

User Manual

ARK-7060

Embedded Box PC



Attention!

Please note:

This package contains a hard-copy user manual in Chinese for China CCC certification purposes. There is an English user manual included as a PDF file on the CD. Please disregard the Chinese hard copy user manual if the product is not to be sold and/or installed in China.

Copyright

The documentation and the software included with this product are copyrighted 2022 by Advantech Co., Ltd. All rights are reserved. Advantech Co., Ltd. reserves the right to make improvements in the products described in this manual at any time without notice. No part of this manual may be reproduced, copied, translated, or transmitted in any form or by any means without the prior written permission of Advantech Co., Ltd. The information provided in this manual is intended to be accurate and reliable. However, Advantech Co., Ltd. assumes no responsibility for its use, nor for any infringements of the rights of third parties that may result from its use.

Acknowledgments

Award is a trademark of Award Software International, Inc.

VIA is a trademark of VIA Technologies, Inc.

IBM, PC/AT, PS/2, and VGA are trademarks of International Business Machines Corporation.

Intel[®] and Pentium[®] are trademarks of Intel Corporation.

Microsoft Windows[®] is a registered trademark of Microsoft Corp.

RTL is a trademark of Realtek Semi-Conductor Co., Ltd.

ESS is a trademark of ESS Technology, Inc.

UMC is a trademark of United Microelectronics Corporation.

SMI is a trademark of Silicon Motion, Inc.

Creative is a trademark of Creative Technology LTD.

CHRONTEL is a trademark of Chrontel Inc.

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

For more information about this and other Advantech products, please visit our website at:

http://www.advantech.com/

http://www.advantech.com/ePlatform/

For technical support and service, please visit our support website at: http://support.advantech.com.tw/support/

> Part No. 2006706000 Printed in China

Edition 1 October 2022

Product Warranty (2 years)

Advantech warrants the original purchaser that each of its products will be free from defects in materials and workmanship for two years from the date of purchase.

This warranty does not apply to any products that have been repaired or altered by persons other than repair personnel authorized by Advantech, or products that have been subject to misuse, abuse, accident, or improper installation. Advantech assumes no liability under the terms of this warranty as a consequence of such events.

Because of Advantech's high quality-control standards and rigorous testing, most customers never need to use our repair service. If an Advantech product is defective, it will be repaired or replaced free of charge during the warranty period. For out-of-warranty repairs, customers will be billed according to the cost of replacement mate-rials, service time, and freight. Please consult your dealer for more details.

If you believe your product to be defective, follow the steps outlined below.

- 1. Collect all the information about the problem encountered. (For example, CPU speed, Advantech products used, other hardware and software used, etc.) Note anything abnormal and list any on-screen messages displayed when the problem occurs.
- 2. Call your dealer and describe the problem. Please have your manual, product, and any helpful information readily available.
- If your product is diagnosed as defective, obtain a return merchandise authorization (RMA) number from your dealer. This allows us to process your return more quickly.
- 4. Carefully pack the defective product, a completed Repair and Replacement Order Card, and a proof of purchase date (such as a photocopy of your sales receipt) into a shippable container. Products returned without a proof of purchase date are not eligible for warranty service.
- 5. Write the RMA number clearly on the outside of the package and ship the package prepaid to your dealer.

Declaration of Conformity

FCC Class B

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 following measures:

- 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/TV technician for assistance.

Technical Support and Assistance

- Visit the Advantech website at www.advantech.com/support to obtain the latest 1. product information.
- Contact your distributor, sales representative, or Advantech's customer service 2. center for technical support if you need additional assistance. Please have the following information ready before calling:
 - Product name and serial number
 - Description of your peripheral attachments
 - Description of your software (operating system, version, application software, etc.)
 - A complete description of the problem
 - The exact wording of any error messages

Warnings, Cautions, and Notes



Warning! Warnings indicate conditions that if not observed can cause personal injury!



Caution! Cautions are included to help prevent hardware damage and data losses. For example,

> "Batteries are at risk of exploding if incorrectly installed. Do not attempt to recharge, force open, or heat the battery. Replace the battery only with the same or equivalent type as recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions."



Notes provide additional optional information.

Packing List

Before system installation, check that the items listed below are included and in good condition. If any item does not accord with the list, contact your dealer immediately.

- 1 x ARK-7060 Unit
- 1 x Mounting Kit
- 1 x User Manual (Simplified Chinese)
- 1 x China RoHS

Ordering Information

Part No.	CPU	DDR4	GbE	10 GbE	VGA	2.5" SATA III HDD Bay	RS-232/ 422/485	USB 3.0	M.2 B Key	M.2 E Key	SIM	IPMI	Power Supply	Expansion
ARK- 7060- U0A1	Intel [®] Xeon [®] D-1746TER	Up to 128GB	2	2 (optional)	1	2 (Up to 4)	4	4	1	1	1	Yes	850W	1 x PCI 1 x PCIex4 1 x PCIx16
ARK- 7060- U4A1	Intel [®] Xeon [®] D-1715TER	Up to 128GB	2	2 (optional)	1	2 (Up to 4)	4	4	1	1	1	Yes	850W	1 x PCI 1 x PCIex4 1 x PCIx16

Note!

e! Memory/Storage and operating system bundled by request.

ARK-7060 Default SKU Option Items

Optional Item for Default SKU

Part Number	Description
1702002600	Power cable 3-pin 183 cm (64.1 in), USA type
1702002605	Power cable 3-pin 183 cm (64.1 in), EU type
1702031801	Power cable 3-pin 183 cm (64.1 in), UK type
170000237	Power cable 3-pin 183 cm (64.1 in), PSE type
AMO-1029	TPM 2.0 module
AMO-1031	2 x 10GbE LAN kit
AMK-A0042	2 x internal HDD bay kit
AMK-A0043	NVIDIA A2/T4 GPU card fan kit

Safety Instructions

- 1. Read these safety instructions carefully.
- 2. Retain this user manual for future reference.
- 3. Disconnect the equipment from all power outlets before cleaning. Use only a damp cloth for cleaning. Do not use liquid or spray detergents.
- 4. For pluggable equipment, the power outlet socket must be located near the equipment and easily accessible.
- 5. Protect the equipment from humidity.
- 6. Place the equipment on a reliable surface during installation. Dropping or letting the equipment fall may cause damage.
- 7. The openings on the enclosure are for air convection. Protect the equipment from overheating. Do not cover the openings.
- 8. Ensure that the voltage of the power source is correct before connecting the equipment to a power outlet.
- 9. Position the power cord away from high-traffic areas. Do not place anything over the power cord.
- 10. All cautions and warnings on the equipment should be noted.
- 11. If the equipment is not used for a long time, disconnect it from the power source to avoid damage from transient overvoltage.
- 12. Never pour liquid into an opening. This may cause fire or electrical shock.
- 13. Never open the equipment. For safety reasons, the equipment should be opened only by qualified service personnel.
- 14. If any of the following occurs, have the equipment checked by service personnel:
 - The power cord or plug is damaged.
 - Liquid has penetrated the equipment.
 - The equipment has been exposed to moisture.
 - The equipment is malfunctioning, or does not operate according to the user manual.
 - The equipment has been dropped and damaged.
 - The equipment shows obvious signs of breakage.
- 15. Do not leave the equipment in an environment with a storage temperature of below -40 °C (-40 °F) or above 85 °C (185 °F) as this may damage the components. The equipment should be kept in a controlled environment.
- 16. Any unverified component may cause unexpected damage. To ensure correct installation, always use the components (e.g., screws) provided in the accessory box.
- 17. CAUTION: Batteries are at risk of exploding if incorrectly replaced. Replace only with the same or equivalent type as recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions.
- 18. Always disconnect the power cord from the chassis before manually handling the hardware. Do not implement connections or configuration changes while the device is powered on. Sudden power surges may damage sensitive electronic components.
- 19. In accordance with IEC 704-1:1982 specifications, the sound pressure level at the operator's position does not exceed 70 dB (A).
- 20. The equipment should only be installed in a restricted access areas.
- 21. Use a power cord connected to a socket-outlet with a grounded connection.
- 22. This product is intended to be supplied by a UL Listed power supply suitable for use at minimum Tma 50 °C (122 °F) whose output meets PS2 (or LPS), ES1(or

SELV) and output is rated: 9-36Vdc, 16.65-4.16A. Please contact Advantech for further information.

DISCLAIMER: These instructions are provided according to IEC 704-1 standards. Advantech disclaims all responsibility for the accuracy of any statements contained herein.

Consignes de Sécurité

- 1. Veuillez lire attentivement ces instructions de sécurité.
- 2. Veuillez conserver ce manuel de l'utilisateur pour référence ultérieure.
- 3. Veuillez débrancher cet équipement de la prise secteur avant le nettoyage. Utilisez un chiffon humide. Ne pas utiliser de détergent liquide ou pulvérisé pour le nettoyage. Utilisez une feuille ou un chiffon humide pour le nettoyage.
- 4. Pour les équipements enfichables, la prise de courant doit être à proximité de l'équipement et doit être facilement accessible.
- 5. S'il vous plaît garder cet équipement de l'humidité.
- 6. Posez cet équipement sur une surface fiable lors de l'installation. Une chute ou une chute pourrait causer des blessures.
- 7. Les ouvertures sur le boîtier sont destinées à la convection d'air, protégeant. ainsi l'équipement de la surchauffe. NE COUVREZ PAS LES OUVERTURES.
- 8. La prise de courant doit avoir une connexion mise à la terre.
- 9. Placez le cordon d'alimentation de sorte que personne ne puisse marcher dessus.

Ne placez rien sur le cordon d'alimentation.

- 10. Tous les avertissements et mises en garde sur l'équipement doivent être notés.
- 11. Si l'appareil n'est pas utilisé pendant une longue période, débranchez-le du secteur pour ne pas être endommagé par une surtension transitoire.
- 12. Ne jamais verser de liquide dans les ouvertures de ventilation; Cela pourrait provoquer un incendie ou un choc électrique.
- 13. N'ouvrez jamais l'équipement. Pour des raisons de sécurité, seul le personnel de maintenance qualifié doit ouvrir l'équipement.
- 14. Si l'une des situations suivantes se présente, faites vérifier le matériel par le personnel de service:
 - Le cordon d'alimentation ou la fiche est endommagé.
 - Un liquide a pénétré dans l'appareil.
 - L'équipement a été exposé à l'humidité.
 - L'équipement ne fonctionne pas bien ou vous ne pouvez pas le faire. fonctionner conformément au manuel d'utilisation.
 - Equipment L'équipement est tombé et a été endommagé.
 - Equipment L'équipement présente des signes évidents de rupture.
- 15. Ne laissez pas cet équipement dans un environnement où la température de stockage peut être inférieure à -40° C (-40° F) ou supérieure à 85° C (185° F). Cela pourrait endommager l'équipement. L'équipement doit être dans un environnement contrôlé.
- 16. Tout composant non vérifié peut causer des dommages inattendus. Pour garantir une installation correcte, veuillez toujours utiliser les composants (ex. Vis) fournis avec la boîte d'accessoires.
- 17. ATTENTION: L'ordinateur est équipé d'un circuit d'horloge temps réel alimenté par batterie. Il y a un risque d'explosion si la batterie est remplacée de manière incorrecte. Remplacez uniquement avec le même type ou un type équivalent recommandé par le fabricant. Jetez les piles usagées conformément aux instructions du fabricant.

- 18. Débranchez toujours complètement le cordon d'alimentation de votre châssis lorsque vous utilisez du matériel. Ne faites pas de connexion quand l'appareil est sous tension. Les composants électroniques sensibles peuvent être endommagés par des surtensions soudaines.
- 19. Niveau de pression acoustique au poste de l'opérateur selon la norme CEI 704-1: 1982 n'est pas supérieur à 70 dB (A).
- 20. L'équipement ne doit être installé que dans une zone d'accès restreint.
- 21. Au moyen d'un cordon d'alimentation connecté à une prise de courant avec mise à la terre.
- 22. Ce produit est destiné à être alimenté par un bloc d'alimentation homologué UL adapté à une utilisation à Tma 50 degrés C min. dont la sortie est conforme à PS2 (ou LPS), ES1 (ou SELV) et dont la sortie est nominale: 9-36Vdc, 16.65-4.16A, si besoin d'aide supplémentaire, veuillez contacter Advantech pour plus d'informations.

AVERTISSEMENT: Cet ensemble d'instructions est donné conformément à la norme CEI 704-1. Advantech décline toute responsabilité quant à l'exactitude des déclarations contenues dans ce.

Contents

Chapter	1	General Introduction	.1
	1.1	Introduction	2
	1.2	Product Features	3
		1.2.1 General	3
		1.2.2 Ethernet	3
	1.3		4
			4
	1 /	1.3.2 SUSI 4.2 Mechanical Specifications	4
	1.4	1 4 1 Dimensions	5
		Figure 1.1 ARK-7060 Mechanical Dimensions Diagram	5
		1.4.2 Weight	6
	1.5	Power Requirements	6
		1.5.1 System Power	6
	1.6	Operating Environment Specifications	6
		1.6.1 Operating Temperature	6
		1.6.2 Relative Humidity	6
		1.6.3 Storage Temperature	b
		1.6.5 EMC	0 6
Chapter	2	Hardware Configuration	./
	2.1	Introduction	8
	2.2	Jumpers	8
		2.2.1 Jumper Description	8
		2.2.2 Jumper List	٥
		Figure 2.1 Jumper Lavout	9 Q
		224 Jumper Settings	9
		2.2.5 Bottom Board Jumper List	. 11
		2.2.6 Jumper Locations.	. 12
		2.2.7 Jumper Settings	. 13
	2.3	Connectors	. 15
		2.3.1 External I/O Locations	. 15
		Figure 2.2 Front I/O Connector Diagram	. 15
		Figure 2.3 COM Port Connector	. 16
		Table 2.1: COM Connector PIN Assignments	10
		Table 2.2: CN5/CN6 Ethernet Connector Pin Assignments	. 17
		Table 2.3: 10G Card LAN1 Ethernet Connector Pin Assignments	nts
		Figure 2.5 Power ON/OFF Button	18
		Figure 2.6 LED Indicators	. 18
		Figure 2.7 USB 3.0 Connector	. 19
		Table 2.4: USB 3.0 Connector Pin Assignments	. 19
		Figure 2.8 BMC Dedicated LAN Connector	. 19
		Table 2.5: CN9 BMC Dedicated LAN Connector Pin Assignme 19	nts
		Figure 2.9 BMC Dedicated COM Port	. 20
		Figure 2.10BMC Dedicated VGA Port	20
	2.4	Table 2.6: VGA Connector Pin Assignments	. 20 . 21
		2.4.1 Remove Top Cover	. 21

	2	2.4.2 Memory Installation	22
	2	2.4.3 HDD/SSD Installation	22
	2	2.4.4 M.2 Module Installation/Internal SIM Slot	23
	2	2.4.5 PCIex16 Graphic Card Installation	24
	2	2.4.6 Mounting Kit Installation	25
	2	2.4.7 Wide Operating Temperature Support	25
Chapter	3 I	BIOS Settings	27
:	3.1 li	ntroduction	
:	3.2 E	Entering the Setup	29
	3	3.2.1 Main Setup	29
	3	3.2.2 Advanced BIOS Features Setup	30
	3	3.2.3 Platform Configuration	45
	3	3.2.4 Socket Configuration	69
	3	3.2.5 Server Management	81
	3	3.2.6 Security	87
	3	3.2.7 Boot	89
	3	3.2.8 Save & Exit	90
Appendix	A ۱	Watchdog Timer Sample Code	91

A.1	EC Watchdog Timer Sample Code	
-----	-------------------------------	--



General Introduction

This chapter details background information on the ARK-7060 series.

1.1 Introduction

Advantech's ARK-7060 is a high-performance edge computer that empowers modeltraining applications via multiple expansion slots and fast data transfer speeds. It is equipped with the Intel® Xeon® D-1700 series processor and 4 x DDR4 SODIMM sockets (supporting up to 128GB). This solution provides PCI, PCIe x4, and PCIe x16 slots to enable the use of 350W graphics cards.

Multiple I/O and Storage Capabilities

ARK-7060 offers 2 x GbE, 4 x USB 3.0, and 4 x COM ports. It also supports up to 4 x 2.5" SATA III hard drive bays and delivers high data transfer rates via optional 10GbE ports and M.2 B key for 5G modules.

Advanced Security and Remote Management

ARK-7060 features dual BIOS for BIOS backup and recovery to enhance security. This lowers the risk of BIOS damage and protects against virus and/or data corruption. ARK-7060 also features an on-board baseboard management controller (BMC) to provide PMI architecture for remote management.

Built-in Intelligent Management Tools — Advantech SUSI API and WISE-DeviceOn

Advantech SUSI API provides a valuable suite of programmable APIs such as multilevel watchdog, hardware monitoring, system restoration, and other user-friendly interfaces.

SUSI API is an intelligent self-management cross platform tool that monitors system status for problems and takes action in the event of abnormalities. SUSI API offers a boot up guarantee in critical, low-temperature environments so systems can automatically recover when voltages dip. SUSI API makes the entire system more reliable and intelligent. ARK-7060 also supports Advantech WISE-DeviceOn software. This software supports remote management; and enables users to monitor, configure, and control a large number of terminals simultaneously, making maintenance and system recovery simpler.

1.2 Product Features

1.2.1 General

- **CPU:** Intel[®] Xeon[®] D-1700 series processor (up to 10 cores 67W)
- System Chipset: SoC
- BIOS: AMI EFI 512Mbit
- System Memory: 4 x DDR4 2666/2933MHz ECC/non-ECC SO-DIMM, up to 128GB
- Watchdog Timer: Single chip Watchdog 255-level interval timer, setup by software
- I/O Interface: 4 x RS232/422/485
- **USB:** 4 x USB 3.0 compliant ports
- IPMI 2.0 support: Aspeed AST2500 BMC supports IPMI 2.0 (Intelligent Platform Management Interface 2.0) via dedicate LAN, VGA, and console port
 - 1 x VGA
 - 1 x GbE management port
 - 1 x console port
- Storage: 2 x 2.5" swappable SATAIII HDD Bay with RAID 0/1 and max height 15 mm/0.59 in (up to 4 x 2.5" SATAIII HDD Bay by AMK-A0042)
- Expansion Interface:
 - 1 x M.2 2230/2280/3052 B Key, supporting M.2 2242/3042 with bracket (support SIM holder)
 - 1 x M.2 2230 E key for Wi-Fi modules
 - Add-on Card Slot: 1 x slot PCI+1 x slot PCIe x 4+1 x slot PCIe x 16
- **TPM:** TPM 2.0 (support by optional AMO-I029)

1.2.2 Ethernet

- Chipset:
 - LAN1/2 Intel[®] i210
 - LAN3/4 Intel[®] X550 (support by optional AMO-I031)
- Speed:
 - LAN1/2 10/100/1000 Mbps
 - LAN3/4 100/1000/10000 Mbps
- Interface: Up to 4 x RJ45

1.3 Chipset

1.3.1 Functional Specifications

1.3.1.1 Processor

Processor	Intel [®] Xeon [®] D-1700 series processor (up to 10 cores 67W) (Suspend mode S3 & S4 are not supported by this platform)
Memory	Supports DDR4 2666/2933MHz up to 128GB 4 x 260-pin SODIMM socket type

1.3.1.2 Chipset

SATA Interface		Supports several optional sections of Serial ATA III: Exten- sions to Serial ATA 1.0 Specification, Revision 1.0
		Supports SATA transfers to 600 Mbytes/sec.
USB Interface	-	USB host interface with support for 4 x USB 3.0 ports All ports are High-Speed, Full-Speed, and Low-Speed capa- ble Supports legacy keyboard/mouse software
		Supports regacy Reyboard/mouse software
BIOS		2 x AMI 512-Mbit EFI Flash BIOS via SPI (Dual BIOS)

1.3.1.3 Others

Serial Ports	÷	4 x serial ports Supports IRQ Sharing among serial ports under Microsoft Windows OS
		COM1, COM2, COM3, and COM4: RS232/422/485
Ethernet		LAN1/2 support 10/100/1000 Mbps, LAN3/4 support 100/ 1000/10000 Mbps LAN Connectors: Phone Jack RJ45 8P 90D (F)
Battery Backup	BAT	TERY 3V/210 mAh with WIRE x 1
ТРМ	TPN	/ 2.0 (support by optional AMO-I029)

1.3.2 SUSI 4.2

SUSI API	
Sequence Control	Supported
Watchdog Timer	Multi-level WDT (set by Advantech iManager) Programmable 1-255 sec/min
Hardware Monitor	CPU Temperature/input Current/input Voltage
System Information	Running HR/Boot record

Dimensions (W x H x D) 230 x 205 x 390 mm/9.05 x 8.07 x 15.35 in

Mechanical Specifications

1.4

1.4.1

Figure 1.1 ARK-7060 Mechanical Dimensions Diagram

1.4.2 Weight

9.7 kg (21.38 lb)

1.5 Power Requirements

1.5.1 System Power

- Power Type: ATX
- Minimum Power Input: 100 ~ 240V_{AC}
- Power Supply: 850W power supply built in

1.6 Operating Environment Specifications

1.6.1 Operating Temperature

■ With extended peripherals: -10 ~ 50 °C; 14 ~ 112 °F, with 0.7m/s air flow

1.6.2 Relative Humidity

- 95% @ 40 °C (104 °F) (non-condensing)
- **1.6.3** Storage Temperature ■ -40 ~ 85 °C (-40 ~ 185 °F)

1.6.4 Safety

CB (62368), UL (62368), CCC, BSMI, and UKCA

1.6.5 EMC

■ CE/FCC Class B, CCC, BSMI, and UKCA



Hardware Configuration

2.1 Introduction

The following sections show the internal jumper settings and the external connector pin assignments for different applications.

2.2 Jumpers

2.2.1 Jumper Description

You may configure ARK-7060 to match the needs of your application by setting jumpers. A jumper is a metal bridge used to close an electric circuit. It consists of two metal pins and a small metal clip (often protected by a plastic cover) that slides over the pins to connect them. To close a jumper, you connect the pins with the clip. To open a jumper, remove the clip. Sometimes a jumper will have three pins, labeled 1, 2 and 3. In this case you would connect either pins 1 and 2, or 2 and 3.



The jumper settings are schematically depicted in this manual as follows.



A pair of needle-nose pliers may be helpful when working with jumpers. If you have any doubts about the best hardware configuration for your application, contact your local distributor or sales representative before you make any changes. Generally, you simply need a standard cable to make most connections.

2.2.2 Jumper List

Table 2.1: Jumper List	
JCMOS1	Clear CMOS
PSON1	Auto Power On Setting
CN15	SMB Enable
SW_422_1	Fail safe
SW_422_2	Fail safe

2.2.3 Jumper Locations



Figure 2.1 Jumper Layout

2.2.4 Jumper Settings

2.2.4.1 Clear CMOS Setting for JCMOS1

JCMOS1 Clear CMOS Settings				
Part Number	1653003101			
Foot Print	HD_3x1P_79_D			
Description	PIN HEADER 3x1P 2.0 mm 180D(M) DIP 2000-13 WS			
Setting	Function			
(1-2)	Normal Operation (Default)			
(2-3)	Clear CMOS			

2.2.4.2 Auto Power On Setting for PSON1

PSON1 Clear CMOS Settings	
Part Number	1653003101
Foot Print	HD_3x1P_79_D
Description	PIN HEADER 3x1P 2.0mm 180D(M) DIP 2000-13 WS
Setting	Function
(1-2)	Auto Power On
(2-3)	Power button for Power On (Default)



2.2.4.3 M.2 E Key SMBus Enable by CN15

M.2 E Key SMBus Enable Settings		
Part Number	1653003101	
Foot Print	HD_3x1P_79_D	
Description	PIN HEADER 3x1P 2.0mm 180D(M) DIP 2000-13 WS	
Setting	Function	
(1-2)	Disable M.2 SMBus Channel	
(2-3)	Enable M.2 SMBus Channel(Default/No Jumper)	



2.2.4.4 Fail Safe by SW_422_1

Fail safe Enable Settings		
Part Number	160000402	
Foot Print	SW_4x2P_50_260x315	
Description	DIP SW SMD 8P SPST P=1.27mm W=5.4mm KHS42E	
Setting	Function	
Switch to Pin 1, 2, 3, 4	OFF(Default)	
Switch to Pin 5, 6, 7, 8	ON	



2.2.4.5 Fail Safe by SW_422_2

Fail safe Settings		
Part Number	160000402	
Foot Print	SW_4x2P_50_260x315	
Description	DIP SW SMD 8P SPST P=1.27 mm W=5.4mm KHS42E	
Setting	Function	
Switch to Pin 1, 2, 3, 4	OFF(Default)	
Switch to Pin 5, 6, 7, 8	ON	

5		4
6		3
7		2
8	ON	1

2.2.5 Bottom Board Jumper List

Table 2.1: Jumper List		
M2_SEL1	M.2 B Key Select Function Source Between SATA and PCIE	
M2_SEL2	M.2 B Key Select Function Source Between USB 3.0 and PCIE	
NGFF_SMBEN1	M.2 B Key SMB Enable	
CN10	5G Module power switch	

2.2.6 Jumper Locations



2.2.7 Jumper Settings

2.2.7.1 M.2 B Key Select Function Source Between SATA and PCIE by M2_SEL1

M2_SEL1 M.2 select function source settings		
Part Number	1653003101	
Foot Print	HD_3x1P_79_D	
Description	PIN HEADER 3x1P 2.0mm 180D(M) DIP 2000-13 WS	
Setting	Function	
(1-2)	Auto detect by card (Default)	
(2-3)	SATA	
Floating	PCIE	

	1
0	2
0	3

2.2.7.2 M.2 B Key Select Function Source Between USB 3.0 and PCIE by M2_SEL2

M2_SEL2 M.2 select function source settings		
Part Number	1653003101	
Foot Print	HD_3x1P_79_D	
Description	PIN HEADER 3x1P 2.0mm 180D(M) DIP 2000-13 WS	
Setting	Function	
(1-2)	Auto detect by card (Default)	
(2-3)	USB 3.0	
Floating	PCIE	

	1
0	2
0	3

2.2.7.3 M.2 B Key SMBus Enable by NGFF_SMBEN1

M.2 SMBus Enable Settings	
Part Number	1653003101
Foot Print	HD_3x1P_79_D
Description	PIN HEADER 3x1P 2.0mm 180D(M) DIP 2000-13 WS
Setting	Function
(1-2)	Disable M.2 SMBus Channel
(2-3)	Enable M.2 SMBus Channel (Default)



2.2.7.4 For 5G Module Power Switch by CN10

Power switch Settings		
Part Number	1653003101	
Foot Print	HD_3x1P_79_D	
Description	PIN HEADER 3x1P 2.0 mm 180D (M) DIP 2000-13 WS	
Setting	Function	
(1-2)	Set Vout 3.805V (For 5G module support +3.805V)	
(2-3)	Set Vout 3.304V (Default)	

2.3 Connectors

2.3.1 External I/O Locations



Figure 2.2 Front I/O Connector Diagram

2.3.1.1 COM Port Connector

ARK-7060 provides up to 4 x D-sub 9-pin connectors, which offers RS-232/422/485 serial communication interface ports. The default setting is RS-232, the mode RS-422/485 of ARK-7060 are supported via BIOS settings.



Figure 2.3 COM Port Connector

Table 2.1: COM Connector Pin Assignments			
	RS-232	RS-422	RS-485
Pin	Signal Name	Signal Name	Signal Name
1	DCD	Tx-	DATA-
2	RxD	Tx+	DATA+
3	TxD	Rx+	NC
4	DTR	Rx-	NC
5	GND	GND	GND
6	DSR	NC	NC
7	RTS	NC	NC
8	CTS	NC	NC
9	RI	NC	NC

2.3.1.2 Ethernet Connector (LAN)

ARK-7060 is equipped with up to 4 x (LAN3/4 are optional by AMO-I031) Ethernet ports. LAN1/2 controllers that are fully compliant with IEEE 802.3u 10/100/1000 Mbps CSMA/CD standards. LAN3/4 are powered by 10GBASE-T controllers providing 10Gb/s of throughput.

These Ethernet ports provides a standard RJ-45 jack connector with LED indicators on the front side to show its Active/Link status (Green LED) and Speed status (Yellow LED).



Figure 2.4 Ethernet Connector

For LAN1/2 Connector:

Table 2.2: CN5/CN6	Ethernet Connector Pin Assignments
Pin	10/100/1000BaseT Signal Name
C1	MDI_LAN_D0_P
C2	MDI_LAN_D0_N
C3	MDI_LAN_D1_P
C4	MDI_LAN_D2_P
C5	MDI_LAN_D2_N
C6	MDI_LAN_D1_P
C7	MDI_LAN_D3_P
C8	MDI_LAN_D3_N



For LAN3/4 Connector:

Table 2.3: 10G Card LAN1 Ethernet Connector Pin Assignments		
Pin	10GBaseT Signal Name	
C1	TRD1+	
C2	TRD1-	
C3	TRD2+	
C4	TRD3+	
C5	TRD3-	
C6	TRD2-	
C7	TRD4+	
C8	TRD4-	

Upper Left LED

Upper Right LED



2.3.1.3 Power On/Off Button

ARK-7060 has a Power On/Off button with LED indicators on the front side that show "On" (Green LED) and "Off/Suspend" statuses (Orange LED). The Power button supports dual functions: Soft Power -On/Off (Instant off or Delay 4 Seconds then off), and Suspend.



Figure 2.5 Power ON/OFF Button

2.3.1.4 LED Indicators

There are four LEDs on the front panel that indicate the system's status: HDD LED is for HDD status.



2.3.1.5 USB 3.0 Connector

ARK-7060 supports 4 x USB 3.0 interfaces. The USB interfaces complies with USB UHCI, Rev. 3.0 standards. Please refer to Table 2.5 for its pin assignments. USB 3.0 connectors contain legacy pins to interface with USB 2.0 devices, and a new set of pins for USB 3.0 connectivity.



Figure 2.7 USB 3.0 Connector

Table 2.4: USB 3.0 Connector Pin Assignments			
Pin	Signal Name	Pin	Signal Name
1	+5V	2	USB_data-
3	USB_data+	4	GND
5	SSRX-	6	SSRX+
7	GND	8	SSTX-
9	SSTX+		

2.3.1.6 BMC Dedicated LAN Connector



Figure 2.8 BMC Dedicated LAN Connector

Table 2.5: CN9 BMC Dedicated LAN Connector Pin Assignments		
Pin	10/100/1000BaseT Signal Name	
C1	MDI_LAN_D0_P	
C2	MDI_LAN_D0_N	
C3	MDI_LAN_D1_P	
C4	MDI_LAN_D2_P	
C5	MDI_LAN_D2_N	
C6	MDI_LAN_D1_P	
C7	MDI_LAN_D3_P	
C8	MDI_LAN_D3_N	



2.3.1.7 BMC Dedicated COM Port



Figure 2.9 BMC Dedicated COM Port

Table 2.6: COM2 BMC Dedicated COM Port Pin Assignments		
Pin	Signal Name (RS232)	
1	NC	
2	RxD	
3	TxD	
4	NC	
5	NC	
6	NC	
7	NC	
8	NC	
9	NC	

2.3.1.8 BMC Dedicated VGA Connector



Figure 2.10 BMC Dedicated VGA Port

Table 2.6: VGA Connector Pin Assignments			
Pin	Signal Name	Pin	Signal Name
1	Red	2	Green
3	Blue	4	NC
5	GND	6	GND
7	GND	8	GND
9	NC	10	GND
11	NC	12	DDAT
13	H-SYNC	14	V-SYNC
15	DCLK		

Chapter 2 Hardware Configuration

2.4 Installation

2.4.1 Remove Top Cover

- 1. Unscrew the 7 screws on the top cover.
- 2. Slightly move the top cover backward, and then lift it up to remove it.



2.4.2 Memory Installation

- 1. Remove top cover (2.4.1).
- 2. Install memory in the system.
- 3. Replace the top cover.
- Memory Configuration Instruction: Using 1 x DIMM: install on CN1 or CN3 slot Using 2 x DIMM: install on CN1 & CN3 slot Using 3 x DIMM is not supported.



2.4.3 HDD/SSD Installation

- 1. Unscrew the 2 x screws on the hard drive bay.
- 2. Install HDD/SSD with 4 x screws on the HDD/SSD tray.
- 3. Push back the hard drive bay into the system and secure it using the same screws.



2.4.4 M.2 Module Installation/Internal SIM Slot

- 1. Remove top cover (2.4.1).
- 2. Install M.2 B Key module (M2B1 with SIM holder) with bracket according to the M.2 module form factor, and secure in place with screw(s).
- 3. Install M.2 E key module with 1 x screw (M2E1).
- 4. Replace the top cover and secure it in place with 7 screws.





2.4.5 PCIex16 Graphic Card Installation

- 1. Remove the top cover (2.4.1).
- 2. Remove the 2 horizontal bars on the top of the system.
- 3. Install the graphics card bracket using 2 screws
- 4. Install the top rubber on top horizontal bar to secure the graphics card. Install the bottom nut according to length of the graphics card.
- 5. Install the graphics card, secure it with a screw (M5X11L) on the bottom nut and connect the cable. If the cable is too short, slightly pull the cable outward.
- 6. Replace/return the 2 horizontal bars on the top of the system.
- 7. Replace the top cover and secure in place with 7 screws.


2.4.6 Mounting Kit Installation

- 1. Take out mounting kit and 6 x screws (M4x6L) from carton.
- 2. Screw each of the 3 x screws (M4x6L) on the left and right sides to secure the system horizontally.



2.4.7 Wide Operating Temperature Support

To make sure the system works well under 0 $^{\circ}$ C (32 $^{\circ}$ F) or over 50 $^{\circ}$ C (122 $^{\circ}$ F), please ensure your peripherals are i-grade. These support wide temperature operation.



BIOS Settings

3.1 Introduction

AMIBIOS has been integrated into motherboards for over two decades. With the AMIBIOS Setup program, users can modify BIOS settings and control various system features. This chapter describes the basic navigation of the ARK-7060 BIOS setup screens.

Main Advanced Platform	Aptio Setup – AMI Configuration Socket Configuration	Server Mgmt Security Boot 🔹
BIOS Information BIOS Vendor Core Version Compliancy Project Version Build Date and Time Access Level Project Board Version Power Type	American Megatrends 5.0.2.3 0.01 x64 UEFI 2.8; PI 1.7 7060000060X014 01/27/2022 13:12:44 Administrator ARK-7060 ATX	Set the Date. Use Tab to switch between Date elements. Default Ranges: Year: 1998–9999 Months: 1–12 Days: Dependent on month Range of Years may vary.
Memory Information Total Memory	8192 MB	
System Date System Time	[Fri 01/01/2021] [23:05:32]	<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
	Version 2.22.1281 Copyright (C) 202	2 AMI

AMI's BIOS ROM has a built-in Setup program that allows users to modify the basic system configuration. This information is stored in flash ROM so it retains the Setup information when the power is turned off.

3.2 Entering the Setup

Turn on the computer and check for the patch code. If there is a number assigned to the patch code, it means that BIOS supports your CPU. If there is no number assigned to the patch code, please contact an Advantech application engineer to obtain an up-to-date patch code file. This will ensure that your CPU's system status is valid. After ensuring that you have a number assigned to the patch code, press and you will immediately be allowed to enter Setup.

3.2.1 Main Setup

When users first enter the BIOS Setup Utility, they will enter the Main setup screen. Users can always return to the Main setup screen by selecting the Main tab. There are two Main Setup options. They are described in this section. The Main BIOS Setup screen is shown below.

Main Advanced Platform Configur	Aptio Setup – AMI ation Socket Configuration	Server Mgmt Security Boot 🕨
BIOS Information BIOS Vendor Core Version Compliancy Project Version Build Date and Time Access Level Project Board Version Power Type Memory Information Total Memory	American Megatrends 5.0.2.3 0.01 x64 UEFI 2.8; PI 1.7 7060000060X014 01/27/2022 13:12:44 Administrator ARK-7060 ATX 8192 MB	Set the Date. Use Tab to switch between Date elements. Default Ranges: Year: 1998–9999 Months: 1–12 Days: Dependent on month Range of Years may vary.
System Date System Time	[Fri 01/01/2021] [23:05:32]	<pre>++: Select Screen f4: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
Version 2.22.1281 Copyright (C) 2022 AMI		

The Main BIOS setup screen has two main frames. The left frame displays all the options that can be configured. Grayed-out options cannot be configured; options in blue can. The right frame displays the key legend.

Above the key legend is an area reserved for a text message. When an option is selected in the left frame, it is highlighted in white. Often a text message will accompany it.

System time/System date

Use this option to change the system time and date. Highlight System Time or System Date using the <Arrow> keys. Enter new values through the keyboard. Press the <Tab> key or the <Arrow> keys to move between fields. The date must be entered in MM/DD/YY format. The time must be entered in HH:MM:SS format.

3.2.2 Advanced BIOS Features Setup

Select the Advanced tab from the ARK-3531 setup screen to enter the Advanced BIOS Setup screen. Users can select any item in the left frame of the screen, such as CPU Configuration, to go to the sub menu for that item. Users can display an Advanced BIOS Setup option by highlighting it using the <Arrow> keys. All Advanced BIOS Setup options are described in this section. The Advanced BIOS Setup screens are shown below. The sub menus are described on the following pages.

Aptio Setup – AMI Main <mark>Advanced</mark> Platform Configuration Socket Configuration	Server Mgmt Security Boot 🔹
 Trusted Computing Embedded Controller SS RTC Wake Settings UEFI Variables Protection Serial Port Console Redirection USB Configuration Network Stack Configuration NVMe Configuration T1s Auth Configuration All Cpu Information 	Trusted Computing Settings ++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.22.1281 Copyright (C) 2022	2 AMI

Chapter 3 BIOS Settings

3.2.2.1 Trusted Computing

Aptio : Main Advanced Platform Configuration Soci	Setup – AMI .et Configuration Server Mgmt Security Boot → ▶
 Trusted Computing Embedded Controller S5 RTC Wake Settings UEFI Variables Protection Serial Port Console Redirection USB Configuration Network Stack Configuration NVMe Configuration T1s Auth Configuration All Cpu Information 	Trusted Computing Settings
	<pre> ++: Select Screen f↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
Version 2.22.1281	Copyright (C) 2022 AMI

Advanced	Aptio Setup — AMI	
TPM 2.0 Device Found Firmware Version: Vendor: Security Device Support Active PCR banks Available PCR banks	7.63 IFX [Enable] SHA-1,SHA256 SHA-1,SHA256	Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INTIA interface will not be available.
SHA-1 PCR Bank SHA256 PCR Bank Pending operation Platform Hierarchy Storage Hierarchy Endorsement Hierarchy TPM 2.0 UEFI Spec Version Physical Presence Spec Version TPM 2.0 InterfaceType Device Select	[Enabled] [Enabled] [Enabled] [Enabled] [Enabled] [TCG_2] [1.3] [TIS] [Auto]	++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version	2.22.1281 Copyright (C) 202	2 AMI

TPM Support

"Enable or Disable" TPM Support.

 Security Device Support Enables or Disables BIOS support for security device.

- SHA-1 PCR Bank Enable or Disable SHA-1 PCR Bank.
- SHA256 PCR Bank Enable or Disable SHA256 PCR Bank.
- Pending Operation Schedule an Operation for the Security Device. NOTE: Your Computer will reboot during restart in order to change State of Security Device.
- Platform Hierarchy Enable or Disable Platform Hierarchy.
- Storage Hierarchy Enable or Disable Storage Hierarchy.
- Endorsement Hierarchy Enable or Disable Endorsement Hierarchy.
- TPM 2.0 UEFI Spec. Version Select the TCG2 Spec Version Support. TCG_1_2:the Compatible mode for Win8/Win10. TCG_2:Support new TCG2 protocol and event format for Win10 or later.
- Physical Presence Spec. Version Select to Tell O.S. to support PPI Spec Version 1.2 or 1.3. Note some HCK tests might not support 1.3.
- Device Selection Select TPM 1.2 or TPM 2.0.

3.2.2.2 Embedded Controller Configuration

Aptio Setup – AMI Main Advanced Platform Configuration Socket Configuration	Server Mømt Security Boot -
 Trusted Computing Embedded Controller S5 RTC Wake Settings UEFI Variables Protection Serial Port Console Redirection USB Configuration Network Stack Configuration NVMe Configuration Tls Auth Configuration All Cpu Information 	Embedded Controller Parameters.
	<pre>++: Select Screen f↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
Version 2.22.1281 Copyright (C) 2022	AMI

Advanced	Aptio Setup – AMI	
Embedded Controller		Select Power Saving Mode
Embedded Controller Firmware Version	EID-201 X00122764	
 Power Saving Mode Serial Port 1 Configuration Serial Port 2 Configuration Serial Port 3 Configuration Serial Port 4 Configuration 	[Normal]	
▶ Hardware Monitor		<pre>++: Select Screen f4: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
Version	2.22.1281 Copyright (C) 2022	AMI

Power Saving Mode

This item allows users to set the board's power saving mode when off.

Advanced	Aptio Setup – AMI	
Embedded Controller		Set Parameters of Serial Port
Embedded Controller Firmware Version	EID-201 X00122764	I (GUNH)
Power Saving Mode	[Normal]	
 Serial Port 1 Configuration Serial Port 2 Configuration Serial Port 3 Configuration Serial Port 4 Configuration Hardware Monitor 		<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
Version	2.22.1281 Copyright (C) 2022	2 AMI



- Serial Port 1 Configuration Set Parameters of Serial Port 1.
- Serial Port 2 Configuration Set Parameters of Serial Port 2.
- Serial Port 3 Configuration Set Parameters of Serial Port 3.
- Serial Port 4Configuration Set Parameters of Serial Port 4.

Advanced	Aptio Setup – AMI	
Embedded Controller		Monitor hardware status
Embedded Controller Firmware Version	EIO-201 X00122764	
Power Saving Mode	[Normal]	
 Serial Port 1 Configuration Serial Port 2 Configuration Serial Port 3 Configuration Serial Port 4 Configuration Hardware Monitor 		
		<pre>++: Select Screen f↓: Select Item Enter: Select +/-: Change Opt.</pre>
		F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Versio	n 2.22.1281 Copyright (C) 20	D22 AMI

Advanced	Aptio Setup – AMI	
PC Health Status		Set CPU smart fan mode and
CPU Temperature System Temperature	: + 42.9°C/ +109.2°F : + 30.9°C/ +87.6°F	pur unic ter s.
CPUFAN1 SYSFAN1	: 888 RPM : O RPM	
+12V 5VSB VBAT + 5V	: +12.05 V : +5.05 V : +3.00 V : +5.04 V	
+3.3V CPU Smart Fan Mode Select Temp threshold of high speed	: +3.28 V [Auto] 80	<pre>++: Select Screen f↓: Select Item Enter: Select</pre>
Maximum PWM Duty Temp threshold of low speed Minimum PWM Duty Temp threshold of stop FAN	100 30 0 0	+/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults
System Smart Fan Mode Select Temp threshold of high speed Maximum PWM Duty Temp threshold of low speed	[Auto] 55 100 35	F4: Save & Exit ESC: Exit
Version	2.22.1283 Copyright (C) 203	22 AMI

Advanced	Aptio Setup – AMI		
CPU Temperature	: + 42.9°C/ +109.2°F	Set temperature threshold of	
System Temperature	: + 30.9 C/ +87.6 F	stop FAN.(Range:0 – 100)	
CRUEAN1	• 976 RPM		
	• 0 PPM		
STOLINE	• • • • • •		
+12V	: +12.06 V		
5VSB	: +5.05 V		
VBAT	: +3.00 V		
+ 5V	: +5.05 V		
+3.3V	: +3.27 V		
CPU Smart Fan Mode Select	[Auto]		
Temp threshold of high speed	80	↔: Select Screen	
Maximum PWM Duty	100	↑↓: Select Item	
Temp threshold of low speed	30	Enter: Select	
Minimum PWM Duty	0	+/-: Change Opt.	
Temp threshold of stop FAN	0	F1: General Help	
		F2: Previous Values	
System Smart Fan Mode Select	[Auto]	F3: Optimized Defaults	
lemp threshold of high speed	55	F4: Save & Exit	
Maximum PWM Duty	100	ESU: EXIT	
Temp threshold of low speed	35		
Town threshold of stop 500	20		
Temp Inreshold of Stop PAN			
Version	Version 2, 22, 1283 Convergent (C), 2022 AMT		

Hardware Monitor

This page displays all information about system Temperature/Voltage/Current/ Fan.

- CPU/System Smart Fan Mode Select Set CPU/System smart fan mode and parameters.
- Temp threshold of high speed
 Set temperature threshold of high speed. (Range: 0 ~ 100)
- Maximum PWM Duty
 Set maximum PWM Duty output value. (Range: 0 ~ 100)
- Temp threshold of low speed
 Set temperature threshold of low speed. (Range: 0 ~ 100)
- Minimum PWM Duty
 Set minimum PWM Duty output value. (Range: 0 ~ 100)
- Temp threshold of stop FAN Set temperature threshold of stop FAN. (Range: 0 ~ 100)

3.2.2.3 S5 RTC Wake Settings

Apti	etup – AMI
Main Advanced Platform Configuration S	et Configuration Server Mgmt Security Boot
 Trusted Computing Embedded Controller S5 RTC Wake Settings UEFI Variables Protection Serial Port Console Redirection USB Configuration Network Stack Configuration NVMe Configuration Tls Auth Configuration All Cpu Information 	Enable system to wake from S5 using RTC alarm
	++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.22.12	Copyright (C) 2022 AMI

Advanced	Aptio Setup – AMI	
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 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
	Version 2.22.1281 Copyright (C)) 2022 AMI

Wake System From S5

Enable or disable System wake on alarm event. Select Fixed Time, system will wake on the hr::min::sec specified.

3.2.2.4 UEFI Variables Protection



Advanced	Aptio Setup - AMI	
Password protection of Runtime Variables	[Enable]	Control the NVRAM Runtime Variable protection through System Admin Password ++: Select Screen fl: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2	2.22.1281 Copyright (C) 2022	AMI

Password protection of Runtime

Control the NVRAM Runtime Variable protection through System Admin Password.

3.2.2.5 Serial Port Console Redirection

Aptio Setup – AMI Main Advanced Platform Configuration Socket Configuration	Server Mgmt Security Boot →
 Trusted Computing Embedded Controller S5 RTC Wake Settings UEFI Variables Protection Serial Port Console Redirection USB Configuration Network Stack Configuration NVMe Configuration Tls Auth Configuration All Cpu Information 	Serial Port Console Redirection
	<pre> ++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
Version 2.22.1281 Copyright (C) 2022	AMI

Advanced	Aptio Setup – AMI	
COMO Console Redirection	[Disabled]	Console Redirection Enable or Disable.
		<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
	Version 2.22.1281 Copyright (C)	2022 AMI

Console Redirection

This item allows users to enable or disable console redirection for Microsoft Windows Emergency Management Services (EMS).

3.2.2.6 USB Configuration

Aptio Setup – AMI Main Advanced Platform Configuration Socket Configuration	Server Mgmt Security Boot
 Trusted Computing Embedded Controller S5 RTC Wake Settings UEFI Variables Protection Serial Port Console Redirection USB Configuration Network Stack Configuration NVMe Configuration Tls Auth Configuration All Cpu Information 	USB Configuration Parameters
	<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
Version 2.22.1281 Copyright (C) 2022	2 AMI

Advanced	Aptio Setup – AMI	
USB Configuration		Enables Legacy USB support.
USB Module Version	27	support if no USB devices are connected. DISABLE option will keen USB devices available
1 XHCI USB Devices:		only for EFI applications.
1 Drive, 1 Keyboard, 1 Mouse,	3 Hubs	
Legacy USB Support XHCI Hand-off	[Enabled] [Enabled]	
USB Mass Storage Driver Support	[Enabled]	
USB hardware delays and time-outs:	[20 sec]	++: Select Screen
Device reset time-out	[20 sec]	Enter: Select
Device power-up delay	[Auto]	+/−: Change Opt. F1: General Help
Mass Storage Devices:	[Auto]	F2: Previous Values
JE(F145111546JFV30 0.07	[Huto]	F4: Save & Exit
		ESC: Exit
Version	2.22.1281 Copyright (C) 2022	AMI

Legacy USB Support

This supports USB devices with legacy OS such as DOS. When choosing "AUTO", the system will automatically detect USB devices. It will enable USB legacy mode when a USB device is plugged in and disable USB legacy mode when no USB device is plugged in.

XHCI Hand-off

This is a workaround for OS without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.

- USB Mass Storage Driver Support "Enable or Disable" USB Mass Storage driver support.
- USB Transfer Time-Out Allows you to select the USB transfer time-out value. [1,5,10,20sec].
- Device Reset Time-Out Allows you to select the USB device reset time-out value. [10,20,30,40sec].

Device Power-Up Delay

Maximum time the device will take before it properly reports itself to the Host Controller. "Auto" uses default value: for a Root port it is 100 ms, for a Hub port the delay is take from Hub descriptor.

Mass Storage Devices

Mass storage device emulation type. "Auto" enumerates device according to their media format. Optical drives are emulated as "CD-ROM", drives with no media will be emulated according to a drive type.

3.2.2.7 Network Stack Configuration

Aptio Setup – AMI			
Main Advanced Platform Configuration	Socket Configuration	Server Mgmt Security Boot 🔹 🕨	
 Trusted Computing Embedded Controller S5 RTC Wake Settings UEFI Variables Protection Serial Port Console Redirection USB Configuration Network Stack Configuration NVMe Configuration T1s Auth Configuration All Cpu Information 		Network Stack Settings	
		<pre>++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>	
Version 2.22.	1281 Copyright (C) 202	2 AMI	

Advanced	Aptio Setup – AMI	
Advanced Network Stack	[Disabled]	Enable/Disable UEFI Network Stack ++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help
		F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
	version 2.22.1281 Copyright (C)	2022 HM1

Network Stack

"Enable or Disable" UEFI Network Stack.

3.2.2.8 NVMe Configuration





NVMe Configuration

Display device information of NVMe. E.g model name/size.

3.2.2.9 TIs Auth Configuration

Aptio Setup – AMI Main Advanced Platform Configuration Socket Configuration	Server Mgmt Security Boot 🌖
 Trusted Computing Embedded Controller S5 RTC Wake Settings UEFI Variables Protection Serial Port Console Redirection USB Configuration Network Stack Configuration NVMe Configuration T1s Auth Configuration All Cpu Information 	Press <enter> to select Tls Auth Configuration.</enter>
	<pre> ++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
Version 2.22.1281 Copyright (C) 203	22 AMI



Server CA Configuration

Configure a server CA (Certificate Authority) settings.

Client Cert Configuration Configure Client Cert settings. Client cert configuration is unsupported currently.

3.2.2.10 All CPU Information

Aptio Setup	- AMI
Main Advanced Platform Configuration Socket Co	nfiguration Server Mgmt Security Boot 🛛 🕨
 Trusted Computing Embedded Controller S5 RTC Wake Settings UEFI Variables Protection Serial Port Console Redirection USB Configuration Network Stack Configuration NVMe Configuration Tls Auth Configuration All Cpu Information 	Display all cpu information
	<pre>++: Select Screen fl: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
Version 2.22.1281 Copyr	ight (C) 2022 AMI

Advanced	otio Setup – AMI
Total CPU Number: 8 CPU0 CPUID: 000606C0 Stepping: 0 MicroCodeRev: FD0001D0 PlatformID: 001000000000000 CpuCoreFreq (MHz): 00001584 CPU1 CPUID: 000606C0 Stepping: 0 MicroCodeRev: FD0001D0 PlatformID: 00100000000000 CpuCoreFreq (MHz): 00001584 CPU2 CPUID: 000606C0 Stepping: 0 MicroCodeRev: FD0001D0 PlatformID: 00100000000000 CpuCoreFreq (MHz): 00001600 ActualCpuFreq (MHz): 00001600 CpuCoreFreq (MHz): 00001600 ActualCpuFreq (MHz): 00001600 CpuCoreFreq (MHz): 00001600 CpUS CPUID: 000606C0 Stepping: 0	<pre>**: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
Version 2.22	.1281 Copyright (C) 2022 AMI

Display the information of each CPU core.

3.2.3 Platform Configuration

3.2.3.1 PCH-IO Configuration

Aptio Setup – AMI Main Advanced Platform Configuration Socket Configuration S	Server Mgmt Security Boot →
Main Advanced Platform Configuration Socket Configuration : PCH-IO Configuration Server ME Configuration System Event Log Intel(R) Time Coordinated Computing 	Server Mgmt Security Boot ► PCH Parameters ++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit
	ESC: Exit
version 2.22.1283 copyright (C) 2022	HUI



- Serial IRQ Mode Configure Serial IRQ Mode.
- State After G3
 Specify what state to go to when power is re-applied after a power failure (G3 state).
- Flash Protection Range Registers (FPRR) Enable Flash Protection Range Registers.

Platform Configurat	Aptio Setup – AMI <mark>ion</mark>	
PCI Express Configuration		PCI Express Port8xh Decode
Port8xh Decode Peer Memory Write Enable Compliance Test Mode	[Disabled] [Disabled] [Disabled]	
 PCI Express Root Port 1(M.2 B Key) PCI Express Root Port 2(M.2 E Key) PCI Express Root Port 5(x4) 		
LAN1 Controller LAN2 Controller Intel X550 Controller	[Enabled] [Enabled] [Enabled]	
		ti: Select Item Enter: Select +/−: Change Opt.
		F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit
		ESC. EXIL
Version 2	.22.1281 Copyright (C) 2022	AMI

PCI Express Configuration

- Port8xh Decode
 Enable/Disable PCI Express Port8xh Decode.
- Peer Memory Write Enable
 Enable/Disable Peer Memory Write.
- Compliance Test Mode
 Enable when using Compliance Load Board.
- LAN1/LAN2 Controller
 Enable/Disable on board LAN1/LAN2 from Intel i210 Controller support.
- Intel X550 Controller
 Enable/Disable on board LAN3/LAN4 from Intel X550 Controller support.
 (LAN3/LAN4 are optional by AMO-I031)

ARK-7060 User Manual



Platform Conf	Aptio Setup - AMI Platform Configuration			
PCI Express Root Port 1 ASPM L1 Substates PCIe Speed	[Enabled] [Disabled] [Disabled] [Gen3]	Control the PCI Express Root Port.		
		<pre>+#: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>		
Ven	sion 2.22.1281 Copyright (C)	2022 AMI		

- PCI Express Root Port

Configure PCI Express Root Port Settings.

- ASPM

PCI Express Active State Power Management settings.

L1 Substates

PCI Express L1 Substates settings.

Chapter 3 BIOS Settings

- PCIe Speed

Configure PCIe Speed. Auto is equal to Gen2 or Gen3 depending on DTR soft strap.

Platform Configura	Aptio Setup – AMI tion	
SATA Controller Speed Controller 1 SATA Configuration Controller 2 SATA Configuration Controller 3 SATA Configuration	[Default]	Indicates the maximum speed the SATA controller can support.
		<pre>++: Select Screen f↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
Version	2.22.1281 Copyright (C) 2022	AMI

SATA Configuration

- SATA Controller Speed

Indicates the maximum speed the SATA controller can support.



- SATA Configuration
 Enable/Disable SATA controller.
- SATA Mode Selection
 Determine how SATA controllers operate.
- Aggressive LPM support Enables/Disables SATA Aggressive Link Power Management. This item will appear when "AHCI" or "RAID" is selected.
- SATA port 1/2/3/4
 Enable/disable SATA port. SATA port 3 & 4 are optional.

Platfor	Aptio Setup – AMI rm Configuration	
Software Feature Mask Co HDD Unlock LED Locate	onfiguration for Controller 1 [Enabled] [Enabled]	If enabled, indicates that the HDD password unlock in the OS is enabled.
		<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
	Version 2.22.1281 Copyright (C) 2022 AMI

- HDD Unlock

If enabled, it indicates that the HDD password unlock in the OS is enabled.

- LED Locate

If enabled, it indicates that the LED/SGPIO hardware is attached and ping to locate feature is enabled on the OS.

USB Configuration

Platform Configur	Aptio Setup – AMI Pation		
USB Configuration		Options to enable Compliance	
XHCI Compliance Mode		Compliance Mode. Change to enabled for Compliance Mode	
xDCI Support	[Disabled]	testing.	
USB Overcurrent USB Overcurrent Lock USB2 PHY Sus Well Power Gating	[Enabled] [Enabled] [Disabled]		
USB Port Disable Override	[Disable]		
XHCI Wake On Usb Enable	[Enabled]	<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>	
Version 2.22.1281 Copyright (C) 2022 AMI			

- XHCI Compliance Mode

Options to enable Compliance Mode. Default is to disable Compliance Mode. Change to enabled for Compliance Mode testing.

- xDCI Support

Enable/Disable xDCI (USB OTG Device).

- USB Overcurrent

Select 'Disabled' for pin-based debug. If pin-based debug is enabled but USB overcurrent is not disabled, USB DbC does not work.

- USB Overcurrent Lock

Select 'Enabled' if Overcurrent functionality is used. Enabling this will make xHCI controller consume the Overcurrent mapping data.

- USB2 PHY Sus Well Power Gating Select 'Enabled' to enable SUS Well PG for USB2 PHY. This option has no effect on PCH-H.
- XHCI Wake On Usb Enable
 Enables/Disables support for XHCI Wake on USB on connect/disconnect.

Security Configuration

Platform Configurat	Aptio Setup — AMI <mark>ion</mark>	
PCH-IO Configuration		Security Configuration settings
 PCI Express Configuration SATA Configuration USB Configuration Security Configuration 		
Serial IRQ Mode State After G3 Flash Protection Range Registers (FPRR)	[Continuous] [85 State] [Enabled]	
		<pre>++: Select Screen fl: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
Version 2	.22.1281 Copyright (C) 2022	AMI

Platform Configura	Aptio Setup – AMI ation	
Security Configuration RTC Memory Lock BIOS Lock Force unlock on all GPIO pads	[Enabled] [Enabled] [Enabled]	Enable will lock bytes 38h–3Fh in the lower/upper 128–byte bank of RTC RAM
		<pre>++: Select Screen fl: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
Version	2.22.1281 Copyright (C) 2022	2 AMI

- RTC Memory Lock

Enable will lock bytes 38h-3Fh in the lower/upper 128-byte bank of RTC RAM.

- BIOS Lock

"Enable or Disable" the PCH BIOS Lock Enable feature. Required to be enabled to ensure SMM protection of flash.

Force unlock on all GPIO pads
 If Enabled BIOS will force all GPIO pads to be in unlocked state.

3.2.3.2 Sever ME Configuration

Main Advance	d Platform	Ap Configuration	tio Setu Socket	u <mark>p – AMI</mark> Configuration	Server Mgmt	Security	Boot 🕨
PCH-IO Configu Server ME Conf System Event Lu	ration iguration og				Configure : Parameters	Server ME T	echnology
Setup Warning: Setting items may cause syst	on this Scr em to malfu	een to incorred nction!	t values	3			
					the Salast	Separa	
					fl: Select Enter: Sel +/-: Change	Item ect e Opt.	
					F1: Genera F2: Previo F3: Optimi: F4: Save & ESC: Exit	l Help us Values zed Default Exit	S
		Version 2.22.	1281 Cop	oyright (C) 202	22 AMI		

Aptio Setup – AMI Platform Configuration			
General ME Configuration Oper. Firmware Version Backup Firmware Version Recovery Firmware Version ME Firmware Status #1 ME Firmware Status #2 Current State Error Code Recovery Cause PTT Support Suppress PTT Commands Altitude	A 11:5.0.2.33 N/A 11:5.0.2.33 0x00000245 0x8911A006 Operational No Error N/A [Disabled] [Disabled] 3000 0	The altitude of the platform location above the sea level, expressed in meters. The hex number is decoded as 2's complement signed integer. Provide the 8000h value if the altitude is unknown.	
Server ME firmware features list SiEn NodeManager ICC MeStorageServices BootGuard HSIO PECIOverDMI PCHDebug PowerThermalUtility FiaMuxConfiguration PCHThermalSensorInit		<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>	
Version	2.22.1281 Copyright (C) 2022	AMI	

Chapter 3 **BIOS Settings**

MCTP Bus Owner

[15:8] bus, [7:3] device, [2:0] function. If all zeros sending bus owner is disabled.

3.2.3.3 System Event Log

	Aptio Setup – AMI	
Main Advanced Platform Configura	ation Socket Configuratio	on Server Mgmt Security Boot 🛛 🖡
 PCH-IO Configuration Server ME Configuration System Event Log Setup Warning: Setting items on this Screen to incompany cause system to malfunction! 	correct values	Press <enter> to view or change the event log configuration.</enter>
		<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
Version	2.22.1281 Copyright (C) 3	2022 AMI
	Antis Ostur ANT	
Platform Configura	ation	
System Event Log		System Error Enable/Disable setup options.
System Errors RAS Log Level System Memory Poison Viral Status Clear Viral Status Cloak Devhide registers from being accessible from OS System Cloaking FatalErrDebugHalt Mca Bank Warm Boot Clear Errors CrashLog Feature CrashLog Feature CrashLog Fon All Reset Shutdown Suppression • eMCA Settings • Whea Settings • Whea Settings • Memory Error Enabling • IIO Error Enabling • DOIS CrashLog Feature	[Enable] [MIN (BASIC_FLOW)] [Enable] [Disable] [Disable] [Disable] [Disable] [Enable] [Enable] [Disable] [Disable] [Disable]	<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit EF0: Evit</pre>

Version 2.22.1281 Copyright (C) 2022 AMI

System Error

IIO Error Enabing
 PCIe Error Enabling
 Error Control Setting

Enable/Disable setup options.

- RAS Log Level RAS Log setup options.
- System Memory Poison Enable/Disable System Memory Poison.
- Viral Status
 Enable/Disable Viral.
- Clear Viral Status
 Enable/Disable Clear Viral Status.
- Cloak Devhide registers from being accessible from OS Enable/Disable OS to access Devhide registers.
- System Cloaking When enabled, Corrected errors are masked from OS/SW visibility. This option is valid only when EMCA is enabled.
- FatalErrDebugHalt DEBUG loop for McBank Fatal error case ONLY. Warning: Enable this knob only in conjunction with ITP as thread will halt in Fatal error flow.
- Mca Bank Warm Boot Clear Errors Enable/Disable Mca Bank Warm Boot Clear Errors.
- CrashLog Feature

The feature helps collecting crash data from PMC SSRAM.

CrashLog On All Reset

Option to invoke CrashLog collection on all reset.

Shutdown Suppression

Configures Shutdown Suppression and Log MCA IERR Support.

eMCA Settings

Platform Configur	Aptio Setup – AMI ation	
System Event Log		Press <enter> to view or change the eMCA configuration.</enter>
System Errors RAS Log Level System Memory Poison Viral Status Clear Viral Status Cloak Devhide registers from being accessible from OS System Cloaking FatalErrDebugHalt Mca Bank Warm Boot Clear Errors CrashLog Feature CrashLog On All Reset Shutdown Suppression • eMCA Settings • Whea Settings • Whea Settings • Error Injection Settings • Memory Error Enabling • IIO Error Enabling • PCIE Error Enabling • Error Control Setting	[Enable] [MIN (BASIC_FLOW)] [Enable] [Disable] [Disable] [Disable] [Disable] [Enable] [Enable] [Disable] [Disable] [Disable]	<pre>++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
Version	2.22.1281 Copyright (C) 2	2022 AMI

Platform Conf.	Aptio Setup – AMI iguration	
Platform Conf: eMCA Settings EMCA Logging Support LMCE Support Ignore OS EMCA Opt-in EMCA CMCI-SMI Morphing EMCA CMCI-SMI Threshold CSMI Dynamic Disable EMCA MCE-SMI Enable Corrected Error eLog Memory Error eLog Processor Error eLog Ubox Error Mask	[Enable] [Enable] [Disable] [EMCA gen 2 CSMI] 0 [Emable] [EMCA gen 2 - MSMI] [Enable] [Enable] [Enable] [Disable] [Disable]	Enable/Disable EMCA Logging ++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

- EMCA Logging Support Enable/Disable EMCA Logging.
- LMCE Support Enable/Disable Local MCE firmware support.
- Ignore OS EMCA Opt-in Enable/Disable Ignore OS EMCA Opt-in and log.
- EMCA CMCI-SMI Morphing Enable/Disable EMCA CSMI.
- EMCA CMCI-SMI Threshold Set the threshold of correctable error for signaling CMCI-CSMI.
- CSMI Dynamic Disable [Enable]:BIOS disables CSMI when error threshold reached.[Disabled]: CSMI always on.
- EMCA MCE-SMI Enable Enable/Disable EMCA Uncorrected SMI for gen2.
- Corrected Error eLog
 Enable/Disable Corrected Error eLog.
- Memory Error eLog Enable/Disable Memory Error eLog.
- Processor Error eLog
 Enable/Disable Processor Error eLog.
- Ubox Error Mask Mask SMI generation for Ubox Error.

WHEA Settings

Aptio Setup – AMI Platform Configuration				
System Event Log		Press <enter> to view or change the WHEA configuration.</enter>		
System Errors RAS Log Level System Memory Poison Viral Status Clear Viral Status Clear Viral Status Cloak Devhide registers from being accessible from OS System Cloaking FatalErrDebugHalt Mca Bank Warm Boot Clear Errors CrashLog Feature CrashLog On All Reset Shutdown Suppression • eMCA Settings • Hhea Settings • Hhea Settings • Error Injection Settings • Memory Error Enabling • TIO Error Enabling • PCIE Error Enabling • Error Control Setting	[Enable] [MIN (BASIC_FLOW)] [Enable] [Disable] [Disable] [Disable] [Disable] [Enable] [Enable] [Disable] [Disable] [Disable]	++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit		
Version	2.22.1281 Copyright (C) :	2022 AMI		



WHEA Support Enable/Disable WHEA support.

 WHEA Log Memory Error Enable/Disable Whea Log Memory Error.

- WHEA Log Processor Error Enable/Disable Whea Log Processor Error.
- WHEA Log PCI Error Enable/Disable Whea Log PCI Error.

Error Injection Setting

Aptio Setup – AMI Platform Configuration				
System Event Log		Press <enter> to view or change the Error Injection configuration.</enter>		
System Errors RAS Log Level System Memory Poison Viral Status Clear Viral Status Cloak Devhide registers from being accessible from OS System Cloaking FatalErrDebugHalt	[Enable] [MIN (BASIC_FLOW)] [Enable] [Disable] [Disable] [Disable] [Disable] [Enable] [Enable] [Disable] [Disable]			
 Mica Bank Marmi Boot Clear Errors CrashLog Feature CrashLog On All Reset Shutdown Suppression eMCA Settings Whea Settings Error Injection Settings Memory Error Enabling IIO Error Enabling PCIE Error Enabling Error Control Setting 		<pre>++: Select Screen fl: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>		
Version	2.22.1281 Copyright (C) 2022	AMI		

Aptio Setup - Platform Configuration	AMI		
Error Injection Settings	Enable/Disable WHEA Error Injection Support		
WHEA Error Injection Support [Disable]			
	<pre>++: Select Screen fl: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>		
Version 2.22.1281 Copyright (C) 2022 AMI			

WHEA Error Injection Support

Finable (Disable W/UEA Error Injection Sup

Enable/Disable WHEA Error Injection Support.

Memory Error Enabling

Aptio Setup – AMI Platform Configuration				
Platform Configura System Event Log System Errors RAS Log Level System Memory Poison Viral Status Clear Viral Status Clear Viral Status Cloak Devhide registers from being accessible from OS System Cloaking FatalErrDebugHalt Mca Bank Warm Boot Clear Errors CrashLog Feature CrashLog On All Reset Shutdown Suppression PeMCA Settings Whena Settings Error Injection Settings	Aptio Setup - AMI tion [Enable] [MIN (BASIC_FLOW)] [Enable] [Disable] [Disable] [Disable] [Disable] [Enable] [Enable] [Enable] [Disable] [Disable] [Disable] [Disable]	Press <enter> to view or change the Memory errors enabling options.</enter>		
 Memory Error Enabling IIO Error Enabling PCIE Error Enabling Error Control Setting 		F3: Uptimized Defaults F4: Save & Exit ESC: Exit		
Version 2.22.1281 Copyright (C) 2022 AMI				
Aptio Setup – AMI Platform Configuration				



- Memory Error Enable/Disable Memory Error.
- Memory Corrected Error Enable/Disable Memory Corrected Error.
- Spare Interrupt Spare Interrupt Selection.
IIO Error Enabling

Platform Configura	Aptio Setup – AMI tion	
System Event Log 	[Enable] [MIN (BASIC_FLOW)] [Fnable]	Press <enter≻ or<br="" to="" view="">change the IIO errors enabling options.</enter≻>
Viral Status Clear Viral Status Cloak Devhide registers from being accessible from OS System Cloaking FatalErrDebugHalt	[Enable] [Disable] [Disable] [Disable] [Disable]	
MCa Bank Warm Boot Clear Errors CrashLog Feature CrashLog On All Reset Shutdown Suppression ► eMCA Settings ► Whea Settings ► Error Injection Settings	[Enable] [Enable] [Disable] [Disable]	<pre>++: Select Screen 1↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values</pre>
 Memory Error Enabling IIO Error Enabling PCIE Error Enabling Error Control Setting 		F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version	2.22.1281 Copyright (C) 2022	2 AMI

Platform Configura	Aptio Setup – AMI tion	
IIO Error Enabling		Enable/Disable IIO/PCH Error Support.
IIO/PCH Global Error Support Os Native AER Support IIO MCA Support Clear PCC for IIO Non-Fatal Error IIO Error PinO Enable IIO 00B Mode IIO Error Registers Clear IIO eDPC Support IIO Coherent Interface Error IIO IRPO protocol parity error IIO IRPO protocol qt overflow underflow error IIO IRPO protocol rcvd unexprsp IIO IRPO protocol rcvd unexprsp IIO IRPO protocol rcvd unexprsp IIO IRPO wrcache unceccs0 error IIO IRPO wrcache unceccs1 error IIO IRPO wrcache correccs0 error IIO IRPO wrcache correccs1 error IIO Vtd Error	<pre>[Enable] [Disable] [Enable] [Enable] [Disable] [Enable] [Enable] [Enable] [Enable] [Enable] [Enable] [Enable] [Enable] [Enable] [Enable] [Enable] [Enable] [Enable] [Enable] [Enable] [Enable] [Enable]</pre>	<pre>++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
Version	2 22 1281 Copupidbt (C) 202	2 AMT

Platform Configura	Aptio Setup – AMI tion	
Platform Configura IID IRPO protocol qt overflow underflow error IID IRPO protocol rcvd unexprsp IID IRPO csr acc 32b unaligned IID IRPO wrcache unceccs0 error IID IRPO wrcache unceccs1 error IID IRPO wrcache correccs0 error IID IRPO wrcache correccs1 error IID IRPO wrcache correccs1 error IID IRPO wrcache correccs1 error IID Misc. Error IID Misc. Error IID Misc. Error IID Dama Error IID Dama Error IID PCIE Additional Corrected Error IID PCIE Additional Received Completion With UR IID PCIE Additional Received Completion With UR IID PCIE Additional Prors PSF UR Error PMSB Router Parity Error	tion [Enable] [Disable] [Disable] [Enable] [Enable] [Enable] [Enable] [Disable] [Enable] [Ena	 Enable/Disable PMSB Router Parity Error ++: Select Screen tl: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

- IIO/PCH Global Error Support Enable/Disable IIO/PCH Error Support.
- OS Native AER Support
 Select FFM or OS native for AER error handling. If select OS native, BIOS also initialize FFM first until handshake, which depends on OS capability.
- IIO MCA Support
 Enable/Disable IIO MCA Support.
- Clear PCC for IIO Non-Fatal Error
 Enable/Disable PCC equal 0 for IIO severity 1 error.
- IIO Error Pin0 Enable
 Enable/Disable IIO Error Pin0
- IIO OOB Mode
 Enable/Disable System Event Generation when Error Pin is enabled.
- IIO Error Registers Clear
 Enable/Disable Clear IIO Error Registers.
- IIO eDPC Support
 Enable/Disable IIO eDPC Support.
- IIO Coherent Interface Error Enable/Disable IIO Coherent Interface Error.
- IIO IRP0 protocol parity error
 Enable or disable Coherent Interface protocol IIO parity error reporting.
- IIO IRP0 protocol qt overflow underflow error
 Enable or disable IIO Coherent Interface protocol queue table overflow or underflow error reporting.
- IIO IRP0 protocol rcvd unexprsp Enable or disable IIO Coherent Interface protocol layer received unexpected response or completion error reporting.

- IIO IRP0 csr acc 32b unaligned
 Enable or disable IIO Coherent Interface CSR Access Crossing 32-bit
 Boundary error reporting.
- IIO IRP0 wrcache uncecccs0 error / IIO IRP0 wrcache uncecccs1 error Enable or disable IIO Coherent Interface Write Cache Un-correctable ECC error reporting.
- IIO IRP0 protocol rcvd poison error
 Enable or disable IIO Coherent Interface Protocol Layer Received Poisoned
 Packet error reporting.
- IIO IRP0 wrcache correcccs0 error / IIO IRP0 wrcache correcccs1 error Enable or disable IIO Coherent Interface Write Cache Correctable ECC error reporting.
- IIO Misc. Error Enable/Disable IIO Misc. Error.
- IIO Vtd Error
 Enable/Disable IIO Vtd Error.
- IIO Dma Error
 Enable/Disable IIO Dma Error.
- IIO Dmi Error Enable/Disable IIO Dmi Error.
- PCIE Error Enable/Disable PCIE Error.
- IIO PCIE Additional Corrected Error Enable/Disable IIO PCIE Additional Corrected Error.
- IIO PCIE Additional Uncorrected Error Enable/Disable IIO PCIE Additional Uncorrected Error.
- IIO PCIE Additional Received Completion With UR Enable/Disable IIO PCIE Additional Received Completion with UR.
- IIO PCIE AER Spec Compliant
 Enable/Disable IIO PCIE AER Spec Compliant.
- ITC/OTC CA/MA Errors
 Enable/Disable Completer Abort and Master Abort (Unsupported Request) on ITC and OTC.
- PSF UR Error Enable/Disable Unsupported Request Error on PSF.
- PMSB Router Parity Erro Enable/Disable PMSB Router Parity Error.

PCle Error Enabling

System Event Log		Press <enter> to view or change the PCIe errors</enter>
System Errors RAS Log Level System Memory Poison Viral Status Clear Viral Status Cloak Devhide registers from being accessible from OS System Cloaking FatalErrDebugHalt Mca Bank Warm Boot Clear Errors CrashLog Feature CrashLog On All Reset Shutdown Suppression • eMCA Settings • Whea Settings • Whea Settings • Memory Error Enabling • IIO Error Enabling • PCIE Error Enabling • Error Control Settings	[Enable] [MIN (BASIC_FLOW)] [Enable] [Disable] [Disable] [Disable] [Enable] [Enable] [Disable] [Disable] [Disable]	<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>

Platform Configura	Aptio Setup – AMI tion	
PCIe Error Enabling		Enable & escalate Correctable
Corrected Error	[Enable]	
Uncorrected Error	[Enable]	
Fatal Error Enable	[Enable]	
PCIE Corrected Error Threshold	[Disable]	
Counter		
PCIe Corrected Error Limit Check	[Disable]	
PCIe Corrected Error Limit	80	
PCIE AER Corrected Errors	[Enable]	
PCIE AER NonFatal Error	[Enable]	
PCIE AER Fatal Error	[Enable]	
PCIE AER Advisory Nonfatal Error	[Enable]	++: Select Screen
PCIE Unsupported Request Error	[Disable]	î∔: Select Item
PCIE Surprise Link Down Error	[Disable]	Enter: Select
Assert NMI on SERR	[Enabled]	+/-: Change Opt.
Assert NMI on PERR	[Enabled]	F1: General Help
		F2: Previous Values
Leaky Bucket Feature		F3: Optimized Defaults
Expected BER	34359738367	F4: Save & Exit
Time Window (Gen1/2)	65535	ESC: Exit
Time Window (Gen3/4)	2	
Error Threshold (Gen1/2)	0	
Error Threshold (Gen3/4)	16	• •
	0.00.4004.Comuniatión (0)	2000 ANT

	Aptio Setup – AMI	
Platform Configura	tion	
Fatal Error Enable PCIE Corrected Error Threshold Counter PCIE Corrected Error Limit Check PCIE Corrected Error Limit PCIE AER Corrected Errors PCIE AER NonFatal Error PCIE AER Fatal Error PCIE AER Fatal Error PCIE AER Fatal Error PCIE Unsupported Request Error PCIE Surprise Link Down Error Assert NMI on SERR	[Enable] [Disable] (Disable] 80 [Enable] [Enable] [Enable] [Enable] [Disable] [Disable] [Enable]	Enable or disable Gen4 link degradation. Applies only when operating at Gen4 speeds. When an event is triggered, 16GT/s and higher modes are disabled.
Assert NMI on PERR Leaky Bucket Feature Expected BER Time Window (Gen1/2) Time Window (Gen3/4) Error Threshold (Gen3/4) Gen3/4 Re-Equalization Gen2 Link Degradation Gen3 Link Degradation Gen4 Link Degradation	[Enabled] 34359738367 65535 2 0 16 [Enable] [Enable] [Enable] [Enable]	<pre>++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
Version	2.22.1281 Copyright (C) 2022	AMI

- Corrected Error
 Enable & escalate Correctable Errors to error pins.
- Uncorrected Error
 Enable & escalate Uncorrectable/Recoverable to error pins.
- Fatal Error Enable
 Enable & escalate fatal errors to error pins.
- PCIE Corrected Error Threshold Counter Enable/Disable PCIE Corrected Error Counter.
- PCle Corrected Error Limit Check
 Enable/Disable the feature to disable reporting PCle corrected errors for a device if they exceed a given limit.
- PCle Corrected Error Limit
 Set the maximum number of corrected errors before corrected error reporting is disabled for a device.
- PCIE AER Corrected Errors
 Enable/Disable PCIE AER Corrected Errors.
- PCIE AER NonFatal Error
 Enable/Disable PCIE AER NonFatal Error.
- PCIE AER Fatal Error
 Enable/Disable PCIE AER Fatal Error.
- PCIE AER Advisory Nonfatal Error Enable/Disable PCIE AER Advisory Nonfatal Error.
- PCIE Unsupported Request Error Enable/Disable PCIE Unsupported Request Error.
- PCIE Surprise Link Down Error Enable/Disable PCIE Surprise Link Down Error.
- Assert NMI on SERR
 On SERR, generate an NMI and log an error. Note: [Enabled] must be selected for the Assert NMI on PERR setup option to be visible.

Assert NMI on PERR

On PERR, generate an NMI and log an error. Note: This option is only active if the Assert NMI on SERR option has [Enabled] selected.

– Expected BER

Set the expected Bit Error Rate for all speeds.

- Time Window (Gen1/2)

Set the error burst protection time window for Gen1 and Gen2 speeds. A burst of errors within the window is counted as one.

- Time Window (Gen3/4)

Set the error burst protection time window for Gen3 and Gen4 speeds. A burst of errors within the window is counted as one.

Error Threshold (Gen1/2)

Set the error threshold for Gen1 and Gen2 speeds. An event is triggered when the error count exceeds the threshold.

Error Threshold (Gen3/4)

Set the error threshold for Gen3 and Gen4 speeds. An event is triggered when the error count exceeds the threshold.

- Gen3/4 Re-Equalization

Enable or disable Gen3 and Gen4 re-equalization. Applies only when operating at Gen2 or Gen4 speeds. When an event is triggered, equalization is rerun.

- Gen2 Link Degradation

Enable or disable Gen2 link degradation. Applies only when operating at Gen2 speeds. When an event is triggered, 5GT/s and higher modes are disabled.

- Gen3 Link Degradation

Enable or disable Gen3 link degradation. Applies only when operating at Gen3 speeds. When an event is triggered, 8GT/s and higher modes are disabled.

- Gen4 Link Degradation

Enable or disable Gen4 link degradation. Applies only when operating at Gen4 speeds. When an event is triggered, 16GT/s and higher modes are disabled.

Error Control Setting

Platform Configur	Aptio Setup – AMI ation	
System Event Log		Press <enter> to view or change the Error Control Setting options.</enter>
System Errors RAS Log Level System Memory Poison Viral Status Clear Viral Status Clear Viral Status Cloak Devhide registers from being accessible from OS System Cloaking FatalErrDebugHalt Mca Bank Warm Boot Clear Errors CrashLog On All Reset Shutdown Suppression Error Injection Settings Whea Settings Error Injection Settings Memory Error Enabling FIIO Error Enabling FCIE Error Enabling Error Control Setting	[Enable] [MIN (BASIC_FLOW)] [Enable] [Disable] [Disable] [Disable] [Disable] [Enable] [Enable] [Disable] [Disable] [Disable]	<pre>**: Select Screen fl: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
Version	2.22.1281 Copyright (C)	2022 AMI

Platform Configurat	Aptio Setup – AMI ion	
Error Control Setting		Enable or disable latch first corrected error in KTI.
Latch First Corrected Error in KTI Patrol Scrub Error Reporting	(Enable) [UCNA]	┿: Select Screen 1↓: Select Item
		Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2	.22.1281 Copyright (C) 2022	AMI

- Latch First Corrected Error in KTI Enable or disable latch first corrected error in KTI.
- Patrol Scrub Error Reporting Patrol Scrub Error type selection.

3.2.3.4 Intel(R) Time Coordinated Computing





Software SRAM

Enable or Disable Software SRAM. Enable will allocate 1 way of LLC; if Cache Configuration subregion is available, it will allocate based on the subregion.

Data Streams Optimizer

Enable or Disable Data Streams Optimizer (DSO). Enable will utilize DSO Sub-

region to tune system. DSO settings supercede Intel(R) TCC Mode settings that overlap between the two.

- TCC Error Log Enable or Disable TCC Error Log. Enable will record errors from TCC flow in memory.
- Wake System From S5 Enable or disable System wake on alarm event. Select Fixed Time, system will wake on the hr::min::sec specified.

3.2.4 Socket Configuration

3.2.4.1 Processor Configuration

Apti Main Advanced Platform Configuration	o Setup – AMI ocket Configuration Server Mgmt Security Boot I
 Processor Configuration Memory Configuration IIO Configuration Advanced Power Management Configuration 	Displays and provides option to change the Processor Settings
	++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.22.12	83 Copyright (C) 2022 AMI

Aptio Setup – AMI Socket Configuration		
Processor Configuration Processor BSP Revision Processor Socket Processor ID	606C0 – ICX–D A0 Socket 0 Socket 1 000606C0*	Enables Hyper Threading (Software Method to Enable/Disable Logical Processor threads.
Processor Frequency Processor Max Ratio Processor Min Ratio Microcode Revision L1 Cache RAM(Per Core) L2 Cache RAM(Per Core) L3 Cache RAM(Per Package)	1.600GHZ 10H 08H FD0001D0 80KB 1280KB 10240KB	
Processor O Version Hyper-Threading [ALL] Check CPU BIST Result	Intel(R) Genuine proces sor [Enable] [Enabled]	<pre>++: Select Screen f↓: Select Item Enter: Select +/-: Change Opt. F1: General Help E2: Previous Values</pre>
		F3: Optimized Defaults F4: Save & Exit ESC: Exit
Vers:	ion 2.22.1281 Copyright (C) 202	22 AMI

- Hyper-Threading Enable or Disable Hyper-Threading Technology.
- Check CPU BIST Result Enable/Disable BIST (Built-in Self Test) on reset.

3.2.4.2 Memory Configuration



	Aptio Setup – AMI Socket Configu	ration
Integrated Memory Controller (Memory Frequency Memory Topology	iMC) [Auto]	Maximum Memory Frequency Selections in Mhz. If Enforce POR is disabled, user will be able to run at higher frequencies than the memory support (limited by processor support). Do not select Reserved
		<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
Ver	sion 2.22.1283 Copyright Aptio Setup – AMI Socket Configu	(C) 2022 AMI : : ration
DIMMAO Populat Size 8192MB Number of Ranks 2 Manufacturer Ox O	ed & Enabled	
		<pre>++: Select Screen 1↓: Select Item Enter: Select</pre>

Memory Frequency

Maximum Memory Frequency Selections in Mhz. If Enforce POR is disabled, user will be able to run at higher frequencies than the memory support (limited by processor support). Do not select Reserved.

3.2.4.3 IIO Configuration



	Aptio Setup – AMI Socket Configuration	
IIO Configuration		All IIO performance tuning configuration options
▶ IIO Global Performance Tuning		
IIO-PCIE Express Global Options PCIE Train by BIOS NTB Link Train by BIOS Delay before link training PCIE Hot Plug Mask PCIE RP warm reset MCA PCIE Low Latency Retimers Skip PCIE retimers detection PCI Completion Timewat	<pre>==== [Yes] [Auto] [No delay] [No] [Enable] [No] [No] [Olobel]</pre>	++: Select Screen
PCI-E Completion Timeout PCI-E Completion Timeout PCI-E ASPM Support (Global) Snoop Response Hold Off PCIe LTR Support PCIE Extended Tag Support PCIE 10-bit Tag Support PCIE Atomic Op Support PCIE Max Read Request Size PCIE PTM Support PCIE Relaxed Ordering	[2600s to 900ms] [Per-Port] 9 [Auto] [Auto] [Auto] [Auto] [4096B] [Auto] [Yes]	Enter: Select Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.	.22.1283 Copyright (C) 2022	AMI

PCIe Train by BIOS

Assume IIO is strapped for Wait-for-BIOS because straps are unreliable in A-0 Silicon.

NTB Link Train by BIOS

This knob enables or disables the BIOS to train the NTB link.

- Delay before link training Custom delay before PCIe link training on IIO ports.
- PCIe Hot Plug Enable/Disable PCIe Hot Plug globally.
- Mask PCIe RP warm reset MCA Enable/Disable Mask CPU Complex PCIe Root Port warm reset MCA.
- PCIe ACPI Hot Plug Enable/Disable PCIe ACPI Hot Plug globally, or allow per-port control. When Disabled, MSI is generated on HP event. When Enabled, _HPGPE message is generated.
- PCIe Low Latency Retimers
 Enable/Disable PCIe low latency retimers.
- Skip PCIe retimers detection Skip PCIe retimers detection to speedup the boot. Retimers are preent only in specific HW configurations.
- PCI-E Completion Timeout Enable/disable the PCIe Completion Timeout in Device Control2 register.
- PCI-E Completion Timeout
 PCIe Completion Timeout to program in Device Control2 register.
- PCI-E ASPM Support (Global) This option enables/disables the ASPM support for all downstream devices.
- Snoop Response Hold Off Sets Snoop Response Hold Off value, 256 cycles as Default.

PCIe LTR Support

This option can disable Latency Tolerance Reporting support in all PCIe root ports. 'Auto' keeps hardware default.

PCIe Extended Tag Support This option can disable 8-bit Tag support in all PCIe re

This option can disable 8-bit Tag support in all PCIe root ports. 'Auto' keeps hardware default.

PCle 10-bit Tag Support This option can disable PCIe 10-bit Tag Requester support in all PCIe root ports. 'Auto' keeps hardware default.

PCle Atomic Op Support
 This option can disable Atomic Operation Routing support in all PCIe root ports and block Atomic Operation Requester in PCI hierarchy. 'Auto' keeps hardware default.

 PCle Max Read Request Size

Set Max Read Request Size in EndPoints.

PCIe PTM Support
 This option can disable Precision Time Management support in PCI hierarchy.
 'Auto' keeps hardware default.

PCle Relaxed Ordering

Enable Relaxed Ordering in PCIe devices where it is supported. Note that in some devices it can be not supported, hardwired to zero.

IIO Global Performance Tuning



- Performance Tuning Mode

Select IIO performance tuning mode, where Safe mode contains the default HW state and Performance Enable Mode has the recommended performance values.

3.2.4.4 Advanced Power Management Configuration



CPU P State Control

Aptic So	Setup – AMI sket Configuration
Advanced Power Management Configuration > CPU P State Control > CPU C State Control > Package C State Control	P State Control Configuration Sub Menu, include Turbo, XE and etc.
	++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.22.128	1 Copyright (C) 2022 AMI

	Apti S	<mark>lo Setup – AMI</mark> Gocket Configuration <mark>–</mark>	
CPU P State Control			Enables AVX ICCP pre-grant
AVX Licence Pre-Grant Overr SpeedStep (Pstates) AVX P1 Dynamic SST-PP Intel SST-PP	ride (Disa [Enab [Norm [Disa [Base	able] ole] nal] able] ?]	
Intel SST-PP Bas Core Count 10 Current P1 Ratio [0] 20 Package TDP (W) 067 Tjmax 102	se Config 3 0 10 0 15 7 056 2 102	Config 4 10 15 056 102	
Activate SST-BF Configure SST-BF EIST PSD Function Boot performance mode Energy Efficient Turbo Turbo Mode CPU Flex Ratio Overnide CPU Core Flex Ratio GPSS timer ▶ Perf P-Limit	[Disa [Enab [HW_A [Max [Enab [Disa 23 [Soo	us]	<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
	Version 2.22.12	283 Copyright (C) 2022	AMI

- AVX Licence Pre-Grant Override
 Enables AVX ICCP pre-grant level over
 - Enables AVX ICCP pre-grant level override.
- SpeedStep (Pstates) Enable/Disable EIST (P-States).
- Config TDP Lock
 Config TDP CONTROL Lock Bit.
- AVX P1

AVX P1 level selection.

- Dynamic SST-PP

Support Dynamic SST-PP Select. NOTE: Disable:Static SST-PP can be displayed.

- Intel SST-PP
 Intel SST-PP Select allows user to choose from up to two additional base frequency conditions.
- Activate SST-BF
 This Option allows SST-BF to be enabled.
- EIST PSD Function

Choose HW_ALL/SW_ALL in _PSD return.

- Boot performance mode
 Select the performance state that the BIOS will set before OS hand off.
- Energy Efficient Turbo
 Energy Efficient Turbo Disable, MSR 0x1FC [19].
- Turbo Mode
 Enable/Disable processor Turbo Mode (requires EMTTM enabled too).
 ODU Flass Detite Occurrida
- CPU Flex Ratio Override Enable/Disable CPU Flex Ratio Programming.
- GPSS timer
 P-state change hysteresis time window.

Perf P-Limit Program PERF_P_LIMIT 1:30:2:0xe4 Sub Menu.

	Aptio Setup – AMI Socket Configuration	
Perf P-Limit Perf P-Limit Differential Perf P-Limit Clip Perf P-Limit Threshold Perf P Limit	1 1F F [Enable]	Parameter used to tune how far below local socket frequency remote socket frequency is allowed to be. Also impacts rate at which frequency drops when feature disengages.
		<pre> ++: Select Screen f↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
Version :	2.22.1281 Copyright (C) 2022	AMI

- Perf P-Limit Differential

Parameter used to tune how far below local socket frequency remote socket frequency is allowed to be. Also impacts rate at which frequency drops when feature disengages.

- Perf P-Limit Clip Maximum value the floor is allowed to be set to for perf P-limit.
- Perf P-Limit Threshold

Uncore frequency threshold above which this socket will trigger the feature and start trying to raise frequency of other sockets.

Perf P Limit
 Enable/Disable Performance P-Limit.

CPU C State Control



	Aptio Setup – AMI Socket Configuration	
CPU C State Control		Allows Monitor and MWAIT
Enable Monitor MWAIT CPU C1 auto demotion CPU C1 auto undemotion CPU C6 report Enhanced Halt State (C1E) OS ACPI Cx	[Enable] [Enable] [Auto] [Auto] [Enable] [ACPI C2]	
		++: Select Screen f: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version	2.22.1281 Copyright (C) 202	2 AMI

- Enable Monitor MWAIT

Allows Monitor and MWAIT instructions.

CPU C1 auto demotion
 Allows CPU to automatically demote to C1. Takes effect after reboot.

- CPU C1 auto undemotion
 Allows CPU to automatically undemote from C1. Takes effect after reboot.
- CPU C6 report
 Enable/Disable CPU C6(ACPI C3) report to OS.
- Enhanced Halt State (C1E)
 Core C1E auto promotion Control. Takes effect after reboot.
- OS ACPI Cx
 Report CC3/CC6 to OS ACPI C2 or ACPI C3.

Package C State Control

Aptio Setup - 6 Socket Conf.	aMI iguration
Advanced Power Management Configuration	Package C State setting
 CPU P State Control CPU C State Control Package C State Control 	
	<pre> ++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
Version 2.22.1281 Copyrig	nt (C) 2022 AMI



- Package C State

Package C State limit.

- Register Access Low Latency Mode
 Enable lower latency mode for register accesses. Note: Enabling this mode
 will prevent PkgC6 as register access fabric is prevented from going into idle.
- C2C3TT
 Default = 0, means [AUTO]. C2 to C3 Transition Timer, PPDN_INIT = 1:10:1:74 Bit[11:0].
- Dynamic L1
- PCU_MISC_CONFIG Bit[21] = dynamic L1 enable. - **PKG C-state Lat. Neg**

MSR 1FCh Bit[30] = PCH_NEG_DISABLE.

- LTR IIO Input

MSR 1FCh Bit[29] = LTR_IIO_DISABLE. Disable = Ignore IIO LTR input.

Chapter 3 BIOS Settings

3.2.5 Server Management

Main Advanced Platform	Aptio Setup – AMI Configuration Socket Configuration	Server Mømt Security Boot
BMC Self Test Status BMC Device ID BMC Device Revision BMC Firmware Revision IPMI Version IPMI BMC Interface BMC Support FRB-2 Timer FRB-2 Timer timeout FRB-2 Timer Policy OS Watchdog Timer	FAILED Unknown Unknown Unknown Unknown Unknown (Enabled) (Enabled) 6 [Do Nothing] [Disabled]	Enable/Disable interfaces to communicate with BMC
US WTO limer limeout OS Wto Timer Policy System Event Log BMC self test log BMC network configuration View System Event Log BMC User Settings	lU [Reset]	<pre>++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
	Version 2.22.1281 Copyright (C) 202	2 AMI

BMC Support

Enable/Disable interfaces to communicate with BMC.

- FRB-2 Timer Enable or Disable FRB-2 timer (POST timer).
- FRB-2 Timer timeout Enter value Between 1 to 30 min for FRB-2 Timer Expiration.
- FRB-2 Timer Policy
 Configure how the system should respond if the FRB-2 Timer expires. Not available if FRB-2 Timer is disabled.

 OS Watchdog Timer

OS Watchdog Timer If enabled, starts a BIOS timer which can only be shut off by Management Software after the OS loads. Helps determine that the OS successfully loaded or follows the OS Boot Watchdog Timer policy.

OS Wtd Timer Timeout
 Enter the value Between 1 to 30 min for OS Boot Watchdog Timer Expiration.
 Not available if OS Boot Watchdog Timer is disabled.

OS Wtd Timer Policy Configure how the system should respond if the OS Boot Watchdog Timer expires. Not available if OS Boot Watchdog Timer is disabled.

3.2.5.1 System Event Log

Main Advanced Platform	Aptio Setup – AMI Configuration Socket Configuration	Server Mgmt Security Boot D
BMC Self Test Status BMC Device ID BMC Device Revision BMC Firmware Revision IPMI Version IPMI BMC Interface BMC Support FRB-2 Timer FRB-2 Timer timeout FRB-2 Timer Policy OS Watchdog Timer OS Wtd Timer Timeout OS Wtd Timer Policy System Event Log BMC self test log BMC network configuration View System Event Log BMC User Settings	FAILED Unknown Unknown Unknown Unknown [Enabled] [Enabled] 6 [Do Nothing] [Disabled] 10 [Reset]	Press <enter> to change the SEL event log configuration. ++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</enter>
	Version 2.22.1281 Copyright (C) 2022	AMI

	Aptio Setup – AMI	Server Mgmt
Enabling/Disabling Options SEL Components	[Enabled]	Change this to enable or disable event logging for error/progress_codes_during
Erasing Settings Erase SEL When SEL is Full	[No] [Do Nothing]	boot.
Custom EFI Logging Options Log EFI Status Codes	[Error code]	
NOTE: All values changed here do not effect until computer is resta	t take arted.	
		↔: Select Screen t↓: Select Item Enter: Select
		+/-: Change Opt. F1: General Help F2: Previous Values
		F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2	2.22.1281 Copyright (C) 2022	2 AMI

SEL Components

Enable/Disable all features of system event logging during boot.

Erase SEL Choose options for erasing SEL.

When SEL is Full

Choose options for reactions to a full SEL.

Log EFI Status Codes

Disable the logging of EFI status codes, or log only error codes, or only progress codes, or both.

3.2.5.2 BMC Self Test Log



	Aptio Setup – AMI	Server Mømt
Log area usage = 02 out of 20 logs Erase Log	[Yes, On every reset]	Erase Log Options
When log is full DATE TIME STATUS CODE 01/01/2021 23:03:46 BMC communicat 01/01/2021 23:03:46 BMC hard fail	[Clear Log] ion error	
		<pre>++: Select Screen f↓: Select Item Enter: Select +/-: Change Opt. F1: General Help</pre>
		F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2	.22.1281 Copyright (C) 2022	AMI

Erase Log Erase log options.

When Log is Full Select the action to be taken when log is full.

3.2.5.3 BMC Network Configuration

BMC Self Test Status BMC Device ID BMC Device Revision IPMI Version IPMI BMC Interface BMC Support FRB-2 Timer FRB-2 Timer timeout FRB-2 Timer Policy OS Watchdog Timer OS Watchdog Timer	FAILED Unknown Unknown Unknown Unknown [Enabled] [Enabled] 6 [Do Nothing] [Disabled]	Configure BMC network parameters
OS Wtd Timer Policy > System Event Log > Bmc self test log > BMC network configuration > View System Event Log > BMC User Settings	[Reset]	++: Select Screen f4: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

	Aptio Setup – AMI	
		Server Mgmt
BMC network configuration жижноноконоконоконоконо Configure IPv4 support жижноноконоконоконоконоконок		 Select to configure LAN channel parameters statically or dynamically(by BIOS or BMC). Unspecified option will not modify any BMC network
Lan channel 1 Configuration Address source Current Configuration Address source Station IP address Subnet mask Station MAC address	[Unspecified] - -	parameters during BIOS phase
Router IP address Router MAC address жожножножножножножнож Configure IPv6 support жожножножножножножножножно	-	++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help E2: Previous Values
Lan channel 1		F3: Optimized Defaults F4: Save & Exit
IPv6 Support	[Enabled]	ESC: Exit
Configuration Address source	[Unspecified]	
Versio	n 2.22.1281 Copyright (C)	2022 AMI

Configuration Address Source

Select to configure LAN channel parameters statically or dynamically (by BMC). Unspecified option will not modify any BMC network parameters during BIOS phase.

3.2.5.4 View System Event Log



If any event logs occur during boot up, the event logs will be display at this page.

3.2.5.5 BMC User Settings

Main Advanced Platform	Aptio Setup – AMI Configuration Socket Configuration	Server Mgmt <u>Security Boot</u>
 BMC Self Test Status BMC Device ID BMC Device Revision BMC Firmware Revision IPMI Version IPMI BMC Interface BMC Support FRB-2 Timer timeout FRB-2 Timer Policy OS Watchdog Timer OS Wtd Timer Timeout OS Wtd Timer Policy System Event Log BMC network configuration View System Event Log BMC User Settings 	FAILED Unknown Unknown Unknown Unknown [Enabled] [Enabled] 6 [Do Nothing] [Disabled] 10 [Reset]	Press <enter> to Add, Delete and Set Privilege level for users. ++: Select Screen fl: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</enter>
	Version 2.22.1281 Copyright (C) 2022	AMI

Aptio Setup — AMI	Server Mgmt
BMC User Settings	Press <enter> to Add a User.</enter>
▶ Add User	
▶ Delete User	
▶ Change User Settings	<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
Version 2.22.1281 Copyright (C) 2022 AMI

- Add User Add user information.
- Delete User
 Delete user information.
- Change User Settings Allow change User settings.

3.2.6 Security

Main Advanced Platform Configu	Aptio Setup – AMI ration Socket Configuration	Server Mgmt Security Boot I
Password Description		Set Administrator Password
If ONLY the Administrator's passu then this only limits access to S only asked for when entering Setu If ONLY the User's password is se is a power on password and must b boot or enter Setup. In Setup the have Administrator rights. The password length must be in the following range: Minimum length	ord is set, etup and is p. t, then this e entered to : User will 3	
Maximum length	20	++: Select Screen
Administrator Password		↑↓: Select Item
User Password ▶ Secure Boot		Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Versio	n 2.22.1281 Copyright (C) 202	2 AMI

Administrator Password Set Administrator Password.

User Password

Set User Password.

Aptio Se Main Advanced Platform Configuration Socke	t <mark>up – AMI</mark> t Configuration Server Mgmt <mark>Security Boot →</mark>
Password Description	Secure Boot configuration
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 Newime length 20	
Administrator Password User Password	<pre> ++: Select Screen fl: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
Version 2.22.1281 C	opyright (C) 2022 AMI

	Aptio Setup — AMI	Security
System Mode	Setup	Secure Boot feature is Active
Secure Boot	[Disabled] Not Active	Platform Key(PK) is enrolled and the System is in User mode. The mode change requires
Secure Boot Mode ▶ Restore Factory Keys ▶ Reset To Setup Mode	[Custom]	platform reset
▶ Key Management		
		<pre>++: Select Screen fl: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
	Version 2.22.1283 Copyright (C) 2	022 AMI

Secure Boot

Secure Boot feature is Active if Secure Boot is Enabled, Platform Key (PK) is enrolled and the System is in User mode. The mode change requires platform reset.

- Secure Boot Mode

Secure Boot mode options: Standard or Custom.

3.2.7 Boot



- Setup Prompt Timeout Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting.
- Bootup NumLock State Select the keyboard NumLock state.
- Quiet Boot Enables or disables Quiet Boot option.
- Boot Option
 Display and select boot devices.

3.2.8 Save & Exit

Aptio Setup - AMI ≺ Save & Exit	
 Save & Exit Save Options Save Changes and Exit Discard Changes and Reset Discard Changes and Reset Save Changes Discard Changes Default Options Restore Defaults Save as User Defaults Restore User Defaults Boot Overnide UEFI: JetFlashTS46JFV30 8.07, Partition 1 (JetFlashTS46JFV30 8.07) UEFI: Built-in EFI Shell 	Exit system setup after saving the changes. ++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2 22 1281 Populaidht (P) 2022	AMT
Version 2.22.1201 copyright (c) 2022	11111

Save Changes and Exit
Exit system setup after saving the changes.
Discard Changes and Exit
Exit system setup without saving any changes.
Save Changes and Reset
Reset the system after saving the changes.
Discard Changes and Reset
Reset system setup without saving any changes.
Save Changes
Save Changes done so far to any of the setup options.
Discard Changes
Discard Changes done so far to any of the setup options.
Restore Defaults
Restore/Load Default values for all the setup options.
Save as User Defaults
Save the changes done so far as User Defaults.
Restore User Defaults

Restore the User Defaults to all the setup options.



Watchdog Timer Sample Code

A.1 EC Watchdog Timer Sample Code

EC_Command_Port = 0x29Ah EC_Data_Port = 0x299h Write EC HW ram = 0x89 Watch dog event flag = 0x57Watchdog reset delay time = 0x5E Reset event = 0x04Start WDT function = 0x28 ______ .model small .486p .stack 256 .data .code org 100h .STARTup mov dx, EC Command Port mov al,89h ; Write EC HW ram. out dx.al mov dx, EC Data Port mov al, 5Fh; Watchdog reset delay time low byte (5Eh is high byte) index, Timebase: 100ms out dx,al mov dx, EC_Data_Port mov al, 64h ;Set 10 seconds delay time. out dx.al mov dx, EC_Command_Port mov al,89h ; Write EC HW ram. out dx,al mov dx, EC Data Port mov al, 57h ; Watch dog event flag. out dx.al mov dx, EC Data Port mov al, 04h ; Reset event. out dx,al mov dx, EC Command Port mov al,28h; start WDT function. (Stop: 0x29, Reset: 0x2A) out dx,al .exit END



www.advantech.com

Please verify specifications before quoting. This guide is intended for reference purposes only.

All product specifications are subject to change without notice.

No part of this publication may be reproduced in any form or by any means, electronic, photocopying, recording or otherwise, without prior written permission from the publisher.

All brand and product names are trademarks or registered trademarks of their respective companies.

© Advantech Co., Ltd. 2022