

# conga-TC170

COM Express 2.1 Type 6 Compact Module with Intel® 6th Generation Processors

***User's Guide***

Revision 1.10

# Revision History

Revision	Date (yyyy-mm-dd)	Author	Changes
0.1	2016-01-07	AEM	<ul style="list-style-type: none"><li>• Preliminary release</li></ul>
1.0	2016-06-29	BEU	<ul style="list-style-type: none"><li>• Updated available product variants in section 1 "Introduction" and section 2 "Specifications"</li><li>• Added section 9 "Resource List", section 10 "BIOS Setup Description" and section 11 "Additional BIOS Features"</li><li>• Official release</li></ul>
1.1	2018-08-24	AEM	<ul style="list-style-type: none"><li>• Removed support for SD card in the whole document</li><li>• Corrected the hardware and BIOS revisions in table 2 "Power Consumption Values"</li><li>• Updated the note in section 2.6.1 "CMOS Battery Power Consumption"</li><li>• Updated the cooling diagrams in section 4 "Cooling Solutions"</li><li>• Corrected the description of pins D63 and D64 in table 29 "Connector C-D Pinout"</li><li>• Updated section 5.1.10 "LVDS/eDP"</li><li>• Updated table 29 "Connector C-D Pinout"</li></ul>
1.2	2020-03-30	AEM	<ul style="list-style-type: none"><li>• Added note about recommended boot mode in section 2.2 "Supported Operating Systems"</li><li>• Updated the input voltage range of VCC_RTC in section 2.4.1 "Electrical Characteristics"</li><li>• Added note about the minimum pulse width required for proper button detection in table 24 "Power and System Management Signal Descriptions"</li><li>• Added section 6.1 "eMMC 5.0"</li><li>• Deleted section 7.4 "DDR4 Memory"</li><li>• Updated sections 10 "BIOS Setup Description" and 11 "Additional BIOS Features"</li><li>• Deleted section 12 "Industry Specification"</li></ul>
1.3	2020-12-08	AEM	<ul style="list-style-type: none"><li>• Corrected typographical error in section 11.3 "Supported Flash Devices"</li></ul>
1.4	2021-04-19	AEM	<ul style="list-style-type: none"><li>• Updated table 2 "conga-TC170 Variants, table 3 "Feature Summary", table 8 "Display Combination (U-processor line)" and table 16 "TMDS Signal Descriptions"</li><li>• Updated section 3 "Block Diagram" and section 5.1.3 "Display Interfaces"</li><li>• Deleted section 5.1.3.1 "HDMI" and section 5.1.3.2 "DVI"</li><li>• Added note to table 16 "TMDS Signal Descriptions"</li></ul>
1.5	2021-07-31	AEM	<ul style="list-style-type: none"><li>• Added Software License Information</li><li>• Changed congatec AG to congatec GmbH</li><li>• Updated the Power Supply Implementation Guidelines in section 5.1.13 "Power Control"</li><li>• Updated section 6.8 "congatec Battery Management Interface"</li></ul>
1.6	2021-11-16	AEM	<ul style="list-style-type: none"><li>• Deleted HDMI references from section 1.2 "Options Information", section 2.1 "Feature List", section 3 "Block Diagram" and section 5.1.3 "Display Interfaces"</li></ul>
1.7	2023-08-02	AEM	<ul style="list-style-type: none"><li>• Corrected the pin numbers of USB port 0 and 1 in table 22 "USB 2.0 Signal Descriptions"</li><li>• Updated section 6.6 "Power Loss Control"</li></ul>
1.8	2023-12-12	AEM	<ul style="list-style-type: none"><li>• Updated the title page</li><li>• Updated the RoHS directive</li><li>• Added a note about optimal storage conditions to section 2.7 "Environmental Specifications"</li><li>• Added a note about the storage of congatec cooling solutions to section 4 "Cooling Solutions"</li><li>• Updated section 6.2.4 "Power Loss Control"</li></ul>
1.9	2024-11-05	AEM	<ul style="list-style-type: none"><li>• Updated section 4.1 "CSA Dimensions"</li><li>• Corrected the standoff height in section 4.3 "HSP Dimensions"</li></ul>

Revision	Date (yyyy-mm-dd)	Author	Changes
1.10	2025-03-06	RVI	<ul style="list-style-type: none"> <li>• Added a WEEE Compliance Declaration to the preface section</li> <li>• Added a note to section 2.3 "Mechanical Dimensions"</li> <li>• Updated section 2.7 "Environmental Specifications"</li> <li>• Added new section 2.8 Storage Specifications</li> <li>• Updated the Table 15 "DDI Signal Descriptions" and removed tables "TMDS Signal Descriptions" and "DisplayPort (DP) Signal Descriptions"</li> </ul>

---

# 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® Module Base Specification
- COM Express® Carrier Design Guide

These documents are available on the PICMG website at [www.picmg.org](http://www.picmg.org). Additionally, check the restricted area of the congatec website at [www.congatec.com](http://www.congatec.com) and the website of the respective silicon vendor for relevant documents (Erratum, PCN, Sighting Reports and others).

## Software Licenses

### Notice Regarding Open Source Software

The congatec products contain Open Source software that has been released by programmers under specific licensing requirements such as the "General Public License" (GPL) Version 2 or 3, the "Lesser General Public License" (LGPL), the "ApacheLicense" or similar licenses.

You can find the specific details at <https://www.congatec.com/en/licenses/>. Search for the revision of the BIOS/UEFI or Board Controller Software (as shown in the POST screen or BIOS setup) to get the complete product related license information. To the extent that any accompanying material such as instruction manuals, handbooks etc. contain copyright notices, conditions of use or licensing requirements that contradict any applicable Open Source license, these conditions are inapplicable.

The use and distribution of any Open Source software contained in the product is exclusively governed by the respective Open Source license. The Open Source software is provided by its programmers without ANY WARRANTY, whether implied or expressed, of any fitness for a particular purpose, and the programmers DECLINE ALL LIABILITY for damages, direct or indirect, that result from the use of this software.

### OEM/ CGUTL BIOS

BIOS/UEFI modified by customer via the congatec System Utility (CGUTL) is subject to the same license as the BIOS/UEFI it is based on. You can find the specific details at <https://www.congatec.com/en/licenses/>.

---

## Disclaimer

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

congatec GmbH 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 GmbH 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 GmbH 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.

## RoHS Directive

All congatec GmbH designs comply with EU RoHS Directive 2011/65/EU and Delegated Directive 2015/863.

## Electrostatic Sensitive Device



All congatec GmbH products are electrostatic sensitive devices. They are enclosed in static shielding bags, and shipped enclosed in secondary packaging (protective packaging). The secondary packaging does not provide electrostatic protection.

Do not remove the device from the static shielding bag or handle it, except at an electrostatic-free workstation. Also, do not ship or store electronic devices near strong electrostatic, electromagnetic, magnetic, or radioactive fields unless the device is contained within its original packaging. Be aware that failure to comply with these guidelines will void the congatec GmbH Limited Warranty.

## Copyright Notice

Copyright © 2015, congatec GmbH. All rights reserved. All text, pictures and graphics are protected by copyrights. No copying is permitted without written permission from congatec GmbH.

congatec GmbH has made every attempt to ensure that the information in this document is accurate yet the information contained within is supplied "as-is".

---

## WEEE Directive



To comply with Directive 2012/19/EU on Waste Electrical and Electronic Equipment (WEEE), ensure that this product is disposed of correctly at the end of its lifecycle. Customers are required to take electrical and electronic equipment to designated collection facilities separate from unsorted municipal waste, following applicable regional laws.

Proper disposal through designated collection points allows for the recycling, recovery, and reuse of valuable materials, supporting a more efficient use of resources and reducing environmental impact.



*Standalone congatec components, such as modules, carrier boards, and cooling solutions are designed to function only within other products. WEEE registration for the complete product must be completed by the entity placing the final product on the market.*

## 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.



Notes call attention to important information that should be observed.

## 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 GmbH, our products, or our website.

---

## Certification

congatec GmbH is certified to DIN EN ISO 9001 standard.



## Warranty

congatec GmbH 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](http://www.congatec.com). congatec GmbH 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](http://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 GmbH 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 GmbH prior to returning the non conforming product freight prepaid. congatec GmbH 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 GmbH 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.

---

## Technical Support

congatec GmbH 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](http://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](mailto:support@congatec.com)

## Terminology

Term	Description
CSA	Active Cooling Solution
CSP	Passive Cooling Solution
DSC	Display Stream Compression
DTR	Dynamic Temperature Range
eDP	Embedded DisplayPort
EU	Execution Unit
DDI	Digital Display Interface
GB	Gigabyte
GHz	Gigahertz
HDA	High Definition Audio
HBR	High Bit Rate
HSP	Heatspreader
kB	Kilobyte
kHz	Kilohertz
MB	Megabyte
Mbit	Megabit
MHz	Megahertz
N.A	Not available
N.C	Not connected
PCIe	PCI Express
PCH	Platform Controller Hub
PEG	PCI Express Graphics
SATA	Serial ATA
TBD	To be determined
TDP	Thermal Design Power



# Contents

1	Introduction .....	12	5.1.6	Gigabit Ethernet .....	29
1.1	COM Express™ Concept.....	12	5.1.7	Audio .....	30
1.2	Options Information.....	13	5.1.8	LPC Bus.....	30
2	Specifications .....	14	5.1.9	I²C Bus .....	30
2.1	Feature List .....	14	5.1.10	ExpressCard .....	30
2.2	Supported Operating Systems .....	15	5.1.11	General Purpose Serial Interface .....	30
2.3	Mechanical Dimensions .....	15	5.1.12	GPIOs.....	31
2.4	Supply Voltage Standard Power .....	16	5.1.13	Power Control .....	31
2.4.1	Electrical Characteristics .....	17	5.1.14	Power Management.....	34
2.4.2	Rise Time .....	17	6	Additional Features.....	35
2.5	Power Consumption .....	17	6.1	eMMC 5.0 .....	35
2.6	Supply Voltage Battery Power .....	19	6.2	congatec Board Controller (cBC) .....	35
2.7	Environmental Specifications .....	19	6.2.1	Board Information .....	35
2.8	Storage Specifications .....	20	6.2.2	Watchdog .....	35
2.8.1	Module.....	20	6.2.3	I²C Bus.....	36
2.8.2	Cooling Solution .....	20	6.2.4	Power Loss Control .....	36
3	Block Diagram.....	21	6.3	OEM BIOS Customization.....	37
4	Cooling Solutions.....	22	6.3.1	OEM Default Settings .....	37
4.1	CSA Dimensions .....	23	6.3.2	OEM Boot Logo.....	37
4.2	CSP Dimensions.....	24	6.3.3	OEM POST Logo .....	37
4.3	HSP Dimensions.....	25	6.3.4	OEM BIOS Code/Data.....	38
5	Connector Rows.....	26	6.3.5	OEM DXE Driver .....	38
5.1	Primary and Secondary Connector Rows.....	26	6.4	congatec Battery Management Interface .....	38
5.1.1	PCI Express™ .....	26	6.5	API Support (CGOS) .....	39
5.1.2	PCI Express Graphics (PEG) .....	26	6.6	Security Features.....	39
5.1.3	Display Interfaces.....	27	6.7	Suspend to Ram.....	39
5.1.3.1	DisplayPort (DP) .....	28	7	conga Tech Notes .....	40
5.1.3.2	LVDS/eDP.....	28	7.1	Intel® Processor Features .....	40
5.1.3.3	VGA.....	28	7.1.1	Adaptive Thermal Monitor and Catastrophic Thermal Protection 40	
5.1.4	SATA .....	29	7.1.2	Intel® SpeedStep® Technology (EIST) .....	41
5.1.5	USB .....	29	7.1.3	Intel® Turbo Boost Technology .....	41
			7.1.4	Intel® Virtualization Technology .....	42
			7.1.5	Thermal Management .....	42

7.2	ACPI Suspend Modes and Resume Events.....	43	10.4.17	CPU Submenu.....	90
8	Signal Descriptions and Pinout Tables.....	44	10.4.17.1	CPU Information .....	93
8.1	Connector Signal Descriptions .....	45	10.4.18	SATA Submenu .....	94
8.2	Boot Strap Signals .....	64	10.4.18.1	Software Feature Mask Configuration .....	96
9	System Resources .....	65	10.4.19	Acoustic Management Submenu.....	97
9.1	I/O Address Assignment.....	65	10.4.20	PCI Express Configuration Submenu .....	97
9.1.1	LPC Bus.....	65	10.4.21	PCI Express Configuration Submenu .....	99
9.2	PCI Configuration Space Map .....	66	10.4.21.1	PCI Express Gen3 Eq Lanes Submenu.....	100
9.3	I <sup>2</sup> C .....	67	10.4.21.2	PCI Express Settings Submenu .....	100
9.4	SM Bus.....	67	10.4.21.3	PCI Express GEN2 Settings Submenu .....	101
10	BIOS Setup Description .....	68	10.4.21.4	PCI Express Port 0 - 7 Submenu .....	102
10.1	Entering the BIOS Setup Program .....	68	10.4.22	UEFI Network Stack Submenu .....	105
10.1.1	Boot Selection Popup.....	68	10.4.23	CSM & Option ROM Control Submenu.....	105
10.2	Setup Menu and Navigation.....	68	10.4.24	NVMe Configuration Submenu .....	106
10.3	Main Setup Screen.....	69	10.4.25	SDIO Configuration Submenu .....	106
10.3.1	Platform Information Submenu.....	70	10.4.26	USB Submenu .....	107
10.4	Advanced Setup .....	71	10.4.27	Diagnostics Settings Submenu .....	109
10.4.1	Graphics Submenu.....	72	10.4.28	GPIO Configuration Submenu .....	110
10.4.1.1	Display Interface Signal Integrity Settings Submenu .....	76	10.4.29	Board Controller Command Control Submenu .....	110
10.4.2	Watchdog Submenu .....	77	10.4.30	PC Speaker Submenu .....	110
10.4.3	Module Serial Ports Submenu .....	79	10.5	Chipset Setup .....	111
10.4.4	Hardware Health Monitoring Submenu .....	81	10.6	Security Setup.....	111
10.4.5	Intel® Ethernet Connection (H) I219-LM Submenu .....	82	10.6.1	Security Settings .....	111
10.4.5.1	NIC Configuration Submenu .....	83	10.6.1.1	BIOS Security Features .....	111
10.4.6	Driver Health Submenu.....	83	10.6.1.2	Hard Disk Security Features .....	113
10.4.7	Trusted Computing Submenu.....	83	10.7	Boot Setup.....	114
10.4.8	RTC Wake Settings Submenu .....	84	10.7.1	Boot Settings Configuration .....	114
10.4.9	LPC Generic I/O Range Decode Submenu.....	84	10.8	Save & Exit Menu.....	116
10.4.10	GPI IRQ Configuration Submenu.....	85	11	Additional BIOS Features .....	117
10.4.11	ACPI Submenu.....	85	11.1	BIOS Versions.....	117
10.4.12	Intel® ICC Submenu .....	87	11.2	Updating the BIOS.....	118
10.4.13	PCH-FW Configuration Submenu.....	87	11.2.1	Update from External Flash .....	118
10.4.14	SMART Settings Submenu .....	88	11.3	Supported Flash Devices .....	118
10.4.15	Super IO Submenu .....	88			
10.4.16	Serial Port Console Redirection Submenu .....	89			
10.4.16.1	Console Redirection Settings Submenu .....	89			

---

# List of Tables

---

Table 1	COM Express™ 2.1 Pinout Types .....	12
Table 2	conga-TC170 Variants.....	13
Table 3	Feature Summary .....	14
Table 4	Measurement Description.....	18
Table 5	Power Consumption Values .....	18
Table 6	CMOS Battery Power Consumption .....	19
Table 7	Cooling Solution Variants.....	22
Table 8	Display Combination (U-processor line).....	27
Table 9	Wake Events.....	43
Table 10	Signal Tables Terminology Descriptions .....	44
Table 11	Connector A–B Pinout .....	45
Table 12	Connector C–D Pinout.....	47
Table 13	PCI Express Signal Descriptions (general purpose) .....	49
Table 14	PCI Express Signal Descriptions (x16 Graphics).....	50
Table 15	DDI Signal Description.....	52
Table 16	Embedded DisplayPort Signal Descriptions.....	54
Table 17	CRT Signal Descriptions.....	54
Table 18	LVDS Signal Descriptions.....	55
Table 19	Serial ATA Signal Descriptions .....	55
Table 20	USB 2.0 Signal Descriptions.....	56
Table 21	USB 3.0 Signal Descriptions.....	57
Table 22	Gigabit Ethernet Signal Descriptions.....	57
Table 23	Intel® High Definition Audio Link Signals Descriptions.....	58
Table 24	ExpressCard Support Pins Signal Descriptions.....	58
Table 25	LPC Signal Descriptions .....	59
Table 26	SPI BIOS Flash Interface Signal Descriptions.....	59
Table 27	Miscellaneous Signal Descriptions.....	59
Table 28	General Purpose I/O Signal Descriptions .....	60
Table 29	Power and System Management Signal Descriptions .....	61
Table 30	General Purpose Serial Interface Signal Descriptions.....	62
Table 31	Module Type Definition Signal Description .....	62
Table 32	Power and GND Signal Descriptions.....	63
Table 33	Boot Strap Signal Descriptions .....	64
Table 34	PCI Configuration Space Map .....	66

# 1 Introduction

## 1.1 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 84 mm x 55 mm
- Compact 95 mm x 95 mm
- Basic 125 mm x 95 mm
- Extended 155 mm x 110 mm

Table 1 COM Express™ 2.1 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.

## 1.2 Options Information

The conga-TC170 is currently available in four variants. The table below shows the different configurations available.

Table 2 conga-TC170 Variants

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
DP++	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 3 Feature Summary

Form Factor	Based on COM Express™ standard pinout Type 6 Rev. 2.1 (Compact size 95 x 95 mm)	
Processor	6 <sup>th</sup> Generation Intel® Core™ i7,i5, i3 Single Chip Ultra Low TDP Processors	
Memory	Two memory sockets (located on the top and bottom side). Supports <ul style="list-style-type: none"><li>- SO-DIMM non-ECC DDR4 (voltage @ 1.2V) modules</li><li>- data rates up to 2133 MT/s</li><li>- maximum 32 GB capacity (16 GB per socket)</li></ul>	
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: <ul style="list-style-type: none"><li>- Intel® Clear Video Technology (HD encode/transcode, Blu-ray playback)</li><li>- DirectX Video Acceleration (full AVC/VC1/MPEG2 hardware decode)</li><li>- OpenGL 4.4, and DirectX12</li><li>- up to 3 independent displays</li></ul>	
	2x DP++ 1x LVDS 1x Optional VGA 1x Optional eDP 1.3 1x Optional PEG x1 or x2	Resolutions up to 4K <b>NOTE:</b> <i>The conga-TC170 does not natively support TMDS. A DP++ to TMDS converter (e.g. PTN3360D) needs to be implemented.</i>
Peripheral Interfaces	8x USB 2.0 (with up to 4x USB 3.0) 3x SATA® 6Gb/s with RAID 0/1/5/10 2x UART Up to 8x PCI Express® Gen. 3 lanes (supports four x1 or one x4 links via special BIOS firmware) GPIOs Optional x1 or x2 PEG port (requires re-routing of PCIe lanes 5 and/or 6) LPC Bus I²C Bus (fast mode, multi-master)	SM Bus SPI <b>NOTE:</b> <sup>1</sup> <i>The conga-TC170 does not natively support TMDS. A DP++ to TMDS converter (e.g. PTN3360D) needs to be implemented.</i> <sup>2</sup> <i>Intel chipset supports a maximum of six PCIe devices at any time.</i> <sup>3</sup> <i>The conga-TC170 offers only seven PCIe lanes if PEG x1 port is implemented and only six PCIe lanes if PEG x2 port is implemented.</i>
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	
BIOS	AMI Aptio® V UEFI 2.x firmware, 8 or 16 MB serial SPI with congatec Embedded BIOS features	
Storage	Optional eMMC 5.0 onboard flash	

<b>Power Management</b>	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
<b>Security</b>	Optional discrete Trusted Platform Module "TPM 1.2/2.0"; new AES Instructions for faster and better encryption

## 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

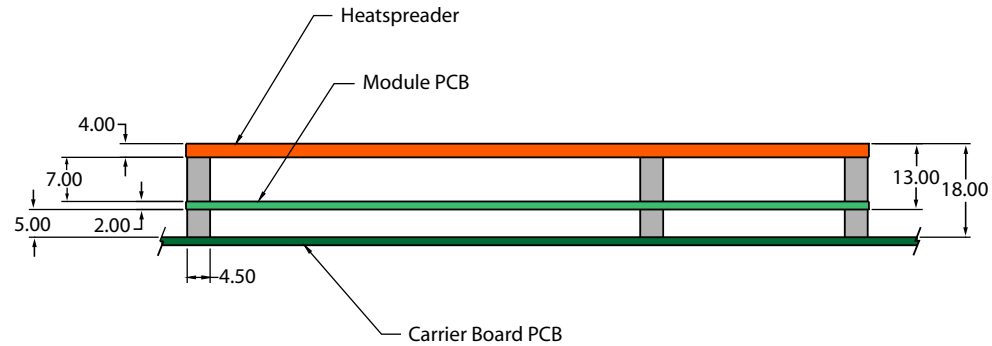


### Note

*The CSM (Compatibility Support Module) is disabled in the BIOS setup menu by default because we recommend to operate the system in native UEFI mode.*

## 2.3 Mechanical Dimensions

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



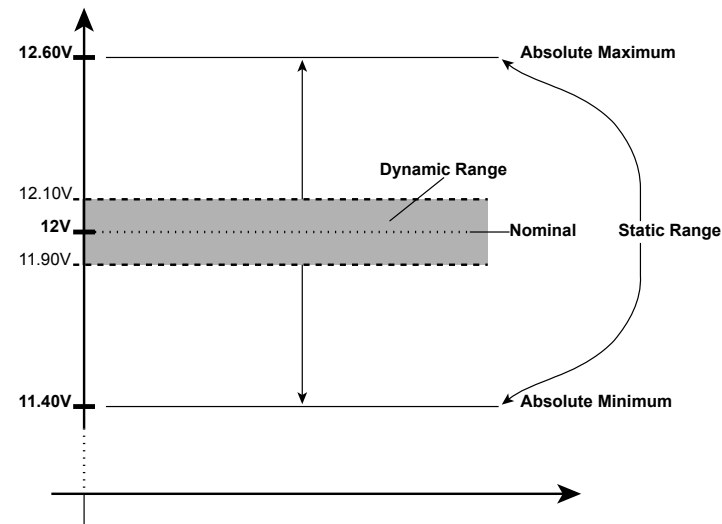
#### Note

3D models of congatec products are available at [www.congatec.com/login](http://www.congatec.com/login). These models indicate the overall length, height and width of each product. If you need login access, contact your local sales representative.

## 2.4 Supply Voltage Standard Power

- 12V DC  $\pm$  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	2.5 - 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

- Input voltage +12 V
- conga-TC170 COM
- modified congatec carrier board
- conga-TC170 cooling solution
- Microsoft Windows 7 (64 bit)



*The CPU was stressed to its maximum workload with the Intel® Thermal Analysis Tool*

**Table 4 Measurement Description**

The power consumption values were recorded during the following system states:

System State	Description	Comment
S0: Minimum value	Lowest frequency mode (LFM) with minimum core voltage during desktop idle	The CPU was stressed to its maximum frequency
S0: Maximum value	Highest frequency mode (HFM/Turbo Boost).	The CPU was stressed to its maximum frequency
S0: Peak value	Highest current spike during the measurement of "S0: Maximum value". This state shows the peak value during runtime	Consider this value when designing the system's power supply to ensure that sufficient power is supplied during worst case scenarios
S3	COM is powered by VCC_5V_SBY	
S5	COM is powered by VCC_5V_SBY	

**Note**

1. The fan and SATA drives were powered externally.
2. All other peripherals except the LCD monitor were disconnected before measurement.

**Table 5 Power Consumption Values**

The table below provides additional information about the conga-TC170 power consumption. The values were recorded at various operating modes.

Part No.	Memory Size	H.W Rev.	BIOS Rev.	OS (64 bit)	CPU			Current (A)				
					Variant	Cores	Freq/Turbo (GHz)	S0: Min	S0: Max	S0: Peak	S3	S5
045200	4 GB	A.2	BVSLR005	Windows 7	Intel® Core™ i7-6600U	2	2.2/3.4	0.34	2.49	3.37	0.11	0.07
045201	4 GB	A.2	BVSLR005	Windows 7	Intel® Core™ i7-6300U	2	2.4/3.0	0.34	2.38	3.03	0.10	0.06
045202	4 GB	A.2	BVSLR005	Windows 7	Intel® Core™ i3-6100U	2	2.3/N.A	0.33	2.36	2.75	0.08	0.06
045203	4 GB	A.2	BUSLR005	Windows 7	Intel® Celeron® 3955U	2	2.0/N.A	0.40	1.43	1.63	0.07	0.06

**Note**

With fast input voltage rise time, the inrush current may exceed the measured peak current.

## 2.6 Supply Voltage Battery Power

Table 6 CMOS Battery Power Consumption

RTC @	Voltage	Current
-10°C	3V DC	1.18 $\mu$ A
20°C	3V DC	1.33 $\mu$ A
70°C	3V DC	1.99 $\mu$ A



- Note**
1. Do not use the CMOS battery power consumption values listed above to calculate CMOS battery lifetime.
  2. Measure the CMOS battery power consumption in your customer specific application in worst case conditions (for example, during high temperature and high battery voltage).
  3. Consider also the self-discharge of the battery when calculating the lifetime of the CMOS battery. For more information, refer to application note AN9\_RTC\_Battery\_Lifetime.pdf on congatec GmbH website at [www.congatec.com/support/application-notes](http://www.congatec.com/support/application-notes).
  4. We recommend to always have a CMOS battery present when operating the conga-TC170.

## 2.7 Environmental Specifications

Temperature	Operation: 0° to 60°C	Storage: -20° to +80°C
Relative 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 heat spreader, the maximum operating temperature refers to any measurable spot on the heat spreader's surface.

Humidity specifications are for non-condensing conditions.

---

## 2.8 Storage Specifications

This section describes the storage conditions that must be observed for optimal performance of congatec products.

### 2.8.1 Module

For long-term storage of the conga-TC170 (more than six months), keep the conga-TC170 in a climate-controlled building at a constant temperature between 5°C and 40°C, with humidity of less than 65% and at an altitude of less than 3000 m. Also ensure the storage location is dry and well ventilated.



#### Note

*We do not recommend storing the conga-TC170 for more than five years under these conditions.*

### 2.8.2 Cooling Solution

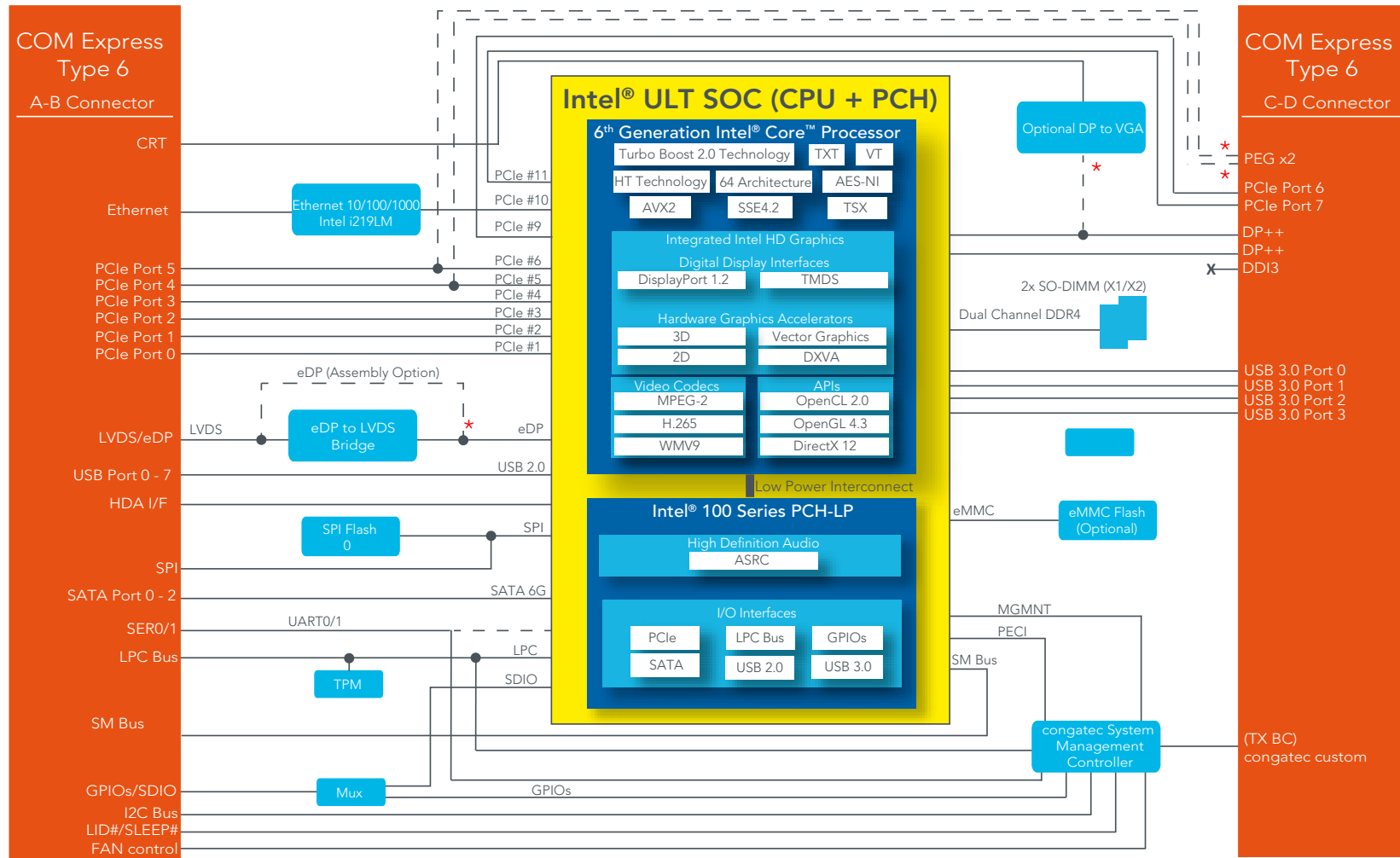
The heatpipes of congatec heatspreaders/cooling solutions are filled with water by default. For optimal cooling performance, do not store the heatspreaders/cooling solutions at temperatures below -20°C.



#### Caution

1. *For temperatures between -10°C and -20°C, preheat the heatpipes before operation. Optionally, the heatpipes can be filled with acetone instead. For more information, contact your local sales representative.*
2. *For optimal thermal dissipation, do not store the congatec cooling solutions for more than six months.*

### 3 Block Diagram



## 4 Cooling Solutions

congatec GmbH offers the following cooling solutions for the conga-TC170. The dimensions of the cooling solutions are shown in the sub-sections. All measurements are in millimeters.

Table 7 Cooling Solution Variants

	Cooling Solution	Part No	Description
1	HSP	045230	Heatspreader with 2.7 mm bore-hole standoffs
		045231	Heatspreader with M2.5 mm threaded standoffs
2	CSP	045232	Passive cooling solution with 2.7 mm bore-hole standoffs
		045233	Passive cooling solution with M2.5 mm threaded standoffs
3	CSA	045234	Active cooling solution with 2.7 mm bore-hole standoffs
		045235	Active cooling with M2.5 mm threaded standoffs



### Note

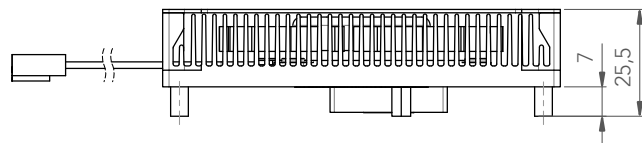
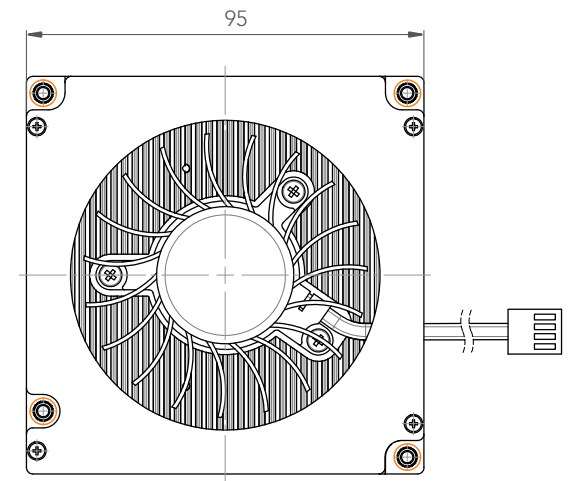
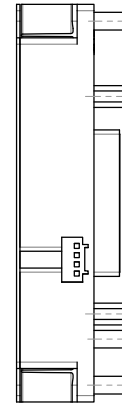
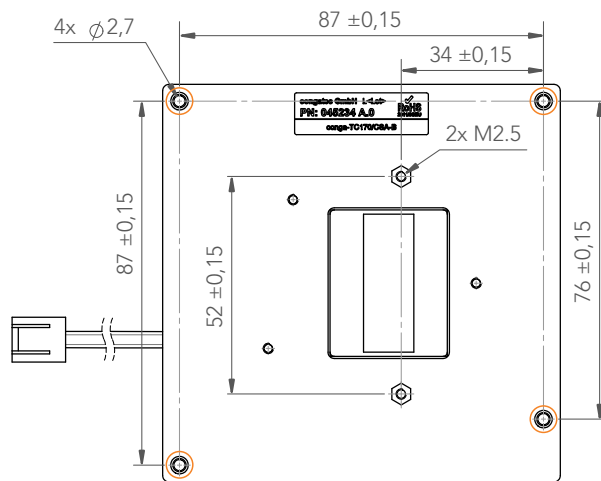
1. We recommend a maximum torque of 0.4 Nm for carrier board mounting screws and 0.5 Nm for module mounting screws.
2. The gap pad material used on congatec heatspreaders may contain silicon oil that can seep out over time depending on the environmental conditions it is subjected to. For more information about this subject, contact your local congatec sales representative and request the gap pad material manufacturer's specification.
3. For optimal thermal dissipation, do not store the congatec cooling solutions for more than six months.



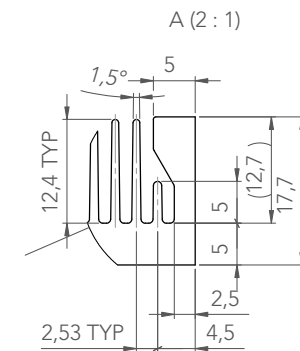
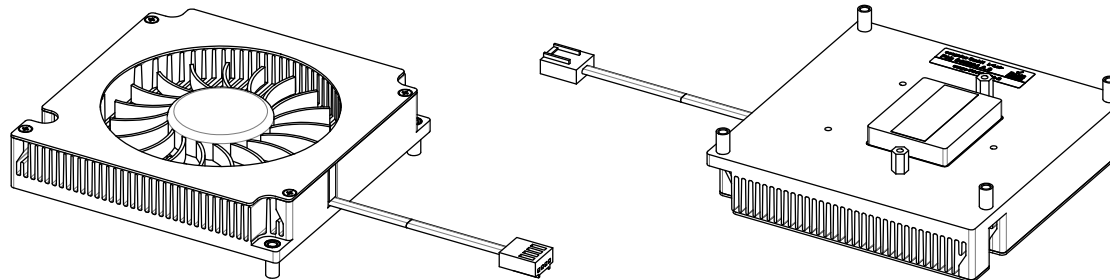
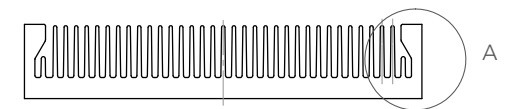
### Caution

1. The congatec heatspreaders/cooling solutions are tested only within the commercial temperature range of 0° to 60°C. If your application that features a congatec heatspreader/cooling solution operates outside this temperature range, ensure the correct operating temperature of the module is maintained at all times. This may require additional cooling components for your final application's thermal solution.
2. For adequate heat dissipation, use the mounting holes on the cooling solution to attach it to the module. Apply thread-locking fluid on the screws if the cooling solution is used in a high shock and/or vibration environment. To prevent the standoff from stripping or cross-threading, use non-threaded carrier board standoffs to mount threaded cooling solutions.
3. For applications that require vertically-mounted cooling solution, use only coolers that secure the thermal stacks with fixing post. Without the fixing post feature, the thermal stacks may move.
4. Do not exceed the recommended maximum torque. Doing so may damage the module or the carrier board, or both.

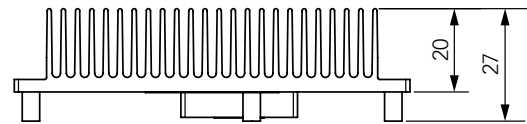
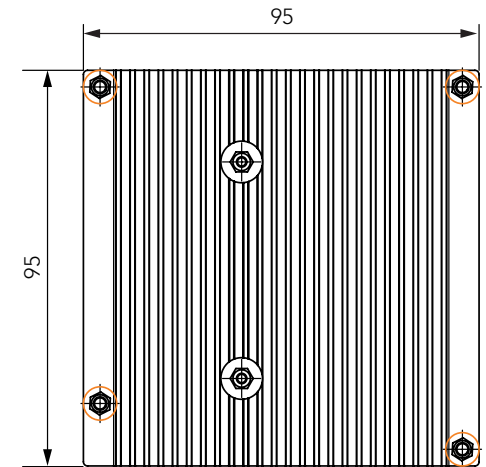
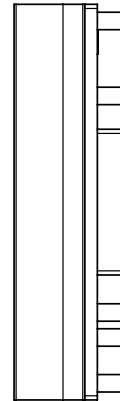
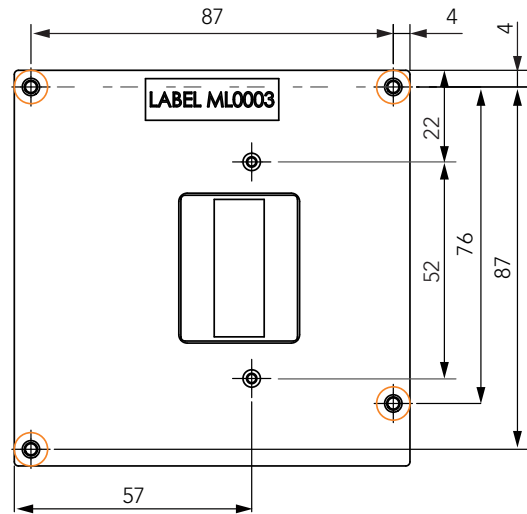
## 4.1 CSA Dimensions




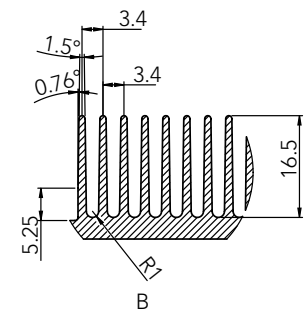
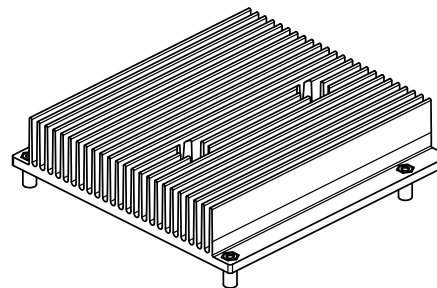
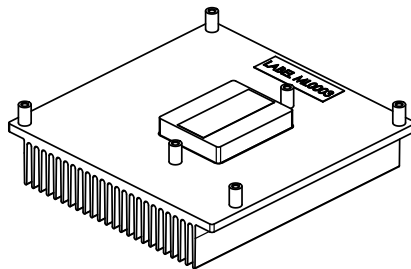
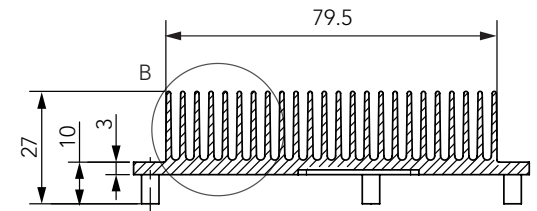
- M2.5 x 10 mm threaded standoff for threaded version or  $\phi 2,7$  x 10 mm non-threaded standoff for borehole version



## 4.2 CSP Dimensions

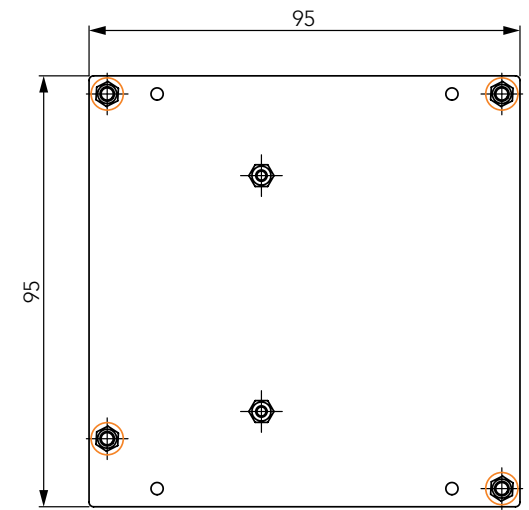
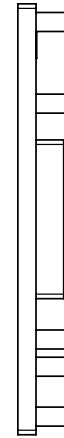
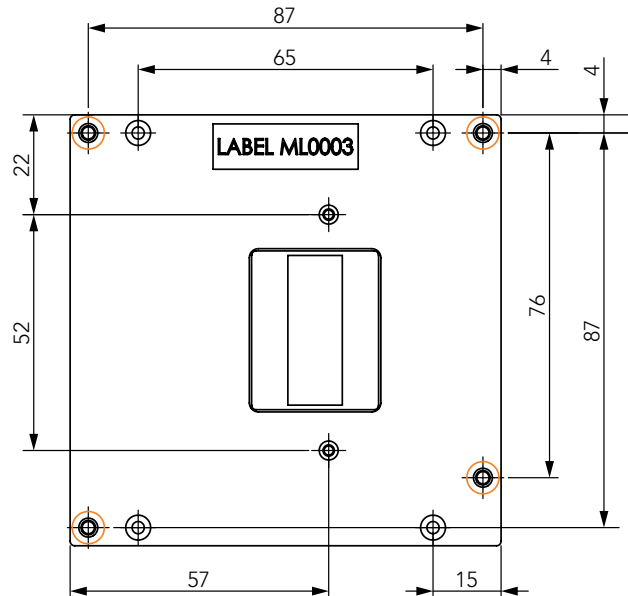



 M2.5 x 10 mm  
threaded standoff  
for threaded version  
or  
ø2.7 x 10 mm  
non-threaded standoff  
for borehole version

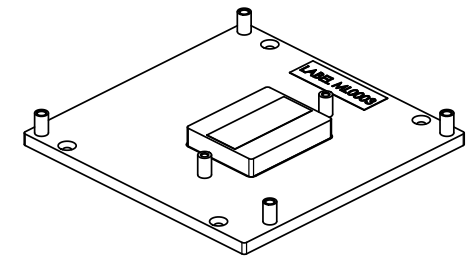
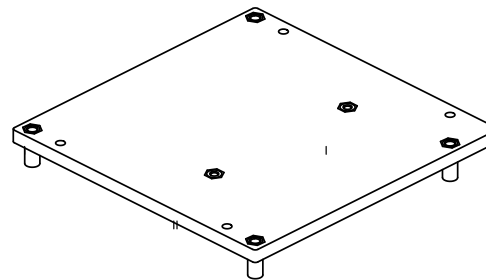
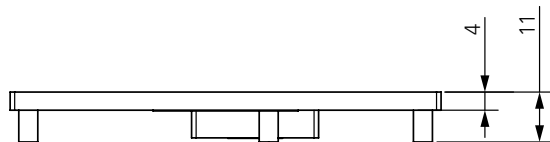




## 4.3 HSP Dimensions



 M2.5 x 11 mm  
threaded standoff  
for threaded version  
or  
ø2.7 x 11 mm  
non-threaded standoff  
for borehole version



---

## 5 Connector Rows

---

The conga-TC170 is connected to the carrier board via two 220-pin connectors (COM Express Type 6 pinout). 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.

### 5.1 Primary and Secondary Connector Rows

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

#### 5.1.1 PCI Express™

The conga-TC170 offers six PCIe lanes on the A–B connector and two PCIe lanes on the C–D connector. The lanes support:

- up to 8 GTps (Gen 3) speed
- an 8 x1 link configuration
- a 1 x4 + 4 x1 link, 1 x4 + 1 x2 + 2 x1 link or a 3 x2 + 2 x1 link via a special/customized BIOS firmware
- lane polarity inversion



#### Note

*The number of supported lanes reduces if the optional PEG port is supported.*

#### 5.1.2 PCI Express Graphics (PEG)

The conga-TC170 supports an optional x1 or x2 PEG port on the C–D connector. To support this optional interface, you need a customized conga-TC170 variant. For more information, contact congatec technical support team.



#### Note

*The PEG lanes can not be linked together with the PCI Express lanes in section 5.1.1 "PCI Express™".*

## 5.1.3 Display Interfaces

The conga-TC170 supports the following:

- up to two DP++
- single- or dual-channel LVDS
- optional VGA (BOM option)
- up to three independent displays (display combinations must be two DP++ and one LVDS/eDP)



### Note

1. DDI2 is not supported if VGA is enabled.
2. Display combination for variants with VGA support must be 1x DP++, 1x VGA and 1x LVDS/eDP

The table below shows the supported display combinations and resolutions.

Table 8 Display Combination (U-processor line)

	Display 1 (DDI1)		Display 2 (DDI2)		Display 3	
	Interface	Max. Resolution	Interface	Max. Resolution	Interface	Max. Resolution
Option 1	DP	4096x2304 @ 60 Hz, 24 bpp	DP	4096x2304 @ 60 Hz, 24 bpp	LVDS	1920x1200 @ 60 Hz (dual LVDS mode)
	Or TMDS	4096x2160 @ 24 Hz, 24 bpp	Or TMDS	4096x2160 @ 24 Hz, 24 bpp	Or eDP	4096x2304 @ 60 Hz, 24 bpp
Option 2	DP	4096x2304 @ 60 Hz, 24 bpp	VGA (BOM option)	1920x1200 @ 60 Hz	LVDS	1920x1200 @ 60 Hz (dual LVDS mode)
	Or TMDS	4096x2160 @ 24 Hz, 24 bpp			Or eDP	4096x2304 @ 60 Hz, 24 bpp



### 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.

---

### 5.1.3.1 DisplayPort (DP)

The conga-TC170 supports the following features:

- up to two DP ports
- VESA DisplayPort Standard 1.2
- data rate of 1.62 GT/s, 2.97 GT/s and 5.4 GT/s on 1, 2 or 4 data lanes
- up to 4096x2304 resolutions at 60 Hz
- several audio formats
- maximum of two independent DP displays

### 5.1.3.2 LVDS/eDP

The conga-TC170 offers an LVDS interface with optional eDP overlay on the A–B connector. The LVDS interface provides LVDS signals by default, but can optionally support eDP signals (assembly option). The LVDS interface supports:

- single or dual channel LVDS (color depths of 18 bpp or 24 bpp)
- integrated flat panel interface with clock frequency up to 112 MHz
- VESA and OpenLDI LVDS color mappings
- automatic panel detection via Embedded Panel Interface based on VESA EDID™ 1.3
- resolution up to 1920x1200 in dual LVDS channel mode



#### Note

*The LVDS/eDP interface does not support both LVDS and eDP signals at the same time.*

### 5.1.3.3 VGA

The Intel® Skylake ULT SoC does not natively support VGA interface. However, the conga-TC170 can support this interface by integrating an optional DisplayPort to VGA adapter chip.



#### Note

1. DDI2 is not supported if VGA is enabled.
2. For VGA support, you need a customized conga-TC170 variant.

---

## 5.1.4 SATA

The conga-TC170 offers three SATA interfaces (SATA 0-2) on the A–B connector. The interfaces support:

- independent DMA operation
- SATA Specification Rev. 3.2 with data transfer rates up to 6.0 Gb/s
- AHCI mode using memory space and RAID mode
- hot-plug detect when operating in non-native IDE mode



### Note

*The interface does not support legacy mode using I/O space.*

## 5.1.5 USB

The conga-TC170 offers eight USB 2.0 interfaces on the A–B connector and four SuperSpeed signals on the C–D connector. The xHCI host controller supports:

- USB 3.0 specification
- SuperSpeed, High-Speed, Full-Speed and Low-Speed USB signaling
- data transfers of up to 5 Gbps
- supports USB debug port on all USB 3.0 capable ports

## 5.1.6 Gigabit Ethernet

The conga-TC170 offers a Gigabit Ethernet interface via an onboard Intel® i219-LM Phy. The interface supports full-duplex operation at 10/100/1000 Mbps and half-duplex operation at 10/100 Mbps.



### Note

1. The GBE0\_LINK# output is not active during a 10 Mb connection. It is only active during a 100 Mb or 1 Gb connection. This is a limitation of Ethernet Phy since it has only three LED outputs—ACT#, LINK100# and LINK1000#.
2. The GBE0\_LINK# signal is a logic AND of the GBE0\_LINK100# and GBE0\_LINK1000# signals on the conga-TC170 module.

---

## 5.1.7 Audio

The conga-TC170 provides an interface that supports the connection of High Definition Audio codecs.

## 5.1.8 LPC Bus

The conga-TC170 offers the LPC (Low Pin Count) bus through the Intel® 100 Series PCH-LP. For information about the decoded LPC addresses, see section 9.1.1 “LPC Bus”.

## 5.1.9 I<sup>2</sup>C Bus

The I<sup>2</sup>C 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 I<sup>2</sup>C bus that has the maximum I<sup>2</sup>C bandwidth.

## 5.1.10 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.

## 5.1.11 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 1 Mbps and can operate in low-speed, full-speed and high-speed modes. The UART interfaces are routed to the A-B connector and require congatec driver to function.



### Note

*The UART interfaces do not support legacy COM port emulation.*

## 5.1.12 GPIOs

The conga-TC170 offers General Purpose Input/Output signals on the A-B connector.

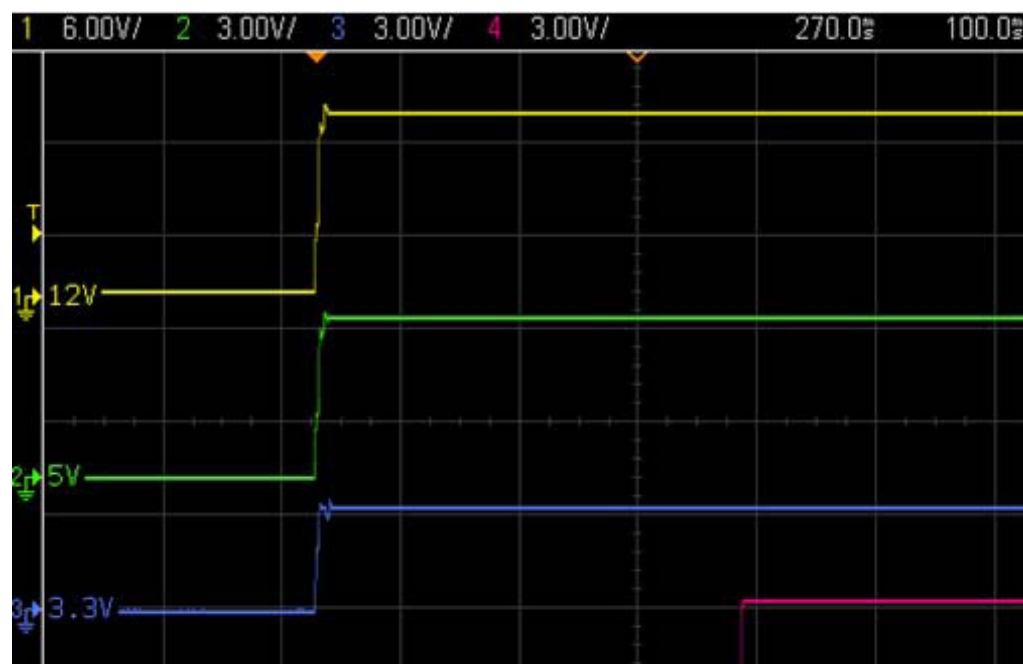
## 5.1.13 Power Control

### 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.

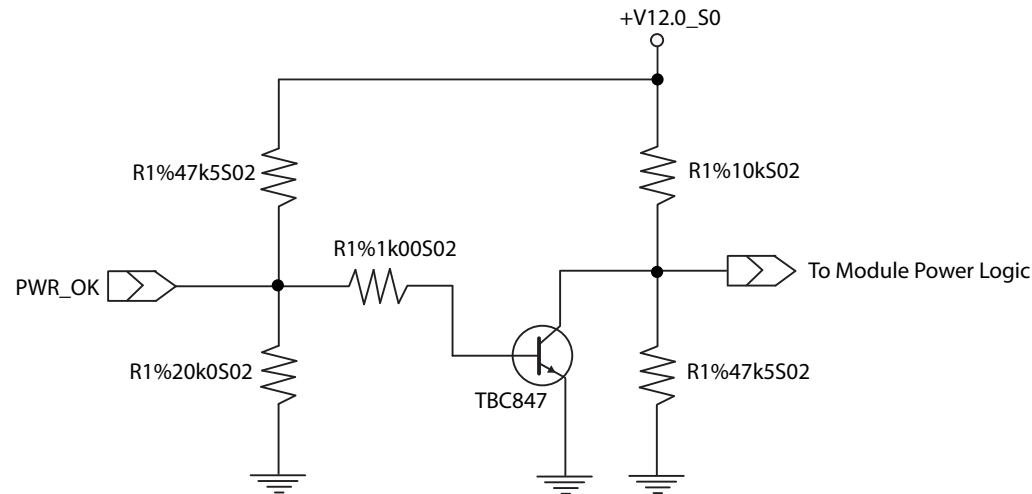
Carrier board hardware must drive this signal low until all power rails and clocks are stable. Releasing PWR\_OK too early or not driving it low at all can cause numerous boot up problems. It is a good design practice to delay the PWR\_OK signal a little (typically 100ms) after all carrier board power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

A sample screenshot is shown below:



*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 3.3 V 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 0.8 V when the 12 V 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 1 kΩ resistor to the carrier board 3.3 V power rail.

With this solution, it must be ensured that by the time the 3.3 V 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. To accomplish this, the signal must be inverted with an inverter or 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 for connecting 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<sub>SB</sub> using a 10 kΩ 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.

## Power Supply Implementation Guidelines

The 12 V input power is the sole operational power source for the conga-TC170. The other voltages required are generated internally on the module using onboard voltage regulators.



### Note

*When designing a power supply for a conga-TC170 application, be aware that the system may malfunction when a 12 V power supply that produces non-monotonic voltage is used to power the system up. Though this problem is rare, it has been observed in some mobile power supply applications.*

*This problem occurs because some internal circuits on the module (e.g. clock-generator chips) 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, thereby resulting in a malfunction.*

*To ensure this problem does not occur, observe the power supply rise waveform through an oscilloscope, during the power supply qualification phase. This will help to determine if the rise is indeed monotonic and does not have any dips. For more information, see the “Power Supply Design Guide for Desktop Platform Form Factors” document at [www.intel.com](http://www.intel.com).*

---

## 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 7.2 "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.

---

## 6 Additional Features

---

### 6.1 eMMC 5.0

The conga-TC170 offers an optional eMMC 5.0 flash onboard. Changes to the onboard eMMC may occur during the lifespan of the module in order to keep up with the rapidly changing eMMC technology.

The performance of the newer eMMC may vary depending on the eMMC technology.



#### Note

*For adequate operation of the eMMC, ensure that at least 15 % of the eMMC storage is reserved for vendor-specific functions."*

### 6.2 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 I<sup>2</sup>C 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.

#### 6.2.1 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.

#### 6.2.2 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 "Watchdog Submenu" of this document and application note AN3\_Watchdog.pdf on the congatec GmbH website at [www.congatec.com](http://www.congatec.com).



#### Note

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

---

### 6.2.3 I<sup>2</sup>C Bus

The conga-TC170 supports I<sup>2</sup>C bus. Thanks to the I<sup>2</sup>C host controller in the cBC, the I<sup>2</sup>C bus is multi-master capable and runs at fast mode.

### 6.2.4 Power Loss Control

The cBC provides the power loss control feature. The power loss control feature determines the behaviour of the system after an AC power loss occurs. This feature applies to systems with ATX-style power supplies which support standby power rail.

The term “power loss” implies that all power sources, including the standby power are lost (G3 state). Once power loss (transition to G3) or shutdown (transition to S5) occurs, the board controller continuously monitors the standby power rail. If the standby voltage remains stable for 30 seconds, the cBC assumes the system was switched off properly. If the standby voltage is no longer detected within 30 seconds, the module considers this an AC power loss condition.

The power loss control feature has three different modes that define how the system responds when standby power is restored after a power loss occurs. The modes are:

- Turn On: The system is turned on after a power loss condition
- Remain Off: The system is kept off after a power loss condition
- Last State: The board controller restores the last state of the system before the power loss condition



#### Note

1. If a power loss condition occurs within 30 seconds after a regular shutdown, the cBC may incorrectly set the last state to “ON”.
2. The settings for power loss control have no effect on systems with AT-style power supplies which do not support standby power rail.
3. The 30 seconds monitoring cycle applies only to the “Last State” power loss control mode.

---

## 6.3 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](http://www.congatec.com) or contact technical support.

The customization features supported are described below:

### 6.3.1 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.

### 6.3.2 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.

### 6.3.3 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.

---

### 6.3.4 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.*

### 6.3.5 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.

## 6.4 congatec Battery Management Interface

In order to facilitate the development of battery powered mobile systems based on embedded modules, congatec GmbH 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 addition 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 the supported Battery Management Interface, contact your local sales representative.

---

## 6.5 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 .

## 6.6 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.

## 6.7 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.

## 7.1 Intel® Processor Features

### 7.1.1 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.

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 activity and therefore does not produce any bus cycles.



#### Note

1. For THERMTRIP# to switch off the system automatically, use an ATX style power supply.
2. The maximum operating temperature for Intel® Xeon, Core™ i7/i5/i3 and Celeron® processors is 100°C.
3. 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.



---

## 7.1.2 Intel® SpeedStep® Technology (EIST)

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.

## 7.1.3 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

1. 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 “Power Consumption” for information about the maximum turbo frequency available for each variant of the conga-TC170.
2. For real-time sensitive applications, disable EIST and Turbo Mode in the BIOS setup to ensure a more deterministic performance.

### 7.1.4 Intel® Virtualization Technology

Intel® Virtualization Technology (Intel® VT) makes a single system appear as multiple independent systems to software. With this technology, multiple, independent operating systems can run simultaneously on a single system. The technology components support virtualization of platforms based on Intel architecture microprocessors and chipsets. Intel® Virtualization Technology for IA-32, Intel® 64 and Intel® Architecture (Intel® VT-x) added hardware support in the processor to improve the virtualization performance and robustness.

RTS Real-Time Hypervisor supports Intel VT and is verified on all current congatec x86 hardware.



#### Note

congatec supports RTS Hypervisor.

### 7.1.5 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.*

## 7.2 ACPI Suspend Modes and Resume Events

The conga-TC170 BIOS supports S3 (Suspend to RAM).

**Table 9 Wake Events**

The table below lists the events that wake the system from S3.

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 unconditionally 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.

## 8 Signal Descriptions and Pinout Tables

The following section describes the signals found on COM Express™ Type VI connectors used for congatec GmbH 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 10 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 Connector Signal Descriptions

Table 11 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	GPIO	B54	GPO1	A109	VCC_12V	B109	VCC_12V
A55	PCIE_TX4+	B55	PCIE_RX4+	A110	GND (FIXED)	B110	GND (FIXED)



\* Not connected on the conga TC170.

Table 12 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	RSVD
C9	USB_SSRX2-	D9	USB_SSTX2-	C64	RSVD	D64	RSVD
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_HPDP	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+ (*)
C37	DDI3_CTRLDATA_AUX- (*)	D37	DDI1_PAIR3-	C92	PEG_RX12- (*)	D92	PEG_TX12- (*)
C38	DDI3_DDC_AUX_SEL (*)	D38	RSVD	C93	GND	D93	GND

Pin	Row C	Pin	Row D	Pin	Row C	Pin	Row D
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	RVSD
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

\* Not supported on the conga TC170.



**Table 13 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_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		
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.



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

Table 14 PCI Express Signal Descriptions (x16 Graphics)

Signal	Pin #	Description	I/O	PU/PD	Comment
PEG_RX0+	C52	PCI Express Graphics Receive Input differential pairs. <i>Note: Can also be used as PCI Express Receive Input differential pairs 16 through 31 known as PCIE_RX[16-31] + and -.</i>	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+	D52	PCI Express Graphics Transmit Output differential pairs. <i>Note: Can also be used as PCI Express Transmit Output differential pairs 16 through 31 known as PCIE_TX[16-31] + and -.</i>	O PCIE		Optional x1 or x2 PEG port (requires re-routing of PCIe lanes 5 and/or 6)
PEG_TX0-	D53				
PEG_TX1+	D55				
PEG_TX1-	D56				
PEG_TX2+	D58				
PEG_TX2-	D59				
PEG_TX3+	D61				
PEG_TX3-	D62				
PEG_TX4+	D65				
PEG_TX4-	D66				
PEG_TX5+	D68				
PEG_TX5-	D69				
PEG_TX6+	D71				
PEG_TX6-	D72				
PEG_TX7+	D74				
PEG_TX7-	D75				
PEG_TX8+	D78				
PEG_TX8-	D79				
PEG_TX9+	D81				
PEG_TX9-	D82				
PEG_TX10+	D85				
PEG_TX10-	D86				
PEG_TX11+	D88				
PEG_TX11-	D89				
PEG_TX12+	D91				
PEG_TX12-	D92				
PEG_TX13+	D94				
PEG_TX13-	D95				
PEG_TX14+	D98				
PEG_TX14-	D99				
PEG_TX15+	D101				
PEG_TX15-	D102				
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 or x2 PEG port via PCIe lanes 5 and 6. The x1 or x2 PEG port is not available by default. To support this feature, you need a customized conga-TC170 variant (assembly option) .

Table 15 DDI Signal Description

Signal	Pin #	Description	I/O	PU/PD	Comment
DDI1_PAIR0+	D26	Multiplexed with DP1_LANE0+ and TMDS1_DATA2+	O PCIE		
DDI1_PAIR0-	D27	Multiplexed with DP1_LANE0- and TMDS1_DATA2-			
DDI1_PAIR1+	D29	Multiplexed with DP1_LANE1+ and TMDS1_DATA1+	O PCIE		
DDI1_PAIR1-	D30	Multiplexed with DP1_LANE1- and TMDS1_DATA1-			
DDI1_PAIR2+	D32	Multiplexed with DP1_LANE2+ and TMDS1_DATA0+	O PCIE		
DDI1_PAIR2-	D33	Multiplexed with DP1_LANE2- and TMDS1_DATA0-			
DDI1_PAIR3+	D36	Multiplexed with DP1_LANE3+ and TMDS1_CLK+	O PCIE		
DDI1_PAIR3-	D37	Multiplexed with DP1_LANE3- and TMDS1_CLK-			
DDI1_PAIR4+	C25	Multiplexed with SDVO1_INT+			Not supported
DDI1_PAIR4-	C26	Multiplexed with SDVO1_INT-			
DDI1_PAIR5+	C29	Multiplexed with SDVO1_TVCLKIN+			Not supported
DDI1_PAIR5-	C30	Multiplexed with SDVO1_TVCLKIN-			
DDI1_PAIR6+	C15	Multiplexed with SDVO1_FLDSTALL+			Not supported
DDI1_PAIR6-	C16	Multiplexed with SDVO1_FLDSTALL-			
DDI1_HPD	C24	Multiplexed with DP1_HPD and HDMI1_HPD	I 3.3V	PD 1M	
DDI1_CTRLCLK_AUX+	D15	Multiplexed with DP1_AUX+ and HDMI1_CTRLCLK		PD100k	
		DP AUX+ function if DDI1_DDC_AUX_SEL is no connect	I/O PCIE		
		HDMI/DVI I2C CTRLCLK if DDI1_DDC_AUX_SEL is pulled high	I/O OD 3.3V		
DDI1_CTRLDATA_AUX-	D16	Multiplexed with DP1_AUX- and HDMI1_CTRLDATA		PU 100k 3.3V	Boot strap signal (see note below). Enable strap is already populated.
		DP AUX- function if DDI1_DDC_AUX_SEL is no connect	I/O PCIE		
		HDMI/DVI I2C CTRLDATA if DDI1_DDC_AUX_SEL is pulled high	I/O OD 3.3V		
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+	D39	Multiplexed with DP2_LANE0+ and TMDS2_DATA2+	O PCIE		
DDI2_PAIR0-	D40	Multiplexed with DP2_LANE0- and TMDS2_DATA2-			
DDI2_PAIR1+	D42	Multiplexed with DP2_LANE1+ and TMDS2_DATA1+	O PCIE		
DDI2_PAIR1-	D43	Multiplexed with DP2_LANE1- and TMDS2_DATA1-			
DDI2_PAIR2+	D46	Multiplexed with DP2_LANE2+ and TMDS2_DATA0+	O PCIE		
DDI2_PAIR2-	D47	Multiplexed with DP2_LANE2- and TMDS2_DATA0-			
DDI2_PAIR3+	D49	Multiplexed with DP2_LANE3+ and TMDS2_CLK+	O PCIE		
DDI2_PAIR3-	D50	Multiplexed with DP2_LANE3- and TMDS2_CLK-			
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		PD 100k	
		DP AUX+ function if DDI2_DDC_AUX_SEL is no connect	I/O PCIE		
		HDMI/DVI I2C CTRLCLK if DDI2_DDC_AUX_SEL is pulled high	I/O OD 3.3V		

Signal	Pin #	Description	I/O	PU/PD	Comment
DDI2_CTRLDATA_AUX-	C33	Multiplexed with DP2_AUX- and HDMI2_CTRLDATA		PU 100k 3.3V	Boot strap signal (see note below). Enable strap is already populated.
		DP AUX- function if DDI2_DDC_AUX_SEL is no connect	I/O PCIE		
		HDMI/DVI I2C CTRLDATA if DDI2_DDC_AUX_SEL is pulled high	I/O OD 3.3V		
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			Not supported
		DP AUX+ function if DDI3_DDC_AUX_SEL is no connect	I/O PCIE		
		HDMI/DVI I2C CTRLCLK if DDI3_DDC_AUX_SEL is pulled high	I/O OD 3.3V		
DDI3_CTRLDATA_AUX-	C37	Multiplexed with DP3_AUX- and HDMI3_CTRLDATA			Not supported
		DP AUX- function if DDI3_DDC_AUX_SEL is no connect	I/O PCIE		
		HDMI/DVI I2C CTRLDATA if DDI3_DDC_AUX_SEL is pulled high	I/O OD 3.3V		
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

1. 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 8.2 "Boot Strap Signals".
2. The conga-TC170 does not natively support TMDS. A DP++ to TMDS converter (e.g. PTN3360D) needs to be implemented.

**Table 16 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 17 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



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

**Table 18 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		
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 19 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

Signal	Pin #	Description	I/O	PU/PD	Comment
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 20 USB 2.0 Signal Descriptions**

Signal	Pin #	Description	I/O	PU/PD	Comment
USB0+	A46	USB Port 0, data + or D+	I/O		USB 2.0 compliant. Backwards compatible to USB 1.1
USB0-	A45	USB Port 0, data - or D-	I/O		USB 2.0 compliant. Backwards compatible to USB 1.1
USB1+	B46	USB Port 1, data + or D+	I/O		USB 2.0 compliant. Backwards compatible to USB 1.1
USB1-	B45	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.
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 21 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 22 Gigabit Ethernet Signal Descriptions

Gigabit Ethernet	Pin #	Description	I/O	PU/PD	Comment
GBE0_MDI0+	A13	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.
GBE0_MDI0-	A12				
GBE0_MDI1+	A10				
GBE0_MDI1-	A9				
GBE0_MDI2+	A7				
GBE0_MDI2-	A6				
GBE0_MDI3+	A3				
GBE0_MDI3-	A2				
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		
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**

1. The GBE0\_LINK# output is not active during a 10 Mb connection. It is only active during a 100 Mb or 1 Gb connection. This is a limitation of Ethernet Phy since it has only three LED outputs—ACT#, LINK100# and LINK1000#.
2. The GBE0\_LINK# signal is a logic AND of the GBE0\_LINK100# and GBE0\_LINK1000# signals on the conga-TC170 module.

**Table 23 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 8.2 "Boot Strap Signals".

**Table 24 ExpressCard Support Pins Signal Descriptions**

Signal	Pin #	Description	I/O	PU/PD	Comment
EXCD0_CPPE#	A49	ExpressCard capable card request.	I 3.3V	PU 10k 3.3VSB	
EXCD1_CPPE#	B48				
EXCD0_PERST#	A48	ExpressCard Reset	O 3.3V	PU 10k 3.3V	
EXCD1_PERST#	B47				

Table 25 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 26 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		
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 27 Miscellaneous Signal Descriptions

Signal	Pin #	Description	I/O	PU/PD	Comment
I2C_CK	B33	General purpose I <sup>2</sup> C port clock output/input	I/O 3.3V	PU 2K2 3.3VSB	
I2C_DAT	B34	General purpose I <sup>2</sup> C 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.

Signal	Pin #	Description	I/O	PU/PD	Comment
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.



*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 8.2 "Boot Strap Signals".*

**Table 28 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	



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

**Table 29 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. Note: For proper detection, assert a pulse width of at least 16 ms.	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. Note: For proper detection, assert a pulse width of at least 16 ms.	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. Note: For proper detection, assert a pulse width of at least 16 ms.	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. Note: For proper detection, assert a pulse width of at least 16 ms.	I OD 3.3V	PU 10k 3.3VSB	

Table 30 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 31 Module Type Definition Signal Description

Signal	Pin #	Description				I/O	Comment
TYPE0#	C54	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).				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.
TYPE1#	C57						
TYPE2#	D57	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.					
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.				PDS	Not connected to indicate "Pinout R2.0".
		TYPE10#					
		NC PD 12V		Pinout R2.0 Pinout Type 10 pull down to ground with 4.7k resistor 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.					

Table 32 Power and GND Signal Descriptions

Signal	Pin #	Description	I/O	PU/PD	Comment
VCC_12V	A104-A109 B104-B109 C104-C109 D104-D109	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 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		

## 8.2 Boot Strap Signals

Table 33 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-	D16	Multiplexed with DP1_AUX- and HDMI1_CTRLDATA		PU100k 3.3V	DDI1_CTRLDATA_AUX- is a boot strap signal (see caution statement below)
DP1_AUX-		DP AUX- function if DDI1_DDC_AUX_SEL is no connect	I/O PCIE		
HDMI_CTRLDATA		HDMI/DVI I2C CTRLDATA if DDI1_DDC_AUX_SEL is pulled high	I/O OD 3.3V		
DDI2_CTRLDATA_AUX-	C33	Multiplexed with DP2_AUX- and HDMI2_CTRLDATA		PU100k 3.3V	DDI2_CTRLDATA_AUX- is a boot strap signal (see caution statement below)
DP2_AUX-		DP AUX- function if DDI2_DDC_AUX_SEL is no connect	I/O PCIE		
HDM2_CTRLDATA		HDMI/DVI I2C CTRLDATA if DDI2_DDC_AUX_SEL is pulled high	I/O OD 3.3V		



### Caution

1. 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.
2. 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.



*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 34 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 to the PCI Express slot on the carrier board.
  3. The table represents a case when a single functional 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 I<sup>2</sup>C

There are no onboard resources connected to the I<sup>2</sup>C 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.



*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
BIOS Information		
Main BIOS Version	No option	Displays the main BIOS version
OEM BIOS Version	No option	Displays the additional OEM BIOS version (blank by default)
Build Date	No option	Displays the date the BIOS was built
Board Information		
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
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 Time	Hour:Minute:Second	Displays the current system time. <b>Note:</b> The time is in 24-hour format

Feature	Options	Description
System Date	Day of week, month/day/year	Displays the current system date. <b>Note:</b> The date is in month-day-year format
System Time	Hour:Minute:Second	Displays the current system time. <b>Note:</b> 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		
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		
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				
	LPC Generic I/O Range Decode				
	GPI IRQ Configuration				
	ACPI				
	Intel® ICC				
	PCH-FW Configuration				
	SMART Settings				
	Super IO				
	Serial Port Console Redirection				
	CPU				
	SATA Configuration				
	Acoustic Management				
	PCI Configuration				
	PCI Express Configuration				
	PEG Port Configuration				
	UEFI Network Stack				
	CSM & Option ROM Control				
	NVMe Configuration				
	SDIO Configuration				
	USB				
	Diagnostic Settings				
	GPIO Configuration				

Main	Advanced	Chipset	Boot	Security	Save & Exit
	Board Controller Command Control				
	PC Speaker				



1. The Intel Ethernet Connection (H) I219-LM and Driver Health submenus are not displayed if the UEFI Network Stack is set to "disabled".
2. The PCH-FW submenu is not displayed if the feature is disabled.

## 10.4.1 Graphics Submenu

Feature	Options	Description
Primary Display	<b>Auto</b> IGD PEG PCI/PCIe	Select primary graphics adapter to be used during boot up: 'Auto' - The system selects the primary graphics adapter 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
Primary PEG	<b>Auto</b> PEG1 PEG2	Select which graphics device should be Primary PEG 'Auto' selects PEG 0 as primary PEG
Primary PCIe	<b>Auto</b> PCIe1 PCIe2 PCIe3 PCIe4 PCIe5 PCIe6 PCIe7	Select which graphics device should be Primary PCIe 'Auto' selects PCIe 0 as primary PCIe
Internal Graphics Device	<b>Auto</b> Disabled Enabled	Set IGD to 'Auto', 'Disabled', or 'Enabled'
Primary IGD Boot Display Device	<b>Auto</b> 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 <b>Note:</b> 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	<b>Disabled</b> CRT LFP EFP EFP2 EFP3	Select the Secondary IGD display device(s) used for boot up <b>Note:</b> 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 <b>Integrated LVDS</b> eDP	Select active local flat panel configuration
Always Try Auto Panel Detect	<b>No</b> 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	<b>Auto</b> 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 <b>Note:</b> Customized EDID™ utilizes an OEM defined EDID™ data set stored in the BIOS flash device
Backlight Inverter Type	None <b>PWM</b> 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	<b>Normal</b> Inverted	Set PWM inverter polarity
PWM Inverter Frequency (Hz)	<b>200</b> - 40000	Set the PWM inverter frequency in Hertz

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

Feature	Options	Description
DisplayPort Spread Spectrum Clock	<b>Disabled</b> Enabled	Enable or disable SSC for DisplayPort. Only valid if the attached DisplayPort panel supports SSC
► Display Interface Signal Integrity Settings	Submenu	Opens the 'Display Interface Signal Integrity Settings submenu
Graphics Turbo IMON Current	<b>31</b> (more values)	Enter the value for the graphics turbo IMON current. Supported values are between 14 - 31
Max. GPU Frequency	<b>Default</b> 800 MHz 700 MHz 600 MHz 500 MHz	Allows to limit the maximum frequency of the integrated graphics engine
GTT Size	2MB 4MB <b>8MB</b>	Select the GTT Size
Aperture Size	128MB <b>256MB</b> 512MB 1024MB 2048MB 4096MB	Select the aperture size Note: To use this feature, disable CSM support Above 4GB MMIO, BIOS assignment is automatically enabled when selecting 2048MB aperture
IGD Pre-Allocated Graphics Memory	<b>32M</b> 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 <b>256M</b> 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 <b>Note:</b> Refer to the DVMT 5.0 specification for more detailed information

Feature	Options	Description
Gfx Low Power Mode	<b>Disabled</b> Enabled	This option applies only to SFF
VDD Enable	Disabled <b>Enabled</b>	Enable or disable VDD in the BIOS
PM Support	<b>Disabled</b> Enabled	Enable or disable PM support
RC6 (Render Standby)	Disabled <b>Enabled</b>	Check to enable render standby support
PAVP Enable	Disabled <b>Enabled</b>	Enable or disable PAVP
Cdynmax Clamping Enable	Disabled <b>Enabled</b>	Enable or disable Cdynmax Clamping
Cd Clock Frequency	337.5 MHz 450 MHz 540 MHz <b>675 MHz</b>	Select the highest Cd clock frequency the platform supports

#### 10.4.1.1 Display Interface Signal Integrity Settings Submenu

Feature	Options	Description
HDMI 1 Level Shifter Config	400mV/0.0dB 400mV/3.5dB 400mV/6.0dB 600mV/0.0dB 600mV/2.0dB 600mV/4.5dB 800mV/0.0dB <b>800mV/2.0dB</b> 1000mV/2.0dB 1200mV/0.0dB	Specifies HDMI level shifter configuration
HDMI 2 Level Shifter Config	400mV/0.0dB 400mV/3.5dB 400mV/6.0dB 600mV/0.0dB 600mV/2.0dB 600mV/4.5dB 800mV/0.0dB <b>800mV/2.0dB</b> 1000mV/2.0dB 1200mV/0.0dB	Specifies HDMI level shifter configuration

Feature	Options	Description
HDMI 3 Level Shifter Config	400mV/0.0dB 400mV/3.5dB 400mV/6.0dB 600mV/0.0dB 600mV/2.0dB 600mV/4.5dB 800mV/0.0dB <b>800mV/2.0dB</b> 1000mV/2.0dB 1200mV/0.0dB	Specifies HDMI level shifter configuration
DisplayPort 1 Trace Lenght	<b>Default</b> Short Long	Determines the DP trace lenght from the silicon to the DP outport port
DisplayPort 2 Trace Lenght	<b>Default</b> Short Long	Determines the DP trace lenght from the silicon to the DP outport port
DisplayPort 3 Trace Lenght	<b>Default</b> Short Long	Determines the DP trace lenght from the silicon to the DP outport port
DDI x IBoost	<b>Disabled</b> Enabled	This setting, when enabled, will activate the IBoost feature for the selected port on all the VSwing/pre-emphasis levels
Magnitude for DP	<b>0x1</b> 0x3 0x7	Selects the supported IBoost magnitude level
Magnitude for HDMI	0x1 0x3 <b>0x7</b>	Selects the supported IBoost magnitude level

## 10.4.2 Watchdog Submenu

Feature	Options	Description
POST Watchdog	<b>Disabled</b> 30sec 1min 2min 5min 10min 30min	Select the timeout value for the POST watchdog <b>Note:</b> The watchdog is only active during the system POST and provides a facility to prevent errors during boot up by performing a reset

Feature	Options	Description
Stop Wdog for User Interaction	No <b>Yes</b>	Select whether the POST watchdog should be stopped during the popup boot selection menu or while waiting for the setup password
Stop Wdog for Password Entry	No <b>Yes</b>	Select whether the POST watchdog should be stopped while waiting for the setup password for password entry
Runtime Watchdog	<b>Disabled</b> 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 <b>Note:</b> This watchdog will be initialized just before the operating system starts booting
Delay	<b>Disabled</b> 10sec 30sec 1min 2min 5min 10min 30min	Select the delay time before the runtime watchdog is activated <b>Note:</b> This feature may be used to ensure that the operating system has enough time to load
Event 1	ACPI Event <b>Reset</b> 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	<b>Disabled</b> ACPI Event Reset Power Button	Select the type of event that will be generated when timeout 2 is reached
Event 3	<b>Disabled</b> ACPI Event Reset Power Button	Select the type of event that will be generated when timeout 3 is reached
Timeout 1	1sec 2sec 5sec 10sec <b>30sec</b> 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

Feature	Options	Description
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



*In ACPI mode, the “Watchdog ACPI Event” handler cannot 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	<b>Disabled</b> Enabled	Enable or disable module serial port 0
I/O Base Address	3F8h 2F8h 220h 228h 238h 2E8h 338h <b>3E8h</b>	Set serial port base address
Interrupt	None IRQ3 IRQ4 <b>IRQ5</b> IRQ6 IRQ14 IRQ15	Set serial port interrupt
PNP ID	None PNP0501 <b>CGT0501</b>	Set serial port ACPI ID

Feature	Options	Description
Baudrate	<b>2400</b> 4800 9600 19200 38400 57600 115200	Set serial port initial baudrate
Serial Port 1	<b>Disabled</b> Enabled	Enable or disable module serial port 1
I/O Base Address	3F8h 2F8h 220h 228h 238h <b>2E8h</b> 338h 3E8h	Set serial port base address
Interrupt	None IRQ3 IRQ4 IRQ5 <b>IRQ6</b> IRQ14 IRQ15	Set serial port interrupt
PNP ID	None PNP0501 CGT0501 <b>CGT0502</b>	Set serial port ACPI ID
Baudrate	<b>2400</b> 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 12 V standard 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 12 V standard voltage
CPU Fan Speed	No option	Displays the CPU Fan Speed in RPM
Fan PWM Frequency Mode	Low Frequency <b>High Frequency</b>	Select the fan PWM base frequency mode: 'Low Frequency' - 11.0 to 88.2Hz 'High Frequency' - 1k to 63kHz
Fan PWM Frequency	11.0 Hz, 14.7 Hz, 22.1 Hz, 29.4 Hz, <b>35.3 Hz</b> , 44.1 Hz, 58.8 Hz, 88.2 Hz	Select fan PWM base frequency (11.0Hz-88.2Hz) (Only visible in low frequency mode)
Fan PWM Frequency (kHz)	1-63 Default: <b>31</b>	Select fan PWM base frequency (1kHz-63kHz) (Only visible in high frequency mode)
Pulses Per Revolution	1 <b>2</b> 3 4	Select the number of pulses per revolution generated by the attached fan
Fan Speed Update Interval (ms)	100ms ----1000ms	A longer update interval lets the fan adjust slower to temperature changes and generate less noise
Fan Speed Stepping Width	1%,2%, 4%, 8%, 16%, 32%, 64%, <b>100%</b>	Defines how much the output value is adjusted to a new set point within one update interval
Default Fan Speed	0%, 10%, 25%, 40%, 50%, 60%, 75%, 90%, <b>100%</b>	Choose the fan speed in percent of the maximum supported speed which is valid if the automatic fan speed control has been disabled
Automatic Fan Speed Control	Disabled <b>Enabled</b>	Enable or disable automatic fan speed control
Fan Control Temperature	<b>CPU Temperature</b> Board Temperature	Choose the temperature sensor used for automatic fan speed control
Lower Temperature Threshold	10°C, 20°C, 30°C, 40°C, <b>50°C</b> , 60°C, 70°C, 80°C, 90°C	Set the temperature which defines the lower limit of the control range
Upper Temperature Threshold	20°C, 30°C, 40°C, 50°C, 60°C, 70°C, <b>80°C</b> , 90°C, 100°C	Set the temperature which defines the upper limit of the control range
Minimum Fan Speed	Fan Off, 10%, 15%, 20%, 25%, 30%, 35%, 40%, 45%, 50%, 55%, 60%, 65%, 70%, 75%, 80%, 85%, 90%, 95%	Choose the fan speed to be set if the temperature is below the lower temperature limit

Feature	Options	Description
Lower Temperature Fan Speed	Fan Off, 10%, 15%, 20%, 25%, 30%, 35%, 40%, 45%, 50%, 55%, <b>60%</b> , 65%, 70%, 75%, 80%, 85%, 90%, 95%	Choose the fan speed to be set if the temperature is within the lower area of the control range
Upper Temperature Fan Speed	Fan Off, 10%, 15%, 20%, 25%, 30%, 35%, 40%, 45%, 50%, 55%, 60%, 65%, 70%, 75%, <b>80%</b> , 85%, 90%, 95%	Choose the fan speed to be set if the temperature is within the upper area of the control range
Maximum Fan Speed	10%, 15%, 20%, 25%, 30%, 35%, 40%, 45%, 50%, 55%, 60%, 65%, 70%, 75%, 80%, 85%, 90%, 95%, <b>100%</b>	Choose the fan speed to be set if the temperature exceeds the upper temperature limit



For more information about fan speed control settings, refer to *congatec technical note CTN20180425.pdf*.

## 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	<b>Auto Negotiated</b> 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	<b>N/A</b> 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	<b>Healthy</b>	Provides Health Status for the drivers/controllers

#### 10.4.7 Trusted Computing Submenu

Feature	Options	Description
Security Device Support	Disable <b>Enable</b>	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
Pending Operation	<b>None</b> TPM Clear	Schedule an operation for the security device
Platform Hierarchy	Disabled <b>Enabled</b>	Enable or disable Platform Hierarchy
Storage Hierarchy	Disabled <b>Enabled</b>	Enable or disable Storage Hierarchy
Endorsement Hierarchy	Disabled <b>Enabled</b>	Enable or disable Endorsement Hierarchy
TPM 2.0 UEFI Spec Version	TCG_1_2 <b>TCG_2</b>	Select the TCG2 spec version support
Physical Presence Spec Version	1.2 <b>1.3</b>	Select the PPI spec version support
Device Select	TPM1.2 TPM2.0 <b>Auto</b>	Auto supports both with the default set to TPM2.0 devices. If TPM2.0 device is not found, TPM1.2 devices will be enumerated



## 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	<b>Disabled</b> 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	<b>0</b>	Specify wake up hour. For example: Enter 3 for 3am and 15 for 3pm
Wake up minute	<b>0</b>	Specify wake up minute
Wake up second	<b>0</b>	Specify wake up second

### 10.4.9 LPC Generic I/O Range Decode Submenu

Feature	Options	Description
LPC Generic I/O Range Decode 2	Disabled <b>Enabled</b>	Enable LPC generic I/O decode range register
Base IO Address	<b>A00</b>	Base I/O address of the LPC decode range (100h – FFFh)
Length	4 Bytes, 8 Bytes, 16 Bytes, <b>32 Bytes</b> , 64 Bytes, 128 Bytes, 256 Bytes	Length of the LPC decode range
LPC Generic I/O Range Decode 3	<b>Disabled</b> Enabled	Enable LPC generic I/O decode range register
Base IO Address	<b>100</b>	Base I/O address of the LPC decode range (100h – FFFh)
Length	4 Bytes, 8 Bytes, 16 Bytes, 32 Bytes, 64 Bytes, 128 Bytes, 256 Bytes	Length of the LPC decode range
LPC Generic I/O Range Decode 4	<b>Disabled</b> Enabled	Enable LPC generic I/O decode range register
Base IO Address	<b>100</b>	Base I/O address of the LPC decode range (100h – FFFh)
Length	4 Bytes, 8 Bytes, 16 Bytes, 32 Bytes, 64 Bytes, 128 Bytes, 256 Bytes	Length of the LPC decode range
Game Port Decoding	Disabled <b>Enabled</b>	Enable address range 200h-20Fh I/O decoding on LPC bus

Feature	Options	Description
Reserve Resources in ACPI	Disabled <b>Enabled</b>	Reserve the LPC I/O resources in ACPI. A PNP0C02 device consuming the selected resources will be reported to the OS
LPC COM Port Decoding 1	<b>Disabled</b> Enabled	Enable LPC COM port I/O decoding
I/O Base Address	<b>3F8h</b> , 2F8h, 220h, 228h, 238h, 2E8h, 338h, 3E8h	Select COM port I/O base address
Reserve Legacy Interrupt	<b>None</b> , IRQ3, IRQ4, IRQ5, IRQ6, IRQ10, IRQ11, IRQ14, IRQ15	The interrupt reserved here will not be assigned to any PCI or PCI Express device and thus might be available for a legacy LPC bus device
LPC COM Port Decoding 2	<b>Disabled</b> Enabled	Enable LPC COM port I/O decoding
I/O Base Address	3F8h, <b>2F8h</b> , 220h, 228h, 238h, 2E8h, 338h, 3E8h	Select COM port I/O base address
Reserve Legacy Interrupt	<b>None</b> , IRQ3, IRQ4, IRQ5, IRQ6, IRQ10, IRQ11, IRQ14, IRQ15	The interrupt reserved here will not be assigned to any PCI or PCI Express device and thus might be available for a legacy LPC bus device
Reserve Legacy Interrupt 1	<b>None</b> , IRQ3, IRQ4, IRQ5, IRQ6, IRQ7, IRQ10, IRQ11, IRQ12, IRQ14, IRQ15	The interrupt reserved here will not be assigned to any PCI or PCI Express device and thus might be available for a legacy LPC bus device
Reserve Legacy Interrupt 2	<b>None</b> , IRQ3, IRQ4, IRQ5, IRQ6, IRQ7, IRQ10, IRQ11, IRQ12, IRQ14, IRQ15	The interrupt reserved here will not be assigned to any PCI or PCI Express device and thus might be available for a legacy LPC bus device

## 10.4.10 GPI IRQ Configuration Submenu

Feature	Options	Description
IRQ on GPIx (x = 0 to 3)	<b>Disabled</b> Enabled	Enables the GPIx to cause an IRQ
IRQ Select	<b>None</b> , IRQ3, IRQ4, IRQ5, IRQ6, IRQ7, IRQ8, IRQ9, IRQ10, IRQ11, IRQ12, IRQ13, IRQ14, IRQ15	Select the IRQ that should be triggered

## 10.4.11 ACPI Submenu

Feature	Options	Description
Enable ACPI Auto Configuration	<b>Disabled</b> Enabled	Enable or disable BIOS ACPI auto configuration
Hibernation Support	Disabled <b>Enabled</b>	Enable or disable system's ability to hibernate (operating system S4 sleep state) <b>Note:</b> Ensure that your operating system supports this feature if you want to use it

Feature	Options	Description
ACPI Sleep State	Suspend Disabled <b>S3 (Suspend to RAM)</b>	Select the state used for ACPI system sleep/suspend
Lock Legacy Resources	<b>Disabled</b> Enabled	Enable or disable locking of legacy resources
S3 Video Repost	<b>Disabled</b> Enabled	Enable or disable video BIOS re-post on S3 resume <b>Note:</b> Enable this feature if it is required by your operating system
ACPI Low Power S0 Idle	<b>Disabled</b> Enabled	Enable or disable ACPI low power S0 idle support
Automatic Critical Trip Point	Disabled <b>Enabled</b>	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 <b>100 C</b> 103 C 111 C 119 C 127 C	Select the temperature threshold at which the ACPI aware operating system performs a critical shutdown <b>Note:</b> Only visible if Automatic Critical Trip Point is set to 'Disabled'
ACPI 3.0 T-States	<b>Disabled</b> Enabled	Enable or disable ACPI 3.0 T-States
Native PCI Express Support	Disabled <b>Enabled</b>	Enable or disable native OS PCI Express support
Native ASPM	<b>Disabled</b> Enabled	Enabled = The OS will control the ASPM support of the PCI Express device Disabled = The BIOS will control the ASPM support of the PCI Express device
BDAT ACPI Table Support	<b>Disabled</b> Enabled	Enables support for the BDAT ACPI table
ACPI Debug	<b>Disabled</b> Enabled	Opens a memory buffer for storing debug strings. Use method ADBG to write strings to buffer
Lid Button Support	<b>Disabled</b> Enabled	If this feature is enabled, the COM Express LID# signal acts as ACPI lid
Sleep Button Support	<b>Disabled</b> Enabled	If this feature is enabled, the COM Express SLEEP# signal acts as ACPI sleep button

## 10.4.12 Intel® ICC Submenu

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

## 10.4.13 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 <b>Enabled</b>	Enable to set ME to Soft Temporary Disabled
fTPM Switch Selection	<b>GPDMA Work-Around</b> MSFT QFE Solution	Selects the desired fTPM solution to be used
TPM Device Selection	<b>dTPM 1.2</b> PTT	Select TPM device: 'PTT' - Enables PTT and disables dTPM in SkuMgr 'dTPM 1.2' - Enables dTPM 1.2 and disables PTT in SkuMgr <b>Warning:</b> 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	<b>Disabled</b> Enabled	Enable or disable Me FW Image Re-Flash function

## 10.4.14 SMART Settings Submenu

Feature	Options	Description
SMART Self Test	<b>Disabled</b> Enabled	Run SMART self test on all HDDs during POST

## 10.4.15 Super IO Submenu

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



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



## 10.4.16 Serial Port Console Redirection Submenu

Feature	Options	Description
COMx Console Redirection	<b>Disabled</b> Enabled	Enable or disable serial port x console redirection
▶ Console Redirection Settings	Submenu	Opens the console redirection configuration submenu
▶ Legacy Console Redirection Settings	Submenu	Opens the Legacy Console Redirection Settings submenu
Serial Port for Out-of-Band Management / Windows Emergency Management Services (EMS) Console Redirection	<b>Disabled</b> 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 submenu



*The Serial Port Console Redirection can be enabled (functional) only if an external Super I/O offering UARTs has been implemented on the carrier board or with the onboard Serial Ports being enabled.*

### 10.4.16.1 Console Redirection Settings Submenu

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

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



*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.*

## 10.4.17 CPU Submenu

Feature	Options	Description
► CPU Information	Submenu	
Set Boot Freq Ratio	<b>255</b> (more values)	Range: 4 – 28. If out of range ratio, maximum ratio is used. This sets the boot ratio. Non-ACPI OSes will use this ratio
Hyper-Threading	Disabled <b>Enabled</b>	Enable or disable hyper-threading technology
Active Processor Cores	<b>All</b> , 1, 2, 3	Set number of cores to be enabled
Overclocking Lock	<b>Disabled</b> Enabled	FLEX_RATIO(194) MSR
Intel Virtualization Technology	Disabled <b>Enabled</b>	When enabled, a VMM can utilize the integrated hardware virtualization support
Hardware Prefetcher	Disabled <b>Enabled</b>	To turn on or off the MLC streamer prefetcher

Feature	Options	Description
Adjacent Cache Line Prefetch	Disabled <b>Enabled</b>	To turn on or off prefetching of adjacent cache lines
CPU AES	Disabled <b>Enabled</b>	Enable or disable CPU Advanced Encryption Standard (AES) instructions
Boot performance mode	Max Battery <b>Max Non-Turbo Performance</b> Turbo Performance	Select the performance state that the BIOS will set before OS handoff
Intel® Speed Shift Technology	Disabled <b>Enabled</b>	Enable or disable Intel(R) Speed Shift Technology support. Enabling will expose the CPPC v2 interface to allow for hardware controlled P-states
Intel® SpeedStep™	Disabled <b>Enabled</b>	Allows more than two frequency ranges to be supported
Turbo Mode	Disabled <b>Enabled</b>	Enable or disable Turbo Mode
TCC Activation Offset	<b>0</b> (more values)	Offset from the Intel factory Thermal Control Circuit (TCC) activation temperature. TCC activation will lower CPU core and graphics core frequency, voltage or both. The factory TCC activation temperature is normally 100C. By entering 10 for TCC offset the TCC will be activated at 90C
P-State Reduction	<b>Disabled</b> by 1 by 2 by 3 by 4 by 5 by 6 by 7 by 8	Limits the maximum non-turbo CPU performance state in an ACPI operating system  <b>Note:</b> Only visible if Intel Speed Shift Technology and Turbo Mode are disabled
Package Power Limit Lock	<b>Disabled</b> Enabled	Enable/Disable locking of Package Power Limit settings. When enabled, PACKAGE_POWER_LIMIT MSR will be locked and a reset will be required to unlock the register
1-Core Ratio Limit Override	<b>0</b> (more values)	This limit is for 1 cores active. 0 means using the factory-configured value
2-Core Ratio Limit Override	<b>0</b> (more values)	This limit is for 2 cores active. 0 means using the factory-configured value
3-Core Ratio Limit Override	<b>0</b> (more values)	This limit is for 3 cores active. 0 means using the factory-configured value
4-Core Ratio Limit Override	<b>0</b> (more values)	This limit is for 4 cores active. 0 means using the factory-configured value
Configurable TDP Boot Mode	<b>Nominal</b> Down Up Deactivate	Configurable TDP Mode as Nominal/Up/Down/Deactivate TDP selection. Deactivate option will set MSR to Nominal and MMIO to Zero
Configurable TDP Lock		Configurable TDP Mode Lock sets the Lock bits on TURBO_ACTIVATION_RATIO and CONFIG_TDP_CONTROL <b>Note:</b> When CTD Lock is enabled Custom ConfigTDP Count will be forced to 1 and Custom ConfigTDP Boot Index will be forced to 0

Feature	Options	Description
CTDP BIOS control	<b>Disabled</b> Enabled	Enables CTDP control via runtime ACPI BIOS methods. This “BIOS only” feature does not require EC or driver support
Platform PL1 Enable	<b>Disabled</b> Enabled	Enable or disable Platform Power Limit 1 programming. If this option is enabled, it activates the PL1 value to be used by the processor to limit the average power of given time window
Platform PL1 Power	<b>0</b> (more values)	Platform Power Limit 1 Power in Milli Watts and step size is 125mW. Any value can be programmed between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). This setting will act as the new PL1 value for the Package RAPL algorithm
Platform PL1 Time Window	<b>0</b> (more values)	Platform Power Limit 1 Time Window value in seconds. The value may vary from 0 to 128. If the value is 0, default values will be programmed. Indicates the time window over which Platform TDP value should be maintained.
Platform PL2 Enable	<b>Disabled</b> Enabled	Enable or disable Platform Power Limit 2 programming. If this option is disabled, BIOS will program the default values for Platform Power Limit 2
Platform PL2 Power	<b>0</b> (more values)	Platform Power Limit 2 Power in Milli Watts and stepsize is 125mW. Any value can be programmed between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). This setting will act as the new PL2 value for the Package RAPL algorithm
CPU C States	<b>Disabled</b> Enabled	Enable or disable CPU C states
Enhanced C1 State	Disabled <b>Enabled</b>	Enable or disable C1E. 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 <b>C1 and C3</b>	Configure C-State Auto Demotion
C-State Un-demotion	Disabled C1 C3 <b>C1 and C3</b>	Configure C-State Un-demotion
Package C State Demotion	Disabled <b>Enabled</b>	Configure C-State demotion
Package C State Undemotion	Disabled <b>Enabled</b>	Configure C-State Un-demotion
CState Pre-Wake	Disabled <b>Enabled</b>	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 <b>AUTO</b>	Package C state limit

Feature	Options	Description
CFG Lock	Disabled <b>Enabled</b>	Configure MSR 0xE2[15], CFG lock bit
Intel® TXT(LT) Support	<b>Disabled</b> Enabled	Enable or disable Intel® TXT(LT) support
Debug Interface	<b>Disabled</b> Enabled	Enable or disable CPU debug feature
Debug Interface Lock	<b>Disabled</b> Enabled	Lock CPU debug feature setting
SW Guard Extensions (SGX)	Disabled Enabled <b>Software Controlled</b>	Enable or disable Software Guard Extensions (SGX)
Select Owner EPOCH input type	<b>No Change in Owner EPOCHs</b> Change to New Random Owner EPOCHs Manual User Defined Owner EPOCHs	Select owner EPOCH mode. Each EPOCH is 64-bit There are three Owner EPOCH modes (Each EPOCH is 64bit): no change in owner epoch, change to new random owner epoch and manually entered by user. After the user enters epoch values manually, the values will not be visible, for security reasons
PRMRR Size	AUTO	

#### 10.4.17.1 CPU Information

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
Hyper Threading 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
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

Feature	Options	Description
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

## 10.4.18 SATA Submenu

Feature	Options	Description
SATA Controller(s)	<b>Enabled</b> Disabled	Enable or disable the onboard SATA controller(s)
SATA Mode Selection	<b>AHCI</b> RAID	Select SATA controller mode <b>Note:</b> RAID option is not supported on all chipsets
SATA RAID ROM	<b>Legacy ROM</b> UEFI Driver Both	Legacy ROM: Legacy option ROM EFI Driver: UEFI Raid Driver Both: Run the legacy Option ROM and UEFI driver
CR#1 - RST Pcie Storage Remapping	Enabled <b>Disabled</b>	Enable or disable RST PCIe storage remapping
CR#1 - Remap Port Selection	<b>Auto</b> Port 9 Port 10 Port 11 Port 12	Select port for RST PCIe storage remapping
CR#2 - RST Pcie Storage Remapping	Enabled <b>Disabled</b>	Enable or disable RST Pcie storage remapping
CR#2 - Remap Port Selection	<b>Auto</b> Port 13 Port 14 Port 15 Port 16	Select port for RST PCIe storage remapping
CR#3 - RST Pcie Storage Remapping	Enabled <b>Disabled</b>	Enable or disable RST PCIe storage remapping
CR#3 - Remap Port Selection	<b>Auto</b> Port 17 Port 18 Port 19 Port 20	Select port for RST PCIe storage remapping

Feature	Options	Description
SATA Test Mode	Enabled <b>Disabled</b>	Only enable this feature for verification measurements
Alternate ID	Enabled <b>Disabled</b>	Enable this feature to report an alternate device ID <b>Note:</b> 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 <b>Disabled</b>	Enable PCH to aggressively enter link power state
SATA Controller Speed	<b>Default</b> Gen1 Gen2 Gen3	Indicates the maximum speed the SATA Controller can support Default = maximum speed Gen1 = 1.5 Gbit/s Gen2 = 3 Gbit/s Gen3 = 6 Gbit/s
Serial ATA Port 0, 1, 2	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
SATA Port	Disabled <b>Enabled</b>	Enable or disable the relevant SATA port
Hot Plug	<b>Disabled</b> Enabled	Enable or disable hot plug support for relevant SATA port
External SATA	<b>Disabled</b> Enabled	Enable or disable external SATA support on relevant SATA port
SATA Power	<b>SATA SSD/HDD</b> SATA DOM	Change the sata power configuration - enable disk on Module
Spin Up Device	<b>Disabled</b> Enabled	Enable this feature to run an initialization sequence for the connected device during startup at relevant SATA port <b>Note:</b> Enable this feature if your hard disk or special (special) solid-state drive requires it
SATA Device Type	<b>Hard Disk Drive</b> Solid State Drive	Select whether the relevant SATA port is connected to solid-state drive or a hard disk drive
Topology	<b>Unknown</b> ISATA, Direct Connect Flex M2	Select the SATA topology
Device Sleep	<b>Disabled</b> Enabled	Enable or disable mSata for RTD3
SATA DEVSLEP Idle Timeout Config	<b>Disabled</b> Enabled	Enable or disable SATA DTIO Config

## 10.4.18.1 Software Feature Mask Configuration

Feature	Options	Description
RAID0	Disabled <b>Enabled</b>	Enable or disable RAID0 feature
RAID1	Disabled <b>Enabled</b>	Enable or disable RAID1 feature
RAID10	Disabled <b>Enabled</b>	Enable or disable RAID10 feature
RAID5	Disabled <b>Enabled</b>	Enable or disable RAID5 feature
Intel® Rapid Recovery Technology	Disabled <b>Enabled</b>	Enable or disable Intel® Rapid Recovery Technology
Option ROM UI and Banner	Disabled <b>Enabled</b>	Enable this feature to display the option ROM user interface <b>Note:</b> No option ROM banner or information are displayed if all disks and RAID volumes are normal
HDD Unlock	Disabled <b>Enabled</b>	If this feature is enabled, the HDD password unlock option is available in the operating system
LED Locate	Disabled <b>Enabled</b>	Enable or disable 'LED Locate'
IRRT Only on eSATA	Disabled <b>Enabled</b>	If this feature is enabled, only Intel® Rapid Recovery Technology (IRRT) volumes can span internal and external SATA (eSATA) drives If this feature is disabled, only RAID volume can span internal and eSATA drives
Smart Response Technology	Disabled <b>Enabled</b>	Enable or disable 'Intel® Smart Response Technology'
Option ROM UI Normal Delay	<b>2 Seconds</b> 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	<b>Disabled</b> Enabled	Enable or disable form for Intel® Rapid Storage Technology



## 10.4.19 Acoustic Management Submenu

Feature	Options	Description
Acoustic Management Configuration	<b>Disabled</b> Enabled	Disable or enable 'Acoustic Management Configuration'
SATA Port 0 Disk drive name Acoustic Mode	<b>Bypass</b> 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	<b>Bypass</b> Quiet Max Performance	Same as at SATA Port 0
SATA Port 2 Disk drive name Acoustic Mode	<b>Bypass</b> Quiet Max Performance	Same as at SATA Port 0
SATA Port 3 Disk drive name Acoustic Mode	<b>Bypass</b> Quiet Max Performance	Same as at SATA Port 0



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

## 10.4.20 PCI Express Configuration Submenu

Feature	Options	Description
PCI Bus Driver Version	No option	
PCI Settings		
PCI Latency Timer	<b>32 PCI Bus Clocks</b> 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 <b>64 PCI Bus Clocks</b> 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	<b>Disabled</b> Enabled	Enable or disable VGA palette registers snooping
PERR# Generation	<b>Disabled</b> Enabled	Enable or disable PCI device to generate PERR#
SERR# Generation	<b>Disabled</b> Enabled	Enable or disable PCI device to generate SERR#
Above 4G Decoding	<b>Disabled</b> Enabled	Enables or disables 64-bit capable devices to be decoded in Above 4G Address Space (only if system supports 64-bit PCI Decoding)
Don't Reset VC-TC Mapping	<b>Disabled</b> Enabled	If the system has Virtual Channels, software can reset traffic class mapping to its default state through virtual channels <b>Note:</b> Enabling this feature will not modify VC resources
BIOS Hot-Plug Support	<b>Disabled</b> Enabled	Enable this feature to allow BIOS build in hot-plug support <b>Note:</b> Use this feature if the operating system does not support PCIe and SHPC hot-plug natively
PCI Buses Padding	Disabled <b>1</b> 2 3 4 5	Padd PCI buses behind the bridge for hot-plug
I/O Resources Padding	Disabled <b>4 K</b> 8 K 16 K 32 K	Select padd PCI I/O resources behind the bridge for hot-plug
MMIO 32 bit Resources Padding	Disabled 1 M 2 M 4 M 8 M <b>16 M</b> 32 M 64 M 128 M	Select padd PCI MMIO 32-bit resources behind the bridge for hot-plug

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

## 10.4.21 PCI Express Configuration Submenu

Feature	Options	Description
PCI Express Clock Gating	<b>Disabled</b> Enabled	Enable or disable PCI Express clock gating for each root port
DMI Link ASPM Processor Side	<b>Disabled</b> Enabled	Enable or disable Active State Power Management of the DMI link on the processor side. DMI link is the main bus between the Processor and Platform Controller Hub (PCH)
Port8xh Decode	<b>Disabled</b> Enabled	Enable or disable Port8xh Decode
Peer Memory Write Enable	<b>Disabled</b> Enabled	Enable or disable Peer Memory Write
Compliance Test Mode	<b>Disabled</b> Enabled	Enable or disable Compliance Test Mode. Enable when using compliance load board
PCIe-USB Glitch W/A	<b>Disabled</b> Enabled	Enable or disable PCIe-USB Glitch W/A for bad USB device(s) connected behind PCIe/PEG port
PCIe Function Swap	<b>Disabled</b> Enabled	Enable or disable PCIe Function Swap. When disabled, it prevents PCIe root port function swap. If any function other than 0th is enabled, 0th will become visible
PCIe Spread Spectrum Clocking	<b>Auto</b> 0.1%, 0.2%, 0.3%, 0.4%, 0.5%, 0.6%, 0.7%, 0.8%, 0.9%, 1.0%, 1.1%, 1.2%, 1.3%, 1.4%, 1.5%, 1.6%, 1.7%, 1.8%, 1.9%, 2.0%	PCIe PLL SSC percentage Auto keeps hardware default, no BIOS override <b>Note:</b> Hardware default is 0.45%
► PCI Express Gen3 Eq Lanes	Submenu	PCI Express Gen3 equalization settings per PCIe lane
► PCI Express Settings	Submenu	Change PCI Express settings
► PCI Express Gen2 Settings	Submenu	Change PCI Express Gen Devices settings
► PCI Express Port 0	Submenu	PCI Express port 0 settings
► PCI Express Port 1	Submenu	PCI Express port 1 settings

Feature	Options	Description
► PCI Express Port 2	Submenu	PCI Express port 2 settings
► PCI Express Port 3	Submenu	PCI Express port 3 settings
► PCI Express Port 4	Submenu	PCI Express port 4 settings
► PCI Express Port 5	Submenu	PCI Express port 5 settings
► PCI Express Port 6	Submenu	PCI Express port 6 settings
► PCI Express Port 7	Submenu	PCI Express port 7 settings

#### 10.4.21.1 PCI Express Gen3 Eq Lanes Submenu

Feature	Options	Description
Override SW EQ Settings	<b>Disabled</b> Enabled	

#### 10.4.21.2 PCI Express Settings Submenu

Feature	Options	Description
PCI Express Device Register Settings		
Relaxed Ordering	<b>Disabled</b> Enabled	Enable or disable PCI Express device relaxed ordering
Extended Tag	<b>Disabled</b> Enabled	Enable or disable Extended Tag. If enabled, a device may use an 8-bit tag field as a requester
No Snoop	Disabled <b>Enabled</b>	Enable or disable PCI Express device 'No Snoop' option
Maximum Payload	<b>Auto</b> 128 Bytes 256 Bytes 512 Bytes 1024 Bytes 2048 Bytes 4096 Bytes	Set maximum payload of PCI Express device or allow system BIOS to select the value
Maximum Read Request	<b>Auto</b> 128 Bytes 256 Bytes 512 Bytes 1024 Bytes 2048 Bytes 4096 Bytes	Set maximum read request size of PCI Express device or allow system BIOS to select the value

Feature	Options	Description
PCI Express Link Register Settings		
ASPM	<b>Disabled</b> Enabled	Enable or disable Active State Power Management settings Warning: Enabling ASPM may cause some PCIe devices to fail
Extended Synch	<b>Disabled</b> Enabled	Enable or disable the generation of extended synchronization patterns
Link Training Retry	<b>Disabled</b> 2 3 5	Defines the number of retry attempts software will take to retrain the link if previous training attempt was unsuccessful
Link Training Timeout (us)	<b>1000</b> (more values)	Defines the number of microseconds software will wait before polling link training bit in the link status register. Value ranges from 10 to 10000 microseconds
Unpopulated Links	<b>Keep Link On</b> Disabled	If set to 'disabled', the software will disable unpopulated PCI Express links in order to save power
Restore PCIe Registers	<b>Disabled</b> Enabled	On non-PCI Express aware operating systems, some devices may not be re-initialized correctly after S3. Setting this mode to 'Enabled' restores PCI Express configuration on S3 resume Warning: Enabling this may cause issues with other hardware after S3 resume

### 10.4.21.3 PCI Express GEN2 Settings Submenu

Feature	Options	Description
PCI Express GEN2 Device Register Settings		
Completion Timeout	<b>Default</b> Shorter Longer Disabled	In device functions that support Completion Timeout programmability, allows system software to modify the Completion Timeout value. Default is between 50 microseconds and 50 milliseconds
ARI Forwarding	<b>Disabled</b> Enabled	If supported by hardware and set to 'Enabled', the downstream port disables its traditional device number field being 00 enforcement when turning a Type1 configuration request in to aType0 configuration request, permitting access to Extended Functions in an ARI device immediately below the port
AtomicOp Requester Enable	<b>Disabled</b> Enabled	If supported by hardware and set to 'Enabled', this function initiates AtomicOp Requests only if Bus Master Enable bit is in the Command Register Set
AtomicOp Egress Blocking	<b>Disabled</b> Enabled	If supported by hardware and set to 'Enabled', outbound AtomicOp Requests via Egress ports will be blocked
IDO Request Enable	<b>Disabled</b> Enabled	If supported by hardware and set to 'Enabled', this permits setting the number of ID-Based Ordering (IDO) bit requests to be initiated
IDO Completion Enable	<b>Disabled</b> Enabled	If supported by hardware and set to 'Enabled', this permits setting the number of ID-Based Ordering (IDO) bit requests to be initiated

Feature	Options	Description
LTR Mechanism Enable	<b>Disabled</b> Enabled	If supported by hardware and set to 'Enabled', this enables the Latency Tolerance Reporting (LTR) Mechanism
End-end TLP Prefix Blocking	<b>Disabled</b> Enabled	If supported by hardware and set to 'Enabled', this function will block forwarding of TLPs containing End-End TLP Prefixes
PCI Express GEN2 Link Register Settings		
Target Link speed	<b>Auto</b> Force to 2.5 GT/s Force to 5.0 GT/s	If supported by hardware and set to 'Force to 2.5 GT/s', for downstream ports, this sets an upper limit on link operational speed by restricting the values advertised by the upstream component in its training sequences. When 'Auto' is selected, hardware initialized data will be used
Clock Power Management	<b>Disabled</b> Enabled	If supported by hardware and set to 'Enabled', the device is permitted to use CLKREQ# signal for power management of link clock
Compliance SOS	<b>Disabled</b> Enabled	If supported by hardware and set to 'Enabled', this will force LTSSM to send SKP Ordered Sets between sequences when sending Compliance Pattern or Modified Compliance Pattern
Hardware Autonomous Width	Disabled <b>Enabled</b>	If supported by hardware and set to 'Disabled', this will disable the hardware's ability to change link width except width size reduction for the purpose of correcting unstable link operation
Hardware Autonomous Speed	Disabled <b>Enabled</b>	If supported by hardware and set to 'Disabled', this will disable the hardware's ability to change link width except width size reduction for the purpose of correcting unstable link operation

#### 10.4.21.4 PCI Express Port 0 - 7 Submenu

Feature	Options	Description
PCI Express Port	Disabled <b>Enabled</b>	Enable or disable the PCI Express Port
Topology	<b>Unknown</b> x1 x4 Sata Express M2	Identify the SATA topology if it is default or ISATA or Flex or DirectConnect or M2
ASPM	<b>Disabled</b> L0s L1 L0sL1 Auto	Enable or disable PCI Express Active State Management settings
Gen3 Eq Phase3 Method	<b>Software Search</b> Hardware Static Coeff.	PCIe Gen3 Equalization Phase 3 method
UPTP	<b>5</b> (more values)	Upstream Port Transmitter Preset

Feature	Options	Description
DPTP	<b>7</b> (more values)	Downstream Port Transmitter Preset
ACS	Disabled <b>Enabled</b>	Enable or disable Access Control Service Extended Capability
URR	<b>Disabled</b> Enabled	Enable or disable PCI Express Unsupported Request Reporting
FER	<b>Disabled</b> Enabled	Enable or disable PCI Express Device Fatal Error Reporting
NFER	<b>Disabled</b> Enabled	Enable or disable PCI Express Device Non-Fatal Error Reporting
CER	<b>Disabled</b> Enabled	Enable or disable PCI Express Device Correctable Error Reporting
CTO	<b>Disabled</b> Enabled	Enable or disable PCI Express Completion Timer TO
SEFE	<b>Disabled</b> Enabled	Enable or disable Root PCI Express System Error or Fatal Error
SENF	<b>Disabled</b> Enabled	Enable or disable Root PCI Express System Error or Non-Fatal Error
SECE	<b>Disabled</b> Enabled	Enable or disable Root PCI Express System Error on Correctable Error
PME SCI	Disabled <b>Enabled</b>	Enable or disable PCI Express PME SCI
Hot Plug	<b>Disabled</b> Enabled	Enable or disable PCI Express hot plug
Advanced Error Reporting	Disabled <b>Enabled</b>	Enable or disable Advanced Error Reporting
PCIe Speed	<b>Auto</b> Gen1 Gen2 Gen3	Select PCI Express port speed
Transmitter Half Swing	<b>Disabled</b> Enabled	Enable or disable Transmitter Half Swing
Detect Non-Compliance Device	<b>Disabled</b> Enabled	Detect Non-Compliance PCI Express Device. If enabled, POST takes longer
Extra Bus Reserved	<b>0</b> (more values)	Extra bus reserved (0-7) for bridges behind this root bridge
Reserved Memory	<b>10</b> (more values)	Reserved memory range for this root bridge

Feature	Options	Description
Prefetchable Memory	<b>10</b> (more values)	Prefetchable memory range for this root bridge
Reserved I/O	<b>4</b> (more values)	Reserved I/O range for this root bridge
PCIe Cp	<b>2</b> (more values)	Gen3 Equalization settings for physical PCIe lane
PCIe Cm	<b>6</b> (more values)	Gen3 Equalization settings for physical PCIe lane
PCIe LTR	Disabled <b>Enabled</b>	Enable or disable PCIe Latency Reporting
PCIe LTR Lock	<b>Disabled</b> Enabled	Enable or disable PCIe LTR Configuration Lock
Snoop Latency Override	Disabled Manual <b>Auto</b>	Snoop Latency Override for PCH PCIe
Snoop Latency Multiplier	1 ns 32 ns <b>1024 ns</b> 32768 ns 1048576 ns 33554432 ns	Snoop latency multiplier for PCH PCIe
Snoop Latency Value	<b>60</b> (more values)	Snoop latency value for PCH PCIe
Non Snoop Latency Override	Disabled Manual <b>Auto</b>	Non Snoop Latency Override for PCH PCIe
Non Snoop Latency Multiplier	1 ns 32 ns <b>1024 ns</b> 32768 ns 1048576 ns 33554432 ns	Non Snoop latency override for PCH PCIe
Force LTR Override	<b>Disabled</b> Enabled	Force LTR Override for PCH PCIE Disabled: LTR override values will not be forced Enable: LTR override values will be forced and LTR messages from the device will be ignored
Non Snoop Latency Value	<b>60</b> (more values)	Non Snoop Latency Value for PCH PCIe



## 10.4.22 UEFI Network Stack Submenu

Feature	Options	Description
UEFI Network Stack	<b>Disabled</b> Enabled	Enable or disable the UEFI network stack
IPv4 PXE Support	Disabled <b>Enabled</b>	Enable or disable IPv4 PXE boot support. If disabled, IPv4 PXE boot option will not be created
IPv6 PXE Support	Disabled <b>Enabled</b>	Enable or disable IPv6 PXE boot support. If disabled, IPv6 PXE boot option will not be created
PXE boot wait time	<b>0</b> (more values)	Set wait time to press ESC key to abort the PXE boot
Media detect count	<b>1</b> (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 <b>Enabled</b>	Enable or disable CSM support
CSM16 Module Version	No option	
Gate A20 Active	<b>Upon Request</b> Always	'Upon Request' - Gate A20 can be disabled with BIOS services 'Always' - Gate A20 cannot be disabled <b>Note:</b> This feature is useful if runtime code above 1MB is executed
Option ROM Messages	<b>Force BIOS</b> Keep Current	Set display mode for option ROMs
INT19 Trap Response	<b>Immediate</b> 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	<b>UEFI and Legacy</b> 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 <b>UEFI ROM Only</b> Legacy ROM Only	This feature controls the execution of UEFI and legacy PXE option ROMs

Feature	Options	Description
Storage Option ROM Launch Policy	Do not launch <b>UEFI ROM Only</b> 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 <b>Legacy ROM Only</b>	This feature controls the execution of UEFI and legacy video option ROMs
Other Option ROM Launch Policy	Do not launch <b>UEFI ROM Only</b> 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

Feature	Options	Description
SD Card or COMx GPIO	SD Card <b>COMx GPIO</b>	SD Card = SD Card signals will be connected and COMx GPIO signals will be not used. COMx GPIO = COM Express (COMx) GPIO signals will be connected and SD Card signals will be not used
UART0 Controller	<b>Disabled</b> Enabled	The SDCard 3.0 Controller, the eMMC 5.0 Controller and some other devices can be enabled only when the UART0 is enabled
SDCard 3.0 Controller	<b>Disabled</b> Enabled	Enable or Disable SCS SDHC 3.0 Controller
eMMC 5.0 Controller	<b>Disabled</b> Enabled	Enable or Disable SCS eMMC 5.0 Controller
eMMC 5.0 HS400 Mode	Disabled <b>Enabled</b>	Enable or Disable SCS eMMC 5.0 HS400 Mode
Driver Strength	<b>33 Ohm</b> 40 Ohm 50 Ohm	Sets I/O driver strength
SDIO Access Mode	No Option	Auto Option: Access SD device in DMA mode if controller supports it, otherwise in PIO mode DMA Option: Access SD device in DMA mode PIO Option: Access SD device in PIO mode

Feature	Options	Description
Detected Device Details	<b>Auto</b> Floppy Forced FDD Hard Disk	Mass storage device emulation type. 'AUTO' enumerates devices less than 530MB as floppies Forced FDD option can be used to force HDD formatted drive to boot as FDD Displayed only if SD Card is detected

## 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	<b>Disabled</b> Enabled	Disable or enable overcurrent protection on all USB ports
USB Precondition	<b>Disabled</b> Enabled	Enable or disable USB Precondition (precondition makes enumeration faster)
XHCI Disable Compliance Mode	<b>FALSE</b> TRUE	Options to disable Compliance Mode 'False' - do not disable compliance mode 'True' - disable compliance mode
XDCI Support	<b>Disabled</b> Enabled	Enable or disable USB OTG device
USB Port Disable Override	<b>Disabled</b> Select Per Port	Selectively enable or disable the corresponding USB port from reporting a device connection to the controller
USB SS Physical Connector #0	Disabled <b>Enabled</b>	
USB SS Physical Connector #1	Disabled <b>Enabled</b>	
USB SS Physical Connector #2	Disabled <b>Enabled</b>	
USB SS Physical Connector #3	Disabled <b>Enabled</b>	
USB HS Physical Connector #0	Disabled <b>Enabled</b>	
USB HS Physical Connector #1	Disabled <b>Enabled</b>	
USB HS Physical Connector #2	Disabled <b>Enabled</b>	
USB HS Physical Connector #3	Disabled <b>Enabled</b>	

USB HS Physical Connector #4	Disabled <b>Enabled</b>	
USB HS Physical Connector #5	Disabled <b>Enabled</b>	
USB HS Physical Connector #6	Disabled <b>Enabled</b>	
USB HS Physical Connector #7	Disabled <b>Enabled</b>	
Legacy USB Support	<b>Enabled</b> 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
External USB Controller Support	Disabled <b>Enabled</b>	Enable or disable BIOS support for external USB controllers
xHCI Hand-off	<b>Enabled</b> Disabled	This feature is a workaround for operating system without xHCI hand-off support <b>Note:</b> If this feature is enabled, the xHCI ownership change should be claimed by the xHCI operating system driver
USB Mass Storage Driver Support	Disabled <b>Enabled</b>	Enable or disable USB mass storage driver support
USB hardware delays and time-outs:		
USB Transfer Timeout	1 sec 5 sec 10 sec <b>20 sec</b>	Select the timeout value for control, bulk, and interrupt transfers
Device Reset Timeout	10 sec <b>20 sec</b> 30 sec 40 sec	Select the USB mass storage device Start Unit command timeout
Device Power-up Delay Selection	<b>Auto</b> 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)	<b>Auto</b> Floppy Forced FDD Hard Disk CD-ROM	Every USB mass storage device that is enumerated by the BIOS will have an emulation type setup option. This option specifies the type of emulation the BIOS has to provide for the device <b>Note:</b> The device's formatted type and the emulation type provided by the BIOS must match for the device to boot properly Select 'Auto' to let the BIOS auto detect the current formatted media If 'Floppy' is selected then the device will be emulated as a floppy drive 'Forced FDD' allows a hard disk image to be connected as a floppy image. Works only for drives formatted with FAT12, FAT16 or FAT32. 'Hard Disk' allows the device to be emulated as hard disk 'CDROM' assumes the CD.ROM is formatted as bootable media, specified by the 'El Torito' Format Specification

## 10.4.27 Diagnostics Settings Submenu

Feature	Options	Description
POST Code Redirection Settings		
Relay Interface	<b>Disabled</b> I2C SMBus BC Diagnostics Console	Select the relay interface to which the POST code will be redirected
Primary Port Addr. Lowbyte (Dec)	0-255 ( <b>128</b> )	Set the address for the primary debug port. The usual address value is 0x80 (i.e. 128 dec lowbyte and 0 highbyte). However, any multiple of 8 is valid for a primary debug port address
Primary Port Addr. Highbyte (Dec)	0-255 ( <b>0</b> )	Set the address for the primary debug port. The usual address value is 0x80 (i.e. 128 dec lowbyte and 0 highbyte). However, any multiple of 8 is valid for a primary debug port address
Relay Device Address (Dec)	0-255 ( <b>226</b> )	Specify the I2C/SMBus device address of e.g. a 7-segment LCD for POST code display. The factory settings for the SparkFun device is 0xE2(226). However, any even device address can be specified
BC Diagnostics Console Settings		
BC Diagnostics Console Interface	<b>Disabled</b> BC AUX Port BC COM Port 0 BC COM Port 1	Select the interface to be used for the congatec Board Controller Diagnostic Console output or disable the diagnostic output
Parity Bit	<b>No Parity</b> Even Parity Odd Parity	Choose the parity bits for the BC Diagnostic Console interface
Stop Bits	<b>1 Stop Bit</b> 2 Stop Bits	Choose the stop bits for the BC Diagnostic Console interface
Data Bits	5 Data Bits 6 Data Bits 7 Data Bits <b>8 Data Bits</b>	Choose the data bits for the BC Diagnostic Console interface
Baudrate	1200 Baud 2400 Baud 4800 Baud <b>9600 Baud</b> 19200 Baud 38400 Baud 115200 Baud	Choose the baudrate for the BC Diagnostic Console interface

## 10.4.28 GPIO Configuration Submenu

Feature	Options	Description
GPO x State (x = 0 to 3)	<b>Low</b> High	Set the state for GPO x
Current GPI configuration	<b>Fh (bitmask)</b>	Each bit represents the state of the corresponding GPI

## 10.4.29 Board Controller Command Control Submenu

Feature	Options	Description
CGBC_CMD_CFG_PINS	<b>Enabled</b> Disabled	Enables or disables the command to set or get the system configuration pin states. On Intel platforms this also controls the Flash Descriptor Override (FDO)
CGBC_CMD_AVR_SPM	<b>Enabled</b> Disabled	Enables or disables the command to update the board controller firmware
BC Command Re-Enabling Event	<b>System Reset</b> S5 Power Cycle G3 Power Cycle	Event that has to occur in order to re-enable a disabled command

## 10.4.30 PC Speaker Submenu

Feature	Options	Description
Debug Beeps	Disabled <b>Enabled</b>	Enable or disable general debug / status beep generation
Input Device Debug Beeps	<b>Disabled</b> Enabled	Enable or disable input device debug beeps
Output Device Debug Beeps	<b>Disabled</b> Enabled	Enable or disable output device debug beeps
USB Driver Beeps	<b>Disabled</b> 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 <b>Enabled</b>	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	<b>Disabled</b> 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 grayed out 'BIOS Update and Write Protection' option. If this option is set to '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 GmbH website at [www.congatec.com](http://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 overview in the windows deployment options section of the Microsoft TechNet Library at [www.technet.microsoft.com](http://www.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.



*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	<b>Disabled</b> Enabled	Enable this feature to display OEM logo instead of POST messages <b>Note:</b> The default OEM logo is a dark screen
Setup Prompt Timeout	<b>1</b> (more values)	Set number of seconds to wait for a setup activation key: '65535' - Waits indefinitely (0xFFFF) '0' - Disables waiting but setup access is still possible (not recommended)
Bootup NumLock State	<b>On</b> Off	Set the keyboard numlock state
Enter Setup If No Boot Device	No <b>Yes</b>	Set whether the setup menu should be started if no boot device is connected
Enable Popup Boot Menu	No <b>Yes</b>	Set whether the popup boot menu can be started
Boot Priority Selection	UEFI Standard <b>Type Based</b>	'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	<b>Legacy First</b> 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
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	<b>Auto (Batt. Manager)</b> 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	<b>G3/Mech Off</b> S5/Soft Off	Set system state after shutdown if a battery system is present

Feature	Options	Description
Power Loss Control	<b>Remain Off</b> 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 <b>Note:</b> This feature only works with an ATX type power supply
AT Shutdown Mode	System Reboot <b>Hot S5</b>	Set the behavior of an AT-powered system after a shutdown
UEFI Fast Boot	<b>Disabled</b> Enabled	Enable to boot with a minimum set of devices <b>Note:</b> This feature has no effect for BBS / legacy boot options
SATA Support	Last Boot HDD Only <b>All SATA Devices</b>	Select SATA support
VGA Support	Auto <b>UEFI Driver</b>	'Auto' - Installs legacy video option ROM for legacy operating system boot <b>Note:</b> The boot logo will not be displayed during POST 'UEFI Driver' - Installs UEFI GOP driver
USB Support	Disabled Full Init <b>Partial Init</b>	'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 <b>Enabled</b>	Disable to skip PS/2 devices
Network Stack Driver Support	<b>Disabled</b> Enabled	Disable to skip the UEFI network stack driver installation
Redirection Support	<b>Disabled</b> Enabled	Disable to deactivate the Redirection function
UEFI Screenshot Capability	<b>Disabled</b> 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**
1. The term 'AC power loss' stands for the state when the module loses 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.
  2. 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
► Generate Menu Layout File	Setup menu layout file will be generated and stored on the first writable file system found
<b>Boot Override</b>	
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 BIOS setup description of the conga-TC170 can be viewed without having access to the module. However, access to the restricted area of the congatec website is required in order to download the necessary tool (CgMlfViewer) and Menu Layout File (MLF).

The MLF contains the BIOS setup description of a particular BIOS revision. The MLF can be viewed with the CgMlfViewer tool. This tool offers a search function to quickly check for supported BIOS features. It also shows where each feature can be found in the BIOS setup menu.

For more information, read the application note "AN42 - BIOS Setup Description" available at [www.congatec.com](http://www.congatec.com).



### Note

*If you do not have access to the restricted area of the congatec website, contact your local congatec sales representative.*

### 11.1 BIOS Versions

The BIOS displays the BIOS project name and the revision code during POST, and on the main setup screen. 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.

---

## 11.2 Updating the BIOS

BIOS updates are recommended to correct platform issues or enhance the feature set of the module. The conga-TC170 features a congatec/AMI AptioEFI firmware on an onboard flash ROM chip. You can update the firmware with the congatec System Utility. The utility has five versions—UEFI shell, DOS based command line <sup>1</sup>, Win32 command line, Win32 GUI, and Linux version.

For more information about “Updating the BIOS” refer to the user’s guide for the congatec System Utility “CGUTLm1x.pdf” on the congatec website at [www.congatec.com](http://www.congatec.com).



### Note

<sup>1</sup>. *Deprecated*



### Caution

*The DOS command line tool is not officially supported by congatec and therefore not recommended for critical tasks such as firmware updates. We recommend to use only the UEFI shell for critical updates.*

### 11.2.1 Update from External Flash

For instructions on how to update the BIOS from external flash, refer to the AN7\_External\_BIOS\_Update.pdf application note on the congatec website at <http://www.congatec.com>.

## 11.3 Supported Flash Devices

The conga-TC170 supports the following flash devices:

- Winbond W25Q128JVS1Q (16 MB)
- Winbond W25Q64JVSS1Q (8 MB)

The flash devices listed above can be used on the carrier board for external BIOS support.