GIGAIPC™

Mini-ITX Motherboard

mITX-H610B (MH610BI-SI)

mITX-H610B (MH610BI-SI)

mITX-H610B Mini-ITX Motherboard

Copyright Notice

Acknowledgement

All other products' name or trademarks are properties of their respective owners.

- Microsoft Windows is a registered trademark of Microsoft Corp.
- Intel, Pentium, Celeron, and Xeon are registered trademarks of Intel Corporation
- Core, Atom are trademarks of Intel Corporation
- ITE is a trademark of Integrated Technology Express, Inc.
- IBM, PC/AT, PS/2, and VGA are trademarks of International Business Machines Corporation.

All other product names or trademarks are properties of their respective owners.

Mini-ITX Motherboard

mITX-H610B (MH610BI-SI)

Packing List

Before setting up your product, please make sure the following items have been shipped:

Item	Quantity
mITX-H610B MB	1
SATA power cable	1
I/O Shield	1

If any of these items are missing or damaged, please contact your distributor or sales representative immediately.

About this Document

This User's Manual contains all the essential information, such as detailed descriptions and explanations on the product's hardware and software features (if any), its specifications, dimensions, jumper/connector settings/definitions, and driver installation instructions (if any), to facilitate users in setting up their product.

Users may refer to the GIGAIPC.com for the latest version of this document.

Safety Precautions

Please read the following safety instructions carefully. It is advised that you keep this manual for future references

1. All cautions and warnings on the device should be noted.

2. Make sure the power source matches the power rating of the device.

3. Position the power cord so that people cannot step on it. Do not place anything over the power cord.

4. Always completely disconnect the power before working on the system's hardware.

5. No connections should be made when the system is powered as a sudden rush of power may damage sensitive electronic components.

6. If the device is not to be used for a long time, disconnect it from the power supply to avoid damage by transient over-voltage.

7. Always disconnect this device from any AC supply before cleaning.

8. While cleaning, use a damp cloth instead of liquid or spray detergents.

9. Make sure the device is installed near a power outlet and is easily accessible.

10. Keep this device away from humidity.

11. Place the device on a solid surface during installation to prevent falls

12. Do not cover the openings on the device to ensure optimal heat dissipation.

13. Watch out for high temperatures when the system is running.

14. Do not touch the heat sink or heat spreader when the system is running

15. Never pour any liquid into the openings. This could cause fire or electric shock.

16. As most electronic components are sensitive to static electrical charge, be sure to ground yourself to prevent static charge when installing the internal components. Use a grounding wrist strap and contain all electronic components in any static-shielded containers.

17. If any of the following situations arises, please the contact our service personnel:
    i. Damaged power cord or plug
    ii. Liquid intrusion to the device
    iii. Exposure to moisture
    iv. Device is not working as expected or in a manner as described in this manual
    v. The device is dropped or damaged
    vi. Any obvious signs of damage displayed on the device

18. **DO NOT LEAVE THIS DEVICE IN AN UNCONTROLLED ENVIRONMENT WITH TEMPERATURES BEYOND THE DEVICE'S PERMITTED STORAGE TEMPERATURES (SEE CHAPTER 1) TO PREVENT DAMAGE.**

FCC Statement

Warning! This device complies with Part 15 FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received including interference that may cause undesired operation.

Caution:

There is a danger of explosion if the battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions and your local government's recycling or disposal directives.

Attention:

Il y a un risque d'explosion si la batterie est remplacée de façon incorrecte. Ne la remplacer qu'avec le même modèle ou équivalent recommandé par le constructeur. Recycler les batteries usées en accord avec les instructions du fabricant et les directives gouvernementales de recyclage.

GIGAIPC™

China RoHS Requirements (CN)

产品中有毒有害物质或元素名称及含量
GIGAIPC Main Board/ Daughter Board/ Backplane

部件名称	有毒有害物质或元素					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr(VI))	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
印刷电路板 及其电 子组件	○	○	○	○	○	○
外部信号 连接器 及线材	○	○	○	○	○	○
O：表示该有毒有害物质在该部件所有均质材料中的含量均在 SJ/T 11363-2006 标准规定的限量要求以下。 X:表示该有毒有害物质至少在该部件的某一均质材料中的含量超出 SJ/T 11363-2006 标准规定的限量要求。 备注：此产品所标示之环保使用期限，系指在一般正常使用状况下。						

www.gigaipc.com

China RoHS Requirement (EN)

Poisonous or Hazardous Substances or Elements in Products
GIGAIPC Main Board/ Daughter Board/ Backplane

Component	Poisonous or Hazardous Substances or Elements					
	Lead (Pb)	Mercury (Hg)	Cadmium (Cd)	Hexavalent Chromium (Cr(VI))	Polybrominated Biphenyls (PBB)	Polybrominated Diphenyl Ethers (PBDE)
PCB & Other Components	O	O	O	O	O	O
Wires & Connectors for External Connections	O	O	O	O	O	O
O : The quantity of poisonous or hazardous substances or elements found in each of the component's parts is below the SJ/T 11363-2006-stipulated requirement. X: The quantity of poisonous or hazardous substances or elements found in at least one of the component's parts is beyond the SJ/T 11363-2006-stipulated requirement. Note: The Environment Friendly Use Period as labeled on this product is applicable under normal usage only						

Table Contents

Chapter 1

Chapter 1 - Product Specifications
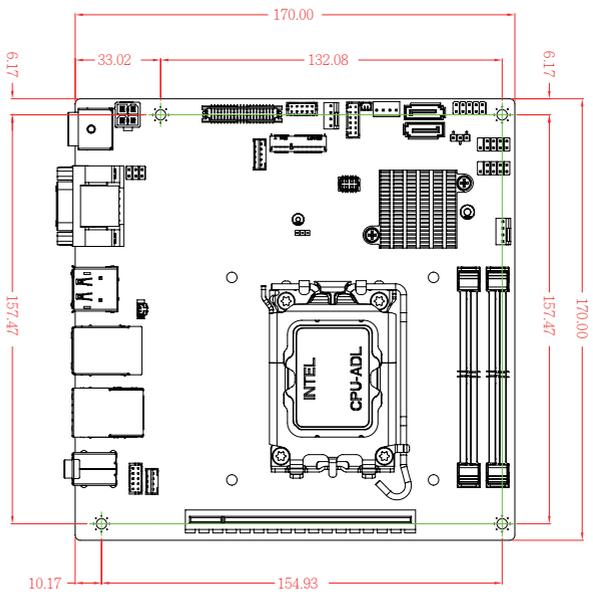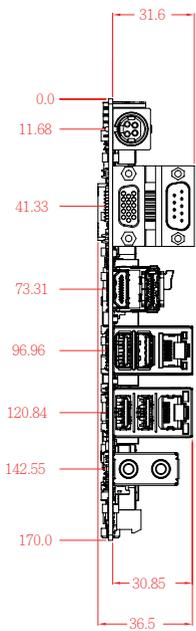
1.1   Specifications

Motherboard	mITX-H610B (MH610BI-SI)
Form Factor	Mini-ITX 170W x 170D (mm)
CPU	Support for 14th/13th/12th Generation Intel® Core™ i9/ i7/ i5/ i3, Pentium® and Celeron® processors in the LGA1700 package TDP under 65W
Socket	1 x LGA 1700
Chipset	Intel® H610 Chipset
Memory	2 x DDR5 SO-DIMM sockets, Max. Capacity 96 GB Support Dual channel DDR5 5600 MHz memory modules
Ethernet	1 x GbE LAN Port (Intel® I219LM) 1 x 2.5GbE LAN Port (Intel® I226V)
Video	Integrated Graphics Processor - depends on CPU: 1 x HDMI 2.0 port, supporting a maximum resolution of 4096x2160 @60Hz 1 x DP port, supporting a maximum resolution of 4096x2160 @60Hz 1 x VGA port, supporting a maximum resolution of 1920x1080 @60Hz 1 x LVDS port, supporting a maximum resolution of 1920x1200 @60Hz (3 independent display outputs)
Audio	Realtek® ALC897
Storage	2 x SATA 6Gb/s Ports
Expansion Slots	1 x PCIe x16 (Gen4 x16) 1 x 2280 M.2 M-Key (PCIe x4) 1 x 2230 M.2 E-Key (WiFi/BT)
Internal I/O	1 x 4-pin ATX main power connector 2 x SATA power connectors 1 x CPU fan header 1 x System fan header 1 x Front panel header 1 x Front panel audio header 1 x 2W Speaker out header 4 x USB 2.0 headers 1 x COM header (RS-232) 1 x GPIO (8 bits) & SMBus header 1 x Backlight Control header 1 x Clear CMOS jumper 1 x Buzzer header 1 x AT/ATX mode select jumper

Motherboard	mITX-H610B (MH610BI-SI)
Rear I/O	2 x Audio Jacks (Line out, Mic in) 1 x COM Port (RS-232/422/485 & RI/5V/12V) 1 x HDMI 1 x Display Port 1 x D-Sub 2 x RJ45 LAN Ports 4 x USB 3.2 Gen 1 1 x DC Jack (+12V/+19V~+24VDC)
TPM	Onboard TPM 2.0 security chip INFINEON SLB9670VQ2.0
OS Compatibility	Windows 11 IoT Enterprise LTSC 2024 (x64) Windows 10 IoT Enterprise LTSC 2021 (x64)
Operating Properties	Operating temperature: 0°C to 60°C Operating humidity: 60°C @ 20-95% (non-condensing) Non-operating temperature: -40°C to 85°C Non-operating humidity: 85°C @ 95% (non-condensing)
Order Information	Motherboard: 9MH610BIMR-SI
Optional kit:	CPU Cooler : 25ST0-037820-Y0R CPU Cooler Backplate : 12KRH-0A1700-00R

Chapter 2

Chapter 2 – Hardware Information

2.1   Jumpers and Connectors
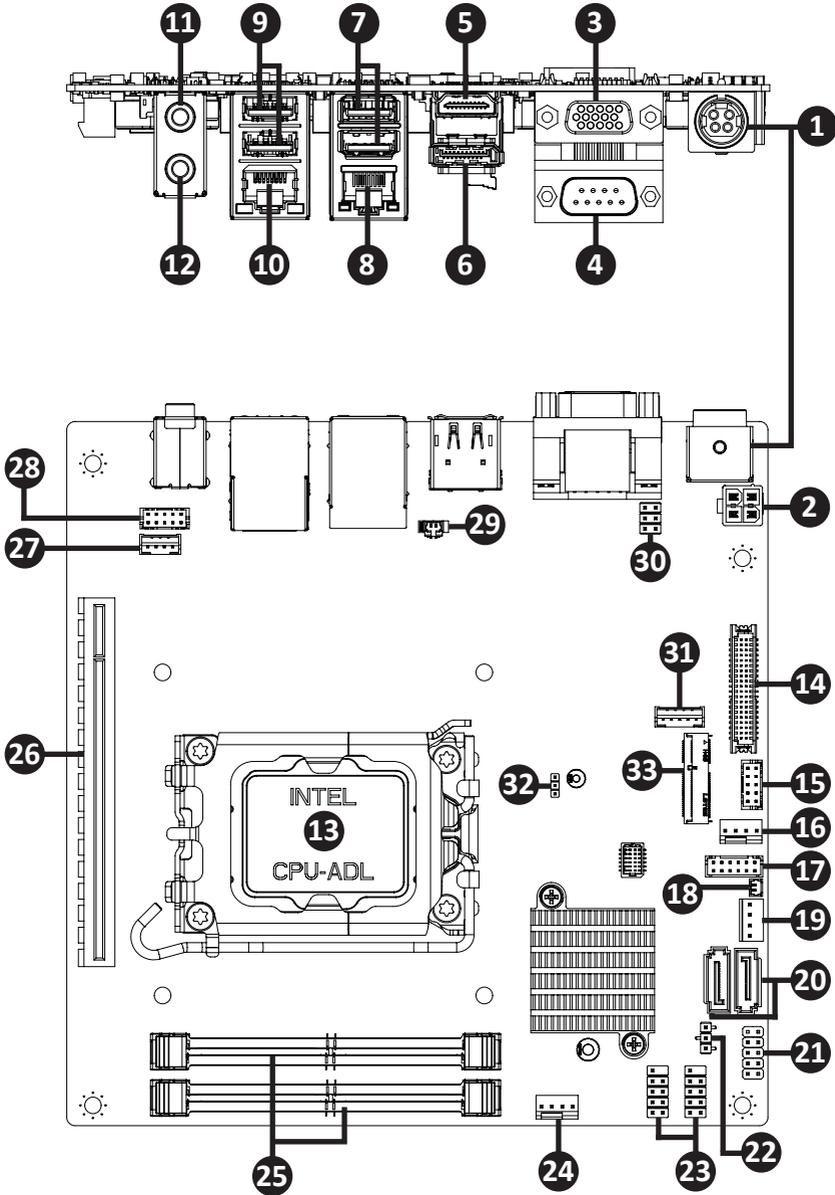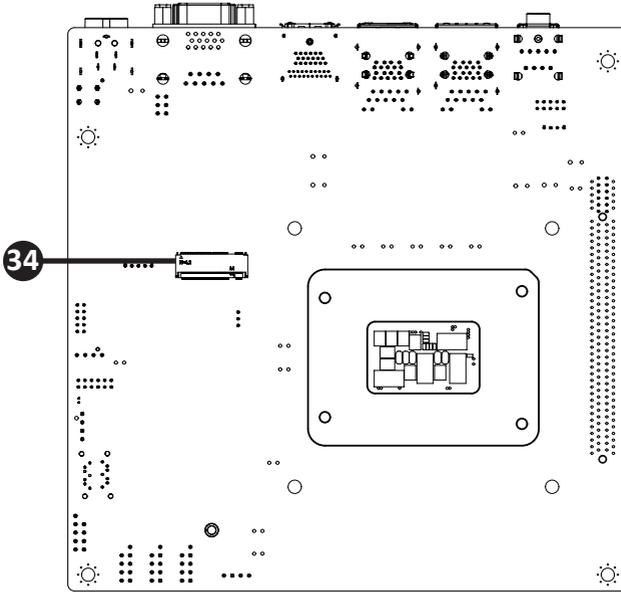
No	Code	Description
1	DC_IN1	DC In Jack 4 pin Din
2	DC_IN2	ATX 2x2 pin power Connector
3	VGA	VGA Port
4	COM1	COM1 Port (RS-232/422/485 & RI/5V/12V)
5	HDMI_DP	HDMI Connector
6		Display Port Connector
7	USB32_LAN1	USB 3.2 Gen 1 Connector
8		GbE LAN port
9	USB32_LAN2	USB 3.2 Gen 1 Connector
10		2.5GbE LAN port
11	AUDIO	Mic In port (Pink)
12		Line out port (Green)
13	CPU Socket	1 x LGA 1700 Socket

No	Code	Description
14	LVDS	LVDS Connector
15	COM2	COM2 header (RS-232)
16	SYS_FAN	System Fan Connector
17	GPIO_CNT	General purpose input/output header
18	BUZZER	Buzzer header
19	SATA_PWR	SATA Power Connector
20	SATA4, SATA5	SATA 6Gb/s Connector x 2
21	SYS_PANEL	System Panel header
22	CLR_CMOS	Clear CMOS jumper
23	FUSB2_1 FUSB2_2	USB 2.0 header
24	CPU_FAN	CPU FAN Connector
25	SODIMM1, SODIMM2	2 x DDR5 SO-DIMM Sockets
26	PCIEX16	1 x PCIe x16 (Gen4 x16 bus) slot
27	SPKR	Speaker out Connector
28	FP_AUDIO	Front Panel Audio header
29	BATTERY	Battery Connector
30	JCOM1	RI# pin RI#/5V/12V Select jumper for COM1 port
31	BKL_CN	Backlight Control connector
32	AT_CN	AT/ATX mode select jumper
33	M2E	M.2 Slot, 2230 E-Key
34	M2M	M.2 Slot, 2280 M-Key

![GIGAIPC™]

2.2.1 IO Connector Information
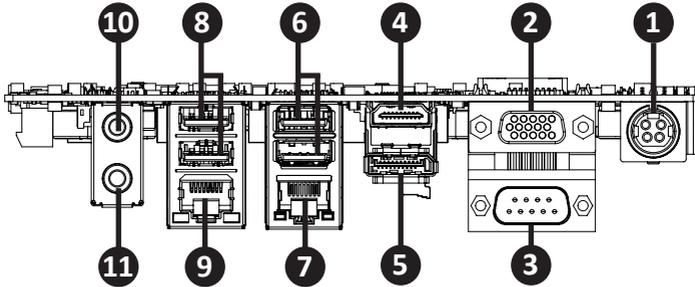
	Code	Description
1	**DC_IN1**	**DC In Jack 4 pin Din**
2	**VGA**	**VGA Port**
3	**COM1**	**COM1 Port (RS-232/422/485 & RI/5V/12V)**
4	**HDMI_DP**	**HDMI Connector**
5		**Display Port Connector**
6	**USB32_LAN1**	**USB 3.2 Gen 1 Connector**
7		**GbE LAN port**
8	**USB32_LAN2**	**USB 3.2 Gen 1 Connector**
9		**2.5GbE LAN port**
10	**MIC_IN**	**Mic In port (Pink)**
11	**LINE_OUT**	**Line out port (Green)**

Mini-ITX Motherboard

mITX-H610B (MH610BI-SI)

2.2.2 DC_IN1 (DC In Jack 4 Pin Din)
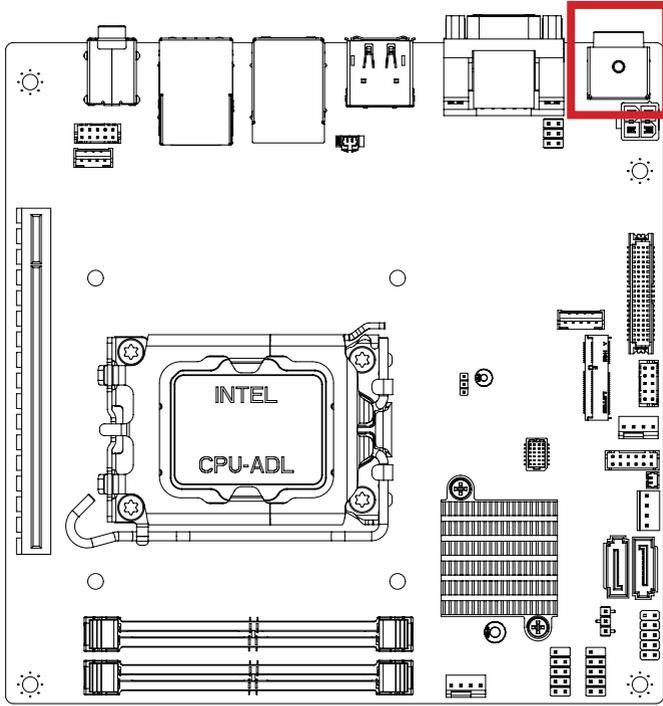
DC In Jack 4 Pin Din
GND — GND Power — Power
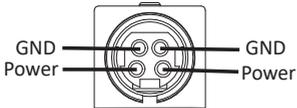
Connector PN	Vendor
2MJ-3422A1I0	SINGATRON

2.2.3   DC_IN2 (ATX 2x2 Pin Power Connector)

Pin 1

Power Connector
3   1 4   2
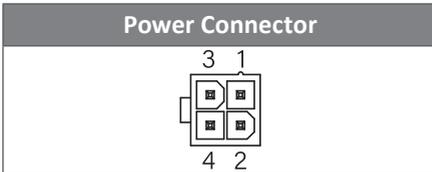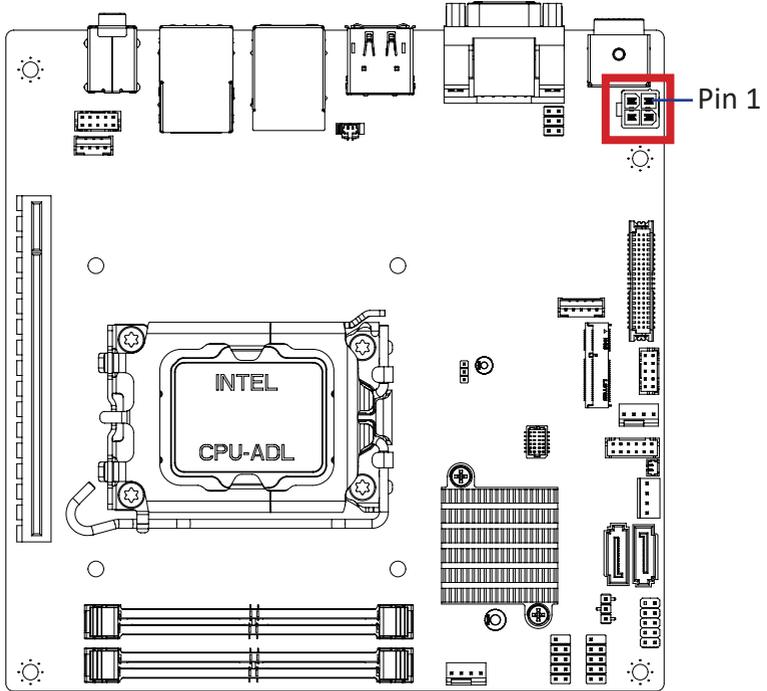
Connector PN	Vendor
740-81-04TW56	PINREX

Connector type
2x2pin header, pitch 4.2mm

Pin No.	Definition
1	GND
2	GND
3	DC IN
4	DC IN

2.2.4   VGA (VGA Port)

3
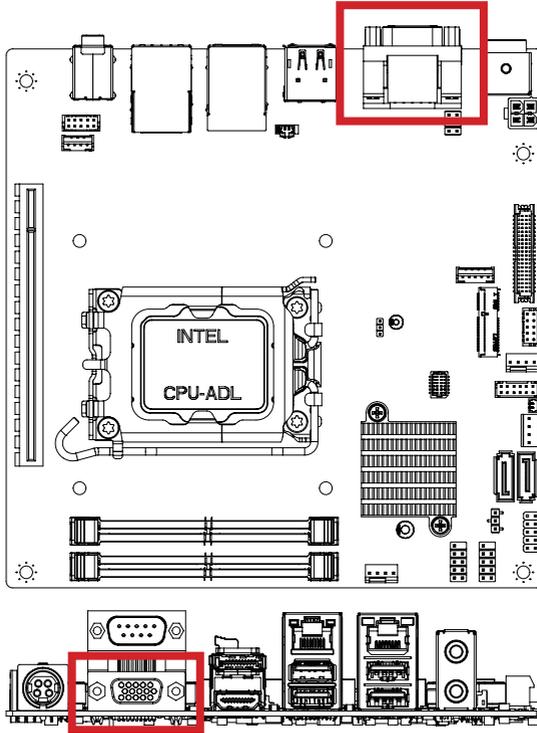
D-sub Connector
5   1 15 11
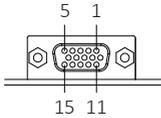
Connector PN	Vendor
D11069S1122E23DB	FENYING

Pin No.	Definition	Pin No.	Definition
1	Red	9	5V
2	Green	10	GND
3	Blue	11	NC
4	NC	12	DDCSDA
5	GND	13	HSYNC
6	GND	14	VSYNC
7	GND	15	DDCSCL
8	GND		

2.2.5 COM1 (COM1 Port (RS-232/422/485 & RI/5V/12V))

❹

Serial Port Connector
1 6

Connector PN	Vendor
DM10151-N5W3-4F	FOXCONN

Note :
For RI/5V/12V jumper setting, please see **P. 48**
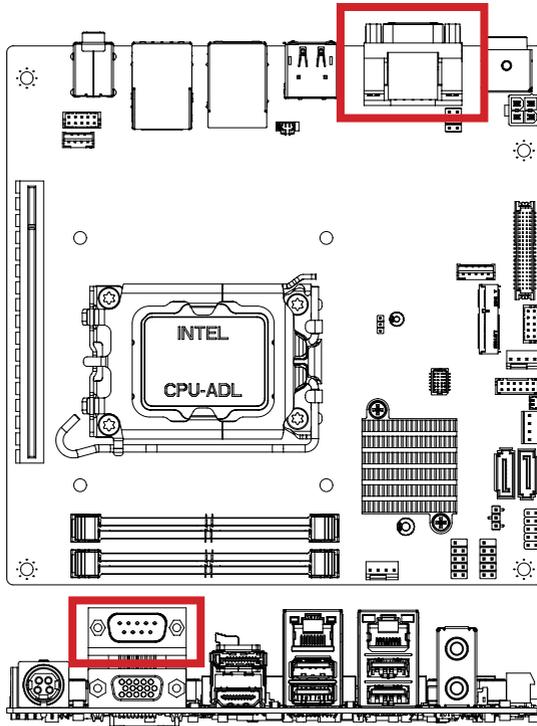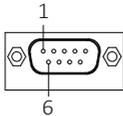
Pin No.	RS-232	RS-422 Full Duplex	RS-485 Half Duplex
1	DCD	TXD-	D-
2	RXD	TXD+	D+
3	TXD	RXD+	–
4	DTR	RXD-	–
5	GND		
6	DSR	–	–
7	RTS	–	–
8	CTS	–	–
9	RI/5V/12V	–	–

2.2.6 HDMI_DP (HDMI + DP Connector)

5 **6**

HDMI & DP Connector

DP port

HDMI port
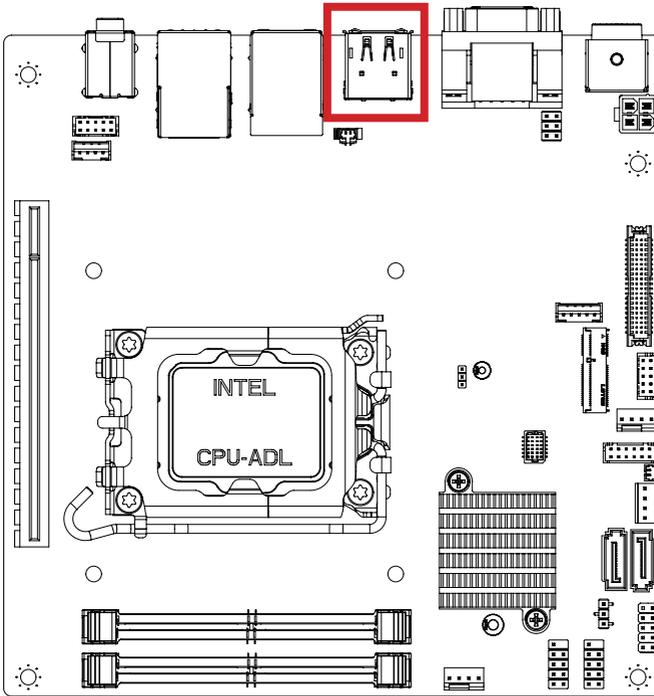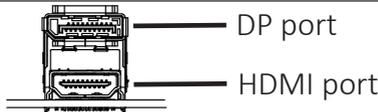
HDMI Connector			
Pin No.	Definition	Pin No.	Definition
1	TX2p	11	GND
2	GND	12	CLKn
3	TX2n	13	NC
4	TX1p	14	NC
5	GND	15	SCL
6	TX1n	16	SDA
7	TX0p	17	GND
8	GND	18	5V
9	TX0n	19	Hot Plug Detect
10	CLKp		

DP Connector			
Pin No.	Definition	Pin No.	Definition
1	TX0p	11	GND
2	GND	12	TX3n
3	TX0n	13	GND
4	TX1p	14	GND
5	GND	15	AUXp
6	TX1n	16	GND
7	TX2p	17	AUXn
8	GND	18	Hot Plug Detect
9	TX2n	19	3.3V
10	TX3p	20	3.3V

2.2.7   USB32_LAN1 (USB + GbE LAN Connector)

7 **8**

USB & LAN Connector

GbE LAN connector

USB 3.2 Gen 1 connector

USB Connector			
Pin No.	Definition	Pin No.	Definition
1	5V	10	5V
2	D1n	11	D0n
3	D1p	12	D0p
4	GND	13	GND
5	USB3_RX1n	14	USB3_RX2n
6	USB3_RX1p	15	USB3_RX2p
7	GND	16	GND
8	USB3_TX1n	17	USB3_TX2n
9	USB3_TX1p	18	USB3_TX2p

LAN Connector			
Pin No.	Definition	Pin No.	Definition
1	TX1+	4	TX3+
2	TX1-	5	TX3-
3	TX2+	7	TX4+
6	TX2-	8	TX4-

State	Description
Orange On	1Gbps data rate
Green On	100Mbps data rate
Off	10Mbps data rate

2.2.8   USB32_LAN2 (USB + 2.5GbE LAN Connector)

9 **10**

USB & LAN Connector

2.5GbE LAN connector

USB 3.2 Gen 1 connector

USB Connector			
Pin No.	Definition	Pin No.	Definition
1	5V	10	5V
2	D1n	11	D0n
3	D1p	12	D0p
4	GND	13	GND
5	USB3_RX1n	14	USB3_RX2n
6	USB3_RX1p	15	USB3_RX2p
7	GND	16	GND
8	USB3_TX1n	17	USB3_TX2n
9	USB3_TX1p	18	USB3_TX2p

LAN Connector			
Pin No.	Definition	Pin No.	Definition
1	TX1+	4	TX3+
2	TX1-	5	TX3-
3	TX2+	7	TX4+
6	TX2-	8	TX4-

State	Description
Orange On	2.5Gbps data rate
Green On	1Gbps data rate
Off	100M&10Mbps data rate

2.2.9   AUDIO (MIC in + Line out connector)

11 12

Line out
MIC in
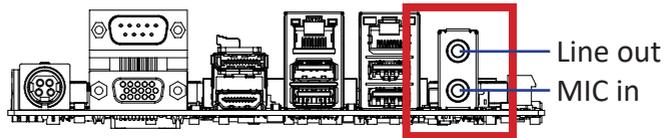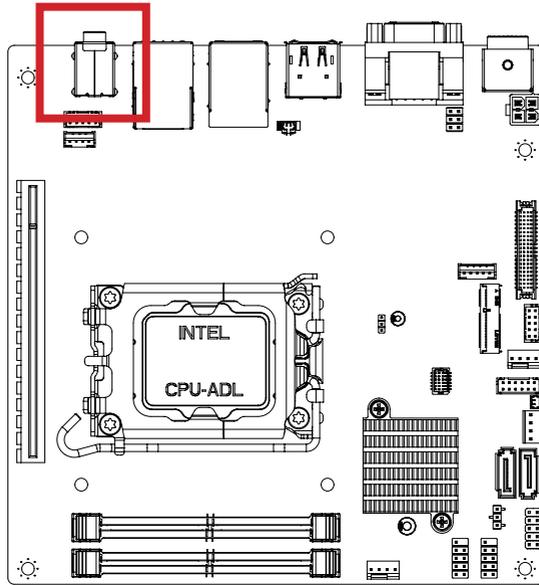
2.2.10   CPU Socket (LGA 1700 Socket)

13
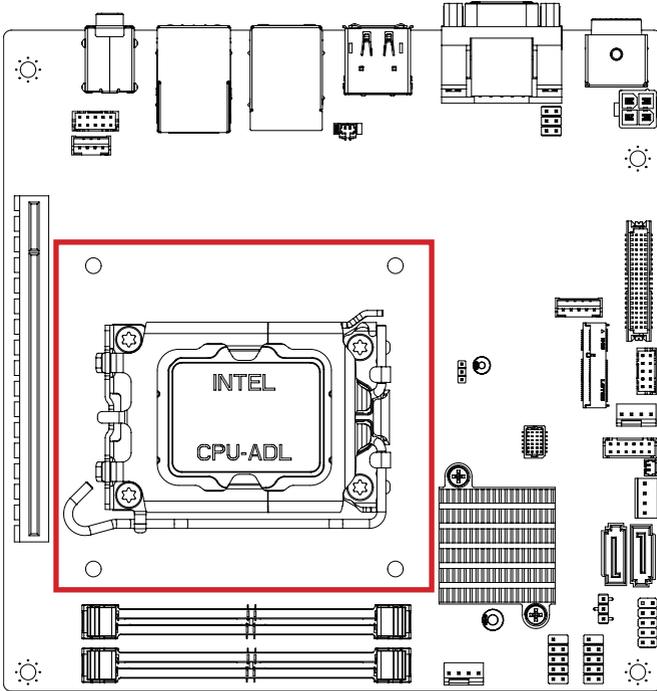
2.2.11   LVDS (LVDS Connector)

14

Pin 1
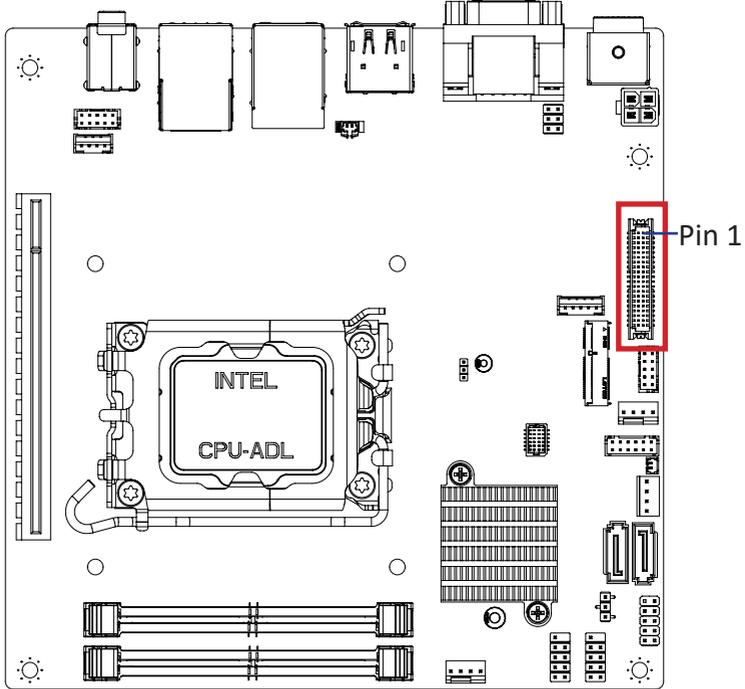
LVDS Connector
2   1
40   39
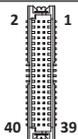
Pin No.	Definition	Pin No.	Definition
1	3.3V	21	A5+
2	5V	22	A4+
3	3.3V	23	A5-
4	5V	24	A4-
5	SPEC0	25	GND
6	SPED0	26	GND
7	GND	27	A7+
8	GND	28	A6+
9	A1+	29	A7-
10	A0+	30	A6-
11	A1-	31	GND
12	A0-	32	GND
13	GND	33	CLK2+
14	GND	34	CLK1+
15	A3+	35	CLK2-

Pin No.	Definition	Pin No.	Definition
16	A2+	36	CLK1-
17	A3-	37	GND
18	A2-	38	GND
19	GND	39	12V
20	GND	40	12V

Connector PN	Vendor
712-76-40GWE0	PINREX
A1252WV-SF-2X20PD01	JOINT-TECH

Connector type
2x20pin header, pitch 1.25mm

For each model support LVDS function.
But below model no need to add.
A0~A3 is odd channel 0~3, A4~A7 is ev en channel.

Note: *The LVDS output connector of the unit is only intended to be connected to an UL/IEC/EN approval equipment with fire enclosure.

2.2.12 COM2 (COM2 header (RS-232))

15

Pin 1

COM 2 header
9 ▫▫ 10 ▫▫ ▫▫ ▫▫ 1 ▫▫ 2
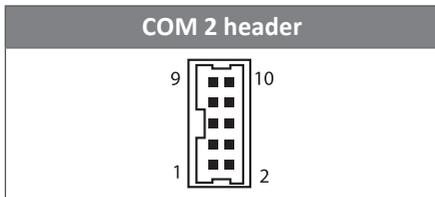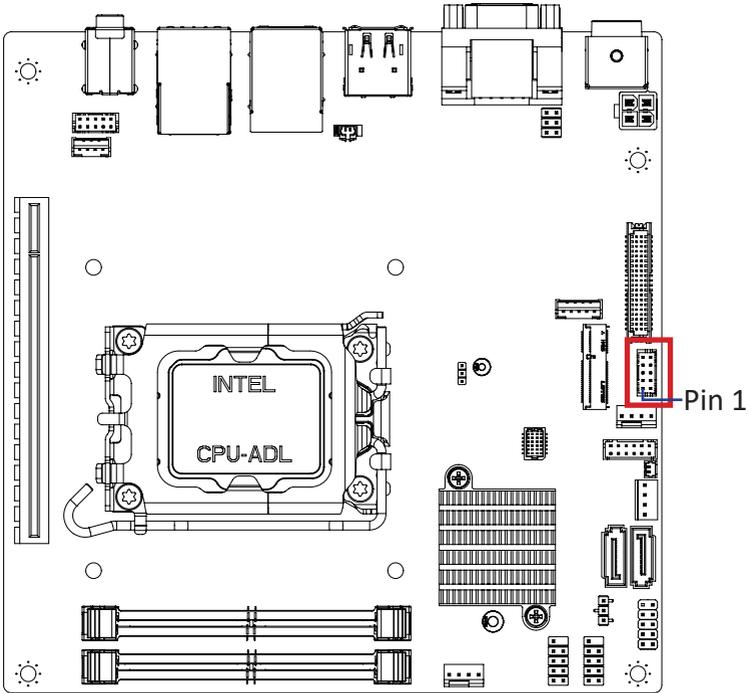
Pin No.	Definition
1	RXD
2	DCD
3	DTR
4	TXD
5	DSR
6	GND
7	CTS
8	RTS
9	No connect
10	RI

Connector PN	Vendor
725-81-10TW00	PINREX
A2004WV-2X05P46	JOINT-TECH

Connector type
2x5pin header, pitch 2.0mm

2.2.13 SYS_FAN (System Fan Connector)

16
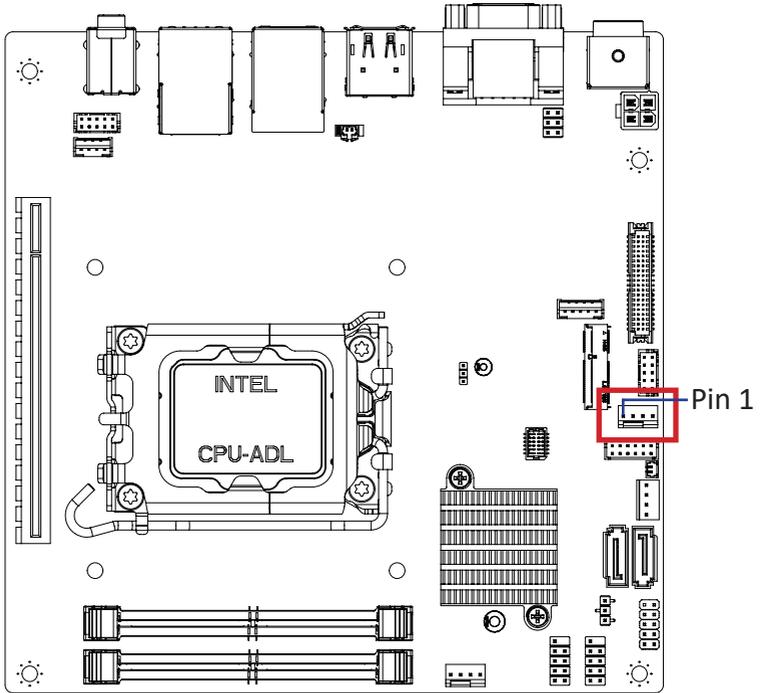
Pin 1

System FAN
1 [· · ·] 4

Pin No.	Definition
1	GND
2	12V
3	Detect
4	Speed Control

Connector PN	Vendor
744-81-045R11	PINREX

Connector type	
1x4pin header, pitch 2.54mm	

2.2.14 GPIO_CNT (General purpose input/out header)

17

Pin 1

GPIO Connector
1   11
2   12
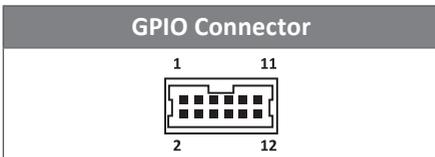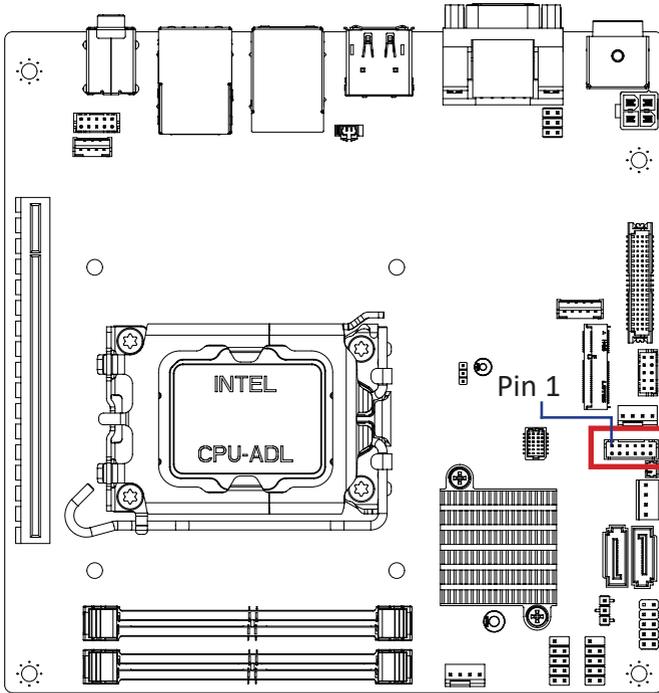
Pin No.	Definition
9	SMBus Clock
10	SMBus DATA
11	5V
12	GND

Pin No.	Definition
1	GPIO-output_1
2	GPIO-input_1
3	GPIO-output_2
4	GPIO-input_2
5	GPIO-output_3
6	GPIO-input_3
7	GPIO-output_4
8	GPIO-input_4

Connector PN	Vendor
725-81-12TW00	PINREX
A2004WV-2X06P46	JOINT-TECH

Connector type
2x6pin header, pitch 2.0mm

2.2.15   BUZZER (Buzzer header)

18

Pin 1

Buzzer

Pin No.	Definition
1	Buzzer
2	5V
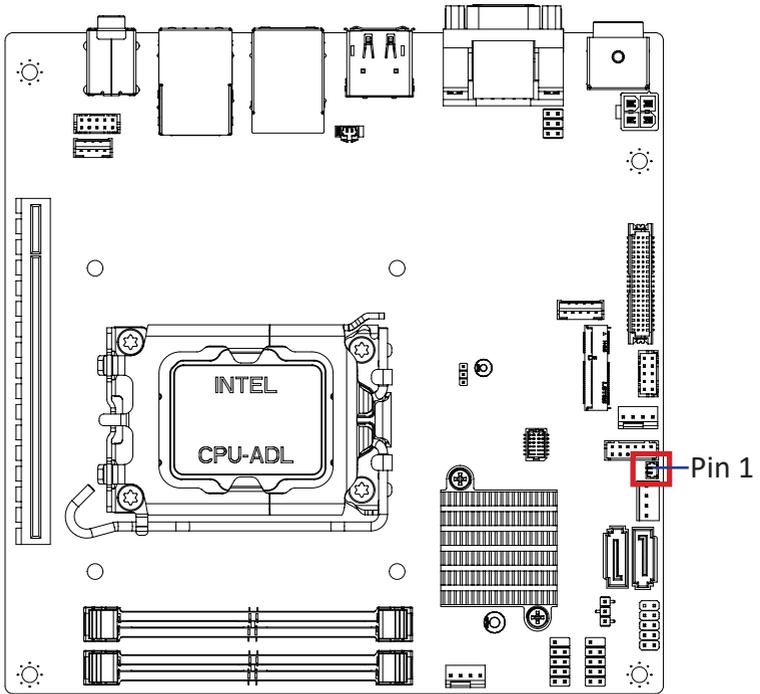
Connector PN	Vendor
712-71-02TW01	PINREX
A1250WV-02P	JOINT-TECH

Connector type
1x2pin header, pitch 1.25mm

2.2.16 SATA_PWR (SATA Power Connector)

19

Pin 1

SATA Power Connector
1
4
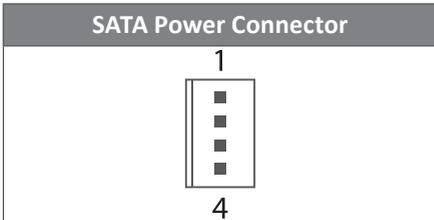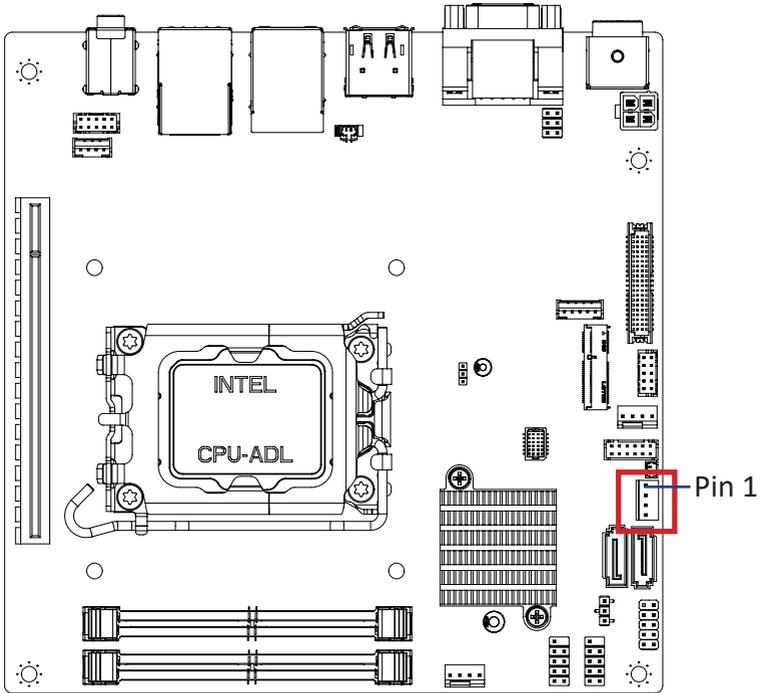
Connector PN	Vendor
743-81-04TW00	PINREX

Connector type
1x4pin header, pitch 2.54mm

Pin No.	Definition
1	5V
2	GND
3	GND
4	5V

2.2.17   SATA4, SATA5 (SATA 6Gb/s Connector)

SATA 6Gb/s Connector
7 1
SATA 4   SATA 5
1 7
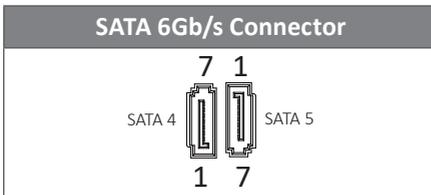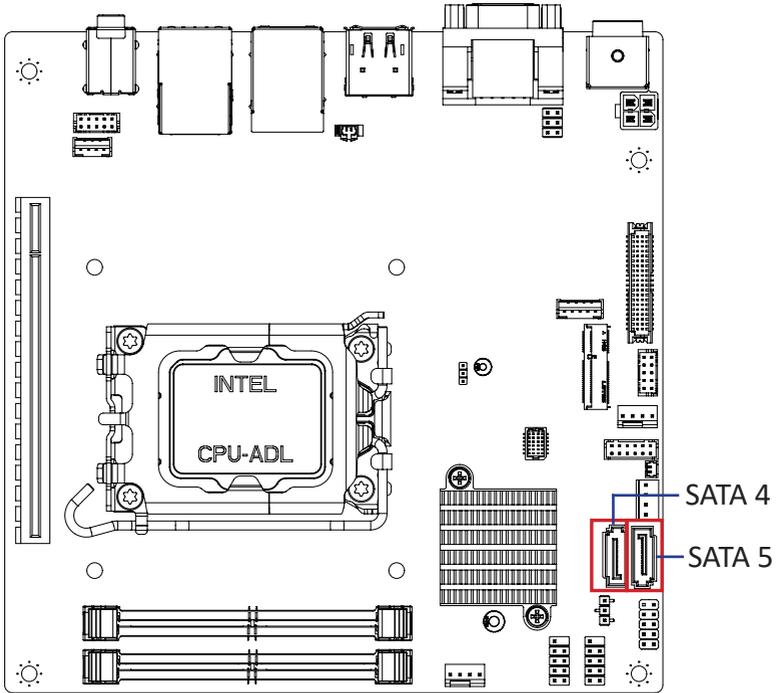
Pin No.	Definition
1	GND
2	TXp
3	TXn
4	GND
5	RXn
6	RXp
7	GND

2.2.18 SYS_PANEL (System Panel header)

21
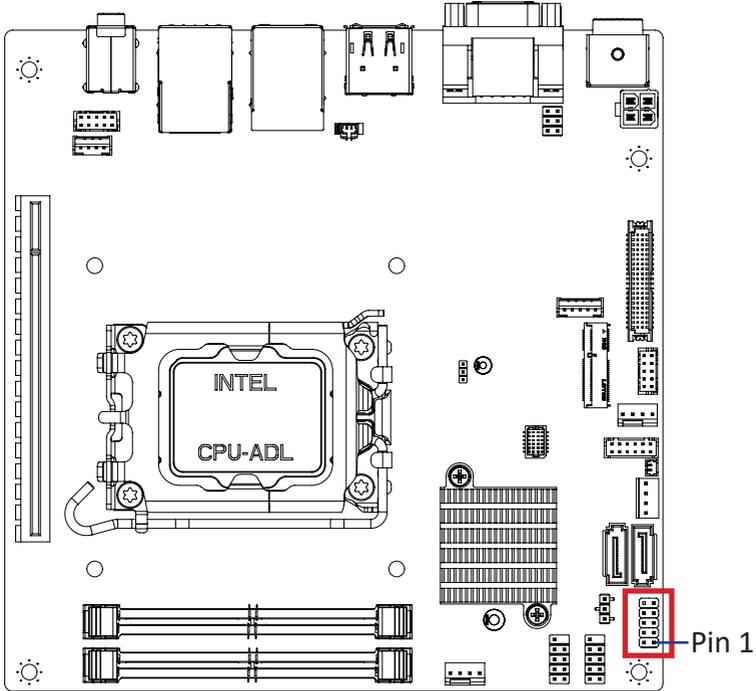
Pin 1

System Panel Header
10 9 2 1

Pin No.	Definition
1	HD-P
2	MPD-P
3	HD-N
4	MPD-N
5	GND
6	POWER-ON
7	Reset
8	GND
9	Reserved
10	NC

Connector PN	Vendor
210-92-05GW5W	PINREX

Connector type
2x5pin header, pitch 2.54mm

2.2.19 CLR_CMOS (Clear CMOS jumper)
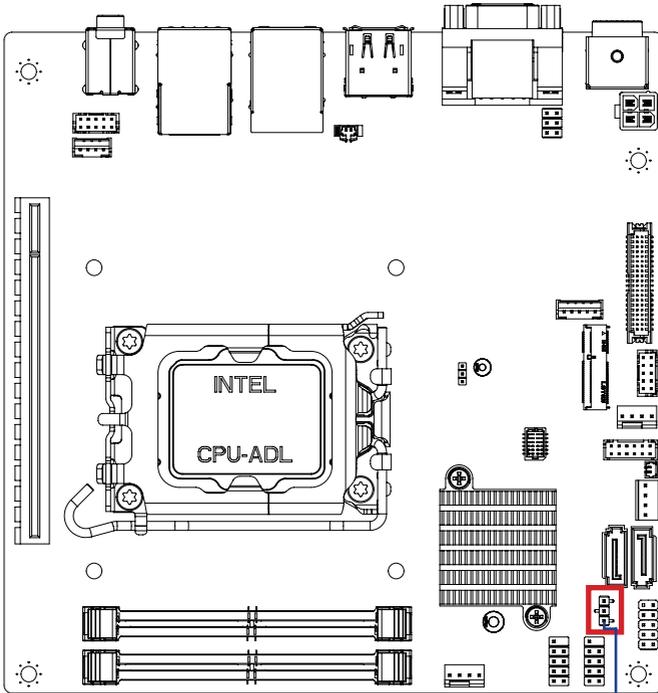
Pin 1

Clear CMOS Jumper
1

Connector PN	Vendor
212-91-03GBE00K	PINREX

Connector type	
1x3pin header, pitch 2.54mm	

Pin No.	Definition
1	NC
2	GND
3	Clear CMOS
1-2 Close: Normal Operation (Default setting) 2-3 Close: Clear CMOS data	

2.2.20　FUSB2_1, FUSB2_2 (USB 2.0 header)

23

Pin 1

USB 2.0 Header
10 9
2 1
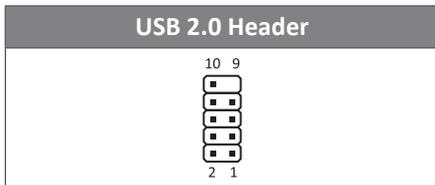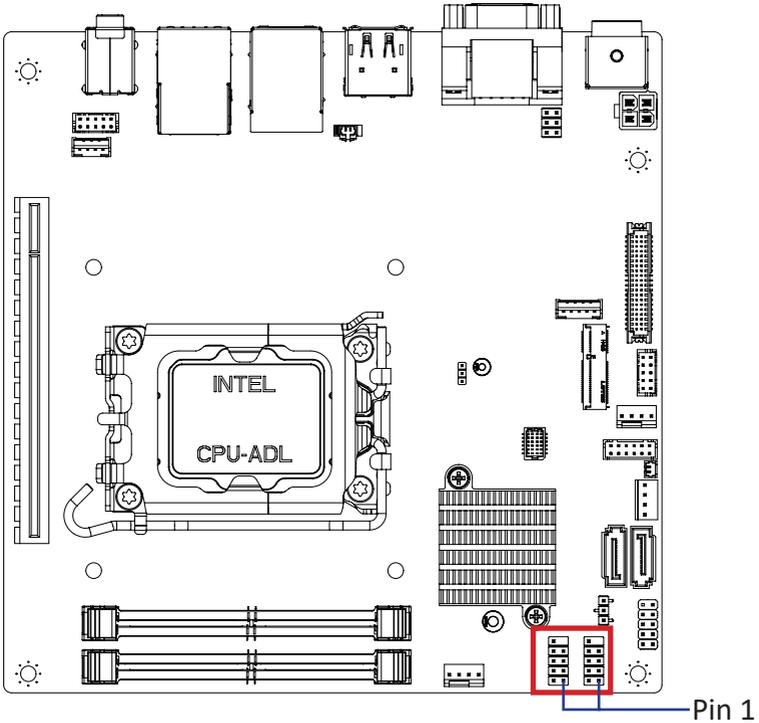
Pin No.	Definition
1	5V
2	5V
3	D2n
4	D1n
5	D2p
6	D1p
7	GND
8	GND
9	No Pin
10	NC

Connector PN	Vendor
210-92-05GB04	PINREX
PH10R53BAZ009	HORNGTONG

Connector type
2x5pin header, pitch 2.54mm

2.2.21   CPU_FAN (CPU FAN Connector)

24
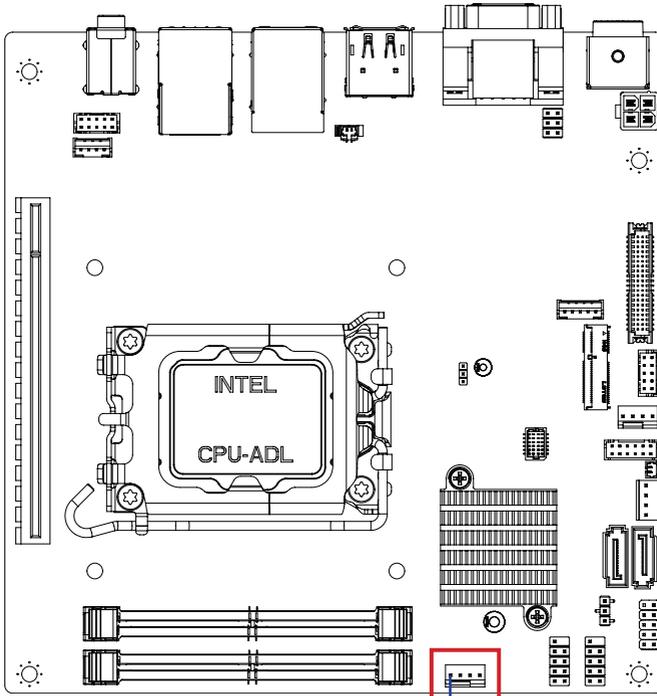
Pin 1

CPU Fan Connector
1 ▢ 4

Connector PN	Vendor
744-81-045W1Z	PINREX

Connector type
1x4pin header, pitch 2.54mm

Pin No.	Definition
1	GND
2	12V
3	Detect
4	Speed Control

2.2.22   SODIMM1, SODIMM2 (2 x DDR5 SO-DIMM Sockets)

GIGAIPC™
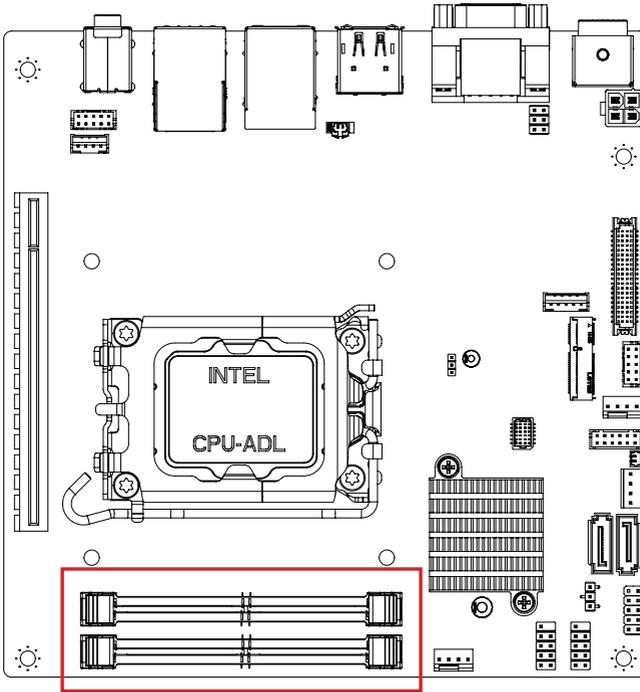
2.2.23 PCIEX16 (1 x PCIe x16 (Gen4 x16 Bus) Slot)

26
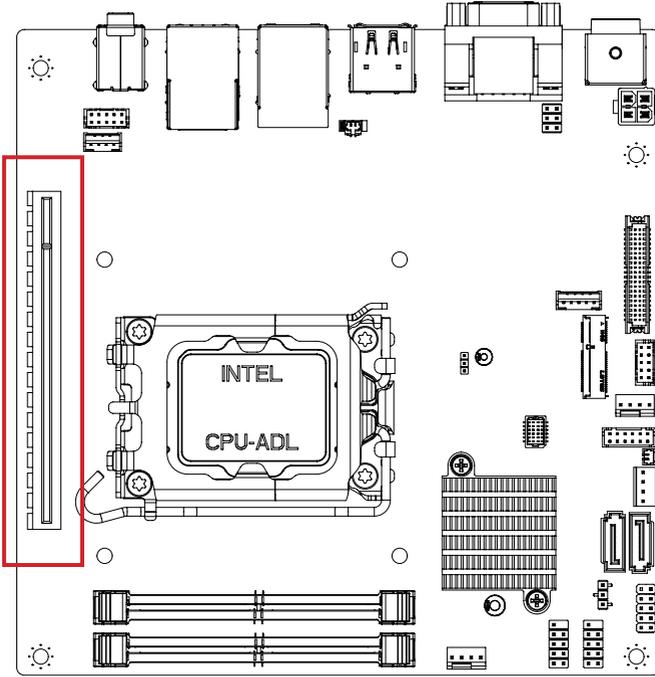
PCIEX16 connector

B2 B1 A1 A2

B82 B81 A81 A82
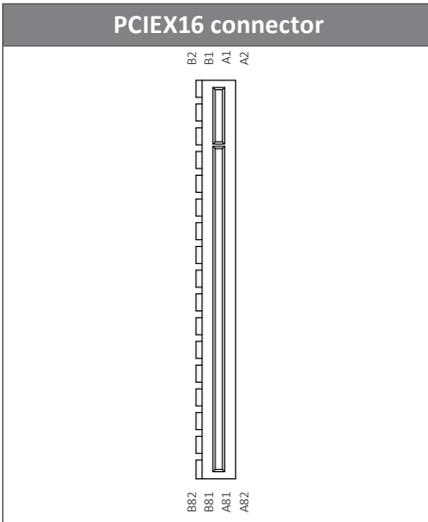
2.2.24 SPKR (Speaker Out Connector)

27

Pin 1
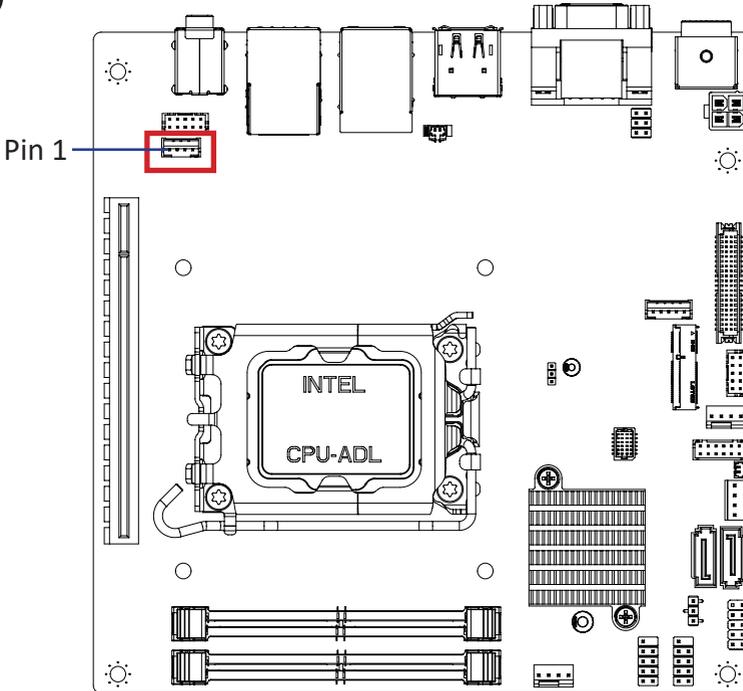
Speaker Out Connector
1

Connector PN	Vendor
721-81-045W00	PINREX
A2001WV-04P146	JOINT-TECH

Connector type
1x4pin header, pitch 2.0mm
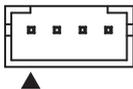
Pin No.	Definition
1	SPEAKER L+
2	SPEAKER L–
3	SPEAKER R–
4	SPEAKER R+

2.2.25 FP_AUDIO (Front Panel Audio header)

28

Pin 1
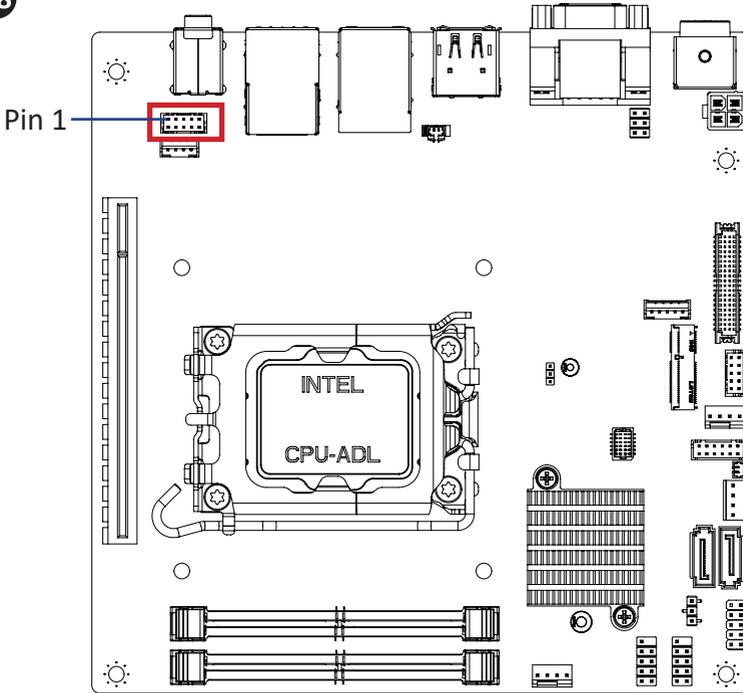
Front Audio Connector
1   9
2   10
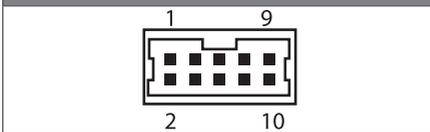
Connector PN	Vendor
725-81-10TW00	PINREX
A2004WV-2X05P46	JOINT-TECH

Connector type
2x5pin header, pitch 2.0mm

Pin No.	Definition	Pin No.	Definition
1	MIC-LEFT	6	GND
2	GND	7	JACKSENCE DETECT
3	MIC-RIGHT	8	NC
4	DETECT	9	LINE-LEFT
5	LINE-RIGHT	10	GND

2.2.26 Battery (Battery Connector)

29

Pin 1
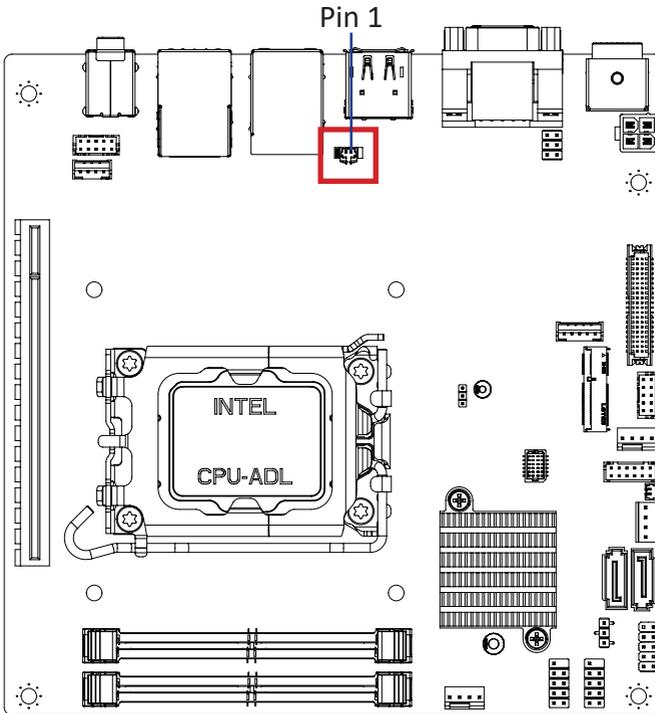
Battery Connector
2 □□□ 1

Pin No.	Definition
1	3V
2	GND

Connector PN	Vendor
85205-0270L	ACES
A1250WV-S-02PC	JOINT-TECH

Connector type
1x2pin header, pitch 1.25mm

2.2.27 JCOM1 (RI# pin RI#/5V/12V Select jumper for COM1 Port)

30

Pin 1
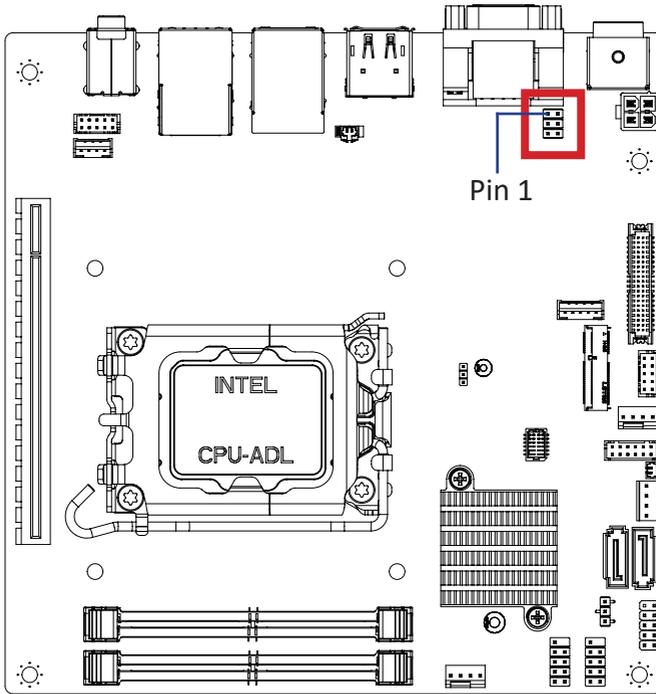
JCOM1 Jumper Select	
1 2 5 6	1-2 Close: 5V (Power COM)
1 2 5 6	3-4 Close: RI (Stand COM)
1 2 5 6	5-6 Close: 12V (Power COM)

Connector PN	Vendor
210-92-03GB01	PINREX
PH06R53BAZ000	HORNGTONG

Connector type
2x3pin header, pitch 2.54mm

2.2.28 BKL_CN (Backlight Control Connector)

31

Pin 1

Backlight Control Connector
1 ⬚⬚⬚⬚⬚ 5

Connector PN	Vendor
721-81-05TW00	PINREX
A2001WV-05P146	JOINT-TECH
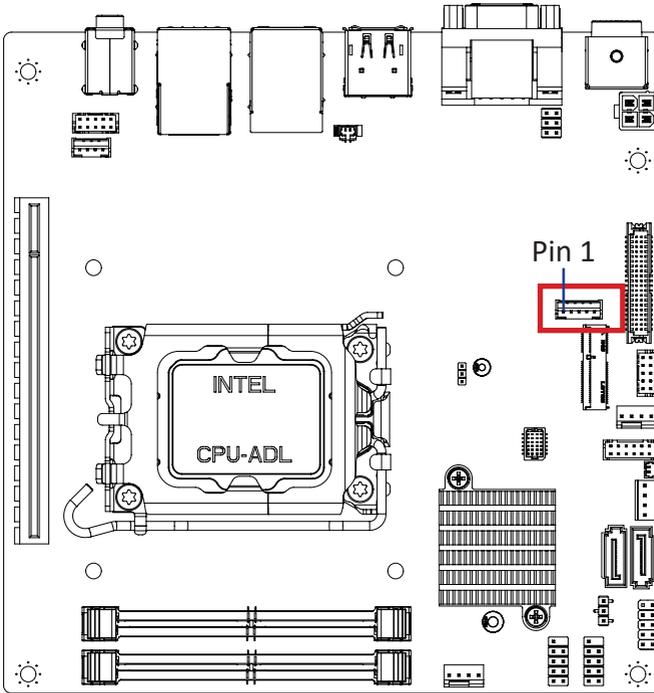
Connector type
1x5pin header, pitch 2.0mm
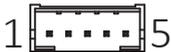
Pin No.	Definition
1	5V (12V optional)
2	PWM
3	Backlight enable
4	GND
5	12V

2.2.29   AT_CN (AT/ATX mode select jumper)

32
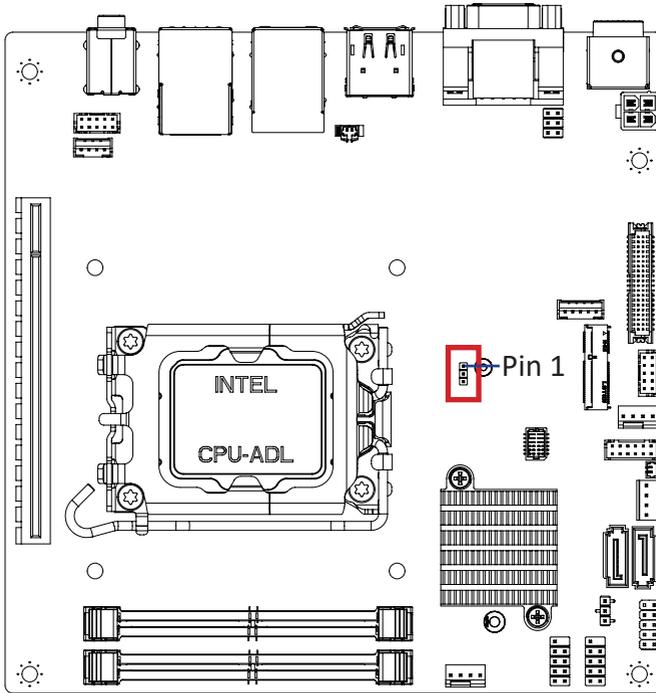
Pin 1

AT/ATX mode select jumper
1

Connector PN	Vendor
220-96-03GB001K	PINREX

Connector type	
1x3pin header, pitch 2.0mm	

Pin No.	Definition
1	AT MODE
2	Detect
3	ATX MODE
Jumper setting 1-2 Close : AT mode. 2-3 Close : ATX mode.(Default setting)	

2.2.30 M2E (M.2 Slot, 2230 E-Key)

33

M.2 E Key Connector

2   1

74   75
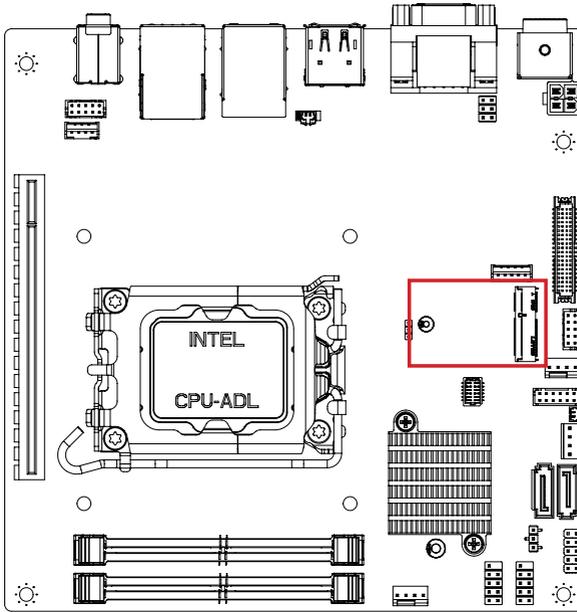
Pin No.	Definition	Pin No.	Definition
1	GND	2	3.3V
3	D1p	4	3.3V
5	D1n	6	NC
7	GND	8	NC
9	NC	10	NC
11	NC	12	NC
13	GND	14	NC
15	NC	16	NC
17	NC	18	GND
19	GND	20	NC
21	NC	22	NC
23	NC		

Pin No.	Definition	Pin No.	Definition
33	GND	32	NC
35	PCIE_TXp	34	NC
37	PCIE_TXn	36	NC
39	GND	38	CL_Reset

Pin No.	Definition	Pin No.	Definition
41	PCIE_RXp	40	CL_DATA
43	PCIE_RXn	42	CL_Clock
45	GND	44	NC
47	PCIE CLOCKp	46	NC
49	PCIE CLOCKn	48	NC
51	GND	50	SUSCLK
53	PCIE Clock Request	52	PCIRST
55	PCIE wake up	54	BT_Disable
57	GND	56	WLAN_DISABLE
59	NC	58	NC
61	NC	60	NC
63	GND	62	NC
65	NC	64	NC
67	NC	66	NC
69	GND	68	NC
71	NC	70	NC
73	NC	72	3.3V
75	GND	74	3.3V

Connector PN	Vendor
2E0BC21-S85BE-LH	FOXCONN
80152-8521	BELLWETHER
APCI0095-P002A	LOTES

2.2.31 M2M (M.2 Slot, 2280 M-Key)

34

M.2 M Key Connector			

1 ⬛ 75
2 ⬛ 74
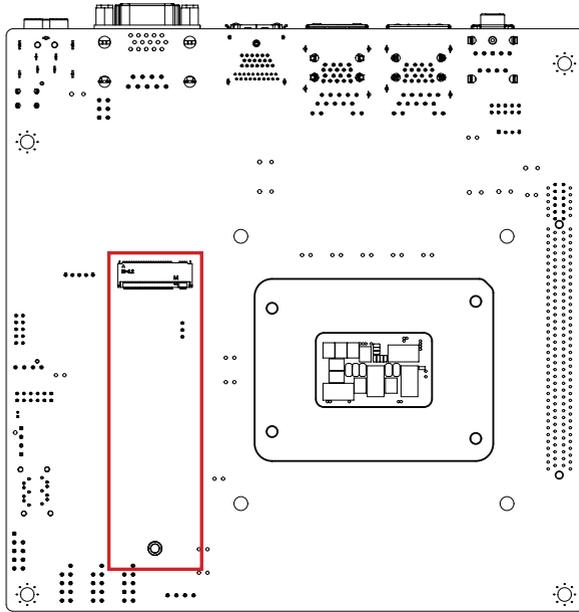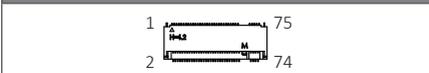
Pin No.	Definition	Pin No.	Definition
1	GND	2	3.3V
3	GND	4	3.3V
5	PCIE3 RXn	6	NC
7	PCIE3 RXp	8	NC
9	GND	10	SSD LED
11	PCIE3 TXn	12	3.3V
13	PCIE3 TXp	14	3.3V
15	GND	16	3.3V
17	PCIE2 RXn	18	3.3V
19	PCIE2 RXp	20	NC
21	GND	22	NC
23	PCIE2 TXn	24	NC
25	PCIE2 TXp	26	NC
27	GND	28	NC
29	PCIE1 RXn	30	NC
31	PCIE1 RXp	32	NC
33	GND	34	NC
35	PCIE1 TXn	36	NC

Pin No.	Definition	Pin No.	Definition
37	PCIE1 TXp	38	DEVSLP
39	GND	40	NC
41	PCIE0 RXn	42	NC
43	PCIE0 RXp	44	NC
45	GND	46	NC
47	PCIE0 TXn	48	NC
49	PCIE0 TXp	50	PCI Reset
51	GND	52	PCIE Clock Request
53	PCIE Clockn	54	Wakeup
55	PCIE Clockp	56	NC
57	GND	58	NC

Pin No.	Definition	Pin No.	Definition
67	NC	68	SUSCLK
69	Detect	70	3.3V
71	GND	72	3.3V
73	GND	74	3.3V
75	GND		

Connector PN	Vendor
AS0BC21-S40BM-7H	FOXCONN
APCI0073-P001A	LOTES

Chapter 3

Chapter 3 – BIOS

3.1   Introduction

BIOS (Basic input/output system) provides hardware detailed information and boot-up options, which include firmware to control, set-up and test all hardware settings. Therefore, BIOS is the communication bridge between OS/application software and hardware.

3.1.1 How to Entering into BIOS menu

Once the system is power on, press the <DEL> key as soon as possible to access into BIOS Setup program.

3.1.2 Function Keys to setup in BIOS Setup program

Function keys	Description
→←	Select Screen
↑↓	Select Item
Enter	Execute command or enter the submenu
+	Increase the numeric value or make changes
—	Decrease the numeric value or make changes
F1	General Help
F2	Previous Values
F3	Load Optimized Defaults Settings
F4	Save changes & Exit the BIOS Setup program
ESC	Exit the BIOS Setup program

3.2   The Main Menu

The main menu shows the basic system information.
Use arrow keys to move among the items.

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

   BIOS Information                                    Set the Date. Use Tab to
                                                       switch between Date elements.
   Project Name              MH610BI-SI                Default Ranges:
   BIOS Version              F1                         Year: 1998-9999
   Build Date and Time       11/17/2025 15:48:01        Months: 1-12
                                                         Days: Dependent on month
   LAN1 MAC Address          30-56-0F-4B-8D-47          Range of Years may vary.
   LAN2 MAC Address          30-56-0F-4B-8D-48

   Total Memory              16384 MB

   ME FW Version             16.1.40.2765

   System Date               [Tue 03/10/2026]         ↔: Select Screen
   System Time               [13:50:08]               ↑↓: Select Item
                                                       Enter: Select
                                                       +/-: Change Opt.
                                                       F1: General Help
                                                       F2: Previous Values
                                                       F3: Optimized Defaults
                                                       F4: Save & Exit
                                                       ESC: Exit




                      Version 2.22.1293 Copyright (C) 2025 AMI
```

Items	Description
Project Name	Shows Project name information
BIOS Version	Shows the BIOS version of the system
Build Date and Time	Shows the Build Date and Time when the BIOS was created.
LAN1 MAC Address	Shows LAN 1 MAC Address information
LAN2 MAC Address	Shows LAN 2 MAC Address information
Total Memory	Shows the total memory size of the installed memory
ME FW version	Shows ME firmware version
System Date	Set the Date for the system (Format : Week - Month - Day - Year)
System Time	Set the time for the system (Format : Hour - Minute - Second)

3.3 Advanced

The Advanced menu is to configure the functions of hardware settings through submenu. Use arrow keys to move among the items, and press <Enter> to access into the related submenu.

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

   ▶ TPM Configuration                                    TPM Configuration
   ▶ CPU Configuration
   ▶ SATA Configuration
   ▶ IT8786 Super IO Configuration
   ▶ Hardware Monitor
   ▶ S5 RTC Wake Settings
   ▶ Network Stack Configuration
   ▶ NVMe Configuration
   ▶ Digital IO Port Configuration

   ▶ Tls Auth Configuration
   ▶ Intel(R) Ethernet Controller I226-V - 30:56:0F:4B:8D:48
   ▶ Intel(R) Ethernet Connection (17) I219-V - 30:56:0F:4B:8D:47
                                                          →←: Select Screen
                                                          ↑↓: Select Item
                                                          Enter: Select
                                                          +/-: Change Opt.
                                                          F1: General Help
                                                          F2: Previous Values
                                                          F3: Optimized Defaults
                                                          F4: Save & Exit
                                                          ESC: Exit



                         Version 2.22.1293 Copyright (C) 2025 AMI
```

GIGAIPC™

3.3.1　TPM Configuration

Use TPM Configuration submenu to choose TPM interface.

Item	Description
TPM Device Selection	**PTT : Internal TPM** **dTPM : External TPM (When using External TPM module or having TPM chip on MB)(Default setting)**

Mini-ITX Motherboard　mITX-H610B (MH610BI-SI)

Trusted Computing : Shows TPM information, and TPM module configuration setting.

```
                              Aptio Setup – AMI
      Advanced

   TPM 2.0 Device Found                              Enables or Disables BIOS
   Firmware Version:          7.85                   support for security device.
   Vendor:                    IFX                    O.S. will not show Security
                                                     Device. TCG EFI protocol and
   Security Device Support    [Enable]               INT1A interface will not be
   Pending operation          [None]                 available.



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



                         Version 2.22.1293 Copyright (C) 2025 AMI
```

Item	Description
Security Device Support	**Enabled : Enables TPM feature (Default setting)** **Disabled : Disables TPM feature**
Pending operation	**None : No execution will be conducted (Default setting)** **TPM clear : Set to clear data on TPM**

3.3.2   CPU Configuration

This submenu shows detailed CPU informations.

```
                              Aptio Setup - AMI
         Advanced

        CPU Configuration                                When enabled, a VMM can
                                                         utilize the additional
         ID                          0x90675             hardware capabilities provided
         Brand String                12th Gen Intel(R)   by Vanderpool Technology.
                                     Core(TM) i5-12500E
         VMX                         Supported
         SMX/TXT                     Supported

         Intel (VMX) Virtualization  [Enabled]
         Technology
         Intel(R) Speed Shift Technology  [Enabled]
         Intel(R) SpeedStep(tm)      [Enabled]
         Turbo Mode                  [Enabled]
         C states                    [Enabled]           ++: Select Screen
         Dual Tau Boost              [Disabled]          ↑↓: Select Item
                                                         Enter: Select
                                                         +/-: Change Opt.
                                                         F1: General Help
                                                         F2: Previous Values
                                                         F3: Optimized Defaults
                                                         F4: Save & Exit
                                                         ESC: Exit


                          Version 2.22.1293 Copyright (C) 2025 AMI
```

Item	Description
Intel (VMX) Virtualization Technology	Virtualization enhanced by Intel® Virtualization Technology will allow a platform to run multiple operating systems and applications in independent partitions. With virtualization, one computer system can function as multiple virtual systems. **Enabled : Enables Intel Virtualization Technology (Default setting)** **Disabled : Disables Intel Virtualization Technology**
Intel(R) Speed Shift Technology	To speed up CPU frequency transition time from basic frequency to maximum frequency. **Enabled : Enables Intel(R) Speed Shift Technology Interrupt control (Default setting)** **Disabled : Disables Intel(R) Speed Shift Technology Interrupt control**
Intel(R) SpeedStep(tm)	According to Intel CPU loading, Intel SpeedStep Technology will automatically adjust the CPU voltage and core frequency to decrease heat and power consumption for power saving. **Enabled : Enables Intel SpeedStep Technology (Default setting)** **Disabled : Disables Intel SpeedStep Technology**
Turbo Mode	**Enabled : Enables Turbo Mode (Default setting)** **Disabled : Disables Turbo Mode**
C states	Command CPU to enter into low power consumption mode when CPU is under idle mode. **Enabled : Enables CPU C states function (Default setting)** **Disabled : Disables CPU C states function**
Dual Tau Boost	To optimize CPU performance. **Enabled : Enables Dual Tau Boost function** **Disabled : Disables Dual Tau Boost function (Default setting)**

3.3.3 SATA Configuration

```
                        Aptio Setup - AMI
     Advanced

SATA Configuration

Serial ATA Port 4            Empty
Serial ATA Port 5            Empty




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




              Version 2.22.1293 Copyright (C) 2025 AMI
```
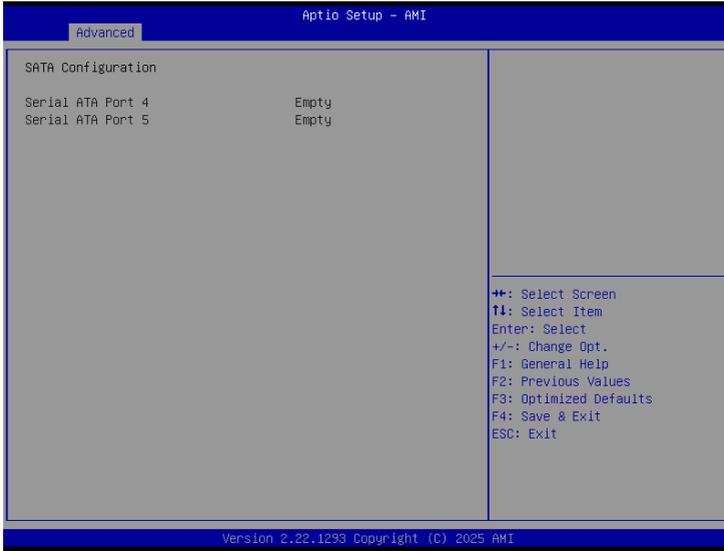
Item	Description
Serial ATA Port 4	shows 2.5" SATA HDD/SSD information
Serial ATA Port 5	

GIGAIPC™

3.3.4   IT8786 Super IO Configuration

Item	Description
Serial Port 1 Configuration	Press [Enter] to configure advanced items : Serial Port : **Enabled : Enables allows you to configure the serial port settings** **Disabled : if Disabled, displays no configuration for the serial port** Device settings : Display the specified Serial Port base I/O address and IRQ COM Port Mode : Choose RS-232, RS-422, or RS-485 feature
Serial Port 2 Configuration	Press [Enter] to configure advanced items : Serial Port : **Enabled : Enables allows you to configure the serial port settings** **Disabled : if Disabled, displays no configuration for the serial port** Device settings : Display the specified Serial Port base I/O address and IRQ

3.3.5   Hardware Monitor

```
                              Aptio Setup - AMI
         Advanced

 CPU Fan Fail Warning               [Enabled]           Enable to set a warning
 System Fan Fail Warning            [Disabled]          message when the CPU fan fail
                                                        or disconnected.
 CPU Fan Speed Control              [Normal]
 System Fan Speed Control           [Normal]

 CPU Temperature                    : +34 %
 System Temperature                 : +30 %
 CPU Fan Speed                      : 917 RPM
 SYS Fan Speed                      : N/A
 VCORE                              : +0.715 V
 DDR                                : +1.155 V
 12V                                : +12.276 V         →←: Select Screen
 5V                                 : +5.087 V          ↑↓: Select Item
 3.3V                               : +3.337 V          Enter: Select
                                                        +/-: Change Opt.
                                                        F1: General Help
                                                        F2: Previous Values
                                                        F3: Optimized Defaults
                                                        F4: Save & Exit
                                                        ESC: Exit


                     Version 2.22.1293 Copyright (C) 2025 AMI
```

Item	Description
CPU Fan Fail Warning	Enabled : Enables CPU FAN Fail warning alert function (Default setting) Disabled : Disables CPU FAN Fail warning alert function
System Fan Fail Warning	Enabled : Enables System FAN Fail warning alert function Disabled : Disables System FAN Fail warning alert function (Default setting)
CPU Fan Speed Control	Normal : Fan speed set by BIOS default (Default setting) Full Speed : Set Fan operates at full speed
System Fan Speed Control	Normal : Fan speed set by BIOS default (Default setting) Full Speed : Set Fan operates at full speed
CPU Temperature	Shows current CPU temperature
System Temperature	Shows current system temperature
CPU Fan Speed	Shows current CPU fan Speed
SYS Fan Speed	Shows current System fan Speed

GIGAIPC™

3.3.6   S5 RTC Wake Settings

```
                              Aptio Setup - AMI
        Advanced

 Wake system from S5              [Disabled]            Enable or disable System wake
                                                        on alarm event. Select
                                                        FixedTime, system will wake on
                                                        the hr::min::sec specified.
                                                        Select DynamicTime , System
                                                        will wake on the current time
                                                        + Increase minute(s)



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



                     Version 2.22.1293 Copyright (C) 2025 AMI
```
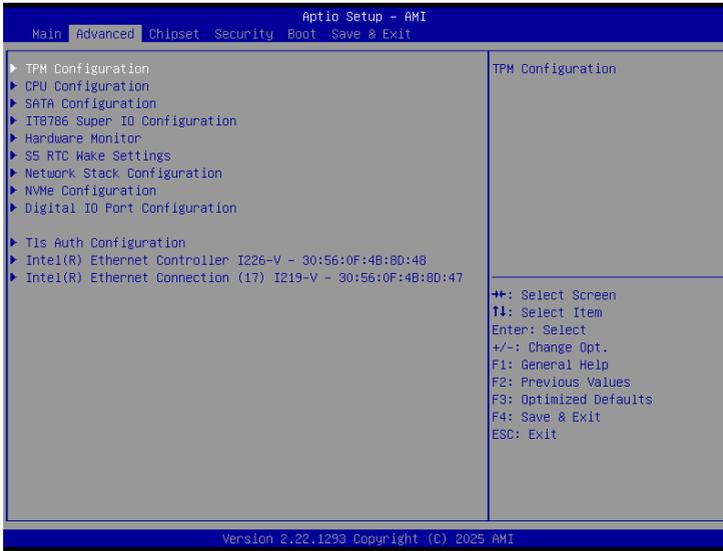
Item	Description
Wake system from S5	Enable or Disable System to wake on a specific time. **Disabled : Disables system to wake on a specific time (Default setting)** **Fixed Time : Enables system to wake on a specific time** **(Format : hr : min : sec)**

3.3.7 Network Stack Configuration

```
                        Aptio Setup - AMI
        Advanced

Network Stack                  [Disabled]          Enable/Disable UEFI Network
                                                   Stack




                                                   →←: Select Screen
                                                   ↑↓: Select Item
```

When Network stack is enabled :

```
                        Aptio Setup - AMI
        Advanced

Network Stack                  [Enabled]           Enable/Disable UEFI Network
IPv4 PXE Support               [Enabled]           Stack
IPv4 HTTP Support              [Enabled]
IPv6 PXE Support               [Enabled]
IPv6 HTTP Support              [Enabled]
PXE boot wait time             0
Media detect count             1




                                                   →←: Select Screen
                                                   ↑↓: Select Item
```
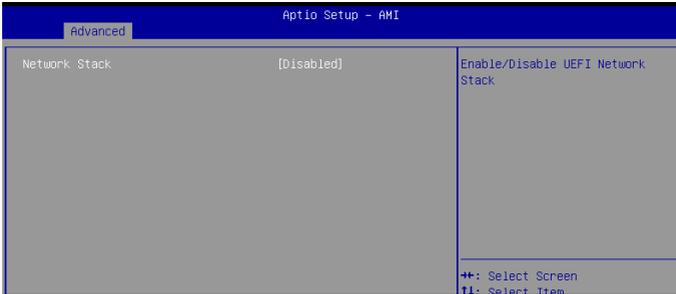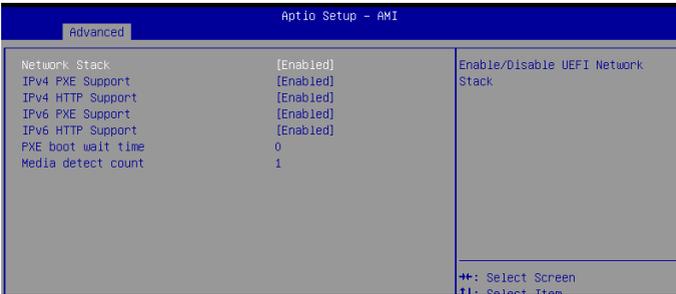
Item	Description
Network Stack	When system is power on, install LAN driver under UEFI mode **Disabled : Disables UEFI Network Stack (Default setting)** **Enabled : Enables UEFI Network Stack**
IPv4 PXE Support	When Network stack is enabled : **Disabled : Disables IPv4 PXE Support** **Enabled : Enables IPv4 PXE Support**
IPv4 HTTP Support	When Network stack is enabled : **Disabled : Disables IPv4 HTTP Support** **Enabled : Enables IPv4 HTTP Support**
IPv6 PXE Support	When Network stack is enabled : **Disabled : Disables IPv6 PXE Support** **Enabled : Enables IPv6 PXE Support**
IPv6 HTTP Support	When Network stack is enabled : **Disabled : Disables IPv6 HTTP Support** **Enabled : Enables IPv6 HTTP Support**
PXE boot wait time	Wait time in seconds, or use ESC key to abort the PXE boot.
Media detect count	Number of times the presence of media will be checked.

3.3.8   NVMe Configuration

NVMe Configuration shows information when your M.2 NVMe PCIe SSD is installed.

```
                              Aptio Setup - AMI
      Advanced

     NVMe Configuration

     No NVME Device Found




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



                    Version 2.22.1293 Copyright (C) 2025 AMI
```

3.3.9   Digital IO Port Configuration

```
                            Aptio Setup – AMI
         Advanced

  Digital IO Port Configuration                          Support OS control BIOS
                                                         Digital IO Item.
  OS control Digital IO              [Disable]           If modify Digital IO Output
                                                         Level in OS, need run S3/S4/S5
  SOGPO_1(Pin 1)                     [Output]            State.
  Select Level                       [LOW]
  SOGPI_1(Pin 2)                     [Input]
  Select Level                       [HIGH]
  SOGPO_2(Pin 3)                     [Output]
  Select Level                       [LOW]
  SOGPI_2(Pin 4)                     [Input]
  Select Level                       [HIGH]
  SOGPO_3(Pin 5)                     [Output]
  Select Level                       [LOW]            ↔: Select Screen
  SOGPI_3(Pin 6)                     [Input]          ↑↓: Select Item
  Select Level                       [HIGH]           Enter: Select
  SOGPO_4(Pin 7)                     [Output]         +/-: Change Opt.
  Select Level                       [LOW]            F1: General Help
  SOGPI_4(Pin 8)                     [Input]          F2: Previous Values
  Select Level                       [HIGH]           F3: Optimized Defaults
                                                      F4: Save & Exit
                                                      ESC: Exit



                     Version 2.22.1293 Copyright (C) 2025 AMI
```

Item	Description
OS control Digital IO	**Disabled : If Digital IO Output value/level is modified in OS, they will not be memorized and kept. (Default setting)** **Enabled : If Digital IO Output value/level is modified in OS, they will be memorized and kept.**
SOGPO_1 (Pin 1) **SOGPI_1 (Pin 2)** **SOGPO_2 (Pin 3)** **SOGPI_2 (Pin 4)** **SOGPO_3 (Pin 5)** **SOGPI_3 (Pin 6)** **SOGPO_4 (Pin 7)** **SOGPI_4 (Pin 8)**	Configure Digital IO Input or Output values for each pin.

3.3.10   Tls Auth Configuration

Item	Description
Enroll Cert	Press [Enter] to configure advanced items : **Server CA Configuration :** Enroll Cert : 1. Enroll Cert Using File 2. Cert GUID : Input digit character in 11111111-2222-3333-4444-1234567 890ab format. 3. Commit Changes and Exit 4. Discard Changes and Exit

3.3.11   Intel(R) Ethernet Controller I226-V - 30:56:0F:4B:8D:48) (MAC address may varied based on different motherboard)

Shows Intel Ethernet controller information

```
                              Aptio Setup - AMI
          Advanced

       UEFI Driver                 Intel(R) 2.5G Ethernet
                                   Controller 0.10.04
       Device Name                 Intel(R) Ethernet
                                   Controller I226-V

       Link Status                 [Disconnected]

       MAC Address                 30:56:0F:4B:8D:48

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

                         Version 2.22.1293 Copyright (C) 2025 AMI
```
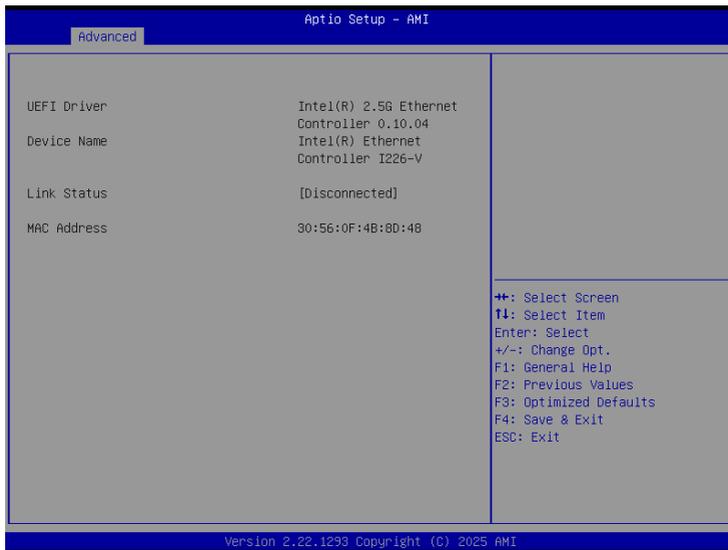
NOTE：MAC address may varied based on different motherboard

3.3.12   Intel(R) Ethernet Connection (17) I219-V - (30:56:0F:4B:8D:47) (MAC address may varied based on different motherboard)

Shows Intel Ethernet controller information
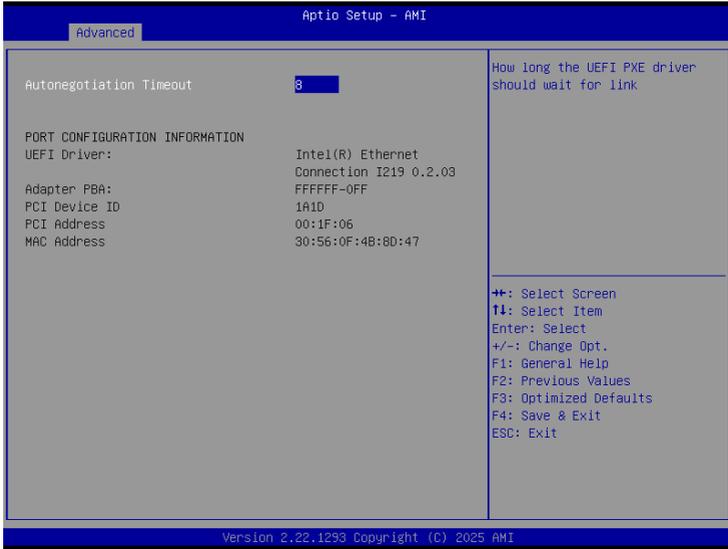
NOTE：MAC address may varied based on different motherboard

3.4   Chipset

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

    VT-d                          [Enabled]          VT-d capability
    DVMT Pre-Allocated            [256M]
    Primary Display               [Auto]
    Internal Graphics             [Auto]

    Onboard LAN 1                 [Enabled]
    Onboard LAN 2                 [Enabled]
    HD Audio                      [Enabled]
    BT Intel LE Audio             [Disabled]

    ErP Lowest Power State Mode   [Disabled]
    Restore AC Power Loss         [Power Off]
    LVDS FW Write Protection      [Enabled]         →←: Select Screen
    LVDS Support                  [Disabled]        ↑↓: Select Item
    LVDS Brightness Level         [100%]            Enter: Select
    LVDS Resolution               [800x600 18bit]   +/-: Change Opt.
    Watchdog Timer                [Disabled]        F1: General Help
    Control Iommu Pre-boot Behavior [Disable IOMMU] F2: Previous Values
                                                    F3: Optimized Defaults
    BIOS Lock                     [Enabled]         F4: Save & Exit
                                                    ESC: Exit




                     Version 2.22.1293 Copyright (C) 2025 AMI
```

Item	Description
VT-d	**Enabled : Enables VT-d function (Default setting)** **Disabled : Disables VT-d function**
DVMT Pre-Allocated	Use DVMT Pre-Allocated to set the amount of system memory which is installed to the integrated graphics processor **Option items : 32M , 64M, 128M, 256M (Default setting)**
Primary Display	**Auto : When detects PCIe Graphic card, primary display will set to PCIe (Default setting)** **IGFX : Force IGFX Graphic card as the primary display device** **PEG : Force PEG Graphic card as the primary display device**
Internal Graphics	Enables or disables the onboard graphics function **Auto : Detects display device automatically (Default setting)** **Enabled : Enables onboard graphics** **Disabled : Disables onboard graphics**
Onboard LAN1 Onboard LAN2	Enable/Disable onboard LAN controller **Enabled : Enables onboard LAN controller (Default setting)** **Disabled : Disables onboard LAN controller**

HD Audio	Enable/Disable onboard audio controller **Enabled : Enables onboard audio controller (Default setting)** **Disabled : Disables onboard audio controller**
ErP Lowest Power State Mode	Enable/Disable power saving funtion **Enabled : Enables ErP Lowest Power State Mode** **Disabled : Disabled ErP Lowest Power State Mode (Default setting)**
Restore AC Power Loss	To set which option the system should returns if a sudden power loss occured **Power off : Do not power on when the power is back (Default setting)** **Power on : System power on when the power is back** **Last state : Restore the system to the state before power loss occures**
LVDS FW Write Protection	Prevent accidental firmware overwrite or removal. **Disabled : Disables LVDS FW Write Protection** **Enabled : Enables LVDS FW Write Protection (Default setting)**
LVDS Support	**Disabled : Disables LVDS Support (Default setting)** **Enabled : Enables LVDS Support**
LVDS Brightness Level	When LVDS Support is enabled : To modified the backlight brightness of the LVDS panel **Option items : 10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%, 90%, 100% (Default Setting)**
LVDS Resolution	When LVDS Support is enabled : To modified the LVDS resolution **Option items : 800x600 18bit (Default Setting) , 1024x768 18bit, 1024x768 24bit, 1024x600 18bit, 1280x800 18bit, 1280x960 18bit, 1280x1024 24bit, 1366x768 18bit, 1366x768 24bit, 1440x900 24bit, 1400x1050 24bit, 1600x900 24bit, 1680x1050 24bit, 1600x1200 24bit, 1920x1080 24bit, 1920x1200 24bit**
Watchdog Timer	Enable/Disable Watchdog Timer function **Disabled : Disables Watchdog Timer function (Default setting)** **Enabled : Enables Watchdog Timer function**
Control Iommu Pre-boot Behavior	Enable/Disable Control Iommu Pre-boot behavior **Disabled : Disables IOMMU during boot (Default setting)** **Enabled : Enables IOMMU during boot**
BIOS Lock	Enable/Disable BIOS Lock function **Enabled : Enables BIOS Lock function (Default setting)** **Disabled : Disabled BIOS Lock funtion**

3.5   Security

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

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

                         Version 2.22.1293 Copyright (C) 2025 AMI
```

Item	Description
Administrator Password	To set up Administrator's password **Minimum length : 3** **Maximum length : 20**
User Password	To set up User's password **Minimum length : 3** **Maximum length : 20**
Secure Boot	Press <Enter> to configure the advanced items

```
                        Aptio Setup - AMI
                  Security

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

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

                  Version 2.22.1293 Copyright (C) 2025 AMI
```

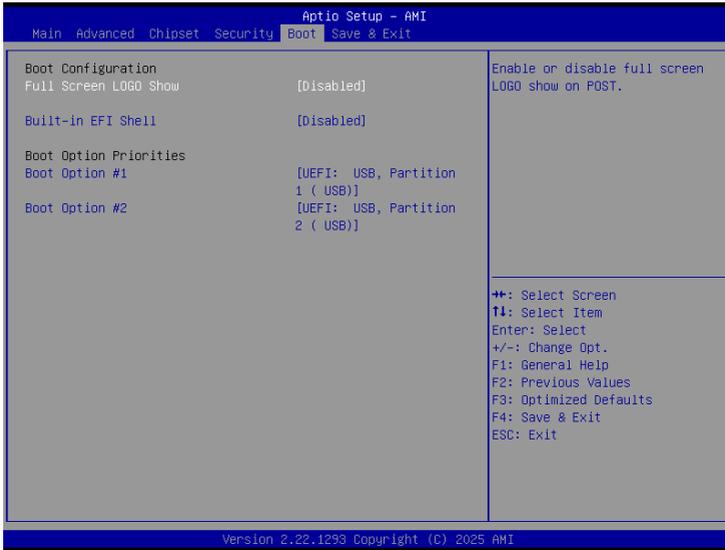| Item	Description
Secure Boot	Secure Boot requires all the applications that are running during the booting process to be pre-signed with valid digital certificates **Enabled : Enables Secure Boot function** **Disabled : Disables Secure Boot function (Default setting)**
Secure Boot Mode	**Standard : Standard mode** **Custom : Custom mode (Default setting)**
Restore Factory Keys	To restore factory settings **Yes : Agree to restore factory settings** **No : Cancel to restore factory settings**
Reset To Setup Mode	**Yes : Agree to setup mode** **No : Cancel to setup mode**
Expert Key Management	Enables expert users to modify Secure boot policy variables without full authentication Press <Enter> to configure the advanced items

```
                          Aptio Setup - AMI
              ┌─Security─┐

   Vendor Keys                      Valid                    Install factory default Secure
                                                             Boot keys after the platform
   Factory Key Provision            [Enabled]                reset and while the System is
 ▶ Restore Factory Keys                                      in Setup mode
 ▶ Reset To Setup Mode
 ▶ Enroll Efi Image
 ▶ Export Secure Boot variables

   Secure Boot variable    | Size| Keys| Key Source
 ▶ Platform Key      (PK)|  823|    1| Factory
 ▶ Key Exchange Keys (KEK)| 3066|    2| Factory
 ▶ Authorized Signatures (db)| 7636|   5| Factory
 ▶ Forbidden  Signatures(dbx)|20668| 430| Factory
 ▶ Authorized TimeStamps(dbt)|    0|   0| No Keys    →←: Select Screen
 ▶ OsRecovery Signatures(dbr)|    0|   0| No Keys    ↑↓: Select Item
                                                     Enter: Select
   MS UEFI CA key                   [Enabled]        +/-: Change Opt.
                                                     F1: General Help
                                                     F2: Previous Values
                                                     F3: Optimized Defaults
                                                     F4: Save & Exit
                                                     ESC: Exit

                Version 2.22.1293 Copyright (C) 2025 AMI
```

Item	Description
Factory Key Provision	Install factory default Secure Boot keys after the platform reset and while the system is in Setup mode **Enabled : Enables Factory Key Provision (Default setting) Disabled : Disables Factory Key Provision**
Restore Factory Keys	To restore factory settings **Yes : Agree to restore factory settings No : Cancel to restore factory settings**
Reset To Setup Mode	**Yes : Agree to setup mode No : Cancel to setup mode**
Enroll Efi Image	Allow the image to run in Secure Boot mode
Export Secure Boot variables	Copy NVRAM content of Secure Boot variables to files in a root folder on a file system device

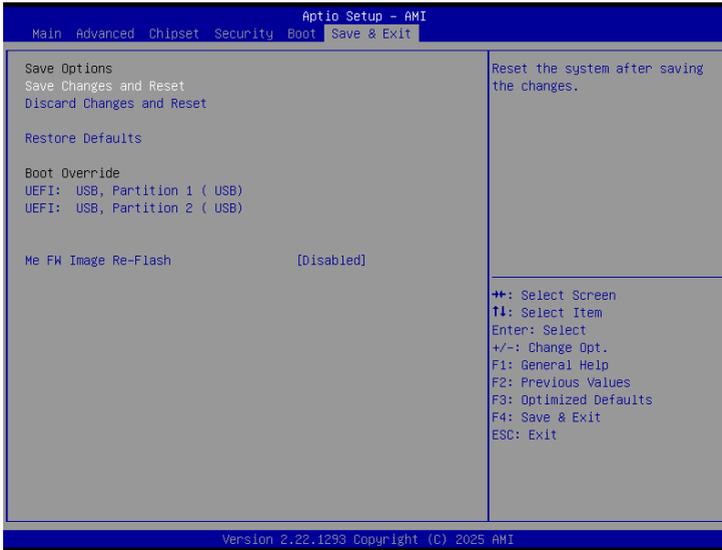| Item	Description
Platform Key (PK)	These items allows you to enroll factory defaults or load Certificates from a file.
Key Exchange Keys (KEK)	
Authorized Signatures (db)	
Forbidden Signatures (dbx)	
Authorized TimeStamps (dbt)	
OsRecovery Signatures (dbr)	
MS UEFI CA Key	Device Guard ready system must not list 'Microsoft UEFI CA' Certificate in Authorized Signature database(db)

3.7　　Save & Exit

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

  Save Options                                    Reset the system after saving
  Save Changes and Reset                          the changes.
  Discard Changes and Reset

  Restore Defaults

  Boot Override
  UEFI:  USB, Partition 1 ( USB)
  UEFI:  USB, Partition 2 ( USB)

  Me FW Image Re-Flash            [Disabled]


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



                    Version 2.22.1293 Copyright (C) 2025 AMI
```

Item	Description
Save Changes and Reset	After configuring all the options that you wish to change, choose this option to save all the changes and reboot the system **Yes : Agree to save and reset** **No : Cancel to save and reset**
Discard Changes and Reset	Choose this option to reboot the system without saving any changes **Yes : Agree to discard changes and reset** **No : Cancel to discard changes and reset**
Restore Defaults	Restore/Load default values for all the setup options **Yes : Agree to load optimized defaults** **No : Cancel to load optimized defaults**
Me FW Image Re-Flash	Enable/Disable Me FW image re-flash function **Enabled : Enables Me FW image re-flash function** **Disabled : Disables Me FW image re-flash function (Default setting)**