Express-BD7

User's Manual

COM Express Basic Size Type 7 Module with up to 16 cores
Intel® Xeon D and Pentium® D SoC

COM Express®

Manual Rev.: 1.0
Revision Date: June 20, 2017
Part Number: 50-1J083-1000

Leading **EDGE COMPUTING**

Preface

Copyright

Disclaimer

The information in this document is subject to change without prior notice in order to improve reliability, design, and function and does not represent a commitment on the part of the manufacturer. In no event will the manufacturer be liable for direct, indirect, special, incidental, or consequential damages arising out of the use or inability to use the product or documentation, even if advised of the possibility of such damages.

Environmental Responsibility

ADLINK is committed to fulfill its social responsibility to global environmental preservation through compliance with the European Union's Restriction of Hazardous Substances (RoHS) directive and Waste Electrical and Electronic Equipment (WEEE) directive. Environmental protection is a top priority for ADLINK. We have enforced measures to ensure that our products, manufacturing processes, components, and raw materials have as little impact on the environment as possible. When products are at their end of life, our customers are encouraged to dispose of them in accordance with the product disposal and/or recovery programs prescribed by their nation or company.

Trademarks

Product names mentioned herein are used for identification purposes only and may be trademarks and/or registered trademarks of their respective companies.

Revision History

Revision	Description	Date	By
1.0	Initial release	2017-06-20	JC

Table of Contents

List of Figures

List of Tables

1. Introduction

The Express-BD7 is a COM Express® COM.0 R3.0 Basic Size Type 7 module supporting the 64-bit Intel® Xeon® processor D and Intel® Pentium® D processor system-on-chip (SoC) (formerly “Broadwell-DE”). The Express-BD7 is specifically designed for customers who need excellent computing performance with balanced power consumption and multiple 10G Ethernet connectivity in a long product life solution.

The Express-BD7 features Intel® Virtualization Technology (including VT-x, VT-d, EPT), Intel® Hyper-Threading Technology (up to 16 cores, 32 threads), Intel® Trusted Execution Technology, Intel® AES-NI Technology, and DDR4 ECC (or non-ECC) dual-channel memory at 1866/2133/2400 MHz (dependent on SoC SKU) to provide excellent overall performance.

An integrated Intel® 10G Ethernet controller supports two 10GBASE-KR interfaces, relevant sideband signals and NC-SI. The Express-BD7 is designed to serve customers with optimized computing capability per watt and high speed connectivity requirements who want to outsource the custom core logic of their systems for reduced development time.

The Express-BD7 has dual stacked SODIMM sockets supporting up to 32 GB of DDR4 ECC (or non-ECC) memory. Input/output features include 24 PCIe Gen3 lanes, up to 8 PCIe Gen2 lanes, a single onboard Gigabit Ethernet port, USB 3.0/2.0 ports, and SATA 6 Gb/s ports. Support is provided for SMBus and I2C. The module is equipped with SPI AMI EFI BIOS with CMOS backup, supporting embedded features such as remote console, hardware monitor, and watchdog timer.

This page intentionally left blank.

2. Specifications

2.1. Core System

CPU	**Intel® Xeon® processor D, Pentium® D processor (formerly "Broadwell-DE")** • Intel® Xeon® D1539 1.6/1.9 GHz 35W (8C, up to 2133MHz) (eTEMP) • Intel® Xeon® D1519 1.5/1.8 GHz 25W (4C, up to 2133MHz) (eTEMP) • Intel® Xeon® D1548 2.0/2.3 GHz 45W (8C, up to 2400MHz) • Intel® Xeon® D1527 2.2/2.5 GHz 35W (4C, up to 2133MHz) • Intel® Pentium® D1508 2.2/2.5 GHz 25W (2C, up to 1866MHz) • Intel® Xeon® D1559 1.5/1.8 GHz 45W (12C, up to 2133MHz) (eTEMP) • Intel® Xeon® D1577 1.3/1.6 GHz 45W (16C, up to 2400MHz) **Note:** D1559, D1577 are supported by project basis. Please contact local sales. Supporting: Intel® VT (including VT-x, VT-d, VT-x with Extended Page Tables), Intel® HT Technology, Intel® SSE4.2, Intel® 64 Architecture, Intel® Turbo Boost Technology 2.0, Intel® AVX2, Intel® TSX-NI, Intel® Platform Protection Technology with Intel® TXT and Execute Disable Bit, Intel® Data Protection Technology with Intel® Secure Key and Intel® AES-NI **Note:** Availability of features may vary between processor SKUs.
Cache	24MB for D1577, 18MB for D1559, 12MB for D1548/D1539, 6MB for D1527/D1519, 3MB for D1508
Memory	Dual channel ECC (or non-ECC) 1866/2133/2400 MHz DDR4 memory up to 32GB in dual stacked SODIMM sockets **Note:** Supported memory frequencies may vary between processor SKUs.
Embedded BIOS	AMI EFI with CMOS backup in 16MB SPI BIOS
Chipset	Integrated in SoC

2.2. Expansion Busses

PCI Express	16 PCI Express Lanes Gen3 (CD): Lanes 16-31 (four controllers, can be configured to 1 x16, 2 x8 or 4 x4/x2/x1) 8 PCI Express Lanes Gen3 (AB): Lanes 8-15 (two controllers, can be configured to 1 x8 or 2 x4/x2/x1) Up to 8 PCI Express Lanes Gen2 (AB/CD): Lanes 0-7 (two controllers defined by PICMG, can be configured to x4, x2, x1) **Notes:** • PCIe lane 7 is supported by build option, in place of GbE • Although Broadwell-DE platform supports eight roots on Lanes 0-7, the PICMG COM.0 R3.0 specification for Lanes 0-7 states: "*Type7 module may support eight x1 root hubs. It is expected that future generation products may limit the number of available root hubs.*"
Other	• LPC bus • SMBus (system) • I^2C (user)

2.3. 10Gigabit Ethernet

Integrated on Processor	Intel® 10G Ethernet Controller

10GbE Feature Support	• Two 10GBASE-KR (on CD connector)
	• Sideband signals (on CD connector) for 10GbE
	  • 10G_INT
	  • 10G_PHY_MDIO_SDA and 10G_PHY_MDC_SCL (manage/control signals between MAC and PHY)
	  • 10G_PHY_CAP (PHY mode capability pin, used to indicate whether the PHY on carrier board needs I2C or MDIO signals from module)
	  • 10G_PHY_RST (PHY reset signal, only for Optical PHY)
	  • 10G_LED_SDA and 10G_LED_SCL (LED signals carried through dedicated I2C bus; additional strapping signal through I2C bus; LED signals programmable for indicating ACT, LINK, Speed)
	  • 10G_SFP_SDA and 10G_SFP_SCL (dedicated for Optical PHY use, connect to external SFP module)
	  • 10G_SDP (Software-Definable Pin for general purpose)

Display Types	• Single/dual channel 18/24-bit LVDS via eDP-to-LVDS chip, supports DE mode and H/V-Sync mode display. Resolution up to 1920x1200 with dual channel LVDS. (eDP 4 lanes available as build option in place of LVDS) • 2x Digital Display Ports: DDI1 supports DisplayPort/HDMI/DVI DDI2 supports DisplayPort/HDMI/DVI • VGA (build option) via DP-to-VGA chip. Resolution up to 1920x1200. in place of DDI 2 **Note:** Supports HDMI 1.4, DP 1.2 and eDP 1.3.

2.4. Gigabit Ethernet

Intel Controller	Intel® i210 Ethernet Controller
Interface	10/100/1000 Mbit/s connection

2.5. NC-SI

- **NC-SI** (on AB connector): manageability interface, connecting to IPMI BMC located on carrier board
  - Routing from Intel® i210 Ethernet Controller to row AB connector by default
  - Build option to support routing from 10GbE controller to row AB connector

2.6. Multi I/O and Storage

I/O Hub	Integrated on SoC
USB	4x USB 3.0/2.0 (USB 0,1,2,3)
SATA*	2x SATA 6Gb/s (SATA 0,1)
GPIO	4 GPO and 4 GPI

***Note:** For SATA 6Gb/s compatibility, it is strongly recommended to use a SATA redriver on the carrier board.

2.7. Serial I/O on Module

- **Chipset:** Nuvoton NCT5104D
  Note: two UART ports native from SoC instead of NCT5104D supported by build option
- **Ports:** 2x UARTs Rx/Tx only
- **Console Redirection:** COM 1 or COM 2 selectable in BIOS

COM Port	Description	IRQ	Address	Console redirection support
COM 1	Supported by module (SER0, A98/A99), via NCT5104D	10	0x240	Yes
COM 2	Supported by module (SER1, A101/A102), via NCT5104D	11	0x248	Yes
COM 3	Supported by Super I/O (W83627DHG) on carrier board	4	0x3F8	Yes
COM 4	Supported by Super I/O (W83627DHG) on carrier board	3	0x2F8	Yes

2.8. Trusted Platform Module (TPM)

- **Chipset:** Infineon
- **Type:** TPM 2.0

2.9. SEMA Board Controller

- **Type:** ADLINK Smart Embedded Management Agent (SEMA)
- **Functions:**
  - Voltage/Current monitoring
  - Power sequence debug support
  - AT/ATX mode control
  - Logistics and forensic information
  - Flat panel control
  - General purpose I2C
  - Failsafe BIOS (dual BIOS)
  - Watchdog timer and fan control

2.10. Debug

- 40-pin flat cable connector to be used with DB-40 debug module
  Supports: BIOS POST code LED, BMC access, SPI BIOS flashing, power testpoints, debug LEDs
- 60-pin XDP header for ICE debug of CPU/chipset

2.11. Power Specifications

Power Modes	AT and ATX mode (AT mode startup controlled by SEMA Board Controller)
Standard Voltage Input	ATX @ 12V±5%,/ 5Vsb ±5% or AT @ 12V ±5%
Wide Voltage Input	ATX @ 8.5-20V, 5Vsb ±5% or AT @ 8.5-20V
Power Management	ACPI 5.0 compliant, Smart Battery support
Power States	Supports C0, C1, C1E, C3, C6, S0, S4, S5, S5 ECO mode (Wake-on-USB S4, WOL S4/S5)
ECO Mode	Supports deep S5 for 5Vsb power saving

2.12. Power Consumption

Please contact your ADLINK representative for the document “COM Express Module Power Consumption”.

2.13. Operating Temperatures

Standard Operating Temperature	0°C to +60°C (Wide Voltage Input) Storage: -20°C to +70°C
Extreme Rugged Operating Temperature (optional)	-40°C to +85°C (Standard Voltage Input, dependent on SoC SKU, build option support) Storage: -40°C to +85°C

2.14. Environmental

Humidity	Operating: 5-90% RH, non-condensing Storage: 5-95% RH (and operating with conformal coating)
Shock and Vibration	IEC 60068-2-64 and IEC-60068-2-27 MIL-STD-202F, Method 213B, Table 213-I, Condition A and Method 214A, Table 214-I, Condition D
HALT	Thermal Stress, Vibration Stress, Thermal Shock and Combined Test

2.15. Specification Compliance

- PICMG COM.0: Rev 3.0 Type 7, Basic size 125 x 95 mm

2.16. Operating Systems

Standard Support	• Windows Server 2012 R2 (64-bit) • Windows 7 (64-bit) • Linux (64-bit)
Extended Support (BSP)	• Linux (64-bit)

2.17. Functional Diagram

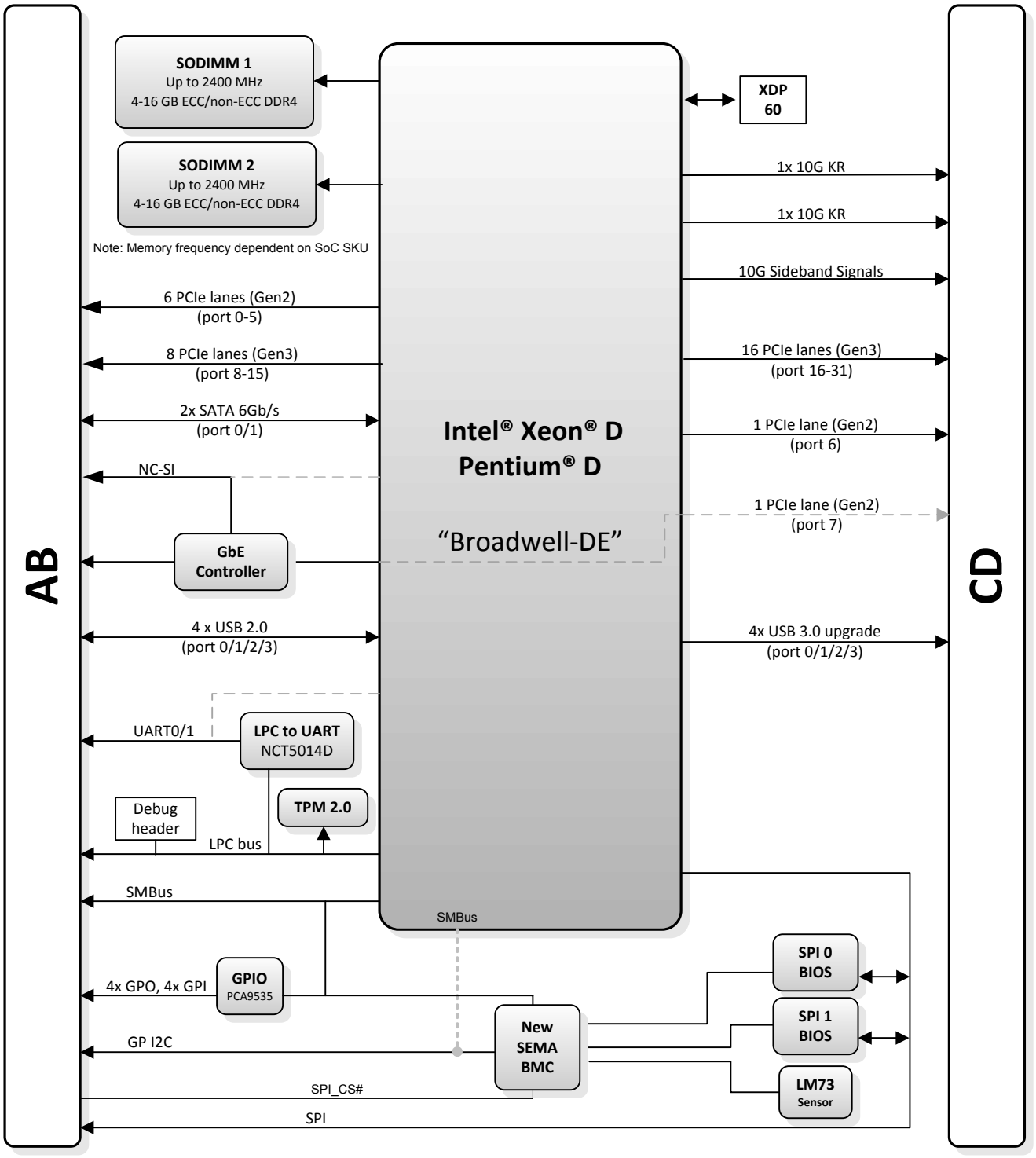
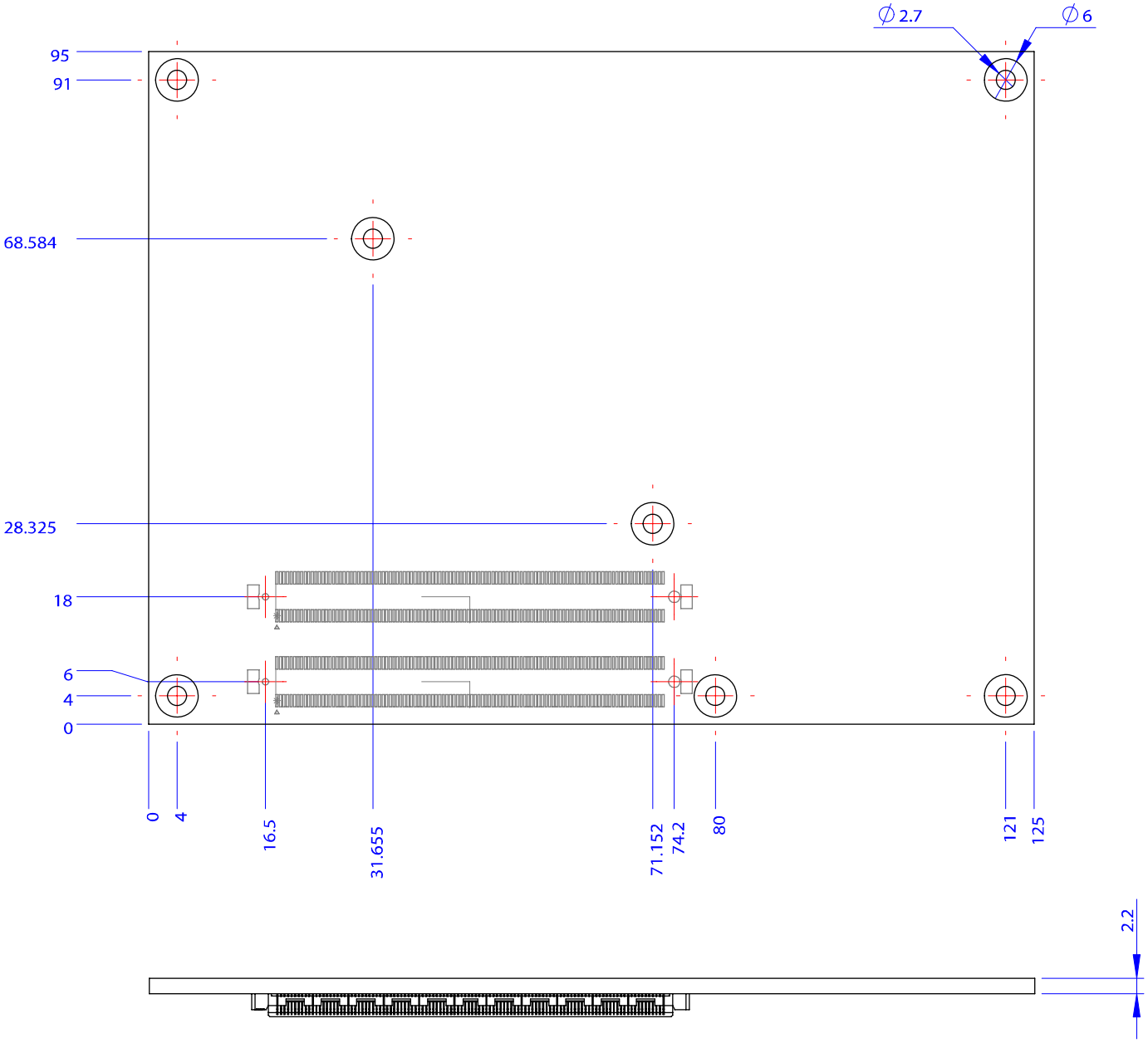


Figure 1: Express-BD7 Functional Block Diagram

2.18. Mechanical Drawing



All dimensions are shown in millimeters. Tolerances should be ± 0.25mm, unless otherwise noted.
The tolerances on the module connector locating peg holes (dimensions [16.50, 6.00] and [16.50, 18.00]) should be ± 0.10mm.

Figure 2: Express-BD7 Mechanical Drawing

3. Pinouts and Signal Descriptions

3.1. AB/CD Pin Definitions

The Express-BD7 is a Type 7 module supporting up to 32 PCIe lanes and 10G Ethernet on the CD connector and NC-SI on the AB connector. In the table below, all standard pins of the COM Express specification are described, including those not supported on the Express-BD7. Signals not supported on the Express-BD7 module are ~~crossed out~~.

Table 1: Express-BD7 AB/CD Pin Definitions

	Row A		Row B		Row C		Row D
Pin	**Name**	**Pin**	**Name**	**Pin**	**Name**	**Pin**	**Name**
A1	GND (fixed)	**B1**	GND (fixed)	**C1**	GND (fixed)	**D1**	GND (fixed)
A2	GBE0_MDI3-	**B2**	GBE0_ACT#	**C2**	GND	**D2**	GND
A3	GBE0_MDI3+	**B3**	LPC_FRAME# ~~/ESPI_CS0#~~	**C3**	USB_SSRX0-	**D3**	USB_SSTX0-
A4	GBE0_LINK100#	**B4**	LPC_AD0 ~~/ESPI_IO_0~~	**C4**	USB_SSRX0+	**D4**	USB_SSTX0+
A5	GBE0_LINK1000#	**B5**	LPC_AD1 ~~/ESPI_IO_1~~	**C5**	GND	**D5**	GND
A6	GBE0_MDI2-	**B6**	LPC_AD2 ~~/ESPI_IO_2~~	**C6**	USB_SSRX1-	**D6**	USB_SSTX1-
A7	GBE0_MDI2+	**B7**	LPC_AD3 ~~/ESPI_IO_3~~	**C7**	USB_SSRX1+	**D7**	USB_SSTX1+
A8	GBE0_LINK#	**B8**	LPC_DRQ0# ~~/ESPI_ALERT0#~~	**C8**	GND	**D8**	GND
A9	GBE0_MDI1-	**B9**	LPC_DRQ1# ~~/ESPI_ALERT1#~~	**C9**	USB_SSRX2-	**D9**	USB_SSTX2-
A10	GBE0_MDI1+	**B10**	LPC_CLK ~~/ESPI_CK~~	**C10**	USB_SSRX2+	**D10**	USB_SSTX2+
A11	GND (fixed)	**B11**	GND (fixed)	**C11**	GND (fixed)	**D11**	GND (fixed)
A12	GBE0_MDI0-	**B12**	PWRBTN#	**C12**	USB_SSRX3-	**D12**	USB_SSTX3-
A13	GBE0_MDI0+	**B13**	SMB_CK	**C13**	USB_SSRX3+	**D13**	USB_SSTX3+
A14	GBE0_CTREF	**B14**	SMB_DAT	**C14**	GND	**D14**	GND
A15	SUS_S3#	**B15**	SMB_ALERT#	**C15**	~~10G_PHY_MDC_SCL3~~	**D15**	~~10G_PHY_MDIO_SDA3~~
A16	SATA0_TX+	**B16**	SATA1_TX+	**C16**	~~10G_PHY_MDC_SCL2~~	**D16**	~~10G_PHY_MDIO_SDA2~~
A17	SATA0_TX-	**B17**	SATA1_TX-	**C17**	~~10G_SDP2~~	**D17**	~~10G_SDP3~~
A18	SUS_S4#	**B18**	SUS_STAT# ~~/ESPI_RESET#~~	**C18**	GND	**D18**	GND
A19	SATA0_RX+	**B19**	SATA1_RX+	**C19**	PCIE_RX6+	**D19**	PCIE_TX6+
A20	SATA0_RX-	**B20**	SATA1_RX-	**C20**	PCIE_RX6-	**D20**	PCIE_TX6-
A21	GND (fixed)	**B21**	GND (fixed)	**C21**	GND (fixed)	**D21**	GND (fixed)
A22	PCIE_TX15+	**B22**	PCIE_RX15+	**C22**	PCIE_RX7+	**D22**	PCIE_TX7+
A23	PCIE_TX15-	**B23**	PCIE_RX15-	**C23**	PCIE_RX7-	**D23**	PCIE_TX7-
A24	SUS_S5#	**B24**	PWR_OK	**C24**	~~10G_INT2~~	**D24**	~~10G_INT3~~
A25	PCIE_TX14+	**B25**	PCIE_RX14+	**C25**	GND	**D25**	GND
A26	PCIE_TX14-	**B26**	PCIE_RX14-	**C26**	~~10G_KR_RX3+~~	**D26**	~~10G_KR_TX3+~~
A27	BATLOW#	**B27**	WDT	**C27**	~~10G_KR_RX3-~~	**D27**	~~10G_KR_TX3-~~
A28	(S)ATA_ACT#	**B28**	RSVD	**C28**	GND	**D28**	GND
A29	RSVD	**B29**	RSVD	**C29**	~~10G_KR_RX2+~~	**D29**	~~10G_KR_TX2+~~
A30	RSVD	**B30**	RSVD	**C30**	~~10G_KR_RX2-~~	**D30**	~~10G_KR_TX2-~~
A31	GND (fixed)	**B31**	GND (fixed)	**C31**	GND (fixed)	**D31**	GND (fixed)
A32	RSVD	**B32**	SPKR	**C32**	~~10G_SFP_SDA3~~	**D32**	~~10G_SFP_SCL3~~
A33	RSVD	**B33**	I2C_CK	**C33**	~~10G_SFP_SDA2~~	**D33**	~~10G_SFP_SCL2~~
A34	BIOS_DIS0# ~~/ESPI_SAFS~~	**B34**	I2C_DAT	**C34**	~~10G_PHY_RST_23~~	**D34**	~~10G_PHY_CAP_23~~
A35	THRMTRIP#	**B35**	THRM#	**C35**	10G_PHY_RST_01	**D35**	10G_PHY_CAP_01

	Row A		Row B		Row C		Row D
Pin	**Name**	**Pin**	**Name**	**Pin**	**Name**	**Pin**	**Name**
A36	PCIE_TX13+	**B36**	PCIE_RX13+	**C36**	10G_LED_SDA	**D36**	RSVD
A37	PCIE_TX13-	**B37**	PCIE_RX13-	**C37**	10G_LED_SCL	**D37**	RSVD
A38	GND	**B38**	GND	**C38**	10G_SFP_SDA1	**D38**	10G_SFP_SCL1
A39	PCIE_TX12+	**B39**	PCIE_RX12+	**C39**	10G_SFP_SDA0	**D39**	10G_SFP_SCL0
A40	PCIE_TX12-	**B40**	PCIE_RX12-	**C40**	10G_SDP0	**D40**	10G_SDP1
A41	GND (fixed)	**B41**	GND (fixed)	**C41**	GND (fixed)	**D41**	GND (fixed)
A42	USB2-	**B42**	USB3-	**C42**	10G_KR_RX1+	**D42**	10G_KR_TX1+
A43	USB2+	**B43**	USB3+	**C43**	10G_KR_RX1-	**D43**	10G_KR_TX1-
A44	USB_2_3_OC#	**B44**	USB_0_1_OC#	**C44**	GND	**D44**	GND
A45	USB0-	**B45**	USB1-	**C45**	10G_PHY_MDC_SCL1	**D45**	10G_PHY_MDIO_SDA1
A46	USB0+	**B46**	USB1+	**C46**	10G_PHY_MDC_SCL0	**D46**	10G_PHY_MDIO_SDA0
A47	VCC_RTC	**B47**	~~ESPI_EN~~	**C47**	10G_INT0	**D47**	10G_INT1
A48	RSVD	**B48**	~~USB0_HOST_PRSNT~~	**C48**	GND	**D48**	GND
A49	GBE0_SDP	**B49**	SYS_RESET#	**C49**	10G_KR_RX0+	**D49**	10G_KR_TX0+
A50	LPC_SERIRQ /~~ESPI_CS1#~~	**B50**	CB_RESET#	**C50**	10G_KR_RX0-	**D50**	10G_KR_TX0-
A51	GND (fixed)	**B51**	GND (fixed)	**C51**	GND (fixed)	**D51**	GND (fixed)
A52	PCIE_TX5+	**B52**	PCIE_RX5+	**C52**	PCIE_RX16+	**D52**	PCIE_TX16+
A53	PCIE_TX5-	**B53**	PCIE_RX5-	**C53**	PCIE_RX16-	**D53**	PCIE_TX16-
A54	GPI0	**B54**	GPO1	**C54**	TYPE0#	**D54**	RSVD
A55	PCIE_TX4+	**B55**	PCIE_RX4+	**C55**	PCIE_RX17+	**D55**	PCIE_TX17+
A56	PCIE_TX4-	**B56**	PCIE_RX4-	**C56**	PCIE_RX17-	**D56**	PCIE_TX17-
A57	GND	**B57**	GPO2	**C57**	TYPE1#	**D57**	TYPE2#
A58	PCIE_TX3+	**B58**	PCIE_RX3+	**C58**	PCIE_RX18+	**D58**	PCIE_TX18+
A59	PCIE_TX3-	**B59**	PCIE_RX3-	**C59**	PCIE_RX18-	**D59**	PCIE_TX18-
A60	GND (fixed)	**B60**	GND (fixed)	**C60**	GND (fixed)	**D60**	GND (fixed)
A61	PCIE_TX2+	**B61**	PCIE_RX2+	**C61**	PCIE_RX19+	**D61**	PCIE_TX19+
A62	PCIE_TX2-	**B62**	PCIE_RX2-	**C62**	PCIE_RX19-	**D62**	PCIE_TX19-
A63	GPI1	**B63**	GPO3	**C63**	RSVD	**D63**	RSVD
A64	PCIE_TX1+	**B64**	PCIE_RX1+	**C64**	RSVD	**D64**	RSVD
A65	PCIE_TX1-	**B65**	PCIE_RX1-	**C65**	PCIE_RX20+	**D65**	PCIE_TX20+
A66	GND	**B66**	WAKE0#	**C66**	PCIE_RX20-	**D66**	PCIE_TX20-
A67	GPI2	**B67**	WAKE1#	**C67**	RSVD	**D67**	GND
A68	PCIE_TX0+	**B68**	PCIE_RX0+	**C68**	PCIE_RX21+	**D68**	PCIE_TX21+
A69	PCIE_TX0-	**B69**	PCIE_RX0-	**C69**	PCIE_RX21-	**D69**	PCIE_TX21-
A70	GND (fixed)	**B70**	GND (fixed)	**C70**	GND (fixed)	**D70**	GND (fixed)
A71	PCIE_TX8+	**B71**	PCIE_RX8+	**C71**	PCIE_RX22+	**D71**	PCIE_TX22+
A72	PCIE_TX8-	**B72**	PCIE_RX8-	**C72**	PCIE_RX22-	**D72**	PCIE_TX22-
A73	GND	**B73**	GND	**C73**	GND	**D73**	GND
A74	PCIE_TX9+	**B74**	PCIE_RX9+	**C74**	PCIE_RX23+	**D74**	PCIE_TX23+
A75	PCIE_TX9-	**B75**	PCIE_RX9-	**C75**	PCIE_RX23-	**D75**	PCIE_TX23-
A76	GND	**B76**	GND	**C76**	GND	**D76**	GND
A77	PCIE_TX10+	**B77**	PCIE_RX10+	**C77**	RSVD	**D77**	RSVD
A78	PCIE_TX10-	**B78**	PCIE_RX10-	**C78**	PCIE_RX24+	**D78**	PCIE_TX24+
A79	GND	**B79**	GND	**C79**	PCIE_RX24-	**D79**	PCIE_TX24-

	Row A		Row B		Row C		Row D
Pin	**Name**	**Pin**	**Name**	**Pin**	**Name**	**Pin**	**Name**
A80	GND (fixed)	**B80**	GND (fixed)	**C80**	GND (fixed)	**D80**	GND (fixed)
A81	PCIE_TX11+	**B81**	PCIE_RX11+	**C81**	PCIE_RX25+	**D81**	PCIE_TX25
A82	PCIE_TX11-	**B82**	PCIE_RX11-	**C82**	PCIE_RX25-	**D82**	PCIE_TX25-
A83	GND	**B83**	GND	**C83**	RSVD	**D83**	RSVD
A84	NCSI_TX_EN	**B84**	VCC_5V_SBY	**C84**	GND	**D84**	GND
A85	GPI3	**B85**	VCC_5V_SBY	**C85**	PCIE_RX26+	**D85**	PCIE_TX26+
A86	RSVD	**B86**	VCC_5V_SBY	**C86**	PCIE_RX26-	**D86**	PCIE_TX26-
A87	RSVD	**B87**	VCC_5V_SBY	**C87**	GND	**D87**	GND
A88	PCIE0_CK_REF+	**B88**	BIOS_DIS1#	**C88**	PCIE_RX27+	**D88**	PCIE_TX27+
A89	PCIE0_CK_REF-	**B89**	NSCI_RX_ER	**C89**	PCIE_RX27-	**D89**	PCIE_TX27-
A90	GND (fixed)	**B90**	GND (fixed)	**C90**	GND (fixed)	**D90**	GND (fixed)
A91	SPI_POWER	**B91**	NCSI_CLK_IN	**C91**	PCIE_RX28+	**D91**	PCIE_TX28+
A92	SPI_MISO	**B92**	NCSI_RXD1	**C92**	PCIE_RX28-	**D92**	PCIE_TX28-
A93	GPO0	**B93**	NCSI_RXD0	**C93**	GND	**D93**	GND
A94	SPI_CLK	**B94**	NCSI_CRS_DV	**C94**	PCIE_RX29+	**D94**	PCIE_TX29+
A95	SPI_MOSI	**B95**	NCSI_TXD1	**C95**	PCIE_RX29-	**D95**	PCIE_TX29-
A96	TPM_PP	**B96**	NCSI_TXD0	**C96**	GND	**D96**	GND
A97	TYPE10#	**B97**	SPI_CS#	**C97**	RSVD	**D97**	RSVD
A98	SER0_TX / ~~CAN_TX~~	**B98**	NCSI_ARB_IN	**C98**	PCIE_RX30+	**D98**	PCIE_TX30+
A99	SER0_RX / ~~CAN_RX~~	**B99**	NCSI_ARB_OUT	**C99**	PCIE_RX30-	**D99**	PCIE_TX30-
A100	GND (fixed)	**B100**	GND (fixed)	**C100**	GND (fixed)	**D100**	GND (fixed)
A101	SER1_TX	**B101**	FAN_PWMOUT	**C101**	PCIE_RX31+	**D101**	PCIE_TX31+
A102	SER1_RX	**B102**	FAN_TACHIN	**C102**	PCIE_RX31-	**D102**	PCIE_TX31-
A103	LID#	**B103**	SLEEP#	**C103**	GND	**D103**	GND
A104	VCC_12V	**B104**	VCC_12V	**C104**	VCC_12V	**D104**	VCC_12V
A105	VCC_12V	**B105**	VCC_12V	**C105**	VCC_12V	**D105**	VCC_12V
A106	VCC_12V	**B106**	VCC_12V	**C106**	VCC_12V	**D106**	VCC_12V
A107	VCC_12V	**B107**	VCC_12V	**C107**	VCC_12V	**D107**	VCC_12V
A108	VCC_12V	**B108**	VCC_12V	**C108**	VCC_12V	**D108**	VCC_12V
A109	VCC_12V	**B109**	VCC_12V	**C109**	VCC_12V	**D109**	VCC_12V
A110	GND (fixed)	**B110**	GND (fixed)	**C110**	GND (fixed)	**D110**	GND (fixed)

Note: LPC and eSPI are muxed in the standard COM Express specification. The Express-BD7 only supports the LPC bus.

3.2. Signal Description Terminology

The following terms are used in the COM Express AB/CD Signal Descriptions below.

I	Input to the Module
O	Output from the Module
I/O	Bi-directional input/output signal
OD	Open drain output
I 3.3V	Input 3.3V tolerant
I 5V	Input 5V tolerant
O 3.3V	Output 3.3V signal level
O 5V	Output 5V signal level
I/O 3.3V	Bi-directional signal 3.3V tolerant
I/O 5V	Bi-directional signal 5V tolerant
I/O 3.3Vsb	Input 3.3V tolerant active in standby state
P	Power Input/Output
REF	Reference voltage output that may be sourced from a module power plane.
PDS	Pull-down strap. This is an output pin on the module that is either tied to GND or not connected. The signal is used to indicate the PICMG module type to the Carrier Board.
PU	ADLINK implemented pull-up resistor on module
PD	ADLINK implemented pull-down resistor on module

3.3. AB Signal Descriptions

3.3.1. Network Controller Sideband Interface (NC-SI)

Signal	Pin	Description	I/O	PU/PD	Comment
NCSI_CLK_IN	B91	Clock reference for receive, transmit and control interface	I 3.3VSB	PD 10k	
NCSI_RXD[1:0]	B92 B93	Receive Data (from NC to BMC)	O 3.3VSB	PU 10k 3.3VSB	PU 10k that aligns with LAN chip specification
NCSI_TXD[1:0]	B95 B96	Transmit Data (from BMC to NC)	I 3.3VSB	PU 10k 3.3VSB	
NCSI_CRS_DV	B94	Carrier Sense/Receive Data valid to MC, indicating that the transmitted data from NC to BMC is valid	O 3.3VSB	PD 10k	PU 10k that aligns with LAN chip specification
NCSI_TX_EN	A84	Transmit enable	I 3.3VSB	PD 10k	
NCSI_RX_ER	B89	Receive error	O 3.3VSB		
NCSI_ARB_IN	B98	Network Controller hardware arbitration input	I 3.3VSB		Left floating on module, that aligns with LAN chip specification
NCSI_ARB_OUT	B99	Network Controller hardware arbitration output	O 3.3VSB		

3.3.2. Gigabit Ethernet

Gigabit Ethernet	Pin	Description	I/O	PU/PD	Comment
GBE0_MDI0+ GBE0_MDI0- GBE0_MDI1+ GBE0_MDI1- GBE0_MDI2+ GBE0_MDI2- GBE0_MDI3+ GBE0_MDI3-	A13 A12 A10 A9 A7 A6 A3 A2	Gigabit Ethernet Controller 0: Media Dependent Interface Differential Pairs 0, 1, 2, 3. The MDI can operate in 1000, 100, and 10Mbit/sec modes. Some pairs are unused in some modes according to the following: 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+/-	I/O Analog		Twisted pair signals for external transformer.
GBE0_ACT#	B2	Gigabit Ethernet Controller 0 activity indicator, active low.	O 3.3VSB		
GBE0_LINK#	A8	Gigabit Ethernet Controller 0 link indicator, active low.	O 3.3VSB		
GBE0_LINK100#	A4	Gigabit Ethernet Controller 0 100Mbit/sec link indicator, active low.	O 3.3VSB		
GBE0_LINK1000#	A5	Gigabit Ethernet Controller 0 1000Mbit/sec link indicator, active low.	O 3.3VSB		
GBE0_CTREF	A14	Reference voltage for Carrier Board Ethernet channel 1 and 2 magnetics center tap. The reference voltage is determined by the requirements of the Module PHY and may be as low as 0V and as high as 3.3V. The reference voltage output shall be current limited on the Module. In the case in which the reference is shorted to ground, the current shall be 250 mA or less.	GND min 3.3V max		NC pin
GBE0_SDP	A49	Gigabit Ethernet Controller 0 Software-Definable Pins. Can also be used for IEEE1588 support such as a 1pps signal.	I/O 3.3VSB	PU 10k 3.3VSB	PU 10k that aligns with LAN chip specification

3.3.3. SATA

Signal	Pin	Description	I/O	PU/PD	Comment
SATA0_TX+ SATA0_TX-	A16 A17	Serial ATA channel 0, Transmit Output differential pair.	O SATA		AC coupled on Module
SATA0_RX+ SATA0_RX-	A19 A20	Serial ATA channel 0, Receive Input differential pair.	I SATA		AC coupled on Module
SATA1_TX+ SATA1_TX-	B16 B17	Serial ATA channel 1, Transmit Output differential pair.	O SATA		AC coupled on Module
SATA1_RX+ SATA1_RX-	B19 B20	Serial ATA channel 1, Receive Input differential pair.	I SATA		AC coupled on Module
(S)ATA_ACT#	A28	ATA (parallel and serial) or SAS activity indicator, active low.	O 3.3V	PU 10K 3.3V	

3.3.4. PCI Express

Signal	Pin	Description	I/O	PU/PD	Comment
PCIE_TX0+ PCIE_TX0-	A68 A69	PCI Express channel 0, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX0+ PCIE_RX0-	B68 B69	PCI Express channel 0, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX1+ PCIE_TX1-	A64 A65	PCI Express channel 1, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX1+ PCIE_RX1-	B64 B65	PCI Express channel 1, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX2+ PCIE_TX2-	A61 A62	PCI Express channel 2, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX2+ PCIE_RX2-	B61 B62	PCI Express channel 2, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX3+ PCIE_TX3-	A58 A59	PCI Express channel 3, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX3+ PCIE_RX3-	B58 B59	PCI Express channel 3, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX4+ PCIE_TX4-	A55 A56	PCI Express channel 4, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX4+ PCIE_RX4-	B55 B56	PCI Express channel 4, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX5+ PCIE_TX5-	A52 A53	PCI Express channel 5, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX5+ PCIE_RX5-	B52 B53	PCI Express channel 5, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX8+ PCIE_TX8-	A71 A72	PCI Express channel 8, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX8+ PCIE_RX8-	B71 B72	PCI Express channel 8, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX9+ PCIE_TX9-	A74 A75	PCI Express channel 9, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX9+ PCIE_RX9-	B74 B75	PCI Express channel 9, Receive Input differential pair.	I PCIE		AC coupled off Module

Signal	Pin	Description	I/O	PU/PD	Comment
PCIE_TX10+ PCIE_TX10-	A77 A78	PCI Express channel 10, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX10+ PCIE_RX10-	B77 B78	PCI Express channel 10, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX11+ PCIE_TX11-	A81 A82	PCI Express channel 11, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX11+ PCIE_RX11-	B81 B82	PCI Express channel 11, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX12+ PCIE_TX12-	A39 A40	PCI Express channel 12, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX12+ PCIE_RX12-	B39 B40	PCI Express channel 12, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX13+ PCIE_TX13-	A36 A37	PCI Express channel 13, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX13+ PCIE_RX13-	B36 B37	PCI Express channel 13, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX14+ PCIE_TX14-	A25 A26	PCI Express channel 14, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX14+ PCIE_RX14-	B25 B26	PCI Express channel 14, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX15+ PCIE_TX15-	A22 A23	PCI Express channel 15, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX15+ PCIE_RX15-	B22 B23	PCI Express channel 15, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_CLK_REF+ PCIE_CLK_REF-	A88 A89	PCI Express Reference Clock output for all PCI Express and PCI Express Graphics Lanes.	O PCIE		

3.3.5. LPC Bus

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		Chipset has internal pull-up
LPC_FRAME#	B3	LPC frame indicates the start of an LPC cycle	O 3.3V		
LPC_DRQ0# LPC_DRQ1#	B8 B9	LPC serial DMA request	I 3.3V		Platform has internal PU
LPC_SERIRQ	A50	LPC serial interrupt	I/O OD 3.3V	PU 8.2k 3.3V	
LPC_CLK	B10	LPC clock output –33MHz nominal	O 3.3V		

Note: eSPI and LPC buses are muxed. Express-BD7 module only supports LPC interface.

3.3.6. USB

Signal	Pin	Description	I/O	PU/PD	Comment
USB0+ USB0-	A46 A45	USB differential data pairs for Port 0	I/O 3.3VSB		USB 1.1/ 2.0 compliant

Signal	Pin	Description	I/O	PU/PD	Comment
USB1+ USB1-	B46 B45	USB differential data pairs for Port 1	I/O 3.3VSB		USB 1.1/ 2.0 compliant
USB2+ USB2-	A43 A42	USB differential data pairs for Port 1	I/O 3.3VSB		USB 1.1/ 2.0 compliant
USB3+ USB3-	B43 B42	USB differential data pairs for Port 2	I/O 3.3VSB		USB 1.1/ 2.0 compliant
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 high on carrier
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 high on carrier
USB0_HOST_PRSNT	A48	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 Supported. Limitation of this platform

3.3.7. USB Root Segmentation

All USB from XHCI controller

3.3.8. SPI (BIOS only)

Signal	Pin	Description	I/O	PU/PD	Comment
SPI_CS#	B97	Chip select for Carrier Board SPI BIOS Flash.	O 3.3VSB	PU 10k 3.3VSB	
SPI_MISO	A92	Data in to module from carrier board SPI BIOS flash.	I 3.3VSB		
SPI_MOSI	A95	Data out from module to carrier board SPI BIOS flash.	O 3.3VSB		
SPI_CLK	A94	Clock from module to carrier board SPI BIOS flash.	O 3.3VSB		
SPI_POWER	A91	Power supply for Carrier Board SPI – sourced from Module – nominally 3.3V. The Module shall provide a minimum of 100mA on SPI_POWER. Carriers shall use less than 100mA of SPI_POWER. SPI_POWER shall only be used to power SPI devices on the Carrier	O P 3.3VSB		
BIOS_DIS0#	A34	Selection strap to determine the BIOS boot device.	I	PU 10k 3.3VSB	Carrier shall pull to GND or leave not-connected.
BIOS_DIS1#	B88	Selection strap to determine the BIOS boot device.	I	PU 10k 3.3VSB	Carrier shall pull to GND or leave not-connected

3.3.9. Miscellaneous

Signal	Pin	Description	I/O	PU/PD	Comment
SPKR	B32	Output for audio enunciator, the “speaker” in PC-AT systems	O 3.3V	PU 1k 3.3V	Platform specification
WDT	B27	Output indicating that a watchdog time-out event has occurred.	O 3.3V	PU 10k 3.3V	
THRM#	B35	Input from off-module temp sensor indicating an over-temp situation.	I 3.3VSB		
THRMTRIP#	A35	Active low output indicating that the CPU has entered thermal shutdown.	O 3.3V	PU 10k 3.3V	
FAN_PWMOUT	B101	Fan speed control. Uses the Pulse Width Modulation (PWM) technique to control the fan’s RPM.	O OD 3.3V	PU 2.2K 3.3V	
FAN_TACHIN	B102	Fan tachometer input for a fan with a two pulse output.	I OD 3.3V	PU 47K 3.3V	
TPM_PP	A96	Trusted Platform Module (TPM) Physical Presence pin. Active high. TPM chip has an internal pull down. This signal is used to indicate Physical Presence to the TPM.	I 3.3V	PD 100k 3.3V	PD only when TPM on module

3.3.10. SMBus

Signal	Pin	Description	I/O	PU/PD	Comment
SMB_CK	B13	System Management Bus bidirectional clock line. Power sourced through 5V standby rail and main power rails.	I/O OD 3.3VSB	PU 2.2k 3.3VSB	Equivalent resistor is 2.2k
SMB_DAT#	B14	System Management Bus bidirectional data line. Power sourced through 5V standby rail and main power rails.	I/O OD 3.3VSB	PU 2.2k 3.3VSB	Equivalent resistor is 2.2k
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. Power sourced through 5V standby rail and main power rails.	I 3.3VSB	PU 10k 3.3VSB	

3.3.11. I2C Bus

Signal	Pin	Description	I/O	PU/PD	Comment
I2C_CK	B33	General purpose I²C port clock output/input	I/O OD 3.3VSB	PU 2.2K 3.3VSB	Source SEMA BMC
I2C_DAT	B34	General purpose I²C port data I/O line	I/O OD 3.3VSB	PU 2.2K 3.3VSB	Source SEMA BMC

3.3.12. General Purpose I/O (GPIO)

Signal	Pin	Description	I/O	PU/PD	Comment
GPO[0]	A93	General purpose output pins.	O 3.3V	PU 10K 3.3V	After hardware RESET output low
GPO[1]	B54	General purpose output pins.	O 3.3V	PU 10K 3.3V	After hardware RESET output low
GPO[2]	B57	General purpose output pins.	O 3.3V	PU 10K 3.3V	After hardware RESET output low
GPO[3]	B63	General purpose output pins.	O 3.3V	PU 10K 3.3V	After hardware RESET output low
GPI[0]	A54	General purpose input pins. Pulled high internally on the module.	I 3.3V	PU 10K 3.3V	
GPI[1]	A63	General purpose input pins. Pulled high internally on the module.	I 3.3V	PU 10K 3.3V	
GPI[2]	A67	General purpose input pins. Pulled high internally on the module.	I 3.3V	PU 10K 3.3V	
GPI[3]	A85	General purpose input pins. Pulled high internally on the module.	I 3.3V	PU 10K 3.3V	

3.3.13. Serial Interface Signals

Signal	Pin	Description	I/O	PU/PD	Comment
SER0_TX	A98	General purpose serial port transmitter (TTL level output)	O CMOS	PU 10k 5V	Power rail tolerance 5V, 12V
SER0_RX	A99	General purpose serial port receiver (TTL level input)	I CMOS	PU 10k 5V	Power rail tolerance 5V, 12V
SER1_TX	A101	General purpose serial port transmitter (TTL level output)	O CMOS	PU 10k 5V	Power rail tolerance 5V, 12V
SER1_RX	A102	General purpose serial port receiver (TTL level input)	I CMOS	PU 10k 5V	Power rail tolerance 5V, 12V

3.3.14. Power and System Management

Signal	Pin	Description	I/O	PU/PD	Comment
PWRBTN#	B12	Power button to bring system out of S5 (soft off), active on falling edge.	I 3.3VSB	PU 10k 3.3VSB	
SYS_RESET#	B49	Reset button input. Active low request for module to reset and reboot. May be falling edge sensitive. For situations when SYS_RESET# is not able to reestablish control of the system, PWR_OK or a power cycle may be used.	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 hold off Module startup to allow carrier based FPGAs or other configurable devices time to be programmed.	I 3.3VSB	PU 1k 3.3VSB	Should have weak pull up

Signal	Pin	Description	I/O	PU/PD	Comment
SUS_STAT#	B18	Indicates imminent suspend operation; used to notify LPC devices.	O 3.3VSB	PU 10k 3.3VSB	
SUS_S3#	A15	Indicates system is in Suspend to RAM state. Active-low output. An inverted copy of SUS_S3# on the carrier board (also known as “PS_ON”) may be used to enable the non-standby power on a typical ATX power supply.	O 3.3VSB		
SUS_S4#	A18	Indicates system is in Suspend to Disk state. Active low output.	O 3.3VSB		
SUS_S5#	A24	Indicates system is in Soft Off state.	O 3.3VSB		
WAKE0#	B66	PCI Express wake up signal.	I 3.3VSB	PU 1k 3.3VSB	
WAKE1#	B67	General purpose wake up signal. May be used to implement wake-up on PS/2 keyboard or mouse activity.	I 3.3VSB	PU 1k 3.3VSB	Connect to WAKE 1#
BATLOW#	A27	Battery low input. This signal may be driven low by external circuitry to signal that the system battery is low, or may be used to signal some other external power-management event.	I 3.3VSB	PU 10k 3.3VSB	
LID#	A103	LID button. Low active signal used by the ACPI operating system for a LID switch.	I OD 3.3VSB	PU 47k 3.3VSB	
SLEEP#	B103	Sleep button. Low active signal used by the ACPI operating system to bring the system to sleep state or to wake it up again.	I OD 3.3VSB	PU 47k 3.3VSB	

3.3.15. Power and Ground

Signal	Pin	Description	I/O	PU/PD	Comment
VCC_12V	A104-A109 B104-B109	Primary power input: +12V nominal (wide range 5-20V). All available VCC_12V pins on the connector(s) shall be used.	P		8.5-20 V
VCC_5V_SBY	B84-B87	Standby power input: +5.0V nominal. See COM.0 Base Specification, Section 7 “Electrical Specifications“ for allowable input range. 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		5Vsb ±5%
VCC_RTC	A47	Real-time clock circuit-power input. Nominally +3.0V.	P		
GND	A1, A11, A21, A31, A41, A51, A57, A66, A80, A90, A96, A100, A110, B1, B11, B21,B31, B41, B51, B60, B70, B80, B90, B100, B110	Ground - DC power and signal and AC signal return path.	P		

3.4. CD Signal Descriptions

3.4.1. USB 3.0 Extension

Signal	Pin	Description	I/O	PU/PD	Comment
USB_SSRX0- USB_SSRX0+	C3 C4	Additional Receive signal differential pairs for the SuperSpeed USB data path on USB0	I PCIE		AC coupled off module
USB_SSTX0- USB_SSTX0+	D3 D4	Additional Transmit signal differential pairs for the SuperSpeed USB data path on USB0	O PCIE		AC coupled on module
USB_SSRX1- USB_SSRX1+	C6 C7	Additional Receive signal differential pairs for the SuperSpeed USB data path on USB1	I PCIE		AC coupled off module
USB_SSTX1- USB_SSTX1+	D6 D7	Additional Transmit signal differential pairs for the SuperSpeed USB data path on USB1	O PCIE		AC coupled on module
USB_SSRX2- USB_SSRX2+	C9 C10	Additional Receive signal differential pairs for the SuperSpeed USB data path on USB2	I PCIE		AC coupled off module
USB_SSTX2- USB_SSTX2+	D9 D10	Additional Transmit signal differential pairs for the SuperSpeed USB data path on USB2	O PCIE		AC coupled on module
USB_SSRX3- USB_SSRX3+	C12 C13	Additional Receive signal differential pairs for the SuperSpeed USB data path on USB3	I PCIE		AC coupled off module
USB_SSTX3- USB_SSTX3+	D12 D13	Additional Transmit signal differential pairs for the SuperSpeed USB data path on USB3	O PCIE		AC coupled on module

3.4.2. PCI Express x1

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

3.4.3. 10G Ethernet

10GbE port 0/1

Signal	Pin	Description	I/O	PU/PD	Comment
10G_KR_RX0+ 10G_KR_RX0- 10G_KR_RX1+ 10G_KR_RX1-	C49 C50 C42 C43	10GBASE-KR ports, Receive Input differential paris	I KR		AC coupled on Module
10G_KR_TX0+ 10G_KR_TX0- 10G_KR_TX1+ 10G_KR_TX1-	D49 D50 D42 D43	10GBASE-KR ports, Transmit Output differential paris	O KR		AC coupled on Carrier
10G_INT0 10G_INT1	C47 D47	Interrupt pin from Copper PHY or Optical SFP+ module to the 10GbE controller	I 3.3VSB	PU 2.2k 3.3VSB	
10G_PHY_MDIO_SDA0	D46	**MDIO Mode** Management Data I/O Interface mode data signal for serial data transfers between the MAC and an external PHY	O 3.3VSB		
		I^2C Mode I^2C Data signal, of the 2-wire management interface used for serial data transfers between the MAC and the external PHY	I/O OD 3.3VSB	PU 2.2k 3.3VSB	
10G_PHY_MDC_SCL0	C46	**MDIO Mode** Management Data I/O Interface mode clock signal for serial data transfers between the MAC and an external PHY	O 3.3VSB		
		I^2C Mode I^2C Data signal, of the 2-wire management interface used for serial data transfers between the MAC and the external PHY	I/O OD 3.3VSB	PU 2.2k 3.3VSB	
10G_PHY_MDIO_SDA1	D45	**MDIO Mode** Management Data I/O Interface mode data signal for serial data transfers between the MAC and an external PHY	O 3.3VSB		
		I^2C Mode I^2C Data signal, of the 2-wire management interface used for serial data transfers between the MAC and the external PHY	I/O OD 3.3VSB	PU 2.2k 3.3VSB	
10G_PHY_MDC_SCL1	C45	**MDIO Mode** Management Data I/O Interface mode clock signal for serial data transfers between the MAC and an external PHY	O 3.3VSB		
		I^2C Mode I^2C Data signal, of the 2-wire management interface used for serial data transfers between the MAC and the external PHY	I/O OD 3.3VSB	PU 2.2k 3.3VSB	
10G_SDP0 10G_SDP1	C40 D40	Software-Definable Pins	I/O 3.3VSB	PU 10k 3.3VSB	
10G_SFP_SDA0 10G_SFP_SDA1	C39 C38	I^2C Data signal, of the 2-wire management interface used by 10GbE	I/O OD 3.3VSB	PU 2.2k 3.3VSB	

Signal	Pin	Description	I/O	PU/PD	Comment
		controller to access the management registers of an external Optical SFP+ module			
10G_SFP_SCL0 10G_SFP_SCL1	D39 D38	I^2C Clock signal, of the 2-wire management interface used by 10GbE controller to access the management registers of an external Optical SFP+ module	I/O OD 3.3VSB	PU 2.2k 3.3VSB	
10G_PHY_RST_01	C35	Output signal that resets and Optical PHY on port 0 and port 1	O 3.3VSB		This signal is not used for Copper PHY
10G_PHY_CAP_01	D35	Phy mode capability pin: Indicates if the PHY for 10G lanes 0 and1 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, in part based on this input. The actual protocol used is indicated over the dedicated I2C interface	I 3.3VSB	PU 10k 3.3VSB	Default state is MDIO mode. For I^2C mode pull down with 1K on carrier
10G_LED_SDA	C36	I^2C Data signal, of the 2-wire that transfers all LED signals and additional Strapping signal for I^2C or MDIO mode of Optical PHY	I/O OD 3.3VSB	PU 2.2k 3.3VSB	LED signals for 10GbE port 2/3 are also transferred through this pin
10G_LED_SCL	C37	I^2C Clock signal, of the 2-wire that transfers all LED signals and additional Strapping signal for I^2C or MDIO mode of Optical PHY	I/O OD 3.3VSB	PU 2.2k 3.3VSB	LED signals for 10GbE port 2/3 are also transferred through this pin

3.4.4. PCI Express

Signal	Pin	Description	I/O	PU/PD	Comment
PCIE_TX16+ PCIE_TX16-	D52 D53	PCI Express channel 16, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX16+ PCIE_RX16-	C52 C53	PCI Express channel 16, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX17+ PCIE_TX17-	D55 D56	PCI Express channel 17, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX17+ PCIE_RX17-	C55 C56	PCI Express channel 17, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX18+ PCIE_TX18-	D58 D59	PCI Express channel 18, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX18+ PCIE_RX18-	C58 C59	PCI Express channel 18, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX19+ PCIE_TX19-	D61 D62	PCI Express channel 19, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX19+ PCIE_RX19-	C61 C62	PCI Express channel 19, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX20+ PCIE_TX20-	D65 D66	PCI Express channel 20, Transmit Output differential pair.	O PCIE		AC coupled on Module

Signal	Pin	Description	I/O	PU/PD	Comment
PCIE_RX20+ PCIE_RX20-	C65 C66	PCI Express channel 20, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX21+ PCIE_TX21-	D68 D69	PCI Express channel 21, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX21+ PCIE_RX21-	C68 C69	PCI Express channel 21, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX22+ PCIE_TX22-	D71 D72	PCI Express channel 22, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX22+ PCIE_RX22-	C71 C72	PCI Express channel 22, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX23+ PCIE_TX23-	D74 D75	PCI Express channel 23, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX23+ PCIE_RX23-	C74 C75	PCI Express channel 23, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX24+ PCIE_TX24-	D78 D79	PCI Express channel 24, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX24+ PCIE_RX24-	C78 C79	PCI Express channel 24, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX25+ PCIE_TX25-	D81 D82	PCI Express channel 25, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX25+ PCIE_RX25-	C81 C82	PCI Express channel 25, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX26+ PCIE_TX26-	D85 D86	PCI Express channel 26, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX26+ PCIE_RX26-	C85 C86	PCI Express channel 26, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX27+ PCIE_TX27-	D88 D89	PCI Express channel 27, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX27+ PCIE_RX27-	C88 C89	PCI Express channel 27, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX28+ PCIE_TX28-	D91 D92	PCI Express channel 28, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX28+ PCIE_RX28-	C91 C92	PCI Express channel 28, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX29+ PCIE_TX29-	D94 D95	PCI Express channel 29, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX29+ PCIE_RX29-	C94 C95	PCI Express channel 29, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX30+ PCIE_TX30-	D98 D99	PCI Express channel 30, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX30+ PCIE_RX30-	C98 C99	PCI Express channel 30, Receive Input differential pair.	I PCIE		AC coupled off Module

Signal	Pin	Description	I/O	PU/PD	Comment
PCIE_TX31+ PCIE_TX31-	D101 D102	PCI Express channel 31, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX31+ PCIE_RX31-	C101 C102	PCI Express channel 31, Receive Input differential pair.	I PCIE		AC coupled off Module

3.4.5. Module Type Definition

Signal	Pin	Description	I/O	Comment
TYPE0# TYPE1# TYPE2# TYPE7#	C54 C57 D57	The TYPE pins indicate to the Carrier Board the Pin-out Type that is implemented on the module. The pins are tied on the module to either ground (GND) or are no-connects (NC). For Pinout Type 1, these pins are don't care (X). TYPE2# TYPE1# TYPE0# X X X Pinout Type 1 NC NC NC Pinout Type 2 NC NC GND Pinout Type 3 (no IDE) NC GND NC Pinout Type 4 (no PCI) NC GND GND Pinout Type 5 (no IDE, no PCI) GND NC NC Pinout Type 6 (no IDE, no PCI) **GND NC GND Pinout Type 7 (server level with 10GbE)** 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.		Type 7

3.4.6. Power and Ground

Signal	Pin	Description	I/O	PU/PD	Comment
VCC_12V	C104-C109 D104-D109	Primary power input: +12V nominal (wide range 5-20V). All available VCC_12V pins on the connector(s) shall be used	P		8.5-20V
GND	C1, C11, C21, C31, C41, C51, C60, C70, C76, C80, C84, C87, C90, C93, C96, C100, C103, C110, D1, D11, D21, D31, D41, D51, D60, D67, D70, 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		

4. Connector Pinouts on Module

This chapter describes connectors and pinouts, LEDs and switches that are used on the module but are not included in the PICMG standard specification

4.1. Connector, Switch and LED Locations

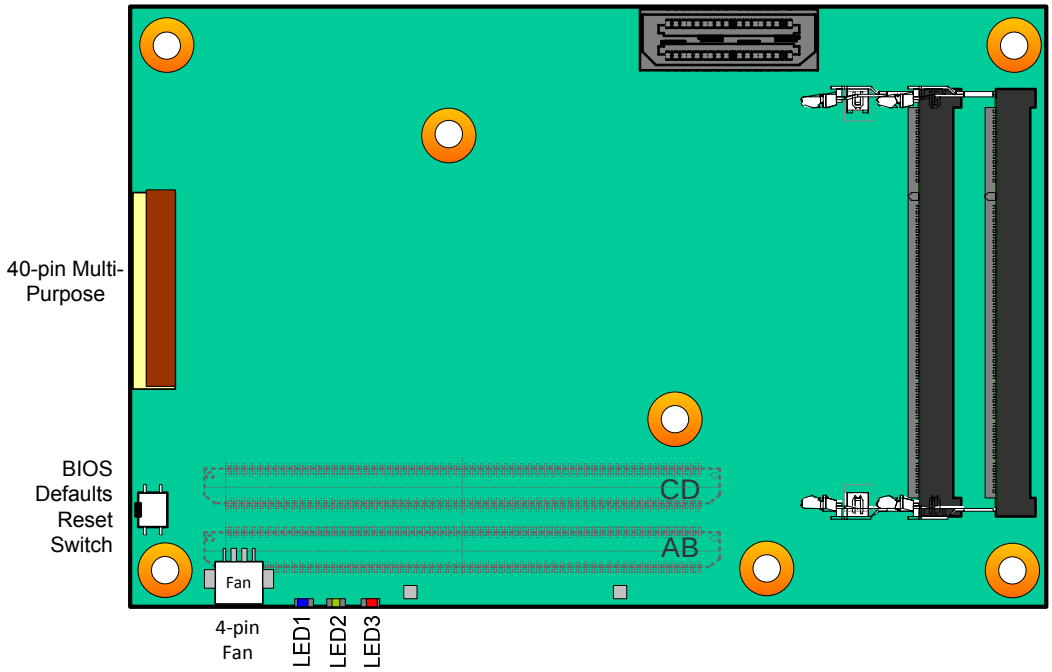


Figure 3: Express-BD7 Connector, Switch and LED Locations

Express-BD7 and the DB40 Debug Module

For illustration purposes only

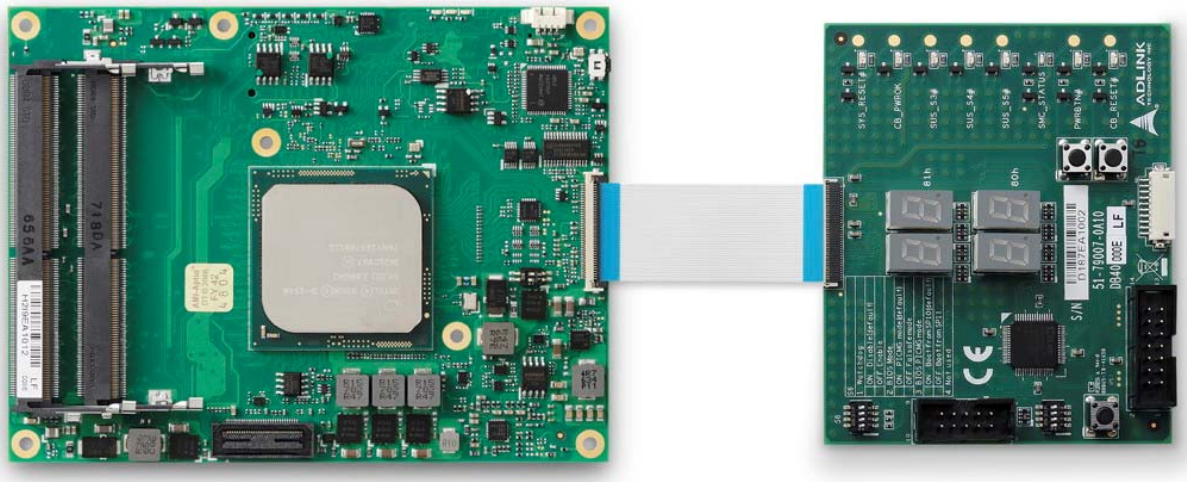


Figure 4: Express-BD7 and the DB40 Debug Module

4.2. 40-pin Debug Connector

FPC Connector Type: Molex 502790-4091

Pin Orientation

1 40

40-pin Debug Connector Pin Definition on the COM Express Module

Pin	Interface	Signal	Remark
40	SPI Program interface	VCC_SPI_IN	
39		GND	
38		SPI_BIOS_CS0#	
37		SPI_BIOS_CS1#	PU 10k 3.3VSB
36		SPI_BIOS_MISO	
35		SPI_BIOS_MOSI	
34		SPI_BIOS_CLK	
33	LPC Bus	3V3_LPC	
32		GND	
31		BIOS_DIS0	PU 10k 3.3VSB
30		RST#	
29		CLK33_LPC	
28		LPC_FRAME#	
27		LPC_AD3	
26		LPC_AD2	
25		LPC_AD1	
24		LPC_AD0	
23	BMC Program interface	3.3V_BMC	
22		3.3V_BMC	
21		GND	

Pin	Interface	Signal	Remark
20	BMC Program interface (cont'd)	TXD6	
19		RXD6	
18		FUMD0	
17		RESET_IN#	PU 10k 3.3VSB
16		DATA	PU 2.2k 3.3VSB Equivalent
15		CLK	PU 2.2k 3.3VSB Equivalent
14		OCD0A	
13		OCD0B	
12	Test points	PWRBTN#	PU 10k 3.3VSB
11		SYS_RESET#	PU 10k 3.3VSB
10		CB_RESET#	PU 1k 3.3VSB
9		CB_PWROK	
8		SUS_S3#	
7		SUS_S4#	
6		SUS_S5#	
5	BMC Debug signals	POSTWDT_DIS#	PU 100k 3.3VSB
4		SEL_BIOS	
3		BIOS_MODE	
2		BMC_STATUS	
1	Reserved		Tied to GND through 0ohm resistor

Table 2: 40-pin Debug Connector Pin Definition

Note: The pin definition on the debug module is the inverse of that on the COM Express module.

4.3. Status LEDs

To facilitate easier maintenance, status LED's are mounted on the board.

LED1 LED2 LED3

LED Descriptions

Name	Color	Connection	Function
LED1	Blue	BMC output	Power Sequence Status Code (BMC) Power Changes, RESET (see 5.1.4 Exception Codes below)
LED2	Green	Power Source 3Vcc	S0 LED ON S3/S4/S5 LED OFF ECO mode LED OFF
LED3	Red	BMC output and same signal as WDT (B27) on BtB connector	Module power up LED OFF Watchdog counting Keep last state Watchdog timed out LED ON Watchdog RESET LED ON Rebooted after WD RESET LED ON Rebooted after PWRBTN LED OFF Rebooted after RESET BTN LED OFF Note: only a RESET not initiated by the BMC can clear the WD LED (user action)

Table 3: Express-BD7 LED Descriptions

4.4. XDP Debug Header

The debug port is a connection into a target-system environment that provides access to JTAG, run control, system control, and observation resources. The XDP target system connector is a Samtec™ 60-pin BSH-030-01 series connector.

Pin	XDP Signal	Target Signal	I/O	Device
1	GND	GND	NA	
3	OBSFN_A0	PREQ#	I/O	Processor
5	OBSFN_A1	PRDY#	I/O	Processor
7	GND	GND	NA	
9	OBSDATA_A0	CFG[0][2]	I/O	Processor
11	OBSDATA_A1	CFG[1][2]	I/O	Processor
13	GND	GND	NA	
15	OBSDATA_A2	CFG[2][2]	I/O	Processor
17	OBSDATA_A3	CFG[3][2]	I/O	Processor
19	GND	GND	NA	
21	OBSFN_B0	BPM#[0][1]	I/O	Processor
23	OBSFN_B1	BPM#[1][1]	I/O	Processor
25	GND	GND	NA	
27	OBSDATA_B0	CFG[4][2]	I/O	Processor
29	OBSDATA_B1	CFG[5][2]	I/O	Processor
31	GND	GND	NA	
33	OBSDATA_B2	CFG[6][2]	I/O	Processor
35	OBSDATA_B3	CFG[7][2]	I/O	Processor
37	GND	GND	NA	
39	HOOK0	PWRGOOD	I	System
41	HOOK11	BP_PWRGD_RST#	O	System
43	VCC_OBS_AB	VCCIO_OUT	I	System
45	HOOK2	PWR_DEBUG	O	Processor
47	HOOK3	PCH_SYS_PWROK	O	System
49	GND	GND	NA	
51	SDA1	SDA	I/O	System
53	SCL1	SCL	I/O	System
55	TCK1	Open	NA	
57	TCK0	TCK	O	Processor
59	GND	GND	NA	

Pin	XDP Signal	Target Signal	I/O	Device
2	GND	GND	NA	
4	OBSFN_C0	CFG[17][2]	I	Processor
6	OBSFN_C1	CFG[16][2]	I	Processor
8	GND	GND	NA	
10	OBSDATA_C0	CFG[8][2]	I/O	Processor
12	OBSDATA_C1	CFG[9][2]	I/O	Processor
14	GND	GND	NA	
16	OBSDATA_C2	CFG[10][2]	I/O	Processor
18	OBSDATA_C3	CFG[11][2]	I/O	Processor
20	GND	GND	NA	
22	OBSFN_D0	CFG[19][2]	I/O	Processor
24	OBSFN_D1	CFG[18][2]	I/O	Processor
26	GND	GND	NA	
28	OBSDATA_D0	CFG[12][2]	I	Processor
30	OBSDATA_D1	CFG[13][2]	I	Processor
32	GND	GND	NA	
34	OBSDATA_D2	CFG[14][2]	I/O	Processor
36	OBSDATA_D3	CFG[15][2]	I/O	Processor
38	GND	GND	NA	
40	ITPCLK/HOOK4	Open	NA	
42	ITPCLK#/HOOK5	Open	NA	
44	VCC_OBS_CD	VCCIO_OUT	I	System
46	HOOK6/RESET#	PLTRSTIN#	I	System
48	HOOK7/DBR#	DBR#	O	System
50	GND	GND	NA	
52	TDO	TDO	I	Processor
54	TRSTn	TRST#	O	Processor
56	TDI	TDI	O	Processor
58	TMS	TMS	O	Processor
60	GND	GND (or XDP_PRESENT# if required)	NA	

Table 4: XDP Debug Header Pin Definition

Notes:

1. These signals are optional, can be left as OPEN/No-Connect if debug by Intel will not be needed.
2. These CFG signals can be left as Open/No Connect if not used as a strapping signal and top side probe will be used to debug processor.

Refer to the "Shark Bay, Denlow and Broadwell U/Y Platforms Debug Port Design Guide", Document Number: 479493, Revision: 2.0

4.5. Fan Connector

Connector Type: JVE 24W1125A-04M00

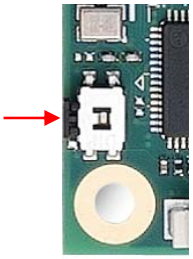
Pin Orientation

Pin Assignment

Name	Signal
1	FAN_PWMOUT
2	FAN_TACHIN
3	Ground
4	5V

Table 5: Fan Connector Pin Definition

4.6. BIOS Setup Defaults Reset Button



To perform a hardware reset of BIOS default settings, perform the following steps:

1. Shut down the system.
2. Press the BIOS Setup Defaults RESET Button continuously and boot up the system. You can release the button when the BIOS prompt screen appears
3. The BIOS prompt screen will display a confirmation that BIOS defaults have been reset and request that you reboot the system.

4.7. Switch Settings

Switch Locations

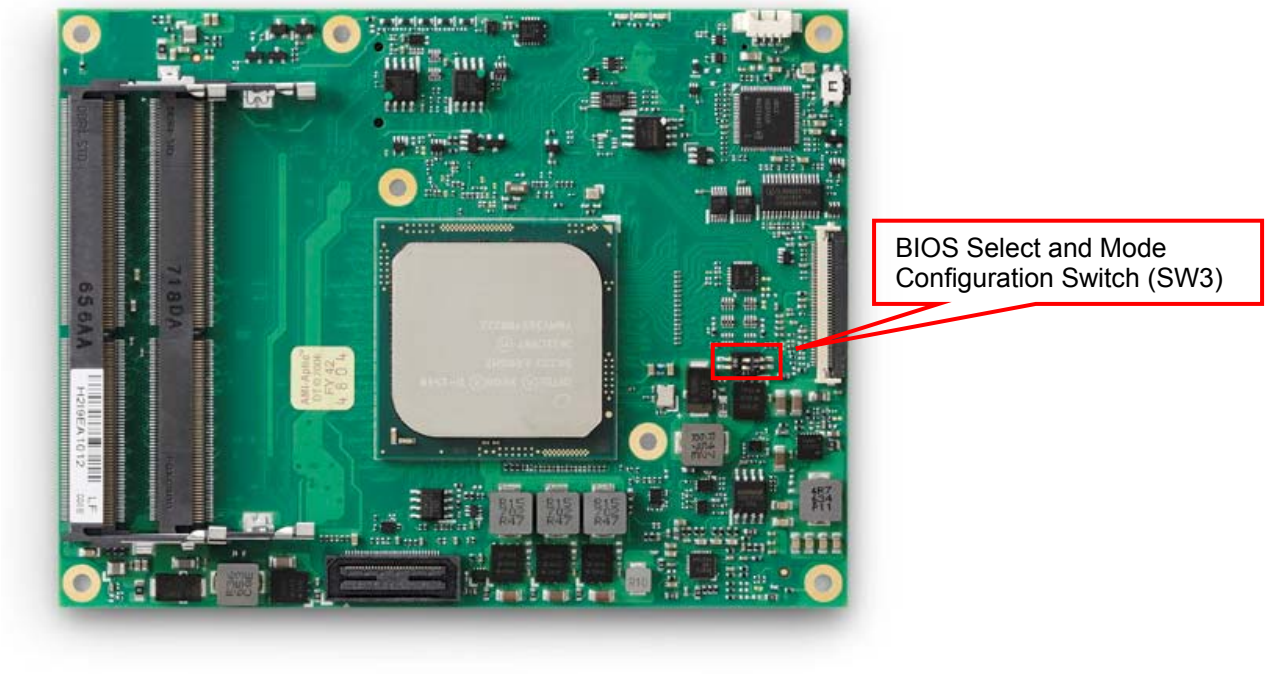


Figure 5: cExpress Switch Locations

BIOS Select and Mode Configuration Switch

The module has two BIOS chips and BIOS operation can be configured to "PICMG" and dual-BIOS "Failsafe" modes using the BIOS Select and Mode Configuration Switch (SW3), Pin 2.

Setting the module to PICMG mode will configure the BIOS chips on the module as SPI0 and SPI1. In PICMG mode, a BIOS chip cannot be placed in the SPI0 slot on the carrier.

In dual-BIOS Failsafe mode, both BIOS chips on the module are configured as SPI1. Only one of the two is connected to the SPI bus at any given time. In case of failure of the primary SPI1 BIOS, the system will reboot and switch to the secondary SPI1 BIOS on the module. In Failsafe mode, the SPI0 BIOS socket on the carrier can be populated.

In either mode, Pin 1 is used to select whether to boot from SPI0 or SPI1.

Mode	Pin 1	Pin 2
Boot from SPI0 (default)	On	—
Boot from SPI1	Off	—
Set BIOS to PICMG mode	—	On
Set BIOS to Failsafe BIOS mode (default)	—	Off

Table 6: BIOS Select and Mode Configuration Switch Settings

4.8. PCIe x16-to-two-x8 Adapter Card

The Express-BD7 can be used with the PCIe x16-to-two-x8 Adapter Card on the Express-BASE7 Reference Carrier to support bifurbication of the PCIe x16 interface. The card reroutes the PCIe x16 to two x8 and allows testing of two independent PCIe add-on cards with x8/x4/x2/x1 width. To use the card, set **BIOS > Chipset > IIO Configuration > IIO0 Configuration > IOU1 (IIO PCIe Port 3)** to "x8x8 ".

PCIex16-to-two-x8 Adapter Card
(Model: P16TO28, Part No.: 91-79301-0010)

4.9. PCIe x8-to-two-x4 Adapter Card

The Express-BD7 can be used with the PCIe x8-to-two-x4 Adapter Card on the Express-BASE7 Reference Carrier to support bifurbication of the PCIe x8 interface. The card reroutes the PCIe x8 to two x4 and allows testing of two independent PCIe add-on cards with x4/x2/x1 width. To use the card, set **BIOS > Chipset > IIO Configuration > IIO0 Configuration > IOU2 (IIO PCIe Port 1)** to "x4x4 ".

PCIex8-to-two-x4 Adapter Card
(Model: P8TO24, Part No.:)

5. Smart Embedded Management Agent (SEMA)

The onboard microcontroller (BMC) implements power sequencing and Smart Embedded Management Agent (SEMA) functionality. The microcontroller communicates via the System Management Bus with the CPU/chipset. The following functions are implemented:

- Total operating hours counter. Counts the number of hours the module has been run in minutes.
- On-time minutes counter. Counts the seconds since last system start.
- Temperature monitoring of CPU and board temperature. Minimum and maximum temperature values of CPU and board are stored in flash.
- Power cycles counter
- Boot counter. Counts the number of boot attempts.
- Watchdog Timer. Set/Reset/Disable Watchdog Timer. Features auto-reload at power-up.
- System Restart Cause. Power loss/BIOS Fail/Watchdog/Internal Reset/External Reset
- Fail-safe BIOS support. In case of a boot failure, hardware signals tells external logic to boot from fail-safe BIOS.
- Flash area. 1kB Flash area for customer data
- 2K Bytes Protected Flash area. Keys, IDs, etc. can be stored in a write- and clear-protectable region.
- Board Identify. Vendor/Board/Serial number/Production Date
- Main-current & voltage. Monitors drawn current and main voltages

For a detailed description of SEMA features and functionality, please refer to **SEMA Technical Manual** and **SEMA Software Manual**, downloadable at: **http://www.adlinktech.com/sema/**.

5.1. Board Specific SEMA Functions

5.1.1. Voltages

The BMC of the Express-BD7 implements a voltage monitor and samples several onboard voltages. The voltages can be read by calling the SEMA function “Get Voltages”. The function returns a 16-bit value divided into high-byte (MSB) and low-byte (LSB).

ADC Channel	Voltage Name	Voltage Formula [V]
0	VCORE	(MSB<<8 + LSB) x 1.0 x 3.3 / 1024
1	VMEM	(MSB<<8 + LSB) x 1.0 x 3.3 / 1024
2	3.3V	(MSB<<8 + LSB) x 1.1 x 3.3 / 1024
3	5VSB	(MSB<<8 + LSB) x 1.826 x 3.3 / 1024
4	VIN	(MSB<<8 + LSB) x 3.7 x 3.3 / 1024
5	3.3VSB	(MSB<<8 + LSB) x 1.1 x 3.3 / 1024
6	5V	(MSB<<8 + LSB) x 1.826 x 3.3 / 1024

Table 7: SEMA Onboard Voltage Monitor

5.1.2. Main Current

The BMC of the Express-BD7 implements a current monitor. The current can be read by calling the SEMA function “Get Main Current”. The function returns four 16-bit values divided in high-byte (MSB) and low-byte (LSB). These 4 values represent the last 4 currents drawn by the board. The values are sampled every 250ms. The order of the 4 values is NOT in chronological order. Access by the BMC may increase the drawn current of the whole system. In this case, there are still 3 samples not influenced by the read access.

Main Current = (MSB_n<<8 + LSB_n) x 8.06mA

5.1.3. BMC Status

This register shows the status of BMC controlled signals on the Express-BD7.

Status Bit	Signal
0	WDT_OUT
1	Reserved
2	Reserved
3	BIOS_MODE
4	POSTWDT_DISn
5	SEL_BIOS
6	BIOS_DIS0n
7	BIOS_DIS1n

Table 8: SEMA BMC Status

5.1.4. Exception Codes

In case of an error, the BMC drives a blinking code on the blue Status LED (LED1). The same error code is also reported by the BMC Flags register. The Exception Code is not stored in the Flash Storage and is cleared when the power is removed. Therefore, a “Clear Exception Code” command is not needed or supported.

Exception Code	Error Message
0	NOERROR
2	NO_SUSCLK
3	NO_SLP_S5
4	NO_SLP_S4
5	NO_SLP_S3
6	BIOS_FAIL
7	RESET_FAIL
8	RESETIN_FAIL
9	NO_CB_PWRGD
10	CRITICAL_TEMP
11	POWER FAIL
12	VOLTAGE_FAIL
13	RFID_MEMFAIL
14	NO_VDDQ_PG
15	NO_V1P05S_PG
16	NO_VCORE_PG
17	NO_SYS_GD
18	NO_V5SBY
19	NO_V3P3A
20	NO_V5_DUAL
21	NO_V12
22	NO_V1V7_A
23	NO_1V3_A
24	NO_V1V05_A
25	NO_P_5V_3V3_PG
26	NO_V2V5_S
28	NO_V1V5_S

Table 9: SEMA Exception Codes

5.1.5. BMC Flags

The BMC Flags register returns the last detected Exception Code since power-up and shows the BIOS in use and the power mode.

Bit	Description
[0 ~ 4]	Exception Code
[6]	0 = AT mode 1 = ATX mode
[7]	0 = Standard BIOS 1 = Fail-safe BIOS.

Table 10: SEMA BMC Flags

6. System Resources

6.1. System Memory Map

Memory Range	Target	Dependency/Comments
0000 0000h-000D FFFFh 0010 0000h-TOM (Top of Memory)	Main Memory	TOM registers in Host controller
000E 0000h-000E FFFFh	LPC or SPI	Bit6 in BIOS Decode Enable register is set
0000F 0000h-0000F FFFFh	LPC or SPI	Bit7 in BIOS Decode Enable register is set
FEC_ _000h-FEC_ _040h	IO(x) APIC inside intel(R) Xeon(R) Processor D-1500 Producy Family	_ _is controlled using APIC Range Select(ASEL) field and APIC Enable (AEN) bit
FEC1 0000h-FEC1 7FFFh	PCI Express Port 1	PCI Express Root Port 1 I/OxAPIC Enable(PAE) set
FEC1 8000h-FEC1 FFFFh	PCI Express Port 2	PCI Express Root Port 2 I/OxAPIC Enable(PAE) set
FEC2 0000h-FEC2 7FFFh	PCI Express Port 3	PCI Express Root Port 3 I/OxAPIC Enable(PAE) set
FEC2 8000h-FEC2 FFFFh	PCI Express Port 4	PCI Express Root Port 4 I/OxAPIC Enable(PAE) set
FEC3 0000h-FEC3 7FFFh	PCI Express Port 5	PCI Express Root Port 5 I/OxAPIC Enable(PAE) set
FEC3 8000h-FEC3 FFFFh	PCI Express Port 6	PCI Express Root Port 6 I/OxAPIC Enable(PAE) set
FEC4 0000h-FEC4 7FFFh	PCI Express Port 7	PCI Express Root Port 7 I/OxAPIC Enable(PAE) set
FEC4 8000h-FEC4 FFFFh	PCI Express Port 8	PCI Express Root Port 8 I/OxAPIC Enable(PAE) set
FEC0 0000h-FFC7 FFFFh FF80 0000h-FF87 FFFFh	LPC or SPI(or PCI)	Bit 8 in BIOS Decode Enable register is set
FEC8 0000h-FFCF FFFFh FF88 0000h-FF8F FFFFh	LPC or SPI(or PCI)	Bit 9 in BIOS Decode Enable register is set
FED0 0000h-FFD7 FFFFh FF90 0000h-FF97 FFFFh	LPC or SPI(or PCI)	Bit 10 in BIOS Decode Enable register is set
FFD8 0000h-FFDF FFFFh FF98 0000h-FF9F FFFFh	LPC or SPI(or PCI)	Bit11 in BIOS Decode Enable register is set
FFE0 0000h-FFE7 FFFFh FFA0 0000h-FFA7 FFFFh	LPC or SPI(or PCI)	Bit 12 in BIOS Decode Enable register is set
FFE8 0000h-FFEF FFFFh FFA8 0000h-FFAF FFFFh	LPC or SPI(or PCI)	Bit 13 in BIOS Decode Enable register is set
FFF0 0000h-FFF7 FFFFh FFB0 0000h-FFB7 FFFFh	LPC or SPI(or PCI)	Bit 14 in BIOS Decode Enable register is set
FFF8 0000h-FFFF FFFFh FFB8 0000h-FFBF FFFFh	LPC or SPI(or PCI)	Always enabled. The top two 64 KB blocks of this range can be swapped,as described in Section 4.4.1(Doc#544044)
FF70 0000h-FF7F FFFFh FF30 0000h-FF3F FFFFh	LPC or SPI(or PCI)	Bit 3 in BIOS Decode Enable register is set
FF60 0000h-FF6F FFFFh FF20 0000h-FF2F FFFFh	LPC or SPI(or PCI)	Bit 2 in BIOS Decode Enable register is set
FF50 0000h-FF5F FFFFh FF10 0000h-FF1F FFFFh	LPC or SPI(or PCI)	Bit 1 in BIOS Decode Enable register is set

Memory Range	Target	Dependency/Comments
FF40 0000h-FF4F FFFFh FF00 0000h-FF0F FFFFh	LPC or SPI(or PCI)	Bit 0 in BIOS Decode Enable register is set
128 KB anywhere in 4GB range	Integrated LAN Controller	Enable using BAR in D25:F0(Integrated LAN Controller MBARA)
4 KB anywhere in 4GB range	Integrated LAN Controller	Enable using BAR in D25:F0(Integrated LAN Controller MBARA)
1 KB anywhere in 4GB range	USB EHCI Controller	Enable using standard PCI mechanism(D29:F0)
64 KB anywhere in 4GB range	USB xHCI Controller	Enable using standard PCI mechanism(D20:F0)
FED0 X000h-FED0 X3FFh	High Precision Event Timers	BIOS determines the “fixed location which is one of four,1-KB ranges where X(in the first column) is 0h,1h,2h,or 3h”
FED0 X000h-FED4 FFFFh	TPM on LPC	None
Memory Base/Limit anywhere in 4 GB range	PCI Bridge	Enable using standard PCI mechanism(D30:F0)
Prefetchable Memory Base/Limit anywhere in 64-bit address range	PCI Bridge	Enable using standard PCI mechanism(D30:F0)
64 KB anywhere in 4 GB range	LPC	LPC Generic Memory Range.Enable using setting bit[0] of the LPC Generic Memory Range register(D31:F0:offset 98h)
32 Bytes anywhere in 64-bit address range	SMBus	Enable using standard PCI mechanism(D31:F3)
2 KB anywhere above 64 KB to 4 GB range	SATA Host Controller # 1	AHCI memory-mapped registers.Enable using standard PCI mechanism.(D31:F2)
Memory Base/Limit anywhere in 4 GB range	PCI Express Root Ports1-8	Enable using standard PCI mechanism(D28:F 0-7)
Prefetchable Memory Base/Limit anywhere in 64-bit address range	PCI Express Root Ports1-8	Enable using standard PCI mechanism(D28:F 0-7)
4 KB anywhere in 64-bit address range	Thermal Reporting	Enable using standard PCI mechanism(D34:F6 TBAR/TBARH)
4 KB anywhere in 64-bit address range	Thermal Reporting	Enable using standard PCI mechanism(D34:F6 TBARB/TBARBH)
16 Bytes anywhere in 64-bit address range	Intel(R) MEI #1,#2	Enable using standard PCI mechanism(D22:F 1:0)
4 KB anywhere in 4 GB range	KT	Enable using standard PCI mechanism(D22:F3)
16 KB anywhere in 4 GB range	Root Complex Register Block(RCRB)	Enable using setting bit[0] of the Root Complex Base Address register(D34:F0 offset F0h)

6.2. Direct Memory Access Channels

Channel Number	Data Width	System Resource
0	8-bits	Generic
1	8-bits	Generic
2	8-bits	Generic
3	8-bits	Generic
4		Reserved - cascade channel
5	16-bits	Generic
6	16-bits	Generic
7	16-bits	Generic

6.3. Fixed I/O Address Range Map

Hex Range	Device
000-008	DMA Controller
009-00E	DMA Controller
0F	DMA Controller
010-018	DMA Controller
019-01E	DMA Controller
020-021	Interrupt Controller
024-025	Interrupt Controller
028-029	Interrupt Controller
02C-02D	Interrupt Controller
02E-02F	LPC SIO
030-031	Interrupt Controller
034-035	Interrupt Controller
038-039	Interrupt Controller
03C-03D	Interrupt Controller
040-042	Timer/Counter
043	Timer/Counter
04E-04F	LPC SIO
050-052	Timer/Counter
053	Timer/Counter
060	Microcontroller
061	NMI Controller
062	Microcontroller
064	Microcontroller
066	Microcontroller

Hex Range	Device
070-077	RTC
080 081-083 084-086 087 088 089-08B 08C-08E 08F	DMA Controller and LPC,PCI,or PCIE
090-091	DMA Controller
093-09F	DMA Controller
092	Reset Generator
0A0-0A1 0A4-0A5 0A8-0A9 0AC-0AD	Interrupt Controller
0B0-0B1 0B4-0B5 0B8-0B9 0BC-0BD	Interrupt Controller
0B2-0B3	Power Management
0C0-0D1 0D2-0DD 0DE-0DF	DMA Controller
0F0	FERR# / Interrupt Controller
170-177	SATA Controller ,PCI,or PCIE
1F0-1F7	SATA Controller ,PCI,or PCIE
200-207	Gameport Low
208-20F	Gameport High
376	SATA Controller ,PCI,or PCIE
3F6	SATA Controller ,PCI,or PCIE
4D0-4D1	Interrupt Controller
CF9	Reset Generator

6.4. Variable I/O Address Range Map

Hex Range	Device
Anywhere in 64 KB I/O Space	ACPI
Anywhere in 64 KB I/O Space	IDE Bus Master
Anywhere in 64 KB I/O Space	Native IDE Command
Anywhere in 64 KB I/O Space	Native IDE Controll
Anywhere in 64 KB I/O Space	SATA Index/Data Pair
Anywhere in 64 KB I/O Space	SMBus

Hex Range	Device
96 Bytes above ACPI Base	TCO
Anywhere in 64 KB I/O Space	GPIO
3 Ranges in 64 KB I/O Space	Parallel
8 Ranges in 64 KB I/O Space	Serial Port 1
8 Ranges in 64 KB I/O Space	Serial Port 2
2 Ranges in 64 KB I/O Space	Floppy Disk Controller
Anywhere in 64 KB I/O Space	LAN
Anywhere in 64 KB I/O Space	LPC Generic 1
Anywhere in 64 KB I/O Space	LPC Generic 2
Anywhere in 64 KB I/O Space	LPC Generic 3
Anywhere in 64 KB I/O Space	LPC Generic 4
Anywhere in 64 KB I/O Space	I/O Trapping Ranges
Anywhere in 64 KB I/O Space	PCI Bridge
Anywhere in 64 KB I/O Space	KT

6.5. APIC Interrupt Mapping

IRQ#	Typical Intterupt Resource	Using SERIRQ
0	Cascade from 8259 #1	No
1		Yes
2	8254 Counter 0,HPET #0(Legacy mode)	No
3		Yes
4		Yes
5		Yes
6		Yes
7		Yes
8	RTC,HPET #1(Legacy mode)	No
9	Option for SCI,TCO	Yes
10	Option for SCI,TCO	Yes
11	HPET #2,Option for SCI,TCO	Yes
12	HPET #3	Yes
13	FERR# logic	No
14	SATA Primary	Yes
15	SATA Secondary	Yes
16	Internal devices are routable.	PIRQA#
17	Internal devices are routable.	PIRQB#
18	Internal devices are routable.	PIRQC#
19	Internal devices are routable.	PIRQD#

IRQ#	Typical Intterupt Resource	Using SERIRQ
20	Option for SCI,TCO,HPET #0,1,2,3.Other internal device are routable.	N/A
21	Option for SCI,TCO,HPET #0,1,2,3.Other internal device are routable.	N/A
22	Option for SCI,TCO,HPET #0,1,2,3.Other internal device are routable.	N/A
23	Option for SCI,TCO,HPET #0,1,2,3.Other internal device are routable.	N/A

6.6. PCI Configuration Space Map

Bus Number	Device Number	Function Number	Description
00h	00h	00h	Intel host Processor Bridge
00h	1Fh	00h	LPC Controller
00h	1Fh	02h	SATA Controller #1
00h	1Fh	03h	SMBus Controller
00h	1Fh	05h	SATA Controller#2
00h	1Dh	00h	USB EHCI Controller #1
00h	1Ch	00h	PCI Express* Port 1
00h	1Ch	01h	PCI Express Port 2
00h	1Ch	02h	PCI Express Port 3
00h	1Ch	03h	PCI Express Port 4
00h	1Ch	04h	PCI Express Port 5
00h	1Ch	05h	PCI Express Port 6
00h	1Ch	06h	PCI Express Port 7
00h	1Ch	07h	PCI Express Port 8
00h	19h	00h	Gigabit Ethernet Controller
00h	16h	00h	Intel(R) Management Engine Interface #1
00h	16h	01h	Intel(R) Management Engine Interface #2
00h	16h	02h	IDE-R
00h	16h	03h	KT
00h	14h	00h	xHCI Controller

6.7. PCI Interrupt Routing Map

INT Line	xHCI Controller	Gigabit Ethernet Controller
Int0		INTE:20
Int1		
Int2		
Int3	INTD:19	

INT Line	PCIE Port1	PCIE Port 2	PCIE Port 3	PCIE Port 4	PCIE Port 5	PCIE Port 6	PCIE Port 7	PCIE Port 8
Int0	INTA:16	INTB:17	INTC:18	INTD:19	INTA:16	INTB:17	INTC:18	INTD:19
Int1	INTB:17	INTC:18	INTD:19	INTA:16	INTB:17	INTC:18	INTD:19	INTA:16
Int2	INTC:18	INTD:19	INTA:16	INTB:17	INTC:18	INTD:19	INTA:16	INTB:17
Int3	INTD:19	INTA:16	INTB:17	INTC:18	INTD:19	INTA:16	INTB:17	INTC:18

INT Line	SATA Controller	SMBus Controller	Thermal Controller
Int0	INTA:16		
Int1			
Int2		INTC:18	INTC:18
Int3			

6.8. SMBus Address Table

Device	Address
BMC	50h
Extend GPIO	40h

This page intentionally left blank.

7. BIOS Setup

7.1. Menu Structure

This section presents the six primary menus of the BIOS Setup Utility. Use the following table as a quick reference for the contents of the BIOS Setup Utility. The subsections in this section describe the submenus and setting options for each menu item. The default setting options are presented in **bold**, and the function of each setting is described in the right hand column of the respective table.

Main	Advanced	Chipset	Security	Boot	Save & Exit
BIOS Information System Information Board Information System Date and Time Access Level	Power Management ► System Management ► Thermal Management ► Watchdog Timer ► CSM Configuration ► Super IO Configuration ► Serial Console Redirection ► USB Configuration ► Network Stack Configuration ► Miscellaneous ► Driver Health ► Trusted Computing ►	Processor Configuration ► Advanced Power Management Configuration ► Memory Configuration ► IIO Configuration ► PCH Configuration ►	Setup Administrator Password ► User Password Secure Boot ►	Boot Configuration ► FIXED BOOT ORDER Priorities ► UEFI USB Key Drive BBS Priorities ►	Save Change and Exit ► Discard Changes and Exit ► Save Changes and Reset ► Discard Changes and Reset ► Save Options Boot Override ►

Notes:

► indicates a submenu
Gray text indicates info only

7.2. Main

The Main Menu provides read-only information about your system and also allows you to set the System Date and Time. Refer to the tables below for details of the settings.

7.2.1. Main > BIOS Information

Feature	Options	Description
BIOS Vender	Info only	American Megatrends
BIOS Version	Info only	ADLINK BIOS version
Build Date	Info only	ADLINK BIOS Build Date
SPS Firmware Version	Info only	Display SPS Firmware Version
BIOS Boot Source	Info only	Display BIOS Boot Source

7.2.2. Main > System Information

Feature	Options	Description
Project Name	Info only	Display Project Name.
CPU Board version	Info only	Display CPU Board Version.
CPU Board String	Info only	Display CPU Board String.
CPU Frequency	Info only	Display CPU Frequency.
Total Memory	Info only	Display Installed Memory Size.

7.2.3. Main > Board Information

Feature	Options	Description
Board Information	Submenu	
Board Information	Info only	
Serial Number	Info only	Display SEMA serial Number.
Manufacturing Date	Info only	Display SEMA manufacturing date.
Last Repair Date	Info only	Display SEMA last repair date.
MAC ID	Info only	Display SEMA MAC ID.
Runtime Statistics	Info only	
Total Runtime	Info only	The returned value specifies the total time in minutes the system is running in S0 state.
Current Runtime	Info only	The returned value specifies the time in seconds the system is running in S0 state. This counter is cleared when the system is removed from the external power supply.
Power Cycles	Info only	The returned value specifies the number of times the external power supply has been shut down
Boot Cycles	Info only	The Boot counter is increased after a HW- or SW-Reset or after a successful power-up.

Feature	Options	Description
Boot Reason	Info only	The boot reason is the event which causes the reboot of the system.

7.2.4. Main >System Date/Time

Feature	Options	Description
System Date	Info only	
System Time	Info only	

7.2.5. Main >Access Level

Feature	Options	Description
Access Level	Info only	

7.3. Advanced

This menu contains the settings for most of the user interfaces in the system.

7.3.1. Advanced > Power Management

Feature	Options	Description
Power Management	Info only	
Enable ACPI Auto Configuration	Disabled **Enabled**	Enable or Disables BIOS ACPI Auto Configuration.
Enable Hibernation	Disabled **Enabled**	Enables or Disables System ability to Hibernate (OS/S4 Sleep State). This option may be not effective with some OS.
Emulation AT/ATX	Emulation AT **ATX**	Select Emulation AT or ATX function. If this option is set to [Emulation AT], BIOS will report no suspend functions to ACPI OS. In windows XP, it will make OS show shutdown
LID Function	**Disabled** Enabled	Enable/Disable LID Function
Lock Legacy Resource	**Disabled** Enabled	Enables or Disables Lock of Legacy Resources
I21x Lan Power Ctrl	**PC2** PC1 C0	
ECO Mode	**Disabled** Enabled	
Power-up Mode	**Turn On** Remain Off Last State	
Power Consumption	Submenu	Power Consumption information.

7.3.2. Advanced > Power Management->Power Consumption

Feature	Options	Description
Power Consumption	Info Only	
Current Input Current	Info Only	Display Current Input Current
Current Input Power	Info Only	Display Current Input Power
VCORE	Info Only	Display VCORE Voltage
VMEM	Info Only	Display VMEM Voltage
5VSB	Info Only	Display 5VSB Voltage
VIN	Info Only	Display VIN Voltage
3.3VSB	Info Only	Display 3.3VSB Voltage
5V	Info Only	Display 5V Voltage

7.3.3. Advanced > System Management

Feature	Options	Description
System Management	Info Only	
Version	Info Only	Display SEMA Module Version.
SEMA Firmware	Info Only	Display SEMA Firmware Version.
Build Date	Info Only	Display SEMA Firmware Build Date.
SEMA Bootloader	Info Only	Display SEMA Bootloader Version.
Build Date	Info Only	Display SEMA Bootloader Build Date.
SEMA Features	Submenu	Display SEMA Supported Features
SEMA Supported Features	Info only	Display SEMA Supported Features
Flags	Submenu	Flag
Flags	Info only	
BMC Flags	Info Only	
BIOS Select	Info Only	
ATX/AT-Mode	Info Only	
Exception Code	Info Only	

7.3.4. Advanced > Thermal Management

Feature	Options	Description
Thermal Configuration Parameters	Info Only	
Thermal and Fan Speed	Submenu	
Smart Fan	Submenu	
Critical Trip Point	**Disabled** 65 C 75 C 85 C	The value is the temperature threshold of the Critical Trip Point.
Passive Cooling Trip Point	**Disabled** 80 C 90 C	The value is the temperature threshold of the Passive Cooling Trip Point.
Watchdog ACPI Event Shutdown	**Disabled** Enabled	Watchdog ACPI Event Shutdown Enabled/Disabled

7.3.4.1. Advanced > Thermal Management > Thermal and Fan Speed

Feature	Options	Description
Temperatures and Fan Speed	Info Only	
CPU Temperature	Info Only	
Current	Info Only	Display Current CPU Temperature
Startup	Info Only	Display Startup CPU Temperature
Min	Info Only	Display Min CPU Temperature
Max	Info Only	Display Max CPU Temperature

Feature	Options	Description
Board Temperature	Info Only	
Current	Info Only	Display Current Board Temperature
Startup	Info Only	Display Startup Board Temperature
Min	Info Only	Display Min Board Temperature
Max	Info Only	Display Max Board Temperature
CPU Fan Speed	Info Only	Display CPU Fan Speed

7.3.4.2. Advanced > Thermal Management > Smart Fan

Feature	Options	Description
Smart Fan	Info Only	
CPU Smart Fan Temperature Source	**CPU Sensor** Board Sensor	CPU Smart Fan Temperature Source
CPU Fan Mode	**AUTO (Smart Fan)** Fan Off Fan On	CPU Fan Mode
Trigger Point 1 to 4	Info Only	Display Trigger Point 1 to 4 information
Trigger Temperature	0-100	Select Trigger Temperature
PWM Level	0-100	Select Trigger Temperature

7.3.5. Advanced > Watchdog Timer

Feature	Options	Description
Watchdog Timer	Info only	
Power-Up Watchdog	**Disabled** Enabled	The Power Up Watchdog resets the system after a certain amount of time after power up.

7.3.6. Advanced > CSM Configuration

Feature	Options	Description
Compatibility Support Module Configuration	Info only	
CSM Support	Disableed **Enabled**	Enabled / Disabled CSM Support.
CSM16 Module Version	Info only	Display CSM16 Module Version
GateA20 Active	**Upon Request** Always	UPON REQUEST – GA20 can be disabled using BIOS services. ALWAYS – do not allow disabling GA20; this option is useful when any RT code is executed above 1MB.
Option ROM Messages	**Force BIOS** Keep Current	Set display mode for Option ROM
INT19 Trap Response	Immediate **Postponed**	BIOS reaction on INT19 trapping by Option ROM:IMMEDIATE – execute the trap right away; POSTPONED – execute the trap during legacy boot.

Feature	Options	Description
Boot option filter	**UEFI and Legacy** Legacy only UEFI only	This option controls Legacy/UEFI ROMs priority
Option ROM execution	Info only	
Network	**Do not launch** UEFI Legacy	Controls the execution of UEFI and Legacy PXE OpROM
Storage	Do not launch UEFI **Legacy**	Controls the execution of UEFI and Legacy Storage OpROM
Video	Do not launch UEFI **Legacy**	Controls the execution of UEFI and Legacy Video OpROM
Other PCI devices	Do not launch **UEFI** Legacy	Determines OpROM execution policy for devices other than Network, Storage, or Video

7.3.7. Advanced > Super IO Configuration

Feature	Options	Description
Super IO Configuration	Info only	
Super IO Chip NCT5104D	Info only	
Serial Port 1 Configuration	Submenu	Set Parameters of Serial Port 1 (COMA).
Serial Port 2 Configuration	Submenu	Set Parameters of Serial Port 2 (COMB).
Super IO Chip W83627DHG	Info Only	
Serial Port 1 Configuration	Submenu	Set Parameters of Serial Port 1 (COMA).
Serial Port 2 Configuration	Submenu	Set Parameters of Serial Port 2 (COMB).

7.3.7.1. Advanced > Super IO Configuration > Serial Port 1 Configuration (NCT5104D)

Feature	Options	Description
Serial Port 1 Configuration	Submenu	Set Parameters of Serial Port 1 (COMA).
Serial Port 1 Configuration	Info only	
Serial Port	Disableed **Enabled**	Enable or Disable Serial Port (COM).
Device Settings	Info Only	Display IO / IRQ information of COM Port.
Change Settings	**Auto** IO=240h; IRQ=10; IO=240h; IRQ=3,4,5,6,7,10,11,12 IO=248h; IRQ=3,4,5,6,7,10,11,12 IO=250h; IRQ=3,4,5,6,7,10,11,12 IO=258h; IRQ=3,4,5,6,7,10,11,12	Select an optimal setting for Super IO Device.

7.3.7.2. Advanced > Super IO Configuration > Serial Port 2 Configuration (NCT5104D)

Feature	Options	Description
Serial Port 2 Configuration	Submenu	Set Parameters of Serial Port 2 (COMB).
Serial Port 2 Configuration	Info only	
Serial Port	Disableed **Enabled**	Enable or Disable Serial Port (COM).
Device Settings	Info Only	Display IO / IRQ information of COM Port.
Change Settings	**Auto** IO=248h; IRQ=11; IO=240h; IRQ=3,4,5,6,7,10,11,12 IO=248h; IRQ=3,4,5,6,7,10,11,12 IO=250h; IRQ=3,4,5,6,7,10,11,12 IO=258h; IRQ=3,4,5,6,7,10,11,12	Select an optimal setting for Super IO Device.

7.3.7.3. Advanced > Super IO Configuration > Serial Port 1 Configuration (W83627DHG)

Feature	Options	Description
Serial Port 1 Configuration	Submenu	Set Parameters of Serial Port 1 (COMA).
Serial Port 1 Configuration	Info only	
Serial Port	Disableed **Enabled**	Enable or Disable Serial Port (COM).
Device Settings	Info Only	Display IO / IRQ information of COM Port.
Change Settings	**Auto** IO=3F8h; IRQ=4; IO=3F8h; IRQ=3,4,5,6,7,10,11,12 IO=2F8h; IRQ=3,4,5,6,7,10,11,12 IO=3E8h; IRQ=3,4,5,6,7,10,11,12 IO=2E8h; IRQ=3,4,5,6,7,10,11,12	Select an optimal setting for Super IO Device.

7.3.7.4. Advanced > Super IO Configuration > Serial Port 2 Configuration (W83627DHG)

Feature	Options	Description
Serial Port 2 Configuration	Submenu	Set Parameters of Serial Port 2 (COMB).
Serial Port 2 Configuration	Info only	
Serial Port	Disableed **Enabled**	Enable or Disable Serial Port (COM).
Device Settings	Info Only	Display IO / IRQ information of COM Port.
Change Settings	**Auto** IO=2F8h; IRQ=3; IO=3F8h; IRQ=3,4,5,6,7,10,11,12 IO=2F8h; IRQ=3,4,5,6,7,10,11,12 IO=3E8h; IRQ=3,4,5,6,7,10,11,12 IO=2E8h; IRQ=3,4,5,6,7,10,11,12	Select an optimal setting for Super IO Device.

7.3.8. Advanced > Serial Console Redirection

Feature	Options	Description
COM1	Info only	
Console Redirection	**Enabled** Disabled	Console Redirection Enable or Disable.
Console Redirection Settings	Submenu	The settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings. The item will be lunched before enable Console Redirection.
COM2	Info only	
Console Redirection	**Enabled** Disabled	Console Redirection Enable or Disable.
Console Redirection Settings	Submenu	The settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings. The item will be lunched before enable Console Redirection.
COM3	Info only	
Console Redirection	Enabled **Disabled**	Console Redirection Enable or Disable.
Console Redirection Settings	Submenu	The settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings. The item will be lunched before enable Console Redirection.
COM4	Info only	
Console Redirection	Enabled **Disabled**	Console Redirection Enable or Disable.
Console Redirection Settings	Submenu	The settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings. The item will be lunched before enable Console Redirection.
Serial Port for Out-of-Band Management Windows Emergency Management Services (EMS)	Info only	
Console Redirection	Disabled **Enabled**	Console Redirection Enable or Disable.
Console Redirection Settings	Submenu	The settings specify how the host computer and the remote computer(which the user is using) will exchange data. Both computers should have the same or compatible settings.

7.3.8.1. Advanced > Serial Console Redirection > Console Redirection Settings (If COM1 Enable)

Feature	Options	Description
COM1	Info only	
Console Redirection Settings	Info only	
Teriminal Type	VT100 VT100+ VT-UTF8 **ANSI**	Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100+: Extends VT100 to support color, function keys, etc. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.
Bits per second	9600 19200 38400 57600 **115200**	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Data Bits	7 **8**	Data Bits
Parity	**None** Even Odd Mark Space	A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the num of 1's in the data bits is even. Odd: parity bit is 0 if num of 1's in the data bits is odd. Mark: parity bit is always 1. Space: Parity bit is always 0. Mark and Space Parity do not allow for error detection.They can be used as an additional data bit.
Stop Bits	**1** 2	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.
Flow Control	**None** Hardware RTS/CTS	Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.
VT-UTF8 Combo Key Support	**Enabled** Disabled	Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals
Recorder Mode	**Disabled** Enabled	With this mode enabled only text will be sent. This is to capture terminal data.
Resolution 100x31	Enabled **Disabled**	On Legacy OS, the Number of Rows and Columns supported redirection
Legacy OS Redirection Resolution	**80x24** 80x25	On Legacy OS, the Number of Rows and Columns supported redirection
Putty KeyPad	**VT100** Intel Linux XTERMR6 SCO ESCN VT400	Select FunctionKey and KeyPad on Putty.

Feature	Options	Description
Redirection After BIOS POST	**Always Enable** BootLoader	When Bootloader is selected, then Legacy Console Redirection is disabled before booting to legacy OS. When Always Enable is selected, then Legacy Console Redirection is enabled for legacy OS. Default setting for this option is set to Always Enable.

7.3.8.2. Advanced > Serial Console Redirection > Console Redirection Settings (If COM2 Enable)

Feature	Options	Description
COM2	Info only	
Console Redirection Settings	Info only	
Teriminal Type	VT100 VT100+ VT-UTF8 **ANSI**	Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100+: Extends VT100 to support color, function keys, etc. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.
Bits per second	9600 19200 38400 57600 **115200**	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Data Bits	7 **8**	Data Bits
Parity	**None** Even Odd Mark Space	A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the num of 1's in the data bits is even. Odd: parity bit is 0 if num of 1's in the data bits is odd. Mark: parity bit is always 1. Space: Parity bit is always 0. Mark and Space Parity do not allow for error detection.They can be used as an additional data bit.
Stop Bits	**1** 2	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.
Flow Control	**None** Hardware RTS/CTS	Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.
VT-UTF8 Combo Key Support	**Enabled** Disabled	Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals
Recorder Mode	**Disabled** Enabled	With this mode enabled only text will be sent. This is to capture Terminal data.
Resolution 100x31	Enabled **Disabled**	On Legacy OS, the Number of Rows and Columns supported redirection
Legacy OS Redirection Resolution	**80x24** 80x25	On Legacy OS, the Number of Rows and Columns supported redirection

Feature	Options	Description
Putty KeyPad	**VT100** Intel Linux XTERMR6 SCO ESCN VT400	Select FunctionKey and KeyPad on Putty.
Redirection After BIOS POST	**Always Enable** BootLoader	When Bootloader is selected, then Legacy Console Redirection is disabled before booting to legacy OS. When Always Enable is selected, then Legacy Console Redirection is enabled for legacy OS. Default setting for this option is set to Always Enable.

7.3.8.3. Advanced > Serial Console Redirection > Console Redirection Settings (If COM3 Enable)

Feature	Options	Description
COM3	Info only	
Console Redirection Settings	Info only	
Teriminal Type	VT100 VT100+ VT-UTF8 **ANSI**	Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100+: Extends VT100 to support color, function keys, etc. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.
Bits per second	9600 19200 38400 57600 **115200**	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Data Bits	7 **8**	Data Bits
Parity	**None** Even Odd Mark Space	A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the num of 1's in the data bits is even. Odd: parity bit is 0 if num of 1's in the data bits is odd. Mark: parity bit is always 1. Space: Parity bit is always 0. Mark and Space Parity do not allow for error detection. They can be used as an additional data bit.
Stop Bits	**1** 2	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.
Flow Control	**None** Hardware RTS/CTS	Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.
VT-UTF8 Combo Key Support	**Enabled** Disabled	Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals
Recorder Mode	**Disabled** Enabled	With this mode enabled only text will be sent. This is to capture Terminal data.

Feature	Options	Description
Resolution 100x31	Enabled **Disabled**	On Legacy OS, the Number of Rows and Columns supported redirection
Legacy OS Redirection Resolution	**80x24** 80x25	On Legacy OS, the Number of Rows and Columns supported redirection
Putty KeyPad	**VT100** Intel Linux XTERMR6 SCO ESCN VT400	Select FunctionKey and KeyPad on Putty.
Redirection After BIOS POST	**Always Enable** BootLoader	When Bootloader is selected, then Legacy Console Redirection is disabled before booting to legacy OS. When Always Enable is selected, then Legacy Console Redirection is enabled for legacy OS. Default setting for this option is set to Always Enable.

7.3.8.4. Advanced > Serial Console Redirection > Console Redirection Settings (If COM4 Enable)

Feature	Options	Description
COM4	Info only	
Console Redirection Settings	Info only	
Teriminal Type	VT100 VT100+ VT-UTF8 **ANSI**	Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100+: Extends VT100 to support color, function keys, etc. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.
Bits per second	9600 19200 38400 57600 **115200**	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Data Bits	7 **8**	Data Bits
Parity	**None** Even Odd Mark Space	A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the num of 1's in the data bits is even. Odd: parity bit is 0 if num of 1's in the data bits is odd. Mark: parity bit is always 1. Space: Parity bit is always 0. Mark and Space Parity do not allow for error detection.They can be used as an additional data bit.
Stop Bits	**1** 2	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.
Flow Control	**None** Hardware RTS/CTS	Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.

Feature	Options	Description
VT-UTF8 Combo Key Support	**Enabled** Disabled	Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals
Recorder Mode	**Disabled** Enabled	With this mode enabled only text will be sent. This is to capture Terminal data.
Resolution 100x31	Enabled **Disabled**	On Legacy OS, the Number of Rows and Columns supported redirection
Legacy OS Redirection Resolution	**80x24** 80x25	On Legacy OS, the Number of Rows and Columns supported redirection
Putty KeyPad	**VT100** Intel Linux XTERMR6 SCO ESCN VT400	Select FunctionKey and KeyPad on Putty.
Redirection After BIOS POST	**Always Enable** BootLoader	When Bootloader is selected, then Legacy Console Redirection is disabled before booting to legacy OS. When Always Enable is selected, then Legacy Console Redirection is enabled for legacy OS. Default setting for this option is set to Always Enable.

7.3.8.5. Advanced > Serial Console Redirection > Legacy Console Redirection Settings

Feature	Options	Description
Legacy Serial Redirection Port	**COM1** COM2 COM3 COM4	Select a COM port to display redirection of Legacy OS and Legacy OPROM Messages

7.3.9. Advanced > USB Configuration

Feature	Options	Description
USB Configuration	Info Only	
USB Module Version	Info Only	Display USB Module Version
USB Controllers:	Info Only	Display USB Controllers is XHCI or EHCI.
USB Devices:	Info Only	Display attatcment USB deviecs.
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 availiable only for EFI applications.
XHCI Hand-off	**Enabled** Disabled	This is a workaround for Oses without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.
EHCI Hand-off	**Disabled** Enabled	This is a workaround for Oses without EHCI hand-off support. The EHCI ownership change should be claimed by EHCI driver.
USB Mass Storage Driver Support	Disableed **Enabled**	Enable / Disable USB Mass Storge Driver Support.

Feature	Options	Description
USB hardware delays and time-outs:	Info Only	
USB transfer rime-out	1 sec 5sec 10sec **20 sec**	The time-out value for Control, Bulk, and Interrupt transfers.
Device reset time-out	10 sec **20 sec** 30 sec 40 sec	USB mass storage device Start Unit command time-out.
Device power-up delay	**Auto** Manual	Maximum time the device will take before it properly reports itself to the Hot Controller. 'Auto' uses default value: for a Root po\rt it is 100 ms, for a Hub port the delay is taken form Hub descriptor.

7.3.10. Advanced > Network Stack Configuration

Feature	Options	Description
Network Stack	**Disable** Enable	Enable / Disable UEFI Network Stack.

7.3.11. Advanced > Miscellaneous

Feature	Options	Description
Miscellanous	Info Only	Control the PCI Express Root Port.
Smart Battery Function	**Disable** Enable	Enable / Disable Battery Function
I2C write protect control	Active **Write protect**	I2C write protect control
Above 4G Decoding	**Disabled** Enabled	Enabls or Disables 64bit capable Devices to be Decode in Above 4G Address Space (Only if System supports 64 bit PCI Decoding).

7.3.12. Advanced > Driver Health

Feature	Options	Description
Driver Name	Info only	Provides Health Status for the Drivers / Controllers.

7.3.13. Advanced > Trusted Computing

Feature	Options	Description
TPM20 Device Found	Info Only	
Security Device Support	Disable **Enable**	Enables or Disable BIOS support for security device. OS will not show Security Device. TCG EFI protocol and available.
Active PCR banks	Info Only	

Feature	Options	Description
Available PCR banks	Info Only	
SHA-1 PCR Bank	Disabled **Enabled**	Enable or Disable SHA-1 PCR Bank
SHA256 PCR Bank	**Disabled** Enabled	Enable or Disable SHA256 PCR Bank
Pending operation	**None** TPM Clear	Schedule an Operation for the Security Device. NOTE: Your Computer will reboot during restart in order to change State of Security Device.
Platform hierarchy	Disable **Enable**	Enable or Disable Platform Hierarchy
Storage Hierarchy	Disable **Enable**	Enable or Disable Storage Hierarchy
Endorsement Hierarchy	Disable **Enable**	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 Win8/Win10, TCG_2: Support new TCG2 protocol and event format for Win10 or later
Physical Presence Spec Version	**1.2** 1.3	Select to Tell O.S. to support PPI Spec Version 1.2 or 1.3. Note some HCK tests might not support 1.3.
TPM 20 Interface Type	Info only	
Device Select	TPM 1.2 TPM 2.0 **Auto**	PM 1.2 will restrict support to TPM 1.2 devices, TPM 2.0 will restrict support to TPM 2.0 devices, Auto will support both with the default set to TPM 2.0 devices if not found, TPM 1.2 devices will be enumerated.

7.4. Chipset

7.4.1. Chipset > Processor Configuration

Feature	Options	Description
Processor Configuration	Info only	
Processor Socket	Info only	Display Processor Socket information
Processor ID	Info only	Display Processor Socket information
Processor Frequency	Info only	Display Processor Frequency information
Processor Max Ratio	Info only	Display Processor Max Ratio information
Processor Min Ratio	Info only	Display Processor Min Ratio information
Microcode Revision	Info only	Display Microcode Revision information
L1 Cache RAM	Info only	Display L1 Cache RAM information
L2 Cache RAM	Info only	Display L2 Cache RAM information
L3 Cache RAM	Info only	Display L3 Cache RAM information
Processor 0 Version	Info only	Display Processor 0 Version information
Hyper-Threading [ALL]	Disable **Enable**	Enable Hyper Threading (Software Method to Enable/Disable Logical Processor threads.)
Execute Disable Bit	Disable **Enable**	When disabled, forces the XD feature flag to always return 0.
Enable Intel TXT Support	**Disable** Enable	Enables Intel Trusted Execution Technology Configuration. Please disable “EV DFX Features“ when TXT is enabled.
VMX	Disable **Enable**	Enables the Vanderpool Technology, takes effect after reboot.
Enable SMX	**Disable** Enable	Enable Safer Mode Extensions
Hardware Prefetcher	**Enable** Disable	= MLC Spatial Prefetcher (MSR 1A4h Bit[0])
Adjacent Cache Prefect	**Enable** Disable	= MLC Spatial Prefetcher (MSR 1A4h Bit[1])
X2APIC	**Disable** Enable	Enable/disable extended APIC support

7.4.2. Chipset > Advanced Power Management Configuration

Feature	Options	Description
Advanced Power Management Configuration	Info only	
EIST (P-states)	Disable **Enable**	When enabled, OS sets CPU frequency according load. When disabled, CPU frequency is set at max non-turbo.
Config TDP	**Disable** Enable	Option to disable/enable Config TDP

Feature	Options	Description
CPU P State Control	Submenu	Controls CPU frequency.
CPU C State Control	Submenu	Control CPU idle states
Long Pwr Limit Ovrd	**Disable**	Enable/Disable Long Term Power Limit override. If this option is disabled, BIOS will program the default values for Long Term Power Limit and Long Term Power Limit Time Window.
Long Dur Pwr Limit	**0**	Turbo Mode Long Duration Power Limit (aka Power Limit 1) in Watts. The value may vary from 0 to Fused Value. If the value is 0, the fused value will be programed. A value greater than fused TDP value will not be programed.
Long Dur Time Window	**1**	Long Duration Time Window (aka Power Limit 1 Time) value in seconds. The value may vary from 0 to 56. Indicates the time window over which TDP value should be maintained. If the value is 0, the fused value will be programed.

7.4.2.1. Chipset > Advanced Power Management Configuration > CPU P State Control

Feature	Options	Description
CPU P State Control	Info only	
P State Domain	**ALL** ONE	Per Logical: indicates the P-state domain for each logical proc in the system. Per Package: all procs indicate the same domain in the same package.
P-state coordination	**HW_ALL** SW_ALL SW_ANY	HW_ALL (hardware) coordination is recommended over SW_ALL and SW_ANY (software coordination).
Energy efficient P-state	Disable **Enable**	Enable/Disable Energy efficient P-state feature. When set to 0,will disable access to ENERGY_PERFORMANCE_BIAS MSR and CPUID Function6 EAX[3] will read 0 indicating nosupport
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 not exceed CPU defined limits.

7.4.2.2. Chipset > Advanced Power Management Configuration > CPU C State Control

Feature	Options	Description
CPU C State Control	Info only	
C2C3TT	Info only	Display PCIE Port assigned to LAN Information.
CPU C State	Disable **Enable**	Enable 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

Feature	Options	Description
CPU C3 report	**Disable** Enable	Enable/Disable CPU C3(ACPI C2) report to OS. Recommended to be disabled.
CPU C6 report	Disable **Enable**	Enable/Disable CPU C6(ACPI C2) report to OS Recommended to be enabled.
Enhanced Halt State (C1E)	Disable **Enable**	Enables the Enhanced C1E state of the CPU, takes effect after reboot.
OS ACPI Cx	**ACPI C2** ACPI C3	Report CC3/CC6 to OS ACPI C2 or ACPI C3

7.4.3. Chipset > Memory Configuration

Feature	Options	Description
Integrated Memory Controller (iMC)	Info only	
Memory Frequency	**Auto** 1333 1400 1600 1800 1867 2000 2133 2200 2400 2600 2667 2800 2933 3000 3200 Reserved	Maximum Memory Frequency Selections in Mhz. Do not select Reserved
Memory Topology	Submenu	Display memory information

7.4.4. Chipset > IIO Configuration

Feature	Options	Description
IIO Configuration	Info only	
PCIe Hot Plug	**Disable** Enable Auto MANUAL	Enable/Disable PCIe Hot Plug globally
PCIe ACPI Hot Plug	**Disable** Enable Per-port	Enable/Disable ACPI Hot Plug globally, or allow per-port control. When Disabled,MSI is generated on HP event. When Enabled, _HPGPE message is generated.
IIO0 Configuration	Submenu	
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.

7.4.4.1. Chipset > IIO Configuration > IIO0 Configuration

Feature	Options	Description
IOU2 (IIO PCIe Port 1)	x4x4 x8 **Auto**	Select PCIe port Bifurcation for selected slot(s)
IOU1 (IIO PCIe Port 3)	x4x4x4x4 x4x4x8 x8x4x4 x8x8 x16 **Auto**	Select PCIe port Bifurcation for selected slot(s)
Socket 0 PcieD02F0 – Port 2A	Submenu	Settings related to PCI Express Ports (0/1A/1B/2A/2B/2C/2D/3A/3B/3C/3D)
Socket 0 PcieD02F2 – Port 2C	Submenu	Settings related to PCI Express Ports (0/1A/1B/2A/2B/2C/2D/3A/3B/3C/3D)
Socket 0 PcieD03F0 – Port 3A	Submenu	Settings related to PCI Express Ports (0/1A/1B/2A/2B/2C/2D/3A/3B/3C/3D)

Chipset > IIO Configuration > IIO0 Configuration > Socket 0 PcieD02F0 – Port 2A

Feature	Options	Description
Socket 0 PcieD02F0 – Port 2A	Info only	
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** Gen1 (2.5 GT/s) Gen2 (5 GT/s) Gen3 (8 GT/s)	
Override Max Link Wid	**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	Info only	
PCI-E Port Link Max	Info only	
PCI-E Port Link Speed	Info only	
PCI-E ASPM Support	Auto **Disable** L1 Only	This option enables / disables the ASPM (L1) support for the downstream devices.

Feature	Options	Description
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 in 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 0.71 Sept	PCIe Gen3 Spec Mode
Gen3 Phase2 Mode	**Hardware Adaptive** Manual	
Gen3 DN Tx Present	**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 Present
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 Present 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)	PCIe Gen3 Upstream Tx Preset

Feature	Options	Description
	P7 (-6.0/3.5 dB) P8 (-3.5/3.5 dB) P9 (0.0/3.5 dB)	
Hide Port?	**no** yes	User can force to hide this root port from OS
Pcie Ecrc	Disable Enable **Auto**	Enable/Disable Pcie Ecrc Support for this port.

Chipset > IIO Configuration > IIO0 Configuration > Socket 0 PcieD02F2 – Port 2C

Feature	Options	Description
Socket 0 PcieD02F2 – Port 2C	Info only	
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** Gen1 (2.5 GT/s) Gen2 (5 GT/s) Gen3 (8 GT/s)	
Override Max Link Wid	**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	Info only	
PCI-E Port Link Max	Info only	
PCI-E Port Link Speed	Info only	
PCI-E ASPM Support	Auto **Disable** L1 Only	This option enables / disables the ASPM (L1) support for the downstream devices.
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 in L0s state

Feature	Options	Description
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 Equilization Mode
Gen3 Spec Mode	**Auto** 0.70 July 0.70 Sept 0.71 Sept	PCIe Gen3 Spec Mode
Gen3 Phase2 Mode	**Hardware Adaptive** Manual	
Gen3 DN Tx Present	**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 Present
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 Present 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 force to hide this root port from OS
Pcie Ecrc	Disable Enable **Auto**	Enable/Disable Pcie Ecrc Support for this port.

Chipset > IIO Configuration > IIO0 Configuration > Socket 0 PcieD03F0 – Port 3A

Feature	Options	Description
Socket 0 PcieD03F0 – Port 3A	Info only	
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** Gen1 (2.5 GT/s) Gen2 (5 GT/s) Gen3 (8 GT/s)	
Override Max Link Wid	**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	Info only	
PCI-E Port Link Max	Info only	
PCI-E Port Link Speed	Info only	
PCI-E ASPM Support	Auto **Disable** L1 Only	This option enables / disables the ASPM (L1) support for the downstream devices.
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 in 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 Equilization Mode

Feature	Options	Description
Gen3 Spec Mode	**Auto** 0.70 July 0.70 Sept 0.71 Sept	PCIe Gen3 Spec Mode
Gen3 Phase2 Mode	**Hardware Adaptive** Manual	
Gen3 DN Tx Present	**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 Present
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 Present 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 force to hide this root port from OS
Pcie Ecrc	Disable Enable **Auto**	Enable/Disable Pcie Ecrc Support for this port.

7.4.4.2. Chipset > IIO Configuration > Intel VT for Directed I/O (VT-d)

Feature	Options	Description
Intel VT for Directeded I/O (VT-d)	Info	
VTd Azalea VCp Optimizations	**Disable** Enable	Enable/Disable Azalea VCp Optimizations
Intel VT for Directed	**Enable** Disable	Enable/Disable Intel Virtualization Technology for Directed I/O (VT-d) by reporting the I/O device assignment to VMM through DMAR ACPI Tables.

Feature	Options	Description
ACS Control	**Enable** Disable	Enable: Programs ACS only to Chipset Pcie Root Ports Bridges; Disable: Programs ACS to all Pcie bridges
Interrupt Remapping	**Enable** Disable	Enable/Disable VT_D Interrupt Remapping Support
Coherency Support (Non-Isoch)	**Enable** Disable	Enable/Disable Non-Isoch VT_D Engine Coherency support
Coherency Support (Isoch)	**Enable** Disable	Enable/Disable Isoch VT_D Engine Coherency support

7.4.5. Chipset > PCH Configuration

Feature	Options	Description
PCH Configuration	Info only	
PCH Devices	Submenu	Enable/Disable Intel(R) IO Controller Hub devices
PCI Express Configuration	Submenu	PCI Express Configuration settings
PCH SATA Configuration	Submenu	SATA devices and settings
USB Configuration	Submenu	USB Configuration Settings
Networking	Submenu	Network devices and setings

7.4.5.1. Chipset > PCH Configuration > PCH Device

Feature	Options	Description
SMBUS Device	Disabled **Enabled**	Enable/Disable SMBUS Device.
Serial irq Mode	Quiet **Continuous**	Configure Serial IRQ Mode.
High Precision Timer	Disabled **Enabled**	Enable or Disable the High Precision Event Timer.
PCH state after G3	S0 **S5** Last State	Select S0/S5 for ACPI state after a G3
PCH CRID	**Disabled** Enabled	Enable/Disable PCH's CRID

7.4.5.2. Chipset > PCH Configuration > PCI Express Configuration

Feature	Options	Description
PCIE Ports 1-4 Config	**4x1 Port** 1x2 2x1 Port 2x2 Port 1x4 Port	To Configure PCI-E Port 1-4 of PCH.
PCIE Ports 5-8 Config	**4x1 Port** 1x2 2x1 Port 2x2 Port 1x4 Port	To Configure PCI-E Port 1-4 of PCH.

Feature	Options	Description
PCIE Clock Gating	Disabled **Enabled**	PCIE Clock Gating Enable/Disable 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
LAN PCIE Port used	**None**	
Subtractive Decode	**Disabled**	
PCIe-USB Glitch W/A	**Disabled** Enabled	PCIe-USB Glitch W/A for bad USB device(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 2	Submenu	
PCI Express Root Port 3	Submenu	
PCI Express Root Port 4	Submenu	
PCI Express Root Port 5	Submenu	
PCI Express Root Port 6	Submenu	
PCI Express Root Port 7	Submenu	
PCI Express Root Port 8	Submenu	

Chipset > PCH Configuration > PCI Express Configuration > PCI Express Root Port1-8

Feature	Options	Description
PCI Express Root Port	Disabled **Enabled**	Control the PCI Express Root Port.
L1 Substates	Disabled L1.1 L1.2 **L1.1 & L1.2**	PCI Express L1 Substates settings.
URR	**Disabled** Enabled	PCI Express Unsupported Request Reporting Enable/Disable.
FER	**Disabled** Enabled	PCI Express Device Fatal Error Reporting Enable/Disable.
NFER	**Disabled** Enabled	PCI Express Device Non-Fatal Error Reporting Enable/Disable.
CER	**Disabled** Enabled	PCI Express Device Correctable Error Reporting Enable/Disable.
CTO	**Disabled** Enabled	PCI Express Completion Timer TO Enable/Disable
SEFE	**Disabled** Enabled	Root PCI Express System Error on Fatal Error Enable/Disable.

Feature	Options	Description
SENFE	**Disabled** Enabled	Root PCI Express System Error on Non-Fatal Error Enable/Disable.
SECE	**Disabled** Enabled	Root PCI Express System Error on Correctable Error Enable/Disable.
PME SCI	**Disabled** Enabled	PCI Express PME SCI Enable/Disable.
Hot Plug	**Disabled** Enabled	PCI Express Hot Plug Enable/Disable.
PCIe Speed	**Auto** Gen1 Gen2	Configure PCIe Speed
PME Interrupt	**Disabled** Enabled	PCI Express PME Interrupt Enable/Disable.
Extra Bus Reserved	**0**	Extra Bus Reserved (0-7) for bridges behind this Root Bridge.
Reserved Memory	**10**	Reserved Memory and Prefetchable Memory (1-20MB) Range for this Root Bridge.
Reserved I/O	**4**	Reserved I/O (4K/8K/12K/16K/20K) Range for this Root Bridge.

7.4.5.3. Chipset > PCH Configuration > PCH SATA Configuration

Feature	Options	Description
PCH SATA Configuration	Info only	
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/Disable SATA test mode
SATA Mode options	Submenu	
SATA AHCI LPM	Disabled Enabled	Enable/Disable Link Power Management
SATA Controller Speed	Default Gen1 **Gen2** Gen3	Indicates the maximum speed the SATA controller can support.
SATA Port 0-1	Info only	
Software Preserve	Info only	
Port 0-1	Disabled **Enabled**	Enable or Disable SATA Port
Hot Plug	**Disabled** Enabled	Designates this port as Hot Pluggable.
Configure as eSATA	**Disabled** Enabled	Configures port as External SATA (eSATA)
Configured as eSATA	Info only	
Spin Up Device	**Disabled**	If enabled for any of ports Staggered Spin Up will be

Feature	Options	Description
	Enabled	performed and only the drives which have this option enabled will spin up at boot. Otherwise all drives spin up at boot.
SATA Device Type	**Hard Disk Drive** Solid State Drive	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive

7.4.5.4. Chipset > PCH Configuration > USB Configuration

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/Disable BTCG
USB Ports Per-Port Disable Control	**Disabled** Enabled	Control each of the USB ports (0~13) disabling.
XHCI Idle L1	**Enabled** Disabled	Enabled XHCI Idle L1. Disabled to workaround USB3 hot plug will fail after 1 hot plug removal. Please put the system to G3 for the new settings to take effect.

7.4.5.5. Chipset > PCH Configuration > Networking

Feature	Options	Description
PCH Internal LAN	**Enabled** Disabled	Enable/Disable PCH Internal LAN
PXE ROM	Enabled **Disabled**	Enable/Disable PXE Option ROM execution for onboard LAN.
EFI Network	Enabled **Disabled**	Enable/Disable EFI Network support for onboard LAN.

7.5. Security

7.5.1. Security > Password Description

Feature	Options	Description
Password Description	Info only	
Setup Administrator Password	Enter Password	Set Setup Administrator Password
User Password	Enter Password	Set User Password
Secure Boot	Submenu	Customizable Secure Boot settings.
System Mode	Info only	
Secure Boot	Info only	
Vender Keys	Info only	
Attempt Secure Boot	Disabled **Enabled**	Secure Boot activated when Platform Key(PK) is enrolled, System mode is User / Deployed, and CSM function is disabled
Secure Boot Mode	**Standard** Custom	Secure Boot Mode - Custom & Standard, Set UEFI Secure Boot Mode to STANDARD mode or CUSTOM mode, this change is effect after save. And after reset, the mode will return to STANDARD mode

7.6. Boot

Feature	Options	Description
Boot Configuration	Info only	
Setup Prompt Timeout	**1**	Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.
Bootup NumLock State	**On** Off	Select the keyboard Number state.
Ouiet Boot	Disabled **Enabled**	Select the keyboard NumLock state.
Fast Boot	**Disabled** Enabled	Enable or Disable FastBoot features. Most probes are skipped to reduce time cost during boot.
New Boot Option Policy	**Default** Place First Place Last	Controls the placement of newly detected UEFI boot option.

7.6.1. Boot > FIXED BOOT ORDER Priorities

Feature	Options	Description
Boot Option #1	**Hardware**	Set the system boot order.
Boot Option #2	**CD/DVD**	Set the system boot order.
Boot Option #3	**USB Hard Disk**	Set the system boot order.
Boot Option #4	**USB CD/DVD**	Set the system boot order.
Boot Option #5	**USB Key**	Set the system boot order.
Boot Option #6	**USB Floppy**	Set the system boot order.
Boot Option #7	**USB Lan**	Set the system boot order.
Boot Option #8	**Network**	Set the system boot order.

7.7. Save & Exit

Feature	Options	Description
Save Changes and Exit		Exit system setup after saving the changes.
Discard Changes and Exit		Exit system setup without saving any changes.
Save Change and Reset		Reset the system after saving the changes.
Discard Changes and Reset		Reset system setup without saving any changes.
Save Options	Info only	
Save Changes		Save Changes done so far to any of the setup options.
Save as User Defaults		Save the changes done so far as User Defaults.
Restore User Defaults		Restore the User Defaults to all the setup options.
Boot Override	Info only	

8. BIOS Checkpoints, Beep Codes

This section of this document lists checkpoints and beep codes generated by AMI Aptio BIOS. The checkpoints defined in this document are inherent to the AMIBIOS generic core, and do not include any chipset or board specific checkpoint definitions.

Checkpoints and Beep Codes Definition

A checkpoint is either a byte or word value output to I/O port 80h. The BIOS outputs checkpoints throughout bootblock and Power-On Self Test (POST) to indicate the task the system is currently executing. Checkpoints are very useful for debugging problems that occur during the preboot process.

Beep codes are used by the BIOS to indicate a serious or fatal error. They are used when an error occurs before the system video has been initialized, and generated by the system board speaker.

Aptio Boot Flow

While performing the functions of the traditional BIOS, Aptio 5.x core follows the firmware model described by the Intel Platform Innovation Framework for EFI (“the Framework”). The Framework refers the following “boot phases”, which may apply to various status code & checkpoint descriptions:

- Security (SEC) – initial low-level initialization
- Pre-EFI Initialization (PEI) – memory initialization[1]
- Driver Execution Environment (DXE) – main hardware initialization[2]
- Boot Device Selection (BDS) – system setup, pre-OS user interface & selecting a bootable device (CD/DVD, HDD, USB, Network, Shell, …)

Viewing BIOS Checkpoints

Viewing all checkpoints generated by the BIOS requires a checkpoint card, also referred to as a □OST Card or POST Diagnostic Card. These are PCI add-in cards that show the value of I/O port 80h on a LED display.

Some computers display checkpoints in the bottom right corner of the screen during POST. This display method is limited, since it only displays checkpoints that occur after the video card has been activated.

Keep in mind that not all computers using AMI Aptio BIOS enable this feature. In most cases, a checkpoint card is the best tool for viewing AMI Aptio BIOS checkpoints.

[1]Analogous to “bootblock” functionality of legacy BIOS
[2]Analogous to “POST” functionality in legacy BIOS

8.1. Status Code Ranges

Status Code Range	Description
0x01 – 0x0B	SEC execution
0x0C – 0x0F	SEC errors
0x10 – 0x2F	PEI execution up to and including memory detection
0x30 – 0x4F	PEI execution after memory detection
0x50 – 0x5F	PEI errors
0x60 – 0x8F	DXE execution up to BDS
0x90 – 0xCF	BDS execution
0xD0 – 0xDF	DXE errors
0xE0 – 0xE8	S3 Resume (PEI)
0xE9 – 0xEF	S3 Resume errors (PEI)
0xF0 – 0xF8	Recovery (PEI)
0xF9 – 0xFF	Recovery errors (PEI)

8.2. Standard Status Codes

8.2.1. SEC Phase

Status Code	Description
0x00	Not used
Progress Codes	
0x01	Power on. Reset type detection (soft/hard).
0x02	AP initialization before microcode loading
0x03	North Bridge initialization before microcode loading
0x04	South Bridge initialization before microcode loading
0x05	OEM initialization before microcode loading
0x06	Microcode loading
0x07	AP initialization after microcode loading
0x08	North Bridge initialization after microcode loading
0x09	South Bridge initialization after microcode loading
0x0A	OEM initialization after microcode loading
0x0B	Cache initialization

SEC Error Codes	
0x0C – 0x0D	Reserved for future AMI SEC error codes
0x0E	Microcode not found
0x0F	Microcode not loaded

8.2.2. SEC Beep Codes

None

8.2.3. PEI Phase

Status Code	Description
Progress Codes	
0x10	PEI Core is started
0x11	Pre-memory CPU initialization is started
0x12	Pre-memory CPU initialization (CPU module specific)
0x13	Pre-memory CPU initialization (CPU module specific)
0x14	Pre-memory CPU initialization (CPU module specific)
0x15	Pre-memory North Bridge initialization is started
0x16	Pre-Memory North Bridge initialization (North Bridge module specific)
0x17	Pre-Memory North Bridge initialization (North Bridge module specific)
0x18	Pre-Memory North Bridge initialization (North Bridge module specific)
0x19	Pre-memory South Bridge initialization is started
0x1A	Pre-memory South Bridge initialization (South Bridge module specific)
0x1B	Pre-memory South Bridge initialization (South Bridge module specific)
0x1C	Pre-memory South Bridge initialization (South Bridge module specific)
0x1D – 0x2A	OEM pre-memory initialization codes
0x2B	Memory initialization. Serial Presence Detect (SPD) data reading
0x2C	Memory initialization. Memory presence detection
0x2D	Memory initialization. Programming memory timing information
0x2E	Memory initialization. Configuring memory
0x2F	Memory initialization (other).
0x30	Reserved for ASL (see ASL Status Codes section below)
0x31	Memory Installed
0x32	CPU post-memory initialization is started
0x33	CPU post-memory initialization. Cache initialization
0x34	CPU post-memory initialization. Application Processor(s) (AP) initialization

Status Code	Description
0x35	CPU post-memory initialization. Boot Strap Processor (BSP) selection
0x36	CPU post-memory initialization. System Management Mode (SMM) initialization
0x37	Post-Memory North Bridge initialization is started
0x38	Post-Memory North Bridge initialization (North Bridge module specific)
0x39	Post-Memory North Bridge initialization (North Bridge module specific)
0x3A	Post-Memory North Bridge initialization (North Bridge module specific)
0x3B	Post-Memory South Bridge initialization is started
0x3C	Post-Memory South Bridge initialization (South Bridge module specific)
0x3D	Post-Memory South Bridge initialization (South Bridge module specific)
0x3E	Post-Memory South Bridge initialization (South Bridge module specific)
0x3F-0x4E	OEM post memory initialization codes
0x4F	DXE IPL is started
PEI Error Codes	
0x50	Memory initialization error. Invalid memory type or incompatible memory speed
0x51	Memory initialization error. SPD reading has failed
0x52	Memory initialization error. Invalid memory size or memory modules do not match.
0x53	Memory initialization error. No usable memory detected
0x54	Unspecified memory initialization error.
0x55	Memory not installed
0x56	Invalid CPU type or Speed
0x57	CPU mismatch
0x58	CPU self test failed or possible CPU cache error
0x59	CPU micro-code is not found or micro-code update is failed
0x5A	Internal CPU error
0x5B	reset PPI is not available
0x5C-0x5F	Reserved for future AMI error codes
S3 Resume Progress Codes	
0xE0	S3 Resume is stared (S3 Resume PPI is called by the DXE IPL)
0xE1	S3 Boot Script execution
0xE2	Video repost
0xE3	OS S3 wake vector call
0xE4-0xE7	Reserved for future AMI progress codes

Status Code	Description
S3 Resume Error Codes	
0xE8	S3 Resume Failed
0xE9	S3 Resume PPI not Found
0xEA	S3 Resume Boot Script Error
0xEB	S3 OS Wake Error
0xEC-0xEF	Reserved for future AMI error codes
Recovery Progress Codes	
0xF0	Recovery condition triggered by firmware (Auto recovery)
0xF1	Recovery condition triggered by user (Forced recovery)
0xF2	Recovery process started
0xF3	Recovery firmware image is found
0xF4	Recovery firmware image is loaded
0xF5-0xF7	Reserved for future AMI progress codes
Recovery Error Codes	
0xF8	Recovery PPI is not available
0xF9	Recovery capsule is not found
0xFA	Invalid recovery capsule
0xFB – 0xFF	Reserved for future AMI error codes

8.2.4. PEI Beep Codes

# of Beeps	Description
1	Memory not Installed
1	Memory was installed twice (InstallPeiMemory routine in PEI Core called twice)
2	Recovery started
3	DXEIPL was not found
3	DXE Core Firmware Volume was not found
4	Recovery failed
4	S3 Resume failed
7	Reset PPI is not available

8.2.5. DXE Status Codes

Status Code	Description
0x60	DXE Core is started
0x61	NVRAM initialization
0x62	Installation of the South Bridge Runtime Services
0x63	CPU DXE initialization is started
0x64	CPU DXE initialization (CPU module specific)
0x65	CPU DXE initialization (CPU module specific)
0x66	CPU DXE initialization (CPU module specific)
0x67	CPU DXE initialization (CPU module specific)
0x68	PCI host bridge initialization
0x69	North Bridge DXE initialization is started
0x6A	North Bridge DXE SMM initialization is started
0x6B	North Bridge DXE initialization (North Bridge module specific)
0x6C	North Bridge DXE initialization (North Bridge module specific)
0x6D	North Bridge DXE initialization (North Bridge module specific)
0x6E	North Bridge DXE initialization (North Bridge module specific)
0x6F	North Bridge DXE initialization (North Bridge module specific)
0x70	South Bridge DXE initialization is started
0x71	South Bridge DXE SMM initialization is started
0x72	South Bridge devices initialization
0x73	South Bridge DXE Initialization (South Bridge module specific)
0x74	South Bridge DXE Initialization (South Bridge module specific)
0x75	South Bridge DXE Initialization (South Bridge module specific)
0x76	South Bridge DXE Initialization (South Bridge module specific)
0x77	South Bridge DXE Initialization (South Bridge module specific)
0x78	ACPI module initialization
0x79	CSM initialization
0x7A – 0x7F	Reserved for future AMI DXE codes
0x80 – 0x8F	OEM DXE initialization codes
0x90	Boot Device Selection (BDS) phase is started
0x91	Driver connecting is started
0x92	PCI Bus initialization is started
0x93	PCI Bus Hot Plug Controller Initialization
0x94	PCI Bus Enumeration

Status Code	Description
0x95	PCI Bus Request Resources
0x96	PCI Bus Assign Resources
0x97	Console Output devices connect
0x98	Console input devices connect
0x99	Super IO Initialization
0x9A	USB initialization is started
0x9B	USB Reset
0x9C	USB Detect
0x9D	USB Enable
0x9E – 0x9F	Reserved for future AMI codes
0xA0	IDE initialization is started
0xA1	IDE Reset
0xA2	IDE Detect
0xA3	IDE Enable
0xA4	SCSI initialization is started
0xA5	SCSI Reset
0xA6	SCSI Detect
0xA7	SCSI Enable
0xA8	Setup Verifying Password
0xA9	Start of Setup
0xAA	Reserved for ASL (see ASL Status Codes section below)
0xAB	Setup Input Wait
0xAC	Reserved for ASL (see ASL Status Codes section below)
0xAD	Ready To Boot event
0xAE	Legacy Boot event
0xAF	Exit Boot Services event
0xB0	Runtime Set Virtual Address MAP Begin
0xB1	Runtime Set Virtual Address MAP End
0xB2	Legacy Option ROM Initialization
0xB3	System Reset
0xB4	USB hot plug
0xB5	PCI bus hot plug
0xB6	Clean-up of NVRAM
0xB7	Configuration Reset (reset of NVRAM settings)

Status Code	Description
0xB8 – 0xBF	Reserved for future AMI codes
0xC0 – 0xCF	OEM BDS initialization codes
DXE Error Codes	
0xD0	CPU initialization error
0xD1	North Bridge initialization error
0xD2	South Bridge initialization error
0xD3	Some of the Architectural Protocols are not available
0xD4	PCI resource allocation error. Out of Resources
0xD5	No Space for Legacy Option ROM
0xD6	No Console Output Devices are found
0xD7	No Console Input Devices are found
0xD8	Invalid password
0xD9	Error loading Boot Option (LoadImage returned error)
0xDA	Boot Option is failed (StartImage returned error)
0xDB	Flash update is failed
0xDC	Reset protocol is not available

8.2.6. DXE Beep Codes

# of Beeps	Description
1	Invalid password
4	Some of the Architectural Protocols are not available
5	No Console Output Devices are found
5	No Console Input Devices are found
6	Flash update is failed
7	Reset protocol is not available
8	Platform PCI resource requirements cannot be met

8.2.7. ACPI/ASL Checkpoint

Status Code	Description
0x01	System is entering S1 sleep state
0x02	System is entering S2 sleep state
0x03	System is entering S3 sleep state
0x04	System is entering S4 sleep state
0x05	System is entering S5 sleep state

Status Code	Description
0x10	System is waking up from the S1 sleep state
0x20	System is waking up from the S2 sleep state
0x30	System is waking up from the S3 sleep state
0x40	System is waking up from the S4 sleep state
0xAC	System has transitioned into ACPI mode. Interrupt controller is in PIC mode.
0xAA	System has transitioned into ACPI mode. Interrupt controller is in APIC mode.

8.3. OEM-Reserved Checkpoint Ranges

Status Code	Description
0x05	OEM SEC initialization before microcode loading
0x0A	OEM SEC initialization after microcode loading
0x1D – 0x2A	OEM pre-memory initialization codes
0x3F – 0x4E	OEM PEI post memory initialization codes
0x80 – 0x8F	OEM DXE initialization codes
0xC0 – 0xCF	OEM BDS initialization codes

This page intentionally left blank.

9. Mechanical Information

9.1. Board-to-Board Connectors

To allow for different stacking heights, the receptacles for COM Express carrier boards are available in two heights: 5 mm and 8 mm. When 5 mm receptacles are chosen, the carrier board should be free of components.

Tyco 3-1827253-6

Foxconn QT002206-2131-3H

- 220-pin board-to-board connector with 0.5mm for a stacking height of 5 mm.
- This connector can be used with 5 mm through-hole standoffs (SMT type).

Tyco 3-6318491-6

Foxconn QT002206-4141-3H

- 220-pin board-to-board connector with 0.5mm for a stacking height of 8 mm.
- This connector can be used with 8 mm through-hole standoffs (SMT type).

Common Specifications

- Current capacity: 0.5A per pin
- Rated voltage: 50 VAC
- Insulation resistance: 100M or greater @ 500 VDC
- Temperature rating: -40°C ~ 85°C
- UL certification (ECBT2.E28476)
- Copper alloy (contacts)
- Housing: thermo-plastic molded compound (L.C.P.)

9.2. Thermal Solution

9.2.1. Heat Spreaders

The function of the heat spreader is to ensure an identical mechanical profile for all COM Express modules. By using a heat spreader, the thermal solution that is built on top of the module is compatible with all COM Express modules.

9.2.2. Heat Sinks

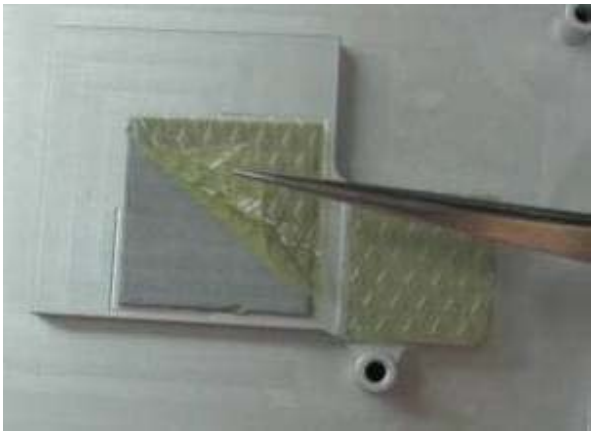
A heat sink can be used as a thermal solution for a specific COM Express module and can have a fan or be fanless, depending on the thermal requirements.

9.2.3. Installation

Install a heat spreader or heat sink using the following instructions.

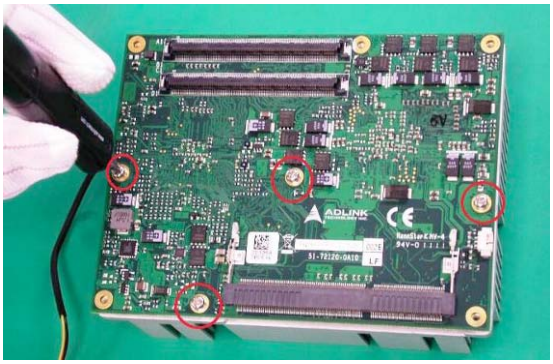
Step 1: Before mounting the heatsink, install the required memory modules onto the SODIMM socket(s) on the COM Express module.

Step 2: Remove the protective membranes from the thermal pads.

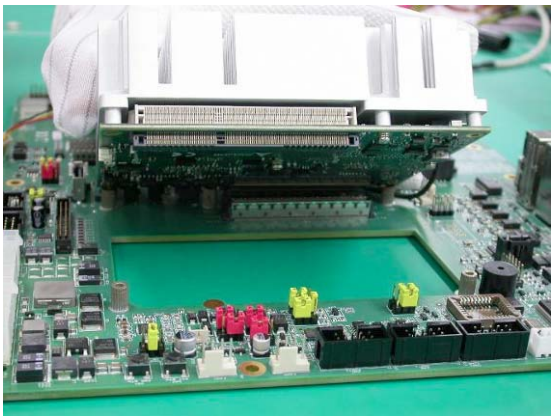


Step 3: Assemble the heatsink onto the COM Express module.

Step 4: Use the four M2.5, L=6mm screws provided to fasten the heatsink to the module.

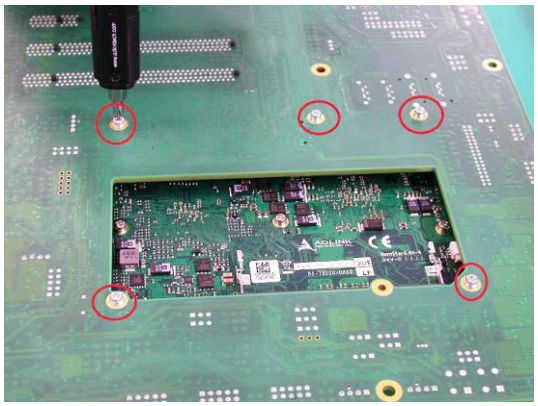


Step 5: Place the COM Express module and heatsink assembly onto the connectors on the carrier board as shown.



Then press down on the module until it is firmly seated on the carrier board.

Step 6: Use the five M2.5, L=16mm screws provided to secure the COM Express module to the carrier board from the solder side.



Step 7: If you are installing a heatsink with a fan, plug the fan connector into the carrier board as shown.

9.3. Mounting Methods

There are several standard ways to mount the COM Express module with a thermal solution onto a carrier board. In addition to the choice of 5 mm or 8mm board-to-board connectors, there is the choice of Top and Bottom mounting. In Top mounting, the threaded standoffs are on the carrier board and the thermal solution is equipped with through-hole standoffs. In Bottom mounting, the threaded standoffs are on the thermal solution and the carrier board has through-hole standoffs.

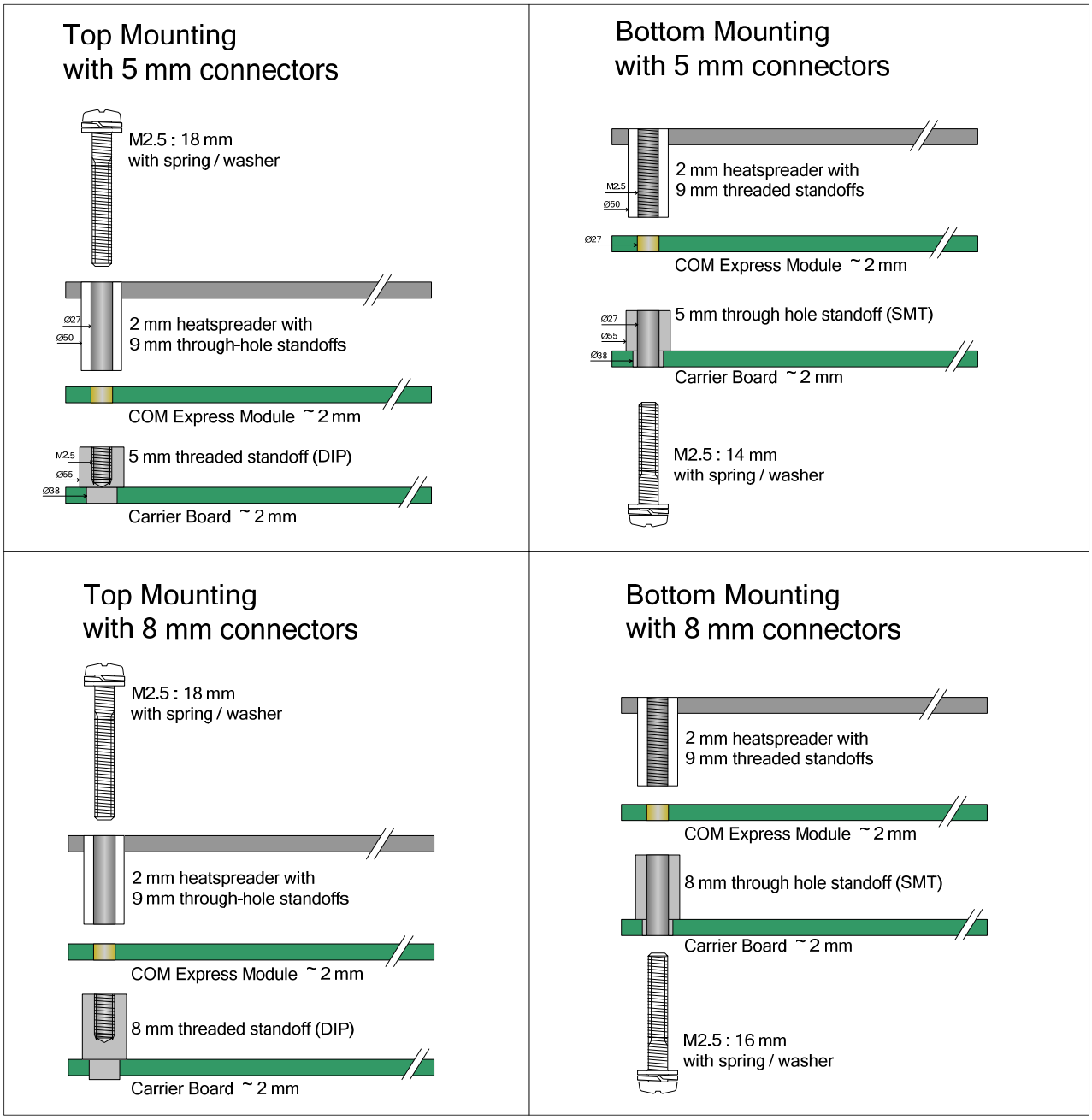


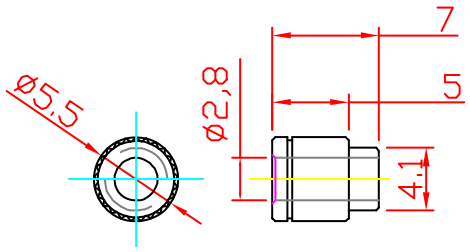
Figure 6: COM Express Mounting Methods

9.4. Standoff Types

The standoffs available for Top and Bottom mounting methods are shown below. Note that threaded standoffs are DIP type and through-hole standoffs are SMT type. Other types not listed are available upon request.

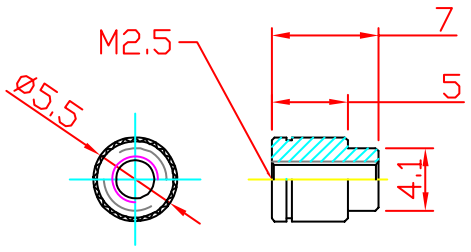
5mm through-hole standoff (SMT type)

P/N: 33-72000-0050



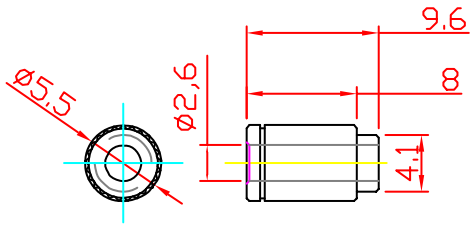
5mm threaded standoff (DIP type)

P/N: 33-72016-0050



8mm through-hole standoff (SMT type)

P/N: 33-72000-0080



8mm threaded standoff (DIP type)

P/N: 33-72015-0050

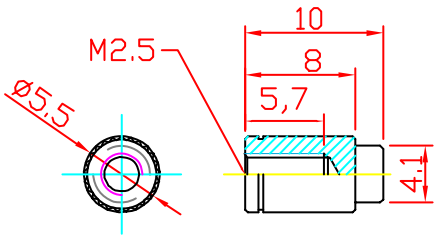


Figure 7: COM Express Standoff Types

Safety Instructions

Read and follow all instructions marked on the product and in the documentation before you operate your system. Retain all safety and operating instructions for future use.

- Please read these safety instructions carefully.
- Please keep this User‘s Manual for later reference.
- Read the specifications section of this manual for detailed information on the operating environment of this equipment.
- When installing/mounting or uninstalling/removing equipment, turn off the power and unplug any power cords/cables.
- To avoid electrical shock and/or damage to equipment:
  - Keep equipment away from water or liquid sources.
  - Keep equipment away from high heat or high humidity.
  - Keep equipment properly ventilated (do not block or cover ventilation openings).
  - Make sure to use recommended voltage and power source settings.
  - Always install and operate equipment near an easily accessible electrical socket-outlet.
  - Secure the power cord (do not place any object on/over the power cord).
  - Only install/attach and operate equipment on stable surfaces and/or recommended mountings.
  - If the equipment will not be used for long periods of time, turn off and unplug the equipment from its power source.
- Never attempt to fix the equipment. Equipment should only be serviced by qualified personnel.

Getting Service

Ask an Expert: http://askanexpert.adlinktech.com

ADLINK Technology, Inc.
Address: 9F, No.166 Jian Yi Road, Zhonghe District
New Taipei City 235, Taiwan
Tel: +886-2-8226-5877
Fax: +886-2-8226-5717
Email: service@adlinktech.com

Ampro ADLINK Technology, Inc.
Address: 5215 Hellyer Avenue, #110, San Jose, CA 95138, USA
Tel: +1-408-360-0200
Toll Free: +1-800-966-5200 (USA only)
Fax: +1-408-360-0222
Email: info@adlinktech.com

ADLINK Technology (China) Co., Ltd.
Address: 300 Fang Chun Rd., Zhangjiang Hi-Tech Park, Pudong New Area
Shanghai, 201203 China
Tel: +86-21-5132-8988
Fax: +86-21-5132-3588
Email: market@adlinktech.com

LiPPERT ADLINK Technology GmbH
Address: Hans-Thoma-Strasse 11, D-68163, Mannheim, Germany
Tel: +49-621-43214-0
Fax: +49-621 43214-30
Email: emea@adlinktech.com

Please visit the Contact page at www.adlinktech.com for information on how to contact the ADLINK regional office nearest you.