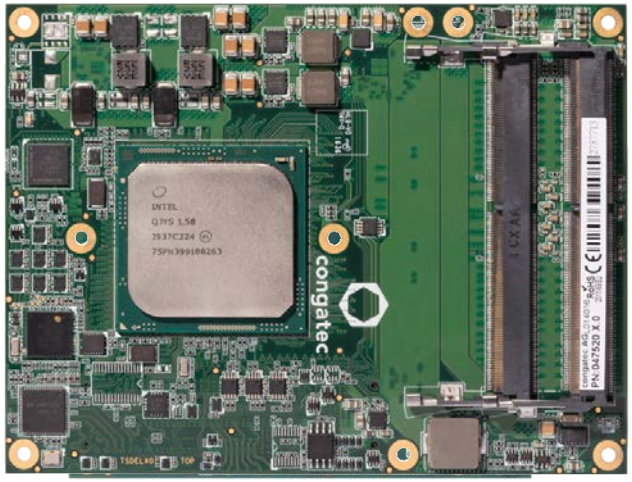


COM Express™ conga-B7XD

Next Generation Intel® Xeon® and Pentium® SoCs

User's Guide

Revision 1.10

congatec

Revision History

Revision	Date (yyyy-mm-dd)	Author	Changes
0.1	2017-05-19	AEM	• Preliminary release
1.0	2018-04-10	AEM	• Changed the maximum turbo frequency of the Intel® Xeon® D-1529 SoC to "N.A" in table 4 "Feature Summary". Also deleted the Suspend to RAM and Intel AMT 10 power management features • Updated table 6 "Power Consumption Values" • Corrected the number of PCIe Gen 2 lanes the Intel® Xeon® D-1577 SoC supports • Added section 5.1.4.1 "PCI Express Routing" • Updated section 5.1.6 "I²C Bus" • Corrected section 5.1.9 "General Purpose Serial Interface" • Added sections 9 "System Resources" and 10 "BIOS Setup Description" • Official release
1.1	2018-07-16	AEM	• Corrected the number of variants supported in section 1.2 "conga-B7XD Options Information". Also corrected the number of SATA ports the Intel® Xeon® D-1529 supports • Corrected the power consumption measurement unit in table 6 "Power Consumption Values" • Corrected the pin numbers of PCIe differential pairs 10 in table 19 "PCI Express Signal Descriptions (general purpose)" and USB ports 0 and 1 differential pairs in table 20 "USB 2.0 Signal Descriptions" • Re-arranged the A-B and C-D connector pinout tables in section 8 "Signal Descriptions and Pinout Tables"
1.2	2019-06-27	AEM	• Corrected the heatspreader thickness in the illustration in section 2.3 "Mechanical Dimensions" • Updated the input voltage range of VCC_RTC in section 2.4.1 "Electrical Characteristics" • Updated table 6 "Power Consumption Values" • Corrected SER1_TX pin number in table 36 "Boot Strap Signal Description" • Corrected typographical error in section 3 "Block Diagram" • Updated section 4 "Cooling Solutions" • Added more content to section 10 "BIOS Setup Description" • Added section 11 "Additional BIOS Information"
1.3	2019-10-30	AEM	• Updated section 6.1.5 "Power Loss Control" • Added note about the required PD resistor on the carrier board for the pins that are reclaimed from the VCC_12V pool in tables 27 , 29 and 30 • Added note about the minimum pulse width required for proper button detection in table 30 "Power and System Management Signal Descriptions"
1.4	2020-04-24	AEM	• Corrected and updated table 1.2 "Options Information" • Added power consumption for PN: 057001 • Updated the cooling diagram in section 4.2 "CSP Dimensions" • Updated the formfactors.org link in "Standard 12V Power Supply Implementation Guidelines" section • Added information about congatec Menu Layout File in section 11 "Additional BIOS Information" • Deleted section 12 "Industry Specifications"
1.5	2020-07-03	AEM	• Changed the supported maximum memory capacity to 96 GB
1.6	2021-03-30	AEM	• Added note about PCI RefClk Spread Spectrum Configuration to section 5.1.4 "PCI Express" • Updated section 10 "BIOS Setup Description"

Revision	Date (yyyy-mm-dd)	Author	Changes
1.7	2021-08-02	AEM	• Added Software License Information • Changed congatec AG to congatec GmbH • Updated the Power Supply Implementation Guidelines in section 5.1.11 "Power Control" • Updated section 6.3 "congatec Battery Management Interface"
1.8	2021-11-16	AEM	• Corrected the number of PCIe lanes in section 5.1.4 "PCI Express"
1.9	2022-03-16	AEM	• Indicated that variants with Intel Xeon D-1529 do not support PCIe lanes 0-7 in table 3 "Industrial Variants" and table 22 "PCI Express Signal Descriptions (general purpose)"
1.10	2022-07-11	AEM	• Added section 1.3 "Supported 10 GbE Configurations"

Preface

This user's guide provides information about the components, features, connectors and BIOS Setup menus available on the conga-B7XD. It is one of three documents that should be referred to when designing a COM Express™ application. The other reference documents that should be used include the following:

COM Express™ Design Guide
COM Express™ Specification

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

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.

Lead-Free Designs (RoHS)

All congatec GmbH designs are completely RoHS compliant.

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.

Symbols

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

Warning

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

Caution

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

Note

Notes call attention to important information that should be observed.

Copyright Notice

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".

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.

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. 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 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.

Certification

congatec GmbH is certified to DIN EN ISO 9001 standard.

Contents

List of Tables

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 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

Terminology

Term	Description
GB	Gigabyte
GHz	Gigahertz
kB	Kilobyte
MB	Megabyte
Mbit	Megabit
Gbps	Gigabit per second
Mbps	Megabit per second
MTps	Megatransfer per second
kHz	Kilohertz
MHz	Megahertz
TDP	Thermal Design Power
PCIe	PCI Express
SATA	Serial ATA
PEG	PCI Express Graphics
PCH	Platform Controller Hub
SM	System Management
BMC	Baseboard Management Controller
N.C	Not connected
N.A	Not available
TBD	To be determined

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 x110 mm

Table 1 COM Express™ 3.0 Pinout Types

Types	Connector Rows	PCIe Lanes	PCI	IDE	SATA Ports	LAN ports	USB 2.0/ USB 3.0	Display Interfaces
Type 1	A-B	Up to 6		-	4	1	8 / 0	VGA, LVDS
Type 2	A-B C-D	Up to 22	32 bit	1	4	1	8 / 0	VGA, LVDS, PEG/SDVO
Type 3	A-B C-D	Up to 22	32 bit	-	4	3	8 / 0	VGA,LVDS, PEG/SDVO
Type 4	A-B C-D	Up to 32		1	4	1	8 / 0	VGA,LVDS, PEG/SDVO
Type 5	A-B C-D	Up to 32		-	4	3	8 / 0	VGA,LVDS, PEG/SDVO
Type 6	A-B C-D	Up to 24		-	4	1	8 / 4 [1]	VGA,LVDS/eDP, PEG, 3x DDI
Type 7	A-B C-D	Up to 32		-	2	5 (1x 1 G, 4x 10 G)	4/ 4 [1]	-
Type 10	A-B	Up to 4		-	2	1	8 / 2	LVDS/eDP, 1xDDI

1. *The SuperSpeed USB ports (USB 3.0) are not in addition to the USB 2.0 ports. Up to 4 of the USB 2.0 ports can support SuperSpeed USB.*

The conga-B7XD modules use the Type 7 pinout definition and comply with COM Express 3.0 specification. They are equipped with two high performance connectors that ensure stable data throughput, and support high bandwidth networking.

The COM (computer on module) integrates all the core components of a common PC 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 embedded PC 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 3.0/2.0, and 10 Gigabit Ethernet. 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-B7XD is currently available in 10 variants (six commercial and four industrial). The table below shows the different configurations available.

Table 2 Commercial Variants

Part-No.		047500	047501	047502	047503	047504	047505
Processor		Intel® Xeon® D-1577 1.3 GHz 16 Cores	Intel® Xeon® D-1567 2.1 GHz 12 Cores	Intel® Xeon® D-1548 2.0 GHz 8 Cores	Intel® Xeon® D-1527 2.2 GHz 4 Cores	Intel® Pentium™ D1509 1.5 GHz 2 Cores	Intel® Pentium™ D1508 2.2 GHz 2 Cores
Intel® Smart Cache		24 MB	18 MB	18 MB	6 MB	3 MB	3 MB
Max. Turbo Frequency		2.1 GHz	2.7 GHz	2.6 GHz	2.7 GHz	N.A	2.6 GHz
Processor Graphics		N.A	N.A	N.A	N.A	N.A	N.A
DDR4 Memory (ECC or Non-ECC)		2133 MTps dual channel (up to 96 GB) [1]	2133 MTps dual channel (up to 96 GB) [1]	2400 MTps dual channel (up to 96 GB) [1]	2133 MTps dual channel (up to 96 GB) [1]	1600 MTps dual channel (up to 96 GB) [1]	1866 MTps dual channel (up to 96 GB) [1]
Gigabit Ethernet		2x 10 GbE (KR) 1x 1 GbE [2]	2x 10 GbE (KR) 1x 1 GbE [2]	2x 10 GbE (KR) 1x 1 GbE [2]	2x 10 GbE (KR) 1x 1 GbE [2]	1x 1 GbE [2]	2x 10 GbE (KR) 1x 1 GbE [2]
PCIe Lanes	Gen 3	24 lanes	24 lanes	24 lanes	24 lanes	24 lanes	24 lanes
	Gen 2	7 lanes [3]	7 lanes [3]	7 lanes [3]	7 lanes [3]	7 lanes [3]	7 lanes [3]
USB Ports		4x USB 3.0/2.0	4x USB 3.0/2.0	4x USB 3.0/2.0	4x USB 3.0/2.0	4x USB 3.0/2.0	4x USB 3.0/2.0
SATA (6 Gbps)		2	2	2	2	2	2
Processor TDP		45 W	65 W	45 W	35 W	19 W	25 W

Note

1. *Supported with congatec qualified memory modules. For the list of qualified memory modules, refer to the conga-B7XD datasheet on the congatec website at www.congatec.com.*

2. *Shares PCIe lane 7 with PCIe root port 7. The shared lane is routed to 1 GbE interface by default.*

3. *Eight lanes are supported if you select PCIe root port 7 via the Advanced -> Module PCIe Configuration submenu of the BIOS setup menu.*

Table 3 Industrial Variants

Part-No.		047520	047521	047522	047523
Processor		Intel® Xeon® D-1559 1.5 GHz 12 Cores	Intel® Xeon® D-1539 1.6 GHz 8 Cores	Intel® Xeon® D-1529 1.3 GHz 4 Cores	Intel® Pentium™ D1519 1.5 GHz 4 Cores
Intel® Smart Cache		18 MB	12 MB	6 MB	6 MB
Max. Turbo Frequency		2.1 GHz	2.2 GHz	N.A	2.1 GHz
Processor Graphics		N.A	N.A	N.A	N.A
DDR4 Memory (ECC or Non-ECC)		2133 MTps dual channel (up to 96 GB) [1]	2133 MTps dual channel (up to 96 GB) [1]	1600 MTps dual channel (up to 96 GB) [1]	2133 MTps dual channel (up to 96 GB) [1]
Gigabit Ethernet		2x 10 GbE (KR) 1x 1 GbE [2]	2x 10 GbE (KR) 1x 1 GbE [2]	N.A	2x 10 GbE (KR) 1x 1 GbE [2]
PCIe Lanes	Gen 3	24 lanes	24 lanes	N.A	24 lanes
	Gen 2	7 lanes [3]	7 lanes [3]	24x IIO PCIe Gen 2 [4]	7 lanes [3]
USB Ports		4x USB 3.0/2.0	4x USB 3.0/2.0	4x USB 2.0	4x USB 3.0/2.0
SATA (6 Gbps)		2	2	1	2
Processor TDP		45 W	35 W	20 W	25 W

Note

1. *Supported with congatec qualified memory modules. For the list of qualified memory modules, refer to the conga-B7XD datasheet on the congatec website at www.congatec.com.*
2. *Shares PCIe lane 7 with PCIe root port 7. The shared lane is routed to 1 GbE interface by default.*
3. *Eight lanes are supported if you select PCIe root port 7 via the Advanced -> Module PCIe Configuration submenu of the BIOS setup menu.*
4. *PCIe lanes 0-7 (Gen 2) are not available.*

1.3 Supported 10 GbE Configuration

The table below lists the 10 GbE configurations the conga-B7XD supports.

Table 4 Supported 10 GbE Configuration

Configurations	conga-B7XD
10GBASE-KR	Supported [1, 2]
Native SFI	Not supported
Inphi CS4227 - SFI	Supported [1, 3]
Intel X557 - 10G-BASE-T	Supported [1, 2]
Marvell 88X3310P - 10G-BASE-T	Not supported
Marvell 88E6190 2500BASE-KX	Not supported

Note

1. *Appropriate NVM image must be used. For instructions on how to deploy 10GbE LAN NVM and PHY NVM images, refer to congatec document "CTN 20180726 001" in the restricted area of our website*
2. *Not validated by congatec*
3. *Default image on conga-B7XD*

2 Specifications

2.1 Feature List

Table 5 Feature Summary

Form Factor	Based on COM Express™ standard pinout Type 7, rev. 3.0 (Basic size 125 x 95 mm)
Processor	Intel® Xeon and Pentium™ processor D-1500 product family SoC
Memory	Three memory sockets (two stacked on the top side and one on the bottom side). Supports - DDR4 ECC and non-ECC SODIMM modules - Dual channel (channel 0, DIMM 0 on the bottom side; channel 0, DIMM 1 (upper slot) and channel 1, DIMM 0 (lower slot) on the top side) - Data rates up to 2400 MTps - Maximum 96 GB capacity (32 GB each) **NOTE**: 1 *Do not mix ECC and non-ECC SODIMM modules.* 2 *Populate DIMM 0 (slot on bottom side or lower slot on the top side) before DIMM 1:* - *If you populate only DIMM 1 socket (upper slot on the top side), the system stops the boot process with post code "b0"* - *The system displays POST code "53" if memory module is not detected.* 3 *See section 7.3 "DDR4 Memory" for additional memory requirements.* 4 *Up to 96 GB capacity with congatec qualified memory modules. See the conga-B7XD datasheet for more information.*
congatec Board Controller	Multi-stage watchdog, non-volatile user data storage, manufacturing and board information, board statistics, hardware monitoring, fan control, I2C bus, Power loss control
Chipset	Integrated in the SoC
Ethernet	Gigabit Ethernet. Supports: - 2x 10 GbE with KR interface - 1x 1 GbE with standard interface **NOTE**: *The 10 GbE PHY must be implemented on the carrier board.*
Audio	N.A
Graphics	N.A
Peripheral Interfaces	USB Interfaces: - Up to 4x USB 2.0 - Up to 4x USB 3.0 Buses - LPC (no DMA) - I²C (fast mode, 400 KHz, multi-master) - SMBus - SPI 2x SATA® (6 Gbps) PCIe Interfaces - Up to 24x PCIe Gen. 3 lanes - Up to 8x PCIe Gen. 2 lanes 2x UART GPIOs
BIOS	AMI Aptio® V UEFI 2.x firmware; 16 MB SPI with congatec Embedded BIOS features
Onboard Storage	N.A

Power Management	Supports: - ACPI 4.0a compliant with battery support. - Hardware power management - System Sleep State Control - Wake events from the Intel Management Engine
Security	Discrete Trusted Platform Module (Infineon SLB9665_TT2.0); new AES Instructions for faster and better encryption.

Note

Some of the features mentioned above are optional. Check the part number of your module and compare it to the Options Information tables on pages 14 and 15 to determine what options are available on your particular module.

2.2 Supported Operating Systems

The conga-B7XD supports the following operating systems.

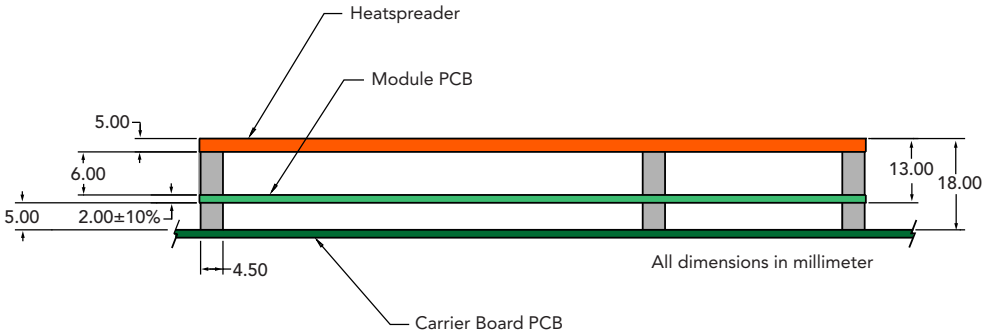
- Red Hat Enterprise Linux Server 6.6 and 7.1
- Novel SuSE Linux Enterprise Server 11 SP4 and 12 SP1
- Fedora 22
- Ubuntu 14.10
- Microsoft® Windows® 7 and 8.1
- Microsoft® Windows® 10 Enterprise
- Microsoft® Windows® Server 2008 R2 SP1 / 2012 / 2012 R2 and 2016
- VMware
- ESXi

Note

For better system performance, use only 64-bit Operating Systems.

2.3 Mechanical Dimensions

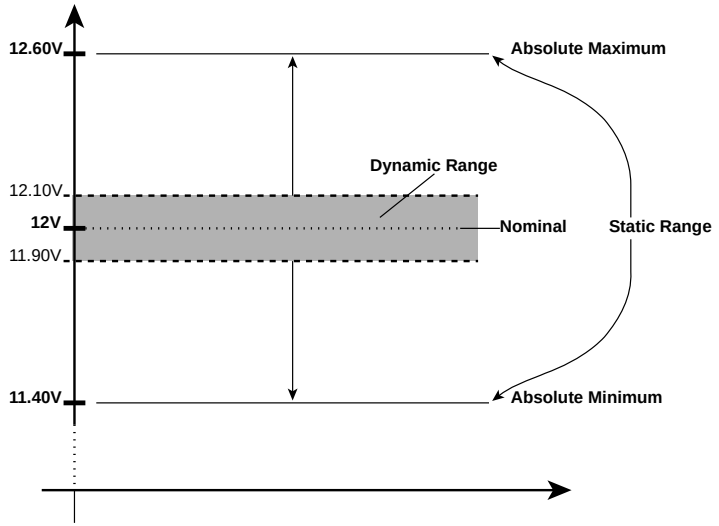
- 125.0 mm x 95.0 mm
- Height approximately 18 or 21 mm (including heatspreader) depending on the carrier board connector that is used. If the 5 mm (height) carrier board connector is used, then approximate overall height is 18 mm. If the 8 mm (height) carrier board connector is used, then approximate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



2.4 Supply Voltage Standard Power

- 12 V DC ± 5 %

The dynamic range shall not exceed the static range.



2.4.1 Electrical Characteristics

Power supply pins on the module's connectors limit the amount of input power. The following table provides an overview of the limitations for pinout Type 7 (dual connector, 440 pins).

Power Rail	Module Pin Current Capability (Ampere)	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 percent of nominal to 90 percent of nominal at a minimum slope of 250 V/s. The smooth turn-on requires that, during the 10 percent to 90 percent portion of the rise time, the slope of the turn-on waveform must be positive.

2.5 Power Consumption

The power consumption values were measured with the following setup:

- Input voltage +12 V
- conga-B7XD COM
- modified congatec carrier board
- conga-B7XD cooling solution
- Microsoft Windows 10 (64 bit)

Note

The CPU was stressed to its maximum workload.

Table 6 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	
S0: Maximum value	Highest frequency mode (HFM/Turbo Boost).	The CPU was stressed to its maximum frequency
S0: Peak current	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
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 7 Power Consumption Values

The table below provides additional information about the conga-B7XD power consumption. The values are recorded at various operating mode.

Part No.	Memory Size	H.W Rev.	BIOS Rev.	OS (64 bit)	CPU			Current (A)				
					Variant	Cores	Freq. /Max. Turbo	S0: Min	S0: Max	S0: Peak	S3	S5
047500	3 x 4 GB	C.1	R115	Windows 10	Intel® Xeon® D-1577	16	1.3 / 2.1 GHz	0.95	4.11	4.81	N.A	0.90
047501	3 x 4 GB	B.0	R115	Windows 10	Intel® Xeon® D-1567	12	2.1 / 2.7 GHz	1.04	5.92	6.90	N.A	0.96
047502	3 x 4 GB	C.1	R115	Windows 10	Intel® Xeon® D-1548	8	2.0 / 2.6 GHz	0.91	4.07	4.25	N.A	0.91
047503	3 x 4 GB	C.1	R115	Windows 10	Intel® Xeon® D-1527	4	2.2 / 2.7 GHz	0.88	3.18	3.79	N.A	0.91
047504	3 x 4 GB	C.1	R115	Windows 10	Intel® Pentium™ D1509	2	1.5 Ghz / N.A	0.83	1.43	1.55	N.A	0.91
047505	3 x 4 GB	C.1	R115	Windows 10	Intel® Pentium™ D1508	2	2.2 / 2.6 Ghz	0.98	2.17	2.28	N.A	0.89
047520	3 x 4 GB	C.1	R115	Windows 10	Intel® Xeon® D-1559	12	1.5 / 2.1 GHz	0.99	4.07	4.18	N.A	0.92
047521	3 x 4 GB	C.1	R115	Windows 10	Intel® Xeon® D-1539	8	1.6 / 2.2 GHz	0.95	3.25	3.39	N.A	0.95
047522	3 x 4 GB	C.1	R115	Windows 10	Intel® Xeon® D-1529	4	1.3 / N.A GHz	1.31	1.77	1.79	N.A	0.88
047523	3 x 4 GB	C.1	R115	Windows 10	Intel® Pentium™ D1519	4	1.5 / 2.1 GHz	0.93	2.16	2.27	N.A	0.93

2.6 Supply Voltage Battery Power

Table 8 CMOS Battery Power Consumption

RTC @	Voltage	Current
-10°C	3V DC	1.20 µA
20°C	3V DC	1.48 µA
70°C	3V DC	2.91 µA

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 of your application in worst case conditions (for example, during high temperature and high battery voltage).*
3. *Consider 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.*

2.7 Environmental Specifications

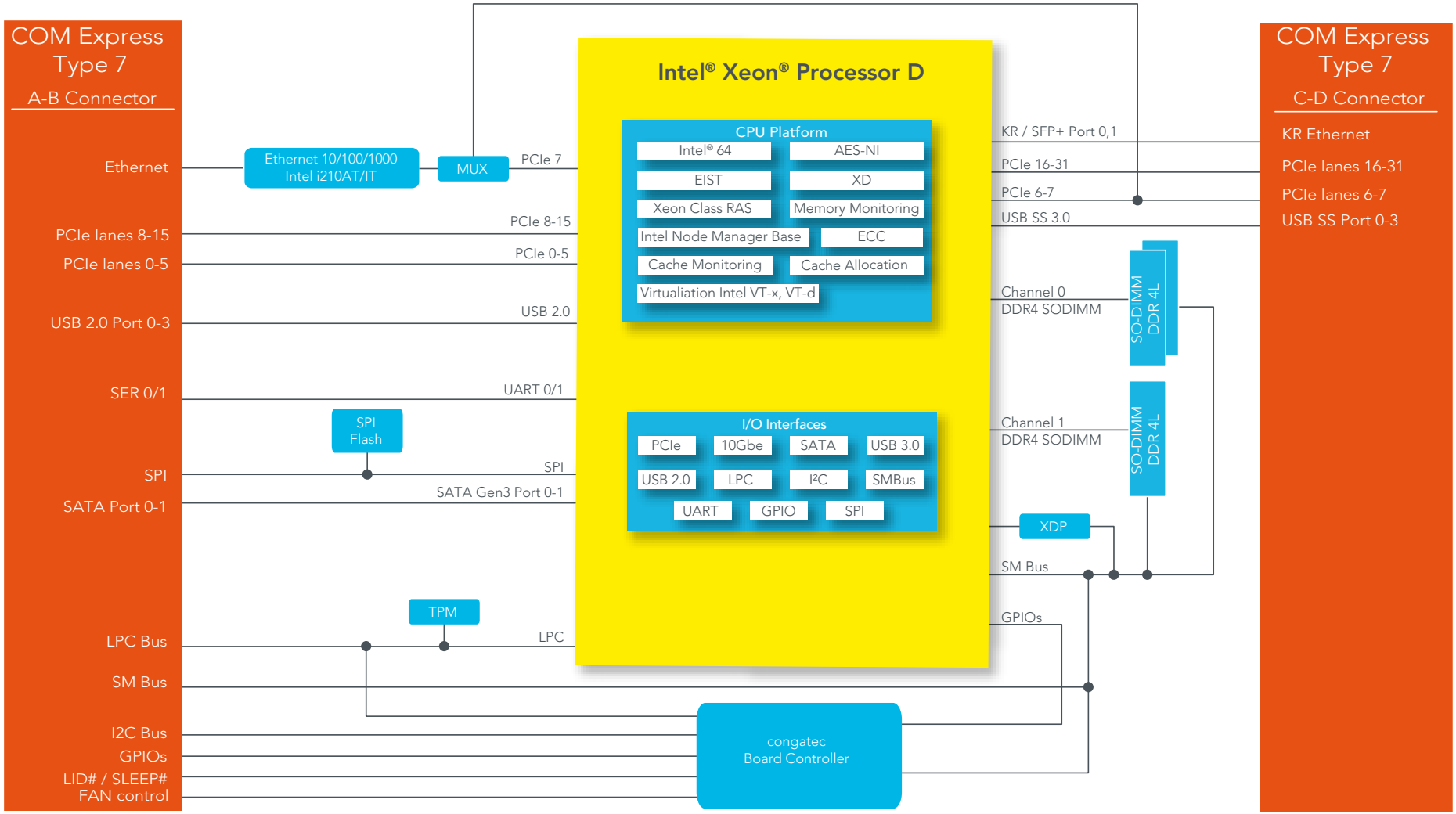
Temperature	Operation: 0° to 60°C	Storage: -20° to 80°C (commercial variants)
Temperature	Operation: -40° to 85°C	Storage: -40° to 85°C (industrial variants)
Humidity	Operation: 10% to 90%	Storage: 5% to 95%

Caution

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

Humidity specifications are for non-condensing conditions.

3 Block Diagram



4 Cooling Solutions

congatec GmbH offers the following cooling solutions for the conga-B7XD. The dimensions of the cooling solutions are shown in the sub-sections. All measurements are in millimeters.

Table 9 Cooling Solution Variants

	Cooling Solution	Intended TDP	Part No	Description
1	CSA-HP	Up to 65 W	047530	Active cooling solution with integrated heat pipes and M2.5 mm threaded standoffs
			047531	Active cooling solution with integrated heat pipes and 2.7 mm bore-hole standoffs
2	CSA-Cu	Up to 35 W	047535	Active cooling solution with integrated copper plate and 2.7 mm bore-hole standoffs
			047536	Active cooling solution with integrated copper plate and M2.5 mm threaded standoffs
3	CSP-Cu	Up to 20 W	047537	Passive cooling solution with integrated copper plate and 2.7 mm bore-hole standoffs
			047538	Passive cooling solution with integrated copper plate and M2.5 mm threaded standoffs
4	HSP-VC	Up to 65 W	047532	Heatspreader with integrated vapor chamber and M2.5 mm threaded standoffs
			047533	Heatspreader with integrated vapor chamber and 2.7 mm bore-hole standoffs
5	HSP-Cu	Up to 35 W	047539	Heatspreader with integrated copper plate and 2.7 mm bore-hole standoffs
			047540	Heatspreader with integrated copper plate and 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.*

Caution

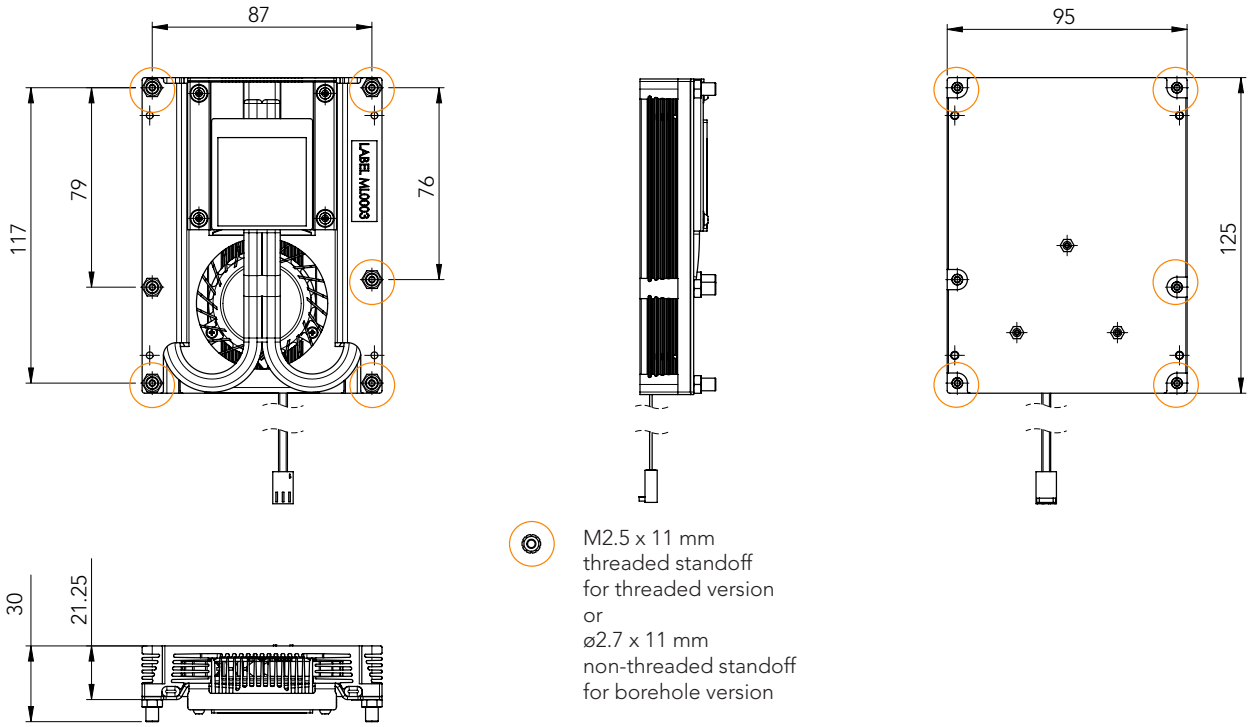
1. *The congatec heatspreaders/cooling solutions are tested only within the commercial temperature range of 0° to 60°C. Therefore, if your application that features a congatec heatspreader/cooling solution operates outside this temperature range, ensure the correct operating temperature of the module is maintained at all times. This may require additional cooling components for your final application's thermal solution.*

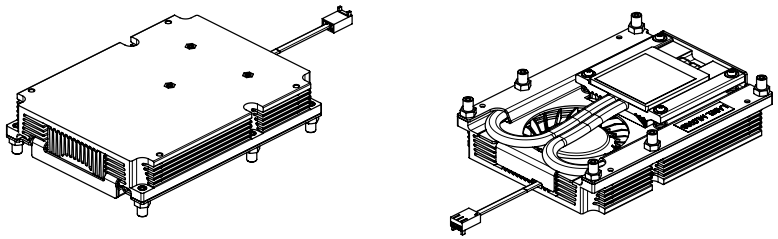
2. *For adequate heat dissipation, use the mounting holes on the cooling solution to attach it to the module. Apply thread-locking fluid on the screws if the cooling solution is used in a high shock and/or vibration environment. To prevent the standoff from stripping or cross-threading, use non-threaded 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

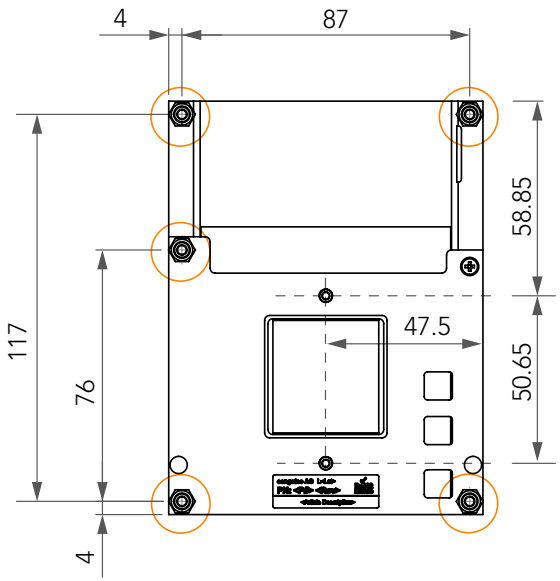


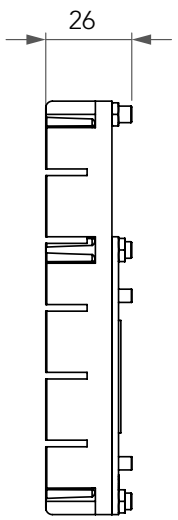


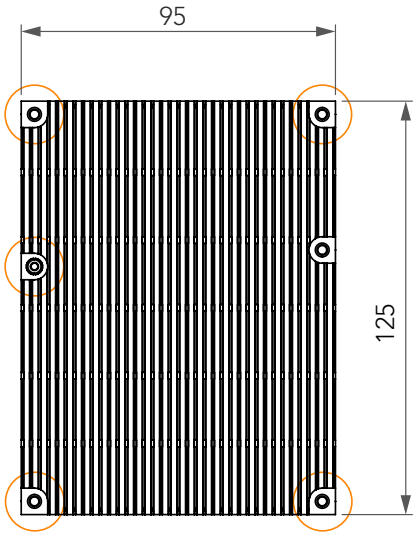
Note

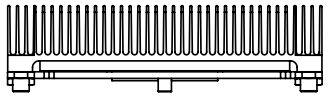
The dimensions are valid for CSA-HP and CSA-Cu

4.2 CSP Dimensions

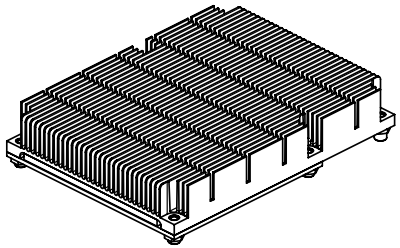


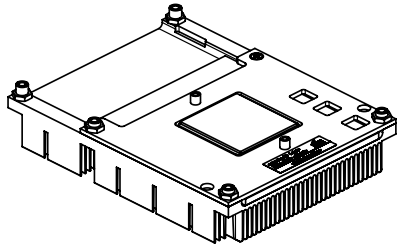




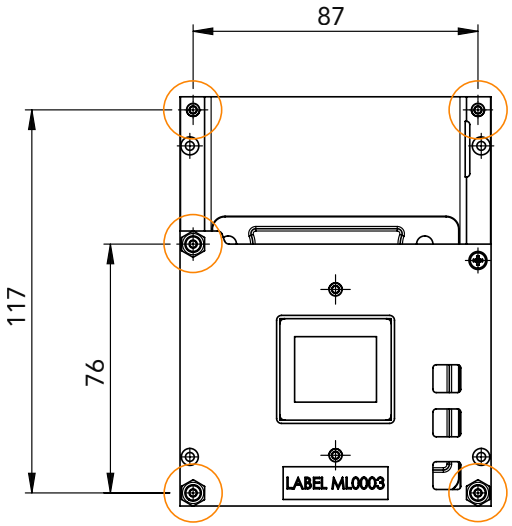


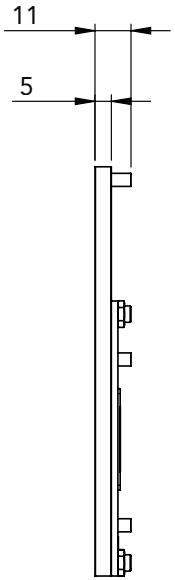
M2.5 x 11 mm
threaded standoff
for threaded version
or
ø2.7 x 11 mm
non-threaded standoff
for borehole version

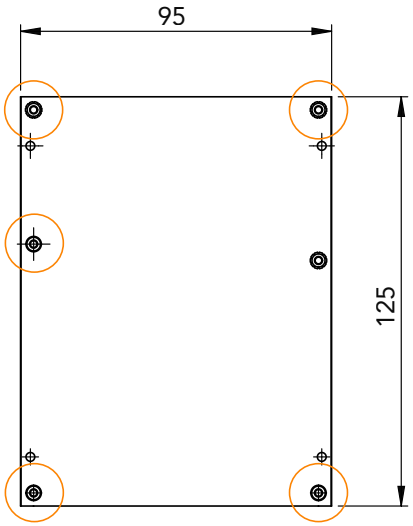




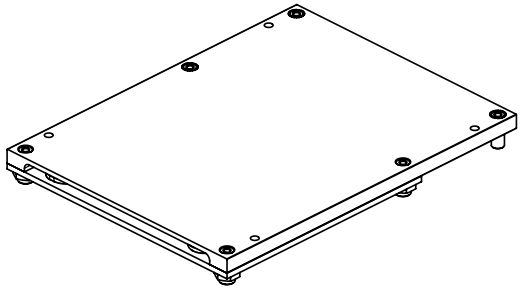
4.3 HSP Dimensions

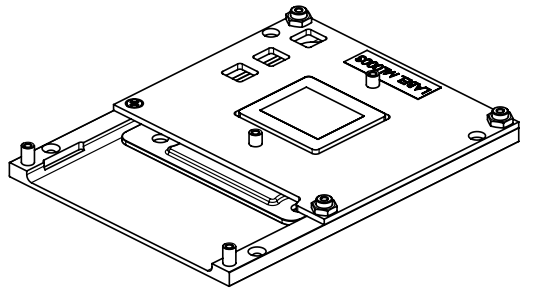






M2.5 x 11 mm
threaded standoff
for threaded version
or
ø2.7 x 11 mm
non-threaded standoff
for borehole version





Note

The dimensions are valid for HSP-VC and HSP-Cu

5 Connector Rows

The conga-B7XD is connected to the carrier board via two 220-pin connectors (COM Express Type 7 pinout). These connectors are broken down into four rows. The primary connector consists of rows A - B while the secondary connector consists of rows C - D.

5.1 Primary and Secondary Connector Rows

The following subsystems can be found on the primary (A - B) and secondary (C - D) connector rows.

Table 10 Supported Interfaces on Rows A-B and C-D

Interfaces	Rows A-B	Rows C-D
SATA	2	-
USB 2.0	4	-
USB 3.0	-	4
Gigabit Ethernet	1 Gbps	10 Gbps (KR Ethernet)
PCIe Gen 2	6 lanes	2 lanes
PCIe Gen 3	8 lanes	16 lanes
UART	2	-
Buses	SPI, LPC, SMB	-

5.1.1 SATA

Table 11 SATA Features

Rows A-B	Rows C-D
Two SATA interfaces with support for - independent DMA operation - data transfer rates up to 6.0 Gbps - legacy mode using I/O space and AHCI mode using memory space	None

5.1.2 USB Interface

Table 12 USB Features

Rows A-B	Rows C-D
Four USB 2.0 ports: - each port can be combined with USB SuperSpeed signals to create USB 3.0 ports - supports data transfers up to 480 Mbps - features EHCI controller - supports USB 1.1 and USB 2.0 compliant devices - supports USB debug feature on port 1	Four USB 3.0 SuperSpeed Tx/Rx differential Signals: - each port requires corresponding USB 2.0 differential pairs - supports data transfers up to 5 Gbps - features xHCI controller

5.1.3 Gigabit Ethernet

Table 13 Gigabit Ethernet Features

Rows A-B	Rows C-D
One 1 GbE interface [1,2]. Supports: - MDI interface - full-duplex operation at 10/100/1000 Mbps - half-duplex operation at 10/100 Mbps - IEE 802.3x flow control specification	Two 10 GbE [3] interface. Supports: - KR interface - full-duplex operation at all supported speeds - 10GBASE-KR for gigabit backplane applications - 1000BASE-KR for gigabit backplane applications

Note

1. *Shares PCIe lane 7 with PCIe root port 7. The shared lane is routed to the 1 GbE interface by default.*
2. *To change the default setting, open the BIOS Setup menu and select the appropriate setting via the Advanced -> Module PCIe Configuration submenu.*
3. *See section 1.3 "Supported 10 GbE configurations" for the list of transceivers and PHYs supported by congatec type 7 modules.*

5.1.4 PCI Express™

Table 14 PCI Express Features

Rows A-B	Rows C-D
14 PCIe lanes - eight Gen. 3 lanes (lanes 8 - 15) with up to 8 GTps - six Gen. 2 lanes (lane 0 - 5) with up to 5 GTps - x1 root hubs for Gen 2 lanes - x4 root hubs for Gen 3 lanes	18 PCIe lanes - 16 Gen. 3 lanes (lanes 16 - 31) with up to 8 GTps - two Gen. 2 lanes (lane 6 - 7 [1,2]) with up to 5 GTps - x1 root hubs for Gen 2 lanes - x4 root hubs for Gen 3 lanes

Note

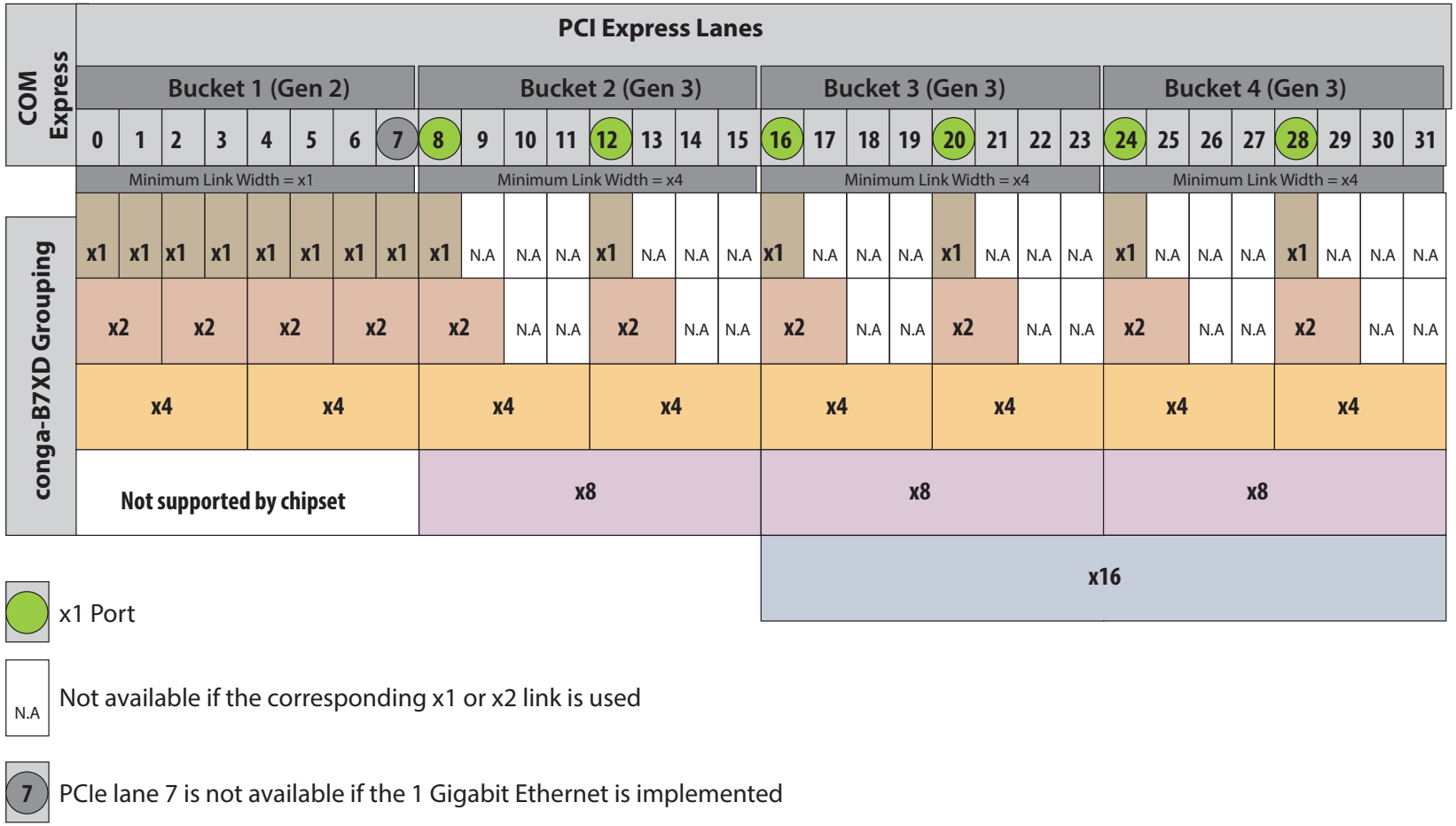
1. *PCIe root port 7 shares COM Express PCIe lane 7 with the 1 Gigabit on-module Ethernet controller. The shared lane is routed to the 1 GbE interface by default.*
2. *To route the shared lane to COM Express PCIe lane 7, open the BIOS Setup menu and change the default setting via the Advanced -> Module PCIe Configuration submenu.*

Note

The PCIe RefClk Spread Spectrum Configuration (SSC) is enabled by default. To change the default settings:

1. *Open the BIOS setup menu.*
2. *Navigate to IntelRCSetup -> Server ME Debug Configuration -> Server ME Generation Configuration -> Override ICC Spread Configuration*
3. *Select SSC2 mode and press "Enter" to see the options.*
4. *Select "Disable" to disable the SSC2 mode.*

5.1.4.1 PCI Express Routing



Note

The minimum width link for buckets 2, 3 and 4 is x4 link. If you use a x1 or a x2 link in these buckets, the remaining lanes that make up the x4 link will not be available.

5.1.5 LPC Bus

The conga-B7XD offers the LPC (Low Pin Count) bus through the integrated PCH. A TPM 1.2/2.0 compliant module is connected to the LPC bus.

Note

The LPC bus does not support DMA devices.

5.1.6 I²C Bus

The I²C bus is implemented through the congatec Board Controller and accessed through the congatec CGOS driver and API. The controller provides a fast-mode multi-master I²C bus that has the maximum I²C bandwidth.

5.1.7 SPI Bus

The conga-B7XD offers the SPI bus through the integrated PCH. The bus supports SPI-compatible flash devices. Integrating an off-module flash device (BIOS) on the carrier board makes it possible to boot the conga-B7XD from the carrier board. This is especially useful when evaluating a customized BIOS.

5.1.8 SMBus

The conga-B7XD offers the SM bus for communicating and managing system devices such as thermal sensors, PCIe devices, RAM's serial presence detect.

Note

Make sure the address space of the carrier board SM bus devices does not overlap with the address space of the module devices. For more information, see the COM Express Specification.

5.1.9 General Purpose Serial Interface

The conga-B7XD offers two UART interfaces via the Intel Broadwell-DE SoC. These interfaces support up to 0.921 Mbps and can operate in low-speed, full-speed and high-speed modes.

Note

Hardware handshake and flow control are not supported.

5.1.10 GPIOs

The conga-B7XD offers General Purpose Input/Output signals on the A-B connector.

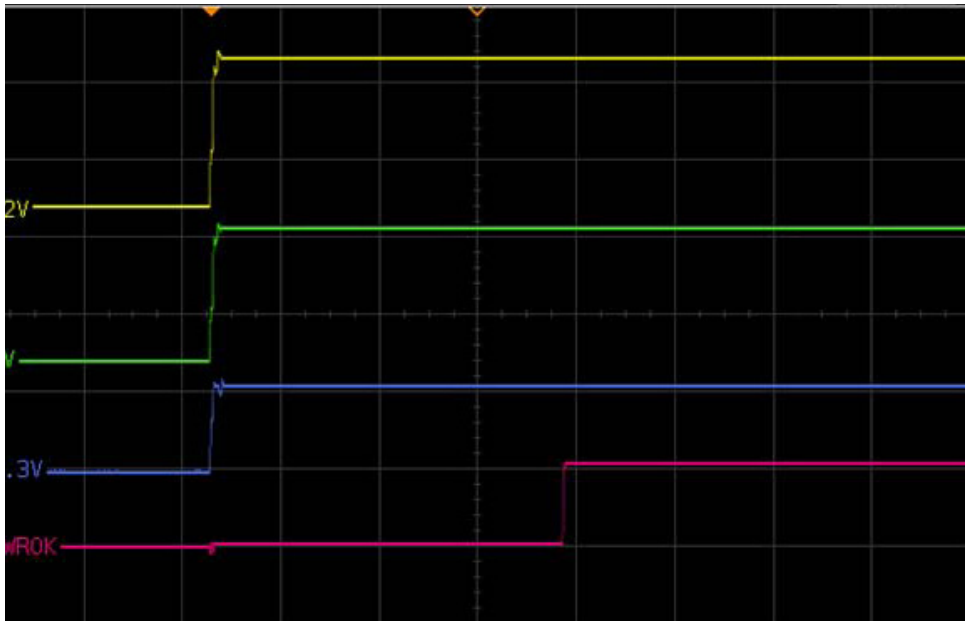
5.1.11 Power Control

PWR_OK

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

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

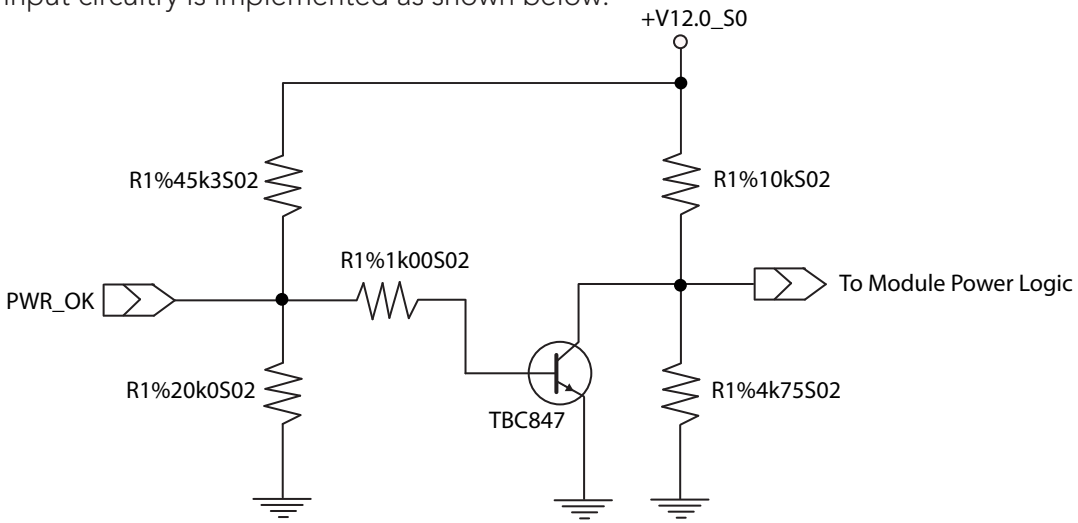
A sample screenshot is shown below:



Note

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

The conga-B7XD PWR_OK input circuitry is implemented as shown below:



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

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

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

- Connect PWR_OK to the "power good" signal of an ATX type power supply.
- Connect PWR_OK to the last voltage regulator in the chain on the carrier board.
- Simply pull PWR_OK with a 1k resistor to the carrier board 3.3V power rail.

With this solution, make sure that before the 3.3 V goes up, all carrier board hardware is fully powered and all clocks are stable.

The conga-B7XD supports the controlling of ATX-style power supplies. If you do not use an ATX power supply, do not connect the conga-B7XD pins SUS_S3/PS_ON, 5V_SB, and PWRBTN# on the conga-B7XD.

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/transistor that is supplied by standby voltage and is located on the carrier board.

PWRBTN#

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

Standard 12V Power Supply Implementation Guidelines

The 12 volt input power is the sole operational power source for the conga-B7XD. Other required voltages are generated internally on the module using onboard voltage regulators.

Note

When designing a power supply for a conga-B7XD application, be aware that the system may malfunction when a 12V 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.

The cause of this problem is that 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 qualication 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.

5.1.12 Power Management

ACPI

The conga-B7XD supports Advanced Configuration and Power Interface (ACPI) specification, revision 4.0a. For more information, see section 7.3 "ACPI Suspend Modes and Resume Events".

6 Additional Features

6.1 congatec Board Controller (cBC)

The conga-B7XD is equipped with Texas Instruments microcontroller. This onboard microcontroller plays an important role for most of the congatec embedded/industrial PC features. It fully isolates some of the embedded features such as system monitoring or the I²C bus from the x86 core architecture, which results in higher embedded feature performance and more reliability, even when the x86 processor is in a low power mode. It also ensures that the congatec embedded feature set is fully compatible amongst all congatec modules.

6.1.1 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.

6.1.2 General Purpose Input/Output

The conga-B7XD offers general purpose inputs and outputs for custom system design. These GPIOs are controlled by the cBC.

6.1.3 Watchdog

The conga-B7XD is equipped with a multi stage watchdog solution that is triggered by software. For more information about the Watchdog feature, see the application note AN3_Watchdog.pdf on the congatec GmbH website at www.congatec.com.

Note

The conga-B7XD module does not support watchdog NMI mode.

6.1.4 I²C Bus

The conga-B7XD supports I²C bus. Thanks to the I²C host controller in the cBC, the I²C bus is multi-master capable and runs at fast mode.

6.1.5 Power Loss Control

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

AC power loss condition occurs 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 within 30 seconds the standby voltage is no longer detected, the module considers this an AC power loss condition. If the standby voltage remains stable for 30 seconds, then it is assumed that the system was switched off properly.

Unlike other module designs available in the embedded market, a CMOS battery is not required by congatec modules to support the ‘Power Loss Control’ feature.

6.1.6 Fan Control

The conga-B7XD has additional signals and functions to further improve system management. One of these signals is an output signal called FAN_PWMOUT that allows system fan control using a PWM (Pulse Width Modulation) output. Additionally, there is an input signal called FAN_TACHOIN that provides the ability to monitor the system’s fan RPMs (revolutions per minute). This signal must receive two pulses per revolution in order to produce an accurate reading. For this reason, a two pulse per revolution fan or similar hardware solution is recommended.

Note

1. *A four wire fan must be used to generate the correct speed readout.*

2. *For the correct fan control (FAN_PWMOUT, FAN_TACHIN) implementation, see the COM Express Design Guide.*

6.2 OEM BIOS Customization

The conga-B7XD is equipped with congatec Embedded BIOS, which is based on American Megatrends Inc. Aptio UEFI firmware. The congatec Embedded BIOS allows system designers to modify the BIOS. For more information about customizing the congatec Embedded BIOS, refer to the congatec System Utility user’s guide CGUTLm1x.pdf on the congatec website at www.congatec.com or contact technical support.

The customization features supported are described below.

6.2.1 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.

6.2.2 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 AN11_Create_And_Add_Bootlogo.pdf on the congatec website for details on how to add OEM boot logo to the congatec Embedded BIOS.

6.2.3 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.

6.2.4 OEM BIOS Code/Data

With the congatec embedded BIOS, system designers can 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 Windows 7, 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 called only 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.

6.2.5 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.

6.3 congatec Battery Management Interface

To facilitate the development of battery powered mobile systems based on embedded modules, congatec GmbH 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 (for example, charge state of the battery, information about the battery, alarms/events for certain battery states and so on) without the need for additional modifications to the system BIOS.

In addition to the ACPI-Compliant Control Method Battery mentioned above, the latest versions of the conga-B7XD 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.

6.4 API Support (CGOS)

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, available on the congatec website.

6.5 Security Features

The conga-B7XD offers a discrete LPC TPM 2.0 (Infineon SLB9665XT2.0) by default. To use the discrete TPM, ensure that the firmware-based TPM is disabled in the BIOS setup menu via the *Advanced -> Platform Trust Technology -> fTPM*. Save the changes and exit to complete the system configuration changes.

6.6 Suspend to Ram

The Suspend to RAM feature is not supported on the conga-B7XD.

7 conga Tech Notes

The conga-B7XD 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® Broadwell-DE Features

Some of the features the Intel Broadwell-DE SoC supports are:

7.1.1 AHCI

The integrated PCH provides hardware support for Advanced Host Controller Interface (AHCI), a standardized programming interface for SATA host controllers. Platforms that support AHCI benefit from performance-enhancing features such as port independent DMA engines (each device is treated as a master) and a hardware-assisted native command queuing. AHCI also provides hot-plug and advanced power management to improve usability.

7.1.2 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

Refer to section 2.5 "Power Consumption" for information about the maximum turbo frequency available for each conga-B7XD variant.

7.1.3 Adaptive Thermal Monitor and Catastrophic Thermal Protection

Intel® Xeon 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 or stop) the processor's internal clocks at a duty cycle of 25% on and 75% off

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

Note

1. *Use a properly designed thermal solution for adequate heat dissipation. This solution ensures the TCC is active for only short periods of time, thus reducing the impact on processor performance to a minimum. The Intel® Xeon processor's respective datasheet can provide you with more information about this subject.*

2. *To enable THERMTRIP# to switch off the system automatically, use an ATX style power supply.*

7.1.4 Processor Performance Control

The Intel® processors found on the conga-B7XD run at different voltage/frequency states (performance states)—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.

7.1.5 Intel® 64 Architecture

The formerly known Intel® Extended Memory 64 Technology is an enhancement to Intel®'s IA-32 architecture. Processors with Intel® 64 architecture support 64-bit-capable operating systems from Microsoft, Red Hat and SuSE. Processors running in legacy mode remain fully

compatible with today's existing 32-bit applications and operating systems

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

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

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

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

Intel® 64 supports:

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

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

7.1.6 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 only RTS Hypervisor.

7.2 ACPI Suspend Modes and Resume Events

The conga-B7XD BIOS does not support S3 (Suspend to RAM). S4 (Suspend to Disk) is however supported. The table below lists the events that wake the system from S4.

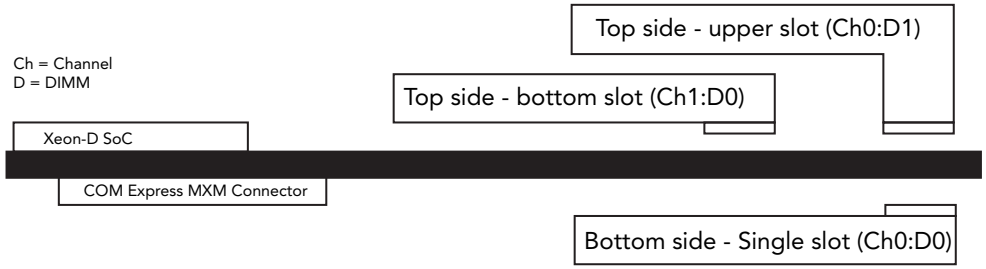
Table 15 Wake Events

Wake Event	Conditions/Remarks
Power Button	Wakes unconditionally from S4-S5.
Onboard LAN Event	Device driver must be configured for Wake On LAN support.
PCI Express WAKE#	Wakes unconditionally from S4-S5.
PME#	Activate the wake up capabilities of a PCI device using Windows Device Manager configuration options for this device or enable 'Resume On PME#' in the Power setup menu.
RTC Alarm	Activate and configure Resume On RTC Alarm in the Power setup menu. Wakes unconditionally from S4-S5.
Watchdog Power Button Event	Wakes unconditionally from S4-S5

7.3 DDR4 Memory

The Intel Broadwell-DE SoC featured on the conga-B7XD supports ECC and non-ECC DDR4 memory modules, up to 2400 MTps. The DDR4 memory modules have lower voltage requirements with higher data rate transfer speeds. They operate at a nominal voltage of 1.2V. With this low voltage system memory interface on the processor, the conga-B7XD offers a system optimized for lowest possible power consumption. The reduction in power consumption due to lower voltage subsequently reduces the heat generated.

The diagram below shows the location of the memory slots on the conga-B7XD.



The following population rules must be observed:

- Do not mix ECC and non-ECC memory modules.
- Do not mix single and dual rank DIMMs.
- Either channel 0 or channel 1, or both can be populated.
- Populate DIMM 0 before DIMM 1:
  - Post code “b0” indicates that you populated only DIMM 1 (upper slot on the top side).
  - Post code “53” indicates that no memory module is detected.
- No requirement to match DIMMs between channels.
- All channels must run at the same interface frequency.
- Each channel may run at different DIMM timings.
- DIMMs with different interface timing will operate at the slower speed.

8 Signal Descriptions and Pinout Tables

The following section describes the signals found on the conga-B7XD. The pinout of the module complies with COM Express Type 7, rev. 3.0.

The table below describes the terminology used in this section. 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 16 Terminology Descriptions

Term	Description
PU	congatec implemented pull-up resistor
PD	congatec implemented pull-down resistor
T	Higher voltage tolerance
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 and 3.0
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.
KR	10GBASE-KR compatible signal
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 Connectors Signal Descriptions

Table 17 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#/ESPI_CS0#	A58	PCIE_TX3+	B58	PCIE_RX3+
A4	GBE0_LINK100#	B4	LPC_AD0/ESPI_IO_0	A59	PCIE_TX3-	B59	PCIE_RX3-
A5	GBE0_LINK1000#	B5	LPC_AD1/ESPI_IO_1	A60	GND (FIXED)	B60	GND (FIXED)
A6	GBE0_MDI2-	B6	LPC_AD2/ESPI_IO_2	A61	PCIE_TX2+	B61	PCIE_RX2+
A7	GBE0_MDI2+	B7	LPC_AD3/ESPI_IO_3	A62	PCIE_TX2-	B62	PCIE_RX2-
A8	GBE0_LINK#	B8	LPC_DRQ0#/ESPI_ALERT0#	A63	GPI1	B63	GPO3
A9	GBE0_MDI1-	B9	LPC_DRQ1#/ESPI_ALERT1#	A64	PCIE_TX1+	B64	PCIE_RX1+
A10	GBE0_MDI1+	B10	LPC_CLK/ESPI_CK	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 [1]	B14	SMB_DAT	A69	PCIE_TX0-	B69	PCIE_RX0-
A15	SUS_S3# [2]	B15	SMB_ALERT#	A70	GND (FIXED)	B70	GND (FIXED)
A16	SATA0_TX+	B16	SATA1_TX+	A71	PCIE_TX8+	B71	PCIE_RX8+
A17	SATA0_TX-	B17	SATA1_TX-	A72	PCIE_TX8-	B72	PCIE_RX8-
A18	SUS_S4#	B18	SUS_STAT#/ESPI_RESET#	A73	GND	B73	GND
A19	SATA0_RX+	B19	SATA1_RX+	A74	PCIE_TX9+	B74	PCIE_RX9+
A20	SATA0_RX-	B20	SATA1_RX-	A75	PCIE_TX9-	B75	PCIE_RX9-
A21	GND (FIXED)	B21	GND (FIXED)	A76	GND	B76	GND
A22	PCIE_TX15+	B22	PCIE_RX15+	A77	PCIE_TX10+	B77	PCIE_RX10+
A23	PCIE_TX15-	B23	PCIE_RX15-	A78	PCIE_TX10-	B78	PCIE_RX10-
A24	SUS_S5#	B24	PWR_OK	A79	GND	B79	GND
A25	PCIE_TX14+	B25	PCIE_RX14+	A80	GND (FIXED)	B80	GND (FIXED)
A26	PCIE_TX14-	B26	PCIE_RX14-	A81	PCIE_TX11+	B81	PCIE_RX11+
A27	BATLOW#	B27	WDT	A82	PCIE_TX11-	B82	PCIE_RX11-
A28	(S)ATA_ACT#	B28	RSVD [1]	A83	GND	B83	GND
A29	RSVD [1]	B29	RSVD [1]	A84	NCSI_TX_EN	B84	VCC_5V_SBY
A30	RSVD [1]	B30	RSVD [1]	A85	GPI3	B85	VCC_5V_SBY

Pin	Row A	Pin	Row B	Pin	Row A	Pin	Row B
A31	GND (FIXED)	B31	GND (FIXED)	A86	RSVD [1]	B86	VCC_5V_SBY
A32	RSVD [1]	B32	SPKR	A87	RSVD [1]	B87	VCC_5V_SBY
A33	RSVD [1]	B33	I2C_CK	A88	PCIE_CK_REF+	B88	BIOS_DIS1#
A34	BIOS_DIS0#/ESPI_SAFS	B34	I2C_DAT	A89	PCIE_CK_REF-	B89	NCSI_RX_ER
A35	THRMTRIP#	B35	THRM#	A90	GND (FIXED)	B90	GND (FIXED)
A36	PCIE_TX13+	B36	PCIE_RX13+	A91	SPI_POWER	B91	NCSI_CLK_IN
A37	PCIE_TX13-	B37	PCIE_RX13-	A92	SPI_MISO	B92	NCSI_RXD1
A38	GND	B38	GND	A93	GPO0	B93	NCSI_RXD0
A39	PCIE_TX12+	B39	PCIE_RX12+	A94	SPI_CLK	B94	NCSI_CRS_DV
A40	PCIE_TX12-	B40	PCIE_RX12-	A95	SPI_MOSI	B95	NCSI_TXD1
A41	GND (FIXED)	B41	GND (FIXED)	A96	TPM_PP	B96	NCSI_TXD0
A42	USB2-	B42	USB3-	A97	TYPE10# [1]	B97	SPI_CS#
A43	USB2+	B43	USB3+	A98	SER0_TX	B98	NCSI_ARB_IN
A44	USB_2_3_OC#	B44	USB_0_1_OC#	A99	SER0_RX	B99	NCSI_ARB_OUT
A45	USB0-	B45	USB1-	A100	GND (FIXED)	B100	GND (FIXED)
A46	USB0+	B46	USB1+	A101	SER1_TX	B101	FAN_PWMOUT
A47	VCC_RTC	B47	ESPI_EN# [1]	A102	SER1_RX	B102	FAN_TACHIN
A48	RSVD [1]	B48	USB0_HOST_PRSNT [1]	A103	LID#	B103	SLEEP#
A49	GBE0_SDP [1]	B49	SYS_RESET#	A104	VCC_12V	B104	VCC_12V
A50	LPC_SERIRQ/ESPI_CS1#	B50	CB_RESET#	A105	VCC_12V	B105	VCC_12V
A51	GND (FIXED)	B51	GND (FIXED)	A106	VCC_12V	B106	VCC_12V
A52	PCIE_TX5+	B52	PCIE_RX5+	A107	VCC_12V	B107	VCC_12V
A53	PCIE_TX5-	B53	PCIE_RX5-	A108	VCC_12V	B108	VCC_12V
A54	GPI0	B54	GPO1	A109	VCC_12V	B109	VCC_12V
A55	PCIE_TX4+	B55	PCIE_RX4+	A110	GND (FIXED)	B110	GND (FIXED)

Note

1. *Not connected on the conga-B7XD.*

2. *Not supported on the conga-B7XD.*

Table 18 Connector C-D Pinout

Pin	Row C	Pin	Row D	Pin	Row C	Pin	Row D
C1	GND (FIXED)	D1	GND (FIXED)	C56	PCIE_RX17-	D56	PCIE_TX17-
C2	GND	D2	GND	C57	TYPE1#	D57	TYPE2#
C3	USB_SSRX0-	D3	USB_SSTX0-	C58	PCIE_RX18+	D58	PCIE_TX18+
C4	USB_SSRX0+	D4	USB_SSTX0+	C59	PCIE_RX18-	D59	PCIE_TX18-
C5	GND	D5	GND	C60	GND (FIXED)	D60	GND (FIXED)
C6	USB_SSRX1-	D6	USB_SSTX1-	C61	PCIE_RX19+	D61	PCIE_TX19+
C7	USB_SSRX1+	D7	USB_SSTX1+	C62	PCIE_RX19-	D62	PCIE_TX19-
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	PCIE_RX20+	D65	PCIE_TX20+
C11	GND(FIXED)	D11	GND (FIXED)	C66	PCIE_RX20-	D66	PCIE_TX20-
C12	USB_SSRX3-	D12	USB_SSTX3-	C67	RAPID_SHUTDOWN	D67	GND
C13	USB_SSRX3+	D13	USB_SSTX3+	C68	PCIE_RX21+	D68	PCIE_TX21+
C14	GND	D14	GND	C69	PCIE_RX21-	D69	PCIE_TX21-
C15	10G_PHY_MDC_SCL3 [1]	D15	10G_PHY_MDIO_SDA3 [1]	C70	GND (FIXED)	D70	GND (FIXED)
C16	10G_PHY_MDC_SCL2 [1 1]	D16	10G_PHY_MDIO_SDA2 [1]	C71	PCIE_RX22+	D71	PCIE_TX22+
C17	10G_SDP2 [1]	D17	10G_SDP3 [1]	C72	PCIE_RX22-	D72	PCIE_TX22-
C18	GND	D18	GND	C73	GND	D73	GND
C19	PCIE_RX6+	D19	PCIE_TX6+	C74	PCIE_RX23+	D74	PCIE_TX23+
C20	PCIE_RX6-	D20	PCIE_TX6-	C75	PCIE_RX23-	D75	PCIE_TX23-
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	PCIE_RX24+	D78	PCIE_TX24+
C24	10G_INT2	D24	10G_INT3	C79	PCIE_RX24-	D79	PCIE_TX24-
C25	GND	D25	GND	C80	GND (FIXED)	D80	GND (FIXED)
C26	10G_KR_RX3+ [1]	D26	10G_KR_TX3+ [1]	C81	PCIE_RX25+	D81	PCIE_TX25+
C27	10G_KR_RX3- [1]	D27	10G_KR_TX3- [1]	C82	PCIE_RX25-	D82	PCIE_TX25-
C28	GND	D28	GND	C83	RSVD	D83	RSVD
C29	10G_KR_RX2+ [1]	D29	10G_KR_TX2+ [1]	C84	GND	D84	GND
C30	10G_KR_RX2- [1]	D30	10G_KR_TX2- [1]	C85	PCIE_RX26+	D85	PCIE_TX26+
C31	GND (FIXED)	D31	GND (FIXED)	C86	PCIE_RX26-	D86	PCIE_TX26-
C32	10G_SFP_SDA3 [1]	D32	10G_SFP_SCL3 [1]	C87	GND	D87	GND

Pin	Row C	Pin	Row D	Pin	Row C	Pin	Row D
C33	10G_SFP_SDA2 [1]	D33	10G_SFP_SCL2 [1]	C88	PCIE_RX27+	D88	PCIE_TX27+
C34	10G_PHY_RST_23 [1]	D34	10G_PHY_CAP_23 [1]	C89	PCIE_RX27-	D89	PCIE_TX27-
C35	10G_PHY_RST_01	D35	10G_PHY_CAP_01	C90	GND (FIXED)	D90	GND (FIXED)
C36	10G_LED_SDA	D36	RSVD [1]	C91	PCIE_RX28+	D91	PCIE_TX28+
C37	10G_LED_SCL	D37	RSVD [1]	C92	PCIE_RX28-	D92	PCIE_TX28-
C38	10G_SFP_SDA1	D38	10G_SFP_SCL1	C93	GND	D93	GND
C39	10G_SFP_SDA0	D39	10G_SFP_SCL0	C94	PCIE_RX29+	D94	PCIE_TX29+
C40	10G_SDP0	D40	10G_SDP1	C95	PCIE_RX29-	D95	PCIE_TX29-
C41	GND (FIXED)	D41	GND (FIXED)	C96	GND	D96	GND
C42	10G_KR_RX1+	D42	10G_KR_TX1+	C97	RSVD	D97	RSVD
C43	10G_KR_RX1-	D43	10G_KR_TX1-	C98	PCIE_RX30+	D98	PCIE_TX30+
C44	GND	D44	GND	C99	PCIE_RX30-	D99	PCIE_TX30-
C45	10G_PHY_MDC_SCL1	D45	10G_PHY_MDIO_SDA1	C100	GND (FIXED)	D100	GND (FIXED)
C46	10G_PHY_MDC_SCL0	D46	10G_PHY_MDIO_SDA0	C101	PCIE_RX31+	D101	PCIE_TX31+
C47	10G_INT0	D47	10G_INT1	C102	PCIE_RX31-	D102	PCIE_TX31-
C48	GND	D48	GND	C103	GND	D103	GND
C49	10G_KR_RX0+	D49	10G_KR_TX0+	C104	VCC_12V	D104	VCC_12V
C50	10G_KR_RX0-	D50	10G_KR_TX0-	C105	VCC_12V	D105	VCC_12V
C51	GND (FIXED)	D51	GND(FIXED)	C106	VCC_12V	D106	VCC_12V
C52	PCIE_RX16+	D52	PCIE_TX16+	C107	VCC_12V	D107	VCC_12V
C53	PCIE_RX16-	D53	PCIE_TX16-	C108	VCC_12V	D108	VCC_12V
C54	TYPE0#	D54	RSVD [1]	C109	VCC_12V	D109	VCC_12V
C55	PCIE_RX17+	D55	PCIE_TX17+	C110	GND (FIXED)	D110	GND (FIXED)

Note

1. *Not connected on the conga-B7XD.*

Table 19 Gigabit Ethernet Signal Descriptions

Gigabit Ethernet	Pin #	Description				I/O	PU/PD	Comment
GBE0_MDI0+ GBE0_MDI0- GBE0_MDI1+ GBE0_MDI1- GBE0_MDI2+ GBE0_MDI2- GBE0_MDI3+ GBE0_MDI3-	A13 A12 A10 A9 A7 A6 A3 A2	Gigabit Ethernet Controller 0: Media Dependent Interface Differential Pairs 0, 1, 2, 3. The MDI can operate in 1000, 100, and 10 Mbps modes. Some pairs are unused in some modes according to the following:				I/O Analog		
			1000BASE-T	100BASE-TX	10BASE-T			
		MDI[0]+/-	B1_DA+/-	TX+/-	TX+/-			
		MDI[1]+/-	B1_DB+/-	RX+/-	RX+/-			
		MDI[2]+/-	B1_DC+/-					
		MDI[3]+/-	B1_DD+/-					
GBE0_ACT#	B2	Gigabit Ethernet Controller 0 activity indicator, active low.				OD 3.3V		
GBE0_LINK#	A8	Gigabit Ethernet Controller 0 link indicator, active low.				OD 3.3V		
GBE0_LINK100#	A4	Gigabit Ethernet Controller 0 100 Mbps link indicator, active low.				OD 3.3V		
GBE0_LINK1000#	A5	Gigabit Ethernet Controller 0 1000 Mbps link indicator, active low.				OD 3.3V		
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 0 V and as high as 3.3 V. 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 250 mA or less.				REF		Not connected
GBE0_SDP	A49	Gigabit Ethernet Controller 0 Software-Definable Pin. Can also be used for IEEE1588 support such as a 1 pps signal.				I/O		Not connected

Table 20 NC-SI Signal Descriptions

Signal	Pin #	Description	I/O	PU/PD	Comment
NCSI_CLK_IN	B91	NC-SI Clock reference for receive, transmit, and control interface.	I 3.3V	PD 10K	
NCSI_RXD0 NCSI_RXD1	B93 B92	NC-SI Receive Data (from NC to BMC)	O 3.3V	PD 5k11	
NCSI_TXD0 NCSI_TXD1	B96 B95	NC-SI Transmit Data (from BMC to NC).	I 3.3V	PD 10K	
NCSI_CRS_DV	B94	NC-SI Carrier Sense/Receive Data Valid to MC, indicating that the transmitted data from NC to BMC is valid.	O 3.3V		
NCSI_TX_EN	A84	NC-SI Transmit enable.	I 3.3V	PD 10K	
NCSI_RX_ER	B89	NC-SI Receive error.	O 3.3V		
NCSI_ARB_IN	B98	NC-SI hardware arbitration input.	I 3.3V		
NCSI_ARB_OUT	B99	NC-SI hardware arbitration output.	O 3.3V		

Table 21 10 Gigabit Ethernet Signal Descriptions

Signal	Pin #	Description	I/O	PU/PD	Comment
10G_KR_TX0+ 10G_KR_TX0-	D49 D50	10GBASE-KR ports, transmit output differential pairs 0	O KR		
10G_KR_RX0+ 10G_KR_RX0-	C49 C50	10GBASE-KR ports, receive input differential pairs 0	I KR		
10G_KR_TX1+ 10G_KR_TX1-	D42 D43	10GBASE-KR ports, transmit output differential pairs 1	O KR		
10G_KR_RX1+ 10G_KR_RX1-	C42 C43	10GBASE-KR ports, receive input differential pairs 1	I KR		
10G_KR_TX2+ 10G_KR_TX2-	D29 D30	10GBASE-KR ports, transmit output differential pairs 2	O KR		Not connected
10G_KR_RX2+ 10G_KR_RX2-	C29 C30	10GBASE-KR ports, receive input differential pairs 2	I KR		Not connected
10G_KR_TX3+ 10G_KR_TX3-	D26 D27	10GBASE-KR ports, transmit output differential pairs 3	O KR		Not connected
10G_KR_RX3+ 10G_KR_RX3-	C26 C27	10GBASE-KR ports, receive input differential pairs 3	I KR		Not connected
10G_PHY_MDIO_SDA[0:3]	D46 D45 D16 D15	MDIO Mode: Management Data I/O interface mode data signal for serial data transfers between the MAC and an external PHY.	O 3.3V		10G_PHY_MDIO_SDA2 and 10G_PHY_MDIO_SDA3 are not connected
		I2C Mode: I2C data signal, of the 2-wire management interface used for serial data transfers between the MAC and an external PHY.	I/O OD 3.3V	PU 4K7	
10G_PHY_MDC_SCL[0:3]	C46 C45 C16 C15	MDIO Mode: Management Data I/O Interface mode clock signal for serial data transfers between the MAC and an external PHY.	O 3.3V		10G_PHY_MDC_SCL2 and 10G_PHY_MDC_SCL3 are not connected.
		I2C Mode: I2C Clock signal, of the 2-wire management interface used for serial data transfers between the MAC and an external PHY.	I/O OD 3.3V	PU 4K7	
10G_PHY_CAP_01	D35	PHY mode capability pin: Indicates if the PHY for 10G lanes 0 and 1 is capable of configuration by I²C. High indicates MDIO-only configuration, and low indicates configuration capability via I²C or MDIO. The actual protocol used for PHY configuration is determined by the module. Based on this input, the actual protocol used is indicated over the dedicated I²C interface.	I 3.3V	PU 4K7	
10G_PHY_CAP_23	D34	Phy mode capability pin: Indicates if the PHY for 10G lanes 2 and 3 is capable of configuration by I²C. High indicates MDIO-only configuration, and low indicates configuration capability via I²C or MDIO. The actual protocol used for PHY configuration is determined by the module. Based on this input, the actual protocol used is indicated over the dedicated I²C interface.	I 3.3V		Not connected
10G_SFP_SDA[0:3]	C39 C38 C33 C32	I2C data signal of the 2-wire management interface used by the 10GbE controller to access the management registers of an external Optical SFP module.	I/O OD 3.3V	PU 4K7	10G_SFP_SDA2 and 10G_SFP_SDA3 are not connected.

10G_SFP_SCL[0:3]	D39 D38 D33 D32	I2C clock signal of the 2-wire management interface used by the 10GbE controller to access the management registers of an external Optical SFP module.	I/O OD 3.3V	PU 2K2	10G_SFP_SCL2 and 10G_SFP_SCL3 are not connected.
10G_LED_SDA	C36	I2C Data of the 2-wire interface that transfers LED signals and PHY straps for I2C or MDIO operation of optical PHYs.	I/O OD 3.3V	PU 2K2	
10G_LED_SCL	C37	I2C Clock of the 2-wire interface that transfers LED and strap signals for I2C or MDIO operation of optical PHYs.	I/O OD 3.3V	PU 2K2	
10G_INT[0:3]	C47 D47 C24 D24	Interrupt pin from copper PHY or optical SFP Module to the 10GbE controller.	I CMOS	PU 2K2	
10G_SDP[0:3]	C40 D40 C17 D17	Software-Definable Pins. Can also be used for IEEE1588 support such as a 1pps signal.	I/O 3.3V		10G_SDP2 and 10G_SDP3 are not connected.
10G_PHY_RST_01	C35	Output signal that resets an optical PHY on port 0 and port1 (with copper PHY this signal is not used).	O 3.3V		
10G_PHY_RST_23	C34	Output signal that resets an Optical PHY on port 2 and port 3 (with copper PHY this signal is not used).	O 3.3V		Not connected.

Table 22 SATA 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
(S)ATA_ACT#	A28	ATA (parallel and serial) or SAS activity indicator, active low.	I/O 3.3V		

Table 23 PCI Express Signal Descriptions (general purpose)

Signal	Pin #	Description	I/O	PU/PD	Comment
PCIE_TX0+ PCIE_TX0-	A68 A69	PCI Express Transmit Output Differential Pairs 0	O PCIE		Supports PCI Express Base Specification, Revision 2.0. Not supported on variants with Intel® Xeon® D-1529.
PCIE_RX0+ PCIE_RX0-	B68 B69	PCI Express Receive Input Differential Pairs 0	I PCIE		
PCIE_TX1+ PCIE_TX1-	A64 A65	PCI Express Transmit Output Differential Pairs 1	O PCIE		Supports PCI Express Base Specification, Revision 2.0. Not supported on variants with Intel® Xeon® D-1529.
PCIE_RX1+ PCIE_RX1-	B64 B65	PCI Express Receive Input Differential Pairs 1	I PCIE		
PCIE_TX2+ PCIE_TX2-	A61 A62	PCI Express Transmit Output Differential Pairs 2	O PCIE		Supports PCI Express Base Specification, Revision 2.0. Not supported on variants with Intel® Xeon® D-1529.
PCIE_RX2+ PCIE_RX2-	B61 B62	PCI Express Receive Input Differential Pairs 2	I PCIE		
PCIE_TX3+ PCIE_TX3-	A58 A59	PCI Express Transmit Output Differential Pairs 3	O PCIE		Supports PCI Express Base Specification, Revision 2.0. Not supported on variants with Intel® Xeon® D-1529.
PCIE_RX3+ PCIE_RX3-	B58 B59	PCI Express Receive Input Differential Pairs 3	I PCIE		
PCIE_TX4+ PCIE_TX4-	A55 A56	PCI Express Transmit Output Differential Pairs 4	O PCIE		Supports PCI Express Base Specification, Revision 2.0. Not supported on variants with Intel® Xeon® D-1529.
PCIE_RX4+ PCIE_RX4-	B55 B56	PCI Express Receive Input Differential Pairs 4	I PCIE		
PCIE_TX5+ PCIE_TX5-	A52 A53	PCI Express Transmit Output Differential Pairs 5	O PCIE		Supports PCI Express Base Specification, Revision 2.0. Not supported on variants with Intel® Xeon® D-1529.
PCIE_RX5+ PCIE_RX5-	B52 B53	PCI Express Receive Input Differential Pairs 5	I PCIE		
PCIE_TX6+ PCIE_TX6-	D19 D20	PCI Express Transmit Output Differential Pairs 6	O PCIE		Supports PCI Express Base Specification, Revision 2.0. Not supported on variants with Intel® Xeon® D-1529.
PCIE_RX6+ PCIE_RX6-	C19 C20	PCI Express Receive Input Differential Pairs 6	I PCIE		
PCIE_TX7+ PCIE_TX7-	D22 D23	PCI Express Transmit Output Differential Pairs 7	O PCIE		Supports PCI Express Base Specification, Revision 2.0. Not supported on variants with Intel® Xeon® D-1529.
PCIE_RX7+ PCIE_RX7-	C22 C23	PCI Express Receive Input Differential Pairs 7	I PCIE		Shared with and connected to the GbE controller.
PCIE_TX8+ PCIE_TX8-	A71 A72	PCI Express Transmit Output Differential Pairs 8	O PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_RX8+ PCIE_RX8-	B71 B72	PCI Express Receive Input Differential Pairs 8	I PCIE		
PCIE_TX9+ PCIE_TX9-	A74 A75	PCI Express Transmit Output Differential Pairs 9	O PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_RX9+ PCIE_RX9-	B74 B75	PCI Express Receive Input Differential Pairs 9	I PCIE		

PCIE_TX10+ PCIE_TX10-	A77 A78	PCI Express Transmit Output Differential Pairs 10	O PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_RX10+ PCIE_RX10-	B77 B78	PCI Express Receive Input Differential Pairs 10	I PCIE		
PCIE_TX11+ PCIE_TX11-	A81 A82	PCI Express Transmit Output Differential Pairs 11	O PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_RX11+ PCIE_RX11-	B81 B82	PCI Express Receive Input Differential Pairs 11	I PCIE		
PCIE_TX12+ PCIE_TX12-	A39 A40	PCI Express Transmit Output Differential Pairs 12	O PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_RX12+ PCIE_RX12-	B39 B40	PCI Express Receive Input Differential Pairs 12	I PCIE		
PCIE_TX13+ PCIE_TX13-	A36 A37	PCI Express Transmit Output Differential Pairs 13	O PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_RX13+ PCIE_RX13-	B36 B37	PCI Express Receive Input Differential Pairs 13	I PCIE		
PCIE_TX14+ PCIE_TX14-	A25 A26	PCI Express Transmit Output Differential Pairs 14	O PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_RX14+ PCIE_RX14-	B25 B26	PCI Express Receive Input Differential Pairs 14	I PCIE		
PCIE_TX15+ PCIE_TX15-	A22 A23	PCI Express Transmit Output Differential Pairs 15	O PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_RX15+ PCIE_RX15-	B22 B23	PCI Express Receive Input Differential Pairs 15	I PCIE		
PCIE_TX16+ PCIE_TX16-	D52 D53	PCI Express Transmit Output Differential Pairs 16	O PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_RX16+ PCIE_RX16-	C52 C53	PCI Express Receive Input Differential Pairs 16	I PCIE		
PCIE_TX17+ PCIE_TX17-	D55 D56	PCI Express Transmit Output Differential Pairs 17	O PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_RX17+ PCIE_RX17-	C55 C56	PCI Express Receive Input Differential Pairs 17	I PCIE		
PCIE_TX18+ PCIE_TX18-	D58 D59	PCI Express Transmit Output Differential Pairs 18	O PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_RX18+ PCIE_RX18-	C58 C59	PCI Express Receive Input Differential Pairs 18	I PCIE		
PCIE_TX19+ PCIE_TX19-	D61 D62	PCI Express Transmit Output Differential Pairs 19	O PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_RX19+ PCIE_RX19-	C61 C62	PCI Express Receive Input Differential Pairs 19	I PCIE		
PCIE_TX20+ PCIE_TX20-	D65 D66	PCI Express Transmit Output Differential Pairs 20	O PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_RX20+ PCIE_RX20-	C65 C66	PCI Express Receive Input Differential Pairs 20	I PCIE		

PCIE_TX21+ PCIE_TX21-	D68 D69	PCI Express Transmit Output Differential Pairs 21	O PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_RX21+ PCIE_RX21-	C68 C69	PCI Express Receive Input Differential Pairs 21	I PCIE		
PCIE_TX22+ PCIE_TX22-	D71 D72	PCI Express Transmit Output Differential Pairs 22	O PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_RX22+ PCIE_RX22-	C71 C72	PCI Express Receive Input Differential Pairs 22	I PCIE		
PCIE_TX23+ PCIE_TX23-	D74 D75	PCI Express Transmit Output Differential Pairs 23	O PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_RX23+ PCIE_RX23-	C74 C75	PCI Express Receive Input Differential Pairs 23	I PCIE		
PCIE_TX24+ PCIE_TX24-	D78 D79	PCI Express Transmit Output Differential Pairs 24	O PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_RX24+ PCIE_RX24-	C78 C79	PCI Express Receive Input Differential Pairs 24	I PCIE		
PCIE_TX25+ PCIE_TX25-	D81 D82	PCI Express Transmit Output Differential Pairs 25	O PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_RX25+ PCIE_RX25-	C81 C82	PCI Express Receive Input Differential Pairs 25	I PCIE		
PCIE_TX26+ PCIE_TX26-	D85 D86	PCI Express Transmit Output Differential Pairs 26	O PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_RX26+ PCIE_RX26-	C85 C86	PCI Express Receive Input Differential Pairs 26	I PCIE		
PCIE_TX27+ PCIE_TX27-	D88 D89	PCI Express Transmit Output Differential Pairs 27	O PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_RX27+ PCIE_RX27-	C88 C89	PCI Express Receive Input Differential Pairs 27	I PCIE		
PCIE_TX28+ PCIE_TX28-	D91 D92	PCI Express Transmit Output Differential Pairs 28	O PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_RX28+ PCIE_RX28-	C91 C92	PCI Express Receive Input Differential Pairs 28	I PCIE		
PCIE_TX29+ PCIE_TX29-	D94 D95	PCI Express Transmit Output Differential Pairs 29	O PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_RX29+ PCIE_RX29-	C94 C95	PCI Express Receive Input Differential Pairs 29	I PCIE		
PCIE_TX30+ PCIE_TX30-	D98 D99	PCI Express Transmit Output Differential Pairs 30	O PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_RX30+ PCIE_RX30-	C98 C99	PCI Express Receive Input Differential Pairs 30	I PCIE		
PCIE_TX31+ PCIE_TX31-	D101 D102	PCI Express Transmit Output Differential Pairs 31	O PCIE		Supports PCI Express Base Specification, Revision 3.0
PCIE_RX31+ PCIE_RX31-	C101 C102	PCI Express Receive Input Differential Pairs 31	I 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.

Table 24 USB 2. 0 Signal Descriptions

Signal	Pin #	Description	I/O	PU/PD	Comment
USB0+ USB0-	A46 A45	USB Port 0, differential data pair	I/O		USB 2.0 compliant. Backwards compatible to USB 1.1
USB1+ USB1-	B46 B45	USB Port 1, differential data pair	I/O		USB 2.0 compliant. Backwards compatible to USB 1.1
USB2+ USB2-	A43 A42	USB Port 2, differential data pair	I/O		USB 2.0 compliant. Backwards compatible to USB 1.1
USB3+ USB3-	B43 B42	USB Port 3, differential data pair	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.
USB0_HOST_ PRSNT	B48	Module USB client may detect the presence of a USB host on USB0. A high value indicates that a host is present	I 3.3VSB		Not connected

Table 25 USB 3.0 Signal Descriptions

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

Signal	Pin #	Description	I/O	PU/PD	Comment
USB_SSRX3+ USB_SSRX3-	C13 C12	Additional receive signal differential pairs for the Superspeed USB data path	I		
USB_SSTX3+ USB_SSTX3-	D13 D12	Additional transmit signal differential pairs for the Superspeed USB data path	O		

Table 26 LPC/eSPI 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_CLK	B10	LPC clock output - 24 MHz nominal	O 3.3V		
LPC_DRQ[0:1]#	B8-B9	LPC serial DMA request	I 3.3V	PU 10K 3.3V	Not connected
LPC_SERIRQ	A50	LPC serial interrupt	I/O OD 3.3V	PU 10K 3.3V	
SUS_STAT#	B18	In LPC mode, SUS_STAT# indicates imminent suspend operation. It is used to notify LPC devices that a low power state will be entered soon. LPC devices may need to preserve memory or isolate outputs during the low power state.	O 3.3V		
ESPI_EN#	B47	This signal is used by the Carrier to indicate the operating mode of the LPC/eSPI bus. If left unconnected on the carrier, LPC mode (default) is selected. If pulled to GND on the carrier, eSPI mode is selected. This signal is pulled to a logic high on the module through a resistor. The Carrier should only float this line or pull it low.	I 3.3V		Not connected

Table 27 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 flas	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.	O 3.3VSB		
BIOS_DIS0#	A34	Selection strap to determine the BIOS boot device	I 3.3VSB	PU 10K 3.3VSB	
BIOS_DIS1#	B88	Selection strap to determine the BIOS boot device	I 3.3VSB	PU 10K 3.3VSB	

Table 28 General Purpose Serial Interface Signal Descriptions

Signal	Pin #	Description	I/O	PU/PD	Comment
SER0_TX [1]	A98	General purpose serial port transmitter	O 3.3V-T		
SER0_RX [1]	A99	General purpose serial port receiver	I 3.3V-T	PU 47K5 3.3V	
SER1_TX [1, 2]	A101	General purpose serial port transmitter	O 3.3V-T		
SER1_RX [1]	A102	General purpose serial port receiver	I 3.3V-T	PU 47K5 3.3V	

Note

1. *Pins are protected on the module by a series schotty diode. Therefore, pull-down resistor is required on the carrier board for proper logic level.*

2. *This signal has special function during the reset process. For more information, see section 8.2 "Boot Strap Signals".*

Table 29 I2C Signal Descriptions

Signal	Pin #	Description	I/O	PU/PD	Comment
I2C_CK	B33	General purpose I²C port clock output	I/O 3.3V	PU 2K2 3.3VSB	
I2C_DAT	B34	General purpose I²C port data I/O line	I/O 3.3V	PU 2K2 3.3VSB	

Table 30 Miscellaneous Signal Descriptions

Signal	Pin #	Description	I/O	PU/PD	Comment
SPKR [1]	B32	Output for audio enunciator, the "speaker" in PC-AT systems	O 3.3V		SPKR 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 [2]	B101	Fan speed control. Uses the Pulse Width Modulation (PWM) technique to control the fan's RPM.	O OD 3.3V		
FAN_TACHIN [2]	B102	Fan tachometer input.	I OD 3.3V	PU 10K 3.3V	Requires a fan with a two pulse output.
TPM_PP	A96	Physical Presence pin of Trusted Platform Module (TPM). Active high. TPM chip has an internal pull-down. This signal is used to indicate Physical Presence to the TPM.	I 3.3V	PD 1K	

Note

1. *This signal has special function during the reset process. For more information, see section 8.2 "Boot Strap Signals".*

2. *Pins are protected on the module by a series schotty diode. Therefore, pull-down resistor is required on the carrier board for proper logic level.*

Table 31 Power and System Management Signal Descriptions

Signal	Pin #	Description	I/O	PU/PD	Comment
PWRBTN#	B12	A falling edge creates a power button event. Power button events can be used to bring a system out of S5 soft off and other suspend states, as well as powering the system down. 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		
PWR_OK	B24	Power OK from main power supply. A high value indicates that the power is good. This signal can be used to delay the startup of the of module to enable the programming of FPGAs or other configurable devices on the carrier board.	I 3.3V		Set by resistor divider to accept 3.3V.
SUS_STAT#	B18	Indicates imminent suspend operation; used to notify LPC devices. Not used in eSPI implementations.	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 may be used to enable the non-standby power on a typical ATX power supply.	O 3.3VSB		Not supported. May be supported in the future
SUS_S4#	A18	Indicates system is in Suspend to Disk state. Active low output.	O 3.3VSB		
SUS_S5#	A24	Indicates system is in Soft Off state.	O 3.3VSB		
WAKE0#	B66	PCI Express wake up signal.	I 3.3VSB	PU 10K 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	Runtime event of the battery sub-system.	I 3.3VSB	PU 10K 3.3VSB	Unlike in mobile platforms, the signal does not influence the power-up behavior of the module.
LID# [1]	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# [1]	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	

Note

1. *Pins are protected on the module by a series schotty diode. Therefore, pull-down resistor is required on the carrier board for proper logic level.*

Table 32 Rapid Shutdown Signal Descriptions

Signal	Pin #	Description	I/O	PU/PD	Comment
RAPID_ SHUTDOWN	C67	Trigger for Rapid Shutdown. Must be driven to 5V though a <=50 ohm source impedance for ≥ 20 µs.	I 3.3V		Not connected.

Note

The conga-B7XD does not support Rapid Shutdown.

Table 33 Thermal Protection Signal Descriptions

Signal	Pin #	Description	I/O	PU/PD	Comment
THRM#	B35	Input from off-module temp sensor indicating an over-temp situation.	I 3.3V	PU 10K 3.3V	
THRMTRIP#	A35	Active low output indicating that the CPU has entered thermal shutdown.	O 3.3V		

Table 34 SMBus Signal Description

Signal	Pin #	Description	I/O	PU/PD	Comment
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	

Table 35 SDIO / General Purpose I/O Signal Descriptions

Signal	Pin #	Description	I/O	PU/PD	Comment
GPO0	A93	General purpose output pins	O 3.3V		
GPO1	B54	General purpose output pins	O 3.3V		
GPO2	B57	General purpose output pins	O 3.3V		
GPO3	B63	General purpose output pins	O 3.3V		
GPI0	A54	General purpose input pins; pulled high internally on the module	I 3.3V	PU 10K 3.3V	
GPI1	A63	General purpose input pins; pulled high internally on the module	I 3.3V	PU 10K 3.3V	
GPI2	A67	General purpose input pins; pulled high internally on the module	I 3.3V	PU 10K 3.3V	
GPI3	A85	General purpose input pins. Pulled high internally on the module	I 3.3V	PU 10K 3.3V	

Note

The conga-B7XD does not support SDIO.

Table 36 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, A38, A41, A51, A57, A60, A66, A70, A73, A76, A79, A80, A83, A90, A100, A110, B1, B11, B21, B31, B38, B41, B51, B60, B70, B73, B76, B79, B80, B83, 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		

Table 37 Module Type Definition Signal Description

<table>
<tr><th>Signal</th><th>Pin #</th><th>Description</th><th>I/O</th><th>Comment</th></tr>
<tr><td>TYPE0#
TYPE1#
TYPE2#</td><td>C54
C57
D57</td><td>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 and Type 10, these pins are don’t care (X).
<table>
<tr><th>TYPE2#</th><th>TYPE1#</th><th>TYPE0#</th><th></th></tr>
<tr><td>X
NC
NC
NC
NC
GND
GND
X</td><td>X
NC
NC
GND
GND
NC
NC
X</td><td>X
NC
GND
NC
GND
NC
GND
X</td><td>Pinout Type 1 (deprecated)
Pinout Type 2 (deprecated)
Pinout Type 3 (deprecated)
Pinout Type 4 (deprecated)
Pinout Type 5 (deprecated)
Pinout Type 6
Pinout Type 7
Pinout Type 10</td></tr>
</table>
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.</td><td>PDS</td><td>TYPE[0:2]# signals are available on all modules following the Type 2-6 Pinout standard.
The conga-B7XD is based on the COM Express Type 7 pinout, therefore pins C54 and D57 are connected to GND and pin C57 is not connected.</td></tr>
<tr><td>TYPE10#</td><td>A97</td><td>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.
<table>
<tr><th>TYPE10#</th><th></th></tr>
<tr><td>NC
PD
12V</td><td>Pinout R2.0
Pinout Type 10 pull down to ground with 4.7K resistor
Pinout R1.0</td></tr>
</table>
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. R3.0 module types 6 and 7 will no-connect this pin. Type 10 modules shall pull this pin to ground through a 4.7K resistor.</td><td>PDS</td><td>Not connected to indicate “Pinout R2.0”.</td></tr>
</table>

8.2 Boot Strap Signals

Table 38 Boot Strap Signal Descriptions

Signal	Pin #	Description of Boot Strap Signal	I/O	PU/PD	Comment
SPKR	B32	Output for audio enunciator, the "speaker" in PC-AT systems	I 3.3V		
NCSI_ARB_OUT	B99	NC-SI hardware arbitration output	O 3.3V	PU 10K	
SER1_TX	A101	Transmitter output for UART port 1 (serial transmit data)	I 3.3V	PD 5.1K	
NCSI_RXD1	B92	NC-SI receive data	O 3.3V	PD 5.1K	

Note

The signals listed in the table above are used as chipset configuration straps during system reset. In this condition (during reset), the COM Express or chipset internally implemented resistors pull these signals to the correct state.

Caution

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 or cause irreparable damage to the module.

9 System Resources

9.1 I/O Address Assignment

The following I/O ranges are used in the conga-B7XD module:

9.1.1 LPC Bus

Table 39 SoC I/O Range

Device	IO Address
DMA Controller	00h – 1Fh, C0h – DFh
8259 Master	20h-21h, 24h-25h, 28h-29h, 2Ch-2Dh, 30h-31h, 34h-35h, 38h-39h, 3Ch-3Dh,
Super I/O Decode Address	2E-2F, 4E-4F
8254s	40h-43h, 50h-53h
PS2 Control	60h, 64h,
NMI Controller	61h, 63h, 65h, 67h
RTC	70h-77h
Postcode (Port 80h)	80h-8Fh
INIT Register	92h
8259 Slave	A0h- A1h, A4h-A5h, A8h-A9h, ACh-ADh, B0h-B1h, B4h-B5h, B8h-B9h, BCh-BDh, 4D0h-4D1h
Legacy PCI Bus	CF8h-CFFh
Reset Control	CF9h
Active Power Management	B2h-B3h
ACPI Base Address	400h – 47Fh
GPIO Base Address	500h – 57Fh
Sata Controller (IDE Mode)	170h – 177h, 1F0h – 1F7h, 376h, 3F6h
SCU UART1	3F8h – 3FFh
SCU UART2	2F8h – 2FFh

9.1.2 congatec Board Controller I/O Range

Device	IO Address
congatec Board Controller	E00h - EFFh

9.1.3 ASPEED Microcontroller I/O Range

Device	IO Address
Serial Port 1 (UART1)	3F8-3FF, 2F8-2FF, 3E8-3EF, 2E8-2EF
Serial Port 2 (UART2)	3E8-3EF, 2E8-2EF
Serial Port 3 (UART3)	3E8-3EF, 2E8-2EF, 2F0-2F8, 2E0-2E8
Serial Port 4 (UART4)	2E8-2EF, 3E8-3EF, 2F0-2F8, 2E0-2E8
Software Wake Control	A00-A3F
Mailbox	A40-A4F
Keyboard Controller Style Interface (BMC)	CA0-CAF

9.2 PCI Configuration Space Map

Table 40 PCI Configuration Space Map

Bus Number (hex)	Device Number (hex)	Function Number (hex)	Description
00h	00h	00h	Intel Host Bridge
00h	01h	00h	Intel PCI-to-PCI Bridge
00h(1)	01h	01h	Intel PCI-to-PCI Bridge
00h	02h	00h	Intel PCI-to-PCI Bridge
00h	02h	02h	Intel PCI-to-PCI Bridge
00h	03h	00h	Intel PCI-to-PCI Bridge
00h [1]	03h	01h	Intel PCI-to-PCI Bridge
00h [1]	03h	02h	Intel PCI-to-PCI Bridge
00h [1]	03h	03h	Intel PCI-to-PCI Bridge
00h	05h	00h	Intel System Peripherals
00h	05h	01h	Intel System Peripherals
00h	05h	02h	Intel System Peripherals

00h	05h	04h	Intel I/O(x) APIC
00h	14h	00h	Intel USB 3.0 XHCI Controller
00h	16h	00h	Intel Communication Device
00h	16h	01h	Intel Communication Device
00h	1Ch	00h	Intel PCI-to-PCI Bridge
00h [1]	1Ch	01h	Intel PCI-to-PCI Bridge
00h [1]	1Ch	02h	Intel PCI-to-PCI Bridge
00h [1]	1Ch	03h	Intel PCI-to-PCI Bridge
00h	1Ch	04h	Intel PCI-to-PCI Bridge
00h [1]	1Ch	05h	Intel PCI-to-PCI Bridge
00h [1]	1Ch	06h	Intel PCI-to-PCI Bridge
00h [1]	1Ch	07h	Intel PCI-to-PCI Bridge
00h	1Dh	00h	Intel USB 2.0 EHCI
00h	1Fh	00h	Intel ISA Bridge
00h	1Fh	02h	Intel AHCI Controller/Intel IDE Controller
00h	1Fh	03h	Intel SMBUS
03h [2]	00h	00h	Intel System Peripherals
03h [2]	00h	01h	Intel System Peripherals
03h [2]	00h	02h	Intel System Peripherals
03h [2]	00h	03h	Intel System Peripherals
04h [2]	00h	00h	Intel Ethernet Controller (x552 10 Gbe)
04h [2]	00h	01h	Intel Ethernet Controller (x552 10 Gbe)
00h	1Fh	02h	Intel AHCI Controller/Intel IDE Controller
0Ch [2, 3]	00h	00h	PCI-to-PCI Bridge (Aspeed)
0Dh [2, 3]	00h	00h	VGA Controller (Aspeed)
10h	00h	00h	Intel Ethernet Controller (i210 Gbe)
0FFh	0Bh	00h	Intel System Peripherals
0FFh	0Bh	01h	Intel Performance counters
0FFh	0Bh	02h	Intel Performance counters
0FFh	0Bh	03h	Intel System Peripherals
0FFh	0Ch	00h	Intel System Peripherals
0FFh	0Ch	01h	Intel System Peripherals
0FFh	0Ch	02h	Intel System Peripherals
0FFh	0Ch	03h	Intel System Peripherals

0FFh	0Ch	04h	Intel System Peripherals
0FFh	0Ch	05h	Intel System Peripherals
0FFh	0Ch	06h	Intel System Peripherals
0FFh	0Ch	07h	Intel System Peripherals
0FFh	0Fh	00h	Intel System Peripherals
0FFh	0Fh	04h	Intel System Peripherals
0FFh	0Fh	05h	Intel System Peripherals
0FFh	0Fh	06h	Intel System Peripherals
0FFh	10h	00h	Intel System Peripherals
0FFh	10h	01h	Intel System Peripherals
0FFh	10h	05h	Intel System Peripherals
0FFh	10h	06h	Intel System Peripherals
0FFh	10h	07h	Intel System Peripherals
0FFh	12h	00h	Intel System Peripherals
0FFh	12h	01h	Intel Performance Counters
0FFh	13h	00h	Intel System Peripherals
0FFh	13h	01h	Intel System Peripherals
0FFh	13h	02h	Intel System Peripherals
0FFh	13h	03h	Intel System Peripherals
0FFh	13h	04h	Intel System Peripherals
0FFh	13h	05h	Intel System Peripherals
0FFh	13h	06h	Intel System Peripherals
0FFh	13h	07h	Intel System Peripherals
0FFh	14h	00h	Intel System Peripherals
0FFh	14h	01h	Intel System Peripherals
0FFh	14h	02h	Intel System Peripherals
0FFh	14h	03h	Intel System Peripherals
0FFh	14h	04h	Intel System Peripherals
0FFh	14h	05h	Intel System Peripherals
0FFh	14h	06h	Intel System Peripherals
0FFh	14h	07h	Intel System Peripherals
0FFh	15h	00h	Intel System Peripherals
0FFh	15h	01h	Intel System Peripherals
0FFh	15h	02h	Intel System Peripherals

0FFh	15h	03h	Intel System Peripherals
0FFh	1Eh	00h	Intel System Peripherals
0FFh	1Eh	01h	Intel System Peripherals
0FFh	1Eh	02h	Intel System Peripherals
0FFh	1Eh	03h	Intel System Peripherals
0FFh	1Eh	04h	Intel System Peripherals
0FFh	1Fh	00h	Intel System Peripherals
0FFh	1Fh	02h	Intel System Peripherals

Note

1. *This PCI to PCI bridge device may disappear when PCI lanes are combined.*
2. *The bus number may change when devices are connected to the PCI to PCI bridge.*
3. *These devices are not available if the ASPEED 2500 BMC is not implemented on the carrier board.*

9.3 I²C Bus

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

9.4 SM Bus

System Management (SM) bus signals are connected to the Intel® SoC. 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

10.1 Navigating the BIOS Setup Menu

The BIOS setup menu shows the features and options supported in the congatec BIOS. To access and navigate the BIOS setup menu, press the <DEL> or <F2> key during POST.

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.

10.2 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 for configuring the system date and time.

Feature	Options	Description
Main BIOS Version	No option	Displays the main BIOS version
OEM BIOS Version	No option	Displays the additional OEM BIOS version
Build Date	No option	Displays the date the BIOS was built
Product Revision	No option	Displays the hardware revision of the board
Serial Number	No option	Displays the serial number of the board
BC Firmware Rev.	No option	Displays the revision of the congatec board controller
MAC Address (Intel X552)	No option	Displays the MAC address of the onboard Ethernet controller
MAC Address (Intel X552)	No option	Displays the MAC address of the onboard Ethernet controller
MAC Address (Intel I210)	No option	Displays the MAC address of the onboard Ethernet controller
Boot Counter	No option	Displays the number of boot-ups (max. 16777215)
Running Time	No option	Displays how long the board is running [in hours max. 65535]
Total Memory	no option	Total amount of low voltage DDR3 present on the system
System Date	Day of week, month/day/year	Specifies the current system date Note: The date is in month-day-year format
System Time	Hour:Minute:Second	Specifies the current system time Note: The time is in 24-hour format

10.3 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:

Main	Advanced	IntelRCSetup	Server Mgmt	Boot	Security	Save & Exit
	Watchdog					
	Hardware Health Monitoring					
	LPC Generic I/O Range Decode					
	Primary Video Device Select					
	Trusted Computing					
	RTC Wake Settings					
	Module Serial Ports					
	ACPI					
	AST2500 Super IO Configuration					
	Serial Port Console Redirection					
	PCI Subsystem Settings					
	UEFI Network Stack					
	CSM & Option ROM Control					
	NVMe Configuration					
	USB					
	Board Controller Command Control					
	GPIO Configuration					
	Diagnostic Settings					
	PC Speaker					
	Module PCIe Configuration					
	Thermal Configuration					
	iSCSI Configuration					
	Intel® Ethernet Connection X552 10 GbE SFP+					
	Intel® Ethernet Connection X552 10 GbE SFP+					
	Intel® I210 Gigabit Network Connection					
	Driver Health					

10.3.1 Watchdog

Feature	Options	Description
POST Watchdog	**Disabled** 30sec 1min 2min 5min 10min 30min	Select the timeout value for the POST watchdog The watchdog is only active during the power-on-self-test of the system and provides a facility to prevent errors during boot up by performing a reset
Stop Watchdog For User Interaction	No **Yes**	Select whether the POST watchdog should be stopped during the popup boot selection menu or while waiting for setup password insertion
Runtime Watchdog	**Disabled** One-time Trigger Single Event Repeated Event	Selects the operating mode of the runtime watchdog. This watchdog will be initialized just before the operating system starts booting If set to 'One-time Trigger' the watchdog will be disabled after the first trigger If set to 'Single Event', every stage will be executed only once, then the watchdog will be disabled If set to 'Repeated Event' the last stage will be executed repeatedly until a reset occurs.
Delay	**Disabled** 10sec 30sec 1min 2min 5min 10min 30min	Select the delay time before the runtime watchdog becomes active. This ensures that an operating system has enough time to load
Event 1	ACPI Event **Reset** Power Button	Selects the type of event that will be generated when timeout 1 is reached. For more information about ACPI Event, see note below
Event 2	**Disabled** ACPI Event Reset Power Button	Selects the type of event that will be generated when timeout 2 is reached
Event 3	**Disabled** ACPI Event Reset Power Button	Selects the type of event that will be generated when timeout 3 is reached

Feature	Options	Description
Timeout 1	1sec 2sec 5sec 10sec **30sec** 1min 2min 5min 10min 30min	Selects the timeout value for the first stage watchdog event
Timeout 2	1sec 2sec 5sec 10sec **30sec** 1min 2min 5min 10min 30min	Selects the timeout value for the second stage watchdog event
Timeout 3	1sec 2sec 5sec 10sec **30sec** 1min 2min 5min 10min 30min	Selects the timeout value for the third stage watchdog event
Watchdog ACPI Event	**Shutdown** Restart	Select the operating system event that is initiated by the watchdog ACPI event. These options perform a critical but orderly operating system shutdown or restart

Note

In ACPI mode, the "Watchdog ACPI Event" handler cannot directly restart or shutdown the Operating System. 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 Operating System.*

10.3.2 Hardware Health Monitoring

Feature	Options	Description
CPU Temperature	No option	Displays the actual CPU temperature in °C.
Board Temperature	No option	Displays the actual board temperature in °C
12V Standard	No option	Displays the actual 12 volt input voltage
Input Current (12V Standard)	No option	Displays the actual input current consumed by the module
CPU Fan Speed	No option	Displays the actual CPU fan speed in RPM
Fan PWM Frequency Mode	Low Frequency **High Frequency**	Select fan PWM base frequency mode. Low frequency: 35.3Hz High frequency: 22.5 kHz
Fan PWM Frequency (kHz)	1-63 default: **31**	Select fan PWM base (1 kHz - 63 kHz). Only visible in high frequency mode
Pulses Per Revolution	1 **2** 3 4	Select the number of pulses per revolution generated by the attached fan
Fan Speed Update Interval (ms)	100 - 1000 default: **100**	A longer update interval lets the fan adjust slowly to temperature changes and generate less noise. Valid range is 100 ms to 1000 ms
Fan Speed Stepping Width	1% 2% 4% 8% 16% 32% 64% **100%**	Defines how much the output value is adjusted to a new set point within one update interval
Fan PWM Speed Settings	0%, 10%, 25%, 40%, 50%, **60%**,75%, 90%, 100%	Boot up fan speed in percent of the maximum supported speed

Feature	Options	Description
Default Fan Speed	10% 15% 20% 25% 30% 35% 40% 45% 50% 55% **60%** 65% 70% 75% 80% 85% 90% 95% 100%	Choose the fan speed value which is valid if the automatic fan speed control has been disabled
Automatic Fan Speed Control	Disabled **Enabled**	Enable or disable automatic fan speed control
Fan Control Temperature	**CPU Temperature** Board Temperature	Choose the temperature sensor used for fan speed
Lower Temperature Threshold	10 C 20 C 30 C 40 C **50 C** 60 C 70 C 80 C 90 C	At the Lower Temperature Threshold, the fan speed is set to the Lower Temperature Fan Speed. Between the Lower and Upper Temperature the temperature is adjusted gradually
Upper Temperature Threshold	20 C 30 C 40 C 50 C 60 C 70 C **80 C** 90 C 100 C	At the Upper Temperature Threshold, the fan speed reaches the Upper Temperature Fan Speed

Feature	Options	Description
Minimum Fan Speed	Fan Off 10% 15% 20% 25% 30% 35% **40%** 45% 50% 55% 60% 65% 70% 75% 80% 85% 90% 95%	If the temperature is below the Lower Temperature Threshold, the fan speed is set to the minimum fan speed
Lower Temperature Fan Speed	Fan Off 10% 15% 20% 25% 30% 35% 40% 45% 50% 55% **60%** 65% 70% 75% 80% 85% 90% 95%	At the Lower Temperature Threshold, the fan speed is set to the Lower Temperature Fan Speed. Between the Lower and Upper Temperature Threshold, the fan speed is adjusted gradually.

Feature	Options	Description
Upper Temperature Fan Speed	Fan Off 10% 15% 20% 25% 30% 35% 40% 45% 50% 55% 60% 65% 70% 75% **80%** 85% 90% 95% 100%	At the Upper Temperature Threshold, the fan speed reaches the Upper Temperature Fan Speed
Maximum Fan Speed	10% 15% 20% 25% 30% 35% 40% 45% 50% 55% 60% 65% 70% 75% 80% 85% 90% 95% **100%**	If the Temperature is above the Upper Temperature Threshold, the fan speed is set to the Maximum Fan Speed

10.3.3 LPC Generic I/O Range Decode

Note

Some features in this submenu may be overridden if you enable features that require generic I/O decode range. For example, one of the generic I/O decode range will not be visible if BMC support is enabled.

Feature	Options	Description
Generic I/O Decode Range One	No Option	If the decode range is available, displays what range is currently being decoded
Generic I/O Decode Range One	Enable **Disable**	Enable or disable the current settings for generic decode
LPC Decode Base Address	0 - FFFFF Default: 0	Base address of the region that should be decoded
LPC Decode Length	**4 bytes** 8 Bytes 16 Bytes 32 Bytes 64 Bytes 128 Bytes 256 Bytes	Length of the region that should be decoded
Generic I/O Decode Range Two	No Option	If the decode range is available, displays what range is currently being decoded
Generic I/O Decode Range Two	Enable **Disable**	Enable or disable the current settings for generic decode
LPC Decode Base Address	0 - FFFFF Default: 0	Base address of the region that should be decoded
LPC Decode Length	**4 bytes** 8 Bytes 16 Bytes 32 Bytes 64 Bytes 128 Bytes 256 Bytes	Length of the region that should be decoded
Generic I/O Decode Range Three	No Option	If the decode range is available, displays what range is currently being decoded
Generic I/O Decode Range Three	Enable **Disable**	Enable or disable the current settings for generic decode
LPC Decode Base Address	0 - FFFFF Default: 0	Base address of the region that should be decoded

LPC Decode Length	**4 bytes** 8 Bytes 16 Bytes 32 Bytes 64 Bytes 128 Bytes 256 Bytes	Length of the region that should be decoded
Generic I/O Decode Range Four	No Option	If the decode range is available, displays what range is currently being decoded
Generic I/O Decode Range Four	Enable **Disable**	Enable or disable the current settings for generic decode
LPC Decode Base Address	0 - FFFFF Default: 0	Base address of the region that should be decoded
LPC Decode Length	**4 bytes** 8 Bytes 16 Bytes 32 Bytes 64 Bytes 128 Bytes 256 Bytes	Length of the region that should be decoded

10.3.4 Primary Video Device Select

Feature	Options	Description
Select the Primary Video Device	**Auto** <detected graphics device>	From the list of detected video devices, select the device that should be used as the primary video

10.3.5 Trusted Computing

Feature	Options	Description
Security Device Support	**Disabled** Enable	Enable or disable BIOS support for security device (TPM1.2 or TPM 2.0)
Active PCR Banks	No Option	SHA-1
Available PCR banks	No option	SHA-1, SHA256
SHA-1 PCR Bank	Disabled **Enabled**	Enable or disable SHA-1 PCR Bank
SHA256 PCR Bank	**Disabled** Enabled	Enable or disable SHA-256 PCR Bank
Pending Operation	**None** TPM Clear	Schedule an operation for the security device

Feature	Options	Description
Platform Hierarchy	Disabled **Enabled**	Enable or disable Platform Hierarchy
Storage Hierarchy	Disabled **Enabled**	Enable or disable Storage Hierarchy
Endorsement	Disabled **Enabled**	Enable or disable Endorsement Hierarchy
TPM2.0 UEFI Spec Version	TCG_1_2 **TCG_2**	Select the TCG2 spec version support. TCG_1_2: the compatible mode for Win 8 / Win 10 TCG_2: Support ne TCG2 Protcol and event
Physical Presence Spec Version	**1.2** 1.3	Select to tell the OS to support PPI spec version 1.2 or 1.3. Note: some HCK tests might not support 1.3
Device Select	TPM 1.2 TPM 2.0 **Auto**	TPM 1.2 will restrict support to TPM 1.2 devices. TPM2.0 will restrict support to TPM 2.0 devices. Auto supports both options with default set to TPM 2.0 devices.

10.3.6 RTC Wake Settings

Feature	Options	Description
RTC Wake Mode	**Disabled** Wake from S5 only Wake from S4 and S5 Wake from S3, S4 and S5	Set system wake mode on alarm event. When enabled, system will wake from the specified Sx states on the specified Hour:Min:Sec
Wake-up Hour	**0** – 23	Select 0-23. For example, enter 3 for 3 am and 15 for 3 pm
Wake-up Minute	**0** – 59	Select 0-59 for the wake up minute
Wake-up Second	**0** – 59	Select 0-59 for the wake up second

10.3.7 Module Serial Ports

Feature	Options	Description
Serial Port 0	Disabled **Enabled**	Enable or disable module serial port 0
Serial Port 1	**Disabled** Enabled	Enable or disable module serial port 1

10.3.8 GPI IRQ Configuration

Feature	Options	Description
IRQ on GPI0	**Disabled** Enabled	Enable GPI to initiate the IRQ
IRQ on GPI1	**Disabled** Enabled	Enable or disable system abilitiy to hibernate (operating system S4 sleep state). This option may not be effective with some operating systems.
IRQ on GPI2	**Disabled** Enabled	Enable or disable lock of legacy resources
IRQ on GPI3	**Disabled** Enabled	Configure COM Express LID# signal to act as an ACPI lid
IRQ Select	**None**, IRQ3, IRQ4, IRQ5, IRQ6, IRQ7, IRQ9, IRQ10, IRQ11, IRQ12, IRQ14, IRQ15	

10.3.9 ACPI

Feature	Options	Description
Enable ACPI Auto Configuration	**Disabled** Enabled	Enable or disable BIOS ACPI Auto Configuration
Hibernation Support	Disabled **Enabled**	Enable or disable system ability to hibernate (operating system S4 sleep state). This option may not be effective with some operating systems
Lock Legacy Resources	**Disabled** Enabled	Enable or disable Lock of Legacy Resources
Lid Support	Disabled **Enabled**	Configure COM Express LID# Signal to act as a ACPI lid
Sleep Button Support	Disabled **Enabled**	Configure COM Express SLEEP# Signal to act as a ACPI sleep button

10.3.10 AST2500 Super IO Configuration

Feature	Options	Description
Super IO Chip	No option	Shows Super IO Chip.
▶Serial Port 1 Configuration	Submenu	Set Parameters of Serial Port 1 (COMA)
▶Serial Port 2 Configuration	Submenu	Set Parameters of Serial Port 2 (COMB)
▶Serial Port 3 Configuration	Submenu	Set Parameters of Serial Port 3 (COMC)
▶Serial Port 4 Configuration	Submenu	Set Parameters of Serial Port 4 (COMD)

10.3.10.1 Serial Port 1 Configuration Submenu

Feature	Options	Description
Serial Port	Disabled **Enabled**	Enable or disable Serial Port (COM)
Device Settings	No option	
Change Settings	**Auto** IO=3F8h; IRQ=4 ; IO=3F8h; IRQ=3,4,5,6,7,9,10,11,12; IO=2F8h; IRQ=3,4,5,6,7,9,10,11,12; IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12; IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12;	

10.3.10.2 Serial Port 2 Configuration Submenu

Feature	Options	Description
Serial Port	Enable **Disable**	Enable or disable Serial Port (COM)
Device Settings	No option	
Change Settings	**Use Automatic Settings** IO=2F8h; IRQ=3; IO=3F8h; IRQ=3,4,5,6,7,9,10,11,12; IO=2F8h; IRQ=3,4,5,6,7,9,10,11,12; IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12; IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12;	Serial Port 2 configuration options

10.3.10.3 Serial Port 3 Configuration Submenu

Feature	Options	Description
Serial Port	Enable **Disable**	Enable or disable Serial Port (COM)
Device Settings	No option	

Feature	Options	Description
Change Settings	**Use Automatic Settings** IO=3E8h; IRQ=7; IO=238h; IRQ=3,4,5,6,7,9,10,11,12; IO=228h; IRQ=3,4,5,6,7,9,10,11,12; IO=220h; IRQ=3,4,5,6,7,9,10,11,12; IO=3F8h; IRQ=3,4,5,6,7,9,10,11,12; IO=2F8h; IRQ=3,4,5,6,7,9,10,11,12; IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12; IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12;	Serial Port 3 configuration options

10.3.10.4 Serial Port 4 Configuration Submenu

Feature	Options	Description
Serial Port	Enable **Disable**	Enable or disable Serial Port (COM)
Device Settings	No option	
Change Settings	**Use Automatic Settings** IO=2E8h; IRQ=7; IO=3F8h; IRQ=3,4,5,6,7,9,10,11,12; IO=2F8h; IRQ=3,4,5,6,7,9,10,11,12; IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12; IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12; IO=2F0h; IRQ=3,4,5,6,7,9,10,11,12; IO=2E0h; IRQ=3,4,5,6,7,9,10,11,12;	Serial Port 4 configuration options

10.3.11 Serial Port Console Redirection

Feature	Options	Description
COM0	No Option	
Console Redirection	Disabled **Enabled**	Enable or disable console redirection for Serial Port 0. Only available when Serial Port 0 is enabled
▶Console Redirection Settings	Submenu	Opens console redirection configuration submenu
COM1	No Option	
Console Redirection	**Disabled** Enabled	Enable or disable console redirection for Serial Port 1. Only available when Serial Port 1 is enabled
▶Console Redirection Settings	Submenu	Opens console redirection configuration submenu
COM2	No Option	

Feature	Options	Description
Console Redirection	**Disabled** Enabled	Enable or disable console redirection for Serial Port 2. Only available when Serial Port 2 is enabled.
▶Console Redirection Settings	Submenu	Opens console redirection configuration submenu
COM3	No Option	
Console Redirection	**Disabled** Enabled	Enable or disable console redirection for Serial Port 3. Only available when Serial Port 3 is enabled
▶Console Redirection Settings	Submenu	Opens console redirection configuration submenu
COM4	No Option	
Console Redirection	**Disabled** Enabled	Enable or disable console redirection for Serial Port 4. Only available when Serial Port 4 is enabled
▶Console Redirection Settings	Submenu	Opens console redirection configuration submenu
COM5	No Option	
Console Redirection	**Disabled** Enabled	Enable or disable console redirection for Serial Port 5. Only available when Serial Port 5 is enabled
▶Console Redirection Settings	Submenu	Opens console redirection configuration submenu
▶Legacy Console Redirection Settings	Submenu	Legacy Console Redirection Settings
Serial Port for Out-of-Band Management / Windows Emergency Management Services (EMS)	No Option	
Console Redirection	**Disabled** Enabled	Enable or disable Serial Port for Out-of-Band Management/Windows Emergency Management Services
▶Console Redirection Settings	Submenu	Opens console redirection configuration submenu

10.3.11.1 Console Redirection Settings Submenu

Feature	Options	Description
Terminal Type	VT100 VT100+ VT-UTF8 **ANSI**	Select terminal type
Baudrate	9600, 19200, 38400, 57600, **115200**	Select baud rate
Data Bits	7, **8**	Set number of data bits

Feature	Options	Description
Parity	**None** Even Odd Mark Space	Select parity
Stop Bits	**1** 2	Set number of stop bits
Flow Control	**None** Hardware RTS/CTS	Select flow control
VT-UTF8 Combo Key Support	Disabled **Enabled**	Enable VT-UTF8 combination key support for ANSI/VT100 terminals
Recorder Mode	**Disabled** Enabled	With recorder mode enabled, only text output will be sent over the terminal. This is helpful to capture and record terminal data
Resolution 100x31	**Disabled** Enabled	Enables or disables extended terminal resolution
Legacy OS Redirection Resolution	**80x24** 80x25	Number of rows and columns supported for legacy OS redirection
Putty KeyPad	**VT100** LINUX XTERMR6 SCO ESCN VT400	Select FunctionKey and KeyPad on Putty
Redirection After BIOS POST	**Enabled** Disabled	If BootLoader is selected then Legacy console redirection is disabled before booting to legacy OS. Default value is always "Enable" which means legacy console redirection is enabled for legacy OS

10.3.11.2 Legacy Console Redirection Settings

Feature	Options	Description
Legacy Serial Redirection Port	**COM0** COM1 COM2 COM3 COM4 COM5	Select the COM port that legacy serial redirection will be displayed on (DOS)

Console Redirection Settings Out-of-Band Management Submenu

Feature	Options	Description
Terminal Type	VT100 VT100+ **VT-UTF8** ANSI	Select terminal type
Baudrate	9600, 19200, 38400, 57600, **115200**	Select baud rate
Flow Control	**None** Hardware RTS/CTS Sotware Xon/Xoff	
Data Bits	**8**	Set number of data bits
Parity	**None**	Select parity
Stop Bits	**1**	Set number of stop bits

10.3.12 PCI Subsystem Settings

Feature	Options	Description
PCI Bus Driver Version	No option	Shows PCI Bus Driver Version
PCI Latency Timer	**32 PCI Bus Clocks** 64 PCI Bus Clocks 96 PCI Bus Clocks 128 PCI Bus Clocks 160 PCI Bus Clocks 192 PCI Bus Clocks 224 PCI Bus Clocks 248 PCI Bus Clocks	Value to be programmed into PCI latency timer register
PCI-X Latency Timer	32 PCI Bus Clocks **64 PCI Bus Clocks** 96 PCI Bus Clocks 128 PCI Bus Clocks 160 PCI Bus Clocks 192 PCI Bus Clocks 224 PCI Bus Clocks 248 PCI Bus Clocks	Value to be programmed into PCI latency timer register
VGA Palette Snoop	**Disabled** Enabled	Enable or Disable VGA palette registers snooping
PERR# Generation	**Disabled** Enabled	Enable or disable PCI device to generate PERR#

Feature	Options	Description
SERR# Generation	**Disabled** Enabled	Enable or disable PCI device to generate SERR#
Above 4G Decoding	**Disabled** Enabled	Enables or disables 64 bit capable devices to be decoded in Above 4G Address Space (Only if system supports 64 bit PCI Decoding)
SR-IOV Support	Disabled **Enabled**	If system has SR-IOV capable PCIe devices, this option enables or disables Single Root IO Virtualization Support
BME DMA Mitigation	Disabled **Enabled**	Re-enable BUS Master Attribute disabled during PCI enumeration for PCI Bridges after SMM Locked
Don't Reset VC-TC Mapping	Disabled **Enabled**	If system has Virtual Channels, Software can reset Traffic Class mapping through Virtual Channels, to its default state. Setting this option to "Enabled" will not modify VC Resources.
▶PCI Express Settings	Submenu	Changes PCI Express settings
▶PCI Express GEN 2 Settings	Submenu	Change PCI Express GEN Devices Settings

10.3.12.1 PCI Express Settings Submenu

Feature	Options	Description
PCI Express Device Register Settings	No option	
Relaxed Ordering	**Disabled** Enabled	Enable or disable PCI Express device relaxed ordering
Extended Tag	**Disabled** Enabled	If enabled a device may use an 8-bit tag field as a requester
No Snoop	Disabled **Enabled**	Enable or disable PCI Express device "No Snoop" option
Maximum Payload	**Auto** 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
PCI Express Link Register Setting	No Option	
WARNING: Enabling ASPM may cause some PCIe devices to fail	No Option	
Extended Synch	**Disabled** Enabled	If enabled the generation of extended synchronization patterns is allowed

Feature	Options	Description
Link Training Retry	Disabled 2 3 **5**	Defines number of retry attempts software will take to retrain the link if previous training attempt was unsuccessful
Link Training Timeout (micro seconds)	**1000** 10 – 1000	Defines number of microseconds software will wait before polling link training bit in the link status register
Unpopulated Links	**Keep Link On** Disabled	In order to save power, software will disable unpopulated PCI Express Links, if this option is set to disabled
Restore PCIe Registers	Enabled **Disabled**	On non-PCI Express aware operating systems some devices may not be re-initialized correctly after S3. Setting this node to Enabled restores PCI Express configuration on S3 Resume Warning: Enabling this may cause issues with other hardware after S3 Resume

10.3.12.2 PCI Express GEN 2 Settings Submenu

Feature	Options	Description
PCI Express GEN2 Device Register Settings	No option	
Completion Timeout	**Default** Shorter Longer Disabled	Allows system software to modify the completion timeout value in device functions that support completion timeout programmability. Default: – 50 us to 50 ms
ARI Forwarding	**Disabled** Enabled	If supported by hardware and set to enabled, the downstream port disables its tradition device number field when turning a type 1 configuration request into a type 0 request.
AtomicOp Requester Enable	**Disabled** Enabled	If support by hardware and set to enabled, this function initiates AtomicOp requests only if the bus master enable bit is set in the command register
AtomicOp Egress Blocking	**Disabled** Enabled	Outbound AtomicOp requests via Egress ports will be blocked when enabled
IDO Request Enable	**Disabled** Enabled	Permits setting the number of ID-Based ordering (IDO) bit (Attribute[2]) requests to be initiated
IDO Completion Enable	**Disabled** Enabled	Permits setting the number of ID-Based ordering (IDO) bit (Attribute[2]) requests to be initiated
LTR Mechanism Enable	**Disabled** Enabled	Enables the Latency Tolerance Reporting (LTR) mechanism
End-End TLP Prefix Blocking	**Disabled** Enabled	Blocks forwarding of TLPs containing End-End TLP prefixes
PCI Express GEN2 Link Register Settings	No Option	

Feature	Options	Description
Target Link Speed	**Auto** Force to 2.5 GT/s Force to 5.0 GT/s	This sets an upper limit on link operational speed by restricting the values reported by the upstream component
Clock Power Management	**Disabled** Enabled	Allows the device to use CLKREQ# signal for power management of link clocks
Compliance SOS	**Disabled** Enabled	Forces LTSSm to send SKP Ordered Sets between sequences when sending compliance pattern or modified compliance pattern
Hardware Autonomous Width	**Enabled** Disabled	Disable the hardware's ability to change link width except for width size reduction for the purpose of correcting unstable link operation
Hardware Autonomous Speed	**Enabled** Disabled	Disable the hardware's ability to change link speed except for the purpose of correcting unstable link operation

10.3.13 UEFI Network Stack

Feature	Options	Description
Network Stack	Enabled **Disabled**	Enable or disable the UEFI network stack
IPv4 PXE Support	**Enabled** Disabled	Enable IPv4 PXE boot support. If disabled IPv6 PXE boot option will not be created
IPv6 PXE Support	**Enabled** Disabled	Enable IPv4 PXE boot support. If disabled IPv6 PXE boot option will not be created
PXE boot wait time	**0** - 5	Wait time to press ESC to abort PXE Boot
Media detect count	**1** - 50	Number of times presence of media will be checked

10.3.14 CSM & Option ROM Control

Feature	Options	Description
CSM Support	**Enabled** Disabled	Enable the Compatibility Support Module
CSM16 Module Version	No option	Display CSM Module Version number
Gate A20 Active	**Upon Request** Always	Configure legacy Gate A behavior
Option ROM Messages	**Force BIOS** Keep Current	Enable Option ROM message

Feature	Options	Description
INT19 Trap Response	**Immediate** Postponed	Define BIOS reaction on INT19 trapping by Option ROM Immediate: executes the trap right away. Postpone: executes the trap during legacy boot.
Boot Option Filter	**UEFI and Legacy** Legacy Only UEFI Only	Controls which devices or boot loaders the system should boot from
Option ROM Execution	No Option	
Network	**Do not launch** UEFI only Legacy only	Controls the execution of UEFI and legacy Network option ROMs
Storage	**Do not launch** UEFI only Legacy only	Controls the execution of UEFI and legacy Storage option ROMs
Video	Do not launch UEFI only **Legacy only**	Controls the execution of UEFI and legacy Video option ROMs
Other PCI Devices	**UEFI only** Legacy only Do not launch	Controls the execution of UEFI and legacy option ROMs for any other PCI device different to network, video and storage
Execute the X552 OpRom (10GBE)	Do Not Run the OpRom **Run the OpRom**	
Execute the i210 OpRom (GBE)	Do Not Run the OpRom **Run the OpRom**	

10.3.15 NVMe Configuration

Feature	Options	Description
NVMe controller and Drive Information	No Option	

10.3.16 USB

Feature	Options	Description
USB Module Version	No option	
USB Controllers	No option	
USB Devices	No option	Displays the detected USB devices.

Feature	Options	Description
Legacy USB Support	**Enabled** Disabled Auto	Enables legacy USB support Auto option disables legacy support if no USB devices are connected Disable option will keep USB devices available only for EFI applications and BIOS setup
xHCI Hand-off	**Enabled** Disabled	This is a workaround for OSes without xHCI hand-off support The xHCI ownership change should be claimed by xHCI OS driver
EHCI Hand-off	Enabled **Disabled**	This is a workaround for OSes without EHCI hand-off support The EHCI ownership change should be claimed by EHCI OS driver
USB Mass Storage Driver Support	Disabled **Enabled**	Enable Mass Storage Driver Support
USB Hardware delays and time-outs:	No Option	
USB Transfer Timeout	1 sec 5 sec 10 sec **20 sec**	The timeout value for control, bulk, and interrupt transfers
Device Reset Timeout	10 sec **20 sec** 30 sec 40 sec	USB legacy mass storage device start unit command timeout
Device Power -Up Delay Selection	**Auto** Manual	Define maximum time a USB device might need before it properly reports itself to the host controller Auto selects a default value which is 100 ms for a root port or derived from the hub descriptor for a hub port
Device Power -Up Delay Value	0-40 Default : **5**	Actual power-up delay value in seconds
Mass Storage Devices		
<List of available USB mass storage devices detected	**Auto** Floppy Forced FDD Hard Disk CD-ROM	Mass storage device emulation type 'Auto' enumerates devices according to their media format. Optical drives are emulated as 'CDROM' Drives with no media will be emulated according to a drive type

10.3.17 Board Controller Command Control

Feature	Options	Description
CGBC_CMD_CG_PINS	**Enabled** Disabled	Command used to set or get system configuration pin states. On Intel platform this also controls the FLash Descriptor Override (FDO).
CGBC_CMD_AVR_SPM	**Enabled** Disabled	Command needed to update the board controller firmware

10.3.18 GPIO Configuration

Feature	Options	Description
Current GPIO Configuration	No Option	
GPO 0 State	**Low** High	Set the State for GPO 0
GPO 1 State	**Low** High	Set the State for GPO 1
GPO 2 State	**Low** High	Set the State for GPO 2
GPO 3 State	**Low** High	Set the State for GPO 3
Current GPI Values	No Option	
GPI 0 State	No Option	
GPI 1 State	No Option	
GPI 2 State	No Option	
GPI 3 State	No Option	

10.3.19 Diagnostic Settings

Feature	Options	Description
Relay Interface	Disabled **I2C** SMBus BC Diagnostic Console	Select the relay interface to which the POST code will be redirected
Primary Port Addr. Lowbyte (Dec)	**128** 0 - 128	Set the address for the primary debug port. The usual address value is 0x80 (128). However, any multiple of 8 is valid for a primary debug port address, i.e. the lower three bits must be zero
Primary Port Addr. Highbyte (Dec)	**0** 0 – 128	Set the address for the primary debug port. The usual address value is 0x80 (128). However, any multiple of 8 is valid for a primary debug port address, i.e. the lower three bits must be zero
Relay Device Addres (Dec)	**226** 0 - 256	Specify the I2C/SMBus device address for a 7 segment LCD. The factory setting for the SparkFun device is 0xE2. However any even device address (bit 0 = 0) can be specified
BC Diagnostic Console Settings	No Option	
BC Diagnostic Console Interface	**Disabled** BC AUX Port BC COM Port 0 BC COM Port 1	Select the interface to be used for the BC diagnostic console output or disable the BC diagnostic console output

Feature	Options	Description
Parity Bit	**No Parity** Even Parity Odd Parity	Choose the parity bits for the bc diagnostic console interface
Stop Bits	**1 Stop Bit** 2 Stop Bits	Choose the stop bits for the bc diagnostic console interface
Data Bits	5 Data Bits 6 Data Bits 7 Data Bits **8 Data Bits**	Choose the data bits for the bc diagnostic console interface
Baudrate	1200 Baud 2400 Baud 4800 Baud **9600 Baud** 19200 Baud 28400 Baud 115200 Baud	Choose the baud rate for the BC diagnostic console interface

10.3.20 Boot Delay Settings

Feature	Options	Description
Boot delays must be between 0 and 255 seconds	No Option	
Seconds to Delay Before Memory Detection	**0** 0 - 255	Delay amount before Memory Detection
Seconds to Delay After Memory Detection	**0** 0 - 255	Delay amount after Memory Detection
Seconds to Delay Before PCI Enumeration	**0** 0 - 255	Delay amount before PCI Enumeration
Seconds to Delay After PCI Enumeration	**0** 0 - 255	Delay amount after PCI Enumeration

10.3.21 PC Speaker

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

10.3.22 Module PCIe Configuration

Feature	Options	Description
PCIe Configuration Lanes 0 – 3	**4 x1 PCIe Links** 1 x2 PCIe Link and 2 x1 PCIe Links 2 x2 PCIe Links 1 x4 PCIe Link	Choose how to configure PCIe Gen2 lanes 0 – 3
PCIe Configuration Lanes 0 – 3 Reversal	**Lanes are not reversed** Lanes are reversed	If set, lanes 0 – 3 are reversed and act as lanes 3 – 0. This is only available in x4 mode
PCIe Configuration Lanes 4 – 7	**4 x1 PCIe Lanes** 1 x2 PCIe Link and 2 x1 PCIe Links 2 x2 PCIe Links 1 x4 PCIe Link	Choose how to configure PCIe Gen2 lanes 4 – 7 NOTE: Lane 7 is routed to the i210 Gigabit Ethernet device. To enable all options for this set of lanes, the Module Gigabit Ethernet feature must be disabled in this submenu
PCIe Configuration Lanes 4 - 7 Reversal	**Lanes are not reversed** Lanes are reversed	If set, lanes 4 – 7 are reversed and act as lanes 7 – 4. This is only available in x4 mode
PCIe Configuration Lanes 8 – 15	**2 x4 PCIe Links** 1 x8 PCIe Link	Choose how to configure PCIe Gen3 Lanes 8 – 15
PCIe Configuration Lanes 16 – 31	4 x4 PCIe Links 1 x8 PCIe Link and 2 x4 PCIe Links 2 x4 PCIe Links and 1 x8 PCIe Link 2 x8 PCIe Links **1 x16 PCIe Lane**	Choose how to configure PCIe Gen3 Lanes 16 – 31
Module Gigabit Ethernet	Disabled **Enabled**	Enable or disable the on-module i210 ethernet controller
The on-module GbE uses PCIe configuration lane 7, which limits the combination of that lane	No Option	

10.3.23 Thermal Configuration

Feature	Options	Description
Processor TjMax	No Option	Displays the TjMax of the processor
Current Processor Temperature	No Option	Displays the current temperature of the processor
Processor Package Temperature	No Option	Displays the current temperature of the processor package (the temperature of the package of all the processors)
Pch Critical Temperature	No Option	Displays the temperature the PCH must reach before it causes the system to shutdown
Current Pch Temperature	No Option	Displays the current temperature of the PCH
Processor Tcc Activation Offset	**0** 0 - 15	Offset below the TjMax value that the TCC circuit will engage and cause the processor to be throttled to attempt to keep it from overheating
Pch ProcHot Temperature	**103** 50 - 130	Temperature where the PCH signals to the processor that the processor should start to throttle so try to keep the pch from overheating
Pch Throttle Level 1	**109** 50 - 130	Temperature to enable the lowest level of PCH throttling
Pch Throttle Level 2	**112** 50 - 130	Temperature to enable the medium level of PCH throttling
Pch Throttle Level 3	**115** 50 - 130	Temperature to enable the maximum level of PCH throttling

10.3.24 iSCSI Configuration

Feature	Options	Description
iSCSI initiator Name	<String Input>	The world wide unique name of iSCSI iniator. Only IQN format is accepted. Range is from 4 to 223
▶Add an Attempt	Submenu	
▶Delete Attempts	Submenu	
▶Change Attempt Order	Submenu	

10.3.25 Intel® Ethernet Connection X552 10 GbE SFP+

Feature	Options	Description
▶ NIC Configuration	Submenu	Configure 10 Gigabit Ethernet device parameters
Blind LEDs	**0** 0 – 15	Identify the physical network port by blinking the associated LED

10.3.25.1 NIC Configuration Submenu

Feature	Options	Description
Link Speed	**Auto Negotiated** 10 Mbps Half 10 Mbps Full 100 Mbps Half 100 Mbps Full	Specifies the port speed used for the selected boot protocol
Wake On LAN	**Disable** Enabled	Enables power on of the system via LAN

10.3.26 Intel® Ethernet Connection X552 10 GbE SFP+

Feature	Options	Description
► NIC Configuration	Submenu	Configure 10 Gigabit Ethernet device parameters
Blind LEDs	**0** 0 – 15	Identify the physical network port by blinking the associated LED

10.3.26.1 NIC Configuration Submenu

Feature	Options	Description
Link Speed	**Auto Negotiated** 10 Mbps Half 10 Mbps Full 100 Mbps Half 100 Mbps Full	Specifies the port speed used for the selected boot protocol
Wake On LAN	**Disable** Enabled	Enables power on of the system via LAN

10.3.27 Intel® I210 Gigabit Network Connection

Feature	Options	Description
►NIC Configuration	Submenu	Configure Gigabit Ethernet device parameters
Blind LEDs	**0** 0 – 15	Identify the physical network port by blinking the associated LED

10.3.27.1 NIC Configuration

Feature	Options	Description
Link Speed	**Auto Negotiated** 10 Mbps Half 10 Mbps Full 100 Mbps Half 100 Mbps Full	Specifies the port speed used for the selected boot protocol
Wake On LAN	**Disable** Enabled	Enables power on of the system via LAN

10.3.28 Driver Health

Feature	Options	Description
▶ Intel® 10GbE Driver 5.1.19 X64	Submenu	Provides Health Status for the drivers/controllers connected to the System
▶ Intel® 10GbE Driver 5.1.19 X64	Submenu	Provides Health Status for the drivers/controllers connected to the System
▶ Intel® PRO/1000 7.4.25 PCI-E	Submenu	Provides Health Status for the drivers/controllers connected to the System

10.3.28.1 Intel® 10GbE Driver 5.1.19 X64

Feature	Options	Description
Controller XXXXXXXX Child 0	No Option	Provides Health Status for the drivers/controllers
Intel® Ethernet Connection X552 10 GbE SFP+	No Option	Provides Health Status for the drivers/controllers

10.3.28.2 Intel® 10GbE Driver 5.1.19 X64

Feature	Options	Description
Controller XXXXXXXX Child 0	Submenu	Provides Health Status for the drivers/controllers
Intel® Ethernet Connection X552 10 GbE SFP+	Submenu	Provides Health Status for the drivers/controllers

10.3.28.3 Intel® PRO/1000 7.4.25 PCI-E

Feature	Options	Description
Controller XXXXXXXX Child 0	No option	Provides Health Status for the drivers/controllers
Intel® I210 Gigabit Network Connection	No option	Provides Health Status for the drivers/controllers

10.4 IntelRC Setup

Select the IntelRC Setup tab from the setup menu to enter the Intel Reference Code setup screen.

Main	Advanced	IntelRCSetup	Server Mgmt	Boot	Security	Save & Exit
		▶Processor Configuration				
		▶Advanced Power Management Configuration				
		▶Common RefCode Configuration				
		▶QPI Configuration				
		▶Memory Configuration				
		▶IIO Configuration				
		▶PCH Configuration				
		▶Miscellaneous Configuration				
		▶Server ME Debug Configuration				
		▶Server ME Configuration				
		▶Runtime Error Logging				
		▶Reserved Memory				

10.4.1 Processor Configuration

Feature	Options	Description
▶Per-Socket Configuration	Submenu	Change Per-Socket Settings
Processor Socket	No Option	
Processor ID	No Option	
Processor Frequency	No Option	
Processor Max Ratio	No Option	
Processor Min Ratio	No Option	

Feature	Options	Description
Microcode Revision	No Option	
L1 Cache RAM	No Option	
L2 Cache RAM	No Option	
L3 Cache RAM	No Option	
Processor 0 Version	No Option	
Hyper-Threading [All]	Disable **Enable**	Enables Hyper Threading (Software Method to Enable/Disable Logical Processor Threads)
Monitor/Mwait	Disable **Enable**	Enable or disable the Monitor/Mwait instruction
Execute Disable Bit	Disable **Enable**	When disabled, forces the XD feature flag to always return 0
Enable Intel TXT Support	**Disable** Enable	Enable Intel Trusted Execution Technology Configuration
VMX	Disable **Enable**	Enables the Vanderpool Technology (takes effect after reboot)
Enable SMX	**Disable** Enable	Enables Safer Mode Extensions
Lock Chipset	Disable **Enable**	Lock or Unlock chipset
MSR Lock Control	Disable **Enable**	Enable MSR 3Ah, MSR 0E2h and CSR 80h lock control. Power good reset is required to remove lock bits
Hardware Prefetcher	**Enable** Disable	MLC Streamer Prefetcher (MAR 1A4h Bit[0])
Adjacent Cache Prefetch	**Enable** Disable	MLC Spatial Prefetcher (MSR 1A4h Bit[1])
DCU Streamer Prefetcher	**Enable** Disable	DCU streamer prefetcher is an L1 data cache prefetcher (MSR 1A4h[2])
DCU IP Prefetcher	**Enable** Disable	DCU IP prefetcher is an L1 data cache prefetcher (MSR 1A4h[3])
DCU Mode	**32KB 8Way without ECC** 16KB 4Way with ECC	MSR 31h Bit[0]
Direct Cache Access (DCA)	Disable Enable **Auto**	Enables Direct Cache Access

Feature	Options	Description
DCA Prefetch Delay	Disable 8 16 24 **32** 40 48 56 64 72 80 88 96 104 112	DCA prefetch Delay
X2APIC	**Disable** Enable	Enable or disable extended APIC support
AES-NI	Disable **Enable**	Enable or disable NES-NI support
Down Stream PECI	**Disable** Enable	Enable PCIe Down Stream PECI write
IIO LLC Ways [10:0](Hex)	**0** 0 – FFFFFh	MSR CB_O_SLICE0_CR_II0_LLC_WAYS bitmask
QLRU Config [63:32](Hex)	**0** 0 – FFFFFFFFh	VIRTUAL_MSR_CR_QLRU_CONFIG bitmask
QLRU Config [31:0](Hex)	**0** 0 – FFFFFFFFh	VIRTUAL_MSR_R_QLRU_CONFIG bitmask
SMM Save State	**Disable** Enable	Enable or disable the SMM Save State Feature
Targeted Smi	**Disable** Enable	Enable or disable Targeted Smi Feature

10.4.1.1 Per-Socket Configuration

Feature	Options	Description
▶CPU Socket 0 Configuration	Submenu	

CPU Socket 0 Configuration

Feature	Options	Description
Cores Enable	**0** 0 – Max Cores on Processor	Number of Cores to enable 0 means all cores
IOT Cfg Cbo Bitmap(Hex)	**0** 0 – FFFFh	Each bit enables IOT/OCLA for a CBo

10.4.2 Advanced Power Management Configuration

Feature	Options	Description
LOT26 Enable	Disable **Enable**	For HEDT only Select whether CR power is turned off to empty DIMM channels
UFS	**Enabled** Disabled	Setting in PCU_MISC_CONFIG bit[28]
CPU PM Tuning	**Auto** Manual	If "Auto" is selected, all bits in MSR 1FCh keeps value as P0
EIST (P-States)	Disable **Enable**	When enabled, OS sets CPU frequency according to load. When disabled, CPU frequency is set at max non-turbo
Config TDP	**Disable** Enable	Option to disable or enable Configurable TDP
Config TDP Level	**Nominal** Level 1 Level 2	Option to set Configurable TDP level
Uncore CLR Freq OVRD	**Auto** Manual	Override Uncore max CLR freq ration programming ot MSR 0x620 bits [6:0]
Uncore Max CLR Freq	**16** 0 - 26	Uncore Max CLR freq ratio programing got MSR0x620
▶CPU P State Control	Submenu	Control CPU Frequency
▶CPU HWPM State Control	Submenu	CPU HWPM State Control Control Configuration submenu
▶CPU C State Control	Submenu	Control CPU Idle states
▶CPU T State Control	Submenu	Control CPU throttling
▶CPU Thermal Management	Submenu	CPU thermal related settings
▶CPU Advanced PM Turning	Submenu	Additional CPU power management settings
▶CPU DRAM RAPL Configuration	Submenu	DRAM RAPL control sub menu
▶SOCKET RAPL Config	Submenu	Turbo power limit settings

10.4.2.1 CPU P State Control Submen

Feature	Options	Description
P State Domain	**ALL** ONE	Per logical: Indicates the P-State domain for each logical processor in the system
P-state coordination	**HW_ALL** SW_ALL SW_ANY	Hardware coordinate is recommended over any other settings
SINGLE_PCTL	**No** Yes	MSR_CR_MISC_PWR_MGMT 0x1AA Bit[0]: SINGLE_PCTL_EN
SPD	**Disable** Enable	PCU_MISC_CONFIG Bit[30]: SPD
PL2_SAFETY_NET_ENABLE	**Disable** Enable	PCU_MISC_CONFIG Bit[1]: PL2_SAFETY_NET_ENABLE
Energy efficient P-state	Disable **Enable**	Disable prevents access to ENTERY_PERFORMANCE_BIAS
Boot performance mode	**Max Performance** Max Efficient	Select the performance state that the BIOS will set before OS handoff
Turbo Mode	Disable **Enable**	Turbo mode allows a CPU logical processor to execute a higher frequency when enough power is available
▶XE Ratio Limit	Submenu	

XE Ratio Limit

Feature	Options	Description
Overclocking Lock	Disable **Enable**	Enable or disable overclocking

10.4.2.2 CPU HWPM State Control Submenu

Feature	Options	Description
Enable CPU HWPM	**Disable** HWPM Native Mode HWPM OOB Mode	Enable CPU HWPM for CPU for better energy performance
Enable CPU Autonomous Cstate	**Disable** Enable	Enable CPU autonomous Csate which converts Halt instructions into MWAIT instructions

10.4.2.3 CPU C State Control Submenu

Feature	Options	Description
C2C3TT	**0** 0 – 255	C2 to C3 transition timer Default= 0 (meaning auto).
CPU C State	Disable **Enable**	Enables the Enhanced Cx state of the CPU. Takes effect after reboot
Package C State Limit	C0/C1 state C2 state C6 (non Retention) state **C6(Retention) state** No Limit	Package C State Limit
CPU C3 report	**Disable** Enable	Enable or disable CPU C3 (ACPI C2) report to OS. Recommended to be disabled
CPU C6 report	Disable **Enable**	Enable or disable CPU C6 (ACPI C2) report to OS. Recommended to be enabled
Enhcanced Halt Sate (C1E)	Disable **Enable**	Enables the enhanced C1E sate of the CPU. Takes effect after reboot
OS ACPI Cx	**ACPI C2** ACPI C3	Report CC3/CC6 to OS ACPI C2 or ACPI C3

10.4.2.4 CPU T State Control Submenu

Feature	Options	Description
ACPI T-States	**Disable** Enable	Enable or disable CPU Throttling by OS. Throttling reduces power consumption

Feature	Options	Description
T-State Throttle	**Default** 6.25% 12.5% 18.75% 25.0% 31.25% 37.5% 43.75% 50.0% 56.25% 62.5% 68.75% 75.0% 81.25% 87.5% 93.75%	On-Die Thermal Throttling

10.4.2.5 CPU Thermal Management Submenu

Feature	Options	Description
Thermal Monitor	Disable **Enable**	Enable or disable Thermal Monitor
PROCHOT RESPONSE	**Pn Clamping** Pm clamping	Force CPU to throttle to a lower power condition such as Pn/Pm by asserting PROCHOT# MSR 0x1FC [26] Pn = minimum frequency Pm = Max efficiency Frequency

10.4.2.6 CPU Advanced PM Turning Submenu

Feature	Options	Description
▶Energy Perf BIAS	Submenu	
▶Program PowerCTL_MSR	Submenu	
▶PP0_CURT_CFG_CTRL_MSR	Submenu	
▶Program CSR_ENTRY_CRITERIA	Submenu	
▶Program CSR_SWLTROVRD	Submenu	

Entery Perf BIAS

Feature	Options	Description
Energy Performance Tuning	**Enable** Disable	Selects whether BIOS or operating system chooses energy performance bias tuning
Enery Performance BIAS setting.	Performance **Balanced Performance** Balanced Power Power	Sets energy performance BIAS which overrides OS settings
Power/Performance Switch	Disable **Enable**	MSR 1FCh Bit[24] PWR_PERF_TUNING_ENABLE_DYN_SWITCHING
Workload Configuration	**UMA** NUMA	Optimization of the workload characterization. Balanced is recommended
Average Time Window	**23** 0 – 255	This is used to control the effective windows of the average for C0 an P0 time
PO TotalTimeThreshole Low	**35** 0 – 255	The HW switching mechanism disables the performance setting when the total P0 time is less than this threshold
P0 TotalTimeThresholeHigh	**58** 0 – 255	The HW switching mechanism enables the performance setting when the total P0 time is greater than this threshold

Program PowerCTL_MSR

Feature	Options	Description
PKG C-state Lat. Neg.	**Enable** Disable	MSR 1FCh Bit[30] PCH_NEG_DISABLE
LTR Software Input	Take SW LTR input **Ignore SW LTR input**	MSR 1FCh Bit[28] = LTR_SW_DISABLE Disable = ignore sw ltr input
SAPM Control	**Enable** Disable	MSR 1FCh Bit[22] PWR_PERF_TUNING_DISABLE_SAPM_CTRL
PHOLD_SR	**Enable** Disable	MSR 1Fc Bit[17] PHOLD_SR_DISABLE
PHOLD_CST_PREVENTION_INIT	**Enable** Disable	MSR 1FCh Bit[16] PHOLD_CST_PREVENTION_INIT
FAST_Brk_Int_En	Enable **Disable**	MSR 1FCh Bit[4] Disable = Use ‘fast” VID swing rate
FAST_Brk_Snp_En	Enable **Disable**	MSR 1FCh Bit[3] Disable = Use “fast” VID swing rate
Energency Efficient Turbo	**Enable** Disable	Energy Efficient Turbo Disable, MSR 0x1FC [19]

Program PP0_CURT_CFG_CTRL_MSR

Feature	Options	Description
PPO Current_Cfg_Ctl Ovrd	Auto **Manual**	Allows manual override for primary plan current config control
Current Config	**Disable** Enable	0 = default: do nothing 1 = manual: override current limitation in 1/8 A increments.

Program PP0_CURT_CFG_CTRL_MSR

Feature	Options	Description
PKGC_ENTRY_CRITERIA OVRD	**Auto** Manual	Allows manual override for PKG_CST_ENTRY_CRITERIA_MASK

Program CSR_SWLTROVRD

Feature	Options	Description
Snoop Latency valid	**Disable** Enable	PCODE will ignore the Snoop Latency override value
Snoop Latency Override	**Disable** Enable	Forces PCODe to always use values provided in SW_LTR_OVERD
Snoop Latency Multiplier	**0** 0 - 7	Value is multiplied by to yield a time value
Snoop Latency Value	**0** 0 - 255	Latency requirement for Snoop requests
Non-Snoop Latency Valid	**Disable** Enable	Pcode will ignore the Non-Snoop latency override value
Non-Snoop Latency Override	**Disable** Enable	Force PCODe to always use values provided in SW_LTR_OVRD
Non-Snoop Latency Multiplier	**0** 0 – 7	Value is multiplied to yield a time value
Non-Snoop Latency Value	**0** 0 - 255	Latency requirements for Non Snoop requests

10.4.2.7 CPU DRAM RAPL Config Submenu

Feature	Options	Description
DRAM RAPL Baseline	Disable DRAM RAPL Mode 0 **DRAM RAPL Mode 1**	DRAM Rapl baseline enable and baseline mode
Override BW_LIMIT_TF	**1** 0 - 16	Allows custom tuning of BW_LIMIT_TF when DRAM RAPL is enabled
DRAM RAPL Extended Range	Disable **Enable**	Select DRAM RAPL Extended Range

10.4.2.8 Socket RAPL Config Submenu

Feature	Options	Description
FAST_RAPL_NSTRIKE_PL2_DUTY_CYCLE	**64** 25 – 64	Duty cycle between 10% (25) and 25% (64)
Turbo Pwr Limit Lock	**Disable** Enable	Enable or disable locking of turbo setting
Long Pwr Limit Ovrd	Disable **Enable**	Enable or disable long term power limit override
Long Dur Pwr Limit	**0** 0 – 32767	Turbo mode long duration power limit in Watts
Long Dur Time Window	**1** 0 – 56	Long duration time windows. Value is in seconds
Pkg Clmp Lim1	Bewtee P1/P0 **Below P1**	Pkg Clamping limit 1
Short Dur Pwr Lmit En	Disable **Enable**	Enable or disable short duration power limit
Short Dur Pwr Limit	**0** 0 – 32767	If 0, value is 125% * TDP
Pkg Clmp Lim2	Bewtee P1/P0 **Below P1**	Pkg clamping limit 2

10.4.3 Common RefCode Configuration

Feature	Options	Description
MMCFG Base	**2G** 1G 3G	Select MMCFG Base
MMIOHBase	**56T** 48T 24T 16T 12T 4T 2T 1T	MMIOH Base [63:32] Must be between 4032 - 4078
MMIO High Size	**256G** 128G 512G 1024G	Select MMIO High size
Isoc Mode	**Disable**	
MeSeg Mode	**Disable** Enable Auto	
Numa	Disable **Enable**	Enable or disable non-uniform memory access (NUMA)

10.4.4 QPI Configuration

Feature	Options	Description
▶QPI General Configuration		
▶QPI Per Socket Configuration		

10.4.4.1 QPI General Configuration Submenu

Feature	Options	Description
Degrade Precedence	**Topology Precedence** Feature Precedence	Choose topology precedence to degrade features if system options are in conflict or choose feature precedence to degrade topology is system options are in conflict
Link Speed Mode	Slow **Fast**	Select the QPI link speed as either the POR speed (fast) or default speed (Slow)

Feature	Options	Description
Link Frequency Select	6.4GB/s 8.0GB/s 9.6GB/s **Auto** Auto Limited	Allows for selecting the QPI link frequency
Link L0p Enable	Disable **Enable**	Link L0p
Link L1 Enable	Disable **Enable**	Link L1
MMIO P2P Disable	**No** Yes	To disable MMIOL P2P traffic across sockets. Default is "no"(do not disable)
E2E Parity Enable	**Disable** Enable	Enable or disable E2E parity
COD Enable	Disable Enable **Auto**	Enable or disable cluster on die
Early Snoop	Disable Enable **Auto**	
Home Dir Snoop with IVT-Style OSB Enable	Disable Enable **Auto**	Enable or disable home dir snoop with IVT- style OSB

10.4.4.2 QPI Per Socket Configuration

Feature	Options	Description
▶CPU 0		

CPU 0

Feature	Options	Description
Bus Resource Allocation Ratio	**1** 0 to 8	Bus resource allocation ratio, range 0 to 8
IO Resource Allocation Ratio	**1** 0 to 8	IO resource allocation ratio, range 0 to 8

Feature	Options	Description
MMIOL Resource Allocation Ratio	**1** 0 to 8	MMIOL resource allocation ratio, range 0 to 8
IIO Disable	**No** Disable Ports and IIO without Memory hotplug Disable ports only with memory hotplug	Disable ports and clock gate IIO

10.4.5 Memory Configuration

Feature	Options	Description
Integrated Memory Controller (iMC)	No Option	
Enfoce POR	**Auto** Enforce POR Disabled Enforce Stretch Goals	Enable to enforce POR restrictions for DDR4 frequency and Voltage Programming
PPR Type	Hard PPR Soft PPR **PPR Disabled**	Select PPR Type – Hard / Soft / Disabled
PPR Error Injection test	**Disabled**	
Memory Frequnecy	**Auto** 1333 1400 1600 1800 1867 2000 2133 2200 2400 2600 2667 2800 2933 3000 3200 Reserved Reserved Reserved	Maximum memory frequency. Selections are in Mhz. Note: Do not select "Reserved"
MRC Promote Warnings	Disabled **Enabled**	Determine if MRC warnings are promoted to system level

Feature	Options	Description
Promote Warnings	Disable **Enable**	Determines if warnings are promoted to system level
Halt on mem training error	Disabled **Enabled**	Enable or disable Halt on mem training error
Multi-Threaded MRC	**Auto** Disabled Enable	Enable to execute the memory reference code multi-threaded
ECC Support	**Auto** Disable Enable	Enable or disable DDR ECC support
Enforce Timeout	**Auto** Disable Enable	Enable or disable forcing cold reset after 3 months
Enhanced Log Parsing	**Disable** Enable	Enables additional output in debug log for easier machine parsing
Backside RMT	**Auto** Disable Enable	Enable backside RMT
Rank Multiplication	**Auto** Enabled	Force the rank multiplication factor for LRDIMM
LRDIMM Module Delay	Disabled **Auto**	When disabled, MRC will not use SPD bytes 90-95 for LRDIMM module Delays In Auto, MRC will boundary check the values and use default values, if speed is 0 or out of range
MemTest	Auto **Disable** Enable	Enable or disable memory test during normal boot
MemTestLoops	**1** 0 – 65532	0 runs memtest infinitely
Dram Maintenance Test	**Auto** Disabled Enable	DRAM maintenance test during normal boot
Memory Type	RDIMMs only UDIMMs only UDIMMs and RDIMMs	Selects the memory type supported by this platform
CECC WA CH Mask	**10** 0 - 15	CH bitmask to apply CECC WA. 1 per CH. Value 2 appies WA on CH2, 3 on CH0 and 1
Training Result Offset COnfig	**Auto** Disabled Enabled	Option to offset the final memory training results

Feature	Options	Description
Attempt Fast Boot	**Auto** Disable Enable	When enabled, portions of memory reference code will be skipped when possible to increase boot speed
Attempt Fast Cold Boot	**Auto** Disable Enable	When enabled, portions of memory reference code will be skipped when possible to increase boot speed
MemTest on Fast Boot	**Auto** Disable Enable	Enable or disable memory test during fast boot
BDAT	Enabled **Disabled**	Enable or disables BDAT
Data Scrambling	**Auto** Disable Enable	Enables Data scrambling
Allow SBE during training	**Auto** Disable Enable	Allows SBE during training knob enable/disable
Platform type input for SPD page selection	**Auto** Disable Enable	This knob controls the SPD page selection feature Disabled by default
CAP ERR FLOW Feature control	**Auto** Disable Enable	This knob controls the cap err flow feature. Disabled by default
Scrambling Seed Low	**41003** 0 – 65532	Low 32 bits of the scrambling seed value
Scrambling Speed High	**54165** 0 – 65532	High 32 bits of scrambling seed value
Enable ADR	**Disabled** Hardware Triggered ADR Software Triggered ADR	Enables the detection and enabling of ADR
MC BGF threshold	**0** 0 – 15	The HA to MC BFG threshold is qused for scheduling MC request in bypass condition
DLL Reset Test	**0** 0 – 255	Set this to the number of loops to execute the DDL reset test. The test will execute RMT for the provided number of loops without DLL reset and then will execute RMT for the same number of loops with DLL reset
MC ODT Mode	**Auto** 100 Ohms 50 Ohms	Select MC ODT Mode

Feature	Options	Description
Opp read during WMM	**Auto** Disabled Enable	Enable or disable issuing read commands opportunistically during WMM
Normal Operation Duration	**1024** 0 – 65535	Set normal operation duration interval
Number of Sparking Transaction	**4** 0 – 65535	Set number of sparing transactions interval
PSMI Support	**Disabled** Enabled	PSMI Support Disable/Enable
C/A Parity Enable	**Auto** Disabled Enabled	Enable or disable DDR4 Command Address Parity
SMB Clock Frequnecy	**Auto** 400 Khz 1 Mhz	Sets DDR4 SMB Clock Frequencies for SPD Access
▶Memory Topology	Submenu	Displays memory topology with DIMM population information. Each socket has 2 nodes/iMCs and each node supports up to 2 channels and up to 3 DIMMs per channel
▶Memory Thermal	Submenu	Set memory thermal settings
▶Memory Timings & Voltage Override	Submenu	Selects the XMP profile to use
▶Memory Map	Submenu	Set memory mapping settings
▶Memory RAS Configuration	Submenu	Displays and provides option to change the memory Ras Settings
DIMM Rank Enable Mask	**Disabled** Enabled	Selects ranks to enable or disable per DIMM

10.4.5.1 Memory Topology

Feature	Options	Description
Socket0.Ch0.Dimm0	No Option	Displays memory information about the DIMM in socket 0, channel 0, Dimm Slot 0
Socket0.Ch0.Dimm1	No Option	Displays memory information about the DIMM in socket 0, channel 0, Dimm slot 1
Socket0.Ch1.Dimm0	No Option	Displays memory information about the DIMM in socket 0, channel 1, Dimm Slot 0

10.4.5.2 Memory Thermal

Feature	Options	Description
Set Throttling Mode	Disabled OLTT **CLTT**	Configure Thermal Throttling Mode
Phase Shedding	**Auto** Disabled Enable	DDR4 VR Static Phase Shedding Support
Memory Power Savings Mode	**Auto** Disabled Slow Fast APD on User Defined	Configures CKE and related Memory Power Savings Features
▶Memory Power Savings Advanced Options	Submenu	Advanced settings for CKE and related memory power savings features
MDLL Off	**Auto** Disabled Enabled	Enable to shutdown MDLL during SR
MEMHOT Throttling Mode	Disabled Output-only **Input-only**	Configure MEMHOT input and Output Mode: MEM hot sense thermal throttling or MEM hot output thermal throttling
Mem Electrical Throttling	**Disabled** Enabled Auto	Configure Memory Electrical Throttling

Memory Power Savings Advanced Options

Feature	Options	Description
CK in SR	**Auto** Driven Tri-State Pulled Low Pulled High	Configures CK behavior during self-refresh

10.4.5.3 Memory Timings & Voltage Override

Feature	Options	Description
DIMM Profile	**Disabled** Manual	Selects the XMP profile to use
Memory Frequency	**Auto** 800 1000 1067 1200 1333 1400 1600 1800 1867 2000 2133 2200 2400 2600 2667 2800 2933 3000 3200	Maximum Memory Frequency selections in Mhz. Do not select reserved
Memory Voltage	**0** 0 - 165	Selects the desired memory voltage To select 1.20 V, enter 120
Command Timing	**Auto** 1N 2N 3N	Selects the desired memory controller command timing
Refresh rate	**0** 0 - 32767	0 = Auto, otherwise time is in nano seconds
CAS Latency	**0** 0 – 32	0 – 4 = Auto, 5 – 11 = desired CAS latency
tRP	**0** 0 – 32	0 – 4 = Auto, 5 – 11 = desired tRP latency
tRCD	**0** 0 – 32	0 – 4 = Auto, 5 – 11 = desired tRCD latency
tRAS	**0** 0 – 63	0 = Auto, else desired tRAS latency
tWR	**0** 0 – 50	0 = Auto, else desired tWR latency

Feature	Options	Description
tRFC	**0** 0 – 255	0 = Auto, else desired tRFC
tRRD	**0** 0 – 255	0 = Auto, else desired tRRD
tRTP	**0** 0 – 255	0 = Auto, else desired tRTP
tWTR	**0** 0 – 255	0 = Auto, else desired tWTR
tFAW	**0** 0 – 63	0 = Auto, else desired tFAW
tRC	**0** 0 – 255	0 = Auto, else desired tRC
tCWL	**0** 0 – 31	0 = Auto, else desired tCWL

10.4.5.4 Memory Map

Feature	Options	Description
Channel Interleaving	**Auto** 1-way Interleave 2-way Interleave 3-way Interleave 4-way Interleave	Select Channel interleaving setting
Rank Interleaving	**Auto** 1-way Interleave 2-way Interleave 4-way Interleave 8-way Interleave	Select Rank Interleaving setting
IOT Memory Buffer Reservation	**0** 0 – 255	Set IOT Memory Buffer Reservation
A7 Mode	Disable **Enable**	Disable or enable A7 Mode

10.4.5.5 Memory RAS Configuration

Feature	Options	Description
Correctable Error Threshold	**32767** 1 – 32767	Correctable Error Threshold (1 – 32767) used for sparing, tagging and leaky bucket
Leaky bucket low bit	**40** 1 – 63	Leaky bucket low bit
Leaky bucket high bit	**41** 1 - 63	Leaky bucket high bit
DRAM Maintenance	**Auto** Manual Disable	Select Manual to customize DRAM Maintenance settings
DRAM Maintenance Mode	pTTR Mode **TTR Mode**	Select between pTTR and TRR mode
TRR Mode	TRR Mode A **TRR Mode B**	Select between TRR mode A and B
Patrol Scrub	Disable **Enable**	Enable or disable Patrol Scrub
Patrol Scrub Interval	**24** 1 – 24	Selects the number of hours (1-24) required to complete full scrub A value of zero means Auto
Demand Scrub	Disable **Enable**	Enable or disable Demand Scrub
Device Tagging	**Disable** Enable	Enable or disable Device Tagging
Memory Power Management	**Disable** Enable	Enable or disable Memory Power Management for this platform

10.4.6 IIO Configuration

Feature	Options	Description
IIO PCIe Link of phase	Before memory chipset init **Post chipset init**	Link training can be done either before memory chipset init or post chipset init
PCIe Train by BIOS	No **Yes**	Assume IIO is strapped for wait-for-bios because straps are unreliable in A-0 Silicon
PCIe Hot Plug	**Disable** Enable Auto Manual	Enable or disable PCIe Hot Plug globally

Feature	Options	Description
PCIe ACPI Hot Plug	**Disable** Enable Per-Port	Enable or disable PCIe ACPI Hot plug globally, or allow per port control. When disabled, MSI is generated on hotplug event, when enabled HPGPE message is generated
EV DFX Features	**Disable** Enable	Set this option to allow DFX Lock Bits to remain clear
▶IIO0 Configuration	Submenu	
▶IOAT Configuration	Submenu	All IOAT configuration options
▶IIO Generation Configuration	Submenu	Option to change the IIO General Settings
▶Intel VT for Directed I/O (VT-d)	Submenu	Press <enter> to bring up the Intel VT for Directed I/O (VT-d) configuration Menu
▶IIO South Complex Configuration	Submenu	Press <enter> to bring-up the south complex configuration menu
Gen3 Phase3 Loop Count	1 4 **16** 256	
Skip Halt on DMI Degradation	**Disable** Enable	Enable this option to avoid the system to be halted on DMI width/link degradation
Power down unused ports	No **Yes**	Power down unused ports
SLD WA Revision	**Auto**	
Rx Clock WA	**Disable** Enable	Rx Clock WA
PCI-E ASPM Support (Global)	Disable **L1 Only**	This option enables or disables the ASPM support for all downstream devices
PCIe Stop & Scream Support	**Disable** Enable	This option enables or disables PCIe strop & scream support
Snoop Response Hold Off	**6** 0 – 255	Sets Snoop Response hold off value, 256 cycles as default

10.4.6.1 IIO0 Configuration

Feature	Options	Description
IOU2 (IIO PCIe Port 1)	**x4x4** x8 Auto	Selects PCIe port Bifurcation for selected slots

Feature	Options	Description
IOU1 (IIO PCIe Port 3)	**x4x4x4x4** x4x4x8 x8x4x4 x8x8 x16 Auto	Selects PCIe port Bifurcation for selected slots
▶Socket 0 PcieD00F0 – Port 0/DMI	Submenu	Settings related to PCI Express Ports (0/1A/1B/2A/2B/2C/2D/3A/3B/3C/3D/)
▶Socket 0 PcieD01F0 - Port 1A	Submenu	
▶Socket 0 PcieD01F1 - Port 1B	Submenu	
▶Socket 0 PcieD03F0 - Port 3A	Submenu	
▶Socket 0 PcieD03F1 - Port 3B	Submenu	
▶Socket 0 PcieD03F2 - Port 3C	Submenu	
▶Socket 0 PcieD03F3 - Port 3D	Submenu	

Socket 0 PcieD00F0 – Port 0/DMI

Feature	Options	Description
Link Speed	**Auto** Gen 1 (2.5 GT/s) Gen 2 (5 GT/s)	
Override Max Link Width	**Auto** x1 x2 x4 x8 x16	
PCI-E Port DeEmphasis	-6.0 dB -2.5 dB	
PCI-E Port Link Max	No Option	
PCI-E Port Link Speed	Max Width x4	
PCI-E Port L0s Exit Latency	Gen 2 (5.0 GT/s)	
PCI-E Port L1 Exit Latency	**4uS – 8uS**	

Feature	Options	Description
Fatal Err Over	<1uS 1uS – 2uS 2uS – 4uS 4uS – 8uS **8uS – 16uS** 16uS – 32uS 32uS – 64 uS >64uS	
Corr Err Over	**Disable** Enable	
Non-Fatal Err Over	**Disable** Enable	
Corr Err Over	**Disable** Enable	
L0s Support	**Disable** Enable	

Socket 0 PcieD01F0 - Port 1A

Feature	Options	Description
PCI-E Port	**Auto** Enable Disable	In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable Disable is used to disable the port and hide its CFG space
Hot Plug Capable	**Disable** Enable	This option specifies if the link is considered Hot Plug capable
PCI-E Port Link	**Enable** Disable	This option disables the link so that the no training occurs but the CFG space is still active
Link Speed	**Auto** Gen 1 (2.5 GT/s) Gen 2 (5 GT/s) Gen 3 (8 GT/s)	
Override Max Link Width	**Auto** X1 X2 X4 X8 X16	Override the max link width that was set by bifurcation
PCI-E Port DeEmphasis	**-6.0 dB** -3.5 dB	De-Emphasis control (LNKCON2[6]) for this PCIe port

PCI-E Port Link Status	No option	
PCI-E Port Link Max	No option	
PCI-E Port Link Speed	No option	
PCI-E Port L0s Exit Latency	**4uS - 8uS**	The length of time this port requires to complete transition form L0s to L0
PCI-E Port L1 Exit Latency	<1uS 1uS - 2uS 2uS - 4uS 4uS - 8uS **8uS - 16uS** 16uS - 32uS 32uS - 64uS >64uS	The length of time this port requires to complete transition from L1 to L0
Fatal Err Over	**Disable** Enable	Enables forcing fatal error propagation to the IIO core error logic for this port
Non-Fatal Err Over	**Disable** Enable	Enables forcing non-fatal error propagation to the IIO core error logic for this port
Corr Err Over	**Disable** Enable	Enables forcing correctable error propagation to the IIO core error logic for this port
L0s Support	**Disable**	When disabled, IIO never puts its transmitter into L0s state
PM ACPI Mode	**Disable** Enable	When disabled, MSI is generated on PM event. When enabled, HPGPE message is generated
Gen3 Eq Mode	**Auto** Enable Phase 0,1,2,3 Disable Phase 0,1,2,3 Enable Phase 1 Only Enable Phase 0,1 Only Advanced Enable MMM Offset West Alt Short Channel	PCIe Gen3 Adaptive Equalization Mode
Gen3 Spec Mode	**Auto** 0.70 July 0.70 Sept 0.071 Sept	PCIe Gen3 Spec Mode
Gen3 Phase2 Mode	Hardware Adaptive Manual	

Gen3 DN Tx Preset	**Auto** P0 (-6.0/0.0 dB) P1 (-3.5/0.0 dB) P2 (-4.5/0.0 dB) P3 (-2.5/0.0 dB) P4 (0.0/0.0 dB) P5 (0.0/2.0 dB) P6 (0.0/2.5 dB) P7 (-6.0/3.5 dB) P8 (-3.5/3.5 dB) P9 (0.0/3.5 dB)	PCIe Gen3 Downstream Tx Preset
Gen3 DN Rx Preset Hint	**Auto** P0 (-6.0 dB) P1 (-7.0 dB) P2 (-8.0 dB) P3 (-9.0 dB) P4 (-10.0 dB) P5 (-11.0 dB) P6 (-12.0 dB)	PCIe Gen3 Downstream Rx Preset Hint
Gen3 UP Tx Preset	**Auto** P0 (-6.0/0.0 dB) P1 (-3.5/0.0 dB) P2 (-4.5/0.0 dB) P3 (-2.5/0.0 dB) P4 (0.0/0.0 dB) P5 (0.0/2.0 dB) P6 (0.0/2.5 dB) P7 (-6.0/3.5 dB) P8 (-3.5/3.5 dB) P9 (0.0/3.5 dB)	PCIe Gen3 Upstream Tx Preset
Hide Port?	**No** Yes	User can forcefully hide this root port from the OS
PCIe Ecrc	Disable Enable **Auto**	Enable or disable PCIe Ecrc Support for this port

Socket 0 PcieD01F1 - Port 1B

Feature	Options	Description
PCI-E Port	**Auto** Enable Disable	In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Disable is used to disable the port and hide its CFG space

Hot Plug Capable	**Disable** Enable	This option specifies if the link is considered Hot Plug capable
PCI-E Port Link	**Enable** Disable	This option disables the link so that the no training occurs but the CFG space is still active
Link Speed	**Auto** Gen 1 (2.5 GT/s) Gen 2 (5 GT/s) Gen 3 (8 GT/s)	
Override Max Link Width	**Auto** X1 X2 X4 X8 X16	Override the max link width that was set by bifurcation
PCI-E Port DeEmphasis	**-6.0 dB** -3.5 dB	De-Emphasis control (LNKCON2[6]) for this PCIe port
PCI-E Port Link Status	No option	
PCI-E Port Link Max	No option	
PCI-E Port Link Speed	No option	
PCI-E Port L0s Exit Latency	**4uS - 8uS**	The length of time this port requires to complete transition form L0s to L0
PCI-E Port L1 Exit Latency	<1uS 1uS - 2uS 2uS - 4uS 4uS - 8uS **8uS - 16uS** 16uS - 32uS 32uS - 64uS >64uS	The length of time this port requires to complete transition from L1 to L0
Fatal Err Over	**Disable** Enable	Enables forcing fatal error propagation to the IIO core error logic for this port
Non-Fatal Err Over	**Disable** Enable	Enables forcing non-fatal error propagation to the IIO core error logic for this port
Corr Err Over	**Disable** Enable	Enables forcing correctable error propagation to the IIO core error logic for this port
L0s Support	**Disable**	When disabled, IIO never puts its transmitter into L0s state
PM ACPI Mode	**Disable** Enable	When disabled, MSI is generated on PM event When enabled, HPGPE message is generated

Gen3 Eq Mode	**Auto** Enable Phase 0,1,2,3 Disable Phase 0,1,2,3 Enable Phase 1 Only Enable Phase 0,1 Only Advanced Enable MMM Offset West Alt Short Channel	PCIe Gen3 Adaptive Equalization Mode
Gen3 Spec Mode	**Auto** 0.70 July 0.70 Sept 0.071 Sept	PCIe Gen3 Spec Mode
Gen3 Phase2 Mode	Hardware Adaptive Manual	
Gen3 DN Tx Preset	**Auto** P0 (-6.0/0.0 dB) P1 (-3.5/0.0 dB) P2 (-4.5/0.0 dB) P3 (-2.5/0.0 dB) P4 (0.0/0.0 dB) P5 (0.0/2.0 dB) P6 (0.0/2.5 dB) P7 (-6.0/3.5 dB) P8 (-3.5/3.5 dB) P9 (0.0/3.5 dB)	PCIe Gen3 Downstream Tx Preset
Gen3 DN Rx Preset Hint	**Auto** P0 (-6.0 dB) P1 (-7.0 dB) P2 (-8.0 dB) P3 (-9.0 dB) P4 (-10.0 dB) P5 (-11.0 dB) P6 (-12.0 dB)	PCIe Gen3 Downstream Rx Preset Hint

Gen3 UP Tx Preset	**Auto** P0 (-6.0/0.0 dB) P1 (-3.5/0.0 dB) P2 (-4.5/0.0 dB) P3 (-2.5/0.0 dB) P4 (0.0/0.0 dB) P5 (0.0/2.0 dB) P6 (0.0/2.5 dB) P7 (-6.0/3.5 dB) P8 (-3.5/3.5 dB) P9 (0.0/3.5 dB)	PCIe Gen3 Upstream Tx Preset
Hide Port?	**No** Yes	User can forcefully hide this root port from the OS
PCIe Ecrc	Disable Enable **Auto**	Enable or disable PCIe Ecrc Support for this port

Socket 0 PcieD03F0 - Port 3A

Feature	Options	Description
PCI-E Port	**Auto** Enable Disable	In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Disable is used to disable the port and hide its CFG space
Hot Plug Capable	**Disable** Enable	This option specifies if the link is considered Hot Plug capable
PCI-E Port Link	**Enable** Disable	This option disables the link so that the no training occurs but the CFG space is still active
Link Speed	**Auto** Gen 1 (2.5 GT/s) Gen 2 (5 GT/s) Gen 3 (8 GT/s)	
Override Max Link Width	**Auto** X1 X2 X4 X8 X16	Override the max link width that was set by bifurcation
PCI-E Port DeEmphasis	**-6.0 dB** -3.5 dB	De-Emphasis control (LNKCON2[6]) for this PCIe port
PCI-E Port Link Status	No option	

PCI-E Port Link Max	No option	
PCI-E Port Link Speed	No option	
PCI-E Port L0s Exit Latency	**4uS - 8uS**	The length of time this port requires to complete transition form L0s to L0
PCI-E Port L1 Exit Latency	<1uS 1uS - 2uS 2uS - 4uS 4uS - 8uS **8uS - 16uS** 16uS - 32uS 32uS - 64uS >64uS	The length of time this port requires to complete transition from L1 to L0
Fatal Err Over	**Disable** Enable	Enables forcing fatal error propagation to the IIO core error logic for this port
Non-Fatal Err Over	**Disable** Enable	Enables forcing non-fatal error propagation to the IIO core error logic for this port
Corr Err Over	**Disable** Enable	Enables forcing correctable error propagation to the IIO core error logic for this port
L0s Support	**Disable**	When disabled, IIO never puts its transmitter into L0s state
PM ACPI Mode	**Disable** Enable	When disabled, MSI is generated on PM event. When enabled, _HPGPE message is generated
Gen3 Eq Mode	**Auto** Enable Phase 0,1,2,3 Disable Phase 0,1,2,3 Enable Phase 1 Only Enable Phase 0,1 Only Advanced Enable MMM Offset West Alt Short Channel	PCIe Gen3 Adaptive Equalization Mode
Gen3 Spec Mode	**Auto** 0.70 July 0.70 Sept 0.071 Sept	PCIe Gen3 Spec Mode
Gen3 Phase2 Mode	Hardware Adaptive Manual	

Gen3 DN Tx Preset	**Auto** P0 (-6.0/0.0 dB) P1 (-3.5/0.0 dB) P2 (-4.5/0.0 dB) P3 (-2.5/0.0 dB) P4 (0.0/0.0 dB) P5 (0.0/2.0 dB) P6 (0.0/2.5 dB) P7 (-6.0/3.5 dB) P8 (-3.5/3.5 dB) P9 (0.0/3.5 dB)	PCIe Gen3 Downstream Tx Preset
Gen3 DN Rx Preset Hint	**Auto** P0 (-6.0 dB) P1 (-7.0 dB) P2 (-8.0 dB) P3 (-9.0 dB) P4 (-10.0 dB) P5 (-11.0 dB) P6 (-12.0 dB)	PCIe Gen3 Downstream Rx Preset Hint
Gen3 UP Tx Preset	**Auto** P0 (-6.0/0.0 dB) P1 (-3.5/0.0 dB) P2 (-4.5/0.0 dB) P3 (-2.5/0.0 dB) P4 (0.0/0.0 dB) P5 (0.0/2.0 dB) P6 (0.0/2.5 dB) P7 (-6.0/3.5 dB) P8 (-3.5/3.5 dB) P9 (0.0/3.5 dB)	PCIe Gen3 Upstream Tx Preset
Hide Port?	**No** Yes	User can forcefully hide this root port from the OS
PCIe Ecrc	Disable Enable **Auto**	Enable or disable PCIe Ecrc support for this port

Socket 0 PcieD03F1 - Port 3B

Feature	Options	Description
PCI-E Port	**Auto** Enable Disable	In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Disable is used to disable the port and hide its CFG space
Hot Plug Capable	**Disable** Enable	This option specifies if the link is considered Hot Plug capable
PCI-E Port Link	**Enable** Disable	This option disables the link so that the no training occurs but the CFG space is still active
Link Speed	**Auto** Gen 1 (2.5 GT/s) Gen 2 (5 GT/s) Gen 3 (8 GT/s)	
Override Max Link Width	**Auto** X1 X2 X4 X8 X16	Override the max link width that was set by bifurcation
PCI-E Port DeEmphasis	**-6.0 dB** -3.5 dB	De-Emphasis control (LNKCON2[6]) for this PCIe port
PCI-E Port Link Status	No option	
PCI-E Port Link Max	No option	
PCI-E Port Link Speed	No option	
PCI-E Port L0s Exit Latency	**4uS - 8uS**	The length of time this port requires to complete transition form L0s to L0
PCI-E Port L1 Exit Latency	<1uS 1uS - 2uS 2uS - 4uS 4uS - 8uS **8uS - 16uS** 16uS - 32uS 32uS - 64uS >64uS	The length of time this port requires to complete transition from L1 to L0
Fatal Err Over	**Disable** Enable	Enables forcing fatal error propagation to the IIO core error logic for this port
Non-Fatal Err Over	**Disable** Enable	Enables forcing non-fatal error propagation to the IIO core error logic for this port
Corr Err Over	**Disable** Enable	Enables forcing correctable error propagation to the IIO core error logic for this port
L0s Support	**Disable**	When disabled, IIO never puts its transmitter into L0s state

PM ACPI Mode	**Disable** Enable	When disbale, MSI is generated on PM event. When enabled, _HPGPE message is generated
Gen3 Eq Mode	**Auto** Enable Phase 0,1,2,3 Disable Phase 0,1,2,3 Enable Phase 1 Only Enable Phase 0,1 Only Advanced Enable MMM Offset West Alt Short Channel	PCIe Gen3 Adaptive Equalization Mode
Gen3 Spec Mode	**Auto** 0.70 July 0.70 Sept 0.071 Sept	PCIe Gen3 Spec Mode
Gen3 Phase2 Mode	Hardware Adaptive Manual	
Gen3 DN Tx Preset	**Auto** P0 (-6.0/0.0 dB) P1 (-3.5/0.0 dB) P2 (-4.5/0.0 dB) P3 (-2.5/0.0 dB) P4 (0.0/0.0 dB) P5 (0.0/2.0 dB) P6 (0.0/2.5 dB) P7 (-6.0/3.5 dB) P8 (-3.5/3.5 dB) P9 (0.0/3.5 dB)	PCIe Gen3 Downstream Tx Preset
Gen3 DN Rx Preset Hint	**Auto** P0 (-6.0 dB) P1 (-7.0 dB) P2 (-8.0 dB) P3 (-9.0 dB) P4 (-10.0 dB) P5 (-11.0 dB) P6 (-12.0 dB)	PCIe Gen3 Downstream Rx Preset Hint

Gen3 UP Tx Preset	**Auto** P0 (-6.0/0.0 dB) P1 (-3.5/0.0 dB) P2 (-4.5/0.0 dB) P3 (-2.5/0.0 dB) P4 (0.0/0.0 dB) P5 (0.0/2.0 dB) P6 (0.0/2.5 dB) P7 (-6.0/3.5 dB) P8 (-3.5/3.5 dB) P9 (0.0/3.5 dB)	PCIe Gen3 Upstream Tx Preset
Hide Port?	**No** Yes	User can forcefully hide this root port from the OS
PCIe Ecrc	Disable Enable **Auto**	Enable or disable PCIe Ecrc Support for this port

Socket 0 PcieD03F2 - Port 3C

Feature	Options	Description
PCI-E Port	**Auto** Enable Disable	In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Disable is used to disable the port and hide its CFG space
Hot Plug Capable	**Disable** Enable	This option specifies if the link is considered Hot Plug capable
PCI-E Port Link	**Enable** Disable	This option disables the link so that the no training occurs but the CFG space is still active
Link Speed	**Auto** Gen 1 (2.5 GT/s) Gen 2 (5 GT/s) Gen 3 (8 GT/s)	
Override Max Link Width	**Auto** X1 X2 X4 X8 X16	Override the max link width that was set by bifurcation
PCI-E Port DeEmphasis	**-6.0 dB** -3.5 dB	De-Emphasis control (LNKCON2[6]) for this PCIe port
PCI-E Port Link Status	No option	

PCI-E Port Link Max	No option	
PCI-E Port Link Speed	No option	
PCI-E Port L0s Exit Latency	**4uS - 8uS**	The length of time this port requires to complete transition form L0s to L0
PCI-E Port L1 Exit Latency	<1uS 1uS - 2uS 2uS - 4uS 4uS - 8uS **8uS - 16uS** 16uS - 32uS 32uS - 64uS >64uS	The length of time this port requires to complete transition from L1 to L0
Fatal Err Over	**Disable** Enable	Enables forcing fatal error propagation to the IIO core error logic for this port
Non-Fatal Err Over	**Disable** Enable	Enables forcing non-fatal error propagation to the IIO core error logic for this port
Corr Err Over	**Disable** Enable	Enables forcing correctable error propagation to the IIO core error logic for this port
L0s Support	**Disable**	When disabled, IIO never puts its transmitter into L0s state
PM ACPI Mode	**Disable** Enable	When disabled, MSI is generated on PM event When enabled, HPGPE message is generated
Gen3 Eq Mode	**Auto** Enable Phase 0,1,2,3 Disable Phase 0,1,2,3 Enable Phase 1 Only Enable Phase 0,1 Only Advanced Enable MMM Offset West Alt Short Channel	PCIe Gen3 Adaptive Equalization Mode
Gen3 Spec Mode	**Auto** 0.70 July 0.70 Sept 0.071 Sept	PCIe Gen3 Spec Mode
Gen3 Phase2 Mode	Hardware Adaptive Manual	

Gen3 DN Tx Preset	**Auto** P0 (-6.0/0.0 dB) P1 (-3.5/0.0 dB) P2 (-4.5/0.0 dB) P3 (-2.5/0.0 dB) P4 (0.0/0.0 dB) P5 (0.0/2.0 dB) P6 (0.0/2.5 dB) P7 (-6.0/3.5 dB) P8 (-3.5/3.5 dB) P9 (0.0/3.5 dB)	PCIe Gen3 Downstream Tx Preset
Gen3 DN Rx Preset Hint	**Auto** P0 (-6.0 dB) P1 (-7.0 dB) P2 (-8.0 dB) P3 (-9.0 dB) P4 (-10.0 dB) P5 (-11.0 dB) P6 (-12.0 dB)	PCIe Gen3 Downstream Rx Preset Hint
Gen3 UP Tx Preset	**Auto** P0 (-6.0/0.0 dB) P1 (-3.5/0.0 dB) P2 (-4.5/0.0 dB) P3 (-2.5/0.0 dB) P4 (0.0/0.0 dB) P5 (0.0/2.0 dB) P6 (0.0/2.5 dB) P7 (-6.0/3.5 dB) P8 (-3.5/3.5 dB) P9 (0.0/3.5 dB)	PCIe Gen3 Upstream Tx Preset
Hide Port?	**No** Yes	User can forcefully hide this root port from the OS
PCIe Ecrc	Disable Enable **Auto**	Enable or disable PCIe Ecrc Support for this port

Socket 0 PcieD03F3 - Port 3D

Feature	Options	Description
PCI-E Port	**Auto** Enable Disable	In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Disable is used to disable the port and hide its CFG space
Hot Plug Capable	**Disable** Enable	This option specifies if the link is considered Hot Plug capable.
PCI-E Port Link	**Enable** Disable	This option disables the link so that the no training occurs but the CFG space is still active
Link Speed	**Auto** Gen 1 (2.5 GT/s) Gen 2 (5 GT/s) Gen 3 (8 GT/s)	
Override Max Link Width	**Auto** X1 X2 X4 X8 X16	Override the max link width that was set by bifurcation
PCI-E Port DeEmphasis	**-6.0 dB** -3.5 dB	De-Emphasis control (LNKCON2[6]) for this PCIe port
PCI-E Port Link Status	No option	
PCI-E Port Link Max	No option	
PCI-E Port Link Speed	No option	
PCI-E Port L0s Exit Latency	**4uS - 8uS**	The length of time this port requires to complete transition form L0s to L0
PCI-E Port L1 Exit Latency	<1uS 1uS - 2uS 2uS - 4uS 4uS - 8uS **8uS - 16uS** 16uS - 32uS 32uS - 64uS >64uS	The length of time this port requires to complete transition from L1 to L0
Fatal Err Over	**Disable** Enable	Enables forcing fatal error propagation to the IIO core error logic for this port
Non-Fatal Err Over	**Disable** Enable	Enables forcing non-fatal error propagation to the IIO core error logic for this port
Corr Err Over	**Disable** Enable	Enables forcing correctable error propagation to the IIO core error logic for this port
L0s Support	**Disable**	When disabled, IIO never puts its transmitter into L0s state

PM ACPI Mode	**Disable** Enable	When disabled, MSI is generated on PM event. When enabled, HPGPE message is generated
Gen3 Eq Mode	**Auto** Enable Phase 0,1,2,3 Disable Phase 0,1,2,3 Enable Phase 1 Only Enable Phase 0,1 Only Advanced Enable MMM Offset West Alt Short Channel	PCIe Gen3 Adaptive Equalization Mode
Gen3 Spec Mode	**Auto** 0.70 July 0.70 Sept 0.071 Sept	PCIe Gen3 Spec Mode
Gen3 Phase2 Mode	Hardware Adaptive Manual	
Gen3 DN Tx Preset	**Auto** P0 (-6.0/0.0 dB) P1 (-3.5/0.0 dB) P2 (-4.5/0.0 dB) P3 (-2.5/0.0 dB) P4 (0.0/0.0 dB) P5 (0.0/2.0 dB) P6 (0.0/2.5 dB) P7 (-6.0/3.5 dB) P8 (-3.5/3.5 dB) P9 (0.0/3.5 dB)	PCIe Gen3 Downstream Tx Preset
Gen3 DN Rx Preset Hint	**Auto** P0 (-6.0 dB) P1 (-7.0 dB) P2 (-8.0 dB) P3 (-9.0 dB) P4 (-10.0 dB) P5 (-11.0 dB) P6 (-12.0 dB)	PCIe Gen3 Downstream Rx Preset Hint

Gen3 UP Tx Preset	**Auto** P0 (-6.0/0.0 dB) P1 (-3.5/0.0 dB) P2 (-4.5/0.0 dB) P3 (-2.5/0.0 dB) P4 (0.0/0.0 dB) P5 (0.0/2.0 dB) P6 (0.0/2.5 dB) P7 (-6.0/3.5 dB) P8 (-3.5/3.5 dB) P9 (0.0/3.5 dB)	PCIe Gen3 Upstream Tx Preset
Hide Port?	**No** Yes	User can forcefully hide this root port from the OS
PCIe Ecrc	Disable Enable **Auto**	Enable or disable PCIe Ecrc Support for this port

10.4.6.2 IOAT Configuration

Feature	Options	Description
Enable IOAT	**Disable** Enable	Control to enable or disable IOAT devices
No Snoop	**Disable** Enable	Enable or disable No Snoop for each CB device
Disable TPH	**Enable** Disable	Disable TLP Processing Hint

10.4.6.3 IIO General Configuration

Feature	Options	Description
TXT DPR memory setting	1M DPR **3M DPR** 64M DPR 128M DPR 255M DPR	Allows selection of the TXT DPR size in system
IIO IoAPIC	Disable **Enable**	Enable or disable the IIO IOAPIC

10.4.6.4 Intel VT for Directed I/O (VT-d)

Feature	Options	Description
VTd Azalea VCp Optimizations	**Disable** Enable	Enable or disable Azalea VCp optimizations
Intel VT for directed I/O (VT-d)	**Disable** Enable	Enable or disable Intel Virtualization technology for Direct I/O (VT-d) by reporting the I/O device assignment to VMM through DMAR ACPI tables
ACS Control	**Disable** Enable	Enable: Programs ACS only to chipset PCIE root port bridges Disable: Programs ACS to all PCIE bridges
Interrupt Remapping	**Disable** Enable	Enable or disable VT-D interrupt remapping support
Coherency Support (Non Isoch)	**Disable** Enable	Enable or disable non-isoch VT-D Engine coherency support
Coherency Support (Isoch)	**Disable** Enable	Enable or disable Iscoh VT-D engine coherency support

10.4.6.5 IIO South Complex Configuration

Feature	Options	Description
SC GbE PF0	**Auto** Enable Disable	Forcefully enable or disable SC GbE physical function 0 For 10 GbE function 0
SC GBe PF1	**Auto** Enable Disable	Forcefully enable or disable SC GbE physical function 1 For 10 GbE function 1

Note

The SC GbE PF0 and SC GbE PF1 setup nodes are accessible on only BIOS version TSDER008 and newer.

10.4.7 PCH Configuration

Feature	Options	Description
▶PCH Devices	Submenu	Enable or disable Intel® IO Controller Hub Setting
▶PCI Express Configuration	Submenu	PCI Express Configuration settings
▶PCH Sata Configuration	Submenu	SATA devices and settings
▶USB Configuration	Submenu	USB configuration settings
▶Security Configuration	Submenu	Security Configuration settings
▶Networking	Submenu	Network devices and settings
▶Platform Thermal Configurational	Submenu	Platform thermal configuration options

10.4.7.1 PCH Devices Submenu

Feature	Options	Description
Board Capability	SUS_PWR_DN_ACT **DeepSx**	Board Capability SUS_PWR_DN_ACK -> Send Disabled to PCH DeepSx - > Show DeepSx policies
DeepSx Power Policies	**Disabled** Enabled in S5 Enabled in S4-S5 Enabled in S3-S4-S5	Configure the DeepSx Mode configuration
GP27 Wake From DeepSx	Enabled **Disabled**	Wake from DeepSx by the assertion of GP27 pin
SMBUS Device	Disabled **Enabled**	Enable or disable SMBUS Device
PCH Server Error Reporting Mode (SERM)	**Disabled** Enabled	When enabled, MCH is the final target of all error reports, otherwise SPCH is the final target for error reports
Serial IRQ Mode	Quiet **Continuous**	Configure Serial IRQ Mode
High Precision timer	**Disabled** Enabled	Enable or disable the high precision event timer
Boot Time with HPET Timer	**Disabled** Enabled	Boot time calculation with High precision event timer enabled

10.4.7.2 PCI Express Configuration Submenu

Feature	Options	Description
PCI-E ASPM Support (Global)	Disable **L1 Only**	This option enables or disables the ASPM support for all downstream devices
PCIE Clock Gating	**Disabled** Enabled	Enable or disable PCIE Clock gating for all PCH PCIe Ports
DMI Link Extended Synch Control	**Disabled** Enabled	The control of extended synch on SB side of the DMI link
Stop and Scream	**Disabled** Enabled	When enabled, DS packets on DMI with the EP bit set will have their UT bit set
PCIe-USB Glitch W/A	**Disabled** Enabled	PCIe-USB glitch W/A for bad USB devices(s) connected behind PCIe/PEG port
PCIe Root Port Function Swapping	Disabled **Enabled**	Enable PCIe root port function swapping feature to dynamically assign function 0 to enabled root port
▶PCI Express Root Port 1	Submenu	PCI Express Root Port 1 Settings
▶PCI Express Root Port 2	Submenu	PCI Express Root Port 2 Settings
▶PCI Express Root Port 3	Submenu	PCI Express Root Port 3 Settings
▶PCI Express Root Port 4	Submenu	PCI Express Root Port 4 Settings
▶PCI Express Root Port 5	Submenu	PCI Express Root Port 5 Settings
▶PCI Express Root Port 6	Submenu	PCI Express Root Port 6 Settings
▶PCI Express Root Port 7	Submenu	PCI Express Root Port 7 Settings
▶PCI Express Root Port 8	Submenu	PCI Express Root Port 8 Settings

PCI Express Root Port 1

Feature	Options	Description
PCI Express Root Port 1	Disabled **Enabled**	Control the PCI Express Root Port
URR	**Disabled** Enabled	Enable or disable PCI Express unsupported request reporting
FER	**Disabled** Enabled	Enable or disable PCI Express device fatal error reporting
NFER	**Disabled** Enabled	Enable or disable PCI Express Device non fatal error reporting

Feature	Options	Description
CER	**Disabled** Enabled	Enable or disable PCI Express Device Correctable error reporting
CTO	**Disabled** Enabled	Enable or disable PCI Express completion timer time out
SEFE	**Disabled** Enabled	Enable or disable Root PCI Express system error on fatal error
SENFE	**Disabled** Enabled	Enable or disable Root PCI Express system error on non-fatal error
SECE	**Disabled** Enabled	Enable or disable Root PCI Express system error on correctable error
PME SCI	**Disabled** Enabled	Enable or disable PCI Express pme sci
Hot Plug	**Disabled** Enabled	Enable or disable PCI Express hot plug
PCIe Speed	**Auto** Gen1 Gen2	Configure PCIe speed
PME Interrupt	**Disabled** Enabled	Enable or disable PCI Express Pme interrupt
Extra Bus Reserved	**0** 0 – 7	Extra Bus reserved for bridges behind this root bridge
Reserved Memory	**10** 1 – 20	Reserved memory and prefetchable memory (1 – 20 MB) range for this root bridge
Reserved I/O	**4** 4 – 20	Reserved I/O range for this root bridge

PCI Express Root Port 2

Feature	Options	Description
PCI Express Root Port 2	Disabled **Enabled**	Control the PCI Express Root Port
URR	**Disabled** Enabled	Enable or disable PCI Express unsupported request reporting
FER	**Disabled** Enabled	Enable or disable PCI Express device fatal error reporting
NFER	**Disabled** Enabled	Enable or disable PCI Express Device non fatal error reporting

Feature	Options	Description
CER	**Disabled** Enabled	Enable or disable PCI Express Device Correctable error reporting
CTO	**Disabled** Enabled	Enable or disable PCI Express completion timer time out
SEFE	**Disabled** Enabled	Enable or disable Root PCI Express system error on fatal error
SENFE	**Disabled** Enabled	Enable or disable Root PCI Express system error on non-fatal error
SECE	**Disabled** Enabled	Enable or disable Root PCI Express system error on correctable error
PME SCI	**Disabled** Enabled	Enable or disable PCI Express pme sci
Hot Plug	**Disabled** Enabled	Enable or disable PCI Express hot plug
PCIe Speed	**Auto** Gen1 Gen2	Configure PCIe speed
PME Interrupt	**Disabled** Enabled	Enable or disable PCI Express Pme interrupt
Extra Bus Reserved	**0** 0 – 7	Extra Bus reserved for bridges behind this root bridge
Reserved Memory	**10** 1 – 20	Reserved memory and prefetchable memory (1 – 20 MB) range for this root bridge
Reserved I/O	**4** 4 – 20	Reserved I/O range for this root bridge

PCI Express Root Port 3

Feature	Options	Description
PCI Express Root Port 3	Disabled **Enabled**	Control the PCI Express Root Port
URR	**Disabled** Enabled	Enable or disable PCI Express unsupported request reporting
FER	**Disabled** Enabled	Enable or disable PCI Express device fatal error reporting
NFER	**Disabled** Enabled	Enable or disable PCI Express device non fatal error reporting

Feature	Options	Description
CER	**Disabled** Enabled	Enable or disable PCI Express Device Correctable error reporting
CTO	**Disabled** Enabled	Enable or disable PCI Express completion timer time out
SEFE	**Disabled** Enabled	Enable or disable Root PCI Express system error on fatal error
SENFE	**Disabled** Enabled	Enable or disable Root PCI Express system error on non-fatal error
SECE	**Disabled** Enabled	Enable or disable Root PCI Express system error on correctable error
PME SCI	**Disabled** Enabled	Enable or disable PCI Express pme sci
Hot Plug	**Disabled** Enabled	Enable or disable PCI Express hot plug
PCIe Speed	**Auto** Gen1 Gen2	Configure PCIE speed
PME Interrupt	**Disabled** Enabled	Enable or disable PCI Express Pme interrupt
Extra Bus Reserved	**0** 0 – 7	Extra Bus reserved for bridges behind this root bridge
Reserved Memory	**10** 1 – 20	Reserved memory and prefetchable memory (1 – 20 MB) range for this root bridge
Reserved I/O	**4** 4 – 20	Reserved I/O range for this root bridge.

PCI Express Root Port 4

Feature	Options	Description
PCI Express Root Port 4	Disabled **Enabled**	Control the PCI Express Root Port
URR	**Disabled** Enabled	Enable or disable PCI Express unsupported request reporting
FER	**Disabled** Enabled	Enable or disable PCI Express device fatal error reporting
NFER	**Disabled** Enabled	Enable or disable PCI Express Device non fatal error reporting

Feature	Options	Description
CER	**Disabled** Enabled	Enable or disable PCI Express Device Correctable error reporting
CTO	**Disabled** Enabled	Enable or disable PCI Express completion timer time out
SEFE	**Disabled** Enabled	Enable or disable Root PCI Express system error on fatal error
SENFE	**Disabled** Enabled	Enable or disable Root PCI Express system error on non-fatal error
SECE	**Disabled** Enabled	Enable or disable Root PCI Express system error on correctable error
PME SCI	**Disabled** Enabled	Enable or disable PCI Express pme sci
Hot Plug	**Disabled** Enabled	Enable or disable PCI Express hot plug
PCIe Speed	**Auto** Gen1 Gen2	Configure PCIE speed
PME Interrupt	**Disabled** Enabled	Enable or disable PCI Express Pme interrupt
Extra Bus Reserved	**0** 0 – 7	Extra Bus reserved for bridges behind this root bridge
Reserved Memory	**10** 1 – 20	Reserved memory and prefetchable memory (1 – 20 MB) range for this root bridge
Reserved I/O	**4** 4 – 20	Reserved I/O range for this root bridge

PCI Express Root Port 5

Feature	Options	Description
PCI Express Root Port 5	Disabled **Enabled**	Control the PCI Express Root Port
URR	**Disabled** Enabled	Enable or disable PCI Express unsupported request reporting
FER	**Disabled** Enabled	Enable or disable PCI Express device fatal error reporting
NFER	**Disabled** Enabled	Enable or disable PCI Express Device non fatal error reporting

Feature	Options	Description
CER	**Disabled** Enabled	Enable or disable PCI Express Device Correctable error reporting
CTO	**Disabled** Enabled	Enable or disable PCI Express completion timer time out
SEFE	**Disabled** Enabled	Enable or disable Root PCI Express system error on fatal error
SENFE	**Disabled** Enabled	Enable or disable Root PCI Express system error on non-fatal error
SECE	**Disabled** Enabled	Enable or disable Root PCI Express system error on correctable error
PME SCI	**Disabled** Enabled	Enable or disable PCI Express pme sci
Hot Plug	**Disabled** Enabled	Enable or disable PCI Express hot plug
PCIe Speed	**Auto** Gen1 Gen2	Configure PCIE speed
PME Interrupt	**Disabled** Enabled	Enable or disable PCI Express Pme interrupt
Extra Bus Reserved	**0** 0 – 7	Extra Bus reserved for bridges behind this root bridge
Reserved Memory	**10** 1 – 20	Reserved memory and prefetchable memory (1 – 20 MB) range for this root bridge
Reserved I/O	**4** 4 – 20	Reserved I/O range for this root bridge

PCI Express Root Port 6

Feature	Options	Description
PCI Express Root Port 6	Disabled **Enabled**	Control the PCI Express Root Port
URR	**Disabled** Enabled	Enable or disable PCI Express unsupported request reporting
FER	**Disabled** Enabled	Enable or disable PCI Express device fatal error reporting
NFER	**Disabled** Enabled	Enable or disable PCI Express Device non fatal error reporting

Feature	Options	Description
CER	**Disabled** Enabled	Enable or disable PCI Express Device Correctable error reporting
CTO	**Disabled** Enabled	Enable or disable PCI Express completion timer time out
SEFE	**Disabled** Enabled	Enable or disable Root PCI Express system error on fatal error
SENFE	**Disabled** Enabled	Enable or disable Root PCI Express system error on non-fatal error
SECE	**Disabled** Enabled	Enable or disable Root PCI Express system error on correctable error
PME SCI	**Disabled** Enabled	Enable or disable PCI Express pme sci
Hot Plug	**Disabled** Enabled	Enable or disable PCI Express hot plug
PCIe Speed	**Auto** Gen1 Gen2	Configure PCIe speed
PME Interrupt	**Disabled** Enabled	Enable or disable PCI Express Pme interrupt
Extra Bus Reserved	**0** 0 – 7	Extra Bus reserved for bridges behind this root bridge
Reserved Memory	**10** 1 – 20	Reserved memory and prefetchable memory (1 – 20 MB) range for this root bridge
Reserved I/O	**4** 4 – 20	Reserved I/O range for this root bridge

PCI Express Root Port 7

Feature	Options	Description
PCI Express Root Port 7	Disabled **Enabled**	Control the PCI Express Root Port
URR	**Disabled** Enabled	Enable or disable PCI Express unsupported request reporting
FER	**Disabled** Enabled	Enable or disable PCI Express device fatal error reporting
NFER	**Disabled** Enabled	Enable or disable PCI Express Device non fatal error reporting

Feature	Options	Description
CER	**Disabled** Enabled	Enable or disable PCI Express Device Correctable error reporting
CTO	**Disabled** Enabled	Enable or disable PCI Express completion timer time out
SEFE	**Disabled** Enabled	Enable or disable Root PCI Express system error on fatal error
SENFE	**Disabled** Enabled	Enable or disable Root PCI Express system error on non-fatal error
SECE	**Disabled** Enabled	Enable or disable Root PCI Express system error on correctable error
PME SCI	**Disabled** Enabled	Enable or disable PCI Express pme sci
Hot Plug	**Disabled** Enabled	Enable or disable PCI Express hot plug
PCIe Speed	**Auto** Gen1 Gen2	Configure PCIE speed
PME Interrupt	**Disabled** Enabled	Enable or disable PCI Express Pme interrupt
Extra Bus Reserved	**0** 0 – 7	Extra Bus reserved for bridges behind this root bridge
Reserved Memory	**10** 1 – 20	Reserved memory and prefetchable memory (1 – 20 MB) range for this root bridge
Reserved I/O	**4** 4 – 20	Reserved I/O range for this root bridge

PCI Express Root Port 8

Feature	Options	Description
PCI Express Root Port 8	Disabled **Enabled**	Control the PCI Express Root Port
URR	**Disabled** Enabled	Enable or disable PCI Express unsupported request reporting
FER	**Disabled** Enabled	Enable or disable PCI Express device fatal error reporting
NFER	**Disabled** Enabled	Enable or disable PCI Express Device non fatal error reporting

Feature	Options	Description
CER	**Disabled** Enabled	Enable or disable PCI Express Device Correctable error reporting
CTO	**Disabled** Enabled	Enable or disable PCI Express completion timer time out
SEFE	**Disabled** Enabled	Enable or disable Root PCI Express system error on fatal error
SENFE	**Disabled** Enabled	Enable or disable Root PCI Express system error on non-fatal error
SECE	**Disabled** Enabled	Enable or disable Root PCI Express system error on correctable error
PME SCI	**Disabled** Enabled	Enable or disable PCI Express pme sci
Hot Plug	**Disabled** Enabled	Enable or disable PCI Express hot plug
PCIe Speed	**Auto** Gen1 Gen2	Configure PCIE speed
PME Interrupt	**Disabled** Enabled	Enable or disable PCI Express Pme interrupt
Extra Bus Reserved	**0** 0 – 7	Extra Bus reserved for bridges behind this root bridge
Reserved Memory	**10** 1 – 20	Reserved memory and prefetchable memory (1 – 20 MB) range for this root bridge
Reserved I/O	**4** 4 – 20	Reserved I/O range for this root bridge

10.4.7.3 PCH SATA Configuration Submenu

Feature	Options	Description
SATA Controller	Disabled **Enabled**	Enable or disable SATA controller
Configure SATA as	IDE **AHCI**	Identify the SATA port is connected to solid state drive or hard disk drive
SATA test mode	Enabled **Disabled**	Enable or disable SATA test mode
▶SATA Mode options	Submenu	SATA mode related options
SATA AHCI LPM		Enables or disable link power management

Feature	Options	Description
Support Aggressive Link Power Management		Enables or disable aggressive link power management

SATA Port 0	No Option	Displays device information
Port 0	Disabled **Enabled**	Enable or disable SATA port
Configure as eSATA	**Disabled** Enabled	Configures port as external SATA (eSATA)
Spin Up Device	**Disabled** Enabled	If enabled for any of the ports, staggered spin up will be performed and only the drives that have this option enabled will spin up at boot
SATA Device Type	**Hard Disk Drive** Solid State Drive	Identify the SATA port that is connected to solid state drive or hard disk drive
SATA Port 1	No Option	Displays device information
Port 1	Disabled **Enabled**	Enable or disable SATA port
Configure as eSATA	**Disabled** Enabled	Configures port as external SATA (eSATA)
Spin up Device	**Disabled** Enabled	If enabled for any of the ports, staggered spin up will be performed and only the drives that have this option enabled will spin up at boot
SATA Device Type	**Hard Disk Drive** Solid State Drive	Identify the SATA port that is connected to solid state drive or hard disk drive

SATA Mode options

Feature	Options	Description
SATA HDD Unlock	Disabled **Enabled**	Enable: HDD password unlock is enabled in the OS

10.4.7.4 USB Configuration Submenu

Feature	Options	Description
USB Precondition	Enabled **Disabled**	Precondition work on USB host controller and root ports for faster enumeration
xHCI Mode	Smart Auto **Auto** Enabled Disabled Manual	Mode of operation of xHCI controller
Trunk Clock Gating (BTCG)	**Enabled** Disabled	Enable or disable BTCG
XHCI Pre-Boot Driver	**Enabled** Disabled	Enable or disable XHCI Pre-Boot driver support
Route USB 2.0 Pins to which HC?	Route Per-Pin **Route all pints to EHCI** Route all pins to XHCI	
Enable USB 3.0 pins	Select Per-Pin Disable all pins **Enable all pin**s	
Usb Ports Per-Port disable Control	**Disabled** Enabled	Control each of the USB ports individually
XHCI Ide L1	**Enabled** Disabled	Enables XHCI idle L1 Disable to workaround the USB hot plug fail after 1 hot plug removal Turn off the system mechanically for the new settings to take effect
USB XHCI Interrupt Remap WA	**Enabled** Disabled	Enable or disable USB XHCI x116 SA Enable: hides MSI capabilities on XHCI

10.4.7.5 Security Configuration Submenu

Feature	Options	Description
GPIO LockDown	No Option	Prevent unauthorized modification of the SoC GPIOs
RTC Lock	No Option	Prevent modification of the RTC clock after BIOS timeframe
BIOS Lock	No Option	Block unauthorized attempts to write or erase the BIOS flash part
Host Flash Lock-Down	No Option	Prevent unauthorized Host flash modifications
GbE Flash Lock-Down	No Option	Prevent GbE Flash modifications Note: this relates to integrated i218 device, which is not used in congatec design

10.4.7.6 Networking Submenu

Feature	Options	Description
PCH Internal LAN	**Enable** Disable	Enable or disable PCH Internal LAN
Wake on LAN	Enable **Disable**	Enable or disable integrated LAN to wake the system
SLP_LAN# Low on DC Power	**Enable** Disable	Enable or disable SLP_LAN# low on dc power
PXE ROM	Enable **Disable**	Enable or disable PXE ROM for onboard LAN Note: This relates to integrated i218 device, which is not used in the congatec design
EFI Network	Enable **Disable**	Enable or disable EFI network support for onboard LAN Note: This relates to integrated i218 device, which is not used in the congatec design

10.4.7.7 Platform Thermal Configuration Submenu

Feature	Options	Description
PCH Thermal Device	**Enable** Disable	Enable or disable PCH Thermal Device (D31:F6)
Alert Enable Lock	Enable **Disable**	Lock all alert enable settings
PCH Alert	Disabled **Enabled**	PCH Alert pin enable
DIMM Alert	Disabled **Enabled**	DIMM Alert pin enable
Enable Thermal Lock-Down	Disable **Enable**	Enable will execute thermal programming Use disable as workaround for PCHHOT

10.4.8 Miscellaneous Configuration

Feature	Options	Description
PCIe Max Read Request Size	Auto leave HW default values 128B 256B 512B 2014B 2048B **4096B**	Set max read request size
PCIe Latency Tolerance Reporting	Disable **Enable**	
PCI Minimum Secondary Bus Number	**1** 0 – 223	Specify the PCI minimum second bus number for the system
PCIe Extended Tag Enable	Auto Disable **Enable**	Enable or disable Extended Tag Enable field support
PCIe AtomicOp Request Support	**Disable** Enable	Enable or disable AtomicOp Request Support
BIOS Guard	No Option	

10.4.9 Server ME Debug Configuration

Feature	Options	Description
▶Server ME General Configuration	Submenu	Server ME basic features configuration
▶NM Configuration	Submenu	Options to configure NM features

10.4.9.1 Server ME Generation Configuration Submenu

Feature	Options	Description
ME Initialization Complete Timeout	**2**	This option defines how long BIOS waits for ME to initialize
Custom HPET timer for SPS HECI	**1**	Custom HPET timer for SPS HECK waiting
▶Override ICC Clock Enables		

Override ICC Clock Enables

Feature	Options	Description
Override ICC Clock Enables	**Disabled** Enabled	This option allows customization of clock enables

10.4.9.2 NM Configuration Submenu

Feature	Options	Description
Cores Disable Override	**Disabled** Enabled	Enables overriding the values of the number of cores to disable requested in NMFS register
Cores to Disable	0 0 – 16	The number of cores to disable instead of the number requested in NMFS register
Power Measurement Override	**Disabled** Enabled	Override power measurements support status reported to ME
Power Measurement	**Disabled** Enabled	Override power measurement support status reported to ME
Hardware Change Override	**Disabled** Enabled	Override hardware change detection status reported to ME
Hardware changed	**No** Yes	Override hardware change detection status reported to ME

10.4.10 Server ME Configuration

Feature	Options	Description
Generation ME Configuration	No Option	
Operation Firmware Version	No Option	
ME Firmware Type	No Option	
Recovery Firmware Version	No Option	
ME Firmware Features	No Option	
ME Firmware Status #2	No Option	
Current State	No Option	
Error Code	No Option	
Altitude	**80000000** 0 - 80000000	The altitude of the platform location above the sea level, expressed in meters
MCTP Bus Owner	**0** 0 - 9999	MCTP bus owner location on PCIe

10.4.11 Runtime Error Logging

Feature	Options	Description
System Errors	**Disable** Enable Auto	System error enabling and logging setup option
S/W Error Injection Support	**Disable** Enable	When enabled, S/W error injection is supported by unlocking MSR 0x790
Clear McBankErrors	**Disable** Enable	Enables or disables clearing MCBank errors on warm reset
System Poison	**Disable** Enable	Enable or disable Core, Uncore and IIO Poison
IIO Error Enable	No **Yes**	
PCH Error Enable	No **Yes**	
▶WHEA Settings	Submenu	Press <Enter> to view or change the WHEA configuration
▶Memory Error Enabling	Submenu	Press <Enter> to view or change the Memory errors enabling options
▶IIO Error Enable	Submenu	Press <Enter> to view or change the IIO errors enabling options.
▶PCI/PCI Error Enabling	Submenu	Press <Enter> to view or change the PCH errors enabling options

10.4.11.1 WHEA Settings Submenu

Feature	Options	Description
WHEA Support	**Disable** Enable	Enable or disable the WHEA Support
WHEA Error Injection 5.0 Extension	**Disable** Enable	WHEA EINJ ACPI 5.0 support for set error type with address and vendor extensions
WHEA FFM Logging	**Disable** Enable	Enable or disable WHEA FFM logging of errors
WHEA UEFI Revisions	**UEFI 2.2** UEFi 2.3.1	UEFI revision of WHEA error format
WHEA PCIe Error Injection	Disable **Enable**	Enable or disable WHEA PCIe Error Injection
WHEA PCIe Error Action Enable	Disable **Enable**	Use Action Table for WHEA PCIe Error Injection

10.4.11.2 Memory Error Enabling Submenu

Feature	Options	Description
Memory corrected Error enabling	**Disable** Enable	Enable or disable Memory corrected Errors
Spare interrupt	SMI **CMCI** **Error Pin**	Select SMI/CMCI/ErrPin for spare interrupt

10.4.11.3 IIO Error Enable Submenu

Feature	Options	Description
Error pin Programming for IIO	**None** SMI	Error pin programming
DMI Errors	Disable **Enable**	Enable or disable DMI errors
Vtd Errors	**Disable** Enable	Enable or disable Vtd errors
Misc Errors	**Disable** Enable	Enable or disable Miscellaneous errors
IIO core Errors	**Disable** Enable	Enable or disable IIO core errors
DMA Errors	**Disable** Enable	Enable or disable DMA errors
Coherency Interface Errors	**Disable** Enable	Enable or disable Coherency Interface Errors
►IIO Coherency Interface Error Enable	Submenu	Press <Enter> to view or change the Coherency errors enabling options

IIO Coherency Interface Error Enable

Feature	Options	Description
IIO IRP0 protocol parity error	Disable **Enable**	Enable or disable Coherent Interface protocol IIO parity error reporting
IIO IRP0 protocol qt overflow underflow error	Disable **Enable**	Enable or disable IIO coherent interface protocol queue table overflow or underflow error reporting
IIO IRP0 protocol rcvd unexprsp	Disable **Enable**	Enable or disable IIO coherent interface protocol layer received unexpected response or completion error reporting

IIO IRP0 csr acc 32b unaligned	Disable **Enable**	Enable or disable IIO coherent interface CSR access crossing 32-bit Boundary error reporting
IIO IRP0 wrcache uncecc error	Disable **Enable**	Enable or disable IIO coherent interface write cache un-correctable ECC error reporting.
IIO IRP0 protocol rcvd poison error	Disable **Enable**	Enable or disable IIO Coherent Interface Protocol Layer Received Poisoned packet error reporting
IIO IRP0 wrcache correcc error	Disable **Enable**	Enable or disable IIO coherent Interface Write Cache Correctable ECC error reporting
IIO IRP1 protocol parity error	Disable **Enable**	Enable or disable Coherent Interface protocol IIO parity error reporting
IIO IRP1 protocol qt overflow underflow error	Disable **Enable**	Enable or disable IIO Coherent Interface protocol queue table overflow or under flow error reporting
IIO IRP1protocol rcvd unexprsp	Disable **Enable**	Enable or disable IIO Coherent Interface protocol layer received unexpected response or completion error reporting
IIO IRP1 csr acc 32b unaligned	Disable **Enable**	Enable or disable IIO Coherent Interface CSR Access Crossing 32-bit Boundary error reporting
IIO IRP1 wrcache uncecc error	Disable **Enable**	Enable or disable IIO Coherent Interface Write Cache un-correctable ECC error reporting
IIO IRP1 protocol rcvd poison error	Disable **Enable**	Enable or disable IIO Coherent Interface Protocol Layer Received Poisoned Packet error reporting
IIO IRP1 wrcache correcc error	Disable **Enable**	Enable or disable IIO coherent interface write cache correctable ECC error reporting

10.4.11.4 PCI/PCI Error Enabling Submenu

Feature	Options	Description
PCI-Ex Error Enable	No **Yes**	
Corrected Error Enable	Disable **Enable**	Enable or disable PCIe Correctable errors
Uncorrected Error Enable	Disable **Enable**	Enable or disable PCIe Uncorrectable errors
Fatal Error Enable	Disable **Enable**	Enable or disable PCIe Fatal errors
PCIe Correctable Error Enable	**0** 0 - 255	PCIe Correctable Error threshold from 1-255 Set “0” for no threshold
Enable SERR propagation	No **Yes**	
Enable PERR propagation	No **Yes**	

PCIe Extended errors	**Disable** Enable	Enable or disable IIO PCIe root port errors

10.4.12 Reserve Memory

Feature	Options	Description
Reserve Memory Range	**Disabled** Enabled	Sets aside an empty memory page that is hidden from the OS
Start Address	**0** 0 - FFFFFFFFFFFF	Address that reserved memory page starts at
Reserve Memory Result	No Option	Result of attempting to reserve memory range
Reserve TAGEC Memory	**Disable** Enable	Reserve 16M for TAGEC

10.5 Server Management

By default, BMC support is disabled in the BIOS. When the BMC is enabled, the boot time increases because the BIOS then initiates communication with the BMC. If the BIOS did not detect a BMC device, the initiated communication will time out after 60 seconds and the boot process will continue.

Note

If a BMC device is undetected or the initiated communication unsuccessful, the Self-test Status will show "failed" while the Device ID, Device Revision, Firmware Revision and IPMI version will all show "Unknown".

Feature	Options	Description
BMC Self Test Status	No Option	Shows the result of the BMC self test
BMC Device ID	No Option	Shows the BMC's self reported Device ID
BMC Device Revision	No Option	Shows the BMC's self reported device revision
BMC Firmware Revision	No Option	Shows the BMC's self reported firmware revision
IPMI Version	No Option	Shows the BMC's self reported IPMI version compliance

BMC Support	Enabled **Disabled**	Enable or disable interfaces to communicate with the BMC
Wait for BMC	Enabled **Disabled**	Wait for BMC response for specified timeout. BMC starts at power up Depending on the BMC implementation, the BMC may take a long time to initialize

FRB-2 Timer	**Enabled** Disabled	Enable or disable FRB-2 timer (POST timer)
FRB-2 Timer timeout	3 minutes 4 minutes 5 minutes **6 minutes**	Enter value between 3 to 6 minutes for FRB-2 timer expiration value
FRB-2 Timre Polity	**Do Nothing** Reset Power Down Power Cycle	Configure how the system should respond if the CRB-2 Timer expires Not available if FRB-2 timer is disabled
OS Watchdog TImer	Enabled **Disabled**	Helps determine if the OS loaded successfully or if the OS boot watchdog timer policy is adhered to. If enabled, a BIOS timer starts. Only the management software can turn this timer off after the OS loads
OS Wtd Timer Timeout	5 minutes **10 minutes** 15 minutes 20 minutes	Configure the length of the OS boot watchdog timer. Not available if OS boot watchdog timer is disabled
OS Wtd Timer Policy	Do Nothing **Reset** Power Down Power Cycle	Configure how the system should respond if the OS boot watchdog timer expires Not available if OS boot watchdog timer is disabled
Serial Mux	Enabled **Disabled**	Press <Enter> to enable or disable Serial Mux Configuration
▶System Event Log	Submenu	Press <Enter> to chagne the SEL event log configuration
▶Bmc self test log	Submenu	Logs the report returned by BMC self test command
▶BMC network configuration	Submenu	Configure BMC network parameters
▶View System Event Log	Submenu	Press <Enter> to view the System Event Logs records
▶BMC User Settings	Submenu	Press <Enter> to Add, Delete and Set Privilege level for users
BMC Warm Reset	No Option	Press <Enter> to do warm reset of BMC

10.5.1 System Event Log

Feature	Options	Description
Enabling/Disabling Options	No Option	
SEL Components	**Enable** Disable	Enable or disable all features of System Event Logging during boot
Erasing Settings	No Option	
Erase SEL	**No** Yes, On next reset Yes, On every reset	Choose options for erasing SEL

When SEL is Full	**Do Nothing** Erase Immediately	Choose options for reactions to a full SEL
Custom EFI logging Options	No Option	
Log EFI Status Codes	Disabled Both **Error code** Progress Code	Disable the logging of EFI status codes or log only error code or only progress code or both
NOTE: All values changed here do not take effect until computer is restarted	No Option	

10.5.2 BMC Self Test Log

This submenu processes the current logs from the BMC and decodes them in a readable format for the user. Therefore, the content of this submenu is determined by the current state of the BMC.

Feature	Options	Description
Log area usage = xx out of 20 logs	No Option	Report of the number of logging areas in use by the BMC
Erase Log	**Yes, On every reset** No	Erase Log Options
When Log is full	**Clear Log** Do not log anymore	Selects teh action to be taken when log is full
DATE TIME STATUS CODE	No Option	Headings for the currently logged codes

10.5.3 BMC Network Configuration

Submenu is not available when network is not detected.

10.5.4 View System Event Log

Submenu does not contain any information when the BMC communication fails.

10.5.5 BMC User Settings

An IPMI protocol error message appears when the BMC communication fails.

10.6 Security Settings

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

Feature	Options	Description
BIOS Password	No Options	Set BIOS password
BIOS Update and Write Protection	**Disabled** Enabled	Enable BIOS update and write protection
HDD Security Configuration:	No Option	
P1: <HDD Name>	Submenu	
P4: <HDD Name>	Submenu	
▶Secure Boot Menu	Submenu	Customizable Secure Boot Settings

10.6.1 Secure Boot Menu

Feature	Options	Description
System Mode	No Options	Displays the Secure Boot mode the system is currently running in
Secure Boot	No Options	Shows the current Secure Boot status
Vendor Keys	No Options	Shows the Vendor Key Status
Secure Boot	**Disabled** Enabled	Secure boot can be enabled if the system is running in User mode with enrolled Platform Key (PK) and CSM function is disabled
Secure Boot Mode	Standard **Custom**	Secure Boot mode selector. Custom mode enables users to change Image Execution policy and manage Secure Boot keys.
▶Key Management	Submenu	Enables experienced user to modify Secure Boot variables
▶Image Execution Policy	Submenu	Manage Image Execution Policy on Security Violation

10.6.1.1 Key Management Submenu

Feature	Options	Description
Provision Factory Default keys	**Disabled** Enabled	Install factory default Secure Boot keys when system is in setup mode
▶Enroll all Factory Default keys	No Option	Force System to setup mode - clears all secure boot variables Changes take effect after reboot
▶Save all Secure Boot variables	No Option	Save NVRAM content of all Secure Boot variables to the files (EFI_SIGNATURE_LIST data format) in root folder on a targeted file system device
Secure Boot Variable	No Option	
▶Platform Key(PK)	No Option	Pop-up menu for modifying the Platform Keys (PK) Set new key or delete current key
▶Key Exchange Keys (KEK)	No Option	Pop-up menu for modifying the Key Exchange Keys (KEK) Set new key, append key or delete key
▶Authorized Signatures	No Option	Pop-up menu for modifying the Authorized Signature keys for Database Keys (db) Set new key, append key or delete key
▶Forbidden Signatures	No Option	Pop-up menu for modifying the Forbidden Signature keys (dbx) Set new key, append key or delete key
▶Authorized TimeStamps	No Option	Pop-up menu for modifying the Authorized Timestamps Keys (dbt) Set new key, append key

10.6.1.2 Image Execution Policy Submenu

Feature	Options	Description
Internal FV	No Option	Internal Firmware volume FFS files are always trusted Read from the system BIOS SPI chip are always trusted
Option Rom	**Deny Execute** Query User	Image Execution Policy per device path on Security Violation
Removable Media	**Deny Execute** Query User	Image Execution Policy per device path on security violation
Fixed Media	**Deny Execute** Query User	Image Execution policy per device path on security violation

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
Boot Configuration	No Option	
Setup Prompt Timeout	**1** 0 - 65535	Number of seconds to wait for setup activation key
Bootup NumLock State	**On** Off	Select the keyboard NumLock state when system powers on
Power Loss Control	**Remain Off** Turn On Last Satate	Determines if the system is turned on/off after a power loss failure
AT Shutdown Mode	System Reboot **Hot S5**	Determines the behavior of an AT-powered system after a shutdown
Drive BATLOW# to PCH on G3-S5	**Enabled** Disabled	Enable to prevent the system from automatically starting up when transitioning from G3 to S5 when no RTC battery is present. Set to disable in case you have RTC Wake
Enter Setup if No Boot Device	No **Yes**	Select whether the setup menu should be started if no boot device is connected
Enable Popup Boot Menu	No **Yes**	Select whether the pop-up boot menu can be started
Boot Priority Selection	UEFI Standard **Type Based**	Set boot priority selection method Type Based: determine boot priority by device type UEFI Standard: determine boot priority by specific device selection. Devices must be present Priority will change if devices are added or removed
Boot Option Sortying Method	**Legacy First** UEFI First	UEFI First: Try all UEFI boot options before first legacy boot option is attempted Legacy First: vice versa
Type Based Boot Priority	No Option	

1st Boot Device	Disabled SATA0 Drive SATA1 Drive NVMe Storage USB Harddisk **USB CDROM** Other USB Device Onboard LAN External LAN Firmware-based BootLoader Other Device	1st Boot Device
2nd Boot Device	Disabled SATA0 Drive SATA1 Drive NVMe Storage **USB Harddisk** USB CDROM Other USB Device Onboard LAN External LAN Firmware-based BootLoader Other Device	2nd Boot Device
3rd Boot Device	Disabled **SATA0 Drive** SATA1 Drive NVMe Storage USB Harddisk USB CDROM Other USB Device Onboard LAN External LAN Firmware-based BootLoader Other Device	3rd Boot Device
4th Boot Device	Disabled SATA0 Drive **SATA1 Drive** NVMe Storage USB Harddisk USB CDROM Other USB Device Onboard LAN External LAN Firmware-based BootLoader Other Device	4th Boot Device

5th Boot Device	Disabled SATA0 Drive SATA1 Drive NVMe Storage USB Harddisk USB CDROM **Other USB Device** Onboard LAN External LAN Firmware-based BootLoader Other Device	5th Boot Device
6th Boot Device	Disabled SATA0 Drive SATA1 Drive **NVMe Storage** USB Harddisk USB CDROM Other USB Device Onboard LAN External LAN Firmware-based BootLoader Other Device	6th Boot Device
7th Boot device	Disabled SATA0 Drive SATA1 Drive NVMe Storage USB Harddisk USB CDROM Other USB Device **Onboard LAN** External LAN Firmware-based BootLoader Other Device	7th Boot Device
8th Boot Device	Disabled SATA0 Drive SATA1 Drive NVMe Storage USB Harddisk USB CDROM Other USB Device Onboard LAN External LAN Firmware-based BootLoader **Other Device**	8th Boot Device

Battery Support	**Auto (Battery Manager)** Battery-Only on I2C Bus Battery-Only on SMBus	Selected the correct battery device for your system's settings
System Off Mode	**G3/Mech Off** S5/Soft Off	Defines system state after shutdown when a battery system is present
Quiet Boot	**Disabled** Enabled	Enables or disables Quiet Boot option
UEFI Screen Shot Capability	**Disabled** Enabled	If enabled, pressing left control, left ALT and F12 at the same time will take a screenshot from the currently displayed BIOS screen. It will be saved as a PNG on the first writable FAT partition found in the system
Isolate SMBus Segments	**Never** During POST Always	Allows the system to isolate the off-module/external SMBus segment from the on-module SMBus segment. This can be a workaround for non-spec conforming external SMBus devices.

10.7.2 Event Logs

Feature	Options	Description
▶Change Smbios Event Log Settings	Submenu	Press <Enter> to change the Smbios Event Log configuration
▶View Smbios Event Log	Submenu	Press <Enter> to view the Smbios Event Log records

10.7.2.1 Change Smbios Event Log Settings Submenu

Feature	Options	Description
Enabling/Disable Options	No Option	
Smbios Event Log	Disabled **Enabled**	Enable or disable all features of Smbios Event Logging during boot
Erasing Settings	No Option	
Erase Event Log	**No** Yes, Next reset Yes, Every reset	Choose options for erasing Smbios Event Log. Erasing is done prior to any logging activation during reset
When Log is Full	**Do Nothing** Erase Immediately	Choose options for reactions to a full Smbios Event Log
Smbios Event Log Standard Settings	No Option	
Log System Boot Event	**Enabled** Disabled	Enable or disable logging of system boot event

MECI	**1** 1 - 255	Multiple event count increment. The number of occurrences of a duplicate vent that must pass before the multiple event counter of log entry is updated
METW	**60** 0 - 99	Multiple event time window. The number of minutes which must pass between duplicate log entries which utilize a multiple event counter
Custom Options	No Option	
Log OEM Codes	**Enabled** Disabled	Enable or disable the logging of EFI Status Codes as OEM codes (if not already converted to legacy)
Convert OEM Codes	Enabled **Disabled**	Enable or disable the converting of EFI Status Codes to standard Smbios types (not all may be translated)

10.7.2.2 View Smbios Event Log Submenu

The display of this submenu is determined by the Smbios records contained in the system. For more information, see the Smbios Specification on DMTF.org

10.8 Save & Exit

Feature	Options	Description
Save Options	No Option	
Save Changes and Exit	No Option	Exit system setup after savings the current changes
Discard Changes and Exit	No Option	Exit system setup without saving any changes
Save Changes and Reset	No Option	Reset the system after saving the changes
Discard Chagnes and Reset	No Option	Reset system without saving any changes
Save Changes	No Option	Save changes made so far to any of the setup options
Discard Changes	No Option	Discard changes made so far to any of the setup options
Default Options	No Option	
Restore Defaults	No Option	Restore or load default values for all setup options
Save as User Defaults	No Option	Save the changes done so far as user defaults
Restore User Defaults	No Option	Restore the user defaults to all the setup options
Generate Menu Layout FIle	No Option	Menu layout file will be generated and stored on the first writable file system found

11 Additional BIOS Information

The BIOS setup description of the conga-B7XD 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.

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 for conga-B7XD is identified as TSDER1xx, where:

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

The conga-B7XD BIOS binary size is 16 MB.

11.2 Updating the BIOS

BIOS updates are recommended to correct platform issues or enhance the feature set of the module. The conga-B7XD 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[1], 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.

Note

1. *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 Updating 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-B7XD supports the following flash devices:

- Winbond W25Q128JVSIQ (16 MB)
- Macronix MX25L12835FM2I-10G (16 MB)
- GigaDevice GD25Q127CSIGR (16 MB)

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