MPT-8000RH
Intelligent Railway Computer System

User's Manual

Version 1.0
(December 2022)

iBASE

iBASE

Copyright

Disclaimer

Trademarks

Compliance

This product has passed CE tests for environmental specifications and limits in accordance with the directives of the Union European (EU). If users modify and/or install other devices in this equipment, the CE conformity declaration may no longer apply.

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 the 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 of 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 is compliant with the current RoHS restrictions that prohibits the use of the following substances in concentrations exceeding 0.1% by weight (1000 ppm) except for cadmium, limited to 0.01% by weight (100 ppm).

- Lead (Pb)
- Mercury (Hg)
- Cadmium (Cd)
- Hexavalent chromium (Cr6+)
- Polybrominated biphenyls (PBB)
- Polybrominated diphenyl ether (PBDE)

iBASE

Important Safety Information

Carefully read the precautions before using the device.

Environmental conditions:

- Lay the device horizontally on a stable and solid surface in case the device may fall, causing serious damage.
- Leave plenty of space around the device and do not block the openings for ventilation. NEVER DROP OR INSERT ANY OBJECTS OF ANY KIND INTO THE VENTIILATION OPENINGS.
- Slots and openings on the chassis are for ventilation. Do not block or cover these openings. Make sure you leave plenty of space around the device for ventilation.
- Use this product in environments with ambient temperatures between -40°C and 70°C for SSD, and between -25°C and 55°C for HDD.
- DO NOT LEAVE THIS DEVICE IN AN ENVIRONMENT WHERE THE STORAGE TEMPERATURE MAY GO BELOW -40°C OR ABOVE 85°C. This could damage the device. The device must be used in a controlled environment.

Care for your IBASE products:

- Before cleaning the device, turn it off and unplug all cables such as power in case a small amount of electrical current may still flow.
- Use neutral cleaning agents or diluted alcohol to clean the device chassis with a cloth. Then wipe the chassis with a dry cloth.
- Vacuum the dust with a computer vacuum cleaner to prevent the air vent or slots from being clogged.

⚠ WARNING

Attention during use:

- Do not use this product near water.
- Do not spill water or any other liquids on your device.
- Do not place heavy objects on the top of the device.
- Operate this device from the type of power indicated on the marking label. If you are not sure of the type of power available, consult your distributor or local power company.
- If you use an extension cord, make sure that the total ampere rating of the product plugged into the extension cord does not exceed its limits.

Avoid Disassembly

You are not suggested to disassemble, repair or make any modification to the device. Disassembly, modification, or any attempt at repair could generate hazards and cause damage to the device, even bodily injury or property damage, and will void any warranty.

 CAUTION

Danger of explosion if internal lithium-ion battery is replaced by an incorrect type. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

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:**

  12-month (1-year) warranty from delivery for the 3ʳᵈ-party parts that are not manufactured by IBASE, such as CPU, memory, HDD, power adapter, panel and touchscreen.

∗ PRODUCTS, HOWEVER, THAT FAILS DUE TO MISUSE, ACCIDENT, IMPROPER INSTALLATION OR UNAUTHORIZED REPAIR SHALL BE TREATED AS OUT OF WARRANTY AND CUSTOMERS SHALL BE BILLED FOR REPAIR AND SHIPPING CHARGES.

Technical Support & Services

1. Visit the IBASE website at www.ibase.com.tw to find the latest information about the product.
2. If the product does not function properly, prepare the following information before contacting the distributor or sales representative:

   - Product model name
   - Product serial number
   - Detailed description of the problem
   - The error messages in text or in screenshots if there is any
   - The arrangement of the peripherals
   - Software in use (such as OS and application software, including the version numbers)

3. If repair service is required, you can download the RMA form at http://www.ibase.com.tw/english/Supports/RMAService/. Fill out the form and contact your distributor or sales representative.

iBASE

Table of Contents

iBASE

Chapter 1
General Information

The information provided in this chapter includes:

- Features
- Packing List
- Specifications
- Product View
- Dimensions

iBASE

1.1 Introduction

The MPT-8000RH is an embedded computer designed for railway applications. compliant. It is powered by 10th Gen Intel® Core™ Desktop processors with robust M12 connectors and operating temperatures from ranging from -10°C and up to 60°C to provide reliable performance in high-speed, rugged environments.

MPT-8000RH

1.2 Features

- EN50155 (2021) / EN45545-2 certified
- AI solution for Transportation
- Supports 10th Gen Intel® Core™ Desktop processors
- Up to 10x GbE ports (8x with PoE capability)
- Optional 10G LAN
- Supports Intel® Movidus Vision Acceleration M.2 modules
- Supports Wi-Fi 6 CNVi, dual WWAN channels, RAID 0/1/5
- 1x USB Type-C with graphics output for quick setting and diagnostics

1.3   Packing List

Your product package should include the items listed below. If any of the items below is missing, contact the distributor or the dealer from whom you purchased the product.

Item		Q'ty	IBASE P/N
MPT-8000RH		1	- -
Mounting Bracket		2	- -
Screw for M.2 Socket		3	H0230321112200000P
Screw for M.2 & Mini PCIe Socket		3	H02203511122000N0P
Screw fo Mounting Bracket		10	H0240861012200B00P
Screw for 2.5 "SSD (if not pre-installed)		8	H0230561B710BN000P
Main Power In Connector		1	A017FWIBS36000100P
Backup Power In Connector		1	A017FWIBS36100100P
Screw for Power In Connector		2	H0230461012200A00P

iBASE

1.4 Specifications

Product Name	MPT-8000RH
Motherboard	MBT- 8000RW
Intel® CPU*	10th Gen Intel® Core™ Desktop processors
Memory	2x DDR4-2666 SO-DIMM, 2x 8GB (default) Maximum size supported: 128GB

Front Panel External I/O	• 2x Accessible 2.5" device bay (SSD/HDD)
	• 2x M12 X-code 8-pin for GbE LAN, isolated
	• 1x M12 4-pin A-code for USB 2.0, isolated
	• 1x M12 4-pin A-code for USB 1.1, isolated
	• 1x 3.5mm pink audio connector for MIC-Input
	• 1x 3.5mm blue audio connector for Line in
	• 4x SMA Antenna holes with cap
	• 2x PCI-Ex4 card slots for IDT8102/IDT 7204 (With cover when empty)
	  - IDT8102: 2x 10G LAN card
	  - IDT7204: 4x 1G PoE card
	• 2x External accessible SIM socket 1x Micro SD card socket
	• 1x Recessed Access Tach-switch for System Reset
	• 1x USB type-C with graphics (No PD function)
	• 1x USB3.2 Gen.2 type-A Indicators: Four light-pipe for four status LED
	  - 1x 0402 SMT green LED for power status
	  - 1x 0402 SMT white LED for storage activity status
	  - 1x 0402 SMT blue LED for WLAN activity status
	  - 1x 0402 SMT amber LED for WWAN activity
	  - 2x 0402 SMT green LED, programmable

Rear I/O	• 1x Main power input, Staubli connector • 2x Removable with screw lock FUSE holder • 1x Backup power source, 24VDC only • 1x DVI-D output 1x HDMI output • 1x USB3.2 Gen.1 type-A • 1x 3.5mm green audio connector for Line-out 1x Male DSUB9 for RS-485, isolated • 1x Male DSUB9 connector for RS-232/485, isolated • 1x Female DSUB9 for 8x DO and ground by cable, isolated • 1x Female DSUB9 for 8x DI and ground by cable, isolated • 1x M4 with washer screw hole for grounding connection • 4x SMA Antenna holes with cap

Storage	• 2x 2,5" Removable device bay for SSD devices • 2x M.2 M-key SSD devices RAID 0/1/5 supported, Max. 4x SATA devices
Expansion Slot	• 1x mPCI-E full/half-size socket • 1x 3042/52 M.2 B-Key socket for WWAN (supports SIM1) This socket comes with USB2.0/3.0/PCI-Ex1 interface • 1x 3042/52 M.2 B-Key socket for WWAN (supports SIM2) This M.2 socket comes with USB2.0/PCI-Ex1 interface • 1x 2242/80 M.2 M-key socket for SSD/VPU/WLAN card • 1x 2242/80 M.2 M-key socket for SSD/VPU/WLAN card (NVMe supported) • 1x 2230 M.2 E-Key socket for WLAN (CNVi supported)
Power Supply	• 24V/72V/110VDC • Backup Power: 24V DC (When main power is not used, 24V backup power is automatically used)

Mechanical	
Construction	Metal, black
Mounting	19" Rack mount
Dimensions	482 (W) x 308 (D) x 132 (H) mm 18.97" (W) x 12.13" (D) x 5.2" (H)
Environmental	
Humidity	10 ~ 95% @ 45°C, (non-condensing)
Temperature	Operating Temperature: -10°C ~60°C Storage Temperature: -40°C ~ 85°C
Shock	EN61373
Vibration	EN61373
Standards	
Certification	• EN50155: 2021 • EN45545-2 • CE/FCC class-A
Operating System	● Windows 10 ● Linux kernel 3.8.0 or above (64 bits)

All specifications are subject to change without prior notice.

iBASE

1.5 Product View

Front View

No.	Name	No.	Name
1	Reset, SIM, SD, DP, USB	7	Two USB Ports (M12)
2	LEDs for P2, P1, SIM, WiFi, HDD, Power	8	Two LAN Ports (M12)
3		9	Slots for PoE Connectors(option)*
4	Four Antenna Connectors	A	Two Slots for 2.5" SSD Storage
5	Audio Line In / Line Out	B	Reserved Expansion
6	LEDs for LAN1, LAN2		

*Up to eight PoE connectors can be supported in RJ45 or M12 types

Rear View

No.	Name	No.	Name
1	Four Antenna Connectors	6	Digital I/O Connectors
2	72~110V DC Input (Main Power)	7	USB 3.0 ports (CN3)
3	24V Backup Power	8	DVI-D Port (CN4)
4	Fuse for Main and Backup Power	9	HDMI Port (CN5)
5	COM1 and COM2 (CN1, CN2)	A	Line-Out (CN6) & Ground

1.6   Dimensions

Unit: mm

Unit: mm
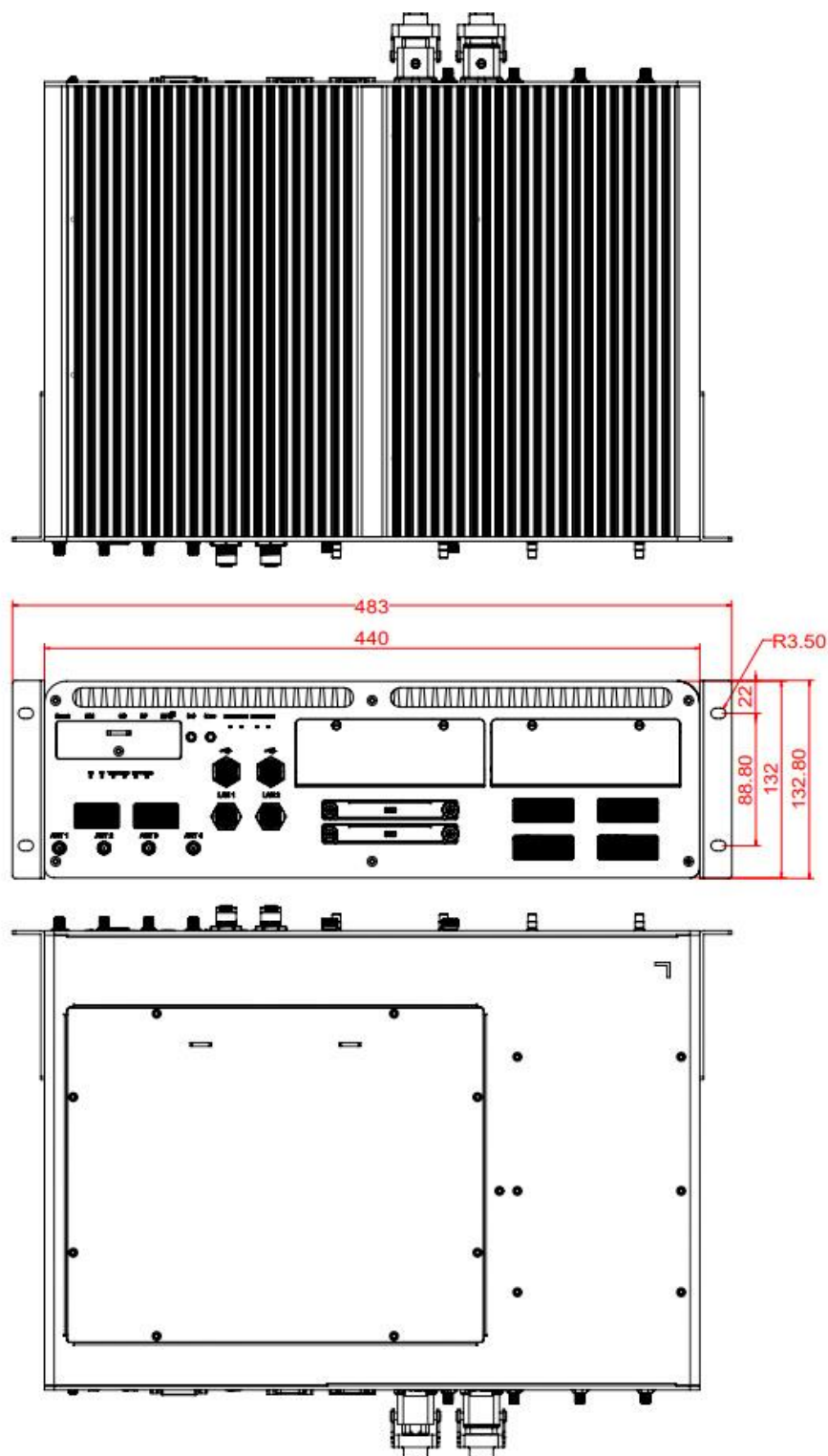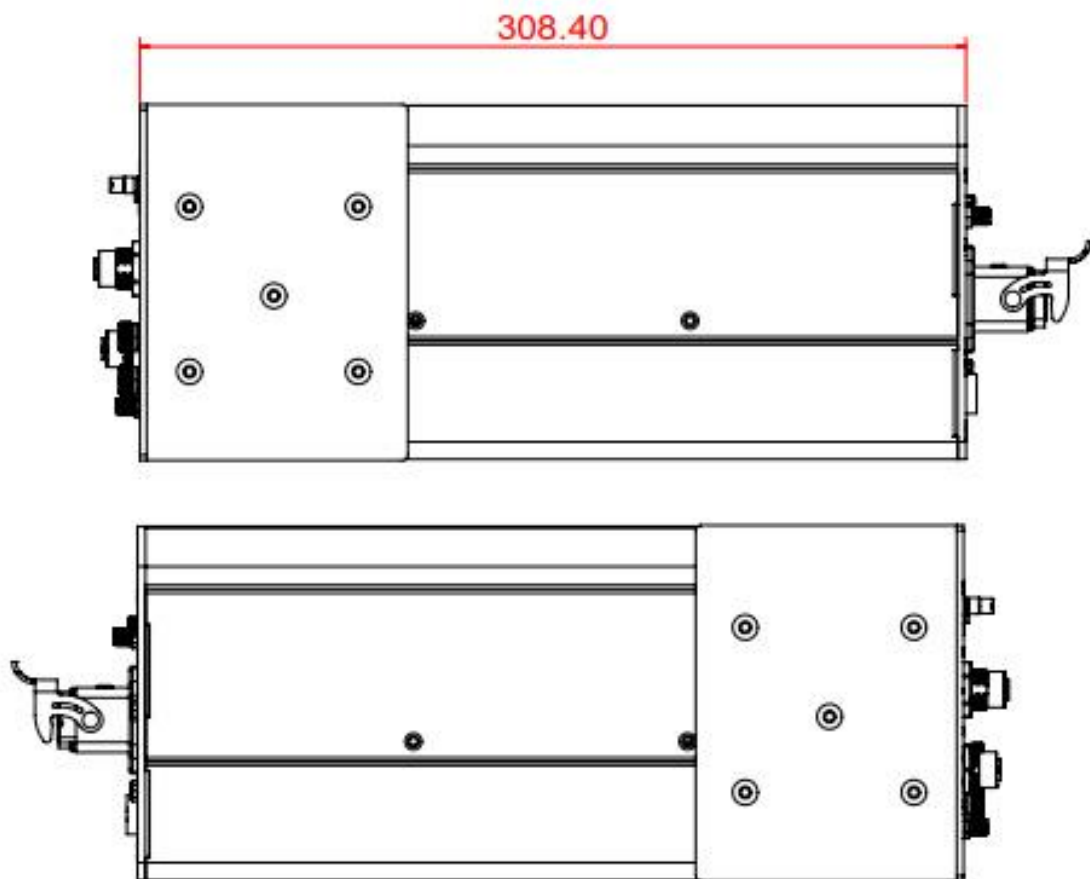
Chapter 2
Hardware Configuration

The information provided in this chapter includes:

- Essential installations
- Switches, Jumpers & Connectors

iBASE

2.1 Essential Installations

2.1.1 CPU Installation

1. Unlock the CPU socket by pressing the lever sideways, then lift up the lever and the metal lid.Position the CPU above the socket such that the CPU corner aligns with the gold triangle matching the socket corner with a small triangle.

2. Carefully insert the CPU into the socket and push down the lever to secure the CPU. Then install the CPU cooler and fan back.

Note: Ensure that the CPU cooler and the CPU top surface are in total contact to avoid overheating problems.

2.1.2   Memory Installation

To install the modules, locate the memory slot on the board as shown below.
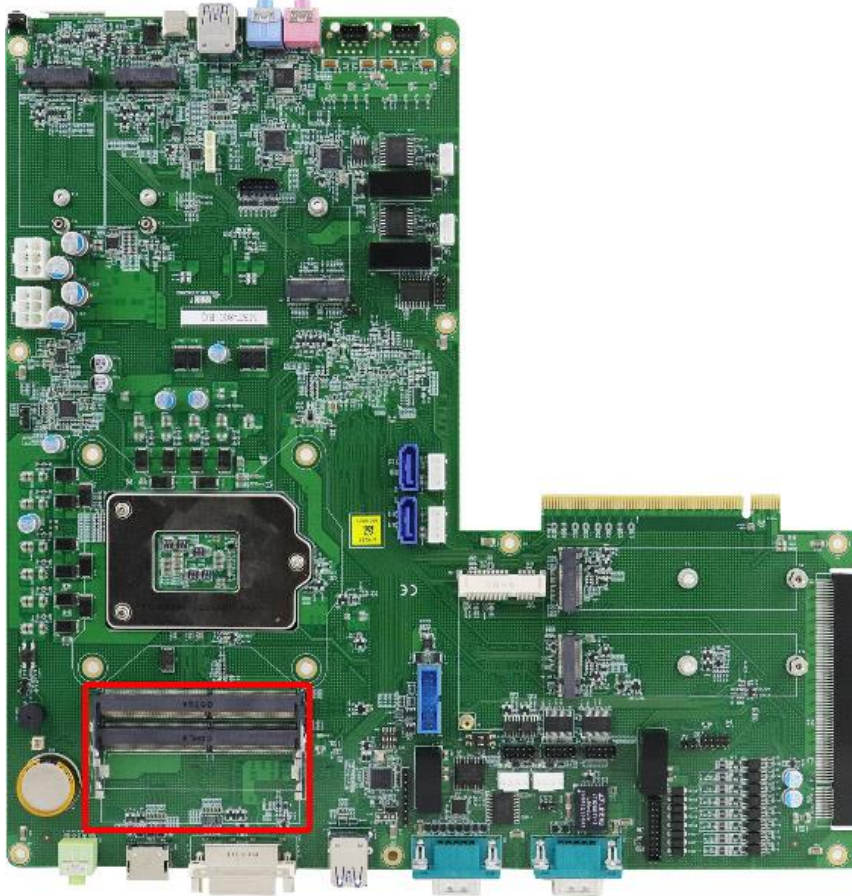
Perform the following steps:
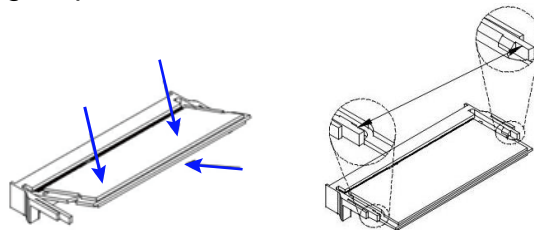
1. Align the key of the memory module with that on the memory slot and insert the module slantwise.
2. Gently push the module in an upright position until the clips of the slot close to hold the module in place when the module touches the bottom of the slot.

To remove the module, press the clips outwards with both hands, and the module will pop-up.

iBASE

2.1.3   Installation of 2.5" SSD Storage

There are two slots for 2.5" SSD drives that are externally accessible as shown in the picture below. Release the screws and pull out the SSD tray to install the SSD drive.
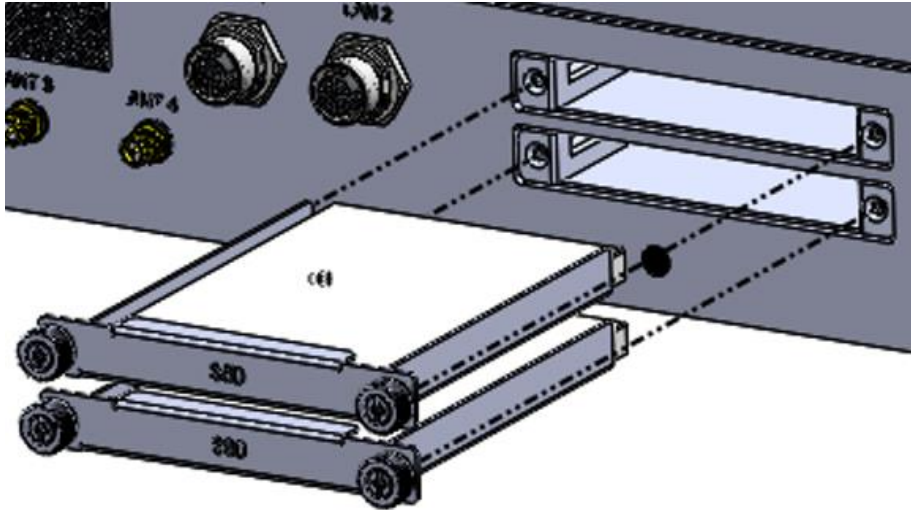
2.1.4   Installation of M.2 Cards and mPCIe Cards

MPT-8000RH supports several M.2 cards including:
- Two M keyed (2280) for SSD storage
- One E keyed (2230) for WiFi card
- Two B keyed (3042/3052) for 4G/5G cards

To access their sockets, remove the eight (8) screws shown below.
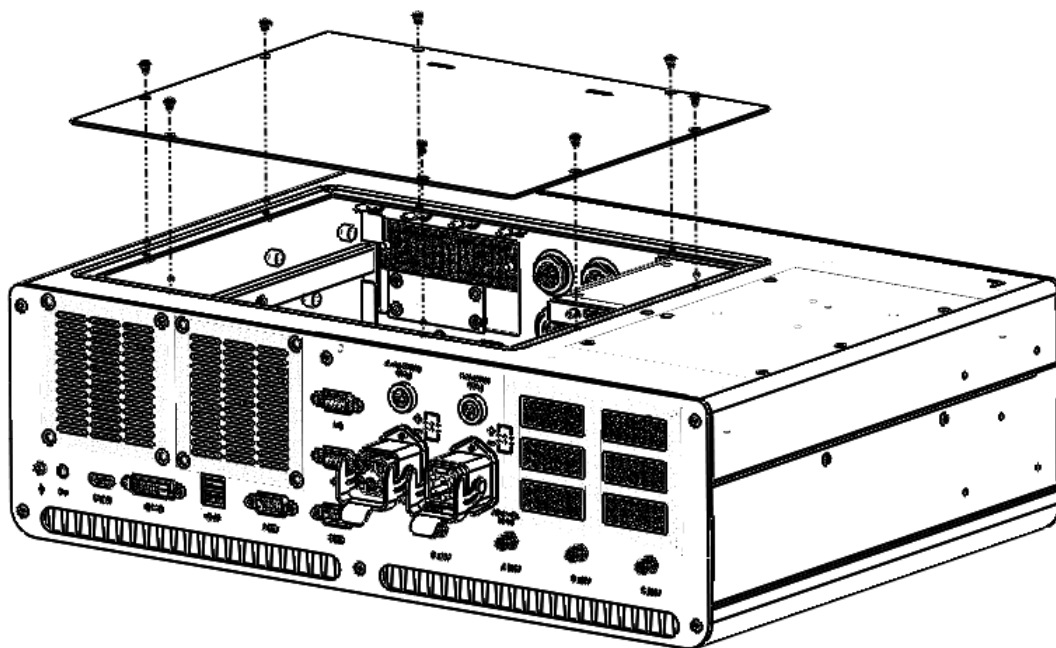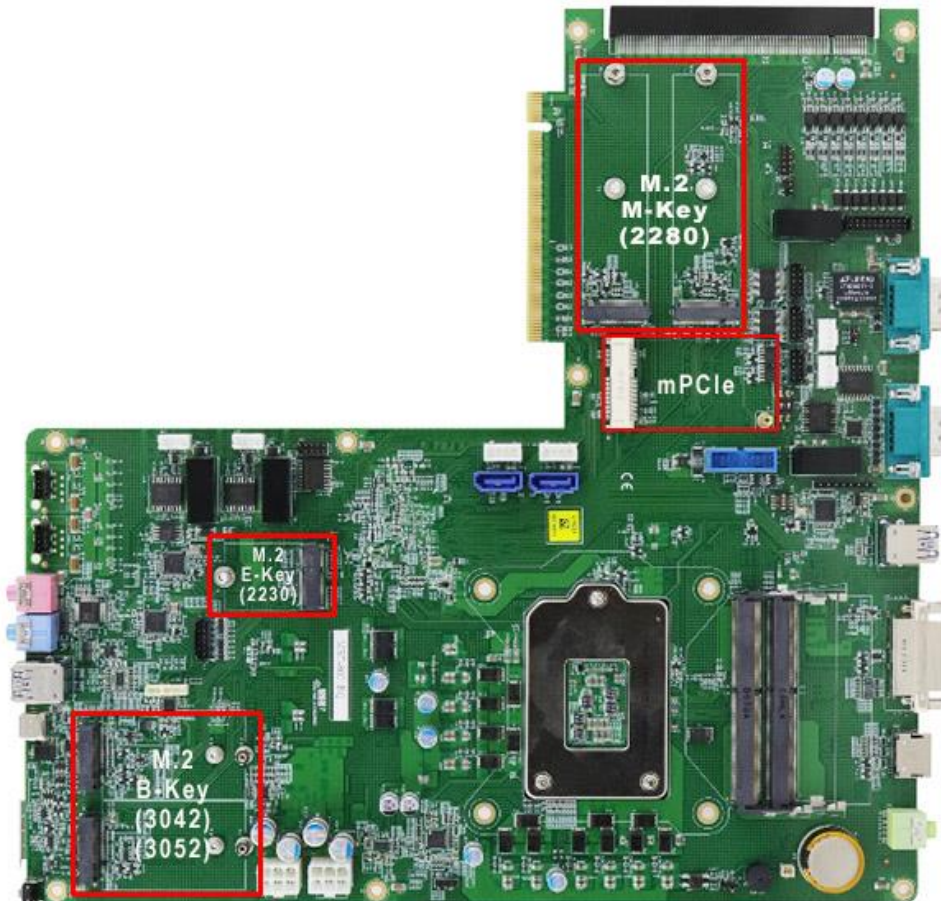
To install or replace a card, align the key of the card to the interface, and insert the card slantwise. Push the card down and fix it with a flat head screw.

iBASE
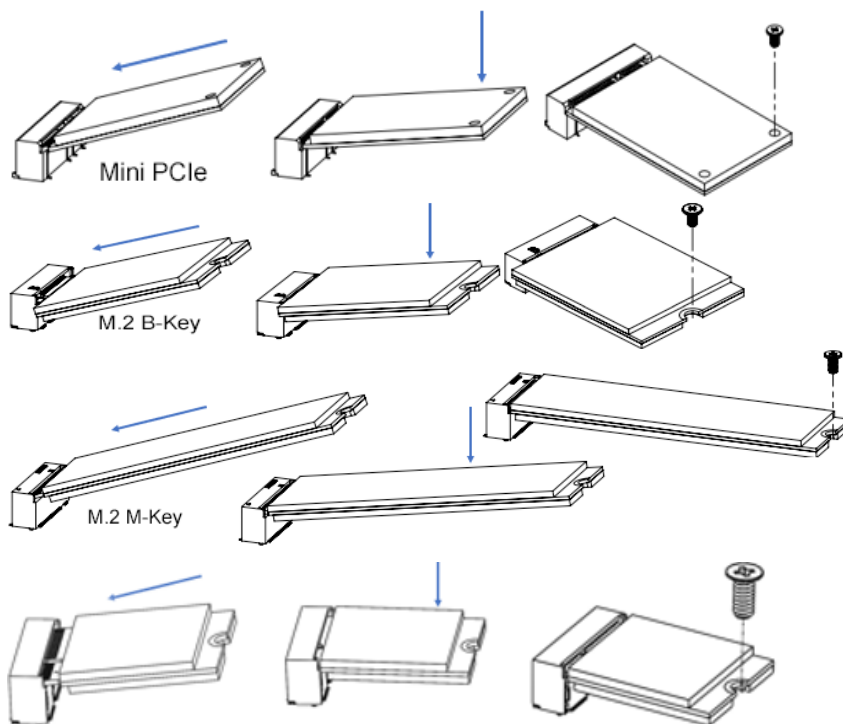
2.1.5   Front Panel Installation

There are several functions located on the upper left corner of the front panel that include Reset, SIM, SD Card, DP Display, and USB Port. To access these functions, remove the single screw fixing the cover as shown below.
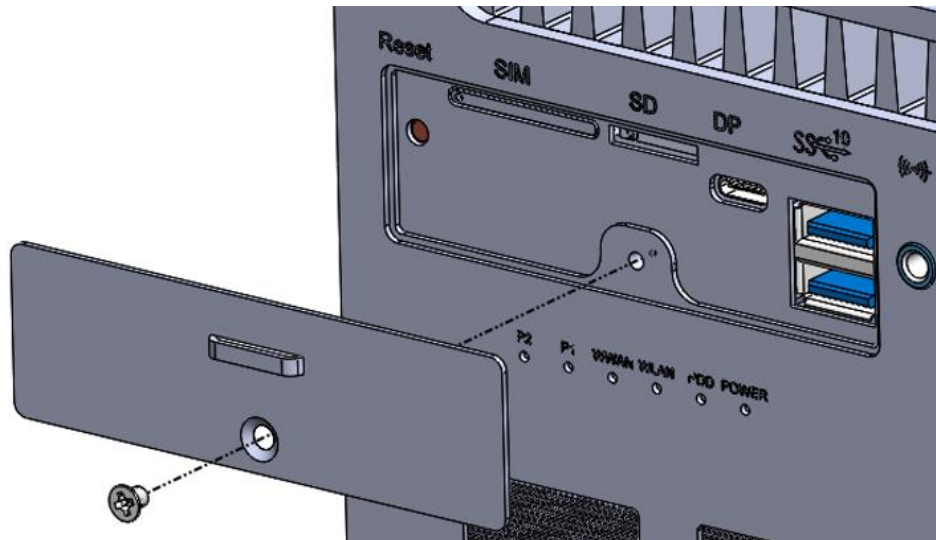
2.1.6   Antenna Installation

Thread the antenna extension cable through the antenna connectors in the system. Fasten the antenna as shown below and apply adhesive to the edge of the hex nut to prevent the extension cable from falling off.

1. Thread and fasten the hex nut and the washer. Then install the antenna.

2. Apply adhesive around here.
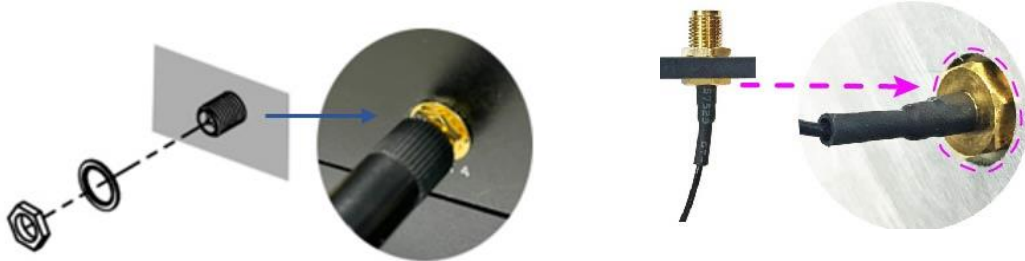
Info: The diameter of the nut is around 6.35 mm (0.25"-36UNC).

There are a total of eight (8) antennas in the system.

2.1.7　Mounting Brackets Installation

1. Turn your MPT-8000RH upside down to attach the mounting brackets and secure the brackets with the supplied screws as shown below.
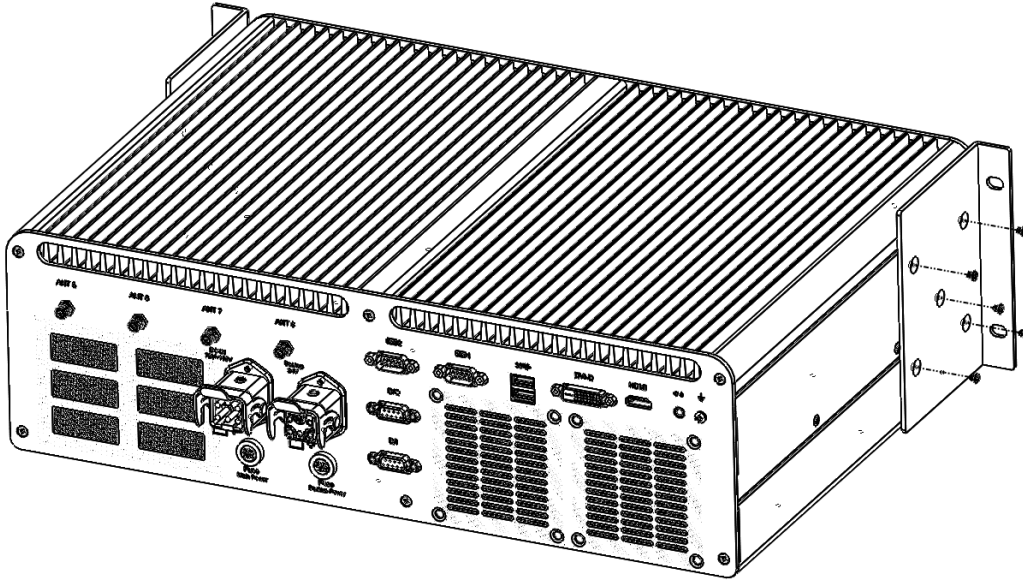
Rack Mount H0240861012200B00P-M4 Screw
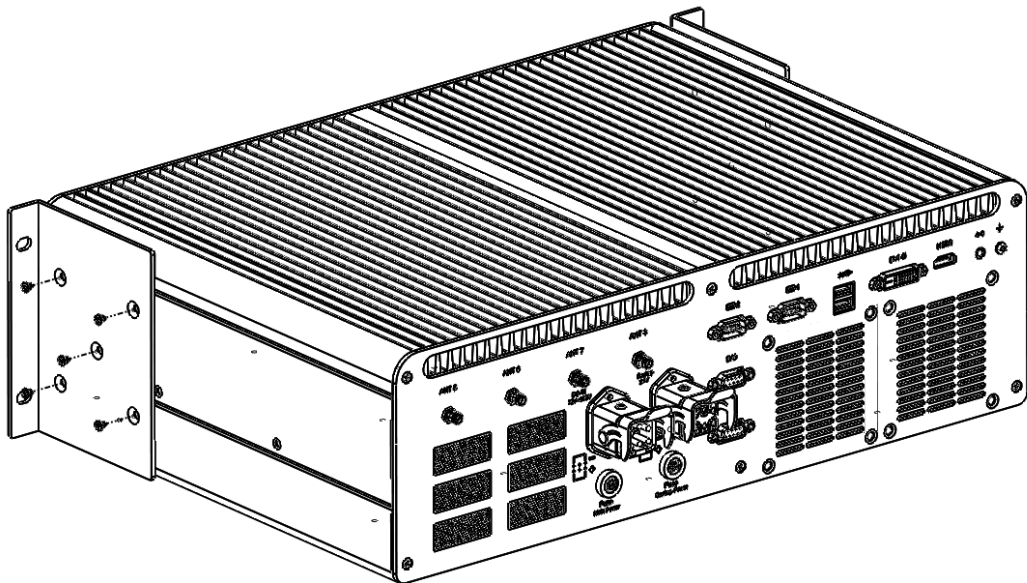
2.1.8   M12 Connectors (USB 2.0, LAN)

- **USB 1.1/2.0 Port (M12, 4-pin female A-code)**

Pin	Assigment	Pin	Assigment
1	Vcc (+5V)	3	Data +
2	Data -	4	Ground-

- **LAN Port (M12, 8-pin, female X-coded)**

Pin	Assigment	Pin	Assigment
1	MX1+	5	MX2-
2	MX3-	6	MX4+
3	MX3+	7	MX1-
4	MX4-	8	MX2+

iBASE

2.2 Setting the Jumpers

Set up and configure your MPT-8000RH by using jumpers for various settings and features according to your needs and applications. Contact your supplier if you have doubts about the best configuration for your use.

2.2.1 How to Set Jumpers

Jumpers are short-length conductors consisting of several metal pins with a non-conductive base mounted on the circuit board. Jumper caps are used to have the functions and features enabled or disabled. If a jumper has 3 pins, you can connect either PIN1 to PIN2 or PIN2 to PIN3 by shorting.

Pin# 1 2 3
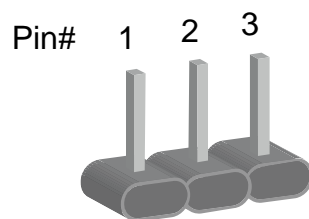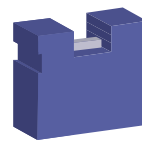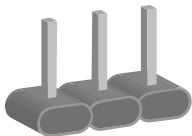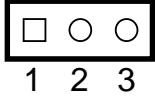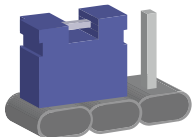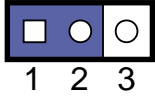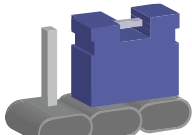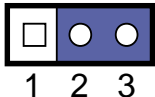
A 3-pin jumper   **A jumper cap**

Refer to the illustration below to set jumpers.

Pin	Oblique view	Illustration
Open		1 2 3
1-2 closed		1 2 3
2-3 closed		1 2 3

When two pins of a jumper are encased in a jumper cap, this jumper is **closed**, i.e. turned **On**.

When a jumper cap is removed from two jumper pins, this jumper is **open**, i.e. turned **Off**.

2.3 Switches, Jumpers & Connectors Locations

iBASE

2.4 Switches, Jumpers and Connectors

2.4.1 SW1_1: COM5 RS-485 Terminal Register

Setting	Function
Pin_1 Off	COM5 Terminal Disable (Default)
Pin_1 On	COM5 Terminal Enable

2.4.2 SW1_2: COM6 RS-485 Terminal Register
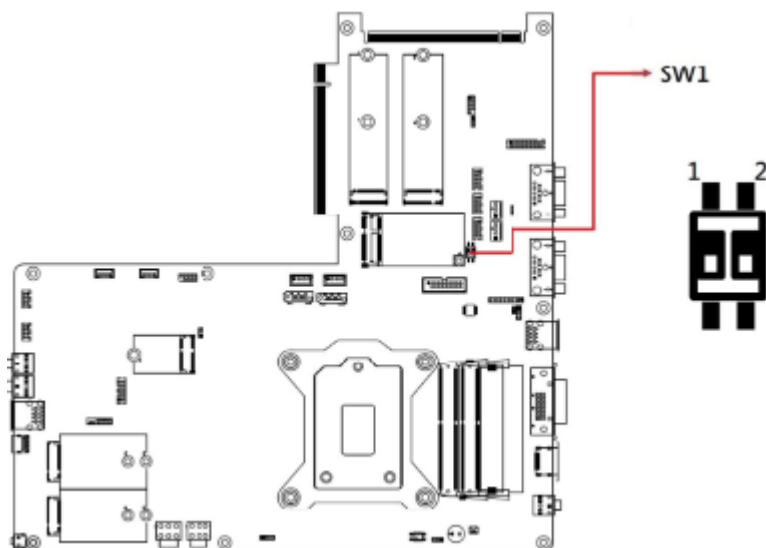
Setting	Function
Pin_2 Off	COM6 Terminal Disable (Default)
Pin_2 On	COM6 Terminal Enable

2.4.3 SW2: Clear CMOS Button
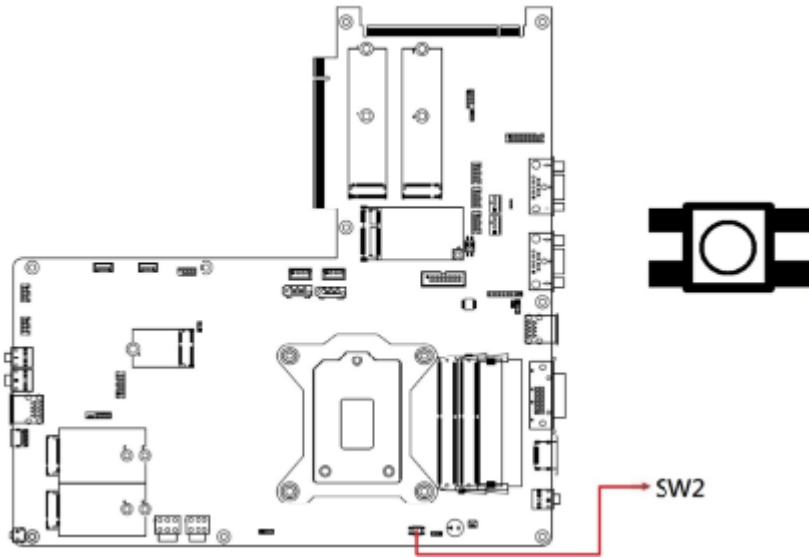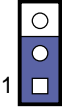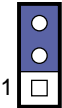
2.4.4 JP5: Clear ME Register
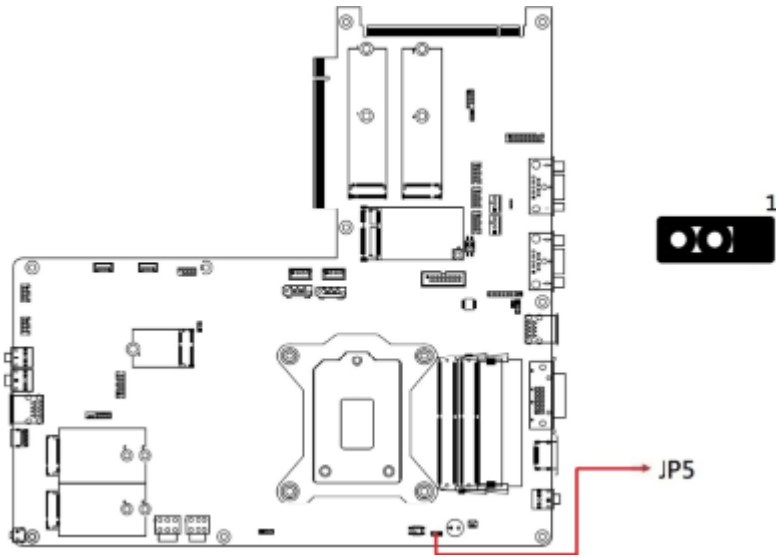
Function	Pin closed	Illustration
Normal (Default)	1-2	
Clear ME	2-3	
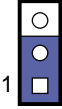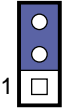
2.4.5 JP2: COM2 Terminator tycilly 120 ohm Mode Selection
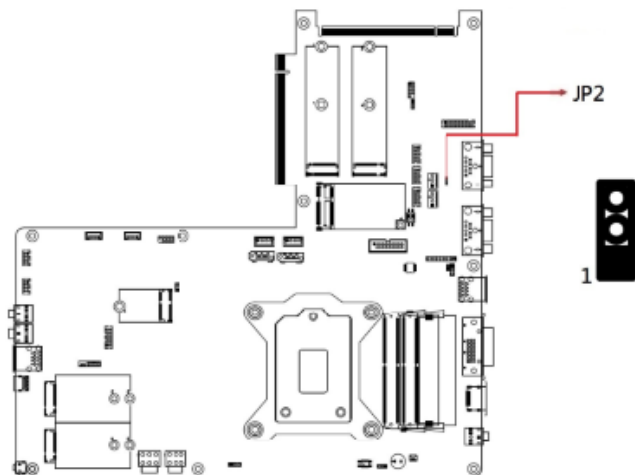
Function	Pin closed	Illustration
Enable	1-2	
Normal (default)	2-3	

2.4.6 JP3: AT/ATX Mode Selection
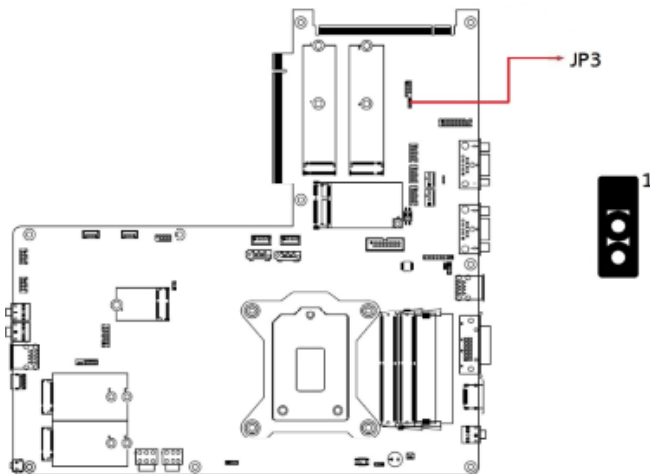
Function	Pin closed	Illustration
ATX (default)	1-2	
AT	2-3	

2.4.7 SW3: Reset Button
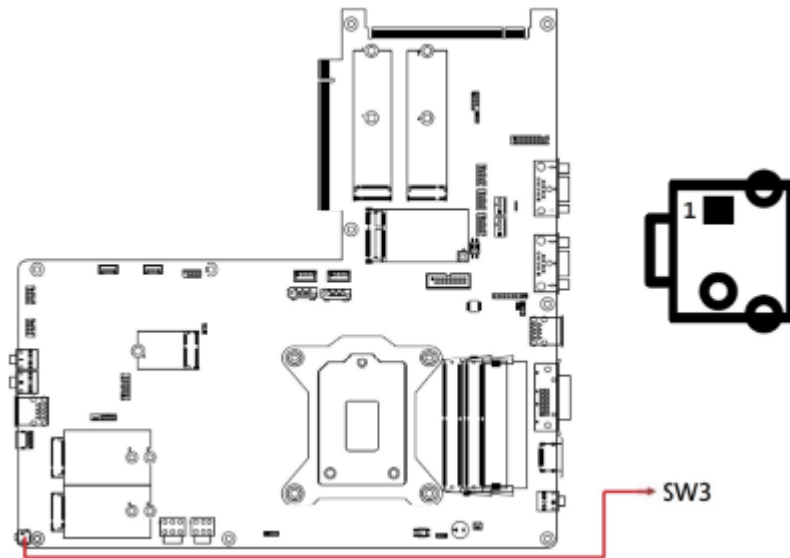
2.4.8 SW4: Digital I/O test (Factory use only)

iBASE
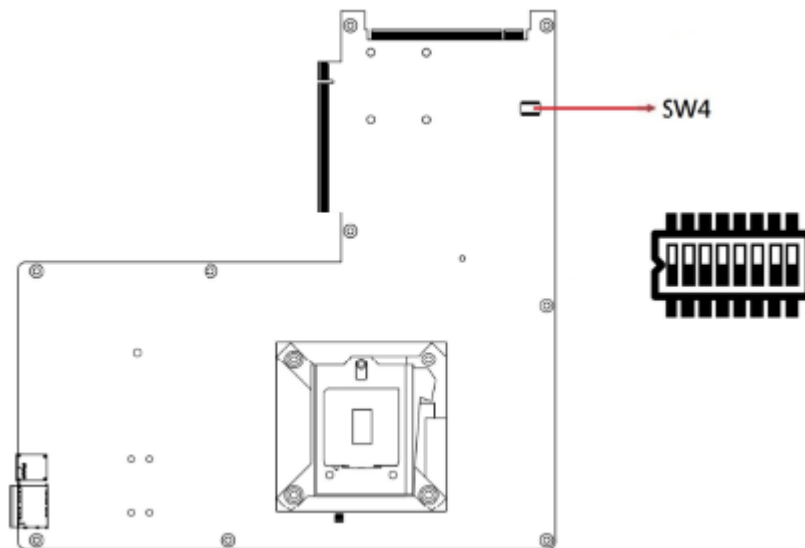
2.4.9   SW5: 4 pin dip switch to control the auto-system delay time:
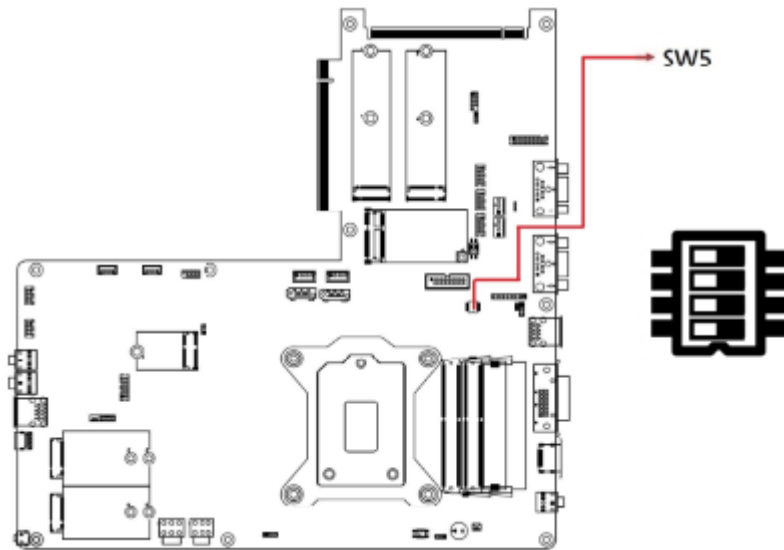
Note: Will have an additional 10 secs delay for checking power source stable when both powering on and off.

Pin No:	1	2	3	4
Disable auto turn-off	0	0	0	0
Delay 10 sec	1	0	0	0
Delay 20 sec	0	1	0	0
Delay 30 sec	1	1	0	0
Delay 40 sec	0	0	1	0
Delay 50 sec	1	0	1	0
Delay 60 sec	0	1	1	0
Delay 70 sec	1	1	1	0
Delay 80 sec (Default)	0	0	0	1
Delay 90 sec	1	0	0	1
Delay 100 sec	0	1	0	1
Delay 110 sec	1	1	0	1
Delay 120 sec	0	0	1	1
Delay 130 sec	1	0	1	1
Delay 140 sec	0	1	1	1
Delay 150 sec	1	1	1	1

Connectors

2.4.10 CN1: COM2 Connector RS-485 (2KV isolation)
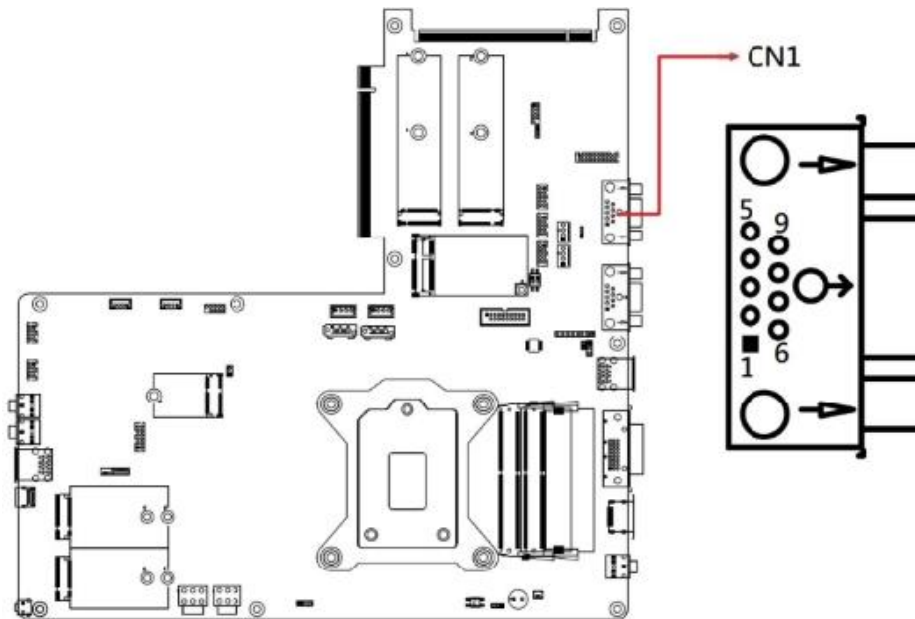
Pin	Signal Name
	RS-485
1	DATA-
2	DATA+
3	NC
4	NC
5	Ground
6	NC
7	NC
8	NC
9	NC

iBASE

2.4.11 CN2: COM1 Connector RS232/422/485 (2KV isolation)
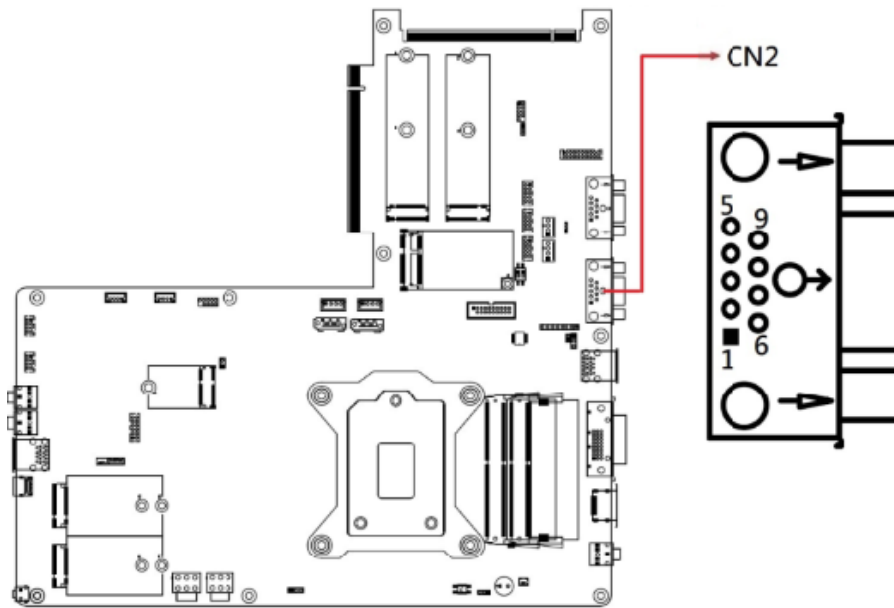
COM1 is jumper-less for RS-232, RS-422 and RS-485 and configured with BIOS Selection.

Pin	Signal Name		
	RS-232	**RS-422**	**RS-485**
1	DCD	TX-	DATA-
2	RX	TX+	DATA+
3	TX	RX+	NC
4	DTR	RX-	NC
5	Ground	Ground	Ground
6	DSR	NC	NC
7	RTS	NC	NC
8	CTS	NC	NC
9	RI	NC	NC

2.4.12 CN3: USB3 Type A Connector (supports USB3 Gen1)
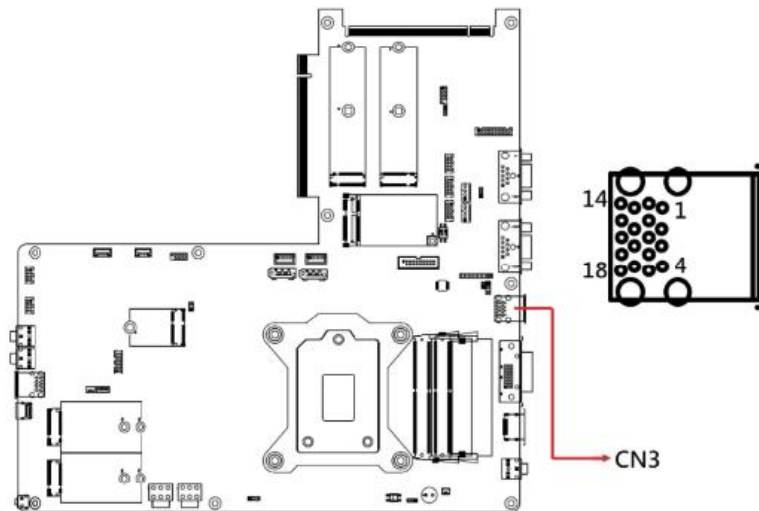
2.4.13 CN4:DVI Connector
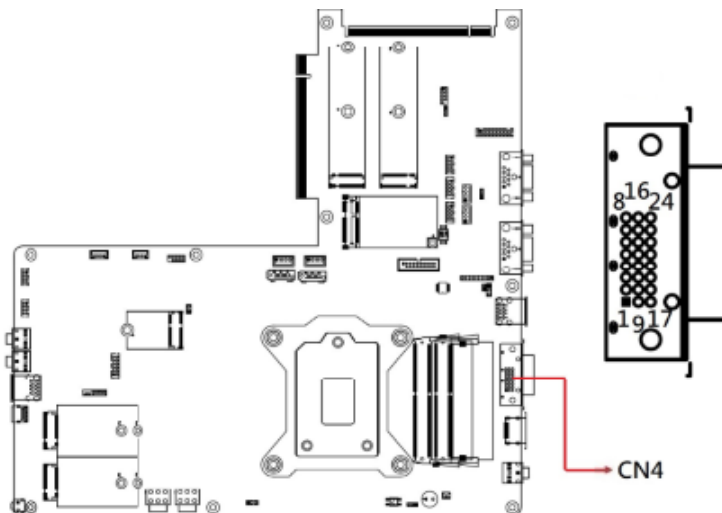
2.4.14 CN5: HDMI Connector

iBASE
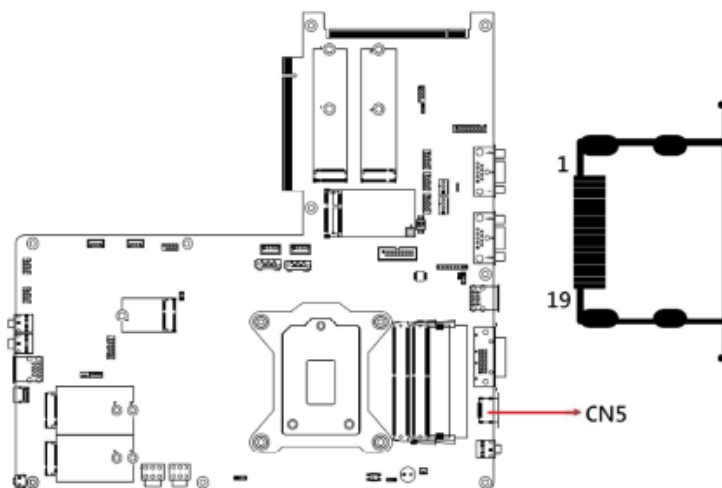
2.4.15 CN6: Audio Connector (Line out)
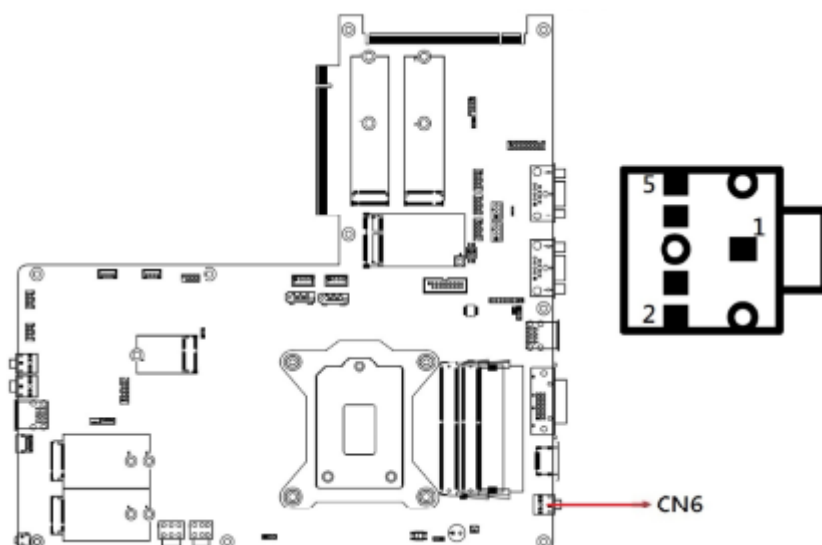
Pin	Assigment	Pin	Assigment
1	Ground	4	Ground
2	Line_out-R	5	Line_out-L
3	Jack Detect		

2.4.16 CN7,CN8: SATA III Connector
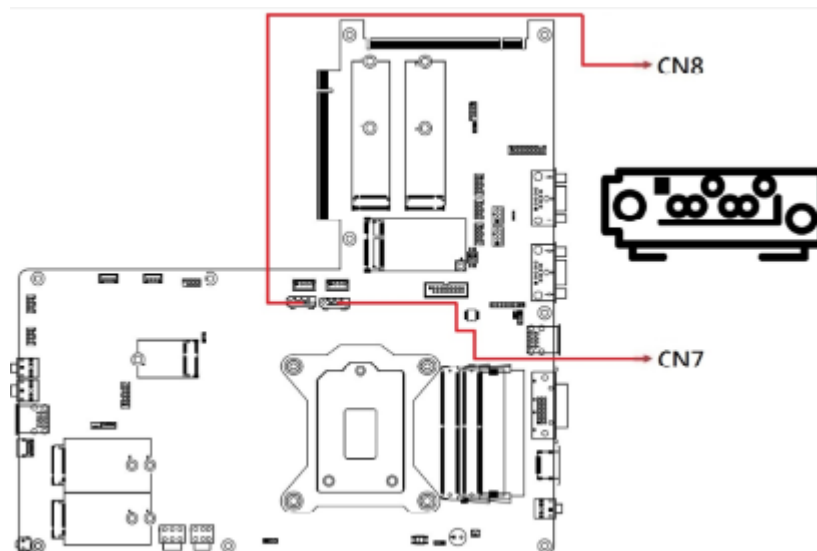
Pin	Assigment	Pin	Assigment
1	Ground	4	Ground
2	TXP0	5	RXN0
3	TXN0		

2.4.17 CN11: Audio Connector (Mic in)
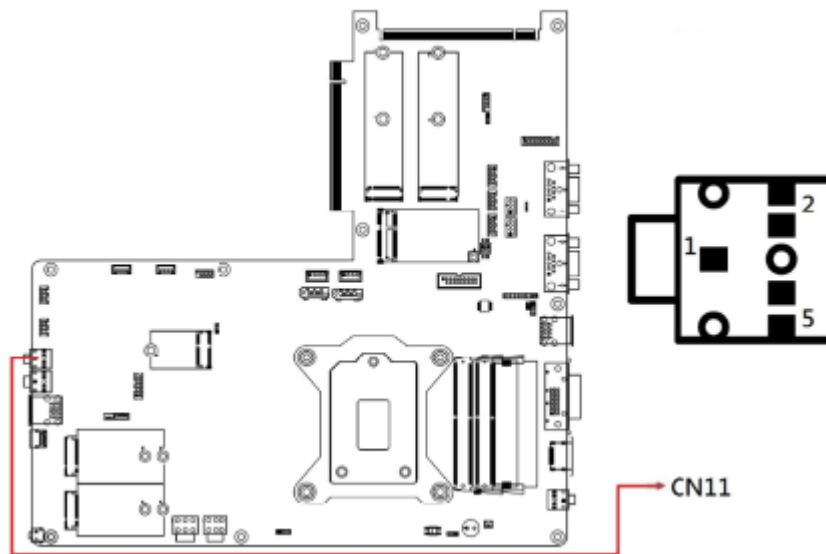
Pin	Assigment	Pin	Assigment
1	Ground	4	Ground
2	Mic_in-R	5	Mic_in-L
3	Jack Detect		

2.4.18 CN12: Audio Connector (Line in)
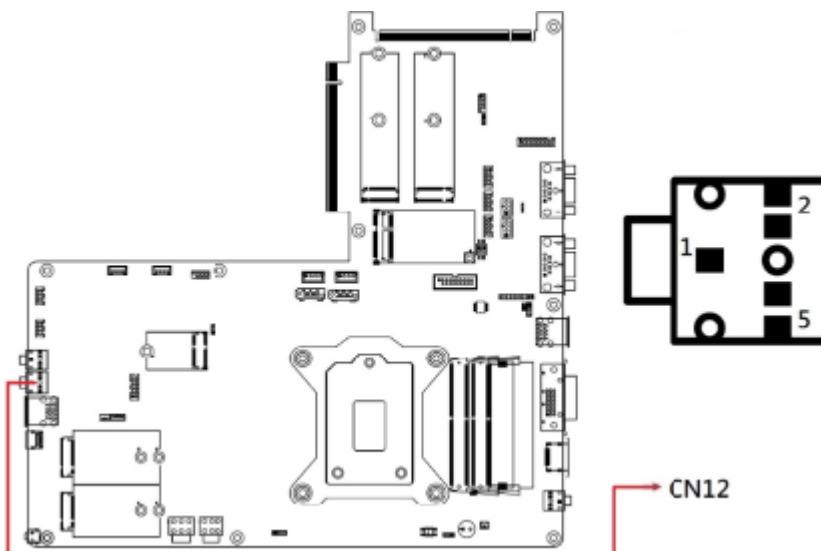
Pin	Assigment	Pin	Assigment
1	Ground	4	Ground
2	Line_in-R	5	Line_in-L
3	Jack Detect		

iBASE

2.4.19 CN13: USB3 Type A Connector (supports USB3 Gen2)
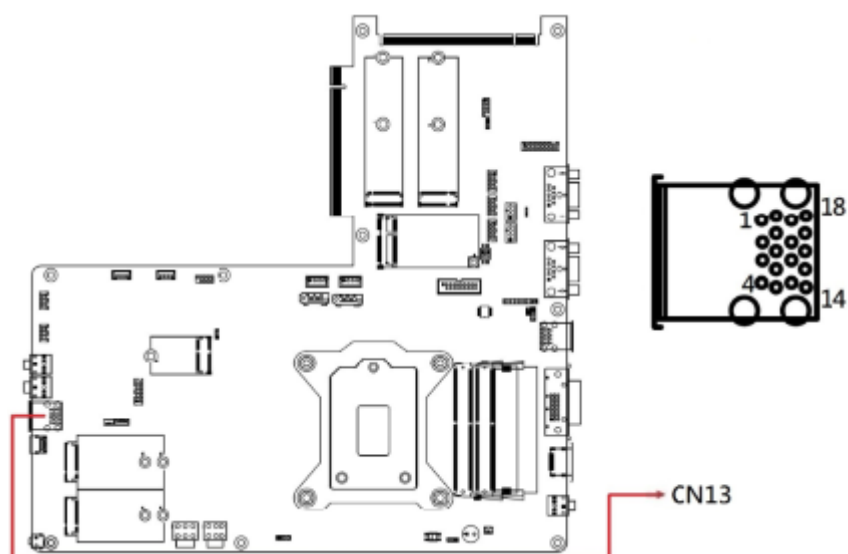
2.4.20 CN14: Type C Connector (supports USB3 Gen1)
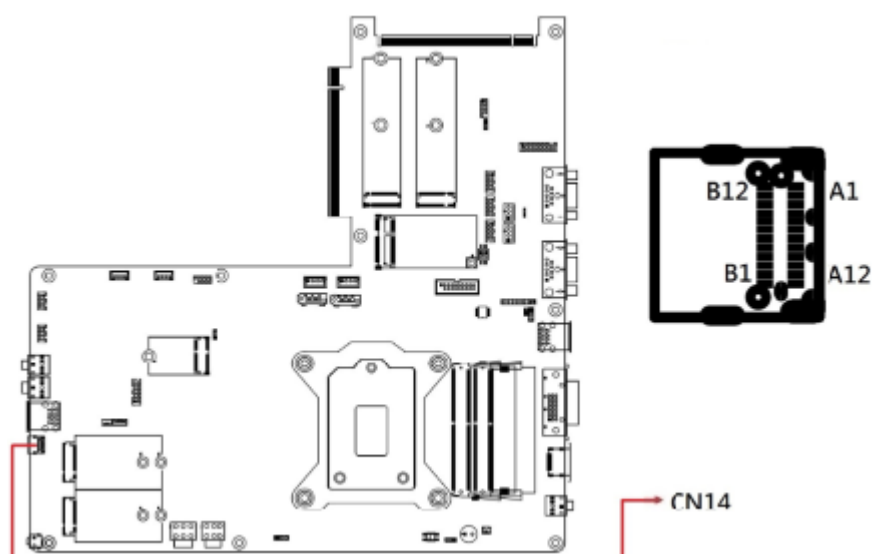
2.4.21 CN15: Nano SIM Card Connector

CN15
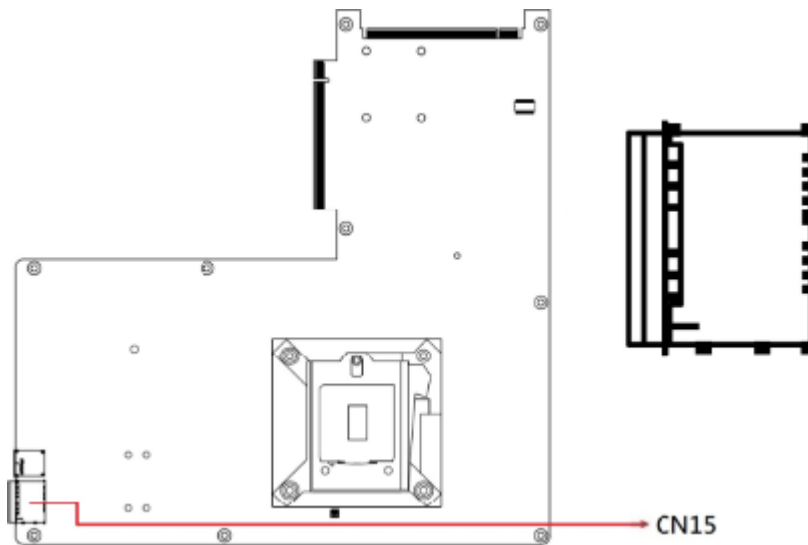
2.4.22 CN16: SD card socket

CN16

iBASE
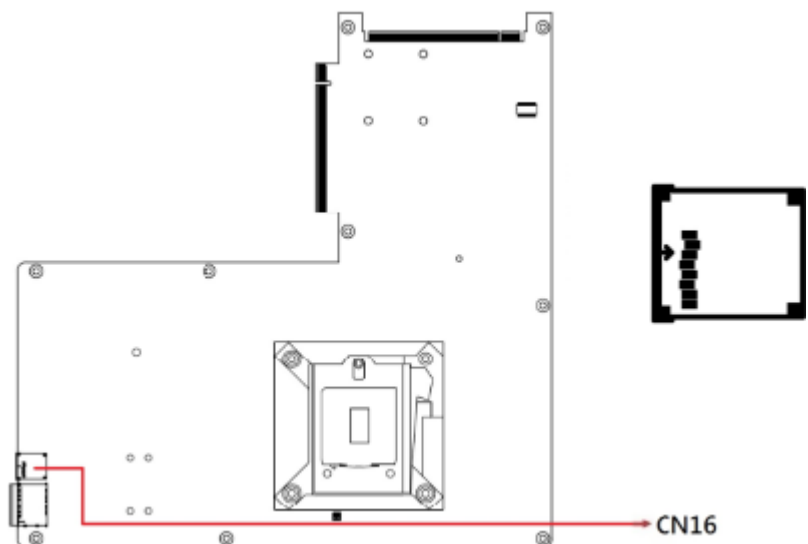
2.4.23 J1: Digital I/O Connector (HK_DF11-20S-PA66H)

Pin	Signal Name	Pin	Signal Name
2	OUT0	1	IN0
4	OUT1	3	IN1
6	OUT2	5	IN2
8	OUT3	7	IN3
10	OUT4	9	IN4
12	OUT5	11	IN5
14	OUT6	13	IN6
16	OUT7	15	IN7
18	Power	17	Ground
20	Ground	19	Ground

Note: J1 is connected to the external digital I/O (D/O and D/O) beside the backup 24V power connector.

2.4.24 J4, J5: COM3, COM4 RS232 Connector (HK_DF11-10S-PA66H)
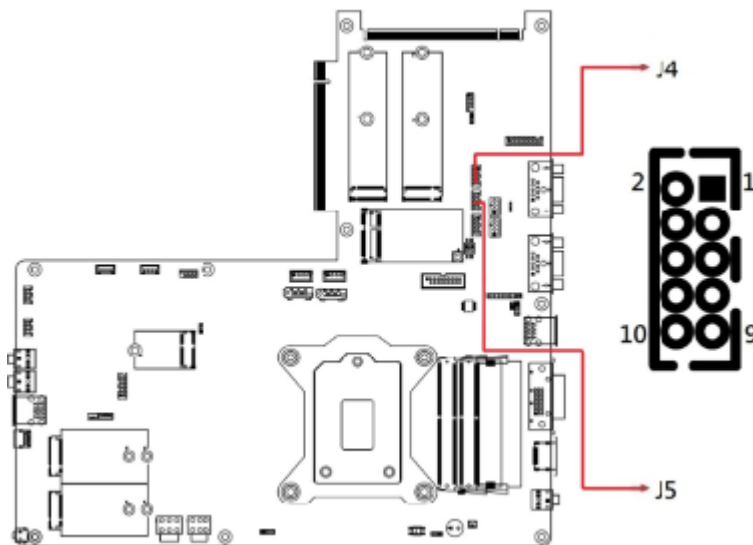
Pin	Signal Name	Pin	Signal Name
1	DCD, Data carrier detect	2	RXD, Receive data
3	TXD, Transmit data	4	DTR, Data terminal ready
5	GND, ground	6	DSR, Data set ready
7	RTS, Request to send	8	CTS, Clear to send
9	RI, Ring indicator	10	Not Used

2.4.25 J6: COM5, COM6 RS-485 Connector (HK_DF11-10S-PA66H)
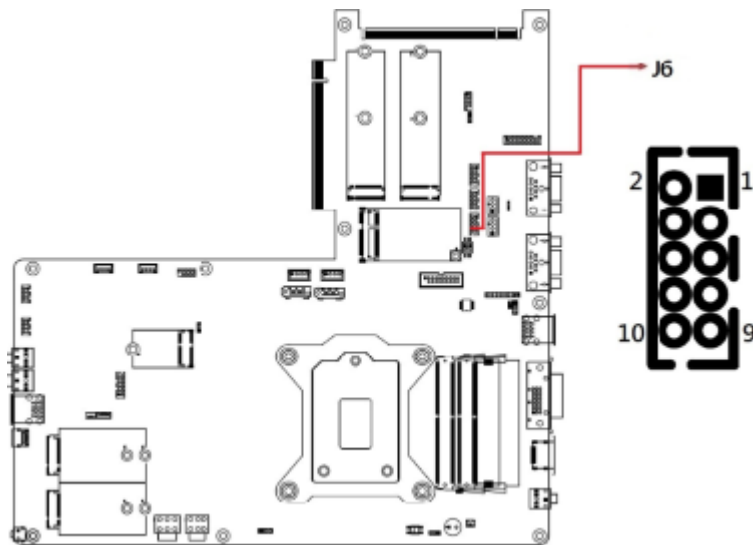
Pin	Signal Name	Pin	Signal Name
1	NC	2	NC
3	GND	4	GND
5	RS485-DATA5-	6	RS485-DATA6-
7	RS485-DATA5+	8	RS485-DATA6+
9	GND	10	GND

2.4.26 J7: Battery Connector (Molex_53047-0210)

iBASE
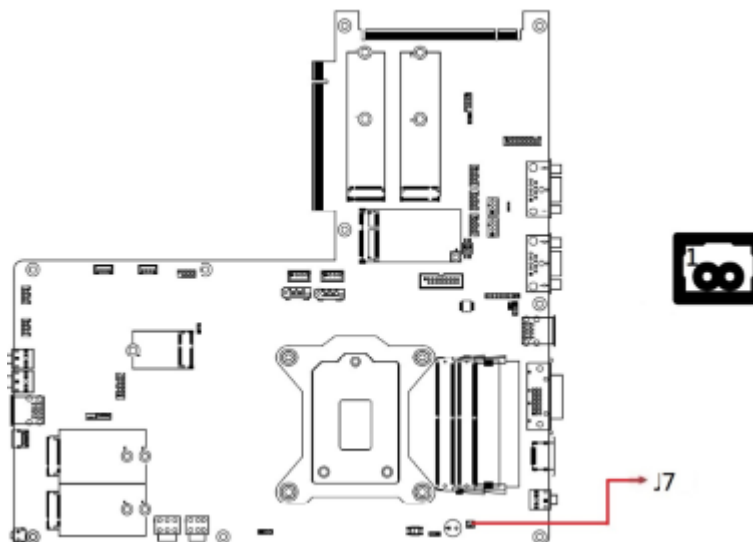
2.4.27 JP7: LED Function Connectors (HK_DF11-12S-PA66H)
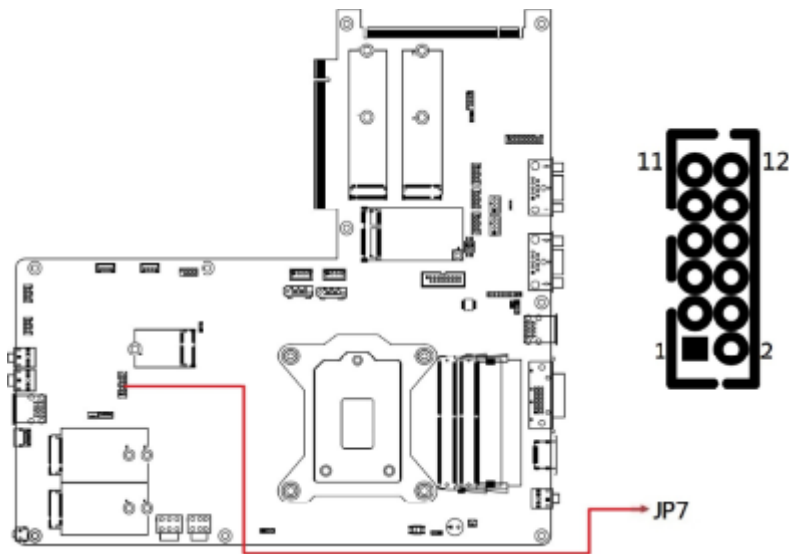
Pin	Signal Name	Pin	Signal Name
1	WLAN LED-	2	WLAN LED +
3	WWAN LED-	4	WWAN LED+
5	HDD LED-	6	HDD LED+
7	Firmware Programming LED1-	8	Firmware Programming LED1+
9	Firmware Programming LED2-	10	Firmware Programming LED2+
11	GND	12	POWER LED+

2.4.28 J8: ESPI Debug 80 Port (Factory use only)
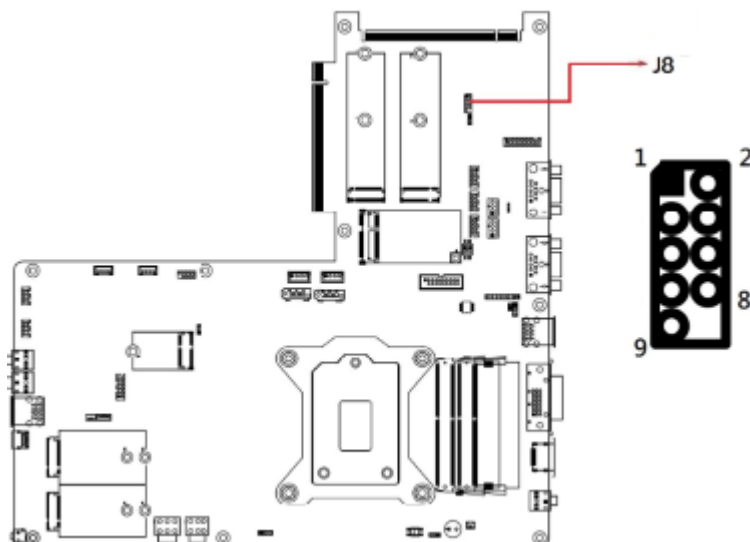
2.4.29   J10:USB 3.0 / USB 2.0 Connector
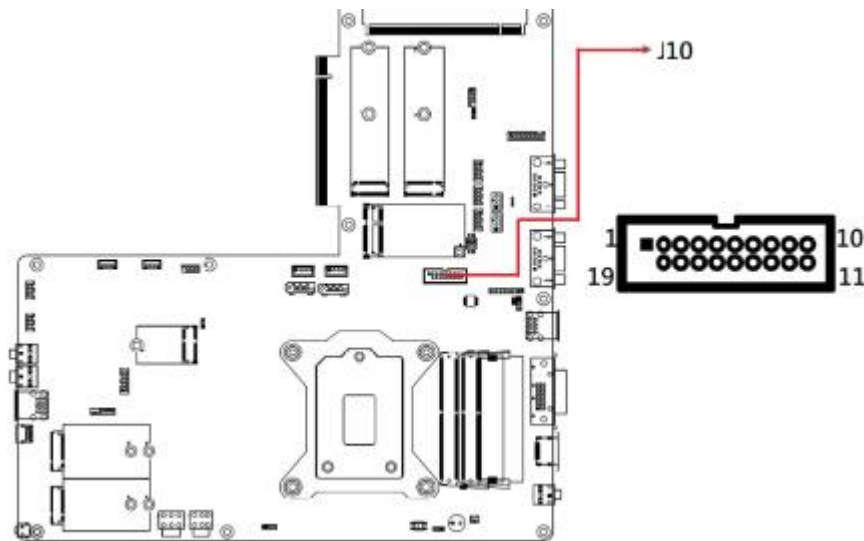
2.4.30   J11, J13: M.2 M-Key (2280) Connector with PCIe(x4)

iBASE
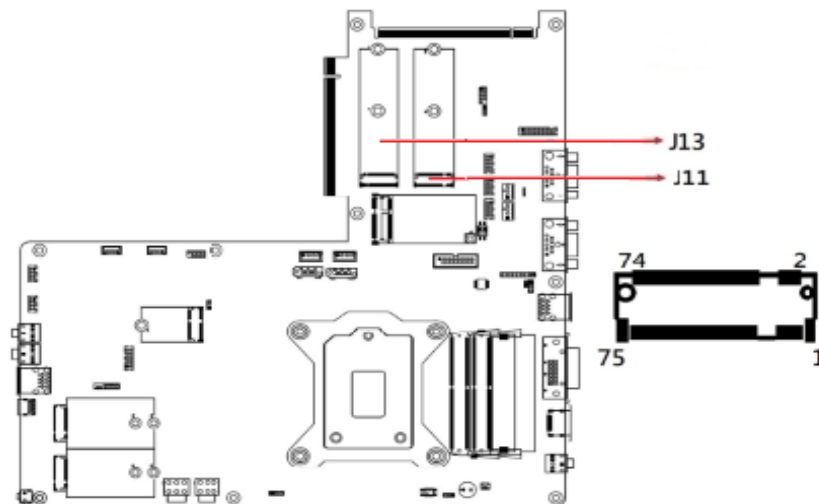
2.4.31 J12: Mini PCIE Connector with PCIe (x1), USB 2.0
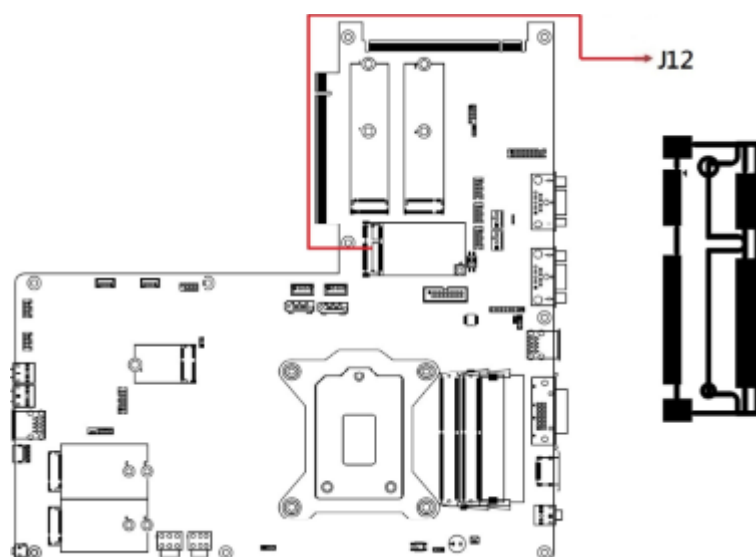
2.4.32 J17: Backup 24V Power Connector
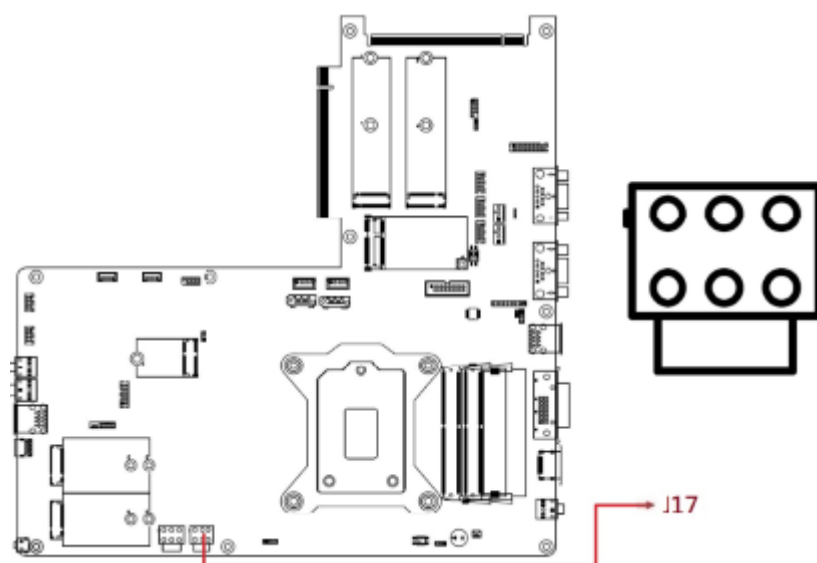
Pin	Signal Name	Pin	Signal Name
1	+24V	4	Ground
2	+24V	5	Ground
3	+24V	6	Ground

2.4.33   J19: DC_IN 24V Power Connector
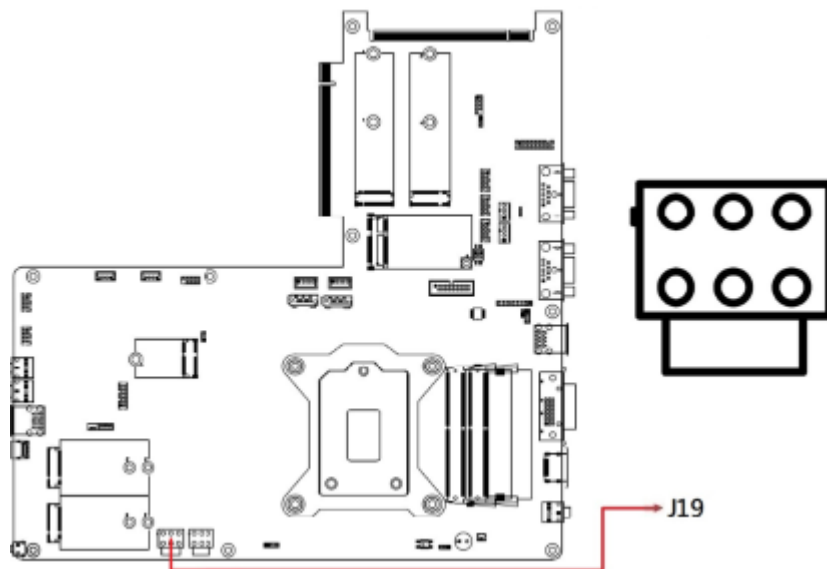
Pin	Signal Name	Pin	Signal Name
1	+24V	4	Ground
2	+24V	5	Ground
3	+24V	6	Ground

2.4.34   J14, J15: SATA HDD Power Connector (E-Call_0110-071-040)
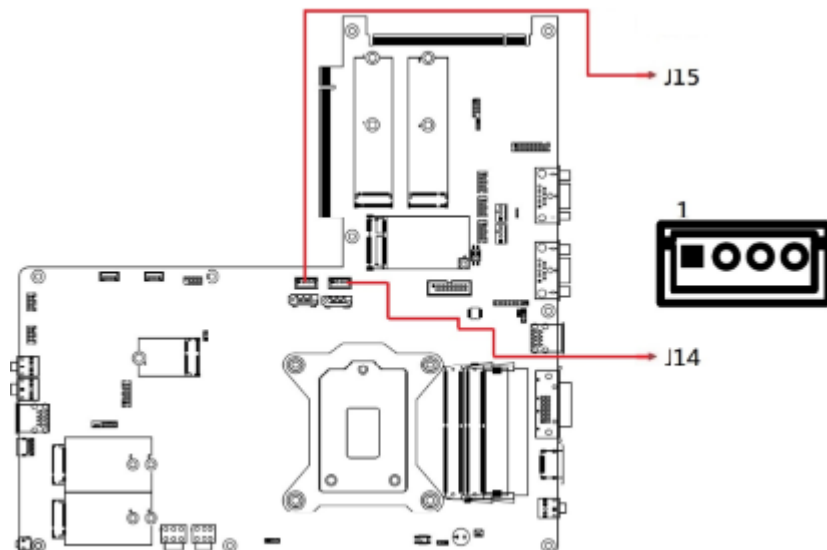
Pin	Assigment	Pin	Assigment
1	+5V	3	Ground
2	Ground	4	+12V

2.4.35   J18: M.2 B-Key (2280/42) Connector with PCIe (x2), USB 2.0
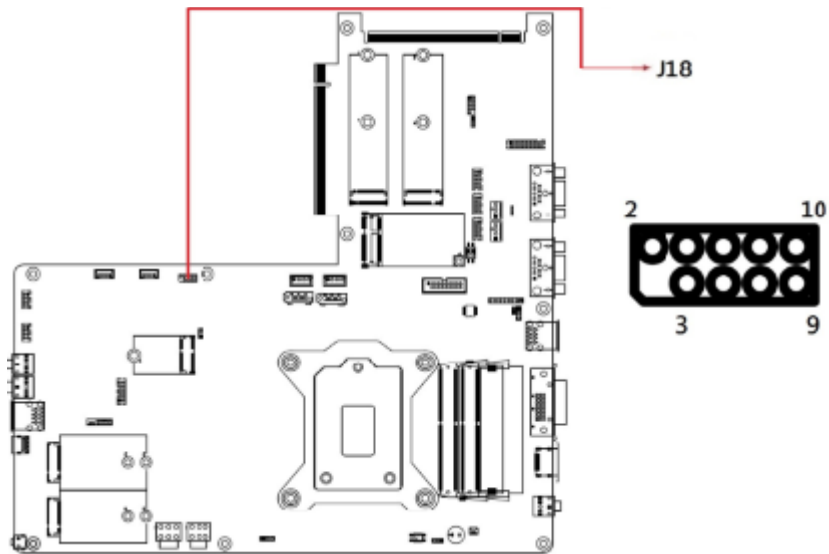
2.4.36   J18: SPI ROM Flash Connector (Factory use only)
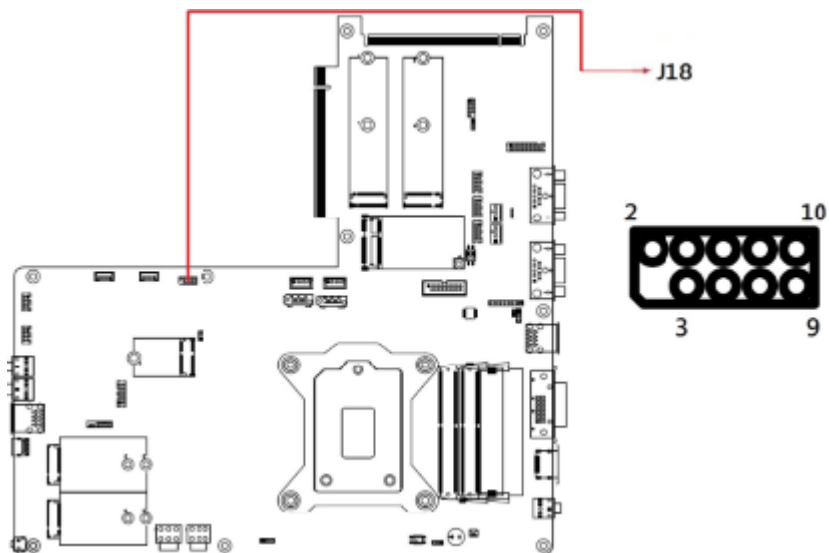
2.4.37   J20: M.2 E-Key (2230) Connector with PCIe (x1), USB 2.0, CNVI
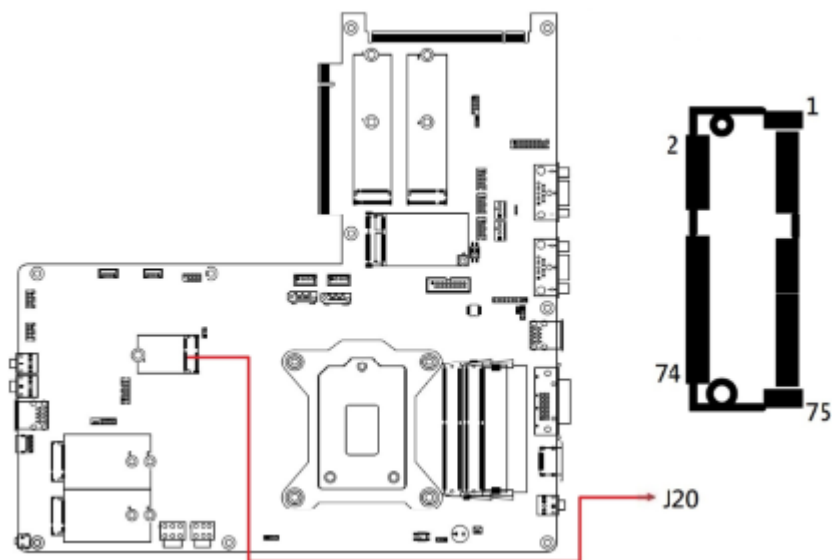
2.4.38   J21: USB_2.0 Connector (E-Call_0110-161-040)
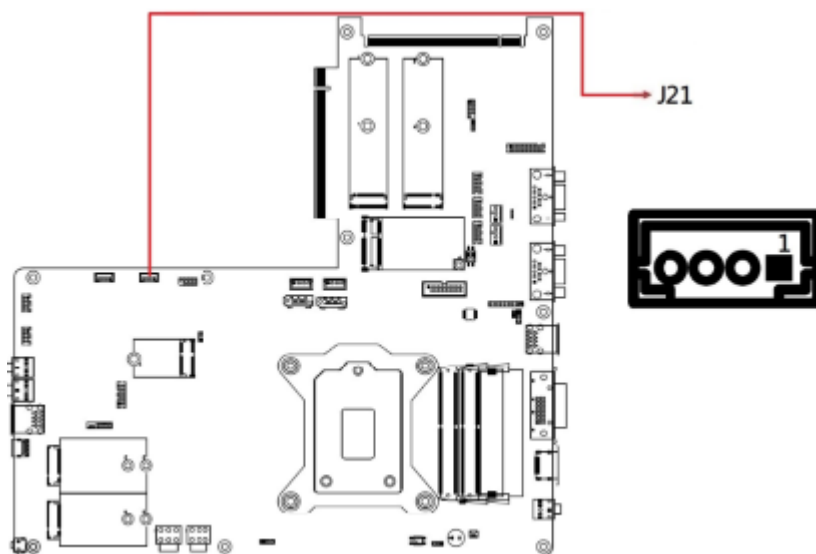
Pin	Assigment	Pin	Assigment
1	VCC	3	D+
2	D-	4	Ground

Note: USB Enable/Disable Selection by BIOS

2.4.39   J22: USB_1.1 Connector (E-Call_0110-161-040)
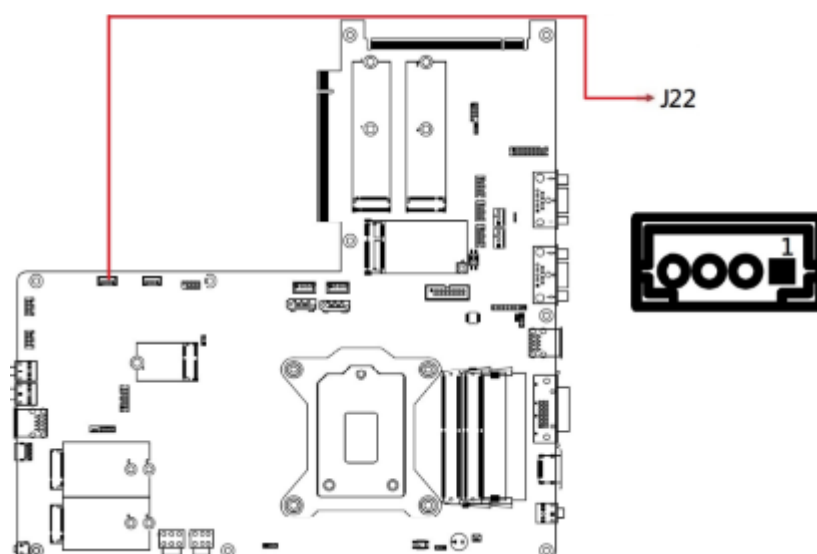
Pin	Assigment	Pin	Assigment
1	VCC	3	D+
2	D-	4	Ground

Note: USB Enable/Disable Selection by BIOS

2.4.40   J23: M.2 B-Key (3042/52) Connector with PCIe (x1), USB 2.0,SIM Card
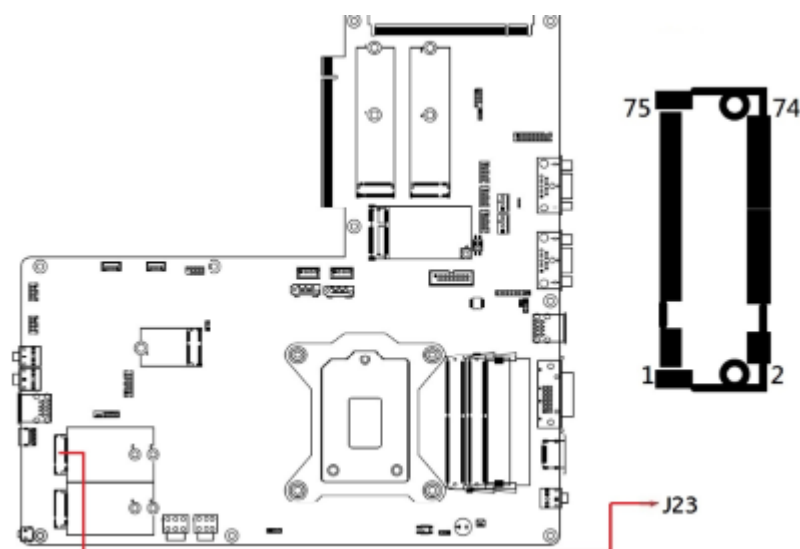
2.4.41 J24: M.2 B-Key (3042/52) Connector with PCIe (x1), USB 2.0, USB 3.0, SIM Card
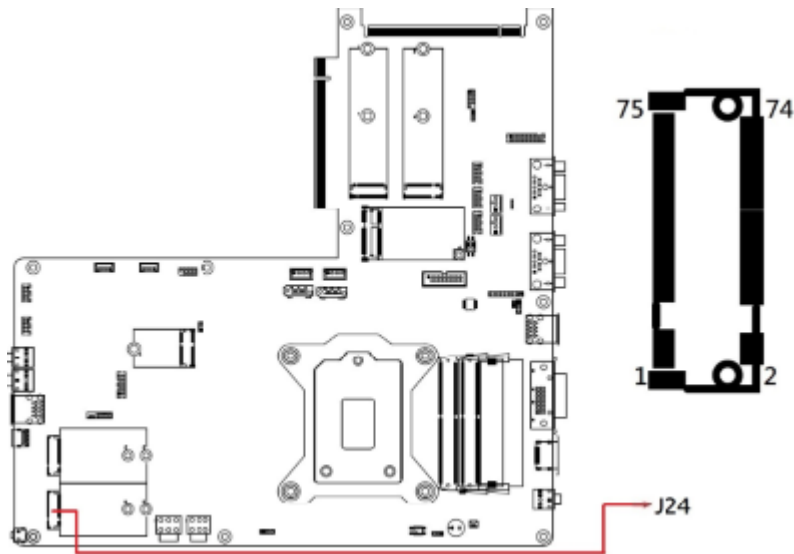
2.4.42 J25, J26: LAN1,2,3 Connector (HRS_DF11-8DP-2DSA(08)
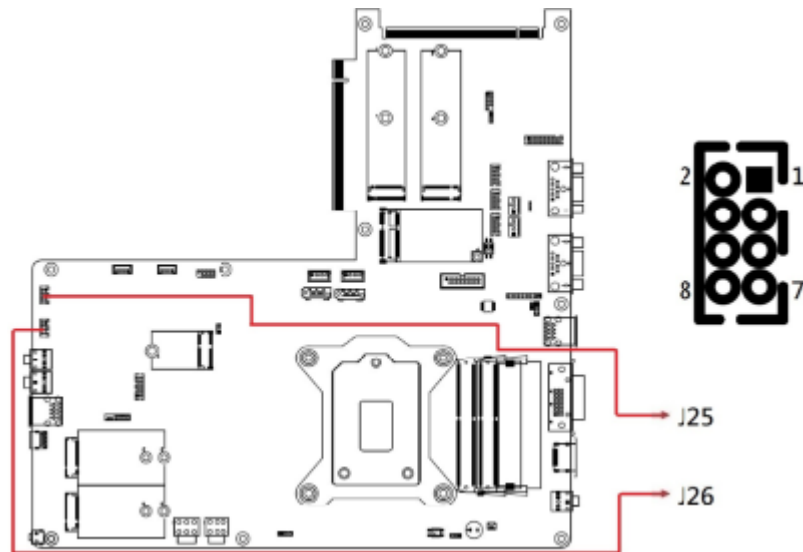
Pin	Signal Name	Pin	Signal Name
1	MDI_P0	2	MDI_N0
3	MDI_P1	4	MDI_N1
5	MDI_N2	6	MDI_P2
7	MDI_P3	8	MDI_N3

2.4.43

iBASE

2.4.44 JTAG1: USB Type C Flash Connector (Factory use only)
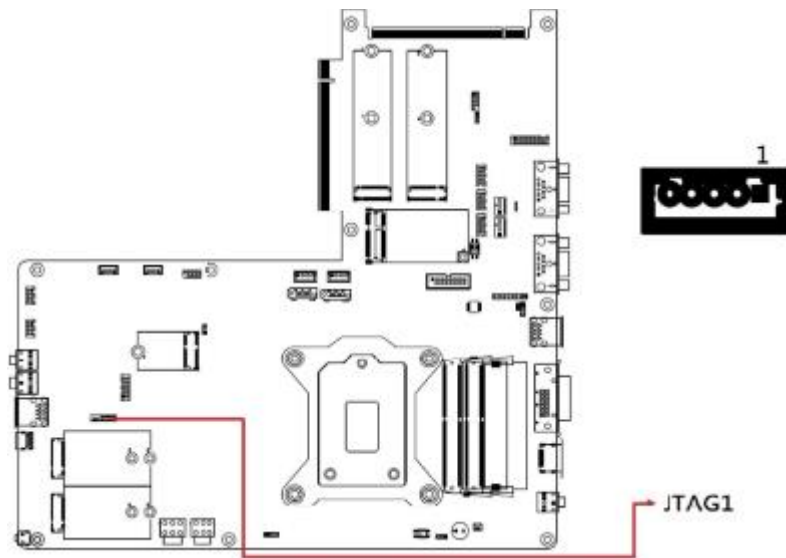
2.4.45 CPU_FAN1: CPU Fan Power Connector
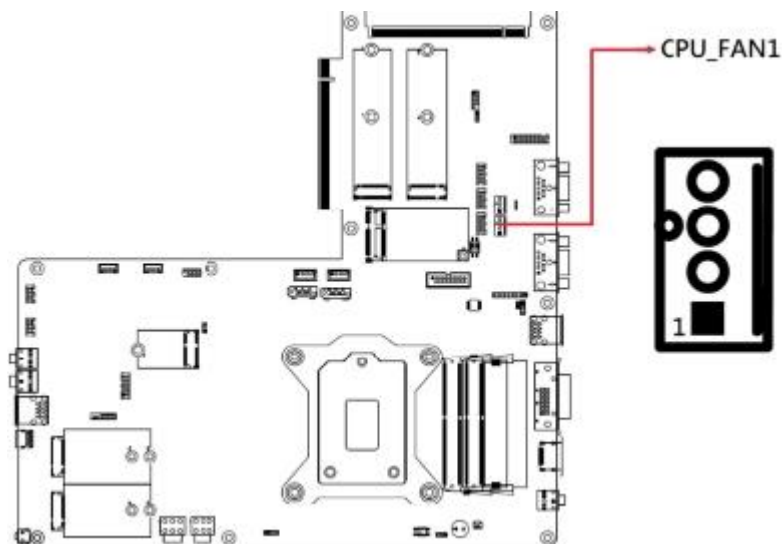
2.4.46 SYS_FAN1: CPU Fan Power Connector
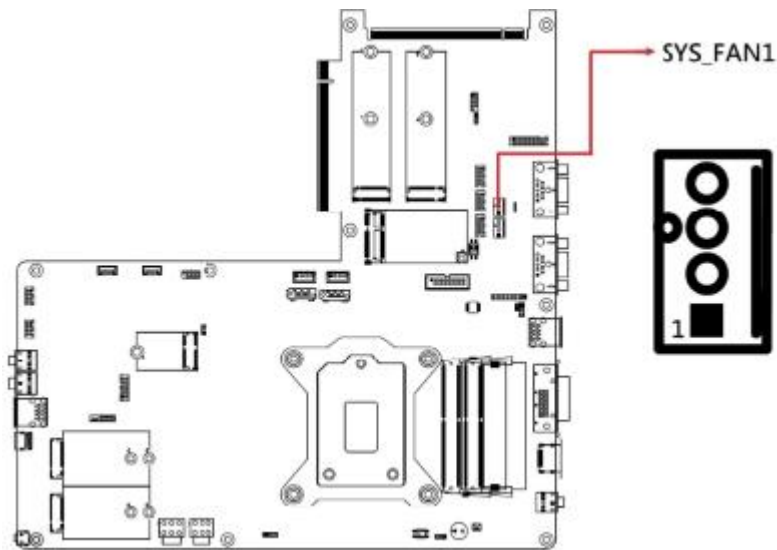
Pin	Assigment
1	Ground
2	+12V
3	Rotation detection
4	Control

Chapter 3
Driver Installation

The information provided in this chapter includes:

- Intel® Chipset Software Installation Utility
- VGA Driver Installation
- HD Audio Driver Installation
- LAN Driver Installation
- Intel® ME Drivers Installation

IBASE

3.1   Introduction

This section describes the installation procedures for software drivers.

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

3.2   Intel® Chipset Software Installation Utility

The Intel® Chipset drivers should be installed first 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. 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 as shown. Click **Intel** and then **Intel(R) CometLake Chipset Drivers**.

iBASE

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

3. When the *Welcome* screen to the Intel® Chipset Device Software appears, click **Next** to continue.

4. Click **Yes** to accept the software license agreement and proceed with the installation process.

5. Click **Install** to proceed with the installation process.

6. The driver has been completely installed. Click **Finish** to complete the setup process.
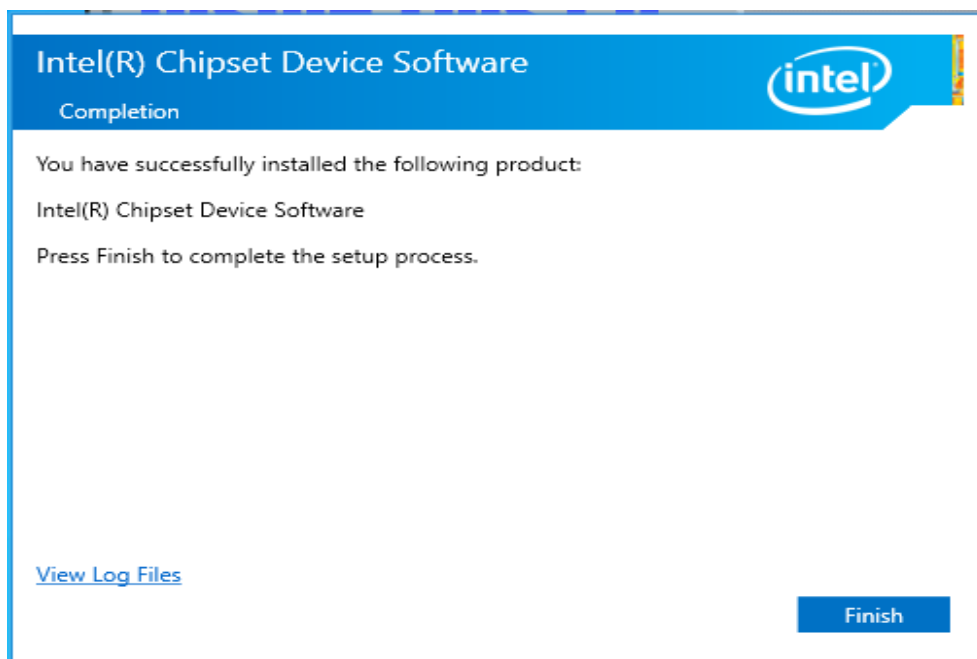
3.3   VGA Driver Installation

1.   Click **Intel** and then **Intel(R) CometLake Chipset Drivers**.

2.   Click **Intel(R) HD Graphics Driver**.

3.   When the *Welcome* screen to the Setup Program of the Intel® Graphics Driver, click **Next** to continue.

iBASE
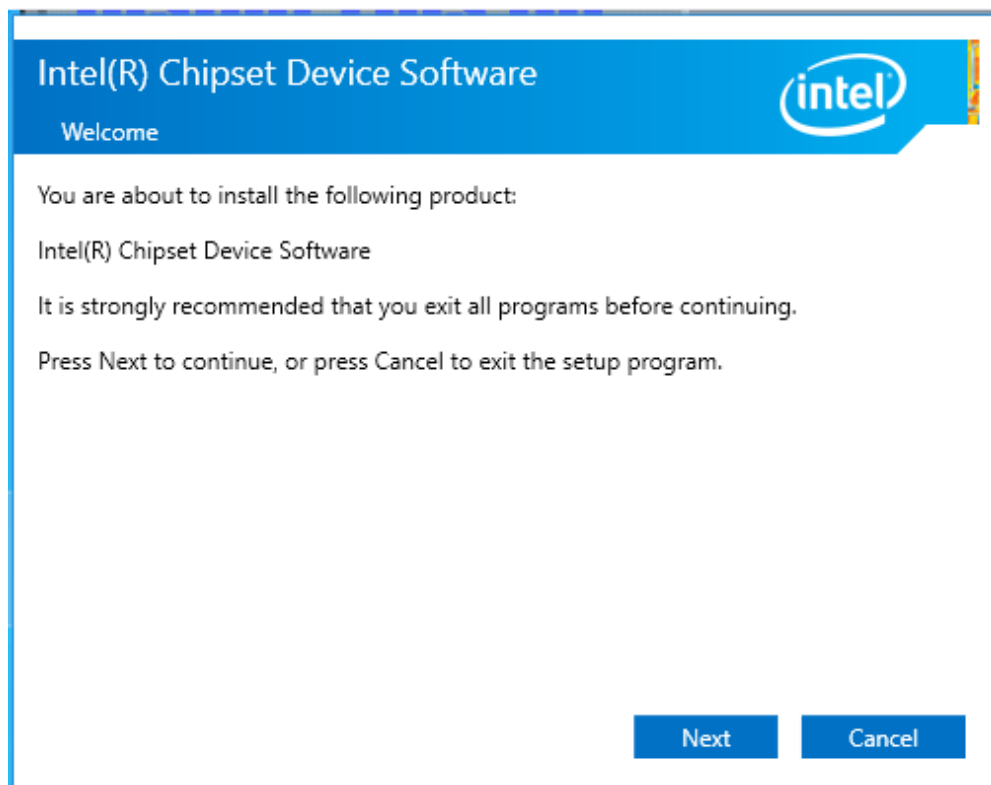
4. Click **Yes** in the Readme File Information screen.
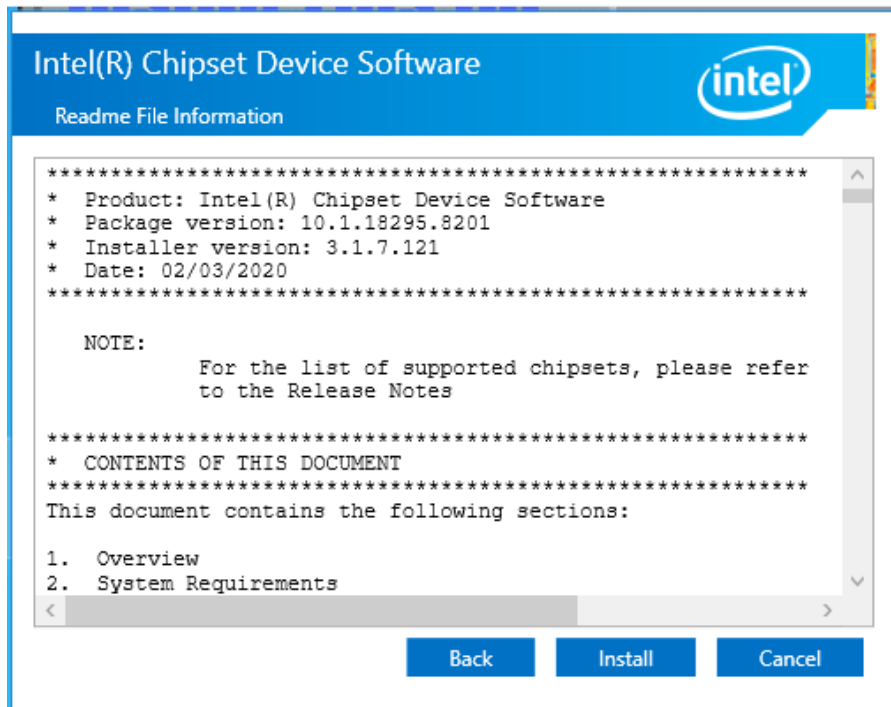
5. Click **Next** in the Setup progress screen.

6. Setup is Complete. Click **Finish** to restart the computer.
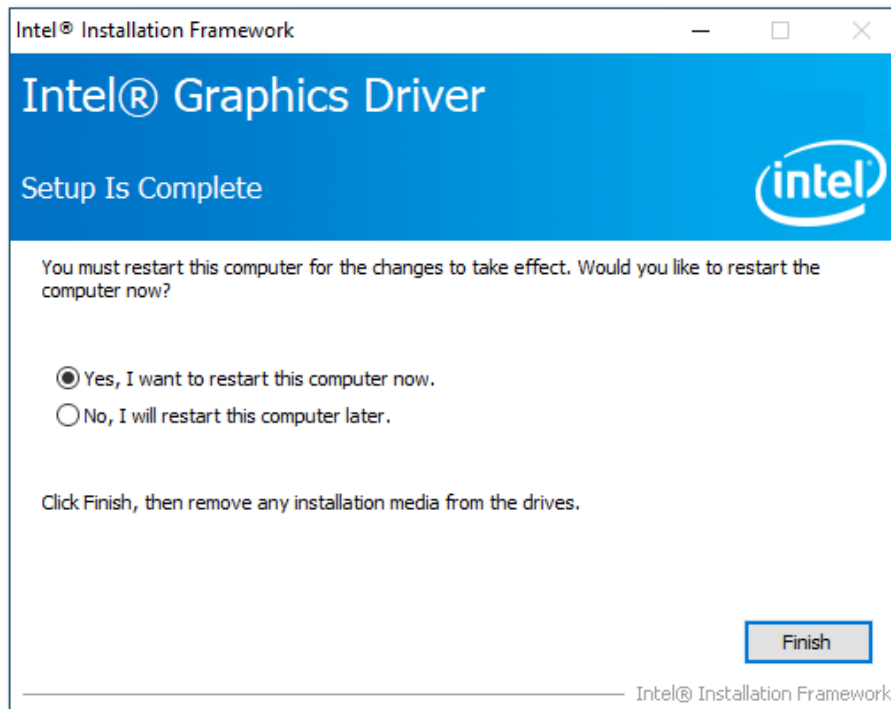
3.4   HD Audio Driver Installation

1. Click **Intel** and then **Intel(R) CometLake Chipset Drivers**.
2. Click **Realtek High Definition Audio Driver**.

3. On the *Welcome* screen of the InstallShield Wizard, click **Next** to start the installation.
4. When the InstallShield Wizard has finished installing the Realtek Audio Driver, click **Finish**.

iBASE
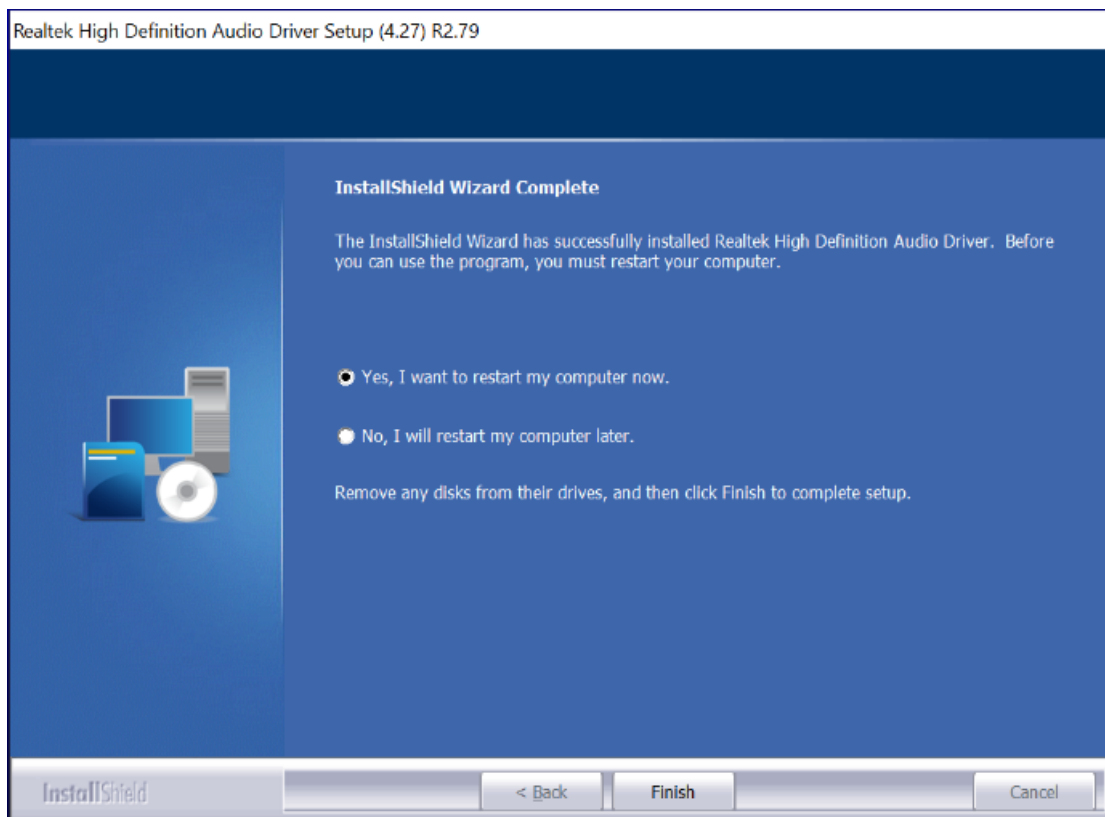
3.5 LAN Driver Installation

1. Click **LAN Card** and then **Intel LAN Controller Drivers**.

2. On the screen of *Intel® Network Connections*, click **Install Drivers and Software**.
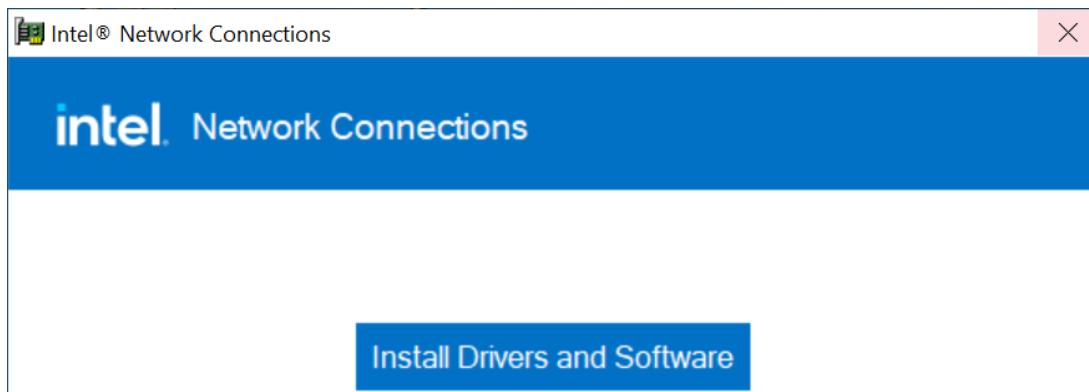
3. When the *Welcome* screen appears, click **Next**.
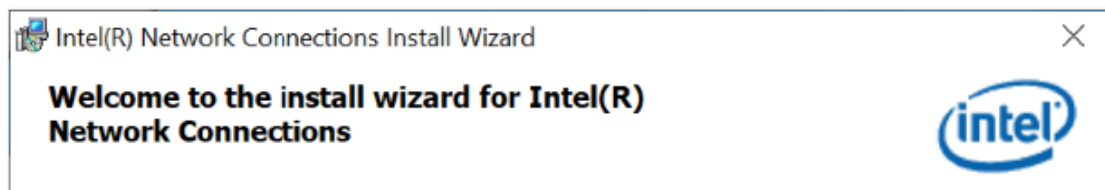
4. In the *Software License Agreement* screen, click **Next** to accept the terms in the license agreement.
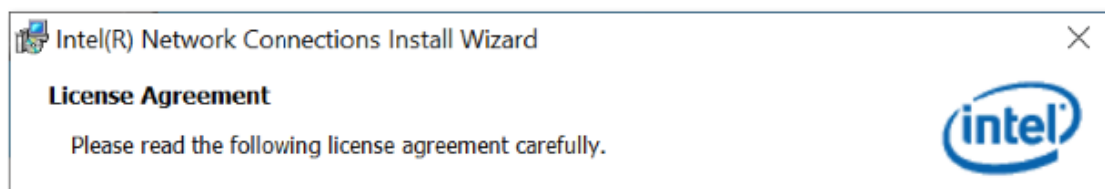
5. In the *Setup Options* screen, click **Next**.
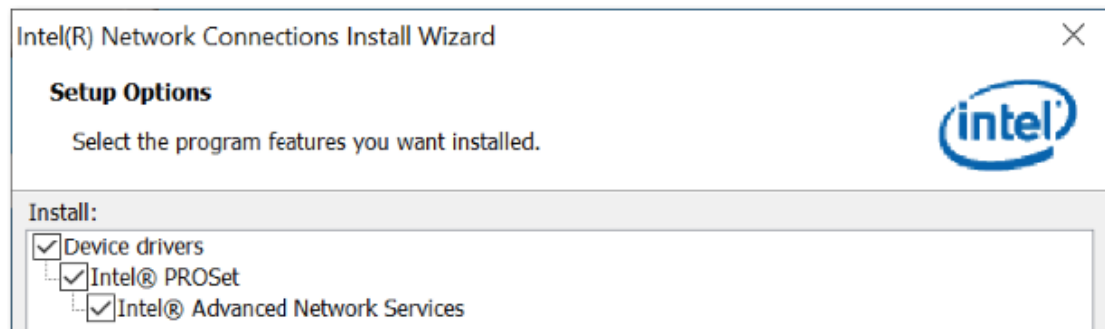
6. The wizard is now ready to begin installation. Click **Install**.
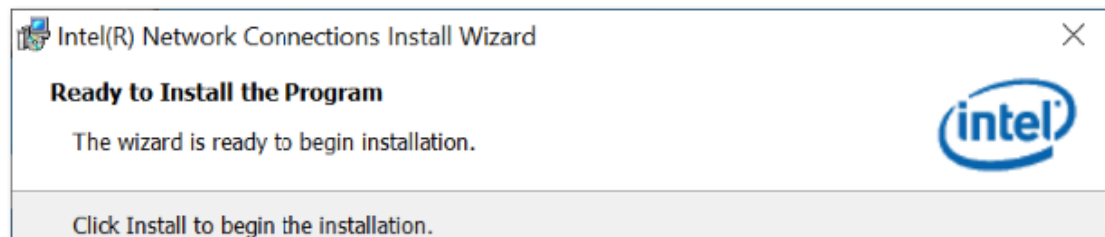
7. In the *Install wizard Completed* screen, click **Finish**.
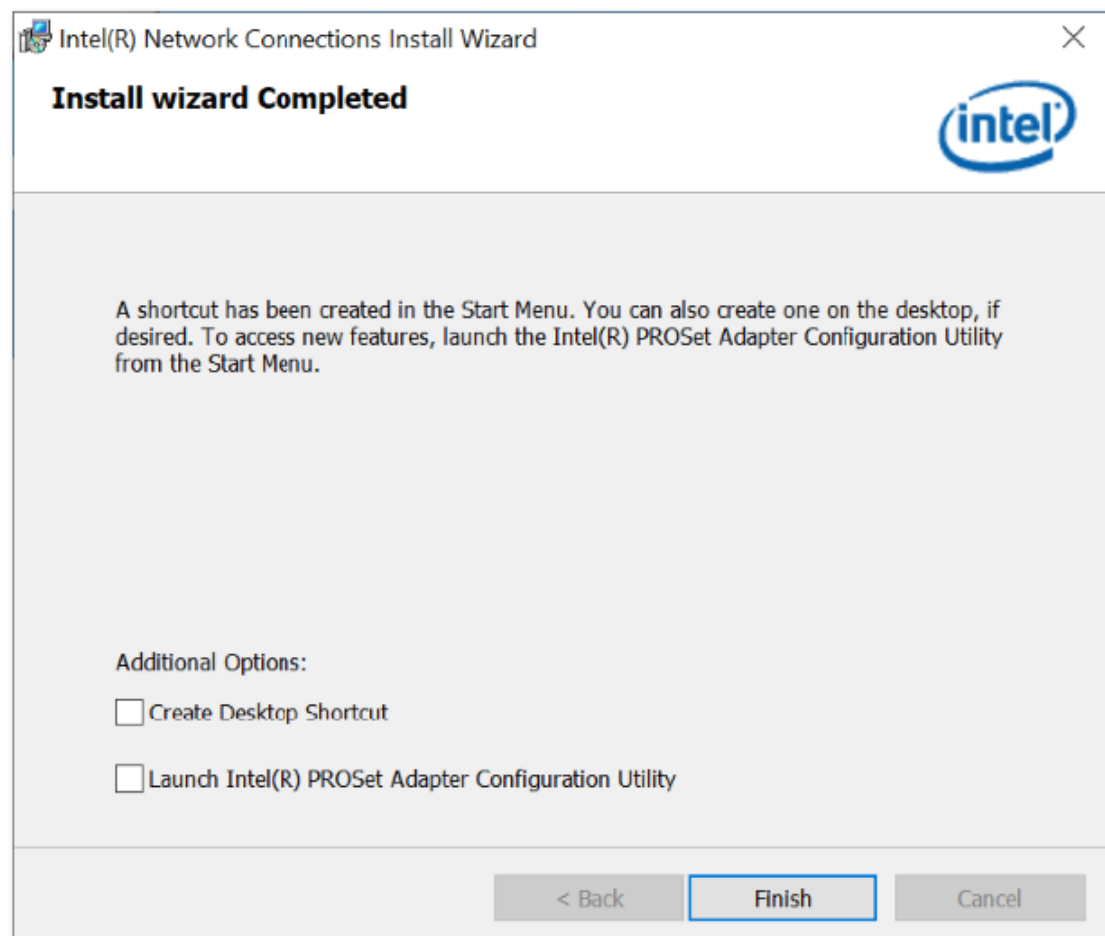
3.6 Intel(R) ME Drivers Installation

1. Click **Intel** and then **Intel(R) CometLake   Chipset Drivers**.

2. When the Welcome screen to the Intel® Management Engine Components Setup appears, click **Next**.

3. Click **Next** to accept the terms in the License Agreement.
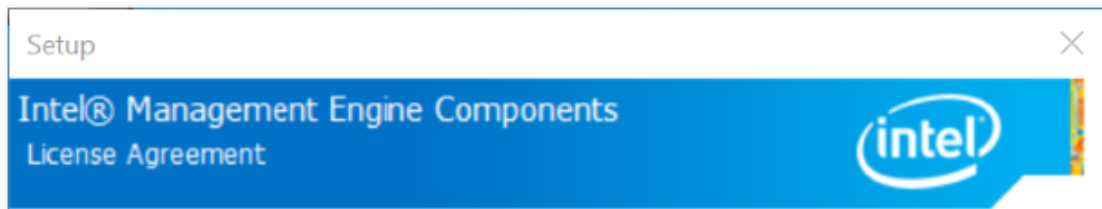
4. Click **Next** to install to the default folder, or click **Change** to choose another destination folder.
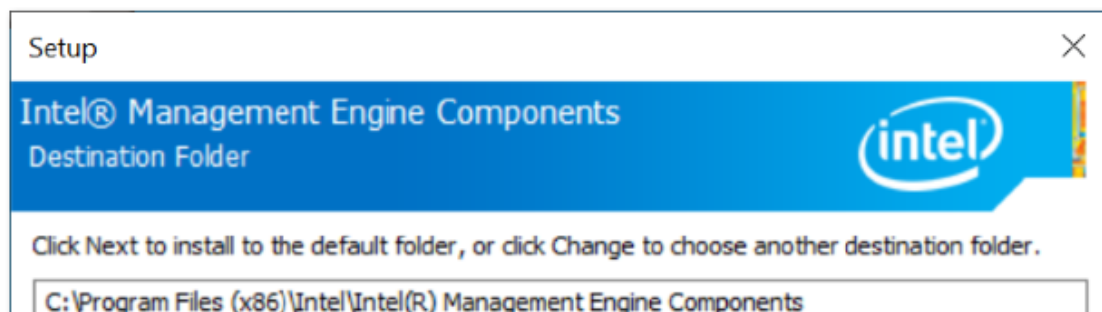
5. When you have successfully installed the components, click **Finish**.

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

iBASE

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 parallel ports. 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 <Del> key immediately allows you to enter the Setup utility. If you are a little bit late pressing the <Del> 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* screen will appear on the screen. 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

```
                              Aptio Setup - AMI
    Main  Advanced  Chipset  Security  Boot  Save & Exit

    BIOS Information                                         Set the Date. Use Tab to
    BIOS Version                  MBT-8001RW-NS003-220530    switch between Date elements.
                                                            Default Ranges:
    Total Memory                  8192 MB                    Year: 1998-9999
    Memory Frequency              2400 MHz                   Months: 1-12
                                                            Days: Dependent on month
    System Date                   [Sat 01/01/2022]           Range of Years may vary.
    System Time                   [00:53:13]




                                                            →←: Select Screen
                                                            ↑↓: Select Item
                                                            Enter: Select
                                                            +/-: Change Opt.
                                                            F1: General Help
                                                            F2: Previous Values
                                                            F3: Optimized Defaults
                                                            F4: Save & Exit
                                                            ESC: Exit



               Version 2.21.1278 Copyright (C) 2022 AMI
```

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.

iBASE

4.4 Advanced Settings

This section allows you to configure, improve your system and allows you to set up some system features according to your preference.

```
                          Aptio Setup - AMI
      Main  Advanced  Chipset  Security  Boot  Save & Exit

 ▶ Connectivity Configuration                    Configure Connectivity related
 ▶ CPU Configuration                             options
 ▶ Power & Performance
 ▶ PCH-FW Configuration
 ▶ ACPI Settings
 ▶ Super IO Configuration
 ▶ Hardware Monitor
 ▶ USB Configuration
 ▶ Network Stack Configuration
 ▶ NVMe Configuration

                                                 →←: Select Screen
                                                 ↑↓: Select Item
                                                 Enter: Select
                                                 +/-: Change Opt.
                                                 F1: General Help
                                                 F2: Previous Values
                                                 F3: Optimized Defaults
                                                 F4: Save & Exit
                                                 ESC: Exit



                   Version 2.21.1278 Copyright (C) 2022 AMI
```

Advanced Settings:

- Connectivity Configuration

- CPU Configuration

- Power & Performance

- PCH-FW Configuration

- ACPI Settings

- Super IO Configuration

- Hardware Monitor

- USB Configuration

- Network Stack Configuration

- NVMe Configuration

4.4.1   Connectivity Configuration

BIOS Setting	Description
CNV1 Mode	This option configures connectivity. Auto Detection means that if Discrete solution is discovered it will be enabled by default. Otherwise Integrated solution (CNV1) will be enabled. Disable Integrated disables Integrated Solution.
Discrete Bluetooth Module	Serial I/O UART0 needs to be enabled to select BT module.
Advanced settings	Configures ACPI objects for wireless devices.
WWAN Configuration	Configure WWAN related options.

iBASE

4.4.2 CPU Configuration

4.4.3   Power & Performance

```
                          Aptio Setup – AMI
  Advanced

  Power & Performance                          CPU – Power Management Control
                                               Options
▶ CPU – Power Management Control




                                               →←: Select Screen
                                               ↑↓: Select Item
                                               Enter: Select
                                               +/–: Change Opt.
                                               F1: General Help
                                               F2: Previous Values
                                               F3: Optimized Defaults
                                               F4: Save & Exit
                                               ESC: Exit



                  Version 2.21.1278 Copyright (C) 2022 AMI
```

```
  CPU – Power Management Control                Select the performance state
                                                that the BIOS will set
  Boot performance mode          [Turbo Performance]   starting from reset vector.
  Intel(R) SpeedStep(tm)         [Enabled]
  Intel(R) Speed Shift Technology [Enabled]
  Turbo Mode                     [Enabled]



                        ┌─── Boot performance mode ───┐
                        │ Max Battery                 │
                        │ Max Non-Turbo Performance   │
                        │ Turbo Performance           │
                                                       →: Select Screen
```

```
  CPU – Power Management Control                Allows more than two frequency
                                                ranges to be supported.
  Boot performance mode          [Turbo Performance]
  Intel(R) SpeedStep(tm)         [Enabled]
  Intel(R) Speed Shift Technology [Enabled]
  Turbo Mode                     [Enabled]



                        ┌─── Intel(R) SpeedStep(tm) ───┐
                        │ Disabled                     │
                        │ Enabled                      │
                                                        →: Select Screen
```

```
  CPU – Power Management Control                Enable/Disable Intel(R) Speed
                                                Shift Technology support.
  Boot performance mode          [Turbo Performance]   Enabling will expose the CPPC
  Intel(R) SpeedStep(tm)         [Enabled]       v2 interface to allow for
  Intel(R) Speed Shift Technology [Enabled]      hardware controlled P-states.
  Turbo Mode                     [Enabled]



                        ┌─── Intel(R) Speed Shift Technology ───┐
                        │ Disabled                              │
                        │ Enabled                               │
```

```
  CPU – Power Management Control                Enable/Disable processor Turbo
                                                Mode (requires Intel Speed
  Boot performance mode          [Turbo Performance]   Step or Intel Speed Shift to
  Intel(R) SpeedStep(tm)         [Enabled]       be available and enabled).
  Intel(R) Speed Shift Technology [Enabled]
  Turbo Mode                     [Enabled]
```

iBASE

4.4.4   PCH-FW Configuration

```
                          Aptio Setup - AMI
     Main  Advanced  Chipset  Security  Boot  Save & Exit
  ┌──────────────────────────────────────┬───────────────────────────────┐
  │ ▶ Connectivity Configuration         │ Configure Management Engine    │
  │ ▶ CPU Configuration                  │ Technology Parameters          │
  │ ▶ Power & Performance                │                                │
  │ ▶ PCH-FW Configuration               │                                │
  │ ▶ ACPI Settings                      │                                │
  │ ▶ Super IO Configuration             │                                │
  │ ▶ Hardware Monitor                   │                                │
  │ ▶ USB Configuration                  │                                │
  │ ▶ Network Stack Configuration        │                                │
  │ ▶ NVMe Configuration                 │                                │
  │                                      │                                │
  │                                      │ ↔: Select Screen               │
  │                                      │ ↑↓: Select Item                │
  │                                      │ Enter: Select                  │
  │                                      │ +/-: Change Opt.               │
  │                                      │ F1: General Help               │
  │                                      │ F2: Previous Values            │
  │                                      │ F3: Optimized Defaults         │
  │                                      │ F4: Save & Exit                │
  │                                      │ ESC: Exit                      │
  │                                      │                                │
  └──────────────────────────────────────┴───────────────────────────────┘
              Version 2.21.1278 Copyright (C) 2022 AMI
```

```
  ME Firmware Version        14.0.39.1339        When Disabled ME will be put
  ME Firmware Mode           Normal Mode         into ME Temporarily Disabled
  ME Firmware SKU            Corporate SKU       Mode.

  ME State                   [Enabled]

                          ┌─── ME State ───┐
                          │ Disabled       │
                          │ Enabled        │
                          └────────────────┘
                                                 ↔: Select Screen
```

4.4.5   ACPI Settings

iBASE

4.4.6   Super IO Configuration

Serial Port 1 Configuration
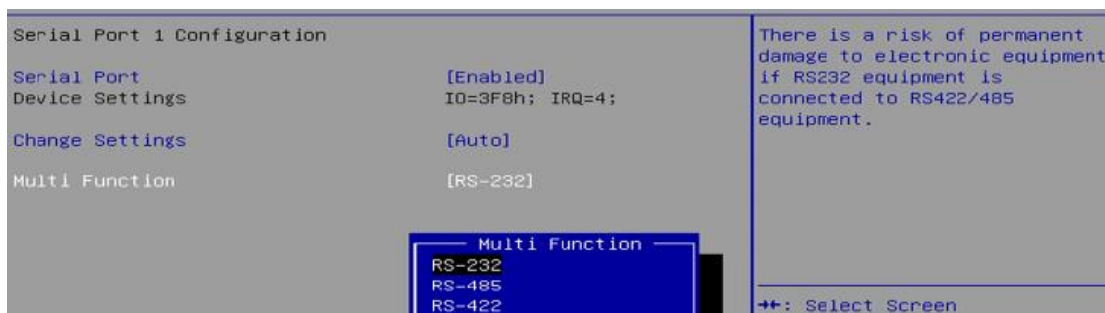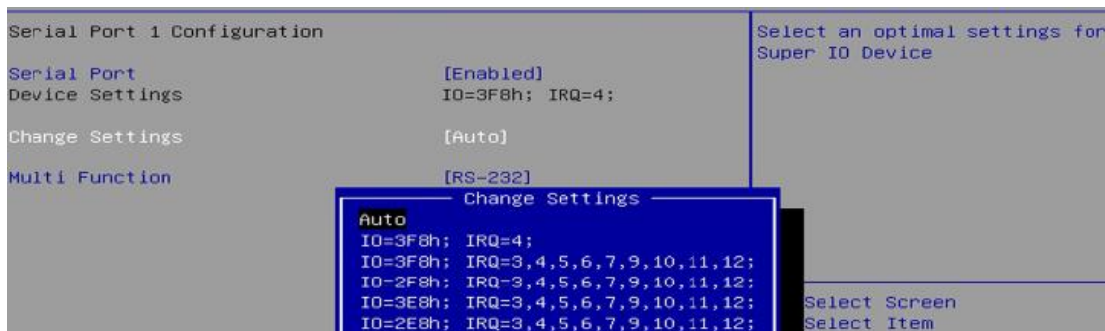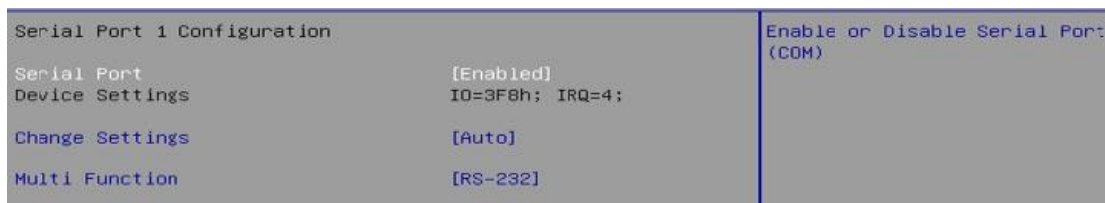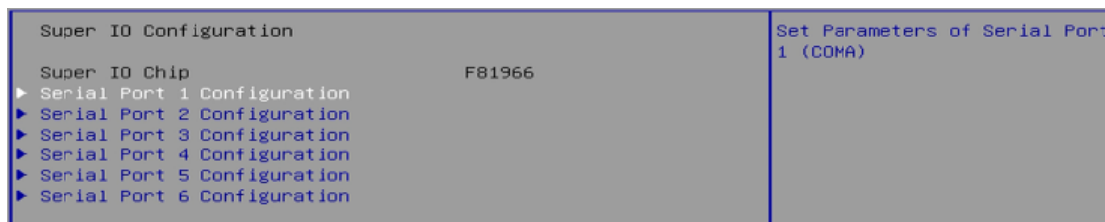
Serial Port 2 Configuration

```
  Super IO Configuration                              Set Parameters of Serial Port
                                                      2 (COMB)
  Super IO Chip                    F81966
▶ Serial Port 1 Configuration
▶ Serial Port 2 Configuration
▶ Serial Port 3 Configuration
▶ Serial Port 4 Configuration
▶ Serial Port 5 Configuration
▶ Serial Port 6 Configuration
```

```
Serial Port 2 Configuration                           Enable or Disable Serial Port
                                                      (COM)
Serial Port                        [Enabled]
Device Settings                    IO=2F8h; IRQ=3;

Change Settings                    [Auto]
```

```
Serial Port 2 Configuration                           Select an optimal settings for
                                                      Super IO Device
Serial Port                        [Enabled]
Device Settings                    IO=2F8h; IRQ=3;

Change Settings                    [Auto]

                  ┌──── Change Settings ────┐
                  │ Auto                     │
                  │ IO=2F8h; IRQ=3;          │
                  │ IO=3F8h; IRQ=3,4,5,6,7,9,10,11,12; │
                  │ IO-2F8h; IRQ-3,4,5,6,7,9,10,11,12; │
                  │ IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12; │ Select Screen
                  │ IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12; │ Select Item
                  └──────────────────────────┘
```

Serial Port 3 Configuration

```
  Super IO Configuration                              Set Parameters of Serial Port
                                                      3 (COMC)
  Super IO Chip                    F81966
▶ Serial Port 1 Configuration
▶ Serial Port 2 Configuration
▶ Serial Port 3 Configuration
▶ Serial Port 4 Configuration
▶ Serial Port 5 Configuration
▶ Serial Port 6 Configuration
```

```
Serial Port 3 Configuration                           Enable or Disable Serial Port
                                                      (COM)
Serial Port                        [Enabled]
Device Settings                    IO=3E8h; IRQ=5;

Change Settings                    [Auto]
```

```
Serial Port 3 Configuration                           Select an optimal settings for
                                                      Super IO Device
Serial Port                        [Enabled]
Device Settings                    IO=3E8h; IRQ=5;

Change Settings                    [Auto]

                  ┌──── Change Settings ────┐
                  │ Auto                     │
                  │ IO=3E8h; IRQ=5;          │
                  │ IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12; │
                  │ IO-2E8h; IRQ-3,4,5,6,7,9,10,11,12; │
                  │ IO=2F0h; IRQ=3,4,5,6,7,9,10,11,12; │ Select Screen
                  │ IO=2E0h; IRQ=3,4,5,6,7,9,10,11,12; │ Select Item
                  └──────────────────────────┘
```

iBASE

Serial Port 4 Configuration

Super IO Configuration | Set Parameters of Serial Port 4 (COMD)

Super IO Chip   F81966
▶ Serial Port 1 Configuration
▶ Serial Port 2 Configuration
▶ Serial Port 3 Configuration
▶ Serial Port 4 Configuration
▶ Serial Port 5 Configuration
▶ Serial Port 6 Configuration

Serial Port 4 Configuration | Enable or Disable Serial Port (COM)

Serial Port   [Enabled]
Device Settings   IO=2E8h; IRQ=7;

Change Settings   [Auto]

Serial Port 4 Configuration | Select an optimal settings for Super IO Device

Serial Port   [Enabled]
Device Settings   IO=2E8h; IRQ=7;

Change Settings   [Auto]

```
──────── Change Settings ────────
Auto
IO=2E8h; IRQ=7;
IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12;
IO=2E8h; IRQ-3,4,5,6,7,9,10,11,12;
IO=2F0h; IRQ=3,4,5,6,7,9,10,11,12;
IO=2E0h; IRQ=3,4,5,6,7,9,10,11,12;
```
Select Screen
Select Item

Serial Port 5 Configuration

Super IO Configuration | Set Parameters of Serial Port 5 (COME)

Super IO Chip   F81966
▶ Serial Port 1 Configuration
▶ Serial Port 2 Configuration
▶ Serial Port 3 Configuration
▶ Serial Port 4 Configuration
▶ Serial Port 5 Configuration
▶ Serial Port 6 Configuration

Serial Port 5 Configuration | Enable or Disable Serial Port (COM)

Serial Port   [Enabled]
Device Settings   IO=2F0h; IRQ=10;

Change Settings   [Auto]

Serial Port 5 Configuration | Select an optimal settings for Super IO Device

Serial Port   [Enabled]
Device Settings   IO=2F0h; IRQ=10;

Change Settings   [Auto]

```
──────── Change Settings ────────
Auto
IO=2F0h; IRQ=10;
IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12;
IO=2E8h; IRQ-3,4,5,6,7,9,10,11,12;
IO=2F0h; IRQ=3,4,5,6,7,9,10,11,12;
IO=2E0h; IRQ=3,4,5,6,7,9,10,11,12;
```
Select Screen
Select Item

Serial Port 6 Configuration

iBASE

4.4.7   Hardware Monitor

BIOS Setting	Description
Smart Fan Function	This field enables or disables the smart fan feature. Options: Disabled (default), 50 ℃, 60℃, 70℃, 80℃, 90℃
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

```
                         Aptio Setup - AMI
     Main  Advanced  Chipset  Security  Boot  Save & Exit

  ▶ Connectivity Configuration                    USB Configuration Parameters
  ▶ CPU Configuration
  ▶ Power & Performance
  ▶ PCH-FW Configuration
  ▶ ACPI Settings
  ▶ Super IO Configuration
  ▶ Hardware Monitor
  ▶ USB Configuration
  ▶ Network Stack Configuration
  ▶ NVMe Configuration
```

```
  USB Configuration

  USB Module Version               24

  USB Controllers:
       1 XHCI
  USB Devices:
       1 Keyboard

  Legacy USB Support               [Enabled]
  XHCI Hand-off                    [Enabled]
  USB Mass Storage Driver Support  [Enabled]

  USB hardware delays and time-outs:
  USB transfer time-out            [20 sec]
  Device reset time-out            [20 sec]
  Device power-up delay            [Auto]
```

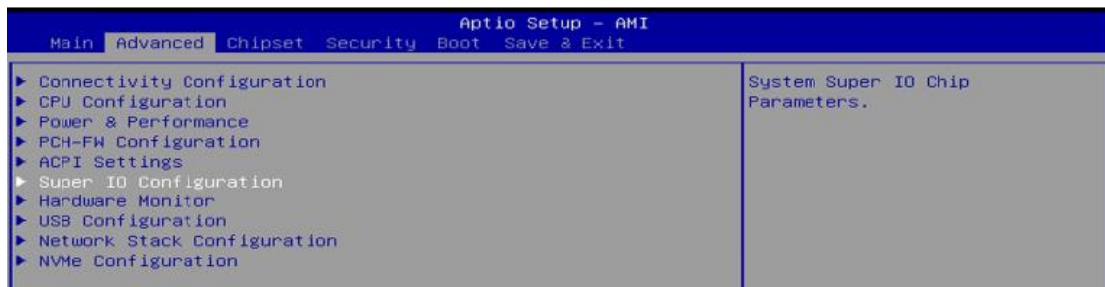| BIOS Setting	Description
Legacy USB Support	• **Enable:** Enables Legacy USB Support. • **Auto:** Disables legacy support if no USB devices are connected. • **Disable:** Keeps USB devices available only for EFI applications.
XHCI Hand-off	This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.
USB Mass Storage Driver Support	Enables / Disables the support for USB mass storage driver.
USB Transfer time-out	The time-out value for Control, Bulk, and Interrupt transfers.
Device reset time-out	Seconds of delaying execution of start unit command to USB mass storage device.
Device power-up delay	The 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 100ms. But for a Hub port, the delay is taken from Hub descriptor.

iBASE

4.4.9   Network Stack Configuration
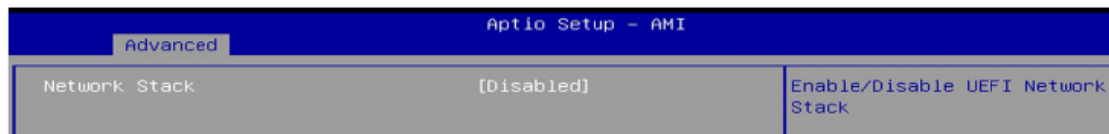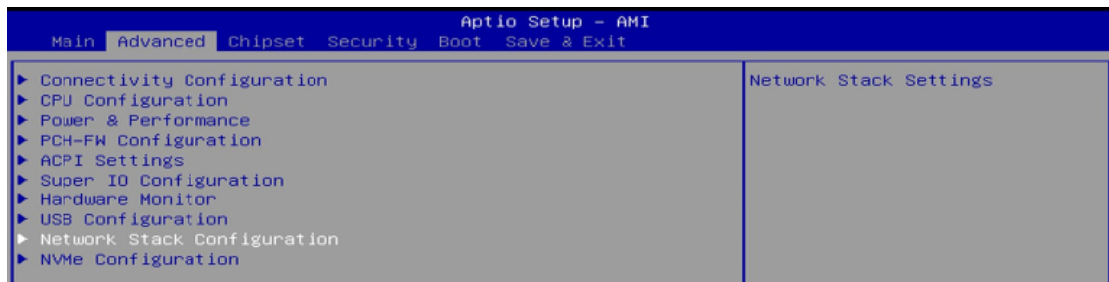
BIOS Setting	Description
Ipv4 PXE Support	Enable/Disable Ipv4 PXE boot support. If disabled, Ipv4 PXE boot support will not be available.
Ipv4 HTTP Support	Enable/Disable Ipv4 HTTP boot support. If disabled, Ipv4 HTTP boot support will not be available.
PXE boot wait time	Wait time in seconds to press 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 +/- or numeric keys to set the value.

4.4.10   NVMe Configuration

```
                          Aptio Setup - AMI
    Main  Advanced  Chipset  Security  Boot  Save & Exit

  ▶ Connectivity Configuration                    NVMe Device Options Settings
  ▶ CPU Configuration
  ▶ Power & Performance
  ▶ PCH-FW Configuration
  ▶ ACPI Settings
  ▶ Super IO Configuration
  ▶ Hardware Monitor
  ▶ USB Configuration
  ▶ Network Stack Configuration
  ▶ NVMe Configuration
```

```
  NVMe Configuration

  No NVME Device Found
```

iBASE
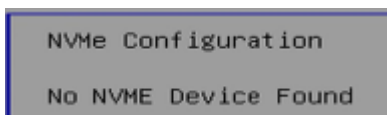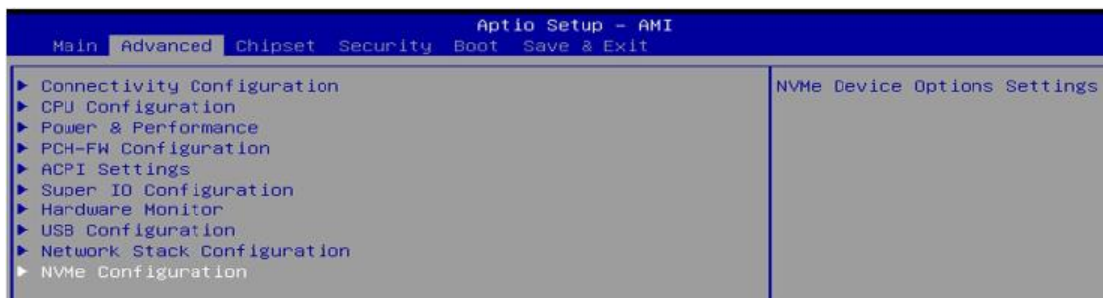
4.5 Chipset Settings
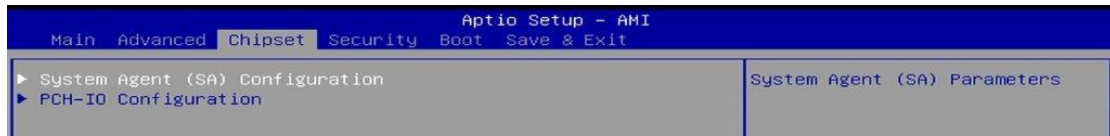
BIOS Setting	Description
System Agent (SA) Configuration	System Agent (SA) parameters
PCH-IO Configuration	PCH parameters

4.5.1 System Agent (SA) Configuration
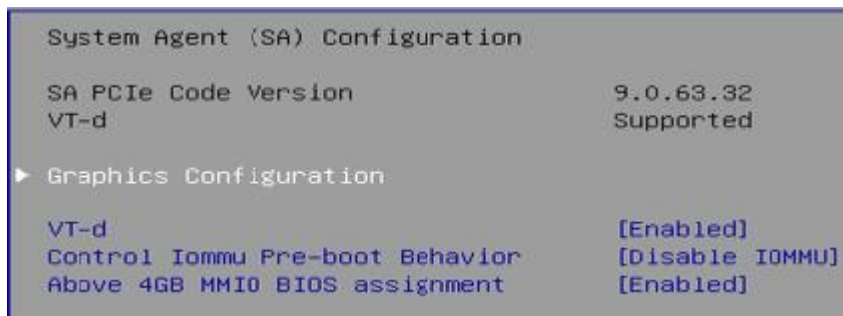
BIOS Setting	Description
Graphics Configuration	Configures the graphics settings.
VT-d	Checks if VT-d function on MCH is supported.
Control Iommu Pre-boot Behavior	Enable dTBT and PCH USB topology IOMMU in Pre-boot environment (If DMAR table is installed in DXE and If VTD_INF_PPI is installed in PEI.) TBT tree won't be included in the exception list.
Above 4GB MMIO BIOS assignment	Enable/Disable above 4GB MemoryMppedIO BIOS assignment. This is enabled automatically when Aperture Size is set to 2048MB.

4.5.1.1. Graphics Configuration

4.5.2   PCH-IO Configuration

```
▶ System Agent (SA) Configuration                    PCH Parameters
▶ PCH-IO Configuration
```

```
  PCH-IO Configuration                         SATA Device Options Settings

▶ SATA And RST Configuration
```

4.5.2.1. SATA Configuration:

```
SATA And RST Configuration

SATA Controller(s)                        [Enabled]
SATA Mode Selection                       [AHCI]

Serial ATA Port 0                         Empty
  Port 0                                  [Enabled]
Serial ATA Port 1                         Empty
  Port 1                                  [Enabled]
Serial ATA Port 2                         Empty
  Port 2                       ┌──── SATA Controller(s) ─
Serial ATA Port 3             │ Enabled
  Port 3                       │ Disabled
Serial ATA Port 4             │
  Port 4                       │
Serial ATA Port 5                         Empty
  Port 5                                  [Enabled]
Serial ATA Port 6                         Empty
  Port 6                                  [Enabled]
Serial ATA Port 7                         Empty
  Port 7                                  [Enabled]
```

BIOS Setting	Description
SATA Controller(s)	Enables / Disables the SATA device.
SATA Mode Selection	Determines how SATA controller(s) operate. Options: AHCI / Intel RST Premium with Intel Optane System Acceleration
Serial ATA Ports	Enables / Disables serial ports.

4.6   Security Settings

```
                                           Aptio Setup - AMI
     Main  Advanced  Chipset  Security  Boot  Save & Exit

    Password Description

    If ONLY the Administrator's password is set,
    then this only limits access to Setup and is
    only asked for when entering Setup.
    If ONLY the User's password is set, then this
    is a power on password and must be entered to
    boot or enter Setup. In Setup the User will
    have Administrator rights.
    The password length must be
    in the following range:
    Minimum length                          3
    Maximum length                          20

    Administrator Password
    User Password


  ▶ Secure Boot
```

BIOS Setting	Description
Administrator Password	Sets an administrator password for the setup utility.
User Password	Sets a user password.
Secure Boot	Configures Secure Boot.

iBASE

4.6.1 Secure Boot

BIOS Setting	Description
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. Deleting all variables will reset the System to Setup Mode.
Key Management	Enables expert users to modify Secure Boot Policy variables without full authentication.

```
Vendor Keys                          Valid                   Copy NVRAM content of Secure
                                                             Boot variables to files in a
    Factory Key Provision            [Enabled]               root folder on a file system
  ► Restore Factory Keys                                     device
  ► Reset To Setup Mode
  ► Export Secure Boot variables
```

```
Vendor Keys                          Valid                   Allow the image to run in
                                                             Secure Boot mode.
    Factory Key Provision            [Enabled]               Enroll SHA256 Hash certificate
  ► Restore Factory Keys                                     of a PE image into Authorized
  ► Reset To Setup Mode                                      Signature Database (db)
  ► Export Secure Boot variables
  ► Enroll Efi Image
```

```
Vendor Keys                          Valid                   Device Guard ready system must
                                                             not list 'Microsoft UEFI CA'
    Factory Key Provision            [Enabled]               Certificate in Authorized
  ► Restore Factory Keys                                     Signature database (db)
  ► Reset To Setup Mode
  ► Export Secure Boot variables
  ► Enroll Efi Image

    Device Guard Ready
  ► Remove 'UEFI CA' from DB    ┌──── Remove 'UEFI CA' from DB ────
                                │
```

```
Vendor Keys                          Valid                   Restore DB variable to factory
                                                             defaults
    Factory Key Provision            [Enabled]
  ► Restore Factory Keys
  ► Reset To Setup Mode
  ► Export Secure Boot variables
  ► Enroll Efi Image

    Device Guard Ready
  ► Remove 'UEFI CA' from DB    ┌──── Restore DB defaults ────
  ► Restore DB defaults         │
```

```
Vendor Keys                          Valid                   Enroll Factory Defaults or
                                                             load certificates from a file:
    Factory Key Provision            [Enabled]                1.Public Key Certificate:
  ► Restore Factory Keys                                        a)EFI_SIGNATURE_LIST
  ► Reset To Setup Mode                                         b)EFI_CERT_X509 (DER)
  ► Export Secure Boot variables                               c)EFI_CERT_RSA2048 (bin)
  ► Enroll Efi Image                                           d)EFI_CERT_SHAXXX
                                                              2.Authenticated UEFI Variable
    Device Guard Ready                                        3.EFI PE/COFF Image(SHA256)
  ► Remove 'UEFI CA' from DB      ┌─────────────────────┐    Key Source:
  ► Restore DB defaults           │  Platform Key(PK)   │      Factory,External,Mixed
                                  │ Details             │
    Secure Boot variable | Size| Ke│ Export              │    ↔↔: Select Screen
  ► Platform Key(PK)       |  862|  │ Update              │    ↑↓: Select Item
  ► Key Exchange Keys      | 1560|  │ Delete              │    Enter: Select
  ► Authorized Signatures| 3143|   └─────────────────────┘    +/-: Change Opt.
  ► Forbidden  Signatures| 3724|  77| Factory                 F1: General Help
  ► Authorized TimeStamps|    0|   0| No Keys                 F2: Previous Values
  ► OsRecovery Signatures|    0|   0| No Keys
```

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.
Boot Option Priorities	Sets the system boot order.
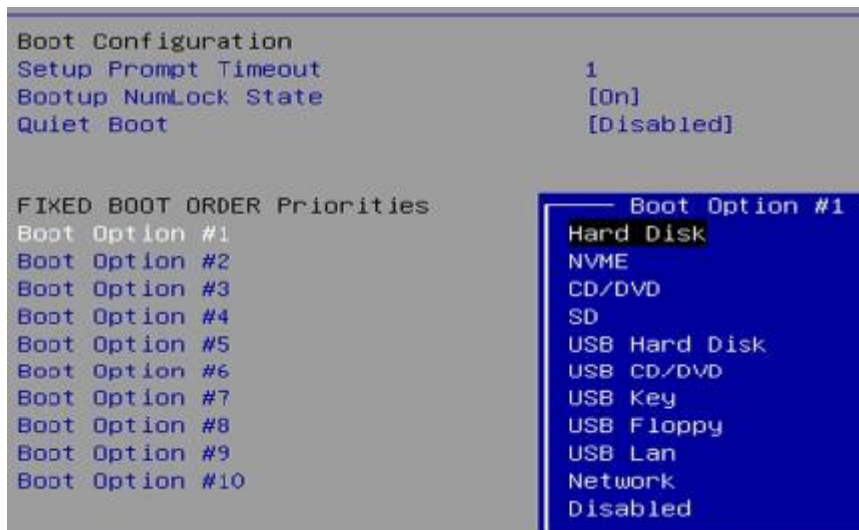
4.8 Save & Exit Settings

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 defaults 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.

Appendix

This section provides the mapping addresses of peripheral devices and the sample code of watchdog timer configuration.

- I/O Port Address Map
- Interrupt Request Lines (IRQ)
- Watchdog Timer Configuration
- Software Development Kit for WDT.DLL

A. I/O Port Address Map

Each peripheral device in the system is assigned a set of I/O port addresses which also becomes the identity of the device. The following table lists the I/O port addresses used.

Address	Device Description
0x00000A00-0x00000A0F	Motherboard resources
0x00000A10-0x00000A1F	Motherboard resources
0x00000A20-0x00000A2F	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
0x00003000-0x0000303F	Microsoft Basic Display Adapter
0x000000F0-0x000000F0	Numeric data processor
0x0000EFA0-0x0000EFBF	SM Bus Controller
0x000003F8-0x000003FF	Communications Port (COM1)
0x000002F8-0x000002FF	Communications Port (COM2)
0x000003E8-0x000003EF	Communications Port (COM3)
0x000002E8-0x000002EF	Communications Port (COM4)
0x000002F0-0x000002F7	Communications Port (COM5)
0x000002E0-0x000002E7	Communications Port (COM6)
0x00000040-0x00000043	System timer
0x00000050-0x00000053	System timer
0x00001800-0x000018FE	Motherboard resources
0x00000000-0x00000CF7	PCI Express Root Complex

iBASE

Address	Device Description
0x00000D00-0x0000FFFF	PCI Express Root Complex
0x00002000-0x000020FE	Motherboard resources
0x00000060-0x00000060	Standard PS/2 Keyboard
0x00000064-0x00000064	Standard PS/2 Keyboard
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
0x000000B0-0x000000B1	Programmable interrupt controller
0x000000B4-0x000000B5	Programmable interrupt controller
0x000000B8-0x000000B9	Programmable interrupt controller
0x000000BC-0x000000BD	Programmable interrupt controller
0x000004D0-0x000004D1	Programmable interrupt controller
0x00003090-0x00003097	Standard SATA AHCI Controller
0x00003080-0x00003083	Standard SATA AHCI Controller
0x00003060-0x0000307F	Standard SATA AHCI Controller
0x00001854-0x00001857	Motherboard resources

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	PCI Express Root Port
IRQ 4294967292	PCI Express Root Port
IRQ 13	Numeric data processor
IRQ 16	High Definition Audio Controller
IRQ 4294967294	PCI Express Root Port
IRQ 4	Communications Port (COM1)
IRQ 3	Communications Port (COM2)
IRQ 5	Communications Port (COM3)
IRQ 7	Communications Port (COM4)
IRQ 10	Communications Port (COM5)
IRQ 11	Communications Port (COM6)
IRQ 0	System timer
IRQ 55~204	Microsoft ACPI-Compliant System
IRQ 256~511	Microsoft ACPI-Compliant System
IRQ 19	Intel SD Host Controller
IRQ 1024	Intel SD Host Controller
IRQ 4294967290	Intel(R) USB 3.1 eXtensible Host Controller - 1.10 (Microsoft)
IRQ 1	Standard PS/2 Keyboard
IRQ 12	Microsoft PS/2 Mouse
IRQ 14	Intel(R) Serial IO GPIO Host Controller - INT3450
IRQ 4294967291	Standard SATA AHCI Controller

iBASE

C. Watchdog Timer Configuration

The Watchdog Timer (WDT) is used to generate a variety of output signals after a user programmable count. The WDT is suitable for the use in the prevention of system lock-up, such as when software becomes trapped in a deadlock. Under these sorts of circumstances, the timer will count to zero and the selected outputs will be driven.

Under normal circumstance, you will need to restart the WDT at regular intervals before the timer counts to zero.

Sample Code:

```
//-------------------------------------------------------------------------
//
// THIS CODE AND INFORMATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY
// KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE
// IMPLIED WARRANTIES OF MERCHANTABILITY AND/OR FITNESS FOR A PARTICULAR
// PURPOSE.
//
//-------------------------------------------------------------------------
#include <dos.h>
#include <conio.h>
#include <stdio.h>
#include <stdlib.h>
#include "F81866.H"
//-------------------------------------------------------------------------
int main (int argc, char *argv[]);  void EnableWDT(int);
void DisableWDT(void);
//-------------------------------------------------------------------------
int main (int argc, char *argv[])
{
unsigned char bBuf;  unsigned char bTime;  char **endptr;

char SIO;
printf("Fintek 81866 watch dog program\n");  SIO = Init_F81866();
if (SIO == 0)
{
printf("Can not detect Fintek 81866, program abort.\n");  return(1);
}//if (SIO == 0)

if (argc != 2)
{
printf(" Parameter incorrect!!\n");  return (1);
}

bTime = strtol (argv[1], endptr, 10);
printf("System will reset after %d seconds\n", bTime);

if (bTime)
{     EnableWDT(bTime);    } else
{     DisableWDT();   } return 0;
```

```
}
//-------------------------------------------------------------------------
void EnableWDT(int interval)
{
unsigned char bBuf;

bBuf = Get_F81866_Reg(0x2B); bBuf &= (~0x20);
Set_F81866_Reg(0x2B, bBuf);   //Enable WDTO

Set_F81866_LD(0x07);      //switch to logic device 7
Set_F81866_Reg(0x30, 0x01); //enable timer

bBuf = Get_F81866_Reg(0xF5); bBuf &= (~0x0F);
bBuf |= 0x52;
Set_F81866_Reg(0xF5, bBuf);          //count mode is second  Set_F81866_Reg(0xF6,
interval);   //set timer
bBuf = Get_F81866_Reg(0xFA); bBuf |= 0x01;
Set_F81866_Reg(0xFA, bBuf);   //enable WDTO output

bBuf = Get_F81866_Reg(0xF5); bBuf |= 0x20;
Set_F81866_Reg(0xF5, bBuf);   //start counting
}
//-------------------------------------------------------------------------
void DisableWDT(void)
{
unsigned char bBuf;
Set_F81866_LD(0x07);      //switch to logic device 7  bBuf = Get_F81866_Reg(0xFA);
bBuf &= ~0x01;
Set_F81866_Reg(0xFA, bBuf);   //disable WDTO output

bBuf = Get_F81866_Reg(0xF5); bBuf &= ~0x20;
bBuf |= 0x40;
Set_F81866_Reg(0xF5, bBuf);   //disable WDT
}
//-------------------------------------------------------------------------
```

iBASE

```
//-----------------------------------------------------------------------
//
// THIS CODE AND INFORMATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY
// KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE
// IMPLIED WARRANTIES OF MERCHANTABILITY AND/OR FITNESS FOR A PARTICULAR
// PURPOSE.
//
//-----------------------------------------------------------------------
#include "F81866.H"
#include <dos.h>
//-----------------------------------------------------------------------
unsigned int F81866_BASE; void Unlock_F81866 (void); void Lock_F81866 (void);
//-----------------------------------------------------------------------
unsigned int Init_F81866(void)
{
unsigned int result; unsigned char ucDid;

F81866_BASE = 0x4E;
result = F81866_BASE;

ucDid = Get_F81866_Reg(0x20);
if (ucDid == 0x07)      //Fintek 81866
{       goto Init_Finish; }

F81866_BASE = 0x2E;
result = F81866_BASE;

ucDid = Get_F81866_Reg(0x20);
if (ucDid == 0x07)      //Fintek 81866
{       goto Init_Finish; }

F81866_BASE = 0x00;
result = F81866_BASE;

Init_Finish:
return (result);
}
//-----------------------------------------------------------------------
void Unlock_F81866 (void)
{
outportb(F81866_INDEX_PORT, F81866_UNLOCK); outportb(F81866_INDEX_PORT,
F81866_UNLOCK);
}
//-----------------------------------------------------------------------
void Lock_F81866 (void)
{
outportb(F81866_INDEX_PORT, F81866_LOCK);
}
//-----------------------------------------------------------------------
void Set_F81866_LD( unsigned char LD)
{
Unlock_F81866();
outportb(F81866_INDEX_PORT, F81866_REG_LD);
outportb(F81866_DATA_PORT, LD); Lock_F81866();
```

```
}
//------------------------------------------------------------------------
void Set_F81866_Reg( unsigned char REG, unsigned char DATA)
{
Unlock_F81866(); outportb(F81866_INDEX_PORT, REG); outportb(F81866_DATA_PORT,
DATA); Lock_F81866();
}
//------------------------------------------------------------------------
unsigned char Get_F81866_Reg(unsigned char REG)
{
unsigned char Result; Unlock_F81866();
outportb(F81866_INDEX_PORT, REG); Result = inportb(F81866_DATA_PORT);
Lock_F81866();
return Result;
}
//------------------------------------------------------------------------
```



```
//------------------------------------------------------------------------
//
// THIS CODE AND INFORMATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY
// KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE
// IMPLIED WARRANTIES OF MERCHANTABILITY AND/OR FITNESS FOR A PARTICULAR
// PURPOSE.
//
//------------------------------------------------------------------------
#ifndef     F81866_H
#define     F81866_H     1
//------------------------------------------------------------------------
#defineF81866_INDEX_PORT   (F81866_BASE)
#defineF81866_DATA_PORT    (F81866_BASE+1)
//------------------------------------------------------------------------
#defineF81866_REG_LD   0x07
//------------------------------------------------------------------------
#define F81866_UNLOCK  0x87
#defineF81866_LOCK        0xAA
//------------------------------------------------------------------------
unsigned int Init_F81866(void);
void Set_F81866_LD( unsigned char);
void Set_F81866_Reg( unsigned char, unsigned char); unsigned char
Get_F81866_Reg( unsigned char);
//------------------------------------------------------------------------
#endif //     F81866_H
```

iBASE

D. Software Development Kit for WDT.DLL

1. OS Supported

Windows SP (32-bit / 64-bit) or above

2. Driver Installation

● **For 32-bit environment:**

Step 1:
Copy the file **KMUI32_1K.SYS** to <%WINDIR%>\SYSTEM32\DRIVERS.

Step 2:
The following parameters must be written to your registry.

HKLM,"System\CurrentControlSet\Services\KMUI32_1K","ErrorControl",%REG_DWORD%,0x00000001

HKLM,"System\CurrentControlSet\Services\KMUI32_1K","Type",%REG_DWORD%,0x00000001

HKLM,"System\CurrentControlSet\Services\KMUI32_1K","Start",%REG_DWORD%,0x00000000

HKLM,"System\CurrentControlSet\Services\KMUI32_1K","DisplayName",%REG_SZ%,"KMUI32_1K"

Step 3:
Restart the system.

● **For 64-bit environment:**

Step 1:
Copy "KMUI64_1K.SYS" file to <%WINDIR%>\SYSTEM32\DRIVERS

Step 2:
The following parameters must be written to your registry.

HKLM,"System\CurrentControlSet\Services\KMUI64_1K","ErrorControl",
%REG_DWORD%,0x00000001

HKLM,"System\CurrentControlSet\Services\
KMUI64_1K","Type",%REG_DWORD%,0x00000001

HKLM,"System\CurrentControlSet\Services\
KMUI64_1K","Start",%REG_DWORD%,0x00000000

HKLM,"System\CurrentControlSet\Services\
KMUI64_1K","DisplayName",%REG_SZ%,"KMUI64_1K"

Step 3:
Restart the system.

Note: Do not install both of the 32-bit and 64-bit drivers on an operating
system.

---

iBASE

3. Exportion from IB_WDT.DLL / IB_WDT.64.DLL

extern "C" __declspec(dllexport) int __stdcall InstallDriver(void);
extern "C" __declspec(dllexport) int __stdcall RemoveDriver(void);
extern "C" __declspec(dllexport) char* __stdcall GetWDTInfo(void);
extern "C" __declspec(dllexport) int __stdcall EnableWDT(int);
extern "C" __declspec(dllexport) int __stdcall DisableWDT(int);
extern "C" __declspec(dllexport) int __stdcall IsDioAvailable(int);
extern "C" __declspec(dllexport) int __stdcall SetDioInputMask(int);
extern "C" __declspec(dllexport) int __stdcall SetDioOutputMask(int);
extern "C" __declspec(dllexport) int __stdcall GetDioInput(int);
extern "C" __declspec(dllexport) int __stdcall SetDioOutput(int);

Note:

1. The **IB_WDT.DLL** is of 32-bit and works on 32-bit and 64-bit Windows operating system. The "IB_WDT.64.DLL" is for 64bit Windows only.

2. The routines are not thread-safe. Your software engineers should take the responsibility to avoid multi-entry condition.

● **Driver Initialization & Deinitalization**

extern "C" __declspec(dllexport) int __stdcall InstallDriver(void);

Input : None
Output : Return 1 if device driver loads successfully; otherwise return 0.

Note: This function should be invoked before Watchdog and Digital I/O routines.

extern "C" __declspec(dllexport) int __stdcall RemoveDriver(void);

Input : None
Output : Always return 1.

Note: This function should be invoked before the program closes and it will release the device driver and memory for **ib_wdt.dll**. If the program is closed without calling this routine, resource leak may occur.

● **Watchdog**

extern "C" __declspec(dllexport) char * __stdcall GetWDTInfo(void);

Input   : None

Output   : Return a string that describes the module information.

extern "C" __declspec(dllexport) int __stdcall EnableWDT(int);

Input   : Timer interval, depending on the WDT chip

Output   : Always return "0"

For further information, refer to the datasheet for WDT or contact your sales representative.

extern "C" __declspec(dllexport) int __stdcall DisableWDT(int);

Input   : Dummy data and will be ignored.

Output   : Always return "0"

iBASE

● **Digital I/O**

extern "C" __declspec(dllexport) int __stdcall IsDioAvailable(int);

Input   : Dummy data and will be ignored

Output   : Return 1 if the digital I/O is available, otherwise return 0.

extern "C" __declspec(dllexport) int __stdcall SetDioInputMask(int);

Input: : Hardware parameter for digital I/O input function call.

For example, the 6 GPIO functions:
GPIO_0 to GPIO_2 are mapped as the input functions, and GPIO_4 to GPIO_6 are mapped as the output functions.

In this case, the parameter for "SetDioInputMask" is 0x07 and it indicates that GPIO_0 to GPIO_2 are the input functions.
The parameter for "SetDioOutputMask" is 0x70 and it indicates that GPIO_4 to GPIO_6 are the output functions.

Output   : Dummy data and should be ignored.

extern "C" __declspec(dllexport) int __stdcall SetDioOutputMask(int);

Input   : Hardware parameter for digital I/O output function call

For further information, refer to the following explanation of "SetDioInputMask" routine.

SetDioInputMask:

```
if ((*lpIsDioAvailable)(0))
        {
                    int DioInput;
                    printf(" Test for digital IO ....\n");

                    //Please check digital IO setting in BIOS setup utility
                    //Here example as follow:
                    //    Digital GPIO [1..3] = Input
                    //    Digital GPIO [4..6] = Output

                    //set hardware information for GPIO chip
                    //bit 0..2 : input for GPIO_0 to GPIO_2
                    //bit 4..6 : output for GPIO_4 to GPIO_6
                (*lpSetDioInputMask)(0x07);
                (*lpSetDioOutputMask)(0x70);

                    DioInput = (*lpGetDioInput)(0);
                    printf(" Current GPIO_0 to GPIO_2 is 0x%X\n", DioInput);

        while(1)
        {
                                (*lpSetDioOutput)(0x00);
                                 printf(" Set GPIO_4 to GPIO_6 to LOW\n");
                                (*lpSetDioOutput)(0x70);
                                 printf(" Set GPIO_4 to GPIO_6 to HIGH\n");
                                (*lpSetDioOutput)(0x30);
                                 printf(" Set GPIO_4 to GPIO_5 to HIGH\n");
                                (*lpSetDioOutput)(0x60);
                                 printf(" Set GPIO_5 to GPIO_6 to HIGH\n");

                                 Sleep(500);
                                 if (_kbhit())
                                 {
                break;
        }//if (kbhit())
                }//while(1)
        }//if ((*lpIsDioAvailable)(0))
```

Note: Be sure to set up the input / output for GPIO bits in BIOS identically with the GPIO hardware information above.

---

iBASE

E. Motherboard MCU ISP Specifications

1. Description

Security MCU provides following functionality

- **Getting Firmware Version**
  Software can get the firmware version, MCU provides commands to get current Major Version, Minor version and build version.

- **Setting Power-On-Delay Timer**
  MCU provides command to set power on delay timer, when arrived the setting time, MCU will send power button to let the system power on.

- **Setting Power-Off-Delay Timer**
  MCU provides command to set power off delay timer, when arrived the setting time, MCU will send power button to let the system power off.

- **Getting Status**
  MCU provides command to get current status which includes the power on delay timer setting value and power off delay timer setting value.

Note: Before using the ISP, your software engineer has to make sure the firmware version (GET_FORMWARE_VERSION) MUST be as follows to make the ISP function workable.

Major version is 0.

Minor version is 0.

Build version is 1 (or above).

---

2. Protocol

- **Signal transmit format**

  Bandwidth
  Baud rate: 19200 bps

  Data Format
  Parity: No Parity
  1 start bit
  8 data bits
  1 stop bit

- **Packet Format**

Header	Size	Command	Data	CRC
2 bytes	1 byte	1 byte	0 – 64 bytes	2 bytes

  Header bytes indicate start of the packet.

  Size specifies number of bytes for data field.

  Command identifies action, which is required to be performed on the data.

  CRC verifies data integrity for header, size, command and data bytes.

- **CRC**

  Protocol uses 16-bit CCITT CRC to verify data integrity.
  $P(x) = X^{16}+X^{12}+X^5+1$

```
unsigned calc_crc(unsigned char *data, unsigned n, unsigned start) {
    unsigned I, k, q, c, crcval;
    crcval=start;
    for (I=0; I<n; I++) {
        c=data(I) & 0xFF;
        q=(crcval^c) & 0x0F;
        crcval=(crcval>>4)^(q*0x1081);
        q=(crcval^(c>>4)) & 0x0F;
        crcval=(crcval>>4)^(q*0x1081);
    }
    return crcval;
}
```

iBASE

- **Communications flow**

  Communication between PC and Security MCU utilizes Master-Slave model, where PC is a master, and Security MCU is a slave. Master sends requests to the slave, and slave has to reply to them. Slave acts like a passive device and cannot send any requests to the master.

3. Command and Reply Codes

- **Summary**

Code	Value	Description
GET_FIRMWARE_VERSION	0x01	Get Firmware version
SET_POWER_ON_DELAY_TIMER	0x04	Power on delay timer setting
SET_POWER_OFF_DELAY_TIMER	0x05	Power off delay timer setting
GET_STATUS	0x10	Get Current Status

- **Getting Firmware Version**

  Parameter: GET_FIRMWARE_VERSION

  Reads version number of the security MCU firmware.

  Request:

Header	Size	Command	Data	CRC
0xFF 0xEE	0x00	GET_FIRMWARE_VERSION	None	

  Reply:

Header	Size	Command	Data	CRC
0xFF 0xEE	Size of Version structure	GET_FIRMWARE_VERSION	BSL Version Structure	

  BSL Version Structure

Field	Type	Description
Major Version	Byte	Major version number
Minor Version	Byte	Minor version number
Build	Byte	Build version number

- **Setting Power-On Delay Timer**

  Parameter: SET_POWER_ON_DELAY_TIMER

  Sets power on delay timer.

  Request:

Header	Size	Command	Data0	Data1	CRC
0xFF 0xEE	0x02	SET_POWER_ON_DELAY_TIMER	N (mins)	N (secs)	

  Reply

Header	Size	Command	Data	CRC
0xFF 0xEE	0x00	SET_POWER_ON_DELAY_TI MER	None	

- **Setting Power-Off Delay Timer**

  Parameter: SET_POWER_OFF_DELAY_TIMER

  Sets power off delay timer.

  Request:

Header	Size	Command	Data0	Data1	CRC
0xFF 0xEE	0x02	SET_POWER_OFF_DELAY_TIMER	N (mins)	N (secs)	

  Reply

Header	Size	Command	Data	CRC
0xFF 0xEE	0x00	SET_POWER_OFF_DELAY_TIMER	None	

iBASE

- **Getting Status**

  Gets the power-on-delay timer and power-off-delay timer.

  Request:

Header	Size	Command	Data	CRC
0xFF 0xEE	0x00	GET_STATUS	None	

  Reply:

Header	Size	Command	Data	CRC
0xFF 0xEE	0x04	GET_STATUS	Status structure	

  BSL Version Structure

Field	Type	Description
Power on delay timer	Word	Byte4+ Byte5
Power off delay timer	Word	Byte6+ Byte7