MSI®

MS-98M3

Industrial Computer Board

User Guide

Contents

Revision

V1.3, 2024/07

Safety Information

- The components included in this package are prone to damage from electrostatic discharge (ESD). Please adhere to the following instructions to ensure successful computer assembly.

- Ensure that all components are securely connected. Loose connections may cause the computer to not recognize a component or fail to start.

- Hold the motherboard by the edges to avoid touching sensitive components.

- It is recommended to wear an electrostatic discharge (ESD) wrist strap when handling the motherboard to prevent electrostatic damage. If an ESD wrist strap is not available, discharge yourself of static electricity by touching another metal object before handling the motherboard.

- Store the motherboard in an electrostatic shielding container or on an anti-static pad whenever the motherboard is not installed.

- Before turning on the computer, ensure that there are no loose screws or metal components on the motherboard or anywhere within the computer case.

- Do not boot the computer before installation is completed. This could cause permanent damage to the components as well as injury to the user.

- If you need help during any installation step, please consult a certified computer technician.

- Always turn off the power supply and unplug the power cord from the power outlet before installing or removing any computer component.

- Keep this user guide for future reference.

- Keep this motherboard away from humidity.

- Make sure that your electrical outlet provides the same voltage as is indicated on the PSU, before connecting the PSU to the electrical outlet.

- Place the power cord such a way that people can not step on it. Do not place anything over the power cord.

- All cautions and warnings on the motherboard should be noted.

- If any of the following situations arises, get the motherboard checked by service personnel:
  - Liquid has penetrated into the computer.
  - The motherboard has been exposed to moisture.
  - The motherboard does not work well or you can not get it work according to user guide.
  - The motherboard has been dropped and damaged.
  - The motherboard has obvious sign of breakage.

- Do not leave this motherboard in an environment above 60°C (140°F), it may damage the motherboard.

Regulatory Notices

CE Conformity

Hereby, Micro-Star International CO., LTD declares that this device is in compliance with the essential safety requirements and other relevant provisions set out in the European Directive.

FCC-B Radio Frequency Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital 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 instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the measures listed below:

• Reorient or relocate the receiving antenna.

• Increase the separation between the equipment and receiver.

• Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

• Consult the dealer or an experienced radio/television technician for help.

Notice 1

The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Notice 2

Shielded interface cables and AC power cord, if any, must be used in order to comply with the emission limits.

This device complies with Part 15 of the 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.

WEEE Statement

Under the European Union ("EU") Directive on Waste Electrical and Electronic Equipment, Directive 2012/19/EU, products of "electrical and electronic equipment" cannot be discarded as municipal waste anymore and manufacturers of covered electronic equipment will be obligated to take back such products at the end of their useful life.

Chemical Substances Information

In compliance with chemical substances regulations, such as the EU REACH Regulation (Regulation EC No. 1907/2006 of the European Parliament and the Council), MSI provides the information of chemical substances in products at:

https://csr.msi.com/global/index

Green Product Features

• Reduced energy consumption during use and stand-by

• Limited use of substances harmful to the environment and health

• Easily dismantled and recycled

• Reduced use of natural resources by encouraging recycling

• Extended product lifetime through easy upgrades

• Reduced solid waste production through take-back policy

Battery Information

Please take special precautions if this product comes with a battery.

• Danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer.

• Avoid disposal of a battery into fire or a hot oven, or mechanically crushing or cutting of a battery, which can result in an explosion.

• Avoid leaving a battery in an extremely high temperature or extremely low air pressure environment that can result in an explosion or the leakage of flammable liquid or gas.

• Do not ingest battery. If the coin/button cell battery is swallowed, it can cause severe internal burns and can lead to death. Keep new and used batteries away from children.

European Union:

Batteries, battery packs, and accumulators should not be disposed of as unsorted household waste. Please use the public collection system to return, recycle, or treat them in compliance with the local regulations.

BSMI:

廢電池請回收
For better environmental protection, waste batteries should be collected separately for recycling or special disposal.

California, USA:

The button cell battery may contain perchlorate material and requires special handling when recycled or disposed of in California.
For further information please visit:
http://www.dtsc.ca.gov/hazardouswaste/perchlorate/

Environmental Policy

- The product has been designed to enable proper reuse of parts and recycling and should not be thrown away at its end of life.

- Users should contact the local authorized point of collection for recycling and disposing of their end-of-life products.

- Visit the MSI website and locate a nearby distributor for further recycling information.

- Users may also reach us at gpcontdev@msi.com for information regarding proper disposal, take-back, recycling, and disassembly of MSI products.

Copyright and Trademarks Notice

Copyright © Micro-Star Int'l Co., Ltd. All rights reserved. The MSI logo used is a registered trademark of Micro-Star Int'l Co., Ltd. All other marks and names mentioned may be trademarks of their respective owners. No warranty as to accuracy or completeness is expressed or implied. MSI reserves the right to make changes to this document without prior notice.

The terms HDMI™, HDMI™ High-Definition Multimedia Interface, HDMI™ Trade dress and the HDMI™ Logos are trademarks or registered trademarks of HDMI™ Licensing Administrator, Inc.

Technical Support

If a problem arises with your product and no solution can be obtained from the user's manual, please contact your place of purchase or local distributor. Alternatively, please visit https://www.msi.com/support/ for further guidance.

Specifications

Model	MS-98M3
Processor	• Embedded SKUs - 11th Gen Intel® IoTG Mobile Tiger Lake-UP3 Core™ i7-1185G7E/ i5-1145G7E, QC, 28W - 11th Gen Intel® IoTG Mobile Tiger Lake-UP3 Core™ i3-1115G4E, DC, 28W - 11th Gen Intel® IoTG Mobile Tiger Lake-UP3 Celeron® 6305E, DC, 15W • Industrial SKUs - 11th Gen Intel® IoTG Mobile Tiger Lake-UP3 Core™ i7-1185GRE/i5-1145GRE, QC, 28W - 11th Gen Intel® IoTG Mobile Tiger Lake-UP3 Core™ i3-1115GRE, DC, 28W
Chipset	Within processor
iAMT Support	• AMT 15.0 supported (Only for Intel i7/ i5 CPU series, not support G3 to S5)
Memory	• 2 x DDR4 SO-DIMM slots - Dual Channel for DDR4, Non-ECC - Up to 3200 MT/s - Up to 64 GB
Network	• 2 x Intel® I225-LM 2.5 GbE LAN (For Embedded SKUs) • 2 x Intel® I225-IT 2.5 GbE LAN (For Industrial SKUs)
Storage	• 1 x SATA 3.0 6Gb/s port • 1 x M.2 M Key (2280) slot - PCIe Gen 4 x4 NVMe signal • 1 x M.2 B Key (2242/ 3042) slot - SATA 3.0
Audio	• Realtek® ALC888S High Definition Audio codec • 1 x Onboard connector for audio (Line-in/ Line-Out/ MIC-in) & amplifier

Model	MS-98M3

Graphics	Within processor
	
	• 2 x LVDS up to 1920x1200 @60Hz (Co-lay eDP)
	
	• 2 x eDP up to 4096×2160 @60 Hz（Co-lay LVDS）
	
	• 1 x DP 1.4a up to 7680 x 4320 @60Hz
	
	• 1 x HDMI™ 1.4 up to 4096x2160 @30Hz
	
	• 4 independent displays
	
	  - LVDS1 or eDP1
	
	  - LVDS2 or eDP2
	
	  - HDMI™
	
	  - DP

Power	12V~24V DC-in power connector* *The power adapter you use should provide at least 90W.
Rear Panel I/O	• 1 x DisplayPort • 1 x HDMI™ connector • 4 x USB 10Gbps Type-A ports • 2 x RJ-45 2.5 GbE LAN ports

Expansion Slots	• 1 x M.2 B Key (2242/ 3042) slot
	
	  - With PCIe x1, SATA 3.0, USB 2.0 signal
	
	  - Support SIM holder
	
	  - Support 5G modules
	   (A thermal kit will be designed for a 5G module based on the requirements of the system.)
	
	• 1 x M.2 E Key (2230) slot
	
	  - With PCIe x1 & USB 2.0 signal
	
	  - Support Intel® Wi-Fi 5 & BT-5.0, Intel® Wi-Fi 6 & BT-5.1 (vPro supported)
	
	• 1 x Nano SIM Holder
	
	  - Supported by M.2 B key (SIM) slot

Model	MS-98M3
Onboard I/O	• 1 x SATA power connector
	• 1 x System fan connector
	• 1 x Front panel connector
	• 2 x Dual COM port box headers (RS232/ 422/ 485)
	• 1 x Audio/ Amplifier/ SMbus box header
	• 1 x LVDS Inverter box header
	• 2 x USB 2.0 box headers
	• 1 x GPIO (DIO) Connector
	• 1 x Clear CMOS jumper
	• 1 x AT/ ATX mode select jumper
	• 2 x COM1~4 select jumpers
	• 1 x ME jumper
Form Factor	3.5-inch size: 146mm (L) x 102mm (W)
ACPI	G3 to S5 mode does not support
Environment	• Operating Temperature
	- Embedded (Non-WT) SKUs: -10 ~ 60°C with 0.7m/s air flow
	- Industrial (WT) SKUs: -40 ~ 70°C with 0.7m/s air flow (w/ Turbo disabled)
	- The standard thermal solution only supports TDP up to 15W. For higher power consumption, redesigning the H/S is required.
	• Storage Temperature
	- Embedded (Non-WT) SKUs: -20 ~ 80°C
	- Industrial (WT) SKUs: -40 ~ 85°C
	• Humidity: 10 ~ 90%, non-condensing

Rear I/O Panel

DisplayPort · HDMI™ HIGH-DEFINITION MULTIMEDIA INTERFACE · USB 10Gbps Ports · 2.5 GbE RJ-45 LAN Ports

DisplayPort

DisplayPort is a digital display interface standard. This connector is used to connect a monitor with DisplayPort inputs.

HDMI™ Connector ⌂HᴰmI™ HIGH-DEFINITION MULTIMEDIA INTERFACE
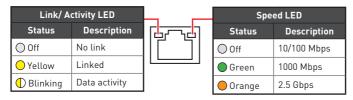
HDMI™ is a digital interface for uncompressed audio/video streams, accommodating all TV formats and multi-channel audio on a single cable.

USB 10Gbps Ports
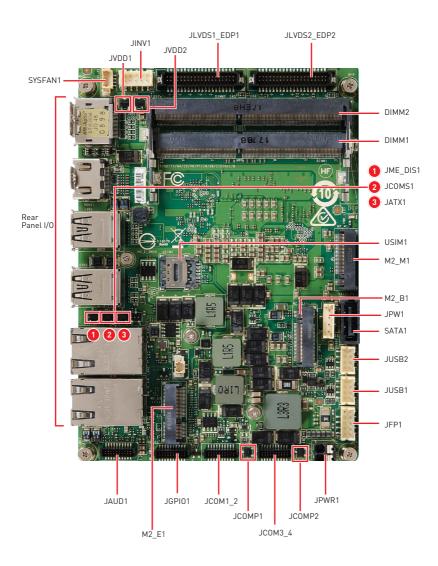
USB 10Gbps, delivers high-speed data transfer for various devices, such as storage devices, hard drives, video cameras, etc.

2.5 GbE RJ-45 LAN Ports

The standard single RJ45 LAN jack is provided for connection to the Local Area Network (LAN). You can connect a network cable to it.

Link/ Activity LED	
Status	Description
⚪ Off	No link
🟡 Yellow	Linked
🌗 Blinking	Data activity

Speed LED	
Status	Description
⚪ Off	10/100 Mbps
🟢 Green	1000 Mbps
🟠 Orange	2.5 Gbps

Motherboard Overview

- SYSFAN1
- JVDD1
- JINV1
- JVDD2
- JLVDS1_EDP1
- JLVDS2_EDP2
- DIMM2
- DIMM1
- 1 JME_DIS1
- 2 JCOMS1
- 3 JATX1
- Rear Panel I/O
- USIM1
- M2_M1
- M2_B1
- JPW1
- SATA1
- JUSB2
- JUSB1
- JFP1
- JAUD1
- JGPIO1
- JCOM1_2
- JCOMP1
- JCOMP2
- JPWR1
- M2_E1
- JCOM3_4
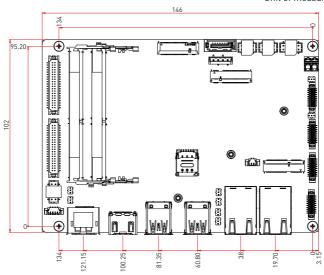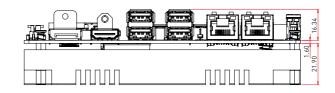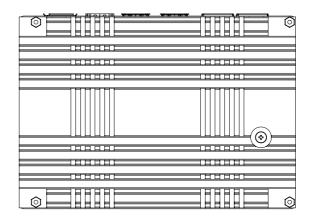
ME Overview

Board Dimension
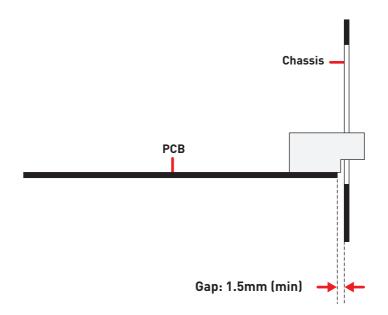
Unit of measurement: mm

Suggested Chassis I/O Gap Dimension

Chassis

PCB

Gap: 1.5mm (min)

Component Contents

Memory

DDR4 SO DIMM Slot: DIMM1, DIMM2

The SO-DIMM slots is intended for memory modules.

1. Locate the SO-DIMM slot. Align the notch on the DIMM with the key on the slot and insert the DIMM into the slot.

2. Push the DIMM gently downwards until the slot levers click and lock the DIMM in place.

3. To uninstall the DIMM, flip the slot levers outwards and the DIMM will be released instantly.
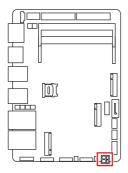
⚠ **Important**
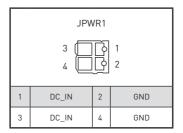
• *You can barely see the golden finger if the DIMM is properly inserted in the DIMM slot.*

• *Always insert memory modules in the DIMM1 slot first.*

• *To ensure system stability for Dual channel mode, memory modules must be of the same type, number and density.*

Power Supply

JPWR1: 12V~24V DC-in Power Connector
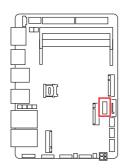
This connector allows you to connect a power supply. To connect to the power supply, make sure the plug of the power supply is inserted in the proper orientation and the pins are aligned. Then push down the power supply firmly into the connector.

JPWR1			
1	DC_IN	2	GND
3	DC_IN	4	GND
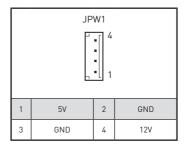
JPW1: SATA Power Connector

This connector is used to provide power to SATA devices.

JPW1			
1	5V	2	GND
3	GND	4	12V
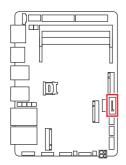
⚠️ *Important*

Make sure that all the power cables are securely connected to a proper power supply to ensure stable operation of the system.

Storage

SATA1: SATA 3.0 6Gb/s Port

This connector is SATA 6Gb/s interface port, it can connect to one SATA device.

SATA1
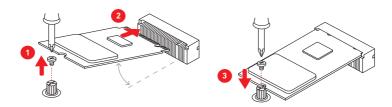
⚠ *Important*

• *This SATA port supports hot plug.*

• *Please do not fold the SATA cable at a 90-degree angle. Data loss may result during transmission otherwise.*

• *SATA cables have identical plugs on either sides of the cable. However, it is recommended that the flat connector be connected to the motherboard for space saving purposes.*

M2_M1: M.2 Slot (M Key, 2280)

Please install the M.2 solid-state drive (SSD) into the M.2 slot as shown below.
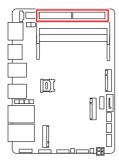
Feature

Supports PCIe Gen 4 x4 NVMe signal.

Graphics

JLVDS1_EDP1, JLVDS2_EDP2: LVDS + eDP Box Header

These connectors are provided for LVDS/eDP interface flat panels. After connecting an LVDS/eDP interface flat panel to this connector, be sure to check the panel datasheet and set the JVDD1/ JVDD2 LVDS jumper to proper power voltage.

⚠️ *Important*

Please refer to the following pages for the pin-out of the LVDS + eDP Box Header and the pin-out for LVDS/eDP interface flat panels.

eDP Panel (P1)	98M3 Motherboard (P2)				eDP Panel (P1)
	JLVDS1_EDP1 JLVDS2_EDP2 40　　　　　　2 39　　　　　　1				
Lane3_P	EDP_LINE3_DP	1	2	EDP_LINE2_DP	Lane2_P
Lane3_N	EDP_LINE3_DN	3	4	EDP_LINE2_DN	Lane2_N
	DDC0_CLK_7513_R	5	6	DDC0_DATA_7513_R	
LCD_VCC	LCD_VDD	7	8	LCD_VDD	LCD_VCC
LCD_VCC	LCD_VDD	9	10	VCC3	
	BKLT_EN	11	12	LVDS_DETECT#	LCD_GND
Lane1_P	LVDSA_DATA1+	13	14	EHPDET/ LVDSA_DATA0+	HPD
Lane1_N	LVDSA_DATA1-	15	16	LVDSA_DATA0-	
H_GND	GND	17	18	GND	H_GND
	LVDSA_DATA3+	19	20	LVDSA_DATA2+	Lane0_P
	LVDSA_DATA3-	21	22	LVDSA_DATA2-	Lane0_N
H_GND	GND	23	24	GND	H_GND
	LVDSB_DATA1+	25	26	LVDSB_DATA0+	
	LVDSB_DATA1-	27	28	LVDSB_DATA0-	
H_GND	GND	29	30	GND	GND
	LVDSB_DATA3+	31	32	LVDSB_DATA2+	
	LVDSB_DATA3-	33	34	LVDSB_DATA2-	
	NA	35	36	GND	GND
	LVDSB_CLK+	37	38	LVDSA_CLK+	AUX_CH_P
	LVDSB_CLK-	39	40	LVDSA_CLK-	AUX_CH_N
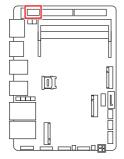
LVDS Panel (P1)	98M3 Motherboard (P2)				LVDS Panel (P1)
	JLVDS1_EDP1 JLVDS2_EDP2 40 2 39 1				
	EDP_LINE3_DP	1	2	EDP_LINE2_DP	
	EDP_LINE3_DN	3	4	EDP_LINE2_DN	
	DDC0_CLK_7513_R	5	6	DDC0_DATA_7513_R	
VCC	LCD_VDD	7	8	LCD_VDD	VCC
VCC	LCD_VDD	9	10	VCC3	
	BKLT_EN	11	12	LVDS_DETECT#	GND
RXO1+	LVDSA_DATA1+	13	14	EHPDET/ LVDSA_DATA0+	RXO0+
RXO1-	LVDSA_DATA1-	15	16	LVDSA_DATA0-	RXO0-
GND	GND	17	18	GND	GND
RXO3+	LVDSA_DATA3+	19	20	LVDSA_DATA2+	RXO2+
RXO3-	LVDSA_DATA3-	21	22	LVDSA_DATA2-	RXO2-
GND	GND	23	24	GND	GND
RXE1+	LVDSB_DATA1+	25	26	LVDSB_DATA0+	RXE0+
RXE1-	LVDSB_DATA1-	27	28	LVDSB_DATA0-	RXE0-
GND	GND	29	30	GND	GND
RXE3+	LVDSB_DATA3+	31	32	LVDSB_DATA2+	RXE2+
RXE3-	LVDSB_DATA3-	33	34	LVDSB_DATA2-	RXE2-
	NA	35	36	GND	GND
RXEC+	LVDSB_CLK+	37	38	LVDSA_CLK+	RXOC+
RXEC-	LVDSB_CLK-	39	40	LVDSA_CLK-	RXOC-

⚠️ Important

Pin 12 is a detect pin. When using a customized LVDS cable, pin 12 should be a signal ground with a low impedance. Otherwise, LVDS will not function.

JINV1: LVDS Inverter Box Header

The connector is provided for LCD backlight options.
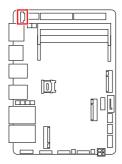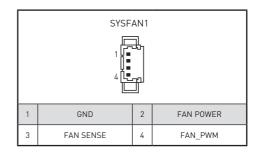
JINV1			
1	GND	2	GND
3	VCC5	4	VCC5
5	+12V	6	+12V
7	INV_ON#1	8	INV_ON#2
9	L_BKLT_CTRL#1	10	L_BKLT_CTRL#2

Connector

SYSFAN1: System Fan Header

The fan power connector supports system cooling fans with +12V. When connecting the wire to the connectors, always note that the red wire is the positive and should be connected to the +12V; the black wire is Ground and should be connected to GND. If the motherboard has a System Hardware Monitor chipset onboard, you must use a specially designed fan with speed sensor to take advantage of the fan control.

SYSFAN1			
1	GND	2	FAN POWER
3	FAN SENSE	4	FAN_PWM

⚠️ *Important*
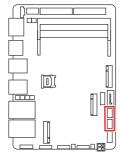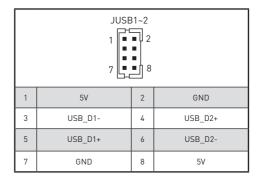
• *Please refer to the recommended CPU fans at processor's official website or consult the vendors for proper CPU cooling fan.*

JUSB1~2: USB 2.0 Box Header

These connectors are ideal for connecting USB devices such as keyboard, mouse, or other USB-compatible devices.

	JUSB1~2		
1	5V	2	GND
3	USB_D1-	4	USB_D2+
5	USB_D1+	6	USB_D2-
7	GND	8	5V
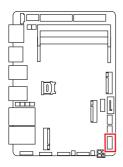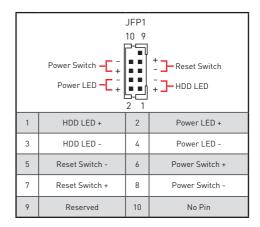
⚠️ *Important*

Note that the VCC and GND pins must be connected correctly to avoid possible damage.

JFP1: Front Panel Box Header
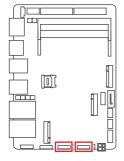
This front-panel connector is provided for electrical connection to the front panel switches & LEDs and is compliant with Intel Front Panel I/O Connectivity Design Guide.

	JFP1		
1	HDD LED +	2	Power LED +
3	HDD LED -	4	Power LED -
5	Reset Switch -	6	Power Switch +
7	Reset Switch +	8	Power Switch -
9	Reserved	10	No Pin
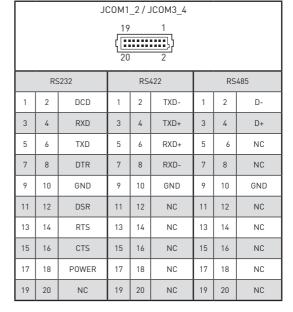
JCOM1_2, 3_4: COM Port Box Header(RS232/ 422/ 485)
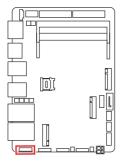
This connector is a 16550A high speed communications port that sends/receives 16 bytes FIFOs. You can attach a serial device to it.

JCOM1_2 / JCOM3_4								
RS232			RS422			RS485		
1	2	DCD	1	2	TXD-	1	2	D-
3	4	RXD	3	4	TXD+	3	4	D+
5	6	TXD	5	6	RXD+	5	6	NC
7	8	DTR	7	8	RXD-	7	8	NC
9	10	GND	9	10	GND	9	10	GND
11	12	DSR	11	12	NC	11	12	NC
13	14	RTS	13	14	NC	13	14	NC
15	16	CTS	15	16	NC	15	16	NC
17	18	POWER	17	18	NC	17	18	NC
19	20	NC	19	20	NC	19	20	NC

JAUD1: Audio/ Amplifier/ SMbus Connector
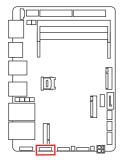
This connector allows you to connect audio. It also supports amplifier function to enhance audio performance and SMBus, known as I2C, for connecting System Management Bus (SMBus) interface.

JAUD1 19 1 20 2			
1	LINE_IN_RA	2	MIC1_RA
3	LINE_IN_LA	4	MIC1_LA
5	LOUT_RA	6	MIC1_JD
7	LOUT_LA	8	LINE1_JD
9	FRONT_JD	10	AGND
11	AGND	12	AGND
13	5VSB	14	AMP_L-
15	SMBCLK	16	AMP_L+
17	SMBDATA	18	AMP_R-
19	GND	20	AMP_R+

JGPIO1: GPIO (DIO) Connector

This connector is provided for the General-Purpose Input/Output (GPIO) peripheral module.
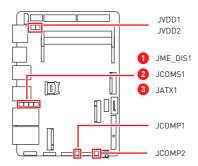
JGPIO1			
1	GND	2	GND
3	GPO0	4	GPI0
5	GPO1	6	GPI1
7	GPO2	8	GPI2
9	GPO3	10	GPI3
11	GPO4	12	GPI4
13	GPO5	14	GPI5
15	GPO6	16	GPI6
17	GPO7	18	GPI7
19	VCC5	20	VCC5

Jumper

⚠️ *Important*
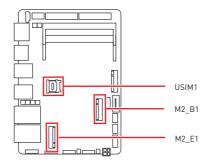
Avoid adjusting jumpers when the system is on; it will damage the motherboard.

Jumper Name	Default Setting	Description	
JVDD1 JVDD2	▣▐ 1	1-2: 3V	2-3: 5V
JME_DIS1	▣▐ 1	1-2: Normal	2-3: ME Disable
JCMOS1	▣▐ 1	1-2: Normal	2-3: Clear CMOS
JATX1	▣▐ 1	1-2: ATX	2-3: AT
JCOMP1 JCOMP2	▐ 1 ▣	1-2: 5V	2-3: 12V

Expansion Slot
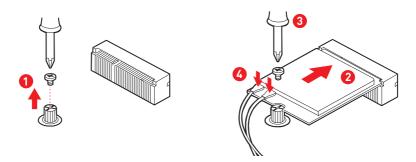
USIM1：Nano SIM Holder

This holder is provided for 3G, 4G, LTE, 5G Nano SIM cards.

M2_E1: M.2 Slot (E Key, 2230)

Please install the Wi-Fi/ Bluetooch card into the M.2 slot as shown below.
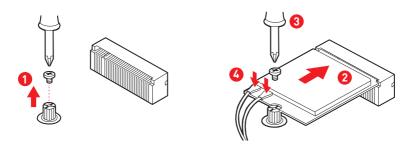
Feature

• M2_E1 slot supports PCIe x 1 & USB 2.0 signal.

M2_B1: M.2 Slot (B Key, 2242/ 3042)

Please install the WWAN Card/ solid-state drive (SSD) into the M.2 slot as shown below.

Feature

• Supports PCIe x 1, SATA 3.0, USB 2.0 signal.

• Supports Innodisk module: EGP2-X401-W1, EGPL-G202-W1, EGPS-3401-C1.

• Supports Thales's Cinterion® MV31-W IoT modem card.

Bios Setup

This chapter provides information on the BIOS Setup program and allows users to configure the system for optimal use.

Users may need to run the Setup program when:

• An error message appears on the screen at system startup and requests users to run SETUP.

• Users want to change the default settings for customized features.

⚠ *Important*

• *Please note that BIOS update assumes technician-level experience.*

• *As the system BIOS is under continuous update for better system performance, the illustrations in this chapter should be held for reference only.*

Entering Setup

Power on the computer and the system will start POST (Power On Self Test) process. When the message below appears on the screen, press <DEL> or <F2> key to enter Setup.

> **Press <DEL> or <F2> to enter SETUP**

If the message disappears before you respond and you still wish to enter Setup, restart the system by turning it **OFF** and **On** or pressing the **RESET** button. You may also restart the system by simultaneously pressing **<Ctrl>, <Alt>, and <Delete>** keys.

⚠ *Important*

The items under each BIOS category described in this chapter are under continuous update for better system performance. Therefore, the description may be slightly different from the latest BIOS and should be held for reference only.

Control Keys

← →	Select Screen
↑ ↓	Select Item
Enter	Select
+ -	Change Value
Esc	Exit
F1	General Help
F7	Previous Values
F9	Optimized Defaults
F10	Save & Reset*
F12	Screenshot capture
<K>	Scroll help area upwards
<M>	Scroll help area downwards

* When you press **F10**, a confirmation window appears and it provides the modification information. Select between **Yes** or **No** to confirm your choice.

Getting Help

Upon entering setup, you will see the Main Menu.

Main Menu

The main menu lists the setup functions you can make changes to. You can use the **arrow keys (↑↓)** to select the item. The on-line description of the highlighted setup function is displayed at the bottom of the screen.

Sub-Menu

If you find a right pointer symbol appears to the left of certain fields that means a sub-menu can be launched from this field. A sub-menu contains additional options for a field parameter. You can use **arrow keys (↑↓)** to highlight the field and press **<Enter>** to call up the sub-menu. Then you can use the **control keys** to enter values and move from field to field within a sub-menu. If you want to return to the main menu, just press the **<Esc>.**

General Help <F1>

The BIOS setup program provides a General Help screen. You can call up this screen from any menu by simply pressing **<F1>**. The Help screen lists the appropriate keys to use and the possible selections for the highlighted item. Press **<Esc>** to exit the Help screen.

BIOS Item Contents

The Menu Bar

▶ **Main**

   Use this menu for basic system configurations, such as time, date, etc.

▶ **Advanced**

   Use this menu to set up the items of special enhanced features.

▶ **Boot**

   Use this menu to specify the priority of boot devices.

▶ **Security**

   Use this menu to set supervisor and user passwords.

▶ **Chipset**

   This menu controls the advanced features of the onboard chipsets.
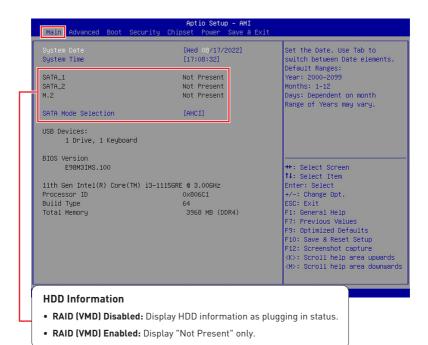
▶ **Power**

   Use this menu to specify your settings for power management.

▶ **Save & Exit**

   This menu allows you to load the BIOS default values or factory default settings into the BIOS and exit the BIOS setup utility with or without changes.

Main

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

 System Date                    [Wed 08/17/2022]        Set the Date. Use Tab to
 System Time                    [17:08:32]              switch between Date elements.
                                                        Default Ranges:
 SATA_1                         Not Present             Year: 2000-2099
 SATA_2                         Not Present             Months: 1-12
 M.2                            Not Present             Days: Dependent on month
                                                        Range of Years may vary.
 SATA Mode Selection            [AHCI]

 USB Devices:
      1 Drive, 1 Keyboard

 BIOS Version
      E98M3IMS.100                                      ↔: Select Screen
                                                        ↑↓: Select Item
 11th Gen Intel(R) Core(TM) i3-1115GRE @ 3.00GHz        Enter: Select
 Processor ID                   0x806C1                 +/-: Change Opt.
 Build Type                     64                      ESC: Exit
 Total Memory                   3968 MB (DDR4)          F1: General Help
                                                        F7: Previous Values
                                                        F9: Optimized Defaults
                                                        F10: Save & Reset Setup
                                                        F12: Screenshot capture
                                                        <K>: Scroll help area upwards
                                                        <M>: Scroll help area downwards
```

HDD Information

• **RAID (VMD) Disabled:** Display HDD information as plugging in status.

• **RAID (VMD) Enabled:** Display "Not Present" only.

▶ **System Date**

This setting allows you to set the system date.

Format: <Day> <Month> <Date> <Year>.

▶ **System Time**

This setting allows you to set the system time.

Format: <Hour> <Minute> <Second>.

▶ **SATA Mode Selection**

This setting specifies the SATA controller mode.

[AHCI]   AHCI (Advanced Host Controller Interface), is a technical standard for an interface that allows the software to communicate with Serial ATA (SATA) devices. It offers advanced SATA features such as Native Command Queuing (NCQ) and hot-plugging.
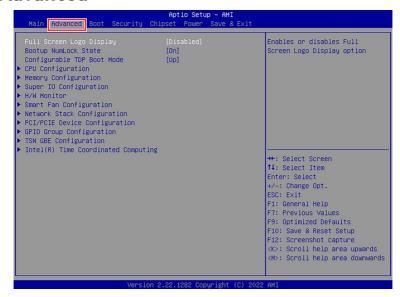
[RAID]   RAID (Redundant Array of Independent Disks) is a virtual disk storage technology that combines multiple physical disks into one unit for data redundancy, performance improvement, or both.

Advanced

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

    Full Screen Logo Display              [Disabled]        Enables or disables Full
    Bootup NumLock State                  [On]              Screen Logo Display option
    Configurable TDP Boot Mode            [Up]
  ▶ CPU Configuration
  ▶ Memory Configuration
  ▶ Super IO Configuration
  ▶ H/W Monitor
  ▶ Smart Fan Configuration
  ▶ Network Stack Configuration
  ▶ PCI/PCIE Device Configuration
  ▶ GPIO Group Configuration
  ▶ TSN GBE Configuration
  ▶ Intel(R) Time Coordinated Computing
                                                            ↔: Select Screen
                                                            ↑↓: Select Item
                                                            Enter: Select
                                                            +/-: Change Opt.
                                                            ESC: Exit
                                                            F1: General Help
                                                            F7: Previous Values
                                                            F9: Optimized Defaults
                                                            F10: Save & Reset Setup
                                                            F12: Screenshot capture
                                                            <K>: Scroll help area upwards
                                                            <M>: Scroll help area downwards

                     Version 2.22.1282 Copyright (C) 2022 AMI
```

▶ **Full Screen Logo Display**

This BIOS feature determines if the BIOS should hide the normal POST messages with the motherboard or system manufacturer's full-screen logo.

[Enabled]   BIOS will display the full-screen logo during the boot-up sequence, hiding normal POST messages.

[Disabled]   BIOS will display the normal POST messages, instead of the full-screen logo.

Please note that enabling this BIOS feature often adds 2-3 seconds of delay to the booting sequence. This delay ensures that the logo is displayed for a sufficient amount of time. Therefore, it is recommended that you disable this BIOS feature for a faster boot-up time.

▶ **Bootup NumLock State**

This setting is to set the Num Lock status when the system is powered on.

[On]   Turn on the Num Lock key when the system is powered on.

[Off]   Allow users to use the arrow keys on the numeric keypad.

▶ **Configurable TDP Boot Mode**

This feature allows you sets the TDP (Thermal Design Power) Boot mode to either Nominal, Down or Up.

TDP Power Spec			
Processor Family	Nominal	Down	Up
Intel® Core™ Processors	28W	12W	15W
Intel® Celeron® Processors	15W	N/A	N/A

▶ **CPU Configuration**

```
        Advanced

  CPU Configuration                              When enabled, a VMM can
                                                 utilize the additional
  11th Gen Intel(R) Core(TM)                     hardware capabilities provided
  i3-1115GRE @ 3.00GHz                           by Vanderpool Technology.
  Processor ID              0x806C1
  Processor Speed           2200 MHz
  L2 Cache                  1280 KB x 2
  L3 Cache                  6 MB

  Intel (VMX) Virtualization  [Enabled]
  Technology
  Active Processor Cores      [All]
  Hyper-Threading             [Enabled]
  Intel(R) SpeedStep(tm)      [Disabled]         →←: Select Screen
  C states                    [Enabled]          ↑↓: Select Item
                                                 Enter: Select
                                                 +/-: Change Opt.
                                                 ESC: Exit
                                                 F1: General Help
                                                 F7: Previous Values
                                                 F9: Optimized Defaults
                                                 F10: Save & Reset Setup
                                                 F12: Screenshot capture
                                                 <K>: Scroll help area upwards
                                                 <M>: Scroll help area downwards
```

▸ **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.

▸ **Active Processor Cores**

This setting specifies the number of active processor cores.

▸ **Hyper-Threading**

The processor uses Hyper-Threading technology to increase transaction rates and reduces end-user response times. The technology treats the two cores inside the processor as two logical processors that can execute instructions simultaneously. In this way, the system performance is highly improved. If you disable the function, the processor will use only one core to execute the instructions. **Please disable this item if your operating system doesn't support HT Function**, or unreliability and instability may occur.

▸ **Intel(R) SpeedStep(TM)**

EIST (Enhanced Intel SpeedStep Technology) allows the system to dynamically adjust processor voltage and core frequency, which can result in decreased average power consumption and decreased average heat production. When disabled, the processor will return the actual maximum CPUID (CPU Identification) input value of the processor when queried.

▶ **Turbo Mode**

Enables or disables the Turbo Mode. This feature only display when **Intel(R) SpeedStep(TM)** is enabled.

[Enabled]   Enables this function to boost CPU performance automatically over specification when system request the highest performance state.

[Disabled]   Disables this function.

▶ **C States**

This setting controls the C-States (CPU Power states).

[Enabled]   Detects the idle state of system and reduce CPU power consumption accordingly.

[Disabled]   Disable this function.

▶ Memory Configuration

```
Memory Configuration                                    Enable/Disable In-Band ECC.
                                                        Either the IBECC or the TME
In-Band ECC Support                 [Enabled]           can be enabled.
In-Band ECC Error Injection         [Disabled]
In-Band ECC Operation Mode          [2]
```

▸ **In-Band ECC Support**

Enables or disables In-Band ECC(Error-Correcting Code) Support.

[Enabled]   When enabled this function, a portion(1/32) of memory space will
                be reserved to store ECC data.

[Disabled]   Disables this function.
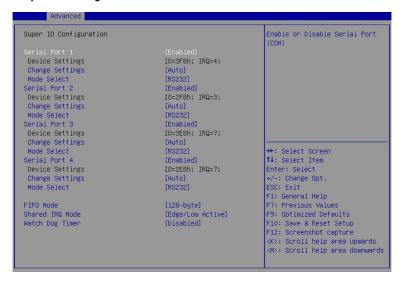
» **In-Band ECC Error Injection**

Enables or disables In-Band ECC Error Injection. This feature only display when
In-Band ECC Support is enabled.

» **In-Band ECC Error Operation Mode**

Select an operation mode from 0-2. This feature only display when **In-Band ECC
Support** is enabled.

▶ Super IO Configuration

```
        Advanced

    Super IO Configuration                              Enable or Disable Serial Port
                                                        (COM)
    Serial Port 1                [Enabled]
     Device Settings             IO=3F8h; IRQ=4;
     Change Settings             [Auto]
     Mode Select                 [RS232]
    Serial Port 2                [Enabled]
     Device Settings             IO=2F8h; IRQ=3;
     Change Settings             [Auto]
     Mode Select                 [RS232]
    Serial Port 3                [Enabled]
     Device Settings             IO=3E8h; IRQ=7;
     Change Settings             [Auto]
     Mode Select                 [RS232]             →←: Select Screen
    Serial Port 4                [Enabled]           ↑↓: Select Item
     Device Settings             IO=2E8h; IRQ=7;     Enter: Select
     Change Settings             [Auto]              +/-: Change Opt.
     Mode Select                 [RS232]             ESC: Exit
                                                     F1: General Help
    FIFO Mode                    [128-byte]          F7: Previous Values
    Shared IRQ Mode              [Edge/Low Active]   F9: Optimized Defaults
    Watch Dog Timer              [Disabled]          F10: Save & Reset Setup
                                                     F12: Screenshot capture
                                                     <K>: Scroll help area upwards
                                                     <M>: Scroll help area downwards
```

▶ **Serial Port 1/ 2/ 3/ 4**

This setting enables/disables the specified serial port.

» **Change Settings**

This setting is used to change the address & IRQ settings of the specified serial port.

» **Mode Select**

Select an operation mode for Serial Port 1/ 2/ 3/ 4.

▶ **FIFO Mode**

This setting controls the FIFO data transfer mode.

▶ **Shared IRQ Mode**
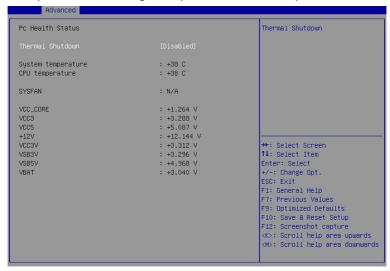
This setting provides the system with the ability to share interrupts among its serial ports.

▶ **Watch Dog Timer**

You can enable the system watchdog timer, a hardware timer that generates a reset when the software that it monitors does not respond as expected each time the watchdog polls it.

▶ H/W Monitor (PC Health Status)

These items display the current status of all monitored hardware devices/ components such as voltages, temperatures and all fans' speeds.

```
  Advanced

  Pc Health Status                                      Thermal Shutdown

  Thermal Shutdown               [Disabled]

  System temperature             : +38 C
  CPU temperature                : +38 C

  SYSFAN                         : N/A

  VCC_CORE                       : +1.264 V
  VCC3                           : +3.288 V
  VCC5                           : +5.087 V
  +12V                           : +12.144 V
  VCC3V                          : +3.312 V            ↔: Select Screen
  VSB3V                          : +3.296 V            ↑↓: Select Item
  VSB5V                          : +4.968 V            Enter: Select
  VBAT                           : +3.040 V            +/-: Change Opt.
                                                       ESC: Exit
                                                       F1: General Help
                                                       F7: Previous Values
                                                       F9: Optimized Defaults
                                                       F10: Save & Reset Setup
                                                       F12: Screenshot capture
                                                       <K>: Scroll help area upwards
                                                       <M>: Scroll help area downwards
```

▸ **Thermal Shutdown**

This setting enables/disables the Thermal Shutdown function. It will automatically shuts down when the internal temperature reaches the critical level.

▶ Smart Fan Configuration
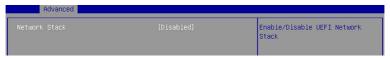
Advanced		
Configuration Smart FAN		Disabled/Enabled Smart FAN Function
SYSFAN	[Disabled]	

▸ SYSFAN

This setting enables/ disables the Smart Fan function. Smart Fan is an excellent feature which will adjust the System fan speed automatically depending on the current system temperature, avoiding the overheating to damage your system.

▶ Network Stack Configuration
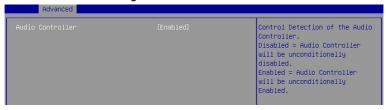
This menu provides Network Stack settings for users to enable network boot (PXE) from BIOS.

Advanced		
Network Stack	[Disabled]	Enable/Disable UEFI Network Stack

▸ Network Stack

This menu provides Network Stack settings for users to enable network boot (PXE) from BIOS. The following items will display when **Network Stak** is enabled.

▶ PCI/ PCIE Device Configuration

Advanced		
Audio Controller	[Enabled]	Control Detection of the Audio Controller. Disabled = Audio Controller will be unconditionally disabled. Enabled = Audio Controller will be unconditionally Enabled.
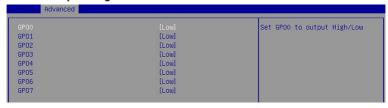
▸ Audio Controller

This setting enables/disables the onboard audio controller.

▶ GPIO Group Configuration

GPO0	[Low]	Set GPO0 to output High/Low
GPO1	[Low]	
GPO2	[Low]	
GPO3	[Low]	
GPO4	[Low]	
GPO5	[Low]	
GPO6	[Low]	
GPO7	[Low]	

▸ **GPO0 ~ GPO7**

These settings control the operation mode of the specified GPIO.

Boot

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

    Boot Option Priorities                              Sets the system boot order
    Boot Option #1                [UEFI:
                                  KingstonDataTraveler
                                  3.0, Partition 1
                                  (KingstonDataTraveler
                                  3.0)]
    Boot Option #2                [UEFI: Built-in EFI
                                  Shell]
```
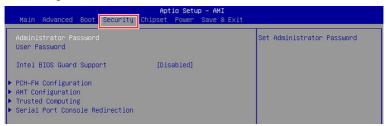
▶ **Boot Option Priorities**

   This setting allows users to set the sequence of boot devices where BIOS
   attempts to load the disk operating system.

Security

▶ **Administrator Password**

Administrator Password controls access to the BIOS Setup utility.
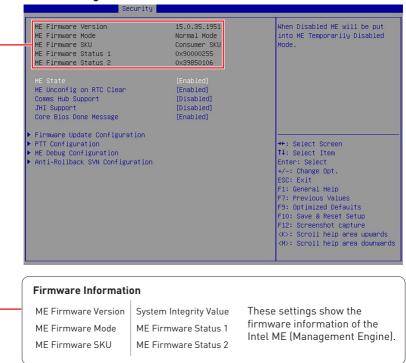
▶ **User Password**

User Password controls access to the system at boot and to the BIOS Setup utility.

▶ **Intel BIOS Guard Support**

Intel BIOS Guard Support ensures that updates to system BIOS flash are secure.

▶ **PCH-FW Configuration**

```
                        Security
ME Firmware Version          15.0.35.1951        When Disabled ME will be put
ME Firmware Mode             Normal Mode         into ME Temporarily Disabled
ME Firmware SKU              Consumer SKU        Mode.
ME Firmware Status 1         0x90000255
ME Firmware Status 2         0x39850106

ME State                     [Enabled]
ME Unconfig on RTC Clear     [Enabled]
Comms Hub Support            [Disabled]
JHI Support                  [Disabled]
Core Bios Done Message       [Enabled]

▶ Firmware Update Configuration
▶ PTT Configuration                              →←: Select Screen
▶ ME Debug Configuration                         ↑↓: Select Item
▶ Anti-Rollback SVN Configuration                Enter: Select
                                                 +/-: Change Opt.
                                                 ESC: Exit
                                                 F1: General Help
                                                 F7: Previous Values
                                                 F9: Optimized Defaults
                                                 F10: Save & Reset Setup
                                                 F12: Screenshot capture
                                                 <K>: Scroll help area upwards
                                                 <M>: Scroll help area downwards
```

Firmware Information

ME Firmware Version	System Integrity Value	These settings show the firmware information of the Intel ME (Management Engine).
ME Firmware Mode	ME Firmware Status 1	
ME Firmware SKU	ME Firmware Status 2	

▶ **ME State**

This setting specifies the Intel Management Engine state.

▶ **ME Unconfig on RTC Clear**

This setting enables/disables ME firmware unconfigure on RTC clear.

▶ **Comms Hub Support**

This setting enables/disables Communications Hub Support.

▶ **JHI Support**

This setting enables/disables support for Intel Dynamic Application Loader Host Interface (JHI).

▶ **Core BIOS Done Message**

This setting enables/disables Core BIOS Done Message sent to ME.

▶ **Firmware Update Configuration**

```
                           Security
 Me FW Image Re-Flash            [Disabled]        Enable/Disable Me FW Image
 FW Update                       [Enabled]         Re-Flash function.
```

» **ME FW Image Re-Flash**

This setting enables/ disables the ME FW (Firmware) image re-flash.

» **FW Update**

This setting enables/ disables the FW (Firmware) update.

▶ **PTT Configuration**

Intel Platform Trust Technology (PTT) is a platform functionality for credential storage and key management used by Microsoft Windows.

```
                           Security
 PTT Capability / State          1 / 0             Selects TPM device: PTT or
                                                   dTPM. PTT - Enables PTT in
 TPM Device Selection            [dTPM]            SkuMgr dTPM 1.2 - Disables PTT
 TPM 1.2 Deactivate              [Disabled]        in SkuMgr Warning !  PTT/dTPM
                                                   will be disabled and all data
                                                   saved on it will be lost.
```

» **TPM Device Selection**
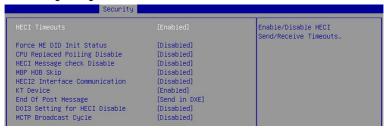
Select TPM (Trusted Platform Module) devices from PTT or dTPM (Discrete TPM).

[PTT]   Enables PTT in SkuMgr.

[dTPM1.2]   Disables PTT in SkuMgr. **Warning! PTT/ Discrete TPM will be disabled and all data saved on it will be lost.**

▶ **ME Debug Configuration**

```
                           Security
 HECI Timeouts                   [Enabled]         Enable/Disable HECI
                                                   Send/Receive Timeouts.
 Force ME DID Init Status        [Disabled]
 CPU Replaced Polling Disable    [Disabled]
 HECI Message check Disable      [Disabled]
 MBP HOB Skip                    [Disabled]
 HECI2 Interface Communication   [Disabled]
 KT Device                       [Enabled]
 End Of Post Message             [Send in DXE]
 DOI3 Setting for HECI Disable   [Disabled]
 MCTP Broadcast Cycle            [Disabled]
```

» **HECI Timeouts**

This setting enables/ disables the HECI (Host Embedded Controller Interface) send/ receive timeouts.

» **Force ME DID Init Status**

Forces the DID initialization status value.

» **CPU Replaced Polling Disable**

Setting this option disables the CPU replacement polling loop.

» **HECI Message Check Disable**

This setting disables message check for BIOS boot path when sending messages.

» **MBP HOB Skip**

Setting this option will skip MBP HOB.

» **HECI2 Interface Communication**

This setting Adds/ Removes HECI2 device from PCI space.

» **KT Device**

This setting enables/ disables KT Device.

» **End of Post Message**

This setting enables/ disables End of Post Message sent to ME.

» **DOI3 Setting for HECI Disable**

Setting this option disables setting DOI3 bit for all HECI devices.

» **MCTP Broadcast Cycle**

This setting enables/ disables Management Component Transport Protocol (MCTP) Broadcast Cycle.

▶ **Anti-Rollback SVN Configuration**


```
            Security

Minimal Allowed Anti-Rollback SVN    0          When enabled,
Executing Anti-Rollback SVN          4          hardware-enforced
Automatic HW-Enforced           [Disabled]      Anti-Rollback mechanism is
Anti-Rollback SVN                               automatically activated: once
Set HW-Enforced Anti-Rollback for  [Disabled]   ME FW was successfully run on
Current SVN                                     a platform, FW with lower
                                                ARB-SVN will be blocked from
                                                execution
```

» **Automatic HW-Enforced Anti-Rollback SVN**

Setting this option enables will automatically activate the hardware-enforced Anti-Rollback security version (HW ERB SVN). Once ME FW was successfully run on a platform, FW with lower ARB-VN will be blocked from execution.

» **Set HW-Enforced Anti-Rollback for Current SVN**

Enable HW ERB mechanism for current ARB SVN value. FW with lower ARB-SVN will be blocked from execution. The value will be restored to disable after the command is sent.

▶ AMT Configuration
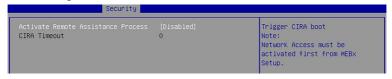
Intel Active Management Technology (AMT) is hardware-based technology for remotely managing and securing PCs out-of-band.

```
┌─────────────────────Security─────────────────────────────────────────┐
│                                                                       │
│  USB Provisioning of AMT        [Disabled]    Enable/Disable of AMT USB│
│  ▶ CIRA Configuration                         Provisioning.           │
│  ▶ ASF Configuration                                                  │
│  ▶ Secure Erase Configuration                                         │
│  ▶ OEM Flags Settings                                                 │
│  ▶ MEBx Resolution Settings                                           │
│                                                                       │
│                                               ⇄: Select Screen        │
│                                               ↑↓: Select Item         │
│                                               Enter: Select           │
│                                               +/-: Change Opt.        │
│                                               ESC: Exit               │
│                                               F1: General Help        │
│                                               F7: Previous Values     │
│                                               F9: Optimized Defaults  │
│                                               F10: Save & Reset Setup │
│                                               F12: Screenshot capture │
│                                               <K>: Scroll help area upwards│
│                                               <M>: Scroll help area downwards│
│                                                                       │
└───────────────────────────────────────────────────────────────────────┘
```

▸ **USB Provisioning of AMT**

   Enables or disable USB Provisioning of AMT.

▸ **CIRA Configuration**

```
┌─────────────────────Security─────────────────────────────────────────┐
│                                                                       │
│  Activate Remote Assistance Process   [Disabled]   Trigger CIRA boot  │
│  CIRA Timeout                         0            Note:               │
│                                                   Network Access must be│
│                                                   activated first from MEBx│
│                                                   Setup.               │
│                                                                       │
└───────────────────────────────────────────────────────────────────────┘
```
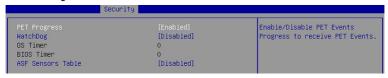
   » **Activate Remote Assistance Process**

      Setting this option enables will trigger CIRA boot.

   » **CIRA Timeout**

      This item displays CIRA Timeout.

▶ ASF Configuration

Security		
PET Progress	[Enabled]	Enable/Disable PET Events
WatchDog	[Disabled]	Progress to receive PET Events.
OS Timer	0	
BIOS Timer	0	
ASF Sensors Table	[Disabled]	

» **PET Progress**

Setting this option enables/ disables to receive PET Events.

» **WatchDog**

This setting enables/ disables the watchdog timer.

» **OS Timer**

This item displays OS Timer.

» **BIOS Timer**

This item displays BIOS Timer.

» **ASF Sensor Table**

This setting enables/ disables Alert Standard Format(ASF) Sensor Table.

▶ Secure Erase Configuration

Security		
Secure Erase mode	[Simulated]	Change Secure Erase module behavior:
Force Secure Erase	[Disabled]	Simulated: Performs SE flow without erasing SSD
		Real: Erase SSD.

» **Secure Erase Mode**

This setting change Secure Erase module behavior.

[Simulated]   Performs SE flow without erasing SSD.

[Real]   Erase SSD.

» **Force Secure Erase**

Setting this option enables/ disables to force Secure Erase on next boot.

▶ **OEM Flag Setting**

```
                      Security

MEBx hotkey Pressed            [Disabled]        OEMFLag Bit 1:
MEBx Selection Screen          [Disabled]        Enable automatic MEBx hotkey
Hide Unconfigure ME Confirmation [Disabled]      press.
Prompt
MEBx OEM Debug Menu Enable     [Disabled]
Unconfigure ME                 [Disabled]
```

» **MEBx hotkey Pressed**

This setting enables/ disables the management Engine BIOS Extension(MEBx) hotkey Pressed.

» **MEBx Selection Screen**

This setting enables/ disables the MEBx Selection Screen.

» **Hide Unconfigure ME Confirmation Prompt**

This setting enables/ disables the Hide Unconfigure ME Confirmation Prompt.

» **MEBx OEM Debug Menu Enable**

This setting enables/ disables the MEBx OEM Debug Menu.

» **Unconfigure ME**

This setting enables/ disables the Unconfigure ME.

▶ **MEBx Resolution Setting**

```
                      Security

Non-UI Mode Resolution         [Auto]            Resolution for non-UI text
UI Mode Resolution             [Auto]            mode.
Graphics Mode Resolution       [Auto]
```

» **Non-UI Mode Resolution**

Resolution for non-UI text mode.

» **UI Mode Resolution**

Resolution for UI text mode.

» **Graphic Mode Resolution**

Resolution for graphics mode.

▶ Trusted Computing

```
                          Security
  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
  Active PCR banks           SHA256             available.
  Available PCR banks        SHA256

  SHA256 PCR Bank            [Enabled]

  Pending operation          [None]
  Platform Hierarchy         [Enabled]
  Storage Hierarchy          [Enabled]
  Endorsement Hierarchy      [Enabled]          →←: Select Screen
  Physical Presence Spec Version [1.3]          ↑↓: Select Item
  TPM 2.0 InterfaceType      [TIS]              Enter: Select
  PH Randomization           [Enabled]          +/-: Change Opt.
  Device Select              [TPM 2.0]          ESC: Exit
                                                F1: General Help
                                                F7: Previous Values
                                                F9: Optimized Defaults
                                                F10: Save & Reset Setup
                                                F12: Screenshot capture
                                                <K>: Scroll help area upwards
                                                <M>: Scroll help area downwards
```

▸ **Security Device Support**

This setting enables/disables BIOS support for security device. When set to [Disable], the OS will not show security device. TCG EFI protocol and INT1A interface will not be available.

▸ **SHA256 PCR Bank**

These settings enable/disable the SHA-1 PCR Bank and SHA256 PCR Bank.

▸ **Pending Operation**

When **Security Device Support** is set to [Enable], **Pending Operation** will appear. Set this item to [TPM Clear] to clear all data secured by TPM or [None] to discard the selection. It is advised that users should routinely back up their TPM secured data.

▸ **Platform Hierarchy, Storage Hierarchy, Endorsement Hierarchy**

These settings enable/disable the Platform Hierarchy, Storage Hierarchy and Endorsement Hierarchy.

▸ **Physical Presence Spec Version**

This settings show the Physical Presence Spec Version.

▸ **TPM 2.0 Interface Type**

This setting shows the TPM 2.0 Interface Type.

▸ **PH Randomization**

This setting enables/disables PH Randomization.

▸ **Device Select**

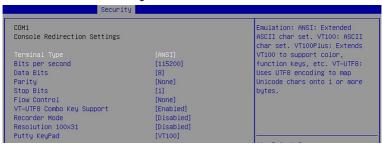Select your TPM device throgh this setting.

▶ Serial Port Console Redirection

```
                        Aptio Setup - AMI
              Security

                                              Console Redirection Enable or
  COM1                                        Disable.
  Console Redirection              [Disabled]
▶ Console Redirection Settings

  Serial Port for Out-of-Band Management/
  Windows Emergency Management Services (EMS)
  Console Redirection EMS          [Disabled]
▶ Console Redirection Settings

                                              →←: Select Screen
                                              ↑↓: Select Item
                                              Enter: Select
                                              +/-: Change Opt.
                                              ESC: Exit
                                              F1: General Help
                                              F7: Previous Values
                                              F9: Optimized Defaults
                                              F10: Save & Reset Setup
                                              F12: Screenshot capture
                                              <K>: Scroll help area upwards
                                              <M>: Scroll help area downwards
```

▷ Console Redirection

Console Redirection operates in host systems that do not have a monitor and keyboard attached. This setting enables/disables the operation of console redirection. When set to [Enabled], BIOS redirects and sends all contents that should be displayed on the screen to the serial COM port for display on the terminal screen. Besides, all data received from the serial port is interpreted as keystrokes from a local keyboard.

▶ **Console Redirection Settings (COM1)**

```
                          Security

COM1
Console Redirection Settings                         Emulation: ANSI: Extended
                                                     ASCII char set. VT100: ASCII
                                                     char set. VT100Plus: Extends
Terminal Type                    [ANSI]              VT100 to support color,
Bits per second                  [115200]            function keys, etc. VT-UTF8:
Data Bits                        [8]                 Uses UTF8 encoding to map
Parity                           [None]              Unicode chars onto 1 or more
Stop Bits                        [1]                 bytes.
Flow Control                     [None]
VT-UTF8 Combo Key Support        [Enabled]
Recorder Mode                    [Disabled]
Resolution 100x31                [Disabled]
Putty KeyPad                     [VT100]
```

» **Terminal Type**

To operate the system's console redirection, you need a terminal supporting ANSI terminal protocol and a RS-232 null modem cable connected between the host system and terminal(s). You can select emulation for the terminal from this setting.

[ANSI]   Extended ASCII character set.

[VT100]   ASCII character set.

[VT100Plus]   Extends VT100 to support color, function keys, etc.

[VT-UTF8]   Uses UTF8 encoding to map Unicode characters onto one or more bytes.

» **Bits per second, Data Bits, Parity, Stop Bits**

These setting specifies the transfer rate (bits per second, data bits, parity, stop bits) of Console Redirection.

» **Flow Control**

Flow control is the process of managing the rate of data transmission between two nodes. It's the process of adjusting the flow of data from one device to another to ensure that the receiving device can handle all of the incoming data. This is particularly important where the sending device is capable of sending data much faster than the receiving device can receive it.

» **VT-UTF8 Combo Key Support**

This setting enables/disables the VT-UTF8 combination key support for ANSI/VT100 terminals.

» **Recorder Mode, Resolution 100x31**

These settings enable/disable the recorder mode and the resolution 100x31.

» **Putty Keypad**

PuTTY is a terminal emulator for Windows. This setting controls the numeric keypad for use in PuTTY.

► **Console Redirection Settings (Out-of-Band Management)**

```
                          Security

Out-of-Band Mgmt Port          COM1              VT-UTF8 is the preferred
Terminal Type EMS              [VT-UTF8]          terminal type for out-of-band
Bits per second EMS            [115200]           management. The next best
Flow Control EMS               [None]             choice is VT100+ and then
Data Bits EMS                  8                  VT100. See above, in Console
Parity EMS                     None               Redirection Settings page, for
Stop Bits EMS                  1                  more Help with Terminal
                                                  Type/Emulation.
```

» **Out-of-Band Mgmt Port**

This setting specifies the Out-of-Band Management Port.

» **Terminal Type EMS (Windows Emergency Management Service)**

You can select the type of terminal device for console redirection from this setting. **[VT-UTF8]** is the preferred terminal type for the out-of-band management. The next best choice is **[VT100+]** and then **[VT100]**. See above in **Console Redirection Setting** page for more help with Terminal Type/ Emulation.
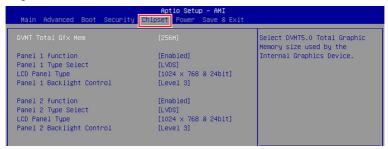
Flow Control EMS (Windows Emergency Management Service)

Flow control is the process of managing the rate of data transmission between two nodes. It's the process of adjusting the flow of data from one device to another to ensure that the receiving device can handle all of the incoming data. This is particularly important where the sending device is capable of sending data much faster than the receiving device can receive it.

» **Bits per second EMS, Data Bits EMS, Parity EMS, Stop Bits EMS**

This setting specifies the transfer rate of Console Redirection.

Chipset

```
     Main  Advanced  Boot  Security  Chipset  Power  Save & Exit

  DVMT Total Gfx Mem                [256M]                    Select DVMT5.0 Total Graphic
                                                              Memory size used by the
  Panel 1 function                  [Enabled]                 Internal Graphics Device.
  Panel 1 Type Select               [LVDS]
  LCD Panel Type                    [1024 x 768 & 24bit]
  Panel 1 Backlight Control         [Level 3]

  Panel 2 function                  [Enabled]
  Panel 2 Type Select               [LVDS]
  LCD Panel Type                    [1024 x 768 & 24bit]
  Panel 2 Backlight Control         [Level 3]
```

▶ **DVMT Total Gfx Mem**

This setting specifies the memory size for DVMT.

▶ **Panel 1/ 2 Function**

This setting enables/disables Panel 1 Function.

▸ **Type Select**

Set your video signal interface as LVDs or eDP. This item will display when **Panel 1 Function** is enabled.

» **LCD Panel Type**

This setting specifies the LCD Panel's resolution and distribution formats. The item will display when **Panel 1 Type is set to LVDs**.

▶ **Panel 1/ 2 Backlight Control**

This setting controls the intensity of the LED's backlight output. When lighting conditions are brighter, set it high for a clearer image and low when it is darker.

LED's backlight output	
[Level 1]	20%
[Level 2]	40%
[Level 3]	60%
[Level 4]	80%
[Level 5]	100%

Power

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

   Restore AC power Loss              [Last State]        Select AC power state when
   Deep Sleep Mode                    [S5]                power is re-applied after a
                                                          power failure.
   Advanced Resume Events Control
   OnChip USB                         [Enabled]
   LAN Wake                           [Enabled]
   PCIE PME                           [Disabled]
   RTC                                [Disabled]
```

▶ **Restore AC Power Loss**

This setting specifies whether your system will reboot after a power failure or interrupt occurs. Available settings are:

[Power Off]   Leaves the computer in the power off state.

[Power On]   Leaves the computer in the power on state.

[Last State]   Restores the system to the previous status before power failure or interrupt occurred.

▶ **Deep Sleep Mode**

The setting enables/disables the Deep S5 power saving mode. S5 is almost the same as G3 Mechanical Off, except that the PSU still supplies power, at a minimum, to the power button to allow return to S0. A full reboot is required. No previous content is retained. Other components may remain powered so the computer can "wake" on input from the keyboard, clock, modem, LAN, or USB device.
** Advanced Resume Events Control **

▶ **OnChip USB**

The item allows the activity of the OnChip USB device to wake up the system from S4/ S5 sleep state.

▶ **PCIE PME**

This field specifies whether the system will be awakened from power saving modes when activity or input signal of onboard PCIE PME is detected.

▶ **RTC**

When [Enabled], your can set the date and time at which the RTC (real-time clock) alarm awakens the system from suspend mode.

Save & Exit

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

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

      Load Optimized Defaults
      Save as User Defaults
      Restore User Defaults

      Launch EFI Shell from filesystem device
```

▶ **Save Changes and Reset**

Save changes to CMOS and reset the system.

▶ **Discard Changes and Exit**

Abandon all changes and exit the Setup Utility.

▶ **Discard Changes**

Abandon all changes.

▶ **Load Optimized Defaults**

Use this menu to load the default values set by the motherboard manufacturer specifically for optimal performance of the motherboard.

▶ **Save as User Defaults**

Save changes as the user's default profile.

▶ **Restore User Defaults**

Restore the user's default profile.

▶ **Launch EFI Shell from filesystem device**

This setting helps to launch the EFI Shell application from one of the available file system devices.

GPIO WDT BKL SMBus Programming

This chapter provides WDT (Watch Dog Timer), GPIO (General Purpose Input/ Output) LVDS Backlight and SMBus Access programming guide.

Abstract

In this section, code examples based on C programming language provided for customer interest. **Inportb, Outportb, Inportl** and **Outportl** are basic functions used for access IO ports and defined as following.

Inportb: Read a single 8-bit I/O port.

Outportb: Write a single byte to an 8-bit port.

Inportl: Reads a single 32-bit I/O port.

Outportl: Write a single long to a 32-bit port.

General Purpose IO

1. General Purposed IO – GPIO/DIO

The GPIO port configuration addresses are listed in the following table:

Name	IO Port	IO address	Name	IO Port	IO address
N_GPI0	0x22	Bit 4	N_GPO0	0x11	Bit 4
N_GPI1	0x22	Bit 5	N_GPO1	0x11	Bit 5
N_GPI2	0x22	Bit 6	N_GPO2	0x11	Bit 6
N_GPI3	0x22	Bit 7	N_GPO3	0x11	Bit 7
N_GPI4	0x42	Bit 0	N_GPO4	0x21	Bit 0
N_GPI5	0x42	Bit 1	N_GPO5	0x21	Bit 1
N_GPI6	0x42	Bit 2	N_GPO6	0x21	Bit 2
N_GPI7	0x42	Bit 3	N_GPO7	0x21	Bit 3

Note: GPIO should be accessed through controller device **0x6E** on SMBus. The associated access method in examples (**SMBus_ReadByte**, **SMBus_WriteByte**) are provided in part 4.

1.1 Set output value of GPO

1. Read the value from GPO port.
2. Set the value of GPO address.
3. Write the value back to GPO port.

Example: Set **N_GPO0** output "high"

```
val =SMBus_ReadByte (0x6E, 0x11);      // Read value from N_GPO0 port through SMBus.
val = val | (1<<4);                    // Set N_GPO0address (bit 4) to 1 (output "high").
SMBus_WriteByte (0x6E, 0x11, val);     // Write back to N_GPO0 port through SMBus.
```

Example: Set **N_GPO1** output "low"

```
val = SMBus_ReadByte (0x6E, 0x11);     // Read value from N_GPO1 port through SMBus..
val = val & (~(1<<5));                 // Set N_GPO1 address (bit 5) to 0 (output "low").
SMBus_WriteByte (0x6E, 0x11, val);     // Write back to N_GPO1 port through SMBus.
```

1.2 Read input value from GPI:

1. Read the value from GPI port.
2. Get the value of GPI address.

Example: Get **N_GPI2** input value.

```
val = SMBus_ReadByte (0x6E, 0x22); // Read value from N_GPI2 port through SMBus.
val = val & (1<<6);                     // Read N_GPI2 address (bit 6).
if (val)       printf ("Input of   N_GPI2   is High");
else           printf ("Input of   N_GPI2   is Low");
```

Example: Get **N_GPI3** input value.

```
val = SMBus_ReadByte (0x6E, 0x22);        // Read value from N_GPI3 port through SMBus.
val = val & (1<<7);                       // Read N_GPI3 address (bit 7).
if (val)       printf ("Input of   N_GPI3   is High");
else           printf ("Input of   N_GPI3   is Low");
```

Watchdog Timer

2. Watchdog Timer – WDT

The base address (WDT_BASE) of WDT configuration registers is 0xA10.

2.1 Set WDT Time Unit

```
val = Inportb (WDT_BASE + 0x05);          // Read current WDT setting
val = val | 0x08;                         // minute mode. val = val & 0xF7 if second mode
Outportb (WDT_BASE + 0x05, val);          // Write back WDT setting
```

2.2 Set WDT Time

```
Outportb (WDT_BASE + 0x06, Time);         // Write WDT time, value 1 to 255.
```

2.3 Enable WDT

```
val = Inportb (WDT_BASE + 0x0A);          // Read current WDT_PME setting
val = val | 0x01;                         // Enable WDT OUT: WDOUT_EN (bit 0) set to 1.
Outportb (WDT_BASE + 0x0A, val);          // Write back WDT setting.
val = Inportb (WDT_BASE + 0x05);          // Read current WDT setting
val = val | 0x20;                         // Enable WDT by set WD_EN (bit 5) to 1.
Outportb (WDT_BASE + 0x05, val);          // Write back WDT setting.
```

2.4 Disable WDT

```
val = Inportb (WDT_BASE + 0x05);          // Read current WDT setting
val = val & 0xDF;                         // Disable WDT by set WD_EN (bit 5) to 0.
Outportb (WDT_BASE + 0x05, val);          // Write back WDT setting.
```

2.5 Check WDT Reset Flag

If the system has been reset by WDT function, this flag will set to 1.

```
val = Inportb (WDT_BASE + 0x05);        // Read current WDT setting.
val = val & 0x40;                       // Check WDTMOUT_STS (bit 6).
if (val)     printf ("timeout event occurred");
else         printf ("timeout event not occurred");
```

2.6 Clear WDT Reset Flag

```
val = Inportb (WDT_BASE + 0x05);        // Read current WDT setting
val = val | 0x40;                       // Set 1 to WDTMOUT_STS (bit 6);
Outportb (WDT_BASE + 0x05, val);        // Write back WDT setting
```

LVDS/EDP Backlight Control - BKL

3. LVDS/EDP Backlight Control – BKL

The controller CH7513A support **LVDS/EDP** backlight level control from 0(0%) to 255(100%), the default backlight level is 100%. It must be controlled by SMBus access. There are two controllers on the board. One controller for **JLVDS1_EDP1** is SMBus device **0x42,** the other for **JLVD2_EDP2** is SMBus device **0x46.**

The details of SMBus access (SMBus_ReadByte, SMBus_WriteByte) are provided in this document.

3.1 Set the Level of LVDS/EDP Backlight

1. Write **0x0D** into address **0x00** on SMBus device.
2. Write desired backlight level from 0(0%) to 255(100%) into address **0x35** on SMBus device.

   Example 3: Set **LVDS backlight level** on SMBus device **0x42** to "100%"
   SMBus_WriteByte (0x42, 0x00, 0x0D)
   SMBus_WriteByte (0x42, 0x35, 0xFF)

3.2 Read the Level of LVDS/EDP Backlight

4. Write **0x0D** into address **0x00** on SMBus device.
5. Read current backlight level from address **0x35** on SMBus device.

   Example 4: Get **LVDS backlight level** on SMBus device **0x46**
   SMBus_WriteByte(0x46, 0x00, 0x0D);
   BKL_Value = SMBus_ReadByte(0x46, 0x35);

SMBus Access

4. SMBus Access

The base address of SMBus must know before access. The relevant bus and device information are as following.

```
#define IO_SC            0xCF8
#define IO_DA            0xCFC
#define PCIBASEADDRESS   0x80000000
#define PCI_BUS_NUM      0
#define PCI_DEV_NUM      31
#define PCI_FUN_NUM      4
```

4.1 Get SMBus Base Address

```
int SMBUS_BASE;
int DATA_ADDR = PCIBASEADDRESS + (PCI_BUS_NUM<<16) +
                                 (PCI_DEV_NUM<<11) +
                                 (PCI_FUN_NUM<<8);

Outportl (DATA_ADDR + 0x20, IO_SC);
SMBUS_BASE = Inportl (IO_DA) & 0xfffffff0;
```

4.2 SMBus_ReadByte (char DEVID, char offset)

Read the value of <u>OFFSET</u> from SMBus device <u>DEVID</u>.

```
Outportb (LOWORD (SMBUS_BASE), 0xFE);
Outportb (LOWORD (SMBUS_BASE) + 0x04, DEVID + 1); //out Base + 04, (DEVID + 1)
Outportb (LOWORD (SMBUS_BASE) + 0x03, OFFSET);   //out Base + 03, OFFSET
Outportb (LOWORD (SMBUS_BASE) + 0x02, 0x48);     //out Base + 02, 48H
mdelay (20);                                     //delay 20ms to let data ready
while ((Inportl (SMBUS_BASE) & 0x01) != 0);      //wait SMBus ready
SMB_DATA = Inportb (LOWORD (SMBUS_BASE) + 0x05); //input Base + 05
```

4.3 SMBus_WriteByte (char DEVID, char offset, char DATA)

Write <u>DATA</u> to <u>OFFSET</u> on SMBus device <u>DEVID</u>.

```
Outportb (LOWORD (SMBUS_BASE), 0xFE);
Outportb (LOWORD (SMBUS_BASE) + 0x04, DEVID);      //out Base + 04, (DEVID)
Outportb (LOWORD (SMBUS_BASE) + 0x03, OFFSET);     //out Base + 03, OFFSET
Outportb (LOWORD (SMBUS_BASE) + 0x05, DATA);       //out Base + 05, DATA
Outportb (LOWORD (SMBUS_BASE) + 0x02, 0x48);       //out Base + 02, 48H
mdelay (20);                                       //wait 20ms
```