

IBS700

**SMARC 2.2 Module with
Intel® Amston Lake Processor**

User's Manual

Version 1.0
August 2026



Copyright

© 2026 IBASE Technology, Inc. All rights reserved.

No part of this publication may be reproduced, copied, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written consent of IBASE Technology, Inc.

Disclaimer

Every effort has been made to ensure the accuracy of the information contained in this document. However, IBASE cannot guarantee that this document is free of errors.

IBASE assumes no liability for any incidental or consequential damages arising from the use of this product or the information contained herein, nor for any infringements of third-party rights which may result from its use.

Trademarks

All trademarks, registered trademarks, and brand names mentioned herein are used for identification purposes only and remain the property of their respective owners.

Compliance



This is a class B product. In a domestic environment, this product may cause radio interference in which case users may be required to take adequate measures.



This product has been tested and found to comply with the limits for a Class B device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with manufacturer's instructions, may cause harmful interference to radio communications.

WEEE



This product must not be disposed of as normal household waste, in accordance with the EU directive for Waste Electrical and Electronic Equipment (WEEE - 2012/19/EU). Instead, it should be disposed of by returning it to a municipal recycling collection point. Check local regulations for disposal of electronic products.

Green IBASE



This product complies with RoHS 2 restrictions, which prohibit the use of certain hazardous substances in electrical and electronic equipment. The following substances must not exceed the specified concentrations:

- Hexavalent chromium: 1,000 ppm
- Poly-brominated biphenyls (PBBs): 1,000 ppm
- Poly-brominated diphenyl ethers (PBDEs): 1,000 ppm
- Cadmium: 100 ppm
- Mercury: 1,000 ppm
- Lead: 1,000 ppm
- Bis(2-ethylhexyl) phthalate (DEHP): 1,000 ppm
- Butyl benzyl phthalate (BBP): 1,000 ppm
- Dibutyl phthalate (DBP): 1,000 ppm
- Diisobutyl phthalate (DIBP): 1,000 ppm

Important Safety Information

Carefully read the precautions before using the board.

Environmental conditions:

- Use this product in environments with ambient temperatures between -40°C and 70°C.
- Do not leave this product in an environment where the storage temperature may be below -40°C or above 85°C. To prevent damage, operate the product only within the specified temperature range.

Care for your IBASE products:

- Before cleaning the PCB, unplug all cables and remove the battery.
- Clean the PCB with a circuit board cleaner, degreaser, or use cotton swabs and alcohol.
- Use a vacuum cleaner designed for electronics to remove dust.



WARNING

Attention during use:

- Do not use this product near water.
- Do not spill water or any other liquids on this product.
- Do not place heavy objects on top of this product.

Anti-static precautions

- Wear an anti-static wrist strap to avoid electrostatic discharge.
- Place the PCB on an anti-static mat.
- Hold the edges of the PCB when handling.
- Handle the board by its edges; avoid touching components or PCB surfaces.
- Ground yourself by touching a grounded metal object.



CAUTION

Replace only with the same or equivalent type recommended by the manufacturer. Recycle used batteries at an appropriate facility in accordance with local regulations.

Warranty Policy

- **IBASE standard products:**

24-month (2-year) warranty from the date of shipment. If the date of shipment cannot be ascertained, the product serial numbers can be used to determine the approximate shipping date.

- **3rd-party parts:**

Third-party parts that are not manufactured by IBASE, such as CPUs, CPU coolers, memory, storage devices, power adapters, panels, and touchscreens, are covered by a 12-month warranty from the date of delivery.

- * Products that fail due to misuse, accidents, improper installation, or unauthorized repairs will be considered out of warranty. Customers will be responsible for repair and shipping costs.

Technical Support & Services

1. Visit IBASE's website at www.ibase.com.tw to find the latest information about the product.
2. If you need any further assistance from your distributor or sales representative concerning problems that you may have encountered, please prepare the following information:
 - Product model name
 - Product serial number
 - Detailed description of the problem
 - Any error messages in text or in screenshots
 - Connected peripheral devices
 - Software in use (such as OS and application software, including the version numbers)
3. If repair service is required, please visit IBASE's website to read the warranty and RMA policy, before logging in to the eRMA System.

Table of Contents

Chapter 1 General Information	1
1.1 Introduction	2
1.2 Features	3
1.3 Packing List	3
1.4 Optional Accessories	3
1.5 Specifications	4
1.6 Block Diagram	6
1.7 Product View	7
1.8 Dimensions	8
Chapter 2 Module Layout and Pin Assignments	9
2.1 Components on IBS700 SMARC Module	10
2.2 SMARC Connector Pinout	11
Chapter 3 Drivers Installation	18
3.1 Introduction	19
3.2 Intel® Chipset Software Installation Utility	19
3.3 Graphics Drivers Installation	23
3.4 Realtek Audio Drivers Installation	26
3.5 Intel 2.5G Network Drivers Installation	28
3.6 Intel® ME Drivers Installation	29
3.7 Intel® Serial IO Drivers Installation	30
3.8 Intel® GNA Drivers Installation	31
Chapter 4 BIOS Setup	32
Appendix	53
A. I/O Port Address Map	54
B. Interrupt Request Lines (IRQ)	55

Chapter 1

General Information

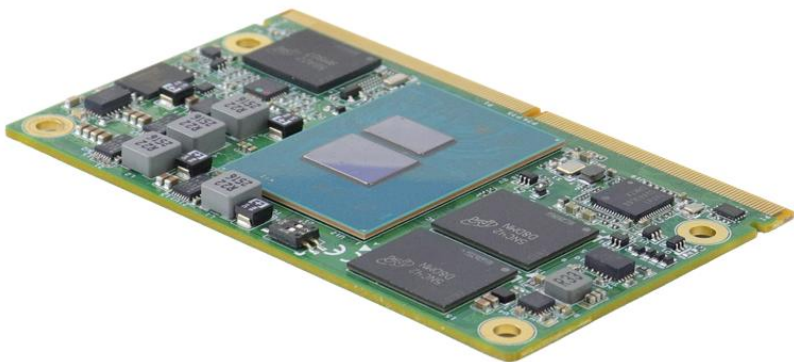
The information provided in this chapter includes:

- Features
- Packing List
- Specifications
- Block Diagram
- Product View
- Board Dimensions

1.1 Introduction

The IBS700 is a compact SMARC® v2.2 computer-on-module powered by Intel® Amston Lake processors, delivering an excellent balance of performance, power efficiency, and scalability for industrial and embedded applications.

Supporting up to eight CPU cores, onboard LPDDR5 memory, eMMC storage, dual 2.5GbE networking, Gen 12 Intel® UHD Graphics, and rich high-speed I/O including PCIe, SATA, USB, UART, GPIO, and I²C, the module provides a flexible platform for a wide range of edge computing solutions. Designed for reliable operation in harsh environments, the IBS700 supports industrial temperatures, TPM 2.0 security, Windows® and Ubuntu Linux, and full compliance with the SMARC® v2.2 specification.



IBS700 SMARC 2.2 Module

1.2 Features

- Intel® Amston Lake processors with up to 8 cores and low-power 6W–12W TDP options
- SMARC® v2.2 compliant 82 mm × 50 mm compact Computer-on-Module
- Onboard LPDDR5 memory (8GB/16GB) and 64GB eMMC storage
- Intel® Gen 12 UHD Graphics supporting up to three displays via 2 x DisplayPort++ and 1× eDP
- Dual 2.5GbE Ethernet with Intel® I226-IT controllers
- Rich expansion interfaces including PCIe, SATA III, USB 2.0/3.2, UART, GPIO, I²C, and SPI
- TPM 2.0 security, watchdog timer, RTC, and intelligent system management
- BIOS Flash programming connector with CMOS and Intel® ME register clearing support
- Industrial-grade design with an operating temperature range of -40°C to 70°C
- Supports Windows® 10/11 and Ubuntu Linux with SDKs and full SMARC® v2.2 compliance

1.3 Packing List

Your product package should include the items listed below.

- IBS700 SMARC board

1.4 Optional Accessories

IBASE provides optional accessories as listed below.

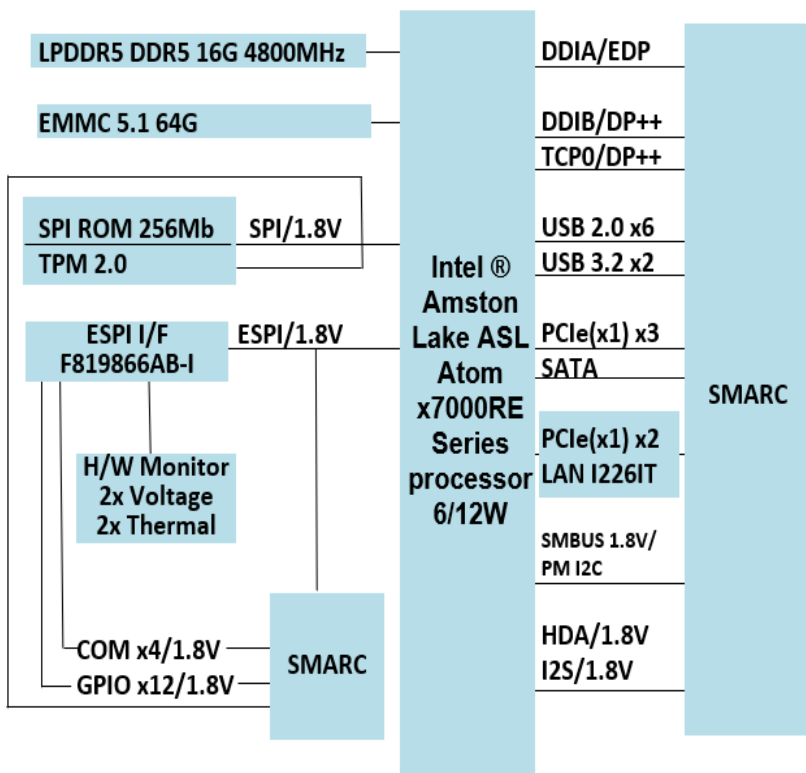
- Heatsink H052IBS700B0000AP

1.5 Specifications

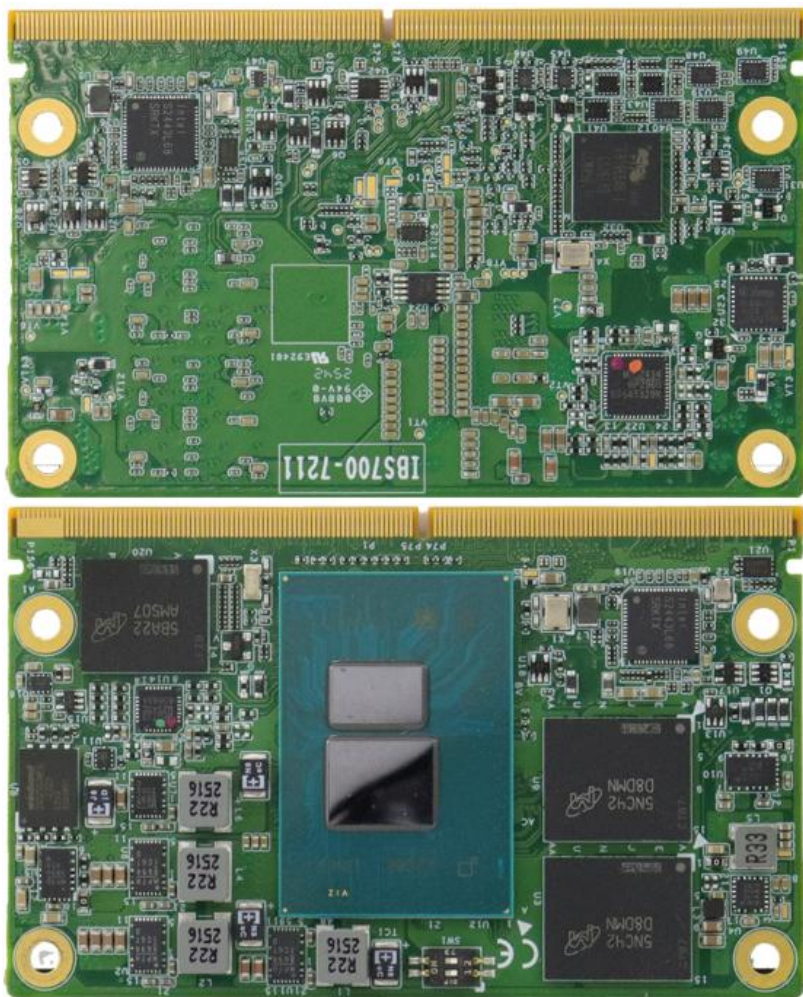
Product Name	IBS700			
Form Factor	SMARC V2.2 (82 mm x 50 mm)			
CPU Intel Amston Lake				
CPU Model	Intel® X7835RE	Intel® X7433RE	Intel® X7211RE	Intel® N150
Speed (HFM/Turbo)	1.3GHz / 3.6GHz	1.5GHz / 3.4GHz	1.0GHz/ 3.2GHz	Max/ 3.6GHz
Cores/Threads	8	4	2	4/4
TDP	12W	9W	6W	6W
Product Model	IBS700-7835-16G IBS700-7835-8G	IBS700-7433-16G IBS700-7433-8G	IBS700-7211-16G IBS700-7211-8G	IBS700-N150-16G IBS700-N150-8G
Cache	6 MB			
Socket	FCBGA1264 35 mm x 24mm			
Others	Default: LPDDR5 16GB/eMMC 64GB			
PCH				
PCH Model	Integrated into Intel Atom® x7000RE processor (Amston Lake)			
BIOS				
Model	AMI AptioV			
SPI Flash	256Mb for BIOS			
Boot Select	Configuration boot mode over BIOS settings / additionally via baseboard (like SMARC v2.2 standard)			
Memory				
Configuration	Onboard LPDDR5 up to 4800 MT/s			
Support	2 variants: 8GB; 16GB			
Display				
Display	Intel® SoC integrated UHD graphics Gen. 12 with 3 display ports support			
Display Interfaces	2x DisplayPort++, 3840 x 2160 at 60 Hz 1 x eDP port			
Communications				
LAN / PHY	2 x 2.5G LAN (Intel® I226-IT Chip (PCIe to LAN))			
Audio	Intel® processor built-in HD audio controller			
Audio Interface	1 × I²S, reserved for Linux applications 1x HDA			
Legacy I/O	Fintek F81966AB-I Fuse protection			

GPIO	12x GPIO GPIO 0–3 and GPIO 6–13 are provided by the F81966AB-I.
Serial Interface	4 x UART ports: • UART 0: 4-wire • UART 1: 2-wire • UART 2: 4-wire • UART 3: 2-wire
I²C	1x I ² C (general purpose on SMARC Connector) 1x I ² C_PM for eDP EDID EEPROM 1x SMBus/ I ² C Power Management for User EEPROM (custom)
SPI	1x SPI (0) for Boot Flash
SATA	1x SATA III (SMARC Spec.)
PCIe	3 x PCIe Config via Intel PCIe table
USB	• 6x USB 2.0 • 2x USB 3.2 (USB2 + USB3 see pinning SMARC connector)
RTC	Intel Processor Built-in RTC
Battery	Voltage monitoring for 3V Battery (BIOS)
Watch Dog	Yes (256 segments, 0–256 seconds or minutes)
TPM 2.0	Infineon SLB9672XU2.0FW16.24 (UQFN32) P/N: C01Z9672XU2016000P
Security	Designed to support Cyber Resilience Act (CRA) compliance requirements effective in 2027.
Connectors	
SMARC	SMARC V2.2 edge connector
Power	
Power	Supplied via SMARC connector with 5.0V ±5% (4.75V to 5.25V). Refer to the SMARC 2.2 Specification for details regarding AT/ATX mode selection.
Add-On Features	
Others	Power management does not support Smart Battery, Lid, Deep Sleep, or power-saving functions.
Environmental	
Temperature	Operating: -40°C ~70°C Storage: -40°C ~ 85°C
Humidity	Operating: 10% ~ 85% (non-condensing) Storage: 5% ~ 85% (non-condensing)
Shock	IBASE Standard Test
Vibration	IBASE Standard Test
Certification	RoHS, CE, FCC Class B
OS Support	MS Windows 10/11, Linux Ubuntu, one SDK for GPIO & Watchdog and another SDK for Temperatures & Voltages

1.6 Block Diagram

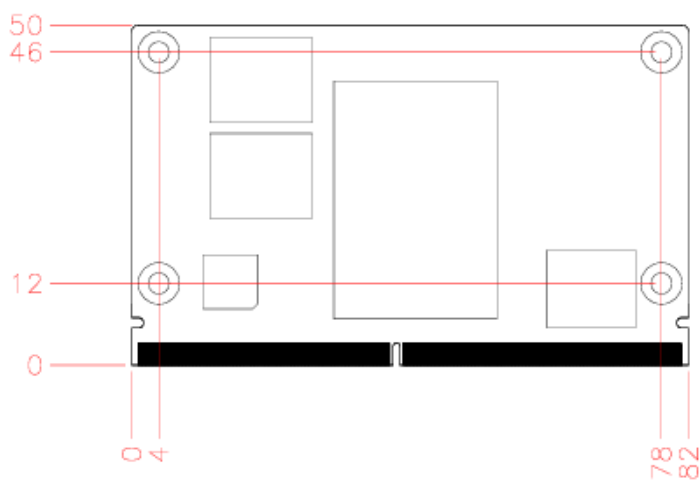


1.7 Product View



1.8 Dimensions

Unit: in mm

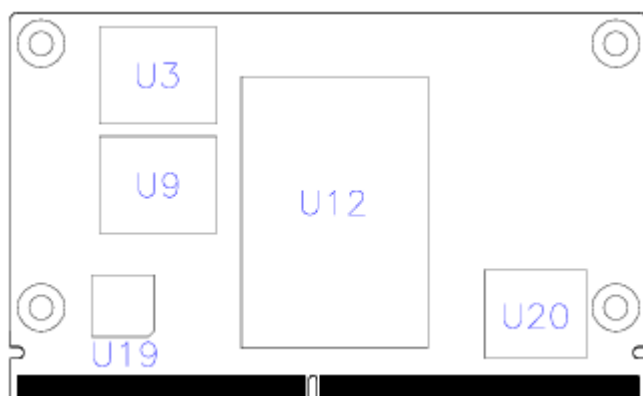


Chapter 2

Module Layout and Pin Assignments

This section provides information on SMARC module images, dimensions, component locations and pin assignments.

2.1 Components on IBS700 SMARC Module



2.2 SMARC Connector Pinout

This section describes the IBS700 connector pin assignment, which is compliant with the SMARC hardware specification version 2.2.

Signal Assignment Abbreviations

Abbreviation	Description
GND	Ground
PWR	Power
I	Input
IPU	Input with pull-up resistor
IPD	Input with pull-down resistor
O	Output
OD	Open drain output
IO	Bi-directional

SMARC Connector Pin Assignment

Pin	Pin-Signal	Description	Type	Level	Remark
P1	SMB_ALERT#	SM Bus Alert# (interrupt) signal	I PU	1.8 V	
P2	GND	Ground	GND		
P3	CS11_CK+	CSI differential clock input	I	LVDS D-PHY	N/A
P4	CS11_CK-	CSI differential clock input	I	LVDS D-PHY	N/A
P5	GBE1_SDP	Gigabit Ethernet Controller 1 Software-Definable Pin	IO	3.3 V	
P6	GBE0_SDP	Gigabit Ethernet Controller 0 Software-Definable Pin	IO	3.3 V	
P7	CS11_RX0+	CSI differential data input	I	LVDS D-PHY	N/A
P8	CS11_RX0-	CSI differential data input	I	LVDS D-PHY	N/A
P9	GND	Ground	GND		
P10	CS11_RX1+	CSI differential data input	I	LVDS D-PHY	N/A
P11	CS11_RX1-	CSI differential data input	I	LVDS D-PHY	N/A
P12	GND	Ground	GND		
P13	CS11_RX2+	CSI differential data input	I	LVDS D-PHY	N/A
P14	CS11_RX2-	CSI differential data input	I	LVDS D-PHY	N/A
P15	GND	Ground	GND		
P16	CS11_RX3+	CSI differential data input	I	LVDS D-PHY	N/A
P17	CS11_RX3-	CSI differential data input	I	LVDS D-PHY	N/A
P18	GND	Ground	GND		
P19	GBE0_MDI3-	Gigabit Ethernet Controller: Media Dependent Interface	IO	GBE MDI	
P20	GBE0_MDI3+	Gigabit Ethernet Controller: Media Dependent Interface	IO	GBE MDI	
P21	GBE0_LINK100#	Link Speed Indication LED for 100 Mbps	OD	3.3 V	
P22	GBE0_LINK1000#	Link Speed Indication LED for 1000 Mbps	OD	3.3 V	
P23	GBE0_MDI2-	Gigabit Ethernet Controller: Media Dependent Interface	IO	GBE MDI	
P24	GBE0_MDI2+	Gigabit Ethernet Controller: Media Dependent Interface	IO	GBE MDI	
P25	GBE0_LINK_ACT#	Link / Activity Indication LED	OD	3.3 V	
P26	GBE0_MDI1-	Gigabit Ethernet Controller: Media Dependent Interface	IO	GBE MDI	
P27	GBE0_MDI1+	Gigabit Ethernet Controller: Media Dependent Interface	IO	GBE MDI	
P28	GBE0_CTREF	Center-Tap reference voltage for Carrier Ethernet magnetics	PWR		N/A
P29	GBE0_MDI0-	Gigabit Ethernet Controller: Media Dependent Interface	IO	GBE MDI	
P30	GBE0_MDI0+	Gigabit Ethernet Controller: Media Dependent Interface	IO	GBE MDI	
P31	SPI0_CS1#	SPI0 Master Chip Select 1 output	O	1.8 V	N/A
P32	GND	Ground	GND		
P33	SDIO_WP	SD Card: Write Protect	I PU	3.3 V	N/A
P34	SDIO_CMD	SD Card: Command line	IO	3.3 V	N/A
P35	SDIO_CD#	SD Card: Card Detect	I PU	3.3 V	N/A

SMARC Connector Pin Assignment (continued)

Pin	Pin-Signal	Description	Type	Level	Remark
P36	SDIO_CLK	SD Card: Clock	O	3.3 V	N/A
P37	SDIO_PWR_EN	SD Card: Power enable	O	3.3 V	N/A
P38	GND	Ground	GND		
P39	SDIO_D0	SD Card: data path	IO	3.3 V	N/A
P40	SDIO_D1	SD Card: data path	IO	3.3 V	N/A
P41	SDIO_D2	SD Card: data path	IO	3.3 V	N/A
P42	SDIO_D3	SD Card: data path	IO	3.3 V	N/A
P43	SPI0_CS0#	SPI0 Master Chip Select 0 output	O	1.8 V	
P44	SPI0_CLK	SPI0 Master Clock output	O	1.8 V	
P45	SPI0_DIN	SPI0 Master Data input (CPU input, SPI device output)	I	1.8 V	
P46	SPI0_DO	SPI0 Master Data output (CPU output, SPI device input)	O	1.8 V	
P47	GND	Ground	GND		
P48	SATA_TX+	Differential SATA transmit data Pair	O	SATA	
P49	SATA_TX-	Differential SATA transmit data Pair	O	SATA	
P50	GND	Ground	GND		
P51	SATA_RX+	Differential SATA receive data Pair	I	SATA	
P52	SATA_RX-	Differential SATA receive data Pair	I	SATA	
P53	GND	Ground	GND		
P54	ESPI_CS0#	ESPI / SPI master chip select	O	1.8 V	
P55	ESPI_CS1#	ESPI master chip select (Not available on TQmx415)	O	1.8 V	N/A
P56	ESPI_CLK	ESPI / SPI master clock output	O	1.8 V	
P57	ESPI_IO_1	ESPI master data I/O / SPI data in	IO	1.8 V	
P58	ESPI_IO_0	ESPI master data I/O / SPI data out	IO	1.8 V	
P59	GND	Ground	GND		
P60	USB0+	USB differential pair	IO	USB	
P61	USB0-	USB differential pair	IO	USB	
P62	USB0_EN_OC#	USB over-current input / enable output (both OD)	IO PU	3.3 V	
P63	USB0_VBUS_DET	Host power detection (when port is used as device)	I PD	5 V	N/A
P64	USB0_OTG_ID	USB OTG ID input, active high (high $\Rightarrow$ device)	I PU	3.3 V	N/A
P65	USB1+	USB differential pair	IO	USB	
P66	USB1-	USB differential pair	IO	USB	
P67	USB1_EN_OC#	USB over-current input / enable output (both OD)	IO PU	3.3 V	
P68	GND	Ground	GND		
P69	USB2+	USB differential pair	IO	USB	
P70	USB2-	USB differential pair	IO	USB	
P71	USB2_EN_OC#	USB over-current input / enable output (both OD)	IO PU	3.3 V	
P72	RSVD	Reserved			
P73	RSVD	Reserved			
P74	USB3_EN_OC#	USB over-current input / enable output (both OD)	IO PU	3.3 V	
P75	PCIE_A_RST#	PCIE Port reset output	O	3.3 V	
P76	USB4_EN_OC#	USB over-current input / enable output (both OD)	IO PU	3.3 V	
P77	PCIE_B_CKREQ#	PCIE Port B clock request	IO PU	3.3 V	
P78	PCIE_A_CKREQ#	PCIE Port A clock request	IO PU	3.3 V	
P79	GND	Ground	GND		
P80	PCIE_C_REFCK+	Differential PCIE Link reference clock output	O	PCIE	
P81	PCIE_C_REFCK-	Differential PCIE Link reference clock output	O	PCIE	
P82	GND	Ground	GND		
P83	PCIE_A_REFCK+	Differential PCIE Link reference clock output	O	PCIE	
P84	PCIE_A_REFCK-	Differential PCIE Link reference clock output	O	PCIE	
P85	GND	Ground	GND		
P86	PCIE_A_RX+	Differential PCIE Link receive data pair	I	PCIE	
P87	PCIE_A_RX-	Differential PCIE Link receive data pair	I	PCIE	
P88	GND	Ground	GND		
P89	PCIE_A_TX+	Differential PCIE Link transmit data pair	O	PCIE	
P90	PCIE_A_TX-	Differential PCIE Link transmit data pair	O	PCIE	
P91	GND	Ground	GND		
P92	HDMI_D2+ / DP1_LANE0+	TMDS / HDMI data differential pair / DP data pair	O	DP++	
P93	HDMI_D2- / DP1_LANE0-	TMDS / HDMI data differential pair / DP data pair	O	DP++	
P94	GND	Ground	GND		
P95	HDMI_D1+ / DP1_LANE1+	TMDS / HDMI data differential pair / DP data pair	O	DP++	
P96	HDMI_D1- / DP1_LANE1-	TMDS / HDMI data differential pair / DP data pair	O	DP++	
P97	GND	Ground	GND		
P98	HDMI_D0+ / DP1_LANE2+	TMDS / HDMI data differential pair / DP data pair	O	DP++	
P99	HDMI_D0- / DP1_LANE2-	TMDS / HDMI data differential pair / DP data pair	O	DP++	
P100	GND	Ground	GND		
P101	HDMI_CLK+ / DP1_LANE3+	HDMI differential clock output pair / DP data pair	O	DP ++	
P102	HDMI_CLK- / DP1_LANE3-	HDMI differential clock output pair / DP data pair	O	DP ++	
P103	GND	Ground	GND		
P104	HDMI_HPD / DP1_HPD	HDMI / DP Hot Plug Detect input	I PD	1.8 V	

SMARC Connector Pin Assignment (continued)

Pin	Pin-Signal	Description	Type	Level	Remark
P105	HDMI_CTRL_CLK / DP1_AUX+	HDMI I ² C clock / DP AUX Channel	IO	3.3 V	
P106	HDMI_CTRL_DAT / DP1_AUX-	HDMI I ² C data / DP AUX Channel	IO	3.3 V	
P107	DP1_AUX_SEL	DP AUX select (to select between DP and HDMI)	I PD	1.8 V	
P108	GPIO0 / CAM0_PWR#	GPIO / Camera power enable (active low output)	IO PU/O	1.8 V	GPIO0
P109	GPIO1 / CAM1_PWR#	GPIO / Camera power enable (active low output)	IO PU/O	1.8 V	GPIO1
P110	GPIO2 / CAM0_RST#	GPIO / Camera reset (active low output)	IO PU/O	1.8 V	GPIO2
P111	GPIO3 / CAM1_RST#	GPIO / Camera reset (active low output)	IO PU/O	1.8 V	GPIO3
P112	GPIO4 / HDA_RST#	GPIO / HD audio reset (active low output)	IO PU/O	1.8 V	HAD_RST
P113	GPIO5 / PWM_OUT	GPIO / PWM out for fan speed control	IO PU/O	1.8 V	N/A
P114	GPIO6 / TACHIN	GPIO / Tachometer input for fan speed measurement	IO PU/O	1.8 V	GPIO6
P115	GPIO7	GPIO	IO PU	1.8 V	
P116	GPIO8	GPIO	IO PU	1.8 V	
P117	GPIO9	GPIO	IO PU	1.8 V	
P118	GPIO10	GPIO	IO PU	1.8 V	
P119	GPIO11	GPIO	IO PU	1.8 V	
P120	GND	Ground	GND		
P121	I2C_PM_CLK	Power management I ² C bus: SMBus	IO PU	1.8 V	
P122	I2C_PM_DAT	Power management I ² C bus: SMBus	IO PU	1.8 V	
P123	BOOT_SEL0#	Boot source select (Not used on IB700)	I	1.8 V	N/A
P124	BOOT_SEL1#	Boot source select (Not used on IB700)	I	1.8 V	N/A
P125	BOOT_SEL2#	Boot source select (tie to GND to boot from carrier SPI)	I PU	1.8 V	
P126	RESET_OUT#	General purpose reset output to carrier board	O	1.8 V	
P127	RESET_IN#	Reset input from Carrier board	I PU	1.8 V	
P128	POWER_BTN#	Power-button input from Carrier board	I PU	1.8 V	
P129	SER0_TX	Serial port data out	O	1.8 V	
P130	SER0_RX	Serial port data in	I	1.8 V	
P131	SER0_RTS#	Serial port handshake: Request to Send	O	1.8 V	
P132	SER0_CTS#	Serial port handshake: Clear to Send	I	1.8 V	
P133	GND	Ground	GND		
P134	SER1_TX	Serial port data out	O	1.8 V	
P135	SER1_RX	Serial port data in	I	1.8 V	
P136	SER2_TX	Serial port data out	O	1.8 V	
P137	SER2_RX	Serial port data in	I	1.8 V	
P138	SER2_RTS#	Serial port handshake: Request to Send	O	1.8 V	
P139	SER2_CTS#	Serial port handshake: Clear to Send	I	1.8 V	
P140	SER3_TX	Serial port data out	O	1.8 V	
P141	SER3_RX	Serial port data in	I	1.8 V	
P142	GND	Ground	GND		
P143	CAN0_TX	CAN Transmit output	O	1.8 V	N/A
P144	CAN0_RX	CAN Receive input	I	1.8 V	N/A
P145	CAN1_TX	CAN Transmit output	O	1.8 V	N/A
P146	CAN1_RX	CAN Receive input	I	1.8 V	N/A
P147	VDD_IN	Module power input voltage	PWR	4.75 to 5.25 V	
P148	VDD_IN	Module power input voltage	PWR	4.75 to 5.25 V	
P149	VDD_IN	Module power input voltage	PWR	4.75 to 5.25 V	
P150	VDD_IN	Module power input voltage	PWR	4.75 to 5.25 V	
P151	VDD_IN	Module power input voltage	PWR	4.75 to 5.25 V	
P152	VDD_IN	Module power input voltage	PWR	4.75 to 5.25 V	
P153	VDD_IN	Module power input voltage	PWR	4.75 to 5.25 V	
P154	VDD_IN	Module power input voltage	PWR	4.75 to 5.25 V	
P155	VDD_IN	Module power input voltage	PWR	4.75 to 5.25 V	
P156	VDD_IN	Module power input voltage	PWR	4.75 to 5.25 V	

2: Configurable through TQ-flexiCFG.

SMARC Connector Pin Assignment (continued)

Pin	Pin-Signal	Description	Type	Level	Remark
S1	CSI1_TX+ / I2C_CAM1_CK	Camera I ² C	IO PU	1.8 V	N/A
S2	CSI1_TX- / I2C_CAM1_DAT	Camera I ² C	IO PU	1.8 V	N/A
S3	GND	Ground	GND		
S4	RSVD	Reserved			
S5	CSIO_TX+ / I2C_CAM0_CK	Camera I ² C	IO PU	1.8 V	N/A
S6	CAM_MCK	Master clock output for CSI camera support	O	1.8 V	N/A
S7	CSIO_TX- / I2C_CAM0_DAT	Camera I ² C	IO PU	1.8 V	N/A
S8	CSIO_CK+	CSI differential clock input	I	LVDS D-PHY	N/A
S9	CSIO_CK-	CSI differential clock input	I	LVDS D-PHY	N/A
S10	GND	Ground	GND		
S11	CSIO_RX0+	CSI differential data input	I	LVDS D-PHY	N/A
S12	CSIO_RX0-	CSI differential data input	I	LVDS D-PHY	N/A
S13	GND	Ground	GND		
S14	CSIO_RX1+	CSI differential data input	I	LVDS D-PHY	N/A
S15	CSIO_RX1-	CSI differential data input	I	LVDS D-PHY	N/A
S16	GND	Ground	GND		
S17	GBE1_MDIO+	Gigabit Ethernet Controller: Media Dependent Interface	IO	GBE MDI	
S18	GBE1_MDIO-	Gigabit Ethernet Controller: Media Dependent Interface	IO	GBE MDI	
S19	GBE1_LINK100#	Link Speed Indication LED for 100 Mbps	OD	3.3 V	
S20	GBE1_MD11+	Gigabit Ethernet Controller: Media Dependent Interface	IO	GBE MDI	
S21	GBE1_MD11-	Gigabit Ethernet Controller: Media Dependent Interface	IO	GBE MDI	
S22	GBE1_LINK1000#	Link Speed Indication LED for 1000 Mbps	OD	3.3 V	
S23	GBE1_MD12+	Gigabit Ethernet Controller: Media Dependent Interface	IO	GBE MDI	
S24	GBE1_MD12-	Gigabit Ethernet Controller: Media Dependent Interface	IO	GBE MDI	
S25	GND	Ground	GND		
S26	GBE1_MD13+	Gigabit Ethernet Controller: Media Dependent Interface	IO	GBE MDI	
S27	GBE1_MD13-	Gigabit Ethernet Controller: Media Dependent Interface	IO	GBE MDI	
S28	GBE1_CTREF	Center-Tap reference voltage for Carrier Ethernet magnetics	PWR		
S29	PCIE_D_TX+	Differential PCIe Link transmit data pair	O	PCIe	
S30	PCIE_D_TX-	Differential PCIe Link transmit data pair	O	PCIe	
S31	GBE1_LINK_ACT#	Link / Activity Indication LED	OD	3.3 V	
S32	PCIE_D_RX+	Differential PCIe Link receive data pair	I	PCIe	N/A
S33	PCIE_D_RX-	Differential PCIe Link receive data pair	I	PCIe	N/A
S34	GND	Ground	GND		
S35	USB4+	USB differential pair	IO	USB	
S36	USB4-	USB differential pair	IO	USB	
S37	USB3_VBUS_DET	Host power detection (when port is used as device)	I PD	5 V	N/A
S38	AUDIO_MCK	I ² S: Master clock output to Audio codecs	O	1.8 V	
S39	I2S0_LRCK	I ² S: Left & Right audio synchronization clock	IO	1.8 V	
S40	I2S0_SDOUT	I ² S: Digital audio Output	O	1.8 V	
S41	I2S0_SDIN	I ² S: Digital audio Input	I	1.8 V	
S42	I2S0_CK	I ² S: Digital audio clock	IO	1.8 V	
S43	ESPI_ALERT0#	ESPI alert	I PU	1.8 V	
S44	ESPI_ALERT1#	ESPI alert (Not available on TQMXE415)	I PU	1.8 V	N/A
S45	MDIO_CLK	MDIO Clock (Not available on TQMXE415)	O	1.8 V	N/A
S46	MDIO_DAT	MDIO Data (Not available on TQMXE415)	IO PU	1.8 V	N/A
S47	GND	Ground	GND		
S48	I2C_GP_CK	General Purpose I ² C bus	IO PU	1.8 V	
S49	I2C_GP_DAT	General Purpose I ² C bus	IO PU	1.8 V	
S50	HDA_SYNC / I2S2_LRCK	HDA: sync / I ² S: L & R audio clock (Only HDA on TQMXE415)	IO	1.8 V	
S51	HDA_SDO / I2S2_SDOUT	HDA: data out / I ² S: Digital Output (Only HDA on TQMXE415)	O	1.8 V	
S52	HDA_SDI / I2S2_SDIN	HDA: data in / I ² S: Digital Input (Only HDA on TQMXE415)	I	1.8 V	

SMARC Connector Pin Assignment (continued)

Pin	Pin-Signal	Description	Type	Level	Remark
S53	HDA_CLK / I2S2_CLK	HDA: clock / I ² S: Digital clock (Only HDA on TQMxE415)	IO	1.8 V	
S54	SATA_ACT#	Active low SATA activity indicator	OD	3.3 V	
S55	USB5_EN_OC#	USB over-current input / enable output (both OD)	IO PU	3.3 V	
S56	ESPI_IO_2	ESPI master data I/O	IO	1.8 V	
S57	ESPI_IO_3	ESPI master data I/O	IO	1.8 V	
S58	ESPI_RESET#	ESPI Reset	IO	1.8 V	
S59	USB5+	USB differential pair	IO	USB	
S60	USB5-	USB differential pair	IO	USB	
S61	GND	Ground	GND		
S62	USB3_SSTX+	Differential USB SuperSpeed transmit data pair	O	USB SS	
S63	USB3_SSTX-	Differential USB SuperSpeed transmit data pair	O	USB SS	
S64	GND	Ground	GND		
S65	USB3_SSRX+	Differential USB SuperSpeed receive data pair	I	USB SS	
S66	USB3_SSRX-	Differential USB SuperSpeed receive data pair	I	USB SS	
S67	GND	Ground	GND		
S68	USB3+	USB differential pair	IO	USB	
S69	USB3-	USB differential pair	IO	USB	
S70	GND	Ground	GND		
S71	USB2_SSTX+	Differential USB SuperSpeed transmit data pair	O	USB SS	
S72	USB2_SSTX-	Differential USB SuperSpeed transmit data pair	O	USB SS	
S73	GND	Ground	GND		
S74	USB2_SSRX+	Differential USB SuperSpeed receive data pair	I	USB SS	
S75	USB2_SSRX-	Differential USB SuperSpeed receive data pair	I	USB SS	
S76	PCIE_B_RST#	PCIE Port reset output	O	3.3 V	
S77	PCIE_C_RST#	PCIE Port reset output	O	3.3 V	
S78	PCIE_C_RX+	Differential PCIE Link receive data pair	I	PCIE	
S79	PCIE_C_RX-	Differential PCIE Link receive data pair	I	PCIE	
S80	GND	Ground	GND		
S81	PCIE_C_TX+	Differential PCIE Link transmit data pair	O	PCIE	
S82	PCIE_C_TX-	Differential PCIE Link transmit data pair	O	PCIE	
S83	GND	Ground	GND		
S84	PCIE_B_REFCK+	Differential PCIE Link reference clock output	O	PCIE	
S85	PCIE_B_REFCK-	Differential PCIE Link reference clock output	O	PCIE	
S86	GND	Ground	GND		
S87	PCIE_B_RX+	Differential PCIE Link receive data pair	I	PCIE	
S88	PCIE_B_RX-	Differential PCIE Link receive data pair	I	PCIE	
S89	GND	Ground	GND		
S90	PCIE_B_TX+	Differential PCIE Link transmit data pair	O	PCIE	
S91	PCIE_B_TX-	Differential PCIE Link transmit data pair	O	PCIE	
S92	GND	Ground	GND		
S93	DP0_LANE0+	DP++ data differential pair	O	DP++	
S94	DP0_LANE0-	DP++ data differential pair	O	DP++	
S95	DP0_AUX_SEL	DP AUX select (to select between DP and HDMI)	I PD	1.8 V	
S96	DP0_LANE1+	DP++ data differential pair	O	DP++	
S97	DP0_LANE1-	DP++ data differential pair	O	DP++	
S98	DP0_HPD	DP++ Hot Plug Detect input	I PD	1.8 V	
S99	DP0_LANE2+	DP++ data differential pair	O	DP++	
S100	DP0_LANE2-	DP++ data differential pair	O	DP++	
S101	GND	Ground	GND		
S102	DP0_LANE3+	DP++ data differential pair	O	DP++	
S103	DP0_LANE3-	DP++ data differential pair	O	DP++	
S104	USB3_OTG_ID	USB OTG ID input, active high (high ⇒ device)	I PU	3.3 V	N/A

SMARC Connector Pin Assignment (continued)

Pin	Pin-Signal	Description	Type	Level	Remark
S105	DP0_AUX+	DP++ AUX Channel (could also be used as 3.3 V I ² C for HDMI)	IO	DP++ /3.3 V	
S106	DP0_AUX-	DP++ AUX Channel (could also be used as 3.3 V I ² C for HDMI)	IO	DP++ /3.3 V	
S107	LCD1_BKLT_EN	LCD Backlight enable: high enables panel backlight	O	1.8 V	N/A
S108	LVDS1_CLK+ / eDP1_AUX+ / DSI1_CLK+	LVDS LCD differential clock pair / eDP AUX Channel	O/IO	LVDS/EDP	N/A
S109	LVDS1_CLK- / eDP1_AUX- / DSI1_CLK-	LVDS LCD differential clock pair / eDP AUX Channel	O/IO	LVDS/EDP	N/A
S110	GND	Ground	GND		
S111	LVDS1_0+ / eDP1_TX0+ / DSI1_D0+	LVDS / eDP data differential pair	O	LVDS/EDP	N/A
S112	LVDS1_0- / eDP1_TX0- / DSI1_D0-	LVDS / eDP data differential pair	O	LVDS/EDP	N/A
S113	eDP1_HPD/DSI1_TE	eDP Hot Plug Detect	I PD	1.8 V	N/A
S114	LVDS1_1+ / eDP1_TX1+ / DSI1_D1+	LVDS / eDP data differential pair	O	LVDS/EDP	N/A
S115	LVDS1_1- / eDP1_TX1- / DSI1_D1-	LVDS / eDP data differential pair	O	LVDS/EDP	N/A
S116	LCD1_VDD_EN	Enable signal for panel power	O	1.8 V	N/A
S117	LVDS1_2+ / eDP1_TX2+ / DSI1_D2+	LVDS / eDP data differential pair	O	LVDS/EDP	N/A
S118	LVDS1_2- / eDP1_TX2- / DSI1_D2-	LVDS / eDP data differential pair	O	LVDS/EDP	N/A
S119	GND	Ground	GND		
S120	LVDS1_3+ / eDP1_TX3+ / DSI1_D3+	LVDS / eDP data differential pair	O	LVDS/EDP	N/A
S121	LVDS1_3- / eDP1_TX3- / DSI1_D3-	LVDS / eDP data differential pair	O	LVDS/EDP	N/A
S122	LCD1_BKLT_PWM	Display Backlight brightness control output (PWM)	O	1.8 V	N/A
S123	GPIO13	GPIO	IO PU	1.8 V	
S124	GND	Ground	GND		
S125	LVDS0_0+ / eDP0_TX0+ / DSI0_D0+	LVDS / eDP data differential pair	O	EDP	
S126	LVDS0_0- / eDP0_TX0- / DSI0_D0-	LVDS / eDP data differential pair	O	EDP	
S127	LCD0_BKLT_EN	LCD Backlight enable: high enables panel backlight	O	1.8 V	
S128	LVDS0_1+ / eDP0_TX1+ / DSI0_D1+	LVDS / eDP data differential pair	O	EDP	
S129	LVDS0_1- / eDP0_TX1- / DSI0_D1-	LVDS / eDP data differential pair	O	EDP	
S130	GND	Ground	GND		
S131	LVDS0_2+ / eDP0_TX2+ / DSI0_D2+	LVDS / eDP data differential pair	O	EDP	
S132	LVDS0_2- / eDP0_TX2- / DSI0_D2-	LVDS / eDP data differential pair	O	EDP	
S133	LCD0_VDD_EN	Enable signal for panel power	O	1.8 V	
S134	LVDS0_CLK+ / eDP0_AUX+ / DSI0_CLK+	LVDS LCD differential clock pair / eDP AUX Channel	O/IO	EDP	
S135	LVDS0_CLK- / eDP0_AUX- / DSI0_CLK-	LVDS LCD differential clock pair / eDP AUX Channel	O/IO	EDP	

SMARC Connector Pin Assignment (continued)

Pin	Pin-Signal	Description	Type	Level	Remark
S136	GND	Ground	GND		
S137	LVDS0_3+ / eDP0_TX3+ / DSIO_D3+	LVDS / eDP data differential pair	O	EDP	
S138	LVDS0_3- / eDP0_TX3- / DSIO_D3-	LVDS / eDP data differential pair	O	EDP	
S139	I2C_LCD_CLK	I ² C bus to read display EDID EEPROMs (for LVDS displays)	IO PU	1.8 V	N/A
S140	I2C_LCD_DAT	I ² C bus to read display EDID EEPROMs (for LVDS displays)	IO PU	1.8 V	N/A
S141	LCDD0_BKLT_PWM	Display Backlight brightness control output (PWM)	O	1.8 V	
S142	GPIO12	GPIO	IO PU	1.8 V	
S143	GND	Ground	GND		
S144	eDP0_HPD	eDP Hot Plug Detect	I PD	1.8 V	
S145	WDT_TIME_OUT#	Watch-Dog-Timer Output	O	1.8 V	
S146	PCI_E_WAKE#	PCIe wake up interrupt to host	I PU	3.3 V	
S147	VDD_RTC	Real-time clock circuit-power input	PWR	2 V to 3.3 V	
S148	LID#	Lid open/close indication to module (low: closed lid)	I PU	1.8 V	N/A
S149	SLEEP#	Sleep indicator from carrier board	I PU	1.8 V	N/A
S150	VIN_PWR_BAD#	Power bad indication from Carrier board	I PU	VDD_IN	
S151	CHARGING#	Held low by carrier during battery charging	I PU	1.8 V	N/A
S152	CHARGER_PRSENT#	Held low by carrier if DC input for battery charger is present	I PU	1.8 V	N/A
S153	CARRIER_STBY#	Driven low by module during standby power state	O	1.8 V	SUS_S3#
S154	CARRIER_PWR_ON	Signal to carrier to turn on determined power supplies	O	1.8 V	RSMRST
S155	FORCE_RECOV#	Force recovery input: pull low to load BIOS defaults (edge triggered)	I PU	1.8 V	
S156	BATLOW#	Battery low indication to module	I PU	3.3 V	N/A
S157	TEST#	Held low by carrier for module vendor specific functions	I PU	1.8 V	N/A
S158	GND	Ground	GND		

Chapter 3

Drivers Installation

The information provided in this chapter includes:

- Intel® Chipset Software Installation Utility
- Graphics Driver
- Realtek Audio Drivers
- Intel® 2.5G Network Drivers
- Intel® ME Drivers
- Intel® Serial IO Drivers
- Intel® GNA Drivers

3.1 Introduction

This section describes the installation procedures for software drivers. Go to the download page of the product. Copy the compressed drivers file to your computer. Double click the file to decompress it. Run “CDGuide” to go to the main drivers page.

Note: After installing your Windows operating system, you must install the Intel® Chipset Software Installation Utility before proceeding with the installation of the other drivers.

3.2 Intel® Chipset Software Installation Utility

The Intel® Chipset drivers should be installed before the software drivers to install INF files for Plug & Play function for the chipset components. Follow the instructions below to complete the installation.

1. Click **Intel** and then **Intel(R) Alder-N/Amston/Twin Lake Chipset Driver**.



2. Click **Intel(R) Chipset Software Installation Utility**.



3. When the Welcome screen appears, click **Next**.



4. Accept the terms of the license agreement. Click **Accept**.



5. Click **Install** to begin installation.



6. After completing the setup process, click **Finish**.



3.3 Graphics Drivers Installation

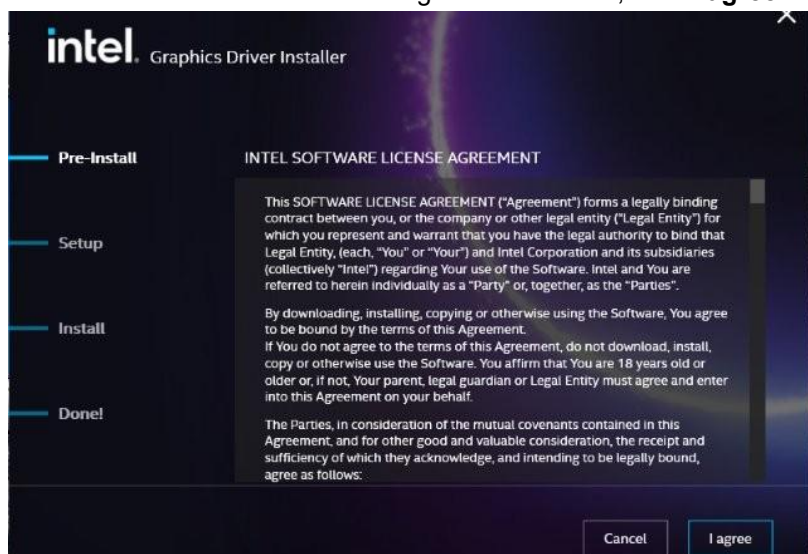
1. Click **Intel** and then **Intel(R) Alder-N/Amston/Twin Lake Chipset Driver**.
2. Click Intel(R) Alder-N/Amston/Twin Lake Graphics Drivers.



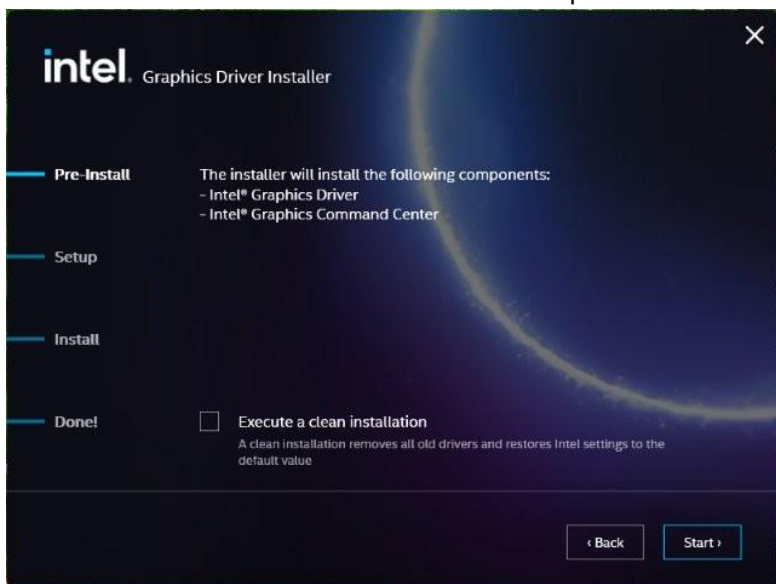
3. Click **Begin Installation**.



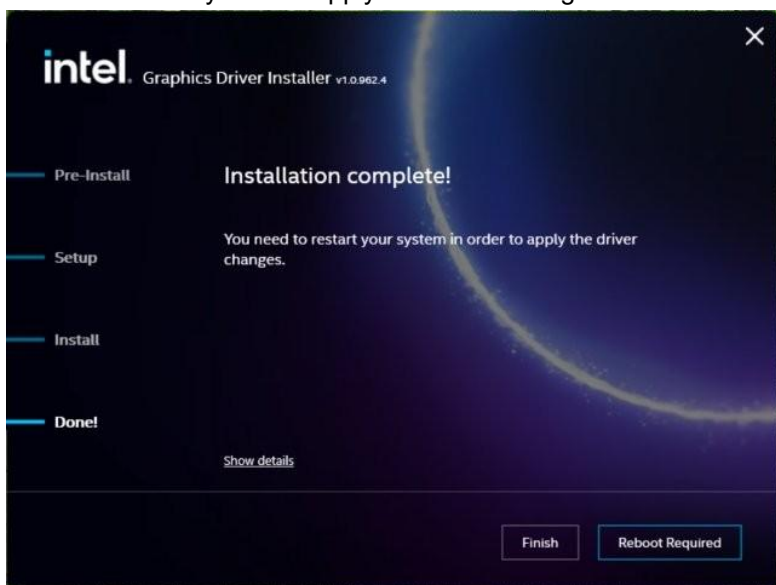
4. In the Intel Software License Agreement screen, click **I agree**.



5. Click **Start** for the installer to install the components.



6. Restart the system to apply the driver changes. Click Finish.



3.4 Realtek Audio Drivers Installation

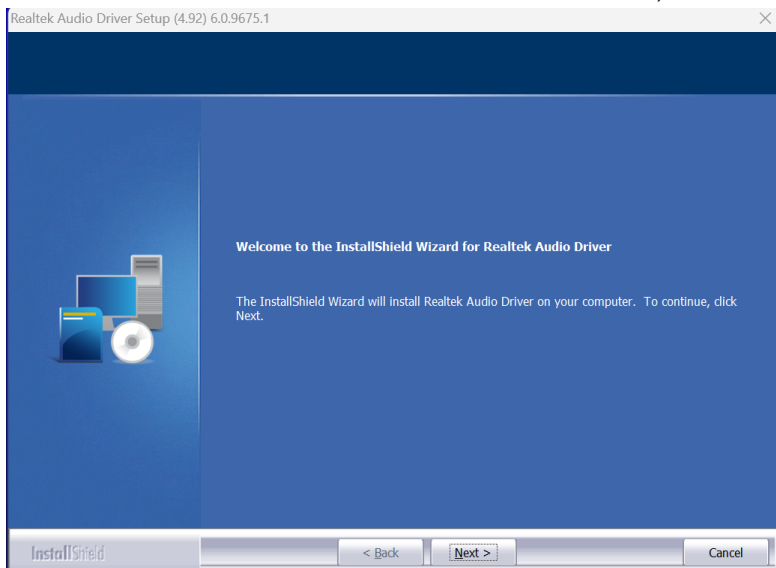
1. Click **Intel** and then **Intel(R) Alder-N/Amston/Twin Lake Chipset Driver**.
2. Click **Realtek Audio Drivers**.



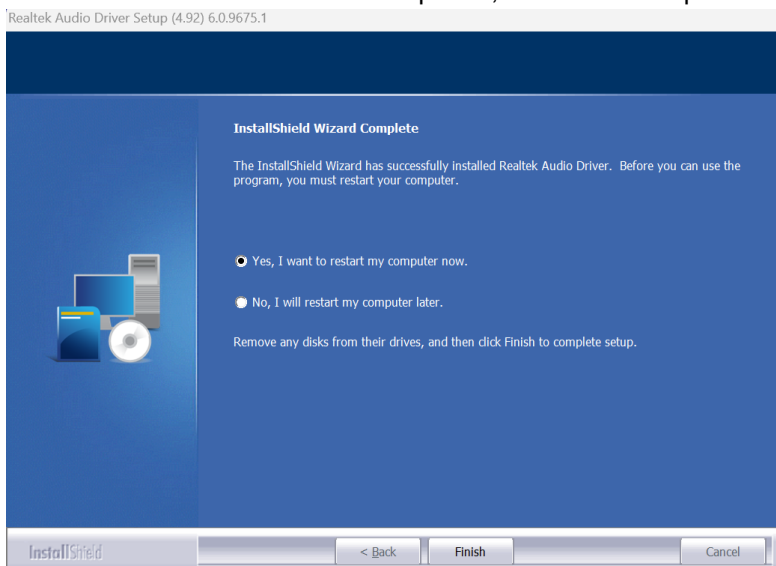
3. Click **Realtek Audio DCH Drivers**.



4. On the Welcome screen of the InstallShield Wizard, click Next.



5. After installation has been completed, restart the computer.



3.5 Intel 2.5G Network Drivers Installation

1. Click **Intel** and then **Intel(R) Alder-N/Amston/Twin Lake Chipset Driver**.
2. Click **Intel(R) 2.5G Network Drivers**.



3. For the installation steps, follow the instructions on the screen until installation is finished.



3.6 Intel® ME Drivers Installation

1. Click **Intel** and then **Intel(R) Alder-N/Amston/Twin Lake Chipset Driver**.
2. Click **Intel(R) ME Drivers**.



3. On the Welcome screen, click **Next**.
4. Accept the terms of the software license agreement and click **Next**.
5. Click **Next** to accept the destination folder or click **Change** to choose another destination folder.
6. Click **Finish** when you have installed the ME components.

You have successfully installed the following components:

- Intel® Management Engine Interface
- Intel® Dynamic Application Loader
- Intel® Trusted Connect Service

3.7 Intel® Serial IO Drivers Installation

1. Click **Intel** and then **Intel(R) Alder-N/Amston/Twin Lake Chipset Driver**.
2. Click **Intel(R) Serial IO Drivers**.

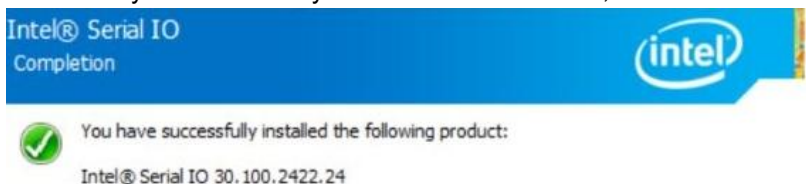


3. When the Welcome screen appears, click Next.

You are about to install the following product:

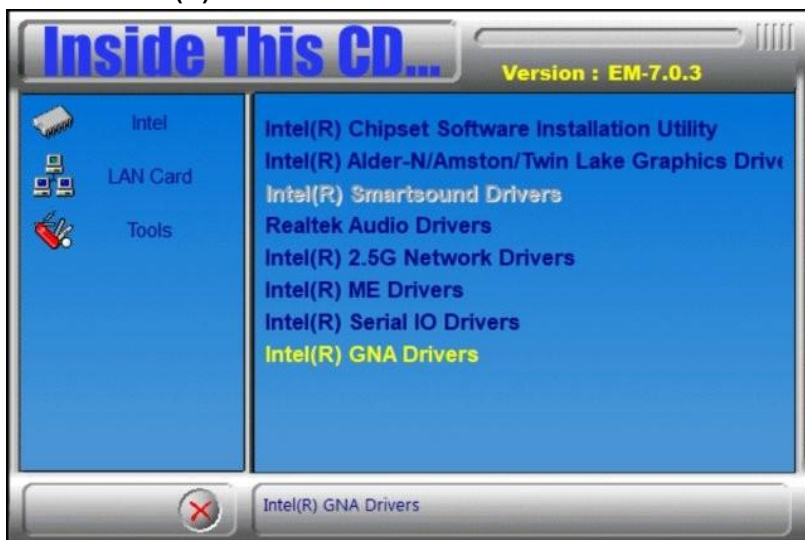
Intel® Serial IO 30.100.2422.24

4. Accept the terms in the license agreement and click Next.
5. In the Readme File Information screen, click Next.
6. When you successfully finished the installation, click Finish.



3.8 Intel® GNA Drivers Installation

1. Click **Intel** and then **Intel(R) Alder-N/Amston/Twin Lake Chipset Driver**.
2. Click **Intel(R) Other Drivers**.



3. Follow the on-screen instructions to complete the installation.



This page is intentionally left blank.

Chapter 4

BIOS Setup

This chapter describes the different settings available in the AMI BIOS that comes with the board. The topics covered in this chapter are as follows:

- Main Settings
- Advanced Settings
- Chipset Settings
- Security Settings
- Boot Settings
- Save & Exit

4.1 Introduction

The BIOS (Basic Input/Output System) installed in the ROM of your computer system supports Intel® processors. The BIOS provides critical low-level support for standard devices such as disk drives, serial ports and storage devices. It also provides password protection as well as special support for detailed fine-tuning of the chipset controlling the entire system.

4.2 BIOS Setup

The BIOS provides a Setup utility program for specifying the system configurations and settings. The BIOS ROM of the system stores the Setup utility. When you turn on the computer, the BIOS is immediately activated. Press the key immediately to enter the Setup utility. If you are a little bit late pressing the key, POST (Power On Self Test) will continue with its test routines, thus preventing you from invoking the Setup.

If you still need to enter Setup, restart the system by pressing the "Reset" button or simultaneously pressing the <Ctrl>, <Alt> and <Delete> keys. You can also restart by turning the system off and back on again.

The following message will appear on the screen:

```
Press <DEL> to Enter Setup
```

In general, press the arrow keys to highlight items, <Enter> to select, the <PgUp> and <PgDn> keys to change entries, <F1> for help, and <Esc> to quit.

When you enter the BIOS Setup utility, the *Main Menu will appear*. The Main Menu allows you to select from various setup functions and exit choices.

Warning: It is strongly recommended that you avoid making any changes to the chipset defaults.

These defaults have been carefully chosen by both AMI and your system manufacturer to provide the absolute maximum performance and reliability. Changing the defaults could make the system unstable and crash in some cases.

4.3 Main Settings



BIOS Setting	Description
System Date	Sets the date. Use the <Tab> key to switch between the Date elements.
System Time	Set the time. Use the <Tab> key to switch between the Time elements.

4.4 Advanced Settings

This section allows you to configure system features according to your preference.



4.4.1 CPU Configuration



BIOS Setting	Description
Efficient-core Information	Submenu displaying the E-core Information.
Intel (VMX) Virtualization Technology	When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.
Active Efficient-cores	Number of E-cores to enable in each processor package. Note: Number of Cores and E-cores are looked at together. When both are [0,0], Pcode will enable all cores.
AES	Enable/Disable AES (Advanced Encryption Standard).

4.4.2 Power & Performance



BIOS Setting	Description
Intel(R) SpeedStep(tm)	Allows more than two frequency ranges to be supported.
Intel(R) Speed Shift Technology	Enable/Disable Intel(R) Speed Shift Technology support. Enabling will expose the CPPC v2 interface to allow for hardware controlled P-states.

4.4.3 PCH-FW Configuration



Advanced		Aptio Setup - AMI
ME Firmware Version	16.50.15.1515	
ME Firmware Mode	Normal Mode	
ME Firmware SKU	Consumer SKU	

BIOS Setting	Options / Value
ME Firmware Version	16.50.15.1515
ME Firmware Mode	Normal Mode
ME Firmware SKU	Consumer SKU

4.4.4 Trusted Computing



BIOS Setting	Description
Security Device Support	Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.
SHA256/384 Bank	Enable or Disable PCR Bank.
Pending operation	Schedule an Operation for the Security Device. NOTE: Your computer will reboot during restart in order to change State of Security Device.
Platform/Storage / Endorsement Hierarchy	Enable or Disable Hierarchy.
Physical Presence Spec Version	Select to tell O.S. to support PPI Spec Version 1.2 or 1.3. Note: some HCK tests might not support 1.3.
Device Select	TPM 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.

4.4.5 ACPI Settings



BIOS Setting	Description
Enable Hibernation	Enables or Disables System ability to Hibernate (OS/S4 Sleep State). This option may not be effective with some operating systems. Options/Value: Disabled / Enabled (default: Enabled)
ACPI Sleep State	Select the highest ACPI sleep state the system will enter when the SUSPEND button is pressed. Options/Value: Suspend Disabled / S3 (Suspend to RAM) (default: S3)

4.4.6 F81966 Super IO Configuration

Serial Port 1~4 Configuration



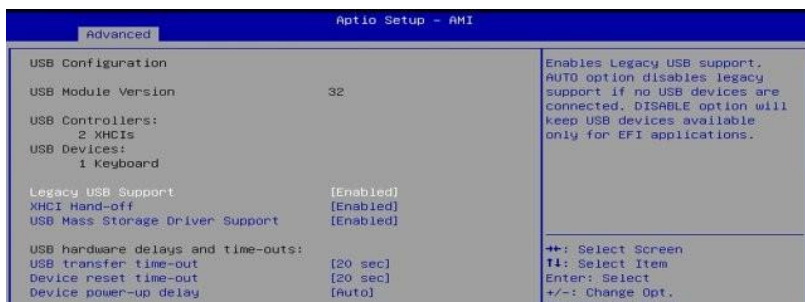
4.4.7 Hardware Monitor



Advanced		Aptio Setup - AMI	
Pc Health Status			
CPU temperature	:	+31 C	
System temperature	:	+31 C	
VCCORE	:	+1.032 V	
Memory Voltage	:	+1.072 V	
VCC3V	:	+3.328 V	

BIOS Setting	Description
Temperatures / Voltages	These fields are the parameters of the hardware monitoring function feature of the motherboard. The values are read-only values as monitored by the system and show the PC health status.

4.4.8 USB Configuration



BIOS Setting	Description
Legacy USB Support	Enables Legacy USB support. AUTO option disables legacy support if no USB devices are connected. DISABLE option will keep USB devices available only for EFI applications.
XHCI Hand-off	This is a workaround for OSES without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.
USB Mass Storage Driver Support	Enable/Disable USB Mass Storage Driver Support.
USB transfer time-out	The time-out value for Control, Bulk, and Interrupt transfers. Options: 1 sec / 5 sec / 10 sec / 20 sec (default: 20 sec)
Device reset time-out	USB mass storage device Start Unit command time-out. Options: 10 sec / 20 sec / 30 sec / 40 sec (default: 20 sec)
Device power-up delay	Maximum time the device will take before it properly reports itself to the Host Controller. 'Auto' uses default value: for a Root port it is 100 ms, for a Hub port the delay is taken from Hub descriptor.

4.4.9 Network Stack Configuration

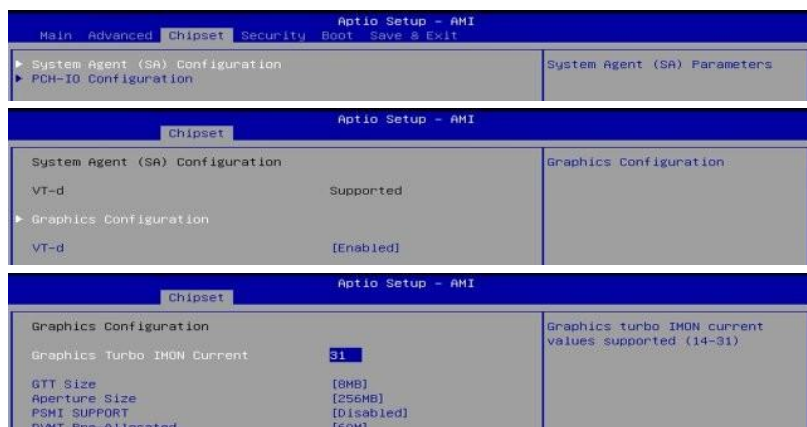


BIOS Setting	Description
Network Stack	Enable/Disable UEFI Network Stack
IPv4 PXE Support	If disabled, IPv4 PXE boot support will not be available.
IPv4 HTTP Support	If disabled, IPv4 HTTP boot support will not be available.
IPv6 PXE Support	Enable/Disable IPv6 support. If disabled, IPv6 support will not be available.
IPv6 HTTP Support	If disabled, IPv6 HTTP boot support will not be available.
PXE boot wait time	Wait time in seconds to press ESC key to abort the PXE boot. Use either +/- or numeric keys to set the value
Media detect count	Number of times the presence of media will be checked. Use either +/- numeric keys to set the value.

4.4.10 NVMe Configuration

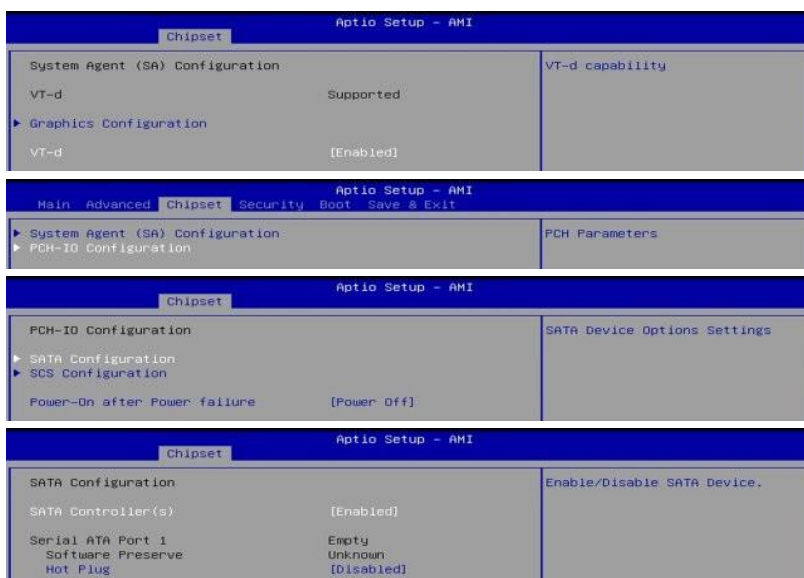


4.5 Chipset Settings



Graphics Configuration (submenu)

BIOS Setting	Description
Graphics Turbo IMON Current	Graphics turbo IMON current values supported (14–31). (default: 31)
GTT Size	Select the GTT Size. Options: 2MB / 4MB / 8MB (default: 8MB)
Aperture Size	Select the Aperture Size. Note: Above 4GB MMIO BIOS assignment is automatically enabled when selecting > 2048MB aperture. To use this feature, please disable CSM Support. Options: 128MB / 256MB / 512MB / 1024MB (default: 256MB)
PSMI SUPPORT	PSMI Enable/Disable.
DVMT Pre-Allocated	Select DVMT 5.0 Pre-Allocated (Fixed) Graphics Memory size used by the Internal Graphics Device. Options: 0M–160M range in fixed steps (default: 60M)



SATA Configuration (submenu)

BIOS Setting	Description
SATA Controller(s)	Enable/Disable SATA Device.
Serial ATA Port 1	Info only.
→ Software Preserve	Info only.
→ Hot Plug	Designates this port as Hot Pluggable.



SCS Configuration (submenu)

BIOS Setting	Description
eMMC 5.1 Controller	Enable or Disable SCS eMMC 5.1 Controller.
eMMC 5.1 HS400 Mode	Enable or Disable SCS eMMC 5.1 HS400 Mode.
Enable HS400 software tuning	Software tuning should improve eMMC HS400 stability at the expense of boot time.
Driver Strength	Sets I/O driver strength.
UFS 2.0 Controller 1	Enable or Disable UFS 2.0 Controller.
Power-On after Power failure	Specify what state to go to when power is re-applied after a power failure (G3 state).

4.6 Security Settings



BIOS Setting	Description
Setup Administrator Password	Sets an administrator password for the setup utility.
User Password	Sets a user password.
Secure Boot	Secure Boot feature is Active if Secure Boot is enabled. Platform Key(PK) is enrolled and the system is in user mode. The mode change requires platform reset.
Secure Boot Mode	Secure Boot mode options: Standard or Custom. In Custom mode, Secure Boot Policy variables can be configured by a physically present user without full authentication.
Restore Factory Keys	Forces system to user mode. Install factory default Secure Boot key databases.
Reset to Setup Mode	Delete all Secure Boot key databases from NVRAM
Expert Key Management	Enables expert users to modify Secure Boot Policy variables without variable authentication.

Aptio Setup - AMI		
Security		
System Mode	User	Secure Boot feature is Active if Secure Boot is Enabled, Platform Key(PK) is enrolled and the System is in User-mode. The mode change requires platform reset
Secure Boot	[Disabled] Not Active	
Secure Boot Mode	[Standard]	
▶ Restore Factory Keys		
▶ Reset To Setup Mode		
▶ Expert Key Management		

Aptio Setup - AMI		
Security		
Vendor Keys	Valid	Install factory default Secure Boot keys after the platform reset and while the System is in Setup mode
Factory Key Provision	[Enabled]	
▶ Restore Factory Keys		
▶ Reset To Setup Mode		
▶ Enroll Efi Image		
▶ Export Secure Boot variables		
Secure Boot variable Size Keys Key Source		
▶ Platform Key (PK) 1575 1 Factory		
▶ Key Exchange Keys (KEK) 3066 2 Factory		
▶ Authorized Signatures (db) 7636 5 Factory		
▶ Forbidden Signatures (dbx) 17836 371 Factory		
▶ Authorized TimeStamps (dbt) 0 0 No Keys		
▶ OsRecovery Signatures (dbr) 0 0 No Keys		
++: Select Screen		
F4: Select Item		
Enter: Select		

BIOS Setting	Description
Factory Key Provision	Install factory default Secure Boot keys after the platform reset and while the System is in Setup mode.
Restore Factory Keys	Force System to User Mode. Install factory default Secure Boot key databases.
Reset To Setup Mode	Delete all Secure Boot key databases from NVRAM.
Enroll EFI Image	Allow EFI image to run in Secure Boot mode. Enroll SHA256 Hash certificate of a PE image into Authorized Signature Database (db).
Export Secure Boot Variables	Save NVRAM content of Secure Boot variable to a file.
Platform Key (PK) Key Exchange Keys (KEK) Authorized Signatures (db) Forbidden Signatures (dbx) Authorized TimeStamps (dbt) OsRecovery Signatures (dbr) Device Signatures (devdb)	Enroll Factory Defaults or load keys from file: 1. Public key Certificate: a) EFI_SIGNATURE_LIST b) EFI_CERT_X509 (DER) c) EFI_CERT_RSA2048 (bin) d) EFI_CERT_SHAxXX 2. Authenticated UEFI Variable 3. EFI PE/COFF Image (SHA256) Key Source: Factory, Modified, Mixed

4.7 Boot Settings



BIOS Setting	Description
Setup Prompt Timeout	Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting.
Bootup NumLock State	Selects the keyboard NumLock state.
Quiet Boot	Enables / Disables Quiet Boot option.
FIXED BOOT ORDER Priorities	Sets the system boot order.

4.8 Save & Exit Settings



BIOS Setting	Description
Save Changes and Exit	Exits system setup after saving the changes.
Discard Changes and Exit	Exits system setup without saving any changes.
Save Changes and Reset	Resets the system after saving the changes.
Discard Changes and Reset	Resets system setup without saving any changes.
Save Changes	Saves changes done so far to any of the setup options.
Discard Changes	Discards changes done so far to any of the setup options.
Restore Defaults	Restores / Loads default values for all the setup options.
Save as User Defaults	Saves the changes done so far as User Defaults.
Restore User Defaults	Restores the user defaults to all the setup options.
Launch EFI Shell from filesystem device	Attempts to launch EFI shell application (Shell.efi) from one of the available filesystem devices.

Appendix

This section provides information on:

- A. I/O Port Address Map
- B. Interrupt Request Lines (IRQ)

A. I/O Port Address Map

Address	Device Description
0x00000A00-0x00000A0F	Motherboard resources
0x00000A10-0x00000A1F	Motherboard resources
0x00000A10-0x00000A1F	Motherboard resources
0x0000002E-0x0000002F	Motherboard resources
0x0000004E-0x0000004F	Motherboard resources
0x00000061-0x00000061	Motherboard resources
0x00000063-0x00000063	Motherboard resources
0x00000065-0x00000065	Motherboard resources
0x00000067-0x00000067	Motherboard resources
0x00000070-0x00000070	Motherboard resources
0x00000080-0x00000080	Motherboard resources
0x00000092-0x00000092	Motherboard resources
0x000000B2-0x000000B3	Motherboard resources
0x00000680-0x0000069F	Motherboard resources
0x0000164E-0x0000164F	Motherboard resources
0x00000040-0x00000043	System timer
0x00000050-0x00000053	System timer
0x000003F8-0x000003FF	Communications Port (COM1)
0x000002F8-0x000002FF	Communications Port (COM2)
0x000003E8-0x000003EF	Communications Port (COM3)
0x000002E8-0x000002EF	Communications Port (COM4)
0x0000EFA0-0x0000EFBF	SMBus - 54A3
0x00001854-0x00001857	Motherboard resources
0x00000000-0x00000CF7	PCI Express Root Complex
0x00000D00-0x0000FFFF	PCI Express Root Complex
0x00003090-0x00003097	Standard SATA AHCI Controller
0x00003080-0x00003083	Standard SATA AHCI Controller
0x00003060-0x0000307F	Standard SATA AHCI Controller
0x00003000-0x0000303F	Intel(R) UHD Graphics
0x00002000-0x000020FE	Motherboard resources
0x00000020-0x00000021	Programmable interrupt controller
0x00000024-0x00000025	Programmable interrupt controller
0x00000028-0x00000029	Programmable interrupt controller
0x0000002C-0x0000002D	Programmable interrupt controller
0x00000030-0x00000031	Programmable interrupt controller
0x00000034-0x00000035	Programmable interrupt controller
0x00000038-0x00000039	Programmable interrupt controller
0x0000003C-0x0000003D	Programmable interrupt controller
0x000000A0-0x000000A1	Programmable interrupt controller
0x000000A4-0x000000A5	Programmable interrupt controller
0x000000A8-0x000000A9	Programmable interrupt controller
0x000000AC-0x000000AD	Programmable interrupt controller

B. Interrupt Request Lines (IRQ)

Peripheral devices use interrupt request lines to notify CPU for the service required. The following table shows the IRQ used by the devices on board.

Level	Function
IRQ 4294967293	Intel(R) USB 3.20 eXtensible Host Controller - 1.20 (Microsoft)
IRQ 0	System timer
IRQ 4294967291	Intel(R) Management Engine Interface #1
IRQ 4	Communications Port (COM1)
IRQ 3	Communications Port (COM2)
IRQ 5	Communications Port (COM3)
IRQ 6	Communications Port (COM4)
IRQ 19	High Definition Audio Controller
IRQ 16	Intel(R) Serial IO UART Host Controller - 54A8
IRQ 16	Intel SD Host Controller
IRQ 55-204	Microsoft ACPI-Compliant System
IRQ 256-511	Microsoft ACPI-Compliant System
IRQ 4294967294	Standard SATA AHCI Controller
IRQ 4294967290	Intel(R) UHD Graphics
IRQ 4294967292	Intel(R) USB 3.10 eXtensible Host Controller - 1.20 (Microsoft)
IRQ 14	Intel(R) Serial IO GPIO Host Controller - INTC1057
IRQ 1	Standard PS/2 Keyboard
IRQ 12	Microsoft PS/2 Mouse