# Com express

## User Manual

# CALYPSO

COM-Express™ Type 6 Compact Module with the
Intel® 11th Generation Core™ / Celeron® Processors
Formerly Tiger Lake-UP3 Family

www.seco.com

# REVISION HISTORY

| Revision | Date | Note | Rif |
|---|---|---|---|
| 1.0 | 18 April 2023 | First Official Release | 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
- Information and assistance
- RMA number request
- Safety
- Electrostatic Discharges
- RoHS compliance
- Safety Police
- Terminology and definitions
- Reference specifications

## 1.1 Warranty

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.

The authorisation is released after completing the specific ticketing procedure https://support.seco.com/ (web RMA). 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.

The error analysis form identifying the fault type must be completed by the customer and has 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 the product is faulty?

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: contact SECO Technical Assistance. A technician is at disposal to understand the exact origin of the problem and suggest the correct solution.

  E-mail: technical.service@seco.com

  Fax (+39) 0575 350210

- Repair center: it is possible to send the faulty product to the SECO Repair Centre. In this case, follow this procedure:
  - Returned items must be accompanied by a RMA Number. Items sent without the RMA number will be not accepted.
  - Returned items must be shipped in an appropriate package. SECO is not responsible for damages caused by accidental drop, improper usage, or customer neglect.

Note: Please have the following information before asking for technical assistance:

- 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 words of every kind of error message encountered.

## 1.3 RMA number request

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

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

## 1.4 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.
>
> Check carefully that all cables are correctly connected and that they are not damaged.

## 1.5 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.

## 1.6 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.

## 1.7 Safety Police

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.

## 1.8 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 |
| CRT | Cathode Ray Tube. Initially used to indicate a type of monitor, this acronym has been used over time to indicate the analog video interface used to drive them. |
| 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 |
| DDR3 | DDR, 3rd generation |
| DP | Display Port, a type of digital video display interface |
| DVI | Digital Visual interface, 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 |
| eDP | embedded Display Port, a type of digital video display interface specifically developed for the internal connections between boards and digital displays |
| EMI | Electromagnetic Interference |
| 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 |
| LPC Bus | Low Pin Count Bus, a low speed interface based on a very restricted number of signals, deemed to management of legacy peripherals |
| LVDS | Low Voltage Differential Signaling, a standard for transferring data at very high speed using inexpensive twisted pair copper cables, usually used for video applications |
| Mbps | Megabits per second |
| N.A. | Not Applicable |

| | |
|---|---|
| N.C. | Not Connected |
| OS | Operating System |
| OTG | On-the-Go, a specification that allows to USB devices to act indifferently as Host or as a Client, depending on the device connected to the port |
| PCH | Platform Controller Hub |
| 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 half duplex serial interface for Hard Disks |
| SD | Secure Digital, a memory card type |
| SDIO | Secure Digital Input/Output, an evolution of the SD standard that allows the use of the same SD interface to drive different Input/Output devices, like cameras, GPS, Tuners and so on |
| SM Bus | System Management Bus, a subset of the I2C bus dedicated to communication with devices for system management, like a smart battery and other power supply-related devices |
| 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 |
| TTL | Transistor-transistor Logic |
| 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 |
| USB | Universal Serial Bus |
| V_REF | Voltage reference Pin |
| VGA | Video Graphics Array. An analog computer display standard, commonly referred to also as CRT. |
| xHCI | eXtensible Host Controller Interface, Host controller for USB 3.0 ports, which can also manage USB 2.0 and USB1.1 ports |

## 1.9 Reference specifications

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

| Reference | Link |
|---|---|
| ACPI | http://www.acpi.info |
| AHCI | http://www.intel.com/content/www/us/en/io/serial-ata/ahci.html |
| Com Express | https://www.picmg.org/openstandards/com-express/ |
| Com Express Carrier Design Guide | http://picmg.org//wp-content/uploads/PICMG_COMDG_2.0-RELEASED-2013-12-061.pdf |
| DDC | http://www.vesa.org |
| DP, eDP | http://www.vesa.org |
| Gigabit Ethernet | http://standards.ieee.org/about/get/802/802.3.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://cache.nxp.com/documents/user_manual/UM10204.pdf?fsrch=1&sr=2&pageNum=1 |
| LPC Bus | http://www.intel.com/design/chipsets/industry/lpc.htm |
| LVDS | http://www.ti.com/ww/en/analog/interface/lvds.shtml<br>http://www.ti.com/lit/ml/snla187/snla187.pdf |
| PCI Express | http://www.pcisig.com/specifications/pciexpress |
| SATA | https://www.sata-io.org |
| SM Bus | http://www.smbus.org/specs |
| UEFI | http://www.uefi.org |
| USB 2.0 and USB OTG | http://www.usb.org/developers/docs/usb_20_070113.zip |
| USB 3.0 | http://www.usb.org/developers/docs/usb_30_spec_070113.zip |
| xHCI | http://www.intel.com/content/www/us/en/io/universal-serial-bus/extensible-host-controler-interface-usb-xhci.html?wapkw=xhci |
| Intel® Tiger Lake family | https://ark.intel.com/content/www/us/en/ark/products/codename/88759/products-formerly-tiger-lake.html#@Embedded |

# Chapter 2.
# OVERVIEW

- Introduction
- Technical Specifications
- Electrical Specifications
- Mechanical Specifications
- Block Diagram

# 2.1 Introduction

CALYPSO is a COM Express® Type 6, Compact Form Factor, based on the 11th Generation Intel® Core™ family of System-on-Chips (SOCs) formerly coded as Tiger Lake-UP3, a series of Dual / Quad SOCs with 64-bit instruction set.

These SOCs embed all the features usually obtained by combination of CPU + platform Controller hubs, all in one single IC, which allows, therefore, the system minimisation and performance optimisation. The CPUs have direct access to the memory, which is available on two SODIMM DDR4 memory modules, speed up to 3200MHz and compatible with In Band Error Correction Code (IBECC). Please notice that total amount of memory available is OS dependant.

All SOCs embed an Integrated Xe Graphics Core Gen12 architecture, which offers an advanced 2D and 3D graphic engine and it is able to manage up to 3 independent displays (any combination possible between HDMI, DVI, DP++, eDP, LVDS and VGA). It makes available three Digital Display Interfaces that can be used to drive external Display Port, HDMI or DVI displays; moreover, the embedded Display Port interface can be carried out on COM Express connectors directly or used to realise a Dual Channel LVDS 18/24bit interface or a VGA interface (these are factory configurations).

The embedded PCH complete the functionalities of the board offering HD Audio Interface, up to 6 x PCI Express ports (one of them used to manage a Gigabit Ethernet controller), 2 x Serial ATA channels, up to 8 USB ports with up to 4 USB 3.0, Real Time Clock, SPI interface, 2xUARTs, LPC and SM Bus.

The module can be offered with an optional additional TPM module.

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

The product is COM Express® Rel.3.0 standard compliant, an open industry standard defined specifically for COMs (computer on modules). Its definition provides the ability to make a smooth transition from legacy parallel interfaces to the newest technologies based on serial buses available.

COM Express® module integrates all the core components and has to be mounted onto an application-specific carrier board; carrier board designers can utilize as little or as many of the I/O interfaces as deemed necessary. The carrier board can therefore provide all the interface connectors required to attach the system to the application specific peripherals. This versatility allows the designer to create a dense and optimised package, which results in a more reliable product while simplifying system integration. Most important, COM Express® modules are scalable, which means that once an application has been created there is the ability to diversify the product range through the use of different performance class or form factor size modules. Simply unplug one module and replace it with another, no redesign is necessary.

The robust thermal and mechanical concept, combined with extended power-management capabilities, is perfectly suited for all applications.

# 2.2 Technical Specifications

CPU

- Intel® Core™ i7-1185G7E, Quad Core @ 2.8GHz (4.4GHz in Turbo Boost) with HT, 12MB Cache, 28/15/12W cTDP
- Intel® Core™ i5-1145G7E, Quad Core @ 2.6GHz (4.1GHz in Turbo Boost) with HT, 8MB Cache, 28/15/12W cTDP
- Intel® Core™ i3-1115G4E, Dual Core @ 3.0GHz (3.9GHz in Turbo Boost) with HT, 6MB Cache, 28/15/12W cTDP
- Intel® Core™ i7-1185GRE, Quad Core @ 2.8GHz (4.4GHz in Turbo Boost) with HT, 12MB Cache, with IBECC and Functional Safety Essential Design package, 28/15/12W cTDP Industrial (w/ Turbo OFF)
- Intel® Core™ i5-1145GRE, Quad Core @ 2.6GHz (4.1GHz in Turbo Boost) with HT, 8MB Cache, with IBECC and Functional Safety Essential Design package, 28/15/12W cTDP - Industrial (w/ Turbo OFF)
- Intel® Core™ i3-1115GRE, Dual Core @ 2.2GHz (3.9GHz in Turbo Boost) with HT, 6MB Cache, with IBECC and Functional Safety Essential Design package , 28/15/12W cTDP - Industrial (w/ Turbo OFF)
- Intel® Celeron® 6305E, Dual Core @ 1.8GHz with HT, 4MB Cache,15W TDP

Memory

Two DDR4 SO-DIMM Slots supporting DDR4-3200 IBECC Memory, up to 64GB

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

Up to 3x DP++ interfaces, supporting DP 1.2, eDP 1.4, HDMI 1.4 and DVI

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

Optional VGA interface

Video Resolutions

| | |
|---|---|
| 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 |
| VGA | up to 2048 x 1536 @ 50Hz (reduced blanking) |

Mass Storage

2x external S-ATA Gen3 interfaces
PCI-e ports can be used to connect, on the carrier board, M.2 NVMe drives

USB

4 x USB 3.0 Host Ports
8 x USB 2.0 Host ports

Networking

Gigabit Ethernet LAN port, implemented using an Intel® I225 Gigabit Ethernet Controller

Audio

HD Audio interface

PCI Express

8 x PCI-e x1 Gen3 lanes

PCI-e Graphics (PEG) x4 Gen 4 port

Serial Ports

2 x UARTs

Other Interfaces

SPI, I2C, SM Bus, LPC bus, Thermal Management, FAN management
4 x GPI, 4 x GPO
LID# / SLEEP# / PWRBTN#, Watchdog
Optional TPM 2.0 on-board

Power supply voltage: +12$V_{DC}$ ± 10% and + 5$V_{SB}$ (optional)

Operating System:

Microsoft® Windows 10 Enterprise (64-bit)
Microsoft® Windows 10 IoT core
Linux Kernel LTS (64 bit)
Yocto (64 bit)

Operating temperature:

0°C ÷ +60°C (Commercial version) **

-40°C ÷ +85°C (Industrial version) **

Dimensions: 95 x 95 mm

! *** 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. Please also check paragraph 5.1*

# 2.3 Electrical Specifications

According to COM Express® specifications, this board needs to be supplied only with an external +12$V_{DC}$ power supply.

5 Volts standby voltage needs to be supplied for working in ATX mode.

For Real Time Clock working and CMOS memory data retention, it is also needed a backup battery voltage. All these voltages are supplied directly through COM Express Connectors CN5-AB and CN5-CD.

All remaining voltages needed for board's working are generated internally from +12$V_{DC}$ power rail.

## 2.3.1 Power Rails meanings

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.

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

### 2.3.2 Power Consumption

This board, like all COM Express™ modules, needs a carrier board for its normal working. All connections with the external world come through this carrier board, which provide also the required voltage to the board, deriving it from its power supply source.

Anyway, power consumption has been measured on +12V_RUN power rail that supplies the board. For this reason, the values indicated in the table below are real average power consumptions of the board and are independent from those of the peripherals connected to the Carrier Board.

Power consumption in Suspend and Soft-Off States have been measured on +5V_ALW power rail. RTC power consumption has been measured on carrier board's backup battery when the system is not powered.

| Status | Configuration | | | | | |
|---|---|---|---|---|---|---|
| | Intel Celeron 6305E<br>DP++, VGA and LVDS<br>TPM 2.0<br>Comm Temp Range | | Intel Core i7-1185GRE<br>DP++ and LVDS<br>TPM 2.0<br>Ind Temp Range | | Intel Core i5-1145GRE<br>DP++ and LVDS<br>TPM 2.0<br>Ind. Temp Range | |
| | Average | Peak | Average | Peak | Average | Peak |
| OS Boot, power saving configuration | 17.51W | 50.67W | 17.27W | 46.30W | 7.06W | 16.41W |
| Idle, power saving configuration | 6.45W | 6.87W | 6.71W | 7.06W | 2.77W | 3.71W |
| Video reproduction@1080p, power saving configuration | 8.08W | 13.48W | 8.90W | 13.67W | 5.58W | 8.25W |
| Video reproduction@4K, power saving configuration | 9.64W | 15.40W | 8.44W | 13.89W | 7.72W | 13.15W |
| Internal Stress Test Tool, maximum performance | 34.08W | 37.76W | 34.53W | 36.83W | 21.17W | 24.72W |
| RTC backup (VDD_RTC, 3.0V) | 2.80uA | | 2.80uA | | 2.80uA | |
| Suspend (5V_STBY, 5.0V) | 148mA | | 150mA | | 120mA | |
| Soft-off (5V_STBY, 5.0V) | 85mA | | 85mA | | 50mA | |

## 2.4 Mechanical Specifications

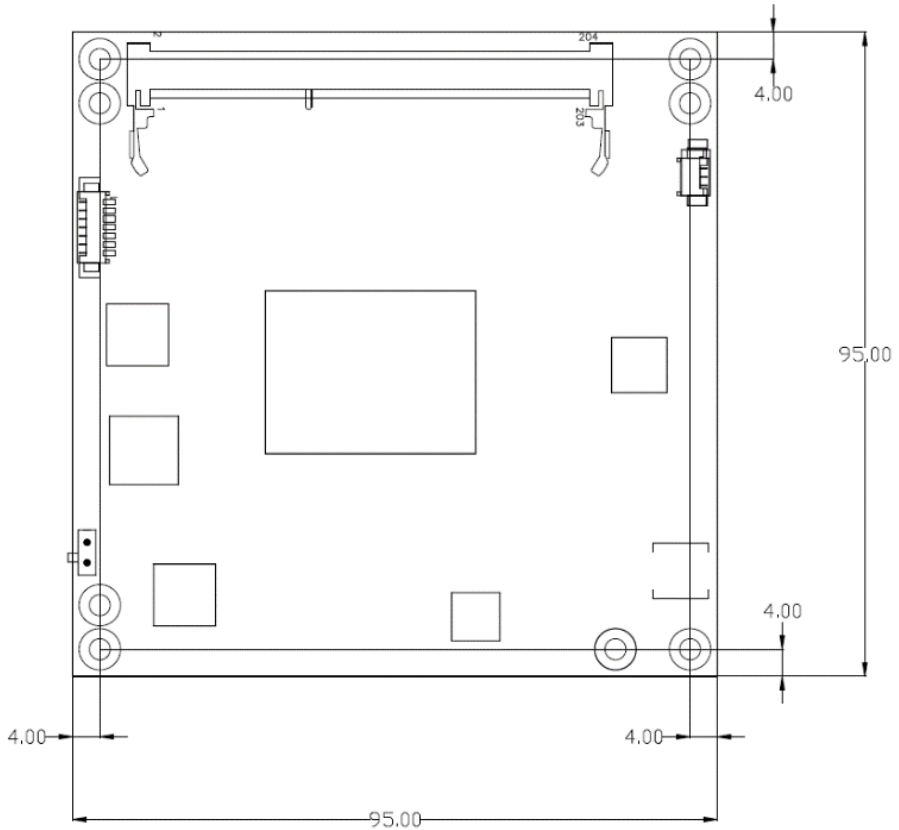
The board is a COM Express board, Compact Form Factor type; therefore its dimensions are 95 mm x 95 mm (3.74" x 3.74").

Printed circuit of the board is made of twelve layers, some of them are ground planes, for disturbance rejection.

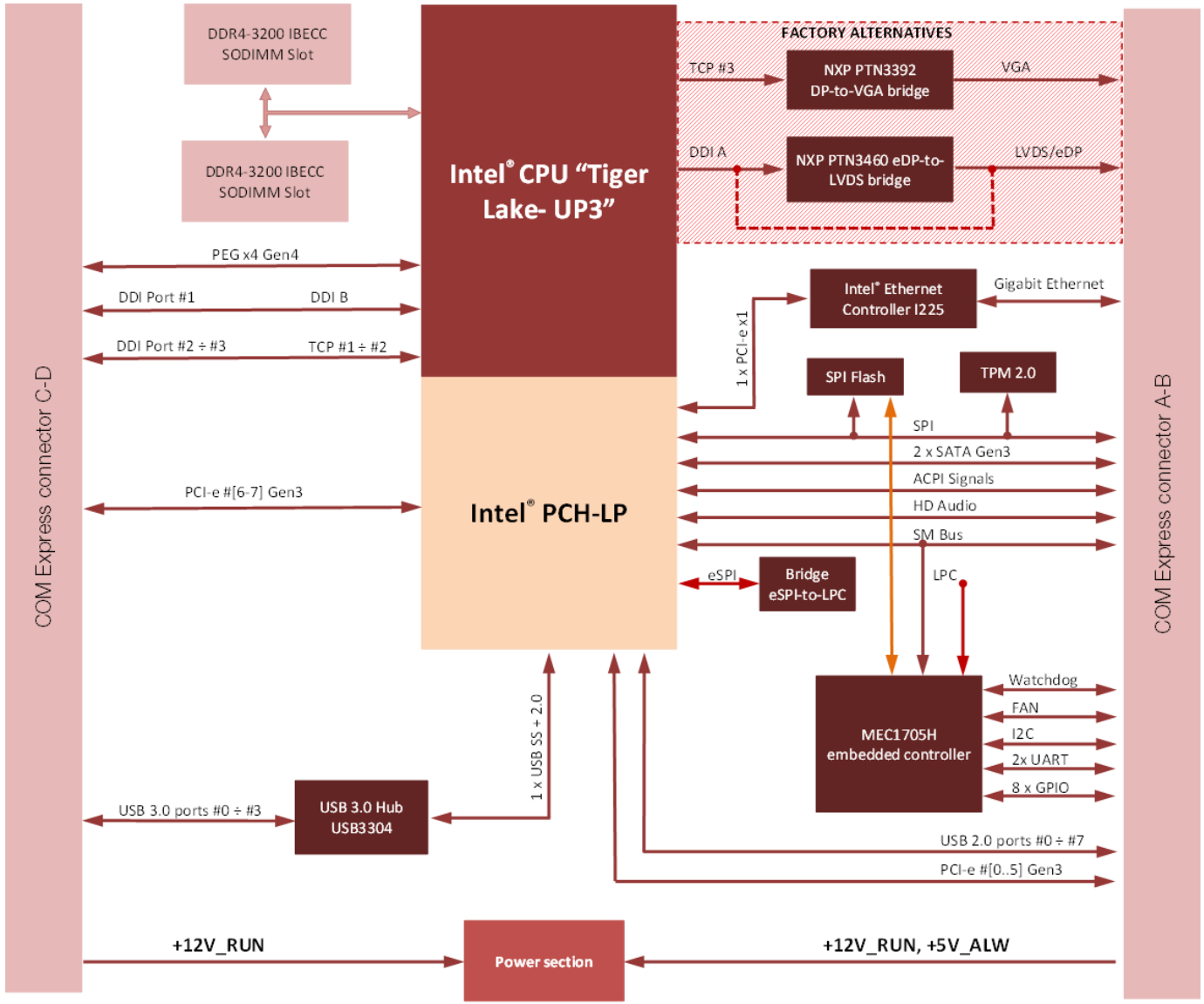
According to COM Express specifications, the carrier board plug can be of two different heights, 5mm and 8mm.

Whichever connector's height is chosen, in designing a custom carrier board please remember that the SO-DIMM connector on bottom side of the board is 4mm high (it is the component with the maximum height).

This value must be kept in high consideration when choosing the carrier board plugs' height, if it is necessary to place components on the carrier board in the zone under the COM Express® module.



# 2.5 Block Diagram



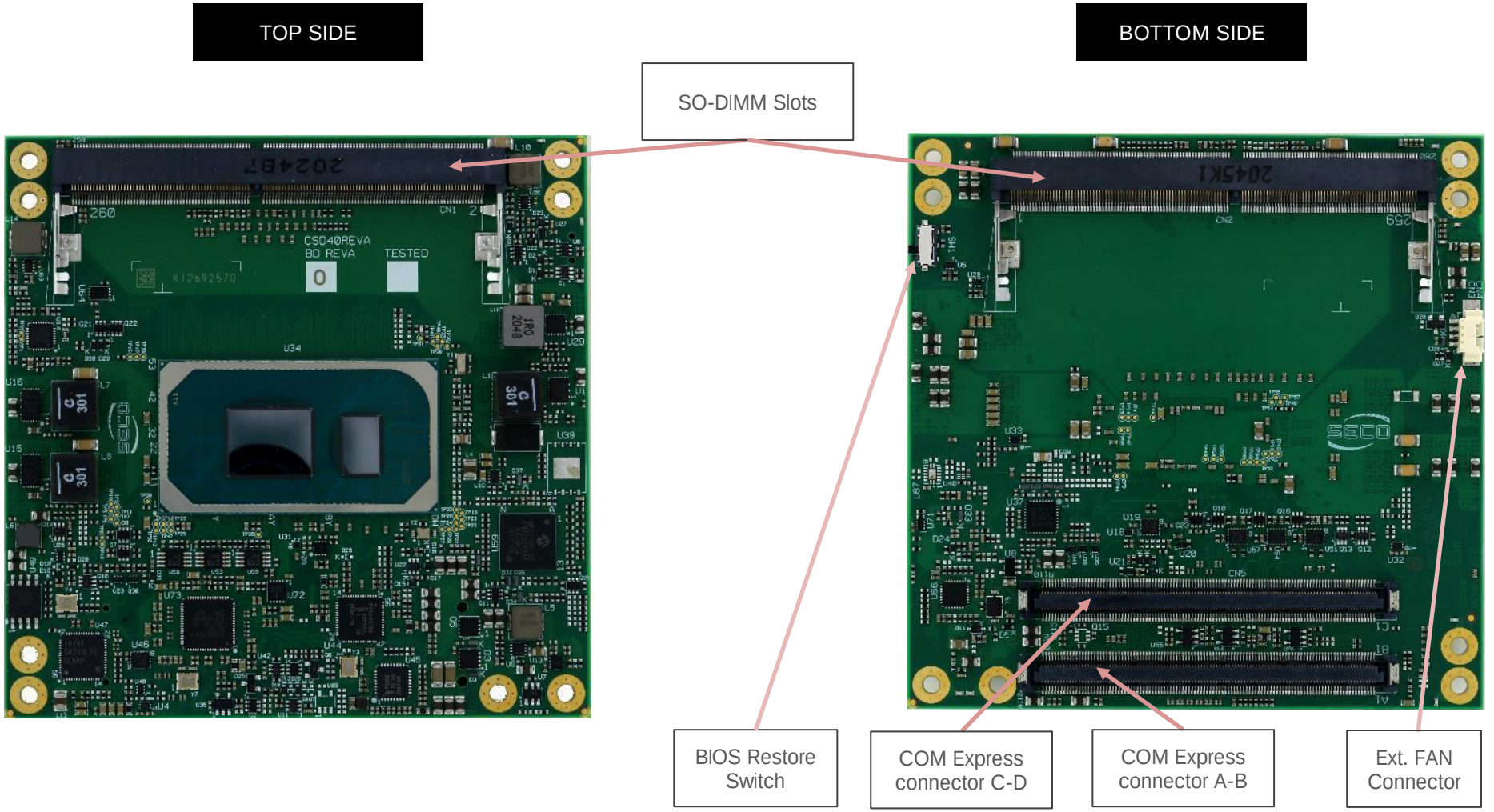
# Chapter 3.
# CONNECTORS

- Introduction
- Connectors description

# 3.1 Introduction

According to COM Express® specifications, all interfaces to the board are available through two 220 pin connectors, for a total of 440 pin. Simplifying the terminology in this documentation, the primary connector is called A-B and the secondary C-D, since each one consists of two rows.

In addition, a Fan connector has been placed on one side of the board, in order to allow an easier connection of active heatsinks to the module.

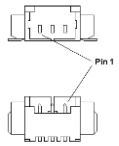


# 3.2 Connectors description

### 3.2.1 FAN Connector

| FAN Connector - CN4 | |
|---|---|
| **Pin** | **Signal** |
| 1 | GND |
| 2 | FAN_POWER |
| 3 | FAN_TACHO_IN |

Depending on the usage model of the board, for critical applications/environments on the module itself it is available a 3-pin dedicated connector for an external +12VDC FAN.




FAN Connector is 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.

Please be aware that the use of an external fan depends strongly on customer's application/installation.

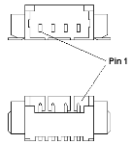
Please refer to chapter 5.1 for considerations about thermal dissipation.

FAN_POWER: +12V_RUN 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 and Schottky diode.

| FAN Connector – CN7 | |
|---|---|
| **Pin** | **Signal** |
| 1 | GND |
| 2 | FAN_POWER |
| 3 | FAN_TACHO_IN |
| 4 | FAN_PWM |

As a factory alternative, onboard it is available a 4-pin connector, type MOLEX 53261-0471 or equivalent, for the connection of tachometric FANs.




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

FAN_POWER: +12V_RUN derived power rail for FAN

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

FAN_PWM: +3.3V_RUN fan PWM input managed by the embedded microcontroller.

### 3.2.2 SO-DIMM DDR4 Slots

CPUs used on the board provide support to DDR4-3200 IBECC memories, up to 64GB, which can be integrated by using the dedicated DDR4 SO-DIMM sockets.

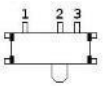
The socket placed on top side (CN1) is type LOTES ADDR0067-P005A or equivalent, a right angle, standard socket, h = 5.2mm.

The socket placed on bottom side (CN2) is type LOTES ADDR0206-P003A or equivalent, a right angle, reversed socket, h = 4mm.

The two sockets together allow the insertion of up to 2 SO-DIMM modules, for support of dual channel memories.

### 3.2.3 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 module it 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 1-2 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 2-3 position.

During normal use, the contact MUST be always placed in 2-3 position.

### 3.2.4 COM Express® Module connectors

For the connection of COM Express® CPU modules, on board there is one double connector, type TYCO 3-1827231-6 (440 pin, ultra thin, 0.5mm pitch, h=4mm), as requested by COM Express® specifications.

The pinout of the module is compliant to COM Express® Type 6 specifications. Not all the signals contemplated in COM Express® standard are implemented on the double connector, due to the functionalities really implemented on the board. Therefore, please refer to the following table for a list of effective signals reported on the connector. For accurate signals description, please consult the following paragraphs.

**COM Express® Connector CN5 – Rows A & B**

| | | ROW A | | | ROW B | | |
|---|---|---|---|---|---|---|---|
| SIGNAL GROUP | Type | Pin name | Pin nr. | Pin nr. | Pin name | Type | SIGNAL GROUP |
| | PWR | GND | A1 | B1 | GND | PWR | |
| GBE | I/O | GBE0_MDI3- | A2 | B2 | GBE0_ACT# | O | GBE |
| GBE | I/O | GBE0_MDI3+ | A3 | B3 | LPC_FRAME# | O | LPC |
| GBE | O | GBE0_LINK100# | A4 | B4 | LPC_AD0 | I/O | LPC |
| GBE | O | GBE0_LINK1000# | A5 | B5 | LPC_AD1 | I/O | LPC |
| GBE | I/O | GBE0_MDI2- | A6 | B6 | LPC_AD2 | I/O | LPC |
| GBE | I/O | GBE0_MDI2+ | A7 | B7 | LPC_AD3 | I/O | LPC |
| GBE | O | GBE0_LINK# | A8 | B8 | LPC_DRQ0# | I | LPC |
| GBE | I/O | GBE0_MDI1- | A9 | B9 | LPC_DRQ1# | I | LPC |
| GBE | I/O | GBE0_MDI1+ | A10 | B10 | LPC_CLK | O | LPC |
| | PWR | GND | A11 | B11 | GND | PWR | |
| GBE | I/O | GBE0_MDI0- | A12 | B12 | PWRBTN# | I | PWR_MGMT |
| GBE | I/O | GBE0_MDI0+ | A13 | B13 | SMB_CK | I/O | SMBUS |
| | | N.C. | A14 | B14 | SMB_DAT | O | SMBUS |
| PWR_MGMT | O | SUS_S3# | A15 | B15 | SMB_ALERT# | I | SMBUS |
| SATA | O | SATA0_TX+ | A16 | B16 | SATA1_TX+ | O | SATA |
| SATA | O | SATA0_TX- | A17 | B17 | SATA1_TX- | O | SATA |
| PWR_MGMT | O | SUS_S4# | A18 | B18 | SUS_STAT# | O | PWR_MGMT |
| SATA | I | SATA0_RX+ | A19 | B19 | SATA1_RX+ | I | SATA |
| SATA | I | SATA0_RX- | A20 | B20 | SATA1_RX- | I | SATA |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | PWR | GND | A21 | B21 | GND | PWR | |
| | | N.C. | A22 | B22 | SATA3_TX+ | O | SATA |
| | | N.C. | A23 | B23 | SATA3_TX- | O | SATA |
| PWR_MGMT | O | SUS_S5# | A24 | B24 | PWR_OK | I | PWR_MGMT |
| | | N.C. | A25 | B25 | SATA3_RX+ | I | SATA |
| | | N.C. | A26 | B26 | SATA3_RX- | I | SATA |
| PWR_MGMT | I | BATLOW# | A27 | B27 | WDT | O | MISC |
| SATA | O | SATA_ACT# | A28 | B28 | N.C | | |
| AUDIO | O | HDA_SYNC | A29 | B29 | HDA_SDIN1 | I/O | AUDIO |
| AUDIO | O | HDA_RST# | A30 | B30 | HDA_SDIN0 | I/O | AUDIO |
| | PWR | GND | A31 | B31 | GND | PWR | |
| AUDIO | O | HDA_BITCLK | A32 | B32 | SPKR | O | MISC |
| AUDIO | O | HDA_SDOUT | A33 | B33 | I2C_CK | O | I2C |
| SPI | I | BIOS_DIS0# | A34 | B34 | I2C_DAT | I/O | I2C |
| MISC | O | THRMTRIP# | A35 | B35 | THRM# | I | MISC |
| USB | I/O | USB6- | A36 | B36 | USB7- | I/O | USB |
| USB | I/O | USB6+ | A37 | B37 | USB7+ | I/O | USB |
| USB | I | USB_6_7_OC# | A38 | B38 | USB_4_5_OC# | I | USB |
| USB | I/O | USB4- | A39 | B39 | USB5- | I/O | USB |
| USB | I/O | USB4+ | A40 | B40 | USB5+ | I/O | USB |
| | PWR | GND | A41 | B41 | GND | PWR | |
| USB | I/O | USB2- | A42 | B42 | USB3- | I/O | USB |
| USB | I/O | USB2+ | A43 | B43 | USB3+ | I/O | USB |
| USB | I | USB_2_3_OC# | A44 | B44 | USB_0_1_OC# | I | USB |
| USB | I/O | USB_0- | A45 | B45 | USB1- | I/O | USB |
| USB | I/O | USB_0+ | A46 | B46 | USB1+ | I/O | USB |
| | PWR | VCC_RTC | A47 | B47 | ESPI_EN# | I | SPI |
| | | N.C. | A48 | B48 | N.C. | | |
| GBE | O | GBE0_SDP | A49 | B49 | SYS_RESET# | I | PWR_MGMT |
| LPC | I/O | LPC_SERIRQ | A50 | B50 | CB_RESET# | O | PWR_MGMT |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | PWR | GND | A51 | B51 | GND | PWR | |
| PCIE | O | PCIE_TX5+ | A52 | B52 | PCIE_RX5+ | I | PCIE |
| PCIE | O | PCIE_TX5- | A53 | B53 | PCIE_RX5- | I | PCIE |
| GPIO | I | GPI0 | A54 | B54 | GPO1 | O | GPIO |
| PCIE | O | PCIE_TX4+ | A55 | B55 | PCIE_RX4+ | I | PCIE |
| PCIE | O | PCIE_TX4- | A56 | B56 | PCIE_RX4- | I | PCIE |
| | PWR | GND | A57 | B57 | GPO2 | O | GPIO |
| PCIE | O | PCIE_TX3+ | A58 | B58 | PCIE_RX3+ | I | PCIE |
| PCIE | O | PCIE_TX3- | A59 | B59 | PCIE_RX3- | I | PCIE |
| | PWR | GND | A60 | B60 | GND | PWR | |
| PCIE | O | PCIE_TX2+ | A61 | B61 | PCIE_RX2+ | I | PCIE |
| PCIE | O | PCIE_TX2- | A62 | B62 | PCIE_RX2- | I | PCIE |
| GPIO | I | GPI1 | A63 | B63 | GPO3 | O | GPIO |
| PCIE | O | PCIE_TX1+ | A64 | B64 | PCIE_RX1+ | I | PCIE |
| PCIE | O | PCIE_TX1- | A65 | B65 | PCIE_RX1- | I | PCIE |
| | PWR | GND | A66 | B66 | WAKE0# | I | PWR_MGMT |
| GPIO | I | GPI2 | A67 | B67 | WAKE1# | I | PWR_MGMT |
| PCIE | O | PCIE_TX0+ | A68 | B68 | PCIE_RX0+ | I | PCIE |
| PCIE | O | PCIE_TX0- | A69 | B69 | PCIE_RX0- | I | PCIE |
| | PWR | GND | A70 | B70 | GND | PWR | |
| eDP/LVDS | O | eDP_TX2+/LVDS_A0+ | A71 | B71 | LVDS_B0+ | O | LVDS |
| eDP/LVDS | O | eDP_TX2-/LVDS_A0- | A72 | B72 | LVDS_B0- | O | LVDS |
| eDP/LVDS | O | eDP_TX1+/LVDS_A1+ | A73 | B73 | LVDS_B1+ | O | LVDS |
| eDP/LVDS | O | eDP_TX1-/LVDS_A1- | A74 | B74 | LVDS_B1- | O | LVDS |
| eDP/LVDS | O | eDP_TX0+/LVDS_A2+ | A75 | B75 | LVDS_B2+ | O | LVDS |
| eDP/LVDS | O | eDP_TX0-/LVDS_A2- | A76 | B76 | LVDS_B2- | O | LVDS |
| eDP/LVDS | O | eDP/LVDS_VDD_EN | A77 | B77 | LVDS_B3+ | O | LVDS |
| LVDS | O | LVDS_A3+ | A78 | B78 | LVDS_B3- | O | LVDS |
| LVDS | O | LVDS_A3- | A79 | B79 | eDP/LVDS_BKLT_EN | O | eDP/LVDS |
| | PWR | GND | A80 | B80 | GND | PWR | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| eDP/LVDS | O | eDP_TX3+/LVDS_A_CK+ | A81 | B81 | LVDS_B_CK+ | O | LVDS |
| eDP/LVDS | O | eDP_TX3-/LVDS_A_CK- | A82 | B82 | LVDS_B_CK- | O | LVDS |
| eDP/LVDS | I/O | eDP_AUX+/LVDS_I2C_CK | A83 | B83 | eDP/LVDS_BKLT_CTRL | O | eDP/LVDS |
| eDP/LVDS | I/O | eDP_AUX-/LVDS_I2C_DAT | A84 | B84 | +5V_ALW | PWR | |
| GPIO | I | GPI3 | A85 | B85 | +5V_ALW | PWR | |
| | | N.C. | A86 | B86 | +5V_ALW | PWR | |
| eDP | I | eDP_HPD | A87 | B87 | +5V_ALW | PWR | |
| PCIE | O | PCIE_CLK_REF+ | A88 | B88 | BIOS_DIS1# | I | SPI |
| PCIE | O | PCIE_CLK_REF- | A89 | B89 | VGA_RED | O | VGA |
| | PWR | GND | A90 | B90 | GND | PWR | |
| SPI | O | SPI_POWER | A91 | B91 | VGA_GRN | O | VGA |
| SPI | I | SPI_MISO | A92 | B92 | VGA_BLU | O | VGA |
| GPIO | O | GPO0 | A93 | B93 | VGA_HSYNC | O | VGA |
| SPI | O | SPI_CLK | A94 | B94 | VGA_VSYNC | O | VGA |
| SPI | O | SPI_MOSI | A95 | B95 | VGA_I2C_CK | I/O | VGA |
| MISC | I | TPM_PP | A96 | B96 | VGA_I2C_DAT | I/O | VGA |
| | | N.C. | A97 | B97 | SPI_CS# | O | SPI |
| UART | O | SER0_TX | A98 | B98 | N.C. | | |
| UART | I | SER0_RX | A99 | B99 | N.C. | | |
| | PWR | GND | A100 | B100 | GND | PWR | |
| UART | O | SER1_TX | A101 | B101 | FAN_PWMOUT | O | MISC |
| UART | I | SER1_RX | A102 | B102 | FAN_TACHIN | I | MISC |
| PWR_MGMT | I | LID# | A103 | B103 | SLEEP# | I | PWR_MGMT |
| | PWR | +12V_RUN | A104 | B104 | +12V_RUN | PWR | |
| | PWR | +12V_RUN | A105 | B105 | +12V_RUN | PWR | |
| | PWR | +12V_RUN | A106 | B106 | +12V_RUN | PWR | |
| | PWR | +12V_RUN | A107 | B107 | +12V_RUN | PWR | |
| | PWR | +12V_RUN | A108 | B108 | +12V_RUN | PWR | |
| | PWR | +12V_RUN | A109 | B109 | +12V_RUN | PWR | |
| | PWR | GND | A110 | B110 | GND | PWR | |

| COM Express® Connector CN5 – Rows C & D | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | ROW C | | | ROW D | | |
| SIGNAL GROUP | Type | Pin name | Pin nr. | Pin nr. | Pin name | Type | SIGNAL GROUP |
| | PWR | GND | C1 | D1 | GND | PWR | |
| | PWR | GND | C2 | D2 | GND | PWR | |
| USB | I | USB_SSRX0- | C3 | D3 | USB_SSTX0- | O | USB |
| USB | I | USB_SSRX0+ | C4 | D4 | USB_SSTX0+ | O | USB |
| | PWR | GND | C5 | D5 | GND | PWR | |
| USB | I | USB_SSRX1- | C6 | D6 | USB_SSTX1- | O | USB |
| USB | I | USB_SSRX1+ | C7 | D7 | USB_SSTX1+ | O | USB |
| | PWR | GND | C8 | D8 | GND | PWR | |
| USB | I | USB_SSRX2- | C9 | D9 | USB_SSTX2- | O | USB |
| USB | I | USB_SSRX2+ | C10 | D10 | USB_SSTX2+ | O | USB |
| | PWR | GND | C11 | D11 | GND | PWR | |
| USB | I | USB_SSRX3- | C12 | D12 | USB_SSTX3- | O | USB |
| USB | I | USB_SSRX3+ | C13 | D13 | USB_SSTX3+ | O | USB |
| | PWR | GND | C14 | D14 | GND | PWR | |
| | | N.C. | C15 | D15 | DDI1_CTRLCLK_AUX+ | I/O | DDI |
| | | N.C. | C16 | D16 | DDI1_CTRLDATA_AUX- | I/O | DDI |
| | | N.C. | C17 | D17 | N.C. | | |
| | | N.C. | C18 | D18 | N.C. | | |
| PCIE | I | PCIE_RX6+ | C19 | D19 | PCIE_TX6+ | O | PCIE |
| PCIE | I | PCIE_RX6- | C20 | D20 | PCIE_TX6- | O | PCIE |
| | PWR | GND | C21 | D21 | GND | PWR | |
| PCIE | I | PCIE_RX7+ | C22 | D22 | PCIE_TX7+ | O | PCIE |
| PCIE | I | PCIE_RX7- | C23 | D23 | PCIE_TX7- | O | PCIE |
| DDI | I | DDI1_HPD | C24 | D24 | N.C. | | |
| | | N.C. | C25 | D25 | N.C. | | |
| | | N.C. | C26 | D26 | DDI1_PAIR0+ | O | DDI |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | N.C. | C27 | D27 | DDI1_PAIR0- | O | DDI |
| | | N.C. | C28 | D28 | N.C. | | |
| | | N.C. | C29 | D29 | DDI1_PAIR1+ | O | DDI |
| | | N.C. | C30 | D30 | DDI1_PAIR1- | O | DDI |
| | PWR | GND | C31 | D31 | GND | PWR | |
| DDI | I/O | DDI2_CTRLCLK_AUX+ | C32 | D32 | DDI1_PAIR2+ | O | DDI |
| DDI | I/O | DDI2_CTRLDATA_AUX- | C33 | D33 | DDI1_PAIR2- | O | DDI |
| DDI | I | DDI2_DDC_AUX_SEL | C34 | D34 | DDI1_DDC_AUX_SEL | I | DDI |
| | | N.C. | C35 | D35 | N.C. | | |
| DDI | I/O | DDI3_CTRLCLK_AUX+ | C36 | D36 | DDI1_PAIR3+ | O | DDI |
| DDI | I/O | DDI3_CTRLDATA_AUX- | C37 | D37 | DDI1_PAIR3- | O | DDI |
| DDI | I | DDI3_DDC_AUX_SEL | C38 | D38 | N.C. | | |
| DDI | O | DDI3_PAIR0+ | C39 | D39 | DDI2_PAIR0+ | O | DDI |
| DDI | O | DDI3_PAIR0- | C40 | D40 | DDI2_PAIR0- | O | DDI |
| | PWR | GND | C41 | D41 | GND | PWR | |
| DDI | O | DDI3_PAIR1+ | C42 | D42 | DDI2_PAIR1+ | O | DDI |
| DDI | O | DDI3_PAIR1- | C43 | D43 | DDI2_PAIR1- | O | DDI |
| DDI | I | DDI3_HPD | C44 | D44 | DDI2_HPD | I | DDI |
| | | N.C. | C45 | D45 | N.C. | | |
| DDI | O | DDI3_PAIR2+ | C46 | D46 | DDI2_PAIR2+ | O | DDI |
| DDI | O | DDI3_PAIR2- | C47 | D47 | DDI2_PAIR2- | O | DDI |
| | | N.C. | C48 | D48 | N.C. | | |
| DDI | O | DDI3_PAIR3+ | C49 | D49 | DDI2_PAIR3+ | O | DDI |
| DDI | O | DDI3_PAIR3- | C50 | D50 | DDI2_PAIR3- | O | DDI |
| | PWR | GND | C51 | D51 | GND | PWR | |
| PEG | I | PEG_RX0+ | C52 | D52 | PEG_TX0+ | O | PEG |
| PEG | I | PEG_RX0- | C53 | D53 | PEG_TX0- | O | PEG |
| | | N.C. | C54 | D54 | PEG_LANE_RV# | I | PEG |
| PEG | I | PEG_RX1+ | C55 | D55 | PEG_TX1+ | O | PEG |
| PEG | I | PEG_RX1- | C56 | D56 | PEG_TX1- | O | PEG |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | N.C. | C57 | D57 | TYPE2# (Tied to GND) | | |
| PEG | I | PEG_RX2+ | C58 | D58 | PEG_TX2+ | O | PEG |
| | I | PEG_RX2- | C59 | D59 | PEG_TX2- | O | PEG |
| | PWR | GND | C60 | D60 | GND | PWR | |
| PEG | I | PEG_RX3+ | C61 | D61 | PEG_TX3+ | O | PEG |
| PEG | I | PEG_RX3- | C62 | D62 | PEG_TX3- | O | PEG |
| | | N.C. | C63 | D63 | N.C. | | |
| | | N.C. | C64 | D64 | N.C. | | |
| | | N.C. | C65 | D65 | N.C. | | |
| | | N.C. | C66 | D66 | N.C. | | |
| | | N.C. | C67 | D67 | GND | PWR | |
| | | N.C. | C68 | D68 | N.C. | | |
| | | N.C. | C69 | D69 | N.C. | | |
| | PWR | GND | C70 | D70 | GND | PWR | |
| | | N.C. | C71 | D71 | N.C. | | |
| | | N.C. | C72 | D72 | N.C. | | |
| | PWR | GND | C73 | D73 | GND | PWR | |
| | | N.C. | C74 | D74 | N.C. | | |
| | | N.C. | C75 | D75 | N.C. | | |
| | PWR | GND | C76 | D76 | GND | PWR | |
| | | N.C. | C77 | D77 | N.C. | | |
| | | N.C. | C78 | D78 | N.C. | | |
| | | N.C. | C79 | D79 | N.C. | | |
| | PWR | GND | C80 | D80 | GND | PWR | |
| | | N.C. | C81 | D81 | N.C. | | |
| | | N.C. | C82 | D82 | N.C. | | |
| | | N.C. | C83 | D83 | N.C. | | |
| | PWR | GND | C84 | D84 | GND | PWR | |
| | | N.C. | C85 | D85 | N.C. | | |
| | | N.C. | C86 | D86 | N.C. | | |

| | | | | | |
|---|---|---|---|---|---|
| PWR | GND | C87 | D87 | GND | PWR |
| | N.C. | C88 | D88 | N.C. | |
| | N.C. | C89 | D89 | N.C. | |
| PWR | GND | C90 | D90 | GND | PWR |
| | N.C. | C91 | D91 | N.C. | |
| | N.C. | C92 | D92 | N.C. | |
| PWR | GND | C93 | D93 | GND | PWR |
| | N.C. | C94 | D94 | N.C. | |
| | N.C. | C95 | D95 | N.C. | |
| PWR | GND | C96 | D96 | GND | PWR |
| | N.C. | C97 | D97 | N.C. | |
| | N.C. | C98 | D98 | N.C. | |
| | N.C. | C99 | D99 | N.C. | |
| PWR | GND | C100 | D100 | GND | PWR |
| | N.C. | C101 | D101 | N.C. | |
| | N.C. | C102 | D102 | N.C. | |
| PWR | GND | C103 | D103 | GND | PWR |
| PWR | +12V_RUN | C104 | D104 | +12V_RUN | PWR |
| PWR | +12V_RUN | C105 | D105 | +12V_RUN | PWR |
| PWR | +12V_RUN | C106 | D106 | +12V_RUN | PWR |
| PWR | +12V_RUN | C107 | D107 | +12V_RUN | PWR |
| PWR | +12V_RUN | C108 | D108 | +12V_RUN | PWR |
| PWR | +12V_RUN | C109 | D109 | +12V_RUN | PWR |
| PWR | GND | C110 | D110 | GND | PWR |

#### 3.2.4.1 Audio interface signals

The board supports HD audio format, thanks to native support offered by the processor to this audio codec standard.

Here following the signals related to HD Audio interface:

HDA_SYNC: HD Audio Serial Bus Synchronization. 48kHz fixed rate output from the module to the Carrier board, electrical level +3.3V_RUN.

HDA_RST#: HD Audio Codec Reset. Active low signal, output from the module to the Carrier board, electrical level +3.3V_RUN.

HDA_BITCLK: HD Audio Serial Bit Clock signal. 24MHz serial data clock generated by the Intel HD audio controller, output from the module to the Carrier board, electrical level +3.3V_RUN.

HDA_SDOUT: HD Audio Serial Data Out signal. Output from the module to the Carrier board, electrical level +3.3V_RUN.

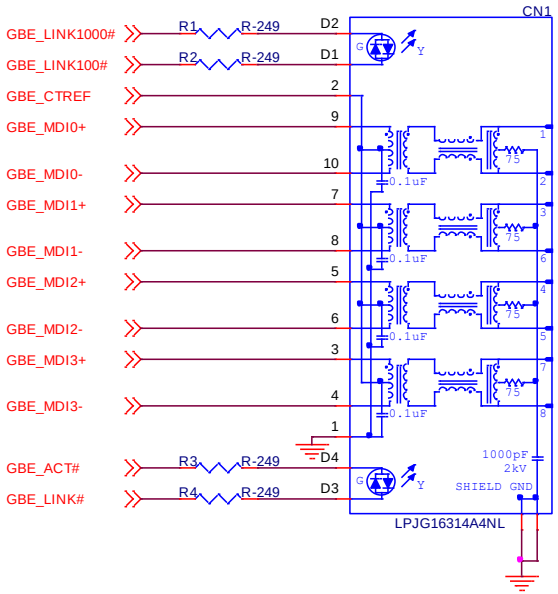
HDA_SDIN0: HD Audio Serial Data In signal. Input to the module from the Codec placed on the Carrier board, electrical level +3.3V_RUN.

HDA_SDIN1: HD Audio Serial Data In signal. Input to the module from the Codec placed on the Carrier board, electrical level +3.3V_RUN.

All these signals have to be connected, on the Carrier Board, to an HD Audio Codec. Please refer to the chosen Codec's Reference Design Guide for correct implementation of audio section on the carrier board.

### 3.2.4.2 Gigabit Ethernet signals

The Gigabit Ethernet interface is realised, on the board, using an Intel® I210 Gigabit Ethernet controller, which is interfaced to the SOC through a dedicated PCI-express root port.




Here following the signals involved in PCI express management

GBE0_MDI0+/GBE0_MDI0-: Media Dependent Interface (MDI) I/O differential pair #0

GBE0_MDI1+/GBE0_MDI1-: Media Dependent Interface (MDI) I/O differential pair #1

GBE0_MDI2+/GBE0_MDI2-: Media Dependent Interface (MDI) I/O differential pair #2, only used for 1Gbps Ethernet mode (not for 10/100Mbps modes)

GBE0_MDI3+/GBE0_MDI3-: Media Dependent Interface (MDI) I/O differential pair #3, only used for 1Gbps Ethernet mode (not for 10/100Mbps modes)

GBE0_ACT#: Ethernet controller activity indicator, Active Low Output signal, electrical level +3.3V_ALW.

GBE0_LINK#: Ethernet controller link indicator, Active Low Output signal, electrical level +3.3V_ALW.

GBE0_LINK100#: Ethernet controller 100Mbps link indicator, Active Low Output signal, electrical level +3.3V_ALW.

GBE0_LINK1000#: Ethernet controller 1Gbps link indicator, Active Low Output signal, electrical level +3.3V_ALW.

GBE0_SDP: Intel® I225 Software Definable Pin can be used for IEEE 1588 auxiliary device connection.

These signals can be connected, on the Carrier board, directly to an RJ-45 connector, in order to complete the Ethernet interface.

Please notice that if just a FastEthernet (i.e. 10/100 Mbps) is needed, then only MDI0 and MDI1 differential lanes are necessary.

Unused differential pairs and signals can be left unconnected. Please look to the schematic given as an example of implementation of Gigabit Ethernet connector. In this example, it is also present GBE_CTREF signal connected on pin #2 of the RJ-45 connector. Intel® I225 Gigabit Ethernet controller, however, doesn't need the analog powered centre tap, therefore the signal GBE_CTREF is not available on COM Express® connector AB.

### 3.2.4.3 S-ATA signals

The Intel® family of SOCs formerly coded as Tiger Lake-UP3 offers two S-ATA interfaces, which are carried out on the golden finger connector.

The interfaces are Gen3 compliant, with support of 1.5Gbps, 3.0 Gbps and 6.0 Gbps data rates.

Here following the signals related to SATA interface:

SATA0_TX+/SATA0_TX-: Serial ATA Channel #0 Transmit differential pair.

SATA0_RX+/SATA0_RX-: Serial ATA Channel #0 Receive differential pair.

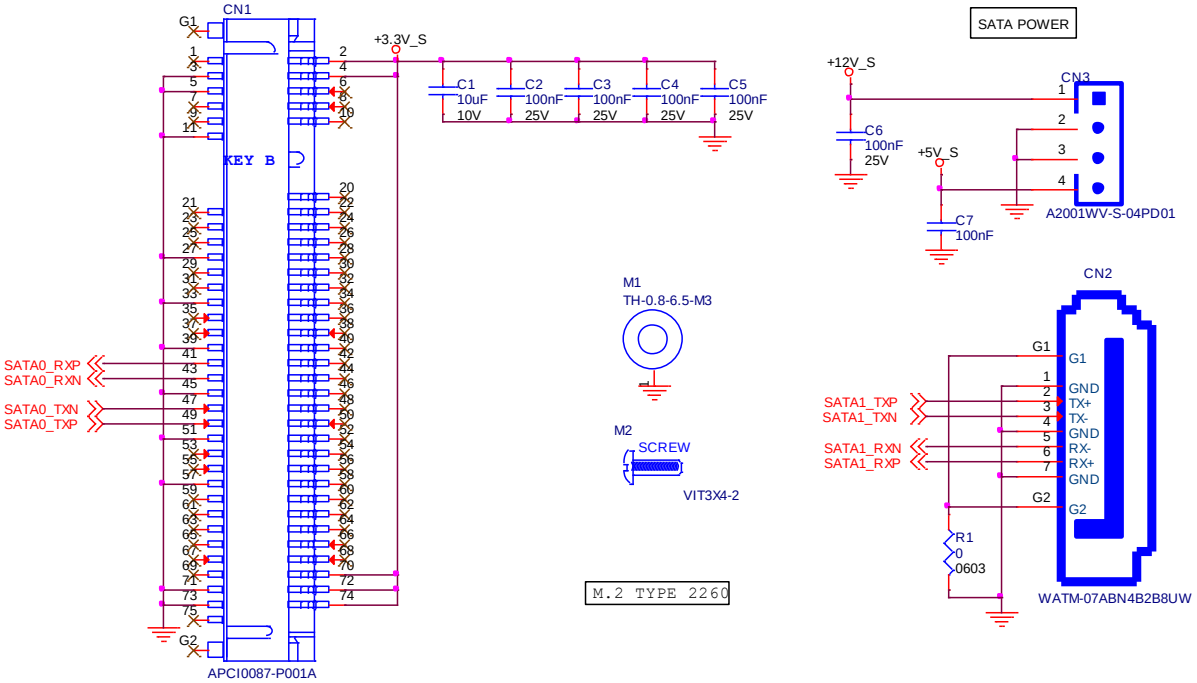
SATA1_TX+/SATA1_TX-: Serial ATA Channel #1 Transmit differential pair.

SATA1_RX+/SATA1_RX-: Serial ATA Channel #1 Receive differential pair.

SATA_ACT#: Serial ATA Activity Led. Active low output signal at +3.3V_RUN voltage.

10nF AC series decoupling capacitors are placed on each line of SATA differential pairs.

On the carrier board, these signals can be carried out directly to the SATA connectors, like in the following example schematics.



#### 3.2.4.4 PCI Express interface signals

The board can offer externally up to 8 PCI Express lane, which are managed by the Intel® family of SOCs formerly coded as Tiger Lake-UP3.

PCI express Gen 3.0 is supported.

Please be aware that groupings cannot be changed dynamically, it is a fixed feature of the BIOS.

When ordering this product, please take care of specifying which are the desired PCI-e groupings.

Here following the signals involved in PCI express management:

PCIE_TXx+/PCIE_TXx-: PCI Express lane #x, Transmitting Output Differential pair

PCIE_RXx+/PCIE_RXx-: PCI Express lane #x, Receiving Input Differential pair

PCIE_CLK_REF+/ PCIE_CLK_REF-: PCI Express 100MHz Reference Clock, Differential Pair. Please consider that only one reference clock is supplied, while there are five different PCI express lanes. When more than one PCI Express lane is used on the carrier board, then a zero-delay buffer must be used to replicate the reference clock to all the devices.

#### 3.2.4.5 PEG interface signals

In addition to the eight PCI express lanes, described in the previous paragraph, the board can offer a PCI-Express graphics (PEG) interface, which can be used for connection of external graphics cards with up to x4 lanes interface. Such an interface is directly managed by the SoC's embedded PCH.

Here following the signals involved in PEG management.

PEG_TXx+/PEG_TXx-: PCI Express Graphics lane #x, Transmitting Output Differential pairs.

PEG_RXx+/PEG_RXx-: PCI Express Graphics lane #x, Receiving Output Differential pairs.

PEG_LANE_RV#: PCI Express Graphics lane reversal input strap, electrical level +3.3V_RUN with a 10kΩ pull-up resistor. This signal must be driven low, on the carrier board, only in case it is necessary to reverse the lane order of PEG interface. It must be left unconnected if lane reversal is not necessary.

#### 3.2.4.6 USB interface signals

The Intel® family of SOCs formerly coded as Tiger Lake-UP3 offers an xHCI controller, which is able to manage up to 4 Superspeed ports (i.e. USB 3.0 compliant), one of them also capable of OTG, plus up to 8 Ports able to work in USB 2.0 mode only. Via BIOS settings it is possible to enable or disable the xHCI controller, therefore enabling USB 3.0 functionalities or leaving only USB 1.1 and USB 2.0 support.

All USB 2.0 ports are able to work in High Speed (HS), Full Speed (FS) and Low Speed (LS).

Here following the signals related to USB interfaces.

USB_x+/USB_x-: Universal Serial Bus Port #x bidirectional differential pair

USB_SSRXx+/USB_SSRXx-: USB Super Speed Port #x receive differential pair

USB_SSTXx+/USB_SSTXx-: USB Super Speed Port #x transmit differential pair

USB_0_1_OC#: USB Over Current Detect Input. Active Low Input signal, electrical level +3.3V_ALW with 10kΩ pull-up resistor. This pin has to be used for overcurrent detection of USB Port#0 and #1

USB_2_3_OC#: USB Over Current Detect Input. Active Low Input signa.l, electrical level +3.3V_ALW with 10kΩ pull-up resistor. This pin has to be used for overcurrent detection of USB Ports #2 and #3

USB_4_5_OC#: USB Over Current Detect Input. Active Low Input signal, electrical level +3.3V_ALW with 10kΩ pull-up resistor. This pin has to be used for overcurrent detection of USB Port #4 and/or #5

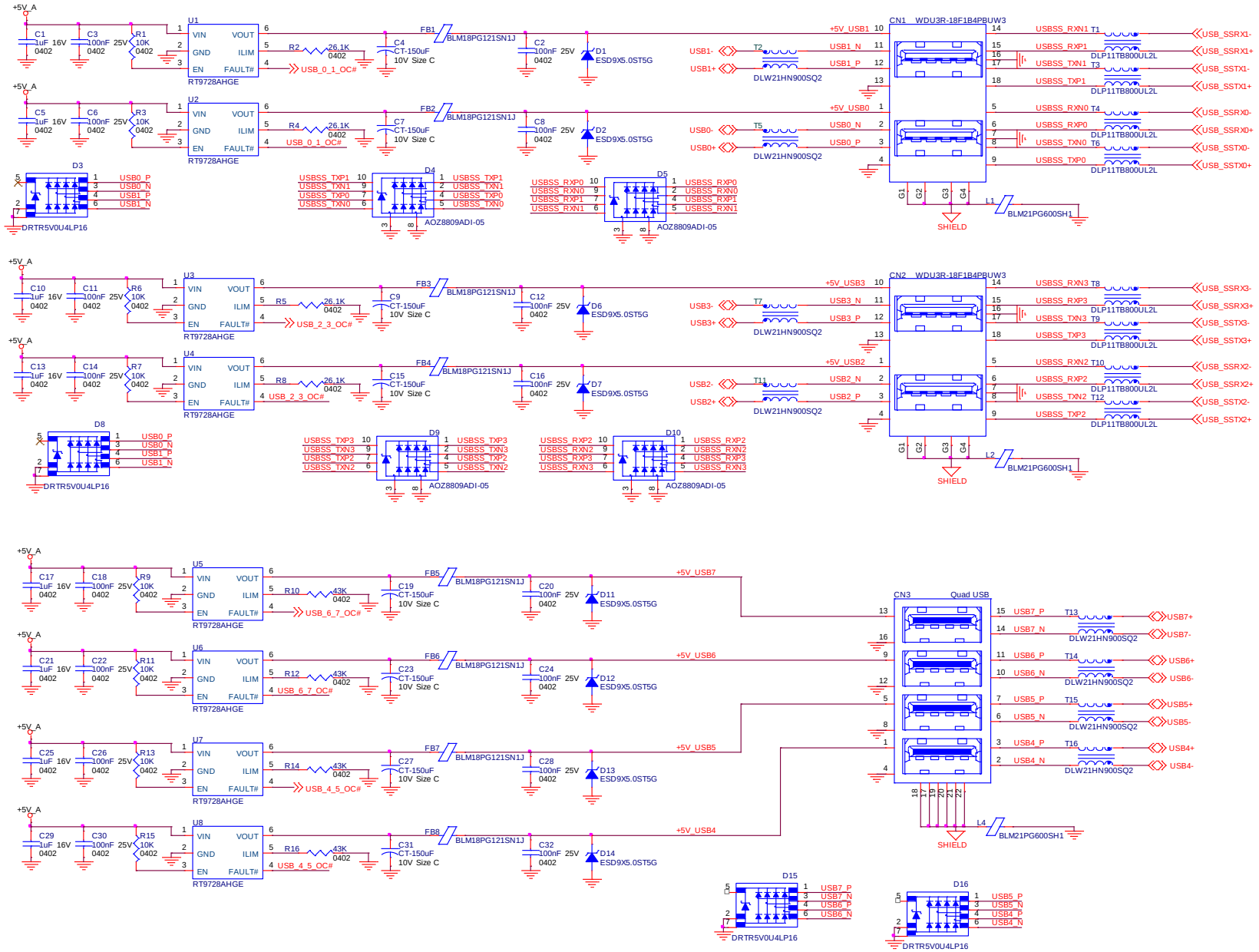
USB_6_7_OC#: USB Over Current Detect Input. Active Low Input signal, electrical level +3.3V_ALW with 10kΩ pull-up resistor. This pin has to be used for overcurrent detection of USB Port #6 and/or #7

100nF AC series decoupling capacitors are placed on each transmitting line of USB Super speed differential pairs.

Please notice that for correct management of Overcurrent signals, power distribution switches are needed on the carrier board.

For EMI/ESD protection, common mode chokes on USB data lines, and clamping diodes on USB data and voltage lines, are also needed.

The schematics in the following page show an example of implementation on the Carrier Board. In there, USB ports #4, #5, #6 and #7 are carried out to standard USB 2.0 Type A receptacles, while USB 2.0 port #0, #1, #2 and #3 along with the corresponding Superspeed USB ports, are carried to standard USB 3.0 Type A receptacles. Always remember that, for correct implementation of USB 3.0 connections, any Superspeed port must be paired with corresponding number of USB 2.0 port (i.e. USB 2.0 port#0 must be paired with USB 3.0 port #0 and so on).


+5V_A
U1
RT9728AHGE
U2
RT9728AHGE
U3
RT9728AHGE
U4
RT9728AHGE
U5
RT9728AHGE
U6
RT9728AHGE
U7
RT9728AHGE
U8
RT9728AHGE
VIN
VOUT
GND
ILIM
EN
FAULT#
USB_0_1_OC#
USB_2_3_OC#
USB_6_7_OC#
USB_4_5_OC#
FB1
FB2
FB3
FB4
FB5
FB6
FB7
FB8
BLM18PG121SN1J
CT-150uF
10V Size C
ESD9X5.0ST5G
DLW21HN900SQ2
DLP11TB800UL2L
DRTR5V0U4LP16
AOZ8809ADI-05
CN1 WDU3R-18F1B4PBUW3
CN2 WDU3R-18F1B4PBUW3
CN3 Quad USB
SHIELD
BLM21PG600SH1
USB0_P
USB0_N
USB1_P
USB1_N
USB_SSRX1-
USB_SSRX1+
USB_SSTX1-
USB_SSTX1+
USB_SSRX0-
USB_SSRX0+
USB_SSTX0-
USB_SSTX0+
USB_SSRX3-
USB_SSRX3+
USB_SSTX3-
USB_SSTX3+
USB_SSRX2-
USB_SSRX2+
USB_SSTX2-
USB_SSTX2+
USB7+
USB7-
USB6+
USB6-
USB5+
USB5-
USB4+
USB4-

### 3.2.4.7 LVDS Flat Panel signals

The Intel® family of SOCs formerly coded as Tiger Lake-UP3 offers offers three Digital Display Interfaces, of which the first is able to support natively embedded Display Port (eDP). Conversely, the LVDS interface, which is frequently used in many application fields, is not directly supported by these CPUs.

For this reason, considering that LVDS interface can be multiplexed on the same pin with the eDP interface, on the board it can be implemented an eDP to LVDS bridge (NXP PTN3460), which allow the implementation of a Dual Channel LVDS, with a maximum supported resolution of 1920x1200 @ 60Hz (dual channel mode).

> **!** Please remember that LVDS interface is not native for the Intel® family of SOCs formerly coded as Apollo Lake, it is derived from an optional eDP-to-LVDS bridge. Depending on the factory option purchased, on the same pins it is possible to have available LVDS first channel or eDP interface.
>
> Please take care of specifying if LVDS interface or eDP is needed, before placing an order of COMe-C24-CT6 module.

Here following the signals related to LVDS management:

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_CK+/LVDS_A_CK-: 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_CK+/LVDS_B_CK-: LVDS Channel #B differential Clock

LVDS_VDD_EN: +3.3V_RUN electrical level Output, Panel Power Enable signal. It can be used to turn On/Off the connected LVDS display.

LVDS_BKLT_EN: +3.3V_RUN electrical level Output, Panel Backlight Enable signal. It can be used to turn On/Off the backlight's lamps of connected LVDS display.

LVDS_BKLT_CTRL: this signal can be used to adjust the panel backlight brightness in displays supporting Pulse Width Modulated (PWM) regulations.

LVDS_I2C_DAT: DisplayID DDC Data line for LVDS flat Panel detection. Bidirectional signal, electrical level +3.3V_RUN.

LVDS_I2C_CK: DisplayID DDC Clock line for LVDS flat Panel detection. Bidirectional signal, electrical level +3.3V_RUN.

Please be aware that External EDID through LVDS_I2C-xxx signals is actually not supported by this board

### 3.2.4.8 Embedded Display Port (eDP) signals

As described in the previous paragraph, the Intel® family of SOCs formerly coded as Tiger Lake-UP3 offers a native 4-lanes embedded Display Port (eDP) interface.

As a factory option, the module can be configured with this eDP interface available on COM Express connector AB, which allows supporting displays with a resolution up 5120x3200 @ 60Hz.

Here following the signals related to eDP management:

eDP_TX0+/eDP_TX0-: eDP channel differential data pair #0.

eDP_TX1+/eDP_TX1-: eDP channel differential data pair #1.

eDP_TX2+/eDP_TX2-: eDP channel differential data pair #2.

eDP_TX3+/eDP_TX3-: eDP channel differential data pair #3.

eDP_AUX+/eDP_AUX-: eDP channel differential auxiliary channel.

eDP_HPD: eDP channel Hot Plug Detect. Active High Signal, +3.3V_RUN electrical level input with 100kΩ pull-down resistor.

eDP_VDD_EN: +3.3V_RUN electrical level output, Panel Power Enable signal. It can be used to turn On/Off the connected display.

eDP_BKLT_EN: +3.3V_RUN electrical level output, Panel Backlight Enable signal. It can be used to turn On/Off the backlight's lamps of connected display.

eDP_BKLT_CTRL: this signal can be used to adjust the panel backlight brightness in displays supporting Pulse Width Modulated (PWM) regulations.

### 3.2.4.9 Analog VGA interface

The Intel® family of SOCs formerly coded as Tiger Lake-UP3 doesn't offer any analog display interface, which could be used for the connection of older VGA/CRT displays.

As a factory option, however, it is possible to purchase this board equipped with an eDP to VGA bridge (NXP PTN3356BS), which allow the implementation of a VGA interface with a maximum supported resolution of 2048x1536 @ 50Hz (reduced blanking). Modules equipped with the eDP-to-VGA bridge can also mount the eDP-to-LVDS bridge, since the two bridges use different eDP lanes.

> **!** Please remember that the VGA interface is not native for the Intel® Apollo Lake family of CPUs, it is derived from an optional eDP-to-VGA bridge.
>
> Please take care of specifying if VGA interface is needed, before placing an order of this product.

Signals dedicated to VGA interface are the following:

VGA_RED: Red Signal video output. A 150Ω pull-down resistor is placed on the line.

VGA_GRN: Green Signal video output. A 150Ω pull-down resistor is placed on the line.

VGA_BLU: Blue Signal video output. A 150Ω pull-down resistor is placed on the line.

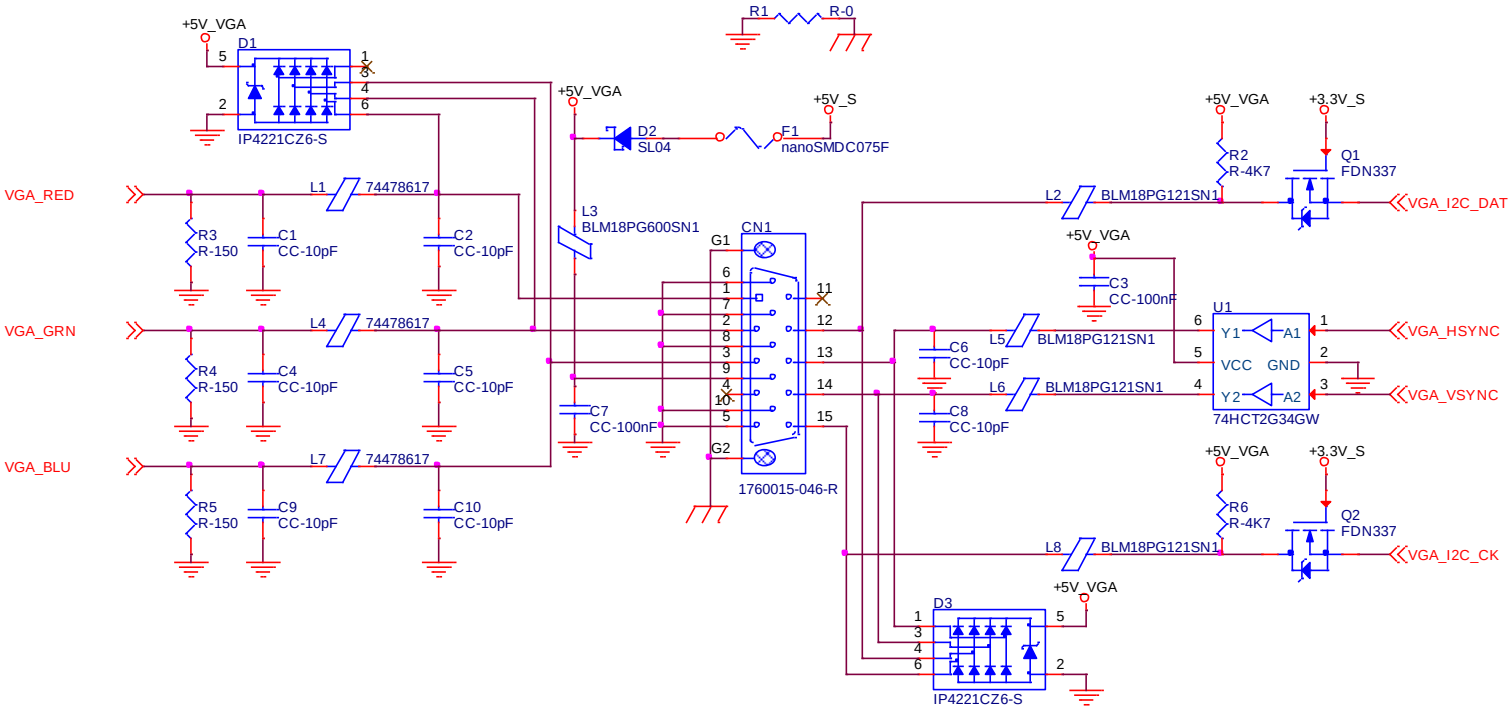
VGA_HSYNC: Horizontal Synchronization output signal.

VGA_VSYNC: Vertical Synchronization output signal.

VGA_I2C_CK: DDC Clock line for VGA displays detection. Output signal, electrical level +3.3V_RUN with 2K2Ω pull-up resistor.

VGA_I2C_DAT: DDC Clock line for VGA displays detection. Bidirectional signal, electrical level +3.3V_RUN with 2K2Ω pull-up resistor.

Please be aware that for the connection to external VGA displays, on the carrier board it is necessary to provide for filters and ESD protection like in the following example schematics.



### 3.2.4.10 Digital Display interfaces

This board with Xe Graphics Core Gen12 architecture, embedded inside the Intel® Tiger Lake-UP3 family of CPUs, offers three Digital Display Interfaces, which can be used for the implementation, on the carrier board, of HDMI/DVI or Multimode Display Port interfaces.

Switching between HDMI/DVI (or, more correctly, TMDS) and Display Port is dynamic, i.e. the interfaces coming out from COM Express® module can be used to implement a multimode Display Port interface (and in this way only AC coupling capacitors are needed on the carrier board) or a HDMI/DVI interface (an in this case TMDS level shifters are needed).

This is reached by multiplexing DP/HDMI interfaces on the same pins.

Depending by the interface chosen, therefore, on COM Express connector CD there will be available the following signals:

| Digital Display Interfaces - Pin multiplexing | | | | | |
|---|---|---|---|---|---|
| | | Multimode Display Port mode | | TMDS (HDMI/DVI) mode | |
| Pin nr. | Pin name | Signal | Description | Signal | Description |
| D26 | DDI1_PAIR0+ | DP1_LANE0+ | DP1 Differential pair #0 non-inverting line | TMDS1_DATA2+ | TMDS1 Differential pair #2 non-inverting line |
| D27 | DDI1_PAIR0- | DP1_LANE0- | DP1 Differential pair #0 inverting line | TMDS1_DATA2- | TMDS1 Differential pair #2 inverting line |
| D29 | DDI1_PAIR1+ | DP1_LANE1+ | DP1 Differential pair #1 non-inverting line | TMDS1_DATA1+ | TMDS1 Differential pair #1 non-inverting line |
| D30 | DDI1_PAIR1- | DP1_LANE1- | DP1 Differential pair #1 inverting line | TMDS1_DATA1- | TMDS1 Differential pair #1 inverting line |
| D32 | DDI1_PAIR2+ | DP1_LANE2+ | DP1 Differential pair #2 non-inverting line | TMDS1_DATA0+ | TMDS1 Differential pair #0 non-inverting line |
| D33 | DDI1_PAIR2- | DP1_LANE2- | DP1 Differential pair #2 inverting line | TMDS1_DATA0- | TMDS1 Differential pair #0 inverting line |
| D36 | DDI1_PAIR3+ | DP1_LANE3+ | DP1 Differential pair #3 non-inverting line | TMDS1_CLK+ | TMDS1 Differential clock non-inverting line |
| D37 | DDI1_PAIR3- | DP1_LANE3- | DP1 Differential pair #3 inverting line | TMDS1_CLK- | TMDS1 Differential clock inverting line |
| C24 | DDI1_HPD | DP1_HPD | DP1 Hot Plug Detect signal | HDMI1_HPD | HDMI #1 Hot Plug Detect signal |
| D15 | DDI1_CTRLCLK_AUX+ | DP1_AUX+ | DP1 Auxiliary channel non-inverting line | HDMI1_CTRLCLK | DDC Clock line for HDMI panel #1. |
| D16 | DDI1_CTRLDATA_AUX- | DP1_AUX- | DP1 Auxiliary channel inverting line | HDMI1_CTRLDATA | DDC Data line for HDMI panel #1. |
| D34 | DDI1_DDC_AUX_SEL | DDI#1 DP or TMDS interface selector: pull this signal low or leave it floating for DP++ interface, pull high (+3.3V_RUN) for TMDS interface | | | |
| D39 | DDI2_PAIR0+ | DP2_LANE0+ | DP2 Differential pair #0 non-inverting line | TMDS2_DATA2+ | TMDS2 Differential pair #2 non-inverting line |
| D40 | DDI2_PAIR0- | DP2_LANE0- | DP2 Differential pair #0 inverting line | TMDS2_DATA2- | TMDS2 Differential pair #2 inverting line |
| D42 | DDI2_PAIR1+ | DP2_LANE1+ | DP2 Differential pair #1 non-inverting line | TMDS2_DATA1+ | TMDS2 Differential pair #1 non-inverting line |
| D43 | DDI2_PAIR1- | DP2_LANE1- | DP2 Differential pair #1 inverting line | TMDS2_DATA1- | TMDS2 Differential pair #1 inverting line |
| D46 | DDI2_PAIR2+ | DP2_LANE2+ | DP2 Differential pair #2 non-inverting line | TMDS2_DATA0+ | TMDS2 Differential pair #0 non-inverting line |

| | | | | | |
|---|---|---|---|---|---|
| D47 | DDI2_PAIR2- | DP2_LANE2- | DP2 Differential pair #2 inverting line | TMDS2_DATA0- | TMDS2 Differential pair #0 inverting line |
| D49 | DDI2_PAIR3+ | DP2_LANE3+ | DP2 Differential pair #3 non-inverting line | TMDS2_CLK+ | TMDS2 Differential clock non-inverting line |
| D50 | DDI2_PAIR3- | DP2_LANE3- | DP2 Differential pair #3 inverting line | TMDS2_CLK- | TMDS2 Differential clock inverting line |
| D44 | DDI2_HPD | DP2_HPD | DP2 Hot Plug Detect signal | HDMI2_HPD | HDMI #2 Hot Plug Detect signal |
| C32 | DDI2_CTRLCLK_AUX+ | DP2_AUX+ | DP2 Auxiliary channel non-inverting line | HDMI2_CTRLCLK | DDC Clock line for HDMI panel #2. |
| C33 | DDI2_CTRLDATA_AUX- | DP2_AUX- | DP2 Auxiliary channel inverting line | HDMI2_CTRLDATA | DDC Data line for HDMI panel #2. |
| C34 | DDI2_DDC_AUX_SEL | DDI#2 DP or TMDS interface selector: pull this signal low or leave floating for DP++ interface, pull high (+3.3V_RUN) for TMDS interface | | | |
| C39 | DDI3_PAIR0+ | DP3_LANE0+ | DP3 Differential pair #0 non-inverting line | TMDS3_DATA2+ | TMDS3 Differential pair #2 non-inverting line |
| C40 | DDI3_PAIR0- | DP3_LANE0- | DP3 Differential pair #0 inverting line | TMDS3_DATA2- | TMDS3 Differential pair #2 inverting line |
| C42 | DDI3_PAIR1+ | DP3_LANE1+ | DP3 Differential pair #1 non-inverting line | TMDS3_DATA1+ | TMDS3 Differential pair #1 non-inverting line |
| C43 | DDI3_PAIR1- | DP3_LANE1- | DP3 Differential pair #1 inverting line | TMDS3_DATA1- | TMDS3 Differential pair #1 inverting line |
| C46 | DDI3_PAIR2+ | DP3_LANE2+ | DP3 Differential pair #2 non-inverting line | TMDS3_DATA0+ | TMDS3 Differential pair #0 non-inverting line |
| C47 | DDI3_PAIR2- | DP3_LANE2- | DP3 Differential pair #2 inverting line | TMDS3_DATA0- | TMDS3 Differential pair #0 inverting line |
| C49 | DDI3_PAIR3+ | DP3_LANE3+ | DP3 Differential pair #3 non-inverting line | TMDS3_CLK+ | TMDS3 Differential clock non-inverting line |
| C50 | DDI3_PAIR3- | DP3_LANE3- | DP3 Differential pair #3 inverting line | TMDS3_CLK- | TMDS3 Differential clock inverting line |
| C44 | DDI3_HPD | DP3_HPD | DP3 Hot Plug Detect signal | HDMI3_HPD | HDMI #3 Hot Plug Detect signal |
| C36 | DDI3_CTRLCLK_AUX+ | DP3_AUX+ | DP3 Auxiliary channel non-inverting line | HDMI3_CTRLCLK | DDC Clock line for HDMI panel #3. |
| C37 | DDI3_CTRLDATA_AUX- | DP3_AUX- | DP3 Auxiliary channel inverting line | HDMI3_CTRLDATA | DDC Data line for HDMI panel #3. |
| C38 | DDI3_DDC_AUX_SEL | DDI#3 DP or TMDS interface selector: pull this signal low or leave it floating for DP++ interface, pull high (+3.3V_RUN) for TMDS interface | | | |

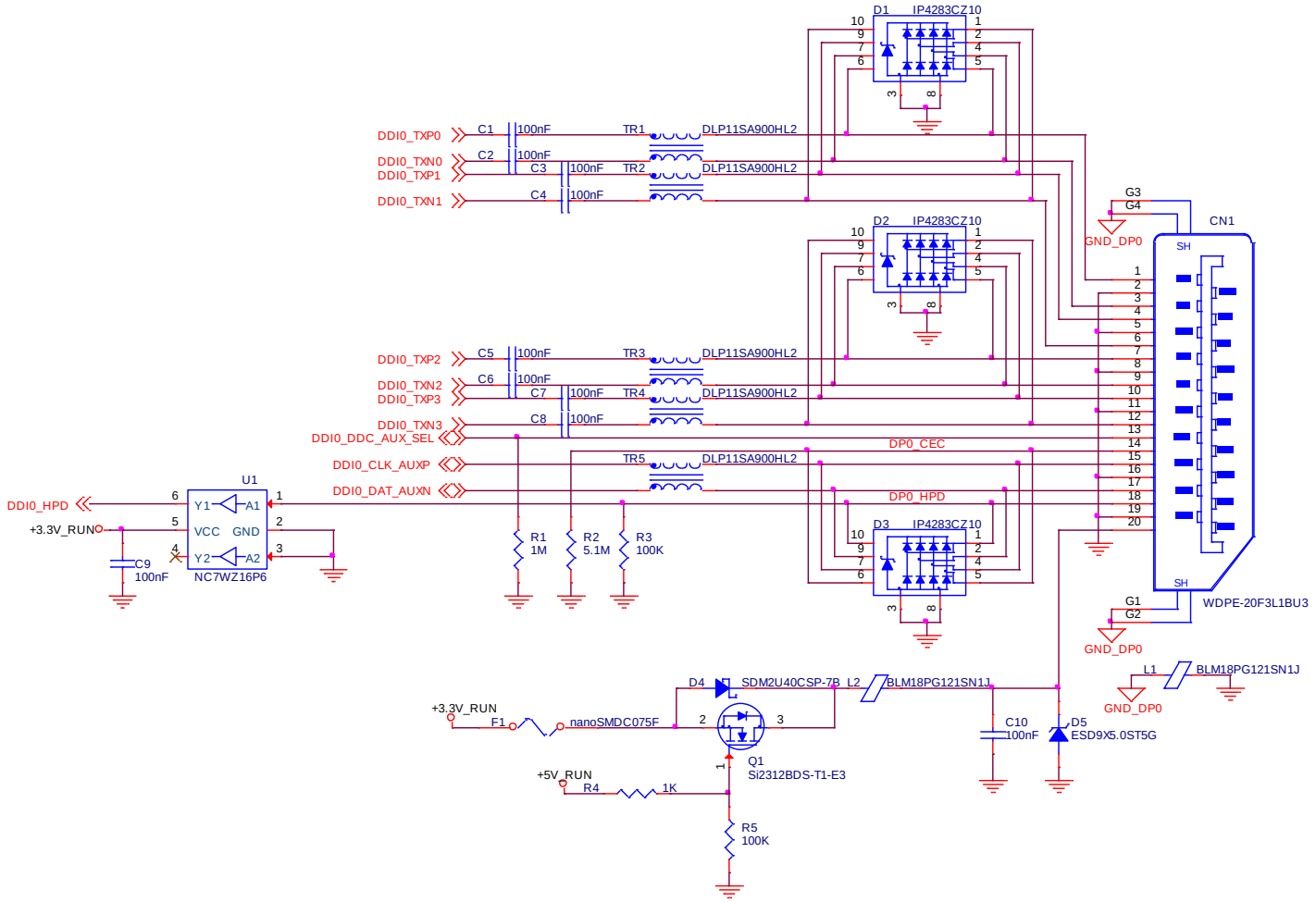
All Hot Plug Detect Input signals (valid both for DP++ and TMDS interface) are +3.3V_RUN electrical level signal, active high with 100KΩ pull-down resistors.

All HDMI Control /DP AUX signals (DDIx_CTRLCK_AUX+ and DDIx_CTRLDATA_AUX-) are bidirectional signal, electrical level +3.3V_RUN with a 100kΩ pull-up (on Data) / pull-down (on clock) resistor

Please be aware that for correct implementation of HDMI/DVI interfaces, it is necessary to implement, on the Carrier board, voltage level shifter for TMDS differential pairs, for Control data/Clock signals and for Hot Plug Detect signal.

Voltage clamping diodes are also highly recommended on all signal lines for ESD suppression.

Here following an example of implementation of multimode Display Port on the carrier board. In this example, are used signals related to Digital Display interface #1, but any DDI interface can be used.



### 3.2.4.11 LPC interface signals

According to COM Express® specifications rel. 3.0, on the on COM Express connector AB there are 8 pins that can be used for implementation of Low Pin Count (LPC) Bus or enhanced SPI (eSPI) interfaces, which are two multiplexed interfaces made available by the PCH. However, since LPC bus is needed for the management of the Embedded microcontroller, then this board makes available only the LPC interface.

The following signals are available:

LPC_AD[0÷3]: LPC address, command and data bus, bidirectional signal, +3.3V_RUN electrical level 47kΩ pull-up resistors.

LPC_CLK: LPC Clock Output line, +3.3V_RUN electrical level. Since only a clock line is available, if more LPC devices are available on the carrier board, then it is necessary to provide for a zero-delay clock buffer to connect all clock lines to the single clock output of COM Express module.

LPC_FRAME#: LPC Frame indicator, active low output line, +3.3V_RUN electrical level. This signal is used to signal the start of a new cycle of transmission, or the termination of existing cycles due to abort or time-out condition.

LPC_SERIRQ: LPC Serialised IRQ request, bidirectional line, +3.3V_RUN electrical level with 47kΩ pull-up resistor. This signal is used only by peripherals requiring Interrupt support.

LPC_DRQ[0÷1]#: LPC Serial DMA Request, +3.3V_RUN electrical level. These signals only have a 100kΩ pull-up resistor on module, internally they are not used by the chipset nor by the Embedded Controller.

ESPI_EN#: this input signal should be used by the carrier board to request eSPI interface configuration, which is, however, not supported by the module. Therefore, driving low this signal would have no effect. Electrical level +3.3V_RUN with 100kΩ pull-up resistor.

### 3.2.4.12 SPI interface signals

The Intel® Tiger Lake-UP3 family of processors offer also one dedicated controller for Serial Peripheral Interface (SPI), which can be used for connection of Serial Flash devices. Please be aware that this interface can be used exclusively to support platform firmware (BIOS).

Signals involved with SPI management are the following:

SPI_CS#: SPI Chip select, active low output signal, +1.8V_ALW electrical level with 10kΩ pull-up resistor.

SPI_MISO: SPI Master In Slave Out, Input to COM Express® module from SPI devices embedded on the Carrier Board. Electrical level +1.8V_ALW.

SPI_MOSI: SPI Master Out Slave In, Output from COM Express® module to SPI devices embedded on the Carrier Board. Electrical level +1.8V_ALW

SPI_CLK: SPI Clock Output to carrier board's SPI embedded devices. Electrical level +1.8V_ALW. Supported clock frequencies are 20, 33 and 50 MHz.

SPI_POWER: +1.8V_ALW Power Supply Output for carrier board's SPI devices.

BIOS_DIS[0÷1]#: BIOS Disable strap signals. These two signals are inputs of the COM Express® Module, that on the carrier board can be left floating or pulled down in order to select which SPI Flash device has to be used for module's boot. Please refer to table 4.13 of COM Express® Module Base Specifications rel. 3.0 for the

meaning of possible configurations of these two signals.

#### 3.2.4.13 UART interface signals

According to COM Express® Rel. 3.0 specifications, since this board is a Type 6 module, it can offer two UART interfaces, which are managed by the embedded controller or directly from Intel® Tiger Lake-UP3 family of CPUs.

Here following the signals related to UART interface:

SER0_TX: UART Interface #0, Serial data Transmit (output) line, 3.3V_RUN electrical level.

SER0_RX: UART Interface #0, Serial data Receive (input) line, 3.3V_RUN electrical level.

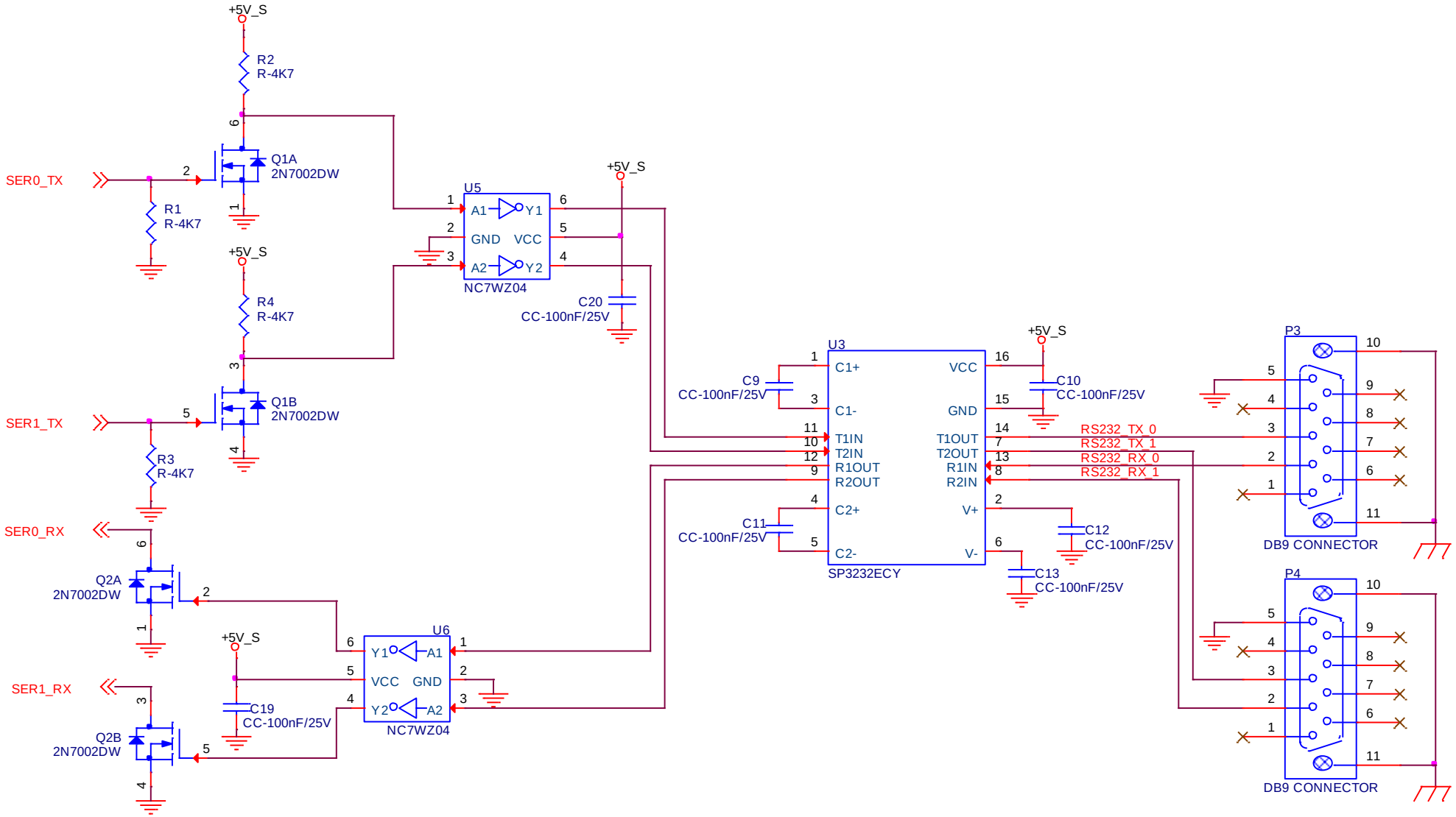
SER1_TX: UART Interface #1, Serial data Transmit (output) line, 3.3V_RUN electrical level.

SER1_RX: UART Interface #1, Serial data Receive (input) line, 3.3V_RUN electrical level.

In COM Express® specifications prior to Rel. 2.0, the pins dedicated to these two UART interfaces were dedicated to +12$V_{IN}$ power rail. In order to prevent damages to the module, in case it is inserted in carrier board not designed for Type 6, then Schottky-diodes have been added on UART interfaces' TX and RX lines so that they are +12V Tolerant.

Please consider that interface is at TTL electrical level; therefore, please evaluate well the typical scenario of application. If it is not explicitly necessary to interface directly at TTL level, for connection to standard serial ports commonly available (like those offered by common PCs, for example) it is mandatory to include an RS-232 transceiver on the carrier board.

The schematic on the next page shows an example of implementation of RS-232 transceiver for the Carrier board.


+5V_S
R2
R-4K7
Q1A
2N7002DW
SER0_TX
R1
R-4K7
U5
A1
Y1
GND
VCC
A2
Y2
NC7WZ04
C20
CC-100nF/25V
R4
R-4K7
Q1B
2N7002DW
SER1_TX
R3
R-4K7
SER0_RX
Q2A
2N7002DW
U6
NC7WZ04
C19
CC-100nF/25V
SER1_RX
Q2B
2N7002DW
U3
C1+
C1-
T1IN
T2IN
R1OUT
R2OUT
C2+
C2-
VCC
GND
T1OUT
T2OUT
R1IN
R2IN
V+
V-
SP3232ECY
C9
CC-100nF/25V
C10
CC-100nF/25V
C11
CC-100nF/25V
C12
CC-100nF/25V
C13
CC-100nF/25V
RS232_TX_0
RS232_TX_1
RS232_RX_0
RS232_RX_1
P3
P4
DB9 CONNECTOR
DB9 CONNECTOR

### 3.2.4.14 I2C interface signals

This interface is managed by the embedded microcontroller.

Signals involved are the following:

I2C_CK: general purpose I2C Bus clock line. Output signal, electrical level +3.3V_ALW with a 2K2Ω pull-up resistor.

I2C_DAT: general purpose I2C Bus data line. Bidirectional signal, electrical level +3.3V_ALW with a 2K2Ω pull-up resistor.

### 3.2.4.15 Miscellaneous signals

Here following, a list of COM Express® compliant signals that complete the features of this board.

SPKR: Speaker output, +3.3V_RUN voltage signal.

WDT: Watchdog event indicator Output. It is an active high signal, +3.3V_ALW voltage. When this signal goes high (active), it reports out to the devices on the Carrier board that internal Watchdog's timer expired without being triggered, neither via HW nor via SW. This signal is managed by the module's embedded microcontroller.

FAN_PWMOUT*: PWM output for FAN speed management, +3.3V_RUN voltage signal. It is managed by the module's embedded microcontroller.

FAN_TACHIN*: External FAN Tachometer Input. +3.3V_RUN voltage signal, directly managed by the module's embedded microcontroller.

TPM_PP: Trusted Platform Module (TPM) Physical Presence Input, +3.3V_ALW voltage signal with 100kΩ pull-down resistor, managed by the optional TPM device on-module.

THRM#: Thermal Alarm Input. Active Low +3.3V_RUN voltage signal with 10kΩ pull-up resistor, directly managed by the module's embedded microcontroller. This input gives the possibility, to carrier board's hardware, to indicate to the main module an overheating situation, so that the CPU can begin thermal throttling.

THRMTRIP#: Active Low +3.3V_ALW voltage output signal. This signal is used to communicate to the carrier board's devices that, due to excessive overheating, the CPU began the shutdown in order to prevent physical damages.

* Note: In COM Express® specifications prior to Rel. 2.0, the pins dedicated to FAN management were dedicated to $+12V_{IN}$ power rail. In order to prevent damages to the module, in case it is inserted in carrier board not designed for Type 6, then protection circuitry has been added on FAN_PWM_OUT and FAN_TACHOIN lines so that they are +12V Tolerant.

### 3.2.4.16 Power Management signals

According to COM Express® specifications, on the connector AB there is a set of signals that are used to manage the power rails and power states.

The signals involved are:

PWRBTN#: Power Button Input, active low, +3.3V_ALW buffered voltage signal with 47kΩ pull-up resistor. When working in ATX mode, this signal can be connected

to a momentary push-button: a pulse to GND of this signal will switch power supply On or Off.

SYS_RESET#: Reset Button Input, active low, +3.3V_ALW buffered voltage signal with 47kΩ pull-up resistor. This signal can be connected to a momentary push-button: a pulse to GND of this signal will reset the board.

CB_RESET#: System Reset Output, active low, +3.3V_ALW voltage buffered signal. It can be used directly to drive externally a single RESET Signal. In case it is necessary to supply Reset signal to multiple devices, a buffer on the carrier board is recommended.

PWR_OK: Power Good Input, +3.3V_RUN active high signal. It must be driven by the carrier board to signal that power supply section is ready and stable. When this signal is asserted, the module will begin the boot phase. The signal must be kept asserted for all the time that the module is working.

SUS_STAT#: Suspend status output, active low +3.3V_ALW electrical voltage signal with 10k pull-up resistor. This output can be used to report to the devices on the carrier board that the module is going to enter in one of possible ACPI low-power states.

SUS_S3#: S3 status output, active low +3.3V_ALW electrical voltage signal. This signal must be used, on the carrier board, to shut off the power supply to all the devices that must become inactive during S3 (Suspend to RAM) power state.

SUS_S5#: S5 status output, active low +3.3V_ALW electrical voltage signal. This signal is used, on the carrier board, to shut off the power supply to all the devices that must become inactive only during S5 (Soft Off) power state. SUS_S4# is connected internally to this signal.

WAKE0#: PCI Express Wake Input, active low +3.3V_ALW electrical voltage signal with 10kΩ pull-up resistor. This signal can be driven low, on the carrier board, to report that a Wake-up event related to PCI Express has occurred, and consequently the module must turn itself on. It can be left unconnected if not used.

WAKE1#: General Purpose Wake Input, active low +3.3V_ALW electrical voltage signal with 2k2Ω pull-up resistor. It can be driven low, on the carrier board, to report that a general Wake-up event has occurred, and consequently the module must turn itself on. It can be left unconnected if not used. While WAKE0# signal is managed directly by the Soc's embedded PCH, WAKE1#signal is managed by the Embedded microcontroller.

BATLOW#: Battery Low Input, active low, +3.3V_ALW voltage signal with 10kΩ pull-up resistor. This signal can be driven on the carrier board to signal that the system battery is low, or that some battery-related event has occurred. It can be left unconnected if not used.

LID# *: LID button Input, active low +3.3V_ALW electrical level signal, with 47kΩ pull-up resistor. This signal can be driven, using a LID Switch on the carrier board, to trigger the transition of the module from Working to Sleep status, or vice versa. It can be left unconnected if not used on the carrier board.

SLEEP# *: Sleep button Input, active low +3.3V_ALW electrical level signal, with 47kΩ pull-up resistor. This signal can be driven, using a pushbutton on the carrier board, to trigger the transition of the module from Working to Sleep status, or vice versa. It can be left unconnected if not used on the carrier board.

* Note: In COM Express® specifications prior to Rel. 2.0, the pins dedicated to LID# and SLEEP# inputs were dedicated to +12$V_{IN}$ power rail. Protection circuitry has been added on LID# and SLEEP# so that they are +12V Tolerant. This has been made in order to prevent damages to the module, in case it is inserted in carrier board not designed for Type 6.

### 3.2.4.17 SMBus signals

This interface is managed by the Soc's embedded PCH.

Signals involved are the following:

SMB_CK: SM Bus control clock line for System Management. Bidirectional signal, electrical level +3.3V_ALW with a 1kΩ pull-up resistor.

SMB_DAT: SM Bus control data line for System Management. Bidirectional signal, electrical level +3.3V_ALW with a 1kΩ pull-up resistor.

SMB_ALERT#: SM Bus Alert line for System Management. Input signal, electrical level +3.3V_ALW with a 1kΩ pull-up resistor. Any device place on the SM Bus can drive this signal low to signal an event on the bus itself.

### 3.2.4.18 GPIO interface signals

According to COM Express® specifications rel. 3.0, there are 8 pins that could be used as General Purpose Inputs and Outputs, managed by embedded microcontroller

Signals involved are the following:

GPI[0÷3]: General Purpose Inputs, electrical level +3.3V_ALW with 10kΩ pull-up resistor each.

GPO[0÷3]: General Purpose Outputs, electrical level +3.3V_ALW with 10kΩ pull-down resistor each.

# 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 | See submenu | Shows board's specific SoC information |
| Power & Performance | See submenu | Power & Performance Options |
| PCH-FW Configuration | See submenu | Configure Management Engine Technology Parameters |
| Platform Settings | See submenu | Platform related settings |
| Trusted Computing | See submenu | Trusted Computing Settings |
| SMART Settings | | → Run SMART Self Test on all HDDs during POST |
| S5 RTC Wake Settings | | → Enable or disable System wake on alarm event |
| UEFI Variables Protection | | → 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 | | SMBIOS Information |
| Super I/O Configuration | See submenu | Super I/O Setup Configuration Utility |
| Main Thermal Configuration | See submenu | Main Thermal Configuration |
| Embedded Controller | See submenu | Embedded Controller |
| | | |
| Tls Auth Configuration | | |
| RAM Disk Configuration | See submenu | Add/remove RAM disks |

### 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<br>Max Non-Turbo Performance<br>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 |
| 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.<br>Disabled: Disable HDC<br>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 |
| 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 / 2 / 3 / 4 / 5 / 6 / 7 / 8 / 10 / 12 / 14 / 16 / 20 / 24 / 28 / 32 / 40 / 48 / 56 / 64 / 80 / 96 / 112 / 128 | Platform Power Limit 1 Time Window value in seconds. The value may vary from 0 to 128. 0 = default 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.<br>Cpu Default: Leaves to factory default value<br>Auto: Intializes to deepest available Package C State Limit |
| • C6/C7 Short Latency Control (MSR 0x60B)<br>• C6/C7 Long Latency Control (MSR 0x60C)<br>• C8 Latency Control (MSR 0x633)<br>• C9 Latency Control (MSR 0x634)<br>• C10 Latency Control (MSR 0x635) | Time Unit (ns):<br>1 / 32 / 1024 / 32768 / 1048576 / 33554432<br>Latency:<br>[0…1023] | Time Unit: Unit of measurement for IRTL value – bits [12:10]<br>Latency: Interrupt Response Time Limit value – bits [9:0], Enter 0-1023 |
| Thermal Monitor | Enabled / Disabled | Enable/Disable Thermal Monitor |
| Interrupt Redirection Mode Selection | Fixed Priority<br>Round robin<br>Hash Vector<br>No Change | Interrupt Redirection Mode<br>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<br>65W AC Brick<br>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 |

| | | |
|---|---|---|
| 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 |
| Power Limit 1 Override | Enabled / Disabled | Enable/Disable Power Limit 1 override. If this option is disabled, BIOS will program the default values for Power Limit 1 and Power Limit 1 Time Window. |
| Power Limit 1 | [0…4095875] | Platform 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. If value is 0, BIOS leaves default value |
| Power Limit 1 Time Window | Enabled / Disabled | 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 |
| Power Limit 2 Override | Enabled / Disabled | Enable/Disable Power Limit 1 override. If this option is disabled, BIOS will program the default values for Power Limit 2 |
| Power Limit 2 | [0…4095875] | Platform Power Limit 2 in Milli Watts. BIOS will round to the nearest 1/8W when programming. If the value is 0, BIOS will program this value as 1.25*TDP. For 12.50W, enter 12500. Processor applies policies such that the package power does not exceed this limit |
| 1-Core Ratio Limit Override | [0…83] | 1-Core Ratio Limit with range 0 to 83. The Minimum range may vary between Processors. This 1-Core Ratio Limit must be grater than or equal to 2-Core Ratio Limit, 3-Core Ratio Limit, 4-Core Ratio Limit |
| 2-Core Ratio Limit Override | [0…83] | 2-Core Ratio Limit with range 0 to 83. The Minimum range may vary between Processors. This 2-Core Ratio Limit must be less than or equal to 1-Core Ratio Limit |
| 3-Core Ratio Limit Override | [0…83] | 3-Core Ratio Limit with range 0 to 83. The Minimum range may vary between Processors. This 3-Core Ratio Limit must be less than or equal to 1-Core Ratio Limit |
| 4-Core Ratio Limit Override | [0…83] | 4-Core Ratio Limit with range 0 to 83. The Minimum range may vary between Processors. This 4-Core Ratio Limit must be less than or equal to 1-Core Ratio Limit |

| | | |
|---|---|---|
| Energy Efficient Turbo | 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 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 |

##### *4.3.1.1.2.1 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<br>Fast/4<br>Fast/8<br>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 |

##### *4.3.1.1.2.2 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 |

#### *4.3.1.1.2.3 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%) |

#### 4.3.1.1.3 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 |
|---|---|---|
| Maximum GTT frequency | Default Max Frequency / 100MHz / …<br>*List of 50MHz increments*<br>… / 1200MHz | Maximum GT frequency limited by the user. Choose between 200MHz (RPN) and 400MHz (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 |

#### 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 Replaces Polling Disable | Enabled / Disabled | Setting this option disables CPU replacement polling loop |
| ME DID Message | Enabled / Disabled | Enable/Disable ME DID Message (disable will prevent the DID message from being sent) |

| | | |
|---|---|---|
| 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 |

#### 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 /<br>Enable UCSI Device /<br>Enable UCMC Device | Select UCSI or UCMC device in ACPI support based on configuration |
| Type C retimer TC 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 |
| Dynamic one-time switch | Enabled / Disabled | Dynamic onr-time switch from iGFx to dGFx after boot to OS |

### 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 |
| IFU Enable | Enabled / Disabled | Enables or Disables SHA256 PCR Bank |
| Software SRAM | Enabled / Disabled | Enables or Disables SHA384 PCR Bank |

### 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<br>TPM 1.2<br>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<br>VT100+<br>VT-UTF8<br>ANSI | Emulation:<br>ANSI: Extended ASCII Char set.<br>VT100: ASCII Char set.<br>VT100+: extends VT100 to support colour, function keys, etc.<br>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<br>Even<br>Odd<br>Mark | A parity bit can be sent with the data bits to detect some transmission errors.<br>Even: parity bit is 0 if the number of 1s in the data bits is even.<br>Odd: parity bit is 0 if the number of 1s in the data bits is odd.<br>Mark: parity bit is always 1. |

| | | |
|---|---|---|
| | Space | 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<br>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<br>COM1 | Microsoft Windows Emergency Management Services (EMS) allows for remote management of a Windows Server OS through a serial port |
| Terminal Type EMS | VT100<br>VT100+<br>VT-UTF8<br>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<br>Hardware RTS/CTS<br>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<br>ADMA<br>SDMA<br>PIO | Auto Option: Access the SD Device in DMA mode if the controller supports it, otherwise in PIO Mode.<br>DMA Option: Access the SD Device in DMA mode<br>ADMA Option: Access the SD Device in Advanced DMA mode<br>PIO Option: Access the SD Device in PIO mode |
| *List of SDIO devices found* | Auto<br>Floppy<br>Forced FDD<br>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<br>Always OFF<br>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<br>Force Closed<br>Normal Polarity<br>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<br>Only From S3<br>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*<br>• *WDT Timeout Expired* | | Show event as Happened or Not Happened |

| | | |
|---|---|---|
| • *Power Failure*<br>• *E.C soft reset* | | |
| 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<br>4-WIRE FAN<br>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<br>4-WIRE FAN<br>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<br>Output Low<br>Output High<br>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)<br>→ Delete Cert |

### 4.3.15 RAM Disk Configuration

| Menu Item | Options | Description |
|---|---|---|
| Disk Memory Type: | Boot Service Data<br>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<br>Auto : Skip GPIO based Power Eable to dGPU<br>Elk Creek 4: DGPU Power Enable = ActiveLow<br>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 |
| Serial IO Configuration | See submenu | Serial IO Configuration Settomgs |
| 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.<br>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.<br>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<br>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 |
| 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<br>SSP (I2S)<br>SoundWire<br>Advanced Link Config | Select link mode:<br>1) HDA-Link [SDIO-1], DMIC[0-1]<br>2) SSP[0-5], DMIC[0-1]<br>3) SNDW[1-4]<br>4) Advanced will allow to enable each interface separately |
| HDA-Link Codec Select | Platform Onboard<br>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 |

#### 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 Link Frequency | 6 MHz<br>12 MHz<br>24 MHz | Selects HD Audio Link frequency.<br>Applicable only if HAD codec supports selected frequency |
| iDisplay Audio Link Frequency | 48 MHz<br>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 # |

### 4.4.2.6 Serial IO Configuration

| Menu Item | Options | Description |
|---|---|---|
| I2C0 Controller<br>I2C1 Controller<br>I2C2 Controller<br>I2C3 Controller<br>SPI0 Controller<br>SPI1 Controller<br>UART0 Controller<br>UART1 Controller | Enabled / Disabled | Enable / Disable SerialIO Controller. If given device is Function 0 PSF disabling is skipped. PSF default will remain and device PCI CFG Space will still be visible. This is needed to allow PCU enumerator access functions above 0 in a multifunction device. |
| SerialIO D3 State | Enabled / Disabled | Enable / Disable SerialIO D3 State |

| | | |
|---|---|---|
| GPIO IRQ Route | IRQ14 / IRQ15 | Route all GPIOs to one of the IRQ |
| Serial IO *Controller#* Settings | | Configure Serial IO Controller --> Set specific parameters |
| WITT/MITT Test Device | Enabled / Disabled | Choose if WITT Device is used and with which controller |
| UART Test Device | Enabled / Disabled | Choose if UART Test Device is used and with which controller |
| Additional Serial IO devices | Enabled / Disabled | When enabled, ACPI will report additional devices connected to Serial IO |
| Serilal IO timing parameters | Enabled / Disabled | Enables additional timing parameters for all Serial IO controllers. Defaults can be changed in each controller setting. Platform restart quired to apply changes. |

# 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)<br>Key Exchange Keys<br>Authorized Signatures<br>Forbidden Signatures<br>Authorized Timestamps<br>OS Recovery Signatures | Set New Var<br>Append Key | Enrol factory Defaults or load certificates from a file:<br>1. Public Key Certificate in:<br>a) EFI_SIGNATURE_LIST<br>b) EFI_CERT_X509 (DER encoded)<br>c) EFI_CERT_RSA2048 (bin)<br>d) EFI_CERT_SHAxxx<br>2. Authenticated UEFI Variable<br>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<br>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<br>Full Initial<br>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<br>• Boot Option #2<br>• Boot Option #3<br>• Boot Option #4<br>• Boot Option #5<br>• Boot Option #6<br>• Boot Option #7<br>• Boot Option #8<br>• Boot Option #9 | Hard Disk0<br>Hard Disk1<br>eMMC<br>CD/DVD<br>SD<br>USB Device<br>Network<br>Other Device<br>Disabled | Select the system boot order |
| UEFI EMMC Drive BBS Priorities | | Specifies the Boot Device Priority sequence from available UEFI EMMC Drivers |
| UEFI SD Drive BBS Priorities | | Specifies the Boot Device Priority sequence from available UEFI SD Drivers |

## 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

A parameter that has to be kept in very high consideration is the thermal design of the system.

Highly integrated modules like CALYPSO offer to the user very good performances in minimal spaces, therefore allowing the system's minimisation. On the counterpart, the miniaturising of IC's and the rise of operative frequencies of processors lead to the generation of a big amount of heat, that must be dissipated to prevent system hang-off or faults.

COM Express® specifications take into account the use of a heatspreader, which will act only as thermal coupling device between the COM Express® module and an external dissipating surface/cooler. The heatspreader also needs to be thermally coupled to all the heat generating surfaces using a thermal gap pad, which will optimise the heat exchange between the module and the heatspreader.

The heatspreader is not intended to be a cooling system by itself, but only as means for transferring heat to another surface/cooler, like heatsinks, fans, heat pipes and so on.

Conversely, heatsink with fan in some situation can represent the cooling solution. Indeed, when using CALYPSO module, it is necessary to consider carefully the heat generated by the module in the assembled final system, and the scenario of utilisation.

Until the module is used on a development Carrier board, on free air, just for software development and system tuning, then a finned heatsink with FAN could be sufficient for module's cooling. Anyhow, please remember that all depends also on the workload of the processor. Heavy computational tasks will generate much heat with all processor versions.

Therefore, it is always necessary that the customer study and develop accurately the cooling solution for his system, by evaluating processor's workload, utilisation scenarios, the enclosures of the system, the air flow and so on. This is particularly needed for industrial grade modules.

SECO can provide CALYPSO module specific heatspreaders and heatsinks, 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. Please ask SECO for specific ordering codes.

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