Safety Instructions

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

Read these safety instructions carefully.

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

Conventions

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

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

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

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

Getting Service

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

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

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

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

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

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

Table of Contents

List of Figures

1. Introduction

The nanoX-EL is the first COM Express® COM.0 R3.0 Mini Size Type 10 module featuring the IT/OT convergence 6th Gen Intel Atom® x6000E and Pentium Celeron processors (formerly "Elkhart Lake"). The processors support up to 4 cores as well as an impressive turbo boost of up to 3.0GHz. In addition, the module is also equipped with Intel® Time Coordinated Computing (Intel® TCC) that allows several controllers to process in a synchronized manner and communicate in real time. These combined features make the nanoX-EL well suited to customers who need to manage both IT and OT in a simplified design.

The nanoX-EL supports BIOS configurable in-band ECC (IBECC) with normal memory chip or supports traditional ECC memory chip that provides ECC level error correction. A maximum 16GB LPDDR4 memory capacity, wide operating temperature range, and MIL-STD environmental specifications make it well suited for mission critical or extreme rugged applications.

Integrated Intel® Gen 11 LP Graphics includes features such as OpenGL 4.5, OpenGL ES 3.1/3.0/2.0/1.1, DirectX 12.1, OpenCL 1.2, Vulkan 1.1 APIs, Intel® Clear Video HD Technology, and support for full H.265/HEVC 10-bit, H.264, VP9, JPEG/MJPEG hardware codecs. Graphics outputs include LVDS and one DDI port supporting HDMI/DVI/DisplayPort with eDP as a BOM option. Displays of up to 4K resolution are supported on DDI/eDP interface.

Input/output features include four PCIe Gen3 lanes that can be used for NVMe SSD allowing applications to utilize the highest speed storage solutions, an optional 2.5Gigabit Ethernet port supporting Time Sensitive Network (TSN), up to two USB 3.0/2.0 ports, six USB 2.0 ports, two SATA 6 Gb/s ports and an optional onboard eMMC (16/32/64GB). 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

6th Gen Intel Atom® x6000E processors and Intel® Celeron® and Pentium® N & J processors (formerly "Elkhart Lake")

- Intel Atom® x6425E, 2.0(3.0) GHz, 12W, 4C/32EU (IBECC/non-ECC)
- Intel Atom® x6413E, 1.5(3.0) GHz, 9W, 4C/16EU (IBECC/non-ECC)
- Intel Atom® x6211E, 1.3(3.0) GHz, 6W, 2C/16EU (IBECC/non-ECC)
- Intel Atom® x6425RE, 1.9 GHz, 12W, 4C/32EU (IBECC/non-ECC, Intel® TCC)
- Intel Atom® x6414RE, 1.5 GHz, 9W, 4C/16EU (IBECC/non-ECC, Intel® TCC)
- Intel Atom® x6212RE, 1.2 GHz, 6W, 2C/16EU (IBECC/non-ECC, Intel® TCC)
- Intel Atom® x6200FE, 1.0 GHz, 4.5W, 2C/No GPU (IBECC/non-ECC, Intel® TCC)
- Intel® Pentium® J6426, 2.0(3.0) GHz, 10W, 4C/32EU (non-ECC)
- Intel® Celeron® J6413, 1.8(3.0) GHz, 10W, 4C/16EU (non-ECC)
- Intel® Pentium® N6415, 1.2(3.0) GHz, 6.5W, 4C/16EU (non-ECC)
- Intel® Celeon® N6211, 1.2(3.0) GHz, 6.5W, 2C/16EU (non-ECC)

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

Note: SKUs with Intel® TCC feature paired with specific LAN solutions can support TSN (TBC).
Pentium, Celeron and some of Atom SKUs are supported by project basis. Please contact your local ADLINK presentative.

Memory

Up to 16GB LPDDR4

In-band ECC (IBECC) with normal memory chip support on selected SKUs. IBECC can be enabled/disabled in BIOS setup

Note: 8GB/16GB is supported by project basis.

Cache

1.5MB

Embedded BIOS

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

2.2. Video

GPU

Intel® Gen 11 LP Graphics core architecture

GPU Feature Support

2 independent and simultaneous combinations of DisplayPort/HDMI/LVDS graphics outputs (eDP optional in place of LVDS)

Encode/transcode of HD content

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

Intel® QuickSync and Intel® Clear Video HD

HEVC/H.265 10-bit/8-bit, H.264, M/JPEG, MPEG2, VC1/WMV9, VP9, VP8 HW decode

HEVC/H.265 10-bit/8-bit, H.264, M/JPEG, VP9 HW encode

DirectX up to 12.1

OpenGL up to 4.5, OpenGL ES up to 3.1

OpenCL 1.2, Vulkan 1.1 APIs

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

Note: Availability of features 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 1.3 up to 4 lane support, in place of LVDS (BOM option), max. resolution 4096x2160@60Hz, 24bpp

DDI x1: Digital Display Ports (DDI) support DisplayPort 1.4, HDMI 1.4b or DVI

2.3. Audio

Intel® HD Audio integrated

Located on carrier miniBASE-10R (ALC262 standard support)

2.4. Expansion Busses

4 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)

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

2.5. Ethernet

Integrated MAC with MaxLinear® 2.5Gigabit Ethernet PHY, GPY211 or GPY215

Supports 2.5Gbit/s or 1000/100/10 Mbit/s connection

Supports TSN on Yocto Linux OS (based on GPY215 and the CPU SKUs with Intel TCC feature) (TSN may support by project basis)

2.6. Multi I/O and Storage

USB

2x USB 3.0/2.0/1.1 (USB 0,1), 6x USB 2.0/1.1 (USB 2,3,4,5,6,7)

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

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

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

LPC Bus

Low Pin Count bus extends from an eSPI-to-LPC bridge IC

GPIO or SD

4 GPO and 4 GPI (GPI with interrupt supported on Linux), SD/GPIO muxed design, SD supported by BOM option by project basis

SD functions as storage device

Note: Supports 3.3V SD cards only

SATA

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

eMMC

16/32/64GB

Note: Boot device support may vary between operating systems.
Combinations (CPU SKUs, memory capacity, eMMC capacity) not listed as standard will be supported by project basis.

Boot Device Support

		Windows 10 Enterprise	Linux (Yotco)	Linux (Ubuntu)	VxWorks
OS Installation	eMMC	Yes	Yes	TBC	TBC
	SD	No	No	No	No

Note: eMMC and SD functionality as an OS installation device may change dependent on Intel updates. Please contact your local sales representative for more information.

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: 4.75-20V, 5Vsb ±5%	or	AT: 4.75-20V

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 our 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, Mini size 84 x 55 mm

Operating Temperature

Standard	0°C to +60°C (Wide Voltage Input)	Storage: -20°C to +80°C
Extreme Rugged (Selected SoC SKUs)	-40°C to +85°C (Standard Voltage Input)	Storage: -40°C to +85°C

Humidity

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

Shock and Vibration

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

HALT tested

Thermal Stress, Vibration Stress, Thermal Shock and Combined Test

3. Block Diagram

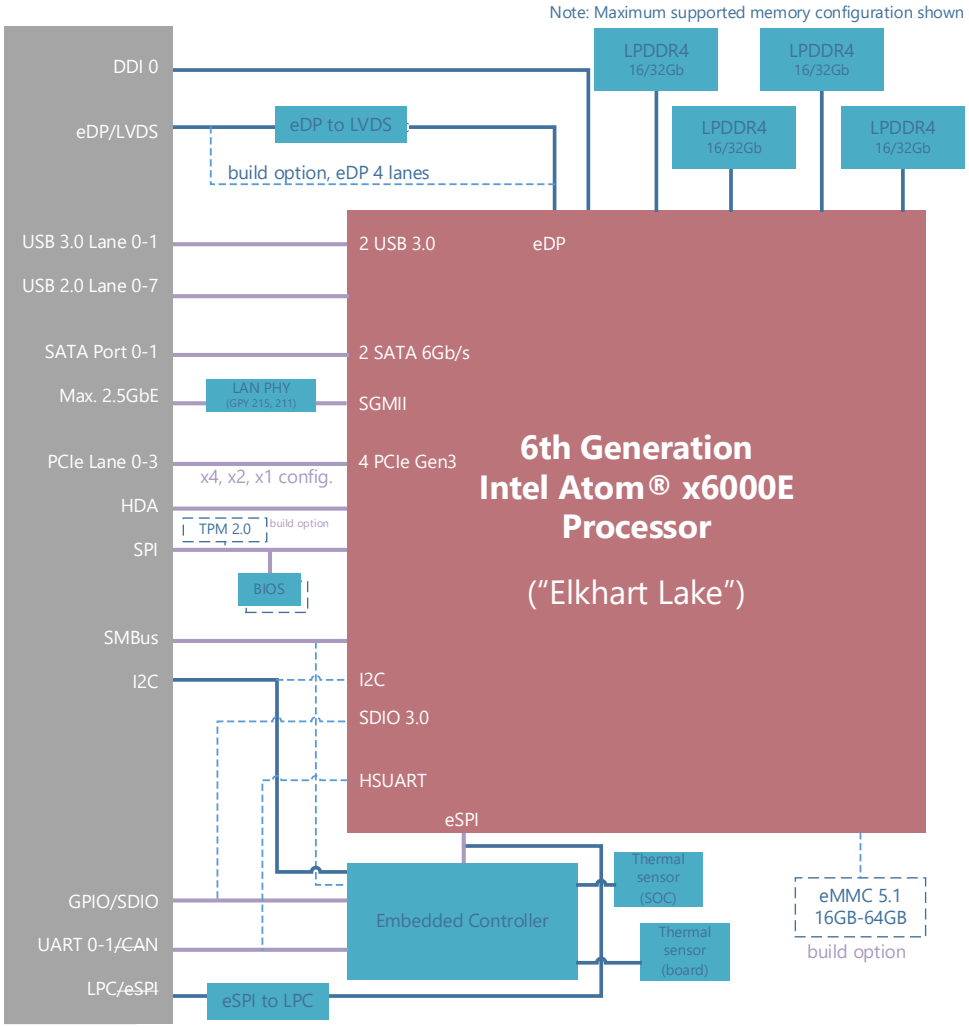


Figure 1 – Module function diagram

4. Pinout and Signal Descriptions

4.1. Pin Summary

The table below is a comprehensive list of all signal pins supported on the single 220-pin COM Express connectors as defined for Type 10 in the PICMG COM.0 R3.0 specification. Signals described in the specification but not supported on the nanoX-EL are strikethrough ~~STRIKETHROUGH.~~

Figure 2 - Module rear side row and pin numbering

Row A			Row B	
A1	GND (FIXED)		B1	GND (FIXED)
A2	GBE0_MDI3-		B2	GBE0_ACT#
A3	GBE0_MDI3+		B3	LPC_FRAME#/~~ESPI_CS0#~~
A4	GBE0_LINK100#		B4	LPC_AD0/~~ESPI_IO_0~~
A5	GBE0_LINK1000#		B5	LPC_AD1/~~ESPI_IO_1~~
A6	GBE0_MDI2-		B6	LPC_AD2/~~ESPI_IO_2~~
A7	GBE0_MDI2+		B7	LPC_AD3/~~ESPI_IO_3~~
A8	GBE0_LINK#		B8	LPC_DRQ0#/~~ESPI_ALERT0#~~
A9	GBE0_MDI1-		B9	LPC_DRQ1#/~~ESPI_ALERT1#~~
A10	GBE0_MDI1+		B10	LPC_CLK/~~ESPI_CK~~
A11	GND (FIXED)		B11	GND (FIXED)
A12	GBE0_MDI0-		B12	PWRBTN#
A13	GBE0_MDI0+		B13	SMB_CK
A14	GBE0_CTREF		B14	SMB_DAT
A15	SUS_S3#		B15	SMB_ALERT#
A16	SATA0_TX+		B16	SATA1_TX+
A17	SATA0_TX-		B17	SATA1_TX-
A18	SUS_S4#		B18	SUS_STAT#/~~ESPI_RESET#~~
A19	SATA0_RX+		B19	SATA1_RX+
A20	SATA0_RX-		B20	SATA1_RX-
A21	GND (FIXED)		B21	GND (FIXED)
A22	USB_SSRX0-		B22	USB_SSTX0-
A23	USB_SSRX0+		B23	USB_SSTX0+
A24	SUS_S5#		B24	PWR_OK
A25	USB_SSRX1-		B25	USB_SSTX1-
A26	USB_SSRX1+		B26	USB_SSTX1+
A27	BATLOW#		B27	WDT
A28	(S)ATA_ACT#		B28	~~AC/HDA_SDIN2~~
A29	HDA_SYNC		B29	AC/HDA_SDIN1
A30	HDA_RST#		B30	AC/HDA_SDIN0
A31	GND (FIXED)		B31	GND (FIXED)
A32	HDA_BITCLK		B32	SPKR
A33	HDA_SDOUT		B33	I2C_CK
A34	BIOS_DIS0#/~~ESPI_SAFS~~		B34	I2C_DAT
A35	THRMTRIP#		B35	THRM#

Row A			Row B	
A36	USB6-		B36	USB7-
A37	USB6+		B37	USB7+
A38	USB_6_7_OC#		B38	USB_4_5_OC#
A39	USB4-		B39	USB5-
A40	USB4+		B40	USB5+
A41	GND (FIXED)		B41	GND (FIXED)
A42	USB2-		B42	USB3-
A43	USB2+		B43	USB3+
A44	USB_2_3_OC#		B44	USB_0_1_OC#
A45	USB0-		B45	USB1-
A46	USB0+		B46	USB1+
A47	VCC_RTC		B47	~~ESPI_EN#~~
A48	RSVD		B48	~~USB0_HOST_PRSNT~~
A49	GBE0_SDP		B49	SYS_RESET#
A50	LPC_SERIRQ~~/ESPI_CS1#~~		B50	CB_RESET#
A51	GND (FIXED)		B51	GND (FIXED)
A52	RSVD		B52	RSVD
A53	RSVD		B53	RSVD
A54	GPI0		B54	GPO1
A55	RSVD		B55	RSVD
A56	RSVD		B56	RSVD-
A57	GND		B57	GPO2
A58	PCIE_TX3+		B58	PCIE_RX3+
A59	PCIE_TX3-		B59	PCIE_RX3-
A60	GND (FIXED)		B60	GND (FIXED)
A61	PCIE_TX2+		B61	PCIE_RX2+
A62	PCIE_TX2-		B62	PCIE_RX2-
A63	GPI1		B63	GPO3
A64	PCIE_TX1+		B64	PCIE_RX1+
A65	PCIE_TX1-		B65	PCIE_RX1-
A66	GND		B66	WAKE0#
A67	GPI2		B67	WAKE1#
A68	PCIE_TX0+		B68	PCIE_RX0+
A69	PCIE_TX0-		B69	PCIE_RX0-
A70	GND (FIXED)		B70	GND (FIXED)

Row A			Row B	
A71	LVDS_A0+ / eDP_TX2+ *		B71	DDI0_PAIR0+
A72	LVDS_A0- / eDP_TX2- *		B72	DDI0_PAIR0-
A73	LVDS_A1+ / eDP_TX1+ *		B73	DDI0_PAIR1+
A74	LVDS_A1- / eDP_TX1- *		B74	DDI0_PAIR1-
A75	LVDS_A2+ / eDP_TX0+ *		B75	DDI0_PAIR2+
A76	LVDS_A2- / eDP_TX0- *		B76	DDI0_PAIR2-
A77	LVDS_VDD_EN / eDP_VDD_EN *		B77	~~DDI0_PAIR4+~~
A78	LVDS_A3+		B78	~~DDI0_PAIR4-~~
A79	LVDS_A3-		B79	LVDS_BKLT_EN *
A80	GND (FIXED)		B80	GND (FIXED)
A81	LVDS_A_CK+ / eDP_TX3+ *		B81	DDI0_PAIR3+
A82	LVDS_A_CK- / eDP_TX3- *		B82	DDI0_PAIR3-
A83	LVDS_I2C_CK / eDP_AUX+ *		B83	LVDS_BKLT_CTRL / eDP_BKLT_CTRL *
A84	LVDS_I2C_DAT / eDP_AUX- *		B84	VCC_5V_SBY
A85	GPI3		B85	VCC_5V_SBY
A86	RSVD		B86	VCC_5V_SBY
A87	eDP_HPD *		B87	VCC_5V_SBY
A88	PCIE0_CK_REF+		B88	BIOS_DIS1#
A89	PCIE0_CK_REF-		B89	DDI0_HPD
A90	GND (FIXED)		B90	GND (FIXED)
A91	SPI_POWER		B91	~~DDI0_PAIR5+~~
A92	SPI_MISO		B92	~~DDI0_PAIR5-~~
A93	GPO0		B93	~~DDI0_PAIR6+~~
A94	SPI_CLK		B94	~~DDI0_PAIR6-~~
A95	SPI_MOSI		B95	DDI0_DDC_AUX_SEL
A96	TPM_PP		B96	~~USB7_HOST_PRSNT~~
A97	TYPE10#		B97	SPI_CS#
A98	SER0_TX		B98	DDI0_CTRLCLK_AUX+
A99	SER0_RX		B99	DDI0_CTRLDATA_AUX-
A100	GND (FIXED)		B100	GND (FIXED)
A101	SER1_TX~~/CAN_TX~~		B101	FAN_PWMOUT
A102	SER1_RX~~/CAN_RX~~		B102	FAN_TACHIN
A103	LID#		B103	SLEEP#
A104	VCC_12V		B104	VCC_12V
A105	VCC_12V		B105	VCC_12V

Row A			Row B	
A106	VCC_12V		B106	VCC_12V
A107	VCC_12V		B107	VCC_12V
A108	VCC_12V		B108	VCC_12V
A109	VCC_12V		B109	VCC_12V
A110	GND (FIXED)		B110	GND (FIXED)

Note: ~~STRIKETHROUGH~~ strike-through entries are not supported functions on this product
eDP (in place of LVDS) is BOM option support by project basis

SD (in place of GPIO) is BOM option support by project basis

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 3.3V		
AC_BITCLK / HDA_BITCLK	A32	Serial data clock generated by the external CODEC(s).	I/O 3.3V		
AC_SDOUT / HDA_SDOUT	A33	Serial TDM data output to the CODEC.	O 3.3V		
AC_SDIN[2:0] / HDA_SDIN[2:0]	B28- B30	Serial TDM data inputs from up to 3 CODECs.	I/O 3.3VSB		B28 (SDIN2) Not supported Elkhart Lake doesn't offer this pin

4.3.2. LVDS or eDP

The module supports a single channel LVDS display panel with up to 24-bit colors by default.
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 A72	LVDS_A0+ LVDS_A0-	eDP_TX2+ eDP_TX2-
A73 A74	LVDS_A1+ LVDS_A1-	eDP_TX1+ eDP_TX1-
A75 A76	LVDS_A2+ LVDS_A2-	eDP_TX0+ eDP_TX0-
A78 A79	LVDS_A3+ LVDS_A3-	- -
A81 A82	LVDS_A_CK+ LVDS_A_CK-	eDP_TX3+ eDP_TX3-
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, eDP is BOM option by project basis

4.3.2.1. 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_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	

4.3.2.2. 4-lane eDP (optional)

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

4.3.3. DDI0 Port

Name	Pin #	DisplayPort (DP)	HDMI
DDI0_PAIR0+ DDI0_PAIR0-	B71 B72	DP0_LANE0+ DP0_LANE0-	TMDS0_DATA2+ TMDS0_DATA2-
DDI0_PAIR1+ DDI0_PAIR1-	B73 B74	DP0_LANE1+ DP0_LANE1-	TMDS0_DATA1+ TMDS0_DATA1-
DDI0_PAIR2+ DDI0_PAIR2-	B75 B76	DP0_LANE2+ DP0_LANE2-	TMDS0_DATA0+ TMDS0_DATA0-
DDI0_PAIR3+ DDI0_PAIR3-	B81 B82	DP0_LANE3+ DP0_LANE3-	TMDS0_CLK+ TMDS0_CLK-
DDI0_PAIR4+ DDI0_PAIR4-	B77 B78	-	-
DDI0_PAIR5+ DDI0_PAIR5-	B91 B92	-	-
DDI0_PAIR6+ DDI0_PAIR6-	B93 B94	-	-
DDI0_HPD	B89	DP0_HPD	HDMI0_HPD
DDI0_CTRLCLK_AUX+	B98	DP0_AUX+	HMDI0_CTRLCLK
DDI0_CTRLCLK_AUX-	B99	DP0_AUX-	HMDI0_CTRLDATA
DDI0_DDC_AUX_SEL	B95	DDI0_DDC_AUX_SEL	DDI0_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 may be used to resolve this problem. The FET gates can be controlled by the AUX_SEL pin function.

4.3.3.1. DisplayPort (DP) Mode

Name	Pin #	Description	I/O	PU / PD	Comment
DP0_LANE0+ DP0_LANE0- DP0_LANE1+ DP0_LANE1- DP0_LANE2+ DP0_LANE2- DP0_LANE3+ DP0_LANE3-	B71 B72 B73 B74 B75 B76 B81 B82	DP Port 1, differential pair data lines	O PCIE		AC coupled off Module 100 nF DC blocking capacitors ***shall*** be placed on the Carrier
DP0_HPD	B89	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.
DP0_AUX+	B98	DP Port 1, Bidirectional Channel used for Link Management and Device Control	I/O PCIE	PD 100k	AC coupled on Module
DP0_AUX-	B99	DP Port 1, Bidirectional Channel used for Link Management and Device Control	I/O PCIE	PU 100k	AC coupled on Module
DDI0_DDC_AUX_SEL	B95	Strapping Signal to select HDMI or DP output 1M pull-down on the module and floating on the carrier enable DisplayPort mode	I 3.3V	PD 1M	DP mode enabled

4.3.3.2. HDMI Mode

Name	Pin #	Description	I/O	PU / PD	Comment
TMDS0_DATA2+ TMDS0_DATA2- TMDS0_DATA1+ TMDS0_DATA1- TMDS0_DATA0+ TMDS0_DATA0-	B71 B72 B73 B74 B75 B76	HDMI / DVI Port, Differential Pair Data Lines	O PCIE		AC coupled off Module 100 nF DC blocking capacitors shall be placed on the Carrier
TMDS0_CLK+ TMDS0_CLK-	B81 B82	HDMI Port, Differential Pair Clock Lines			
HDMI0_HPD	B89	Detection of Hot Plug / Unplug and notification of the link layer	I 3.3V	PD 100k	
HDMI0_CTRLCLK	B98	I2C_CLK Line for HDMI	I/O PCIE	PU 2.2k	AC couple on Module
HDMI0_CTRLDATA	B99	I2C_DAT Line for HDMI	I/O PCIE	PU 2.2k	AC couple on Module
DDI0_DDC_AUX_SEL	B95	Strapping Signal to select HDMI or DP output. 1M pull-down on the module and pull-high on the carrier enable HDMI mode	I 3.3V	PD 1M	HDMI mode enabled

4.3.4. Gigabit Ethernet

Name	Pin #	Description	I/O	PU / PD	Comment
GBE0_MDI0+ GBE0_MDI0- GBE0_MDI1+ GBE0_MDI1- GBE0_MDI2+ GBE0_MDI2- GBE0_MDI3+ GBE0_MDI3-	A13 A12 A10 A9 A7 A6 A3 A2	Gigabit Ethernet Controller 0: Media Dependent Interface Differential Pairs 0, 1, 2, 3. The MDI can operate in 1000, 100, and 10Mbit/sec modes. Some pairs are unused in some modes according to the following: **1000 / 100 / 10** MDI[0]+/- B1_DA+/- TX+/- TX+/- MDI[1]+/- B1_DB+/- RX+/- RX+/- MDI[2]+/- B1_DC+/- MDI[3]+/- B1_DD+/-	I/O Analog		Twisted pair signals for external transformer.
GBE0_ACT#	B2	Gigabit Ethernet Controller 0 activity indicator, active low.	OD 3.3VSB	PU TBD	LED behaviour is TBC
GBE0_LINK#	A8	Gigabit Ethernet Controller 0 link indicator, active low.	OD 3.3VSB	PU TBD	LED behaviour is TBC
GBE0_LINK100#	A4	Gigabit Ethernet Controller 0 100Mbit/sec link indicator, active low.	OD 3.3VSB	PU TBD	LED behaviour is TBC
GBE0_LINK1000#	A5	Gigabit Ethernet Controller 0 1000Mbit/sec link indicator, active low.	OD 3.3VSB	PU TBD	LED behaviour is TBC
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: TSN supported by GPY 215 PHY and Yocto Linux OS on selected CPU SKUs.
GBE0_LINK1000# will be active for 2.5GbE speed indication.
GBE0_LINK100# will be active for 1GbE speed indication.
GBE0_LINK100# will be active for 1GbE speed indication.
The LAN LED for 100Mbit/sec and 10Mbit/sec speed will be OFF.

This product supports up to 2.5GbE Ethernet speed. The LAN LED behavior is optimized for maximum 2.5GbE speed (TBC).

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
(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	

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_CLK_REF+ PCIE_CLK_REF-	A88 A89	PCI Express Reference Clock output for all PCI Express and PCI Express Graphics Lanes.	O PCIE		

4.3.6.1. PCH HSIO Lane Assignments

Name	HSIO name on SOC	Comment
PCIE0	HSIO 2	
PCIE1	HSIO 3	
PCIE2	HSIO 4	
PCIE3	HSIO 5	

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 2.0/1.1

Name	Pin #	Description	I/O	PU / PD	Comment
USB0+ USB0-	A46 A45	USB differential data pairs for Port 0	I/O 3.3VSB		USB 1.1/ 2.0 compliant
USB1+ USB1-	B46 B45	USB differential data pairs for Port 1	I/O 3.3VSB		USB 1.1/ 2.0 compliant
USB2+ USB2-	A43 A42	USB differential data pairs for Port 1	I/O 3.3VSB		USB 1.1/ 2.0 compliant
USB3+ USB3-	B43 B42	USB differential data pairs for Port 2	I/O 3.3VSB		USB 1.1/ 2.0 compliant
USB4+ USB4-	A40 A39	USB differential data pairs for Port 3	I/O 3.3VSB		USB 1.1/ 2.0 compliant
USB5+ USB5-	B40 B39	USB differential data pairs for Port 4	I/O 3.3VSB		USB 1.1/ 2.0 compliant
USB6+ USB6-	A37 A36	USB differential data pairs for Port 5	I/O 3.3VSB		USB 1.1/ 2.0 compliant
USB7+ USB7-	B37 B37	USB differential data pairs for Port 6	I/O 3.3VSB		USB 1.1/ 2.0 compliant
USB_0_1_OC#	B44	USB over-current sense, USB ports 0 and 1 (see *Note)	I 3.3VSB	PU 10k 3.3VSB	Do not pull high on carrier
USB_2_3_OC#	A44	USB over-current sense, USB ports 2 and 3 (see *Note)	I 3.3VSB	PU 10k 3.3VSB	Do not pull high on carrier
USB_4_5_OC#	B38	USB over-current sense, USB ports 4 and 5 (see *Note)	I 3.3VSB	PU 10k 3.3VSB	Do not pull high on carrier
USB_6_7_OC#	A38	USB over-current sense, USB ports 6 and 7 (see *Note)	I 3.3VSB	PU 10k 3.3VSB	Do not pull high on carrier
~~USB0_HOST_PRSNT~~	~~B48~~	~~Module USB client may detect the presence of a USB host on USB0. A high value indicates that a host is present.~~	~~I 3.3VSB~~		Not supported
~~USB7_HOST_PRSNT~~	~~B96~~	~~Module USB client may detect the presence of a USB host on USB7. 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. USB 3.x Extension

Name	Pin #	Description	I/O	PU / PD	Comment
USB_SSRX0- USB_SSRX0+	A22 A23	Additional Receive signal differential pairs for the SuperSpeed USB data path on USB0	I PCIE		AC coupled off module
USB_SSTX0- USB_SSTX0+	B22 B23	Additional Transmit signal differential pairs for the SuperSpeed USB data path on USB0	O PCIE		AC coupled on module
USB_SSRX1- USB_SSRX1+	A25 A26	Additional Receive signal differential pairs for the SuperSpeed USB data path on USB1	I PCIE		AC coupled off module
USB_SSTX1- USB_SSTX1+	B25 B26	Additional Transmit signal differential pairs for the SuperSpeed USB data path on USB1	O PCIE		AC coupled on module

4.3.9.1. USB 3.x Extension Root Segmentation

Name	HSIO name on SOC	Comment
USB 0	HSIO 0	from XHCI controller
USB 1	HSIO 1	from XHCI controller

4.3.10. 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

4.3.11. 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 3.3V	PU 10k 3.3V	
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

4.3.12. 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	

Note: SMBus from EC is BOM option supported by project basis

4.3.13. I2C Bus

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

Note: I2C from 6th Gen Intel Atom® x6000E processor is BOM option supported by project basis

4.3.14. 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	

Note: 8x GPIO from 6th Gen Intel Atom® x6000E processor is BOM option supported by project basis (TBC).

GPO[0:3] PU 10k 3.3V is by build option for programming these pins to be GPI.
GPI [0:3] PD 10k is by build option for programming these pins to be GPO.

4.3.15. 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 47k 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 47k 3.3V	Power rail tolerance 5V, 12V

Note: 2x UART from 6th Gen Intel Atom® x6000E processor are BOM option support by project basis

4.3.16. 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)

4.3.17. 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		4.75-20 V
VCC_5V_SBY	B84, B85, B86, B87	Standby power input: +5.0V nominal. If VCC5_SBY is used, all available VCC_5V_SBY pins on the connector(s) shall be used. Only used for standby and suspend functions. May be left unconnected if these functions are not used in the system design.	P		5Vsb ±5%
VCC_RTC	A47	Real-time clock circuit-power input. Nominally +3.0V.	P		
GND	A1, A11, A21, A31, A41, A51, A57, A60, A66, A70, A80, A90, A100, A110, B1, B11, B21, B31, B41, B51, B60, B70, B80, B90, B100, B110	Ground - DC power and signal and AC signal return path.	P		

5. Additional Features

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

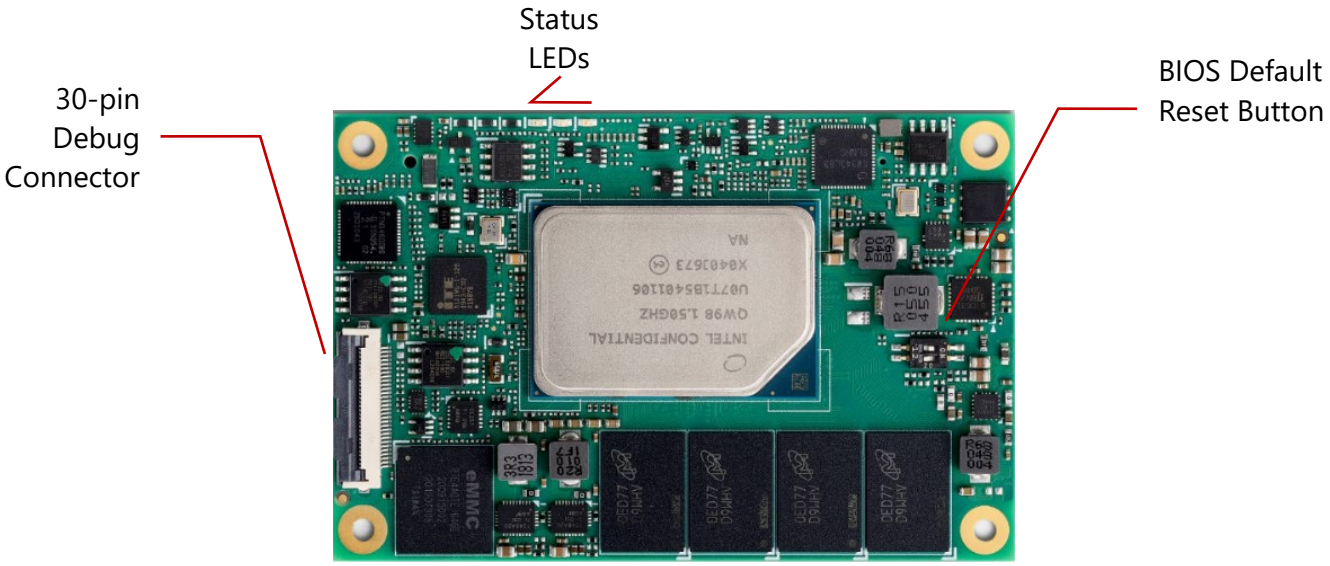


Figure 3 – Module feature locations

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

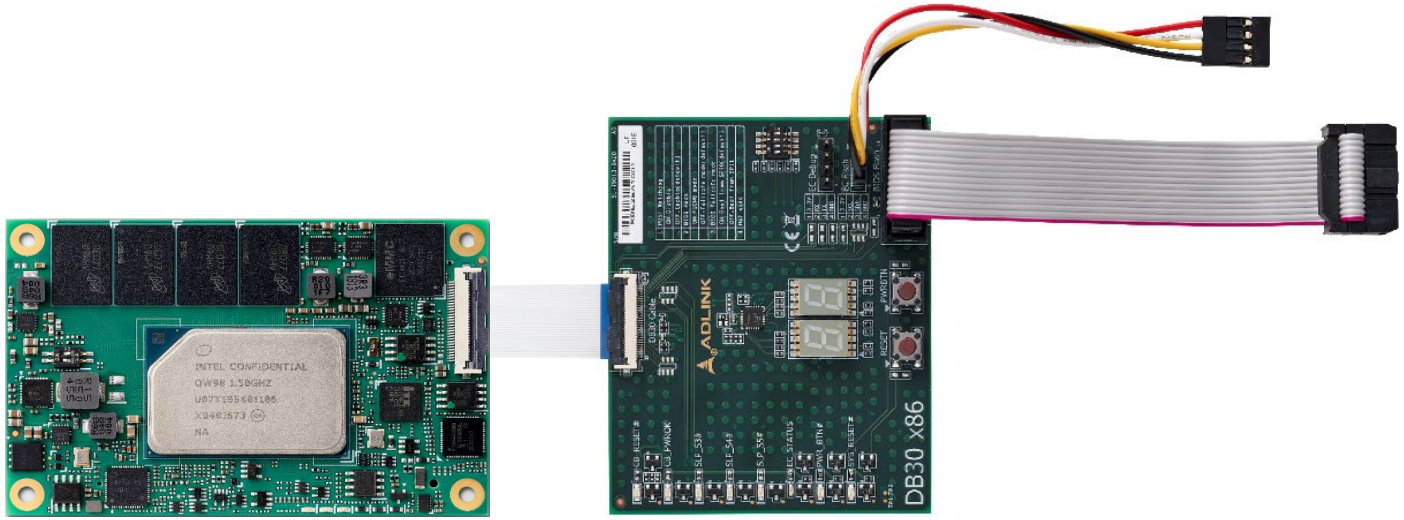
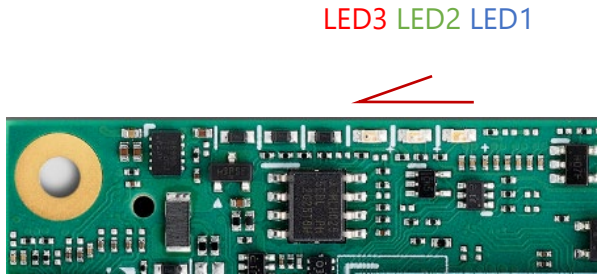


Figure 4 – nanoX-EL and Debug Module

5.2. Status LEDs

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



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

5.3. Exception Codes

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

Note: Exception codes in ~~STRIKETHROUGH~~ are not used by the nanoX-EL module.

5.4. 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	Target	Dependency / Comments
000E 0000h-000E FFFFh	SPI	Bit6 in BIOS Decode Enable register is set
0000F 0000h-0000F FFFFh	SPI	Bit7 in BIOS Decode Enable register is set
FECX X000h-FECX X040h	IO(x) APIC inside PCH	XX controlled via APIC Range Select (ASEL) field and APIC Enable IOAC.AE bit.
FEC1 0000h-FEC1 7FFFh	PCI Express* Port 1	PCI Express Root Port 1 I/OxAPIC Enable(PAE) set
FEC1 8000h-FEC1 FFFFh	PCI Express* Port 2	PCI Express Root Port 2 I/OxAPIC Enable(PAE) set
FEC2 0000h-FEC2 7FFFh	PCI Express* Port 3	PCI Express Root Port 3 I/OxAPIC Enable(PAE) set
FEC2 8000h-FEC2 FFFFh	PCI Express* Port 4	PCI Express Root Port 4 I/OxAPIC Enable(PAE) set
FEC3 8000h-FEC3 FFFFh	PCI Express* Port 5	PCI Express Root Port 5 I/OxAPIC Enable(PAE) set
FEC3 8000h-FEC3 FFFFh	PCI Express* Port 6	PCI Express Root Port 6 I/OxAPIC Enable(PAE) set
FEC4 0000h-FEC4 7FFFh	PCI Express* Port 7	PCI Express* Root Port 7 I/OxAPIC Enable(PAE) set
FEF0 0000h-FEFF FFFFh	SPI	uCode Patch Region Enable UCPR.UPRE is set
FEC0 0000h-FFC7 FFFFh FF80 0000h-FF87 FFFFh	SPI	Bit 8 in BIOS Decode Enable register is set
FFC8 0000h-FFCF FFFFh FF88 0000h-FF8F	SPI	Bit 9 in BIOS Decode Enable register is set
FED0 0000h-FFD7 FFFFh FF90 0000h-FF97 FFFFh	SPI	Bit 10 in BIOS Decode Enable register is set
FFD8 0000h-FFDF FFFFh FF98 0000h-FF9F FFFFh	SPI	Bit11 in BIOS Decode Enable register is set
FFE0 0000h-FFE7 FFFFh FFA0 0000h-FFA7 FFFFh	SPI	Bit 12 in BIOS Decode Enable register is set
FFE8 0000h-FFEF FFFFh FFA8 0000h-FFAF FFFFh	SPI	Bit 13 in BIOS Decode Enable register is set
FFF0 0000h-FFF7 FFFFh FFB0 0000h-FFB7 FFFFh	SPI	Bit 14 in BIOS Decode Enable register is set
FFFC 0000h-FFFFh	SPI	Always Enabled.
FFF8 0000h-FFFB FFFFh FFB8 0000h-FFBF FFFFh	SPI	Always enabled.
FF70 0000h-FF7F FFFFh FF30 0000h-FF3F FFFFh	SPI	Bit 3 in BIOS Decode Enable register is set

Memory Range	Target	Dependency / Comments
FF60 0000h-FF6F FFFFh FF20 0000h-FF2F FFFFh	SPI	Bit 2 in BIOS Decode Enable register is set
FF50 0000h-FF5F FFFFh FF10 0000h-FF1F FFFFh	SPI(	Bit 1 in BIOS Decode Enable register is set
FF40 0000h-FF4F FFFFh FF00 0000h-FF0F FFFFh	SPI	Bit 0 in BIOS Decode Enable register is set
FED0 X000h-FED0 X3FFh	HPET	BIOS determines "fixed" location which is one of four 1KB ranges where X (in the first column) is 0h,1h,2h,or 3h.
FED4 0000h-FED4 7FFFh	SPI or CSE(set by strap)	TPM and Trusted Mobile KBC
FED4 C000h-FED4 FFFFh	PCH Internal(PSE Error Handler)	Always Enable
FED5 0000h-FED5 FFFFh	CSE	Always Enable
FED6 0000h-FED6 1FFFh	XHCI	NOT positively decoded in PCH(OPI/PSF)
FED7 0000h-FED7 4FFFh	Internal Device	Security feature related
64Kb(MBAR) anywhere in 64-bit address range	XHCI	Enable via standard PCI mechanism(D20:F0)
2MB(BAR)&4Kb(BAR1) anywhere in 64-bit address range	USB extensible Device Controller Interface(xDCI)	Enable via standard PCI mechanism(D20:F1)
16kB(HDAxBA),4kB(SPCxBA) &1MB(ADSPxBA) anywhere in 64-bit address range	Converged Audio, Video Speech(cAVS) Controller	Enable via standard PCI mechanism(D20:F3)
64 KB anywhere in 4 GB range	eSPI	LPC Generic Memory Range. Enable via setting bit[0] of the LPC Generic Memory Range Register(D31:F0:offset98h).
32B(SMBBAR) anywhere in 64-bit address range	SM Bus	Enable via standard PCI mechanism(D31:F4)
2 KB anywhere above 64 KB to 4 GB range	SATA Controller(AHCI)	Enable via standard PCI mechanism(D23:F0)
Memory Base/Limit anywhere in 4 GB range	PCI Express Root Ports1-7	Enable via standard PCI mechanism(D28:F[0:6])
Pre-fetchable Memory Base/Limit anywhere in 64-bit address range	PCI Express Root Ports1-7	Enable via standard PCI mechanism(D28:F[0:6])
16B(HECIx_MMIO_BAR) anywhere in 64-bit address range	HECI #0,#1,#2,#4	Enable via standard PCI mechanism(D22:F[0:1,4:5])
16 MB(SBREG_BAR) anywhere in 64-bit address range	P2SB	Enable via standard PCI mechanism(D31:F1)
4kB(BAR & BAR1) anywhere in 64-bit address range	Intel(R) Serial I/O Controllers	Enable via standard PCI mechanism(D30:F[0:3,D25:F[0:2],D21:F[0:3],D18:F0,D16:F[1:0])
4kB(BAR & BAR1) anywhere in 64-bit	Embedded Multi Media Card(eMMC)	Enable via standard PCI mechanism(D26:F0)

Memory Range	Target	Dependency / Comments
address range	Controller	
4kB(BAR & BAR1) anywhere in 64-bit address range	Secure Digital (SD) & Secure Digital I/O Controller	Enable via standard PCI mechanism(D26:F1)
4kB(BAR & BAR1) anywhere in 64-bit address range	Universal Flash Storage(UFS) Controller	Enable via standard PCI mechanism(D18:F[5,7])

6.2. Fixed I/O Address Range Map

Hex Range	Device
020-021	Interrupt Controller
024-025	Interrupt Controller
028-029	Interrupt Controller
02C-02D	Interrupt Controller
02E-02F	Super I/O
030-031	Interrupt Controller
034-035	Interrupt Controller
038-039	Interrupt Controller
03C-03D	Interrupt Controller
040	Timer/Counter
042-043	Timer/Counter
04E-04F	Microcontroller
050	Timer/Counter
052-053	Timer/Counter
060	Keyboard Controller
061	NMI Controller
062	Microcontroller
063	NMI Controller
064	Keyboard Controller
065	NMI Controller
066	Microcontroller
067	NMI Controller
070	RTC Controller
071	RTC Controller
072	RTC Controller
073	RTC Controller

Hex Range	Device
074	RTC Controller
075	RTC Controller
076-077	RTC Controller
080	eSPI or PCIe
084-086	eSPI or PCIe
088	eSPI or PCIe
08C-08E	eSPI or PCIe
090	eSPI
092	Reset Generator
094-096	eSPI
098	eSPI
09C-09E	eSPI
0A0-0A1 0A4-0A5 0A8-0A9 0AC-0AD	Interrupt Controller
0B0-0B1	Interrupt Controller
0B2-0B3	Power Management
0B4-0B5 0B8-0B9 0BC-0BD	Interrupt Controller
200-207	Gameport Low
208-20F	Gameport High
4D0-4D1	Interrupt Controller
CF9	Reset Generator

6.3. Variable I/O Address Range Map

Hex Range	Device
Anywhere in 64 K I/O Space	ACPI
Anywhere in 64 K I/O Space	SMBus
Anywhere in 64 KB I/O Space	TCO
3 ranges in 64 KB I/O Space	Parallel Port
8 ranges in 64 KB I/O Space	Serial Port1
8 ranges in 64 KB I/O Space	Serial Port2
2 ranges in 64 KB I/O Space	Serial Port3
Anywhere in 64 K I/O Space	Floppy Disk Controller
Anywhere in 64 KB I/O Space	LPC Generic 1
Anywhere in 64 KB I/O Space	LPC Generic 2
Anywhere in 64 KB I/O Space	LPC Generic 3
Anywhere in 64 KB I/O Space	LPC Generic 4
Anywhere in 64 KB I/O Space	Serial ATA Index/Data Pair
Anywhere in 64 KB I/O Space	PCI Express Root Ports

6.4. PCI Configuration Space Map

PCH Global Device IDs

Bus Number	Device Number	Function Number	Dependency / Comments
00h	31h	00h	Enhanced Serial Peripheral Interface(eSPI) Controller
00h	31h	01h	Primary to Sideband Bridge(P2SB)
00h	31h	02h	Power Management Controller(PMC)
00h	31h	03h	Converged Audio, Video, Speech(cAVS) Controller
00h	31h	04h	System Management Bus(SMBus) Controller
00h	31h	05h	Serial Peripheral Interface(SPI) Controller for Flash & TPM
00h	31h	07h	Intel(R) Trace Hub
00h	30h	00h	Intel(R) Serial I/O: Universal Asynchronous Receiver/Transmitter(UART) Controller #0
00h	30h	01h	Intel(R) Serial I/O: UART Controller #1
00h	30h	02h	Intel(R) Serial I/O: Serial Peripheral Interface(SPI) Controller #0
00h	30h	03h	Intel(R) Serial I/O:SPI Controller #1
00h	30h	04h	Gigabit Ethernet TSN Controller
00h	30h	06h	High Precision Event Timer(HPET)

Bus Number	Device Number	Function Number	Dependency / Comments
00h	30h	07h	I/O Advanced Programmable Interrupt Controller(IOAPIC)
00h	29h	00h	Intel(R) Programmable Services Engine(Intel(R) PSE):Local Host to PSE(LH2OSE) IPC
00h	29h	01h	Intel(R) Programmable Services Engine(Intel(R) PSE):Gigabit Ethernet TSN Controller #0(RGMII:1 Gb Mode)
00h	29h	01h	Intel(R) PSE: Gigabit Ethernet TSN Controller #0(SGMII:1 Gb Mode)
00h	29h	01h	Intel(R) PSE: Gigabit Ethernet TSN Controller #0(SGMII:2.5 Gb Mode)
00h	29h	02h	Intel(R) PSE: Gigabit Ethernet Time Sensitive Networking(TSN) Controller #1(RGMII:1 Gb Mode)
00h	29h	02h	Intel(R) PSE: Gigabit Ethernet TSN Controller #1(SGMII:1 Gb Mode)
00h	29h	02h	Intel(R) PSE: Gigabit Ethernet TSN Controller #1(SGMII:2.5 Gb Mode)
00h	29h	03h	Intel(R) PSE: Direct Memory Access (DMA) Controller #0
00h	29h	04h	Intel(R) PSE: DMA Controller #1
00h	29h	05h	Intel(R) PSE: DMA Controller #2
00h	29h	06h	Intel(R) PSE: Pulse Width Modulation(PWM) Controller
00h	29h	07h	Intel(R) PSE: Analog to Digital Converter(ADC)
00h	28h	00h	PCI Express*(PCIe*) Root Port #0(PCIe 0,Single VC)
00h	28h	01h	PCIe* Root Port #1(PCIe 0,Single VC)
00h	28h	02h	PCIe* Root Port #2(PCIe 0,Single VC)
00h	28h	03h	PCIe* Root Port #3(PCIe 0,Single VC)
00h	28h	04h	PCIe* Root Port #4(PCIe 0,Multi VC)
00h	28h	05h	PCIe* Root Port #5(PCIe 0, Multi VC)
00h	28h	06h	PCIe* Root Port #6(PCIe 0, Multi VC)
00h	27h	00h	Intel(R) PSE: Inter-Integrated Circuit(I2C) Controller #0
00h	27h	01h	Intel(R) PSE: I2C Controller #1
00h	27h	02h	Intel(R) PSE: I2C Controller #2
00h	27h	03h	Intel(R) PSE: I2C Controller #3
00h	27h	04h	Intel(R) PSE: I2C Controller #4
00h	27h	05h	Intel(R) PSE: I2C Controller #5
00h	27h	06h	Intel(R) PSE: I2C Controller #6
00h	26h	00h	Embedded Multi Media Card (eMMC) Controller
00h	26h	01h	Secure Digital (SD) & Secure Digital I/O Controller
00h	26h	03h	Intel(R) Safely Island(Intel(R) SI) Controller
00h	25h	00h	Intel(R) Serial I/O: Inter-Integrated Circuit(I2C) Controller #4
00h	25h	01h	Intel(R) Serial I/O I2C Controller #5
00h	25h	02h	Intel(R) Serial I/O: Universal Asynchronous Receiver/Transmitter(UART) Controller #2
00h	24h	00h	Intel(R) Programmable Services Engine(Intel(R) PSE):I2C Controller #7
00h	24h	01h	Intel(R) PSE: Controller Area Network (CAN) Controller #0
00h	24h	02h	Intel(R) PSE: CAN Controller #1
00h	24h	03h	Intel(R) PSE: Quadrature Encoder Peripheral,(QEP) Controller #0

Bus Number	Device Number	Function Number	Dependency / Comments
00h	24h	04h	Intel(R) PSE:QEP Controller #1
00h	24h	05h	Intel(R) PSE: QEP Controller #2
00h	24h	06h	Intel(R) PSE: QEP Controller #3
00h	22h	00h	Intel(R)
00h	22h	01h	Intel(R) CSE:HECI #1
00h	22h	04h	Intel(R) CSE:HECI #2
00h	22h	05h	Intel(R) CSE:HECI #3
00h	21h	00h	Intel(R) Serial I/O: Inter-Integrated Circuit(I2C) Controller #0
00h	21h	01h	
00h	21h	02h	Intel(R) Serial I/O:I2C Controller #1
00h	21h	03h	Intel(R) Serial I/O:I2C Controller #2
00h	21h	07h	Intel(R) Serial I/O:I2C Controller #3
00h	19h	00h	Intel(R) PSE: Serial Peripheral Interface(SPI) Controller #0
00h	19h	01h	Intel(R) PSE: SPI Controller #1
00h	19h	02h	Intel(R) PSE: SPI Controller #2
00h	19h	03h	Intel(R) PSE: SPI Controller #3
00h	19h	04h	Intel(R) PSE: General Purpose Input Output(GPIO) Controller #0
00h	19h	05h	Intel(R) PSE: General Purpose Input Output(GPIO) Controller #1
00h	18h	00h	Intel(R) Serial I/O:SPI Controller #2
00h	18h	03h	Intel(R) Converged Security Engine(Intel(R) CSE):UMA Access
00h	18h	04h	Intel(R) CSE: Intel(R) PTT DMA Controller
00h	18h	05h	Universal Flash Storage(UFS) Controller #0
00h	18h	07h	UFS Controller #1
00h	17h	00h	Intel(R) PSE: Universal Asynchronous Receiver/Transmitter(UART) Controller#0
00h	17h	01h	Intel(R) PSE: UART Controller #1
00h	17h	02h	Intel(R) PSE: UART Controller #2
00h	17h	03h	Intel(R) PSE :UART Controller #3
00h	17h	04h	Intel(R) PSE: UART Controller #4
00h	17h	05h	Intel(R) PSE: UART Controller #5
00h	17h	06h	Intel(R) PSE: Inter-Integrated Circuit Sound(I2S) Controller #0
00h	17h	07h	Intel(R) PSE: I2S Controller #1
00h	16h	00h	Intel(R) Serial I/O: Inter-Integrated Circuit(I2C) Controller #6
00h	16h	01h	Intel(R) Serial I/O: I2C Controller #7
00h	16h	05h	Integrated Error Handler(IEH)

6.5. PCI Interrupt Routing Map

INT Line	xHCI Controller	SATA Controller	SMBus Controller
Int0	INTA:16	INTA:16	INTA:16
Int1	INTB:17		
Int2	INTC:18		
Int3	INTD:19		

INT Line	PCIe Port 1	PCIe Port 2	PCIe Port 3	PCIe Port 4	PCIe Port 5	PCIe Port 6	PCIe Port 7
Int0	INTA:16	INTB:17	INTC:18	INTD:19	INTA:16	INTB:17	INTC:18
Int1	INTB:17	INTC:18	INTD:19	INTA:16	INTB:17	INTC:18	INTD:19
Int2	INTC:18	INTD:19	INTA:16	INTB:17	INTC:18	INTD:19	INTA:16
Int3	INTD:19	INTA:16	INTB:17	INTC:18	INTD:19	INTA:16	INTB:17

6.6. SMBus Address Table

Device	Address
PTN3460	C0h

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 Access Level	CPU Configuration Power & Performance Graphics Configuration AMI Graphic Output Protocol Policy Power Management System Management Thermal Management Watchdog Timer Super IO Configuration Miscellaneous USB Configuration Serial Port Console Redirection Network Stack Configuration Trusted Computing	System Agent (SA) Configuration PCH-IO Configuration	Setup Administrator Password User Password Secure Boot	Boot Configuration FIXED BOOT ORDER Priorities UEFI USB Key Drive BBS Priorities	Save Change and Exit Discard Changes and Exit Save Changes and Reset Discard Changes and Reset Save Options Boot Override

7.2. Main

7.2.1. Main > BIOS Information

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

7.2.2. Main > System Information

Feature	Options	Description
Project Name	Info only	Display Project Name.
CPU Board version	Info only	Display CPU Board Version.
CPU Board String	Info only	Display CPU Board String.
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 SKU Version

7.2.3. Main > Board Information

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

7.2.4. Main > System Date/Time

Feature	Options	Description
System Date	Info only	
System Time	Info only	

7.2.5. Main > Access Levl

Feature	Options	Description
Access Level	Info only	

7.3. Advanced

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

7.3.1. Advanced > CPU Configuration

Feature	Options	Description
CPU Configuration	Info only	
Type	Info only	Socket Specific CPU Information.
ID	Info only	Display Microcode Patch.
Speed	Info only	Display Max CPU speed.
Stepping	Info only	Display Min CPU stepping.
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 VMX support info.
SMX/TXT	Info only	Display SMX/TXT support info.
Intel 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	Number of cores to enable in each processor package.

7.3.2. Advanced > Power & Performance

Feature	Options	Description
CPU – Power Management Control	Submenu	CPU- Power Management Control Options
GT – Power Management Control	Submenu	GT- Power Management Control

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

Feature	Options	Description
CPU – Power Management Control	Info only	
P0 Fused Max Core Ratio	Info only	
P1 Fused Max Core Ratio	Info only	
P2 Fused Max Core Ratio	Info only	
P3 Fused Max Core Ratio	Info only	
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 features. 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.
HwP Autononmous 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 =

Feature	Options	Description
		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 to1. 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. Disabled: Disable HDC Enabled: Can be enabled by OS if OS native support is available.
View/Configure Turbo Options	Submenu	View/Configure Turbo Options
CPU VR Settings	Submenu	CPU VR Settings
Platform PL1 Enable	**Disabled** Enabled	Enable/Disable Platform Power Limit 1 programming. If this option is enabled, it activates the PL1 value to be used by the processor to limit the average power of given time window.
Platform PL2 Enable	**Disabled** Enabled	
Power Limit 4 override	**Disabled** Enabled	Enable/Disable Power Limit 4 override. If this option is disabled, BIOS will leave the default values for Power Limit 4.
C states	Disabled **Enabled**	Enable/Disable CPU Power Management. Allows CPU to go to C states when it's not 100% utilized.
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	Disbled **C1**	Configure C-State Un-demotion
Package C-State Demotion	Disabled	Package C-State Demotion

Feature	Options	Description
	Enabled	
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**	Maximum Package C State Limit Setting. CPU Default: Leaves to Factory default value. Auto: Initializes to deepest available Package C State Limit.
C6/C7 Short Latency Control(MSR 0x60B)	Info only	
Time Unit	1 ns 32ns **1024ns** 32768 ns 1048576 ns 33554432 ns	Unit of measurement for IRTL value – bits [12:10]
Latency	**0**-1023	Interrupt Response Time Limit value- bits [9:0], Enter 0-1023
C6/C7 Long Latency Control(MSR 0x60C)	Info only	

Feature	Options	Description
Time Unit	1 ns 32ns **1024ns** 32768 ns 1048576 ns 33554432 ns	Unit of measurement for IRTL value – bits [12:10]
Latency	**0**-1023	Interrupt Response Time Limit value- bits [9:0], Enter 0-1023
C8 Latency Control(MSR 0x633)		
Time Unit	1 ns 32ns **1024ns** 32768 ns 1048576 ns 33554432 ns	Unit of measurement for IRTL value – bits [12:10]
Latency	**0**-1023	Interrupt Response Time Limit value- bits [9:0], Enter 0-1023
C9 Latency Control(MSR 0x634)		
Time Unit	1 ns 32ns **1024ns** 32768 ns 1048576 ns 33554432 ns	Unit of measurement for IRTL value – bits [12:10]
Latency	**0**-1023	Interrupt Response Time Limit value- bits [9:0], Enter 0-1023
C10 Latency Control(MSR 0x635)		
Time Unit	1 ns 32ns **1024ns** 32768 ns 1048576 ns	Unit of measurement for IRTL value – bits [12:10]

Feature	Options	Description
	33554432 ns	
Latency	**0**-1023	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	
EC Turbo Control Mode	**Disabled** Enabled	Enable/Disable EC Turbo Control mode
Energy Performance Gain	**Disabled** Enabled	Enable/Disable Energy Performance Gain.
EPG DIMM Idd3N	26	Active standby current (Idd3N) in milliamps from datasheet. Must be calculated on a per DIMM basis.
EPG DIMM Idd3P	11	Active power-down current(Idd3P) in milliamps from datasheet. Must be calculated on a per DIMM basis.
Power Limit 3 Settings	Submenu	
CPU Lock Configuration	Submenu	CPU Lock Configuration

7.3.2.1.1. Advanced > Power & Performance > CPU – Power Management Control > View/Configure Turbo Options

Feature	Options	Description
Current Turbo Settings	Info only	
Max Turbo Power Limit	Info only	
Min Turbo Power Limit	Info only	
Package TDP Limit	Info only	
Power Limit 1	Info only	
Power Limit 2	Info only	
1-core Turbo Ratio	Info only	
2-core Turbo Ratio	Info only	
3-core Turbo Ratio	Info only	
4-core Turbo Ratio	Info only	
Energy Efficient P-state	Disabled **Enabled**	Enable/Disable Energy Efficient P-state feature. When set to 0, will disable access to ENERGY_PERFORMANCE_BIAS MSR and CPUID Function 6 ECX[3] will read 0 indicating no support for Energy Efficient policy setting. When set to 1 will enable access to ENERGY_PERFORMANCE_BIAS MSR
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.
Power Limit 1 Override	**Disabled** Enabled	Enable/Disable Power Limit 1 override. If this option is disabled, BIOS will program the default values for Power Limit 1 and Power Limit 1 Time Window.
Power Limit 2 Override	Disabled **Enabled**	Enable/Disable Power Limit 2 override. If this option is disabled, BIOS will program the default values for Power Limit 2.
Power Limit 2	0	Power Limit 2 value in milliWatts. BIOS will round to

Feature	Options	Description
		the nearest 1/8W when programming. If the value is 0, BIOS will program this value as 1.25*TDP. For 12.50W, enter 12500. Processor applies control policies such that the package power does not exceed this limit.
1-Core Ratio Limit Override	19	1-Core Ratio Limit with range 0 to 83. The Minimum range may vary between Processors. This 1-Core Ratio Limit Must be greater than or equal to 2-Core Ratio Limit, 3-Core Ratio Limit, 4-Core Ratio Limit.
2-Core Ratio Limit Override	19	2-Core Ratio Limit with range 0 to 83. The Minimum range may vary between Processors. This 2-Core Ratio Limit Must be Less than or equal to 1-Core Ratio Limit.
3-Core Ratio Limit Override	19	3-Core Ratio Limit with range 0 to 83. The Minimum range may vary between Processors. This 3-Core Ratio Limit Must be Less than or equal to 1-Core Ratio Limit.
4-Core Ratio Limit Override	19	4-Core Ratio Limit with range 0 to 83. The Minimum range may vary between Processors. This 4-Core Ratio Limit Must be Less than or equal to 1-Core 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.

7.3.2.1.2. Advanced > Power & Performance > CPU – Power Management Control > CPU VR Settings

Feature	Options	Description
CPU VR Settings	Info only	
PSYS Slope	0	
PSYS Offset	0	
PSYS PMax Power	+ -	
Acoustic Noise Settings	Submenu	Configure Acoustic Noise Settings for IA, GT and SA domains
VccIn VR Settings	Submenu	VccIn VR Settings
RFI Settings	Submenu	RFI Settings

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

Feature	Options	Description
Custom P-state Table	Info only	
Number of P states	0	Sets the number of custom P-states. At least 2 states must be present.

7.3.2.1.4. Advanced > Power & Performance > CPU – Power Management Control > CPU Lock Configuration

Feature	Options	Description
CFG Lock	Disabled	Configure MSR 0xE2[15], CFG Lock bit

Feature	Options	Description
	Enabled	
Overclocking Lock	**Disabled** Enabled	Enable/Disable Overclocking Lock (BIT 20) in FLEX_RATIO(194) MSR

7.3.2.2. Advanced > Power & Performance > GT – Power Management Control

Feature	Options	Description
GT – Power Management Control	Info only	
RC6(Render Standby)	Disabled **Enabled**	
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	Maximum GT frequency limited by the user. Choose between 400MHz (RPN) and 400MHz (RP0). Value beyond the range will be clipped to min/max supported by SKU

Feature	Options	Description
	1150Mhz 1200Mhz	
Disable Turbo GT frequency	Enabled **Disabled**	Enabled: Disables Turbo GT frequency. Disabled: GT frequency is not limited

7.3.3. Advanced > Graphics Configuration

Feature	Options	Description
Nxp configuration	Info Only	
Data format and Color Depth	VESA 24 bpp JEIDA 24 bpp **JEIDA/vesa 18 bpp**	Data format and Color Depth select
LVDS Output Mode	Dual LVDS bus **Single LVDS bus**	Single/Dual mode select
DE Polarity	**Active High** Active Low	DE Polarity select
Vsync Polarity	**Active High** Active Low	Vsync Polaity select
Hsync Polarity	**Active High** Active Low	Hsync 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

Feature	Options	Description
LFP Panel Type	**VBIOS Default** 640x480 800x600 1024x768 1280x1024 1400x1050 LVDS1 1400x1050 LVDS2 1600x1200 1366x768 1680x1050 1920x1200 1440x900 1600x900 1024x768 1280x800 1920x1080 2048x1536	Select LFP panel used by Internal Graphics Device by selecting the appropriate setup item.
LVDS Backlight Mode	**EC Mode** GTT Mode	Select LVDS Backlight control function.
LVDS Backlight	Submenu	
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

7.3.3.1. Advanced > Graphics Configuration > LVDS Backlight

Feature	Options	Description
LVDS Backlight	Info Only	
LVDS Backlight Brightness	0-**255**	A change takes effect immediately. The value range starts by 0 and ends by 255.

7.3.4. Advanced> AMI Graphic Output Protocol Policy

Feature	Options	Description
Intel (R) Graphics Controller	Info Only	
Intel (R) GOP Driver	Info Only	
Output Select	DP1[ACTIVE Current]	Output Interface

7.3.5. Advanced > Power Management

Feature	Options	Description
Power Management	Info Only	
Enable ACPI Auto Configuration	**Disabled** Enabled	Enables or Disables BIOS ACPI Auto Configuration

7.3.6. Advanced > System Management

Feature	Options	Description
System Management	Info Only	
Version	Info Only	Display SEMA Module Version.

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

7.3.6.1. Advanced > System Management > SEMA Flags

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

7.3.7. Advanced > Thermal Management

Feature	Options	Description
Thermal Management	Info Only	
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.

Feature	Options	Description
Watchdog ACPI Event Shutdown	**Disabled** Enabled	Watchdog ACPI Event Shutdown Enabled/Disabled
Temperature and Fan Speed	Submenu	

7.3.7.1. 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
Min	Info Only	Display Min Board Temperature
Max	Info Only	Display Max Board Temperature
CPU Fan Speed	Info Only	Display CPU Fan Speed
Smart Fan	Submenu	

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

Feature	Options	Description
Smart Fan	Info Only	
CPU Smart Fan Temperature Source	**CPU Sensor** Board Sensor	CPU Smart Fan Temperature Source
Trigger Point 1/2/3/4	Info Only	
Trigger Temperature	**40/55/70/85**	Trigger Temperature
PWM Level	**25/50/75/100**	PWM Level

7.3.8. 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 druing 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	**30**	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.

7.3.9. 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.

7.3.9.1. Advanced > Super IO Configuration > IT5121E Super IO Configuration

Feature	Options	Description
IT5121E Super IO Configuration	Info only	
Serial Port 1/2 Configuration	Submenu	Set Parameters of Serial Port 1/2
Serial Port 1/2 Configuration	Info only	
Serial Port	Disableed **Enabled**	Enable or Disable Serial Port (COM).
Device Settings	Info Only	Display IO / IRQ information of COM Port.
Change Settings	**Auto** IO=3F8h/2F8h; IRQ=4; IO=3F8h; IRQ=3,4,5,6,7,10,11,12 IO=2F8h; IRQ=3,4,5,6,7,10,11,12 IO=3E8h; IRQ=3,4,5,6,7,10,11,12 IO=2E8h; IRQ=3,4,5,6,7,10,11,12	Select an optimal setting for Super IO Device.
Change Settings	**Normal** High Speed	Select an optimal settings for Super IO Device

7.3.9.2. Advanced > Super IO Configuration > W83627DHGSEC Super IO Configuration

Feature	Options	Description
Serial Port 1/2 Configuration	Submenu	Set Parameters of Serial Port 2 (COMB).
Serial Port 1/2 Configuration	Info only	
Serial Port	Disableed **Enabled**	Enable or Disable Serial Port (COM).
Device Settings	Info Only	Display IO / IRQ information of COM Port.
Change Settings	**Auto** IO=248h; IRQ=11; 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	Select an optimal setting for Super IO Device.

7.3.10. Advanced > Serial Console Redirection

Feature	Options	Description
COM1	Info only	
Console Redirection	Enabled **Disabled**	Console Redirection Enable or Disable.
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. The item will be lunched before enable Console Redirection.

Feature	Options	Description
COM2	Info only	
Console Redirection	Enabled **Disabled**	Console Redirection Enable or Disable.
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. The item will be lunched before enable Console Redirection.
COM3	Info only	
Console Redirection	Enabled **Disabled**	Console Redirection Enable or Disable.
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. The item will be lunched before enable Console Redirection.
COM4	Info only	
Console Redirection	Enabled **Disabled**	Console Redirection Enable or Disable.
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. The item will be lunched before enable Console Redirection.
Legacy Console Redirection	Info only	
Legacy Console Redirection Settings	Submenu	Legacy Console Redirection Settings

7.3.10.1. Advanced > Serial Console Redirection > Console Redirection Settings (w/ COM1 enabled)

Feature	Options	Description
COM1	Info only	
Console Redirection Settings	Info only	
Terminal Type	VT100 VT100+ VT-UTF8 **ANSI**	Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100+: Extends VT100 to support color, function keys, etc. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.
Bits per second	9600 19200 38400 57600 **115200**	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Data Bits	7 **8**	Data Bits
Parity	**None** Even Odd Mark Space	A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the num of 1's in the data bits is even. Odd: parity bit is 0 if num of 1's in the data bits is odd. Mark: parity bit is always 1. Space: Parity bit is always 0. Mark and Space Parity do not allow for error detection. They can be used as an additional data bit.
Stop Bits	**1** 2	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.
Flow Control	**None** Hardware RTS/CTS	Flow control can prevent data loss from buffer over-flow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow.

Feature	Options	Description
		Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.
VT-UTF8 Combo Key Support	**Enabled** Disabled	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	Enabled **Disabled**	On Legacy OS, the Number of Rows and Columns supported redirection
Legacy OS Redirection Resolution	**80x24** 80x25	On Legacy OS, the Number of Rows and Columns supported redirection
Putty KeyPad	**VT100** Intel Linux XTERMR6 SCO ESCN VT400	Select FunctionKey and KeyPad on Putty.
Redirection After BIOS POST	**Always Enable** BootLoader	When Bootloader is selected, then Legacy Console Redirection is disabled before booting to legacy OS. When Always Enable is selected, then Legacy Console Redirection is enabled for legacy OS. Default setting for this option is set to Always Enable.

7.3.10.2. Advanced > Serial Console Redirection > Console Redirection Settings (w/ COM2 enabled)

Feature	Options	Description
COM2	Info only	
Console Redirection Settings	Info only	
Terminal Type	VT100 VT100+ VT-UTF8 **ANSI**	Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100+: Extends VT100 to support color, function

Feature	Options	Description
		keys, etc. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.
Bits per second	9600 19200 38400 57600 **115200**	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Data Bits	7 **8**	Data Bits
Parity	**None** Even Odd Mark Space	A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the num of 1's in the data bits is even. Odd: parity bit is 0 if num of 1's in the data bits is odd. Mark: parity bit is always 1. Space: Parity bit is always 0. Mark and Space Parity do not allow for error detection. They can be used as an additional data bit.
Stop Bits	**1** 2	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.
Flow Control	**None** Hardware RTS/CTS	Flow control can prevent data loss from buffer over-flow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.
VT-UTF8 Combo Key Support	**Enabled** Disabled	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	Enabled **Disabled**	On Legacy OS, the Number of Rows and Columns supported redirection

Feature	Options	Description
Legacy OS Redirection Resolution	**80x24** 80x25	On Legacy OS, the Number of Rows and Columns supported redirection
Putty KeyPad	**VT100** Intel Linux XTERMR6 SCO ESCN VT400	Select FunctionKey and KeyPad on Putty.
Redirection After BIOS POST	**Always Enable** BootLoader	When Bootloader is selected, then Legacy Console Redirection is disabled before booting to legacy OS. When Always Enable is selected, then Legacy Console Redirection is enabled for legacy OS. Default setting for this option is set to Always Enable.

7.3.10.3. Advanced > Serial Console Redirection > Console Redirection Settings (w/ COM3 enabled)

Feature	Options	Description
COM3	Info only	
Console Redirection Settings	Info only	
Teriminal Type	VT100 VT100+ VT-UTF8 **ANSI**	Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100+: Extends VT100 to support color, function keys, etc. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.
Bits per second	9600 19200 38400 57600 **115200**	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Data Bits	7 **8**	Data Bits

Feature	Options	Description
Parity	**None** Even Odd Mark Space	A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the num of 1's in the data bits is even. Odd: parity bit is 0 if num of 1's in the data bits is odd. Mark: parity bit is always 1. Space: Parity bit is always 0. Mark and Space Parity do not allow for error detection. They can be used as an additional data bit.
Stop Bits	**1** 2	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.
Flow Control	**None** Hardware RTS/CTS	Flow control can prevent data loss from buffer over-flow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.
VT-UTF8 Combo Key Support	**Enabled** Disabled	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	Enabled **Disabled**	On Legacy OS, the Number of Rows and Columns supported redirection
Legacy OS Redirection Resolution	**80x24** 80x25	On Legacy OS, the Number of Rows and Columns supported redirection
Putty KeyPad	**VT100** Intel Linux XTERMR6 SCO ESCN VT400	Select FunctionKey and KeyPad on Putty.

Feature	Options	Description
Redirection After BIOS POST	**Always Enable** BootLoader	When Bootloader is selected, then Legacy Console Redirection is disabled before booting to legacy OS. When Always Enable is selected, then Legacy Console Redirection is enabled for legacy OS. Default setting for this option is set to Always Enable.

7.3.10.4. Advanced > Serial Console Redirection > Console Redirection Settings (w/ COM4 enabled)

Feature	Options	Description
COM4	Info only	
Console Redirection Settings	Info only	
Terminal Type	VT100 VT100+ VT-UTF8 **ANSI**	Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100+: Extends VT100 to support color, function keys, etc. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.
Bits per second	9600 19200 38400 57600 **115200**	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Data Bits	7 **8**	Data Bits
Parity	**None** Even Odd Mark Space	A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the num of 1's in the data bits is even. Odd: parity bit is 0 if num of 1's in the data bits is odd. Mark: parity bit is always 1. Space: Parity bit is always 0. Mark and Space Parity do not allow for error detection. They can be used as an

Feature	Options	Description
		additional data bit.
Stop Bits	**1** 2	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.
Flow Control	**None** Hardware RTS/CTS	Flow control can prevent data loss from buffer over-flow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.
VT-UTF8 Combo Key Support	**Enabled** Disabled	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	Enabled **Disabled**	On Legacy OS, the Number of Rows and Columns supported redirection
Legacy OS Redirection Resolution	**80x24** 80x25	On Legacy OS, the Number of Rows and Columns supported redirection
Putty KeyPad	**VT100** Intel Linux XTERMR6 SCO ESCN VT400	Select FunctionKey and KeyPad on Putty.
Redirection After BIOS POST	**Always Enable** BootLoader	When Bootloader is selected, then Legacy Console Redirection is disabled before booting to legacy OS. When Always Enable is selected, then Legacy Console Redirection is enabled for legacy OS. Default setting for this option is set to Always Enable.

7.3.10.5. Advanced > Serial Console Redirection > Legacy Console Redirection Settings

Feature	Options	Description
Legacy Serial Redirection Port	**COM1** COM2 COM3 COM4	Select a COM port to display redirection of Legacy OS and Legacy OPROM Messages

7.3.11. Advanced > Miscellaneous

Feature	Options	Description
Miscellaneous	Info Only	
Power Supply Unit	Emulate AT Mode **ATX Mode**	Select Emulation AT or ATX function. If this option set to [Emulation AT], BIOS will report no suspend functions (S3 & S4) to ACPI OS. In windows XP, it will make OS show shutdown message during system shutdown. ATX: OS will turn off system power when shutdown.
I2C Speed Control	**100 kbps** 400 kbps	I2C Speed Control
Smart Battery Function	**Disabled** Enabled Auto	Enable/Disable Smart Battery function. Auto: disable Smart Battery function if charger IC not be detected.
SD Card/GPIO Mode	**GPIO** SD Card	Select SD Card or GPIO function.
WOL From S5	**ON** OFF	Select SMBUS Routine

7.3.12. 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 availiable 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 rime-out	1 sec 5sec 10sec **20 sec**	The time-out value for Control, Bulk, and Interrupt transfers.
Device reset time-out	10 sec **20 sec** 30 sec 40 sec	USB mass storage device Start Unit command time-out.
Device power-up delay	**Auto** Manual	Maximum time the device will take before it properly reports itself to the Hot Controller. 'Auto' uses default value: for a Root po\rt it is 100 ms, for a Hub port the delay is taken form Hub descriptor.

7.3.13. Advanced > Network Stack Configuration

Feature	Options	Description
Network Stack	**Disable** Enable	Enable / Disable UEFI Network Stack.

7.3.14. Advanced > Trusted Computing

Feature	Options	Description
TPM20 Device Found	Info Only	
Security Device Support	**Disable** Enable	Enables or Disable BIOS support for security device. OS will not show Security Device. TCG EFI protocol and available.

7.4. Chipset

7.4.1. Chipset > System Agent (SA) Configuration

Feature	Options	Description
Memory Configuration	Submenu	Memory Configuration Parameters
Graphics Configuration	Submenu	Graphics Configuration
VT-D	Disabled **Enabled**	VT-d capability
GNA Device	Disabled **Enabled**	Enable/Disable SA GNA Device.
Above 4GB MMIO BIOS assignment	Disabled **Enabled**	Enable/Disable above 4GB Memory / Mapped I/O BIOS assignment. This is enabled automatically when Aperture Size is set to 2048MB.

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

Feature	Options	Description
Memory Thermal Configuration	Submenu	Memory Thermal Configuration
Memory Training Algorithms	Submenu	Enable/Disable Memory Training Algorithms.
Memory Configuration	Info Only	
Memory RC Version	Info Only	
Memory Data Rate	Info Only	
Memory Timings (tCL-tRCD-tRP-tRAS)	Info Only	
Channel 0 Slot 0	Info Only	
Channel 0 Slot 1	Info Only	

Feature	Options	Description
Channel 1 Slot 0	Info Only	
Size	Info Only	
Number of Ranks	Info Only	
Manufacturer	Info Only	
Channel 1 Slot 1	Info Only	
Memory ratio/reference clock options moved to Overclock->Memory->Custom Profile menu	Info Only	
MRC ULT Safe Config	**Disabled** Enabled	MRC ULT Safe Config for P0
Safe Mode Support	**Disabled** Enabled	Safe Mode enable support. Option will be used for changes/WAs that may affect an stable MRC
Maximum Memory Frequency	**Auto** 1067 1200 1333 1400 ……. 4267	Maximum Memory Frequency in Mhz. Must divide by 133 or 100 according to the refclk. In Gear2 must divide by 266 or 200. Lowest Gear2 speed is 2133
HOB Buffer Size	Auto 1B 1KB Max (assuming 63KB total HOB size)	Size to set HOB Buffer
Max TOLUD	Dynamioc 1 GB 1.25 GB …… 3.5GB	Maximum Value of TOLUD. Dynamic assignment would adjust TOLUD automatically based on largest MMIO length of installed graphic controller
SA GV	Disabled Fixed Low	System Agent Geyserville. Can disable, fix to a specific point, or enable frequency switching.

Feature	Options	Description
	Fixed Mid Fixed High **Enabled**	
DDR Speed Control	Auto Manual	DDR Frequency and Gear1 / Gear2 control for all SAGV points
Retrain on Fast Fail	Disabled **Enabled**	Restart MRC in Cold mode if SW MemTest fails during Fast flow. Default = Enabled
DDR4_1DPC	Disabled Enabled on DIMM0 only Enabled on DIMM1 only **Enabled**	DDR4 1DPC performance feature for 2R DIMMs. Can be enabled on DIMM0 or DIMM1 only, or on both
Enable RH Prevention	**Disabled** Enabled	Actively prevent Row Hammer
REFRESH_PANIC_WM	9	Range 1-9, default 9
REFRESH_HP_WM	8	Range 1-9, default 8
Exit On Failure (MRC)	Disabled **Enabled**	Exit On Failure for MRC training steps
Enable/Disable IED (Intel Enhanced Debug)	Enabled **Disabled**	Intel Enhanced Debug requires 4MB Runtime memory
Ch Hash Support	Disabled **Enabled**	Enable/Disable Channel Hash Support. NOTE: ONLY if Memory interleaved Mode
Ch Hash Mask	12492	Set the BIT(s) to be included in the XOR function. NOTE BIT mask corresponds to BITS [19:6}
Ch Hash Interleaved Bit	**BIT8**	Select the BIT to be used for Channel Interleaved mode. NOTE: BIT7 will interlace the channels at a 2 cache line granularity, BIT8 at 4 and BIT9 at 8
Extended Bank Hashing	Disabled **Enabled**	Extended Bank Hashing
Per Bank Refresh	Disabled **Enabled**	Enables and Disables the per bank refresh. This only impacts memory technologies that support PBR: LPDDR3, LPDDR4.

Feature	Options	Description
Power Down Mode	**Auto** No Power Down APD PPD-DLLoff	CKE Power Down Mode Control
Page Close Idle Timeout	**Enabled** Disabled	Page Close Idle Timeout Control
Memory Scrambler	Disabled **Enabled**	Enable/Disable Memory Scrambler support.
Force ColdReset	Enabled **Disabled**	Force ColdReset OR Choose MrcColdBoot mode, when Coldboot is required during MRC execution. Note: If ME 5.0MB is present, ForceColdReset is required!
Channel 0 DIMM Control	**Enable both DIMMs** Disable DIMM0 Disable DIMM1 Disable both DIMMS	Channel 0 DIMM Control Support - Enable or Disable Dimms on Channel 0.
Channel 1 DIMM Control	**Enable both DIMMs** Disable DIMM0 Disable DIMM1 Disable both DIMMS	Channel 1 DIMM Control Support - Enable or Disable Dimms on Channel 1.
Force Single Rank	**Disabled** Enabled	When enabled, only Rank 0 will be used in each DIMM
Force Single Sub Channel	**Disabled** Enabled	When enabled, single Sub channel will be used in each DIMM
MRC TASK Debug Print Enable	**0**	This enable debug print for specific MRC task. Please consult value from BWG
Memory Remap	**Enabled** Disabled	Enable/Disable Memory Remap above 4GB
Time Measure	**Disabled** Enabled	Enable/Disable printing of the time it takes to execute MRC.
DLL Weak Lock Support	Disabled	Enable/Disable Dll Weaklock support

Feature	Options	Description
	Enabled	
Fast Boot	Disabled **Enabled**	Enable/Disable fast path thru the MRC
Train On Warm boot	**Disabled** Enabled	Enable/Disable training on warm boot
Rank Margin Tool Per Task	**Disabled** Enabled	Enables/Disables RMT running at every major training step
Training Tracing	**Disabled** Enabled	Enables/Disables printing of the current trained state at every major training step.
Lpddr Mem WL Set	Set A **Set B**	Only applicable to LPDDR, Memory Write Latency Set selection (A is default, B will be used if memory devices support it)
BDAT Memory Test Type	**Rang Margin Tool Rank**	Indicates the type of Memory Training data to populate into the BDAT ACPI table.
Rank Margin Tool Loop Count	**0**	Specifies the Loop Count to be used during Rank Margin Tool Testing. 0 - AUTO
Low Supply for LPDDR4 Data	**Disabled** Enabled	Low Supply for LPDDR4 Data
Low Supply for LPDDR4 Clock/Command/Control	**Disabled** Enabled	Low Supply for LPDDR4 Clock/Command/Control
Memory Test on Warm Boot	Disabled **Enabled**	Enable Or Disable Base Memory Test Run on Warm Boot

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

Feature	Options	Description
Graphics Configuration	Info Only	
Primary Display	**Auto** IGFX	Select which of IGFX/PEG/PCIe Graphics device should be Primary Display Or select HG for Hybrid

Feature	Options	Description
	PEG PCIe	Gfx.
External Gfx Card Primary Display Configuration	Submenu	External Gfx Card Primary Display Configuration
Internal Graphics	**Auto** Disabled Enabled	Keep IGFX enabled based on the setup options.
GTT Size	2MB 4MB **8MB**	Select the GTT Size
Aperture Size	128MB **256MB** 512MB 1024MB 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

7.4.1.2.1 Advanced > System Agent (SA) Configuration > Graphics Configuration > External Gfx Card Primary Display Configuration

Feature	Options	Description
External Gfx Card Primary Display Configuration	Info Only	
Primary PCIE	**Auto**	Select Auto/PCIE1/PCIE2/PCIE3/PCIE4/PCIE5/PCIE6/PCIE7 of D28:F0/F1/F2/F3/F4/F5/F6/F7, PCIE8/PCIE9/PCIE10/PCIE11/PCIE12/PCIE13/PCIE14/PCIE15 of D29:F0/F1/F2/F3/F4/F5/F6/F7, PCIE16/PCIE17/PCIE18/PCIE19 of D27:F0/F1/F2/F3, Graphics device should be Primary PCIE.

7.4.2. Chipset > PCH-IO Configuration

Feature	Options	Description
PCH-IO Configuration	Info Only	Memory Configuration Parameters
PCI Express Configuration	Submenu	PCI Express Configuration setting
SATA Configuration	Submenu	SATA Device Options Settings
USB Configuration	Submenu	USB Configuration settings
Security Configuration	Submenu	Security Configuration setting
HD Audio Configuration	Submenu	HD Audio Subsystem Configuration Settings
SerialIo Configuration	Submenu	SerialIo Configuration Settings
SCS Configuration	Submenu	Storage and Communication Subsystem (SCS) Configuration
PSE Configuration	Submenu	Programmable Service Engine (PSE) Configuration
TSN GBE Configuration	Submenu	Time Sensitive Network GBE Configuration

Feature	Options	Description
Enhance Port 80h LPC Decoding	Disabled **Enabled**	Support the word/dword decoding of port 80h behind LPC
Enable TCO Timer	**Disabled** Enabled	Enable/Disable TCO timer. When disabled, it disables PCH ACPI timer, stops TCO timer, and ACPI WDAT table will not be published.
Pcie Pll SSC	**Auto**	Pcie Pll 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.

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

Feature	Options	Description
PCI Express Configuration	Info Only	
DMI Link ASPM Control	**Disabled** L0s L1 L0sL1 Auto	The control of Active State Power Management of the DMI Link.
PCIE Ports 1-4 Configuration	**4x1 Port** 1x2 2x1 Port 2x2 Port 1x4 Port	To configure PCI-E Port 1-4 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)
Port8xh Decode	**Disabled** Enabled	
Peer Memory Write Enable	**Disabled** Enabled	
Compliance Test Mode	**Disabled** Enabled	

Feature	Options	Description
PCH PCI Express Clock Gating	**Platform-POR** Enabled Disabled	
PCIe function swap	Disabled **Enabled**	
PCIe EQ settings	Submenu	
PCI Express Root Port 1/2/3/4/5/6/7	Submenu	
PCIE clocks	Submenu	

7.4.2.1.1 Advanced > PCH-IO Configuration > PCI Express Configuration > PCIe EQ settings

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

7.4.2.1.2 Advanced > PCH-IO Configuration > PCI Express Configuration > PCIe Express Root Port 1/2/3/4/5/6/7/

Feature	Options	Description
PCI Express Root Port 1/2/3/4/5/6/7/	Disabled **Enabled**	Control the PCI Express Root Port.
Connection Type	Build-in **Slot**	Built-In: a built-in device is connected to this root port. Slot Implemented bit will be clear. Slot: this root port connects to user-accessible slot. Slot Implemented bit will be set.
ASPM	**Disabled** L0s L1 L0sL1	Set the ASPM Level: Force L0s – Force all links to L0s State Auto – BIOS auto configure DISABLE – Disables ASPM

Feature	Options	Description
	Auto	
L1 Substates	Disabled L1.1 L1.1 & L1.2	PCI Express L1 Substates settings.
ACS	Disabled **Enabled**	Enable/Disable Access Control Services Extended Capability
PTM	**Disabled** Enabled	Enable/Disable Precision Time Measurement
DPC	Disabled **Enabled**	Enable/Disable Downstream Port Containment
EDPC	Disabled **Enabled**	Enable/Disable Rootport extensions for Downstream Port Containment
URR	**Disabled** Enabled	PCI Express Unsupported Request Reporting Enable/Disable.
FER	**Disabled** Enabled	PCI Express Device Fatal Error Reporting Enable/Disable.
NFER	**Disabled** Enabled	PCI Express Device Non-Fatal Error Reporting Enable/Disable.
CER	**Disabled** Enabled	PCI Express Device Correctable Error Reporting Enable/Disable.
SEFE	**Disabled** Enabled	Root PCI Express System Error on Fatal Error Enable/Disable.
SENFE	**Disabled** Enabled	Root PCI Express System Error on Non-Fatal Error Enable/Disable.
SECE	**Disabled** Enabled	Root PCI Express System Error on Correctable Error Enable/Disable.
PME SCI	Disabled **Enabled**	PCI Express PME SCI Enable/Disable.
Hot Plug	**Disabled**	PCI Express Hot Plug Enable/Disable.

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

Feature	Options	Description
LTR Lock	**Disabled** Enabled	PCIE LTR Configuration Lock
Extra options	Submenu	

7.4.2.1.2.1 Advanced > PCH-IO Configuration > PCI Express Configuration > PCIe Express Root Port 1/2/3/4/5/6/7 > Extra options

Feature	Options	Description
Detect Non-Compliance Device/	**Disabled** Enabled	Detect Non-Compliance PCI Express Device. If enable, it will take more time at POST time.
Prefetchable Memory	**10**	Prefetchable Memory Range for this Root Bridge.
Reserved Memory Alignment	**1**	Reserved Memory Alignment (0 - 31 bits)
Prefetchable Memory Alignment	**1**	Prefetchable Memory Alignment (0 - 31 bits)

7.4.2.1.3 Advanced > PCH-IO Configuration > PCI Express Configuration > PCIE clocks

Feature	Options	Description
Clock0 assignment	**Platform-POR** Enabled Disabled	Platform-POR = clock is assigned to PCIe port or LAN according to board layout. Enabled = keep clock enabled even if unused. Disabled = Disable clock.
ClkReq for Clock0	**Platform-POR** Disabled	Platform-POR = CLKREQ signal is assigned to CLKSRC according to board layout. Disabled = CLKREQ will not be used.
Clock1 assignment	**Platform-POR** Enabled Disabled	Platform-POR = clock is assigned to PCIe port or LAN according to board layout. Enabled = keep clock enabled even if unused. Disabled = Disable clock.
ClkReq for Clock1	**Platform-POR** Disabled	Platform-POR = CLKREQ signal is assigned to CLKSRC according to board layout. Disabled =

Feature	Options	Description
		CLKREQ will not be used.
Clock2 assignment	**Platform-POR** Enabled Disabled	Platform-POR = clock is assigned to PCIe port or LAN according to board layout. Enabled = keep clock enabled even if unused. Disabled = Disable clock.
ClkReq for Clock2	**Platform-POR** Disabled	Platform-POR = CLKREQ signal is assigned to CLKSRC according to board layout. Disabled = CLKREQ will not be used.
Clock3 assignment	**Platform-POR** Enabled Disabled	Platform-POR = clock is assigned to PCIe port or LAN according to board layout. Enabled = keep clock enabled even if unused. Disabled = Disable clock.
ClkReq for Clock3	**Platform-POR** Disabled	Platform-POR = CLKREQ signal is assigned to CLKSRC according to board layout. Disabled = CLKREQ will not be used.
Clock4 assignment	**Platform-POR** Enabled Disabled	Platform-POR = clock is assigned to PCIe port or LAN according to board layout. Enabled = keep clock enabled even if unused. Disabled = Disable clock.
ClkReq for Clock4	**Platform-POR** Disabled	Platform-POR = CLKREQ signal is assigned to CLKSRC according to board layout. Disabled = CLKREQ will not be used.
Clock5 assignment	**Platform-POR** Enabled Disabled	Platform-POR = clock is assigned to PCIe port or LAN according to board layout. Enabled = keep clock enabled even if unused. Disabled = Disable clock.
ClkReq for Clock5	**Platform-POR** Disabled	Platform-POR = CLKREQ signal is assigned to CLKSRC according to board layout. Disabled = CLKREQ will not be used.

7.4.2.2. Chipset > PCH-IO Configuration > SATA Configuration

Feature	Options	Description
SATA Configuration	Info Only	
SATA Controller	Submenu	PCI Express Configuration setting
SATA Mode Selection	AHCI	Determines how SATA controller(s) operate.
SATA Controller Speed	Default Gen1 **Gen2** Gen3	Indicates the maximum speed the SATA controller can support.
SATA Ports Multiplier	Enabled **Disabled**	Ports Multiplier Enable/Disable
SATA Test Mode	Enabled **Disabled**	Test Mode Enable/Disable (Loop Back).
Software Feature Mask Configuration	Submenu	RST Legacy OROM/RST UEFI driver will refer to the SWFM configuration to enable/disable the storage features.
Aggressive LPM Support	Disabled **Enabled**	Enable PCH to aggressively enter link power state.
Serial ATA Port x	Info Only	
Software Preserve	Info Only	
Port0	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**	If enabled for any of ports Staggered Spin Up will be performed and only the drives which have this option

Feature	Options	Description
	Enabled	enabled will spin up at boot. Otherwise all drives spin up at boot.
SATA Device Type	**Hard Disk Drive** Solid State Drive	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive
Topology	**Unknown** ISATA Direct Connect Flex M2	Identify the SATA Topology if it is Default or ISATA or Flex or DirectConnect or M2
SATA Portx DevSlp	**Disabled** Enabled	Enable/Disable SATA Port 0 DevSlp. For DevSlp to work, both hard drive and SATA port need to support DevSlp function, otherwise an unexpected behavior might happen. Please check board design before enabling it.
SATA Portx RxPolarity	**Disabled** Enabled	Enable/Disable SATA Port 0 RxPolarity. Default should disable, please check board design before enable it.
DITO Configuration	**Disabled** Enabled	Enable/Disable DITO Configuration
DITO value	Info Only	
DM Value	Info Only	

7.4.2.2.1 Advanced > PCH-IO Configuration > SATA Configuration > Software Feature Mask Configuration

Feature	Options	Description
Software Feature Mask Configuration	Info Only	
HDD Unlock	Disabled **Enabled**	If enabled, indicates that the HDD password unlock in the OS is enabled.
LED Locate	Disabled **Enabled**	If enabled, indicates that the LED/SGPIO hardware is attached and ping to locate feature is enabled on the OS.

7.4.2.3. Chipset > PCH-IO Configuration > USB Configuration

Feature	Options	Description
USB Configuration	Info Only	
XHCI Compliance Mode	**Disabled** Enabled	Option to enable Compliance Mode. Default is to disable Compliance Mode. Change to enabled for Compliance Mode testing.
xDCI Support	**Disabled** Enabled	Enable/Disable xDCI (USB OTG Device).
USB2 PHY Sus Well Power Gating	GEN1 **GEN2**	Select 'Enabled' to enable SUS Well PG for USB2 PHY. This option has no effect on PCH-H
USB3 Link Speed Selection	Disabled **Enabled**	This option is to select USB3 Link Speed GEN1 or GEN2
USB PD0 Programming	Disabled **Enabled**	Select 'Enabled' if Port Disable Override functionality is used.
USB Overcurrent	Disabled **Enabled**	Select 'Disabled' for pin-based debug. If pin-based debug is enabled but USB overcurrent is not disabled, USB DbC does not work.
USB Overcurrent Lock	Disabled **Enabled**	Select 'Enabled' if Overcurrent functionality is used. Enabling this will make xHCI controller consume the Overcurrent mapping data
USB Port Disable Override	**Disabled** Select Per-Pin	Selectively Enable/Disable the corresponding USB port from reporting a Device Connection to the controller.
USB Device/HOST Mode Override	**Disabled** Select Per-Pin	Selectively Enable/Disable the corresponding USB 2.0 and USB 3.0 port device mode
USB UCSI ACPI device	**Disabled** Enabled	Enable/Disable USB UCSI ACPI device

7.4.2.4. Chipset > PCH-IO Configuration > Security Configuration

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

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

Feature	Options	Description
HD Audio Subsystem Configuration Settings	Info Only	
HD Audio	Disabled **Enabled**	Control Detection of the HD-Audio device. Disabled = HDA will be unconditionally disabled Enabled = HDA will be unconditionally enabled.

7.4.2.6. Chipset > PCH-IO Configuration > SerialIo Configuration

Feature	Options	Description
SerialIo Configuration	Info Only	
I2C0 Controller	Disabled **Enabled**	Enables/Disables SerialIo Controller
I2C1 Controller	**Disabled** Enabled	Enables/Disables SerialIo Controller

Feature	Options	Description
I2C2 Controller	**Disabled** Enabled	Enables/Disables SerialIo Controller
I2C3 Controller	**Disabled** Enabled	Enables/Disables SerialIo Controller
I2C4 Controller	**Disabled** Enabled	Enables/Disables SerialIo Controller
I2C5 Controller	**Disabled** Enabled	Enables/Disables SerialIo Controller
I2C6 Controller	**Disabled** Enabled	Enables/Disables SerialIo Controller
I2C7 Controller	**Disabled** Enabled	Enables/Disables SerialIo Controller
SPI0 Controller	**Disabled** Enabled	Enables/Disables SerialIo Controller
SPI1 Controller	Disabled Enabled **Post Code Only**	Enables/Disables SerialIo Controller
SPI2 Controller	**Disabled** Enabled	Enables/Disables SerialIo Controller
UART0 Controller	Disabled **Enabled** Communication port (COM)	Enables/Disables SerialIo Controller
UART1 Controller	Disabled **Enabled** Communication port (COM)	Enables/Disables SerialIo Controller
UART2 Controller	Disabled **Enabled** Communication port (COM)	Enables/Disables SerialIo Controller

Feature	Options	Description
GPIO IRQ Route	**IRQ14** IRQ15	Route all GPIOs to one of the IRQ.
Serial IO I2C0 Settings	Submenu	Configure SerialIo Controller
Serial IO SPI1 Settings	Submenu	Configure SerialIo Controller
Serial IO UART0 Settings	Submenu	Configure SerialIo Controller
Serial IO UART1 Settings	Submenu	Configure SerialIo Controller
Serial IO UART2 Settings	Submenu	Configure SerialIo Controller
WITT/MITT I2C Test Device	**Disabled** Enabled	Enable SIO I2C WITT Device and select which are all controller used it
WITT/MITT SPI Test Device	**Disabled** Enabled	Enable SIO SPI WITT Device and select which are all controller used it
UART Test Device	**Disabled** Enabled	Enable SIO UART Test Device and select which are all controller used it
LPSS Device D3 State	Disabled **Enabled**	Enable/Disable the LPSS D3 before entering to OS.
Additional Serial IO devices	**Disabled** Enabled	When enabled, ACPI will report additional devices connected to Serial IO.
SerialIO timing parameters	Disabled **Enabled**	Enables additional timing parameters for all SeraialIO controllers.

7.4.2.6.1 Advanced > PCH-IO Configuration > SerialIo Configuration > Serial IO I2C0 Settings

Feature	Options	Description
Serial io i2c0 Settings	Info Only	
Set Serial IO I2C #0 Speed	Standard Mode **Fast Mode** Fast Plus Mode High Speed Mode	Select Serial IO I2C #0 Speed

Feature	Options	Description
Timing parameters		
StandardSpeed SCL High	**429**	
StandardSpeed SCL Low	**495**	
StandardSpeed SDA Hold	**30**	
FastSpeed SCL High	**81**	
FastSpeed SCL Low	**153**	
FastSpeed SDA Hold	**30**	
FastSpeedPlus SCL High	**9**	
FastSpeedPlus SCL Low	**16**	
FastSpeedPlus SDA Hold	**11**	
HighSpeed SCL High	**8**	
HighSpeed SCL Low	**16**	
HighSpeed SDA Hold	**8**	
D0->D3 idle timout (screen off)	**200**	
D0->D3 idle timout (screen on)	**2000**	

7.4.2.6.2 Advanced > PCH-IO Configuration > SerialIo Configuration > Serial IO SPI1 Settings

Feature	Options	Description
Serial io SPI1 Settings	Info Only	
ChipSelect 0 polarity	Active Low **Active High**	Sets initial polarity for ChipSelect signal
ChipSelect 1 polarity	Active Low **Active High**	Sets initial polarity for ChipSelect signal
Delay Rx Clock	As Is Internal	Configure the SPI Delayed Rx Clock option:

Feature	Options	Description
	Tx Clock Rx Clock	
Chip Select 0	Disabled **Enabled**	This enabled SPI device for testing purpose. This option has dependency on WITT device. If WITT device is enabled with SPI, this option will grey out.
Chip Select 1	Disabled **Enabled**	This enabled SPI device for testing purpose. This option has dependency on WITT device. If WITT device is enabled with SPI, this option will grey out.
Timing parameters	Info Only	
D0->D3 idle timeout (screen off)	**200**	
D0->D3 idle timeout (screen on)	**2000**	

7.4.2.6.3 Advanced > PCH-IO Configuration > SerialIo Configuration > Serial IO UART0 Settings

Feature	Options	Description
Serial io UART0 Settings	Info Only	
Hardware Flow Control	Disabled **Enabled**	
DMA Enable	Disabled **Enabled**	
Timing Parameters	Info Only	
D0->D3 idle Timeout (screen off)	200	
D0->D3 idle Timeout (screen on)	200	

7.4.2.6.4 Advanced > PCH-IO Configuration > SerialIo Configuration > Serial IO UART1 Settings

Feature	Options	Description
Serial io UART1 Settings	Info Only	
Hardware Flow Control	Disabled **Enabled**	
DMA Enable	Disabled **Enabled**	
Timing Parameters	Info Only	
D0->D3 idle Timeout (screen off)	200	
D0->D3 idle Timeout (screen on)	200	

7.4.2.6.5 Advanced > PCH-IO Configuration > SerialIo Configuration > Serial IO UART2 Settings

Feature	Options	Description
Serial I/O UART2 Settings	Info Only	
Hardware Flow Control	Disabled **Enabled**	
DMA Enable	Disabled **Enabled**	
Timing Parameters	Info Only	
D0->D3 idle Timeout (screen off)	200	
D0->D3 idle Timeout (screen on)	200	

7.4.2.7. Chipset > PCH-IO Configuration > SCS Configuration

Feature	Options	Description
eMMC 5.1 Controller	Disabled **Enabled**	Enable or Disable SCS eMMC 5.1 Controller
eMMC 5.1 HS400 Mode	Disabled **Enabled**	Enable or Disable SCS eMMC 5.1 HS400 Mode
Enable HS400 software tuning	**Disabled** Enabled	Software tuning should improve eMMC HS400 stability at the expense of boot time
Driver Strength	33 0hm **40 0hm** 50 0hm	Sets I/O driver strength
SDCard 3.0 Controller	Disabled **Enabled**	Enable or Disable SCS SDHC 3.0 Controller

7.4.2.8. Chipset > PCH-IO Configuration > PSE Configuration

Feature	Options	Description
PSE Controller	Disabled **Enabled**	Enables/Disables Programmable Service Engine (PSE) Device
PSE Dash Board Configuration	Info Only	
LOG OUTPUT CHANNEL	3	Determine the PSE log output channel
LOG PUTPUT OFFSET	0	Determine the PSE log output region offset in memory
LOT OUTPUT SIZE	0	Determine the PSE log output region size limitation in memory
Shell	**Disabled** Enabled	Enable/Disable PSE Shell
Eclite	**Disabled** Enabled	Enable/Disable PSE Eclite Service

Feature	Options	Description
OOB	Disabled **Enabled**	Enable/Disable PSE OOB Service
WOL	Disabled **Enabled**	Enable/Disable PSE GBE WoL
PSE Debug (JTAGSWD) Enable	**Disabled** Enabled	PSE JTAG/SWD Debug enable. Set to enable. Unset to disable
PSE JTAG/SWD PIN MUX	**Disabled** Enabled	Enable/Disable PSE Jtag Pin Mux. Grayed out if Sci Pin Mux is enabled
PSE Add-In-Card	**Disabled** Enabled	Enable/Disable PSE Add-In-Card
PSE IP Ownership and GPIO Mux Assignment Configuration	Info Only	
I2S0	**None** PSE owned with pin muxed Host owned with pin muxed	I2S0 has pin conflict with CAN0, CAN1, TGPIO 14-17. I2S1 does not have conflict. If it is grayed out, check the above option. The same pin cannot be assigned to multiple IP.
PSE I2S0 PIN Assignment	**Group E** Group R	PSE I2S0 PIN Assignment. Choose I2S0 pin out to GPIO Group E or Group R
I2S1	**None** PSE owned with pin muxed Host owned with pin muxed	I2S0 has pin conflict with CAN0, CAN1, TGPIO 14-17. I2S1 does not have conflict. If it is grayed out, check the above option. The same pin cannot be assigned to multiple IP.
PWM	None **PSE owned with pin muxed** Host owned with pin muxed	PWM has pin conflict with UART3, SPI0, SPI1, I2C5 and TGPIO. If it is grayed out, check the above options. The sam pin cannot be assigned to multiple IP. I2S1 does not have conflict.
PWM Pin Mux Selection	Submenu	Enable individual pin as PWM
UART0	None PSE owned with pin	If UART0 is disabled, UART1-5 will be disabled too due to sharing same function

Feature	Options	Description
	muxed **Host owned with pin muxed**	
HSUART0/RS485	None PSE owned with pin muxed **Host owned with pin muxed**	Select this to enable UART to support HSUART/RS485.Each HSUART pin conflict dependency is similar to UART.
UART1	None PSE owned with pin muxed **Host owned with pin muxed**	To assign this device to host owned, you must enable PSE UART0 to host owned because UART0 is the function 0 of this device.
HSUART1RS485	None PSE owned with pin muxed **Host owned with pin muxed**	Select this to enable UART to support HSUART/RS485.Each HSUART pin conflict dependency is similar to UART.
UART3	**None** PSE owned with pin muxed Host owned with pin muxed	UART3 has pin conflict with GBE0-1, PWM, TGPIO, and Seriallo controller.
HSUART3/RS485	**None** PSE owned with pin muxed Host owned with pin muxed	Select this to enable UART to support HSUART/RS485.
UART4	**None** PSE owned with pin muxed Host owned with pin muxed	To assign this device to host owned, you must enable PSE UART0 to host owned because UART0 is the function 0 of this device.
UART5	**None** PSE owned with pin	To assign this device to host owned, you must enable PSE UART0 to host owned because UART0 is the

Feature	Options	Description
	muxed Host owned with pin muxed	function 0 of this device.
QEP0	**None** PSE owned with pin muxed	To assign this device to host owned, you must enable PSE I2C7 to host owned because I2C7 is the function 0 of this device. If it is grayed out, check the above options. The same pin connot be assigned to multiple IP.
QEP1	**None** PSE owned with pin muxed	To assign this device to host owned, you must enable PSE I2C7 to host owned because I2C7 is the function 0 of this device. If it is grayed out, check the above options. The same pin connot be assigned to multiple IP.
QEP2	**None** PSE owned with pin muxed	To assign this device to host owned, you must enable PSE I2C7 to host owned because I2C7 is the function 0 of this device. If it is grayed out, check the above options. The same pin connot be assigned to multiple IP.
QEP3	**None** PSE owned with pin muxed	To assign this device to host owned, you must enable PSE I2C7 to host owned because I2C7 is the function 0 of this device. If it is grayed out, check the above options. The same pin connot be assigned to multiple IP.
I2C0	**None** PSE owned with pin muxed	If I2C0 is not set to host owned, I2C 1-6 could not be set to host owned too due to sharing same function
I2C1	**None** PSE owned with pin muxed	To assign this device to host owned, you must enable PSE I2C0 to host owned because I2C0 is the function 0 of this device.
I2C2	None **PSE owned with pin muxed**	Grayed out to reserve for ECLite
I2C3	I2C3 is not configurable as it is shared with SMBUS	To assign this device to host owned, you must enable PSE I2C0 to host owned because I2C0 is the function 0 of this device.

Feature	Options	Description
I2C4	**None** PSE owned with pin muxed	To assign this device to host owned, you must enable PSE I2C0 to host owned because I2C0 is the function 0 of this device.
I2C5	**None** PSE owned with pin muxed	To assign this device to host owned, you must enable PSE I2C0 to host owned because I2C0 is the function 0 of this device.
I2C6	**None** PSE owned with pin muxed	To assign this device to host owned, you must enable PSE I2C0 to host owned because I2C0 is the function 0 of this device.
I2C7	None **PSE owned with pin muxed**	If I2C7 is not set to host owned, all PSE CAN and QEP devices could not be set to host owned too due to sharing same function.
SPI0	None PSE owned with pin muxed **Host owned with pin muxed**	SPI0 has pin conflict with PWM pin 3, TGPIO pin 10-13 and 39, serial SPI 2.
SPI0 CS0	Disabled **Enabled**	Set SPI CS pin to PSE SPI CS native function
SPI0 CS1	Disabled **Enabled**	Set SPI CS pin to PSE SPI CS native function
SPI1	**None** PSE owned with pin muxed Host owned with pin muxed	To assign this device to host owned, you must enable PSE SPI0 to host owned because SPI0 is the function 0 of this device.
SPI2	**None** PSE owned with pin muxed Host owned with pin muxed	SPI2 has pin conflict with WWAN WAKE GPIO.
SPI3	**None** PSE owned with pin muxed	To assign this device to host owned, you must enable PSE SPI0 to host owned because SPI0 is the function 0 of this device.

Feature	Options	Description
	Host owned with pin muxed	
CAN0	**None** PSE owned with pin muxed	To assign this device to host owned, you must enable PSE I2C7 to host owned because I2C7 is the function 0 of this device.
CAN1	**None** PSE owned with pin muxed	To assign this device to host owned, you must enable PSE I2C7 to host owned because I2C7 is the function 0 of this device.
DMA0	None **PSE owned with pin muxed** Host owned with pin muxed	Select ownership for DMA.
DMA1	None **PSE owned with pin muxed** Host owned with pin muxed	Select ownership for DMA.
DMA2	None **PSE owned with pin muxed** Host owned with pin muxed	Select ownership for DMA.
GBE0	**None** PSE owned with pin muxed Host owned with pin muxed	Select ownership for GBE
GBE1	None PSE owned with pin muxed **Host owned with pin muxed**	Select ownership for GBE
PSE GBE1 DLL Overrid	**Disabled** Enabled	Enable/Disable PSE GBE1 DLL.To Enable this GBE1 must be Enabled

Feature	Options	Description
GPIO/TGPIO 0	None **PSE owned with pin muxed** Host owned with pin muxed	Owner of GPIO/TGPIO 0 Controller(PSE or HOST owned).
GPIO/TGPIO 0 MUX SELECTION	LOWER MID TOP **All pins are GPIO**	Choose Top, Mid, Lower or All mux for GPIO/TGPIO 1 Controller Instance.
GPIO/TGPIO 0 Pin Selection	Submenu	Enable individual GPIO/TGPIO pin
GPIO/TGPIO 1	None **PSE owned with pin muxed** Host owned with pin muxed	Owner of GPIO/TGPIO 1 Controller(PSE or HOST owned).
GPIO/TGPIO 1 MUX SELECTION	LOWER MID TOP **All pins are GPIO**	Choose Top, Mid, Lower or All mux for GPIO/TGPIO 1 Controller Instance.
GPIO/TGPIO 1 Pin SELECTION	Submenu	Enable individual GPIO/TGPIO pin
PSE Interrupt Assignment Configuration	Info Only	
I2S0	**Disabled** Enabled	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.
I2S1	**Disabled** Enabled	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.
PWM	**Disabled** Enabled	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.
UART0	**Disabled** Enabled	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.
UART1	**Disabled** Enabled	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.

Feature	Options	Description
UART2	**Disabled** Enabled	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.
UART3	**Disabled** Enabled	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.
UART4	**Disabled** Enabled	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.
UART5	**Disabled** Enabled	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.
HSUART0	**Disabled** Enabled	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.
HSUART1	**Disabled** Enabled	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.
HSUART2	**Disabled** Enabled	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.
HSUART3	**Disabled** Enabled	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.
QEP0	**Disabled** Enabled	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.
QEP1	**Disabled** Enabled	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.
QEP2	**Disabled** Enabled	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.
QEP3	**Disabled** Enabled	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.
I2C0	**Disabled** Enabled	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.
I2C1	**Disabled** Enabled	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.
I2C2	**Disabled**	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.

Feature	Options	Description
	Enabled	
I2C3	**Disabled** Enabled	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.
I2C4	**Disabled** Enabled	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.
I2C5	**Disabled** Enabled	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.
I2C6	**Disabled** Enabled	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.
I2C7	**Disabled** Enabled	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.
SPI0	**Disabled** Enabled	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.
SPI1	**Disabled** Enabled	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.
SPI2	**Disabled** Enabled	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.
SPI3	**Disabled** Enabled	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.
DMA0	**Disabled** Enabled	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.
DMA1	Disabled **Enabled**	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.
DMA2	Disabled **Enabled**	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.
LH2PSE	**Disabled** Enabled	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.
CAN0	**Disabled** Enabled	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.

Feature	Options	Description
CAN1	**Disabled** Enabled	Checked = Interrupt set to SB mode. Default unchecked is MSI mode.
DMA Test	**Disabled** Enabled	Enable/Disable DMA test Device
PSE I2C Test Device	**Disabled** Enabled	Enable PSE I2C WITT Device and select which are all controller used it
PSE SPI Test Device	**Disabled** Enabled	Enable PSE SPI WITT Device and select which are all controller used it
PSE UART Test Device	**Disabled** Enabled	Enable PSE UART Test Device and select which are all controller used it

7.4.2.9. Chipset > PCH-IO Configuration > TSN GBE Configuration

Feature	Options	Description
PCH TSN LAN Controller	Enabled **Disabled**	Enable/Disable TSN LAN.
PCH TSN GBE Multi-Vc	Enabled **Disabled**	Enable/Disable TSN Multi Virtual Channels.
PCH TSN GBE SGMII Support	**Enabled** Disabled	Enable/Disable SGMII mode for PCH TSN GBE. Ports in SGMII mode with the same PLL common lane must use the same link speed. SATA or UFS may need to be disabled if TSN port is using the same PLL common lane. Please make sure IFWI has proper straps set for SGMII. Make sure Flex IO Lane Assignment is not NONE.
PCH TSN Link Speed	RefClk 24Mhz 2.5Gbps RefClk 24Mhz 1Gbps RefClk 38.4Mhz 2.5Gbps **RefClk 38.4Mhz 1Gbps**	PCH TSN Link Speed configuration.
Flex IO Lane Assignment:	Info Only	

Feature	Options	Description
PSE TSN GBE 0 Multi-Vc	Enabled **Disabled**	Enable/Disable TSN Multi Virtual Channels. TSN GBE must be host owned.
PSE TSN GBE 0 SGMII Support	Enabled **Disabled**	Enable/Disable Modphy support for SGMII mode for PSE TSN GBE 0. Ports in SGMII mode with the same PLL common lane must use the same link speed. UFS will need to be disabled as this TSN port uses the same PLL common lane. Please make sure IFWI has proper straps set for SGMII. Make sure Flex IO Lane Assignment is not NONE.
PSE TSN GBE 0 Link Speed	RefClk 24Mhz 2.5Gbps RefClk 24Mhz 1Gbps RefClk 38.4Mhz 2.5Gbps **RefClk 38.4Mhz 1Gbps**	PSE TSN GBE 0 Link Speed configuration.
PSE TSN GBE1 Multi-Vc	**Enabled** Disabled	Enable/Disable TSN Multi Virtual Channels. TSN GBE must be host owned.
PSE TSN GBE1 SGMII Support	**Enabled** Disabled	Enable/Disable Modphy support for SGMII mode for PSE TSN GBE 1. Ports in SGMII mode with the same PLL common lane must use the same link Speed. SATA or UFS may need to be disabled if TSN port is using the same PLL common lane. Please make sure IFWI has proper straps set for SGMII. Make sure Flex IO Lane Assignment is not NONE.
PSE TSN GBE 1 Link Speed	RefClk 24Mhz 2.5Gbps RefClk 24Mhz 1Gbps RefClk 38.4Mhz 2.5Gbps **RefClk 38.4Mhz 1Gbps**	PSE TSN GBE 1 Link Speed configuration.
Flex IO Lane Assignment:	Info Only	
PLL Common Lane 1	Info Only	
GBE AIC Status	Connected Not Connected	GBE Add In Card connection status.

7.5. Security Menu

7.5.1. Security > Password Description

Feature	Options	Description
Password Description	Info only	
Setup Administrator Password	Enter Password	Set Setup Administrator Password
User Password	Enter Password	Set User Password
Secure Boot	Submenu	Customizable Secure Boot settings.
System Mode	Info only	
Secure Boot	Info only	
Secure Boot Control	**Disabled** Enabled	Secure Boot activated when Platform Key(PK) is enrolled, System mode is User / Deployed, and CSM function is disabled

7.6. Boot Menu

7.6.1. 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 Number state.
Quiet Boot	Disabled **Enabled**	Select the keyboard NumLock state.

Feature	Options	Description
Fast Boot	**Disabled** Enabled	Enable or Disable FastBoot features. Most probes are skipped to reduce time cost during boot.
New Boot Option Policy	**Default** Place First Place Last	Controls the placement of newly detected UEFI boot option.
Boot Mode select	LEGACY **UEFI**	Select boot mode LEGACY/UEFI

7.6.2. Boot > FIXED BOOT ORDER Priorities

Feature	Options	Description
Boot Option #1	Hardware	Set the system boot order.
Boot Option #2	CD/DVD	Set the system boot order.
Boot Option #3	USB Hard Disk	Set the system boot order.
Boot Option #4	USB CD/DVD	Set the system boot order.
Boot Option #5	USB Key	Set the system boot order.
Boot Option #6	USB Floppy	Set the system boot order.
Boot Option #7	USB Lan	Set the system boot order.
Boot Option #8	Network	Set the system boot order.

7.7. Save & Exit Menu

7.7.1. Save and 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.
Save as User Defaults		Save the changes done so far as User Defaults.
Restore User Defaults		Restore the User Defaults to all the setup options.
Boot Override	Info only	

8. BIOS Checkpoints, Beep Codes

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

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

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

8.2.4. PEI Beep Codes

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

8.2.5. DXE Status Codes

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

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

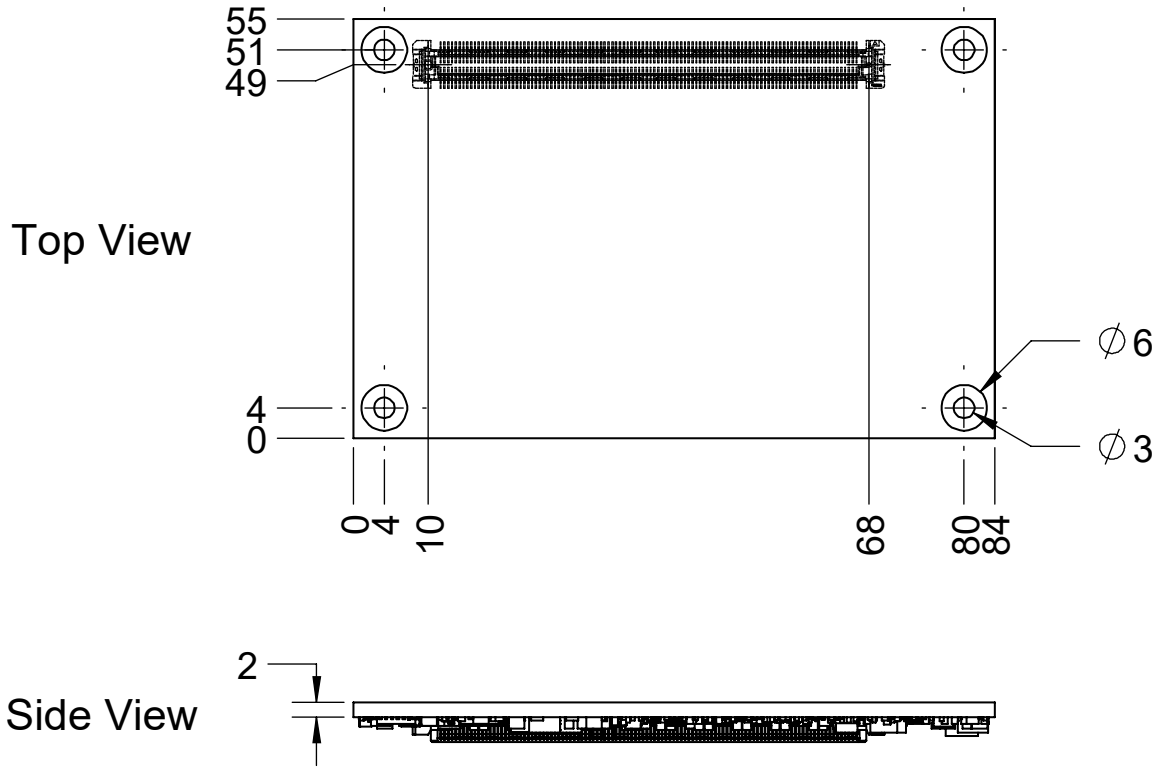
9.1. Windows 10 IoT Enterprise 64-bit

9.2. Yocto Linux 64-bit

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

10. Mechanical and Thermal

10.1. Module Dimensions



All dimensions are shown in millimeters. Tolerances should be ± 0.25mm, unless otherwise noted.
The tolerances on the module connector locating peg holes (dimensions [9.8, 49]) should be ± 0.10mm.

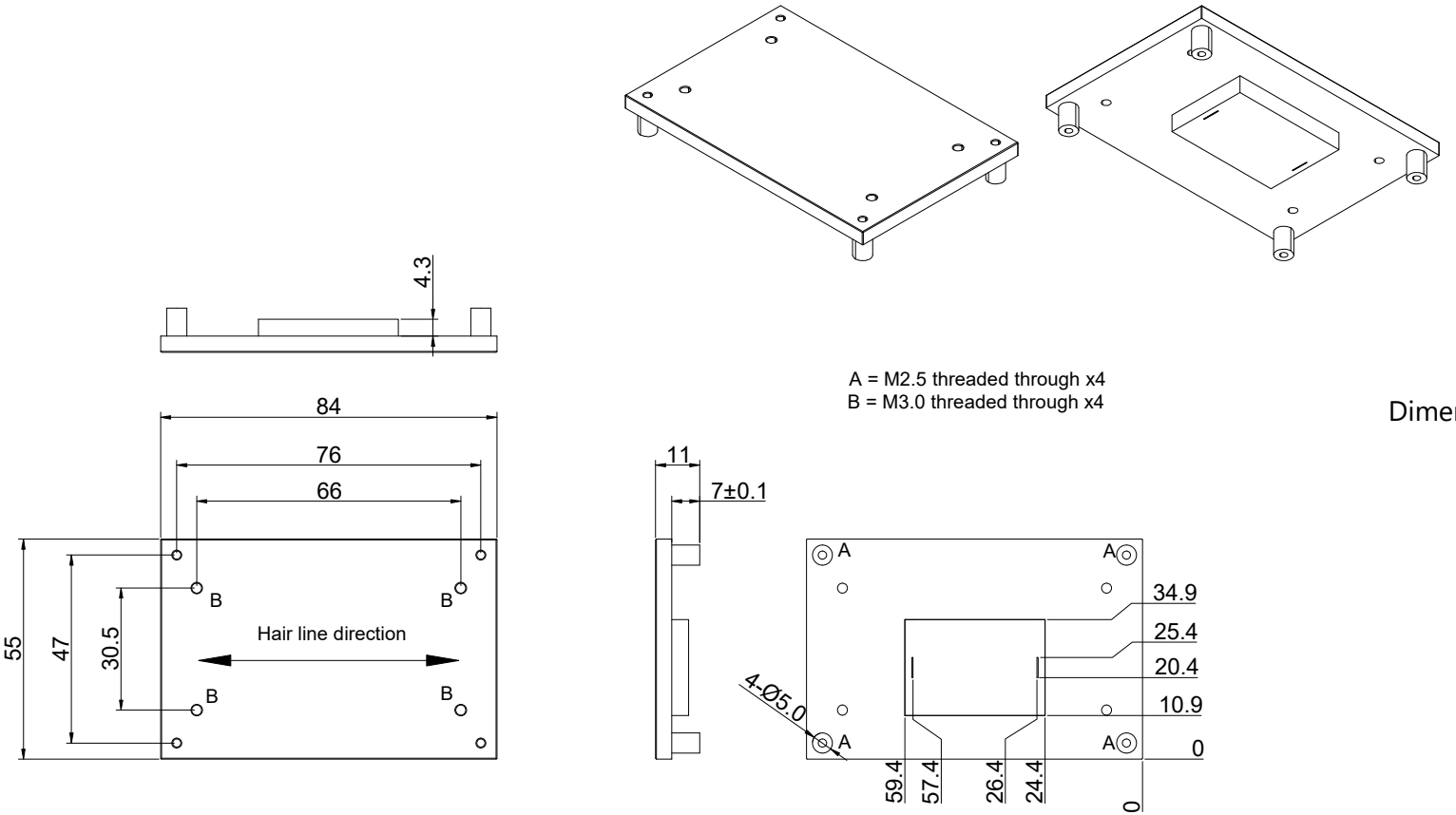
Dimensions: mm

Figure 5 – Module mechanical dimensions

10.2. Thermal Solutions

10.2.1. Heatspreader – Bottom Mount: HTS-nXEL-B-I

Heatspreader with threaded standoffs for bottom mounting



Dimensions: mm

Figure 6 – Heatspreader – Bottom Mount: HTS-nXEL-B-I

10.2.2. Heatsink High Profile – Bottom Mount: THSH-nXEL-B-I

High profile heatsink with threaded standoffs for bottom mounting

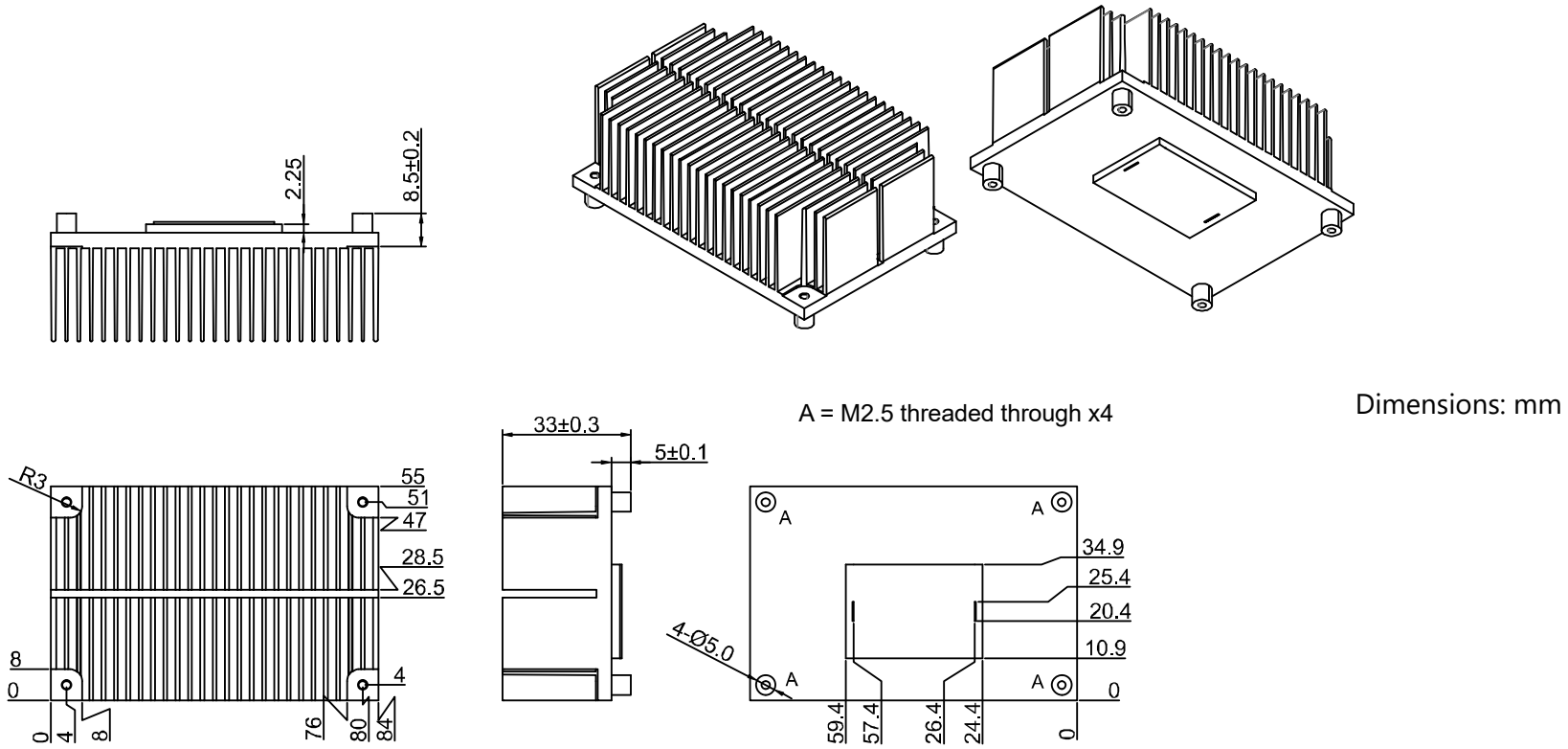


Figure 7 – Heatsink High Profile –Bottom Mount: THSH-nXEL-B-I

10.2.3. Heatsink Low Profile – Bottom Mount: THS-nXEL-B-I

Low profile heatsink with threaded standoffs for bottom mounting

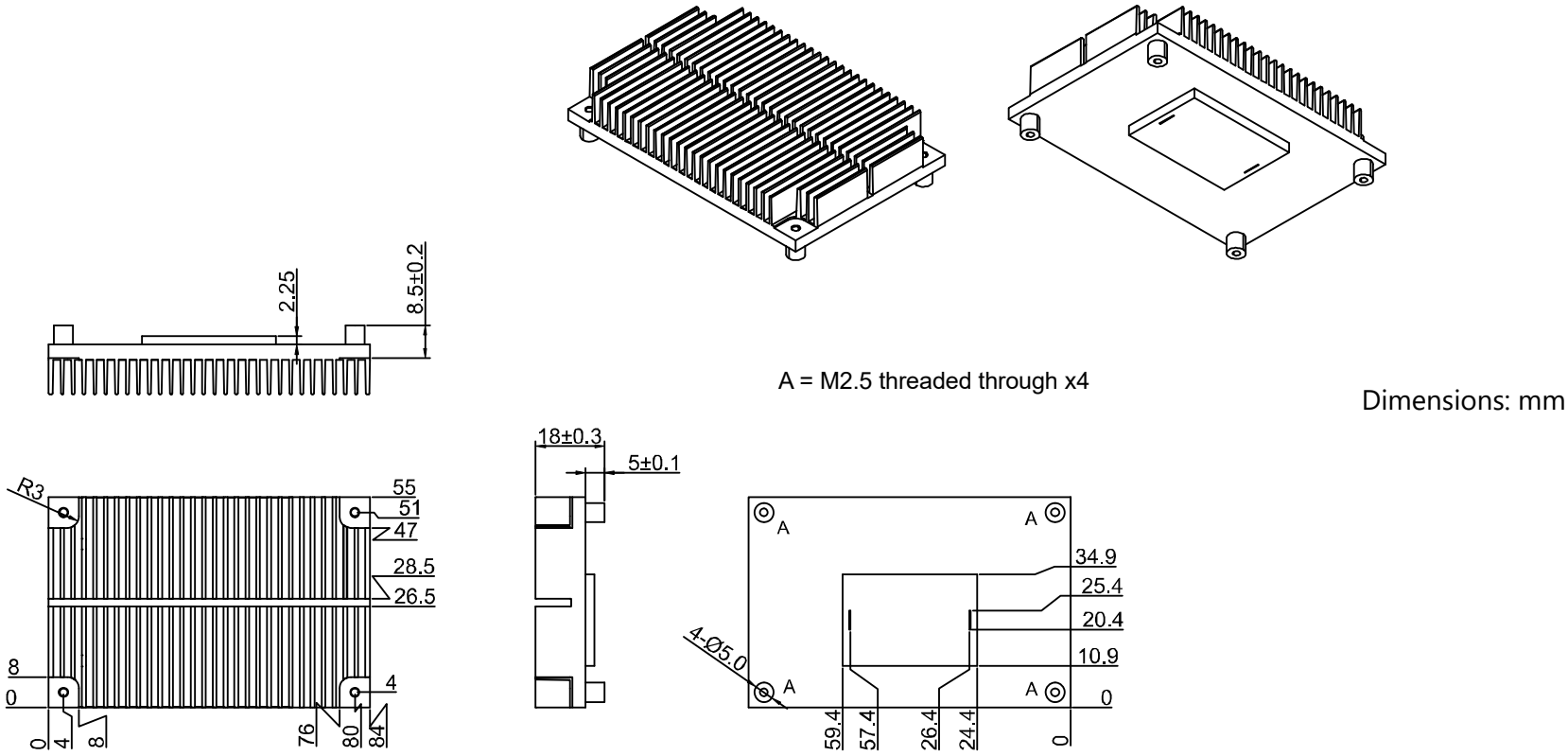


Figure 8 – Heatsink Low Profile – Bottom Mount: THS-nXEL-B-I