Com express

User Manual

COMe-C42
BT7

COM-Express™ Type 7 Module with the AMD EPYC™ Embedded 3000 Series of SoCs.

www.seco.com

REVISION HISTORY

Revision	Date	Note	Rif
1.0	22 July 2021	First Official Release	SB

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 http://www.seco.com (registration required).

Our team is ready to assist you.

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 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 form available on the web-site http://www.seco.com/en/prerma (RMA Online). 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 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.

Warning!
All changes or modifications to the equipment not explicitly approved by SECO S.p.A. could impair the equipments 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 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 340434
- Repair centre: 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 COMe-C42-BT7 module 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 COMe-C42-BT7 module, 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 a COMe-C42-BT7 module, 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 COMe-C42-BT7 module 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, the COMe-C42 Module 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 a COMe-C42 module 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 conditions
- 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.

1.8 Terminology and definitions

10GBASE-KR	Backplane Ethernet, 10 Gbps datarate, designed to operate over a single lane with up to 1m (39”) of copper PCB.
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
BMC	Baseboard Management Controller
DDR	Double Data Rate, a typology of memory devices which transfer data both on the rising and on the falling edge of the clock
DDR4	DDR, 4th generation
DF	Data Fabric
FCH	Firmware Controller Hub, rhe integrated platform subsystem that contains the IO interfaces and bridges them to the system BIOS. Previously included in the Southbridge
GbE	Gigabit Ethernet
Gbps	Gigabits per second
GT/s	Gigatransfers per second
GND	Ground
GPI/O	General purpose Input/Output
I2C Bus	Inter-Integrated Circuit Bus, a simple serial bus consisting only of data and clock line, with multi-master capability
iSCSI	Internet Small Computer Systems Interface, an Internet Protocol based storage networking standard for linking data storage facilities via networking.
LPC Bus	Low Pin Count Bus, a low speed interface based on a very restricted number of signals, deemed to management of legacy peripherals
Mbps	Megabits per second
NC-SI	Network Controller Sideband Interface, electrical interface and protocol which enables the connection of a BMC to enable out-of-band remote manageability.
N.A.	Not Applicable
N.C.	Not Connected
NTB	Non-transparent bridge. A device that links the memory space of two separate systems together. The processor implements a NTB that connects two systems together using the PCI-e interface
OS	Operating System

PCI-e	Peripheral Component Interface Express
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
RAS	Reliability, Availability and Serviceability. Reliability refers to the ability to detect errors. Availability is the ability to still operate in the face of failure. Serviceability refers to capabilities that reduce the effort required to service a component.
SATA	Serial Advance Technology Attachment, a differential half duplex serial interface for Hard Disks
SEV	Secure Encrypted Virtualization
SEV-ES	Secure Encrypted Virtualization Encrypted State
SM Bus	System Management Bus, a subset of the I2C bus dedicated to communication with devices for system management, like smart batteries 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
TLB	Translation Lookaside Buffer, a memory cache that is used to reduce the time taken to access a user memory location
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
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.uefi.org/acpi/specs
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
10GBASE-KR	https://standards.ieee.org/standard/802_3ap-2007.html
Gigabit Ethernet	https://www.techstreet.com/ieee/standards/ieee-802-3-2018?product_id=1999889
I2C	https://www.nxp.com/docs/en/user-guide/UM10204.pdf
LPC Bus	https://www.intel.com/content/dam/www/program/design/us/en/documents/low-pin-count-interface-specification.pdf
NC-SI	http://www.dmtf.org/sites/default/files/standards/documents/DSP0222_1.0.0.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	https://usb.org/document-library/usb-20-specification
USB 3.x	https://usb.org/document-library/usb-32-specification-released-september-22-2017-and-ecns
xHCI	http://www.intel.com/content/www/us/en/io/universal-serial-bus/extensible-host-controler-interface-usb-xhci.html?wapkw=xhci
AMD EPYC™ Embedded 3000	https://www.amd.com/en/products/embedded-epyc-3000-series

Chapter 2.
OVERVIEW

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

2.1 Introduction

The COMe-C42-BT7 is a COM Express® Type 7, basic Form Factor, based on the AMD EPYC™ Embedded 3000 3000 processors, specifically targeted for networking/server applications. The complete list of processors is available in the next chapter.

The main features of this new processor are I/O integration, flexibility, and security capabilities, scalable offering, harnessing the power of the new “Zen” CPU architecture.

Moreover, the performance is enhanced by the four DDR4 SO-DIMM slots supporting DDR4-2666 memory with ECC, up to 128GB.

This innovative solution provides scalable offerings with outstanding performance and connectivity, managing 4x 10GBASE-KR interfaces + 1x 1GbE port with NC-SI, four USB 3.1 ports and 24x PCI-e Gen3 lanes.

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. Specifically, COMe-C42-BT7 is a COM Express® module, Basic Form factor, Type 7 (125mm x 95mm).

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

AMD EPYC™ Embedded 3251, Eight Core Dual Thread @ 2.5GHz (3.1 Boost), 16MB L3 shared Cache, TDP 55W
AMD EPYC™ Embedded 3201, Eight Core Single Thread @ 1.5GHz (3.1 Boost), 16MB L3 shared Cache, TDP 30W
AMD EPYC™ Embedded 3151, Quad Core Dual Thread @ 2.7GHz (2.9 Boost), 16MB L3 shared Cache, TDP 45W
AMD EPYC™ Embedded 3101, Quad Core Single Thread @ 2.1GHz (2.9 Boost), 8MB L3 shared Cache, TDP 35W
AMD EPYC™ Embedded 3255, Eight Core Dual Thread @ 2.5GHz (3.1 Boost), 16MB L3 Shared Cache, TDP 25-55W, industrial grade

Memory

Up to 4x DDR4 SO-DIMM Slots supporting DDR4-2666 ECC and non-ECC Memory, up to 128GB

Mass Storage

2 x external S-ATA Gen3 Channels

USB

4 x USB 3.1 (SS+ USB 2.0 interfaces) Host ports

Networking

1x Gigabit Ethernet LAN port with NC-SI (Network Controller Sideband Interface) functionality, managed by an Intel® I210 Gigabit Ethernet Controller
4x 10Gigabit Ethernet interfaces (10GBASE-KR) directly managed by the EPYC™ Embedded 3000 SoC

PCI Express

24 x PCI-e Gen3 lanes

Serial Ports

2 x legacy UARTs, 16C550 compatible

Other Interfaces

SPI, I2C, SM Bus, LPC bus
Thermal Management, FAN management
4 x GPI, 4 x GPO
LID# / SLEEP# / PWRBTN#, Watchdog
Speaker Out
Optional TPM 1.2 or 2.0 on-board

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

Operating System:

Microsoft® Windows 10 Enterprise (64-bit)
Microsoft® Windows Server 2016
Linux 64-bit

Operating temperature:

0°C ÷ +60°C (Commercial version) **

-40°C ÷ +85°C (Industrial version) **

Dimensions: 125 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, the COMe-C42-BT7 board needs to be supplied only with an external +12V_{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 +12V_{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:

VCC_5V_SBY: 5V Standby voltage for the module

VCC_12V: 12V Power In Voltage for the module.

_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) and S5 (Soft Off) state. Examples: +5V_ALW, +3.3V_ALW. S3 (Standby) Status is not supported.

3.3V_LAN: 3.3V always-on voltage, derived from 3.3V_ALW, specifically used for 1GbE Ethernet section

2.3.2 Power Consumption

COMe-C42-BT7 module, 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.

Therefore, power consumptions of the board are measured using a CCOMe-C79 Carrier board on the dedicated +12V_RUN power rail that supplies the board. For this reason, the values indicated in the table below are real 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 (VCC_RTC power rail). For the measurements, it has been used a DC Power Analyzer Keysight N6700B.

The current consumptions, written in the table of next page, have been measured using the following setup:

Board Configurations:

- O.S. Windows 10
- 4x 32GB DDR4-2666 SO-DIMM, S-LINK J4BGDS2G8QHKC
- TPM Present, Ethernet Controller I210 or I211, 3-Wire FAN configuration, Commercial temperature range

- USB mouse and keyboard connected

Status	CPU & board configuration							
	AMD EPYC™ Embedded 3251 2.5GHz I210 Eth Controller		AMD EPYC™ Embedded 3201 1.5GHz I210 Eth Controller		AMD EPYC™ Embedded 3151 2.7GHz I211 Eth Controller		AMD EPYC™ Embedded 3101 2.1GHz I211 Eth Controller	
	Average	Peak	Average	Peak	Average	Peak	Average	Peak
Idle (Win 10), high performance configuration	1.19A	1.46A	1.20A	1.88A	1.13A	1.84A	1.10A	1.69A
Idle (Win 10), power saving configuration	1.00A	1.44A	1.00A	1.31A	1.07A	1.16A	0.98A	1.44A
Boot (Win 10), high performance configuration	3.10A	5.27A	2.14A	3.14A	1.97A	2.92A	2.14A	2.95A
Internal Stress Test Tool, maximum performance	4.70A	4.76A	2.42A	2.49A	2.84A	2.85A	2.84A	3.00A
Soft Off (typical)	139mA		131mA		128mA		110mA	

2.4 Mechanical Specifications

The COMe-C42-BT7 is a COM Express board, Basic form Factor type; therefore its dimensions are 125 mm x 95 mm (4.92" x 3.74").

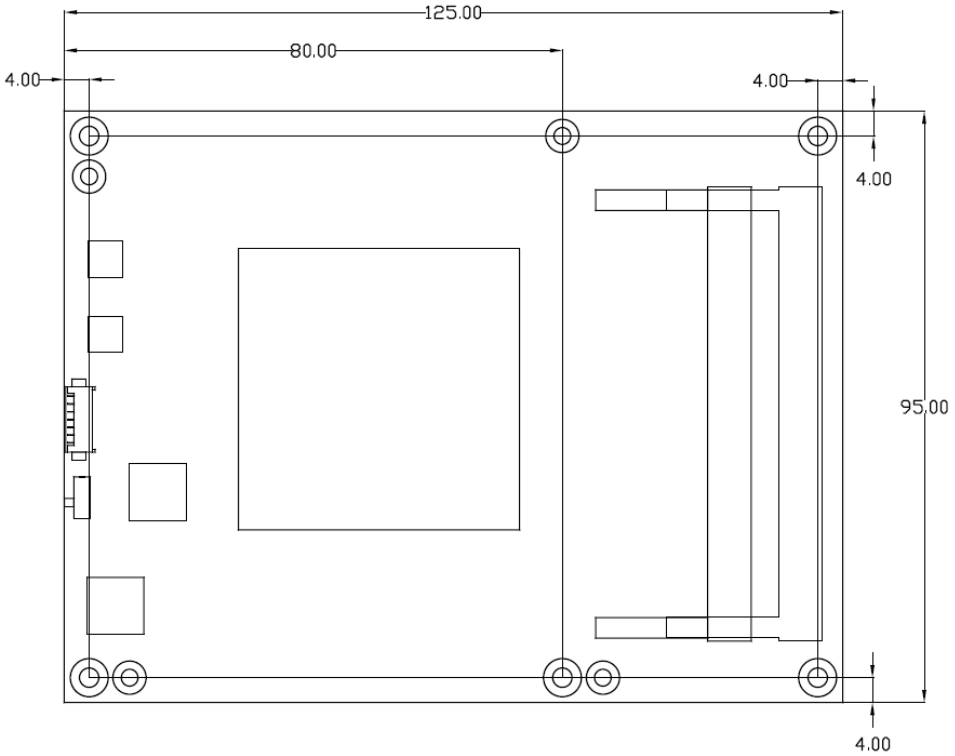
Printed circuit of the board is made of twelve layers, some of them are ground planes, for disturbance rejection.

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

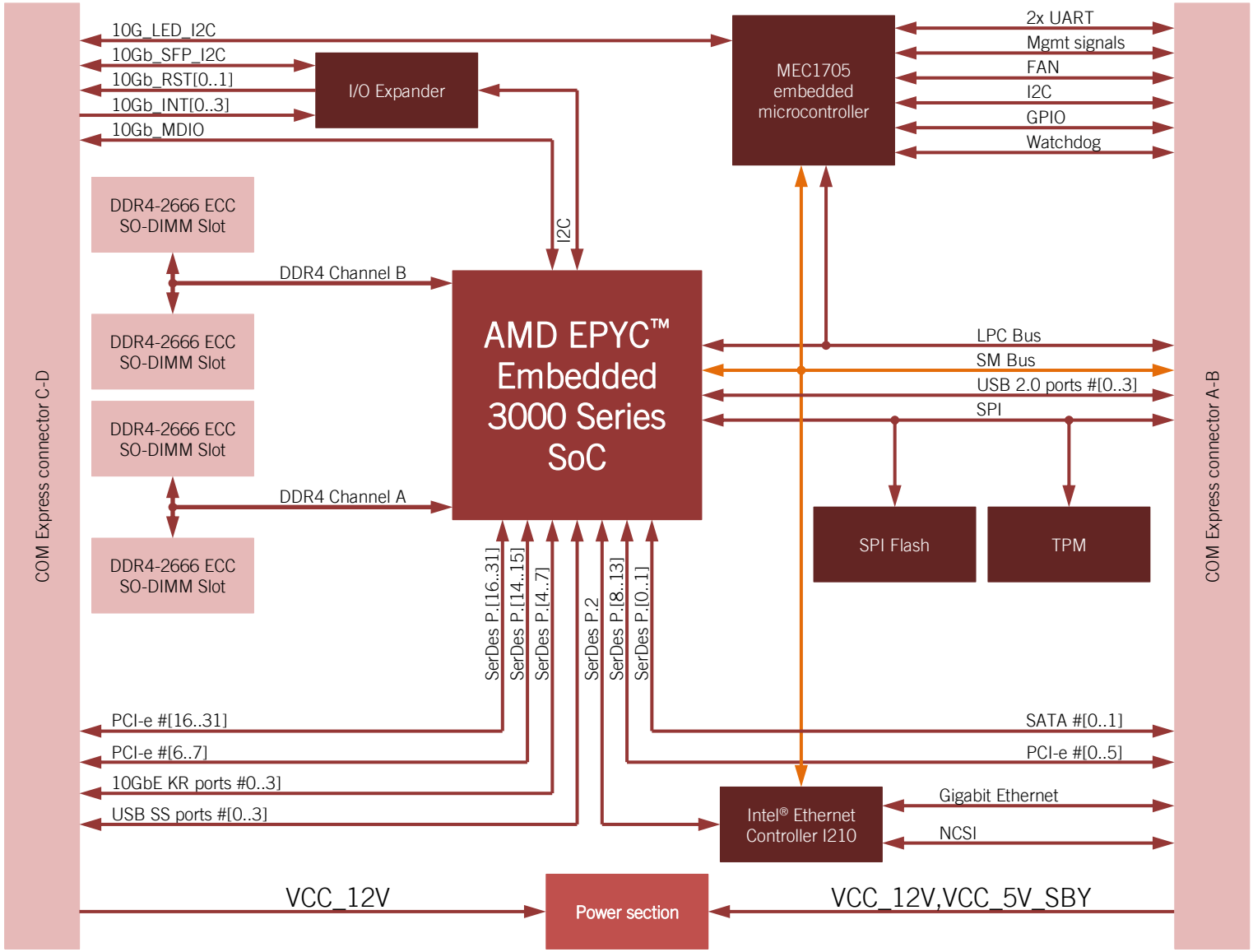
Please be aware that the COMe-C42-BT7 module can be equipped with up to four SO-DIMM slots, where the secondary slot for each channel is located on bottom side of the module. In this case, SO-DIMM secondary slot for Channel #A is 4mm high, while secondary slot for Channel #B is 8mm high.

This means that, in order to deploy the maximum quantity of memory that can be managed by COMe-C42-BT7 module, it is necessary to consider a 8mm carrier board's plug height.

It is also necessary to avoid placing components on the carrier board in the zone under the COM Express® module, especially under the two SO-DIMM slots



2.5 Block Diagram



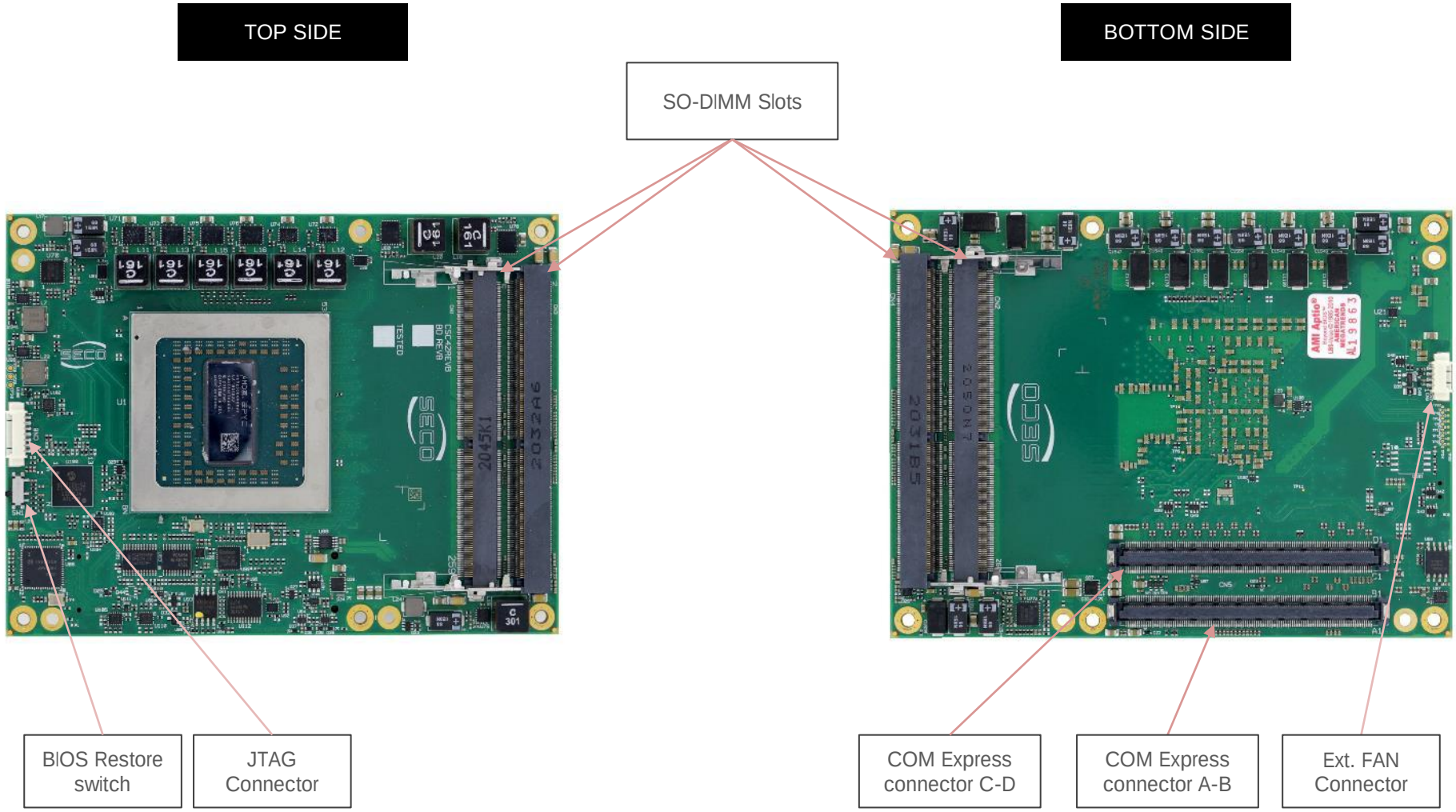
Chapter 3.
CONNECTORS

- 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.



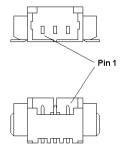
3.2 Connectors' description

3.2.1 FAN Connector

3-Wires FAN Connector – CN6	
Pin	**Signal**
1	GND
2	FAN_POWER
3	FAN_TACHO_IN

Depending on the usage model of COMe-C42-BT7 module, 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.



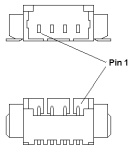
Mating connector: MOLEX 51021-0300 receptacle with MOLEX 50079-8000 female crimp terminals.

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.

4-Wires 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 53261-0371 or equivalent, with pinout shown in the table on the left.



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

Here following the description of the signals available on these connectors (FAN_PWM available only on CN7 connector)

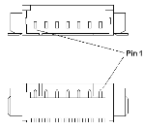
FAN_POWER: +12V_RUN derived power rail for FAN, managed by the embedded microcontroller via PWM signal.

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

3.2.2 JTAG Connector

JTAG connector– CN8	
Pin	**Signal**
1	+3.3V_ALW
2	LM4_TMS
3	LM4_TCK
4	LM4_TDI
5	LM4_TD0
6	LM4_NRST
7	GND



The Embedded controller MEC1705 mounted on COMe-C42-BT7 module provides a JTAG interface, for test and debug purposes. This interface is available through an on-module connector, CN8, type MOLEX p/n 53261-0719. Mating connector MOLEX p/n 51021-0700 receptacle with 50079 female crimp terminals.

All these JTAG signals are at electrical level +3.3V_ALW with 10k pull-up resistor and are directly connected to SOC pins with same name. Please refer to EPYC™ Embedded 3000 family of processors documentation for a description of the signals and their usage.

LM4_TMS: JTAG Test Mode Select Signal, +3.3V_ALW electrical level with 10k Ohm pull-up resistor.

LM4_TCK: JTAG Test Clock Signal, +3.3V_ALW electrical level with 10k Ohm pull-up resistor.

LM4_TDI: JTAG Test Data Input Signal, +3.3V_ALW electrical level with 1k Ohm pull-up resistor.

LM4_TDO: JTAG Test Data Output Signal, +3.3V_ALW electrical level with 1k Ohm pull-up resistor.

LM4_NRST: JTAG Test Reset Output Signal, +3.3V_ALW electrical level with 10k Ohm pull-up resistor.

3.2.3 SO-DIMM DDR4 Slots

CPUs used on the COMe-C42-BT7 board provide support to DDR4-2666 SO-DIMM memory modules. Both ECC and non-ECC modules are supported.

For use of this memories, on board there can be up to four SO-DIMM DDR4 slots.

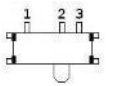
The sockets placed on top side are CN1, type LOTES p/n ADDR0206-P003A or equivalent, and CN3, type LOTES p/n ADDR0070-P011A or equivalent. These sockets are always available.

The sockets placed on bottom side, instead, are optional. They are CN2, type LOTES p/n ADDR0205-P003A or equivalent, and CN4, type LOTES p/n ADDR0069-P011A or equivalent. CN2 is the secondary slot for memory Channel #A, CN4 is the secondary slot for memory Channel #B.

All of these sockets are right angle, low profile, standard type sockets, used for high speed system memory applications.

The four sockets together allow the insertion of up to 4 SO-DIMM modules, for support to four channel memories, reaching up to 128GB.

3.2.4 BIOS Restore switch



In some cases, a wrong configuration of BIOS parameters could lead the module in an unusable state (e.g., 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.

3.2.5 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 COMe-C42-BT7 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 CN1 – 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	N.C.	N.A.	
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.A.	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.A.	N.C.	A22	B22	N.C.	N.A.	
	N.A.	N.C.	A23	B23	N.C.	N.A.	
PWR_MGMT	O	SUS_S5#	A24	B24	PWR_OK	I	PWR_MGMT
	N.A.	N.C.	A25	B25	N.C.	N.A.	
	N.A.	N.C.	A26	B26	N.C.	N.A.	
	N.A.	N.C.	A27	B27	WDT	O	MISC
	N.A.	N.C.	A28	B28	N.C.	N.A.	
	N.A.	N.C.	A29	B29	N.C.	N.A.	
	N.A.	N.C.	A30	B30	N.C.	N.A.	
	PWR	GND	A31	B31	GND	PWR	
	N.A.	N.C.	A32	B32	N.C.	N.A.	
	N.A.	N.C.	A33	B33	I2C_CK	O	I2C
LPC	I	BIOS_DIS0#	A34	B34	I2C_DAT	I/O	I2C
MISC	O	THRMTRIP#	A35	B35	THRM#	I	MISC
	N.A.	N.C.	A36	B36	N.C.	N.A.	
	N.A.	N.C.	A37	B37	N.C.	N.A.	
	PWR	GND	A38	B38	GND	PWR	
	N.A.	N.C.	A39	B39	N.C.	N.A.	
	N.A.	N.C.	A40	B40	N.C.	N.A.	
	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	N.C.	N.A.	
	N.A.	N.C.	A48	B48	N.C.	N.A.	
GBE	I/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	
	N.A.	N.C.	A71	B71	N.C.	N.A.	
	N.A.	N.C.	A72	B72	N.C.	N.A.	
	PWR	GND	A73	B73	GND	PWR	
	N.A.	N.C.	A74	B74	N.C.	N.A.	
	N.A.	N.C.	A75	B75	N.C.	N.A.	
	PWR	GND	A76	B76	GND	PWR	
	N.A.	N.C.	A77	B77	N.C.	N.A.	
	N.A.	N.C.	A78	B78	N.C.	N.A.	
	PWR	GND	A79	B79	GND	PWR	
	PWR	GND	A80	B80	GND	PWR	

	N.A.	N.C.	A81	B81	N.C.	N.A.	
	N.A.	N.C.	A82	B82	N.C.	N.A.	
	PWR	GND	A83	B83	GND	PWR	
NC-SI	I	NCSI_TX_EN	A84	B84	VCC_5V_SBY	PWR	
GPIO	I	GPI3	A85	B85	VCC_5V_SBY	PWR	
	N.A.	N.C.	A86	B86	VCC_5V_SBY	PWR	
	N.A.	N.C.	A87	B87	VCC_5V_SBY	PWR	
PCIE	O	PCIE_CLK_REF+	A88	B88	BIOS_DIS1#	I	LPC
PCIE	O	PCIE_CLK_REF-	A89	B89	NCSI_RX_ER	O	NC-SI
	PWR	GND	A90	B90	GND	PWR	
SPI	O	SPI_POWER	A91	B91	NCSI_CLK_IN	I	NC-SI
SPI	I	SPI_MISO	A92	B92	NCSI_RXD1	O	NC-SI
GPIO	O	GPO0	A93	B93	NCSI_RXD0	O	NC-SI
SPI	O	SPI_CLK	A94	B94	NCSI_CRS_DV	O	NC-SI
SPI	O	SPI_MOSI	A95	B95	NCSI_TXD1	I	NC-SI
MISC	I	TPM_PP	A96	B96	NCSI_TXD0	I	NC-SI
TYPE	N.A.	TYPE10#: N.C.	A97	B97	SPI_CS#	O	SPI
UART	O	SER0_TX	A98	B98	NCSI_ARB_IN	I	NC-SI
UART	I	SER0_RX	A99	B99	NCSI_ARB_OUT	O	NC-SI
	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	VCC_12V	A104	B104	VCC_12V	PWR	
	PWR	VCC_12V	A105	B105	VCC_12V	PWR	
	PWR	VCC_12V	A106	B106	VCC_12V	PWR	
	PWR	VCC_12V	A107	B107	VCC_12V	PWR	
	PWR	VCC_12V	A108	B108	VCC_12V	PWR	
	PWR	VCC_12V	A109	B109	VCC_12V	PWR	
	PWR	GND	A110	B110	GND	PWR	

COM Express® Connector CN1 – 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	
10GbE	I/O	10G_PHY_MDC_SCL3 (*)	C15	D15	10G_PHY_MDIO_SDA3 (*)	I/O	10GbE
10GbE	I/O	10G_PHY_MDC_SCL2 (*)	C16	D16	10G_PHY_MDIO_SDA2 (*)	I/O	10GbE
	N.A.	N.C.	C17	D17	N.C.	N.A.	
	PWR	GND	C18	D18	GND	PWR	
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
10GbE	I	10G_INT2	C24	D24	10G_INT3	I	10GbE
	PWR	GND	C25	D25	GND	PWR	

10GbE	I	10G_KR_RX3+	C26	D26	10G_KR_TX3+	O	10GbE
10GbE	I	10G_KR_RX3-	C27	D27	10G_KR_TX3-	O	10GbE
	PWR	GND	C28	D28	GND	PWR	
10GbE	I	10G_KR_RX2+	C29	D29	10G_KR_TX2+	O	10GbE
10GbE	I	10G_KR_RX2-	C30	D30	10G_KR_TX2-	O	10GbE
	PWR	GND	C31	D31	GND	PWR	
10GbE	I/O	10G_SFP_SDA3	C32	D32	10G_SFP_SCL3	I/O	10GbE
10GbE	I/O	10G_SFP_SDA2	C33	D33	10G_SFP_SCL2	I/O	10GbE
10GbE	O	10G_PHY_RST_23	C34	D34	10G_PHY_CAP_23	I	10GbE
10GbE	O	10G_PHY_RST_01	C35	D35	10G_PHY_CAP_01	I	10GbE
10GbE	I/O	10G_LED_SDA	C36	D36	N.C.	N.A.	
10GbE	I/O	10G_LED_SCL	C37	D37	N.C.	N.A.	
10GbE	I/O	10G_SFP_SDA1	C38	D38	10G_SFP_SCL1	I/O	10GbE
10GbE	I/O	10G_SFP_SDA0	C39	D39	10G_SFP_SCL0	I/O	10GbE
	N.A.	N.C.	C40	D40	N.C.	N.A.	
	PWR	GND	C41	D41	GND	PWR	
10GbE	I	10G_KR_RX1+	C42	D42	10G_KR_TX1+	O	10GbE
10GbE	I	10G_KR_RX1-	C43	D43	10G_KR_TX1-	O	10GbE
	PWR	GND	C44	D44	GND	PWR	
10GbE	I/O	10G_PHY_MDC_SCL1 (*)	C45	D45	10G_PHY_MDIO_SDA1 (*)	I/O	10GbE
10GbE	I/O	10G_PHY_MDC_SCL0 (*)	C46	D46	10G_PHY_MDIO_SDA0 (*)	I/O	10GbE
10GbE	I	10G_INT0	C47	D47	10G_INT1	I	10GbE
	PWR	GND	C48	D48	GND	PWR	
10GbE	I	10G_KR_RX0+	C49	D49	10G_KR_TX0+	O	10GbE
10GbE	I	10G_KR_RX0-	C50	D50	10G_KR_TX0-	O	10GbE
	PWR	GND	C51	D51	GND	PWR	
PCIE	I	PCIE_RX16+	C52	D52	PCIE_TX16+	O	PCIE
PCIE	I	PCIE_RX16-	C53	D53	PCIE_TX16-	O	PCIE
TYPE	N.A.	TYPE0#: GND	C54	D54	N.C.	N.A.	
PCIE	I	PCIE_RX17+	C55	D55	PCIE_TX17+	O	PCIE

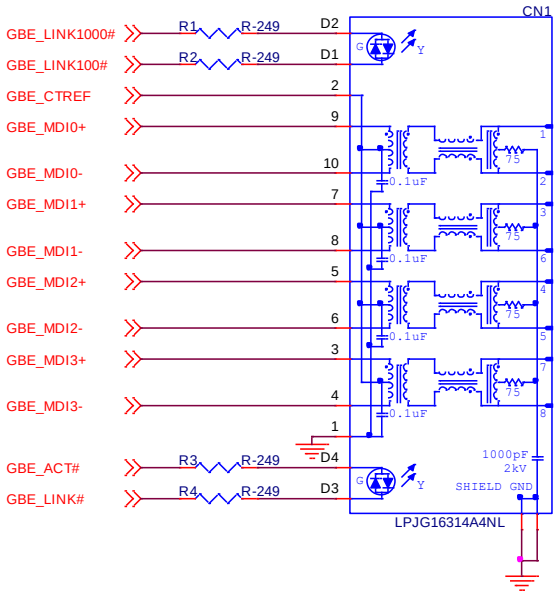
PCIE	I	PCIE_RX17-	C56	D56	PCIE_TX17-	O	PCIE
TYPE	N.A.	TYPE1#: N.C.	C57	D57	TYPE2#: GND	N.A.	TYPE
PCIE	I	PCIE_RX18+	C58	D58	PCIE_TX18+	O	PCIE
PCIE	I	PCIE_RX18-	C59	D59	PCIE_TX18-	O	PCIE
	PWR	GND	C60	D60	GND	PWR	
PCIE	I	PCIE_RX19+	C61	D61	PCIE_TX19+	O	PCIE
PCIE	I	PCIE_RX19-	C62	D62	PCIE_TX19-	O	PCIE
	N.A.	N.C.	C63	D63	N.C.	N.A.	
	N.A.	N.C.	C64	D64	N.C.	N.A.	
PCIE	I	PCIE_RX20+	C65	D65	PCIE_TX20+	O	PCIE
PCIE	I	PCIE_RX20-	C66	D66	PCIE_TX20-	O	PCIE
	N.A.	N.C.	C67	D67	GND	PWR	
PCIE	I	PCIE_RX21+	C68	D68	PCIE_TX21+	O	PCIE
PCIE	I	PCIE_RX21-	C69	D69	PCIE_TX21-	O	PCIE
	PWR	GND	C70	D70	GND	PWR	
PCIE	I	PCIE_RX22+	C71	D71	PCIE_TX22+	O	PCIE
PCIE	I	PCIE_RX22-	C72	D72	PCIE_TX22-	O	PCIE
	PWR	GND	C73	D73	GND	PWR	
PCIE	I	PCIE_RX23+	C74	D74	PCIE_TX23+	O	PCIE
PCIE	I	PCIE_RX23-	C75	D75	PCIE_TX23-	O	PCIE
	PWR	GND	C76	D76	GND	PWR	
	N.A.	N.C.	C77	D77	N.C.	N.A.	
PCIE	I	PCIE_RX24+	C78	D78	PCIE_TX24+	O	PCIE
PCIE	I	PCIE_RX24-	C79	D79	PCIE_TX24-	O	PCIE
	PWR	GND	C80	D80	GND	PWR	
PCIE	I	PCIE_RX25+	C81	D81	PCIE_TX25+	O	PCIE
PCIE	I	PCIE_RX25-	C82	D82	PCIE_TX25-	O	PCIE
	N.A.	N.C.	C83	D83	N.C.	N.A.	
	PWR	GND	C84	D84	GND	PWR	
PCIE	I	PCIE_RX26+	C85	D85	PCIE_TX26+	O	PCIE

PCIE	I	PCIE_RX26-	C86	D86	PCIE_TX26-	O	PCIE
	PWR	GND	C87	D87	GND	PWR	
PCIE	I	PCIE_RX27+	C88	D88	PCIE_TX27+	O	PCIE
PCIE	I	PCIE_RX27-	C89	D89	PCIE_TX27-	O	PCIE
	PWR	GND	C90	D90	GND	PWR	
PCIE	I	PCIE_RX28+	C91	D91	PCIE_TX28+	O	PCIE
PCIE	I	PCIE_RX28-	C92	D92	PCIE_TX28-	O	PCIE
	PWR	GND	C93	D93	GND	PWR	
PCIE	I	PCIE_RX29+	C94	D94	PCIE_TX29+	O	PCIE
PCIE	I	PCIE_RX29-	C95	D95	PCIE_TX29-	O	PCIE
	PWR	GND	C96	D96	GND	PWR	
	N.A.	N.C.	C97	D97	N.C.	N.A.	
PCIE	I	PCIE_RX30+	C98	D98	PCIE_TX30+	O	PCIE
PCIE	I	PCIE_RX30-	C99	D99	PCIE_TX30-	O	PCIE
	PWR	GND	C100	D100	GND	PWR	
PCIE	I	PCIE_RX31+	C101	D101	PCIE_TX31+	O	PCIE
PCIE	I	PCIE_RX31-	C102	D102	PCIE_TX31-	O	PCIE
	PWR	GND	C103	D103	GND	PWR	
	PWR	VCC_12V	C104	D104	VCC_12V	PWR	
	PWR	VCC_12V	C105	D105	VCC_12V	PWR	
	PWR	VCC_12V	C106	D106	VCC_12V	PWR	
	PWR	VCC_12V	C107	D107	VCC_12V	PWR	
	PWR	VCC_12V	C108	D108	VCC_12V	PWR	
	PWR	VCC_12V	C109	D109	VCC_12V	PWR	
	PWR	GND	C110	D110	GND	PWR	

(*) these signals are referred according to COM Express standard, but they are managed at quartetses (i.e., 10G_PHY_MDC_SCL0 is connected to 10G_PHY_MDC_SCL1, 10G_PHY_MDC_SCL2 and 10G_PHY_MDC_SCL3 , 10G_PHY_MDC_SDA0 is tied to 10G_PHY_MDC_SDA1, 10G_PHY_MDC_SDA2 and 10G_PHY_MDC_SDA3)

3.2.5.1 Gigabit Ethernet signals

The Gigabit Ethernet interface is realised, on COMe-C42-BT7 module, using an Intel® I21x Gigabit Ethernet controller, which is interfaced to the SOC through a dedicated PCI-express root port.



Here following the signals involved in GbE 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: Gigabit Ethernet controller Software Definable Pin, managed by the controller's SDP0 Pin, electrical level 3.3V_LAN with internal 30kΩ pull-up resistor.

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® I210 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.

3.2.5.2 NC-SI Signals

According to COM Express Specifications' requirements for Type 7 modules, the COMe-C42-BT7 module supports NC-SI signals for BMC management.

These signals are associated to the Gigabit Ethernet interface defined at previous paragraph, and are therefore managed by the on-board Intel® I210 Gigabit Ethernet controller.

Here following the signals related to NC-SI interface.

NCSI_CLK_IN: NC-SI 50MHz reference Clock input for Rx, Tx and control interfaces. Electrical level 3.3V_LAN with 10kΩ pull-down resistor.

NCSI_RXD0: NC-SI Receive Data #0 Output, from I210 Network Controller to external BMC. Electrical level 3.3V_LAN with 10kΩ pull-up resistor.

NCSI_RXD1: NC-SI Receive Data #1 Output, from I210 Network Controller to external BMC. Electrical level 3.3V_LAN with 10kΩ pull-up resistor.

NCSI_TXD0: NC-SI Transmit Data #0 Input, from external BMC to I210 Network Controller. Electrical level 3.3V_LAN with 10kΩ pull-up resistor.

NCSI_TXD1: NC-SI Transmit Data #1 Input, from external BMC to I210 Network Controller. Electrical level 3.3V_LAN with 10kΩ pull-up resistor.

NCSI_CRS_DV: NC-SI Carrier Sense/Receive Data Valid Output, from I210 Network Controller to external BMC. Electrical level 3.3V_LAN with 10kΩ pull-down resistor.

NCSI_TX_EN: NC-SI Transmit Enable Input, from external BMC to I210 Network Controller. Electrical level 3.3V_LAN with 10kΩ pull-down resistor.

NCSI_RX_ER: NC-SI Receive Error Output, managed by I210 GbE controller Software Definable Pin #2. Electrical level 3.3V_LAN with internal 30kΩ pull-up resistor.

NCSI_ARB_IN: NC-SI Hardware arbitration Input from external BMC to I210 Network Controller. Electrical level 3.3V_LAN

NCSI_ARB_OUT: NC-SI Hardware arbitration Output from I210 Network Controller to external BMC. Electrical level 3.3V_LAN

All these signals can be used to connect to a Baseboard management controller.

3.2.5.3 10Gb Ethernet signals

First introduced with COM Express Specifications Revision 3.0, the 10GBASE-KR support is available on COM Express modules Type 7, like COMe-C42-BT7.

Four different 10GBASE-KR interfaces are available, all of them managed by the AMD EPYC™ Embedded 3000 SoC.

Here following the signals involved in PCI express management

10G_KR_TX0+/10G_KR_TX0-: 10GBASE-KR port #0 Transmit output differential pair.

10G_KR_RX0+/10G_KR_RX0-: 10GBASE-KR port #0 Receive Input differential pair.

10G_KR_TX1+/10G_KR_TX1-: 10GBASE-KR port #1 Transmit output differential pair.

10G_KR_RX1+/10G_KR_RX1-: 10GBASE-KR port #1 Receive Input differential pair.

10G_KR_TX2+/10G_KR_TX2-: 10GBASE-KR port #2 Transmit output differential pair.

10G_KR_RX2+/10G_KR_RX2-: 10GBASE-KR port #2 Receive Input differential pair.

10G_KR_TX3+/10G_KR_TX3-: 10GBASE-KR port#3 Transmit output differential pair.

10G_KR_RX3+/10G_KR_RX3-: 10GBASE-KR port#3 Receive Input differential pair.

10G_PHY_MDIO_SDA0/10G_PHY_MDIO_SDA1/10G_PHY_MDIO_SDA2/10G_PHY_MDIO_SDA3: these four signals are all tied together. I2C Data signal of the 2-wire management interface used for serial data transfers between the MAC and an external PHY. 3.3V_ALW bidirectional signal with 2k2Ω pull-up resistor. Managed by EPYC™ Embedded 3000 I2C Port #1/SFP I2C Port.

10G_PHY_MDC_SCL0/10G_PHY_MDC_SCL1/10G_PHY_MDC_SCL2/10G_PHY_MDC_SCL3: these four signals are all tied together. I2C Clock signal of the 2-wire management interface used for serial data transfers between the MAC and an external PHY. 3.3V_ALW bidirectional signal with 2k2Ω pull-up resistor. Managed by EPYC™ Embedded 3000 I2C Port #1/SFP I2C Port

10G_PHY_CAP_01: PHY Mode capability input for lanes #0 and #1, electrical level 3.3V_ALW with 10kΩ pull-up resistor. Managed by the embedded controller.

10G_PHY_CAP_23: PHY Mode capability input for lanes #2 and #3, electrical level 3.3V_ALW with 10kΩ pull-up resistor. Managed by the embedded controller.

10G_SFP_SDA0: I2C data port #0 signal used by the 10GbE controller to access the registers of an external Optical SFP Module. 3.3V_ALW bidirectional signal with 2k2Ω pull-up resistor. Managed by EPYC™ Embedded 3000 I2C Port #1/SFP I2C Port through an on-module I2C Switch

10G_SFP_SCL0: I2C clock port #0 signal used by the 10GbE controller to access the registers of an external Optical SFP Module. 3.3V_ALW bidirectional signal with 2k2Ω pull-up resistor. Managed by EPYC™ Embedded 3000 I2C Port #1/SFP I2C Port through an on-module I2C Switch

10G_SFP_SDA1: I2C data port #1 signal used by the 10GbE controller to access the registers of an external Optical SFP Module. 3.3V_ALW bidirectional signal with 2k2Ω pull-up resistor. Managed by EPYC™ Embedded 3000 I2C Port #1/SFP I2C Port through an on-module I2C Switch

10G_SFP_SCL1: I2C clock port #1 signal used by the 10GbE controller to access the registers of an external Optical SFP Module. 3.3V_ALW bidirectional signal with 2k2Ω pull-up resistor. Managed by EPYC™ Embedded 3000 I2C Port #1/SFP I2C Port through an on-module I2C Switch

10G_SFP_SDA2: I2C data port #2 signal used by the 10GbE controller to access the registers of an external Optical SFP Module. 3.3V_ALW bidirectional signal with 2k2Ω pull-up resistor. Managed by EPYC™ Embedded 3000 I2C Port #1/SFP I2C Port through an on-module I2C Switch

10G_SFP_SCL2: I2C clock port #2 signal used by the 10GbE controller to access the registers of an external Optical SFP Module. 3.3V_ALW bidirectional signal with 2k2Ω pull-up resistor. Managed by EPYC™ Embedded 3000 I2C Port #1/SFP I2C Port through an on-module I2C Switch

10G_SFP_SDA3: I2C data port #3 signal used by the 10GbE controller to access the registers of an external Optical SFP Module. 3.3V_ALW bidirectional signal with 2k2Ω pull-up resistor. Managed by EPYC™ Embedded 3000 I2C Port #1/SFP I2C Port through an on-module I2C Switch

10G_SFP_SCL3: I2C clock port #3 signal used by the 10GbE controller to access the registers of an external Optical SFP Module. 3.3V_ALW bidirectional signal with 2k2Ω pull-up resistor. Managed by EPYC™ Embedded 3000 I2C Port #1/SFP I2C Port through an on-module I2C Switch

10G_LED_SDA: I2C dedicated data port to transfer LED signals and PHY straps for I2C or MDIO operation of optical PHYs. 3.3V_ALW bidirectional signal with 2k2Ω pull-up resistor. Managed by EPYC™ Embedded 3000 I2C Port #1/SFP I2C Port

10G_LED_SCL: I2C dedicated clock port to transfer LED signals and PHY straps for I2C or MDIO operation of optical PHYs. 3.3V_ALW bidirectional signal with 2k2Ω pull-up resistor. Managed by EPYC™ Embedded 3000 I2C Port #1/SFP I2C Port

10G_INT0: Interrupt pin for xGbE port #0. 3.3V_ALW input signal with 2k2Ω pull-up resistor. Managed through the on-module I2C I/O Expander

10G_INT1: Interrupt pin for xGbE port #1. 3.3V_ALW input signal with 2k2Ω pull-up resistor. Managed through the on-module I2C I/O Expander

10G_INT2: Interrupt pin for xGbE port #2. 3.3V_ALW input signal with 2k2Ω pull-up resistor. Managed through the on-module I2C I/O Expander

10G_INT3: Interrupt pin for xGbE port #3. 3.3V_ALW input signal with 2k2Ω pull-up resistor. Managed through the on-module I2C I/O Expander

10G_PHYRST_01: Output signal to reset optical PHYs on XGbE ports #0 and/or #1. 3.3V_ALW output signal, managed through the on-module I2C I/O Expander.

10G_PHYRST_23: Output signal to reset optical PHYs on XGbE ports #2 and/or #3. 3.3V_ALW output signal, managed through the on-module I2C I/O Expander.

Please refer to COM Express specifications about possible implementations of XGbE interfaces on the carrier board.

3.2.5.4 S-ATA signals

The AMD EPYC™ Embedded 3000 family of SOCs offers up to eight S-ATA interfaces. According to COM Express requirements for Type 7 modules, two of these interfaces are made available on connector AB.

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.

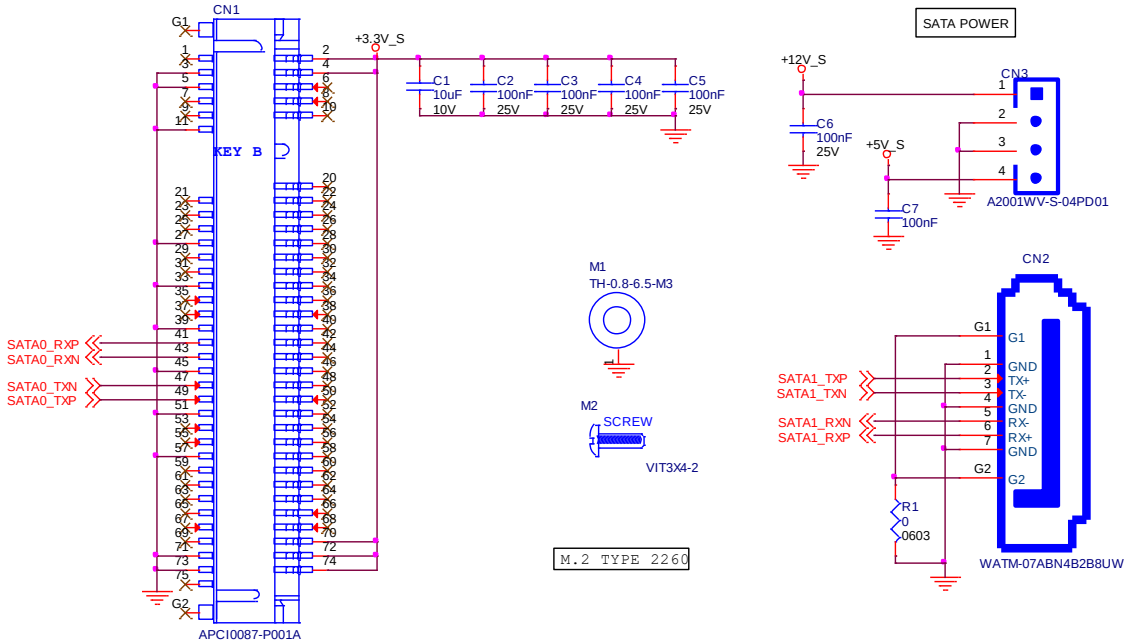
SATA0_RX+/SATA0_RX-: Serial ATA Channel #0 Receive differential pair.

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

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

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, where are shown the implementations for a M.2 Key B SATA module and for a standard SATA Male 7 poles connector.



3.2.5.5 PCI Express interface signals

COMe-C42-BT7 offers externally twenty-four PCI Express lanes, which are managed by the AMD EPYC™ Embedded 3000 family of SOCs.

PCI express Gen 3 (8.0GT/s) is supported.

The eight PCI-e lanes from #0 to #7 can be grouped to form any possible combination of PCI-e x8, PCI-e x4, PCI-e x2 and PCI-e x1 ports, with the limit of a maximum 7 root ports. Grouping selection is made via BIOS, please check par. 4.3.8 (Bucket 1 configuration).

The sixteen PCI-e lanes from #16 to #31 can be grouped to form any possible combination of PCI-e x8, PCI-e x4, PCI-e x2 and PCI-e x1 ports, with the limit of a maximum 8 root ports. Grouping selection is made via BIOS, please check par. 4.3.8 (Bucket 3-4 configuration).

Here following the signals involved in PCI express management:

PCIE_TX0+/PCIE_TX0-/PCIE_RX0+/PCIE_RX0-: PCI Express lane #0, Transmitting Output and Receiving Input Differential pairs

PCIE_TX1+/PCIE_TX1-/PCIE_RX1+/PCIE_RX1-: PCI Express lane #1, Transmitting Output and Receiving Input Differential pairs

PCIE_TX2+/PCIE_TX2-/PCIE_RX2+/PCIE_RX2-: PCI Express lane #2, Transmitting Output and Receiving Input Differential pairs

PCIE_TX3+/PCIE_TX3-/PCIE_RX3+/PCIE_RX3-: PCI Express lane #3, Transmitting Output and Receiving Input Differential pairs

PCIE_TX4+/PCIE_TX4-/PCIE_RX4+/PCIE_RX4-: PCI Express lane #4, Transmitting Output and Receiving Input Differential pairs

PCIE_TX5+/PCIE_TX5-/PCIE_RX5+/PCIE_RX5-: PCI Express lane #5, Transmitting Output and Receiving Input Differential pairs

PCIE_TX6+/PCIE_TX6-/PCIE_RX6+/PCIE_RX6-: PCI Express lane #6, Transmitting Output and Receiving Input Differential pairs

PCIE_TX7+/PCIE_TX7-/PCIE_RX7+/PCIE_RX7-: PCI Express lane #7, Transmitting Output and Receiving Input Differential pairs

PCIE_TX16+/PCIE_TX16-/PCIE_RX16+/PCIE_RX16-: PCI Express lane #16, Transmitting Output and Receiving Input Differential pairs

PCIE_TX17+/PCIE_TX17-/PCIE_RX17+/PCIE_RX17-: PCI Express lane #17, Transmitting Output and Receiving Input Differential pairs

PCIE_TX18+/PCIE_TX18-/PCIE_RX18+/PCIE_RX18-: PCI Express lane #18, Transmitting Output and Receiving Input Differential pairs

PCIE_TX19+/PCIE_TX19-/PCIE_RX19+/PCIE_RX19-: PCI Express lane #19, Transmitting Output and Receiving Input Differential pairs

PCIE_TX20+/PCIE_TX20-/PCIE_RX20+/PCIE_RX20-: PCI Express lane #20, Transmitting Output and Receiving Input Differential pairs

PCIE_TX21+/PCIE_TX21-/PCIE_RX21+/PCIE_RX21-: PCI Express lane #21, Transmitting Output and Receiving Input Differential pairs

PCIE_TX22+/PCIE_TX22-/PCIE_RX22+/PCIE_RX22-: PCI Express lane #22, Transmitting Output and Receiving Input Differential pairs

PCIE_TX23+/PCIE_TX23-/PCIE_RX23+/PCIE_RX23-: PCI Express lane #23, Transmitting Output and Receiving Input Differential pairs

PCIE_TX24+/PCIE_TX24-/PCIE_RX24+/PCIE_RX24-: PCI Express lane #24, Transmitting Output and Receiving Input Differential pairs

PCIE_TX25+/PCIE_TX25-/PCIE_RX25+/PCIE_RX25-: PCI Express lane #25, Transmitting Output and Receiving Input Differential pairs

PCIE_TX26+/PCIE_TX26-/PCIE_RX26+/PCIE_RX26-: PCI Express lane #26, Transmitting Output and Receiving Input Differential pairs

PCIE_TX27+/PCIE_TX27-/PCIE_RX27+/PCIE_RX27-: PCI Express lane #27, Transmitting Output and Receiving Input Differential pairs

PCIE_TX28+/PCIE_TX28-/PCIE_RX28+/PCIE_RX28-: PCI Express lane #28, Transmitting Output and Receiving Input Differential pairs

PCIE_TX29+/PCIE_TX29-/PCIE_RX29+/PCIE_RX29-: PCI Express lane #29, Transmitting Output and Receiving Input Differential pairs

PCIE_TX30+/PCIE_TX30-/PCIE_RX30+/PCIE_RX30-: PCI Express lane #30, Transmitting Output and Receiving Input Differential pairs

PCIE_TX31+/PCIE_TX31-/PCIE_RX31+/PCIE_RX31-: PCI Express lane #31, Transmitting Output and Receiving Input Differential pairs

PCIE_CLK_REF+/ PCIE_CLK_REF-: PCI Express 100MHz Reference Clock, Differential Pair. Please consider that only one reference clock is supplied, while it is possible to manage up to fifteen root ports using the tweny-four PCI-e lanes. When more than one PCI Express root port is used on the carrier board, then a zero-delay buffer must be used to replicate the reference clock to all the devices.

3.2.5.6 USB interface signals

The AMD EPYC™ Embedded 3000 family of SOCs supports USB 2.0 and USB 3.1 Gen1 interfaces, up to four ports are supported. All of these are carried out on COM Express connectors (USB 2.0 related signals are carried to connector AB, while USB Superspeed signals, necessary to complete USB 3.1 functionalities, are carried to connector CD.

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_0+/USB_0-: Universal Serial Bus Port #0 bidirectional differential pair

USB_1+/USB_1-: Universal Serial Bus Port #1 bidirectional differential pair

USB_2+/USB_2-: Universal Serial Bus Port #2 bidirectional differential pair

USB_3+/USB_3-: Universal Serial Bus Port #3 bidirectional differential pair

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

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

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

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

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

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

USB_SSRX3+/USB_SSRX3-: USB Super Speed Port #3 receive differential pair

USB_SSTX3+/USB_SSTX3-: USB Super Speed Port #3 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 of COMe-C42-BT7 module

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 of COMe-C42-BT7 module.

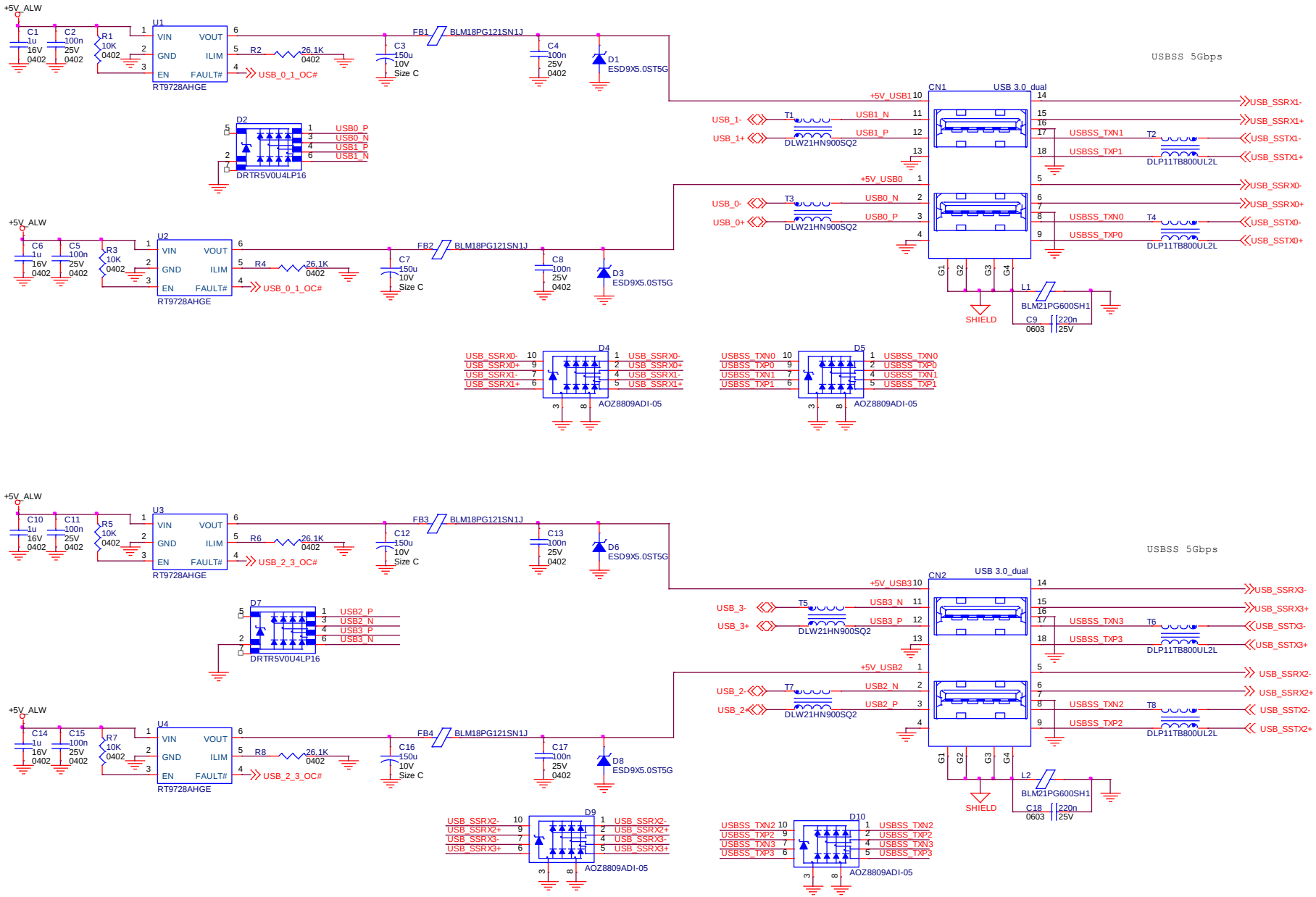
220nF AC series decoupling capacitors are placed on each transmitting line of USB Super speed differential pairs.

330nF AC series decoupling capacitors are placed on each receiving 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 2.0 port #0, #1, #2 and #3 along with the corresponding Superspeed USB ports, are all 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_ALW
U1
RT9728AHGE
VIN
VOUT
GND
ILIM
EN
FAULT#
C1 1u 16V 0402
C2 100n 25V 0402
R1 10K 0402
R2 26.1K 0402
USB_0_1_OC#
C3 150u 10V Size C
FB1 BLM18PG121SN1J
C4 100n 25V 0402
D1 ESD9X5.0ST5G
D2 DRTR5V0U4LP16
USB0_P
USB0_N
USB1_P
USB1_N
USBSS 5Gbps
CN1 USB 3.0_dual
+5V_USB1
+5V_USB0
USB_1-
USB_1+
USB_0-
USB_0+
T1 DLW21HN900SQ2
T3 DLW21HN900SQ2
USBSS_TXN1
USBSS_TXP1
USBSS_TXN0
USBSS_TXP0
T2 DLP11TB800UL2L
T4 DLP11TB800UL2L
USB_SSRX1-
USB_SSRX1+
USB_SSTX1-
USB_SSTX1+
USB_SSRX0-
USB_SSRX0+
USB_SSTX0-
USB_SSTX0+
G1
G2
G3
G4
SHIELD
L1 BLM21PG600SH1
C9 220n 25V 0603
U2
C6 1u 16V 0402
C5 100n 25V 0402
R3 10K 0402
R4 26.1K 0402
C7 150u 10V Size C
FB2 BLM18PG121SN1J
C8 100n 25V 0402
D3 ESD9X5.0ST5G
D4 AOZ8809ADI-05
D5 AOZ8809ADI-05
USB_SSRX0-
USB_SSRX0+
USB_SSRX1-
USB_SSRX1+
USBSS_TXN0
USBSS_TXP0
USBSS_TXN1
USBSS_TXP1
U3
C10 1u 16V 0402
C11 100n 25V 0402
R5 10K 0402
R6 26.1K 0402
USB_2_3_OC#
C12 150u 10V Size C
FB3 BLM18PG121SN1J
C13 100n 25V 0402
D6 ESD9X5.0ST5G
D7 DRTR5V0U4LP16
USB2_P
USB2_N
USB3_P
USB3_N
CN2 USB 3.0_dual
+5V_USB3
+5V_USB2
USB_3-
USB_3+
USB_2-
USB_2+
T5 DLW21HN900SQ2
T7 DLW21HN900SQ2
USBSS_TXN3
USBSS_TXP3
USBSS_TXN2
USBSS_TXP2
T6 DLP11TB800UL2L
T8 DLP11TB800UL2L
USB_SSRX3-
USB_SSRX3+
USB_SSTX3-
USB_SSTX3+
USB_SSRX2-
USB_SSRX2+
USB_SSTX2-
USB_SSTX2+
L2 BLM21PG600SH1
C18 220n 25V 0603
U4
C14 1u 16V 0402
C15 100n 25V 0402
R7 10K 0402
R8 26.1K 0402
C16 150u 10V Size C
FB4 BLM18PG121SN1J
C17 100n 25V 0402
D8 ESD9X5.0ST5G
D9 AOZ8809ADI-05
D10 AOZ8809ADI-05
USB_SSRX2-
USB_SSRX2+
USB_SSRX3-
USB_SSRX3+
USBSS_TXN2
USBSS_TXP2
USBSS_TXN3
USBSS_TXP3

3.2.5.7 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 COMe-C42-BT7 module 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, 50kΩ internal 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 with 10kΩ pull-up resistor. 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 4k7Ω pull-up resistor. This signal is used only by peripherals requiring Interrupt support.

LPC_DRQ0#: LPC Serial DMA Request, +3.3V_RUN electrical level with 10kΩ pull-up resistor.

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. When BIOS_DIS0# is high and BIOS_DIS1# is low, the module will attempt to boot using SPI flashes placed on the carrier board. In all other cases, the module will boot from internal SPI Flash

3.2.5.8 SPI interface signals

The AMD EPYC™ Embedded 3000 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.

3.2.5.9 UART interface signals

According to COM Express® Rel. 3.0 specifications, since the COMe-C42-BT7 is a Type 6 module, it can offer two UART interfaces, which are managed by the embedded controller.

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.

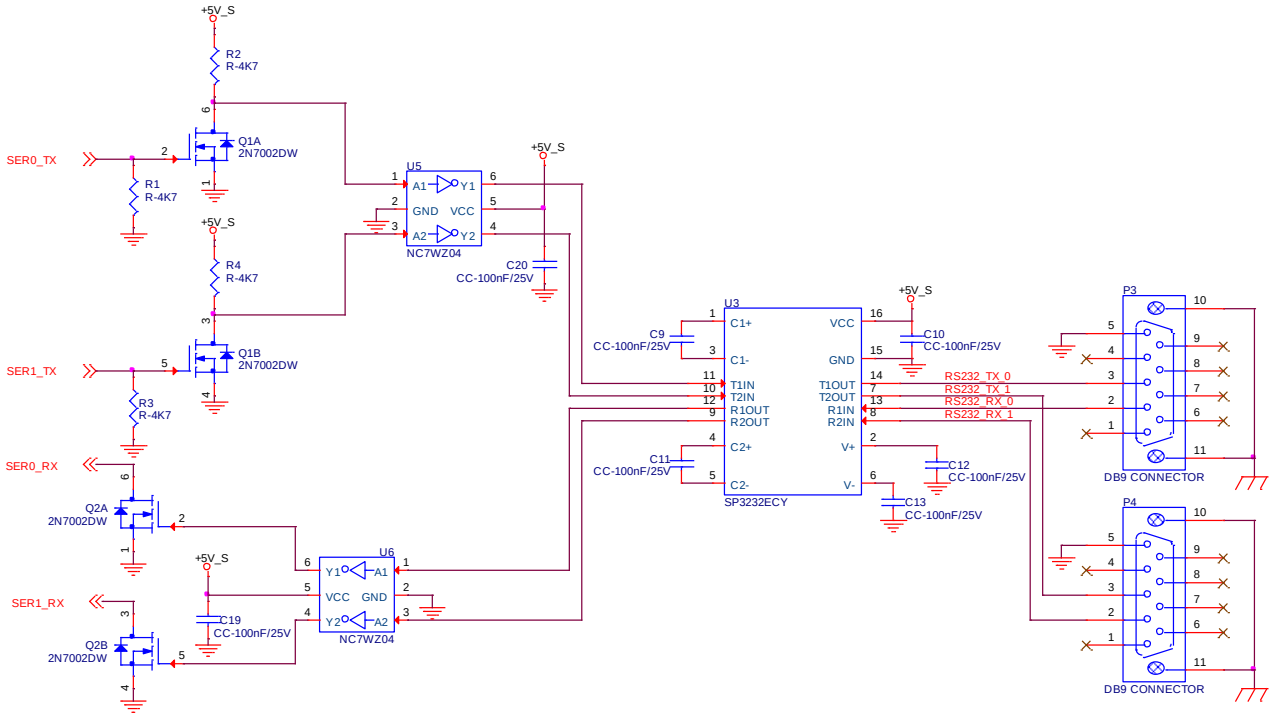
SER1_TX: UART Interface #1, Serial data Transmit (output) line, 3.3V_RUN electrical level.

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 +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 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 right shows an example of implementation of RS-232 transceiver for the Carrier board.



3.2.5.10 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.

3.2.5.11 Miscellaneous signals

Here following, a list of COM Express® compliant signals that complete the features of COMe-C42-BT7 module.

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 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_RUN voltage output signal with 4k7Ω pull-up resistor. 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.

3.2.5.12 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 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 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 COMe-C42-BT7 module.

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 with 100kΩ pull-up resistor. 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. 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_S4#, 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# and SUS_S5# are internally connected together.

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', WAKE1#signal is managed by the Embedded microcontroller.

LID# *: LID button Input, active low +3.3V_ALW electrical level signal, with 10kΩ 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 10kΩ 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 +12V_{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.

3.2.5.13 SMBus signals

This interface is managed by the Embedded Controller.

Signals involved are the following:

SMB_CK: SM Bus control clock line for System Management. Bidirectional signal, electrical level +3.3V_ALW with a 2k2Ω pull-up resistor.

SMB_DAT: SM Bus control data line for System Management. Bidirectional signal, electrical level +3.3V_ALW with a 2k2Ω 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.

3.2.5.14 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
- Event Logs 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.

Please remember that COMe-C42-BT7 module doesn’t offer integrated video interface. The Setup utility therefore can be controlled using the redirection on Serial Port or using an external PCI-e Video Card.

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
AMD CBS	See submenu	Common items for configuration of AMD module-related information
iSCSI Configuration	See submenu	Internet SCSI configuration
Intel® I21x Gigabit Network Connections - *MAC Address*	See submenu	1GbE controller parameters
Battery Failure Manager	See submenu	Module's Behaviour for Battery Failure
Trusted Computing	See submenu	Trusted Computing Settings
PSP Firmware Versions	See submenu	Informative screen only
ACPI Settings	See submenu	System ACPI parameters
Board Parameters Settings	See submenu	PCIe root ports stings
S5 RTC Wake Settings	See submenu	Enable System to wake from S5 using RTC alarm
Serial Port Console Redirection	See submenu	Configures Console Redirection on Serial Port
CPU Configuration	See submenu	CPU Configuration Parameters
PCI Subsystem Settings	See submenu	PCI Subsystem Settings
USB Configuration	See submenu	USB Configuration Parameters
Network Stack Configuration	See submenu	Network Stack Settings
CSM Configuration	See submenu	Compatibility Support Module (CSM) Configuration: Enable/Disable, Option ROM execution Settings, etc...
NVMe Configuration	See submenu	NVMe Device Options Settings
SATA configuration	See submenu	SATA Device Options Settings
Main Thermal Configuration	See submenu	Main thermal Configuration Parameters
SMBIOS Information	See submenu	SMBIOS Information
Embedded Controller	See submenu	Embedded Controller Parameters

4.3.1 AMD CBS Configuration submenu

Menu Item	Options	Description
Zen Common Options	See Submenu	Sets Zen Common Options
DF Common Options	See Submenu	Sets Data Fabric (DF) Common Options
UMC Common Options	See Submenu	Sets Unified Memory Controller (UMC) Common Options
NBIO Common Options	See Submenu	Sets Northbridge IO (NBIO) Common Options
FCH Common Options	See Submenu	Sets FCH Common Options
NTB Common Options	See Submenu	Sets NTB Common Options

4.3.1.1 Zen Common Options submenu

Menu Item	Options	Description
RedirectForReturnDis	Auto / 1 / 0	Derived from a Workaround for GCC compiler, issue C000005 for Xv Core on CZ A0, allows setting MSRC001_1029 Decode Configuration bit 14 [DecfgNoRdrctForReturns] to1
L2 TLB Associativity	Auto / 1 / 0	Allow setting if L2 TLB on ways [11:8] must be fully associative (value 0) or 4K only associative. (value 1).
Platform First Error Handling	Enabled / Disabled / Auto	Enables or disables the PFEH (Platform First Error Handling), cloak individual banks and mask deferred error interrupts from each bank.
Core Performance Boost	Auto / Disabled	Allows disabling the Core Performance Boost (CPB)
Enable IBS	Enabled / Disabled / Auto	Enables or disables Instruction Based Sampling (IBS)
Global C-State Control	Enabled / Disabled / Auto	Controls IO based C-State generation and Data Fabric (DF) C-States
Opcache Congtrol	Enabled / Disabled / Auto	Enables or Disables the Opcache.
SEV-ES ASID Space Limit	1..16	SEV Virtual Machines using Address Space Identifiers (ASIDs) below the SEV-ES ASID Space Limit must enable the SEV-ES feature. The valid values for this field are from 0x1 (1) to 0x10 (16).
Core Thread Enablement	See Submenu	Allows Enables individual Core and Thread management
Streaming Stores Control	Enabled / Disabled / Auto	Enables or disables the streaming stores functionality.
Prefetches setting	See submenu	Settings for Hardware pre-fetcher

4.3.1.1.1 Core Thread Enablement Submenu

Menu Item	Options	Description
Disagree		By Selecting Disagree, you will return to previous menu 4.3.1.1
Agree		By selecting Agree, the following menu items will appear (additional submenu)
Downcore control	ONE (1+0) TWO (1+1) TWO (2+0) THREE (3+0) FOUR (2+2) FOUR (4+0) SIX (3+3) AUTO	Sets the number of cores to be used. Once this option has been changed, a POWER CYCLE is required in order for future selection to make effect.)
SMTEN	Disable / Auto	Can be used to disable symmetric Multithreading (SMT). To re-enable SMT, a power cycle is need after selecting the 'Auto' Option. Warning – S3 IS NOT SUPPORTED on systems where cores/threads have been removed or disabled.

4.3.1.1.2 Prefetcher Setting Submenu

Menu Item	Options	Description
L1 Stream HW Prefetcher	Enabled / Disabled / Auto	Allows enabling or disabling L1 Stream's Hardware prefetcher
L2 Stream HW Prefetcher	Enabled / Disabled / Auto	Allows enabling or disabling L2 Stream's Hardware prefetcher

4.3.1.2 DF Common Options submenu

Menu Item	Options	Description
DRAM scrub time	1 hour / 4 hours / 8 hours / 16 hours / 24 hours / 48 hours / Auto/ Disabled	Allows setting the frequency (hours) for DRAM scrubbing, i.e. memory reading and error correcting, or to disable it.
Redirect scrubber control	Enabled / Disabled / Auto	Enables or disables redirect scrubs to correct single-bit correctable errors in a cache line.

Disable DF sync flood propagation	Sync flood disabled Sync flood enabled Auto	Configures Sync flood propagation to all DF components.
Freeze DF module queues on error	Enabled / Disabled / Auto	Enables or disables the Sync flood propagation on Fatal errors.
GMI encryption control	Enabled / Disabled / Auto	Enables or disables Global Memory Interconnect (GMI) Link encryption
xGMI encryption control	Enabled / Disabled / Auto	Enables or disables external GMI (xGMI) Link encryption
CC6 memory region encryption	Enabled / Disabled / Auto	Controls whether the CC6 save/restore memory is encrypted.
Location of private memory regions	Distributed / Consolidated / Auto	Controls whether the private memory regions (Platform Security Processor, System Management Unit and CC6) are at the top of DRAM or distributed. Please notice that “distributed” requires memory an all dies.
System probe filter	Enabled / Disabled / Auto	Controls whether the probe filter is enabled. Has no effect on parts where the probe filter is fuse disabled
Memory interleaving	None / Channel / Die / Socket / Auto	Controls the fabric level memory interleaving (automatic, no interleaving, channel / die/ socket interleaving. Note that channel, die and socket has specific requirement on memory populations and it will be ignored if the memory doesn’t support the selected option.
Memory interleaving Size	256 Bytes/ 512 Bytes / 1KB / 2KB / Auto	Controls the memory interleaving size. The valid values are Auto, 256 Bytes, 512 Bytes, 1 Kbytes or 2Kbytes. This determines the starting address of the interleave (bit 8, 9, 10 or 11),
Channel interleaving hash	Enabled / Disabled / Auto	Controls whether the address bits are hashed during channel interleave mode. This field should not be used unless the interleaving is set to “Channel” and the “Memory interleaving size” is 256 or 512 bytes.
Memory Clear	Enabled / Disabled / Auto	When this feature is disabled, BIOS does not implement MemClear after memory training (only if non-ECC DIMMs are used).
1TB remap	Do not remap Attempt to remap Auto	Attempt to remap DRAM out of the space just below the 1TB boundary. The ability to remap depends on DRAM confirguation and interleaving selection, and may not always be possible.
ACPI SRAT below 1MB reporting mode	Do not report Report as DRAM Auto	Controls whether 0xA0000 – 1MB is reported as DRAM in the Static Resource Affinity Table (SRAT).

4.3.1.3 UMC Common Options submenu

Menu Item	Options	Description
DDR4 Common Options	See submenu	Allows selecting Common options for DDR4
DRAM Memory Mapping	See submenu	Allows selecting Memory Mapping parameters
Memory MBIST	See submenu	Allows selecting Memory Built-In Self Test (MBIST) parameters

4.3.1.3.1 DDR4 Common Options Submenu

Menu Item	Options	Description
DRAM Timing Configuration	See submenu	Allows setting DRAM Timing parameters
DRAM Controller Configuration	See submenu	Allow configuring the DRAM Controller
Data Bus Configuration	See submenu	Allow configuring specific parameters for DRAM data Bus
Common RAS	See submenu	Allows setting common RAS parameters
Security	See submenu	DRAM Security Parameters

4.3.1.3.1.1 DRAM Timing Configuration Submenu

This menu allows setting specific DRAM timing parameters, whose manual configuration could however lead to faults not covered by manufacturer's warranty. For this reason, the first screen will show a Disclaimer asking to Decline the responsibility or to accept it.

By declining, you will return at the menu described at 4.3.1.3.1, by accepting it, the following menu items will appear.

Menu Item	Options	Description
Overclock	Auto / Enabled	Memory clock and overclock setting. By enabling it, all the following menu items will appear
Memory Clock Speed	333MHz / 400MHz / 533MHz / 667MHz / 800MHz / 933MHz / 1050MHz / 1066MHz / 1067MHz / 1200MHz / 1333MHz / 1467MHz / Auto	Set the memory clock frequency
Tcl	Auto / 08h Clk .. 21h Clk	Sets the tCL time.

Trcdrd	Auto / 08h Clk .. 1Ah Clk	Sets the RAS# Active to CAS# read delay.
Trcdwr	Auto / 08h Clk .. 1Bh Clk	Sets the RAS# Active to CAS# write delay.
Trp	Auto / 08h Clk .. 1Bh Clk	Specify the row precharge time.
Tras	Auto / 15h Clk .. 3Ah Clk	Specify the min RAS# active time.
Trc Ctrl	Auto /Manual	Specify Trc set mode. When set to Manual, the following menu item will appear
Trc	*Hex value*	Active to Active / Refresh Delay Time. Valid values 87h-1Dh
TrrdS	Auto / 04h Clk .. 0Ch Clk	Activate to Activate Delay Time, different bank group (tRRD_S)
TrrdL	Auto / 04h Clk .. 0Ch Clk	Activate to Activate Delay Time, same bank group (tRRD_L)
Tfaw Ctrl	Auto /Manual	Specify Tfaw set mode. When set to Manual, the following menu item will appear
TfaW	*Hex value*	Four Activate Window Time. Valid Values 36h-6h
TwtrS	Auto / 02h Clk .. 0Eh Clk	Minimum Write to Read Time, different bank group
TwtrL	Auto / 02h Clk .. 0Eh Clk	Minimum Write to Read Time, same bank group
Twr Ctrl	Auto / Manual	Specify Twr set mode. When set to Manual, the following menu item will appear
Twr	*Hex value*	Minimum Write Recovery Time. Valid vale 51h-Ah
Trcpage Ctrl	Auto / Manual	Specify Trcpage set mode. When set to Manual, the following menu item will appear
Tcrpage	*Hex value*	SDRAM Optional Features (tMAW, MAC). Valid value 3FFh – 0h
TrdrdScL Ctrl	Auto / Manual	Specify TrdrdScLset mode. When set to Manual, the following menu item will appear
TrdrdScL	*Hex value*	CAS to CAS Delay Time, same bank group. Valid values Fh – 1h
TwrwrScL Ctrl	Auto / Manual	Specify TwrwrScL set mode. When set to Manual, the following menu item will appear
TwrwrScL	*Hex value*	CAS to CAS Delay Time, same bank group. Valid values Fh – 1h
Trfc Ctrl	Auto / Manual	Specify Trfc set mode. When set to Manual, the following menu item will appear
Trfc	*Hex value*	Refresh Recovery Delay Time (tRFC1). Valid values 3DEh-3Ch
Trfc2 Ctrl	Auto / Manual	Specify Trfc2 set mode. When set to Manual, the following menu item will appear
Trfc2	*Hex value*	Refresh Recovery Delay Time (tRFC2). Valid values 3DEh-3Ch
Trfc4 Ctrl	Auto / Manual	Specify Trfc4 set mode. When set to Manual, the following menu item will appear

Trfc4	*Hex value*	Refresh Recovery Delay Time (tRFC4). Valid values 3DEh-3Ch
ProcODT	Auto / High Impedance / 480 ohm / 240 ohm / 160 ohm / 120 ohm / 96 ohm / 80 ohm / 68.6 ohm / 60 ohm / 53.3 ohm / 48 ohm / 43.6 ohm / 40 ohm / 36.9 ohm / 34.3 ohm / 32 ohm / 30 ohm	Specifies the Processor On-Die Termination (ODT)
Tcwl	Auto / 09h Clk .. 16h Clk	
Trtp	Auto / 05h Clk .. 0Eh Clk	Specifies the read CAS# to precharge time.
Trdwr	Auto / 01h Clk .. 1Fh Clk	Specifies the tWRTTO time.
Twrrd	Auto / 01h Clk .. 0Fh Clk	Specifies the write to read delay when accessing differemy DIMMs-
TwrwrSc	Auto / 01h Clk .. 0Fh Clk	Write-to-write timing, same chip select
TwrwrSd	Auto / 01h Clk .. 0Fh Clk	Write-to-write timing, same DIMM
TwrwrDd	Auto / 01h Clk .. 0Fh Clk	Write-to-write timing, different DIMM
TrdrdSc	Auto / 01h Clk .. 0Bh Clk	Read-to-read timing, same chip select
TrdrdSd	Auto / 01h Clk .. 0Fh Clk	Read-to-read timing, same DIMM
TrdrdDd	Auto / 01h Clk .. 0Fh Clk	Read-to-read timing, different DIMM
Tcke	Auto / 01h Clk .. 1Fh Clk	Specifies the CKE minimum high and low pulse width in memory clock cycles.

4.3.1.3.1.2 DRAM Controller Configuration Submenu

Menu Item	Options	Description
DRAM Power Options	See submenu	Allows, in the subsequent submenu, to enable or disable DDR Power down mode
Cmd2T	1T / 2T / Auto	Select the Address / Command rate between 1T and 2T
Gear Down Mode	Auto / Disabled /Enabled	Allow enabling or disabling the Gear Down Mode, which allows the memory to run at half speed some of the time.

4.3.1.3.1.3 Data Bus Configuration Submenu

Menu Item	Options	Description
Data Bus Configuration User Controls	Auto / Manual	Specify the mode of drive strength. When set to Manual , the following items will appear
RttNom	Rtt_Nom Disable / Auto / RZQ/4 / RZQ/2 / RZQ/6 / RZQ/1 / RZQ/5 / RZQ/3 / RZQ/7	
RttWr	Dynamic ODT Off / Auto / RZQ/2 / RZQ/1 / RZQ/3 / Hi-Z	
RttPark	Rtt_PARK Disable / Auto / RZQ/4 / RZQ/2 / RZQ/6 / RZQ/1 / RZQ/5 / RZQ/3 / RZQ/7	

4.3.1.3.1.4 Common RAS Submenu

Menu Item	Options	Description
Data Poisoning	Auto / Disabled /Enabled	Enables or disables Data poisoning
RCD Parity	Auto / Disabled /Enabled	Enables or Disables Register Command Driver (RCD) Parity
DRAM Address Command Parity Retry	Auto / Disabled /Enabled	Enables or disables the retry on Address or Command Parity Error. When enabled, the following item can be changed
Max Parity Error Replay	*Hex Value*	Numbers of retries possible. Value in hexadecimal, range 0 ..3F. 1, 2, or 3 are invalid.
Write CRC Enable	Auto / Disabled /Enabled	Enables or disables the Write Cyclic Redundancy Check (CRC) transmission
Disable Memory Error Injection	False / True	Allows disabling the Memory Error Injection used to check ECC functionality
ECC Configuration	See Submenu	ECC Configuration parameters

4.3.1.3.1.4.1 ECC Configuration Submenu

Menu Item	Options	Description
DRAM ECC Symbol Size	x4 / x8 / Auto	Specifies the size in bits of ECC Symbol
DRAM ECC Enable	Auto / Disabled /Enabled	Use this option to enable / disable DRAM ECC. Auto will set ECC to enabled.

4.3.1.3.1.5 Security Submenu

Menu Item	Options	Description
TSME	Auto / Disabled /Enabled	Enables or disables Transparent Security Memory Encryption (TSME)
Data Scramble	Auto / Disabled /Enabled	Enables or disables Data scrambling

4.3.1.3.2 DRAM Memory Mapping Submenu

Menu Item	Options	Description
Chipselect Interleaving	Auto / Disabled	Interleave memory blocks across the DRAM chip selects for node 0.
BankGroupSwap	Auto / Disabled /Enabled	Enables or disables the BankGroupSwap functionality
BankGroupSwapAlt	Auto / Disabled /Enabled	Enables or disables the BankGroupSwapAlt functionality
Address Hash Bank	Auto / Disabled /Enabled	Enables or disables bank address hashing
Address Hash CS	Auto / Disabled /Enabled	Enables or disables CS address hashing

4.3.1.3.3 Memory MBIST Submenu

Menu Item	Options	Description
MBIST Enable	Disabled / Enabled	Enables or disables Memory BIST. Whenn disabled, all following items will be grayed out
MBIST Test mode	Interface Mode Data Eye Mode	Selects MBIST Test Mode. Interface Mode: tests single and multiple CS transactions and basic connectivity Data Eye mode: measures voltage vs. timings
MBIST Aggressors	Auto / Disabled /Enabled	Enables or disables MBITS Aggressor test
MBIST per Bit Slave Die Reporting	Auto / Disabled /Enabled	Allows reporting of 2D Data Eye results in ABL Log for each DQ, Chipselect and Channel

4.3.1.4 NBIO Common Options submenu

Menu Item	Options	Description
NB Configuration	See submenu	NB Configuration parameters
NBIO Internal Poison Consumption	Auto / Disabled /Enabled	Enables or disables Internal Poison consumption
NBIO RAS Control	Auto / Disabled /Enabled	Enables or disables the NBIO RAS Control
Determinism Slider	Auto / Power / Performance	Sets the operating mode of the processor. When set to Performance, the processor processor will run at the best performance with little deviations. When set to Power, the processor will run at the maximum allowable performance on a per die basis.
cTDP Control	Auto / Manual	Alows setting manually the configurable TDP (cTDP) or use the fused one. When set to manual, the following item will appear
cTDP	*Numerical Value*	Allows setting manually the cTDP value, with 0 = Invalid Value
Fan Control	See submenu	Fan control menu
PSI	Auto / Disabled	Allows disabling Power Status Indicator (PSI).
ACS Enable	Auto / Disabled /Enabled	Enables the PCI Express Access Control Services (ACS)
PCIe ARI Support	Auto / Disabled /Enabled	Enables Alternative Routing-ID Interpretation (ARI)
CLDO_VDDP Control	Auto / Manual	Allows setting automatically or manually a customized CLDO_VPP voltage (i.e. the voltage for the DDR4 PHY on the SoC)
CLDO_VPP	*Numerical Value*	Value in mV for CLDO_VPP. Upon changing this value, it is necessary a cold rest of the system in order to re-latch the CLDOs, otherwise the changes will not take into effect.
Block PCIe Loopback	Auto / Disabled /Enabled	Blocks PCIe loopback mode for hot plug slots
CRS Delay	*Numerical Value*	Configuration Request Retry Status (CRS) Delay for hot plug ports
CRS Limit	*Numerical Value*	CRS Limit for hot plug ports
Hot Plug Flags	See submenu	

4.3.1.4.1 NB Configuration submenu

Menu Item	Options	Description
IOMMU	Auto / Disabled /Enabled	Allows enabling or disabling the Input–output memory management unit (IOMMU)
Concurrent Training	Auto / True / False	Enables or disables concurrent training

4.3.1.4.2 Fan Control submenu

Menu Item	Options	Description
Fan Control	Auto / Manual	Auto: sets the default fan controller settings. Manual: the user can set customized fan controller settings
Force PWM Control	Force / Unforce	Unforce: do not force the FAN PWM. Force: forces the FAN PWM to use the specified value
Force PWM	0..100	Specify the PWM Duty cycle to force the fan to.
Fan Table Control	Auto / Manual	Auto: Use the default fan Table. Manual: use the following customized fan table
Low temperature	*Numerical Value*	Low Temperature (°C)
Medium temperature	*Numerical Value*	Medium Temperature (°C)
High temperature	*Numerical Value*	High Temperature (°C)
Critical temperature	*Numerical Value*	Critical Temperature (°C)
Low PWM	0..100	PWM at Low temperature
Medium PWM	0..100	PWM at Medium temperature
High PWM	0..100	PWM at High temperature
Temperature Hysteresis	*Numerical Value*	Temperature Hysteresis (°C)
PWM frequency	25kHz / 100kHz	Sets the PWM Frequency
Fan Polarity	Negative / Positive	Sets the Fan polarity

4.3.1.4.3 Hot Plug flags submenu

Menu Item	Options	Description
Ignore sideband	Auto / Disabled /Enabled	Disable sideband
Disable L1 w/a	Auto / Disabled /Enabled	Disable L1 w/a
Disable BridgeDis	Auto / Disabled /Enabled	No BridgeDis update based on sideband
Toggle RRC Enable	Auto / Disabled /Enabled	Toggle RRC Enable during hot plug events
IRQ Sets BridgeDis	Auto / Disabled /Enabled	Register control of BridgeDis only follows DL_Active

4.3.1.5 FCH Common Options submenu

Menu Item	Options	Description
SATA Configuration Options	See submenu	Allows setting the configuration parameters for SATA Channels
USB Configuration Options	See submenu	Allows setting the configuration parameters for USB interfaces
XGBE Configuration Options	See submenu	Allows setting the configuration parameters for XGbE interfaces

4.3.1.5.1 SATA Configuration Options submenu

Menu Item	Options	Description
SATA Controller	Auto / Disabled /Enabled	Allows configuring and disabling the on-chip SATA Controller
SATA Mode	Auto / RAIS / AHCI / AHCI as ID 0x7904	Only available when “SATA Controller” is set to Enabled. Allows selecting the on-chip SATA working mode
Sata RAS Support	Auto / Disabled /Enabled	Enables or disables the support for SATA RAS
Sata Disabled AHCI Prefetch Function	Auto / Disabled /Enabled	Enables or disables the SATA AHCI Prefetch Function
Aggressive SATA Device Sleep Port 0 Aggressive SATA Device Sleep Port 1	Auto / Disabled /Enabled	Enables or disables the Aggressive SATA Device Sleep on port #x, which makes the SATA drive to spin down when idle, independently by drive’s firmware or by OS settings.
DevSleep0 Port Number DevSleep1 Port Number	0..8	Only available when “Aggressive SATA Device Sleep Port x” is set to Enabled. Allows setting the DevSleep*x* Port Number

4.3.1.5.2 USB Configuration Options submenu

Menu Item	Options	Description
XHCI Port number	0 / 1 / 2 / 3 / 4	Allows enabling the desired number of xHCI ports. When the ports enabled are less than 4 (four), then the ports will be disabled following a descending order, i.e.: 4 XHCI ports enabled, on COM Express connector all USB ports (#0, #1, #2 and #3) will be available, 3 XHCI ports enabled, on COM Express connector only ports #0, #1 and #2 will be available, 2 XHCI ports enabled, on COM Express connector only ports #0 and #1 will be available, 1 XHCI ports enabled, on COM Express connector only port #0 will be available,

4.3.1.5.3 XGBE Configuration Options submenu

Menu Item	Options	Description
XGBE Port number	0 / 1 / 2 / 3 / 4	Allows enabling the desired number of XGbE ports. When the ports enabled are less than 4 (four), then the ports will be disabled following a descending order, i.e.: 4 XGBE ports enabled, on COM Express connector all XGbE ports (#0, #1, #2 and #3) will be available, 3 XGBE ports enabled, on COM Express connector only ports #0, #1 and #2 will be available, 2 XGBE ports enabled, on COM Express connector only ports #0 and #1 will be available, 1 XGBE ports enabled, on COM Express connector only port #0 will be available,

4.3.1.6 NTB Common Options submenu

Menu Item	Options	Description
NTB Enable	Auto / Enable	Allows forcing enabling the Non-Transparent Bridging (NTB) on the PCIe bus, which allows the CPU to see the memory in a remote node's PCIe memory space. When enabled, the following menu items will appear.
NTB Location	Auto Socket0-Die0 Socket0-Die1 Socket0-Die2 Socket0-Die3 Socket1-Die0 Socket1-Die1 Socket1-Die2 Socket1-Die3	Identifies the CPU cores associated to NTB
NTB Active on PCIeCore	Auto / Core 0 / Core1	Enables NTB on specific PCIeCores
NTB Mode	NTB Disabled NTB Primary NTB Secondary NTB Random Auto	Selects the NTB mode
Link Speed	Max Speed / Gen1 / Gen2 / Gen3 / Auto	Sets the Link Speed for NTB Mode

4.3.2 iSCSI Configuration submenu

Menu Item	Options	Description
iSCSI initiator Name	*Text box*	Allows setting the worldwide unique name of iSCSI Initiator in IQN format, with range from 4 to 223.

4.3.3 Intel® I21x Gigabit Network Connection - *MAC Address* submenu

Menu Item	Options	Description
NIC Configuration	See submenu	Enter the submenu to configure the network device port
Blink LEDs	0 / 1	Identify the physical network port by blinking the associated LED

4.3.3.1 NIC Configuration submenu

Menu Item	Options	Description
Link Speed	Auto Negotiated 10 Mbps Half 10 Mbps Full 100 Mbps Half 100 Mbps Full	Specifies the port speed used for the selected boot protocol
Wake On LAN	Disabled / Enabled	Enables powering on the system via LAN. Note that configuring Wake on LAN in the operating system does not change the value of this setting, but does override the behaviour of Wake on LAN in OS controlled power states

4.3.4 Battery Failure Manager submenu

Menu Item	Options	Description
Battery Failure Action	None Restore Defaults Restore NVRAM	Sets the action that must be done when a backup battery failure occurs. None: no action Restore defaults: restore BIOS factory default, preserving the password(s) Reset NVRAM: restore all factory defaults, clearing also the password(s)

4.3.5 Trusted computing submenu

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.
Pending Operation	None / TPM Clear	Schedule an Operation for the Security Device. NOTE: your module 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
TPM2.0 UEFI Spec Version	TCG_1_2 TCG_2	Select the TCG Spec Version support. TCG_1_2 is the compatible mode for Windows 8 / Windows 10. TCG 2 supports the new TCG2 protocol and event format for Windows 10 or later.
Physical Presence Spec Version	1.2 / 1.3	Select to tell OS to support PPI Spec Version 1.2 or 1.3. Please note that some HCK tests might not support 1.3
Device Select	Auto TPM 1.2 TPM 2.0	TPM 1.2 will restrict the support to TPM 1.2 devices only, TPM 2.0 will restrict the support to TPM 2.0 devices only, Auto will support both with the default set to TPM 2.0 devices if not found, TPM 1.2 devices will be enumerated

4.3.6 PSP Firmware Versions submenu

Informative screen only

4.3.7 ACPI Settings submenu

Menu Item	Options	Description
Enable ACPI Auto Configuration	Disabled / Enabled	Enables or Disables BIOS ACPI Auto Configuration. The following menu items will appear only when this menu item is Disabled
Lock Legacy resources	Disabled / Enabled	Enables or Disables Lock of Legacy resources

4.3.8 Board Parameters Setting submenu

Menu Item	Options	Description
Spread Spectrum	Enabled/Disabled	Enables or disables CG1_PLL Spread Spectrum
Bucket 1 + Internal GbE Grouping	Gbe + [*all possible groupings of PCI-e lanes with max 5 root ports] / [all possible groupings of PCI-e lanes with max 6 root ports]*	Configures the width of the Link(s) of Bucket 1 (COM-Express PCIe0-7 lanes) and Internal GbE enabling. A maximum of 6 root ports (included Internal GbE controller) are allowed for these PCI-e groupings.
Bucket 1 + Internal GbE Configuration	See submenu	Configures the Link (s) parameters: Hotplug, Speed, ASPM and Compliance Mode
Buckets 3-4 Grouping	*Possible groupings of 16 PCI-e lanes with max 8 root ports*	Configures the width of the Link(s) of Buckets 3-4 (COM-Express PCIe16-31 lanes) A maximum of 8 root ports are allowed for these PCI-e groupings.
Bucket 3-4 Configuration	See Submenu	Configures the Link (s) parameters: Hotplug, Speed, ASPM and Compliance Mode

4.3.8.1 Bucket 1 + Internal GbE Configuration & Bucket 3-4 Configuration submenus

Menu Item	Options	Description
PCIEx	See submenus	Depending on the quantity of PCIe groupings enabled for the various buckets, there will be as many menu items here, each one numbered according to the starting PCIe lane on COM Express connector. Every one of these items will allow to configure the specific Link parameters described in the following paragraph

4.3.8.1.1 PCIEx submenus

Menu Item	Options	Description
ASPM	Disable / L0s Entry	PCI Express Active State Power Management Settings
Link Speed	Max Speed PCIe Gen1 PCIe Gen2	Configure PCIe Speed
Hotplug Mode	Disabled / Hotplug Basic / Hotplug Server / Hotplug Enhanced/ Hotplug Inboard	Sets Hotplug Mode Control
Compliance Mode	Enabled / Disabled	When enabled, forces port into compliance mode

4.3.9 S5 RTC Wake Settings submenu

Menu Item	Options	Description
Wake system from S5	Disabled By Every Day By Day of Month	Enables or disables System Wake on Alarm event. The following menu items will appear only when this voice is not set to Disabled
Wake up hour	0..23	Sets the wake up hour in 0..23 format (i.e.,3 means 3am, 15 means 3pm)
Wake up minute	0..59	Sets the wake up minute
Wake up second	0..59	Sets the wake up second
Day of Month	1..31	This item is available only when “Wake system from S5” is set to “By Day of Month”. Sets the day of month for Wake on Alarm event. Valid range s from 1 to 31, error checking will be done against month/day/year combinations that are not valid.

4.3.10 Serial Port Console Redirection submenu

Menu Item	Options	Description
Console redirections	Enabled / Disabled	Enables or Disables the Console redirection on various ports. For every port enables, 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

4.3.10.1 Console Redirection Settings submenu

Menu Item	Options	Description
Terminal Type	VT100 VT100+ VT-UTF8 ANSI	Emulation: ANSI: Extended ASCII Char set. VT100: ASCII Char set. VT100+: extends VT100 to support colour, function keys, etc. VT-UTF8: uses UTF8 encoding to map Unicode chars onto 1 or more bytes
Bits per second	9600 / 19200 / 38400 / 57600 / 115200	Select Serial port Transmission Speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Data bits	7 / 8	Set Console Redirection data bits
Parity	None Even Odd Mark Space	A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the number of 1s in the data bits is even. Odd: parity bit is 0 if the number of 1s in the data bits is odd. Mark: parity bit is always 1. Space: parity bit is always 0. Mark and Space do not allow for error detection
Stop bits	1 / 2	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit
Flow Control	None Hardware RTS/CTS	Flow Control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses RTS# / CTS# lines to send the start / stop signals.
VT-UTF8 Combo Key Support	Enabled / Disabled	Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals
Recorder Mode	Enabled / Disabled	When this mode is enabled, only text will be sent. This is to capture Terminal data.
Resolution 100x31	Enabled / Disabled	Enables or disables extended terminal resolution
Putty Keypad	VT100 / Linux / XTERMR6 / SCO / ESCN /V T400	Select FunctionKey and KeyPad on Putty

4.3.11 CPU Configuration submenu

Menu Item	Options	Description
SVM Mode		Enables or disables CPU Virtualization
SMEE	Disabled / Enabled	Controls secure memory encryption enable
Node 0 Information Node 1 Information		Opens an informative-only screen with all information related to CPU node x: Processor name, number of cores and threads, Cache memory information

4.3.12 PCI Subsystem Settings submenu

Menu Item	Options	Description
Above 4G Decoding	Disabled / Enabled	Globally Enabled or Disabled 64-bitcapable Devices to be decoded in Address Space above 4GB (only if system supports 64-bit PCI Decoding).
SR-IOV Support	Disabled / Enabled	Enables or disables Single Root IO Virtualization Support (SR-IOV) for systems having devices capable to support it.

4.3.13 USB configuration submenu

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
Port 60/64 Emulation	Enabled/ Disabled	Enables I/O port 60h/64h emulation support. This should be enabled for a complete USB keyboard legacy support for non-USB aware OSes
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

4.3.14 Network Stack configuration submenu

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
IP6 Configuration Policy	Automatic / Manual	
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

4.3.15 CSM configuration submenu

Menu Item	Options	Description
CSM Support	Enabled / Disabled	Enables or disables the Compatibility Support Module (CSM) Support. When enabled, the following menu items will appear
GateA20 Active	Upon Request Always	Upon Request: GateA20 can be disabled using BIOS services, Always: do not allow disabling GateA20; this option is useful when any RT code is executed above 1MB.
Option ROM Messages	Force BIOS Keep Current	Set display mode for Option ROM
INT19 Trap Response	Immediate Postponed	BIOS Reaction on INT19 trapping by Option ROM: IMMEDIATE - execute the trap right away; POSTPONED - execute the trap during legacy boot
Boot option filter	UEFI and Legacy Legacy only UEFI only	This option controls Legacy / UEFI ROMs priority
Network	Do not launch UEFI Legacy	Controls the execution of UEFI and Legacy PXE OpROM
Storage	Do not launch UEFI	Controls the execution of UEFI and Legacy Storage OpROM

	Legacy	
Video	Do not launch UEFI Legacy	Controls the execution of UEFI and Legacy Video OpROM
Other PCI devices	Do not launch UEFI Legacy	Determines the OpROM execution policy for devices other than Network, Storage or Video

4.3.16 NVMe configuration submenu

NVMe Device Options Settings, depend on NVMe Devices found in the system.

4.3.17 SATA configuration submenu

SATA Device Options Settings, depend on the SATA Devices found in the system.

4.3.18 Main Thermal Configuration submenu

Menu Item	Options	Description
Critical Temperature (°C)	80 .. 110	Above this threshold, an ACPI aware OS will perform a critical shut-down. Allowed range is from 80 to 110, where 110 means disabled.
Passive Cooling Temperature (°C)	60 .. 100	This value controls the temperature of the ACPI Passive Trip Point - the point in which the OS will begin lowering the CPU speed. Allowed range is from 60 to 100, where values above Critical Temperature means Disabled.
TC1	1 .. 16	Thermal Constant 1: part of the ACPI Passive Cooling Formula
TC2	1 .. 16	Thermal Constant 1: part of the ACPI Passive Cooling Formula
TSP (seconds)	2 .. 32	Period of temperature sampling when Passive Cooling

4.3.19 SMBIOS Information

Display only screen, shows information about the module and the Carrier board.

4.3.20 Embedded Controller submenu

Menu Item	Options	Description
LID_BTN# Configuration	Force Open Force Closed Normal Polarity Inverted Polarity	Configures the LID_BTN# signal as always open or closed, no matter the pin level, or configures the pin polarity: High = Open (Normal), Low = Open (Inverted)
LID_BTN# Wake Configuration	No Wake Only From S3 Wake From S3/S4/S5	Configures LID_BTN# wake capability (when not forced to Open or Closed). According to the pin configuration, when the LID is open it can cause a system wake from a sleep state.
SMB_ALERT# wake	Disabled / Enabled	Enables or disables SMBUS Alert Wake from Suspend State.
OUT 80 redirection port	None 1 2 1+2	Select on which E.C. UART(s) to redirect OUT 80 (Post Codes): can be None, 1, 2 or 1+2
Hardware Monitor		By selecting this item, an information screen with System parameters will appear
Reset Causes Handling		By selecting this item, an information screen with the handling of latest resets causes will appear.
Super IO Configuration	See Submenu	Sets the parameters for Serial Ports
Internal FAN Settings	See Submenu	Sets the parameters for Internal (i.e. on-module) FAN
External FAN/PWM Settings	See Submenu	Sets the parameters for external (i.e. on-carrier FAN
Watchdog configuration	See Submenu	Configures the Embedded Controller's Watchdog Timer
COM-Express GPIO Configurations	See Submenu	Sets the parameters for GPIOs
MAC address(es) visualization		By selecting this item, an information screen with the MAC Addresses assigned to the 10GbE interfaces will appear.

4.3.20.1 *Super IO Configurations submenu*

Menu Item	Options	Description
Serial Port 1	Enabled / Disabled	Enables or Disables Serial Port 1
Address	0x3F8 / 0x3E8 / 0x2F8 / 0x2F0 / 0x2E8 / 0x2E0 / 0x2A8 / 0x2A0 / 0x288 / 0x280	Serial Port IO Base Address
IRQ	3 / 4 / 5 / 6 / 7 / 10 / 11 / 14 / 15	Serial Port IRQ
Serial Port 2	Enabled / Disabled	Enables or Disables Serial Port 2
Address	0x3F8 / 0x3E8 / 0x2F8 / 0x2F0 / 0x2E8 / 0x2E0 / 0x2A8 / 0x2A0 / 0x288 / 0x280	Serial Port IO Base Address
IRQ	3 / 4 / 5 / 6 / 7 / 10 / 11 / 14 / 15	Serial Port IRQ

4.3.20.2 *Internal FAN Settings submenu*

Menu Item	Options	Description
FAN_PWMOUT device type	3-Wire FAN 4-Wire FAN Generic PWM	Specifies if FAN_PWMOUT signal is connected to a 3-wire or 4-Wire Fan or to a generic PWM
Enhanced 3 wire RPM measurement	Enabled / Disabled	Enabled: on each measurement phase Duty Cycle will be raised to 100% for 100mS then restored to original value to allow a more precise measure avoiding unwanted ripple on tachometer. Disabled: periodic fan speed up will not occur, but RPM measurement will not be accurate
Automatic Temperature FAN Control	Enabled / Disabled	Disable / Enable Thermal Feed-back FAN Control
AC0 Temperature (°C)	70 / 75 / 80 / 85 / 90 / 95 / 100	Only available when "Automatic Temperature FAN Control" is Enabled AC0: above this temperature the FAN runs at full speed
AC1 Temperature (°C)	5 / 10 / 15 / 20 /25 / 30 / 35 / 40 / 45 / 50 / 55 / 60 / 65 / 70 / 75 / 80 / 85 / 90 / 95 / 100	Only available when "Automatic Temperature FAN Control" is Enabled. 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	0 .. 10	Only available when “Automatic Temperature FAN Control” is Enabled. Value added (when temperature is growing) to the ACx thresholds or subtracted from them (when temperature is decreasing) to avoid oscillations.
Linear Speed change	Enabled / Disabled	Only available when “Automatic Temperature FAN Control” is Enabled. Linear FAN Duty Cycle growth between AC1 and AC0
FAN Duty Cycle (%) Above AC1	0 .. 100	Only available when “Automatic Temperature FAN Control” is Enabled and “Linear Speed change” is Disabled Fan Duty Cycle (%) between AC1 and AC0 (low speed)
Speed Change Duration	0 .. 50	Only available when “Automatic Temperature FAN Control” is Enabled and “Linear Speed change” is Disabled Duration in seconds of linear FAN Speed Change. Allowed range: from 0 to 50.
FAN_PWM Frequency	1 .. 60000	Only available when “Automatic Temperature FAN Control” is Disabled. Sets the frequency of the FAN_PWMOUT signal. Typical values are 100 for a 3-wire device and 20000 for a 4-wire one. Allowed range is 1-60000.
FAN_PWM Duty Cycle	0 .. 100	Only available when “Automatic Temperature FAN Control” is Disabled. Default FAN Duty Cycle (%).
FAN_PWMOUT Frequency	1 .. 60000	Only available when “FAN_PWMOUT device type” is set to Generic PWM. Sets the frequency of the FAN_PWMOUT signal.
FAN_PWMOUT Duty Cycle	0 .. 100	Only available when “FAN_PWMOUT device type” is set to Generic PWM. Default FAN_PWMOUT Signal Duty Cycle (%).

4.3.20.3 External FAN/PWM Settings submenu

Menu Item	Options	Description
FAN_PWMOUT Device Type	3-Wire FAN 4-Wire FAN Generic PWM	Specifies if FAN_PWMOUT is connected to a 3-wire or 4-wire FAN or to a generic PWM.
Enhanced 3 wire RPM measurement	Enabled / Disabled	Only available when “FAN_PWMOUT Device Type” is set to 3-Wire FAN Enabled: on each measurement phase Duty Cycle will be raised to 100% for 100mS then restored to original value to allow a more precise measure avoiding unwanted ripple on tachometer. Disabled: periodic fan speed up will not occur, but RPM measurement will not be accurate
Automatic Temperature FAN Control	Enabled / Disabled	Only available when “FAN_PWMOUT Device Type” is set to 3-Wire FAN or 4-Wire FAN Disable / Enable Thermal Feed-back FAN Control
AC0 Temperature (°C)	70 / 75 / 80 / 85 / 90 / 95 / 100	Only available when “Automatic Temperature FAN Control” is Enabled AC0: above this temperature the FAN runs at full speed

AC1 Temperature (°C)	5 / 10 / 15 / 20 /25 / 30 / 35 / 40 / 45 / 50 / 55 / 60 / 65 / 70 / 75 / 80 / 85 / 90 / 95 / 100	Only available when “Automatic Temperature FAN Control” is Enabled. 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	0 .. 10	Only available when “Automatic Temperature FAN Control” is Enabled. Value added (when temperature is growing) to the ACx thresholds or subtracted from them (when temperature is decreasing) to avoid oscillations.
Linear Speed change	Enabled / Disabled	Only available when “Automatic Temperature FAN Control” is Enabled. Linear FAN Duty Cycle growth between AC1 and AC0
FAN Duty Cycle (%) Above AC1	0 .. 100	Only available when “Automatic Temperature FAN Control” is Enabled and “Linear Speed change” is Disabled Fan Duty Cycle (%) between AC1 and AC0 (low speed)
Speed Change Duration	0 .. 50	Only available when “Automatic Temperature FAN Control” is Enabled and “Linear Speed change” is Disabled Duration in seconds of linear FAN Speed Change. Allowed range: from 0 to 50.
FAN PWM Frequency	1 .. 60000	Only available when “Automatic Temperature FAN Control” is Disabled. Sets the frequency of the FAN_PWMOUT signal. Typical values are 100 for a 3-wire device and 20000 for a 4-wire one. Allowed range is 1-60000.
FAN Duty Cycle	0 .. 100	Only available when “Automatic Temperature FAN Control” is Disabled. Default FAN Duty Cycle (%).

4.3.20.4 Watchdog Configuration submenu

Menu Item	Options	Description
Watchdog Status	Disabled / Enabled	Enables or disables the Watchdog. When disabled, all following items will disappear
Event action	Raisw WDT Signal Power Button Pulse	Action executed at the expiring of the Event time-out.
Reset action	System Reset Power Button Override Raise WDT Signal	Action executed at the expiring of the reset time-out.
Watchdog Delay	0 .. 60	Minutes before watchdog normal operations start. During delay time-out, a refresh operation will immediately trigger the normal operation. Valid range is from 0 to 60.
Event Timeout	0 .. 60	Time-out minutes that can pass without refresh before triggering the Event Action. A refresh will restart the time-out. Valid range is from 0 to 60.
Reset Timeout	1 .. 60	Time-out minutes that can pass without refresh before triggering the Reset Action, this timer will start counting when event time-out is expired.. A refresh will restart the time-out. Valid range is from 1 to 60.

4.3.20.5 COM-Express GPIO Configurations submenu

Menu Item	Options	Description
GPO0 GPO1 GPO2 GPO3	Output Low Output High Output Last	Configure pin as input or output with a fixed starting value. Last means no changes with respect to the last boot.

4.4 Chipset menu

Menu Item	Options	Description
SMT Mode	Auto / Off	Simultaneous multithreading. Off: 1T single-Thread Auto: 2T two-thread if the processor is capable of it.
PCIe Link Training Type	1 Step / 2Step	Specifies if PCI Express Link Training happens in 1 or 2 Steps
North Bridge		By selecting this item, an information screen with data related to the memory will appear.

4.5 Security menu

Menu Item	Options	Description
Administrator Password		Set Setup Administrator Password. If only the Administrator Password is set, then this only limits the access to setup, and it is asked for entering it.
User Password		Set User Password. If only the user's password is set, then this will be a power-on password and must be entered to boot or to enter setup. In setup, the User will have Administrator rights.
Secure Boot	See Submenu	Customizable Secure Boot Settings

4.5.1 Secure Boot submenu

Menu Item	Options	Description
Attempt Secure Boot	Enabled / Disabled	Secure Boot is activated when the Platform Key (PK) is enrolled, System Mode is User/Deployed and CSM function is disabled.
Secure Boot Mode	Standard / Custom	Sets Secure Boot mode selector to Standard Mode or Custom Mode. In Custom Mode, the Secure Boot variables can be configured without authentication.
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	Description
Provision Factory Default keys	Enabled / Disabled	Provision factory default keys on next re-boot only when System in Setup Mode
Install Factory Default Keys		Force System to User Mode. Configure NVRAM to contain OEM- defined factory default Secure Boot keys
Enroll Efi Image	*File System Image*	Allow the selected image to run in Secure Boot mode. Enrol SHA256 Hash Certificates of the Image into Authorized Signature Database (db)
Platform key Key Exchange Keys Authorized Signatures Forbidden Signatures Authorized Timestamps OS Recovery Signatures	Set New Var Append Key	Enrol factory Defaults or load certificates from a file: 1. Public Key Certificate in: a) EFI_SIGNATURE_LIST b) EFI_CERT_X509 (DER encoded) c) EFI_CERT_RSA2048 (bin) d) EFI_CERT_SHA256,384,512 2. Authenticated UEFI variables 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 at boot
Quiet Boot	Enabled / Disabled	Enables or Disables Quiet Boot options
Fast Boot	Enabled / Disabled	Enables or disables boot with the initialization of a minimal set of devices required to launch active boot option. It has no effect for BBS boot option.
SATA Support	Last Boot HDD only All SATA devices	Only available when Fast Boot is set to “Enabled”. Specifies if only the SATA drive used during last boot must be available in POST or if all SATA devices must be available in OS and POST
VGA Support	Auto EFI Driver	Only available when Fast Boot is set to “Enabled”. When set to Auto,it will install only the Legacy OpRom with Legacy OS and the logo will not be shown during post. The EFI driver will still be installed with EFI OS.
USB Support	Disabled Full Initial Partial Initial	Only available when Fast Boot is set to “Enabled”. When Disable, all the USB devices will not be available until the completion of OS boot. With Partial Initial, USB Mass Storage and specific USB port/device will not be available before OS boot. With Full Initial, all USB devices will be available both in OS and POST.
PS2 Devices Support	Enabled / Disabled	Only available when Fast Boot is set to “Enabled”. Allows skipping the PS2 devices
Network Stack Driver Support	Enabled / Disabled	Only available when Fast Boot is set to “Enabled”. When Disabled, Network Stack Driver will be skipped.
Redirection Support	Enabled / Disabled	Only available when Fast Boot is set to “Enabled”. When Disabled, the Redirection function will be disabled.
New Boot Option Policy	Default / Place First / Place Last	Controls the placement of newly detected UEFI boot options
Boot Mode Select	LEGACY / UEFI	Select the boot mode between Legacy and UEFI
Boot Option #1 Boot Option #2 Boot Option #3 Boot Option #4 Boot Option #5 Boot Option #6 Boot Option #7	SATA 0 HD SATA 1 HD NVME CD/DVD USB Device Network Other Device: UEFI: Built-In EFI Shell Disabled	Select the system boot order
UEFI Other Drive BBS Priorities		By entering this menu, it will be possible to determine the specific boot order considering only the devices connected to the system, optionally removing them from the boot order.

4.7 Save & Exit menu

Menu Item	Options	Description
Save Changes and Exit		Exit system setup after saving the changes.
Discard Changes and Exit		Exit system setup without saving any changes.
Save 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.
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
UEFI: Built-In EFI Shell		
Launch EFI Shell from filesystem device		Attempt to Launch the EFI Shell application (Shell.efi) from one of the available filesystem devices

4.8 Event Logs menu

Menu Item	Options	Description
Change Smbios Event Log Settings	See submenu	SMBios Event Log parameters configuration
View Smbios Event Log		By selecting this item, it will appear a list of all records of the Smbios Event Log

4.8.1 Change Smbios Event Log Settings Submenu

Menu Item	Options	
Smbios Event Log	Enabled / Disabled	Use this option to enable or disable all features of Smbios Event Logging during boot. When Enabled, all following items will appear
Erase Event Log	No / Yes Next reset / Yes Every reset	Choose option for erasing Smbios Event Logs. Erasing is done prior to any logging activation during reset.
When Log is Full	Do Nothing Erase Immediately	Choose the behaviour to adopt when the Smbios Event Log is full.
Log System Boot Event	Enabled / Disabled	Choose option to enable or disable logging of System boot event.
MECI	1..255	Multiple Event Count Increment: the number of occurrences of a duplicate event that must pass before the multiple-event counter of the log entry be updated. The value ranges from 1 to 255.
METW	0..99	Multiple Event Time Window: the number of minutes which must pass between duplicate log entries which utilize a multiple-event counter. The value ranges from 0 to 99 minutes.
Log OEM Codes	Enabled / Disabled	Enables or disables the logging of EFI Status Codes as OEM Codes (if not already converted to legacy.)
Convert OEM Codes	Enabled / Disabled	Enables or disables the conversion of EFI Status Codes to Standard Smbios Types (Not all may be translated).

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 COMe-C42-BT7 module, 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 COMe-C42-BT7 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 COMe-C42-BT7 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