Qseven

User Manual

ATLAS

Qseven® Rel. 2.1 Compliant Module
with the Intel® Atom™ x6000E Series and Intel®
Pentium® and Celeron® N and J Series
(formerly Elkhart Lake) SoCs

SECO

www.seco.com

REVISION HISTORY

Revision	Date	Note	Rif
1.0	14th December 2022	First Official Release	SO
1.1	29th December 2022	Added BIOS documentation	SO
1.2	31st March 2023	Included power consumptions	SO

Every effort has been made to ensure the accuracy of this manual. However, SECO S.r.l. accepts no responsibility for any inaccuracies, errors or omissions herein. SECO S.r.l. 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.

INDEX

Chapter 1.
INTRODUCTION

- Warranty
- Information and assistance
- RMA number request
- Safety
- Electrostatic Discharges
- RoHS compliance
- Safety Policy
- Terminology and definitions
- Reference specifications

1.1 Warranty

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

The warranty on this product lasts for 1 year.

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

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

Items cannot be returned unless previously authorised by the supplier.

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

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

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

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

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

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

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

1.2 Information and assistance

What do I have to do if the product is faulty?

SECO S.r.l. offers the following services:

- SECO website: visit http://www.seco.com to receive the latest information on the product. In most of the cases it is possible to find useful information to solve the problem.
- SECO Sales Representative: the Sales Rep can help to determine the exact cause of the problem and search for the best solution.
- SECO Help-Desk: contact SECO Technical Assistance. A technician is at disposal to understand the exact origin of the problem and suggest the correct solution.

  E-mail: technical.service@seco.com

  Fax (+39) 0575 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

This board uses only extremely-low voltages.

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

!

Always switch the power off, and unplug the power supply unit, before handling the board and/or connecting cables or other boards.

Avoid using metallic components - like paper clips, screws and similar - near the board when connected to a power supply, to avoid short circuits due to unwanted contacts with other board components.

If the board has become wet, never connect it to any external power supply unit or battery.

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

1.5 Electrostatic Discharges

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

!

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

1.6 RoHS compliance

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

1.7 Safety Policy

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

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

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

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

1.8 Terminology and definitions

ACPI	Advanced Configuration and Power Interface, an open industrial standard for the board's devices configuration and power management
AHCI	Advanced Host Controller Interface, a standard which defines the operation modes of SATA interface
API	Application Program Interface, a set of commands and functions that can be used by programmers for writing software for specific Operating Systems
BIOS	Basic Input / Output System, the Firmware Interface that initializes the board before the OS starts loading
CEC	Consumer Electronics Control, an HDMI feature which allows controlling more devices connected together by using only one remote control
CRT	Cathode Ray Tube. Initially used to indicate a type of monitor, this acronym has been used over time to indicate the analog video interface used to drive them.
DDC	Display Data Channel, a kind of I2C interface for digital communication between displays and graphics processing units (GPU)
DDR	Double Data Rate, a typology of memory devices which transfer data both on the rising and on the falling edge of the clock
DDR3	DDR, 3rd generation
DP	Display Port, a type of digital video display interface
DVI	Digital Visual interface, a type of digital video display interface
eDP	embedded Display Port, a type of digital video display interface developed especially for internal connections between boards and digital displays
EHCI	Enhanced Host Controller interface, a high-speed controller for USB ports, able to support USB2.0 standard
GbE	Gigabit Ethernet
Gbps	Gigabits per second
GND	Ground
GPI/O	General purpose Input/Output
HD Audio	High Definition Audio, most recent standard for hardware codecs developed by Intel® in 2004 for higher audio quality
HDMI	High Definition Multimedia Interface, a digital audio and video interface
I2C Bus	Inter-Integrated Circuit Bus, a simple serial bus consisting only of data and clock line, with multi-master capability
JTAG	Joint Test Action Group, common name of IEEE1149.1 standard for testing printed circuit boards and integrated circuits through the Debug port
LPC Bus	Low Pin Count Bus, a low speed interface based on a very restricted number of signals, deemed to management of legacy peripherals
LVDS	Low Voltage Differential Signalling, a standard for transferring data at very high speed using inexpensive twisted pairs copper cables, usually used for video applications
MAC	Medium Access Controller, the hardware implementing the Data Link Layer of ISO/OSI-7 model for communication systems
Mbps	Megabits per second

MMC/eMMC	MultiMedia Card / embedded MMC, a type of memory card having the same interface of SD cards. The eMMC is the embedded version of the MMC. They are devices that incorporate both the memory controller and the flash memories on a single BGA chip.
N.A.	Not Applicable
N.C.	Not Connected
OpenCL	Open Computing Language, a software library based on C99 programming language, conceived explicitly to realise parallel computing using Graphics Processing Units (GPU)
OpenGL	Open Graphics Library, an Open Source API dedicated to 2D and 3D graphics
OS	Operating System
PCI-e	Peripheral Component Interface Express
PHY	Abbreviation of Physical, it is the device implementing the Physical Layer of ISO/OSI-7 model for communication systems
PSU	Power Supply Unit
PWM	Pulse Width Modulation
PWR	Power
PXE	Preboot Execution Environment, a way to perform the boot from the network ignoring local data storage devices and/or the installed OS
SATA	Serial Advance Technology Attachment, a differential half duplex serial interface for Hard Disks
SD	Secure Digital, a memory card type
SDHC	Secure Digital Host Controller or Secure Digital High Capacity
SM Bus	System Management Bus, a subset of the I2C bus protocol dedicated to communication with devices for system management, like a smart battery and other power supply-related devices
SPI	Serial Peripheral Interface, a 4-Wire synchronous full-duplex serial interface which is composed of a master and one or more slaves, individually enabled through a Chip Select line
TBM	To be measured
TMDS	Transition-Minimized Differential Signaling, a method for transmitting high speed serial data, normally used on DVI and HDMI interfaces
TTL	Transistor-transistor Logic
UEFI	Unified Extensible Firmware Interface, a specification defining the interface between the OS and the board’s firmware. It is meant to replace the original BIOS interface
USB	Universal Serial Bus
V_REF	Voltage reference Pin
VGA	Video Graphics Array. An analog computer display standard, commonly referred to also as CRT.
xHCI	eXtensible Host Controller Interface, Host controller for USB 3.0 ports, which can also manage USB 2.0 and USB1.1 ports

1.9 Reference specifications

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

Reference	Link
ACPI	http://www.acpi.info
AHCI	http://www.intel.com/content/www/us/en/io/serial-ata/ahci.html
DDC	http://www.vesa.org
DP, eDP	http://www.vesa.org
Gigabit Ethernet	http://standards.ieee.org/about/get/802/802.3.html
HD Audio	http://www.intel.com/content/dam/www/public/us/en/documents/product-specifications/high-definition-audio-specification.pdf
HDMI	http://www.hdmi.org/index.aspx
I2C	http://www.nxp.com/documents/other/UM10204_v5.pdf
JTAG	http://standards.ieee.org/develop/wg/Boundary_Scan_Architecture.html
LPC Bus	http://www.intel.com/design/chipsets/industry/lpc.htm
LVDS	http://www.ti.com/ww/en/analog/interface/lvds.shtml http://www.ti.com/lit/ml/snla187/snla187.pdf
MMC/eMMC	http://www.jedec.org/committees/jc-649
OpenCL	http://www.khronos.org/opencl
OpenGL	http://www.opengl.org
PCI Express	http://www.pcisig.com/specifications/pciexpress
Qseven® Design Guide	https://www.sget.org/fileadmin/_migrated/content_uploads/Qseven_Design_Guide_2_0.pdf
Qseven® specifications	https://www.sget.org/fileadmin/file_management/SDT02/Qseven-Spec_2.1.pdf
SATA	https://www.sata-io.org
SD Card	https://www.sdcard.org/home
SM Bus	http://www.smbus.org/specs
TMDS	http://www.siliconimage.com/technologies/tmds

UEFI	http://www.uefi.org
USB 2.0 and USB OTG	http://www.usb.org/developers/docs/usb_20_070113.zip
USB 3.0	http://www.usb.org/developers/docs/usb_30_spec_070113.zip
Intel® Atom™ Elkhart Lake family	https://ark.intel.com/content/www/us/en/ark/products/codename/80644/Elkhart-lake.html#@Embedded

Chapter 2.
OVERVIEW

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

2.1 Introduction

ATLAS is a in Qseven® Rel. 2.1 compliant module based on the Intel® Atom® x6000E Series and Intel® Pentium® and Celeron® N and J Series processors (formerly Elkhart Lake), a series of Dual / Quad SOCs with 64-bit instruction set.

These new family of processors offers different use conditions, such as PC Client, Embedded and Industrial targets and is optimized for usage in vertical applications for IOT including Industrial, Office Automation, Retail, Gaming, Healthcare, Transportation.

New features introduced by Elkhart Lake are, but not limited to the following: Time Sensitive Network (TSN) and Time Coordinate Computing (TCC) for real-time and responsive applications, Scalability and consolidation of temporally deterministic workloads, In band and OOB remote manageability (reboot/power-on/power-off), Platform Trust Technology (PTT), Dynamic Application Loader (DAL) and Secure Guard Extension (SGX), Intel Programmable Service Engine, Intel UHD Graphics, media, and display supporting, Fully Integrated Voltage Regulator (FIVR).

These SOCs embed all the features usually obtained by combination of CPU + platform Controller hubs, all in one single IC, which allows, therefore, the system

minimisation and performance optimisation, which is essential for boards with sizes so reduced as for the computing abilities of a standard board, with the possibilities of combining with a ready-to-use carrier board like the SECO CQ7-D59 or customised carrier board.

The Embedded Memory Controller allows the integration of up to 16GB of LPDDR4 Memory directly soldered onboard with In-Band Error Correction Code supported and speed up to 4267MT/s on single rank and 3733MT/s on dual rank.

All SOCs embed an Intel® Gen11 UHD Graphics controller with up to 32 Execution Units, which offer high graphical performances, with support for Microsoft®

DirectX12.1, OpenGL 4.5, OpenCLTM 1.2, OpenGL ES 3.1, Vulkan 1.1 and HW acceleration for video encoding and decoding of HEVC (H.265), H.264, VP8, VP9, JPEG/MJPEG. It is also possible the HW video decoding only of MPEG2, VC-1.

This embedded GPU is able to drive three independent displays, by using the interfaces available on SMARC connector: one DP++ 1.4, one HMDI 1.4 or DP++ 1.4 and one eDP 1.3 or Dual Channel 18/24bit LVDS (factory alternatives).

Mass Storage capabilities of the board include two external S-ATA Gen3 channel, a standard 4-bit SD interface and one optional eMMC 5.1 Drive soldered on board with up to 128GB capabilities.

Other than the interfaces already discussed previously, on Qseven® golden finger connector there are the signals necessary for the implementation of Gigabit Ethernet, two USB 3.0 ports, 6 x USB 2.0 ports, 3 x PCI-Express x 1 lanes, HD Audio interface, I2C, SPI, LPC and SM buses, UART interface.

Interfacing to the board comes through a single card edge connector, whose pinout is defined by Qseven® specifications Rel.2.1. For external interfacing to standard devices, a carrier board with a 230-pin MXM connector is needed. This board will implement all the routing of the interface signals to external standard connectors, as well as integration of other peripherals/devices not already included in the module.

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

2.2 Technical Specifications

Processors

Intel Atom™/Pentium®/Celeron® Processor "Elkhart Lake" CPUs:

- Celeron® J6413 Quad Core @ 1.8GHz (3GHz Turbo) 10W TDP
- Pentium® J6426 Quad Core @2.0GHz (3GHz Turbo) 10W TDP
- Celeron® N6211 Dual Core @1.2GHz (3GHz Turbo) 6.5W TDP
- Pentium® N6415 Quad Core @1.2GHz (3GHz Turbo) 6.5W TDP
- Atom™ x6211E Dual Core @1.2GHz (3GHz Turbo) 6W TDP, IBECC
- Atom™ x6413E Quad Core @1.5GHz (3GHz Turbo) 9W TDP, IBECC
- Atom™ x6425E Quad Core @2.0GHz (3GHz Turbo) 12W TDP, IBECC
- Atom™ x6212RE Dual Core @1.2GHz (no Turbo) 6W TDP, IBECC, TCC
- Atom™ x6414RE Quad Core @1.5GHz (no Turbo) 9W TDP, IBECC, TCC
- Atom™ x6425RE Quad Core @1.9GHz (no Turbo) 12W TDP, IBECC, TCC

(*)IBECC: In-Band Error-Correcting Code Memory

(**)TCC: Time Coordinated Computing

Memory

32-bit LPDDR4x Soldered Down Memory
Up to 16GB Quad Channel with In-Band Error Correction Code (IBECC, Safety Related feature) supported
4GB Dual Channel, 8GB or 16GB Quad Channel
Speed:4267MT/s single rank (1GB/2GB/4GB/8GB), 3733MT/s dual rank (16GB)

Graphics

Up to 3 independent displays

Integrated Gen11 UHD Graphics controller with up to 32 EU

4K HW decoding and encoding of HEVC (H.265), H.264, VP8/ VP9, WMV9/VC1 (decoding only)

DirectX 12.1, OpenGL ES 3.1, OpenGL 4.5, OpenCL™ 1.2, Vulkan 1.0

Video Interfaces

HDMI or Multimode Display Port (DP++) interface
Embedded Display Port or 18/24 bit dual channel LVDS interface

Video Resolutions

HDMI, eDP:	Up to 3840x2160 (4K)
DP++:	Up to 4096x2160
LVDS:	Up to 1920x1200

Mass Storage

2 x external S-ATA Gen3 channels
SD interface
Optional eMMC Drive soldered onboard

USB

2 x USB 3.0 Host Port
6 x USB2.0 Host ports

Networking

Gigabit Ethernet PHY with precision clock synchronization and synchronous Ethernet clock output for IEEE 1588

Optional SGMII Interface for additional second and third Gigabit Ethernet (factory option, alternative to 2 x S-ATA Gen3 channels)

Audio

HD Audio interface

PCI Express

4 x PCI-e x1 root ports (including the PCI-e port used for Gigabit Ethernet controller)

Serial Ports

1 x UART (TTL interface)

Other Interfaces

I2C bus
LPC Bus
SM Bus
SPI interface
Watchdog Timer
Thermal / FAN management
Power Management Signals

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

Operating temperature: 0°C ÷ +60°C (commercial version) **
-40°C ÷ +85°C (industrial version) **

Dimensions: 70 x70 mm (2.76” x 2.76”)

! *** 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 Qseven® specifications, the board needs to be supplied only with an external +5V$_{DC}$ power supply.

5Volts standby voltage needs to be supplied to allow Suspend to RAM and Soft Off functionalities 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 card edge fingers (see connector's pinout).

All remaining voltages needed for board's working are generated internally from +5V_S power rail.

2.3.1 Power Rails meanings

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

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

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

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

2.3.2 Power Consumption

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

Anyway, power consumption has been measured on +5V_S power rail that supplies the board. For this reason, the values indicated in the table below are real average power consumptions of the board, and are independent from those of the peripherals connected to the Carrier Board.

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

Status	Configuration							
	Intel Pentium® N6415 2GB LPDDR4 32GB eMMC eDP and 2x DP++ TPM 2.0 Comm Temp Range		Intel Pentium® J6426 8GB LPDDR4 16GB eMMC LVDS and HDMI TPM 2.0 Comm Temp Range		Intel Atom™ x6425E 16GB LPDDR4 32GB eMMC eDP and 2x DP++ TPM 2.0 Ind. Temp Range		Intel Atom™ x6425RE 8GB LPDDR4 64GB eMMC eDP, DP++ and HDMI TPM 2.0 Ind Temp Range	
	Average	Peak	Average	Peak	Average	Peak	Average	Peak
Idle, power saving configuration	2.54W	7.79W	2.64W	5.89W	2.54W	5.56W	2.39W	4.40W
OS Boot, power saving configuration	5.20W	11.32W	5.28W	11.12W	4.69W	10.95W	4.54W	12.65W
Video reproduction@1080p, power saving configuration	4.76W	9.84W	4.60W	7.00W	4.28W	6.73W	4.06W	5.42W
Video reproduction@4K, power saving configuration	4.91W	10.31W	5.30W	8.15W	5.08W	7.79W	5.09W	8.51W
Internal Stress Test Tool, maximum performance	9.48W	10.56W	11.95W	14.47W	11.93W	13.39W	14.48W	19.18W
RTC backup (VDD_RTC, 3.0V)	3.14uA		3.60uA		2.42uA		2.55uA	
Suspend (5V_STBY, 5.0V)	275mA		270mA		255mA		266mA	
Soft-off (5V_STBY, 5.0V)	262mA		250mA		240mA		250mA	

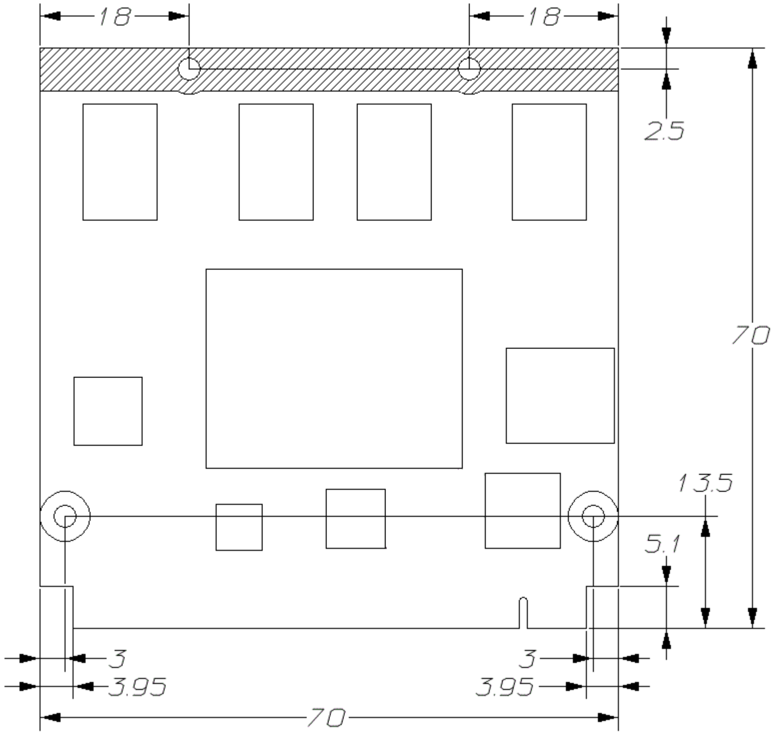
2.4 Mechanical Specifications

According to Qseven® specifications, board dimensions are: 70 x 70 mm (2.76" x 2.76").

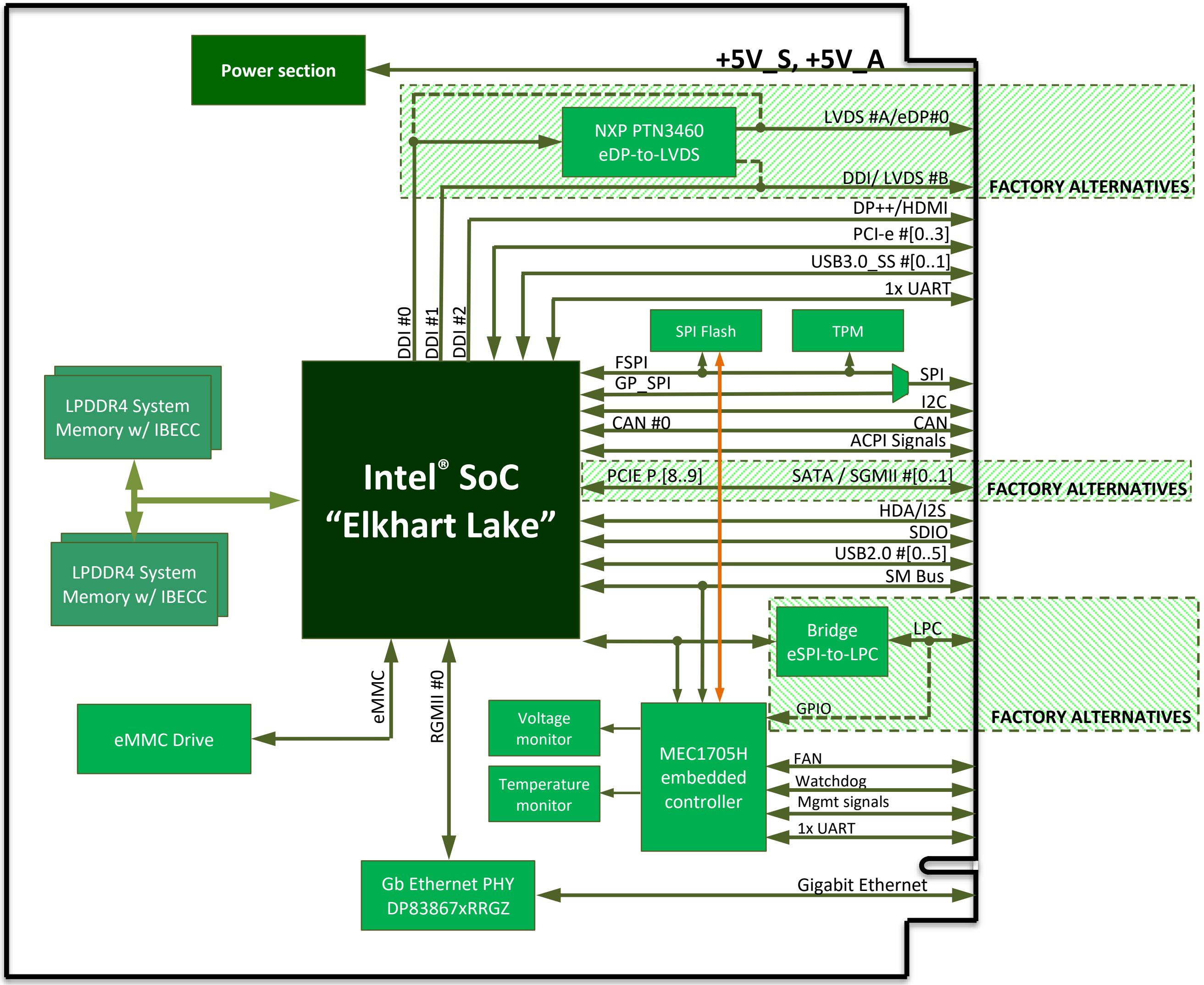
Printed circuit of the board is made of twelve layers, some of them are ground planes, for disturbance rejection.

The MXM connector accommodates various connector heights for different carrier board applications needs. Qseven® specification suggests two connector heights, 7.8mm and 7.5mm, but it is also possible to use different connector heights, also remaining compliant to the standard.

When using different connector heights, please consider that, according to Qseven® specifications, components placed on bottom side of board will have a maximum height of 2.2mm ± 0.1. Keep this value in mind when choosing the MXM connector's height, if it is needed to place components on the carrier board in the zone below the Qseven® module.



2.5 Block Diagram



Chapter 3.

CONNECTORS

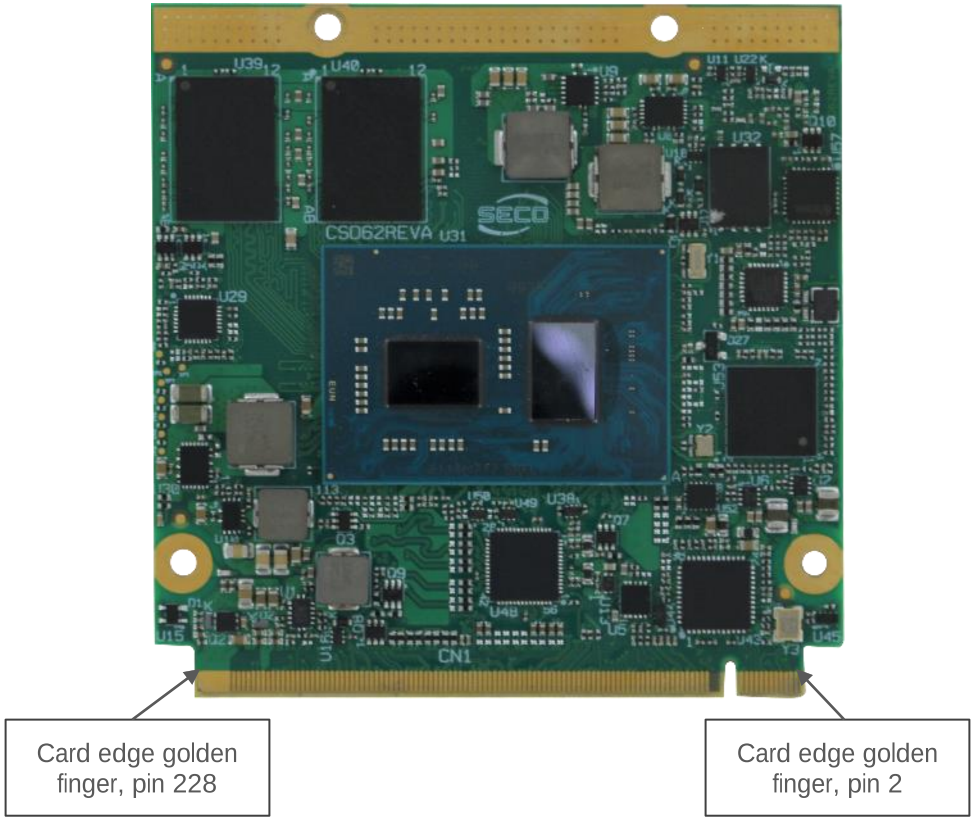
- Introduction
- Connectors description

3.1 Introduction

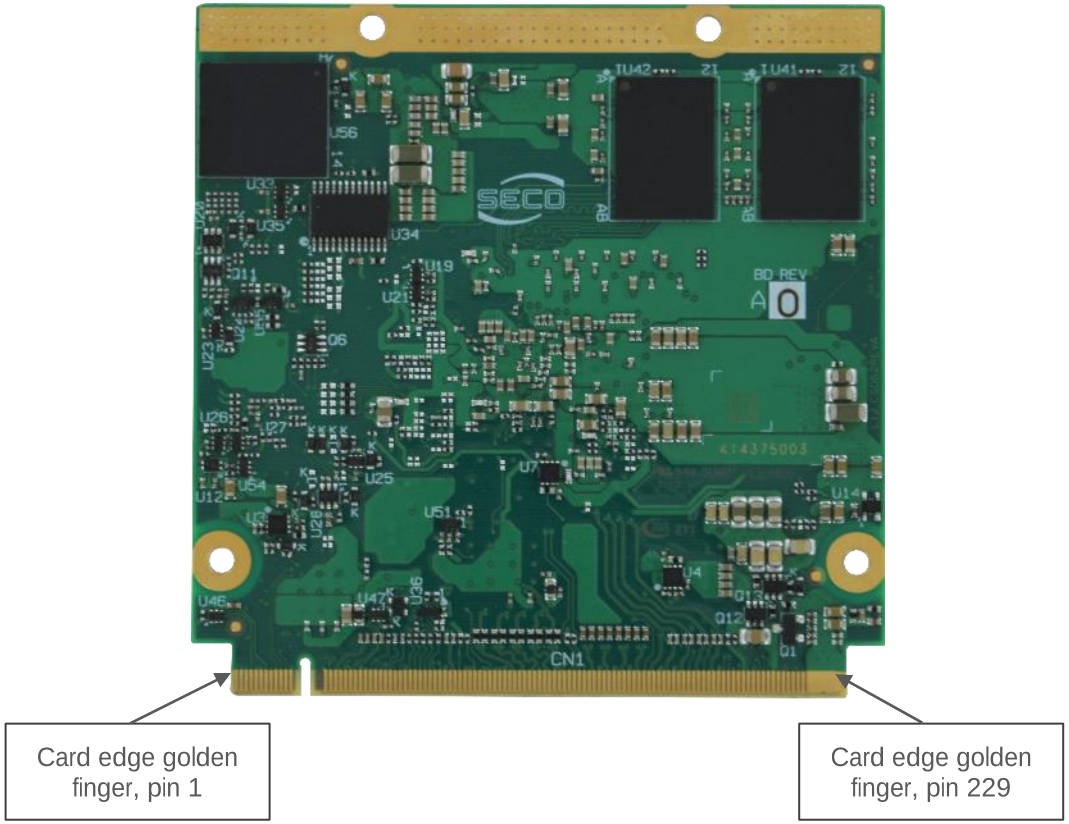
According to Qseven® specifications, all interfaces to the board are available through a single card edge connector.

Moreover, an additional Fan connector has been placed on the right side of the board, in order to allow an easier connection of active heatsinks to the module

TOP SIDE


Card edge golden finger, pin 228
Card edge golden finger, pin 2

BOTTOM SIDE


Card edge golden finger, pin 1
Card edge golden finger, pin 229

3.2 Connectors description

3.2.1 Qseven® Connector

According to Qseven® specifications, all interface signals are reported on the card edge connector, which is a 230-pin Card Edge that can be inserted into standard 230 pin MXM connectors, as described in Qseven® specifications.

Not all signals contemplated in Qseven® standard are implemented on MXM connector, due to the functionalities really implemented on the board. Therefore, please refer to the following table for a list of effective signals reported on MXM connector.

For accurate signals description, please consult the following paragraphs.

NOTE: Even pins are available on top side of CPU board; odd pins are available on bottom side of CPU board. Please refer to board photos.

Qseven® Golden Finger Connector - CN4

		BOTTOM SIDE				TOP SIDE	
SIGNAL GROUP	Type	Pin name	Pin nr.	Pin nr.	Pin name	Type	SIGNAL GROUP
	PWR	GND	1	2	GND	PWR	
GBE	I/O	GBE_MDI3-	3	4	GBE_MDI2-	I/O	GBE
GBE	I/O	GBE_MDI3+	5	6	GBE_MDI2+	I/O	GBE
GBE	O	GBE_LINK100#	7	8	GBE_LINK1000#	O	GBE
GBE	I/O	GBE_MDI1-	9	10	GBE_MDI0-	I/O	GBE
GBE	I/O	GBE_MDI1+	11	12	GBE_MDI0+	I/O	GBE
GBE	O	GBE_LINK#	13	14	GBE_ACT#	O	GBE
	N.A.	N.C.	15	16	SUS_S5#	O	ACPI
ACPI	I	WAKE#	17	18	SUS_S3#	O	ACPI
ACPI	O	SUS_STAT#	19	20	PWRBTN#	I	ACPI
ACPI	I	SLP_BTN#	21	22	LID_BTN#	I	ACPI
	PWR	GND	23	24	GND	PWR	
	PWR	GND	25	26	PWGIN	I	ACPI
ACPI	I	BATLOW#	27	28	RSTBTN#	I	ACPI
SATA / SGMII	O	SATA0_TX+ / SGMII0_TX+	29	30	SATA1_TX+	O	SATA / SGMII
SATA / SGMII	O	SATA0_TX- / SGMII0_TX-	31	32	SATA1_TX-	O	SATA / SGMII

SATA / SGMII	O	SATA_ACT#	33	34	GND	PWR	
SATA / SGMII	I	SATA0_RX+ / SGMII0_RX+	35	36	SATA1_RX+ / SGMII0_RX+	O	SATA / SGMII
SATA / SGMII	I	SATA0_RX- / SGMII0_RX-	37	38	SATA1_RX- / SGMII0_RX-	O	SATA / SGMII
	PWR	GND	39	40	GND	PWR	
MISC	I	BIOS_DISABLE#	41	42	SDIO_CLK	O	SDIO
SDIO	I	SDIO_CD#	43	44	N.C.	N.A.	
SDIO	I/O	SDIO_CMD	45	46	SDIO_WP	I	SDIO
SDIO	O	SDIO_PWR#	47	48	SDIO_DAT1	I/O	SDIO
SDIO	I/O	SDIO_DAT0	49	50	SDIO_DAT3	I/O	SDIO
SDIO	I/O	SDIO_DAT2	51	52	N.C.	N.A.	
	N.A.	N.C.	53	54	N.C.	N.A.	
	N.A.	N.C.	55	56	USB_OTG_PEN	O	USB
	PWR	GND	57	58	GND	PWR	
AUDIO	O	HDA_SYNC	59	60	SMB_CLK	I/O	MISC
AUDIO	O	HDA_RST#	61	62	SMB_DAT	I/O	MISC
AUDIO	O	HDA_BCLK	63	64	SMB_ALERT#	I/O	MISC
AUDIO	I	HDA_SDI	65	66	GP0_I2C_CLK	I/O	MISC
AUDIO	O	HDA_SDO	67	68	GP0_I2C_DAT	I/O	MISC
MISC	I	THRM#	69	70	WDTRIG#	I	MISC
MISC	O	THRMTRIP#	71	72	WDOUT	O	MISC
	PWR	GND	73	74	GND	PWR	
USB	I/O	USB_SSTX0-	75	76	USB_SSRX0-	I/O	USB
USB	I/O	USB_SSTX0+	77	78	USB_SSRX0+	I/O	USB
USB	I	USB_6_7_OC#	79	80	USB_4_5_OC#	I	USB
USB	I/O	USB_P5-	81	82	USB_P4-	I/O	USB
USB	I/O	USB_P5+	83	84	USB_P4+	I/O	USB
USB	I	USB_2_3_OC#	85	86	USB_0_1_OC#	I	USB
USB	I/O	USB_P3-	87	88	USB_P2-	I/O	USB
USB	I/O	USB_P3+	89	90	USB_P2+	I/O	USB
USB	I	USB_VBUS	91	92	USB_ID	O	USB

USB	I/O	USB_P1-	93	94	USB_P0-	I/O	USB
USB	I/O	USB_P1+	95	96	USB_P0+	I/O	USB
	PWR	GND	97	98	GND	PWR	
LVDS/eDP	O	LVDS_A0+ / eDP0_TX0+	99	100	LVDS_B0+	O	LVDS
LVDS/eDP	O	LVDS_A0- / eDP0_TX0-	101	102	LVDS_B0-	O	LVDS
LVDS/eDP	O	LVDS_A1+ / eDP0_TX1+	103	104	LVDS_B1+	O	LVDS
LVDS/eDP	O	LVDS_A1- / eDP0_TX1-	105	106	LVDS_B1-	O	LVDS
LVDS/eDP	O	LVDS_A2+ / eDP0_TX2+	107	108	LVDS_B2+	O	LVDS
LVDS/eDP	O	LVDS_A2- / eDP0_TX2-	109	110	LVDS_B2-	O	LVDS
LVDS/eDP	O	LVDS_PPEN	111	112	LVDS_BLEN	O	LVDS/eDP
LVDS/eDP	O	LVDS_A3+ / eDP0_TX3+	113	114	LVDS_B3+	O	LVDS
LVDS/eDP	O	LVDS_A3- / eDP0_TX3-	115	116	LVDS_B3-	O	LVDS
	PWR	GND	117	118	GND	PWR	
LVDS	O	LVDS_A_CLK+ / eDP0_AUX+	119	120	LVDS_B_CLK+	O	LVDS
LVDS	O	LVDS_A_CLK- / eDP0_AUX-	121	122	LVDS_B_CLK-	O	LVDS
LVDS/eDP	O	LVDS_BLT_CTRL	123	124	HDMI_CEC	I/O	HDMI
LVDS	O	LVDS_DID_DAT	125	126	eDP0_HPD#	I	eDP
LVDS	O	LVDS_DID_CLK	127	128	DP_HPD#	I	DP
CAN	O	CAN0_TX	129	130	CAN0_RX	I	CAN
HDMI/DP	O	TMDS_CLK+ / DP_LANE3+	131	132	USB_SSTX1-	I/O	USB
HDMI/DP	O	TMDS_CLK- / DP_LANE3-	133	134	USB_SSTX1+	I/O	USB
	PWR	GND	135	136	GND	PWR	
HDMI/DP	O	TMDS_TX1+ / DP_LANE1+	137	138	DP_AUX+	I/O	DP
HDMI/DP	O	TMDS_TX1- / DP_LANE1-	139	140	DP_AUX-	I/O	DP
	PWR	GND	141	142	GND	PWR	
HDMI/DP	O	TMDS_TX0+ / DP_LANE2+	143	144	USB_SSRX1-	I/O	USB
HDMI/DP	O	TMDS_TX0- / DP_LANE2-	145	146	USB_SSRX1+	I/O	USB
	PWR	GND	147	148	GND	PWR	
HDMI/DP	O	TMDS_TX2+ / DP_LANE0+	149	150	HDMI_CTRL_DAT	I/O	HDMI
HDMI/DP	O	TMDS_TX2- / DP_LANE0-	151	152	HDMI_CTRL_CLK	I/O	HDMI

HDMI	I	HDMI_HPD#	153	154	DP++_HPD#	I	DP
PCI-E	O	PCIE_CLK_REF+	155	156	PCIE_WAKE#	I	PCI-E
PCI-E	O	PCIE_CLK_REF-	157	158	PCIE_RST#	O	PCI-E
	PWR	GND	159	160	GND	PWR	
PCI-E	O	PCIE3_TX+	161	162	PCIE3_RX+	I	PCI-E
PCI-E	O	PCIE3_TX-	163	164	PCIE3_RX-	I	PCI-E
	PWR	GND	165	166	GND	PWR	
PCI-E	O	PCIE2_TX+	167	168	PCIE2_RX+	I	PCI-E
PCI-E	O	PCIE2_TX-	169	170	PCIE2_RX-	I	PCI-E
UART	O	UART0_TX	171	172	UART0_RTS#	O	UART
PCI-E	O	PCIE1_TX+	173	174	PCIE1_RX+	I	PCI-E
PCI-E	O	PCIE1_TX-	175	176	PCIE1_RX-	I	PCI-E
UART	I	UART0_RX	177	178	UART0_CTS#	I	UART
PCI-E	O	PCIE0_TX+	179	180	PCIE0_RX+	I	PCI-E
PCI-E	O	PCIE0_TX-	181	182	PCIE0_RX-	I	PCI-E
	PWR	GND	183	184	GND	PWR	
LPC / GPIO	I/O	LPC_AD0 / GPIO0	185	186	LPC_AD1 / GPIO1	I/O	LPC / GPIO
LPC / GPIO	I/O	LPC_AD2 / GPIO2	187	188	LPC_AD3 / GPIO3	I/O	LPC / GPIO
LPC / GPIO	O	LPC_CLK / GPIO4	189	190	LPC_FRAME# / GPIO5	I/O	LPC / GPIO
LPC / GPIO	I/O	SERIRQ / GPIO6	191	192	LPC_LDRQ# / GPIO7	I/O	LPC / GPIO
	PWR	VCC_RTC (+3.3V_A)	193	194	SPKR	O	MISC
MISC	I	FAN_TACHOIN	195	196	FAN_PWM_OUT	O	MISC
	PWR	GND	197	198	GND	PWR	
SPI	O	SPI_MOSI	199	200	SPI_CS0#	O	SPI
SPI	I	SPI_MISO	201	202	SPI_CS1#	O	SPI
SPI	O	SPI_CLK	203	204	MFG_NC4	N.A.	MFG
	PWR	+5V_A	205	206	+5V_A	PWR	
MFG	I	SOC_UART0_RTS#	207	208	SOC_UART0_RX	O	MFG
MFG	I	SOC_UART0_TX	209	210	SOC_UART0_CTS#	O	MFG
	N.A.	N.C.	211	212	N.C.	N.A.	

N.A.	N.C.	213	214	N.C.	N.A.
N.A.	N.C.	215	216	N.C.	N.A.
N.A.	N.C.	217	218	N.C.	N.A.
PWR	+5V_S	219	220	+5V_S	PWR
PWR	+5V_S	221	222	+5V_S	PWR
PWR	+5V_S	223	224	+5V_S	PWR
PWR	+5V_S	225	226	+5V_S	PWR
PWR	+5V_S	227	228	+5V_S	PWR
PWR	+5V_S	229	230	+5V_S	PWR

3.2.1.1 PCI Express interface signals

The board can offer externally four PCI Express lane, which are directly managed by the SOCs.

PCI express Gen 2.0 (5Gbps) is supported.

Here following the signals involved in PCI express management

PCIE0_TX+/PCIE0_TX-: PCI Express lane #0, Transmitting Output Differential pair

PCIE0_RX+/PCIE0_RX-: PCI Express lane #0, Receiving Input Differential pair

PCIE1_TX+/PCIE1_TX-: PCI Express lane #1, Transmitting Output Differential pair

PCIE1_RX+/PCIE1_RX-: PCI Express lane #1, Receiving Input Differential pair

PCIE2_TX+/PCIE2_TX-: PCI Express lane #2, Transmitting Output Differential pair

PCIE2_RX+/PCIE2_RX-: PCI Express lane #2, Receiving Input Differential pair

PCIE3_TX+/PCIE3_TX-: PCI Express lane #3, Transmitting Output Differential pair

PCIE3_RX+/PCIE3_RX-: PCI Express lane #3, Receiving Input Differential pair

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

PCIE_WAKE#: Qseven® Module's Wake Input, +3.3V_S voltage, with 10kΩ pull-up resistor;it must be externally driven by devices requiring waking up the system. On the carrier board, connect it directly to the PCI-e/miniPCI-e connector's WAKE# signal, or to WAKE# signal of any eventual PCI-e Controller present on the Carrier Board.

PCIE_RST#: Reset Signal that is sent from Qseven® Module to any PCI-e device available on the carrier board. It is a 3.3V_A active-low signal; it can be used directly to drive externally a single RESET Signal. In case Reset signal is needed for multiple devices, it is recommended to provide for a buffer on the carrier board.

The four PCI-e lanes available on the Qseven® card edge connector can be managed as a single PCI-e x4 port, 2 PCI-e x2 ports, one PCI-e x2 + 2 PCI-e ports x1 or 4 PCI-e x1 ports.

3.2.1.2 UART interface signals

According to the Qseven® Rel. 2.1 specifications, the board offers one UART interface, directly managed by the SOCs.

Here following the signals related to UART interface:

UART0_TX: UART Interface, Serial data Transmit (output) line, 3.3V_S electrical level.

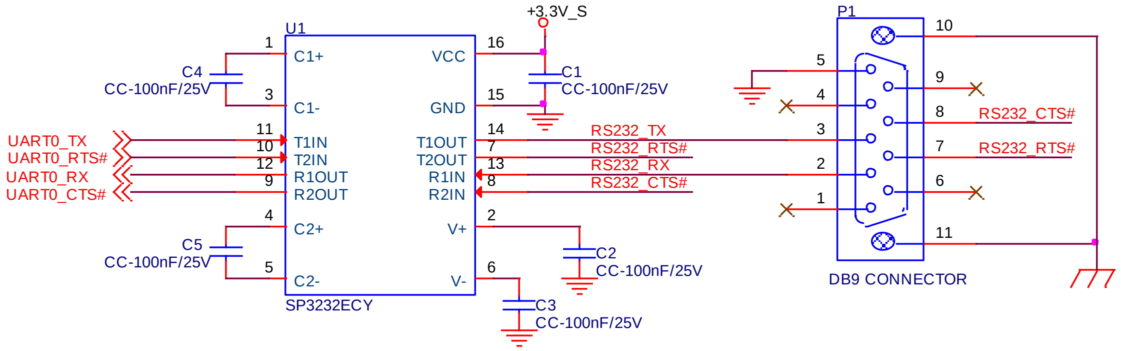
UART0_RX: UART Interface, Serial data Receive (input) line, 3.3V_S electrical level.

UART0_RTS#: UART Interface, Handshake signal, Request to Send (output) line, 3.3V_S electrical level.

UART0_CTS#: UART Interface, Handshake signal, Clear to Send (Input) line, 3.3V_S electrical level.

Please consider that interface is at TTL electrical level; therefore, please evaluate well the typical scenario of application. If it isn't needed explicitly 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 following schematic shows an example of implementation of RS-232 transceiver for the Carrier board



!

All schematics (henceforth also referred to as material) contained in this manual are provided by SECO S.r.l. for the sole purpose of supporting the customers' internal development activities.

The schematics are provided "AS IS". SECO makes no representation regarding the suitability of this material for any purpose or activity and disclaims all warranties and conditions with regard to said material, including but not limited to, all expressed or implied warranties and conditions of merchantability, suitability for a specific purpose, title and non-infringement of any third party intellectual property rights.

The customer acknowledges and agrees to the conditions set forth that these schematics are provided only as an example and that he will conduct an independent analysis and exercise judgment in the use of any and all material. SECO declines all and any liability for use of this or any other material in the customers' product design

3.2.1.3 Gigabit Ethernet signals

The Gigabit Ethernet interface is realized on the module by using a TI Gigabit Ethernet PHY transceiver DP83867, which is interfaced to Intel processor through RGMII interface.

Here following the signals involved in Gigabit Ethernet management

GBE_MDI0+/GBE_MDI0-: Media Dependent Interface (MDI) I/O differential pair #0

GBE_MDI1+/GBE_MDI1-: Media Dependent Interface (MDI) I/O differential pair #1

GBE_MDI2+/GBE_MDI2-: Media Dependent Interface (MDI) I/O differential pair #2, only used for 1Gbps Ethernet mode (not for 10/100Mbps modes)

GBE_MDI3+/GBE_MDI3-: Media Dependent Interface (MDI) I/O differential pair #3, only used for 1Gbps Ethernet mode (not for 10/100Mbps modes)

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

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

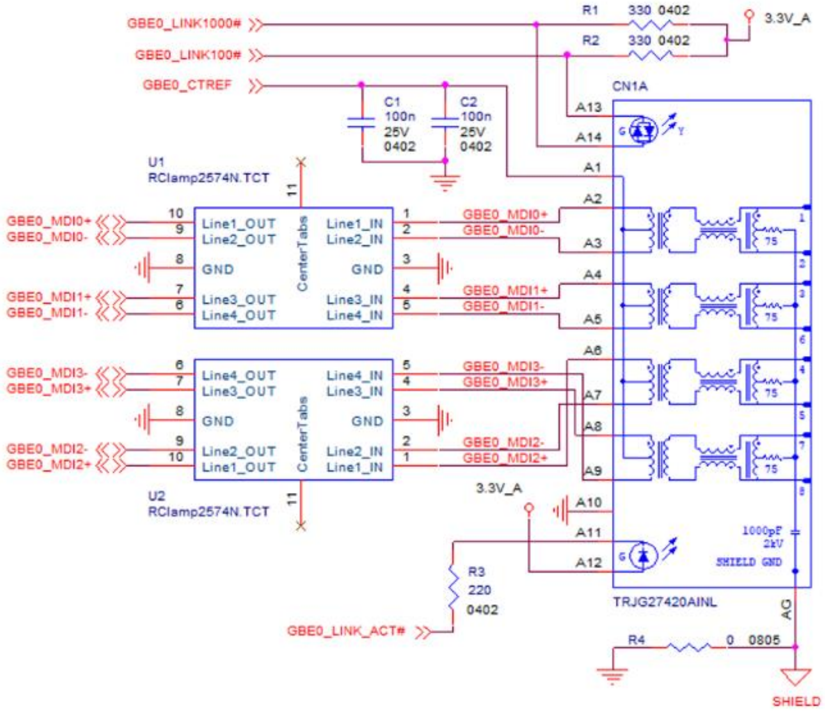
GBE_LINK100#: Ethernet controller 100Mbps link indicator, Active Low Output signal, electrical level +3.3V_A.

GBE_LINK1000#: Ethernet controller 1Gbps link indicator, Active Low Output signal, electrical level +3.3V_A.

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.

Please refer to the following schematics as an example of connection of Ethernet interface on the carrier board, with TVS diodes specifically designed to protect sensitive components which are connected to high-speed data and transmission lines from overvoltage caused by ESD. In this example, it is also present GBE_CTREF signal connected on pin #2 of the RJ-45 connector. TI Gigabit Ethernet PHY transceiver, however, doesn't need the analog powered centre tap, therefore the signal GBE_CTREF is not available on Qseven® golden finger connector



3.2.1.4 S-ATA signals

The SOCs offer two S-ATA interfaces, which are carried out on the golden finger connector.

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

Here following the signals related to SATA interface:

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

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

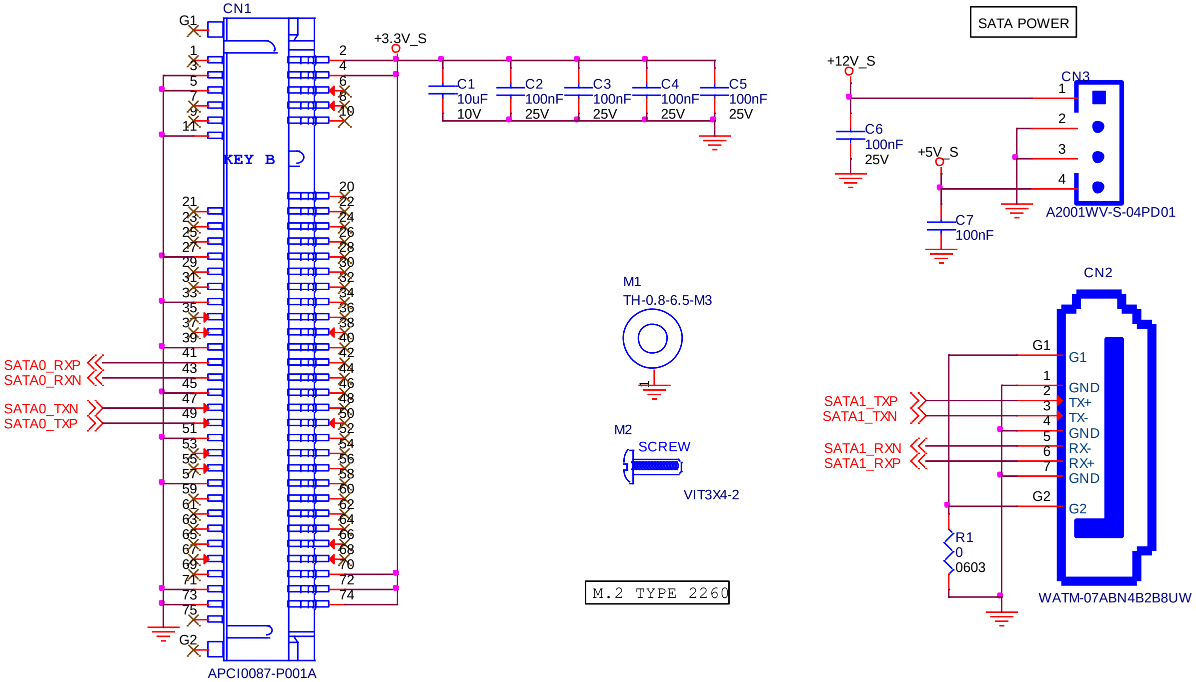
SATA1_TX+/SATA1_TX-: Serial ATA Channel #1 Transmit differential pair.

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

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

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

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



3.2.1.5 USB interface signals

The SoCs offer an xHCI controller, which is able to manage up to 6 Superspeed ports (i.e. USB 3.0 compliant), one of them also capable of OTG, plus two Ports able to work in USB 2.0 mode only. All these ports are also USB 2.0 backward compatible.

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_P0+/USB_P0-: Universal Serial Bus Port #0 differential pair (managed by xHCI port #1).

USB_P1+/USB_P1-: Universal Serial Bus Port #1 differential pair.

USB_P2+/USB_P2-: Universal Serial Bus Port #2 differential pair.

USB_P3+/USB_P3-: Universal Serial Bus Port #3 differential pair.

USB_P4+/USB_P4-: Universal Serial Bus Port #4 differential pair.

USB_P5+/USB_P5-: Universal Serial Bus Port #5 differential pair.

USB_SSRX0+/USB_SSRX0-: USB Super Speed Port #0 receive differential pair (managed by xHCI port #1)

USB_SSTX0+/USB_SSTX0-: USB Super Speed Port #0 transmit differential pair (managed by xHCI port #1).

USB_SSRX1+/USB_SSRX1-: USB Super Speed Port #1 receive differential pair (managed by xHCI port #0).

USB_SSTX1+/USB_SSTX1-: USB Super Speed Port #1 transmit differential pair (managed by xHCI port #0).

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

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

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

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

USB_VBUS: USB Client mode Power Input. This is an input signal which is used to detect the 5V power rail coming from the external USB Host

USB_ID: USB ID input pin, it must be tied to GND when USB Port #1 has to be set to work in Host mode. When not driven, USB Port#1 will work in Client mode.

USB_OTG_PEN: USB Power enable pin for USB Port 1. Active High Output signal, electrical level +3.3V_A. This signal has to be used to enable the Power rail of the USB Port #1 when working in Host mode

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

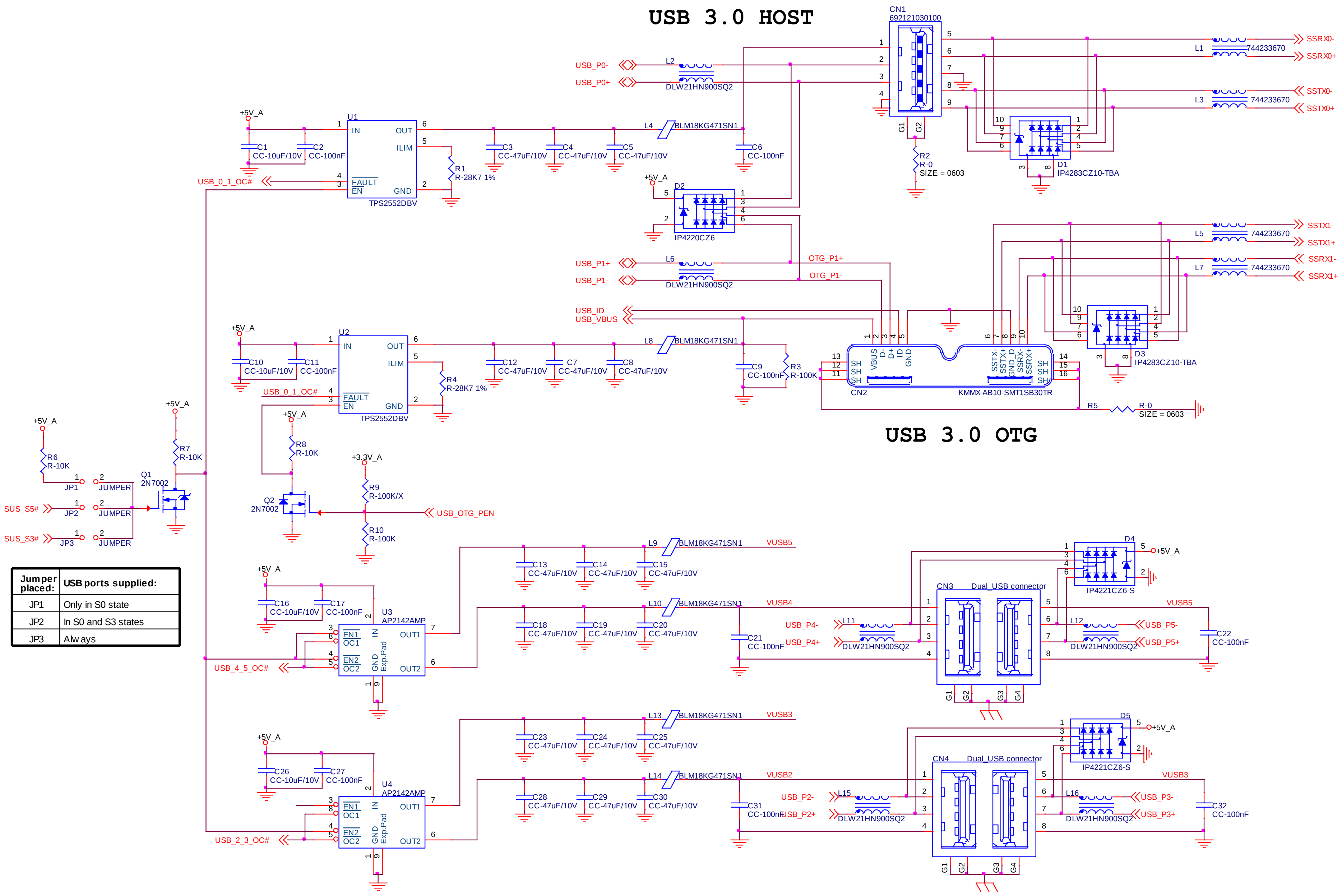
For EMI/ESD protection, common mode chokes on USB data lines, and clamping diodes on USB data and voltage lines, are also needed.

The schematics in the following page show an example of implementation on the Carrier Board.

In there:

- USB ports #2, #3, #4 and #5 are carried out to standard USB 2.0 Type A receptacles;
- USB 2.0 port #0, along with the Superspeed USB port #0, is carried to a standard USB 3.0 Type A receptacle;
- USB 2.0 port #1, along with the Superspeed USB port #1, is carried to a standard USB 3.0 Type micro-AB receptacle for OTG functionalities.

For correct implementation of USB 3.0 connections, the Superspeed port #0 must be paired with USB 2.0 port #0, and the Superspeed port #1 must be paired with USB 2.0 port #1.



Jumper placed:	USB ports supplied:
JP1	Only in S0 state
JP2	In S0 and S3 states
JP3	Always

3.2.1.6 SD interface signals

The SoCs offer one SD Card controller, able to support SD Card 3.0 interface.

Such an SD controller complies with SD Host Controller Standard Specification version 3.01.

The SD port is externally accessible through the golden edge finger connector, and can work in 1-bit and 4-bit mode.

Signals involved with SD interface are the following:

SDIO_PWR#: SD power enable. Active Low Output signal, electrical level +3.3V_S. This signal can be used on the Carrier board to enable the power line for the SD card.

SDIO_CD#: Card Detect Input. Active Low Signal, electrical level +3.3V_S with 100kΩ pull-up resistor. This signal must be externally pulled low to signal that a SD Card Device is present.

SDIO_CLK: Clock Line (output), 50MHz maximum frequency for High Speed Mode.

SDIO_CMD: Command/Response line. Bidirectional signal, electrical level +3.3V_S, used to send command from the Host to the connected card, and to send the response from the card to the Host.

SDIO_WP: Write Protect input, electrical level +3.3V_S with 100kΩ pull-up resistor. It is used to communicate the status of Write Protect switch of the external SD card. Since microSD cards don't manage this signal, it is important that, when designing carrier boards with microSD slots, this signal must be tied to GND, otherwise the OS will always consider the card as protected from writing.

SDIO_DAT[0÷3]: SD Card data bus. SDIO_DAT0 signal is used for all communication modes. SDIO_DAT[1÷3] signals are required for 4-bit communication mode.

3.2.1.7 Audio interface signals

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

Here following the signals related to HD Audio interface:

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

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

HDA_BCLK: HD Audio Serial Bit Clock signal. 24MHz serial data clock generated by the SoC's HD audio controller, output from the module to the Carrier board, electrical level +3.3V_S.

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

HDA_SDI: HD Audio Serial Data In signal. Input to the module from the Carrier board, electrical level +3.3V_S.

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

3.2.1.8 LVDS Flat Panel signals

The SoCs offer two multi-purpose Digital Display Interfaces, which allow the implementation of HDMI/DVI, Display Port (DP) or embedded Display Port (eDP), and a dedicated eDP interface.

The LVDS interface, which is frequently used in many application fields, is not directly supported by the SOC.

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

> **!** Please remember that LVDS interface is not native for this Intel® family of SOCs, it is derived from an optional eDP-to-LVDS bridge. Depending on the factory option purchased, on the same pins it is possible to have available LVDS or eDP interface.
>
> Please take care of specifying if it is necessary LVDS interface or eDP, before placing an order of this product.

Here following the signals related to LVDS management:

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

LVDS_A1+/LVDS_A1-: LVDS Primary Channel #0 differential data pair #1.

LVDS_A2+/LVDS_A2-: LVDS Primary Channel #0 differential data pair #2.

LVDS_A3+/LVDS_A3-: LVDS Primary Channel #0 differential data pair #3.

LVDS_A_CLK+/LVDS_A_CLK-: LVDS Primary Channel #0 differential clock.

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

LVDS_B1+/LVDS_B1-: LVDS Secondary Channel #0 differential data pair #1.

LVDS_B2+/LVDS_B2-: LVDS Secondary Channel #0 differential data pair #2.

LVDS_B3+/LVDS_B3-: LVDS Secondary Channel #0 differential data pair #3.

LVDS_B_CLK+/LVDS_B_CLK-: LVDS Secondary Channel differential Clock

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

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

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

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

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

3.2.1.9 Embedded Display Port (eDP) signals

As described in the previous paragraph, the SoCs offer a native embedded Display Port (eDP) interface, compliant to eDP 1.3 specifications.

When the board is not configured with the eDP-to-LVDS bridge, then on the golden edge finger connector is available this native eDP interface, which allows supporting displays with a resolution up to 3840 x 2160 @ 60Hz.

Here following the signals related to eDP management:

eDP0_TX0+/eDP0_TX0-: eDP channel differential data pair #0.

eDP0_TX1+/eDP0_TX1-: eDP channel differential data pair #1.

eDP0_TX2+/eDP0_TX 2-: eDP channel differential data pair #2.

eDP0_TX3+/eDP0_TX3-: eDP channel differential data pair #3.

eDP0_AUX+/eDP0_AUX-: eDP channel differential auxiliary channel.

eDP0_HPD#: eDP channel Hot Plug Detect. Active Low Signal, +3.3V_S electrical level input with 100kΩ pull-up resistor.

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

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

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

3.2.1.10 HDMI interface signals

As told in the previous paragraph, the SoCs offer two Digital Display Interfaces, configurable to work in HDMI/DVI/DP++/eDP modes.

Digital Display Interface #0, in particular, is used to implemented HDMI or Multimode Display Port interface.

> **!** Please be aware that the board is factory configured to have HDMI or Multimode Display Port interface.
>
> If the board purchased is in HDMI configuration, then voltage level shifters on the carrier board are not necessary (they can also interfere with regular working of the board). When placing an order of this product, please take care of specifying if it must have HDMI interface or DP++.

Signals involved in HDMI management are the following:

TMDS_CLK+/TMDS_CLK-: TMDS differential Clock.

TMDS_TX0+/TMDS_TX0-: TMDS differential pair #0

TMDS_TX1+/TMDS_TX1-: TMDS differential pair #1

TMDS_TX2+/TMDS_TX2-: TMDS differential pair #2

HDMI_CTRL_DAT: DDC Data line for HDMI panel. Bidirectional signal, electrical level +3.3V_S with a 2k2Ω pull-up resistor.

HDMI_CTRL_CLK: DDC Clock line for HDMI panel. Bidirectional signal, electrical level +3.3V_S with a 2k2Ω pull-up resistor.

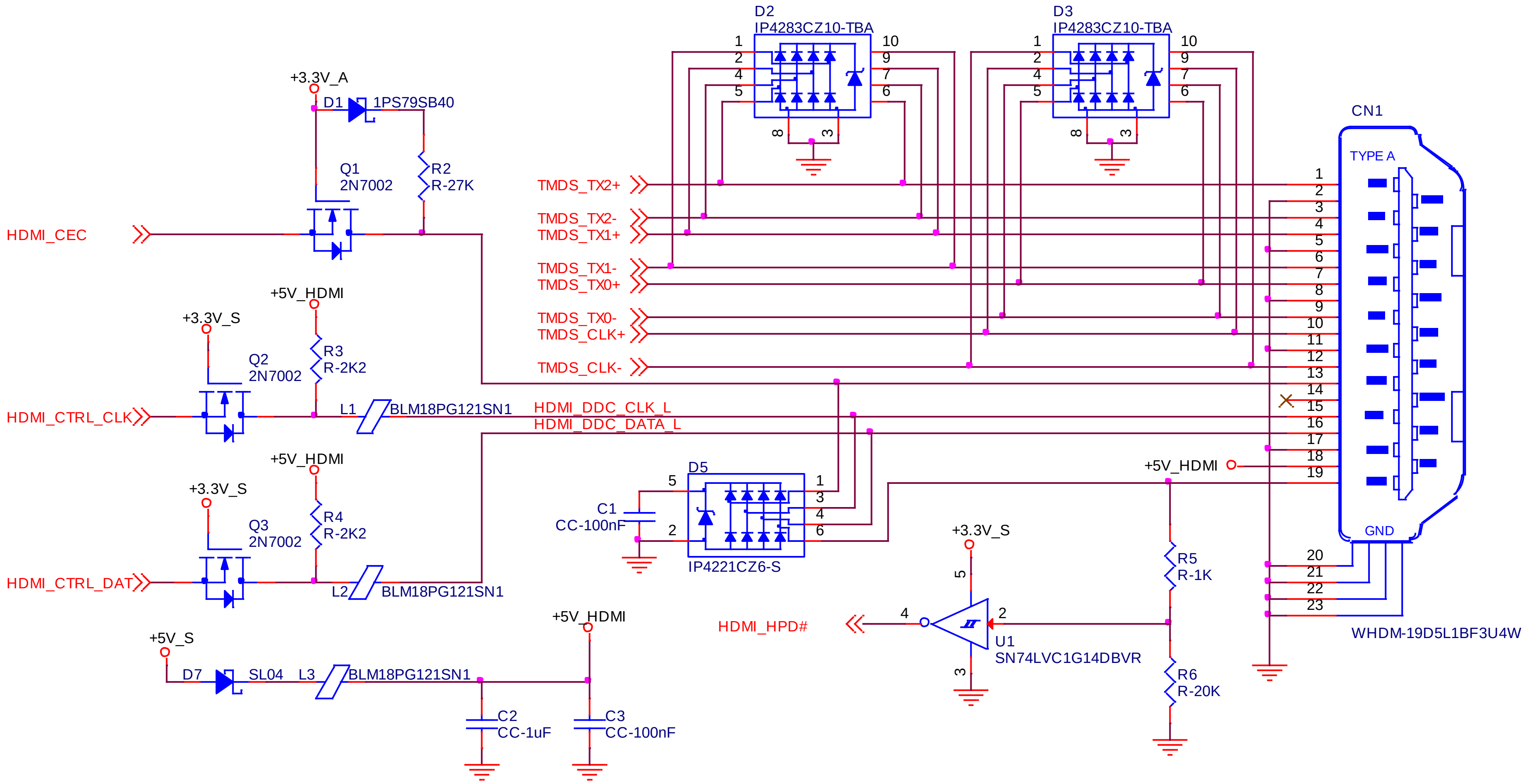
HDMI_CEC: HDMI Consumer Electronics Control (CEC) Line. Bidirectional signal, electrical level +3.3V_S. According to Qseven® specifications, the signal is, in reality, a General Purpose 1_wire bus interface, that can be used for implementation of HDMI_CEC. Real usage of this signal depends on the board dedicated API libraries.

HDMI_HPD#: Hot Plug Detect Input signal. +3.3V_S electrical level signal, active low with 100kΩ pull-up resistor. Please consider that HDMI specification assume that the Hot Plug signal is active high, and at +5V_S level. An inverting voltage level shifter is therefore needed on the Carrier board to ensure the working of HDMI port

Please be aware that it is not necessary to implement voltage level shifter for TMDS differential pairs on the Carrier board, but such level shifters are still necessary on Control data/Clock signals, as well as for Hot Plug Detect signal.

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

Please refer to the following schematics as an example of implementation of HDMI connection + voltage level shifters on the carrier board.



D2
IP4283CZ10-TBA
D3
IP4283CZ10-TBA
+3.3V_A
D1
1PS79SB40
Q1
2N7002
R2
R-27K
HDMI_CEC
TMDS_TX2+
TMDS_TX2-
TMDS_TX1+
TMDS_TX1-
TMDS_TX0+
TMDS_TX0-
TMDS_CLK+
TMDS_CLK-
CN1
TYPE A
GND
+5V_HDMI
+3.3V_S
Q2
2N7002
R3
R-2K2
HDMI_CTRL_CLK
L1
BLM18PG121SN1
HDMI_DDC_CLK_L
HDMI_DDC_DATA_L
+5V_HDMI
+3.3V_S
Q3
2N7002
R4
R-2K2
HDMI_CTRL_DAT
L2
BLM18PG121SN1
D5
C1
CC-100nF
IP4221CZ6-S
+5V_HDMI
+3.3V_S
R5
R-1K
HDMI_HPD#
U1
SN74LVC1G14DBVR
R6
R-20K
WHDM-19D5L1BF3U4W
+5V_S
D7
SL04
L3
BLM18PG121SN1
+5V_HDMI
C2
CC-1uF
C3
CC-100nF

3.2.1.11 DP interface signals

As told in the previous paragraph, the Intel® Bay Trail family of SOCs offers two Digital Display Interfaces, configurable to work in HDMI/DVI/DP/eDP modes.

Digital Display Interface #0, in particular, is used to implemented HDMI or Multimode Display Port interface.

Please be aware that this interface is a multimode Display Port: this means that it is possible to use it directly for the connection of Display Port compatible monitors or converted to HDMI/DVI interface on the carrier board or on the external connector (by using an adapter)

If the board purchased is in DP configuration, then the following signals will be available on Qseven® golden finger connector:

DP_LANE3+/DP_LANE3-: Display Port differential pair #3.

DP_LANE2+/DP_LANE2-: Display Port differential pair #2.

DP_LANE1+/DP_LANE1-: Display Port differential pair #1

DP_LANE0+/DP_LANE0-: Display Port differential pair #0

DP_AUX+/DP_AUX-: Display Port auxiliary channel differential pair.

DP_HPD#. DisplayPort Hot Plug Detect Input signal. +3.3V_S electrical level signal, active low with 100kΩ pull-up resistor. This signal was present on Qseven specifications until rev. 1.2, while it has been deleted with Qseven specifications rev. 2.1, since the Hot Plug signal for Display Port had been merged with the HPD signal for HDMI. Qseven® specification Errata Sheet for version 2.1, published by SGET consortium, reintroduced this signal for compatibility with Qseven® modules Rel 1.2 compliant. On the board, this signal is electrically tied to DPHDMI_HPD#.

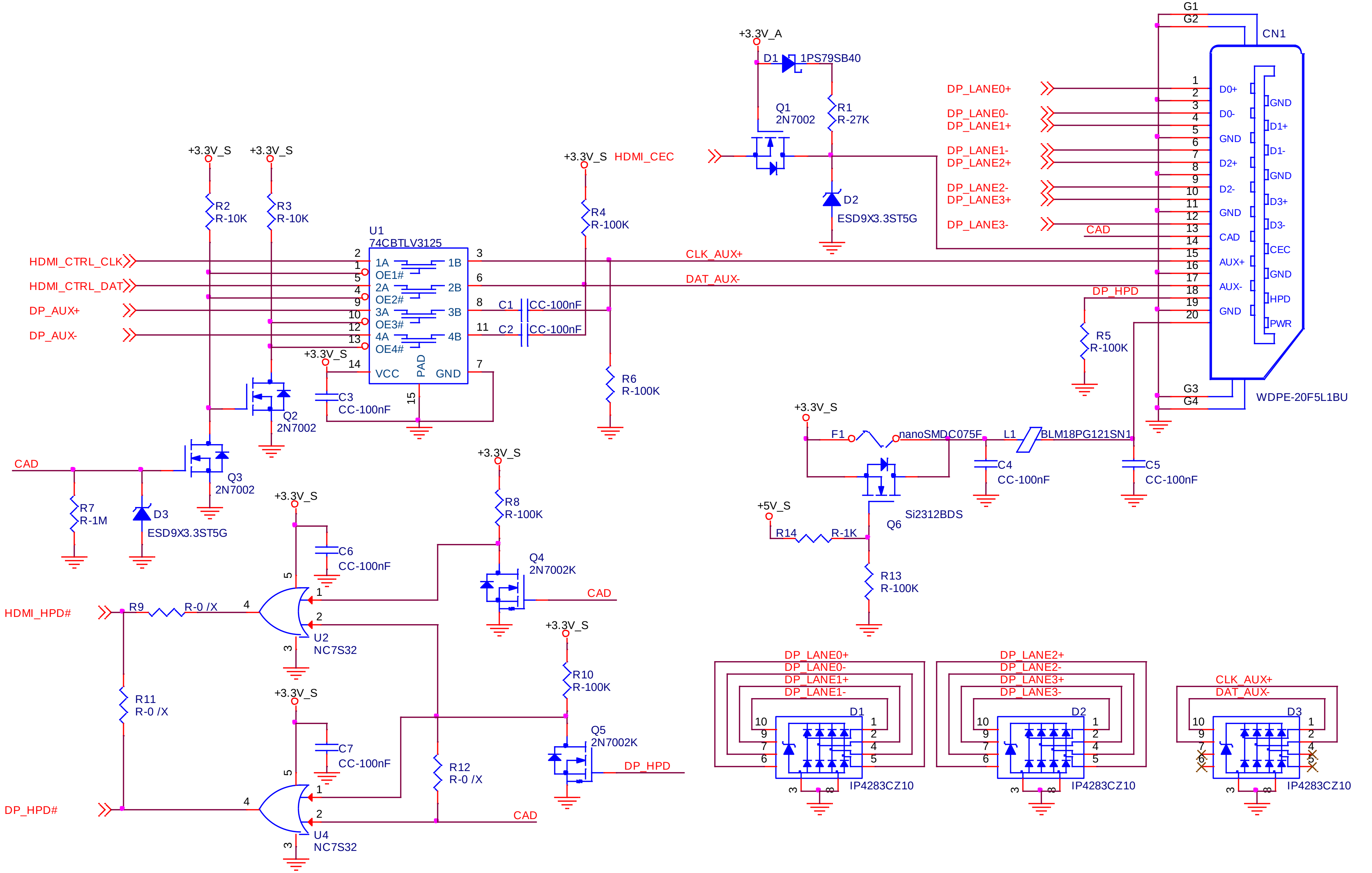
The following signals, used only for HDMI interface, are also available, for a correct implementation, on the Carrier Board, of a multi-mode Display Port connection.

HDMI_CTRL_DAT: DDC Data line for HDMI panel. Bidirectional signal, electrical level +3.3V_S with a 2k2Ω pull-up resistor.

HDMI_CTRL_CLK: DDC Clock line for HDMI panel. Bidirectional signal, electrical level +3.3V_S with a 2k2Ω pull-up resistor.

HDMI_CEC: HDMI Consumer Electronics Control (CEC) Line. Bidirectional signal, electrical level +3.3V_S. According to Qseven® specifications, the signal is, in reality, a General Purpose 1_wire bus interface, that can be used for implementation of HDMI_CEC. Real usage of this signal depends on the board dedicated API libraries.

Please refer to the following schematics as an example of implementation of multimode DisplayPort connection on the carrier board, which will allow the use of external adapters for the conversion to HDMI/DVI.


+3.3V_S
+3.3V_S
R2
R-10K
R3
R-10K
HDMI_CTRL_CLK
HDMI_CTRL_DAT
DP_AUX+
DP_AUX-
U1
74CBTLV3125
1A
OE1#
2A
OE2#
3A
OE3#
4A
OE4#
1B
2B
3B
4B
VCC
PAD
GND
+3.3V_S
C3
CC-100nF
Q2
2N7002
CAD
R7
R-1M
D3
ESD9X3.3ST5G
Q3
2N7002
+3.3V_S
HDMI_CEC
R4
R-100K
C1
CC-100nF
C2
CC-100nF
R6
R-100K
CLK_AUX+
DAT_AUX-
+3.3V_A
D1
1PS79SB40
Q1
2N7002
R1
R-27K
D2
ESD9X3.3ST5G
DP_LANE0+
DP_LANE0-
DP_LANE1+
DP_LANE1-
DP_LANE2+
DP_LANE2-
DP_LANE3+
DP_LANE3-
CAD
DP_HPD
R5
R-100K
G1
G2
CN1
D0+
D0-
GND
D2+
D2-
GND
CAD
AUX+
AUX-
GND
GND
D1+
D1-
GND
D3+
D3-
CEC
GND
HPD
PWR
G3
G4
WDPE-20F5L1BU
+3.3V_S
F1
nanoSMDC075F
L1
BLM18PG121SN1
C4
CC-100nF
C5
CC-100nF
Si2312BDS
Q6
+5V_S
R14
R-1K
R13
R-100K
+3.3V_S
R8
R-100K
Q4
2N7002K
CAD
+3.3V_S
C6
CC-100nF
HDMI_HPD#
R9
R-0 /X
U2
NC7S32
R11
R-0 /X
+3.3V_S
R10
R-100K
Q5
2N7002K
DP_HPD
+3.3V_S
C7
CC-100nF
R12
R-0 /X
CAD
DP_HPD#
U4
NC7S32
DP_LANE0+
DP_LANE0-
DP_LANE1+
DP_LANE1-
D1
IP4283CZ10
DP_LANE2+
DP_LANE2-
DP_LANE3+
DP_LANE3-
D2
IP4283CZ10
CLK_AUX+
DAT_AUX-
D3
IP4283CZ10

3.2.1.12 LPC interface signals

According to Qseven® specifications rel. 2.1, on the golden edge finger connector there are 8 pins that are used for implementation of Low Pin Count (LPC) Bus interface.

> **!**
>
> Warning: Although the Qseven® specification states that pins 185-192 can be used for the implementation of the LPC bus or as 8 GPIOs, this option is intended only for the manufacturers of the modules who are free to choose the option they deem more appropriate.
>
> On this product, the aforementioned pins have been dedicated to the LPC bus; use of these pins for different implementations other than LPC (i.e. as GPIOs) is therefore not possible.

The following signals are available:

LPC_AD[0÷3]: LPC address, command and data bus, bidirectional signal, +3.3V_S electrical level.

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

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

SERIRQ: LPC Serialised IRQ request, bidirectional line, +3.3V_S electrical level. This signal is used only by peripherals requiring Interrupt support.

3.2.1.13 SPI interface signals

The Intel® Bay Trail family of SOCs offers also one dedicated controller for Serial Peripheral Interface (SPI), which can be used for connection of EEPROMs and Serial Flash devices. This interface does not support platform firmware (BIOS).

SPI interface supports master mode only can support speed up to 15Mbps.

Signals involved with SPI management are the following:

SPI_MOSI: SPI Master Out Slave In, Output from Qseven® module to SPI devices embedded on the Carrier Board. Electrical level +3.3V_S.

SPI_MISO: SPI Master In Slave Out, Input to Qseven® module from SPI devices embedded on the Carrier Board. Electrical level +3.3V_S.

SPI_CLK: SPI Clock Output to carrier board's SPI embedded devices. Electrical level +3.3V_S.

SPI_CS0#: SPI Chip select #0, active low output signal (+3.3V_S electrical level).

SPI_CS1#: SPI Chip select #1, active low output signal (+3.3V_S electrical level).

3.2.1.14 Power Management signals

According to Qseven® specifications, on the golden edge finger connector there is a set of signals that are used to manage the power rails and power states.

The signals involved are:

PWGIN: Power Good Input, +5V_S tolerant active high signal. It must be driven on 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.

PWRBTN#: Power Button Input, active low, +3.3V_A electrical level signal with 100kΩ pull-up resistorand. 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.

RSTBTN#: Reset Button Input, active low, +3.3V_A electrical level signal with 100kΩ pull-up resistor. This signal can be connected to a momentary push-button: a pulse to GND of this signal will reset the Qseven® module.

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

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

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

SUS_S5#: S4 status output, active low +3.3V_A 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 S4 and S5 (Suspend to Disk / Soft Off) power states.

SLP_BTN#: Sleep button Input, active low +3.3V_A 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.

LID_BTN#: LID button Input, active low +3.3V_A 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.

3.2.1.15 Miscellaneous signals

Here following, a list of Qseven® compliant signals that complete the features of the board module.

SMB_CLK: SM Bus control clock line for System Management. Bidirectional signal, electrical level +3.3V_A with a 1kΩ pull-up resistor. It is managed by the SOCs' PCU System Management Bus controller.

SMB_DAT: SM Bus control data line for System Management. Bidirectional signal, electrical level +3.3V_A with a 1kΩ pull-up resistor. It is managed by the SOCs' PCU System Management Bus controller.

SMB_ALERT#: SM Bus Alert line for System Management. Bidirectional signal, electrical level +3.3V_A with a 1kΩ pull-up resistor. It is managed by the SOCs' PCU System Management Bus controller. Any device place on the SM Bus can drive this signal low to signal an event on the bus itself.

GP0_I2C_CLK: general purpose I2C Bus clock line. Bidirectional signal, electrical level +3.3V_S with a 1KΩ pull-up resistor. It is managed by the SOCs' I2C controller #2. I2C Bus is able to work in Standard mode (bitrate up to 100Kbps), Fast mode (bitrate up to 400Kbps), Fast-mode Plus (bitrate up to 1Mbps).

GP0_I2C_DAT: general purpose I2C Bus data line. Bidirectional signal, electrical level +3.3V_S with a 1kΩ pull-up resistor. It is managed by the SOCs' I2C controller #2.

WDTRIG#: Watchdog Trigger Input. It is an active low signal, +3.3V_S voltage, with 10kΩ pull-up resistor, managed by the STM32F100R4H6 microcontroller. This signal can be used to reset and restart, via Hardware, the internal Watchdog Timer (which is usually managed via Software using the board dedicated API - Application Program Interface - libraries).

WDOUT: Watchdog event indicator Output. It is an active high signal, +3.3V_S voltage, managed by the STM32F100R4H6 microcontroller. 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.

THRM#: Thermal Alarm Input. Active Low +3.3V_S voltage signal with 100kΩ pull-up resistor, directly managed by ST Microelectronics STM32F100R4H6 microcontroller. This input gives the possibility, to carrier board's hardware, to indicate to the main module an overheating situation, so that the SOC can begin thermal throttling.

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

FAN_TACHOIN: External FAN Tachometer Input. +3.3V_S voltage signal with 10kΩ pull-up resistor, directly managed by ST Microelectronics STM32F100R4H6 microcontroller.

FAN_PWM_OUT: PWM output for FAN speed management, +3.3V_S voltage signal. It is managed by ST Microelectronics STM32F100R4H6 microcontroller.

SPKR: Speaker output, +3.3V_S voltage signal, directly managed by the SoC.

3.2.1.16 Manufacturing signals

According to Qseven® Standard specifications, rel. 2.1, on pin designed as MFG_NCx (pins 204, 207÷210) are carried the JTAG signal necessary to program the board embedded microcontroller.

! The JTAG interface available on MFG_NCx pins is reserved only for the manufacturing phase; it must not be used by the customer.

It is not possible at all to use these pins to trace the software (for debug purposes)

Chapter 4.
BIOS SETUP

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

4.1 Aptio setup Utility

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

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

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

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

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

Right frame shows the key legend.

KEY LEGEND:

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

↑ / ↓ Select a setup item or a submenu

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

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

<F2> Previous Values

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

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

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

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

4.2 Main setup menu

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

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

Only two options can be configured:

4.2.1 System Date / System Time

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

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

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

4.3 Advanced menu

Menu Item	Options	Description
CPU Configuration	See submenu	CPU Configuration Parameters
Power & Performance	See submenu	Power & Performance Options
PCH-FW Configuration	See submenu	Configure Management Engine Technology Parameters
Trusted Computing	See submenu	Trusted Computing Settings
ACPI Settings	See submenu	System ACPI parameters
Serial Port Console Redirection	See submenu	Serial Port Console Redirection
AMI Graphic Output Protocol Policy	See submenu	User Selected Monitor Output by Graphic Output protocol
USB Configuration	See submenu	USB Configuration Parameters
Network Stack Configuration	See submenu	Network Stack Settings
NVMe Configuration	See submenu	NVMe Device Options Settings
SDIO Configuration	See submenu	SDIO Configuration Parameters
SMBIOS Information		SMBIOS Information
Super I/O Configuration	See submenu	Super I/O Setup Configuration Utility
Main Thermal Configuration	See submenu	Main Thermal Configuration
LVDS Configuration	See submenu	LVDS Configuration
Embedded Controller	See submenu	Embedded Controller
RAM Disk Configuration	See submenu	Add/remove RAM disks
User Password Management		Handle user's password
Driver Health		Health Status for the Drivers/Controllers

4.3.1 CPU Configuration

Menu Item	Options	Description
CPU Configuration		Shows board's specific SoC information
CPU Flex Ratio Override	Disabled / Enabled	Enable/Disable CPU Flex Ratio Programming
CPU Flex Ratio Settings	[1…63]	This value must be between Max Efficiency Ratio (LFM) and Maximum non-turbo ratio set by Hardware (HFM)
Hardware Prefetcher	Disabled / Enabled	To turn on/off the MLC streamer prefetcher
Intel (VMX) Virtualization Technology	Disabled / Enabled	When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology
PECI	Disabled / Enabled	Enable/Disable PECI
Active Processor Cores	All 1 2 3	Number of Cores to enable in each processor package
BIST	Disabled / Enabled	Enable/Disable BIST (Built-In Self Test) on reset
AP threads Idle Manner	HALT Loop MWAIT Loop RUN Loop	AP threads Idle Manner for waiting signal to run
AES	Disabled / Enabled	Enable/Disable AES (Advanced Encryption Standard)
MachineCheck	Disabled / Enabled	Enable/Disable MachineCheck
MonitorMWait	Disabled / Enabled	Enable/Disable MonitorMWait (MWAIT)
CPU SMM Enhancement	See Submenu	CPU SMM Enhancement
#AC Split Lock	Disabled / Enabled	Enable/Disable Alignment Check Exception (#AC). When enabled, this will assert an #AC when any atomic operation has an operand that crosses two cache lines

4.3.1.1 CPU SMM Enhancement

Menu Item	Options	Description
SMM Use Delay Indication	Disabled / Enabled	Enable/Disable usage of SMM_DELAYED MSR for MP sync in SMI
SMM Use Block Indication	Disabled / Enabled	Enable/Disable usage of SMM_BLOCKED MSR for MP sync in SMI

SMM Use SMM en-US Indication	Disabled / Enabled	Enable/Disable usage of SMM_ENABLE MSR for MP sync in SMI

4.3.2 Power & Performance

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

4.3.2.1 CPU - Power Management Control

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

Platform PL1 Enable	Enabled / Disabled	Enable/Disable Platform Power Limit 1 programming. If this option is enabled, it activates the PL1 value to be used by the processor to limit the average power of given time window
Platform PL1 Power	[0…4095875]	Platform Power Limit 1 Power in Milli Watts. BIOS will round to the nearest 1/8W when programming. Any value can be programmed between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). For 12.50W, enter 12500. This setting will act as the new PL1 value for the Package RAPL algorithm.
Platform PL1Time Window	0 / 1 / 2 / 3 / 4 / 5 / 6 / 7 / 8 / 10 / 12 / 14 / 16 / 20 / 24 / 28 / 32 / 40 / 48 / 56 / 64 / 80 / 96 / 112 / 128	Platform Power Limit 1 Time Window value in seconds. The value may vary from 0 to 128. 0 = default value. Indicates the time window over which Platform TDP value should be maintained
Platform PL2 Enable	Enabled / Disabled	Enable/Disable Platform Power Limit 2 programming. If this option is enabled, BIOS will program the default values for Platform Limit 2
Platform PL2 Power	[0…4095875]	Platform Power Limit 2 Power in Milli Watts. BIOS will round to the nearest 1/8W when programming. Any value can be programmed between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). For 12.50W, enter 12500. This setting will act as the new PL2 value for the Package RAPL algorithm.
Power Limit 4 Override	Enabled / Disabled	Enable/Disable Power Limit 4 override. If this option is disabled, BIOS will leave the default values for Poer Limit 4.
Power Limit 4	[0…4095875]	Platform Power Limit 4 in Milli Watts. BIOS will round to the nearest 1/8W when programming. For 12.50W, enter 12500. If the value is 0, BIOS leaves default value
Power Limit 4 Lock	Enabled / Disabled	Power Limit 4 MSR 601h Lock. When enabled PL4 configurations are locked during OS. When disabled PL4 configuration can be changed during OS
C states	Enabled / Disabled	Enable/Disable CPU Power Management. Allows CPU to go to C states when it's not 100% utilized
Enhanced C-states	Enabled / Disabled	Enable/Disable C1E. When enabled, CPU will switch to minimum speed when all cores enter C-state
C-State Auto Demotion	Disabled / C1	Configure C-State Auto Demotion
C-State Un-demotion	Disabled / C1	Configure C-State Un-demotion
Package C-State Demotion	Enabled / Disabled	Package C-State Demotion
Package C-State Un-demotion	Enabled / Disabled	Package C-State Un-demotion
CState Pre-Wake	Enabled / Disabled	Disable – Sets bit 30 of POWER_CTL MSR (0x1FC) to 1 to disable the Cstate Pre-Wake
IO MWAIT Redirection	Enabled / Disabled	When set, will map IO_read instructions sent to IO registers. PMG_IO_BASE_ADDRBASE+offset to MWAIT (offset)

Package C State Limit	C0/C1 / C2 / C3 / C6 / C7 / C7S / C8 / C9 / C10 / Cpu Default / Auto	Maximum Package C State Limit Setting. Cpu Default: Leaves to factory default value Auto: Intializes to deepest available Package C State Limit
• C6/C7 Short Latency Control (MSR 0x60B) • C6/C7 Long Latency Control (MSR 0x60C) • C8 Latency Control (MSR 0x633) • C9 Latency Control (MSR 0x634) • C10 Latency Control (MSR 0x635)	Time Unit (ns): 1 / 32 / 1024 / 32768 / 1048576 / 33554432 Latency: [0…1023]	Time Unit: Unit of measurement for IRTL value – bits [12:10] Latency: Interrupt Response Time Limit value – bits [9:0], Enter 0-1023
Thermal Monitor	Enabled / Disabled	Enable/Disable Thermal Monitor
Interrupt Redirection Mode Selection	Fixed Priority Round robin Hash Vector No Change	Interrupt Redirection Mode Select for logical Interrupts
Timed MWAIT	Enabled / Disabled	Enable/Disable Timed MWAIT Support
Custom P-state Table		Add Custom P-state Table --> Sets the number of custom P-states. At least 2 states must be present
EC Turbo Control Mode	Enabled / Disabled	Enable/Disable EC Turbo Control mode
AC Brick Capacity	90W AC Brick 65W AC Brick 75W AC Brick	Specify the AC Brick capacity
EC Polling Period	[1…255]	Count 1 to 255 for a range of 10ms to 2.55 seconds (1 count = 10ms)
EC Guard Band Value	[1…20]	Count 1 to 20 for a range of 1 Watt to 20 Watts
EC Algorithm Selection	[1…10]	Count 1 to 10 for Algorithm Selection
Energy Performance Gain	Enabled / Disabled	Enable/Disable Energy Performance Gain
EPG DIMM Idd3N	26 (default)	Active standby current (Idd3N) in milliamps from datasheet. Must be calculated on a per DIMM basis
EPG DIMM Idd3P	11 (default)	Active power-down current (Idd3P) in milliamps from datasheet. Must be calculated on a per DIMM basis
CPU Lock Configuration	See submenu	CPU Lock Configuration

4.3.2.1.1 View/Configure Turbo Options

Menu Item	Options	Description
Current Turbo Settings		Shows cores' specific Turbo information
Energy Efficient P-state	Enabled / Disabled	Enable/Disable Energy Efficient P-state feature. When set to 0, will disable access to ENERGY_PERFORMANCE_BIAS MSR and CPUID Function 6 ECX[3] will read 0 indicating no support for Energy Efficient policy setting. When set to 1 will enable access to ENERGY_PERFORMANCE_BIAS MSR
Package Power Limit MSR Lock	Enabled / Disabled	Enable/Disable locking of Package Power Limit settings. When enabled, PACKAGE_POWER_LIMIT MSR will be locked and a reset will be required to unlock the register
Power Limit 1 Override	Enabled / Disabled	Enable/Disable Power Limit 1 override. If this option is disabled, BIOS will program the default values for Power Limit 1 and Power Limit 1 Time Window.
Power Limit 1	[0…4095875]	Platform Power Limit 1 in Milli Watts. BIOS will round to the nearest 1/8W when programming. 0 = no custom override. For 12.50W, enter 12500. Overclocking SKU: Value must be between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). Other SKUs: This value must be between Min Power Limit and TDP Limit. If value is 0, BIOS leaves default value
Power Limit 1 Time Window	Enabled / Disabled	Platform Power Limit 1 Time Window value in seconds. The value may vary from 0 to 128. 0 = default value. Indicates the time window over which Platform TDP value should be maintained
Power Limit 2 Override	Enabled / Disabled	Enable/Disable Power Limit 1 override. If this option is disabled, BIOS will program the default values for Power Limit 2
Power Limit 2	[0…4095875]	Platform Power Limit 2 in Milli Watts. BIOS will round to the nearest 1/8W when programming. If the value is 0, BIOS will program this value as 1.25*TDP. For 12.50W, enter 12500. Processor applies policies such that the package power does not exceed this limit
1-Core Ratio Limit Override	[0…83]	1-Core Ratio Limit with range 0 to 83. The Minimum range may vary between Processors. This 1-Core Ratio Limit must be grater than or equal to 2-Core Ratio Limit, 3-Core Ratio Limit, 4-Core Ratio Limit
2-Core Ratio Limit Override	[0…83]	2-Core Ratio Limit with range 0 to 83. The Minimum range may vary between Processors. This 2-Core Ratio Limit must be less than or equal to 1-Core Ratio Limit
3-Core Ratio Limit Override	[0…83]	3-Core Ratio Limit with range 0 to 83. The Minimum range may vary between Processors. This 3-Core Ratio Limit must be less than or equal to 1-Core Ratio Limit
4-Core Ratio Limit Override	[0…83]	4-Core Ratio Limit with range 0 to 83. The Minimum range may vary between Processors. This 4-Core Ratio Limit must be less than or equal to 1-Core Ratio Limit
Energy Efficient Turbo	Enabled / Disabled	Enable/Disable Energy Efficient Turbo Feature. This feature will opportunistically lower the turbo frequency to increase efficiency. Recommended only to disable in overclocking situations where turbo frequency must remain constant. Otherwise, leave enabled.

4.3.2.1.2 CPU VR Settings

Menu Item	Options	Description
PSYS Slope	[0…200]	PSYS Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x9
PSYS Offset	[0…63999]	PSYS Offset defined in 1/1000 increments. Range is 0-63999. For an offset of 25.348, enter 25348. Uses BIOS VR mailbox command 0x9
PSYS Prefix	+ / -	Sets the offset value as positive or negative
PSYS Pmax Power	[0…8192]	PSYS Pmax power, defined in 1/8 Watt increments. Range 0-8192. For a Pmax of 125W, enter 1000. 0 = AUTO. Uses BIOS VR mailbox command 0xB
Acoustic Noise Settings	See submenu	Configure Acoustic Noise Settings for IA, GT and SA domains
VccIn VR Settings	See submenu	VccIn VR Settings
RFI Settings	See submenu	RFI Settings

4.3.2.1.2.1 Acoustic Noise Settings

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

4.3.2.1.2.2 VccIn VR Settings

Menu Item	Options	Description
VR Config Enable	Enabled / Disabled	VR Config Enable
AC Loadline	[0…6249]	AC Loadline defined in 1/100 mOhms. A value of 100 = 1.00 mOhm, and 1255 = 12.55 mOhm. Range is 0-6249 (0-62.49 mOhms). 0 = AUTO/HW default. Uses BIOS mailbox command 0x2

DC Loadline	[0…6249]	DC Loadline defined in 1/100 mOhms. A value of 100 = 1.00 mOhm, and 1255 = 12.55 mOhm. Range is 0-6249 (0-62.49 mOhms). 0 = AUTO/HW default. Uses BIOS mailbox command 0x2
PS Current Threshold1	[0…512]	PS Current Threashold1, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3
PS Current Threshold2	[0…512]	PS Current Threashold2, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3
PS Current Threshold3	[0…512]	PS Current Threashold3, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3
PS3 Enable	Enabled / Disabled	PS3 Enable/Disable. 0 – Disabled, 1 – Enabled. Uses BIOS VR mailbox command 0x3
PS4 Enable	Enabled / Disabled	PS4 Enable/Disable. 0 – Disabled, 1 – Enabled. Uses BIOS VR mailbox command 0x3
IMON Slope	[0…200]	IMON Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x4
IMON Offset	[0…63999]	IMON Offset defined in 1/1000 increments. Range is 0-63999. For an offset of 25.348, enter 25348. Uses BIOS VR mailbox command 0x4
IMON Prefix	+ / -	Sets the offset value as positive or negative
VR Current Limit	[0…512]	Voltage Regulator Current Limit (Icc Max). This value represents the Maximum instantaneous current allowed at any given time. The value is represented in 1/4 A increments. A value of 400 = 100A. 0 means AUTO. Uses BIOS VR mailbox command 0x6
TDC Enable	Enabled / Disabled	TDC Enable. 0 – Disable, 1 – Enable
TDC Current Limit	[0…32767]	TDC Current Limit, defined in 1/8 increments. Range 0-32767. For a TDC Current Limit of 125A, enter 1000. 0 = 0 Amps. Uses BIOS VR mailbox command 0x1A
TDC Time Window	[1…8, 10]	TDC Time Window, value in milliseconds. 1ms is default. Range from 1ms to 1ms, except for 9ms. 9ms has no valid encoding in the MSR definition
TDC Lock	Enabled / Disabled	TDC Lock

4.3.2.1.2.3 RFI Settings

Menu Item	Options	Description
RFI Current Frequency		Shows current RFI Frequency setting
RFI Frequency	[1300…1600]	Set desired RFI Frequency, in increments of 100KHz. The RFI Frequency Range is between 130 MHz to 160 MHz, and the default h/w frequency is 139.6 MHz. For a frequency of 139.6 MHz, enter 1396

RFI Spread Spectrum	[0…100]	Adjust the Spread Spectrum, in increments of 0.1%. For a spread of 5.0%, enter 50. The value of 0 will disable the FIVR FRI Spread Spectrum, Range 0-100 (0.0% to 10.0%)

4.3.2.1.3 CPU Lock Configuration

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

4.3.2.2 GT- Power Management Control

Menu Item	Options	Description
Maximum GTT frequency	Default Max Frequency / 100MHz / … *List of 50MHz increments* … / 1200MHz	Maximum GT frequency limited by the user. Choose between 200MHz (RPN) and 400MHz (RP0). Value beyond the range will be clipped to min/max supported by SKU
Disable Turbo GT frequency	Enabled / Disabled	Enabled: Disables Turbo GT frequency. Disabled: GT frequency is not limited

4.3.3 PCH-FW Configuration

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

Anti-Rollback SVN Configuration	See submenu	Configure Anti-Rollback SVN
OEM Key Revocation Configuration	See submenu	Configure OEM Key Revocation

4.3.3.1 Firmware Update Configuration

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

4.3.3.2 PTT Configuration

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

4.3.3.3 FIPS Configuration

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

4.3.3.4 ME Debug Configuration

Menu Item	Options	Description
HECI Timeous	Enabled / Disabled	Enable/Disable HECI Send/Receive Timeouts
Force ME DID Init Status	Enabled / Disabled	Forces the DID Initialization Status value
CPU Replaces Polling Disable	Enabled / Disabled	Setting this option disables CPU replacement polling loop
ME DID Message	Enabled / Disabled	Enable/Disable ME DID Message (disable will prevent the DID message from being sent)
HECI Message check Disable	Enabled / Disabled	Settings this option disables message check for Bios Boot Path when sending
MBP HOB Skip	Enabled / Disabled	Setting this option will skip MBP HOB
HECI2 Interface Communication	Enabled / Disabled	Adds and Removes HECI2 Device from PCI space
KT Device	Enabled / Disabled	Enable/Disable KT Device

DOI3 Setting for HECI Disable	Enabled / Disabled	Setting this option disables setting DOI3 bit for all HECI devices
MCTP Broadcast Cycle	Enabled / Disabled	Enable/Disable Management Component Transport Protocol Broadcast Cycle and Set PMT as Bus Owner

4.3.3.5 Anti-Rollback SVN Configuration

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

4.3.3.6 OEM Key Revocation Configuration

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

4.3.4 Trusted computing

Menu Item	Options	Description
Security Device Support	Enabled / Disabled	Enables or Disables BIOS support for security device. OS will not show the Security Device. TCG EFI protocol and INT1A interface will not be available. When enabled all the following items will be available.
SHA256 PCR Bank	Enabled / Disabled	Enables or Disables SHA256 PCR Bank
SHA384 PCR Bank	Enabled / Disabled	Enables or Disables SHA384 PCR Bank
SM3_256 PCR Bank	Enabled / Disabled	Enables or Disables SM3_256 PCR Bank
Pending Operation	None / TPM Clear	Schedule an Operation for the Security Device. NTE: your Computer will reboot during restart in order to change State of Security Device.
Platform Hierarchy	Enabled / Disabled	Enables or Disabled the Platform Hierarchy
Storage Hierarchy	Enabled / Disabled	Enables or Disabled the Storage Hierarchy
Endorsement Hierarchy	Enabled / Disabled	Enables or Disabled the Endorsement Hierarchy
Physical Presence Spec Version	1.2 / 1.3	Select to tell OS to support PPI Spec Version 1.2 or 1.3. Please note that some HCK tests might not support 1.3

Device Select	Auto TPM 1.2 TPM 2.0	TPM 1.2 will restrict the support to TPM 1.2 devices only, TPM 2.0 will restrict the support to TPM 2.0 devices only, Auto will support both with the default set to TPM 2.0 devices if not found, TPM 1.2 devices will be enumerated

4.3.5 ACPI Settings

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
Enable Hibernation	Disabled / Enabled	Enables or disables system ability to Hybernate (OS/S4 Sleep State). This option may be not effective with some OS.
ACPI Sleep State	Suspend Disabled S3 (Suspend to RAM)	Select the highest ACPI Sleep state the system will enter when the SUSPEND button is pressed.
Lock Legacy resources	Disabled / Enabled	Enables or Disables Lock of Legacy resources

4.3.6 Serial Port Console Redirection

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

4.3.6.1 Console Redirection Settings (COM#)

Menu Item	Options	Description
Terminal Type	VT100 VT100+	Emulation: ANSI: Extended ASCII Char set.

	VT-UTF8 ANSI	VT100: ASCII Char set. VT100+: extends VT100 to support colour, function keys, etc. VT-UTF8: uses UTF8 encoding to map Unicode chars onto 1 or more bytes
Bits per second	9600 / 19200 / 38400 / 57600 / 115200	Select Serial port Transmission Speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Data bits	7 / 8	Set Console Redirection data bits
Parity	None Even Odd Mark Space	A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the number of 1s in the data bits is even. Odd: parity bit is 0 if the number of 1s in the data bits is odd. Mark: parity bit is always 1. Space: parity bit is always 0. Mark and Space do not allow for error detection
Stop bits	1 / 2	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit
Flow Control	None Hardware RTS/CTS	Flow Control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses RTS# / CTS# lines to send the start / stop signals.
VT-UTF8 Combo Key Support	Enabled / Disabled	Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals
Recorder Mode	Enabled / Disabled	When this mode is enabled, only text will be sent. This is to capture Terminal data.
Resolution 100x31	Enabled / Disabled	Enables or disables extended terminal resolution
Putty Keypad	VT100 / Intel Linux / XTERMR6 / SCO / ESCN /VT400	Select FunctionKey and KeyPad on Putty

4.3.6.2 Console Redirection Settings (EMS)

Menu Item	Options	Description
Out-of-Band Mgmt Port	COM0 COM1	Microsoft Windows Emergency Management Services (EMS) allows for remote management of a Windows Server OS through a serial port
Terminal Type EMS	VT100 VT100+ VT-UTF8 ANSI	VT-UTF8 is the preferred terminal type for out-of-band management. The next best choice is VT100+ and then VT100. See above, in Console redirection Settings page, for more help with Terminal Type/Emulation
Bits per second	9600 / 19200 /	Select Serial port Transmission Speed. The speed must be matched on the other side. Long or

	57600 / 115200	noisy lines may require lower speeds.
Flow Control	None Hardware RTS/CTS Software Xon/Xoff	Flow Control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.

4.3.7 AMI Graphic Output Protocol Policy

Menu Item	Options	Description
Output Select	*List of available / connected module's video interfaces*	Output Interface, this menu is visible when more than one interface is available
Brightness Settings	20 / 40 / 60 / 80 / 100 / 120 / 140 / 160 / 180 / 200 / 220 / 240 / 255	Set GOP Brightness value
BIST Enable	Enabled / Disabled	Starts or stops the BIST on the integrated display panel

4.3.8 USB Configuration

Menu Item	Options	Description
Legacy USB Support	Enabled / Disabled / Auto	Enables Legacy USB Support. AUTO Option disables legacy support if no USB devices are connected. DISABLE option will keep USB devices available only for EFI applications.
XHCI hand-off	Enabled/ Disabled	This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.
USB Mass Storage Driver Support	Enabled/ Disabled	Enables or disables USB Mass Storage Driver Support
USB Transfer time-out	1 sec / 5 sec / 10 sec / 20 sec	Sets the time-out value for Control, Bulk and Interrupt transfers
Device reset time-out	10 sec / 20 sec / 30 sec / 40 sec	USB mass storage device Start Unit command time-out
Device power-up delay	Auto / Manual	Sets the maximum time that the device will take before it properly reports itself to the Host controller. 'Auto' uses the default vale (for a Root port it is 100ms, for a Hub port the delay is taken from the Hub descriptor).
Device power-up delay in seconds	[1..40]	Delay range in seconds, in one second increment, visible when delay is set to Manual

4.3.9 Network Stack configuration

Menu Item	Options	Description

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

4.3.10 NVMe configuration

Menu Item	Options	Description
List of NVMe devices found		

4.3.11 SDIO configuration

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

4.3.12 Super I/O Configuration

Menu Item	Options	Description
Exar XR28V38x (0x2E)		
Serial Port *#1-4*	Enabled / Disabled	Serial Port #
Address	List of hex addresses	Serial Port IO Base Address
IRQ	3 / 4 / 5 / 7 / 10 / 11	Serial Port IRQ

4.3.13 Main Thermal Configuration

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

4.3.14 LVDS Configuration

Menu Item	Options	Description
LVDS interface	Enabled / Disabled	Enables or Disables the LVDS interface. When enabled all the following parameters will appear
Edid Mode	External / Default / Custom	Select the source (EDID, Extended Display Identification Data) to be used for the internal flat panel. Depending on the setting chosen, only some of the following option or none will appear.
EDID	640x480 / 800x480 / 800x600 / 1024x600 / 1024x768 / 1280x720 / 1280x800 / 1280x1024 / 1366x768 / 1400x900 / 1600x900 / 1680x1050 / 1920x1080	Only available when Edid Mode is set to “default”. Select a software resolution (EDID settings) to be used for the internal flat panel.
Color Mode	VESA 24bpp / JEIDA 24bpp / 18 bpp	Select the color depth of LVDS interface. For 24-bit color depth, it is possible to choose also the color mapping on LVDS channels, i.e. if it must be VESA-compatible or JEIDA compatible.
Interface	Single Channel / Dual Channel	Allows configuration of LVDS interface in Single or Dual channel mode
DE Polarity	Active High / Active Low	Data Enable Polarity
V-Sync Polarity	Negative / Positive	Vertical Sync Polarity
H-Sync Polarity	Negative / Positive	Horizontal Sync Polarity
LVDS Advanced Options	See Submenu	LVDS Advanced Options Configurations

4.3.14.1 LVDS Advanced options

Menu Item	Options	Description
Spreading Depth	No Spreading / 0.5% / 1.0% / 1.5% / 2.0% / 2.5%	Sets percentage of bandwidth of LVDS clock frequency for spreading spectrum
Output Swing	150 mV / 200 mV / 250 mV / 300 mV / 350 mV / 400 mV / 450 mV	Sets the LVDS differential output swing
T3 Timing	[0..255]	Minimum T3 timing of panel power sequence to enforce (expressed in units of 50ms). Default is 10 (500ms)
T4 Timing	[0..255]	Minimum T4 timing of panel power sequence to enforce (expressed in units of 50ms). Default is 2 (100ms)
T12 Timing	[0..255]	Minimum T12 timing of panel power sequence to enforce (expressed in units of 50ms). Default is 20 (1s)
T2 Delay	Enabled / Disabled	When Enabled, T2 is delayed by 20ms ± 50%
T5 Delay	Enabled / Disabled	When Enabled, T5 is delayed by 20ms ± 50%
P/N Pairs Swapping	Enabled / Disabled	Enable or disable LVDS Differential pairs swapping (Positive ⇔ Negative)
Pairs Order Swapping	Enabled / Disabled	Enable or disable channel differential pairs order swapping (A ⇔ D, B ⇔ CLK, C ⇔ C)
Bus Swapping	Enabled / Disabled	Enable or disable Bus swapping (Odd ⇔ Even)
Firmware PLL	0: +/- 1.56% 1: +/- 3.12% 2: +/- 6.25% 3: +/- 12.5% 4: +/- 25% 5: +/- 50% 6: +/- 100%	Firmware PLL range

4.3.15 Embedded Controller

Menu Item	Options	Description
Embedded Controller information		Shows Embedded Controller specific information

Power Fail Resume Type	Always ON Always OFF Last State	Specify what state to go to when power is re-applied after a power failure (G3 state). If Batteryless Operation, the chipset always powers on after a power failure: Always OFF Resume Type or Last State when Last State was OFF will therefore require an immediate shutdown.
No C-MOS battery handling	Enabled / Disabled	In systems with no C-MOS battery, the chipset always powers on after a power failure: Always OFF Resume Type or Last State when Last State was OFF will therefore require an immediate shutdown.
LID_BTN# Configuration	Force Open Force Closed Normal Polarity Inverted Polarity	Configures the LID_BTN# signal as always open or closed, no matter the pin level, or configures the pin polarity: High = Open (Normal), Low = Open (Inverted)
LID_BTN# Wake Configuration	No Wake Only From S3 Wake From S3/S4/S5	Configures LID_BTN# wake capability (when not forced to Open or Closed). According to the pin configuration, when the LID is open it can cause a system wake from a sleep state.
OUT 80 serial redirection port	None / 1 / 2 / 1+2	Select on which E.C. UART(s) to redirect OUT 80 (Post Codes)
Hardware Monitor		Shows Monitored Hardware parameters and settings
Reset Causes Handling	See Submenu	Reset Causes Handling
Super IO Configuration	See Submenu	Super IO Configuration
External FAN/PWM Settings	See Submenu	Visible when PWM/FAN Management is Enabled under SMARC Related Configuration
Watchdog Configuration		Configure the Watchdog Timer --> Disables/Enables the Watchdog Timer Mechanism
MAC address(es) visualization		MAC address(es) visualization

4.3.15.1 Reset Causes Handling

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

4.3.15.2 Super IO Configuration

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

4.3.15.3 External FAN/PWM Settings

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

4.3.16 RAM Disk Configuration

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

4.4 Chipset menu

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

4.4.1 System Agent (SA) Configuration

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

4.4.1.1 Graphics Configuration

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

DiSM Size (GB)	[0..7]	DiSM Size for 2LM Sku
Intel Graphics Pei Display Peim	Enabled / Disabled	Enable / Disable Pei (Early) Display
VDD Enable	Enabled / Disabled	Enable / Disable forcing of VDD in the BIOS
Configure GT for use	Enabled / Disabled	Enable / Disable GT configuration in BIOS
PAVP Enable	Enabled / Disabled	Enable / Disable Protected Audio Video Playback (PAVP)
Cdynmax Clamping Enable	Enabled / Disabled	Enable / Disable Cdynmax Clamping
Cd Clock Frequency	172.8 MHz / 307.2 MHz / 556.8 MHz / 652.8 MHz / Max CdClock freq based on Reference Clk	Select the highest CD Clock frequency supported by the platform
GT PM Support	Enabled / Disabled	Enable / Disable GT Power Management Support
Skip Full CD Clock Init	Enabled / Disabled	Enabled: Skip Full CD clock initialization; Disabled: Initialize the full CD clock if not initialized by Gfx PEIM
VBT Select	eDP / MIPI	Select VBT for GOP Driver
IUER Button Enable	Enabled / Disabled	Enable / Disable IUER Button Functionality
LCD Control	See Submenu	

4.4.1.2 LCD Control

Menu Item	Options	Description
Primary IGFX Boot Display	VBIOS Default EFP LFP EFP3 EFP2 EFP4	Select the Video Device which will be activated during POST. This has no effect if external graphics present. Secondary boot display selection will appear based on your selection. VGA modes will be supported only on primary display
LCD Panel Type	VBIOS Default 640x480 LVDS 800x600 LVDS 1024x768 LVDS 1280x1024 LVDS 1400x1050 LVDS 1 1400x1050 LVDS 2 1600x1200 LVDS	Select LCD panel used by Internal Graphics Device by selecting the appropriate setup item

	1280x768 LVDS 1680x1050 LVDS 1920x1200 LVDS 1600x900 LVDS 1280x800 LVDS 1280x600 LVDS 2048x1536 LVDS 1366x768 LVDS	
Panel Scaling	Auto Off Force Scaling	Select the LCD panel scaling option used by the Internal Graphics Device
Backlight Control	PWM Inverted PWM Normal	Backlight Control Settings
Active LFP	*List of active options*	Select the Active LFP Configuration. No LVDS: VBIOS does not enable LVDS Int-LVDS: VBIOS enables LVDS driver by Integrated encoder SDV0 LVDS: VBIOS eables LVDS driver by SDV0 encoder No eDP: VBIOS does not enable eDP eDP Port-A: LFP Driven by Int-DisplayPort encoder from Port-A
Panel Colour Depth	18 bit / 24 bit	Select the LFP Panel Color Depth
Backlight Brightness	[0..255]	Set Panel Brightness

4.4.2 PCH-IO Configuration

Menu Item	Options	Description
PCI Express Configuration	See submenu	PCI Express Configuration Settings
SATA Configuration	See submenu	SATA Device Options Settings
USB Configuration	See submenu	USB Configuration Settings
Security Configuration	See submenu	Security Configuration Settings
HD Audio Configuration	See submenu	HD Audio Subsystem Configuration Settings
Serial IO Configuration	See submenu	Serial IO Configuration Settomgs
SCS Configuration	See submenu	Storage and Communication Subsystem (SCS) Configuration
PSE Configuration	See submenu	Programmable Service Engine (PSE) Configuration

TSN GBE Configuration	See submenu	Time Sensitive Network GBE Configuration
PCIe Ref Pll SSC	Auto / 0.0% / 0.1% / 0.2% / 0.3% / 0.4% / 0.5% / Disabled	Pcie Ref Pll SSC Percentage. AUTO – Keep hw default, no BIOS override.
Flash Potection Range Registers (FPRR)	Enabled / Disabled	Enable Flash Protection Range Registers
PinCntrl Driver GPIO Scheme	Enabled / Disabled	Enable/Disable PinCntrl Driver GPIO Scheme

4.4.2.1 PCI Express Configuration

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

4.4.2.1.1 PCI Express Root Port #

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

4.4.2.2 SATA Configuration

Menu Item	Options	Description

SATA Controller(s)	Enabled / Disabled	Enable/Disable SATA Devices
SATA Test Mode	Enabled / Disabled	Test Mode Enable / Disable (Loop Back)
Port #	Enabled / Disabled	Enable / Disable SATA Port
Hot Plug	Enabled / Disabled	Designate this port as Hot Pluggable

4.4.2.3 USB Configuration

Menu Item	Options	Description
xHCI Compliance Mode	Enable / Disable	Option to Enable Compliance Mode. Default is Disabled.
USB3 Link Speed Selection	GEN1 / GEN2	Select USB3 Link Speed as GEN1 or GEN2

4.4.2.4 Security Configuration

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

4.4.2.5 HD Audio Configuration

Menu Item	Options	Description
HD Audio	Enabled / Disabled	Control Detection of the HD-Audio device. When enabled, following menu items will appear
Audio DSP	Enabled / Disabled	Enables/Disables Audio DSP
Audio Link Mode	HD Audio Link SSP (I2S) SoundWire Advanced Link Config	Select link mode: 1) HDA-Link [SDIO-1], DMIC[0-1] 2) SSP[0-5], DMIC[0-1] 3) SNDW[1-4] 4) Advanced will allow to enable each interface separately
HDA-Link Codec Select	Platform Onboard External Kit	Selects whether Platform Onboard Codec (single Verb Table installed) or External Codec Kit (multiple Verb Tables installed) will be used
HD Audio Advanced Configuration	See submenu	HD Audio Subsystem Advanced Configuration Settings

4.4.2.5.1 HD Audio Advanced Configuration

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

4.4.2.6 Serial IO Configuration

Menu Item	Options	Description
I2C3 Controller	Enabled / Disabled	The following devices depend on each other: I2C0 and I2C1-2-3
SPI2 Controller	Enabled / Disabled	This device depends on Thermal Subsystem in PCI mode. SPI2 will be Disabled if PSE SPI0 or PWM or TGPIO is Enabled
UART2 Controller	Enabled / Disabled / Communication port (COM)	Set UART2 mode: - DBG used for BIOS log print and/or Kernel OS Debug - COM 16550 compatible serial port with Power Gating support
GPIO IRQ Route	IRQ14 / IRQ15	Route all GPIOs to one of the IRQ
Serial IO I2C# Settings		Configure Serial IO Controller --> Set specific parameters
Serial IO SPI# Settings		Configure Serial IO Controller --> Set specific parameters
Serial IO UART# Settings		Configure Serial IO Controller --> Set specific parameters

WITT/MITT I2C Test Device	Enabled / Disabled	Enable SIO I2C WITT Device and select which controller use it
WITT/MITT SPI Test Device	Enabled / Disabled	Enable SIO SPI WITT Device and select which controller use it
UART Test Device	Enabled / Disabled	Enable SIO UART Test Device and select which controller use it
LPSS Device D3 State	Enabled / Disabled	Enable / Disable the LPSS D3 before entering to OS
Additional Serial IO devices	Enabled / Disabled	When enabled, ACPI will report additional devices connected to Serial IO
Serial IO timing parameters	Enabled / Disabled	Enables additional timing parameters for all Serial IO controllers. Defaults can be changed in each controller setting. Platform restart quired to apply changes.

4.4.2.7 SCS Configuration

Menu Item	Options	Description
eMMC 5.1 Controller	Enabled / Disabled	Enable or Disable SCS eMMC 5.1 Controller
eMMC 5.1 HS400 Mode	Enabled / Disabled	Enable or Disable SCS eMMC HS400 Mode
Enable HS400 software tuning	Enabled / Disabled	Software tuning should improve eMMC HS400 stabilit at the expense of boot time
Driver Strength	33 / 40 / 50 Ohm	Sets IO driver strength
SDCard 3.0 Controller	Enabled / Disabled	Enable or Disable SCS SDHC 3.0 Controller

4.4.2.8 PSE Configuration

Menu Item	Options	Description
PSE Controller	Enabled / Disabled	Enables/Disables Programmable Service Engine (PSE). When enabled, following menu items will appear
LOG OUTPUT OFFSET		Determine the PSE log output region offset in memory
LOG OUTPUT SIZE		Determine the PSE log output region size limitation in memory
Shell	Enabled / Disabled	Enables/Disables PSE Shell
Eclite	Enabled / Disabled	Enables/Disables PSE Eclite Service
OOB	Enabled / Disabled	Enables/Disables PSE OOB Service
WoL	Enabled / Disabled	Enables/Disables PSE GBE Wake On Lan
PSE Debug (JTAG/SWD) Enable	Enabled / Disabled	Enables/Disables PSE JTAG/SWD Debug
PSE JTAG/SWD PIN MUX	Enabled / Disabled	Enables/Disables PSE JTAG Pin Mux. Not allowed if Sci Pin Mux is enabled.

PWM	None PSE owned Host owned	PWM has pin conflict with UART3, SPI0, SPI1, I2C5 and TGPIO
UART2	None PSE owned Host owned	UART2 is default enabled for PSE logging purpose
CAN0	None PSE owned Host owned	CAN0 has pin conflict with I2S0 and TGPIO 16-17
DMA#	None PSE owned Host owned	Select ownership for DMA #
GBE0	None PSE owned Host owned	Select ownership for GBE0
PSE GBE0 DLL Override	Enabled / Disabled	Enable/Disable PSE GBE0 DLL. To Enable this GBE0 must be Enabled.
PSE GBE0 Tx_Delay		Configure total number of delay elements in DLL slave. Default 16, Min 1, Max 63
GPIO/TGPIO 0 MUX SELECTION	LOWER / MID / TOP / All GPIO	Lower: TGPIO(0-19), GPIO(20-29) Lower: TGPIO(0-9, 20-29), GPIO(10-19) Lower: TGPIO(10-29)
GPIO/TGPIO 0 Pin Selection		Enables / Disables individual GPIO/TGPIO 0 pins
GPIO/TGPIO 1 MUX SELECTION	LOWER / MID / TOP / All GPIO	Lower: TGPIO(30-49), GPIO(50-59) Lower: TGPIO(30-39, 50-59), GPIO(40-49) Lower: TGPIO(40-59)
GPIO/TGPIO 1 Pin Selection		Enables / Disables individual GPIO/TGPIO 1 pins
List of PSE peripherals that can generate interrupts	Enabled / Disabled	Enabled = Interrupt set to SB mode; Disabled = MSI mode
DMA Test	Enabled / Disabled	Enables / Disables DMA test Device

4.4.2.9 TSN GBE Configuration

Menu Item	Options	Description

PCH TSN LAN Controller	Enabled / Disabled	Enable/Disable Time Sensitive Network (TSN) LAN
PCH TSN GBE Multi-Vc	Enabled / Disabled	Enable/Disable TSN Multi Virtual Channels
PCH TSN GBE SGMII Support	Enabled / Disabled	Enable/Disable SGMII mode for PCH TSN GBE. Ports in SGMII mode with the same PLL common lane must use the same link speed. SATA or UFS may need to be disabled if TSN port is using the same PLL common lane. Please make sure IFWI has proper straps set for SGMII. Make sure Flex IO Lane Assignment is not NONE
PCH TSN Link Speed	24MHz 2.5Gbps 24MHz 1Gbps 38.4MHz 2.5Gbps 38.4MHz 1bps	PCH TSN Link Speed configuration
PCH TSN GBE # Multi-Vc	Enabled / Disabled	Enable/Disable TSN Multi Virtual Channels. TSN GBE # must be host owned.
PCH TSN GBE # SGMII Support	Enabled / Disabled	Enable/Disable SGMII mode for PCH TSN GBE #. Ports in SGMII mode with the same PLL common lane must use the same link speed. UFS will need to be disabled as this TSN port uses the same PLL common lane. Please make sure IFWI has proper straps set for SGMII. Make sure Flex IO Lane Assignment is not NONE
PCH TSN GBE # Link Speed	24MHz 2.5Gbps 24MHz 1Gbps 38.4MHz 2.5Gbps 38.4MHz 1bps	PCH TSN GBE # Link Speed configuration

4.5 Security menu

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

4.5.1 Secure Boot submenu

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

4.5.1.1 Key Management submenu

Menu Item	Options	
Factory Key Provision	Enabled / Disabled	Install factory default Secure Boot keys after the platform reset and while the system is in Setup mode
Restore Factory Keys		Force System to User Mode. Install factory default Secure Boot key databases
Reset To Setup Mode		Delete all Secure Boot key databases from NVRAM
Enroll Efi Image	*File System Image*	Allow the image to run in Secure Boot mode. Enrol SHA256 Hash certificate of a PE Image into Authorized Signature Database (db)
Remove 'UEFI CA' from DB		Device Guard ready system must not list 'Microsoft UEFI CA' Certificate in Authorized Signature database (db)

Restore DB defaults		Restore DB variable to factory defaults
Platform key (PK) Key Exchange Keys Authorized Signatures Forbidden Signatures 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_SHAxxx 2. Authenticated UEFI Variable 3. EFI PE/COFF Image (SHA256), Key Source: Factory, External, Mixed

4.6 Boot menu

Menu Item	Options	Description
Setup Prompt Timeout	0 .. 65535	Number of seconds to wait for setup activation key. 655535 means indefinite waiting.
Bootup NumLock State	On / Off	Select the keyboard NumLock state
Quiet Boot	Enabled / Disabled	Enables or disables Quiet Boot option
Fast Boot	Enabled / Disabled	Enables or disables boot with initialization of a minimal set of devices required to launch active boot option. Has no effect for BBS boot options.
SATA Support	Last Boot SATA Devices Only All SATA Devices	If Last Boot SATA Devices Only, only last boot SATA device will be available in Post. If All SATA Devices, all SATA devices will be available in OS and Post.
NVMe Support	Enabled / Disabled	If Disabled, NVMe device will be skipped
USB Support	Disabled Full Initial Partial Initial	If Disabled, all USB devices will NOT be available until after OS boot. If Partial Initial, USB Mass Storage and specific USB port/device will NOT be available before OS boot. If Enabled, all USB devices will be available in OS and Post.
PS2 Devices Support	Enabled / Disabled	If Disabled, PS2 devices will be skipped
Network Stack Driver Support	Enabled / Disabled	If Disabled, Network Stack Driver will be skipped
Redirection Support	Enabled / Disabled	If Disabled, Redirection function will be disabled
• Boot Option #1 • Boot Option #2 • Boot Option #3 • Boot Option #4 • Boot Option #5 • Boot Option #6 • Boot Option #7 • Boot Option #8 • Boot Option #9	Hard Disk0 Hard Disk1 eMMC CD/DVD SD USB Device Network Other Device Disabled	Select the system boot order
UEFI EMMC Drive BBS Priorities		Specifies the Boot Device Priority sequence from available UEFI EMMC Drivers
UEFI SD Drive BBS Priorities		Specifies the Boot Device Priority sequence from available UEFI SD Drivers

4.7 Save & Exit menu

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

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

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

Chapter 5.
Appendices

- Thermal Design

5.1 Thermal Design

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

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

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

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

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

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

Ordering Code	Description
QD62-DISS-1-PK	ATLAS Heat Spreader (Passive)
QD62-DISS-2-PK	ATLAS Heatsink (Passive)
QD62-DISS-3-PK	ATLAS Active Heatsink with FAN

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 Srl - Via Calamandrei 91
52100 Arezzo - ITALY
Ph: +39 0575 26979 - Fax: +39 0575 350210
www.seco.com