Single Board Computer

User Manual

SBC-3.5-TGL-UP3

Single Board Computer on 3.5" form factor with the Intel® 11th Generation Core™ / Celeron® Processors formerly Tiger Lake-UP3 Family

REVISION HISTORY

Revision	Date	Note	Ref
1.0	12th April 2024	First Official Release.	SO
1.1	10th January 2025	Updated BIOS reset switch behaviour GPIO electrical level correction Audio Header electrical levels added Minor corrections	SO

Every effort has been made to ensure the accuracy of this manual. However, SECO S.p.A. accepts no responsibility for any inaccuracies, errors or omissions herein. SECO S.p.A. reserves the right to change precise specifications without prior notice to supply the best product possible.

For further information on this module or other SECO products, but also to get the required assistance for any and possible issues, please contact us using the dedicated web form available at www.seco.com (registration required).

Our team is ready to assist.

INDEX

Chapter 1. INTRODUCTION

- Warranty and RMA
- Information and assistance
- Safety
- Electrostatic discharges
- RoHS compliance
- Safety Policy
- Reference specifications

1.1 Warranty and RMA

This product is subject to the Italian Law Decree 24/2002, acting European Directive 1999/44/CE on matters of sale and warranties to consumers.

The warranty on this product lasts for 1 year.

Under the warranty period, the Supplier guarantees the buyer assistance and service for repairing, replacing or credit of the item, at the Supplier's own discretion.

Shipping costs that apply to non-conforming items or items that need replacement are to be paid by the customer.

Items cannot be returned unless previously authorised by the supplier.

To request a RMA number, please visit SECO's web-site. On the home page, please select "Online RMA" and follow the procedure described.

A RMA Number will be sent within 1 working day (only for on-line RMA requests).

The authorisation is released after completing the specific ticketing procedure https://support.seco.com/ (Help Topic: Return Merchandise Authorization). The RMA authorisation number must be put both on the packaging and on the documents shipped with the items, which must include all the accessories in their original packaging, with no signs of damage to, or tampering with, any returned item.

To open a new account for RMA write to web.rma@seco.com .

The error analysis form identifying the fault type must be completed by the customer and must accompany the returned item.

If any of the above-mentioned requirements for RMA is not satisfied, the item will be shipped back and the customer will have to pay any and all shipping costs.

Following a technical analysis, the supplier will verify if all the requirements, for which a warranty service applies, are met. If the warranty cannot be applied, the Supplier will calculate the minimum cost of this initial analysis on the item and the repair costs. Costs for replaced components will be calculated separately.

SECO offers Engineering Samples for early evaluation and development. Engineering Samples are sold "as-is" with no warranty of any kind, neither explicit nor implied.

Here https://www.seco.com/it/EngineeringSamplesPolicy is defined the framework of SECO and customer responsibilities regarding Engineering Samples.

⚠ Warning!
All changes or modifications to the equipment not explicitly approved by SECO S.p.A. could impair the equipment's functionality and could void the warranty.

1.2 Information and assistance

What do I have to do if I need assistance?

SECO S.p.A. offers the following services:

- SECO website: visit http://www.seco.com to receive the latest information on the product. In most of the cases it is possible to find useful information to solve the problem.
- SECO Sales Representative: the Sales Rep can help to determine the exact cause of the problem and search for the best solution.
- SECO Help-Desk: place a ticket in the support portal https://support.seco.com/ (Help Topic: HW/SW Support Request).

Note: Please provide the following information when placing a support request on the ticketing portal:

- Name and serial number of the product;
- Description of Customer's peripheral connections;
- Description of Customer's software (operating system, version, application software, etc.);
- A complete description of the problem;
- The exact transcript of every error message encountered.

1.3 Safety

The board uses only extremely-low voltages.

While handling the board, please use extreme caution to avoid any kind of risk or damages to electronic components.

> **!**
>
> Always switch the power off, and unplug the power supply unit, before handling the board and/or connecting cables or other boards.
>
> Avoid using metallic components - like paper clips, screws and similar - near the board when connected to a power supply, to avoid short circuits due to unwanted contacts with other board components.
>
> If the board has become wet, never connect it to any external power supply unit or battery.

1.4 Electrostatic discharges

The board, like any other electronic product, is an electrostatic sensitive device: high voltages caused by static electricity could damage some or all the devices and/or components on-board.

> **!**
>
> Whenever handling this product, ground yourself through an anti-static wrist strap. Placement of the board on an anti-static surface is also highly recommended.

1.5 RoHS compliance

The board is designed using RoHS compliant components and is manufactured on a lead-free production line. It is therefore fully RoHS compliant.

1.6 Safety Policy

In order to meet the safety requirements of EN62368-1:2014 standard for Audio/Video, information and communication technology equipment, this product shall be:

- used inside a fire enclosure made of non-combustible material or V-1 material (the fire enclosure is not necessary if the maximum power supplied to the module never exceeds 100 W, even in worst-case fault);
- used inside an enclosure (the enclosure is not necessary if the temperature of the parts likely to be touched never exceeds 70 °C);
- installed inside an enclosure compliant with all applicable IEC 62368-1 requirements;

The manufacturer which includes this product in his end-user product shall:

- verify the compliance with B.2 and B.3 clauses of the EN62368-1 standard when the module works in its own final operating condition;
- Prescribe temperature and humidity range for operating, transport and storage conditions;
- Prescribe to perform maintenance on the module only when it is off and has already cooled down;
- Prescribe that the connections from or to the Module have to be compliant to ES1 requirements;
- The module in its enclosure must be evaluated for temperature and airflow considerations;
- Install in a way that prevents the access to the board from children;
- Use along with CPU heatspreader/heatsinks designed according to the thermal and mechanical characteristics.
- Verify compliance with chapter 8 of EN62368-1 for mechanical testing based on final product installation
- Verify compliance with chapter Annex V of EN62368-1 for determination of accessible parts based on final product installation
- Prescribe safeguard instructions for parts and surfaces classified as TS3 on final product installation

1.7 Terminology and definitions

ACPI	Advanced Configuration and Power Interface, an open industrial standard for the board's devices configuration and power management
AHCI	Advanced Host Controller Interface, a standard which defines the operation modes of SATA interface
API	Application Program Interface, a set of commands and functions that can be used by programmers for writing software for specific Operating Systems
BIOS	Basic Input / Output System, the Firmware Interface that initializes the board before the OS starts loading
CEC	Consumer Electronics Control, an HDMI feature which allows controlling more devices connected together by using only one remote control
DDC	Display Data Channel, a kind of I2C interface for digital communication between displays and graphics processing units (GPU)
DDR	Double Data Rate, a typology of memory devices which transfer data both on the rising and on the falling edge of the clock
DDR4	DDR, 4th generation
DP	Display Port, a type of digital video display interface
ECC	Error Correcting Code, a peculiar type of memory module with 72-bit of data instead of 64, where the additional 8 bit are used to detect and correct possible errors on the remaining 64-bit data bus
GBE	Gigabit Ethernet
Gbps	Gigabits per second
GND	Ground
GPI/O	General purpose Input/Output
HD Audio	High Definition Audio, most recent standard for hardware codecs developed by Intel® in 2004 for higher audio quality
HDMI	High Definition Multimedia Interface, a digital audio and video interface
I2C Bus	Inter-Integrated Circuit Bus, a simple serial bus consisting only of data and clock line, with multi-master capability
Mbps	Megabits per second
N.A.	Not Applicable
N.C.	Not Connected
OpenCL	Open Computing Language, a software library based on C99 programming language, conceived explicitly to realise parallel computing using Graphics Processing Units (GPU)
OpenGL	Open Graphics Library, an Open Source API dedicated to 2D and 3D graphics
OS	Operating System
PCI-e	Peripheral Component Interface Express

PSU	Power Supply Unit
PWM	Pulse Width Modulation
PWR	Power
PXE	Preboot Execution Environment, a way to perform the boot from the network ignoring local data storage devices and/or the installed OS
SATA	Serial Advance Technology Attachment, a differential full duplex serial interface for Hard Disks
SD	Secure Digital, a memory card type
SDHC	Secure Digital Host Controller
SIM	Subscriber Identity Module, a card which stores all data of the owner necessary to allow him accessing to mobile communication networks
SPI	Serial Peripheral Interface, a 4-Wire synchronous full-duplex serial interface which is composed of a master and one or more slaves, individually enabled through a Chip Select line
TBM	To be measured
TMDS	Transition-Minimized Differential Signaling, a method for transmitting high speed serial data, normally used on DVI and HDMI interfaces
UEFI	Unified Extensible Firmware Interface, a specification defining the interface between the OS and the board's firmware. It is meant to replace the original BIOS interface
UIM	User Identity Module, an extension of SIM modules.
UMA	Unified Memory Architecture, synonym of Integrated Graphics, uses a portion of a computer's system RAM dedicated to graphics rather than using dedicated graphics memory only.
USB	Universal Serial Bus
V_REF	Voltage reference Pin
xHCI	eXtensible Host Controller Interface, Host controller for USB 3.0 ports, which can also manage USB 2.0 and USB1.1 ports

1.7.1 Trademark Notice

The terms HDMI, HDMI High-Definition Multimedia Interface, and the HDMI Logo are trademarks or registered trademarks of HDMI Licensing Administrator, Inc.

1.8 Reference specifications

Here below it is a list of applicable industry specifications and reference documents.

Reference	Link
ACPI	https://uefi.org/specifications
AHCI	http://www.intel.com/content/www/us/en/io/serial-ata/ahci.html
Gigabit Ethernet	https://standards.ieee.org/standard/802_3-2018.html
HD Audio	http://www.intel.com/content/dam/www/public/us/en/documents/product-specifications/high-definition-audio-specification.pdf
HDMI	http://www.hdmi.org/index.aspx
I2C	https://www.nxp.com/docs/en/user-guide/UM10204.pdf
Intel® Front Panel I/O	Intel Technical Library
LVDS	http://www.ti.com/lit/ug/snla187/snla187.pdf
M.2	http://www.pcisig.com/specifications/pciexpress
MMC/eMMC	https://www.jedec.org/committees/jc-64
OpenCL	http://www.khronos.org/opencl
OpenGL	http://www.opengl.org
PCI Express	http://www.pcisig.com/specifications/pciexpress
SATA	https://www.sata-io.org
SD Card Association	https://www.sdcard.org
SM Bus	http://www.smbus.org/specs
TMDS	https://www.cablestogo.com/learning/library/digital-signage/intro-to-tmds
UEFI	http://www.uefi.org
USB OTG	https://www.usb.org/sites/default/files/usb_20_20190524.zip
USB 3.0	https://usb.org.10-1-108-210.causewaynow.com/sites/default/files/usb_32_20191024.zip
Intel® Tiger Lake UP3 family	https://www.intel.com/content/www/us/en/products/platforms/details/tiger-lake-up3.html

Chapter 2.
OVERVIEW

- Introduction
- Technical specifications
- Electrical specifications
- Mechanical specifications
- Block diagram

2.1 Introduction

SBC-3.5-TGL-UP3 is a Single Board Computer in 3.5" form factor (146 x 102mm) based on Intel® 11th Gen CoreTM processors, formerly known with the Tiger Lake UP3 name, specifically targeted for IoT Applications, with HyperThreading capabilities and scalable TDP.

The 11th Generation Intel Core processors combine high performance, low power consumption and IoT-centric features. With up to 4 Processor Cores delivering high-level computing performance, this brand-new family of Processors supports up to 64 GB of memory, also featuring IBECC (In-Band Error Correction Code) to provide ECC protection without additional devices and data pins. Intel® Iris® Xe graphics with up to 96 execution units, along with improved display capabilities – up to 4 simultaneous 4K displays – greatly enhance graphic and media performance. The platform's combination of speed, high powered Graphics, AI/Deep Learning Instruction Sets, including hardware support for real time computing, make it ideal for applications that demand vision, voice, or text recognition alongside processing power.

This board offers the possibility to connect up to 4 displays simultaneously, deploying the 4x DP++ interfaces (two of them available on dedicated DP connectors, the other two available on USB Type-C connectors) and an eDP or LVDS interface.

The board also offers a wide range of expandability, considering the 6 USB ports externally accessible (2x USB 3.2, 2x USB 3.1 and 2x USB 2.0)

Mass storage possibilities are 1x M.2 Key B SATA slot + 1x M.2 Key M NVE Slot (PCI-e x4 Gen4) and an additional M.2 Socket 3 Key M slot with PCI-e x4 Gen 3, UART and USB 3.2, to be used for a second NVME module or an expansion module.

Networking capabilities of the board include two Ethernet ports supporting 2.5Gbps speeds, available on 2x RJ-45 connectors, one WWAN M.2 Socket 2 Key B Slot connected to a microSIM card slot for modems and one M.2 Socket 1 Key E Slot for WiFi+BT M.2 modules.

The board is available both in commercial and in industrial temperature range.

Please refer to following chapter for a complete list of all peripherals integrated and characteristics.

2.2 Technical specifications

CPU

Commercial temp. range

- · Intel® Core i7-1185G7E, Quad Core @ 2.8GHz (4.4GHz in Turbo Boost) with HT, 12MB Cache, 28/15/12W cTDP – vPro, Intel AMT enabled with "Corporate" BIOS
- · Intel® Core i5-1145G7E, Quad Core @ 2.6GHz (4.1GHz in Turbo Boost) with HT, 8MB Cache, 28/15/12W cTDP - vPro, Intel AMT enabled with "Corporate" BIOS
- · Intel® Core i3-1115G4E, Dual Core @ 3.0GHz (3.9GHz in Turbo Boost) with HT, 6MB Cache, 28/15/12W cTDP
- · Intel® Celeron® 6305E, Dual Core @ 1.8GHz, 4MB Cache,15W TDP

Industrial temp. range

- · Intel® Core i7-1185GRE, Quad Core @ 2.8GHz (4.4GHz Turbo) with HT, 12MB Cache, 28/15/12W cTDP - vPro, Intel AMT enabled with "Corporate" BIOS
- · Intel® Core i5-1145GRE, Quad Core @ 2.6GHz (4.1GHz Turbo) with HT, 8MB Cache, 28/15/12W cTDP - vPro, Intel AMT enabled with "Corporate" BIOS
- · Intel® Core i3-1115GRE, Dual Core @ 2.2GHz (3.9GHz Turbo) with HT, 6MB Cache, 28/15/12W cTDP

Memory

2x DDR4 SODIMM Slots Support DDR4-3200 memories, up to 64 GB total

Graphics

Integrated Xe Graphics Core Gen12 architecture, with up to 96 Execution Units

MPEG2, WMV9, AVC/H.264, JPEG/MJPEG, HEVC/H.265, VP9, AV1 HW decoding, up to 8k @60.

AVC/H.264, HEVC/H.265, JPEG, VP9 HW encoding

Support up to 4 independent displays.

Video Interfaces

2x DP++ interfaces, supporting DP 1.2 and HDMI 1.4

eDP or Single/Dual-Channel 18-/24- bit LVDS interface

Video Resolution

eDP, DP	Up to 5120x3200 @60Hz 24bpp / 7680x4320@60Hz 30bpp with DSC
HDMI 1.4	Up to 4Kx2K 24-30Hz 24bpp
LVDS	up to 1920 x 1200 @ 60Hz

Mass Storage

2x M.2 NVMe slots (Socket 2 Key M Type 2280), PCI-e x4 interface
M.2 SATA slot (Socket 2 Key B Type 2242/3042) same as for WWAN module

Networking

2 x Ethernet ports compatible with 2.5GbE
M.2 WWAN slot (Socket 2 Key B Type 2242/3042) same as for SATA module
M.2 Connectivity WiFi/BT Slot (Socket 1 Key E Type 2230)

USB

2 x USB 10Gbps Host ports on Type-A sockets
2 x USB 10Gbps Host ports on Type-C sockets
2 x USB Hi-Speed Host ports on internal pin header
1 x USB 10Gbps Host port on M.2 WWAN Slot
1 x USB Hi-Speed Host port on M.2 Connectivity Slot

Audio

HD Audio codec
Line Out + Microphone + S/PDIF Out interfaces on internal pin header

Serial Ports

2 x RS-232/RS-422/RS-485 Serial ports on internal pin header

Other Interfaces

microSIM slot for M.2 modems
8 x GPI/Os on internal pin header
I2C and SPI on internal pin header
FAN connector
Button / LED Front Header connector
Optional TPM 1.2 or 2.0 onboard

Power supply voltage: +12 ÷ 24 V_{DC}, RTC battery

Operating temperature: **
0°C ÷ +60°C (Commercial temperature)
-40° ÷ +85°C (Industrial temperature)

Dimensions: 146 x 102 mm (3.5" form factor)

Supported Operating Systems (64bit):

Microsoft® Windows® 10 and 11 Enterprise LTSC

SECO Clea OS (Linux Kernel, Yocto image)

> **!** *** Temperatures indicated are the minimum and maximum temperature that the heatspreader / heatsink can reach in any of its parts. This means that it is customer's responsibility to use any passive cooling solution along with an application-dependent cooling system, capable to ensure that the heatspreader / heatsink temperature remains in the range above indicated.*

2.3 Electrical specifications

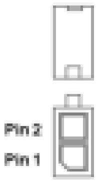
The board can be supplied using any voltage in the range +12 ÷ +24 V_{DC} ±5%. All the others voltages necessary for the working of the board and of the connected peripherals are derived from the main V_{IN} power rail

Power Connectors – CN52/CN53

Pin	Signal
1	GND
2	V_{IN}

Power Connector is type Molex Mega-Fit® connector, and can be available, as a factory option, in vertical version (p/n 76829-0102 or equivalent, connector CN52) or in the right angle version (p/n 76825-0002 or equivalent, connector CN53)

In both cases, the pin-out is indicated in the table here on the left, and the mating connector will be MOLEX p/n 171692-0102 or equivalent, with female crimp terminal MOLEX series 172063 or 78623.



2.3.1 Power consumption

The power consumption has been measured for the following board configurations,

Status	Configuration											
	Cfg#1				Cfg#2				Cfg#3			
	Average		Peak		Average		Peak		Average		Peak	
Idle (Win10), power saving configuration	---	---	---	---	---	---	---	---	---	---	---	---
OS Boot (Win10)	---	---	---	---	---	---	---	---	---	---	---	---
Video reproduction 4K, power saving configuration	---	---	---	---	---	---	---	---	---	---	---	---
AMD System Stress Test, high performance config.	---	---	---	---	---	---	---	---	---	---	---	---

Battery Backup power consumption:	---
Soft-Off State power consumption:	---
Suspend State power consumption:	---

2.3.2 RTC Battery

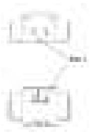
For the occurrences when the module is not powered with an external power supply, on board there is a cabled coin Lithium Battery to supply, with a 3V voltage, the Real Time Clock embedded inside the SoC.

Battery used is a non-rechargeable cabled CR2032, Lithium based, coin-cell battery, with a nominal capacity of 210mAh.

Battery connector – CN49

Pin	Signal
1	V_{RTC}
2	GND

The battery can be connected to the board using dedicated connector CN49 which is a 2-pin p1.27 mm type HR p/n A1250WRA-S-02PNLNG1G00R or equivalent, with pinout shown in the table on the left.



In case of exhaustion, the battery should only be replaced with devices of the same type. Always check the orientation before inserting and make sure that they are aligned correctly and are not damaged or leaking.

Never allow the batteries to become short-circuited during handling.

! CAUTION: handling batteries incorrectly or replacing with not-approved devices may present a risk of fire or explosion.

Batteries supplied with the board are compliant to requirements of European Directive 2006/66/EC regarding batteries and accumulators. When putting out of order the board, remove the batteries from the board in order to collect and dispose them according to the requirement of the same European Directive above mentioned. Even when replacing the batteries, the disposal has to be made according to these requirements.

2.3.3 Power rails naming convention

In all the tables contained in this manual, Power rails are named with the following meaning:

_RUN: Switched voltages, i.e. power rails that are active only when the board is in ACPI's S0 (Working) state. Examples: +3.3V_RUN, +5V_RUN.

_ALW: Always-on voltages, i.e. power rails that are active both in ACPI's S0 (Working), S3 (Standby) and S5 (Soft Off) state. Examples: +5V_ALW, +3.3V_ALW.

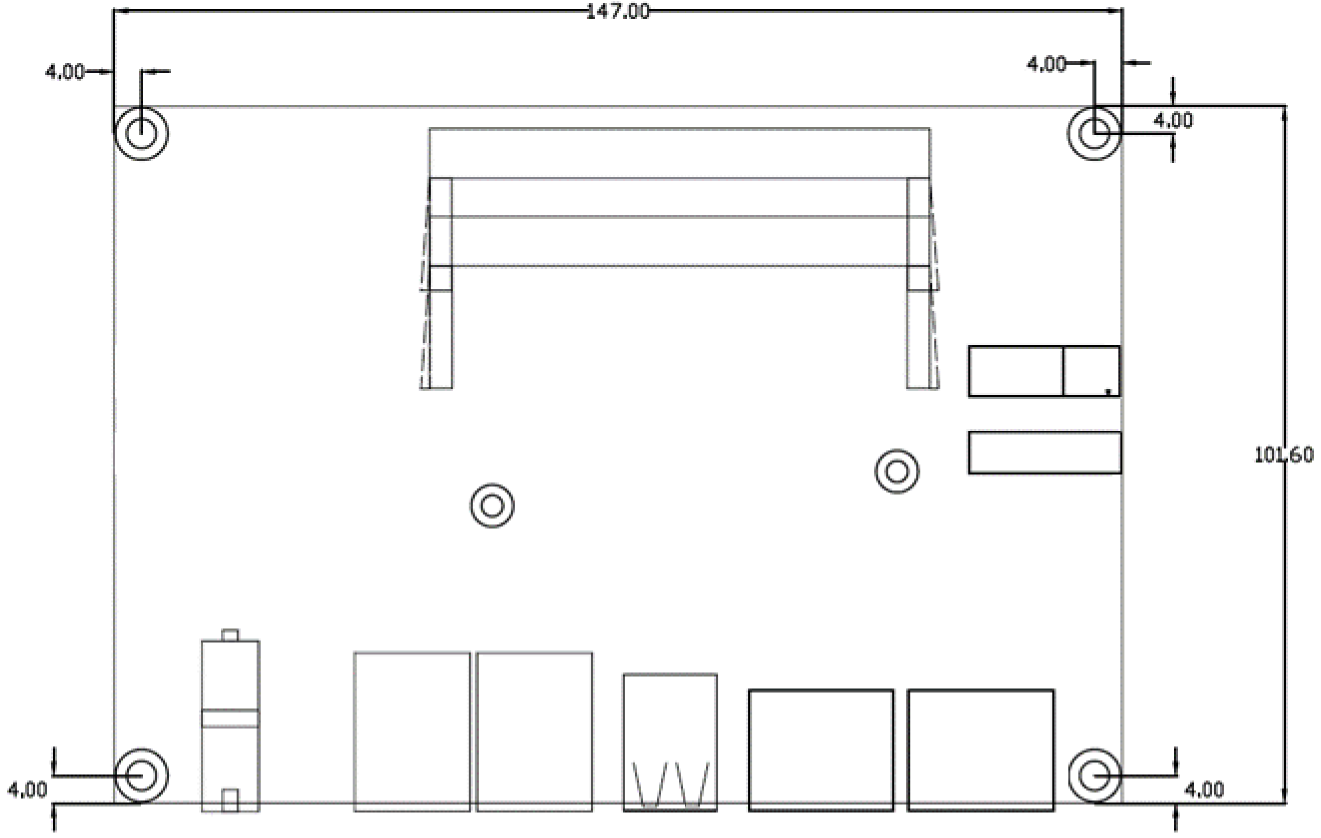
_U: unswitched ACPI S3 voltages, i.e. power rails that are active both in ACPI's S0 (Working) and S3 (Standby) state. Examples: +1.5V_U

Other suffixes are used for application specific power rails, which are derived from same voltage value of voltage switched rails, if it is not differently stated (for example, $+5V_{HDMI}$ is derived from +5V_RUN, and so on).

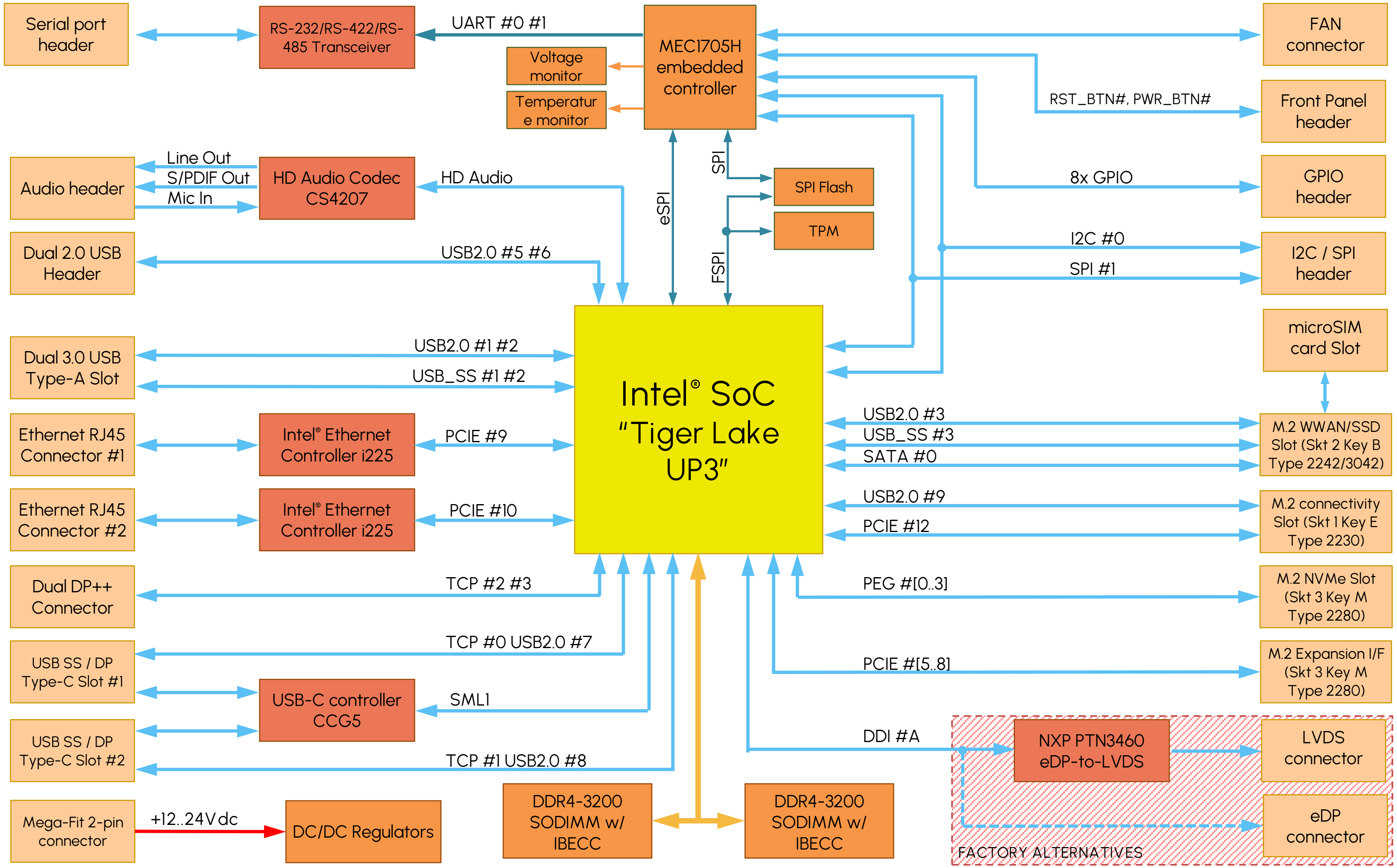
2.4 Mechanical specifications

Board dimensions are 146 x 102 mm (5,75" x 4,02").

The printed circuit of the board is made of ten layers, some of them are ground planes, for disturbance rejection.



2.5 Block diagram



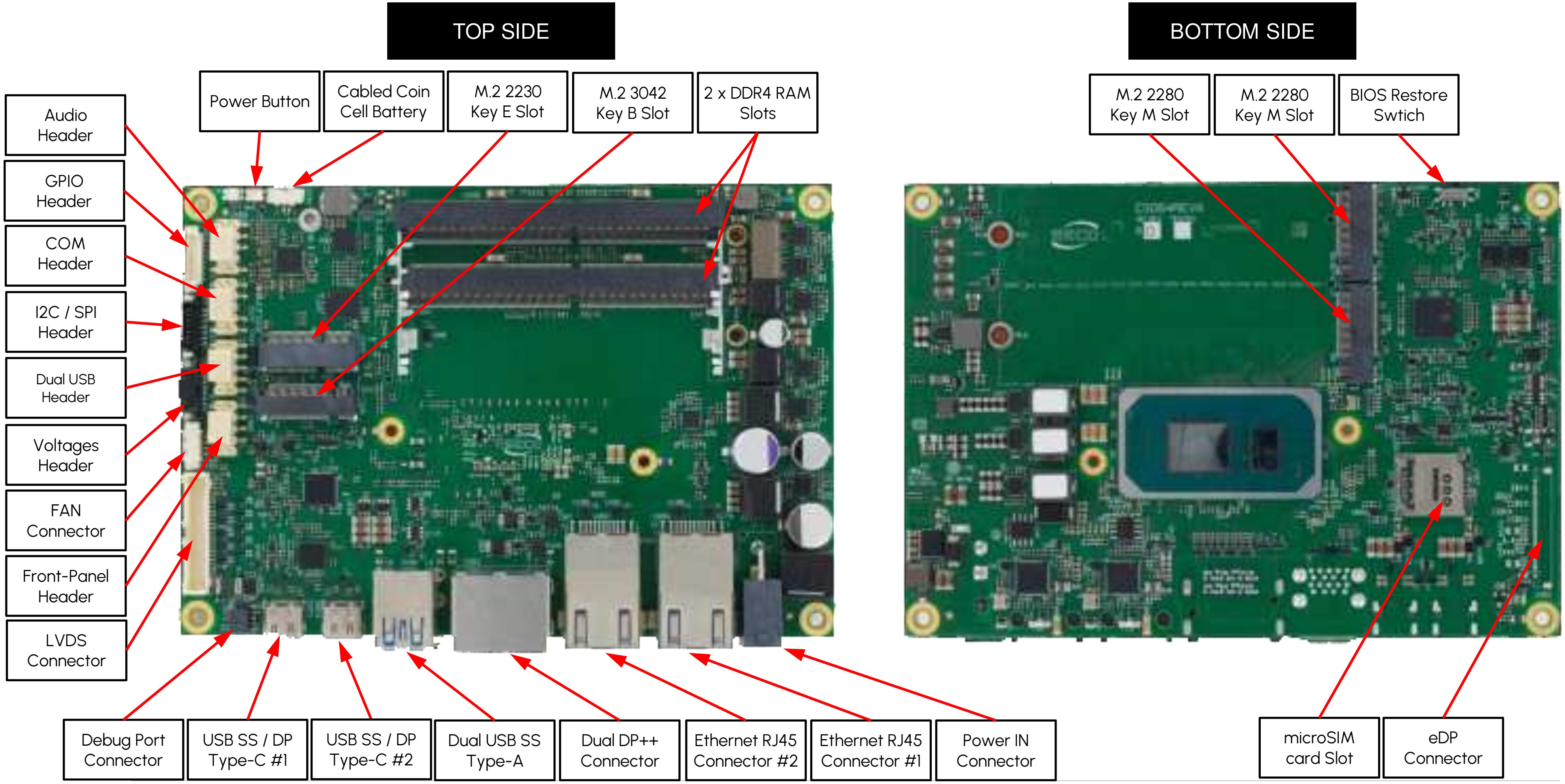
Chapter 3.
CONNECTORS

- Introduction
- Connectors overview
- Connectors description

3.1 Introduction

On the board, there are several slots located on the bottom side. Standard connectors are all placed on the top side and facing the same direction to be available on the same panel of an eventual enclosure.

> **!** Please be aware that, depending on the configuration purchased, the appearance of the board could be slightly different from the following pictures.



3.2 Connectors overview

Name	Description	Name	Description
CN49	Cabled Coin Cell Battery Connector	CN65	Voltages Header
CN50	DDR4 SODIMM Slot #A	CN66	Front Panel Header
CN51	DDR4 SODIMM Slot #B	CN67	microSIM card Slot
CN52 / CN53	Power IN Vertical / Horizontal	CN68	M.2 3042 Socket 2 Key B (SATA + WWAN)
CN54 / CN55	FAN connector 4-Wire / 3-Wire	CN69	M.2 2230 Socket 1 Key E (Connectivity Slot)
CN56	Ethernet RJ-45 Connector #1	CN70	M.2 2280 Socket 3 Key M (NVMe + Expansion Slot)
CN57	Ethernet RJ-45 Connector #2	CN71	M.2 2280 Socket 3 Key M (NVMe Slot)
CN58	Audio Header	CN72	COM Port Internal Header
CN59	Dual 3.0 USB Type-A	CN73	USB SS / DP Type-C #1
CN60	Dual 2.0 USB Header	CN74	USB SS / DP Type-C #2
CN61	Dual DP++ Connector	CN75	Debug Port Connector
CN62	eDP connector	CN76	GPIO Header
CN63	LVDS Connector	SW1	BIOS Reset Switch
CN64	I2C / SPI Header	SW2	Power Button

3.3 Connectors description

3.3.1 DDR4 SO-DIMM Sockets

CPUs used on the board provide support for DDR4-3200 SO-DIMM Memory Modules, up to 64GB total, which can be integrated by using the dedicated DDR4 SO-DIMM sockets:

CN50 is type LOTES p/n ADDR0110-P003A or equivalent, right angle socket, h = 9.2mm.

CN51 is type LOTES p/n ADDR0208-P003A or equivalent, right angle socket, h = 5.2mm.

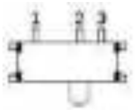
Both of them are usually used for high speed system memory applications.

3.3.2 BIOS Restore switch

In some cases, a wrong configuration of BIOS parameters could lead the module in an unusable state (i.e. no video output, all USB HID devices disabled).

For these cases, on the board has been placed a 3-way switch SW1 which can be used to restore the BIOS to factory default configuration. To do so, it is necessary to place the contact of the switch in 2-3 position, then turn on the module, wait until the board has started regularly then turn off the module. The contact MUST be now placed back to 1-2 position.

During normal use, the contact MUST be always placed in 1-2 position.



3.3.3 Debug port

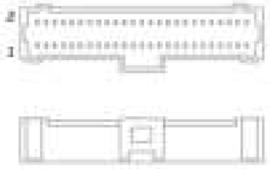
Debug port – CN75

Pin	Signal	Pin	Signal
1	+3.3V	2	SWD_IO
3	GND	4	SWD_CLK
5	GND	6	---
7	---	8	---
9	GND	10	XRES

3.3.4 LVDS Interface Connector

LVDS connector – CN63

Pin	Signal	Pin	Signal
1	VDD_LCD	2	VDD_BKLT
3	VDD_LCD	4	VDD_BKLT
5	VDD_LCD	6	VDD_BKLT
7	3.3V_RUN	8	GND
9	GND	10	LVDS_A0+ / eDP_0+
11	LVDS_A1+ / eDP_1+	12	LVDS_A0- / eDP_0-
13	LVDS_A1- / eDP_1-	14	GND
15	GND	16	LVDS_A2+ / eDP_2+
17	LVDS_A3+ / eDP_3+	18	LVDS_A2- / eDP_2-
19	LVDS_A3- / eDP_3-	20	GND
21	GND	22	LVDS_A_CLK+ / eDP_AUX+
23	LVDS_B0+	24	LVDS_A_CLK- / eDP_AUX-
25	LVDS_B0-	26	GND
27	GND	28	LVDS_B1+
29	LVDS_B2+	30	LVDS_B1-
31	LVDS_B2-	32	GND
33	GND	34	LVDS_B3+
35	LVDS_B_CLK+	36	LVDS_B3-
37	LVDS_B_CLK-	38	GND
39	GND	40	GND
41	BKLT_EN	42	BKLT_CTRL
43	N.C.	44	PANEL_EN
45	N.C.	46	N.C.
47	N.C.	48	N.C. / eDP_HPD
49	LVDS_DID_DAT	50	LVDS_DID_CLK



The board can be interfaced to LCD displays using its LVDS interface, which allows connecting 18 or 24 bit, single or dual channel displays. This interface is a factory alternative to an eDP interface with dedicated connector (see next paragraph).

The LVDS interface is implemented using an eDP to LVDS bridge (NXP PTN3460), which allow the implementation of a Dual Channel LVDS, with a maximum supported resolution of 1920x1200 @ 60Hx (dual channel mode). Such an interface is derived from Processor's eDP Interface.

For the connection, a connector type MOLEX 501190-5017 or equivalent (2 x 25p, male, straight, P1, low profile, polarised) is provided.

Mating connector, MOLEX 501189-5010 with crimp terminals series 501334.

On the same connectors, are also implemented signals for direct driving of display's backlight: voltages (VDD_LCD and VDD_BKLT) and control signals (LCD enable signal, PANEL_EN, Backlight enable signal, BKLT_EN, and Backlight Brightness Control signal, BKLT_CTRL).

There are also the signals necessary for driving I2C touchscreens (I2C signals, reset and interrupt request signals).

When building a cable for connection of LVDS displays, please take care of twist as tight as possible differential pairs' signal wires, in order to reduce EMI interferences. Shielded cables are also recommended.

VDD_LCD: LCD Voltage rail. Its value can be set to +3.3V_RUN or +5V_RUN by factory configuration of the circuit breakers BR4 (+5V_RUN) and BR5 (+3.3V_RUN).

VDD_BKLT: Backlight Voltage rail. Its value can be set to +5V_ALW or +12V_ALW by factory configuration of the circuit breakers BR1 (+12V_ALW), BR2 (VIN_FILT) and BR3 (+5V_RUN).

Signal description

LVDS_A0+/ LVDS_A0-: LVDS Channel A differential data pair #0.

LVDS_A1+/ LVDS_A1-: LVDS Channel A differential data pair #1.

LVDS_A2+/ LVDS_A2-: LVDS Channel A differential data pair #2.

LVDS_A3+/ LVDS_A3-: LVDS Channel A differential data pair #3.

LVDS_A_CLK+/LVDS_A_CLK-: LVDS Channel A differential Clock.

LVDS_B0+/ LVDS_B0-: LVDS Channel B differential data pair #0.

LVDS_B1+/ LVDS_B1-: LVDS Channel B differential data pair #1.

LVDS_B2 +/ LVDS_B2-: LVDS Channel B differential data pair #2.

LVDS_B3+/ LVDS_B3-: LVDS Channel B differential data pair #3.

LVDS_B_CLK+/LVDS_B_CLK-: LVDS Channel B differential Clock.

LVDS_I2C_DAT: DisplayID I2C Data line for LVDS flat Panel detection. Bidirectional signal, electrical level +3.3V_RUN with a 2k2Ω pull-up resistor.

LVDS_I2C_CLK: DisplayID I2C Clock line for LVDS flat Panel detection. Bidirectional signal, electrical level +3.3V_RUN with a 2k2Ω pull-up resistor.

3.3.5 eDP Interface Connector

Standard 40 poles eDP interface connector CN62 (factory alternative to LVDS interface connector CN63).

3.3.6 Multimode Display Port Connectors

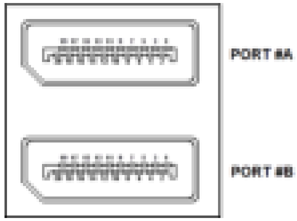
The board can offer up to four independent DP++ interfaces.

Two of these interfaces are available on a Dual DP++ connector CN61, type FOXCONN 3VD11203-DPA1-4H.

DP Port #0 will be available on Port #A of CN61 while DP Port #1 will be available on Port #B of CN61 (see image on the right).

The other two interfaces are available on USB Type-C connectors in alternate mode.

DP Port #2 will be available on CN74 while DP Port #3 will be available on CN73 (see next paragraph).

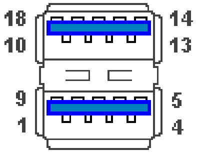


3.3.7 USB Connectors

The board offers USB ports in many different standard connectors.

USB 3.2 Gen2x1 ports Type-A double receptacle – CN59

Pin	Signal	Pin	Signal
1	+5V$_{USB1}$	10	+5V$_{USB2}$
2	USB_H0-	11	USB_H1-
3	USB_H0+	12	USB_H1+
4	GND	13	GND
5	USB_SSRX0-	14	USB_SSRX1-
6	USB_SSRX0+	15	USB_SSRX1+
7	GND	16	GND
8	USB_SSTX0-	17	USB_SSTX1-
9	USB_SSTX0+	18	USB_SSTX1+



USB 3.2 Gen2x1 ports are carried to a double type-A USB 3.0 receptacle, CN59, type Würth Elektronik p/n 692141030100 or equivalent.

More specifically, USB 3.2 port #0 is carried to the lower USB receptacle of CN12, while USB 3.2 port #1 is carried to the upper USB receptacle of CN59.

Since this connector is a standard type receptacle, it can be connected to all types of USB 1.x / USB 2.x / USB 3.x devices using standard Type-A USB 3.x or USB 2.x plugs.

For USB 3.x connections it is mandatory the use of SuperSpeed certified cables, whose SuperSpeed differential pairs are individually shielded inside the global cable's external shielding.

Signal description:

USB_H0+/USB_H0-: USB 2.0 Port #0 differential pair

USB_SSRX0+/USB_SSRX0-: USB Super Speed Port #0 receive differential pair

USB_SSTX0+/USB_SSTX0-: USB Super Speed Port #0 transmit differential pair

USB_H1+/USB_H1-: USB Port #1 differential pair;

USB_SSRX1+/USB_SSRX1-: USB Super Speed Port #1 receive differential pair

USB_SSTX1+/USB_SSTX1-: USB Super Speed Port #1 transmit differential pair

Common mode chokes are placed on all USB differential pairs for EMI compliance.

For ESD protection, on all data and voltage lines are placed clamping diodes for voltage transient suppression.

Other than the two USB 3.2 Gen2x1 ports available through the standard connector CN59, there are two USB 3.2 Gen2x1 ports available on standard USB 4.0 Type-C sockets, CN73 and CN74, both supporting Power Delivery functionality.

USB 3.2 Gen2x1 port#1 Type-C socket – CN73

Pin	Signal	Pin	Signal
A1	GND	B12	GND
A2	USBC0-_Tx0+	B11	USBC0_Rx0+
A3	USBC0_Tx0-	B10	USBC0_Rx0-
A4	VBUS_C0	B9	VBUS_C0
A5	USBC0_CC1	B8	USBC0_SBU2
A6	USB0_D1+	B7	USB0_D1-
A7	USB0_D1-	B6	USB0_D1+
A8	USBC0_SBU1	B5	USBC0_CC2
A9	VBUS_C0	B4	VBUS_C0
A10	USBC0_Rx1-	B3	USBC0_Tx1-
A11	USBC0_Rx1+	B2	USBC0_Tx1+
A12	GND	B1	GND

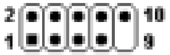
USB3.2 Gen2x1 port#2 Type-C socket – CN74

Pin	Signal	Pin	Signal
A1	GND	B12	GND
A2	USBC1_Tx0+	B11	USBC1_Rx0+
A3	USBC1_Tx0-	B10	USBC1_Rx0-
A4	VBUS_C1	B9	VBUS_C1
A5	USBC1_CC1	B8	USBC1_SBU2
A6	USB1_D1+	B7	USB1_D1-
A7	USB1_D1-	B6	USB1_D1+
A8	USBC1_SBU1	B5	USBC1_CC2
A9	VBUS_C1	B4	VBUS_C1
A10	USBC1_Rx1-	B3	USBC1_Tx1-
A11	USBC1_Rx1+	B2	USBC1_Tx1+
A12	GND	B1	GND

Dual USB 2.0 Internal Header #4 #5 – CN60

Pin	Signal	Pin	Signal
1	$+5V_{USB0}$	2	$+5V_{USB3}$
3	USB_P4-	4	USB_P5-
5	USB_P4+	6	USB_P5+
7	GND	8	GND
		10	---

There are also two additional USB 2.0 ports (USB #4 and USB #5), which are hosted on a 9-pin p2.54mm pin header, h= 6mm, type NELTRON p/n 2213SM-10G-E9-CR or equivalent, with the pinout shown in the tables on the left (it is a common pinout for USB headers in PC motherboards).



All USB ports' voltages ($+5V_{USBx}$) are derived from +5V_ALW standby voltages. This means that the ports can be powered also when the OS is in Suspend-to-RAM (S3) state in order to support (if enabled) e the "Wake-Up on USB" functionality.

Signal description:

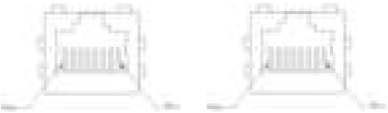
USB_P4+/USB_P4-: USB Port #4 differential pair

USB_P5+/USB_P5-: USB Port #5 differential pair

Common mode chokes are placed on all USB differential pairs for EMI compliance.

For ESD protection, on all data and voltage lines are placed clamping diodes for voltage transient suppression.

3.3.8 2.5 Gigabit Ethernet connectors



On board, there are two 2.5 Gigabit Ethernet connectors, for the direct connection of the board to two different wired LANs.

The Ethernet connections are realised using two distinct Intel® I225 Gigabit Ethernet controllers.

This interface is compatible with 2.5 Gigabit Ethernet (2.5Gbps) and Fast Ethernet (10/100Mbps) Networks. Configuration is automatic to work with the existing network.

Please be aware that it will work in 2.5 Gigabit mode only in case that it is connected to 2.5 Gigabit Ethernet switches/hubs/routers. For the connection, cables category Cat5e or better are required. Cables category Cat6 are recommended for noise reduction and EMC compatibility issues, especially when the length of the cable is significant.

Placed below each Ethernet connector there are two LEDs, signaling 100Mbps (green LED) / 2.5Gbps (yellow LED) connection and ACTIVITY presence (green LED).

2.5 Gigabit Ethernet Port #1 – CN57

Pin	Signal	Pin	Signal
1	GBE1_MDI0+	5	GBE1_MDI2-
2	GBE1_MDI0-	6	GBE1_MDI1-
3	GBE1_MDI1+	7	GBE1_MDI3+
4	GBE1_MDI2+	8	GBE1_MDI3-

2.5 Gigabit Ethernet Port #0 – CN56

Pin	Signal	Pin	Signal
1	GBE0_MDI0+	5	GBE0_MDI2-
2	GBE0_MDI0-	6	GBE0_MDI1-
3	GBE0_MDI1+	7	GBE0_MDI3+
4	GBE0_MDI2+	8	GBE0_MDI3-

Signal description:

GBEx_MDI0+/GBEx_MDI0-: Ethernet Controller #x Media Dependent Interface (MDI) I/O differential pair #0. It is the first differential pair in 2.5 Gigabit Ethernet mode, and the Transmit differential pair in 10/100 Mbps modes.

GBEx_MDI1+/GBEx_MDI1-: Ethernet Controller #x Media Dependent Interface (MDI) I/O differential pair #1. It is the second differential pair in 2.5 Gigabit Ethernet mode, and the Receive differential pair in 10/100 Mbps modes.

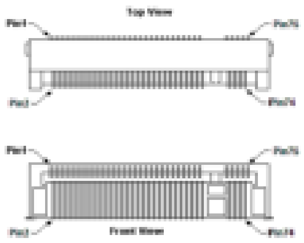
GBEx_MDI2+/GBEx_MDI2-: Ethernet Controller #x Media Dependent Interface (MDI) I/O differential pair #2. It is the third differential pair in Gigabit Ethernet mode; it is not used in 10/100Mbps modes.

GBEx_MDI3+/GBEx_MDI3-: Ethernet Controller #x Media Dependent Interface (MDI) I/O differential pair #3. It is the fourth differential pair in Gigabit Ethernet mode; it is not used in 10/100Mbps modes.

3.3.9 M.2 2280 Socket 3 Key M NVMe Slot

M.2 NVMe Slot (Socket 3 Key M type 2280) – CN71

Pin	Signal	Pin	Signal
1	GND	2	+3.3V_RUN
3	GND	4	+3.3V_RUN
5	PEG_Rx3-	6	---
7	PEG_Rx3+	8	---
9	GND	10	---
11	PEG_Tx3-	12	+3.3V_RUN
13	PEG_Tx3+	14	+3.3V_RUN
15	GND	16	+3.3V_RUN
17	PEG_Rx2-	18	+3.3V_RUN
19	PEG_Rx2+	20	---
21	GND	22	---
23	PEG_Tx2-	24	---
25	PEG_Tx2+	26	---
27	GND	28	---
29	PEG_Rx1-	30	---
31	PEG_Rx1+	32	---
33	GND	34	---
35	PEG_Tx1-	36	---
37	PEG_Tx1+	38	---
39	GND	40	---
41	PEG_Rx0-	42	---
43	PEG_Rx0+	44	---
45	GND	46	---
47	PEG_Tx0-	48	---
49	PEG_Tx0+	50	PCIE_RST#
51	GND	52	CLK_REQ0#
53	PCIE_CLK0-	54	---
55	PCIE_CLK0+	56	---
57	GND	58	---
67	---	68	---
69	---	70	+3.3V_RUN
71	GND	72	+3.3V_RUN
73	GND	74	+3.3V_RUN
75	GND		



Possibility for connecting mass storage devices is given by two M.2 Key M Slots CN71 and CN70 (see next paragraph), which allows the plugging of NVMe storage drives with PCI-e x4 interface.

CN71 is a standard 75 pin M.2 Key M connector, type LOTES p/n APCI0079-P001A, H=3.2mm, with the pinout shown in the table on the left.

On the board, a Threaded Spacer allows the placement of M.2 Socket 3 Key M PCI-e modules in 2280 size.

Signal Description

PEG_Tx0+/ PEG_Tx0-: Transmitting Output for PCI Express lane #0, Differential pair

PEG_Tx1+/ PEG_Tx1-: Transmitting Output for PCI Express lane #1, Differential pair

PEG_Tx2+/ PEG_Tx2-: Transmitting Output for PCI Express lane #2, Differential pair

PEG_Tx3+/ PEG_Tx3-: Transmitting Output for PCI Express lane #3, Differential pair

PEG_Rx0+/ PEG_Rx0-: Receiving Input for PCI Express lane #0, Differential pair

PEG_Rx1+/ PEG_Rx1-: Receiving Input for PCI Express lane #1, Differential pair

PEG_Rx2+/ PEG_Rx2-: Receiving Input for PCI Express lane #2, Differential pair

PEG_Rx3+/ PEG_Rx3-: Receiving Input for PCI Express lane #3, Differential pair

PCIE_CLK0+ / PCIE_CLK0-: Reference Clock Output #0, Differential Pair

CLK_REQ0#: Clock Request Input for Reference Clock Output #0. Active low signal, electrical level +3.3V_RUN with a 10KΩ pull-up resistor. This signal shall be driven low by any module inserted in the connectivity slot, in order to ensure that the SoC makes available the reference clock.

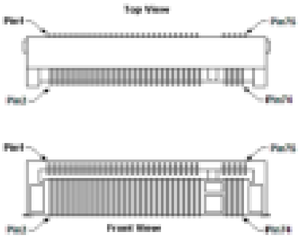
PCIE_RST#: Reset Signal that is sent from the SoC to all PCI-e devices available on the board. It is a +3.3V_RUN active-low signal.

3.3.10 M.2 2280 Socket 3 Key M expansion I/F Slot

Other than plugging of NVMe storage drives with PCI-e x4 interface, the CN70 M.2 slot allows the plugging of expansion interface modules requiring PCIe, UART and USB 3.2 signals.

CN70 is a standard 75 pin M.2 Key M connector, type LOTES p/n APCI0079-P001A, H=3.2mm, with the pinout shown in the table on the left.

On the board, a Threaded Spacer allows the placement of M.2 Socket 3 Key M PCI-e modules in 2280 size.



M.2 expansion I/F Slot (Socket 3 Key M type 2280) – CN70

Pin	Signal	Pin	Signal
1	GND	2	+3.3V_RUN
3	GND	4	+3.3V_RUN
5	PCIE_Rx8-	6	---
7	PCIE_Rx8+	8	---
9	GND	10	---
11	PCIE_Tx8-	12	+3.3V_RUN
13	PCIE_Tx8+	14	+3.3V_RUN
15	GND	16	+3.3V_RUN
17	PCIE_Rx7-	18	+3.3V_RUN
19	PCIE_Rx7+	20	PCH_UART_RTS0#
21	GND	22	---
23	PCIE_Tx7-	24	PCH_UART_TXD0
25	PCIE_Tx7+	26	PCH_UART_RXD0
27	GND	28	PCH_UART_CTS0#
29	PCIE_Rx6-	30	---
31	PCIE_Rx6+	32	---
33	GND	34	USB_P4+
35	PCIE_Tx6-	36	USB_P4-
37	PCIE_Tx6+	38	---
39	GND	40	---
41	PCIE_Rx5-	42	---
43	PCIE_Rx5+	44	---
45	GND	46	USB_SSTX4-
47	PCIE_Tx5-	48	USB_SSTX4+
49	PCIE_Tx5+	50	PCIE_RST#
51	GND	52	CLK_REQ2#
53	PCIE_CLK2-	54	---
55	PCIE_CLK2+	56	USB_SSRX4-
57	GND	58	USB_SSRX4+
67	---	68	---
69	---	70	+3.3V_RUN
71	GND	72	+3.3V_RUN
73	GND	74	+3.3V_RUN
75	GND		

Signal Description

PCIE_Tx5+/ PCIE_Tx5-: Transmitting Output for PCI Express lane #5, Differential pair

PCIE_Tx6+/ PCIE_Tx6-: Transmitting Output for PCI Express lane #6, Differential pair

PCIE_Tx7+/ PCIE_Tx7-: Transmitting Output for PCI Express lane #7, Differential pair

PCIE_Tx8+/ PCIE_Tx8-: Transmitting Output for PCI Express lane #8, Differential pair

PCIE_Rx5+/ PCIE_Rx5-: Receiving Input for PCI Express lane #5, Differential pair

PCIE_Rx6+/ PCIE_Rx6-: Receiving Input for PCI Express lane #6, Differential pair

PCIE_Rx7+/ PCIE_Rx7-: Receiving Input for PCI Express lane #7, Differential pair

PCIE_Rx8+/ PCIE_Rx8-: Receiving Input for PCI Express lane #8, Differential pair

PCIE_CLK2+ / PCIE_CLK2-: Reference Clock Output #2, Differential Pair

CLK_REQ2#: Clock Request Input for Reference Clock Output #2. Active low signal, electrical level +3.3V_RUN with a 10KΩ pull-up resistor. This signal shall be driven low by any module inserted in the connectivity slot, in order to ensure that the SoC makes available the reference clock.

PCIE_RST#: Reset Signal that is sent from the SoC to all PCI-e devices available on the board. It is a +3.3V_RUN active-low signal.

PCH_UART_TXD0: SoC PCH UART port Transmit data lane

PCH_UART_RXD0: SoC PCH UART port Receive data lane

PCH_UART_RTS0#: SoC PCH UART port Request to Send handshaking signal

PCH_UART_CTS0#: SoC PCH UART port Clear To Send handshaking signal

USB_P4+/USB_P4-: USB 2.0 Port #4 differential pair

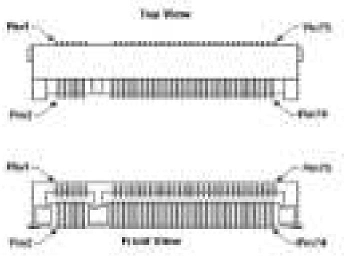
USB_SSRX4+/USB_SSRX4-: USB Super Speed Port #4 receive differential pair

USB_SSTX4+/USB_SSTX4-: USB Super Speed Port #4 transmit differential pair

3.3.11 M.2 2230 Socket 1 Key E Connectivity Slot

It is possible to increase the connectivity of the board by using M.2 Socket 1 Key E connectivity slot.

The connector used for the M.2 Connectivity slot is CN69, which is a standard 75 pin M.2 Key E connector, type LOTES p/n APCI0076-P001A, H=4.2mm, with the pinout shown in the table on the left.



On the board there is also a Threaded Spacer which allows the placement of M.2 Socket 1 Key E connectivity modules in 2230 size.

M.2 Connectivity Slot (Socket 1 Key E type 2230) – CN69

Pin	Signal	Pin	Signal
1	GND	2	+3.3V_ALW
3	USB_P10+	4	+3.3V_ALW
5	USB_P10-	6	---
7	GND	8	---
9	---	10	---
11	---	12	---
13	---	14	---
15	---	16	---
17	---	18	GND
19	---	20	---
21	---	22	---
23	---		
		32	---
33	GND	34	---
35	PCIE_Tx12+	36	---
37	PCIE_Tx12-	38	---
39	GND	40	---
41	PCIE_Rx12+	42	---
43	PCIE_Rx12-	44	---
45	GND	46	---
47	PCIE_CLK1+	48	---
49	PCIE_CLK1-	50	SUS_CLK
51	GND	52	PCIE_RST#
53	CLK_REQ1#	54	BT_DISABLE#
55	PCIE_WAKE#	56	WIFI_DISABLE#
57	GND	58	---
59	---	60	---
61	---	62	---
63	GND	64	---
65	---	66	---
67	---	68	---
69	GND	70	---
71	---	72	+3.3V_ALW
73	---	74	+3.3V_ALW
75	GND		

Signal Description

USB_P9+ / USB_P9-: USB Port #9. Differential pair

PCIE_Tx12+/PCIE_Tx12-: Transmitting Output for PCI Express lane #12, Differential pair

PCIE_Rx12+/PCIE_Rx12-: Receiving Input for PCI Express lane #12, Differential pair

PCIE_CLK1+/ PCIe_CLK1-: Reference Clock Output #1, Differential pair

CLK_REQ1#: Clock Request Input for Reference Clock Output #1. Active low signal, electrical level +3.3V_RUN with a 10KΩ pull-up resistor. This signal shall be driven low by any module inserted in the connectivity slot, in order to ensure that the SoC makes available the reference clock.

PCIE_WAKE#: Board's Wake Input, it must be externally driven by the plugged module when it requires waking up the system. Active low signal, electrical level +3.3V_RUN with a 47KΩ pull-up resistor

PCIE_RST#: Reset Signal that is sent from the SoC to all PCI-e devices available on the board. It is a +3.3V_RUN active-low signal.

SUS_CLK: 32.768kHz Clock provided by the board to the plugged module. +3.3V_ALW electrical level

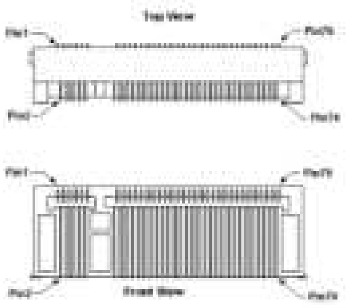
BT_DISABLE#: M.2 Key E Bluetooth module functionality disable signal #1, active low signal, +3.3V_ALW electrical level

WIFI_DISABLE#: M.2 Key E Wireless module functionality disable signal #2, active low signal, +3.3V_ALW electrical level

3.3.12 M.2 3042 Socket 2 Key B WWAN/SSD Slot

M.2 WWAN/SSD Slot (Socket 2 Key B type 2242/3042) – CN68

Pin	Signal	Pin	Signal
1	CONFIG_3	2	+3.3V_ALW
3	GND	4	+3.3V_ALW
5	GND	6	PWR_OFF#
7	USB_P2+	8	W_DISABLE1#
9	USB_P2-	10	---
11	GND		
		20	---
21	CONFIG_0	22	---
23	WAKE_ON_WWAN#	24	---
25	---	26	W_DISABLE2#
27	GND	28	---
29	USB_SSRX2-	30	UIM_RST#
31	USB_SSRX2+	32	UIM_CLK
33	GND	34	UIM_DATA
35	USB_SSTX2-	36	UIM_PWR
37	USB_SSTX2+	38	---
39	GND	40	---
41	PCIe_Rx+ / SATA_Rx+	42	---
43	PCIe_Rx- / SATA_Rx-	44	---
45	GND	46	---
47	PCIe_Tx-/ SATA_Tx+	48	---
49	PCIe_Tx+ / SATA_Tx+	50	PCIE_RST#
51	GND	52	CLK_REQ3#
53	PCIe_CLK3-	54	M.2_WAKE#
55	PCIe_CLK3+	56	---
57	GND	58	---
59	---	60	---
61	---	62	---
63	---	64	---
65	---	66	---
67	---	68	SUS_CLK
69	CONFIG_1	70	+3.3V_ALW
71	GND	72	+3.3V_ALW
73	GND	74	+3.3V_ALW
75	CONFIG_2		



It is possible to increase the networking possibilities of the board by using M.2 Socket 2 Key B WWAN modules (i.e. modem modules) or alternatively increase storage capabilities by using M.2 Socket 2 Key B SATA drives (i.e. SSD).

The connector used for the M.2 WWAN / SATA slot is CN68, which is a standard 75 pin M.2 Key B connector, type LOTES p/n APCI0087-P001A, H=8.5mm, with the pinout shown in the table on the left.

Othe bottom side of the board is located a standard microSIM slot, CN67, for enabling the WWAN module communication. For ESD protection, on all signal lines are placed clamping diodes for voltage transient suppression.

For increasing storage capabilities, in place of installing a WWAN module, the CN68 slot offers a SATA interface for using M.2 Socket 2 Key B SSD modules. On the board there is a Threaded Spacer which allows the placement of M.2 Socket 2 Key B WWAN, or SSD modules, in 2242 or 3042 size.

Signal Description

USB_P2+ / USB_P2-: USB Port #2, Differential pair

USB_SSRX2+/USB_SSRX2-: USB Super Speed Port #2 receive, Differential pair

USB_SSTX2+/USB_SSTX2-: USB Super Speed Port #2 transmit, Differential pair

PCIe_Tx+/SATA_Tx+ / PCIe_Tx-/SATA_Tx-: PCI Express lane / SATA interface, Transmitting Output, Differential pair
PCIe_Rx+/SATA_Rx+ / PCIe_Rx-/SATA_Rx-: PCI Express lane / SATA interface, Receiving Input, Differential pair
PCIe_CLK3+/ PCIe_CLK3-: PCI Express Reference Clock for lane, Differential pair

WAKE_ON_WWAN#: Board's Wake Input, 1.8V_ALW active low signal with 100kΩ pull-up resistor. It must be externally driven by the Connectivity module plugged in the slot when it requires waking up the system.

PWR_OFF#: Power Off signal for plugged modules, usually used in battery-powered systems. Fixed 20kΩ pull-up @ 3.3V_ALW

W_DISABLE1#: M.2 Key B module disable signal #1, active low output

W_DISABLE2#: M.2 Key B module disable signal #2, active low output

UIM_RST#: Reset signal line, sent from M.2 WWAN card to the UIM module.

UIM_DATA: Bidirectional Data line between M.2 WWAN card and UIM module.

UIM_CLK: Clock line, output from M.2 WWAN card to the UIM module.

UIM_PWR: Power line for UIM module.

PCIE_RST#: Reset Signal that is sent from the SoC to all PCI-e devices available on the board. It is a +3.3V_RUN active-low signal.

CONFIG_[0..3]: Configuration inputs, +3.3V_ALW signals with 10kΩ pull-up. These signals are used to configure properly the Main Host interface according to the Add-In Card plugged in CN20 Slot. These configuration pins are managed according to PCI Express M.2 Specifications Table 5.5.

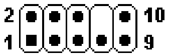
3.3.13 Audio Header

HD Audio Front Panel Header – CN58

Pin	Signal	Pin	Signal
1	Mic_In_L	2	Audio_GND
3	Mic_In_R	4	S/PDIF_Out
5	Line_Out_R	6	Sense1_Return
7	Audio_GND		
9	Line_Out_L	10	Sense2_Return

The board integrates an High Definition Audio Codec, Cirrus Logic CS4207-CNRZ, for high quality audio implementation.

In order to give the maximum flexibility to the board, it is available a dedicated AAFP (Analog Audio Front Panel) connector CN58, 2x5 2.54mm pitch Pin header, for external connection of a Line Out output, a Mic In input and also an S/PDIF Output.



Pinout hereby shown is compliant to standard HD Audio front panel connectors.

Signal Description

Mic_In_L: Analog Port 1 - Microphone Left Channel, full-scale input voltage range -2V ÷ +2V

Mic_In_R: Analog Port 1 - Microphone Right Channel, full-scale input voltage range -2V ÷ +2V

Sense1_Return: Analog Port 1 –Mic Jack detection return signal, active low.

Line_Out_L: Analog Port 2 – Line Out Left Channel, full-scale output voltage range -2V ÷ +2V

Line_Out_R: Analog Port 2 – Line Out Right Channel, full-scale output voltage range -2V ÷ +2V

Sense2_Return: Analog Port 2 – Line Jack detection return signal, active low.

S/PDIF_Out: S/PDIF AC-coupled output.

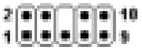
3.3.14 COM Port Header

Dual RS-232/RS-422/RS-485 pin header- CN72

Pin	Signal RS-232 mode	Signal RS-422 mode	Signal RS-485 mode
1	COM0_RxD	COM0_Rx+	
2	COM1_RxD	COM1_Rx+	
3	COM0_TxD	COM0_Tx-	COM0_Data-
4	COM1_TxD	COM1_Tx-	COM1_Data-
5	GND	GND	GND
7	COM0_RTS#	COM0_Tx+	COM0_Data+
8	COM1_RTS#	COM1_Tx+	COM1_Data+
9	COM0_CTS#	COM0_Rx-	
10	COM1_CTS#	COM1_Rx-	

The embedded controller of the board manages two 4-wire legacy UARTs, which are carried to as many multistandard RS-232/RS-422/RS-485 transceivers, allowing the implementation of two multistandard serial ports (from now on respectively named COM0 and COM1).

These ports are available on dedicated connector CN72, which is an internal 9-pin standard male pin header, p 2.54 mm, 5+4 pin, h = 6mm, type NELTRON p/n 2213S-10G-E06 or equivalent.



The selection of the kind of interface (RS-232, RS-422 or RS-485) can be made via BIOS.

Please be aware that for proper RS-485 working, the RTS# signals must be used as a handshaking signal, i.e. it is used to control the data flow direction. When RTS# signal is driven low, then the RS-485 port is in receiving mode, when RTS# signal is driven high then the RS-458 port is in transmitting mode.

Signal Description

COM0_RxD/COM1_RxD: COM port #0 / #1 RS-232 Receive data lane

COM0_TxD/COM1_TxD: COM port #0 / #1 RS-232 Transmit data lane

COM0_RTS#/COM1_RTS#: COM port #0 / #1 RS-232 Request to Send handshaking signal.

COM0_CTS#/COM1_CTS#: COM port #0 / #1 RS-232 Clear To Send handshaking signal

COM0_RX+/COM0_RX-: COM port #0 RS-422 receive differential pair

COM0_TX+/COM0_TX-: COM port #0 RS-422 Transmit differential pair

COM1_RX+/COM1_RX-: COM port #1 Full Duplex RS-485 (RS-422) Receive differential pair

COM1_TX+/COM1_TX-: COM port #1 Full Duplex RS-485 (RS-422) Transmit differential pair

COM0_Data+/COM0_Data-: COM Port #0 Half Duplex RS-485 Differential Pair

COM1_Data+/COM1_Data-: COM Port #1 Half Duplex RS-485 Differential Pair

3.3.15 Front Panel Header

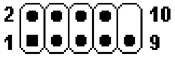
Buttons / LED Header – CN66

Pin	Signal	Pin	Signal
1	HD_LED_P	2	FP PWR_P/SLP_N
3	HD_LED_N	4	FP PWR_N/SLP_P
5	RST_SW_N	6	PWR_SW_P
7	RST_SW_P	8	PWR_SW_N
9	---		

To allow the integration of the board inside a box PC-like, there is a connector on the board that allows to remote signals for the Power Button (to be used to put the system in a Soft Off State, or awake from it), for the Reset Button, and the signal for optional LED signaling activity on SATA Channel and Power On states.

The pinout of this connector complies with Intel® Front Panel I/O connectivity Design Guide, Switch/LED Front Panel section, chapter 2.2. It is shown in the table on the left.

Connector CN6 is an internal 9-pin standard male pin header, p 2.54 mm, 5+4 pin, h= 6mm, type NELTRON p/n 2213SM-10G-E10 or equivalent.



The power button input (pins #6 and #8) is also connected to the on-board power button SW2, located on the top side of the board.

Signals Description:

HD_LED_P: Hard Disk Activity LED signal's pull-up to +5V_RUN voltage (510Ω pull-up).

HD_LED_N: Hard Disk Activity LED output signal

RST_SW_N: Reset Button GND

RST_SW_P: Reset button input signal. This signal has to be connected to an external momentary pushbutton (contacts normally open). When the pushbutton is pressed, the pulse of Reset signal will cause the reset of the board. +3.3V_ALW electrical level with 4.7kΩ pull-up.

PWR_SW_P: Power button input signal, +3.3V_ALW electrical level with 4.7kΩ pull-up. This signal has to be connected to an external momentary pushbutton (contacts normally open). Upon the pressure of this pushbutton, the pulse of this signal will let the switched voltage rails turn on or off.

PWR_SW_N: Power button GND

FP PWR_P/SLP_N: Power/Sleep messaging LED terminal 1 with 510Ω pull-up resistor to +5V_ALW voltage. Connect it to an extremity of a dual-color power LED for power ON/OF, sleep and message waiting signaling. Please refer to Intel® Front Panel I/O connectivity Design Guide, chapter 2.2.4, for LED functionalities and signal meaning.

FP PWR_N/SLP_P: Power/Sleep messaging LED terminal 2 with 510Ω pull-up resistor to +5V_ALW voltage. Connect it to the other extremity of the dual-color power LED above mentioned.

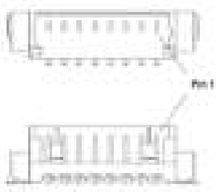
3.3.16 GPIO Header

GPIO Header – CN76

Pin	Signal	Pin	Signal
1	EXT_GPIO0	2	EXT_GPIO1
3	EXT_GPIO2	4	EXT_GPIO3
5	EXT_GPIO4	6	EXT_GPIO5
7	EXT_GPIO6	8	EXT_GPIO7

Managed by the Embedded Controller, on the board there are 8 (eight) GPIOs at electrical level 3.3V (5V tolerant).

Access to these General Purpose I/Os is available on a 8-pin male connector, type MOLEX p/n 53398-0871 or equivalent, with the pinout shown in the tables on the left.



Signal Description

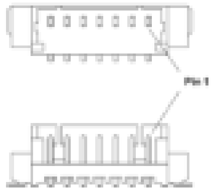
EXT_GPIO*n*: general purpose Input / Output line, as Input 3.3V level and 5V tolerant, as Output 0V and 3.3V levels.

3.3.17 I2C/SPI Header

I2C/SPI Header – CN64

Pin	Signal	Pin	Signal
1	GND	2	I2C0_SCL
3	I2C0_SDA	4	SPI_CS#
5	SPI_MOSI	6	SPI_MISO
7	SPI_CLK		

The dedicated connector is a 7-pin male connector, type HR p/n A1250WV-S-07P or equivalent,
with pinout shown in the table on the left.



Signal Description

I2C0_SCL: general purpose I2C Bus clock line. Output signal, electrical level +3.3V_ALW with a 4k7Ω pull-up resistor.

I2C0_SDA: general purpose I2C Bus data line. Input/Output signal, electrical level +3.3V_ALW with a 4k7Ω pull-up resistor.

SPI_CS#: SPI chip select, output signal, active low, electrical level +3.3V

SPI_MOSI: SPI Master Output Slave Input, output signal, electrical level +3.3V

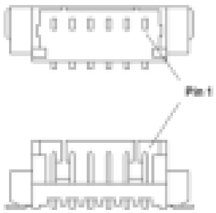
SPI_MISO: SPI Master Input Slave Output, input signal, electrical level +3.3V
SPI_CLK: SPI Serial Clock, electrical level +3.3V

3.3.18 Voltages Header

Voltages Header – CN65

Pin	Signal	Pin	Signal
1	+12V_EXT	2	+5V_EXT
3	+3.3V_EXT	4	GND
5	GND	6	GND

The dedicated connector is a 6-pin male connector, type HR p/n A1250WV-S-06P or equivalent,
with pinout shown in the table on the left.



Signal Description:

+12V_EXT: Dedicated +12V power rail for external use, obtained by +12V_ALW through a power switch (limited to 1.0A)
+5V_EXT: Dedicated +5V power rail for external use, obtained by +5V_ALW through a power switch (limited to 0.7A)
+3.3V_EXT: Dedicated +3.3V power rail for external use, obtained by +3.3V_ALW through a power switch (limited to 0.7A)

3.3.19 FAN Connectors

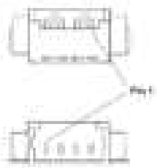
Depending on the use case, on the board is available a 4-pin dedicated connector for an external +12V_{DC} FAN.

4-Wire FAN Connector – CN54

Pin	Signal
1	GND
2	FAN_POWER
3	FAN_TACHO_IN
4	FAN_PWM

The default FAN Connector is a 4-pin single line SMT connector, type HR p/n A1250WRA-S-04PNLNG1G00R or equivalent, with pinout shown in the table on the left.

Mating connector: MOLEX 51021-0400 receptacle with MOLEX 50079-8000 female crimp terminals.

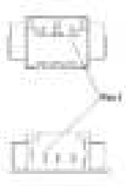


3-Wire FAN Connector – CN55

Pin	Signal
1	GND
2	FAN_POWER
3	FAN_TACHO_IN

Alternatively, as a factory option, the board can be equipped with a 3-pin single line SMT connector, type MOLEX 53261-0371 or equivalent, with pinout shown in the table on the left.

Mating connector: MOLEX 51021-0300 receptacle with MOLEX 50079-8000 female crimp terminals.



Signal Description:

FAN_POWER: +12V_{IN} derived power rail for FAN, managed by the embedded microcontroller via PWM signal

FAN_TACHO_IN: tachometric input from the fan to the embedded microcontroller, +3.3V_RUN electrical level signal with 10kΩ pull-up resistor.

FAN_PWM: PWM output from the embedded microcontroller to the FAN (4-pin connector only).

Chapter 4.
BIOS SETUP

- Aptio setup Utility
- Main setup menu
- Advanced menu
- Chipset menu
- Security menu
- Boot menu
- Save & Exit menu

4.1 Aptio setup Utility

Basic setup of the board can be done using American Megatrends, Inc. "Aptio Setup Utility", that is stored inside an onboard SPI Serial Flash.

It is possible to access to Aptio Setup Utility by pressing the <ESC> key after System power up, during POST phase. On the splash screen that will appear, select "SCU" icon.

On each menu page, on left frame are shown all the options that can be configured.

Grayed-out options are only for information and cannot be configured.

Only options written in blue can be configured. Selected options are highlighted in white.

Right frame shows the key legend.

KEY LEGEND:

← / → Navigate between various setup screens (Main, Advanced, Security, Power, Boot...)

↑ / ↓ Select a setup item or a submenu

+ / - + and - keys allows to change the field value of highlighted menu item

<F1> The <F1> key allows displaying the General Help screen.

<F2> Previous Values

<F3> <F3> key allows loading Optimised Defaults for the board. After pressing <F3> BIOS Setup utility will request for a confirmation, before loading such default values. By pressing <ESC> key, this function will be aborted

<F4> <F4> key allows save any changes made and exit Setup. After pressing <F10> key, BIOS Setup utility will request for a confirmation, before saving and exiting. By pressing <ESC> key, this function will be aborted

<ESC> <Esc> key allows discarding any changes made and exit the Setup. After pressing <ESC> key, BIOS Setup utility will request for a confirmation, before discarding the changes. By pressing <Cancel> key, this function will be aborted

<ENTER> <Enter> key allows to display or change the setup option listed for a particular setup item. The <Enter> key can also allow displaying the setup sub- screens.

4.2 Main setup menu

When entering the Setup Utility, the first screen shown is the Main setup screen. It is always possible to return to the Main setup screen by selecting the Main tab.

In this screen, are shown details regarding BIOS version, Processor type, Bus Speed and memory configuration.

Only two options can be configured:

4.2.1 System Date / System Time

Use this option to change the system time and date. Highlight System Time or System Date using the <Arrow> keys. Enter new values directly through the keyboard, or using + / - keys to increase / reduce displayed values. Press the <Enter> key to move between fields. The date must be entered in MM/DD/YY format. The time is entered in HH:MM:SS format.

Note: The time is in 24-hour format. For example, 5:30 A.M. appears as 05:30:00, and 5:30 P.M. as 17:30:00.

The system date is in the format mm/dd/yyyy.

4.3 Advanced menu

Menu Item	Options	Description
CPU Configuration	→	Display CPU Configuration Parameters
Power & Performance	See submenu	Power & Performance Options
PCH-FW Configuration	See submenu	Configure Management Engine Technology Parameters
Platform Settings	See submenu	Platform related settings
Intel Time Coordinated Computing	See submenu	Intel Time Coordinated Computing (TCC) options
Battery Failure Manager	→	Recovery action when a backup battery failure occurs: None / Restore Defaults / Reset NVRAM
Trusted Computing	See submenu	Trusted Computing Settings
SMART Settings	→	Enable/Disable Run SMART Self Test on all HDDs during POST
S5 RTC Wake Settings	→	Enable/Disable System wake on alarm event
UEFI Variables Protection	→	Enable/Disable Control the NVRAM Runtime Variable protection through System Admin Password
Serial Port Console Redirection	See submenu	Serial Port Console Redirection
Intel TXT Information	→	Display Intel TXT Information
AMI Graphic Output Protocol Policy	See submenu	User Selected Monitor Output by Graphic Output protocol
USB Configuration	See submenu	USB Configuration Parameters
Network Stack Configuration	See submenu	Network Stack Settings
NVMe Configuration	See submenu	NVMe Device Options Settings
SDIO Configuration	See submenu	SDIO Configuration Parameters
SMBIOS Information	→	Display SMBIOS Information
Super I/O Configuration	See submenu	Super I/O Setup Configuration Utility
Main Thermal Configuration	See submenu	Main Thermal Configuration
LVDS Configuration	See submenu	LVDS Configuration
Embedded Controller	See submenu	Embedded Controller
Tls Auth Configuration	See submenu	Tls Auth Configuration
RAM Disk Configuration	See submenu	Add/remove RAM disks
Intel Ethernet Contrller I225-LM - ***MAC***	→	Display Gigabit Ethernet device parameters

4.3.1 Power & Performance

Menu Item	Options	Description
CPU - Power Management Control	See submenu	CPU – Power Management Control Options
GT - Power Management Control	See submenu	GT – Power Management Control Options

4.3.1.1 CPU - Power Management Control

Menu Item	Options	Description
Boot performance mode	Max Battery Max Non-Turbo Performance Turbo Performance	Select the performance state that the BIOS will set starting from reset vector
Intel® SpeedStep(tm)	Enabled / Disabled	Allows more than two frequencies ranges to be supported
Race to Halt (RTH)	Enabled / Disabled	Enable/Disable Race to Halt feature. RTH will dynamically increase CPU frequency in order to enter pkg C-state faster to reduce overall power. (RTH is controlled through MSR 1FC bit 20)
Intel® Speed Shift Technology	Enabled / Disabled	Enable/Disable Intel® Speed Shift Technology support. Enabling will expose the CPPC v2 interface to allow for hardware controlled P-states
Per Core P State OS control mode	Enabled / Disabled	Enable/Disable Per Core P state OS control mode. Disabling will set Bit 31 = 1 command 0x06. When set, the highest core request is used for all other core requests.
HwP Autonomous Per Core P State	Enabled / Disabled	Enable PCPS (default Bit 30 = 0, command 0x11). Disable Autonomous PCPS (Bit 30 = 1, command 0x11) Autonomous will request the same value for all cores all the time.
HwP Autonomous EPP Grouping	Enabled / Disabled	Enable EPP grouping (default Bit 29 = 0 , command 0x11). Autonomous will request the same values for all cores with same EPP. Disable EPP grouping (Bit 29 =1, command 0x11) autonomous will not necessarily request same values for all cores with same EPP
EPB override over PECI	Enabled / Disabled	Enable/Disable EPB override over PECI. Enable by sending pcode command 0x2b, subcommand 0x3 to 1. This will allow OOB EPB PECI override control
HwP fast MSR Support	Enabled / Disabled	Enable/Disable HwP Fast MSR Support for IA32_HWP_REQUEST MSR
HDC Control	Enabled / Disabled	This option allows HDC configuration. Disabled: Disable HDC Enabled: Can be enabled by OS if OS native support is available
Turbo Mode	Enabled / Disabled	Enable/Disable processor Turbo Mode (requires EMTTM enabled too). AUTO means enabled.
View/Configure Turbo Options	See submenu	View/Configure Turbo Options
Config TDP Configurations	See submenu	

CPU VR Settings	See submenu	CPU VR Settings
Platform PL1 Enable	Enabled / Disabled	Enable/Disable Platform Power Limit 1 programming. If this option is enabled, it activates the PL1 value to be used by the processor to limit the average power of given time window
Platform PL1 Power	[0…4095875]	Platform Power Limit 1 Power in Milli Watts. BIOS will round to the nearest 1/8W when programming. Any value can be programmed between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). For 12.50W, enter 12500. This setting will act as the new PL1 value for the Package RAPL algorithm.
Platform PL1Time Window	[0 / 1 / … / 128]	Platform Power Limit 1 Time Window value in seconds. The value may vary from 0 to 128. 0 = default value. Indicates the time window over which Platform TDP value should be maintained
Platform PL2 Enable	Enabled / Disabled	Enable/Disable Platform Power Limit 2 programming. If this option is enabled, BIOS will program the default values for Platform Limit 2
Platform PL2 Power	[0…4095875]	Platform Power Limit 2 Power in Milli Watts. BIOS will round to the nearest 1/8W when programming. Any value can be programmed between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). For 12.50W, enter 12500. This setting will act as the new PL2 value for the Package RAPL algorithm.
Power Limit 4 Override	Enabled / Disabled	Enable/Disable Power Limit 4 override. If this option is disabled, BIOS will leave the default values for Poer Limit 4.
Power Limit 4	[0…4095875]	Platform Power Limit 4 in Milli Watts. BIOS will round to the nearest 1/8W when programming. For 12.50W, enter 12500. If the value is 0, BIOS leaves default value
Power Limit 4 Lock	Enabled / Disabled	Power Limit 4 MSR 601h Lock. When enabled PL4 configurations are locked during OS. When disabled PL4 configuration can be changed during OS
C states	Enabled / Disabled	Enable/Disable CPU Power Management. Allows CPU to go to C states when it's not 100% utilized
Enhanced C-states	Enabled / Disabled	Enable/Disable C1E. When enabled, CPU will switch to minimum speed when all cores enter C-state
C-State Auto Demotion	Disabled / C1	Configure C-State Auto Demotion
C-State Un-demotion	Disabled / C1	Configure C-State Un-demotion
Package C-State Demotion	Enabled / Disabled	Package C-State Demotion
Package C-State Un-demotion	Enabled / Disabled	Package C-State Un-demotion
CState Pre-Wake	Enabled / Disabled	Disable – Sets bit 30 of POWER_CTL MSR (0x1FC) to 1 to disable the Cstate Pre-Wake
IO MWAIT Redirection	Enabled / Disabled	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: Intializes to deepest available Package C State Limit
• C6/C7 Short Latency Control (MSR 0x60B) • C6/C7 Long Latency Control (MSR 0x60C)	Time Unit (ns): 1 / 32 / 1024 / 32768 / 1048576 / 33554432 Latency:	Time Unit: Unit of measurement for IRTL value – bits [12:10] Latency: Interrupt Response Time Limit value – bits [9:0], Enter 0-1023

• C8 Latency Control (MSR 0x633) • C9 Latency Control (MSR 0x634) • C10 Latency Control (MSR 0x635)	[0...1023]	
Thermal Monitor	Enabled / Disabled	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	Enabled / Disabled	Enable/Disable Timed MWAIT Support
Custom P-state Table	→	Add Custom P-state Table --> Sets the number of custom P-states. At least 2 states must be present
EC Turbo Control Mode	Enabled / Disabled	Enable/Disable EC Turbo Control mode
AC Brick Capacity	90W AC Brick 65W AC Brick 75W AC Brick	Specify the AC Brick capacity
EC Polling Period	[1...255]	Count 1 to 255 for a range of 10ms to 2.55 seconds (1 count = 10ms)
EC Guard Band Value	[1...20]	Count 1 to 20 for a range of 1 Watt to 20 Watts
EC Algorithm Selection	[1...10]	Count 1 to 10 for Algorithm Selection
Energy Performance Gain	Enabled / Disabled	Enable/Disable Energy Performance Gain
EPG DIMM Idd3N	26 (default)	Active standby current (Idd3N) in milliamps from datasheet. Must be calculated on a per DIMM basis
EPG DIMM Idd3P	11 (default)	Active power-down current (Idd3P) in milliamps from datasheet. Must be calculated on a per DIMM basis
Power Limit 3 Settings	See submenu	Power Limit 3 Settings
CPU Lock Configuration	See submenu	CPU Lock Configuration

4.3.1.1.1 View/Configure Turbo Options

Menu Item	Options	Description
Current Turbo Settings		Shows cores' specific Turbo information
Energy Efficient P-state	Enabled / Disabled	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	Enabled / Disabled	Enable/Disable locking of Package Power Limit settings. When enabled, PACKAGE_POWER_LIMIT MSR will be locked and a reset will be required to unlock the register

1-Core Turbo Ratio Limit Ratio (TRLR) Override	[0…120]	1-Core Turbo Ratio Limit Ratio (TRLR) with range of Max Non-Turbo Ratio up to 120. This 1-Core Turbo Ratio Limit must be greater than or equal to other Turbo Core Ratio Limit.
2-Core Turbo Ratio Limit Ratio (TRLR) Override	[0…120]	2-Core Turbo Ratio Limit Ratio (TRLR) with range of Max Non-Turbo Ratio up to 120. This 2-Core Turbo Ratio Limit must be less than or equal to 1-Core Turbo Ratio Limit.
Energy Efficient Turbo	Enabled / Disabled	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.

4.3.1.1.2 Config TDP Configurations

Menu Item	Options	Description
Enable Configurable TDP	Applies to cTDP Applies to non-cTDP	Applies TDP initialization settings based on non-cTDP or cTDP. Default is 1: Applies to cTDP; if 0 then applies non-cTDP and BIOS will bypass cTDP initialization flow
Configurable TDP Boot Mode	Nominal Down Up Deactivate	Deactivate option will set MSR to Nominal and MMIO to Zero. For TGL-UP3: Nominal = nominal, Up = cTDP down1, Down = cTDP down2
Configurable TDP Lock	Enabled / Disabled	Sets the lock bits on TURBO_ACTIVATION_RATIO and CONFIG_TDP_CONTROL. Note: When cTDP is enabled Custom ConfigTDP count will be forced to 1 and Custom ConfigTDP boot Index will be forced to 0.
Custom Settings Nominal/Down/Up		
Power Limit 1	[0…4095875]	Power Limit 1 in Milli Watts. BIOS will round to the nearest 1/8W when programming. 0 = no custom override. For 12.50W enter 12500. Overclocking SKU: Value must be between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). Other SKUs: This value must be between Min Power Limit and TDP Limit.
Power Limit 2	[0…4095875]	Power Limit 2 in Milli Watts. BIOS will round to the nearest 1/8W when programming. 0 = no custom override. For 12.50W enter 12500. Processor applies control policies such that the package power does not exceed this limit.
Power Limit 1 Time Window	[0 / … / 128]	Power Limit 1 Time Window value in seconds. The value may vary from 0 to 128. 0 = default value (28 sec for Mobile and 8 sec for Desktop). Defines time window which TDP value should be maintained.
ConfigTDP Turbo Activation Ratio	[0…100]	Custom value for Turbo Activation Ratio. Needs to configured with valid values from LFM to Max Turbo. 0 means don't use custom value

4.3.1.1.3 CPU VR Settings

Menu Item	Options	Description
PSYS Slope	[0…200]	PSYS Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x9
PSYS Offset	[0…63999]	PSYS Offset defined in 1/1000 increments. Range is 0-63999. For an offset of 25.348, enter 25348. Uses BIOS VR mailbox command 0x9

PSYS Prefix	+ / -	Sets the offset value as positive or negative
PSYS Pmax Power	[0…8192]	PSYS Pmax power, defined in 1/8 Watt increments. Range 0-8192. For a Pmax of 125W, enter 1000. 0 = AUTO. Uses BIOS VR mailbox command 0xB
Acoustic Noise Settings	See submenu	Configure Acoustic Noise Settings for IA, GT and SA domains
VccIn VR Settings	See submenu	VccIn VR Settings
RFI Settings	See submenu	RFI Settings

4.3.1.1.3.1 Acoustic Noise Settings

Menu Item	Options	Description
Acoustic Noise Mitigation	Enabled / Disabled	Enabling this option will help mitigate acoustic noise on certain SKUs when the CPU is in deeper C state
Disable Fast PKG C State Ramp for VccIn Domain	FALSE / TRUE	This option needs to be configured to reduce acoustic noise during deeper C state. FALSE: Don't disable Fast ramp during deeper C state; TRUE: Disable Fast ramp during deeper C state
Slow Slew Rate for VccIn Domain	Fast/2 Fast/4 Fast/8 Fast/16	Set VR VccIn Slow Slew Rate for Deep Package C state ramp time; Slow slew rate equals to Fast divided by number, the number is 2, 4, 8, 16 to slow down the slew rate to help minimize acoustic noise

4.3.1.1.3.2 VccIn VR Settings

Menu Item	Options	Description
VR Config Enable	Enabled / Disabled	VR Config Enable
AC Loadline	[0…6249]	AC Loadline defined in 1/100 mOhms. A value of 100 = 1.00 mOhm, and 1255 = 12.55 mOhm. Range is 0-6249 (0-62.49 mOhms). 0 = AUTO/HW default. Uses BIOS mailbox command 0x2
DC Loadline	[0…6249]	DC Loadline defined in 1/100 mOhms. A value of 100 = 1.00 mOhm, and 1255 = 12.55 mOhm. Range is 0-6249 (0-62.49 mOhms). 0 = AUTO/HW default. Uses BIOS mailbox command 0x2
PS Current Threshold1	[0…512]	PS Current Threashold1, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3
PS Current Threshold2	[0…512]	PS Current Threashold2, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3
PS Current Threshold3	[0…512]	PS Current Threashold3, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3
PS3 Enable	Enabled / Disabled	PS3 Enable/Disable. 0 – Disabled, 1 – Enabled. Uses BIOS VR mailbox command 0x3
PS4 Enable	Enabled / Disabled	PS4 Enable/Disable. 0 – Disabled, 1 – Enabled. Uses BIOS VR mailbox command 0x3

IMON Slope	[0…200]	IMON Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x4
IMON Offset	[0…63999]	IMON Offset defined in 1/1000 increments. Range is 0-63999. For an offset of 25.348, enter 25348. Uses BIOS VR mailbox command 0x4
IMON Prefix	+ / -	Sets the offset value as positive or negative
VR Current Limit	[0…512]	Voltage Regulator Current Limit (Icc Max). This value represents the Maximum instantaneous current allowed at any given time. The value is represented in 1/4 A increments. A value of 400 = 100A. 0 means AUTO. Uses BIOS VR mailbox command 0x6
TDC Enable	Enabled / Disabled	TDC Enable. 0 – Disable, 1 – Enable
TDC Current Limit	[0…32767]	TDC Current Limit, defined in 1/8 increments. Range 0-32767. For a TDC Current Limit of 125A, enter 1000. 0 = 0 Amps. Uses BIOS VR mailbox command 0x1A
TDC Time Window	[1…8, 10]	TDC Time Window, value in milliseconds. 1ms is default. Range from 1ms to 1ms, except for 9ms. 9ms has no valid encoding in the MSR definition
TDC Lock	Enabled / Disabled	TDC Lock

4.3.1.1.3.3 RFI Settings

Menu Item	Options	Description
RFI Current Frequency		Shows current RFI Frequency setting
RFI Frequency	[1300…1600]	Set desired RFI Frequency, in increments of 100KHz. The RFI Frequency Range is between 130 MHz to 160 MHz, and the default h/w frequency is 139.6 MHz. For a frequency of 139.6 MHz, enter 1396
RFI Spread Spectrum	[0…100]	Adjust the Spread Spectrum, in increments of 0.1%. For a spread of 5.0%, enter 50. The value of 0 will disable the FIVR FRI Spread Spectrum, Range 0-100 (0.0% to 10.0%)

4.3.1.1.4 Power Limit 3 Settings

Menu Item	Options	Description
Power Limit 3 Override	Enabled / Disabled	Enable/Disable Power Limit 3 override. If this option is disabled, BIOS will leave the hardware default values for Poer Limit 3 and Power Limit 3 Time Window.
Power Limit 3	[0…4095875]	Power Limit 3 in Milli Watts. BIOS will round to the nearest 1/8W when programming. For 12.50W enter 12500. XE SKU: Any value can be programmed. Overclocking SKU: Value must be between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR).
Power Limit 3 Time Window	[0 / 3 / … / 64]	Power Limit 3 Time Window value in Milli seconds. The value may vary from 3 to 64 (max). Indicates the time window over which Power Limit 3 value should be maintained. If the value is 0, BIOS leaves the hardware default value.
Power Limit 3 Duty Cycle	[0…100]	Specify the duty cycle in percentage that the CPU is required to maintain over the configured time window.

Power Limit 3 Lock	Enabled / Disabled	Power Limit 3 MSR 615h Lock. When enabled PL3 configurations are locked during OS. When disabled PL3 configurations can be changed during OS.

4.3.1.1.5 CPU Lock Configuration

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

4.3.1.2 GT- Power Management Control

Menu Item	Options	Description
RC6 (Render Standby)	Enabled / Disabled	Check to enable render standby support.
Maximum GTT frequency	[Default Max Frequency / 100MHz / … / 1200MHz]	Maximum GT frequency limited by the user. Choose between 100MHz (RPN) and 1250MHz (RP0). Value beyond the range will be clipped to min/max supported by SKU
Disable Turbo GT frequency	Enabled / Disabled	Enabled: Disables Turbo GT frequency. Disabled: GT frequency is not limited

4.3.2 PCH-FW Configuration

Menu Item	Options	Description
ME Firmware information		Shows ME Firmware specific information
ME State	Enabled / Disabled	When Disabled ME will be put into ME Temporarily Disabled Mode
ME Unconfig on RTC Clear	Enabled / Disabled	When Disabled ME will not be unconfigured on RTC Clear
Comms Hub Support	Enabled / Disabled	Enable/Disable support for Comms Hub
JHI Support	Enabled / Disabled	Enable/Disable Intel® DAL Host Interface Service (JHI)
Core Bios Done Message	Enabled / Disabled	Enable/Disable Core Bios Done message sent to ME
Firmware Update Configuration	See submenu	Configure Management Engine Technology Parameters
PTT Configuration	See submenu	Configure PTT
FIPS Configuration	See submenu	FIPS Mode help
ME Debug Configuration	See submenu	Configure ME debug options. NOTE: This menu is provided testing purposes. It is recommended to leave the options in their default states

Anti-Rollback SVN Configuration	See submenu	Configure Anti-Rollback SVN
OEM Key Revocation Configuration	See submenu	Configure OEM Key Revocation
Extend CSME Measurement to TPM-PCR	Enabled / Disabled	Enable / Disable Extend CSME Measurement to TPM-PCR [0] and AMT Config to TPM-PCR [1]

4.3.2.1 Firmware Update Configuration

Menu Item	Options	Description
ME FW Image Re-Flash	Enabled / Disabled	Enable/Disable ME FW Image Re-Flash function
FW Update	Enabled / Disabled	Enable/Disable ME FW Update function

4.3.2.2 PTT Configuration

Menu Item	Options	Description
TPM Device Selection	dTPM / PTT	Selects TPM device: PTT or dTPM. PTT – Enables PTT in SkuMgr dTPM 1.2 – Disables PTT in SkuMgr Warning ! PTT/dTPM will be disabled and all data saved on it will be lost

4.3.2.3 FIPS Configuration

Menu Item	Options	Description
FIPS Mode Select	Enabled / Disabled	FIPS Mode configuration
FIPS Mode information		Shows FIPS Mode specific information

4.3.2.4 ME Debug Configuration

Menu Item	Options	Description
HECI Timeous	Enabled / Disabled	Enable/Disable HECI Send/Receive Timeouts
Force ME DID Init Status	Enabled / Disabled	Forces the DID Initialization Status value
CPU Replaced Polling Disable	Enabled / Disabled	Setting this option disables CPU replacement polling loop
HECI Message check Disable	Enabled / Disabled	Settings this option disables message check for Bios Boot Path when sending
MBP HOB Skip	Enabled / Disabled	Setting this option will skip MBP HOB
HECI2 Interface Communication	Enabled / Disabled	Adds and Removes HECI2 Device from PCI space
KT Device	Enabled / Disabled	Enable/Disable KT Device
DOI3 Setting for HECI Disable	Enabled / Disabled	Setting this option disables setting DOI3 bit for all HECI devices
MCTP Broadcast Cycle	Enabled / Disabled	Enable/Disable Management Component Transport Protocol Broadcast Cycle and Set PMT as Bus Owner

SMBIOS type 130 OEM capabilities	See submenu	This menu allows changing SMBIOS type 130 OEM capabilites

4.3.2.4.1 SMBIOS type 130 OEM capabilities

Menu Item	Options	Description
BIOS Reflash Capability State	Enabled / Disabled	Change BIOS Reflash Capability State
BIOS Boot to Setup Capability State	Enabled / Disabled	Change BIOS Boot to Setup Capability State
BIOS Pause Before Booting Capability State	Enabled / Disabled	Change BIOS Pause Before Booting Capability State
BIOS Secure Boot Capability Exposure to FW State	Enabled / Disabled	Change BIOS Secure Capability Exposure State to FW. This does not affect SecureBoot as such

4.3.2.5 Anti-Rollback SVN Configuration

Menu Item	Options	Description
Automatic HW-Enforced Anti-Rollback SVN	Enabled / Disabled	When enabled, hardware-enforced Anti-Rollback mechanism is automatically activated: once ME FW was successfully run on a platform, FW with lower ARB-SVN will be blocked from execution
Set HW-Enforced Anti-Rollback for Current SVN	Enabled / Disabled	Enable hardware-enforced Anti-Rollback mechanism for current ARB-SVN value. FW with lower ARB-SVN will be blocked from execution. The value will be restored to disable after the command is sent

4.3.2.6 OEM Key Revocation Configuration

Menu Item	Options	Description
Automatic OEM Key Revocation	Enabled / Disabled	When enabled, BIOS will automatically send HECI command to revoke OEM keys
Invoke OEM Key Revocation	Enabled / Disabled	A HECI command will be sent to revoke OEM keys

4.3.3 Platform Settings -> TCSS Platform Setting

Menu Item	Options	Description
Control Iommu Pre-boot Behaviour	Enabled / Disabled	Enable IOMMU in Pre-boot environment (if DMAR table is installed in DXE and if VTD_INFO_PPI is installed in PEI)
USBC connector manager selection	Disabled / Enable UCSI Device / Enable UCMC Device	Select UCSI or UCMC device in ACPI support based on configuration
Type C retimer TX Compliance Mode	Enabled / Disabled	Default is disable Compliance Mode. Change to enabled for Type C reitmer Tx Compliance Mode testing
BIOS-TCSS handshake	Enabled / Disabled	Enable/Disable BIOS TCSS handshake messages. Disabled: TCSS handshake disabled. Enabled: TCSS handshake with either EC or PMC is enabled based on the board ID
Timeout for EC USB enumeration message	[..]	BIOS-EC handshake message USBC_GetUSBConStatus timeout value in milli seconds
USBC and USBA Wake Capability	S3 / S4	USBC and USBA Wake Capability

Thunderbolt Configuration	See submenu	Thunderbolt related configuration
Dynamic one-time switch	Enabled / Disabled	Dynamic onr-time switch from iGFx to dGFx after boot to OS

4.3.3.1 *Thunderbolt Configuration*

Menu Item	Options	Description
Control Iommu Pre-boot Behaviour	Enabled / Disabled	Enable or disable integrated Thunderbolt support
USBC connector manager selection	Enabled / Disabled	Enable or disable system wake from Thunderbolt devices
Type C retimer TX Compliance Mode	Enabled / Disabled	Enable Native OS security solution for Thunderbolt hosts
BIOS-TCSS handshake	See submenu	Integrated Thunderbolt Related Configuration

4.3.3.1.1 Integrated Thunderbolt Configuration

Menu Item	Options	Description
OS Native Resource Balance	Enabled / Disabled	OS Native Resource Balance
PCIE Tunneling for USB4	Enabled / Disabled	Enable or disable PCIE Tunneling for USB4
Connecto Topology Timeout value for ITBT	[default 5000]	Connect Topology Timeout value for Integrated Thunderbolt Controller
Force Poweron Timeout value for ITBT	[default 500]	Force Poweron Timeout value for Integrated Thunderbolt
ITBT RTD3	Enabled / Disabled	ITBT RTD 3
ITBT RTD3 EXIT DELAY	[default 0]	ITBT RTD 3 EXIT DELAY (milli seconds)

4.3.4 Intel Time Coordinated Computing

Menu Item	Options	Description
#AC Split Lock	Enabled / Disabled	Enable or Disable Alignment Check Exception (#AC). When enabled, this will assert an #AC when any atomic operation has an operand that crosses two cache lines.
IFU Enable	Enabled / Disabled	Enable or Disable Instruction Fetch Unit (IFU). When enabled, Instructions will be prefetch to the cache
Software SRAM	Enabled / Disabled	Enable or Disable Software SRAM. Enable will allocate 1 way of LLC; if Cache Configuration subregion is available, it will allocate based on the subregion.
Data Streams Optimizer	Enabled / Disabled	Enable or Disable Data Stream Optimizer (DSO). Enable will utilize DSO Subregion to tune system. DSO settings supercede Intel TCC Mode settings that overlap between the two.
Error Log	Enabled / Disabled	Enable or Disable Error Log. Enable will record errors related to Intel TCC and save them memory.

Intel TCC Authentication	Disabled / Non-OEM Enrolled Key / OEM Enrolled Key	Intel TCC Authtentication determines the key to be used. OEM Enrolled Key is built in by OEM. Non-OEM Enrolled Key can be add by user.
Intel TCC Mode	Enabled / Disabled	Enable or Disable Intel TCC Mode. When enabled, this will modify system settings to improve real-time performance. The fill list of settings and their current state are displayed below when Intel TCC is enabled.
IO Fabric Low Latency	Enabled / Disabled	Enable or Disable IO Fabric Low Latency. This will turn off some power management in the PCH IO brics. This option provides the most aggressive IO Fabric performance setting. S3 state is NOT supported.
GT CLOS	Enabled / Disabled	Enable or Disable Graphics Technology Class of Service. Enable will reduce Gfx LLC allocation to minimize impact of Gfx workload on LLC.
OPIO Recentering	Enabled / Disabled	Enable or Disable Opio Recentering to improve Pcie latency.
C States	→	Jump to CPU - Power Management Control
Intel SpeedStep	→	Jump to CPU - Power Management Control
Intel Speed Shift Technology	→	Jump to CPU - Power Management Control
Hyper Threading		Display CPU Configuration parameters
ACPI D3Cold Support	Enabled / Disabled	Enable or Disable ACPI D3Cold support to be executed on D3 entry and exit
Low Power SO Idle Capability	See submenu	ACPI Settings

4.3.4.1 ACPI Settings

Menu Item	Options	Description
Enable ACPI Auto Configuration	Enabled / Disabled	Enable or Disable BIOS ACPI Auto Configuration
Enable Hibernation	Enabled / Disabled	Enable or Disable System ability to Hibernate (OS/S4 Sleep State). This option may not be effective with some operating systems.
ACPI Sleep State	Suspend Disabled / S3 (Suspend to RAM)	Select the highest ACPI sleep state the system will enter when the SUSPEND button is pressed.
Lock Legacy Resources	Enabled / Disabled	Enable or Disable Lock of Legacy Resources

4.3.5 Trusted computing

Menu Item	Options	Description
Security Device Support	Enabled / Disabled	Enables or Disables BIOS support for security device. OS will not show the Security Device. TCG EFI protocol and INT1A interface will not be available. When enabled all the following items will be available.
SHA256 PCR Bank	Enabled / Disabled	Enables or Disables SHA256 PCR Bank
SHA384 PCR Bank	Enabled / Disabled	Enables or Disables SHA384 PCR Bank

SM3_256 PCR Bank	Enabled / Disabled	Enables or Disables SM3_256 PCR Bank
Pending Operation	None / TPM Clear	Schedule an Operation for the Security Device. NTE: your Computer will reboot during restart in order to change State of Security Device.
Platform Hierarchy	Enabled / Disabled	Enables or Disabled the Platform Hierarchy
Storage Hierarchy	Enabled / Disabled	Enables or Disabled the Storage Hierarchy
Endorsement Hierarchy	Enabled / Disabled	Enables or Disabled the Endorsement Hierarchy
Physical Presence Spec Version	1.2 / 1.3	Select to tell OS to support PPI Spec Version 1.2 or 1.3. Please note that some HCK tests might not support 1.3
Device Select	Auto TPM 1.2 TPM 2.0	TPM 1.2 will restrict the support to TPM 1.2 devices only, TPM 2.0 will restrict the support to TPM 2.0 devices only, Auto will support both with the default set to TPM 2.0 devices if not found, TPM 1.2 devices will be enumerated

4.3.6 Serial Port Console Redirection

Menu Item	Options	Description
COM#		
Console Redirection	Enabled / Disabled	Enables or Disables the Console redirection. When enabled the following item will appear
Console Redirection Settings	See Submenu	The settings specify how the host and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings
Windows Emergency Management Service (EMS)		
Console Redirection EMS	See Submenu	Enables or Disables the Console redirection. When enabled the following item will appear
Console Redirection Settings	See Submenu	The settings specify how the host and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings

4.3.6.1 Console Redirection Settings (COM#)

Menu Item	Options	Description
Terminal Type	VT100 VT100+ VT-UTF8 ANSI	Emulation: ANSI: Extended ASCII Char set. VT100: ASCII Char set. VT100+: extends VT100 to support colour, 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	Select 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	Set Console Redirection 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 number of 1s in the data bits is even. Odd: parity bit is 0 if the number of 1s in the data bits is odd. Mark: parity bit is always 1. Space: parity bit is always 0. Mark and Space do not allow for error detection
Stop bits	1 / 2	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit
Flow Control	None Hardware RTS/CTS	Flow Control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses RTS# / CTS# lines to send the start / stop signals.
VT-UTF8 Combo Key Support	Enabled / Disabled	Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals
Recorder Mode	Enabled / Disabled	When this mode is enabled, only text will be sent. This is to capture Terminal data.
Resolution 100x31	Enabled / Disabled	Enables or disables extended terminal resolution
Putty Keypad	VT100 / Intel Linux / XTERMR6 / SCO / ESCN /VT400	Select FunctionKey and KeyPad on Putty

4.3.6.2 Console Redirection Settings (EMS)

Menu Item	Options	Description
Out-of-Band Mgmt Port	COM0 COM1	Microsoft Windows Emergency Management Services (EMS) allows for remote management of a Windows Server OS through a serial port
Terminal Type EMS	VT100 VT100+ VT-UTF8 ANSI	VT-UTF8 is the preferred terminal type for out-of-band management. The next best choice is VT100+ and then VT100. See above, in Console redirection Settings page, for more help with Terminal Type/Emulation
Bits per second	9600 / 19200 / 57600 / 115200	Select Serial port Transmission Speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Flow Control	None Hardware RTS/CTS Software Xon/Xoff	Flow Control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.

4.3.7 AMI Graphic Output Protocol Policy

Menu Item	Options	Description
Output Select	*List of available / connected module's video interfaces*	Output Interface, this menu is visible when more than one interface is available

Brightness Settings	20 / 40 / 60 / 80 / 100 / 120 / 140 / 160 / 180 / 200 / 220 / 240 / 255	Set GOP Brightness value
BIST Enable	Enabled / Disabled	Starts or stops the BIST on the integrated display panel

4.3.8 USB Configuration

Menu Item	Options	Description
Legacy USB Support	Enabled / Disabled / Auto	Enables Legacy USB Support. AUTO Option disables legacy support if no USB devices are connected. DISABLE option will keep USB devices available only for EFI applications.
XHCI hand-off	Enabled/ Disabled	This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.
USB Mass Storage Driver Support	Enabled/ Disabled	Enables or disables USB Mass Storage Driver Support
USB Transfer time-out	1 sec / 5 sec / 10 sec / 20 sec	Sets 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	Sets the maximum time that the device will take before it properly reports itself to the Host controller. 'Auto' uses the default vale (for a Root port it is 100ms, for a Hub port the delay is taken from the Hub descriptor).
Device power-up delay in seconds	[1..40]	Delay range in seconds, in one second increment, visible when delay is set to Manual

4.3.9 Network Stack configuration

Menu Item	Options	Description
Network Stack	Enabled / Disabled	Enables or disables UEFI Network Stack. When enabled, following menu items will appear
Ipv4 PXE Support	Enabled / Disabled	Enables or disables IPV4 PXE Boot Support. If disabled, IPV4 PXE boot option will not be created
Ipv4 HTTP Support	Enabled / Disabled	Enables or disables IPV4 HTTP Boot Support. If disabled, IPV4 HTTP boot option will not be created
Ipv6 PXE Support	Enabled / Disabled	Enables or disables IPV6 PXE Boot Support. If disabled, Ipv6 PXE boot option will not be created
Ipv6 HTTP Support	Enabled / Disabled	Enables or disables IPV6 HTTP Boot Support. If disabled, Ipv6 HTTP boot option will not be created
PXE boot wait time	[0..5]	Wait time to press ESC key to abort the PXE boot
Media detect count	[1..50]	Number of times that the presence of media will be checked

4.3.10 NVMe configuration

Menu Item	Options	Description
List of NVMe devices found		

4.3.11 SDIO configuration

Menu Item	Options	Description
SDIO Access Mode	Auto ADMA SDMA PIO	Auto Option: Access the SD Device in DMA mode if the controller supports it, otherwise in PIO Mode. DMA Option: Access the SD Device in DMA mode ADMA Option: Access the SD Device in Advanced DMA mode PIO Option: Access the SD Device in PIO mode
List of SDIO devices found	Auto Floppy Forced FDD Hard Disk	Mass storage device emulation type. 'Auto' enumerates devices less than 530Mb as floppies. Forced FDD option can be used to force HDD formatted drive to boot as FDD.

4.3.12 Main Thermal Configuration

Menu Item	Options	Description
Critical Temperature (°C)	90 / 95 / 100 / 105 / 110 / 115 / 117 / 119 / Disabled	Above this threshold, an ACPI aware OS performs a critical shut down. Allowed range is from 90°C to 119°C included or disabled.
Passive Cooling Temperature (°C)	80 / 85 / 90 / 95 / 100 / 105 / 107 / 109 / Disabled	Above this threshold, an ACPI aware OS begins to lower the CPU speed. Allowed range is from 80 to 109 °C included or disabled.
TC1	1 (default)	Thermal Constant 1: part of the ACPI Passive Cooling Formula
TC2	1 (default)	Thermal Constant 2: part of the ACPI Passive Cooling Formula
TSP (tenths of a second)	5 (default)	Period of temperature sampling when Passive Cooling

4.3.13 Embedded Controller

Menu Item	Options	Description
Embedded Controller information		Shows Embedded Controller specific information
Power Fail Resume Type	Always ON Always OFF Last State	Specify what state to go to when power is re-applied after a power failure (G3 state). If Batteryless Operation, the chipset always powers on after a power failure: Always OFF Resume Type or Last State when Last State was OFF will therefore require an immediate shutdown.
No C-MOS battery handling	Enabled / Disabled	In systems with no C-MOS battery, the chipset always powers on after a power failure: Always OFF Resume Type or Last State when Last State was OFF will therefore require an immediate shutdown.
LID_BTN# Configuration	Force Open Force Closed Normal Polarity Inverted Polarity	Configures the LID_BTN# signal as always open or closed, no matter the pin level, or configures the pin polarity: High = Open (Normal), Low = Open (Inverted)

LID_BTN# Wake Configuration	No Wake Only From S3 Wake From S3/S4/S5	Configures LID_BTN# wake capability (when not forced to Open or Closed). According to the pin configuration, when the LID is open it can cause a system wake from a sleep state.
OUT 80 serial redirection port	None / 1 / 2 / 1+2	Select on which E.C. UART(s) to redirect OUT 80 (Post Codes)
Hardware Monitor		Shows Monitored Hardware parameters and settings
Reset Causes Handling	See Submenu	Reset Causes Handling
Super IO Configuration	See Submenu	Super IO Configuration
Internal FAN Settings	See Submenu	Internal FAN Settings
External FAN/PWM Settings	See Submenu	Visible when PWM/FAN Management is Enabled under SMARC Related Configuration
Watchdog Configuration	→	Disables/Enables the Watchdog Timer Mechanism
GPIO Configurations	See Submenu	GPIO Configurations

4.3.13.1 Reset Causes Handling

Menu Item	Options	Description
• ***Reset Button Pressed*** • ***WDT Timeout Expired*** • ***Power Failure*** • ***E.C soft reset***		Show event as Happened or Not Happened
Clear from log	Enabled / Disabled	For Happened events if Enabled will require system reset

4.3.13.2 Super IO Configuration

Menu Item	Options	Description
Serial Port #	Enabled / Disabled	Serial Port #
Address	List of hex addresses	Serial Port IO Base Address
IRQ	3 / 4 / 5 / 7 / 10 / 11 / 14 / 15	Serial Port IRQ

4.3.13.3 Internal FAN Settings

Menu Item	Options	Description
FAN_PWMOUT device type	3-WIRE FAN 4-WIRE FAN Generic PWM	Specifies if FAN_PWMOUT is connected to a 3-wire or 4-wire FAN or to a generic PWM

Automatic Temperature FAN Control	Enabled / Disabled	Disable/Enable Thermal Feed-back FAN Control
AC0 Temperature (C)	[70..100]	AC0: above this temperature the FAN runs at full speed
AC1 Temperature (C)	[5..100]	AC1: below this temperature the FAN is OFF; between AC1 and AC0 the FAN runs at low speed: this never happens if AC1 is not below AC0
Temperature Hysteresis	[..]	Added to ACx Thresholds when temperature is growing and subtracted when it is lowering
Linear Speed change	Enabled / Disabled	Linear FAN Duty Cycle growth between AC1 and AC0
FAN Duty Cycle (%) Above AC1	[..]	FAN Duty Cycle (%) between AC1 and AC0 (low speed)
Speed change duration	[..]	Duration in seconds of linear FAN speed change. Allowed range: from 0 to 50

4.3.13.4 External FAN/PWM Settings

Menu Item	Options	Description
FAN_PWMOUT device type	3-WIRE FAN 4-WIRE FAN Generic PWM	Specifies if FAN_PWMOUT is connected to a 3-wire or 4-wire FAN or to a generic PWM
Automatic Temperature FAN Control	Enabled / Disabled	Disable/Enable Thermal Feed-back FAN Control
FAN PWM Frequency	[1..60000]	Sets the frequency of the FAN_PWMOUT signal. Typical values are 100 for a 3-wire device and 20000 for a 4-wire one
FAN Duty Cycle (%)	[0..100]	Sets the Duty Cycle of the FAN_PWMOUT signal

4.3.13.5 GPIO Configurations

Menu Item	Options	Description
GPIO#		
Configuration	Input Output Low Output High Output Last	Configure pin as input or output with a fixed starting value. Last means no changes with respect to the last boot.

4.3.14 Tls Auth Configuration

Menu Item	Options	Description
Server CA Configuration	→	Enroll Cert → Cert GUID (Input digit character in 11111111-2222-3333-4444-1234567890ab format) Delete Cert

4.3.15 RAM Disk Configuration

Menu Item	Options	Description
Disk Memory Type:	Boot Service Data Reserved	Specifies type of memory to use from available memory pool in system to create a disk
Create Raw		Create a raw RAM disk
Create from file		Create a RAM disk from a given file
Remove selected RAM disk(s)		Remove selected RAM disks

4.4 Chipset menu

Menu Item	Options	Description
System Agent (SA) Configuration	See Submenu	System Agent (SA) Parameters
PCH-IO Configuration	See Submenu	PCH Parameters

4.4.1 System Agent (SA) Configuration

Menu Item	Options	Description
Memory Configuration		Memory Configuration Parameters
Graphics Configuration	See Submenu	Graphics Configuration

4.4.1.1 Graphics Configuration

Menu Item	Options	Description
Graphics Turbo IMON Current	[14..31]	Graphics Turbo IMON Current values supported (14 – 31)
Skip Scanning of External Gfx Card	Enabled / Disabled	If Enabled, it will not scan for External Gfx Card on PEG and PCH PCIE ports
Primary Display	Auto / IGFX / PEG / PCI	Set which graphics device should be the Primary Display
Select PCIe Card	Auto / Elk Creek 4 / PEG Eval	Select the card used on the platform Auto : Skip GPIO based Power Eable to dGPU Elk Creek 4: DGPU Power Enable = ActiveLow PEG Eval : DGPU Power Enable = ActiveHigh
External Gfx Card Primary Display Conf.	Auto / PCIEx	External Gfx Card Primary Display Configuration --> Select Auto or Primary PCIe
Internal Graphics	Auto / Disabled / Enabled	Keep IGFX enabled based on the setup options
GTT Size	2 MB / 4 MB / 8 MB	Select the GTT (Graphics Translation Table) Size
Aperture Size	256 MB	Use this item to set the total size of Memory that must be left to the GFX Engine
PSMI SUPPORT	Enabled / Disabled	PSMI Enabled / Disabled
DVMT Pre-Allocated	64M / 96M / 128M / 160M / 192M / 224M / 256M / 288M / 320M / 352M / 384M / 416M / 448M / 480M / 512M	Select DVMT5.0 Pre-Allocated (Fixed) Graphics Memory size used by the Internal Graphic Device
DVMT Total Gfx Mem	128M / 256M / MAX	Select the size of DVMT (Dynamic Video Memory) 5.0 that the Internal Graphics Device will use

DFD Restore	Enabled / Disabled	Select Display memory map programming for DFD Restore
DiSM Size (GB)	[0..7]	DiSM Size for 2LM Sku
Intel Graphics Pei Display Peim	Enabled / Disabled	Enable / Disable Pei (Early) Display
VDD Enable	Enabled / Disabled	Enable / Disable forcing of VDD in the BIOS
Configure GT for use	Enabled / Disabled	Enable / Disable GT configuration in BIOS
RC1p Support	Enabled / Disabled	Enable / Disable RC1p support. If RC1p is enabled, send a RC1p frequency request to PMA based other conditions being met
PAVP Enable	Enabled / Disabled	Enable / Disable Protected Audio Video Playback (PAVP)
Cdynmax Clamping Enable	Enabled / Disabled	Enable / Disable Cdynmax Clamping
Cd Clock Frequency	172.8 MHz / 307.2 MHz / 556.8 MHz / 652.8 MHz / Max CdClock freq based on Reference Clk	Select the highest CD Clock frequency supported by the platform
Skip Full CD Clock Init	Enabled / Disabled	Enabled: Skip Full CD clock initialization; Disabled: Initialize the full CD clock if not initialized by Gfx PEIM
VBT Select	eDP / MIPI	Select VBT for GOP Driver

4.4.2 PCH-IO Configuration

Menu Item	Options	Description
PCI Express Configuration	See submenu	PCI Express Configuration Settings
SATA and RST Configuration	See submenu	SATA Device Options Settings
USB Configuration	See submenu	USB Configuration Settings
Security Configuration	See submenu	Security Configuration Settings
HD Audio Configuration	See submenu	HD Audio Subsystem Configuration Settings
PCIe Ref Pll SSC	Auto / 0.0% / 0.1% / 0.2% / 0.3% / 0.4% / 0.5% / Disabled	Pcie Ref Pll SSC Percentage. AUTO – Keep hw default, no BIOS override.
Flash Potection Range Registers (FPRR)	Enabled / Disabled	Enable Flash Protection Range Registers
SPD Write Disable	TRUE / FALSE	Enable/Disable setting SPD Write Disable. For security recommendations, SPD write disable bit must be set.

4.4.2.1 PCI Express Configuration

Menu Item	Options	Description

DMI Link ASPM Control	Disabled / L0s / L1 / LosL1 / Auto	The control of Active State Power Management of the DMI Link
Compliance Mode	Enabled / Disabled	Enable when using Compliance Load Board
PCI Express Root Port #	See submenu	Sets the parameters for each single PCI-e Root Port

4.4.2.1.1 PCI Express Root Port

Menu Item	Options	Description
PCI Express Root Port #	Enabled / Disabled	Controls the PCI Express Root Port
Connection Type	Built-in / Slot	Built-In: a built-in device is connected to this rootport. SlotImplemented bit will be clrear. Slot: this rootport connects to used-sccessible slot. SlotImplemented but will be set.
ASPM	Disabled / L0s / L1 / L0sL1 / Auto	Set the ASPM level
L1 Substates	Disabled / L1.1 / L1.1 & L1.2	PCI Express L1 Substates
Hot Plug	Enabled / Disabled	PCI Express Hot Plug Enable / Disable
PCIe Speed	Auto / Gen1 / Gen2 / Gen3	Configure PCIe Speed

4.4.2.2 SATA and RST Configuration

Menu Item	Options	Description
SATA Controller(s)	Enabled / Disabled	Enable/Disable SATA Devices
SATA Mode Selection	[AHCI]	Determines how SATA controller(s) operate
SATA Test Mode	Enabled / Disabled	Test Mode Enable / Disable (Loop Back)
Software Feature Mask Configuration	See Submenu	RST Legacy OROM/RST UEFI driver will refer to the SWFM configuration to enable/disable the storage features
Aggressive LPM Support	Enabled / Disabled	Enable PCH to aggressively enter link power state
Port #	Enabled / Disabled	Enable / Disable SATA Port
Hot Plug	Enabled / Disabled	Designate this port as Hot Pluggable
External	Enabled / Disabled	Marks this port as external
Spin Up Device	Enabled / Disabled	If enabled for any of ports Staggerred Spin Up will be performed and only the drivers which have this option enabled will spin up at boot. Otherwise all drives spin up at boot.
SATA Device Type	Hard Disk Drive Solid State Drive	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive
Topology	Unknown / ISATA / Direct Connect / Flex / M2	Identify the SATA Topology if it is Default or ISATA or Flex or DirectConnect or M2

SATA Port # DevSlp	Enabled / Disabled	Enable / Disable SATA Port # DevSlp. For DevSlp to work both hard drive and SATA port need to support DevSlp function, otherwise and unexpected behaviour might happen. Please check board design before enabling it.
DITO Configuration	Enabled / Disabled	Enable / Disable DITO Configuration
DITO Value	[..]	DITO Value
DM Value	[..]	DM Value

4.4.2.3 USB Configuration

Menu Item	Options	Description
xDCI Support	Enabled / Disabled	Enable / Disable xDCI (USB OTG Device)
USB2 PHY Sus Well Power Gating	Enabled / Disabled	Select Enabled to enable SUS Well PG for USB2 PHY. This option has no effect on PCH-H
USB3 Link Speed Selection	GEN1 / GEN2	This option is to select USB3 Link Speed GEN1 or GEN2
USB PD0 Programming	Enabled / Disabled	Select Enable if Port Disable Override functionality is used
XHCI LTR Mode	Enabled / Disabled	Enable / Disable XHCI LTR Mode
Enable HSII on xHCI	Enabled / Disabled	Enable / Disable HSII feature. It may lead to increased power consumption.
USB Overcurrent	Enabled / Disabled	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	Enabled / Disabled	Select Enabled is Overcurrent functionality is used. Enabling this will make xHCI controller consume the Overcurrent mapping data
USB Port Disable Override	Enabled / Disabled	Selectively Enable / Disable the corresponding USB port from reporting a Device Connection to the controller

4.4.2.4 Security Configuration

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

4.4.2.5 HD Audio Configuration

Menu Item	Options	Description
HD Audio	Enabled / Disabled	Control Detection of the HD-Audio device. When enabled, following menu items will appear
Audio DSP	Enabled / Disabled	Enables/Disables Audio DSP

Audio Link Mode	HD Audio Link SSP (I2S) SoundWire Advanced Link Config	Select link mode: 1) HDA-Link [SDIO-1], DMIC[0-1] 2) SSP[0-5], DMIC[0-1] 3) SNDW[1-4] 4) Advanced will allow to enable each interface separately
HDA-Link Codec Select	Platform Onboard External Kit	Selects whether Platform Onboard Codec (single Verb Table installed) or External Codec Kit (multiple Verb Tables installed) will be used
HD Audio Advanced Configuration	See submenu	HD Audio Subystem Advanced Configuration Settings
HD Audio DSP Features Configuration	See submenu	HD Audio Subsystem Features Configuration (ACPI)
HD Audio Bus Controller Subsystem Id	[...]	Selects HD Audio Bus Controller Subsystem Id

4.4.2.5.1 HD Audio Advanced Configuration

Menu Item	Options	Description
iDisplay Audio Disconnect	Enabled / Disabled	Disconnects SDI2 signal to hide (disable) iDisplay Audio Codec
Codec Sx Wake Capability	Enabled / Disabled	Capability to detect wake initiated by a codec in Sx (e.g. by modem codec)
PME Enable	Enabled / Disabled	Enables PME wake of HD Audio controller during POST
HD Audio Link Frequency	6 MHz 12 MHz 24 MHz	Selects HD Audio Link frequency. Applicable only if HAD codec supports selected frequency
iDisplay Audio Link Frequency	48 MHz 96 MHz	Selects iDisplay Link frequency
iDisplay Audio Link T-Mode	2T / 4T / 8T / 16T	Indicate whether SDI is operating in 1T, 2T (CNL) or 2T, 4T, 8T mode (ICL)
Autonomous Clock Stop SNDW #	Enabled / Disabled	Enable / Disable Autonomous Clock Stop for SoundWire LINK #
Data on Active Interval Select SNDW #	3 / 4 / 5 / 6	Data on Active Interval Select Clock Periods for SoundWire LINK #
Data on Delay Select SNDW #	2 / 3	Data on Delay Select Clock Periods for SoundWire LINK #

4.4.2.5.2 HD Audio Subsystem Features Configuration (ACPI)

Menu Item	Options	Description
WoV (Wake on Voice)	Enabled / Disabled	Disconnects SDI2 signal to hide (disable) iDisplay Audio Codec
Bluetooth Sideband	Enabled / Disabled	Capability to detect wake initiated by a codec in Sx (e.g. by modem codec)
BT Intel HFP	Enabled / Disabled	Enables PME wake of HD Audio controller during POST

BT Intel A2DP	Enabled / Disabled	Selects HD Audio Link frequency. Applicable only if HAD codec supports selected frequency
Codec based VAD	Enabled / Disabled	Selects iDisplay Link frequency
Voice Activity Detection	Intel Wake on Voice Windows 10 Voice Activation	Indicate whether SDI is operating in 1T, 2T (CNL) or 2T, 4T, 8T mode (ICL)
Waves Post-process	Enabled / Disabled	Enable/Disable 3rd Party Processing Module Support (identified by GUID). WoV must be Enabled
DTS	Enabled / Disabled	"
IntelSST Speech	Enabled / Disabled	"
Dolby	Enabled / Disabled	"
Waves Pre-process	Enabled / Disabled	"
Audyssey	Enabled / Disabled	"
Maxim Smart AMP	Enabled / Disabled	"
ForteMedia SAMSoft	Enabled / Disabled	"
Sound Research IP	Enabled / Disabled	"
Conexant Pre-Process	Enabled / Disabled	"
Conexant Smart AMP	Enabled / Disabled	"
Realtek Post-Process	Enabled / Disabled	"
Realtek Smart Amp	Enabled / Disabled	"
Icepower IP MFX sub module	Enabled / Disabled	"
Icepower IP EFX sub module	Enabled / Disabled	"
Icepower IP SFX sub module	Enabled / Disabled	"
Voice Preprocessing	Enabled / Disabled	"
Custom Module 'Alpha'	Enabled / Disabled	"
Custom Module 'Beta'	Enabled / Disabled	"
Custom Module 'Gamma'	Enabled / Disabled	"

4.5 Security menu

Menu Item	Options	Description
Administrator Password		Set Administrator Password
User Password		Set User Password
List of available storage units		HDD Security Configuration for selected drive --> Set HDD User Password
Secure Boot	See submenu	Secure Boot configuration

4.5.1 Secure Boot submenu

Menu Item	Options	
Secure Boot	Enabled / Disabled	Secure Boot feature is Active if Secure Boot is Enabled, Platform Key (PK) is enrolled and System is in User Mode. The mode change requires platform reset.
Secure Boot Mode	Standard / Custom	Secure Boot Mode options: Standard or Custom. In Custom mode, Secure Boot Policy variables can be configured by a physically present user without full authentication.
Restore Factory Keys		Force system to User Mode. Install factory default Secure Boot key databases.
Reset To Setup Mode		Delete all Secure Boot key databases from NVRAM
Key management	See submenu	Enable expert users to modify Secure Boot Policy variables without full authentication.

4.5.1.1 Key Management submenu

Menu Item	Options	
Factory Key Provision	Enabled / Disabled	Install factory default Secure Boot keys after the platform reset and while the system is in Setup mode
Restore Factory Keys		Force System to User Mode. Install factory default Secure Boot key databases
Reset To Setup Mode		Delete all Secure Boot key databases from NVRAM
Enroll Efi Image	*File System Image*	Allow the image to run in Secure Boot mode. Enrol SHA256 Hash certificate of a PE Image into Authorized Signature Database (db)
Remove 'UEFI CA' from DB		Device Guard ready system must not list 'Microsoft UEFI CA' Certificate in Authorized Signature database (db)
Restore DB defaults		Restore DB variable to factory defaults
Platform key (PK) Key Exchange Keys Authorized Signatures Forbidden Signatures	Set New Var Append Key	Enrol factory Defaults or load certificates from a file: 1. Public Key Certificate in: a) EFI_SIGNATURE_LIST b) EFI_CERT_X509 (DER encoded)

Authorized Timestamps OS Recovery Signatures		c) EFI_CERT_RSA2048 (bin) d) EFI_CERT_SHAxxx 2. Authenticated UEFI Variable 3. EFI PE/COFF Image (SHA256), Key Source: Factory, External, Mixed

4.6 Boot menu

Menu Item	Options	Description
Setup Prompt Timeout	0 .. 65535	Number of seconds to wait for setup activation key. 655535 means indefinite waiting.
Bootup NumLock State	On / Off	Select the keyboard NumLock state
Quiet Boot	Enabled / Disabled	Enables or disables Quiet Boot option
Fast Boot	Enabled / Disabled	Enables or disables boot with initialization of a minimal set of devices required to launch active boot option. Has no effect for BBS boot options.
SATA Support	Last Boot SATA Devices Only All SATA Devices	If Last Boot SATA Devices Only, only last boot SATA device will be available in Post. If All SATA Devices, all SATA devices will be available in OS and Post.
NVMe Support	Enabled / Disabled	If Disabled, NVMe device will be skipped
USB Support	Disabled Full Initial Partial Initial	If Disabled, all USB devices will NOT be available until after OS boot. If Partial Initial, USB Mass Storage and specific USB port/device will NOT be available before OS boot. If Enabled, all USB devices will be available in OS and Post.
PS2 Devices Support	Enabled / Disabled	If Disabled, PS2 devices will be skipped
Network Stack Driver Support	Enabled / Disabled	If Disabled, Network Stack Driver will be skipped
Redirection Support	Enabled / Disabled	If Disabled, Redirection function will be disabled
• Boot Option #1 • Boot Option #2 • Boot Option #3 • Boot Option #4 • Boot Option #5 • Boot Option #6 • Boot Option #7 • Boot Option #8 • Boot Option #9 • Boot Option #10	Hard Disk NVME CD/DVD SD USB Hard Disk USB CD/DVD USB Key USB Floppy USB Lan Network Disabled	Select the system boot order

4.7 Save & Exit menu

Menu Item	Options	Description
Save Options		
Save Changes and Exit		Exit system setup after saving the changes.
Discard Changes and Exit		Exit system setup without saving any changes.
Save Changes and Reset		Reset the system after saving the changes.
Discard Changes and Reset		Reset the system without saving any changes.
Save Changes		Save the changes done so far to any of the setup options.
Discard Changes		Discard the changes done so far to any of the setup options.
Default Options		
Restore Defaults		Restore/Load Default values for all the setup options
Save as User Defaults		Save the changes done so far as User Defaults
Restore User Defaults		Restore the User Defaults to all the setup options
Boot Override		
List of EFI boot managers available		Boot override to selected boot manager
Launch EFI Shell from filesystem device		Attempts to Launch EFI Shell application (Shell.efi) from one of the available filesystem devices

Note:
For a "Save Changes" to take effect the system will reboot twice therefore Boot Override selection will not be effective.

Boot Override selection will be effective when no changes are applied to BIOS parameters.

Chapter 5.
Appendices

- Thermal Design

5.1 Thermal Design

Highly integrated modules, like this product, offer very high performance within small dimensions. On the other hand, the miniaturization of ICs and the high operating frequencies of the processors lead to high heat generation that must be dissipated in order to maintain the CPU within its allowed temperature range.

The operating temperature specified in the Technical Features of this product indicates the temperature range in which any and all parts of the heat spreader / heat sink must remain, in order for SECO to guarantee functionality. Hence, these numbers do not necessarily indicate the suitable environmental temperature.

The heat spreader is not intended to be a guaranteed standalone cooling system, but should be used only as a supplemental means of transferring heat to another dissipation system (i.e. heat sinks, fans, heat pipes etc).

It is the customer's responsibility to design and apply an application-dependent cooling system, capable of ensuring that the heat spreader / heat sink temperature remain within the indicated range of the module.

It is an absolute requirement that the customer, after thorough evaluation of the processor's workload in the actual system application, the system enclosure and consequent air flow/Thermal analysis, accurately study and develop a suitable cooling solution for the assembled system.

SECO can provide specific heatspreaders and heatsinks for this module, but please remember that their use must be evaluated accurately inside the final system, and that they should be used only as a part of a more comprehensive ad-hoc cooling solutions.

Ordering Code	Description
SD64-DISS-1-PK	Heat Spreader (PASSIVE) - Packaged
SD64-DISS-3-PK	Heat Sink (ACTIVE) – Packaged

Warning!

The thermal solutions available with SECO boards are tested in the commercial temperature range (0-60°C), without housing and inside climatic chamber. Therefore, the customer is suggested to study, develop and validate the cooling solution for his system, considering ambient temperature, processor's workload, utilisation scenarios, enclosures, air flow and so on.

In particular, the heatspreader is not intended to be a cooling system by itself, but only as the standard means for transferring heat to cooler, like heatsinks, cold plate, heat pipes and so on.

SECO S.p.A. - Via A. Grandi, 20
52100 Arezzo - ITALY
Ph: +39 0575 26979 - Fax: +39 0575 350210
www.seco.com