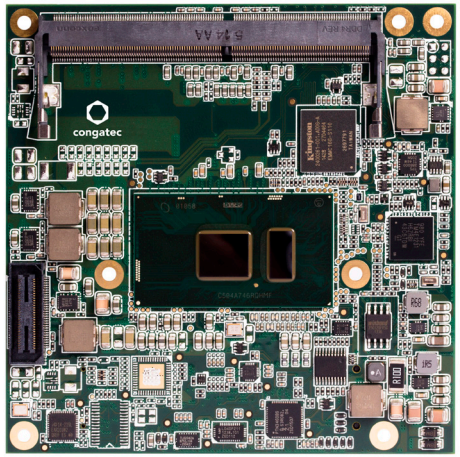


COM Express™ conga-TC170

6th Generation Intel® Core™ i7, i5, i3 and Celeron® Single Chip Ultra Low TDP Processors

User's Guide

Revision 1.0

Revision History

Revision	Date (yyyy.mm.dd)	Author	Changes
0.1	2016.01.07	AEM	• Preliminary release
1.0	2016.06.29	BEU	• Updated available product variants in section 1 "Introduction" and section 2 " Specifications" • Added section 9 "Resource List", section 10 "BIOS Setup Description" and section 11 "Additional BIOS Features". • Official release

Preface

This user's guide provides information about the components, features, connectors and BIOS Setup menus available on the conga-TC170. It is one of three documents that should be referred to when designing a COM Express™ application. The other reference documents that should be used include the following:

COM Express™ Design Guide
COM Express™ Specification

The links to these documents can be found on the congatec AG website at www.congatec.com

Disclaimer

The information contained within this user's guide, including but not limited to any product specification, is subject to change without notice.

congatec AG provides no warranty with regard to this user's guide or any other information contained herein and hereby expressly disclaims any implied warranties of merchantability or fitness for any particular purpose with regard to any of the foregoing. congatec AG assumes no liability for any damages incurred directly or indirectly from any technical or typographical errors or omissions contained herein or for discrepancies between the product and the user's guide. In no event shall congatec AG be liable for any incidental, consequential, special, or exemplary damages, whether based on tort, contract or otherwise, arising out of or in connection with this user's guide or any other information contained herein or the use thereof.

Intended Audience

This user's guide is intended for technically qualified personnel. It is not intended for general audiences.

Lead-Free Designs (RoHS)

All congatec AG designs are created from lead-free components and are completely RoHS compliant.

Electrostatic Sensitive Device

All congatec AG products are electrostatic sensitive devices and are packaged accordingly. Do not open or handle a congatec AG product except at an electrostatic-free workstation. Additionally, do not ship or store congatec AG products near strong electrostatic, electromagnetic, magnetic, or radioactive fields unless the device is contained within its original manufacturer's packaging. Be aware that failure to comply with these guidelines will void the congatec AG Limited Warranty.

Symbols

The following symbols are used in this user's guide:

Warning

Warnings indicate conditions that, if not observed, can cause personal injury.

Caution

Cautions warn the user about how to prevent damage to hardware or loss of data.

Note

Notes call attention to important information that should be observed.

Terminology

Term	Description
GB	Gigabyte (1,073,741,824 bytes)
GHz	Gigahertz (one billion hertz)
kB	Kilobyte (1024 bytes)
MB	Megabyte (1,048,576 bytes)
Mbit	Megabit (1,048,576 bits)
kHz	Kilohertz (one thousand hertz)
MHz	Megahertz (one million hertz)
TDP	Thermal Design Power
PCIe	PCI Express
SATA	Serial ATA
PEG	PCI Express Graphics
PCH	Platform Controller Hub
eDP	Embedded DisplayPort
T.O.M.	Top of memory = max. DRAM installed
HDA	High Definition Audio
N.C.	Not connected
N.A.	Not available
TBD	To be determined

Trademarks

Product names, logos, brands, and other trademarks featured or referred to within this user's guide, or the congatec website, are the property of their respective trademark holders. These trademark holders are not affiliated with congatec AG, our products, or our website.

Warranty

congatec AG makes no representation, warranty or guaranty, express or implied regarding the products except its standard form of limited warranty ("Limited Warranty") per the terms and conditions of the congatec entity, which the product is delivered from. These terms and conditions can be downloaded from www.congatec.com. congatec AG may in its sole discretion modify its Limited Warranty at any time and from time to time.

The products may include software. Use of the software is subject to the terms and conditions set out in the respective owner's license agreements, which are available at www.congatec.com and/or upon request.

Beginning on the date of shipment to its direct customer and continuing for the published warranty period, congatec AG represents that the products are new and warrants that each product failing to function properly under normal use, due to a defect in materials or workmanship or due to non conformance to the agreed upon specifications, will be repaired or exchanged, at congatec's option and expense.

Customer will obtain a Return Material Authorization ("RMA") number from congatec AG prior to returning the non conforming product freight prepaid. congatec AG will pay for transporting the repaired or exchanged product to the customer.

Repaired, replaced or exchanged product will be warranted for the repair warranty period in effect as of the date the repaired, exchanged or replaced product is shipped by congatec, or the remainder of the original warranty, whichever is longer. This Limited Warranty extends to congatec's direct customer only and is not assignable or transferable.

Except as set forth in writing in the Limited Warranty, congatec makes no performance representations, warranties, or guarantees, either express or implied, oral or written, with respect to the products, including without limitation any implied warranty (a) of merchantability, (b) of fitness for a particular purpose, or (c) arising from course of performance, course of dealing, or usage of trade.

congatec AG shall in no event be liable to the end user for collateral or consequential damages of any kind. congatec shall not otherwise be liable for loss, damage or expense directly or indirectly arising from the use of the product or from any other cause. The sole and exclusive remedy against congatec, whether a claim sound in contract, warranty, tort or any other legal theory, shall be repair or replacement of the product only.

Certification

congatec AG is certified to DIN EN ISO 9001 standard.

Technical Support

congatec AG technicians and engineers are committed to providing the best possible technical support for our customers so that our products can be easily used and implemented. We request that you first visit our website at www.congatec.com for the latest documentation, utilities and drivers, which have been made available to assist you. If you still require assistance after visiting our website then contact our technical support department by email at support@congatec.com

Contents

List of Tables

1 INTRODUCTION

COM Express™ Concept

COM Express™ is an open industry standard defined specifically for COMs (computer on modules). Its creation makes it possible to smoothly transition from legacy interfaces to the newest technologies available today. COM Express™ modules are available in following form factors:

- Mini 84mm x 55mm
- Compact 95mm x 95mm
- Basic 125mm x 95mm
- Extended 155mm x110mm

The COM Express™ specification 2.1 defines seven different pinout types.

Types	Connector Rows	PCI Express Lanes	PCI	IDE Channels	LAN ports	USB 2.0/ USB 3.0	Display Interfaces
Type 1	A-B	Up to 6			1	8 / 0	VGA, LVDS
Type 2	A-B C-D	Up to 22	32 bit	1	1	8 / 0	VGA, LVDS,PEG/SDVO
Type 3	A-B C-D	Up to 22	32 bit		3	8 / 0	VGA,LVDS,PEG/SDVO
Type 4	A-B C-D	Up to 32		1	1	8 / 0	VGA,LVDS,PEG/SDVO
Type 5	A-B C-D	Up to 32			3	8 / 0	VGA,LVDS,PEG/SDVO
Type 6	A-B C-D	Up to 24			1	8 / 4	VGA,LVDS,PEG, 3x DDI
Type 10	A-B	Up to 4			1	8 / 0	1x DDI

The conga-TC170 modules use the Type 6 pinout definition and comply with COM Express 2.1 specification. They are equipped with two high performance connectors that ensure stable data throughput.

The COM (computer on module) integrates all the core components and is mounted onto an application specific carrier board. COM modules are legacy-free design (no Super I/O, PS/2 keyboard and mouse) and provide most of the functional requirements for any application. These functions include, but are not limited to a rich complement of contemporary high bandwidth serial interfaces such as PCI Express, Serial ATA, USB 2.0, and Gigabit Ethernet. The Type 6 pinout provides the ability to offer PCI Express, Serial ATA, and LPC options thereby expanding the range of potential peripherals. The robust thermal and mechanical concept, combined with extended power-management capabilities, is perfectly suited for all applications.

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

conga-TC170 Options Information

The conga-TC170 is currently available in four variants. This user's guide describes all of these variants. The table below shows the different configurations available. Check for the Part No. that applies to your product. This will tell you what options described in this user's guide are available on your particular module.

conga-TC170

Part-No.	045200	045201	045202	045203
Processor	Intel® Core™ i7-6600U 2.6 GHz Dual Core™	Intel® Core™ i5-6300U 2.4 GHz Dual Core™	Intel® Core™ i3-6100U 2.3 GHz Dual Core™	Intel® Celeron® 3955U 2.0 GHz Dual Core
Intel® Smart Cache	4 MByte	3 MByte	3 MByte	2 MByte
Max. Turbo Frequency	3.4 GHz	3 GHz	N.A	N.A
Processor Graphics	Intel® HD Graphics 520 (GT2)	Intel® HD Graphics 520 (GT2)	Intel® HD Graphics 520 (GT2)	Intel® HD Graphics 510 (GT1)
Graphics Max. Dynamic Freq	1.0 GHz	1.0 GHz	1.0 GHz	900 MHz
Memory (DDR4)	2133 MT/s dual channel	2133 MT/s dual channel	2133 MT/s dual channel	2133 MT/s dual channel
LVDS	Yes	Yes	Yes	Yes
DisplayPort (DP)	Yes	Yes	Yes	Yes
HDMI	Yes	Yes	Yes	Yes
Processor TDP (cTDP)	15 (7.5) W	15 (7.5) W	15 (7.5) W	15 (10) W

2 Specifications

2.1 Feature List

Table 1 Feature Summary

Form Factor	Based on COM Express™ standard pinout Type 6 Rev. 2.1 (Compact size 95 x 95 mm).	
Processor	6th Generation Intel® Core™ i7,i5, i3 Single Chip Ultra Low TDP Processors.	
Memory	2 sockets: SO-DIMM DDR4 (voltage @ 1.2V) up to 2133 MT/s, with 32GB maximum capacity. Sockets located top and bottom side of module.	
congatec Board Controller	Multi-stage watchdog, non-volatile user data storage, manufacturing and board information, board statistics, hardware monitoring, fan control, I2C bus, Power loss control.	
Chipset	Intel® 100 Series PCH-LP integrated in the Multi-Chip Package.	
Audio	High Definition Audio (HDA)/digital audio interface with support for multiple codecs	
Ethernet	Gigabit Ethernet support via the onboard Intel® I219LM GbE Phy. Also offers AMT 11 support.	
Graphics Options	Next Generation Intel® HD/Iris Graphics (520/540) with support for Intel® Clear Video Technology (HD encode/transcode, Blu-ray playback), DirectX Video Acceleration (full AVC/VC1/MPEG2 hardware decode), OpenGL 4.4, and DirectX12. Up to 3 independent displays supported (Must be two DDI's (DP, HDMI/DVI) plus one eDP/LVDS)	
	1x LVDS (Integrated flat panel interface with 25-112MHz single/dual-channel LVDS Transmitter). Supports: - Single-channel LVDS interface: 1 x 18 bpp or 1 x 24 bpp. - Dual channel LVDS interface: 2 x 18 bpp or 2 x 24 bpp panel. - VESA LVDS color mappings - Automatic Panel Detection via Embedded Panel Interface based on VESA EDID™ 1.3. - Resolution up to 1920x1200 in dual LVDS mode. 1x Optional eDP 1.3 interface (assembly option) **NOTE**: LVDS interface is supported by default. The eDP interface is only offered as an assembly option. For more information, contact congatec technical support center.	Up to 2x DDIs (Digital Display Interfaces) with support for: - 2x DisplayPort 1.2 with support for Multi-Stream Transport (MST) - 2x HDMI 1.4a (requires external level shifter) - 2x DVI port (requires external level shifter) - Resolutions up to 4K Optional VGA interface - This option is offered on digital port C. The display combination for revisions with VGA support is 1x DDI, 1x VGA and 1x LVDS/eDP. **NOTE**: - To support HDMI/DVI, an external level shifter should be implemented on the user's carrier board. - To support HDMI 2.0 via the DDI, you need a Level Shifter Protocol Converter (LSPCON) on the carrier board.
Peripheral Interfaces	USB Interfaces: - Up to 8x USB 2.0 - Up to 4x USB 3.0 3x Serial ATA® 6Gb/s with RAID support 0/1/5/10 2x Serial Interfaces (UART0/1) Up to 8x PCI Express® Gen. 3 lanes (can be configured via customized/ special BIOS firmware to support four x1 or one x4 links.) **NOTE**: The Intel chipset supports a maximum of 6 PCIe devices at any time.	LPC Bus I²C Bus, Fast Mode, multi-master SM Bus SPI GPIOs Optional x1 or x2 PEG port (requires re-routing of PCIe lanes 5 and/or 6) **NOTE**: The conga-TSCL offers only 7 PCIe lanes if x1 PEG port is implemented and only 6 PCIe lanes if x2 PEG port is implemented.
BIOS	AMI Aptio® UEFI 5.x firmware, 8 or 16 MByte serial SPI with congatec Embedded BIOS features.	

Storage	Optional eMMC 5.0 onboard flash
Power Management	ACPI 4.0 compliant with battery support. Also supports Suspend to RAM (S3) and Intel AMT 10. Configurable TDP Ultra low standby power consumption, Deep Sx.
Security	Optional discrete Trusted Platform Module "TPM 1.2/2.0"; new AES Instructions for faster and better encryption.

Note

Some of the features mentioned above are optional. Check the article number of your module and compare it to the Options Information list on page 11 to determine what options are available on your particular module.

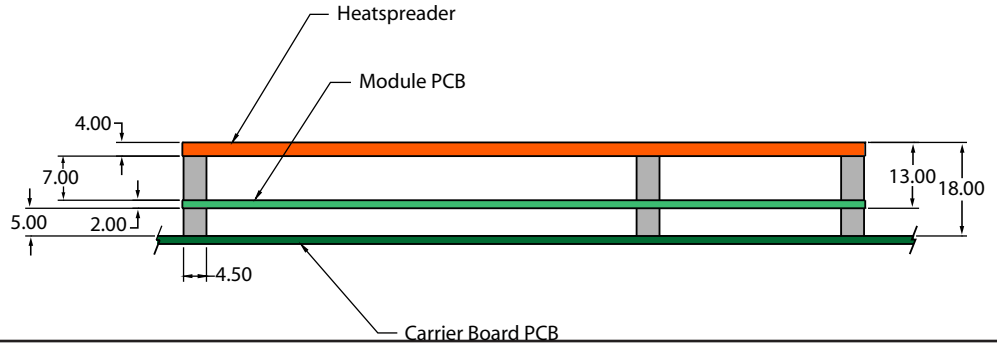
2.2 Supported Operating Systems

The conga-TC170 supports the following operating systems.

- Microsoft® Windows® 10
- Microsoft® Windows® 8
- Microsoft® Windows® 7
- Microsoft® Windows® Embedded Standard
- Linux

2.3 Mechanical Dimensions

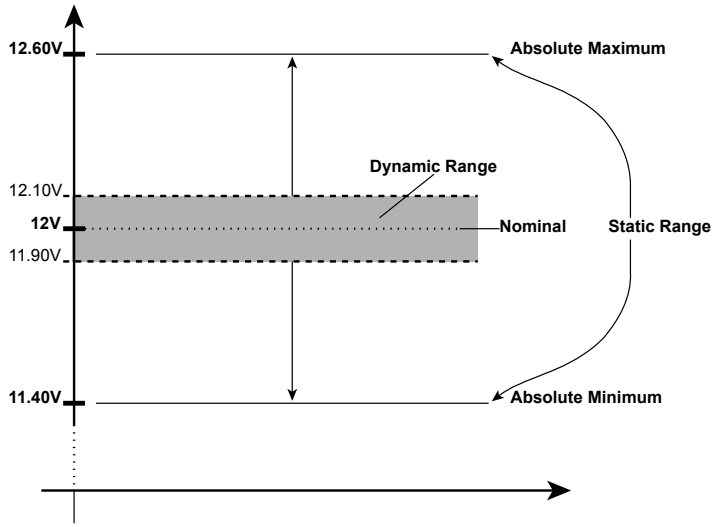
- 95.0 mm x 95.0 mm (3.74" x 3.74")
- Height approximately 18 or 21mm (including heatspreader) depending on the carrier board connector that is used. If the 5mm (height) carrier board connector is used, then approximate overall height is 18mm. If the 8mm (height) carrier board connector is used, then approximate overall height is 21mm.



2.4 Supply Voltage Standard Power

- 12V DC ± 5%

The dynamic range shall not exceed the static range.



2.4.1 Electrical Characteristics

Power supply pins on the module's connectors limit the amount of input power. The following table provides an overview of the limitations for pinout Type 6 (dual connector, 440 pins).

Power Rail	Module Pin Current Capability (Amps)	Nominal Input (Volts)	Input Range (Volts)	Derated Input (Volts)	Max. Input Ripple (10Hz to 20MHz) (mV)	Max. Module Input Power (w. derated input) (Watts)	Assumed Conversion Efficiency	Max. Load Power (Watts)
VCC_12V	12	12	11.4-12.6	11.4	+/- 100	137	85%	116
VCC_5V-SBY	2	5	4.75-5.25	4.75	+/- 50	9		
VCC_RTC	0.5	3	2.0-3.3		+/- 20			

2.4.2 Rise Time

The input voltages shall rise from 10% of nominal to 90% of nominal at a minimum slope of 250V/s. The smooth turn-on requires that, during the 10% to 90% portion of the rise time, the slope of the turn-on waveform must be positive.

2.5 Power Consumption

The power consumption values listed in this document were measured under a controlled environment. The hardware used for testing includes a conga-TC170 module, conga-TEVAL carrier board, HDMI-equipped LCD monitor, SATA SSD drive, and USB keyboard/mouse. The SATA drive was powered externally by an ATX power supply so that it does not influence the power consumption value that is measured for the module. To ensure that only the power consumption of the CPU module is measured, the conga-TEVAL power consumption was determined before the measurement and subtracted from the overall power consumption value measured.

The USB keyboard/mouse were detached once the module was configured within the OS. All recorded values were averaged over a 30 second time period. Cooling of the module was done by the module specific heatspreader and a fan cooled heatsink to measure the power consumption under normal thermal conditions.

Each module was measured while running Windows 7 Professional 64Bit, Hyper Threading enabled, Speed Step enabled, CPU Turbo Mode enabled and Power Plan set to "Power Saver". This setting ensures that Core™ processors run in LFM (lowest frequency mode) with minimal core voltage during desktop idle. Each module was tested while using two 4GB memory modules. Using different sizes of RAM, as well as one or two memory modules, will cause slight variances in the measured results.

To measure the worst case power consumption the cooling solution was removed and the CPU core temperature was allowed to run up to between 90° and 95°C while running 100% workload with the Power Plan set to "Balanced". The peak current value was then recorded. This value should be taken into consideration when designing the system's power supply to ensure that the power supply is sufficient during worst case scenarios.

Power consumption values were recorded during the following stages:

Windows 7 (64 bit)

- Desktop Idle (power plan = Power Saver)
- 100% CPU workload (see note below, power plan = Power Saver)
- 100% CPU workload at approximately 100°C peak power consumption (power plan = Balanced)
- Suspend to RAM. Supply power for S3 mode is 5V.

Note

A software tool was used to stress the CPU to Max Turbo Frequency.

Processor Information

The tables below provide additional information about the power consumption data for each of the conga-TC170 variants offered. The values are recorded at various operating mode.

2.5.1 Intel® Core™ i7-6600U 2.2 GHz Dual Core™ 4MB Cache

conga-TC170 Art. No. 045200 (GT2 Graphics)	Intel® Core™ i7-6600U 2.6 GHz 2 Core™ 4MB Intel® Smart Cache (14nm) Layout Rev. TCSLLA0 /BIOS Rev. TCSLR000			
Max Turbo Frequency	3.4 GHz			
Memory Size	4GB			
Operating System	Windows 7 (64 bit)			
Power State	Desktop Idle C-States Enabled	100% workload	100% workload in Turbo mode (peak)	Suspend to Ram (S3) 5V Input Power
Power consumption (measured in Amps./Watts)	0.34 A / 4.1 W	2.49 A / 29.9 W	3.37 A / 40.4 W	0.11A / 0.53 W

2.5.2 Intel® Core™ i5-6300U 2.4 GHz Dual Core™ 3MB Cache

conga-TC170 Art. No. 045201 (GT2 Graphics)	Intel® Core™ i5-6300U 2.4 GHz 2 Core™ 3MB Intel® Smart Cache (14nm) Layout Rev. TCSLLA0 /BIOS Rev. TCSLR000			
Max Turbo Frequency	3.0 GHz			
Memory Size	4GB			
Operating System	Windows 7 (64 bit)			
Power State	Desktop Idle C-States Enabled	100% workload	100% workload in Turbo mode (peak)	Suspend to Ram (S3) 5V Input Power
Power consumption (measured in Amps./Watts)	0.34 A / 4.1 W	2.38 A / 28.6 W	3.03 A / 36.4 W	0.1A A / 0.49 W

2.5.3 Intel® Core™ i3-6100U 2.3 GHz Dual Core™ 3MB Cache

conga-TC170 Art. No. 045202 (GT2 Graphics)	Intel® Core™ i3-6100U 2.3 GHz 2 Core™ 3MB Intel® Smart Cache (14nm) Layout Rev. TCSLLA0 /BIOS Rev. TCSLR000			
Max Turbo Frequency	N.A			
Memory Size	4GB			
Operating System	Windows 7 (64 bit)			
Power State	Desktop Idle C-States Enabled	100% workload	100% workload in Turbo mode (peak)	Suspend to Ram (S3) 5V Input Power
Power consumption (measured in Amps./Watts)	0.33 A / 4.0 W	2.36 A / 28.31 W	2.75 A / 33 W	0.08 A / 0.42 W

2.5.4 Intel® Celeron® 3955U 2.0 GHz Dual Core™ 2MB Cache

conga-TC170 Art. No. 045203 (GT1 Graphics)	Intel® Core™ i5-6360U 2.0 GHz 2 Core™ 4MB Intel® Smart Cache (14nm) Layout Rev. TCSLLA0 /BIOS Rev. TCSLR000			
Max Turbo Frequency	N.A			
Memory Size	4GB			
Operating System	Windows 7 (64 bit)			
Power State	Desktop Idle C-States Enabled	100% workload	100% workload in Turbo mode (peak)	Suspend to Ram (S3) 5V Input Power
Power consumption (measured in Amps./Watts)	0.4 A / 4.8 W	1.43 A / 17.16 W	1.63 A / 19.5 W	0.07 A / 0.36 W

2.6 Supply Voltage Battery Power

- 2.0V-3.5V DC
- Typical 3V DC

2.6.1 CMOS Battery Power Consumption

RTC @	Voltage	Current
-10°C	3V DC	1.50 µA
20°C	3V DC	1.69 µA
70°C	3V DC	2.46 µA

The CMOS battery power consumption value listed above should not be used to calculate CMOS battery lifetime. You should measure the CMOS battery power consumption in your customer specific application in worst case conditions, for example during high temperature and high battery voltage. The self-discharge of the battery must also be considered when determining CMOS battery lifetime. For more information about calculating CMOS battery lifetime refer to application note AN9_RTC_Battery_Lifetime.pdf on congatec AG website at www.congatec.com.

2.7 Environmental Specifications

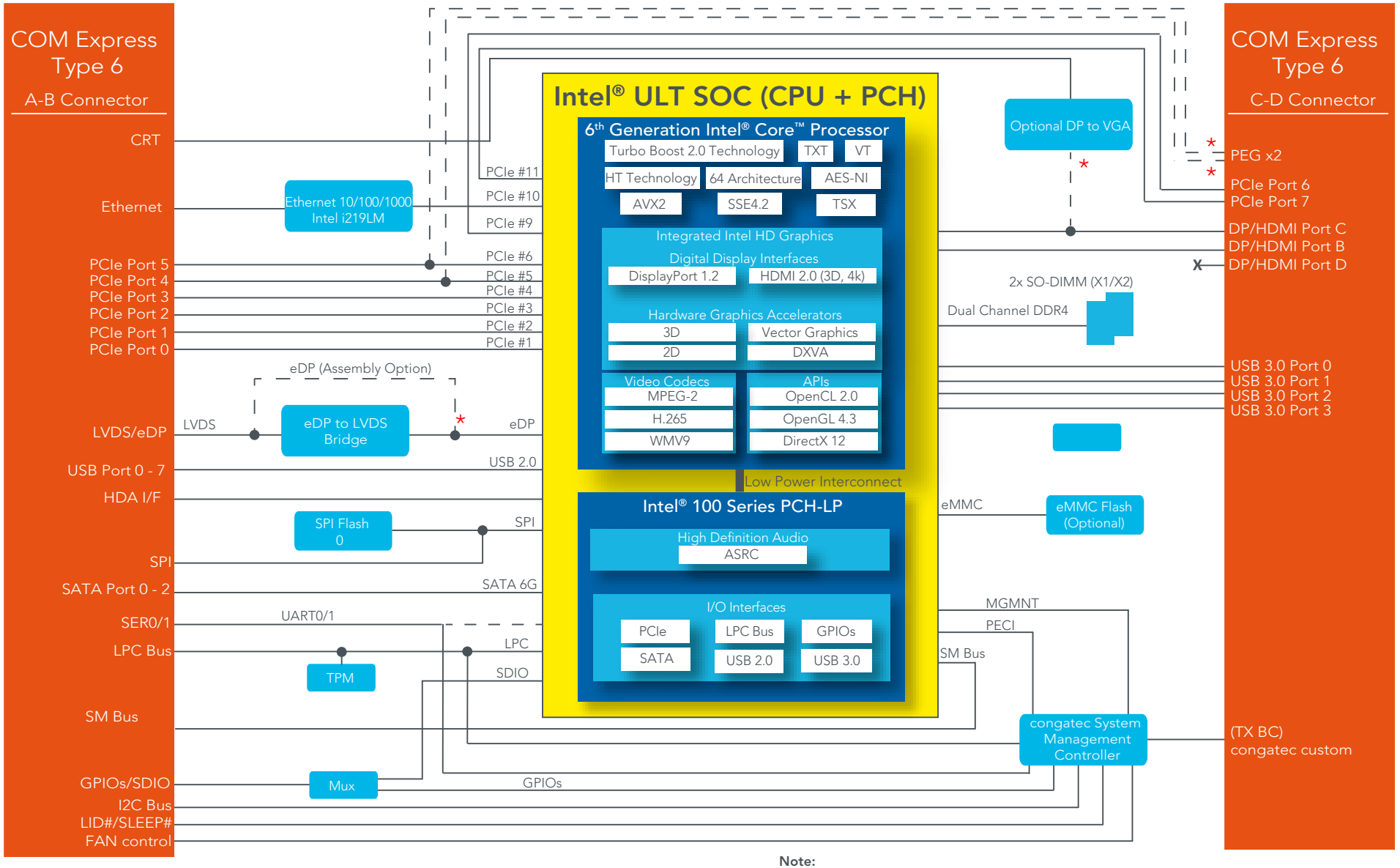
Temperature	Operation: 0° to 60°C	Storage: -20° to +80°C
Humidity	Operation: 10% to 90%	Storage: 5% to 95%

Caution

The above operating temperatures must be strictly adhered to at all times. When using a congatec heatspreader, the maximum operating temperature refers to any measurable spot on the heatspreader's surface.

Humidity specifications are for non-condensing conditions.

3 Block Diagram



Note:

* Not supported by default. Only available as assembly option.

4 Cooling Solutions

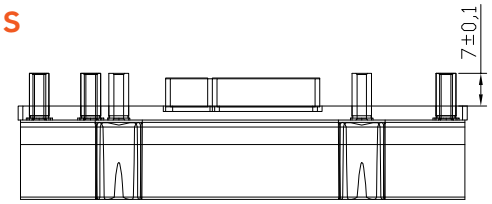
congatec AG offers two cooling solutions for the conga-TC170:

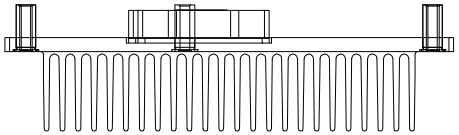
- Passive cooling solution (CSP)
- Heatspreader

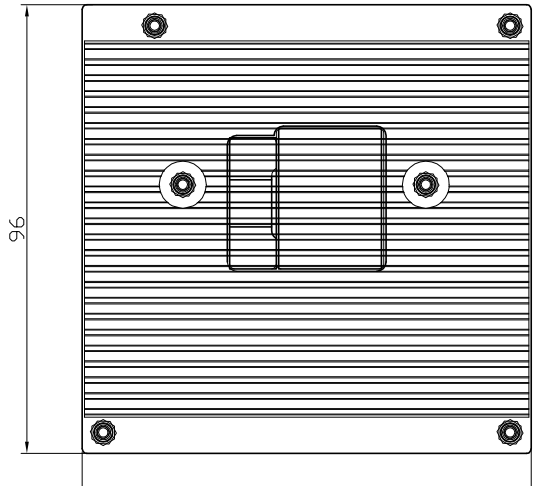
The dimensions of the cooling solutions are shown below and all measurements are in millimeters. The mechanical system assembly mounting shall follow the valid DIN/ISO specifications.

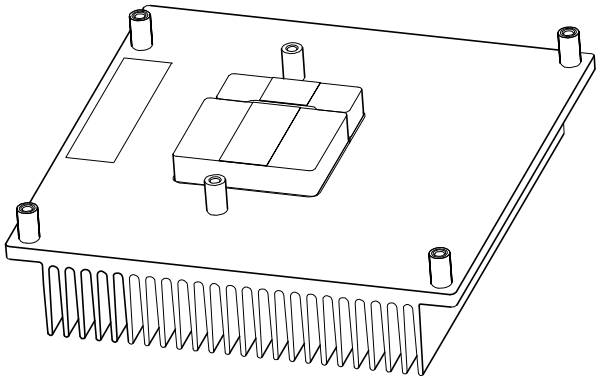
The maximum torque specification for all screws is 0.3 Nm. Higher torque may damage the module and/or carrier board.

4.1 CSP Dimensions





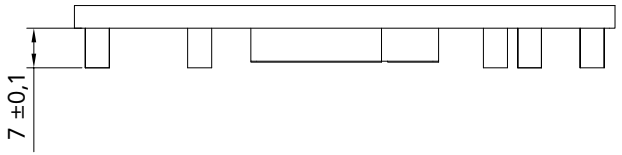


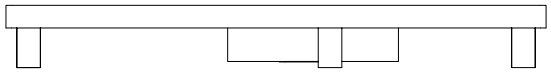


4.2 Heatspreader

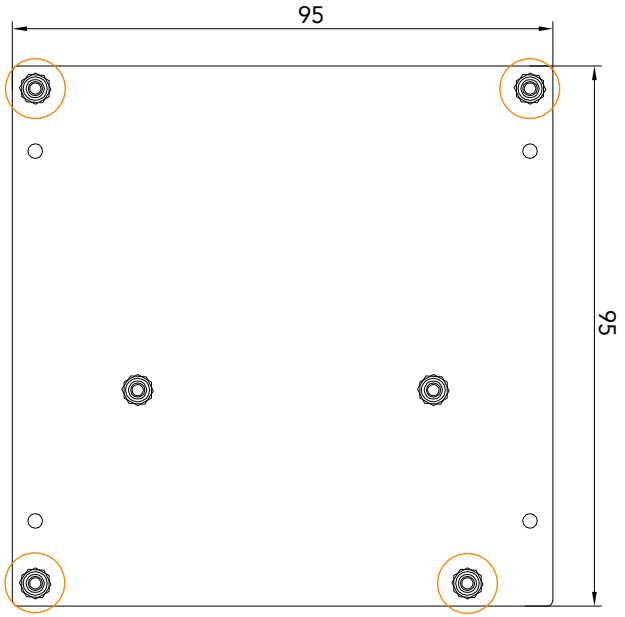
The heatspreader acts as a thermal coupling device to the module and is thermally coupled to the CPU via a thermal gap filler. On some modules, it may also be thermally coupled to other heat generating components with the use of additional thermal gap fillers. Although the heatspreader is the thermal interface where most of the heat generated by the module is dissipated, it is not to be considered as a heatsink. It has been designed as a thermal interface between the module and the application specific thermal solution.

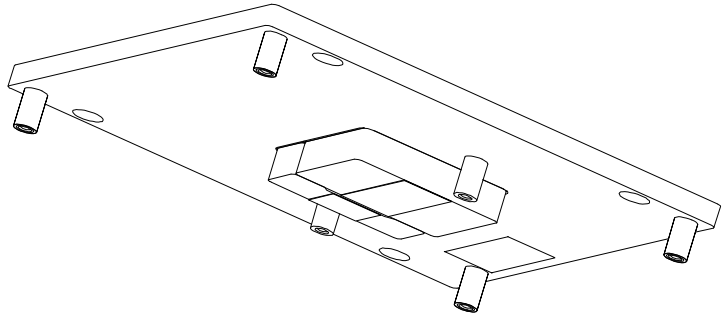
The application specific thermal solution may use heatsinks with fans, and/or heat pipes, which can be attached to the heatspreader. Some thermal solutions may also require that the heatspreader is attached directly to the systems chassis thereby using the whole chassis as a heat dissipater.





M2.5x11mm
threaded standoff
for threaded version
or
ø2.7x11mm
nonthreaded
standoff for
bore hole version





Note

The gap pad material used on all congatec heatspreaders contains silicon oil that can seep out over time depending on the environmental conditions it is subjected to. For more information about this subject, contact your local congatec sales representative and request the gap pad material manufacturer's specification.

Caution

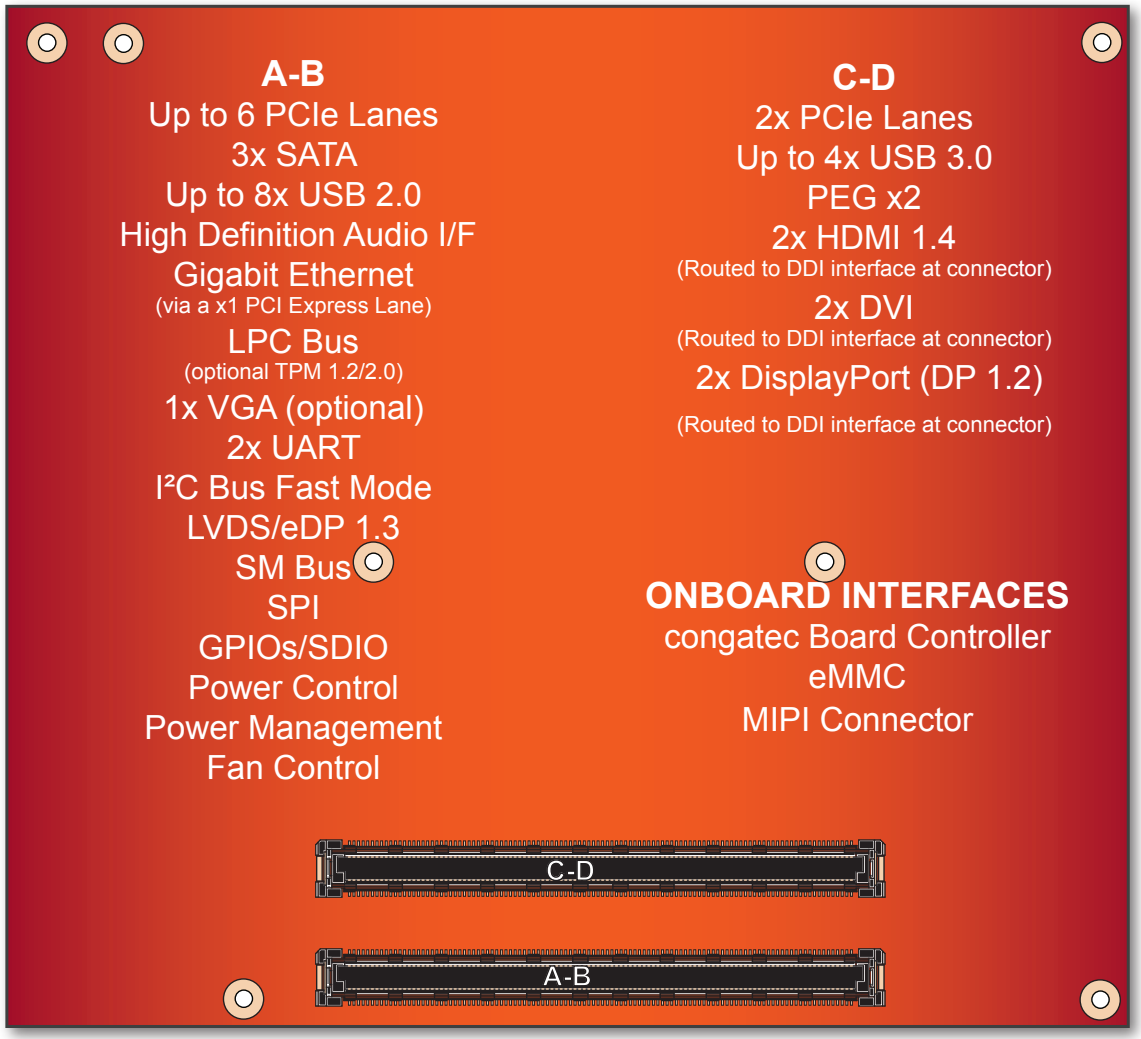
congatec heaspreaders are designed for commercial temperature range only (0° to 60°C). Therefore, do not use the heatspreaders in temperatures above 60°C or below 0°C. If an end user's system operates above 60°C or below 0°C, then the end user is responsible for designing an optimized thermal solution that meets the needs of their application.

For adequate heat dissipation, use the mounting holes on the heatspreader to attach it to the module. Apply thread-locking fluid on the screws if the heatspreader is used in a high shock and/or vibration environment. Also to prevent the standoff from stripping or cross-threading, use non-threaded carrier board standoffs to mount threaded heatspreaders.

For applications that require vertically-mounted heatspreader, use only heatspreaders that secure the thermal stacks with fixing post. Without the fixing post feature, the thermal stacks may move.

5 Connector Subsystems Rows A, B, C, D

The conga-TC170 is connected to the carrier board via two 220-pin connectors (COM Express Type 6 pinout) for a total of 440 pins connectivity. These connectors are broken down into four rows. The primary connector consists of rows A and B while the secondary connector consists of rows C and D.



top view

5.1 Primary Connector Rows A and B

The following subsystems can be found on the primary connector rows A and B.

5.1.1 Serial ATA™ (SATA)

The conga-TC170 provides three SATA interfaces (SATA 0-2) externally via the Intel® 100 Series PCH-LP integrated in the Multi-Chip Package. The SATA ports can perform DMA operation independently and are based on Serial ATA Specification, revision 3.2 with up to 6.0 Gb/s data transfer rates.

The Intel® 100 Series PCH-LP featured on the conga-TC170 has one integrated SATA host controller. This controller supports two modes of operation - AHCI mode using memory space and RAID mode. It does not support legacy mode using I/O space. Hot-plug is also supported when operating in non-native IDE mode. For more information, refer to section 10 “BIOS Setup Description”.

5.1.2 USB 2.0

The conga-TC170 offers 8 USB 2.0 interfaces on the A-B connector. The xHCI host controller in the PCH supports these interfaces with High-Speed, Full-Speed and Low-Speed USB signaling. The controller complies with USB standard 1.1 and 2.0.

5.1.3 High Definition Audio (HDA) Interface

The conga-TC170 provides an interface that supports the connection of HDA audio codecs.

5.1.4 Gigabit Ethernet

The conga-TC170 is equipped with a Gigabit Ethernet Controller that is integrated within the Intel® 100 Series PCH-LP. This controller is routed to the onboard Intel® I219-LM Phy through PCI Express lane 10. The Ethernet interface consists of 4 pairs of low voltage differential pair signals designated from GBE0_MD0± to GBE0_MD3± plus control signals for link activity indicators. These signals can be used to connect to a 10/100/1000 BaseT RJ45 connector with integrated or external isolation magnetics on the carrier board.

Note

The GBE0_LINK# output is only active during a 100Mbit or 1Gbit connection. It is not active during a 10Mbit connection. This is a limitation of Ethernet controller since it only has 3 LED outputs, ACT#, LINK100# and LINK1000#. The GBE0_LINK# signal is a logic AND of the GBE0_LINK100# and GBE0_LINK1000# signals on the conga-TC170 module.

5.1.5 LPC Bus

The conga-TC170 offers the LPC (Low Pin Count) bus through the Intel® 100 Series PCH-LP. There are many devices available for this Intel® defined bus. The LPC bus corresponds approximately to a serialized ISA bus yet with a significantly reduced number of signals. Due to the software compatibility to the ISA bus, I/O extensions such as additional serial ports can be easily implemented on an application specific baseboard using this bus. See section 9.1.1 for more information about the LPC Bus.

5.1.6 I²C Bus Fast Mode

The I²C bus is implemented through the congatec board controller (Texas Instruments Tiva™ TM4E1231H6ZRB) and accessed through the congatec CGOS driver and API. The controller provides a Fast Mode multi-master I²C Bus that has maximum I²C bandwidth.

5.1.7 PCI Express™

The conga-TC170 offers up to 6 PCI Express™ lanes on the A-B connector via the Intel® 100 Series PCH-LP. The lanes are based on PCI Express Specification 3.0 with up to 8 GT/s (Gen 3) speed.

The lanes are configured by default as 6x1 link. A 1x4 and 2x2 link configuration is also possible but requires a special/customized BIOS firmware. Contact congatec technical support for more information about this subject.

For more information on supported PCI Express lanes, see section 5.2.1.

5.1.8 ExpressCard™

The conga-TC170 supports the implementation of ExpressCards, which requires the dedication of one USB 2.0 port or a x1 PCI Express link for each ExpressCard used.

5.1.9 Graphics Output (VGA/CRT)

The Intel® Skylake ULT SoC does not natively support VGA interface. The conga-TC170 however offers the VGA interface as an option via a DisplayPort to VGA controller, connected on DDI digital port C.

Note

The conga-TC170 does not support VGA interface by default. For VGA support, you need a customized conga-TC170 variant.

5.1.10 LVDS/eDP

The conga-TC170 offers an LVDS interface with optional eDP overlay on the AB connector. The LVDS/eDP interface is by default configured to provide LVDS signals. The interface can optionally support eDP signals (assembly option). For more information, contact congatec technical center.

The single/dual channel LVDS interface is provided through an onboard eDP to LVDS bridge device. The eDP to LVDS bridge processes incoming DisplayPort stream and converts the DP protocol to LVDS, before transmitting the processed stream in LVDS format. The bridge supports single and dual channel signalling with color depths of 18 bits or 24 bits per pixel and pixel clock frequency up to 112 MHz.

Note

The LVDS/eDP interface supports either LVDS or eDP signals. Both interfaces are not supported simultaneously.

5.1.11 General Purpose Serial Interface

Two TTL compatible two wire ports are available on Type 6 COM Express modules. These pins are designated SER0_TX, SER0_RX, SER1_TX and SER1_RX. Data out of the module is on the _TX pins. Hardware handshaking and hardware flow control are not supported. The module asynchronous serial ports are intended for general purpose use and for use with debugging software that make use of the "console redirect" features available in many operating systems.

The conga-TC170 offers two UART interfaces via two UART controllers integrated in the congatec Board Controller. These controllers support up to 1MBit/s and can operate in low-speed, full-speed and high-speed modes. The UART interfaces are routed to the AB connector and require congatec driver to function.

Note

The UART interfaces do not support legacy COM port emulation.

5.1.12 GPIOs/SDIO

The conga-TC170 offers General Purpose Input/Output signals on the AB connector. The GPIO signals are multiplexed with 4 bit SD signals and controlled by the congatec Board controller. The SD card controller supports SDXC card specification 3.0.

Note

This interface by default offers General Purpose Input/Output signals on the COM Express connector.

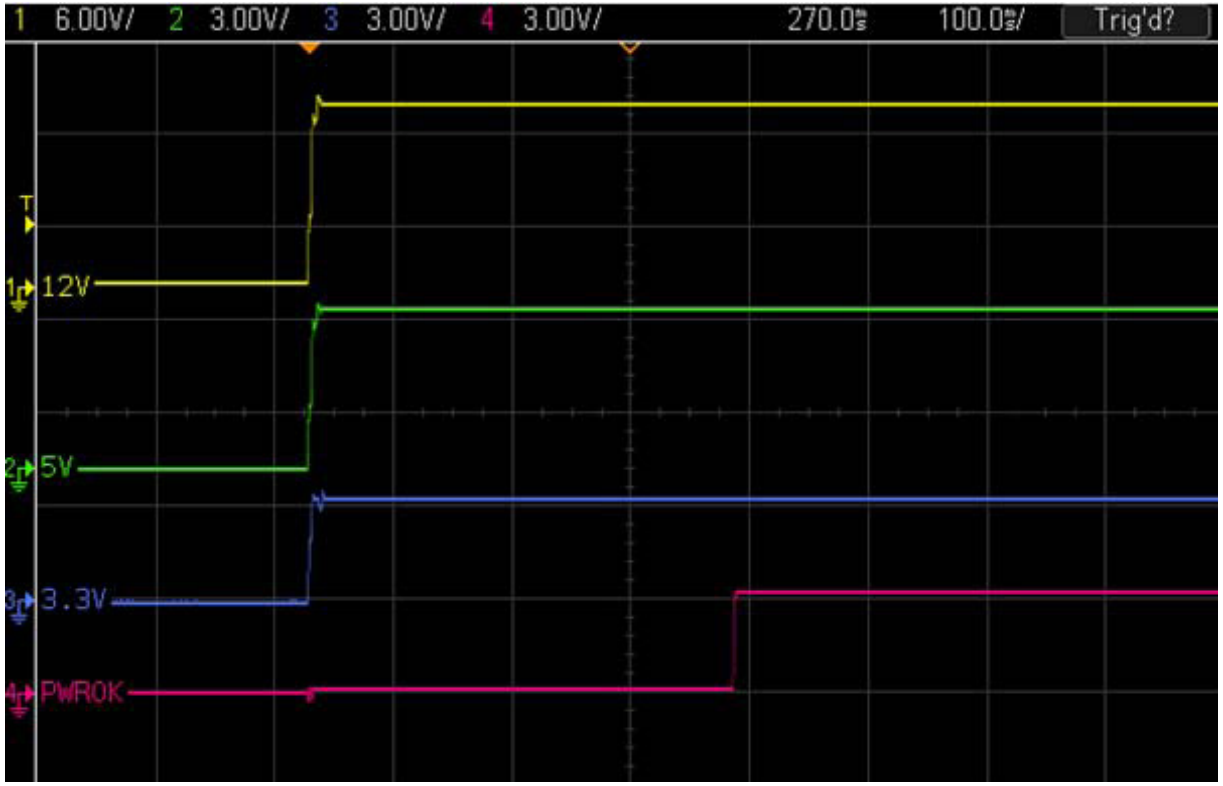
5.1.13 Power Control

PWR_OK

Power OK from main power supply or carrier board voltage regulator circuitry. A high value indicates that the power is good and the module can start its onboard power sequencing.

Carrier board hardware must drive this signal low until all power rails and clocks are stable. Releasing PWR_OK too early or not driving it low at all can cause numerous boot up problems. It is a good design practice to delay the PWR_OK signal a little (typically 100ms) after all carrier board power rails are up, to ensure a stable system.

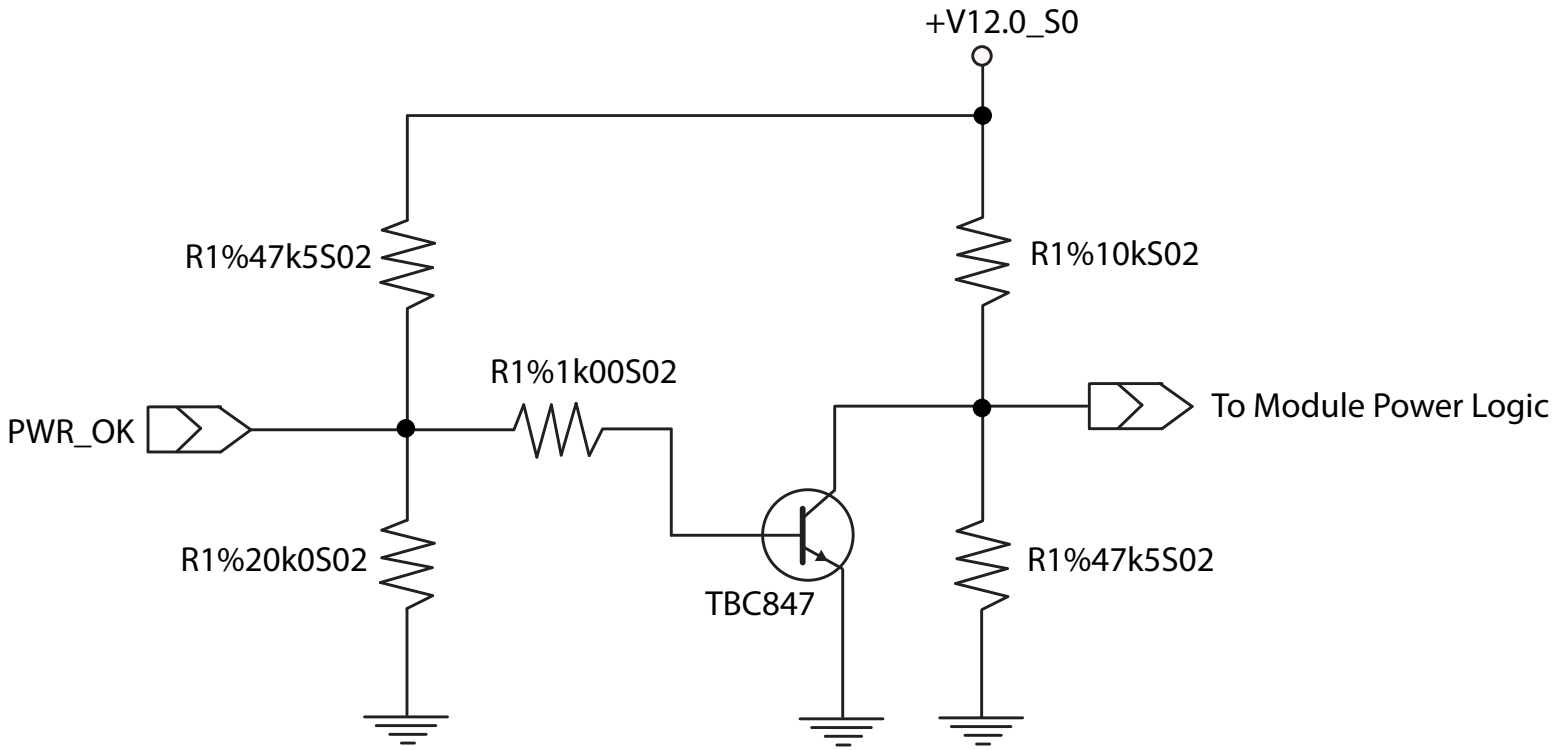
A sample screenshot is shown below:



Note

The module is kept in reset as long as the PWR_OK is driven by carrier board hardware.

The conga-TC170 PWR_OK input circuitry is implemented as shown below:



The voltage divider ensures that the input complies with 3.3V CMOS characteristic and also allows for carrier board designs that are not driving PWR_OK. Although the PWR_OK input is not mandatory for the onboard power-up sequencing, it is strongly recommended that the carrier board hardware drives the signal low until it is safe to let the module boot-up.

When considering the above shown voltage divider circuitry and the transistor stage, the voltage measured at the PWR_OK input pin may be only around 0.8V when the 12V is applied to the module. Actively driving PWR_OK high is compliant to the COM Express specification but this can cause back driving. Therefore, congatec recommends driving the PWR_OK low to keep the module in reset and tri-state PWR_OK when the carrier board hardware is ready to boot.

The three typical usage scenarios for a carrier board design are:

- Connect PWR_OK to the “power good” signal of an ATX type power supply.

- Connect PWR_OK to the last voltage regulator in the chain on the carrier board.
- Simply pull PWR_OK with a 1k resistor to the carrier board 3.3V power rail.

With this solution, it must be ensured that by the time the 3.3V is up, all carrier board hardware is fully powered and all clocks are stable.

The conga-TC170 provides support for controlling ATX-style power supplies. When not using an ATX power supply then the conga-TC170's pins SUS_S3/PS_ON, 5V_SB, and PWRBTN# should be left unconnected.

SUS_S3#/PS_ON#

The SUS_S3#/PS_ON# (pin A15 on the A-B connector) signal is an active-low output that can be used to turn on the main outputs of an ATX-style power supply. In order to accomplish this the signal must be inverted with an inverter/transistor that is supplied by standby voltage and is located on the carrier board.

PWRBTN#

When using ATX-style power supplies PWRBTN# (pin B12 on the A-B connector) is used to connect to a momentary-contact, active-low debounced push-button input while the other terminal on the push-button must be connected to ground. This signal is internally pulled up to 3V_SB using a 10k resistor. When PWRBTN# is asserted it indicates that an operator wants to turn the power on or off. The response to this signal from the system may vary as a result of modifications made in BIOS settings or by system software.

Standard 12V Power Supply Implementation Guidelines

12 volt input power is the sole operational power source for the conga-TC170. The remaining necessary voltages are internally generated on the module using onboard voltage regulators. A carrier board designer should be aware of the following important information when designing a power supply for a conga-TC170 application:

- It has also been noticed that on some occasions, problems occur when using a 12V power supply that produces non monotonic voltage when powered up. The problem is that some internal circuits on the module (e.g. clock-generator chips) will generate their own reset signals when the supply voltage exceeds a certain voltage threshold. A voltage dip after passing this threshold may lead to these circuits becoming confused resulting in a malfunction. It must be mentioned that this problem is quite rare but has been observed in some mobile power supply applications. The best way to ensure that this problem is not encountered is to observe the power supply rise waveform through the use of an oscilloscope to determine if the rise is indeed monotonic and does not have any dips. This should be done during the power supply qualification phase therefore ensuring that the above mentioned problem doesn't arise in the application. For more information about this issue visit www.formfactors.org and view page 25 figure 7 of the document "ATX12V Power Supply Design Guide V2.2".

5.1.14 Power Management

ACPI

The conga-TC170 supports Advanced Configuration and Power Interface (ACPI) specification, revision 4.0a. It also supports Suspend to RAM (S3). For more information, see section 7.3 “ACPI Suspend Modes and Resume Events”.

DEEP Sx

The Deep Sx is a lower power state employed to minimize the power consumption while in S3/S4/S5. In the Deep Sx state, the system entry condition determines if the system context is maintained or not. All power is shut off except for minimal logic which supports limited set of wake events for Deep Sx. The Deep Sx on resumption, puts system back into the state it is entered from. In other words, if Deep Sx state was entered from S3 state, then the resume path will place system back into S3.

5.2 Secondary Connector Rows C and D

The following subsystems can be found on the secondary connector rows C and D.

5.2.1 PCI Express™

The conga-TC170 offers two PCI Express lanes (lanes 6 and 7) on the CD connector. For more information on supported PCI Express lanes, see section 5.1.7.

5.2.2 PCI Express Graphics (PEG)

The conga-TC170 supports a x1 or x2 PEG port on the CD connector. The x1 or x2 PEG port is not available by default. The interface is only available as an assembly option (you need a customized conga-TC170 variant).

5.2.3 Digital Display Interface

The conga-TC170 supports up to two Digital Display Interfaces (digital port B & C). Each interface can be configured as DisplayPort, HDMI/DVI and also supports dual mode (DP++). The conga-TC170 can optionally support VGA on the DDI digital port C via a DP to VGA adapter IC. This option however requires a customized conga-TC170 variant.

The conga-TC170 supports up to three independent displays. The display combination must be 2 DDI and 1 LVDS/eDP. For customized variants with optional VGA, the combination must be 1x DDI (Port B), 1x VGA (via Port C) and 1x eDP. The table below shows the conga-TC170 display combination. This table does not apply to customized variants equipped with optional VGA interface.

Table 2 Display Combination (U-processor line)

Display 1 (DDI Port B)	Display 2 (DDI Port C)	Display 3	Display 1 Max. Resolution	Display 2 Max. Resolution	Display 3 Max. Resolution
HDMI 1.4	HDMI 1.4	eDP	4096x2160 @24Hz, 24 bpp	4096x2160 @24Hz, 24 bpp	4096x2304 @ 60Hz, 24bpp
DP	DP	eDP	4096x2304 @ 60Hz, 24bpp	4096x2304 @ 60Hz, 24bpp	4096x2304 @ 60Hz, 24bpp
HDMI 1.4	DP	eDP	4096x2160 @24Hz, 24 bpp	4096x2304 @ 60Hz, 24bpp	4096x2304 @ 60Hz, 24bpp

Note

The DP and eDP resolutions in the table above are supported for four lanes with HBR2 link data rate. The DisplayPort Aux CH, DDC channel, panel power sequencing and HPD are supported through the PCH.

5.2.3.1 HDMI

The conga-TC170 offers two HDMI ports on the CD connector via the Digital Display Interfaces. The HDMI interfaces are based on HDMI 1.4 specification with support for 3D, 4Kx2K@24Hz, Deep Color and x.v Color. These interfaces are multiplexed onto the Digital Display Interface of the COM Express connector.

Supported audio formats are AC-3 Dolby Digital, Dolby Digital Plus, DTS-HD, LPCM, 192 KHz/24 bit, 8 channel, Dolby TrueHD, DTS-HD Master Audio (Lossless Blu-Ray Disc Audio Format).

Note

The conga-TC170 supports a maximum of two independent HDMI displays. Revisions equipped with optional VGA interface support only one HDMI interface. See table 2 above for possible display combinations. Consumer electronics control (CEC) is not supported.

5.2.3.2 DVI

The conga-TC170 offers two DVI ports on the CD connector. The DVI interfaces are multiplexed onto the Digital Display Interface of the COM Express connector.

Note

The conga-TC170 supports a maximum of two independent DVI displays. Revisions equipped with optional VGA interface support only one DVI interface. See table 2 above for possible display combinations.

5.2.3.3 DisplayPort (DP)

The conga-TC170 offers two DP ports, each capable of supporting data rate of 1.62 GT/s, 2.97 GT/s and 5.4 GT/s on 1, 2 or 4 data lanes. The DP is multiplexed onto the Digital Display Interface (DDI) of the COM Express connector and can support up to 4096x2304 resolutions at 60Hz.

The DisplayPort specification is a VESA standard aimed at consolidating internal and external connection methods to reduce device complexity, supporting key cross industry applications, and providing performance scalability to enable the next generation of displays. See section 8.5 of this document for more information about enabling DisplayPort peripherals.

Note

The conga-TC170 supports a maximum of two independent DisplayPort displays. Revisions equipped with optional VGA interface support only one DP interface. See table 2 above for possible display combinations.

5.2.4 USB 3.0

The conga-TC170 offers four SuperSpeed USB 3.0 ports on the CD connector. These ports are controlled by the xHCI host controller provided by the Intel® 100 Series PCH-LP integrated in the Multi-Chip Package. The host controller allows data transfers of up to 5 Gb/s and supports SuperSpeed, High-Speed, Full-Speed and Low-Speed traffic.

Note

The xHCI controller supports USB debug port on all USB 3.0 capable ports.

6 Additional Features

6.1 congatec Board Controller (cBC)

The conga-TC170 is equipped with Texas Instruments Tiva™ TM4E1231H6ZRB microcontroller. This onboard microcontroller plays an important role for most of the congatec embedded/industrial PC features. It fully isolates some of the embedded features such as system monitoring or the I²C bus from the x86 core architecture, which results in higher embedded feature performance and more reliability, even when the x86 processor is in a low power mode. It also ensures that the congatec embedded feature set is fully compatible amongst all congatec modules.

6.2 Board Information

The cBC provides a rich data-set of manufacturing and board information such as serial number, EAN number, hardware and firmware revisions, and so on. It also keeps track of dynamically changing data like runtime meter and boot counter.

6.3 Watchdog

The conga-TC170 is equipped with a multi stage watchdog solution that is triggered by software. The COM Express™ Specification does not provide support for external hardware triggering of the Watchdog, which means the conga-TC170 does not support external hardware triggering. For more information about the Watchdog feature, see the BIOS setup description in section 10.4.2 of this document and application note AN3_Watchdog.pdf on the congatec AG website at www.congatec.com.

Note

The conga-TC170 module does not support the watchdog NMI mode.

6.4 I²C Bus

The conga-TC170 supports I²C bus. Thanks to the I²C host controller in the cBC, the I²C bus is multi-master capable and runs at fast mode.

6.5 Power Loss Control

The cBC has full control of the power-up of the module and therefore can be used to specify the behavior of the system after an AC power loss condition. Supported modes are “Always On”, “Remain Off” and “Last State”.

6.6 OEM BIOS Customization

The conga-TC170 is equipped with congatec Embedded BIOS, which is based on American Megatrends Inc. Aptio UEFI firmware. The congatec Embedded BIOS allows system designers to modify the BIOS. For more information about customizing the congatec Embedded BIOS, refer to the congatec System Utility user's guide CGUTLm1x.pdf on the congatec website at www.congatec.com or contact technical support.

The customization features supported are described below:

6.6.1 OEM Default Settings

This feature allows system designers to create and store their own BIOS default configuration. Customized BIOS development by congatec for OEM default settings is no longer necessary because customers can easily perform this configuration by themselves using the congatec system utility CGUTIL. See congatec application note AN8_Create_OEM_Default_Map.pdf on the congatec website for details on how to add OEM default settings to the congatec Embedded BIOS.

6.6.2 OEM Boot Logo

This feature allows system designers to replace the standard text output displayed during POST with their own BIOS boot logo. Customized BIOS development by congatec for OEM Boot Logo is no longer necessary because customers can easily perform this configuration by themselves using the congatec system utility CGUTIL. See congatec application note AN8_Create_And_Add_Bootlogo.pdf on the congatec website for details on how to add OEM boot logo to the congatec Embedded BIOS.

6.6.3 OEM POST Logo

This feature allows system designers to replace the congatec POST logo displayed in the upper left corner of the screen during BIOS POST with their own BIOS POST logo. Use the congatec system utility CGUTIL 1.5.4 or later to replace/add the OEM POST logo.

6.6.4 OEM BIOS Code/Data

With the congatec embedded BIOS it is possible for system designers to add their own code to the BIOS POST process. The congatec Embedded BIOS first calls the OEM code before handing over control to the OS loader.

Except for custom specific code, this feature can also be used to support Win XP SLP installation, Window 7 SLIC table (OA2.0), Windows 8 OEM activation (OA3.0), verb tables for HDA codecs, PCI/PCIe opROMs, bootloaders, rare graphic modes and Super I/O controller initialization.

Note

The OEM BIOS code of the new UEFI based firmware is only called when the CSM (Compatibility Support Module) is enabled in the BIOS setup menu. Contact congatec technical support for more information on how to add OEM code.

6.6.5 OEM DXE Driver

This feature allows designers to add their own UEFI DXE driver to the congatec embedded BIOS. Contact congatec technical support for more information on how to add an OEM DXE driver.

6.7 congatec Battery Management Interface

In order to facilitate the development of battery powered mobile systems based on embedded modules, congatec AG has defined an interface for the exchange of data between a CPU module (using an ACPI operating system) and a Smart Battery system. A system developed according to the congatec Battery Management Interface Specification can provide the battery management functions supported by an ACPI capable operating system (e.g. charge state of the battery, information about the battery, alarms/events for certain battery states, ...) without the need for any additional modifications to the system BIOS.

In addtion to the ACPI-Compliant Control Method Battery mentioned above, the latest versions of the conga-TC170 BIOS and board controller firmware also support LTC1760 battery manager from Linear Technology and a battery only solution (no charger). All three battery solutions are supported on the I2C bus and the SMBus. This gives the system designer more flexibility when choosing the appropriate battery sub-system.

For more information about this subject visit the congatec website and view the following documents:

- congatec Battery Management Interface Specification
- Battery System Design Guide
- conga-SBM^3 User's Guide

6.8 API Support (CGOS)

In order to benefit from the above mentioned non-industry standard feature set, congatec provides an API that allows application software developers to easily integrate all these features into their code. The CGOS API (congatec Operating System Application Programming Interface) is the congatec proprietary API that is available for all commonly used Operating Systems such as Win32, Win64, Win CE, Linux. The architecture of the CGOS API driver provides the ability to write application software that runs unmodified on all congatec CPU modules. All the hardware related code is contained within the congatec embedded BIOS on the module. See section 1.1 of the CGOS API software developers guide, which is available on the congatec website .

6.9 Security Features

The conga-TC170 can be equipped optionally with a "Trusted Platform Module" (TPM 1.2/2.0). This TPM 1.2/2.0 includes coprocessors to calculate efficient hash and RSA algorithms with key lengths up to 2,048 bits as well as a real random number generator. Security sensitive applications like gaming and e-commerce will benefit also with improved authentication, integrity and confidence levels.

6.10 Suspend to Ram

The Suspend to RAM feature is available on the conga-TC170.

7 conga Tech Notes

The conga-TC170 has some technological features that require additional explanation. The following section will give the reader a better understanding of some of these features. This information will also help to gain a better understanding of the information found in the System Resources section of this user's guide as well as some of the setup nodes found in the BIOS Setup Program description section.

7.1 Intel® PCH-LP Features

7.1.1 Intel® Rapid Storage Technology

The Intel® 100 Series PCH-LP provides support for Intel® Rapid Storage Technology, allowing AHCI functionality and RAID 0/1/5/10 support.

7.1.1.1 AHCI

The Intel® 100 Series PCH-LP provides hardware support for Advanced Host Controller Interface (AHCI), a standardized programming interface for SATA host controllers. Platforms supporting AHCI may take advantage of performance features such as port independent DMA engines (each device is treated as a master) and hardware-assisted native command queuing. AHCI also provides usability enhancements such as Hot-Plug and advanced power management.

7.1.1.2 RAID

The integrated RAID capability provides RAID 0, 1, 5, and 10 functionality on the 4 SATA ports of Intel® 100 Series PCH-LP. Software components include an Option ROM for pre-boot configuration and boot functionality, a Microsoft Windows compatible driver, and a user interface for configuration and management of the RAID capability of the Intel® 100 Series PCH-LP.

7.1.1.3 Intel® Smart Response Technology

Intel® Smart Response Technology is a disk caching solution that can provide improved computer system performance with improved power savings. It allows configuration of a computer systems with the advantage of having HDDs for maximum storage capacity with system performance at or near SSD performance levels.

Note

This feature requires an Intel® Core Processor and a solid state hybrid drive with minimum 16GB capacity and SATA-10 Hybrid Information support.

7.2 Intel® Processor Features

7.2.1 Intel® Turbo Boost Technology

Intel® Turbo Boost Technology allows processor cores to run faster than the base operating frequency if it's operating below power, current, and temperature specification limits. Intel® Turbo Boost Technology is activated when the Operating System (OS) requests the highest processor performance state. The maximum frequency of Intel® Turbo Boost Technology is dependent on the number of active cores. The amount of time the processor spends in the Intel Turbo Boost 2 Technology state depends on the workload and operating environment. Any of the following can set the upper limit of Intel® Turbo Boost Technology on a given workload:

- Number of active cores
- Estimated current consumption
- Estimated power consumption
- Processor temperature

When the processor is operating below these limits and the user's workload demands additional performance, the processor frequency will dynamically increase by 100 MHz on short and regular intervals until the upper limit is met or the maximum possible upside for the number of active cores is reached. For more information about Intel® Turbo Boost 2 Technology visit the Intel® website.

Note

Only conga-TC170 module variants that feature the Core™ i7 and i5 processors support Intel® Turbo Boost 2 Technology. Refer to the power consumption tables in section 2.5 of this document for information about the maximum turbo frequency available for each variant of the conga-TC170.

7.2.2 Adaptive Thermal Monitor and Catastrophic Thermal Protection

Intel® Xeon, Core™ i7/i5/i3 and Celeron® processors have a thermal monitor feature that helps to control the processor temperature. The integrated TCC (Thermal Control Circuit) activates if the processor silicon reaches its maximum operating temperature. The activation temperature that the Intel® Thermal Monitor uses to activate the TCC can be slightly modified via TCC Activation Offset in BIOS setup submenu "CPU submenu".

The Adaptive Thermal Monitor controls the processor temperature using two methods:

- Adjusting the processor's operating frequency and core voltage (EIST transitions)
- Modulating (start/stop) the processor's internal clocks at a duty cycle of 25% on and 75% off

When activated, the TCC causes both processor core and graphics core to reduce frequency and voltage adaptively. The Adaptive Thermal Monitor will remain active as long as the package temperature remains at its specified limit. Therefore, the Adaptive Thermal Monitor will continue to reduce the package frequency and voltage until the TCC is de-activated. Clock modulation is activated if frequency and voltage adjustments are insufficient. Additional hardware, software drivers, or operating system support is not required.

Note

The maximum operating temperature for Intel® Xeon, Core™ i7/i5/i3 and Celeron® processors is 100°C.

To ensure that the TCC is active for only short periods of time, thus reducing the impact on processor performance to a minimum, it is necessary to have a properly designed thermal solution. The Intel® Xeon, Core™ i7/i5/i3 and Celeron® processor's respective datasheet can provide you with more information about this subject.

Intel®'s Core™ i7/i5/i3 and Celeron® processors use the THERMTRIP# signal to shut down the system if the processor's silicon reaches a temperature of approximately 125°C. The THERMTRIP# signal activation is completely independent from processor activitiy and therefore does not produce any bus cycles.

Note

In order for THERMTRIP# to be able to automatically switch off the system, it is necessary to use an ATX style power supply.

7.2.3 Processor Performance Control

Intel® processors found on the conga-TC170 run at different voltage/frequency states (performance states), which is referred to as Enhanced Intel® SpeedStep® technology (EIST). Operating systems that support performance control take advantage of microprocessors that use several different performance states in order to efficiently operate the processor when it's not being fully used. The operating system will determine the necessary performance state that the processor should run at so that the optimal balance between performance and power consumption can be achieved during runtime.

The Windows family of operating systems links its processor performance control policy to the power scheme setting. You must ensure that the power scheme setting you choose has the ability to support Enhanced Intel® SpeedStep® technology.

Intel Speed Shift is a new and energy efficient method for frequency control featured in the 6th Generation *Intel® Core™* processor family. This feature is also referred to as Hardware-controlled Performance States (HWP). It is a hardware implementation of the ACPI defined Collaborative Processor Performance Control (CPPC2) and is supported by newer operating systems (Win 8.1 or newer).

With this feature enabled, the processor autonomously selects performance states based on workload demand and thermal limits while also considering information provided by the OS e.g., the performance limits and workload history.

7.2.4 Intel® 64 Architecture

The formerly known Intel® Extended Memory 64 Technology is an enhancement to Intel®'s IA-32 architecture. Intel® 64 is only available on Intel® processors and is designed to run with newly written 64-bit code and access more than 4GB of memory. Processors with Intel® 64 architecture support 64-bit-capable operating systems from Microsoft, Red Hat and SuSE. Processors running in legacy mode remain fully compatible with today's existing 32-bit applications and operating systems

Platforms with Intel® 64 can be run in three basic ways :

1. **Legacy Mode:** 32-bit operating system and 32-bit applications. In this mode no software changes are required, however the benefits of Intel® 64 are not utilized.

2. **Compatibility Mode:** 64-bit operating system and 32-bit applications. This mode requires all device drivers to be 64-bit. The operating system will see the 64-bit extensions but the 32-bit application will not. Existing 32-bit applications do not need to be recompiled and may or may not benefit from the 64-bit extensions. The application will likely need to be re-certified by the vendor to run on the new 64-bit extended operating system.

3. **64-bit Mode:** 64-bit operating system and 64-bit applications. This usage requires 64-bit device drivers. It also requires applications to be modified for 64-bit operation and then recompiled and validated.

Intel® 64 supports:

- 64-bit flat virtual address space
- 64-bit pointers
- 64-bit wide general purpose registers
- 64-bit integer support
- Up to one Terabyte (TB) of platform address space

You can find more information about Intel® 64 Technology at: http://developer.intel.com/technology/intel64/index.htm

7.2.5 Intel® Virtualization Technology

Virtualization solutions enhanced by Intel® VT will allow a Xeon and Core™ i7/i5/i3 platform to run multiple operating systems and applications in independent partitions. When using virtualization capabilities, one computer system can function as multiple "virtual" systems. With processor and I/O enhancements to Intel®'s various platforms, Intel® Virtualization Technology can improve the performance and robustness of today's software-only virtual machine solutions.

Intel® VT is a multi-generational series of extensions to Intel® processor and platform architecture that provides a new hardware foundation for virtualization, establishing a common infrastructure for all classes of Intel® based systems. The broad availability of Intel® VT makes it possible to create entirely new applications for virtualization in servers, clients as well as embedded systems thus providing new ways to improve system reliability, manageability, security, and real-time quality of service.

The success of any new hardware architecture is highly dependent on the system software that puts its new features to use. In the case of virtualization technology, that support comes from the virtual machine monitor (VMM), a layer of software that controls the underlying physical platform resources sharing them between multiple "guest" operating systems. Intel® VT is already incorporated into most commercial and open-source VMMs including those from VMware, Microsoft, XenSource, Parallels, Virtual Iron, Jaluna and TenAsys.

You can find more information about Intel® Virtualization Technology at: http://developer.intel.com/technology/virtualization/index.htm

Note

congatec does not offer virtual machine monitor (VMM) software. All VMM software support questions and queries should be directed to the VMM software vendor and not congatec technical support.

7.2.6 Thermal Management

ACPI is responsible for allowing the operating system to play an important part in the system's thermal management. This results in the operating system having the ability to take control of the operating environment by implementing cooling decisions according to the demands put on the CPU by the application.

The conga-TC170 supports Critical Trip Point. This cooling policy ensures that the operating system shuts down properly if the temperature in the thermal zone reaches a critical point, in order to prevent damage to the system as a result of high temperatures. Use the "critical trip point" setup node in the BIOS setup program to determine the temperature threshold that the operating system will use to shut down the system.

For processor passive cooling, use the Thermal Control Circuit (TCC) Activation Offset setting in the CPU configuration setup sub menu. The TCC in the processor is activated at 100°C by default but can be lowered by the Activation Offset e.g., setting 10 activates TCC at 90°C. ACPI OS support is not required.

Note

The end user must determine the cooling preferences for the system by using the setup nodes in the BIOS setup program to establish the appropriate trip points.

7.3 ACPI Suspend Modes and Resume Events

conga-TC170 supports S3 (STR= Suspend to RAM). For more information about S3 wake events, see section 10.4.5 “ACPI Configuration Submenu”.

S4 (Suspend to Disk) is not supported by the BIOS (S4_BIOS) but it is supported by the following operating systems (S4_OS= Hibernate):

- Windows 8, Windows 7, Windows 10, Linux.

This table lists the “Wake Events” that resume the system from S3 unless otherwise stated in the “Conditions/Remarks” column:

Wake Event	Conditions/Remarks
Power Button	Wakes unconditionally from S3-S5.
Onboard LAN Event	Device driver must be configured for Wake On LAN support.
SMBALERT#	Wakes unconditionally from S3-S5.
PCI Express WAKE#	Wakes unconditionally from S3-S5.
WAKE#	Wakes uncondionally from S3.
PME#	Activate the wake up capabilities of a PCI device using Windows Device Manager configuration options for this device OR set Resume On PME# to Enabled in the Power setup menu.
USB Mouse/Keyboard Event	When Standby mode is set to S3, USB hardware must be powered by standby power source. Set USB Device Wakeup from S3/S4 to ENABLED in the ACPI setup menu (if setup node is available in BIOS setup program). In Device Manager look for the keyboard/mouse devices. Go to the Power Management tab and check ‘Allow this device to bring the computer out of standby’.
RTC Alarm	Activate and configure Resume On RTC Alarm in the Power setup menu. Only available in S5.
Watchdog Power Button Event	Wakes unconditionally from S3-S5.

7.4 DDR4 Memory

The Intel Skylake ULT SoC featured on the conga-TC170 supports DDR4 memory modules up to 2133 MT/s. The DDR4 memory modules have lower voltage requirements with higher data rate transfer speeds. They operate at a voltage of 1.2V. With this low voltage system memory interface on the processor, the conga-TC170 offers a system optimized for lowest possible power consumption. The reduction in power consumption due to lower voltage subsequently reduces the heat generated.

8 Signal Descriptions and Pinout Tables

The following section describes the signals found on COM Express™ Type VI connectors used for congatec AG modules. The pinout of the modules complies with COM Express Type 6 Rev. 2.1.

Table 3 describes the terminology used in this section for the Signal Description tables. The PU/PD column indicates if a COM Express™ module pull-up or pull-down resistor has been used. If the field entry area in this column for the signal is empty, then no pull-up or pull-down resistor has been implemented by congatec.

The "#" symbol at the end of the signal name indicates that the active or asserted state occurs when the signal is at a low voltage level. When "#" is not present, the signal is asserted when at a high voltage level.

Note

The Signal Description tables do not list internal pull-ups or pull-downs implemented by the chip vendors, only pull-ups or pull-downs implemented by congatec are listed. For information about the internal pull-ups or pull-downs implemented by the chip vendors, refer to the respective chip's datasheet.

Table 3 Signal Tables Terminology Descriptions

Term	Description
PU	congatec implemented pull-up resistor
PD	congatec implemented pull-down resistor
I/O 3.3V	Bi-directional signal 3.3V tolerant
I/O 5V	Bi-directional signal 5V tolerant
I 3.3V	Input 3.3V tolerant
I 5V	Input 5V tolerant
I/O 3.3VSB	Input 3.3V tolerant active in standby state
O 3.3V	Output 3.3V signal level
O 5V	Output 5V signal level
OD	Open drain output
P	Power Input/Output
DDC	Display Data Channel
PCIE	In compliance with PCI Express Base Specification, Revision 2.0
PEG	PCI Express Graphics
SATA	In compliance with Serial ATA specification Revision 2.6 and 3.0.
REF	Reference voltage output. May be sourced from a module power plane.
PDS	Pull-down strap. A module output pin that is either tied to GND or is not connected. Used to signal module capabilities (pinout type) to the Carrier Board.

8.1 A-B Connector Signal Descriptions

Table 4 Intel® High Definition Audio Link Signals Descriptions

Signal	Pin #	Description	I/O	PU/PD	Comment
AC/HDA_RST#	A30	Intel® High Definition Audio Reset: This signal is the master hardware reset to external codec(s).	O 3.3VSB		AC'97 codecs are not supported.
AC/HDA_SYNC	A29	Intel® High Definition Audio Sync: This signal is a 48 kHz fixed rate sample sync to the codec(s). It is also used to encode the stream number.	O 3.3VSB		AC'97 codecs are not supported.
AC/HDA_BITCLK	A32	Intel® High Definition Audio Bit Clock Output: This signal is a 24.000MHz serial data clock generated by the Intel® High Definition Audio controller.	O 3.3VSB		AC'97 codecs are not supported.
AC/HDA_SDOUT	A33	Intel® High Definition Audio Serial Data Out: This signal is the serial TDM data output to the codec(s). This serial output is double-pumped for a bit rate of 48 Mb/s for Intel® High Definition Audio.	O 3.3VSB	PU 1K 3.3VSB	AC'97 codecs are not supported. AC/HDA_SDOUT is a boot strap signal (see note below)
AC/HDA_SDIN[1:0]	B29-B30	Intel® High Definition Audio Serial Data In [0]: These signals are serial TDM data inputs from the three codecs. The serial input is single-pumped for a bit rate of 24 Mb/s for Intel® High Definition Audio.	I 3.3VSB		Pin B28 (HDA_SDIN2) is not connected.

Note

Some signals have special functionality during the reset process. They may bootstrap some basic important functions of the module.

For more information refer to section 8.5 of this user's guide.

Table 5 Gigabit Ethernet Signal Descriptions

Gigabit Ethernet	Pin #	Description				I/O	PU/PD	Comment
GBE0_MDI0+ GBE0_MDI0- GBE0_MDI1+ GBE0_MDI1- GBE0_MDI2+ GBE0_MDI2- GBE0_MDI3+ GBE0_MDI3-	A13 A12 A10 A9 A7 A6 A3 A2	Gigabit Ethernet Controller 0: Media Dependent Interface Differential Pairs 0, 1, 2, 3. The MDI can operate in 1000, 100, and 10Mbit/sec modes. Some pairs are unused in some modes according to the following:				I/O Analog		Twisted pair signals for external transformer.
			1000	100	10			
		MDI[0]+/-	B1_DA+/-	TX+/-	TX+/-			
		MDI[1]+/-	B1_DB+/-	RX+/-	RX+/-			
		MDI[2]+/-	B1_DC+/-					
		MDI[3]+/-	B1_DD+/-					
GBE0_ACT#	B2	Gigabit Ethernet Controller 0 activity indicator, active low.				O 3.3VSB		
GBE0_LINK#	A8	Gigabit Ethernet Controller 0 link indicator, active low.				O 3.3VSB		
GBE0_LINK100#	A4	Gigabit Ethernet Controller 0 100Mbit/sec link indicator, active low.				O 3.3VSB		
GBE0_LINK1000#	A5	Gigabit Ethernet Controller 0 1000Mbit/sec link indicator, active low.				O 3.3VSB		

Gigabit Ethernet	Pin #	Description	I/O	PU/PD	Comment
GBE0_CTREF	A14	Reference voltage for Carrier Board Ethernet channel 0 magnetics center tap. The reference voltage is determined by the requirements of the module PHY and may be as low as 0V and as high as 3.3V. The reference voltage output shall be current limited on the module. In the case in which the reference is shorted to ground, the current shall be limited to 250mA or less.			Not connected

Note

The GBE0_LINK# output is only active during a 100Mbit or 1Gbit connection, it is not active during a 10Mbit connection. This is a limitation of the Ethernet controller because it has only three LED outputs (ACT#, LINK100# and LINK1000#).

The GBE0_LINK# signal is a logic AND of the GBE0_LINK100# and GBE0_LINK1000# signals on the conga-TC170 module.

Table 6 Serial ATA Signal Descriptions

Signal	Pin #	Description	I/O	PU/PD	Comment
SATA0_RX+ SATA0_RX-	A19 A20	Serial ATA channel 0, Receive Input differential pair.	I SATA		Supports Serial ATA specification, Revision 3.0
SATA0_TX+ SATA0_TX-	A16 A17	Serial ATA channel 0, Transmit Output differential pair.	O SATA		Supports Serial ATA specification, Revision 3.0
SATA1_RX+ SATA1_RX-	B19 B20	Serial ATA channel 1, Receive Input differential pair.	I SATA		Supports Serial ATA specification, Revision 3.0
SATA1_TX+ SATA1_TX-	B16 B17	Serial ATA channel 1, Transmit Output differential pair.	O SATA		Supports Serial ATA specification, Revision 3.0
SATA2_RX+ SATA2_RX-	A25 A26	Serial ATA channel 2, Receive Input differential pair.	I SATA		Supports Serial ATA specification, Revision 3.0
SATA2_TX+ SATA2_TX-	A22 A23	Serial ATA channel 2, Transmit Output differential pair.	O SATA		Supports Serial ATA specification, Revision 3.0
SATA3_RX+ SATA3_RX-	B25 B26	Serial ATA channel 3, Receive Input differential pair.	I SATA		Not supported. The Intel chipset supports only 3 SATA ports.
SATA3_TX+ SATA3_TX-	B22 B23	Serial ATA channel 3, Transmit Output differential pair.	O SATA		Not supported. The Intel chipset supports only 3 SATA ports.
(S)ATA_ACT#	A28	ATA (parallel and serial) or SAS activity indicator, active low.	I/O 3.3v		

Table 7 PCI Express Signal Descriptions (general purpose)

Signal	Pin #	Description	I/O	PU/PD	Comment
PCIE_RX0+ PCIE_RX0-	B68 B69	PCI Express channel 0, Receive Input differential pair.	I PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_TX0+ PCIE_TX0-	A68 A69	PCI Express channel 0, Transmit Output differential pair.	O PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_RX1+ PCIE_RX1-	B64 B65	PCI Express channel 1, Receive Input differential pair.	I PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_TX1+ PCIE_TX1-	A64 A65	PCI Express channel 1, Transmit Output differential pair.	O PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_RX2+ PCIE_RX2-	B61 B62	PCI Express channel 2, Receive Input differential pair.	I PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_TX2+ PCIE_TX2-	A61 A62	PCI Express channel 2, Transmit Output differential pair.	O PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_RX3+ PCIE_RX3-	B58 B59	PCI Express channel 3, Receive Input differential pair.	I PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_TX3+ PCIE_TX3-	A58 A59	PCI Express channel 3, Transmit Output differential pair.	O PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_RX4+ PCIE_RX4-	B55 B56	PCI Express channel 4, Receive Input differential pair.	I PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_TX4+ PCIE_TX4-	A55 A56	PCI Express channel 4, Transmit Output differential pair.	O PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_RX5+ PCIE_RX5-	B52 B53	PCI Express channel 5, Receive Input differential pair.	I PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_TX5+ PCIE_TX5-	A52 A53	PCI Express channel 5, Transmit Output differential pair.	O PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_CLK_REF+ PCIE_CLK_REF-	A88 A89	PCI Express Reference Clock output for all PCI Express and PCI Express Graphics Lanes.	O PCIE		A PCI Express Gen2/3 compliant clock buffer chip must be used on the carrier board if the design involves more than one PCI Express device.

Note

PCIe lanes 4 and 5 are not supported if the optional PEG port is implemented.

Table 8 ExpressCard Support Pins Signal Descriptions

Signal	Pin #	Description	I/O	PU/PD	Comment
EXCD0_CPPE# EXCD1_CPPE#	A49 B48	ExpressCard capable card request.	I 3.3V	PU 10k 3.3VSB	

EXCD0_PERST# EXCD1_PERST#	A48 B47	ExpressCard Reset	O 3.3V	PU 10k 3.3V	

Table 9 LPC Signal Descriptions

Signal	Pin #	Description	I/O	PU/PD	Comment
LPC_AD[0:3]	B4-B7	LPC multiplexed address, command and data bus	I/O 3.3V		
LPC_FRAME#	B3	LPC frame indicates the start of an LPC cycle	O 3.3V		
LPC_DRQ[0:1]#	B8-B9	LPC serial DMA request	I 3.3V	PU 10k 3.3V	
LPC_SERIRQ	A50	LPC serial interrupt	I/O OD 3.3V	PU 10k 3.3V	
LPC_CLK	B10	LPC clock output - 24 MHz nominal	O 3.3V		

Table 10 USB Signal Descriptions

Signal	Pin #	Description	I/O	PU/PD	Comment
USB0+	B46	USB Port 0, data + or D+	I/O		USB 2.0 compliant. Backwards compatible to USB 1.1
USB0-	B45	USB Port 0, data - or D-	I/O		USB 2.0 compliant. Backwards compatible to USB 1.1
USB1+	A46	USB Port 1, data + or D+	I/O		USB 2.0 compliant. Backwards compatible to USB 1.1
USB1-	A45	USB Port 1, data - or D-	I/O		USB 2.0 compliant. Backwards compatible to USB 1.1
USB2+	A43	USB Port 2, data + or D+	I/O		USB 2.0 compliant. Backwards compatible to USB 1.1
USB2-	A42	USB Port 2, data - or D-	I/O		USB 2.0 compliant. Backwards compatible to USB 1.1
USB3+	B43	USB Port 3, data + or D+	I/O		USB 2.0 compliant. Backwards compatible to USB 1.1
USB3-	B42	USB Port 3, data - or D-	I/O		USB 2.0 compliant. Backwards compatible to USB 1.1
USB4+	A40	USB Port 4, data + or D+	I/O		USB 2.0 compliant. Backwards compatible to USB 1.1
USB4-	A39	USB Port 4, data - or D-	I/O		USB 2.0 compliant. Backwards compatible to USB 1.1
USB5+	B40	USB Port 5, data + or D+	I/O		USB 2.0 compliant. Backwards compatible to USB 1.1
USB5-	B39	USB Port 5, data - or D-	I/O		USB 2.0 compliant. Backwards compatible to USB 1.1
USB6+	A37	USB Port 6, data + or D+	I/O		USB 2.0 compliant. Backwards compatible to USB 1.1
USB6-	A36	USB Port 6, data - or D-	I/O		USB 2.0 compliant. Backwards compatible to USB 1.1
USB7+	B37	USB Port 7, data + or D+	I/O		USB 2.0 compliant. Backwards compatible to USB 1.1
USB7-	B36	USB Port 7, data - or D-	I/O		USB 2.0 compliant. Backwards compatible to USB 1.1
USB_0_1_OC#	B44	USB over-current sense, USB ports 0 and 1. A pull-up for this line shall be present on the module. An open drain driver from a USB current monitor on the carrier board may drive this line low.	I 3.3VSB	PU 10k 3.3VSB	Do not pull this line high on the carrier board.
USB_2_3_OC#	A44	USB over-current sense, USB ports 2 and 3. A pull-up for this line shall be present on the module. An open drain driver from a USB current monitor on the carrier board may drive this line low. .	I 3.3VSB	PU 10k 3.3VSB	Do not pull this line high on the carrier board.
USB_4_5_OC#	B38	USB over-current sense, USB ports 4 and 5. A pull-up for this line shall be present on the module. An open drain driver from a USB current monitor on the carrier board may drive this line low.	I 3.3VSB	PU 10k 3.3VSB	Do not pull this line high on the carrier board.

Signal	Pin #	Description	I/O	PU/PD	Comment
USB_6_7_OC#	A38	USB over-current sense, USB ports 6 and 7. A pull-up for this line shall be present on the module. An open drain driver from a USB current monitor on the carrier board may drive this line low.	I 3.3VSB	PU 10k 3.3VSB	Do not pull this line high on the carrier board.

Table 11 CRT Signal Descriptions

Signal	Pin #	Description	I/O	PU/PD	Comment
VGA_RED	B89	Red for monitor. Analog DAC output, designed to drive a 37.5-Ohm equivalent load.	O Analog	PD 150R	Optional
VGA_GRN	B91	Green for monitor. Analog DAC output, designed to drive a 37.5-Ohm equivalent load.	O Analog	PD 150R	Optional
VGA_BLU	B92	Blue for monitor. Analog DAC output, designed to drive a 37.5-Ohm equivalent load.	O Analog	PD 150R	Optional
VGA_HSYNC	B93	Horizontal sync output to VGA monitor	O 3.3V		Optional
VGA_VSYNC	B94	Vertical sync output to VGA monitor	O 3.3V		Optional
VGA_I2C_CK	B95	DDC clock line (I²C port dedicated to identify VGA monitor capabilities)	I/O OD 5V	PU 1k2 3.3V	Optional
VGA_I2C_DAT	B96	DDC data line.	I/O OD 5V	PU 1k2 3.3V	Optional

Note

The conga-TC170 does not support the VGA interface by default. To support VGA, you need a customized conga-TC170 variant.

Table 12 LVDS Signal Descriptions

Signal	Pin #	Description	I/O	PU/PD	Comment
LVDS_A0+ LVDS_A0- LVDS_A1+ LVDS_A1- LVDS_A2+ LVDS_A2- LVDS_A3+ LVDS_A3-	A71 A72 A73 A74 A75 A76 A78 A79	LVDS Channel A differential pairs	O LVDS		
LVDS_A_CK+ LVDS_A_CK-	A81 A82	LVDS Channel A differential clock	O LVDS		
LVDS_B0+ LVDS_B0- LVDS_B1+ LVDS_B1- LVDS_B2+ LVDS_B2- LVDS_B3+ LVDS_B3-	B71 B72 B73 B74 B75 B76 B77 B78	LVDS Channel B differential pairs	O LVDS		
LVDS_B_CK+ LVDS_B_CK-	B81 B82	LVDS Channel B differential clock	O LVDS		

Signal	Pin #	Description	I/O	PU/PD	Comment
LVDS_VDD_EN	A77	LVDS panel power enable	O 3.3V	PD 10k	
LVDS_BKLT_EN	B79	LVDS panel backlight enable	O 3.3V	PD 10k	
LVDS_BKLT_CTRL	B83	LVDS panel backlight brightness control	O 3.3V		
LVDS_I2C_CK	A83	DDC lines used for flat panel detection and control.	O 3.3V	PU 2k2 3.3V for LVDS support (default)	
LVDS_I2C_DAT	A84	DDC lines used for flat panel detection and control.	I/O 3.3V	PU 2k2 3.3V for LVDS support (default)	.

Table 13 Embedded DisplayPort Signal Descriptions

Signal	Pin #	Description	I/O	PU/PD	Comment
eDP_TX3+ eDP_TX3- eDP_TX2+ eDP_TX2- eDP_TX1+ eDP_TX1- eDP_TX0+ eDP_TX0-	A81 A82 A71 A72 A73 A74 A75 A76	eDP differential pairs.	AC coupled off module.		
eDP_VDD_EN	A77	eDP power enable.	O 3.3V	PD 10k	
eDP_BKLT_EN	B79	eDP backlight enable.	O 3.3V	PD 10k	
eDP_BKLT_CTRL	B83	eDP backlight brightness control.	O 3.3V		
eDP_AUX+	A83	eDP AUX+.	AC coupled off module.		
eDP_AUX-	A84	eDP AUX-.	AC coupled off module.		
eDP_HPD	A87	Detection of Hot Plug / Unplug and notification of the link layer.	I 3.3V		

Table 14 SPI BIOS Flash Interface Signal Descriptions

Signal	Pin #	Description	I/O	PU/PD	Comment
SPI_CS#	B97	Chip select for Carrier Board SPI BIOS Flash.	O 3.3VSB		Carrier shall pull to SPI_POWER when external SPI is provided but not used.
SPI_MISO	A92	Data in to module from carrier board SPI BIOS flash.	I 3.3VSB		
SPI_MOSI	A95	Data out from module to carrier board SPI BIOS flash.	O 3.3VSB		
SPI_CLK	A94	Clock from module to carrier board SPI BIOS flash.	O 3.3VSB		
SPI_POWER	A91	Power source for carrier board SPI BIOS flash. SPI_POWER shall be used to power SPI BIOS flash on the carrier only.	+ 3.3VSB		

Signal	Pin #	Description	I/O	PU/PD	Comment
BIOS_DIS0#	A34	Selection strap to determine the BIOS boot device.	I 3.3VSB	PU 10K 3.3VSB	Carrier shall be left as no-connect.
BIOS_DIS1#	B88	Selection strap to determine the BIOS boot device.	I 3.3VSB	PU 10K 3.3VSB	Carrier shall be left as no-connect

Table 15 Miscellaneous Signal Descriptions

Signal	Pin #	Description	I/O	PU/PD	Comment
I2C_CK	B33	General purpose I²C port clock output/input	I/O 3.3V	PU 2K2 3.3VSB	
I2C_DAT	B34	General purpose I²C port data I/O line	I/O 3.3V	PU 2K2 3.3VSB	
SPKR	B32	Output for audio enunciator, the "speaker" in PC-AT systems	O 3.3V		SPEAKER is a boot strap signal (see note below)
WDT	B27	Output indicating that a watchdog time-out event has occurred.	O 3.3V	PD 10K	
FAN_PWMOUT	B101	Fan speed control. Uses the Pulse Width Modulation (PWM) technique to control the fan's RPM.	O OD 3.3V		
FAN_TACHIN	B102	Fan tachometer input.	I OD	PU 10K 3.3V	Requires a fan with a two pulse output.
TPM_PP	A96	Physical Presence pin of Trusted Platform Module (TPM). Active high. TPM chip has an internal pull-down. This signal is used to indicate Physical Presence to the TPM.	I 3.3V		Trusted Platform Module chip is optional.

Note

Some signals have special functionality during the reset process. They may bootstrap some basic important functions of the module. For more information refer to section 8.5 of this user's guide.

Table 16 General Purpose I/O Signal Descriptions

Signal	Pin #	Description	I/O	PU/PD	Comment
GPO0	A93	General purpose output pins. Shared with SD_CLK. Output from COM Express, input to SD	O 3.3V		
GPO1	B54	General purpose output pins. Shared with SD_CMD. Output from COM Express, input to SD	O 3.3V		
GPO2	B57	General purpose output pins. Shared with SD_WP. Output from COM Express, input to SD	O 3.3V		
GPO3	B63	General purpose output pins. Shared with SD_CD. Output from COM Express, input to SD	O 3.3V		
GPI0	A54	General purpose input pins. Pulled high internally on the module. Shared with SD_DATA0. Bidirectional signal	I 3.3V	PU 10K 3.3V	
GPI1	A63	General purpose input pins. Pulled high internally on the module. Shared with SD_DATA1. Bidirectional signal	I 3.3V	PU 10K 3.3V	
GPI2	A67	General purpose input pins. Pulled high internally on the module. Shared with SD_DATA2. Bidirectional signal	I 3.3V	PU 10K 3.3V	
GPI3	A85	General purpose input pins. Pulled high internally on the module. Shared with SD_DATA3. Bidirectional signal.	I 3.3V	PU 10K 3.3V	

Note

The conga-TC170 provides GPIO signals on the COM Express connector by default.

Table 17 Power and System Management Signal Descriptions

Signal	Pin #	Description	I/O	PU/PD	Comment
PWRBTN#	B12	Power button to bring system out of S5 (soft off), active on falling edge.	I 3.3VSB	PU 10k 3.3VSB	
SYS_RESET#	B49	Reset button input. Active low input. Edge triggered. System will not be held in hardware reset while this input is kept low.	I 3.3VSB	PU 10k 3.3VSB	
CB_RESET#	B50	Reset output from module to Carrier Board. Active low. Issued by module chipset and may result from a low SYS_RESET# input, a low PWR_OK input, a VCC_12V power input that falls below the minimum specification, a watchdog timeout, or may be initiated by the module software.	O 3.3V	PD 100k	
PWR_OK	B24	Power OK from main power supply. A high value indicates that the power is good.	I 3.3V		Set by resistor divider to accept 3.3V.
SUS_STAT#	B18	Indicates imminent suspend operation; used to notify LPC devices.	O 3.3VSB	PU 10k 3.3VSB	
SUS_S3#	A15	Indicates system is in Suspend to RAM state. Active-low output. An inverted copy of SUS_S3# on the carrier board (also known as "PS_ON") may be used to enable the non-standby power on a typical ATX power supply.	O 3.3VSB		
SUS_S4#	A18	Indicates system is in Suspend to Disk state. Active low output.	O 3.3VSB		Not supported
SUS_S5#	A24	Indicates system is in Soft Off state.	O 3.3VSB		
WAKE0#	B66	PCI Express wake up signal.	I 3.3VSB	PU 1k 3.3VSB	
WAKE1#	B67	General purpose wake up signal. May be used to implement wake-up on PS/2 keyboard or mouse activity.	I 3.3VSB	PU 10k 3.3VSB	
BATLOW#	A27	Battery low input. This signal may be driven low by external circuitry to signal that the system battery is low, or may be used to signal some other external power-management event.	I 3.3VSB	PU 10k 3.3VSB	
THRM#	B35	Input from off-module temp sensor indicating an over-temp situation.	I 3.3V	PU 10k 3.3V	
THERMTRIP#	A35	Active low output indicating that the CPU has entered thermal shutdown.	O 3.3V	PU 10k 3.3V	
SMB_CK	B13	System Management Bus bidirectional clock line.	I/O 3.3VSB	PU 2k2 3.3VSB	
SMB_DAT#	B14	System Management Bus bidirectional data line.	I/O OD 3.3VSB	PU 2k2 3.3VSB	
SMB_ALERT#	B15	System Management Bus Alert – active low input can be used to generate an SMI# (System Management Interrupt) or to wake the system.	I 3.3VSB	PU 2k2 3.3VSB	
LID#	A103	Lid button. Used by the ACPI operating system for a LID switch.	I OD 3.3V	PU 10k 3.3VSB	
SLEEP	B103	Sleep button. Used by the ACPI operating system to bring the system to sleep state or to wake it up again.	I OD 3.3V	PU 10k 3.3VSB	

Table 18 General Purpose Serial Interface Signal Descriptions

Signal	Pin #	Description	I/O	PU/PD	Comment
SER0_TX	A98	General purpose serial port transmitter	O 3.3V		
SER1_TX	A101	General purpose serial port transmitter	O 3.3V		
SER0_RX	A99	General purpose serial port receiver	I 3.3V	PU 47k 3.3V	
SER1_RX	A102	General purpose serial port receiver	I 3.3V	PU 47k 3.3V	

Table 19 Power and GND Signal Descriptions

Signal	Pin #	Description	I/O	PU/PD	Comment
VCC_12V	A104-A109 B104-B109	Primary power input: +12V nominal. All available VCC_12V pins on the connector(s) shall be used.	P		
VCC_5V_SBY	B84-B87	Standby power input: +5.0V nominal. If VCC5_SBY is used, all available VCC_5V_SBY pins on the connector(s) shall be used. Only used for standby and suspend functions. May be left unconnected if these functions are not used in the system design.	P		
VCC_RTC	A47	Real-time clock circuit-power input. Nominally +3.0V.	P		
GND	A1, A11, A21, A31, A41, A51, A57, A60, A66, A70, A80, A90, A100, A110, B1, B11, B21, B31, B41, B51, B60, B70, B80, B90, B100, B110	Ground - DC power and signal and AC signal return path. All available GND connector pins shall be used and tied to Carrier Board GND plane.	P		

8.2 A-B Connector Pinout

Table 20 Connector A-B Pinout

Pin	Row A	Pin	Row B	Pin	Row A	Pin	Row B
A1	GND (FIXED)	B1	GND (FIXED)	A56	PCIE_TX4-	B56	PCIE_RX4-
A2	GBE0_MDI3-	B2	GBE0_ACT#	A57	GND	B57	GPO2
A3	GBE0_MDI3+	B3	LPC_FRAME#	A58	PCIE_TX3+	B58	PCIE_RX3+
A4	GBE0_LINK100#	B4	LPC_AD0	A59	PCIE_TX3-	B59	PCIE_RX3-
A5	GBE0_LINK1000#	B5	LPC_AD1	A60	GND (FIXED)	B60	GND (FIXED)
A6	GBE0_MDI2-	B6	LPC_AD2	A61	PCIE_TX2+	B61	PCIE_RX2+
A7	GBE0_MDI2+	B7	LPC_AD3	A62	PCIE_TX2-	B62	PCIE_RX2-
A8	GBE0_LINK#	B8	LPC_DRQ0#	A63	GPI1	B63	GPO3
A9	GBE0_MDI1-	B9	LPC_DRQ1#	A64	PCIE_TX1+	B64	PCIE_RX1+
A10	GBE0_MDI1+	B10	LPC_CLK	A65	PCIE_TX1-	B65	PCIE_RX1-
A11	GND (FIXED)	B11	GND (FIXED)	A66	GND	B66	WAKE0#
A12	GBE0_MDI0-	B12	PWRBTN#	A67	GPI2	B67	WAKE1#
A13	GBE0_MDI0+	B13	SMB_CK	A68	PCIE_TX0+	B68	PCIE_RX0+
A14	GBE0_CTREF (*)	B14	SMB_DAT	A69	PCIE_TX0-	B69	PCIE_RX0-
A15	SUS_S3#	B15	SMB_ALERT#	A70	GND (FIXED)	B70	GND (FIXED)
A16	SATA0_TX+	B16	SATA1_TX+	A71	eDP_TX2+/LVDS_A0+	B71	LVDS_B0+
A17	SATA0_TX-	B17	SATA1_TX-	A72	eDP_TX2-/LVDS_A0-	B72	LVDS_B0-
A18	SUS_S4#	B18	SUS_STAT#	A73	eDP_TX1+/LVDS_A1+	B73	LVDS_B1+
A19	SATA0_RX+	B19	SATA1_RX+	A74	eDP_TX1-/LVDS_A1-	B74	LVDS_B1-
A20	SATA0_RX-	B20	SATA1_RX-	A75	eDP_TX0+/LVDS_A2+	B75	LVDS_B2+
A21	GND (FIXED)	B21	GND (FIXED)	A76	eDP_TX0-/LVDS_A2-	B76	LVDS_B2-
A22	SATA2_TX+	B22	SATA3_TX+ (*)	A77	eDP/LVDS_VDD_EN	B77	LVDS_B3+
A23	SATA2_TX-	B23	SATA3_TX- (*)	A78	LVDS_A3+	B78	LVDS_B3-
A24	SUS_S5#	B24	PWR_OK	A79	LVDS_A3-	B79	eDP/LVDS_BKLT_EN
A25	SATA2_RX+	B25	SATA3_RX+ (*)	A80	GND (FIXED)	B80	GND (FIXED)
A26	SATA2_RX-	B26	SATA3_RX- (*)	A81	eDP_TX3+/LVDS_A_CK+	B81	LVDS_B_CK+
A27	BATLOW#	B27	WDT	A82	eDP_TX3-/LVDS_A_CK-	B82	LVDS_B_CK-
A28	(S)ATA_ACT#	B28	AC/HDA_SDIN2 (*)	A83	eDP_AUX+/LVDS_I2C_CK	B83	eDP/LVDS_BKLT_CTRL
A29	AC/HDA_SYNC	B29	AC/HDA_SDIN1	A84	eDP_AUX-/LVDS_I2C_DAT	B84	VCC_5V_SBY
A30	AC/HDA_RST#	B30	AC/HDA_SDIN0	A85	GPI3	B85	VCC_5V_SBY
A31	GND (FIXED)	B31	GND (FIXED)	A86	RSVD	B86	VCC_5V_SBY
A32	AC/HDA_BITCLK	B32	SPKR	A87	eDP_HPD	B87	VCC_5V_SBY
A33	AC/HDA_SDOUT	B33	I2C_CK	A88	PCIE0_CK_REF+	B88	BIOS_DIS1#
A34	BIOS_DIS0#	B34	I2C_DAT	A89	PCIE0_CK_REF-	B89	VGA_RED
A35	THRMTRIP#	B35	THRM#	A90	GND (FIXED)	B90	GND (FIXED)
A36	USB6-	B36	USB7-	A91	SPI_POWER	B91	VGA_GRN (*)

Pin	Row A	Pin	Row B	Pin	Row A	Pin	Row B
A37	USB6+	B37	USB7+	A92	SPI_MISO	B92	VGA_BLU
A38	USB_6_7_OC#	B38	USB_4_5_OC#	A93	GPO0	B93	VGA_HSYNC
A39	USB4-	B39	USB5-	A94	SPI_CLK	B94	VGA_VSYNC
A40	USB4+	B40	USB5+	A95	SPI_MOSI	B95	VGA_I2C_CK
A41	GND (FIXED)	B41	GND (FIXED)	A96	TPM_PP	B96	VGA_I2C_DAT
A42	USB2-	B42	USB3-	A97	TYPE10# (*)	B97	SPI_CS#
A43	USB2+	B43	USB3+	A98	SER0_TX	B98	RSVD
A44	USB_2_3_OC#	B44	USB_0_1_OC#	A99	SER0_RX	B99	RSVD
A45	USB0-	B45	USB1-	A100	GND (FIXED)	B100	GND (FIXED)
A46	USB0+	B46	USB1+	A101	SER1_TX	B101	FAN_PWMOUT
A47	VCC_RTC	B47	EXCD1_PERST#	A102	SER1_RX	B102	FAN_TACHIN
A48	EXCD0_PERST#	B48	EXCD1_CPPE#	A103	LID#	B103	SLEEP#
A49	EXCD0_CPPE#	B49	SYS_RESET#	A104	VCC_12V	B104	VCC_12V
A50	LPC_SERIRQ	B50	CB_RESET#	A105	VCC_12V	B105	VCC_12V
A51	GND (FIXED)	B51	GND (FIXED)	A106	VCC_12V	B106	VCC_12V
A52	PCIE_TX5+	B52	PCIE_RX5+	A107	VCC_12V	B107	VCC_12V
A53	PCIE_TX5-	B53	PCIE_RX5-	A108	VCC_12V	B108	VCC_12V
A54	GPI0	B54	GPO1	A109	VCC_12V	B109	VCC_12V
A55	PCIE_TX4+	B55	PCIE_RX4+	A110	GND (FIXED)	B110	GND (FIXED)

Note

The signals marked with asterisk symbol (*) are not connected on the conga TC170.

8.3 C-D Connector Signal Descriptions

Table 21 PCI Express Signal Descriptions (general purpose)

Signal	Pin #	Description	I/O	PU/PD	Comment
PCIE_RX6+ PCIE_RX6-	C19 C20	PCI Express channel 6, Receive Input differential pair.	I PCIE		
PCIE_TX6+ PCIE_TX6-	D19 D20	PCI Express channel 6, Transmit Output differential pair.	O PCIE		
PCIE_RX7+ PCIE_RX7-	C22 C23	PCI Express channel 7, Receive Input differential pair.	I PCIE		
PCIE_TX7+ PCIE_TX7-	D22 D23	PCI Express channel 7, Transmit Output differential pair.	O PCIE		

Table 22 USB 3.0 Signal Descriptions

Signal	Pin #	Description	I/O	PU/PD	Comment
USB_SSRX0+	C4	Additional receive signal differential pairs for the Superspeed USB data path	I		
USB_SSRX0-	C3		I		
USB_SSTX0+	D4	Additional transmit signal differential pairs for the Superspeed USB data path	O		
USB_SSTX0-	D3		O		
USB_SSRX1+	C7	Additional receive signal differential pairs for the Superspeed USB data path	I		
USB_SSRX1-	C6		I		
USB_SSTX1+	D7	Additional transmit signal differential pairs for the Superspeed USB data path	O		
USB_SSTX1-	D6		O		
USB_SSRX2+	C10	Additional receive signal differential pairs for the Superspeed USB data path	I		
USB_SSRX2-	C9		I		
USB_SSTX2+	D10	Additional transmit signal differential pairs for the Superspeed USB data path	O		
USB_SSTX2-	D9		O		
USB_SSRX3+	C13	Additional receive signal differential pairs for the Superspeed USB data path	I		
USB_SSRX3-	C12		I		
USB_SSTX3+	D13	Additional transmit signal differential pairs for the Superspeed USB data path	O		
USB_SSTX3-	D12		O		

Table 23 PCI Express Signal Descriptions (x16 Graphics)

Signal	Pin #	Description	I/O	PU/PD	Comment
PEG_RX0+	C52	PCI Express Graphics Receive Input differential pairs. *Note: Can also be used as PCI Express Receive Input differential pairs 16 through 31 known as PCIE_RX[16-31] + and -.*	I PCIE		Optional x1 or x2 PEG port (requires re-routing of PCIe lanes 5 and/or 6)
PEG_RX0-	C53				
PEG_RX1+	C55				
PEG_RX1-	C56				
PEG_RX2+	C58				
PEG_RX2-	C59				
PEG_RX3+	C61				
PEG_RX3-	C62				
PEG_RX4+	C65				
PEG_RX4-	C66				
PEG_RX5+	C68				
PEG_RX5-	C69				
PEG_RX6+	C71				
PEG_RX6-	C72				
PEG_RX7+	C74				
PEG_RX7-	C75				
PEG_RX8+	C78				
PEG_RX8-	C79				
PEG_RX9+	C81				
PEG_RX9-	C82				
PEG_RX10+	C85				
PEG_RX10-	C86				
PEG_RX11+	C88				
PEG_RX11-	C89				
PEG_RX12+	C91				
PEG_RX12-	C92				
PEG_RX13+	C94				
PEG_RX13-	C95				
PEG_RX14+	C98				
PEG_RX14-	C99				
PEG_RX15+	C101				
PEG_RX15-	C102				

Signal	Pin #	Description	I/O	PU/PD	Comment
PEG_TX0+ PEG_TX0- PEG_TX1+ PEG_TX1- PEG_TX2+ PEG_TX2- PEG_TX3+ PEG_TX3- PEG_TX4+ PEG_TX4- PEG_TX5+ PEG_TX5- PEG_TX6+ PEG_TX6- PEG_TX7+ PEG_TX7- PEG_TX8+ PEG_TX8- PEG_TX9+ PEG_TX9- PEG_TX10+ PEG_TX10- PEG_TX11+ PEG_TX11- PEG_TX12+ PEG_TX12- PEG_TX13+ PEG_TX13- PEG_TX14+ PEG_TX14- PEG_TX15+ PEG_TX15-	D52 D53 D55 D56 D58 D59 D61 D62 D65 D66 D68 D69 D71 D72 D74 D75 D78 D79 D81 D82 D85 D86 D88 D89 D91 D92 D94 D95 D98 D99 D101 D102	PCI Express Graphics Transmit Output differential pairs. *Note: Can also be used as PCI Express Transmit Output differential pairs 16 through 31 known as PCIE_TX[16-31] + and -.*	O PCIE		Optional x1 or x2 PEG port (requires re-routing of PCIe lanes 5 and/or 6)
PEG_LANE_RV#	D54	PCI Express Graphics lane reversal input strap. Pull low on the carrier board to reverse lane order.	I	PU 10k 3.3V	Not supported.

Note

The conga-TC170 offers optional x1/x2 PEG port via PCIe lanes 5 or/and 6. The x1/x2 PEG port is not available by default. To support this feature, you need a customized conga-TC170 variant (assembly option) .

Table 24 DDI Signal Description

Signal	Pin #	Description	I/O	PU/PD	Comment
DDI1_PAIR0+ DDI1_PAIR0-	D26 D27	Multiplexed with DP1_LANE0+ and TMDS1_DATA2+. Multiplexed with DP1_LANE0- and TMDS1_DATA2-.	O PCIE		
DDI1_PAIR1+ DDI1_PAIR1-	D29 D30	Multiplexed with DP1_LANE1+ and TMDS1_DATA1+. Multiplexed with DP1_LANE1- and TMDS1_DATA1-.	O PCIE		
DDI1_PAIR2+ DDI1_PAIR2-	D32 D33	Multiplexed with DP1_LANE2+ and TMDS1_DATA0+. Multiplexed with DP1_LANE2- and TMDS1_DATA0-.	O PCIE		
DDI1_PAIR3+ DDI1_PAIR3-	D36 D37	Multiplexed with DP1_LANE3+ and TMDS1_CLK+. Multiplexed with DP1_LANE3- and TMDS1_CLK-.	O PCIE		
DDI1_PAIR4+ DDI1_PAIR4-	C25 C26	Multiplexed with SDVO1_INT+. Multiplexed with SDVO1_INT-.			Not supported
DDI1_PAIR5+ DDI1_PAIR5-	C29 C30	Multiplexed with SDVO1_TVCLKIN+. Multiplexed with SDVO1_TVCLKIN-.			Not supported
DDI1_PAIR6+ DDI1_PAIR6-	C15 C16	Multiplexed with SDVO1_FLDSTALL+. Multiplexed with SDVO1_FLDSTALL-.			Not supported
DDI1_HPD	C24	Multiplexed with DP1_HPD and HDMI1_HPD.	I 3.3V	PD 1M	
DDI1_CTRLCLK_AUX+	D15	Multiplexed with DP1_AUX+ and HMDI1_CTRLCLK. DP AUX+ function if DDI1_DDC_AUX_SEL is no connect. HDMI/DVI I2C CTRLCLK if DDI1_DDC_AUX_SEL is pulled high	 I/O PCIE I/O OD 3.3V	PD100k	
DDI1_CTRLDATA_AUX-	D16	Multiplexed with DP1_AUX- and HDMI1_CTRLDATA. DP AUX- function if DDI1_DDC_AUX_SEL is no connect. HDMI/DVI I2C CTRLDATA if DDI1_DDC_AUX_SEL is pulled high	 I/O PCIE I/O OD 3.3V	PU 100k 3.3V	DDI1_CTRLDATA_AUX- is a boot strap signal (see note below). DDI enable strap already populated.
DDI1_DDC_AUX_SEL	D34	Selects the function of DDI1_CTRLCLK_AUX+ and DDI1_CTRLDATA_AUX-. This pin shall have a IM pull-down to logic ground on the module. If this input is floating, the AUX pair is used for the DP AUX+/- signals. If pulled-high, the AUX pair contains the CTRLCLK and CTRLDATA signals.	I 3.3V	PD 1M	
DDI2_PAIR0+ DDI2_PAIR0-	D39 D40	Multiplexed with DP2_LANE0+ and TMDS2_DATA2+. Multiplexed with DP2_LANE0- and TMDS2_DATA2-.	O PCIE		
DDI2_PAIR1+ DDI2_PAIR1-	D42 D43	Multiplexed with DP2_LANE1+ and TMDS2_DATA1+. Multiplexed with DP2_LANE1- and TMDS2_DATA1-.	O PCIE		
DDI2_PAIR2+ DDI2_PAIR2-	D46 D47	Multiplexed with DP2_LANE2+ and TMDS2_DATA0+. Multiplexed with DP2_LANE2- and TMDS2_DATA0-.	O PCIE		
DDI2_PAIR3+ DDI2_PAIR3-	D49 D50	Multiplexed with DP2_LANE3+ and TMDS2_CLK+. Multiplexed with DP2_LANE3- and TMDS2_CLK-.	O PCIE		
DDI2_HPD	D44	Multiplexed with DP2_HPD and HDMI2_HPD.	I 3.3V	PD 1M	
DDI2_CTRLCLK_AUX+	C32	Multiplexed with DP2_AUX+ and HDMI2_CTRLCLK. DP AUX+ function if DDI2_DDC_AUX_SEL is no connect. HDMI/DVI I2C CTRLCLK if DDI2_DDC_AUX_SEL is pulled high	 I/O PCIE I/O OD 3.3V	PD 100k	
DDI2_CTRLDATA_AUX-	C33	Multiplexed with DP2_AUX- and HDMI2_CTRLDATA. DP AUX- function if DDI2_DDC_AUX_SEL is no connect. HDMI/DVI I2C CTRLDATA if DDI2_DDC_AUX_SEL is pulled high.	 I/O PCIE I/O OD 3.3V	PU 100k 3.3V	DDI2_CTRLCLK_AUX- is a boot strap signal (see note below). DDI enable strap already populated.

Signal	Pin #	Description	I/O	PU/PD	Comment
DDI2_DDC_AUX_SEL	C34	Selects the function of DDI2_CTRLCLK_AUX+ and DDI2_CTRLDATA_AUX-. This pin shall have a IM pull-down to logic ground on the module. If this input is floating, the AUX pair is used for the DP AUX+/- signals. If pulled-high, the AUX pair contains the CTRLCLK and CTRLDATA signals	I 3.3V		
DDI3_PAIR0+ DDI3_PAIR0-	C39 C40	Multiplexed with DP3_LANE0+ and TMDS3_DATA2+. Multiplexed with DP3_LANE0- and TMDS3_DATA2-.	O PCIE		Not supported
DDI3_PAIR1+ DDI3_PAIR1-	C42 C43	Multiplexed with DP3_LANE1+ and TMDS3_DATA1+. Multiplexed with DP3_LANE1- and TMDS3_DATA1-.	O PCIE		Not supported
DDI3_PAIR2+ DDI3_PAIR2-	C46 C47	Multiplexed with DP3_LANE2+ and TMDS3_DATA0+. Multiplexed with DP3_LANE2- and TMDS3_DATA0-.	O PCIE		Not supported
DDI3_PAIR3+ DDI3_PAIR3-	C49 C50	Multiplexed with DP3_LANE3+ and TMDS3_CLK+. Multiplexed with DP3_LANE3- and TMDS3_CLK-.	O PCIE		Not supported
DDI3_HPD	C44	Multiplexed with DP3_HPD and HDMI3_HPD.	I 3.3V		Not supported
DDI3_CTRLCLK_AUX+	C36	Multiplexed with DP3_AUX+ and HDMI3_CTRLCLK. DP AUX+ function if DDI3_DDC_AUX_SEL is no connect. HDMI/DVI I2C CTRLCLK if DDI3_DDC_AUX_SEL is pulled high	 I/O PCIE I/O OD 3.3V		Not supported
DDI3_CTRLDATA_AUX-	C37	Multiplexed with DP3_AUX- and HDMI3_CTRLDATA. DP AUX- function if DDI3_DDC_AUX_SEL is no connect. HDMI/DVI I2C CTRLDATA if DDI3_DDC_AUX_SEL is pulled high.	 I/O PCIE I/O OD 3.3V		Not supported
DDI3_DDC_AUX_SEL	C38	Selects the function of DDI3_CTRLCLK_AUX+ and DDI3_CTRLDATA_AUX-. This pin shall have a IM pull-down to logic ground on the module. If this input is floating, the AUX pair is used for the DP AUX+/- signals. If pulled-high, the AUX pair contains the CTRLCLK and CTRLDATA signals	I 3.3V		Not supported

Note

Some signals have special functionality during the reset process. They may bootstrap some basic important functions of the module. For more information refer to section 8.5 of this user's guide.

The Digital Display Interface (DDI) signals are multiplexed with HDMI and DisplayPort (DP). The signals for these interfaces are routed to the DDI interface of the COM Express connector. Refer to the HDMI and DisplayPort signal description tables in this section for information about the signals routed to the DDI interface of the COM Express connector.

Table 25 HDMI Signal Descriptions

Signal	Pin #	Description	I/O	PU/PD	Comment
TMDS1_CLK + TMDS1_CLK -	D36 D37	HDMI/DVI TMDS Clock output differential pair. Multiplexed with DDI1_PAIR3+ and DDI1_PAIR3-.	O PCIE		
TMDS1_DATA0+ TMDS1_DATA0-	D32 D33	HDMI/DVI TMDS differential pair. Multiplexed with DDI1_PAIR2+ and DDI1_PAIR2-.	O PCIE		
TMDS1_DATA1+ TMDS1_DATA1-	D29 D30	HDMI/DVI TMDS differential pair. Multiplexed with DDI1_PAIR1+ and DDI1_PAIR1-..	O PCIE		
TMDS1_DATA2+ TMDS1_DATA2-	D26 D27	HDMI/DVI TMDS differential pair. Multiplexed with DDI1_PAIR0+ and DDI1_PAIR0-.	O PCIE		
HDMI1_HPD	C24	HDMI/DVI Hot-plug detect. Multiplexed with DDI1_HPD.	I PCIE	PD 1M	
HDMI1_CTRLCLK	D15	HDMI/DVI I²C Control Clock Multiplexed with DDI1_CTRLCLK_AUX+	I/O OD 3.3V	PD 100k	
HDMI1_CTRLDATA	D16	HDMI/DVI I²C Control Data Multiplexed with DDI1_CTRLDATA_AUX-	I/O OD 3.3V	PU 100k 3.3V	HDMI1_CTRLDATA is a boot strap signal (see note below). HDMI enable strap already populated
TMDS2_CLK + TMDS2_CLK -	D49 D50	HDMI/DVI TMDS Clock output differential pair.. Multiplexed with DDI2_PAIR3+ and DDI2_PAIR3-.	O PCIE		
TMDS2_DATA0+ TMDS2_DATA0-	D46 D47	HDMI/DVI TMDS differential pair. Multiplexed with DDI2_PAIR2+ and DDI2_PAIR2-.	O PCIE		
TMDS2_DATA1+ TMDS2_DATA1-	D42 D43	HDMI/DVI TMDS differential pair. Multiplexed with DDI2_PAIR1+ and DDI2_PAIR1-.	O PCIE		
TMDS2_DATA2+ TMDS2_DATA2-	D39 D40	HDMI/DVI TMDS differential pair. Multiplexed with DDI2_PAIR0+ and DDI2_PAIR0-..	O PCIE		
HDMI2_HPD	D44	HDMI/DVI Hot-plug detect. Multiplexed with DDI2_HPD	I PCIE	PD 1M	
HDMI2_CTRLCLK	C32	HDMI/DVI I²C Control Clock Multiplexed with DDI2_CTRLCLK_AUX+	I/O OD 3.3V	PD 100k	
HDM12_CTRLDATA	C33	HDMI/DVI I²C Control Data Multiplexed with DDI2_CTRLDATA_AUX-	I/O OD 3.3V	PU 100k 3.3V	HDMI2_CTRLDATA is a boot strap signal (see note below). HDMI enable strap is already populated.
TMDS3_CLK + TMDS3_CLK -	C49 C50	HDMI/DVI TMDS Clock output differential pair.. Multiplexed with DDI3_PAIR3+ and DDI3_PAIR3-.	O PCIE		Not supported
TMDS3_DATA0+ TMDS3_DATA0-	C46 C47	HDMI/DVI TMDS differential pair. Multiplexed with DDI3_PAIR2+ and DDI3_PAIR2-.	O PCIE		Not supported
TMDS3_DATA1+ TMDS3_DATA1-	C42 C43	HDMI/DVI TMDS differential pair. Multiplexed with DDI3_PAIR1+ and DDI3_PAIR1-..	O PCIE		Not supported
TMDS3_DATA2+ TMDS3_DATA2-	C39 C40	HDMI/DVI TMDS differential pair. Multiplexed with DDI3_PAIR0+ and DDI3_PAIR0-.	O PCIE		Not supported
HDMI3_HPD	C44	HDMI/DVI Hot-plug detect. Multiplexed with DDI3_HPD.	I PCIE		Not supported
HDMI3_CTRLCLK	C36	HDMI/DVI I²C Control Clock Multiplexed with DDI3_CTRLCLK_AUX+	I/O OD 3.3V		Not supported

Signal	Pin #	Description	I/O	PU/PD	Comment
HDMI3_CTRLDATA	C37	HDMI/DVI I²C Control Data Multiplexed with DDI3_CTRLDATA_AUX-	I/O OD 3.3V		Not supported

Note

Some signals have special functionality during the reset process. They may bootstrap some basic important functions of the module. For more information refer to section 8.5 of this user's guide.

Table 26 DisplayPort (DP) Signal Descriptions

Signal	Pin #	Description	I/O	PU/PD	Comment
DP1_LANE3+ DP1_LANE3-	D36 D37	Uni-directional main link for the transport of isochronous streams and secondary data. Multiplexed with DDI1_PAIR3+ and DDI1_PAIR3-.	O PCIE		
DP1_LANE2+ DP1_LANE2-	D32 D33	Uni-directional main link for the transport of isochronous streams and secondary data. Multiplexed with DDI1_PAIR2+ and DDI1_PAIR2-.	O PCIE		
DP1_LANE1+ DP1_LANE1-	D29 D30	Uni-directional main link for the transport of isochronous streams and secondary data. Multiplexed with DDI1_PAIR1+ and DDI1_PAIR1-.	O PCIE		
DP1_LANE0+ DP1_LANE0-	D26 D27	Uni-directional main link for the transport of isochronous streams and secondary data. Multiplexed with DDI1_PAIR0+ and DDI1_PAIR0-.	O PCIE		
DP1_HPD	C24	Detection of Hot Plug / Unplug and notification of the link layer. Multiplexed with DDI1_HPD.	I 3.3V	PD 1M	
DP1_AUX+	D15	Half-duplex bi-directional AUX channel for services such as link configuration or maintenance and EDID access.	I/O PCIE	PD 100k	
DP1_AUX-	D16	Half-duplex bi-directional AUX channel for services such as link configuration or maintenance and EDID access.	I/O PCIE	PU 100k 3.3V	DP1_AUX- is a boot strap signal (see note below). DP enable strap is already populated.
DP2_LANE3+ DP2_LANE3-	D49 D50	Uni-directional main link for the transport of isochronous streams and secondary data. Multiplexed with DDI2_PAIR3+ and DDI2_PAIR3-	O PCIE		
DP2_LANE2+ DP2_LANE2-	D46 D47	Uni-directional main link for the transport of isochronous streams and secondary data. Multiplexed with DDI2_PAIR2+ and DDI2_PAIR2-	O PCIE		
DP2_LANE1+ DP2_LANE1-	D42 D43	Uni-directional main link for the transport of isochronous streams and secondary data. Multiplexed with DDI2_PAIR1+ and DDI2_PAIR1-	O PCIE		
DP2_LANE0+ DP2_LANE0-	D39 D40	Uni-directional main link for the transport of isochronous streams and secondary data. Multiplexed with DDI2_PAIR0+ and DDI1_PAIR0-	O PCIE		

Signal	Pin #	Description	I/O	PU/PD	Comment
DP2_HPD	D44	Detection of Hot Plug / Unplug and notification of the link layer. Multiplexed with DDI2_HPD.	I 3.3V	PD 1M	
DP2_AUX+	C32	Half-duplex bi-directional AUX channel for services such as link configuration or maintenance and EDID access.	I/O PCIE	PD 100k	
DP2_AUX-	C33	Half-duplex bi-directional AUX channel for services such as link configuration or maintenance and EDID access.	I/O PCIE	PU 100k 3.3V	DP2_AUX- is a boot strap signal (see note below). DP enable strap already populated.
DP3_LANE3+ DP3_LANE3-	C49 C50	Uni-directional main link for the transport of isochronous streams and secondary data. Multiplexed with DDI3_PAIR3+ and DDI3_PAIR3-.	O PCIE		Not supported
DP3_LANE2+ DP3_LANE2-	C46 C47	Uni-directional main link for the transport of isochronous streams and secondary data. Multiplexed with DDI3_PAIR2+ and DDI3_PAIR2-.	O PCIE		Not supported
DP3_LANE1+ DP3_LANE1-	C42 C43	Uni-directional main link for the transport of isochronous streams and secondary data. Multiplexed with DDI3_PAIR1+ and DDI3_PAIR1-.	O PCIE		Not supported
DP3_LANE0+ DP3_LANE0-	C39 C40	Uni-directional main link for the transport of isochronous streams and secondary data. Multiplexed with DDI3_PAIR0+ and DDI3_PAIR0-.	O PCIE		Not supported
DP3_HPD	C44	Detection of Hot Plug / Unplug and notification of the link layer. Multiplexed with DDI3_HPD.	I 3.3V		Not supported
DP3_AUX+	C36	Half-duplex bi-directional AUX channel for services such as link configuration or maintenance and EDID access.	I/O PCIE		Not supported
DP3_AUX-	C37	Half-duplex bi-directional AUX channel for services such as link configuration or maintenance and EDID access.	I/O PCIE		Not supported

Note

Some signals have special functionality during the reset process. They may bootstrap some basic important functions of the module. For more information refer to section 8.5 of this user's guide.

Table 27 Module Type Definition Signal Description

Signal	Pin #	Description	I/O	Comment
TYPE0# TYPE1# TYPE2#	C54 C57 D57	The TYPE pins indicate to the Carrier Board the Pin-out Type that is implemented on the module. The pins are tied on the module to either ground (GND) or are no-connects (NC). For Pinout Type 1, these pins are don't care (X). TYPE2# / TYPE1# / TYPE0# / X / X / X / Pinout Type 1 NC / NC / NC / Pinout Type 2 NC / NC / GND / Pinout Type 3 (no IDE) NC / GND / NC / Pinout Type 4 (no PCI) NC / GND / GND / Pinout Type 5 (no IDE, no PCI) GND / NC / NC / Pinout Type 6 (no IDE, no PCI) The Carrier Board should implement combinatorial logic that monitors the module TYPE pins and keeps power off (e.g deactivates the ATX_ON signal for an ATX power supply) if an incompatible module pin-out type is detected. The Carrier Board logic may also implement a fault indicator such as an LED.	PDS	TYPE[0:2]# signals are available on all modules following the Type 2-6 Pinout standard. The conga-TC170 is based on the COM Express Type 6 pinout therefore the pins 0 and 1 are not connected and pin 2 is connected to GND.
TYPE10#	A97	Dual use pin. Indicates to the carrier board that a Type 10 module is installed. Indicates to the carrier that a Rev. 1.0/2.0 module is installed. TYPE10# NC – Pinout R2.0 PD – Pinout Type 10 pull down to ground with 4.7k resistor 12V – Pinout R1.0 This pin is reclaimed from VCC_12V pool. In R1.0 modules this pin will connect to other VCC_12V pins. In R2.0 this pin is defined as a no-connect for Types 1-6. A carrier can detect a R1.0 module by the presence of 12V on this pin. R2.0 module Types 1-6 will no-connect this pin. Type 10 modules shall pull this pin to ground through a 4.7k resistor.	PDS	Not connected to indicate "Pinout R2.0".

Table 28 Power and GND Signal Descriptions

Signal	Pin #	Description	I/O	PU/PD	Comment
VCC_12V	C104-C109 D104-D109	Primary power input: +12V nominal. All available VCC_12V pins on the connector(s) shall be used.	P		
GND	C1, C2, C5, C8, C11, C14, C21, C31, C41, C51, C60, C70,C73, C76, C80, C84, C87, C90, C93, C96, C100, C103, C110, D1, D2, D5, D8, D11, D14, D21, D31, D41, D51, D60, D67, D70, D73, D76, D80, D84, D87, D90, D93, D96, D100, D103, D110	Ground - DC power and signal and AC signal return path. All available GND connector pins shall be used and tied to carrier board GND plane.	P		

8.4 C-D Connector Pinout

Table 29 Connector C-D Pinout

Pin	Row C	Pin	Row D	Pin	Row C	Pin	Row D
C1	GND (FIXED)	D1	GND (FIXED)	C56	PEG_RX1- (*)	D56	PEG_TX1- (*)
C2	GND	D2	GND	C57	TYPE1#	D57	TYPE2#
C3	USB_SSRX0-	D3	USB_SSTX0-	C58	PEG_RX2+ (*)	D58	PEG_TX2+ (*)
C4	USB_SSRX0+	D4	USB_SSTX0+	C59	PEG_RX2- (*)	D59	PEG_TX2- (*)
C5	GND	D5	GND	C60	GND (FIXED)	D60	GND (FIXED)
C6	USB_SSRX1-	D6	USB_SSTX1-	C61	PEG_RX3+ (*)	D61	PEG_TX3+ (*)
C7	USB_SSRX1+	D7	USB_SSTX1+	C62	PEG_RX3- (*)	D62	PEG_TX3- (*)
C8	GND	D8	GND	C63	RSVD	D63	DDPC_CTRLCLK
C9	USB_SSRX2- (*)	D9	USB_SSTX2- (*)	C64	RSVD	D64	DDPC_CTRLDATA
C10	USB_SSRX2+ (*)	D10	USB_SSTX2+ (*)	C65	PEG_RX4+ (*)	D65	PEG_TX4+ (*)
C11	GND (FIXED)	D11	GND (FIXED)	C66	PEG_RX4- (*)	D66	PEG_TX4- (*)
C12	USB_SSRX3- (*)	D12	USB_SSTX3- (*)	C67	RSVD	D67	GND
C13	USB_SSRX3+ (*)	D13	USB_SSTX3+ (*)	C68	PEG_RX5+ (*)	D68	PEG_TX5+ (*)
C14	GND	D14	GND	C69	PEG_RX5- (*)	D69	PEG_TX5- (*)
C15	DDI1_PAIR6+ (*)	D15	DDI1_CTRLCLK_AUX+	C70	GND (FIXED)	D70	GND (FIXED)
C16	DDI1_PAIR6- (*)	D16	DDI1_CTRLDATA_AUX-	C71	PEG_RX6+ (*)	D71	PEG_TX6+ (*)
C17	RSVD	D17	RSVD	C72	PEG_RX6- (*)	D72	PEG_TX6- (*)
C18	RSVD	D18	RSVD	C73	GND	D73	GND
C19	PCIE_RX6+ (*)	D19	PCIE_TX6+ (*)	C74	PEG_RX7+ (*)	D74	PEG_TX7+ (*)
C20	PCIE_RX6- (*)	D20	PCIE_TX6- (*)	C75	PEG_RX7- (*)	D75	PEG_TX7- (*)
C21	GND (FIXED)	D21	GND (FIXED)	C76	GND	D76	GND
C22	PCIE_RX7+ (*)	D22	PCIE_TX7+ (*)	C77	RSVD	D77	RSVD
C23	PCIE_RX7- (*)	D23	PCIE_TX7- (*)	C78	PEG_RX8+ (*)	D78	PEG_TX8+ (*)
C24	DDI1_HPD	D24	RSVD	C79	PEG_RX8- (*)	D79	PEG_TX8- (*)
C25	DDI1_PAIR4+ (*)	D25	RSVD	C80	GND (FIXED)	D80	GND (FIXED)
C26	DDI1_PAIR4- (*)	D26	DDI1_PAIR0+	C81	PEG_RX9+ (*)	D81	PEG_TX9+ (*)
C27	RSVD	D27	DDI1_PAIR0-	C82	PEG_RX9- (*)	D82	PEG_TX9- (*)
C28	RSVD	D28	RSVD	C83	RSVD	D83	RSVD
C29	DDI1_PAIR5+ (*)	D29	DDI1_PAIR1+	C84	GND	D84	GND
C30	DDI1_PAIR5- (*)	D30	DDI1_PAIR1-	C85	PEG_RX10+ (*)	D85	PEG_TX10+ (*)
C31	GND (FIXED)	D31	GND (FIXED)	C86	PEG_RX10- (*)	D86	PEG_TX10- (*)
C32	DDI2_CTRLCLK_AUX+	D32	DDI1_PAIR2+	C87	GND	D87	GND
C33	DDI2_CTRLDATA_AUX-	D33	DDI1_PAIR2-	C88	PEG_RX11+ (*)	D88	PEG_TX11+ (*)
C34	DDI2_DDC_AUX_SEL	D34	DDI1_DDC_AUX_SEL	C89	PEG_RX11- (*)	D89	PEG_TX11- (*)
C35	RSVD	D35	RSVD	C90	GND (FIXED)	D90	GND (FIXED)
C36	DDI3_CTRLCLK_AUX+ (*)	D36	DDI1_PAIR3+	C91	PEG_RX12+ (*)	D91	PEG_TX12+ (*)

Pin	Row C	Pin	Row D	Pin	Row C	Pin	Row D
C37	DDI3_CTRLDATA_AUX- (*)	D37	DDI1_PAIR3-	C92	PEG_RX12- (*)	D92	PEG_TX12- (*)
C38	DDI3_DDC_AUX_SEL (*)	D38	RSVD	C93	GND	D93	GND
C39	DDI3_PAIR0+ (*)	D39	DDI2_PAIR0+	C94	PEG_RX13+ (*)	D94	PEG_TX13+ (*)
C40	DDI3_PAIR0- (*)	D40	DDI2_PAIR0-	C95	PEG_RX13- (*)	D95	PEG_TX13- (*)
C41	GND (FIXED)	D41	GND (FIXED)	C96	GND	D96	GND
C42	DDI3_PAIR1+ (*)	D42	DDI2_PAIR1+	C97	RVSD	D97	RSVD
C43	DDI3_PAIR1- (*)	D43	DDI2_PAIR1-	C98	PEG_RX14+ (*)	D98	PEG_TX14+ (*)
C44	DDI3_HPD	D44	DDI2_HPD	C99	PEG_RX14- (*)	D99	PEG_TX14- (*)
C45	RSVD	D45	RSVD	C100	GND (FIXED)	D100	GND (FIXED)
C46	DDI3_PAIR2+ (*)	D46	DDI2_PAIR2+	C101	PEG_RX15+ (*)	D101	PEG_TX15+ (*)
C47	DDI3_PAIR2- (*)	D47	DDI2_PAIR2-	C102	PEG_RX15- (*)	D102	PEG_TX15- (*)
C48	RSVD	D48	RSVD	C103	GND	D103	GND
C49	DDI3_PAIR3+ (*)	D49	DDI2_PAIR3+	C104	VCC_12V	D104	VCC_12V
C50	DDI3_PAIR3- (*)	D50	DDI2_PAIR3-	C105	VCC_12V	D105	VCC_12V
C51	GND (FIXED)	D51	GND (FIXED)	C106	VCC_12V	D106	VCC_12V
C52	PEG_RX0+ (*)	D52	PEG_TX0+ (*)	C107	VCC_12V	D107	VCC_12V
C53	PEG_RX0- (*)	D53	PEG_TX0- (*)	C108	VCC_12V	D108	VCC_12V
C54	TYPE0#	D54	PEG_LANE_RV# (*)	C109	VCC_12V	D109	VCC_12V
C55	PEG_RX1+ (*)	D55	PEG_TX1+ (*)	C110	GND (FIXED)	D110	GND (FIXED)

Note

The signals marked with an asterisk symbol (*) are not supported on the conga-TC170.

8.5 Boot Strap Signals

Table 30 Boot Strap Signal Descriptions

Signal	Pin #	Description of Boot Strap Signal	I/O	PU/PD	Comment
AC/HDA_SDOUT	A33	High Definition Audio Serial Data Out: This signal is the serial TDM data output to the codec(s). This serial output is double-pumped for a bit rate of 48 Mb/s for High Definition Audio.	O 3.3VSB	PU 1K 3.3VSB	AC/HDA_SDOUT is a boot strap signal (see caution statement below)
SPKR	B32	Output for audio enunciator, the "speaker" in PC-AT systems	O 3.3V		SPKR is a boot strap signal (see caution statement below)
DDI1_CTRLDATA_AUX- DP1_AUX- HDMI_CTRLDATA	D16	Multiplexed with DP1_AUX- and HDMI1_CTRLDATA. DP AUX- function if DDI1_DDC_AUX_SEL is no connect. HDMI/DVI I2C CTRLDATA if DDI1_DDC_AUX_SEL is pulled high.	 I/O PCIE I/O OD 3.3V	PU100k 3.3V	DDI1_CTRLDATA_AUX- is a boot strap signal (see not below).
DDI2_CTRLDATA_AUX- DP2_AUX- HDM2_CTRLDATA	C33	Multiplexed with DP2_AUX- and HDMI2_CTRLDATA. DP AUX- function if DDI2_DDC_AUX_SEL is no connect. HDMI/DVI I2C CTRLDATA if DDI2_DDC_AUX_SEL is pulled high.	 I/O PCIE I/O OD 3.3V	PU100k 3.3V	DDI2_CTRLDATA_AUX- is a boot strap signal (see not below).

Caution

The signals listed in the table above are used as chipset configuration straps during system reset. In this condition (during reset), they are inputs that are pulled to the correct state by either COM Express™ internally implemented resistors or chipset internally implemented resistors that are located on the module. No external DC loads or external pull-up or pull-down resistors should change the configuration of the signals listed in the above table.

External resistors may override the internal strap states and cause the COM Express™ module to malfunction and/or cause irreparable damage to the module.

9 System Resources

9.1 I/O Address Assignment

The I/O address assignment of the conga-TC170 module is functionally identical with a standard PC/AT.

Note

The BIOS assigns PCI and PCI Express I/O resources from FFF0h downwards. Non PnP/PCI/PCI Express compliant devices must not consume I/O resources in that area.

9.1.1 LPC Bus

On the conga-TC170, the PCI Express Bus acts as the subtractive decoding agent. All I/O cycles that are not positively decoded are forwarded to the PCI Bus not the LPC Bus. Only specified I/O ranges are forwarded to the LPC Bus. In the congatec Embedded BIOS the following I/O address ranges are sent to the LPC Bus:

2Eh – 2Fh

4Eh – 4Fh

60h, 64h

A00h – A1Fh

E00h - EFFh (always used internally)

Parts of these ranges are not available if a Super I/O is used on the carrier board. If a Super I/O is not implemented on the carrier board then these ranges are available for customer use. If you require additional LPC Bus resources other than those mentioned above, or more information about this subject, contact congatec technical support for assistance.

9.2 PCI Configuration Space Map

Table 31 PCI Configuration Space Map

Bus Number (hex)	Device Number (hex)	Function Number (hex)	Description
00h	00h	00h	HOST and DRAM Controller
00h	02h	00h	Integrated Graphics Device
00h	08h	00h	Gaussian Mixture Model Device
00h	14h	00h	USB 3.0 xHCI Controller
00h	14h	02h	Thermal Subsystem
00h (Note1)	16h	00h	Management Engine (ME) Interface 1
00h (Note1)	16h	01h	Intel ME Interface 2
00h (Note1)	16h	02h	ME IDE Redirection (IDE-R) Interface
00h (Note1)	16h	03h	ME Keyboard and Text (KT) Redirection
00h (Note1)	16h	04h	Intel ME Interface 3
00h	17h	00h	SATA Controller
00h (Note2)	1Ch	00h	PCI Express Root Port 0
00h (Note2)	1Ch	01h	PCI Express Root Port 1
00h (Note2)	1Ch	02h	PCI Express Root Port 2
00h (Note2)	1Ch	03h	PCI Express Root Port 3
00h (Note2)	1Ch	04h	PCI Express Root Port 4
00h (Note2)	1Ch	05h	PCI Express Root Port 5
00h (Note2)	1Dh	00h	PCI Express Root Port 6
00h (Note2)	1Dh	02h	PCI Express Root Port 7
00h	1Fh	00h	PCI to LPC Bridge
00h	1Fh	02h	Power Management Controller
00h	1Fh	03h	Intel® High Definition Audio (Intel® HD Audio)
00h	1Fh	04h	SMBus Controller
00h	1Fh	06h	GbE Controller
01h (Note3)	00h	00h	PCI Express Port 0
02h (Note3)	00h	00h	PCI Express Port 1
03h (Note3)	00h	00h	PCI Express Port 2
04h (Note3)	00h	00h	PCI Express Port 3
05h (Note3)	00h	00h	PCI Express Port 4
06h (Note3)	00h	00h	PCI Express Port 5

Bus Number (hex)	Device Number (hex)	Function Number (hex)	Description
07h (Note3)	00h	00h	PCI Express Port 6
08h (Note3)	00h	00h	PCI Express Port 7

Note

1. *In the standard configuration, the Intel Management Engine (ME) related devices are partly present or not present at all.*
2. *The PCI Express Ports are visible only if a device is attached behind them to the PCI Express Slot on the carrier board.*
3. *The table represents a case when a single function PCI/PCIe device is connected to all possible slots on the carrier board. The given bus numbers will change based on actual hardware configuration.*
4. *Internal PCI devices not connected to the conga-TC170 are not listed.*

9.3 I²C

There are no onboard resources connected to the I²C bus. Address 16h is reserved for congatec Battery Management solutions.

9.4 SM Bus

System Management (SM) bus signals are connected to the Intel® QM170 or HM170 PCH. The SM bus is not intended to be used by off-board non-system management devices. For more information about this subject contact congatec technical support.

10 BIOS Setup Description

The following section describes the BIOS setup program. The BIOS setup program can be used to view and change the BIOS settings for the module. Only experienced users should change the default BIOS settings.

10.1 Entering the BIOS Setup Program

The BIOS setup program can be accessed by pressing the <DEL> or <F2> key during POST.

10.1.1 Boot Selection Popup

The BIOS offers the possibility to access a Boot Selection Popup menu by pressing the <F11> key during POST. If this option is used, a selection will be displayed immediately after POST allowing the operator to select either the boot device that should be used or an option to enter the BIOS setup program.

10.2 Setup Menu and Navigation

The congatec BIOS setup screen is composed of the menu bar and two main frames. The menu bar is shown below:

Main	Advanced	Chipset	Security	Boot	Save & Exit

The left frame displays all the options that can be configured in the selected menu. Grayed-out options cannot be configured. Only the blue options can be configured. When an option is selected, it is highlighted in white.

The right frame displays the key legend. Above the key legend is an area reserved for text messages. These text messages explain the options and the possible impacts when changing the selected option in the left frame.

Note

Entries in the option column that are displayed in bold print indicate BIOS default values.

The setup program uses a key-based navigation system. Most of the keys can be used at any time while in setup. The table below explains the supported keys:

Key	Description
← → Left/Right	Select a setup menu (e.g. Main, Boot, Exit).
↑ ↓ Up/Down	Select a setup item or sub menu.
+ - Plus/Minus	Change the field value of a particular setup item.
Tab	Select setup fields (e.g. in date and time).
F1	Display General Help screen.
F2	Load previous settings.
F9	Load optimal default settings.
F10	Save changes and exit setup.
ESC	Discard changes and exit setup.
ENTER	Display options of a particular setup item or enter submenu.

10.3 Main Setup Screen

When you first enter the BIOS setup, you will enter the Main setup screen. You can always return to the Main setup screen by selecting the Main tab. The Main screen reports BIOS, processor, memory and board information and is used to configure the system date and time.

Feature	Options	Description
Main BIOS Version	No option	Displays the main BIOS version.
OEM BIOS Version	No option	Displays the additional OEM BIOS version.
Build Date	No option	Displays the date the BIOS was built.
Product Revision	No option	Displays the hardware revision of the board.
Serial Number	No option	Displays the serial number of the board.
BC Firmware Revision	No option	Displays the congatec board controller firmware revision.
MAC Address (1st Ethernet)	No option	Displays the MAC address of the onboard i218 Ethernet controller.
MAC Address (2nd Ethernet)	No option	Displays the MAC address of the onboard i210/i211 Ethernet controller.
Boot Counter	No option	Displays the number of boot-ups (maximum 16777215).
Running Time	No option	Displays the time the board is running (in hours, maximum 65535).
▶Platform Information	Submenu	Opens the 'Platform Information' submenu.
System Date	Day of week, month/day/year	Displays the current system date. **Note:** The date is in month-day-year format.
System Time	Hour:Minute:Second	Displays the current system time. **Note:** The time is in 24-hour format.

10.3.1 Platform Information Submenu

The platform information submenu offers additional hardware and software information.

Feature	Options	Description
Processor Information	No option	Subtitle.
Processor Type	No option	Displays the processor ID string. The “Processor Type” text is not displayed.
Codename	No option	Displays the processor codename.
Processor Speed	No option	Displays the processor speed.
Processor Signature	No option	Displays the processor signature.
Stepping	No option	Displays the processor stepping.
Processor Cores	No option	Displays the number of processor cores.
Microcode Revision	No option	Displays the processor microcode revision.
IGD HW Version	No option	Displays the version of the graphics controller.
IGD VBIOS Version	No option	Displays the video BIOS version.
Total Memory	No option	Displays the total amount of installed memory.
PCH Information	No option	Subtitle.
Codename	No option	Displays the codename of the Platform Controller Hub (PCH).
PCH SKU	No option	Displays the SKU name of the PCH.
Stepping	No option	Displays the PCH stepping.
ME FW Version	No option	Displays the ME Firmware (FW) Version if available.
ME Firmware SKU	No option	Displays the ME FW SKU if available.

10.4 Advanced Setup

Select the Advanced tab from the setup menu to enter the Advanced BIOS Setup screen. The menu is used for setting advanced features. Only enabled features are displayed.

Main	Advanced	Chipset	Boot	Security	Save & Exit
	Graphics				
	Watchdog				
	Module Serial Ports				
	Hardware Health Monitoring				
	Intel® Ethernet Connection (H) I219-LM				
	Driver Health				
	Trusted Computing				
	RTC Wake Settings				
	ACPI				
	Intel® ICC				
	OverClocking Performance Menu				
	PCH-FW Configuration				
	SMART Settings				
	Super IO				
	Serial Port Console Redirection				
	CPU				
	Platform Misc Configuration				
	SATA Configuration				
	Thermal Configuration				
	Acoustic Management				
	PCI & PCI Express				
	UEFI Network Stack				
	CSM & Option ROM Control				
	NVMe Configuration				
	SDIO Configuration				
	USB				
	PC Speaker				

10.4.1 Graphics Submenu

Feature	Options	Description
Primary Display	**Auto** IGD PEG PCI/PCIe	Select primary graphics adapter to be used during boot up: 'Auto' - Selects it automatically. 'IGD' - Uses the Internal Graphics Device (IGD) located in the chipset. 'PEG' - Uses the external PCI Express Graphics (PEG) card attached to the PEG port. 'PCI/PCIe' - Uses a PCI/PCIe graphics card attached to a PCI/PCIe port.
Internal Graphics Device	**Auto** Disabled Enabled	Set IGD to 'Auto', 'Disabled', or 'Enabled'.
IGD Pre-Allocated Graphics Memory	**32M** 64M 96M 128M 160M 192M 224M 256M 288M 320M 352M 384M 416M 448M 480M 512M 1024M 1536M 2048M	Select amount of pre-allocated graphics memory to be used by the IGD.
IGD Total Graphics Memory	128M **256M** MAX	Select amount of total graphics memory that may be used by the IGD. Memory above the fixed graphics memory is dynamically allocated by the graphics driver. **Note:** Refer to the DVMT 5.0 specification for more detailed information.
Primary IGD Boot Display Device	**Auto** CRT LFP EFP EFP2 EFP3	Select the Primary IGD display device(s) to be used for boot up: 'CRT' - Uses the analog VGA display port. 'LFP' - Uses the LVDS panel connected to the integrated LVDS port. 'EFPx' - Uses the HDMI/DVI or DisplayPort device connected to DDI1, DDI2 and DDI3. **Note:** EFP selections are valid only when at least one DDI is enabled. The first enabled DDI is assigned to EFP. Therefore, EFP and DDI numbering do not necessarily match.

Feature	Options	Description
Secondary IGD Boot Display Device	**Disabled** CRT LFP EFP EFP2 EFP3	Select the Secondary IGD display device(s) used for boot up. **Note:** VGA modes are only supported on the primary display. For further details, see 'Primary IGD Boot Display Device'.
Active LFP Configuration	No Local Flat Panel **Integrated LVDS** eDP	Select active local flat panel configuration.
Always Try Auto Panel Detect	**No** Yes	If set to 'Yes', the BIOS will use the EDID™ data set in an external EEPROM to configure the LFP. In case it cannot be found, the data set selected under 'Local Flat Panel Type' will be used.
Local Flat Panel Type	**Auto** VGA 640x480 1x18 (002h) VGA 640x480 1x18 (013h) WVGA 800x480 1x18 (01Fh) WVGA 800x480 1x24 (01Bh) SVGA 800x600 1x18 (01Ah) XGA 1024x768 1x18 (006h) XGA 1024x768 2x18 (007h) XGA 1024x768 1x24 (008h) XGA 1024x768 2x24 (012h) WXGA 1280x800 1x18 (01Eh) WXGA 1280x768 1x24 (01Ch) SXGA 1280x1024 2x24 (00Ah) SXGA 1280x1024 2x24 (018h) UXGA 1600x1200 2x24 (00Ch) HD 1920x1080 2x24 (01Dh) WUXGA 1920x1200 2x18 (015h) WUXGA 1920x1200 2x24 (00Dh) Customized EDID™ 1 Customized EDID™ 2 Customized EDID™ 3	Select a predefined LFP type or choose 'Auto' to let the BIOS automatically detect and configure the attached LVDS panel. Auto detection is performed by reading an EDID™ data set via the video I²C bus. The number in brackets specifies the congatec internal number of the respective panel data set. **Note:** Customized EDID™ utilizes an OEM defined EDID™ data set stored in the BIOS flash device.
Backlight Inverter Type	None **PWM** I2C	Select the type of backlight inverter: 'PWM' - IGD PWM signal. 'I2C' - I2C backlight inverter device connected to the video I²C bus.
PWM Inverter Polarity	**Normal** Inverted	Set PWM inverter polarity.
PWM Inverter Frequency (Hz)	**200** - 40000	Set the PWM inverter frequency in Hertz.

Feature	Options	Description
Backlight Setting	0% 10% 25% 40% 50% 60% 75% 90% **100%**	Select the backlight value in percentage of the maximum setting.
Force Backlight Enable	**No** Yes	Set to 'Yes', if the operating system driver does not activate the backlight signal.
Inhibit Backlight	**No** Permanent Until End Of POST	Select whether the backlight enable signal should be activated when the panel is activated. **Note:** The signal should be permanently activated or remain inhibited until the end of BIOS POST.
Backlight Delay	**No delay** 100ms Delay 250ms Delay 500ms Delay 1s Delay	Select delay to adjust LVDS panel timings. **Note:** The congatec board controller will add the delay to the backlight signal coming from the SoC according this setup node. This feature may help to avoid panel flickering.
Invert Backlight Setting	**No** Yes	Set 'Yes' to invert backlight control values. **Note:** This feature may be required for the actual I2C type backlight hardware controller.
LVDS SSC	**Disabled** 0.5% 1.0% 1.5% 2.0% 2.5%	Select LVDS spread spectrum clock modulation depth. **Note:** Performs center spreading and DDI1 fixed modulation frequency of 32.9kHz.
Digital Display Interface 1 (DDI1)	**Auto Selection** Disabled DisplayPort HDMI/DVI	Select the output type of the DDI.
Digital Display Interface 2 (DDI2)	**Auto Selection** Disabled DisplayPort HDMI/DVI	Select the output type of the DDI.
Digital Display Interface 3 (DDI3)	**Auto Selection** Disabled DisplayPort HDMI/DVI	Select the output type of DDI3. **Note:** If 'VGA Port' is enabled, 'Auto Selection' and 'DisplayPort' are not supported.
VGA Port	**Disabled** Enabled	Enable or disable VGA port. **Note:** If enabled, the Auto Selection and DisplayPort is not supported on DDI3.

10.4.2 Watchdog Submenu

Feature	Options	Description
POST Watchdog	**Disabled** 30sec 1min 2min 5min 10min 30min	Select the timeout value for the POST watchdog. **Note:** The watchdog is only active during the system POST and provides a facility to prevent errors during boot up by performing a reset.
Stop Watchdog For User Interaction	No **Yes**	Select whether the POST watchdog should be stopped during the popup boot selection menu or while waiting for the setup password.
Runtime Watchdog	**Disabled** One-time Trigger Single Event Repeated Event	Select the operating mode of the runtime watchdog. 'One-time Trigger' - Disables watchdog after first trigger. 'Single Event' - Executes every stage only once before the watchdog is disabled. 'Repeated Event' - Executes last stage repeatedly until reset. **Note:** This watchdog will be initialized just before the operating system starts booting.
Delay	**Disabled** 10sec 30sec 1min 2min 5min 10min 30min	Select the delay time before the runtime watchdog is activated. **Note:** This feature may be used to ensure that the operating system has enough time to load.
Event 1	ACPI Event **Reset** Power Button	Select the type of event that will be generated when timeout 1 is reached. For more information about ACPI Event read the note at the end of this table.
Event 2	**Disabled** ACPI Event Reset Power Button	Select the type of event that will be generated when timeout 2 is reached.
Event 3	**Disabled** ACPI Event Reset Power Button	Select the type of event that will be generated when timeout 3 is reached.

Feature	Options	Description
Timeout 1	1sec 2sec 5sec 10sec **30sec** 1min 2min 5min 10min 30min	Select the timeout value for the first stage watchdog event.
Timeout 2	see above	Select the timeout value for the second stage watchdog event.
Timeout 3	see above	Select the timeout value for the third stage watchdog event.
Watchdog ACPI Event	Shutdown Restart	Select the operating system event to be initiated by the watchdog ACPI event. This feature performs a critical but orderly operating system shutdown or restart.

Note

In ACPI mode, it is not possible for a "Watchdog ACPI Event" handler to directly restart or shutdown the OS. The congatec BIOS will perform one of the following actions instead:

Shutdown: An over temperature notification is executed. This causes the operating system to shut down in an orderly fashion.

Restart: An ACPI fatal error is reported to the OS.

10.4.3 Module Serial Ports Submenu

Feature	Options	Description
Serial Port 0	**Disabled** Enabled	Enable or disable module serial port 0.
I/O Base Address	3F8h 2F8h 220h 228h 238h 2E8h 338h **3E8h**	Set serial port base address.
Interrupt	None IRQ3 IRQ4 **IRQ5** IRQ6 IRQ14 IRQ15	Set serial port interrupt.
PNP ID	None PNP0501 **CGT0501**	Set serial port ACPI ID.
Baudrate	**2400** 4800 9600 19200 38400 57600 115200	Set serial port initial baudrate.
Serial Port 1	**Disabled** Enabled	Enable or disable module serial port 1.
I/O Base Address	3F8h 2F8h 220h 228h 238h **2E8h** 338h 3E8h	Set serial port base address.

Feature	Options	Description
Interrupt	None IRQ3 IRQ4 IRQ5 **IRQ6** IRQ14 IRQ15	Set serial port interrupt.
PNP ID	None PNP0501 CGT0501 **CGT0502**	Set serial port ACPI ID.
Baudrate	**2400** 4800 9600 19200 38400 57600 115200	Set serial port initial baudrate.

10.4.4 Hardware Health Monitoring Submenu

Feature	Options	Description
CPU Temperature	No option	Displays the module CPU temperature in °C.
Board Temperature	No option	Displays the module board temperature in °C.
DC Input Voltage	No option	Displays the actual voltage of the standard DC power supply.
5V Standby	No option	Displays the actual voltage of the 5V standby power rail.
DC Input Current	No option	Displays the module input current from DC standard voltage.
CPU Fan Speed	No option	Displays the CPU Fan Speed in RPM.
Fan PWM Frequency Mode	Low Frequency **High Frequency**	Select the fan PWM base frequency mode: 'Low Frequency' - 11.0 to 88.2Hz. 'High Frequency' - 1k to 63kHz.
Fan PWM Frequency (kHz)	**31** (more values)	Select the fan PWM base frequency.
Fan Speed Setting	0%, 10%, 25%, 40%, 50%, 60%, 75%, 90%, **100%**	Select boot up fan speed in percent of the maximum supported speed.

10.4.5 Intel® Ethernet Connection (H) I219-LM Submenu

Feature	Options	Description
► NIC Configuration	Submenu	Opens the NIC Configuration submenu.
Blink LEDs	0 (more values)	Set the duration in seconds for the Ethernet LEDs to blink.
UEFI Driver	No option	Displays the UEFI Driver version.
Adapter PBA	No option	Displays the Adapter PBA.
Chip Type	No option	Displays the type of the chip in which the Ethernet controller is integrated.
PCI Device ID	No option	Displays the PCI Device ID of the Ethernet controller.
PCI Address	No option	Displays the PCI Bus:Device:Function number of the Ethernet controller.
Link Status	No option	Displays the Link Status.
MAC Address	No option	Displays the MAC Address.

10.4.5.1 NIC Configuration Submenu

Feature	Options	Description
Link Speed	**Auto Negotiated** 10 Mbps Half 10 Mbps Full 100 Mbps Half 100 Mbps Full	Select the port speed used for the selected boot protocol.
Wake On LAN	**N/A** Disabled Enabled	Enable for the server to power on after receiving an in-band magic packet.

10.4.6 Driver Health Submenu

Feature	Options	Description
Intel® Gigabit 0.0.09	**Healthy**	Provides Health Status for the drivers/controllers.

10.4.7 Trusted Computing Submenu

Feature	Options	Description
Security Device Support	Disable **Enable**	Enable or disable BIOS support for security device. Operating system will not show the security device. TCG EFI protocol and INT1A interface will not be available.

Note

Additional features are shown in this submenu if a TPM device is connected.

10.4.8 RTC Wake Settings Submenu

Feature	Options	Description
RTC Wake Mode	**Disabled** Wake from S4 and S5 Wake from S3, S4 and S5	Set system wake mode on alarm event. Enable this feature to wake from the specified Sx states on the hr::min::sec as specified.
Wake up hour	**0**	Specify wake up hour. For example: Enter 3 for 3am and 15 for 3pm.
Wake up minute	**0**	Specify wake up minute.
Wake up second	**0**	Specify wake up second.

10.4.9 ACPI Submenu

Feature	Options	Description
Enable ACPI Auto Configuration	**Disabled** Enabled	Enable or disable BIOS ACPI auto configuration.
Hibernation Support	Disabled **Enabled**	Enable or disable system's ability to hibernate (operating system S4 sleep state). **Note:** Ensure that your operating system supports this feature if you want to use it.
ACPI Sleep State	Suspend Disabled **S3 (Suspend to RAM)**	Select the state used for ACPI system sleep/suspend.
Lock Legacy Resources	**Disabled** Enabled	Enable or disable locking of legacy resources.
S3 Video Repost	**Disabled** Enabled	Enable or disable video BIOS re-post on S3 resume. **Note:** Enable this feature if it is required by your operating system.
ACPI Low Power S0 Idle	**Disabled** Enabled	Enable or disable ACPI low power S0 idle support.

Feature	Options	Description
Active Trip Point	Disabled 15 C 23 C 31 C 39 C 47 C 55 C 63 C **71 C** 79 C 87 C 95 C 103 C 111 C 119 C	Select the temperature threshold at which the ACPI aware operating system turns the fan on or off.
Automatic Critical Trip Point	Disabled **Enabled**	Enable this feature to set the critical trip point (temperature threshold) to the recommended value at which the ACPI aware operating system performs a critical shutdown automatically. Disable this feature to configure the critical trip point manually.
Critical Trip Point Value	71 C 79 C 87 C 95 C **100 C** 103 C 111 C 119 C 127 C	Select the temperature threshold at which the ACPI aware operating system performs a critical shutdown.
Lid Button Support	**Disabled** Enabled	If this feature is enabled, the COM Express LID# signal acts as ACPI lid.
Sleep Button Support	**Disabled** Enabled	If this feature is enabled, the COM Express SLEEP# signal acts as ACPI sleep button.

10.4.10 Intel® ICC Submenu

Feature	Options	Description
ICC/OC Watchdog Timer	**Disabled** Enabled	Enable this feature to expose the ICC/OC watchdog timer to the operating system as an ACPI device. **Note:** WDT HW is always used by BIOS when clock settings are changed.
ICC Locks after EOP	Default	
ICC Profile	0	

10.4.11 OverClocking Performance Submenu

The description of this feature is beyond the scope of this document.

10.4.12 PCH-FW Configuration Submenu

Displayed only if this feature is enabled.

Feature	Options	Description
ME FW Version	No option	Displays ME FW Version.
ME Firmware Mode	No option	Displays ME Firmware Mode.
ME Firmware Type	No option	Displays ME Firmware Type.
ME Firmware SKU	No option	Displays ME Firmware SKU.
PTT Capability / State	No option	Displays PTT Capability / State.
NFC Support	No option	Displays NFC Support.
ME State	Disabled **Enabled**	Enable to set ME to Soft Temporary Disabled.
fTPM Switch Selection	**GPDMA Work-Around** MSFT QFE Solution	Selects the desired fTPM solution to be used.
TPM Device Selection	**dTPM 1.2** PTT	Select TPM device: 'PTT' - Enables PTT and disables dTPM in SkuMgr. 'dTPM 1.2' - Enables dTPM 1.2 and disables PTT in SkuMgr. **Warning:** If you enable PTT, dTPM will be disabled and all data saved on it will be lost. Likewise, if you enable dTPM, PTT will be disabled and all data saved on it will be lost.
▶Firmware Update Configuration	Submenu	Opens submenu to configure management engine technology parameters.
Me FW Image Re-Flash	**Disabled** Enabled	Enable or disable Me FW Image Re-Flash function.

10.4.13 SMART Settings Submenu

Feature	Options	Description
SMART Self Test	**Disabled** Enabled	Run SMART self test on all HDDs during POST.

10.4.14 Super IO Submenu

Feature	Options	Description
Super IO Chip	W83627	
SIO Clock	**24MHz** 48MHz	Select Super IO base clock.
Serial Port	Disabled **Enabled**	Enable or disable serial port (COM).
Device Settings	IO=3F8h IRQ=4	Displays the currently used settings.
Serial Port	Disabled **Enabled**	Enable or disable serial port (COM).
Device Settings	O=2F8h IRQ=3	Displays the currently used settings.
Parallel Port	**Disabled** Enabled	Enable or disable parallel port (LPT/LPTE).
Device Settings	IO=378h IRQ=5	Displays the currently used settings.
Device Mode	**STD Printer Mode** SPP Mode EPP-1.9 and SPP Mode EPP-1.7 and SPP Mode ECP Mode ECP and EPP 1.9 Mode ECP and EPP 1.7 Mode	Select the parallel port mode.

Note

This setup menu is available only if an external Winbond W83627 Super I/O is implemented on the carrier board.

10.4.15 Serial Port Console Redirection Submenu

Feature	Options	Description
COM0 Console Redirection	**Disabled** Enabled	Enable or disable serial port 0 console redirection.
▶Console Redirection Settings	Submenu	Opens the console redirection configuration sub menu.
▶ Legacy Console Redirection Settings	Submenu	Opens the Legacy Console Redirection Settings sub menu.
Serial Port for Out-of-Band Management / Windows Emergency Management Services (EMS) Console Redirection	**Disabled** Enabled	Enable or disable the Serial Port for Out-of-Band Management/ Windows Emergency Management Services (EMS) Console Redirection.
▶Console Redirection Settings	Submenu	Opens the console redirection configuration sub menu.

Note

The Serial Port Console Redirection can be enabled only if an external Super I/O offering UARTs has been implemented on the carrier board.

10.4.15.1 Console Redirection Settings Submenu

Feature	Options	Description
Terminal Type	VT100 VT100+ VT-UTF8 **ANSI**	Select terminal type.
Baudrate	9600 19200 38400 57600 **115200**	Select baud rate.
Data Bits	7 **8**	Set the number of data bits.
Parity	**None** Even Odd Mark Space	Select the parity.
Stop Bits	**1** 2	Set the number of stop bits.

Feature	Options	Description
Flow Control	**None** Hardware RTS/CTS	Select the flow control.
VT-UTF8 Combo Key Support	Disabled **Enabled**	Enable the VT-UTF8 combination key support for ANSI/VT100 terminals.
Recorder Mode	**Disabled** Enabled	Enable this feature to only send text output over the terminal. **Note:** This feature is helpful to capture and record terminal data.
Resolution 100x31	**Disabled** Enabled	Enable or disable the extended terminal resolution.
Legacy OS Redirection Resolution	**80x24** 80x25	Select the number of rows and columns supported for legacy operating system redirection.
Putty KeyPad	**VT100** LINUX XTERMR6 SCO ESCN VT400	Select function key and keypad on Putty.
Redirection After BIOS POST	**Enabled** Disabled	Enable to continue serial redirection after POST.

Note

The Console Redirection Settings submenu for Serial Port for Out-of-Band Management/ Windows Emergency Management Services (EMS) Console Redirection does not contain all above listed items and contains the additional Out-of-Band Management Port selection item.

10.4.16 CPU Submenu

Feature	Options	Description
Processor Type	No option	Displays the processor ID string. The "Processor Type" text is not displayed.
CPU Signature	No option	Displays the CPU signature.
Microcode Patch	No option	Displays the revision of the microcode patch.
Max CPU Speed	No option	Displays the maximum CPU speed.
Min CPU Speed	No option	Displays the min CPU speed.
CPU Speed	No option	Displays the current CPU speed.
Processor Cores	No option	Displays the number of the processor cores.
Intel® HT Technology	No option	Displays whether Intel® HT technology is supported.
Intel® VT-x Technology	No option	Displays whether Intel® VT-x technology is supported.
Intel® SMX Technology	No option	Displays whether Intel® SMX technology is supported.
64-bit	No option	Displays whether 64-bit is supported.

Feature	Options	Description
EIST Technology	No option	Displays whether enhanced Intel® SpeedStep Technology (EIST) is supported.
CPU C3 State	No option	Displays whether CPU C3 state is supported.
CPU C6 State	No option	Displays whether CPU C6 state is supported.
CPU C7 State	No option	Displays whether CPU C7 state is supported.
CPU C8 State	No option	Displays whether CPU C8 state is supported.
CPU C9 State	No option	Displays whether CPU C9 state is supported.
CPU C10 State	No option	Displays whether CPU C10 state is supported.
L1 Data Cache	No option	Displays the size of the L1 data cache.
L1 Code Cache	No option	Displays the size of the L1 code cache.
L2 Cache	No option	Displays the size of the L2 cache.
L3 Cache	No option	Displays the size of the L3 cache.
L4 Cache	No option	Displays the size of the L4 cache.
Hyper-Threading	Disabled **Enabled**	Enable or disable the Hyper-Threading technology.
Active Processor Cores	**All** 1 2 3	Enable the desired number of cores.
Overclocking Lock	**Disabled** Enabled	FLEX_RATIO(194) MSR.
Intel® Virtualization Technology	Disabled **Enabled**	Enable this feature if you need a VMM to utilize the integrated hardware virtualization support.
Hardware Prefetcher	Disabled **Enabled**	Enable or disable the MLC streamer prefetcher.
Adjacent Cache Line Prefetch	Disabled **Enabled**	Enable or disable prefetching of adjacent cache lines.
CPU AES	Disabled **Enabled**	Enabl or disable CPU Advanced Encryption Standard (AES) instructions.
Boot performance mode	Max Battery **Max Non-Turbo Performance** Turbo Performance	Select the performance state the BIOS will set before operating system handoff.
Intel® Speed Shift Technology	Disabled **Enabled**	Enable this feature to expose the CPPC v2 interface, allowing hardware controlled P-states.
Intel® SpeedStep(tm)	Disabled **Enabled**	Enable this feature if you require support for more than two frequency ranges.
Turbo Mode	Disabled **Enabled**	Enable or disable 'Turbo Mode'.
Package Power Limit Lock	**Disabled** Enabled	If this feature is enabled, PACKAGE_POWER_LIMIT MSR will be locked and a reset will be required to unlock the register.
Power Limit 1 Override	**Disabled** Enabled	If this feature is disabled, BIOS will program the default values for power limit 1 and power limit 1 time window.

Feature	Options	Description
CPU Power Limit 2	Disabled **Enabled**	Enable or disable the CPU power limit 2 value.
Power Limit 2	**0** (more values)	Select the power limit 2 value in 125mW steps. '0' sets the value to 1.25*TDP. **Note:** The processor applies control policies to protect the package power from exceeding this limit.
1-Core Ratio Limit Override	**0** (more values)	This limit is for 1 cores active. '0' sets the factory-configured value.
2-Core Ratio Limit Override	**0** (more values)	This limit is for 2 cores active. '0' sets the factory-configured value.
3-Core Ratio Limit Override	**0** (more values)	This limit is for 3 cores active. '0' sets the factory-configured value.
4-Core Ratio Limit Override	**0** (more values)	This limit is for 4 cores active. '0' sets the factory-configured value.
Platform PL1 Enable	**Disabled** Enabled	Enable or disable the platform Power Limit 1 (PL1) programming. If this option is enabled, the PL1 is used by the processor to limit the average power of a given time window.
Platform PL2	**Disabled** Enabled	Enable or disable the platform Power Limit 2 (PL2) programming. If this option is disabled, the BIOS will program the default values for platform PL2.
CPU C States	**Disabled** Enabled	Enable or disable CPU C states.
Enhanced C1 State	Disabled **Enabled**	If this feature is enabled, the CPU will switch to minimum speed when all cores enter C-State.
C-State Auto Demotion	Disabled C1 C3 **C1 and C3**	Configure C-State Auto Demotion.
C-State Un-demotion	Disabled C1 C3 **C1 and C3**	Configure C-State Un-demotion.
Package C State Demotion	Disabled **Enabled**	Configure C-State demotion.
Package C State Undemotion	Disabled **Enabled**	Configure C-State Un-demotion.
CState Pre-Wake	Disabled **Enabled**	Disable this feature to set bit 30 of POWER_CTL MSR(0x1FC) to 1, disabling the Cstate Pre-Wake.
Package C State Limit	C0/C1 C2 C3 C6 C7 C7s C8 C9 C10 **AUTO**	Package C state limit.

Feature	Options	Description
CFG Lock	Disabled **Enabled**	Configure MSR 0xE2[15], CFG lock bit.
▶Power Limit 3 Settings	Submenu	
Power Limit 3 Override	**Disabled** Enabled	Enable or disable power limit 3 override. If this feature is disabled, BIOS will keep the default values for 'Power Limit 3' and 'Power 'Limit 3 Time'.
CPU Power Limit 3	**0** (more values)	Set CPU power limit 3 value.
CPU Power Limit 3 Time	**0** (more values)	Set time window in which the PowerLimit 3 is maintained.
CPU Power Limit 3 Duty Cycle	**0** (more values)	Specify the duty cycle (in percentage) the CPU is required to maintain over the configured power limit 3 time windows.
Power Limit 3 Lock	Disabled **Enabled**	'Enable' - Locks PL3 configuration in the operating system. 'Disable' - Allows PL3 configurations in the operating system.
▶Power Limit 4 Settings	Submenu	
Power Limit 4 Override	**Disabled** Enabled	If this feature is disabled, BIOS will keep the default values for Power Limit 4.
Power Limit 4	**0** (more values)	Select power limit 4 in in 125mW steps. '0' sets the default value.
Power Limit 4 Lock	**Disabled** Enabled	Enable or disable power limit 4 MSR 601h lock. 'Enable' - Locks PL4 configuration in the operating system. 'Disable' - Allows PL4 configurations in the operating system.
▶CPU Thermal Configuration	Submenu	
CPU DTS	**Disabled** Enabled	'Disabled' - ACPI thermal management uses EC reported temperature values. 'Enabled' - ACPI thermal management uses DTS SMM mechanism to obtain CPU temperature values. 'Out of Spec' - ACPI Thermal Management uses EC reported temperature values and DTS SMM is used to handle Out of Spec.
TCC Activation Offset	**0** (more values)	Set the offset from the Intel® factory Thermal Control Circuit (TCC) activation temperature. For example: If the factory TCC activation temperature is 100C, enter 10 to activate TCC at 90C. **Note:** TCC activation will lower CPU core and graphics core frequency, voltage or both.
ACPI 3.0 T-States	**Disabled** Enabled	Enable or disable ACPI 3.0 T-states.
Intel® TXT(LT) Support	**Disabled** Enabled	Enable or disable Intel® TXT(LT) support.
Debug Interface	**Disabled** Enabled	Enableor disable CPU debug feature.
Debug Interface Lock	**Disabled** Enabled	Lock CPU debug feature setting.
SW Guard Extensions (SGX)	Disabled Enabled **Software Controlled**	Enable or disable Software Guard Extensions (SGX).

Feature	Options	Description
Select Owner EPOCH input type	**No Change in Owner EPOCHs** Change to New Random Owner EPOCHs Manual User Defined Owner EPOCHs	Select owner EPOCH mode. Each EPOCH is 64-bit.
PRMRR Size	AUTO	

10.4.17 Platform Misc Configuration Submenu

Feature	Options	Description
Native PCI Express Support	Disabled **Enabled**	Enable or disable native operating system PCIe support.
Native ASPM	**Disabled** Enabled Auto	Enable this feature to let the operating system control ASPM support of the PCIe device. Disable this feature to let the BIOS control ASPM support of the PCIe device.
BDAT ACPI Table Support	**Disabled** Enabled	Enable this feature to support the BDAT ACPI table.
Intel® Ready Mode Technology	**Disabled** Enabled	Enable or disable the ready mode support based on Windows away-mode. **Note:** Only available on DT/AIO.
ACPI Debug	**Disabled** Enabled	Enable this feature to open a memory buffer for storing debug strings. **Note:** Use the method ADBG to write strings to buffer.
PTID Support	**Disabled** Enabled	Enable this feature to load the PTID SSDT table.
PECI Access Method	**Direct I/O** ACPI	Select 'Direct I/O' or 'ACPI PECI' access method.
Firmware Configuration	Ignore Policy Update Production **Test**	Select firmware configuration option. **Note:** Select 'Ignore Policy Update' (STR_FW_CONFIG_DEFAULT_VA LUE) to skip policy update. This option only works on a platform.
PCI Delay Optimization	**Disabled** Enabled	Enable this feature to use experimental ACPI additions for FW latency optimizations.
▶DPTF Configuration	Submenu	The description of this feature is beyond the scope of this document.
▶Platform Setting	Submenu	The description of this feature is beyond the scope of this document.

10.4.18 SATA Submenu

Feature	Options	Description
SATA Controller(s)	**Enabled** Disabled	Enable or disable the onboard SATA controller(s).
SATA Mode Selection	**AHCI** RAID	Select SATA controller mode. **Note:** RAID option is not supported on all chipsets.
CR#1 - RST Pcie Storage Remapping	Enabled **Disabled**	Enable or disable RST PCIe storage remapping.
CR#1 - Remap Port Selection	**Auto** Port 9 Port 10 Port 11 Port 12	Select port for RST PCIe storage remapping,
CR#2 - RST Pcie Storage Remapping	Enabled **Disabled**	Enable or disable RST Pcie storage remapping.
CR#2 - Remap Port Selection	**Auto** Port 13 Port 14 Port 15 Port 16	Select port for RST PCIe storage remapping,
CR#3 - RST Pcie Storage Remapping	Enabled **Disabled**	Enable or disable RST PCIe storage remapping.
CR#3 - Remap Port Selection	**Auto** Port 17 Port 18 Port 19 Port 20	Select port for RST PCIe storage remapping.
SATA Test Mode	Enabled **Disabled**	Only enable this feature for verification measurements.
Alternate ID	Enabled **Disabled**	Enable this feature to report an alternate device ID. **Note:** Displayed only for RAID SATA mode.
▶ Software Feature Mask Configuration	Submenu	RAID option ROM and Intel® Rapid Storage Technology driver will refer to the 'Software Feature Mask Configuration' to enable or disable the storage features.
Aggressive LPM Support	Enabled **Disabled**	Enable PCH to aggressively enter link power state.
Serial ATA Port 0, 1, 2, 3	No option	Displays the name of the connected Hard Disk or DVDROM if the port is enabled. No options are displayed if the port is disabled or when the port is enabled but no device is connected to it.
Software Preserve	No option	Indicates whether the detected drive supports software settings preservation.

Feature	Options	Description
SATA Port	Disabled **Enabled**	Enable or disable the relevant SATA port.
Hot Plug	**Disabled** Enabled	Enable or disable hot plug support for relevant SATA port.
External SATA	**Disabled** Enabled	Enable or disable external SATA support on relevant SATA port.
Spin Up Device	**Disabled** Enabled	Enable this feature to run an initialization sequence for the connected device during startup at relevant SATA port. **Note:** Enable this feature if your hard disk or special (special) solid-state drive requires it.
SATA Device Type	**Hard Disk Drive** Solid State Drive	Select whether the relevant SATA port is connected to solid-state drive or a hard disk drive.
Topology	**Unknown** ISATA, Direct Connect Flex M2	Select the SATA topology.
Device Sleep	**Disabled** Enabled	Enable or disable mSata for RTD3.
SATA DEVSLEP Idle Timeout Config	**Disabled** Enabled	Enable or disable SATA DTIO Config.

10.4.18.1 Software Feature Mask Configuration

Feature	Options	Description
RAID0	Disabled **Enabled**	Enable or disable RAID0 feature.
RAID1	Disabled **Enabled**	Enable or disable RAID1 feature.
RAID10	Disabled **Enabled**	Enable or disable RAID10 feature.
RAID5	Disabled **Enabled**	Enable or disable RAID5 feature.
Intel® Rapid Recovery Technology	Disabled **Enabled**	Enable or disable Intel® Rapid Recovery Technology.
Option ROM UI and Banner	Disabled **Enabled**	Enable this feature to display the option ROM user interface. **Note:** No option ROM banner or information are displayed if all disks and RAID volumes are normal.

Feature	Options	Description
HDD Unlock	Disabled **Enabled**	If this feature is enabled, the HDD password unlock option is available in the operating system.
LED Locate	Disabled **Enabled**	Enable or disable 'LED Locate'.
IRRT Only on eSATA	Disabled **Enabled**	If this feaute is enabled, only Intel® Rapid Recovery Technology (IRRT) volumes can span internal and external SATA (eSATA) drives. If this feautre is disabled, only RAID volume can span internal and eSATA drives.
Smart Response Technology	Disabled **Enabled**	Enable or disable 'Intel® Smart Response Technology'.
Option ROM UI Normal Delay	**2 Seconds** 4 Seconds 6 Seconds 8 Seconds	If this feature is enabled, select the delay of the option ROM user interface splash screen in normal status.
RST Force Form	**Disabled** Enabled	Enable or disable form for Intel® Rapid Storage Technology.

10.4.19 Thermal Configuration Submenu

Feature	Options	Description
▶Platform Thermal Configuration	Submenu	
PCH Thermal Device	Disabled **Enabled in PCI mode** Enabled in ACPI mode	Enable or disable PCH thermal device (D20:F2).
PCH Temp Read	Disabled **Enabled**	Disable or enable PCH temperature read.
CPU Energy Read	Disabled **Enabled**	Disable or enable CPU energy read.
CPU Temp Read	Disabled **Enabled**	Disable or enable CPU temperature read.
Alert Enable Lock	**Disabled** Enabled	Lock all alert enable settings.

10.4.20 Acoustic Management Submenu

Feature	Options	Description
Acoustic Management Configuration	**Disabled** Enabled	Disable or enable 'Acoustic Management Configuration'.
SATA Port 0 Disk drive name Acoustic Mode	**Bypass** Quiet Max Performance	Select acoustic noise level and performance optimization of optical or hard disk drives: 'Bypass' - Uses drive's preset value. 'Quiet' - Reduces the drive's speed. 'Max Performance' - Maximizes the drive's speed.
SATA Port 1 Disk drive name Acoustic Mode	**Bypass** Quiet Max Performance	Same as at SATA Port 0.
SATA Port 2 Disk drive name Acoustic Mode	**Bypass** Quiet Max Performance	Same as at SATA Port 0.
SATA Port 3 Disk drive name Acoustic Mode	**Bypass** Quiet Max Performance	Same as at SATA Port 0.

Note

SATA ports are only displayed if an optical or hard disk drive is detected.

10.4.21 PCI & PCI Express Submenu

Feature	Options	Description
PCI Bus Driver Version	No option	
PCI Settings		
PCI Latency Timer	**32 PCI Bus Clocks** 64 PCI Bus Clocks 96 PCI Bus Clocks 128 PCI Bus Clocks 160 PCI Bus Clocks 192 PCI Bus Clocks 224 PCI Bus Clocks 248 PCI Bus Clocks	Select value to be programmed into PCI latency timer register.

Feature	Options	Description
PCI-X Latency Timer	32 PCI Bus Clocks **64 PCI Bus Clocks** 96 PCI Bus Clocks 128 PCI Bus Clocks 160 PCI Bus Clocks 192 PCI Bus Clocks 224 PCI Bus Clocks 248 PCI Bus Clocks	Select value to be programmed into the PCI latency timer register.
VGA Palette Snoop	**Disabled** Enabled	Enable or disable VGA palette registers snooping.
PERR# Generation	**Disabled** Enabled	Enable or disable PCI device to generate PERR#.
SERR# Generation	**Disabled** Enabled	Enable or disable PCI device to generate SERR#.
Above 4G Decoding	**Disabled** Enabled	Enable this feautre for 64-bit capable devices to be decoded in Above 4G address space. **Note:** The system must support 64 bit PCI decoding for this feature.
Don't Reset VC-TC Mapping	**Disabled** Enabled	If the system has Virtual Channels, software can reset traffic class mapping to its default state through virtual channels. **Note:** Enabling this feature will not modify VC resources.
▶PCI Hot-Plug Settings	Submenu	

10.4.21.1 PCI Hot Plug Settings Submenu

Feature	Options	Description
BIOS Hot-Plug Support	Disabled **Enabled**	Enable this feature to allow BIOS build in hot-plug support. **Note:** Use this feature if the operating system does not support PCIe and SHPC hot-plug natively.
PCI Buses Padding	Disabled **1** 2 3 4 5	Padd PCI buses behind the bridge for hot-plug.
I/O Resources Padding	Disabled **4 K** 8 K 16 K 32 K	Select padd PCI I/O resources behind the bridge for hot-plug.

Feature	Options	Description
MMIO 32 bit Resources Padding	Disabled 1 M 2 M 4 M 8 M **16 M** 32 M 64 M 128 M	Select padd PCI MMIO 32-bit resources behind the bridge for hot-plug.
PFMMIO 32 bit Resources Padding	Disabled 1 M 2 M 4 M 8 M **16 M** 32 M 64 M 128 M	Select padd PCI MMIO 32-bit prefetchable resources behind the bridge for hot-plug.

10.4.22 UEFI Network Stack Submenu

Feature	Options	Description
UEFI Network Stack	**Disabled** Enabled	Enable or disable the UEFI network stack.
IPv4 PXE Support	Disabled **Enabled**	Enable or disable IPv4 PXE boot support. If disabled, IPv4 PXE boot option will not be created.
IPv6 PXE Support	Disabled **Enabled**	Enable or disable IPv6 PXE boot support. If disabled, IPv6 PXE boot option will not be created.
PXE boot wait time	**0** (more values)	Set wait time to press ESC key to abort the PXE boot.
Media detect count	**1** (more values)	Set the number of times to check for the presence of media.

10.4.23 CSM & Option ROM Control Submenu

Feature	Options	Description
CSM Support	Disabled **Enabled**	Enable or disable CSM support.
CSM16 Module Version	No option	
Gate A20 Active	**Upon Request** Always	'Upon Request' - Gate A20 can be disabled with BIOS services. 'Always' - Gate A20 cannot be disabled. **Note:** This feature is useful if runtime code above 1MB is executed.
Option ROM Messages	**Force BIOS** Keep Current	Set display mode for option ROMs.
INT19 Trap Response	**Immediate** Postponed	Set BIOS reaction on INT19 trapping by option ROM: 'Immediate' - Executes the trap right away. 'Postponed' - Executes the trap during legacy boot.
Boot Option Filter	**UEFI and Legacy** Legacy only UEFI only	This feature controls which devices/boot loaders the system should boot to.
Option ROM execution		
PXE Option ROM Launch Policy	Do not launch **UEFI ROM Only** Legacy ROM Only	This feature controls the execution of UEFI and legacy PXE option ROMs.
Storage Option ROM Launch Policy	Do not launch **UEFI ROM Only** Legacy ROM Only	This feature controls the execution of UEFI and legacy mass storage device option ROMs.
Video Option ROM Launch Policy	Do not launch UEFI ROM Only **Legacy ROM Only**	This feature controls the execution of UEFI and legacy video option ROMs.
Other Option ROM Launch Policy	Do not launch **UEFI ROM Only** Legacy ROM Only	This feature controls the execution of option ROMs for PCI / PCI Express devices other than network, mass storage and video.

10.4.24 NVMe Configuration Submenu

Settings are displayed if an NVMe device is connected.

10.4.25 SDIO Configuration Submenu

Settings are displayed if an SD Card is connected.

10.4.26 USB Submenu

Feature	Options	Description
USB Controllers	No option	Displays the number of enabled EHCI (USB2.0) and xHCI (USB3.0) controllers.
USB Devices	No option	Displays the detected USB devices.
Overcurrent Protection	**Disabled** Enabled	Disable or enable overcurrent protection on all USB ports.
Legacy USB Support	**Enabled** Disabled Auto	Disable this feature to keep USB devices available for EFI applications and BIOS setup only. Select 'Auto' to disable legacy support if no USB devices are connected.
xHCI Hand-off	**Enabled** Disabled	This feature is a workaround for operating system without xHCI hand-off support. **Note:** If this feature is enabled, the xHCI ownership change should be claimed by the xHCI operating system driver.
USB Mass Storage Driver Support	Disabled **Enabled**	Enable or disable USB mass storage driver support.
Port 60/64 Emulation	**Disabled** Enabled	Enable this feature for I/O port 60h/64h emulation support (the complete USB keyboard legacy support with non-USB aware OS).
USB Transfer Timeout	1 sec 5 sec 10 sec **20 sec**	Select the timeout value for control, bulk, and interrupt transfers.
Device Reset Timeout	10 sec **20 sec** 30 sec 40 sec	Select the USB mass storage device Start Unit command timeout.
Device Power-up Delay Selection	**Auto** Manual	'Manual' - Set maximum time a USB device requires to report itself to the host controller. 'Auto' - Sets maximum time a USB device requires to report itself to the host controller to 100ms for a root port or derives the value from the hub descriptor of a hub port.
USB Mass Storage Device Name (Auto detected USB mass storage devices are listed here dynamically)	**Auto** Floppy Forced FDD Hard Disk CD-ROM	Select the emulation type for each USB mass storge device:[1] 'AUTO' - Lets the BIOS auto detect the current formatted media. 'Floppy' - Emulates the device as a floppy drive. 'Forced FDD' - Allows a HDD to be connected as a floppy image.[2] 'Hard Disk' - Allows the hard disk to be emulated as a HDD. 'CD-ROM' - Assumes the CD-ROM is formatted as a bootable media.[3] **Notes:** [1]The device's formatted type and the emulation type provided by the BIOS must match for the device to boot properly. [2]The drive must be formatted with FAT12, FAT16 or FAT32. [3]As specified by the 'El Torito' Format Specification

10.4.27 PC Speaker Submenu

Feature	Options	Description
Debug Beeps	Disabled **Enabled**	Enable or disable general debug / status beep generation.
Input Device Debug Beeps	**Disabled** Enabled	Enable or disable input device debug beeps.
Output Device Debug Beeps	**Disabled** Enabled	Enable or disable output device debug beeps.
USB Driver Beeps	**Disabled** Enabled	Enable or disable USB driver beeps.

10.5 Chipset Setup

The description of this feature is beyond the scope of this document.

10.6 Security Setup

Select the Security tab from the setup menu to enter the Security setup screen.

10.6.1 Security Settings

Feature	Options	Description
BIOS Password	Enter password	Set the desired BIOS and setup administrator password.
BIOS Lock	Disabled **Enabled**	Enable or disable BIOS Lock Enable (BLE) and SMM BIOS Write Protect (SMM_BWP) bits. If enabled, BIOS flash write access is only possible via dedicated BIOS SMM interfaces.
BIOS Update & Write Protection	**Disabled** Enabled	If enabled, the congatec flash software will require the BIOS password to perform write or erase operations.
HDD Security Configuration	List of all detected hard disks supporting the security feature set	Select the device to open its security configuration submenu.
▶Secure Boot Menu	Submenu	

10.6.1.1 BIOS Security Features

BIOS Password/ BIOS Write Protection

A BIOS password protects the BIOS setup program from unauthorized access. This ensures that end users cannot change the system configuration without authorization. With an assigned BIOS password, the BIOS prompts the user for a password on a setup entry. If the password entered is wrong, the BIOS setup program will not launch.

The congatec BIOS uses a SHA256 based encryption for the password, which is more secured than the original AMI encryption. The BIOS password is case sensitive with a minimum of 3 characters and a maximum of 20 characters. Once a BIOS password has been assigned, the BIOS activates the disabled 'BIOS Update and Write Protection' option. If this option enabled, only authorized users (users with the correct password) can update the BIOS. To update the BIOS, use the congatec system utility cgutlcmd.exe with the following syntax:

```
CGUTLCMD BFLASH <BIOS file> /BP: <password> where <password> is the assigned BIOS password.
```

For more information about "Updating the BIOS" refer to the congatec system utility user's guide, which is called CGUTLm1x.pdf and can be found on the congatec AG website at www.congatec.com.

With the BIOS password protection and the BIOS update and write protection, the system configuration is completely secured. If the BIOS is password protected, you cannot change the configuration of an end application without the correct password.

Note

Use cgutlcmd.exe version 1.5.3 or later.

Built in BIOS recovery is disabled in the congatec BIOS firmware to prevent the BIOS from updating itself due to the user pressing a special key combination or a corrupt BIOS being detected. congatec considers such a recovery update a security risk because the BIOS internal update process bypasses the implemented BIOS security explained above.

Only the congatec utility interface to the SMI handler of the BIOS flash update is enabled. Other interfaces to the SMI handler are disabled to prevent non congatec tools from writing to the BIOS flash. As a result of this restriction, flash utilities supplied by AMI or Intel will not work .

UEFI Secure Boot

Secure Boot is a security standard defined in UEFI specification 2.3.1 that helps prevent malicious software applications and unauthorized operating systems from loading during system start up process. Without secure boot enabled (not supported or disabled), the computer simply hands over control to the bootloader without checking whether it is a trusted operating system or malware. With secure boot supported and enabled, the UEFI firmware starts the bootloader only if the bootloader's signature has maintained integrity and also if one of the following conditions is true:

- The bootloader was signed by a trusted authority that is registered in the UEFI database.
- The user has added the bootloader's digital signature to the UEFI database. The BIOS provides the key management setup sub-menu for this purpose.

Note

The congatec BIOS by default enables CSM (Compatibility Support Module) and disables secure boot because most of the industrial computers today boot in legacy (non-UEFI) mode. Since secure boot is only enabled when booting in native UEFI mode, you must therefore disable the CSM (compatibility support module) in the BIOS setup to enable Secure Boot.

A full description of secure boot is beyond the scope of this users guide. For more information about how secure boot leverages signature databases and keys, see the secure boot vverview in the windows deployment options section of the Microsoft TechNet Library at http://technet.microsoft.com.

10.6.1.2 Hard Disk Security Features

Hard Disk Security uses the Security Mode feature commands defined in the ATA specification. This functionality allows users to protect data using drive-level passwords. The passwords are kept within the drive, so data is protected even if the drive is moved to another computer system.

The BIOS provides the ability to 'lock' and 'unlock' drives using the security password. A 'locked' drive will be detected by the system, but no data can be accessed. Accessing data on a 'locked' drive requires the proper password to 'unlock' the disk.

The BIOS enables users to enable/disable hard disk security for each hard drive in setup. A master password is available if the user can not remember the user password. Both passwords can be set independently however the drive will only lock if a user password is installed. The max length of the passwords is 32 bytes.

During POST each hard drive is checked for security mode feature support. In case the drive supports the feature and it is locked, the BIOS prompts the user for the user password. If the user does not enter the correct user password within four attempts, the user is notified that the drive is locked and POST continues as normal. If the user enters the correct password, the drive is unlocked until the next reboot.

In order to ensure that the ATA security features are not compromised by viruses or malicious programs when the drive is typically unlocked, the BIOS disables the ATA security features at the end of POST to prevent their misuse. Without this protection it would be possible for viruses or malicious programs to set a password on a drive thereby blocking the user from accessing the data.

Note

If the user enables password support, a power cycle must occur for the hard drive to lock using the new password. Both user and master password can be set independently however the drive will only lock if a user password is installed.

10.7 Boot Setup

Select the Boot tab from the setup menu to enter the Boot setup screen.

10.7.1 Boot Settings Configuration

Feature	Options	Description
Quiet Boot	**Disabled** Enabled	Enable this feature to display OEM logo instead of POST messages. **Note:** The default OEM logo is a dark screen.
Setup Prompt Timeout	**1** (more values)	Set number of seconds to wait for a setup activation key: '65535' - Waits indefinitely (0xFFFF). '0' - Disables waiting (not recommended).
Bootup NumLock State	**On** Off	Set the keyboard numlock state.
Power Loss Control	**Remain Off** Turn On Last State	Set the mode of operation if an AC power loss occurs: 'Remain Off' - Keeps the power off until the power button is pressed. 'Turn On' - Restores power to the computer. 'Last State' - Restores the power state before power loss occurred. **Note:** This feature only works with an ATX type power supply.
AT Shutdown Mode	System Reboot **Hot S5**	Set the behavior of an AT-powered system after a shutdown.
Enter Setup If No Boot Device	No **Yes**	Set whether the setup menu should be started if no boot device is connected.
Enable Popup Boot Menu	No **Yes**	Set whether the popup boot menu can be started.
Boot Priority Selection	UEFI Standard **Type Based**	'UEFI Based' - Select boot priority from a list of currently detected devices. 'Type Based' - Select boot priority from a list of device types even if they are not connected yet.
Boot Option Sorting Method	**Legacy First** UEFI First	Set boot option sorting method: 'UEFI First' - Tries all UEFI boot options before first legacy boot option. 'Legacy First' Tries all Legacy boot options before first UEFI boot option.

Feature	Options	Description
1st, 2nd, 3rd, ... Boot Device (Up to 12 boot devices can be prioritized if "UEFI Standard" priority list control is selected. If "Type Based" priority list control is enabled only 8 boot devices can be prioritized.)	Disabled SATA 0 Drive SATA 1 Drive USB Harddisk USB CDROM Other USB Device Onboard SD Card Storage Onboard LAN External LAN Firmware-based Bootloader Other Device	This view is only available in the default "Type Based" mode. In "UEFI Standard" mode, you will only see the devices that are connected to the system.
Battery Support	**Auto (Batt. Manager)** Battery-Only On I2C Bus Battery-Only On SMBus	'Battery-Only On I2C Bus' - Battery-only systems using I2C bus. 'Battery-Only On SMBus' - Battery-only systems using SMBus. 'Auto' - Real battery system manager systems using I2C or SMBus.
System Off Mode	**G3/Mech Off** S5/Soft Off	Set system state after shutdown if a battery system is present.
UEFI Fast Boot	**Disabled** Enabled	Enable to boot with a minimum set of devices. **Note:** This feature has no effect for BBS / legacy boot options.
SATA Support	Last Boot HDD Only **All SATA Devices**	Select SATA support.
VGA Support	Auto **UEFI Driver**	'Auto' - Installs legacy video option ROM for legacy operating system boot. **Note:** The boot logo will not be displayed during POST. 'UEFI Driver' - Installs UEFI GOP driver.
USB Support	Disabled Full Init **Partial Init**	'Disabled' - The USB devices will not be available before operating system boot. 'Full Init' - All USB devices will be available during POST and after operating system boot. 'Partial Init' - Specific USB ports/devices will not be available before operating system boot.
PS/2 Device Support	Disabled **Enabled**	Disable to skip PS/2 devices.
Network Stack Driver Support	**Disabled** Enabled	Disable to skip the UEFI network stack driver installation.
Redirection Support	**Disabled** Enabled	Disable to deactivate the Redirection function.
UEFI Screenshot Capability	**Disabled** Enabled	Enable this feature to take a screenshots from the current screen by pressing LCtrl+LAlt+F12. The image will be saved as PNG on the first writable FAT32 partition found.

Note

The term 'AC power loss' stands for the state when the module looses the standby voltage on the 5V_SB pins. On congatec modules, the standby voltage is continuously monitored after the system is turned off. If the standby voltage is not detected within 30 seconds, this is considered an AC power loss condition. If the standby voltage remains stable for 30 seconds, it is assumed that the system was switched off properly.

Inexpensive ATX power supplies often have problems with short AC power sags. When using these ATX power supplies it is possible that the system turns off but does not switch back on, even when the PS_ON# signal is asserted correctly by the module. In this case, the internal circuitry of the ATX power supply has become confused. Usually, another AC power off/on cycle is necessary to recover from this situation.

10.8 Save & Exit Menu

Select the Save & Exit tab from the setup menu with the <Arrow> keys to enter the Save & Exit setup screen.

Feature	Description
Save Changes and Exit	Exit setup menu after saving the changes. The system is only reset if settings have been changed.
Discard Changes and Exit	Exit setup menu without saving any changes.
Save Changes and Reset	Save changes and reset the system.
Discard Changes and Reset	Reset the system without saving any changes.
Save Options	
Save Changes	Save changes made so far to any of the setup options. Stay in setup menu.
Discard Changes	Discard changes made so far to any of the setup options. Stay in setup menu.
Restore Defaults	Restore default values for all the setup options.
Boot Override	
List of all boot devices currently detected	Select device to leave setup menu and boot from the selected device. Only visible and active if Boot Priority Selection setup node is set to "Device Based".

11 Additional BIOS Features

The conga-TC170 uses a congatec/AMI AptioEFI that is stored in an onboard Flash Rom chip and can be updated using the congatec System Utility, which is available in a DOS based command line, Win32 command line, Win32 GUI, and Linux version.

The BIOS displays a message during POST and on the main setup screen identifying the BIOS project name and a revision code. The initial production BIOS is identified as BVSLR1xx or BUSLR1xx for conga-TC170, where:

- R is the identifier for a BIOS ROM file,
- 1 is the so called feature number and
- xx is the major and minor revision number.

The BVSL binary size is 16 MB and the BUSL binary size is 8 MB.

11.1 Supported Flash Devices

The conga-TC170 supports the following flash devices:

- Winbond W25Q128FVSIG (16 MB)
- Winbond W25Q64CVSSIG (8 MB)

The flash devices listed above can be used on the carrier board for external BIOS support. For more information about external BIOS support, refer to the Application Note AN7_External_BIOS_Update.pdf on the congatec website at http://www.congatec.com.

11.2 Updating the BIOS

BIOS updates are often used by OEMs to correct platform issues discovered after the board has been shipped or when new features are added to the BIOS.

For more information about "Updating the BIOS" refer to the user's guide for the congatec System Utility, which is called CGUTLm1x.pdf and can be found on the congatec AG website at www.congatec.com.

12 Industry Specifications

The list below provides links to industry specifications that apply to congatec AG modules.

Specification	Link
Low Pin Count Interface Specification, Revision 1.0 (LPC)	http://developer.intel.com/design/chipsets/industry/lpc.htm
Universal Serial Bus (USB) Specification, Revision 2.0	http://www.usb.org/home
PCI Specification, Revision 2.3	http://www.pcisig.com/specifications
Serial ATA Specification, Revision 3.0	http://www.serialata.org
PICMG® COM Express Module™ Base Specification	http://www.picmg.org/
PCI Express Base Specification, Revision 2.0	http://www.pcisig.com/specifications