

User Manual

SOM-5992

Intel Xeon Processor D-1500 COM Express R3.0 Type 7 Module



Copyright

The documentation and the software included with this product are copyrighted 2017 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. 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, which may result from its use.

Acknowledgements

Intel is a trademark of Intel Corporation.

Microsoft Windows and MS-DOS are registered trademarks of Microsoft Corp. All other product names or trademarks are properties of their respective owners.

Product Warranty (2 years)

Advantech warrants to you, 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 which have been repaired or altered by persons other than repair personnel authorized by Advantech, or which 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 of our customers never need to use our repair service. If an Advantech product is defective, it will be repaired or replaced at no charge during the warranty period. For outof-warranty repairs, you will be billed according to the cost of replacement materials, service time and freight. Please consult your dealer for more details.

If you think you have a defective product, follow these steps:

- 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 onscreen messages you get when the problem occurs.
- 2. Call your dealer and describe the problem. Please have your manual, product, and any helpful information readily available.
- 3. If your product is diagnosed as defective, obtain an RMA (return merchandize authorization) number from your dealer. This allows us to process your return more quickly.
- 4. Carefully pack the defective product, a fully-completed Repair and Replacement Order Card and a photocopy proof of purchase date (such as your sales receipt) in a shippable container. A product returned without proof of the purchase date is not eligible for warranty service.
- 5. Write the RMA number visibly on the outside of the package and ship it prepaid to your dealer.

Part No. 2006599200 Printed in Taiwan Edition 1 November 2017

Declaration of Conformity

CE

This product has passed the CE test for environmental specifications. Test conditions for passing included the equipment being operated within an industrial enclosure. In order to protect the product from being damaged by ESD (Electrostatic Discharge) and EMI leakage, we strongly recommend the use of CE-compliant industrial enclosure products.

FCC Class B

Note: 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 instructions, 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 help.

FM

This equipment has passed the FM certification. According to the National Fire Protection Association, work sites are classified into different classes, divisions and groups, based on hazard considerations. This equipment is compliant with the specifications of Class I, Division 2, Groups A, B, C and D indoor hazards.

Technical Support and Assistance

- 1. Visit the Advantech website at http://support.advantech.com where you can find the latest information about the product.
- 2. Contact your distributor, sales representative, or Advantech's customer service center for technical support if you need additional assistance. Please have the following information ready before you call:
 - 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, which if not observed, can cause personal injury!





Caution! Cautions are included to help you avoid damaging hardware or losing data. e.g.

There is a danger of a new battery exploding if it is incorrectly installed. Do not attempt to recharge, force open, or heat the battery. Replace the battery only with the same or equivalent type recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions.

Note!

Notes provide optional additional information.

Document Feedback

To assist us in making improvements to this manual, we would welcome comments and constructive criticism. Please send all such - in writing to: support@advantech.com

Packing List

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

- SOM-5992 CPU module
- 1 x Heatspreader (1960073944N001)

Safety Instructions

- 1. Read these safety instructions carefully.
- 2. Keep this User Manual for later reference.
- 3. Disconnect this equipment from any AC outlet before cleaning. Use a damp cloth. Do not use liquid or spray detergents for cleaning.
- 4. For plug-in equipment, the power outlet socket must be located near the equipment and must be easily accessible.
- 5. Keep this equipment away from humidity.
- 6. Put this equipment on a reliable surface during installation. Dropping it or letting it 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. Make sure the voltage of the power source is correct before connecting the equipment to the power outlet.
- 9. Position the power cord so that people cannot step on it. 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 by transient overvoltage.
- 12. Never pour any 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 one of the following situations arises, get the equipment checked by service personnel:
 - The power cord or plug is damaged.
 - Liquid has penetrated into the equipment.
 - The equipment has been exposed to moisture.
 - The equipment does not work well, or you cannot get it to work according to the user's manual.
 - The equipment has been dropped and damaged.
 - The equipment has obvious signs of breakage.
- 15. DO NOT LEAVE THIS EQUIPMENT IN AN ENVIRONMENT WHERE THE STORAGE TEMPERATURE MAY GO BELOW -20° C (-4° F) OR ABOVE 60° C (140° F). THIS COULD DAMAGE THE EQUIPMENT. THE EQUIPMENT SHOULD BE IN A CONTROLLED ENVIRONMENT.
- 16. CAUTION: DANGER OF EXPLOSION IF BATTERY IS INCORRECTLY REPLACED. REPLACE ONLY WITH THE SAME OR EQUIVALENT TYPE RECOMMENDED BY THE MANUFACTURER, DISCARD USED BATTERIES ACCORDING TO THE MANUFACTURER'S INSTRUCTIONS.

The sound pressure level at the operator's position according to IEC 704-1:1982 is no more than 70 dB (A).

DISCLAIMER: This set of instructions is given according to IEC 704-1. Advantech disclaims all responsibility for the accuracy of any statements contained herein.

Safety Precaution - Static Electricity

Follow these simple precautions to protect yourself from harm and the products from damage.

- To avoid electrical shock, always disconnect the power from your PC chassis before you work on it. Don't touch any components on the CPU card or other cards while the PC is on.
- Disconnect power before making any configuration changes. The sudden rush of power as you connect a jumper or install a card may damage sensitive electronic components.

Acronyms

Term	Define
AC'97	Audio CODEC (Coder-Decoder)
ACPI	Advanced Configuration Power Interface – standard to implement power saving modes in PC-AT systems
BIOS	Basic Input Output System – firmware in PC-AT system that is used to ini- tialize system components before handing control over to the operating sys- tem
CAN	Controller-area network (CAN or CAN-bus) is a vehicle bus standard designed to allow microcontrollers to communicate with each other within a vehicle without a host computer
DDI	Digital Display Interface – containing DisplayPort, HDMI/DVI, and SDVO
EAPI	Embedded Application Programmable Interface Software interface for COM Express® specific industrial function System information Watchdog timer I2C Bus Flat Panel brightness control User storage area GPIO
GbE	Gigabit Ethernet
GPIO	General purpose input output
HDA	Intel High Definition Audio (HD Audio) refers to the specification released by Intel in 2004 for delivering high definition audio that is capable of playing back more channels at higher quality than AC'97
I2C	Inter Integrated Circuit – 2 wire (clock and data) signaling scheme allowing communication between integrated circuit, primarily used to read and load register values
ME	Management Engine
PC-AT	"Personal Computer – Advanced Technology" – an IBM trademark term used to refer to Intel based personal computer in 1990s
PEG	PCI Express Graphics
RTC	Real Time Clock – battery backed circuit in PC-AT systems that keeps sys- tem time and date as well as certain system setup parameters
SPD	Serial Presence Detect – refers to serial EEPROM on DRAMs that has DRAM Module configuration information
ТРМ	Trusted Platform Module, chip to enhance the security features of a com- puter system
UEFI	Unified Extensible Firmware Interface
WDT	Watch Dog Timer

Contents

Chapter	1	General Information	1
	1 1	Introduction	2
	1.2	Functional Block Diagram	
	1.3	Product Specification	4
Chapter	2	Mechanical Information	.13
	2.1	Board Information	14
		Figure 2.1 Board Chips Identify - Front	14
		Figure 2.2 Board Chips Identify - Back	14
		2.1.1 Connector List	15
	2.2	Table 2.1: FANT Fan	15
	2.2	Figure 2.3. Board Mechanical Drawing - Front	15
		Figure 2.4 Board Mechanical Drawing - Back	16
		Figure 2.5 Board Mechanical Drawing - Side	16
	2.3	Assembly Drawing	17
		Figure 2.6 Assembly Drawing	17
	2.4	Assembly Drawing	18
		Figure 2.7 Main Chip Height and Tolerance	18
			10
Chapter	3	BIOS Operation	.19
	3.1	Entering Setup	20
		Figure 3.1 Setup program initial screen	20
	3.2	Entering Setup	21
		3.2.1 Main Selup	
		5.2.2 Advanced BIOS features setup screen	22
		Figure 3.3 Trusted Computing	23
		Figure 3.4 ACPI Settings	24
		Figure 3.5 iManager Configuration	25
		Figure 3.6 Serial Port 1 Configuration	26
		Figure 3.7 Serial Port 2 Configuration	27
		Figure 3.8 Hardware Monitor	28
		Figure 3.9 Serial Port Console Redirection	28
		Figure 3.10PCI Subsystem Settings	29
		Figure 3.12CSM Configuration	30
		Figure 3.13NVMe Configuration	
		Figure 3.14USB Configuration	33
		3.2.3 IntelRCSetup	34
		Figure 3.15IntelRCSetup	34
		Figure 3.16Processor Configuration #1	35
		Figure 3.17Processor Configuration #2	36
		Figure 3.18Advanced Power Management Configuration	38
		Figure 3.19CPU P State Control	39
		Figure 3.20AE Ralio Limit	40 ⊿1
		Figure 3.22CPU HWPM State Control	4 1 42
		Figure 3.23CPU Advanced PM Turning	
		Figure 3.24DRAM RAPL Configuration	44

		Figure 3.25SOCKET RAPL Config	45
		Figure 3.26Common RefCode Configuration	
		Figure 3.27Memory Configuration -1	47
		Figure 3.28Memory Configuration -2	48
		Figure 3.29Memory Topology	50
		Figure 3.30Memory Thermal	51
		Figure 3.31 Memory Power Savings Advanced Options	52
		Figure 3.32Memory Timings & Voltage Override	52
		Figure 3.33Memory RAS Configuration	54
		Figure 3.34IIO Configuration	
		Figure 3.35IIO Configuration	55
		Figure 3.36Socket 0 PcieD01F0 - Port 1A	
		Figure 3.37 Socket 0 PcieD02F0 - Port 2A	
		Figure 3 38Socket 0 PcieD02F2 – Port 2C	57
		Figure 3 39Socket 0 PcieD03E0 – Port 3A	58
		Figure 3 4010AT Configuration	58
		Figure 3 41110 General Configuration	50
		Figure 3.42 Intel V/T for Directed I/O (V/T-d)	
		Figure 3.43110 South Complex Configuration	
		Figure 2.44DCH Configuration	01 62
		Figure 3.45PCH Devices	
		Figure 3.46PCH Express Configuration	
		Figure 3.47 PCH SATA Configuration	
		Figure 3.48USB Configuration	
		Figure 3.49Security Configuration	67
		Figure 3.50Miscellaneous Configuration	
		Figure 3.51Server ME Configuration	69
		Figure 3.52Runtime Error Logging	70
		Figure 3.53Reserve Memory	71
	3.2.4	Server Mgmt	72
		Figure 3.54Server Mgmt	72
		Figure 3.55System Event Log	73
		Figure 3.56BMC self test log	74
		Figure 3.57BMC network configuration	75
		Figure 3.58BMC User Settings	
	3.2.5	Security	77
		Figure 3.59Security	
	3.2.6	Boot	
	0.2.0	Figure 3 60Boot	78
	327	Event Logs	70
	0.2.7	Figure 3 61 Event Logs	70
	3 2 8	Save & Evit	
	5.2.0	Figure 2 62 Save & Exit	00 مو
Chaptor 4	сW	Introduction & Installation	83
	3/4		05
4 1	S/W Ir	ntroduction	
4.2	Driver	Installation	
T: E	421	Windows Driver Setun	
	422	Other OS	+0 ۸ ی
4.3	Advan	tech iManager	
		-	
Appendix A	Pin	Assignment	
A.1	SOM-	5992 Type 7 Pin Assignment	88
Appendix B	Wa	tchdog Timer	93
		-	

B.1	Programming the Watchdog Timer	94
Appendix C	Programming GPIO	95
C.1	GPIO Register	
Appendix D	System Assignments	97
D.1	System I/O Ports Table D.1: System I/O ports	
D.2	DMA Channel Assignments Table D.2: DMA Channel Assignments	
D.3	Interrupt Assignments	



General Information

This chapter gives background information on the SOM-5992 CPU Computer on Module.
Sections include:
Introduction
Functional Block Diagram
Product Specification

1.1 Introduction

SOM-5992, designed around the Intel® Xeon® Processor D-1500 family, brings the performance and advanced intelligence of Intel® Xeon® processors into a dense, low-power system-on-a-chip. With enhanced reliability, availability, and serviceability features, platform storage extensions, and built-in hardware virtualization, the Intel® Xeon® processor D-1500 product family offers new possibilities for a variety of applications. SOM-5992 is suitable for midrange routers, network appliances, security appliances, wireless base stations, embedded midrange IoT devices, entry networking, midrange storage area networks (SANs), network attached storage (NAS) appliances, warm cloud storage, and more.

In a breakthrough move, SOM-5992 supports a maximum of 64 GB DDR4 memory which should help fulfill the ever-increasing server application demands in the area of COM Express. The Intel® Xeon® processor D-1500 delivers 16 processor cores and 64 GB memory, combined with computer on module flexibility, this is an optimal solution for users who want extreme computing performance and non-stop service.

Moreover, the SOM-5992 incorporates two 10GBase-KR interfaces for integrating with 10GbE customer carrier boards. PCIe x16 and 8 PCIe x1 Supports Non-Transparent Bridge (NTB), which allows redundancy via PCIe. This helps reduce data loss, allowing a secondary system to take over PCIe storage device management if a CPU fails, and provides high availability for applications requiring continuous service.

SOM-5992 has four screw holes near the CPU, positioned in compliance with the Intel® standard thermal design guide. The thermal module is attached to the CPU in a balanced torque design, and it is the first COM Express to have an added backplane to increase rigidity like single board, so the thermal module makes tight contact with the CPU with no board bending. This result is highly efficient heat dissipation with outstanding computing performance. Advantech also offers SOM-5992-thermal-solution pre assembly service that can assist in system-level assembly.

1.2 Functional Block Diagram



1.3 Product Specification

Compliance

PICMG COM.0 (COM Express) Revision 3.0 Basic Size - 125 x 95mm Pin-out Type 7 compatible

Feature List

Row	System I/O	R3.0 Type 7	SOM-5992
	PCI Express Lanes 0 - 5	6 / 6	6
	PCI Express Lanes 8 - 15 (Type 7)	0/8	8
	LVDS Channel A	N/A	N/A
	LVDS Channel B	N/A	N/A
	eDP on LVDS CH A Pins	N/A	N/A
	VGA Port	N/A	N/A
	Serial Ports 1 - 2	0/2	2
A-B	CAN Interfaces on SER1	0 / 1	0
	SATA / SAS Ports	0/2	2
	HDA Digital Interface	N/A	N/A
	USB 2.0 Ports (Host)	4 / 4	4
	USB0 Client (USB2.0)	0 / 1	0
	1Gb LAN Port 0	1/1	1
	LPC Bus/eSPI	1/1	1 (LPC)
	SPI	1/2	2
Row	System Management	R3.0 Type 7	SOM-5992
	SDIO (Muxed on GPIO)	0 / 1	0
	General Purpose I/O	8/8	8
	SMBus	1/1	1
	12C	1/1	1
A-B	Watchdog Timer	0 / 1	1
	Speaker Out	1 / 1	1
	External BIOS ROM Support	0 / 1	1
	Reset Function	1/1	1
	Trusted Platform Modules	0 / 1	1
Row	Power Management	R3.0 Type 7	SOM-5992
	Thermal Protection	0 / 1	1
	Battery Low Alarm	0 / 1	1
	Suspend / Wake Signals	0/3	2
	Power Button Support	1 / 1	1
A-B	Power Good	1/1	1
	VCC_5V_SBY Contacts	4 / 4	4
	Sleep Input	0 / 1	1
	Lid Input	0 / 1	1
	Carrier Board Fan Control	0 / 1	1
Row	Power	R3.0 Type 7	SOM-5992

A-B	VCC_12V Contacts	12 / 12	12
Row	System I/O	R3.0 Type 7	SOM-5992
	PCI Express Lanes 16 - 31 (PEG)	0 / 16	16
	PCI Express Lanes 6 - 7	0 / 2	2
	10G LAN Port 0-3	0 / 4	2
C-D	Digital Display Interfaces 1 - 3	N/A	N/A
	USB 3.0 Ports	0 / 4	4
	Rapid Shutdown	0/1	1
Row	Power	R3.0 Type 7	SOM-5992
C-D	VCC_12V Contacts	12 / 12	12

Processor System

CPU	Std. Freq.	Max. Turbo Freq.	Core/Thread	LLC Cache	TDP(W)
Xeon D-1577	1.3 GHz	2.1 GHz	16/32	24MB	45W
Xeon D-1548	2.0 GHz	2.6 GHz	8/16	12MB	45W
Xeon D-1539	1.6 GHz	2.2 GHz	8/16	12MB	35W

Memory

Supports dual channels (CH-A & CH-B) and 4 sockets of DDR4 up to a maximum of 64 GB of ECC or non ECC memory (up to 2400GHz based on specific CPU SKU). Maximum support is 16GB in each socket (total 64GB), two sockets on the front side and the other two on the rear side, CH-A0 is the first priority for system boot up.



Graphics / Audio

Intel® Xeon® Processor D Family is without graphics. SOM-5992 does not support display and audio. Graphics will be defined according to specific user scenarios based on system specification. Please contact Advantech sales or FAE for more details.

Expansion Interface

PCle x16

Intel Xeon® Processor D natively integrates one x16 PCI Express interface supporting up to 4 devices at up to Gen3 speeds (8 GHz). SOM-5992 supports one PCIe x16, and is configurable to 2 x8, 1 x8 & 2 x4, or 4 x4.

PCIe x8

Intel Xeon® Processor D natively integrates one x8 PCI Express interface supporting up to 4 devices at up to Gen3 speeds (8 GHz). SOM-5992 supports one PCIe x8, and is configurable to 2 x4.

PCle x1

Intel Xeon® Processor D natively integrates eight PCI Express x1 lanes up to eight devices, which supports up to Gen2 (5.0 Gb/s). SOM-5992 supports eight PCIe x1 by default, and is configurable to the three options in the following table.

Туре 7		Row	Row A,B						Row C,D	
		P0	P1	P2	P3	P4	P5	P6	P7	
Default		X1	X1	X1	X1	X1	X1	X1	X1	
Option 1		X1	X1	X2		X1	X1	X2	·	
Option 2		X2		X2		X2		X2		
Option 3		X4				X4	X4			

LPC

Supports Low Pin Count (LPC) 1.1 specification, without DMA or bus mastering. Also able to connect to Super I/O, embedded controller, or TPM. LPC clock is 25MHz.

Serial Bus

SMBus

Supports SMBus 2.0 specification with Alert pin.

I2C Bus

Supports I2C bus 8-bit and 10-bit address modes, at both 100KHz and 400KHz.

I/O

Gigabit Ethernet

On-module Intel i210AT supports IEEE802.3 for 1000BASE-T, 100BASE-TX, and 10BASE-T (802.3, 802.3u, and 802.3ab). Supports IPv4, IPv6, TCP/UDP, SCTP, ARP, Neighbor Discovery, EUI-64.

SATA

Supports four ports SATA Gen3 (6.0 Gb/s), backward compliant to SATA Gen2 (3.0 Gb/s) and Gen1 (1.5 Gb/s). Maximum data rate is 600 MB/s. Supports AHCI 1.3 mode.

USB3.0/USB2.0

There are four ports USB3.0 (5.0 Gbps) and four ports USB2.0 (480 Mbps) which are backward compatible to USB1.x. USB3.0 supports LPM (U0, U1, U2, and U3) manageability to save power.

USB3.0

Туре 7	P0	P1	P2	P3
SoC	P0	P1	P2	P3
Туре 7	OC_01		OC_23	
SoC USB_OC#	OC_0		OC_2	

USB2.0

Туре 7	P0	P1	P2	P3
SoC	P0	P1	P2	P3
Туре 7	OC_01		OC_23	
SoC USB_OC#	OC_0		OC_2	

SPI Bus

Supports BIOS flash only. SPI clock can be 50MHz, 33MHz, or 20MHz, capacity up to 16MB.

GPIO

Eight programmable general purpose Input or output (GPIO).

Watchdog

Supports multi-level watchdog time-out output. Provides 1-65535 levels, from 100ms to 109.22 minutes interval.

Serial port

2 ports, 2-wire serial ports(Tx/Rx) supports 16550 UART compliance.

- Programmable FIFO or character mode
- 16-byte FIFO buffer on transmitter and receiver in FIFO mode
- Programmable serial-interface characteristics: 5, 6, 7, or 8-bit character
- Even, odd, or no parity bit selectable
- 1, 1.5, or 2 stop bit selectable
- Baud rate up to 115.2K

TPM

Supports TPM 2.0 module by default.

Smart Fan

Supports two Fan PWM control signals and two tachometer inputs for fan speed detection. Provides one on module with connector, and the other on the carrier board following the PICMG COM Express R3.0 specification.

BIOS

The BIOS chip is on the module by default. This also allows users to place the BIOS chip on the carrier board with an appropriate design and jumper setting on BIOS_DIS#[1:0].

BIOS_DIS0#	BIOS_DIS#1	Boot up destination/function
Open	Open	Boot from module's SPI BIOS
GND	Open	Boot from carrier board LPC/FWH BIOS
Open	GND	SPI_CS0# to carrier board, SPI_CS1# to module
GND	GND	SPI_CS0# to module, SPI_CS1# to carrier board

Note!

If system COMs are cleared, we strongly suggest to go to the BIOS setup menu and load default settings at the first time of boot up.

Power Management

Power Supply

Supports both ATX and AT power modes. VSB is for suspend power and can be optional if standby is not required (suspend-to-RAM). Supports RTC Battery as optional if keep time/date is not required.

VCC: 8.5V (9V-5%) – 20V (19V+5%)

VSB: 5V +/- 5% (Suspend power)

RTC Battery Power: 2.0V – 3.3V

PWROK

From the main power supply, a high value indicates that the power is good. This signal can be used to hold off module startup to allow carrier based FPGAs or other configurable devices time to be programmed.

Power Sequence

According to PICMG COM Express R3.0 specification

Wake Event

Various wake-up events support for different scenarios. Wake-on-LAN(WOL): Wake to S0 from S4/S5 USB Wake: Wake to S0 from S4 PCIe Device Wake: depends on user inquiry and may need customized BIOS LPC Wake: depends on user inquiry and may need customized BIOS

Advantech S5 ECO Mode (Deep Sleep Mode)

Advantech iManager provides additional features to allow the system to enter a very low suspend power mode – S5 ECO mode. In this mode, the module will cut all power including suspend and active power into the chipset and keep an on-module controller active. Therefore, only under 50mW power will be consumed which means the user's battery pack will last a longer time. With this mode enabled in BIOS, the system (or module) will only allow a power button to boot rather than others such as WOL.

Environment

Temperature

- $-\,$ Operating: 0 ~ 60° C (32 ~ 140° F), with an active heat sink under 0.7m/s air flow chamber
- Extend: -40 ~ 85° C (32 ~ 140° F), supported by specific SKU
- Storage: -40 ~ 85° C (-40 ~ 185° F)

Humidity

- Operating: 40° C @ 95% relative humidity, non-condensing
- Storage: 60° C @ 95% relative humidity, non-condensing

Vibrations

IEC60068-2-64: Random vibration test under operation mode, 3.5Grms

Drop Test (Shock)
 Federal standard 101 method 5007 test procedure with standard packing

EMC

CE EN55032 Class B and FCC certifications: validate with standard development boards in Advantech chassis

MTBF

Please refer Advantech SOM-5992 Series Reliability Prediction Report No: TBD. Link: http://com.advantech.com

OS Support (duplicate with SW chapter)

The mission of Advantech Embedded Software Services is to "Enhance quality of life with Advantech platforms and Microsoft Windows embedded technology." We enable Windows Embedded software products on Advantech platforms to more effectively support the embedded computing community. Customers are freed from the hassle of dealing with multiple vendors (Hardware suppliers, System integrators, Embedded OS distributor) for projects. Our goal is to make Windows Embedded Software solutions easily and widely available to the embedded computing community.

To install the drivers for Linux or other OS, please connect to the internet to download the setup file.

Link: http://support.advantech.com

Advantech iManager

Supports APIs for GPIO, smart fan control, multi-stage watchdog timer and output, temperature sensor, hardware monitor, etc. iManager follows PICMG EAPI 1.0 specification and provides backward compatibility.

Power Consumption Table (Watt.)						
VCC=12V, VSB=5V	Active Power Domain			Suspend Power Domain		Mechanical off
Power State	S0 Max. Load	S0 Burn-in	S0 Idle	S5	S5 ECO	RTC (uA)
SOM-5992D8-U0A1	55.53 W	50.26 W	12.34 W	1.76 W	0.015 W	4.04 uA

Power Consumption

Hardware Configurations:

- 1. MB: SOM-5992D8-U0A1 (PCB_A101-2, CPU: Intel Xeon D-1548)
- 2. DRAM: 16GB DDR4 2400MHz *4
- 3. Carrier board: SOM-DB5920_A101-2

Test Condition:

- 1. Test temperature: room temperature
- 2. Test voltage: rated voltage DC +12.0V
- 3. Test loading:
 - 3.1 Idle mode: DUT power management off and no running any program.
 - 3.2 Maximum load mode: Running programs.
- 4. OS: Windows Server 2012 R2 Standard.
- 5. Test software:
 - 5.1 Burn In Test V8.1 Pro (1022) for 64 bit Windows
 - 5.2 Intel® Power Thermal Utility Tool Rev1.1

Performance

For reference performance or benchmark data that compare with other modules, please refer to "Advantech COM Performance & Power Consumption Table". Link: http://com.advantech.com

Packing list

Part No.	Description	Quantity
-	SOM-5992 CPU Module	1
1960081925N001	Heat spreader	1

Development Board

Part No.	Description
SOM-DB5920-00A1	COM-Express Development Board, Type 7 Pin-out

Optional Accessory

Part No.	Description
1960048820N001	Semi-Cooler 125x95x33.5mm with 12V Fan
1960075879N001	Cooler 66x60x23mm with 12V Fan

Pin Description

Advantech provides useful checklists for schematic design and layout routing. In schematic checklist, it will specify details about each pins electrical properties and how to connect for different uses. In layout checklist, it will specify the layout constrains and recommendations for trace length, impedance, and other necessary information during design.

Please contact your nearest Advantech branch office or call for getting the design documents and further advanced support.

Link: http://com.advantech.com



Mechanical Information

This chapter gives mechanical information on the SOM-5992 CPU Computer on Module.

- Sections include:
- Board Information
- Mechanical Drawing
- Assembly Drawing

2.1 Board Information

The figures below indicate the main chips on SOM-5992 Computer-on-Module. Please aware of these positions while designing your own carrier board to avoid mechanical issues, as well as designing thermal solution contact points for best thermal dissipation performance.



Figure 2.1 Board Chips Identify - Front



COM Express Connector

Figure 2.2 Board Chips Identify - Back

2.1.1 Connector List

Table 2.1: FAN1 Fan			
FAN1	Fan		
Description	Wafer 2.0mm 3P 90D(M)DIP 2001-WR-03-LF W/Lock		
Pin	Pin Name		
1	Fan Tacho-Input		
2	Fan Out		
3	GND		



2.2 Mechanical Drawing

For more details about 2D/3D models, find out more on Advantech's COM support service website

Link: http://com.advantech.com







Figure 2.4 Board Mechanical Drawing - Back



Figure 2.5 Board Mechanical Drawing - Side

There are two memory sockets on the rear side at a height of 8.00mm in total. If users need 64GB memory, please adopt a H:8mm board-to-board connector on carrier board.

If there is no need for 64GB memory, users can keep the H:5mm board-to-board connector on the carrier board. Please contact Advantech sales or FAE for more details.

2.3 Assembly Drawing

These figures demonstrate the assembly order from thermal module, to the COM module, to the carrier board.



Figure 2.6 Assembly Drawing

There are four reserved screw holes for SOM-5992 to be pre-assembled with the heat spreader.

Assembly Drawing 2.4

It is important to consider the CPU and chip height tolerance when designing your thermal solution.



*(2-8 Core) F5=NOM : 3.556mm TOL:±0.076mm **(12-16 Core) F5=NOM : 3.772mm TOL:±0.076mm (POST SMT STACKUP HEIGHT BASED ON LIMITED DATA FROM INTEL REFER-ENCE BOARD DESIGN)

Figure 2.7 Main Chip Height and Tolerance





Caution! SOM-5992 has a clean area for a thermal solution backplane on the rear side, which is for a thermal module and the backplane is designed to help strengthen the contact of the thermal module and the CPU. If the space is used, please reserve a relative clean area on the carrier board according to the following dimensions.



Figure 2.8 Backplane of Optional Thermal Solution



BIOS Operation

This chapter gives BIOS setup information for the SOM-5992 CPU Computer on Module. Sections include:

- Introduction
- Entering Setup
- Hot / Operation Key
- Exit BIOS Setup Utility

3.1 Entering Setup

With the AMI BIOS Setup Utility, users can modify BIOS settings and control various system features. This chapter describes the basic navigation of the BIOS Setup Utility.

Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc. Main Advanced IntelRCSetup Server Mgmt Security Boot Event Logs Save & Exit			
BIOS Information BIOS Vendor Core Version Compliancy Project Version Build Date and Time Access Level	American Megatrends 5.0.1.1 0.31 x64 UEFI 2.4.0; PI 1.3 5992000060X008 08/23/2017 16:06:01 Administrator	Set the Date. Use Tab to switch between Date elements.	
Memory Information			
Total Memory	8192 MB		
System Date System Time	[Sat 07/29/2017] [07:57:10]	<pre>++: Select Screen 1↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>	
Version 2.18.1260. Copyright (C) 2017 American Megatrends. Inc.			

Figure 3.1 Setup program initial screen

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 Setup

Turn on the computer and then press or <ESC> to enter Setup menu.

3.2.1 Main Setup

When users first enter the BIOS Setup Utility, users 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.

Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc. Main Advanced IntelRCSetup Server Mgmt Security Boot Event Logs Save & Exit			
BIOS Information BIOS Vendor Core Version Compliancy Project Version Build Date and Time Access Level Memory Information Total Memory	American Megatrends 5.0.1.1 0.31 x64 UEFI 2.4.0; PI 1.3 5992000060X008 08/23/2017 16:06:01 Administrator 8192 MB	Set the Date. Use Tab to switch between Date elements.	
System Date System Time	[Sat 07/29/2017] [07:57:10]	<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 2.18.1260. Copyright (C) 2017 American Megatrends, Inc.			

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 SOM-5992 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.



Figure 3.2 Advanced BIOS features setup screen

3.2.2.1 Trusted Computing

Aptio Setup Utility - Advanced	Copyright (C) 2017 American	Megatrends, Inc.
TPM20 Device Found Security Device Support Active PCR banks Available PCR banks SHA-1 PCR Bank SHA-256 PCR Bank Pending operation Platform Hierarchy Storage Hierarchy Endorsement Hierarchy TPM2.0 UEFI Spec Version Physical Presence Spec Version TPM 20 InterfaceType Device Select	[Enable] SHA-1 SHA-1,SHA256 [Enabled] [Disabled] [Enabled] [Enabled] [Enabled] [Enabled]	Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.
	[TCG_2] [1.2] [TIS] [Auto]	<pre>14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>

Figure 3.3 Trusted Computing

Security Device Support

Enables or disables BIOS support for security device. OS will not show security Device. TCG EFI protocol and INT1A interface will not be available.

- 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 secured device.

Platform Hierarchy
 Enable or disable platform hierarchy.

Storage Hierarchy

Enable or disable storage hierarchy.

Endorsement Hierarchy

Enable or disable endorsement hierarchy.

TPM2.0 UEFI Spec Version

Select the TCG2 Spec version support. TCG_1_2: Compatible modes for Win8/Win10, TCG_2: supports new TCG2 protocols and event formats for Win10 or later.

Device Select

TPM 1.2 will restrict support to TPM 1.2 devices, TPM 2.0 will restrict support to TPM 2.0 devices, Auto will support both with the default set to TPM 2.0 devices, if not found, TPM 1.2 devices will be enumerated.

3.2.2.2 ACPI Settings



Figure 3.4 ACPI Settings

Enable ACPI Auto Configuration

Enables or disables BIOS ACPI Auto Configuration.

Enable Hibernation Enables or disables system ability to Hibernate (OS/S4 Sleep State). This option may be not effective with some OS.

Lock Legacy Resources

Enables or disables Lock of Legacy Resources.

3.2.2.3 iManager Configuration

Aptio Setup Utility - Advanced	Copyright (C) 2017 American	Megatrends, Inc.
iManager Configuration		CPU Shutdown Temperature
iManager Chipset Firmware Version	ITE8528E I28C4×0003	
CPU Shutdown Temperature iManager Smart Fan – COM Module iManager Smart Fan – Carrier Board Backlight Enable Polarity Power Saving Mode	[Disable] [Enabled] [Enabled] [Native] [Normal]	
 Serial Port 1 Configuration Serial Port 2 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 2.18.1260. Co	pyright (C) 2017 American M	egatrends, Inc.

Figure 3.5 iManager Configuration

- CPU Shutdown Temperature
 Enable/disable CPU Shutdown Temperature.
- iManager Smart Fan COM Module Control iManager Smart FAN function
- iManager Smart Fan Carrier Board
 Control iManager Smart FAN Carrier Board function.
- Backlight Enable Polarity
 Switch Backlight Enable Polarity for native or invert
- Power Saving Mode
 Select ITE8528 power saving mode
- Serial Port 1 Configuration
 Set parameters of serial port 1 (COMA)
- Serial Port 2 Configuration Set parameters of serial port 2 (COMB)
- Hardware Monitor
 Monitor hardware status

Serial Port 1 Configuration



Figure 3.6 Serial Port 1 Configuration

- Serial Port
 Enable or disable Serial Port (COM)
- Change Settings
 Select an optimal setting for Super IO device.
Serial Port 2 Configuration



Figure 3.7 Serial Port 2 Configuration

Serial Port

Enable or disable Serial Port (COM)

Change Settings
 Select an optimal setting for Super IO device.

Hardware Monitor Information

This item shows hardware information parameters.



Figure 3.8 Hardware Monitor

3.2.2.4 Serial Port Console Redirection

Aptio Setup Utility - Co Advanced	opyright (C) 2017 American	Megatrends, Inc.
COM1 Console Redirection ▶ Console Redirection Settings	[Disabled]	Console Redirection Enable or Disable.
COM2 Console Redirection Console Redirection Settings Legacy Console Redirection	[Disabled]	
 Legacy Console Redirection Settings Serial Port for Out-of-Band Management Windows Emergency Management Services Console Redirection Console Redirection Settings 	t/ (EMS) [Disabled]	<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 2.18.1260. Copy	yright (C) 2017 American Me	egatrends, Inc.

Figure 3.9 Serial Port Console Redirection

- COM1 Console Redirection
 Console Redirection enable or disable
- COM2 Console Redirection
 Console Redirection enable or disable
- Legacy Console Redirection Settings
 Select a COM port to display redirection of legacy OS and legacy OPROM messages
- Console Redirection Console Redirection enable or disable
- PCI Subsystem Settings

Aptio Setup Utility - Advanced	Copyright (C) 2017 American	Megatrends, Inc.
PCI Bus Driver Version	A5.01.08	Value to be programmed into PCI Latency Timer Register.
PCI Devices Common Settings: PCI Latency Timer PCI-X Latency Timer VGA Palette Snoop PERR# Generation SERR# Generation Above 4G Decoding Don't Reset VC-TC Mapping PCH PCIE Port Currect Setting 1 PCH PCIE Port Config 1 PCH PCIE Port Currect Setting 2 PCH PCIE Port Config 2	<pre>[32 PCI Bus Clocks] [64 PCI Bus Clocks] [Disabled] [Disabled] [Disabled] [Enabled] [Enabled] 1 Lane x4 1 Lane x4] 1 Lane x4 [1 Lane x4]</pre>	++: Select Screen fl: Select Item Enter: Select +/-: Change Opt. F1: General Help
		F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

Figure 3.10 PCI Subsystem Settings

PCI, PCI-X and PCI Express settings.

- PCI Latency Timer
 Press enter to select the PCI Bus clocks
- PCI-X Latency Timer
 Value to be programmed into PCI Latency Timer Register
- VGA Palette Snoop
 Enable or disable VGA Palette Registers Snoop
- PERR# Generation
 Enable or disable PCI Device to generate PERR#
- SERR# Generation
 Enable or disable PCI Device to generate SERR#
- Above 4G Decoding
 Enables or disables 64-bit capable devices to be decoded in above 4G
 Address Space (Only if System Supports 64 bit PCI Decoding)
- Don't Reset VC-TC Mapping

If system has Virtual Channels, Software can reset Traffic Class mapping through Virtual Channels to it's default state. Setting this option to Enabled will not modify VC Resources

- PCH PCle Port Current Setting 1
 PCH PCle Port Config 1
- Config PCH PCle Lane 0~3 setting
 PCH PCle Port Current Setting 2
- PCH PCle Port Config 2
 Config PCH PCle Lane 4~7 setting

3.2.2.5 Network Stack Configuration

Network Stack	[Disabled]	Enable/Disable UEFI Network Stack
		<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>

Figure 3.11 Network Stack Configurations

Network Stack

Enable or disable Network Stack.

Ipc4 PXE Support

Enable or disable Ipv4 PXE support. (If disabled IPV4 PXE boot option will not be created).

Ipv6 PXE Support

Enable or disable Ipv6 PXE support. (If disabled IPV6 PXE boot option will not be created).

PXE boot wait time

Wait time to press ESC key to abort the PXE boot.

Media detect count

Number of times presence of media will be checked.

3.2.2.6 CSM Configuration

Aptio Setup Utility - Advanced	Copyright (C) 2017 American	Megatrends, Inc.
Compatibility Support Module Configu	ration	Enable/Disable CSM Support.
CSM Support	[Enabled]	
CSM16 Module Version	07.79	
GateA20 Active INT19 Trap Response	[Upon Request] [Immediate]	
Boot option filter	[UEFI only]	
Option ROM execution		
Network Storage Video Other PCI devices	[Do not launch] [UEFI] [UEFI] [UEFI]	<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 2.18.1260. Cc	pyright (C) 2017 American M	egatrends, Inc.

Figure 3.12 CSM Configuration

CSM Support

Enable/disable CSM support

GateA20 Active

UPON Request- GA20 can be disabled using BIOS services. Do not allow disabling GA20; this option is useful when any RT code is executed above 1MB.

Boot option filter

This option controls legacy/UEFI ROMs priority

Network

Controls the execution of UEFI and legacy PXE OpROM

Storage

Controls the execution of UEFI and legacy storage OpROM

Video

Controls the execution of UEFI and legacy video OpROM

Other PCI devices

Determines OpROM execution policy for devices other than network, storage, or video

3.2.2.7 NVMe Configuration



Figure 3.13 NVMe Configuration

NVMe Device Options Setting

User can start the setting after inserting NVMe device.

3.2.2.8 USB Configuration

USB Configuration USB Module Version	13	Enables Legacy USB support. AUTO option disables legacy support if no USB devices are
USB Module Version	13	support if no USB devices are
		connected. DISABLE option will
USB Controllers:		keep USB devices available
USB Devices:		only for Eri appricacions.
1 Drive, 1 Keyboard, 1 Mouse,	1 Hub	
Legacy USB Support	[Enabled]	
XHCI Hand-off	[Enabled]	
EHCI Hand-Off USB Macc Storade Driver Support	[UISabled]	
Port 60/64 Emulation	[Enabled]	++: Select Screen
For Covor Endiateron	[2:105100]	↑↓: Select Item
USB hardware delays and time-outs:		Enter: Select
USB transfer time–out	[20 sec]	+/−: Change Opt.
Device reset time-out	[20 sec]	F1: General Help
Device power-up delay	[Auto]	F2: Previous Values
		F3: Optimized Defaults
Mass Storage Devices:	[0	F4: Save & Exit
UDISK3.0G1gaStone	[Huto]	ESU: EXIL

Figure 3.14 USB Configuration

Legacy USB Support

Enables Legacy USB Support. Auto option disables legacy support if no USB devices are connected. Disable option will keep USB devices available only for EFI applications.

XHCI Hand-off

This is a workaround for OS without XHCI ownership change should be claimed by XHCI driver.

EHCI Hand-off

This is a workaround for OS without EHCI ownership change should be claimed by EHCI driver.

USB Mass Storage Driver Support

Enable or disable USB Mass Storage driver support.

Port 60/64 Emulation

Enable I/O port 60h/64h emulation support. This should be enabled for the complete USB keyboard legacy support for non-USB aware OS.

USB transfer time-out

This time-out value for Control, Bulk, and Interrupt transfers.

Device reset time-out

USB mass storage device start unit command time-out.

Device power-up delay

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

AMI Storage Devices

Mass storage device emulation type. 'Auto' enumerates devices according to their media format. Optical drives are emulated as 'CDROM', drives with no media will be emulated according to a drive type.

AMI Virtual CDROMO 1.00

Select the device emulation type as Auto, Floppy, Forced FDD, Hard Disk or CD-ROM.

AMI Virtual Floppy0 1.00

Select the device emulation type as Auto, Floppy, Forced FDD, Hard Disk or CD-ROM

AMI Virtual HDISK0 1.00

Select the device emulation type as Auto, Floppy, Forced FDD, Hard Disk or CD-ROM $\,$

3.2.3 IntelRCSetup

Select the IntelRCSetup tab from the SOM-5992 setup screen to enter the BIOS Setup screen. You can select the items by highlighting it using the <Arrow> keys. All Plug and Play BIOS Setup options are described in this section. The Plug and Play BIOS Setup screen is shown below. Displays and provides options to change the processor settings.

Aptio Setup Utility – Copyright (C) 2017 American Main Advanced <mark>IntelRCSetup</mark> Server Mgmt Security Boot Ever	Megatrends, Inc. nt Logs Save & Exit
 Processor Configuration Advanced Power Management Configuration Common RefCode Configuration Memory Configuration IIO Configuration PCH Configuration Miscellaneous Configuration Server ME Configuration Runtime Error Logging Reserve Memory 	Displays and provides option to change the Processor Settings
Setup Warning: Setting items on this Screen to incorrect values may cause system to malfunction!	<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 2.18.1260. Copyright (C) 2017 American Me	egatrends, Inc.

Figure 3.15 IntelRCSetup

Processor Configuration

Displays and provides option to change the processor settings.

- Advanced Power Management Configuration
 Displays and provides option to change the power management settings.
- Common RefCode Configuration
 Displays and provides option to change the common RefCode settings.
- Memory Configuration

Displays and provides option to change the memory settings.

- IIO Configuration
 Displays and provides option to change the IIO settings.
- PCH Configuration
 Displays and provides option to change the PCH settings.
- Miscellaneous Configuration
 User defined.
- Server ME Configuration
 Configure Server ME Technology parameters.
- Runtime Configuration
 Press <Enter> to view or change the runtime error log configuration.
- Reserve Memory Reserve memory

3.2.3.1 Processor Configuration

Processor Configuration Enables Hyper Threading 00050663* Processor ID 00050663* Processor Frequency 2.000GHz Processor Max Ratio 14H Processor Min Ratio 08H Microcode Revision 0700000D L1 Cache RAM 512KB L2 Cache RAM 2049KB L3 Cache RAM 12288KB Processor O Version Intel(R) Xeon(R) CPU D- 1548 @ 2.00GHz ++: Select Screen Hyper-Threading (ALL) [Enable] Enable (Antional Antional A	Aptio Setup Utility IntelRCSetup	– Copyright (C) 2017 America	n Megatrends, Inc.
Processor ID00050663*Enable/Disable LogicalProcessor Frequency2.000GHzProcessor threads.Processor Max Ratio14HProcessor Min Ratio08HMicrocode Revision0700000DL1 Cache RAM512KBL2 Cache RAM2048KBL3 Cache RAM12288KBProcessor 0 VersionIntel(R) Xeon(R) CPU D- 1548 @ 2.00GHzHyper-Threading (ALL)[Enable]Hyper-Threading (ALL)[Enable]Hyper-Threading (ALL)[Enable]Execute Disable Bit[Enable]Enable Intel TXT Support[Disable]VMX[Enable]Enable SMX[Disable]Lock Chipset[Enable]KSR Lock Control[Enable]PFIN Control[Unlock/Enable]DEBUG INTERFACE[Disable]	Processor Configuration		Enables Hyper Threading
Hyper-Threading [ALL] [Enable] ++: Select Screen Monitor/Mwait [Enable] 14: Select Item Execute Disable Bit [Enable] Enter: Select Enable Intel TXT Support [Disable] +/-: Change Opt. VMX [Enable] F1: General Help Enable SMX [Disable] F2: Previous Values Lock Chipset [Enable] F3: Optimized Defaults MSR Lock Control [Enable] F4: Save & Exit PPIN Control [Unlock/Enable] ESC: Exit	Processor ID Processor Frequency Processor Max Ratio Processor Min Ratio Microcode Revision L1 Cache RAM L2 Cache RAM L3 Cache RAM Processor O Version	00050663* 2.000GHz 14H 08H 0700000D 512KB 2048KB 12288KB Intel(R) Xeon(R) CPU D-	Enable/Disable Logical Processor threads.
Hardware Prefetcher [Enable]	Hyper-Threading [ALL] Monitor/Hwait Execute Disable Bit Enable Intel TXT Support VMX Enable SMX Lock Chipset MSR Lock Control PPIN Control DEBUG INTERFACE Hardware Prefetcher Adjacent Cache Prefetch	<pre>[Enable] [Enable] [Enable] [Disable] [Enable] [Disable] [Enable] [Enable] [Unlock/Enable] [Disable] [Enable] [Enable]</pre>	<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>

Figure 3.16 Processor Configuration #1

Aptio Setup Utili [.] IntelRCSetup	ty – Copyright (C) 2017 America	an Megatrends, Inc.
Hyper-Threading [ALL] Monitor/Mwait Execute Disable Bit Enable Intel TXT Support VMX Enable SMX Lock Chipset MSR Lock Control PPIN Control DEBUG INTERFACE Hardware Prefetcher Adjacent Cache Prefetch DCU Streamer Prefetcher DCU JP Prefetcher DCU Mode Direct Cache Access (DCA) DCA Prefetch Delay X2APIC AES-NI Down Stream PECI IIO LLC Ways [19:0] (Hex) QLRU Config [31:0] (Hex) SMM Save State Targeted Smi	[Enable] [Enable] [Enable] [Disable] [Enable] [Disable] [Enable] [Enable] [Enable] [Enable] [Enable] [Enable] [S2KB 8Way Without ECC] [Auto] [32] [Disable] [Enable] [Disable] [Disable] [Disable] [Disable] [Disable] [Disable] [Disable]	 Enable or Disable Targeted Smi Feature **: Select Screen **: Select Item Enter: Select */-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.18.1260). Copyright (C) 2017 American	Megatrends, Inc.

Figure 3.17 Processor Configuration #2

Hyper-Threading [ALL]

Enable Hyper Threading (software method to enable/disable logical processor threads.

Monitor/Mwait
 Enable or disable the Monitor/Mwait instruction.

Execute Disable Bit

When disabled, forces the XD feature flag to always return 0.

Enable Intel TXT Support

Enable Intel Trusted Execution Technology Configuration. Please disable "EV DFX Features" when TXT is enabled.

VMX

Enable Vanderpool Technology, takes effect after reboot.

Enable SMX

Enable Safe Mode Extensions.

Lock Chipset

Lock or unlock chipset.

MSR Lock Control

Enable – MSR 3Ah, MSR 0E2h and CSR 80h will locked. Power good reset is needed to remove locked bits.

PPIN Control

Unlock and enable/disable PPIN Control.

Debug Interface

MSR 0C80h bit [0], When set enables debugging features.

Hardware Prefetcher

= MLC Streamer Prefectcher (MSR 1A4h Bit[0]).

- **Adjacent Cache Prefetch** = MLC Spatial Prefectcher (MSR 1A4h Bit[1]). **DCU Streamer Prefetch** DCU streamer prefetcher is an L1 data cache prefetcher (MSR 1A4h [2]). **DCU IP Prefetch** DCU IP prefetcher is an L1 data cache prefetcher (MSR 1A4h [3]). **DCU Mode** MSR 31h Bit [0] – A write of 1 selects the DCU mode as 16KB 4-way with ECC. **Direct Cache Access (DCA)** Enables Direct Cache Access. **DCA** prefetch Delay
- DCA Prefetch Delay help.
 X2APIC
 Enable/disable extended APIC support.
- AES-NI Enable/disable AES-NI support.
- Down Stream PECI
 Enable PCIe Down Stream PECI Write.
- IIO LLC Ways [19:0] (Hex) MSR CB0_SLICE0_CR_IIO_LLC_WAYS bitmask.
- QLRU Config [63:32] (Hex)
 VIRTUAL_MSR_CR_QLRU_CONFIG bitmask.
- QLRU Config [31:0] (Hex)
 VIRTUAL_MSR_CR_QLRU_CONFIG bitmask.
- SMM Save State
 Enable or disable the SMM Save State feature.
- Targeted Smi
 Enable or disable Targeted Smi Feature.

3.2.3.2 Advanced Power Management Configuration

Aptio Setup Utili [.] IntelRCSetup	ty – Copyright (C) 2017 A	merican Megatrends, Inc.
Advanced Power Management Config	guration	For HEDT *only*, select
LOT26 Enable UFS CPU PM Tuning EIST (P-states) Config TDP IOTG Setting Uncore CLR Freq OVRD CPU P State Control CPU HWPM State Control CPU G State Control CPU T State Control CPU T State Control CPU Thermal Management CPU Advanced PM Turning DRAM RAPL Configuration SOCKET RAPL Config	[Enable] [Enabled] [Auto] [Enable] [Disable] [Disable] [Auto]	whether VR power is turned off to empty DIMM channels. ++: Select Screen fl: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.18.126). Copyright (C) 2017 Ame	rican Megatrends, Inc.

Figure 3.18 Advanced Power Management Configuration

LOT26 Enable

For HEDT *only*, select whether VR power is turned off to empty DIMM channels.

UFS

Setting in PCU_MISC_CONFIG Bit [28].

CPU PM Tuning
 It extented as 'ALITO' all bit in MSD 150b (coming value as D)

It selected as 'AUTO', all bit in MSR 1FCh keeping value as P0.

EIST (P-states)

When enabled, OS sets CPU frequency according to load. When disabled, CPU frequency is set at Max non-Turbo.

Config TDP

Setting in PCU_MISC_CONFIG Bit [28]. Option to disable/enable Config TDP.

IOTG Setting

IOTG setting via sticky scratch pad register.

Uncore CLR Freq OVRD

Override uncore max CLR Freq ratio programming to MSR 0x620 bits [6:0].

CPU P State Control

Aptio Setup Utility — (IntelRCSetup	Copyright (C) 2017 American	Megatrends, Inc.
CPU P State Control P State Domain P-state coordination SINGLE_PCTL SPD PL2_SAFETY_NET_ENABLE Energy efficient P-state Boot performance mode Turbo Mode Mode XE Ratio Limit	[ALL] [HW_ALL] [no] [Disable] [Enable] [Enable] [Max Performance] [Enable]	Per Logical: indicates the P-state domain for each logical proc in the system. Per Package: all procs indicate the same domain in the same package.
		<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 2.18.1260. Co	oyright (C) 2017 American M	egatrends, Inc.

Figure 3.19 CPU P State Control

P State Domain

Per Logical: indicates the P-state domain for each logical proc in the system. Per Package: all procs indicate the same domain in the same package.

- P-state coordination

HW_ALL (hardware) coordination is recommended over SW_ALL and SW_ANY (software coordination)

- SINGLE_PCTL
 MSR_CR_MISC_PWR_MGMT 0x1AA Bit [0] : SINGLE_PCTL_EN.
- SPD

PCU_MISC_CONFIG Bit [30] : SPD.

- PL2_SAFETY_NET_ENABLE

PCU_MISC_CONFIG Bit [1] : PL@_SAFETY_NET_ENABLE.

Energy efficient P-state

Enable/disable Energy efficient P-state feature. When set to 0, will disable access to ENERGY_PERFORMANCE_BIAS MSR and CPUID Function 6 EAX [3] will read 0 indicating nosupport for Energy Efficient policy setting. When set to 1 will enable access to ENERGY_PERFORMANCE_BIAS MSR.

Boot performance mode

Select the performance state that BIOS will set before OS handoff.

- Turbo Mode

Turbo mode allows a CPU logical processor to execute a higher frequency when enough power is available not exceeding CPU defined limits.

- XE Ratio Limit



Figure 3.20 XE Ratio Limit

Overclocking Lock

Enable/disable Overclocking.

3.2.3.3 CPU C State Control

Aptio Setup Utility - IntelRCSetup	Copyright (C) 2017 American	Megatrends, Inc.
CPU C State Control C2C3TT CPU C State Package C State limit CPU C3 report CPU C6 report Enhanced Halt State (C1E) OS ACPI Cx	O [Enable] [C6(Retention) state] [Disable] [Enable] [Enable] [ACPI C2]	Default = 0, means [AUTO]. C2 to C3 Transition Timer, PPDN_INIT = 1:10:1:74 Bit[11:0].
		<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 2.18.1260. Co	ppyright (C) 2017 American M	egatrends, Inc.

Figure 3.21 CPU C State Control

C2C3TT

Default = 0, means [AUTO].

C2 to C3 Transition Timer, PPDN_INIT = 1:10:1:74 Bit [11:0].

CPU C State

Enable or disable the Enhanced Cx state of the CPU, takes effect after reboot.

- Package C state limit Press enter to select C State limit option.
- CPU C3 report Enable/disable CPU C3(ACPI C2) report to OS. Recommended to be disabled.
- CPU C6 report Enable/disable CPU C6(ACPI C2) report to OS. Recommended to be disabled.
- Enhances Halt State (C1E) Enable or disable the Enhanced C1E state of the CPU, takes effect after reboot.
- OS ACPI Cx Report CC3/CC6 to OS ACPI C2 or ACPI C3.

3.2.3.4 CPU HWPM State Control



Figure 3.22 CPU HWPM State Control

HWPM States

Enable CPU HWPM for CPU for better energy performance.

3.2.3.5 CPU Advanced PM Turning

Aptio Setup Utility – Copyright (C) 2017 American IntelRCSetup	Megatrends, Inc.
CPU Advanced PM Turning • Energy Perf BIAS • Program PowerCTL_MSR • Program PPO_CURT_CFG_CTRL_MSR • Program CSR_ENTRY_CRITERIA • Program CSR_SWLTROVRD	Provides hint to CPU for better performance or power savings.
	<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 2.18.1260. Copyright (C) 2017 American Me	egatrends, Inc.

Figure 3.23 CPU Advanced PM Turning

Energy Perf BIAS

Provide hint to CPU for better performance or power savings.

- Program PowerCTL_MSR Program PowerCTL MSR 0x1FC Sub Menu
- Program PRO_CURT_CFG_CTRL_MSR Program PRI_PLANE_CURT_CFG_CTRL_MSR 0x601 Sub Menu.
- Program CSR_ENTRY_CRITERIA
 Program CSR_ENTRY_CRITERIA 1:10:2:0x7C Sub Menu.
 Dragman CSR_ENVL_TROVER
- Program CSR_SWL TROVRD Program CSR_SWL TROVRD 1:10:1:0x78 Sub Menu.

3.2.3.6 DRAM RAPL Configuration



Figure 3.24 DRAM RAPL Configuration

DRAM RAPL Baseline
 DRAM RAPL Baseline enabled and baseline mode.
 Override BW_LIMIT_TF

Allows custom tuning of BW_LIMIT_TF when DRAM RAPL is enabled.

DRAM RAPL Extended Range Select DRAM RAPL Extended Range

Chapter 3 BIOS Operation

3.2.3.7 SOCKET RAPL Config

Aptio Setup Utility - IntelRCSetup	Copyright (C) 2017 American	Megatrends, Inc.
SOCKET RAPL Config FAST_RAPL_NSTRIKE_PL2_DUTY_CYCLE Turbo Pwr Limit Lock Long Pwr Limit Ovrd Long Dur Pwr Limit Long Dur Time Window Pkg Clmp Lim1 Short Dur Pwr Limit En Short Dur Pwr Limit Pkg Clmp Lim2	64 [Disable] [Enable] 0 1 [Below P1] [Enable] 0 [Below P1]		FAST_RAPL_NSTRIKE_PL2_DUTY_CYCL E value between 25 (10%) - 64 (25%)
			<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 2.18.1260. Cc	pyright (C)	2017 American Me	egatrends, Inc.

Figure 3.25 SOCKET RAPL Config

■ Fast_RAPL_NSTRIKE_PL2_DUTY_CYCLE

Fast_RAPL_NSTRIKE_PL2_DUTY_CYCLE value between 25 (10%) - 64 (25%)

Turbo Pwr Limit Lock

Enable or disable locking of turbo settings.

Long Pwr Limit Ovrd

Enable or disable Long Term Power Limit override.

Long Dur Pwr Limit

Turbo Mode Long Duration Power Limit (aka Power Limit 1) in Watts. The value may vary from 0 to Fused Value.

Long Dur Time Window

Long Duration Time Window (aka Power Limit 1 Time) value in seconds. The value may vary from 0 to 56.

Pkg Clmp Lim1

Pkg Clamping limit 1, Allow going below P1.

Short Dur Pwr Limit En

Enable or disable Short Duration Power Limit (aka Power Limit 2)

Short Dur Pwr Limit

Short Duration Power Limit (aka Power Limit 2) value n Watts. The value may vary from 0 to 32767.

Pkg Clmp Lim2 Pkg Clamping limit 2, Allow going below P1.

Short Dur Pwr Limit En Enable or disable Short Duration Power Limit (aka Power Limit 2).

Short Dur Pwr Limit

Short Duration Power Limit (aka Power Limit 2) value n Watts. The value may vary from 0 to 32767.

Pkg Clmp Lim2

Pkg Clamping limit 2, allows going below P1.

3.2.3.8 Common RefCode Configuration



Figure 3.26 Common RefCode Configuration

- MMCFG Base Select MMCFG Base
- MMIOBase MMIOH Base [63:32] ; must be between 4032 – 4078.
- MMIO High Size
 Select MMIO High Size
- Isoc Mode IsocL Disable, Enable
- NeSeg Mode MeSeg: Disable, Enable

3.2.3.9 Memory Configuration

Aptio Setup Utility IntelRCSetup	– Copyright (C) 2017 Amer.	ican Megatrends, Inc.
Integrated Memory Controller (iMC Enforce POR) [Auto]	 Enable to enforce POR restrictions for DDR4 frequency and voltage programming
PPR Type	[PPR Disabled]	
PPR Error Injection test	[Disabled]	
Memory Frequency	[Auto]	
MRC Promote Warnings	[Enabled]	
Promote Warnings	[Enable]	
Halt on mem Training Error	[Enabled]	
Multi-Threaded MRC	[Auto]	
ECC Support	[Auto]	
Enforce Timeout	[Auto]	++: Select Screen
Enhanced Log Parsing	[Disable]	T∔: Select Item
Backside RMT	[Auto]	Enter: Select
Rank Multiplication	[AUTO]	+/-: Change Upt.
LRDIMM Module Delay	[AUTO]	F1: General Help
MemTest opp	[HU(U] 1	F2: Previous values
Dram Maintenance Test	 [Auto]	F4. Save & Evit
Memoru Tune	[UDIMMs and RDIMMs]	ESC: Exit
CECC WA CH Mask	10	
Rank Margin Tool	[Auto]	
RMT Pattern Length	32767	** ▼
-		
Version 2 18 1260	Conunight (C) 2017 Americs	an Meratrands Inc

Figure 3.27 Memory Configuration -1

Enforce POR

Enable to enforce restrictions for DDR4 frequency and voltage programming.

- PPR Type Select PPR Type – Hard/Soft/Disable
- PPR Error Injection test

Enable or disable support for C-script error injection test.

- Memory Frequency Maximum memory frequency selections in Mhz. Do not select reserved.
- MRC Promote Warnings
 Determines if MRV warnings are promoted to system level1
- Promote Warnings
 Determines if warnings are promoted to system level1
- Halt on mem Training Error
 Halt on mem Training Error Disable/Enable
- Multi-Treaded MRC Enable to execute the Memory Reference Code multi-threaded.
- ECC Support
 Enable or disable DDR ECC support
- Enforce Timeout
 Enable or disable forcing cold reset after three months.
- Enhanced Log Parsing Enables additional output in debug log for easier machine parsing.
- Backside RMT
 Enable backside RMT

Rank Multiplication

Force rank multiplication factor for LRDIMM

LRDIMM Module Delay

When 'Disabled', MRC will not use SPD bytes 90-95 for LRDIMM Module Delay. When 'Auto', MRC will boundary check the values and use default values, if SPD is 0 or not of range.

MemTest.

Enable or disable memory test during normal boot.

MemTestLoops

Number of memory test loops during normal boot, set to 0 to run memtest infinitely.

Dram Maintenance Test

Dram Maintenance Test during normal boot.

Memory Type

Select the memory type supported by this platform.

CECC WA CH Mask

CH bitmask to apply CECC WA. 1 bit per CH. Value 2 applies WA on CH1, 3 on CH0 and 1.

Rank Margin Tool

Enables the rank margin tool to run after DDR4 memory training

RMT Pattern Length

Set the pattern length for the Rank Margin Tool.

IntelRCSetup	Copyright (C) 2017 America	n Megatrends, Inc.
CMD Pattern Length Per Bit Margin Training Result Offset Config Attempt Fast Boot Attempt Fast Cold Boot MemTest On Fast Boot RMT On Cold Fast Boot BDAT Data Scrambling Allow SBE during training Platform type input for SPD page s CECC WA Control	32767 [Auto] [Auto] [Auto] [Auto] [Auto] [Disabled] [Auto] [[Auto] [[[[[[[[[[[[[Sets DDR4 SMB Clock Frequencys For SPD Access
Scrambling Seed Low Scrambling Seed High Enable ADR MC BGF threshold DLL Reset Test MC ODT Mode Opp read during WMM Normal Operation Duration Number of Sparing Transaction PSMI Support C/A Parity Enable SMB Clock Frequency	(Auto) 41003 54165 [Disabled] 0 (Auto] [Auto] 1024 4 [Disabled] [Auto] [Auto]	<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>

Figure 3.28 Memory Configuration -2

CMD Pattern Length

Set the pattern length for the Rank Margin Tool.

Per Bit Margin Enable the logging from the sorial part of DDP n

Enable the logging from the serial port of DDR per bit margin data.

Training Result Offset Config

Option to offset the final memory training results.

Attempt Fast Boot

When enabled, portions of memory reference code will be skipped when possible to increase boot speed.

Attempt Fast Cold Boot

When enabled, portions of memory reference code will be skipped when possible to increase boot speed.

MemTest On Fast Boot

Enable or disable memory test during fast boot.

RMT on Cold Fast Boot.

Enable or disable Rank Margin Tool on Cold Fast Boot.

BDAT Enable or disable BDAT

Data Scrambling
 Enable data scrambling.

Allow SBE during training Allows SBE during training, choose enable or disable.

Platform type input for SPD page s This controls the SPD page selection feature. Disabled by Default.

 CECC WA Control This controls the CECC WA. Disabled by Default on L0 and later processor.

CAP ERR FLOW feature Control This controls the CAP ERR FLOW feature. Disabled by Default.

Scrambling Seed Low
 Low 43 bits of the scrambling seed.

Scrambling Seed High

Low 32 bits of the scrambling seed.

Enable ADR Enable the detecting and enabling of ADR.

 MC BGF threshold The HA to MC BGF threshold is used for scheduling MC request in bypass condition.

DLL Reset Test Set this to the number of lops to execute the DDL reset test.

MC ODT Mode Select MC ODT Mode.

Opp read during WMM Enable or disable issuing read commands opportunistically during WMM.

Normal Operation Duration
 Set normal operation duration interval (0 - 65535).

Number of Sparing Transaction Set number of sparing transactions interval (0 - 65535).

- PSMI Support
 PSMI Supports disable or enable
- C/A Parity Enable
 Enable or disable DDR4 Command Address Parity.
- SMB Clock Frequency Sets DDR4 SMB Clock Frequency for SPD Access.
- DIMM Rank Enable Mask

Select ranks to enable or disable per DIMM.

Memory Topology



Figure 3.29 Memory Topology

Display memory topology with DIMM population information.

Chapter 3 BIOS Operation

3.2.3.10 Memory Thermal

Aptio Setup Utility - C IntelRCSetup	opyright (C) 2017 American	Megatrends, Inc.
Set Throttling Mode Phase Shedding Memory Power Savings Mode Memory Power Savings Advanced Options MDLL Off MEMHOT Throttling Mode Mem Electrical Throttling	[CLTT] [Auto] [Auto] [Input-only] [Disabled]	Configure Thermal Throttling Mode. Select OLTT or CLTT mode. ++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.18.1260. Cop	yright (C) 2017 American Mo	egatrends, Inc.

Figure 3.30 Memory Thermal

Set memory thermal settings.

- Set Throttling Mode
 Configure Thermal Throttling Mode, select OLTT or CLTT mode.
- Phase Shedding
 SSR4 VR Static Phase Shedding support.
- Memory Power Saving Mode
 Configures CKE and related Memory Power Saving features.
 Memory Power Savings Advanced Options
- MDLL Off

Enable to shut down MDLL during SR

- MEMHOT Throttling Mode
 Configure MEMHOT Input and Output Mode: Mem Hot Sense Therm Throt or Mem Hot Output Therm Throt.
- MEM Electrical Throttling
 Configure Memory Electrical Throttling

 Aptio Setup Utility - Copyright (C) 2017 American Megatrends, Inc.

 IntelRCSetup

 CK in SR
 [Auto]

 Ch in SR
 [Auto]

- Memory Power Savings Advanced Options

Figure 3.31 Memory Power Savings Advanced Options

Allows users to configure CK behaviors during self-refresh.

Memory Timings & Voltage Override





- DIMM profile

Select the XMP profile to use.

Memory Frequency

Maximum memory frequency selection in Mhz. Do not select reserved.

Memory Map



Memory Map

- Socket Interleave Below 4GB

Splits the 0-4GB address space between two sockets, so that both sockets get a chunk of local memory below 4GB.

- Channel Interleaving
 Select Channel Interleaving setting
- Rank Interleaving
 Select Rank Interleaving setting
- IOT Memory Buffer Reservation
 Select IOT Memory Buffer Reservation
- A7 Mode

A7 Mode disable or enable.

Memory RAS Configuration



Figure 3.33 Memory RAS Configuration

Display and provide options to change the memory RAS Settings.

3.2.3.11 IIO Configuration

Aptio Setup Utility - IntelRCSetup	Copyright (C) 2017 American	Megatrends, Inc.
IIO Configuration		Link training can be done
IIO PCIE Link on phase PCIE Train by BIOS PCIE Hot Plug PCIE ACPI Hot Plug IIOO Configuration IOAT Configuration IIO General Configuration Intel VT for Directed I/O (VT-d) IIO South Complex Configuration	[Post chipset init] [yes] [Disable] [Disable]	init or post chipset init
PCI Express Global Options		
	==== [Epoble]	++: Select Screen
WA 4167453	[Disable]	Fnter: Select
DMI Vc1 Control	[Disable]	+/-: Change Opt.
DMI Vcp Control	[Disable]	F1: General Help
DMI Vom Control	[Disable]	F2: Previous Values
VCO No-Snoop Configuration	[Disable]	F3: Optimized Defaults
Gen3 Phase3 Loop Count	[16]	F4: Save & Exit
SKip Halt On DMI Degradation	[Ulsable]	ESU: EXIT
SLD WA Revision	[ges]	
RX Clock WA	[Disable]	
Version 2.18.1260. Co	pyright (C) 2017 American M	legatrends, Inc.

Figure 3.34 IIO Configuration

IIO PCIe Link on phase Link training can be done either before memory chipset init or post chipset init

- PCI Express Global Options:
- TX EQ WA Use special table for TX_EQ and vendor specific cards.
- WA 4167453 Disable IIO VCP. Disable PCH VC1, set IIO CV1 & PCH VCP to TC2, clear irp_misc_dfx0.force_no_snp_on_vc1_vcm
- DMI Vc1 Control Enable or disable DMI Vc1
- DMI Vcp Control Enable or disable DMI Vcp
- DMI Vcm Control Enable or disable DMI Vcm
- VC0 No-Snoop Configuration Enable No-Snoop on reads and writes for Vc0 traffic.
- Gen3 Phase3 Loop Count
 Change Loop Count to 1, 4, 16, or 256.
- Skip Phase3 Loop Count Enable this option to avoid the system to be halted on DMI width/link degradation.
- Power Halt on DMI Degradation Power down unused ports
- IIO Configuration

Aptio Setup Utility - (IntelRCSetup	Copyright (C) 2017 American	Megatrends, Inc.
IOU2 (IIO PCIE Port 1) IOU1 (IIO PCIE Port 3) No PCIE port active ECO Socket O PcieDO1FO - Port 1A Socket O PcieD02FO - Port 2A Socket O PcieD02F2 - Port 2C Socket O PcieD03FO - Port 3A	[Auto] [Auto] [PCU Squelch exit ig]	Selects PCIe port Bifurcation for selected slot(s)
IOU1 Non-Posted Prefetch	[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 2.18.1260. Cop	oyright (C) 2017 American Mu	egatrends, Inc.

Figure 3.35 IIO Configuration

- IOU2 (IIO PCIe Port 1)

Select PCIe port bifurcation for selected slot(s). Options: x4x4, x8, Auto

- IOU1 (IIO PCIe Port 2)
 Select PCIe port bifurcation for selected slot(s)
 Options: x4x4x4x4, x4x4x8, x8x4x4, x8x8, x16, auto
- No PCle port active ECO
 Workaround settings when no PCle port active
- Socket 0 PcieD01F0 Port 1A



Figure 3.36 Socket 0 PcieD01F0 - Port 1A

In auto mode the BIOS will remove the EXP port if there is no device or errors on that device or device is not HP capable. Use disable to hide its CFG space.

- Socket 0 PcieD02F0 - Port 2A

Aptio Setup Utility - IntelRCSetup	- Copyright (C) 2017 American	Megatrends, Inc.
Socket O PcieDO2FO – Port 2A		In auto mode the BIOS will nemous the EVP port if there
PCI-E Port Hot Plug Capable PCI-E Port Link Link Speed Override Max Link Width PCI-E Port DeEmphasis PCI-E Port Link Status PCI-E Port Link Max PCI-E Port Link Speed PCI-E ASPM Support	[Auto] [Disable] [Enable] [Auto] [Auto] [-6.0 dB] Linked as x1 ERROR: Not Available Gen 1 (2.5 GT/s) [Auto]	is no device or errors on that device and the device is not HP capable. Disable is used to disable the port and hide its CFG space.
PCI-E Port LOS Exit Latency PCI-E Port L1 Exit Latency Fatal Err Over Corr Err Over LOS Support PM ACPI Mode Gen3 Eq Mode Gen3 Spec Mode Gen3 DN TX Preset Gen3 DN TX Preset Hint Gen3 UP TX Preset	[4uS - 8uS] [8uS - 16uS] [Disable] [Disable] [Disable] [Disable] [Disable] [Auto] [Auto] [Auto] [Auto] [Auto]	<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 2.18.1260. (Copyright (C) 2017 American M	legatrends, Inc.

Figure 3.37 Socket 0 PcieD02F0 - Port 2A

In auto mode the BIOS will remove the EXP port if there is no device or errors on that device or device is not HP capable. Disable is used to disable the port and hide its CFG space.

- Socket 0 PcieD02F2 - Port 2C

Aptio Setup Utility - IntelRCSetup	Copyright (C) 2017 America	n Megatrends, Inc.
Socket 0 PcieD02F2 – Port 2C		▲ In auto mode the BIOS will
PCT_E Port	[Auto]	is no device or errors on that
Hot Plug Canable	[Disable]	device and the device is not
PCT-E Port Link	[Enable]	HP canable Disable is used
Link Speed	[Auto]	to disable the nort and hide
Override Max Link Width	[Auto]	its CEG snace
PCI-E Port DeEmohasis	[-6.0.dB]	rto ora opace.
PCI-E Port Link Status	Linked as x1	
PCI-E Port Link Max	ERROR: Not Available	
PCI-E Port Link Sneed	Gen 1 (2 5 GT/s)	
PCT-E ASPM Support	[Auto]	
PCI-E Port LOs Exit Latency	[4uS - 8uS]	
PCI-E Port 11 Exit Latency	[8uS - 16uS]	++: Select Screen
Fatal Err Over	[Disable]	↑↓: Select Item
Non-Fatal Err Over	[Disable]	Enter: Select
Corr Err Over	[Disable]	+/-: Change Opt.
LOs Support	[Disable]	F1: General Help
PM ACPI Mode	[Disable]	F2: Previous Values
Gen3 Ea Mode	[Auto]	F3: Optimized Defaults
Gen3 Spec Mode	[Auto]	F4: Save & Exit
Gen3 Phase2 Mode	[Hardware Adaptive]	ESC: Exit
Gen3 DN Tx Preset	[Auto]	
Gen3 DN Rx Preset Hint	[Auto]	
Gen3 UP Tx Preset	[Auto]	▼
Version 2.18.1260. C	opyright (C) 2017 American	Megatrends, Inc.

Figure 3.38 Socket 0 PcieD02F2 – Port 2C

In auto mode the BIOS will remove the EXP port if there is no device or errors on that device or device is not HP capable. Disable is used to disable the port and hide its CFG space.

- Socket 0 PcieD03F0 - Port 3A

Socket O PcieDO3FO – Port 3A		▲ In auto mode the BIOS will
PCI-E Port	[Auto]	is no device or errors on that
PCI-E Port Link	[Fnahle]	HP canable Disable is used
Link Sneed	[Auto]	to disable the nort and hide
Override Max Link Width	[Auto]	its CEG snare
PCI-E Port DeEmphasis	[-6.0 dB]	
PCI-E Port Link Status	Link Did Not Train	
PCI-E Port Link Max	Max Width x16	
PCI–E Port Link Speed	Link Did Not Train	
PCI-E ASPM Support	[Auto]	
PCI-E Port LOs Exit Latency	[4uS - 8uS]	
PCI—E Port L1 Exit Latency	[8uS - 16uS]	↔: Select Screen
Fatal Err Over	[Disable]	t↓: Select Item
Non-Fatal Err Over	[Disable]	Enter: Select
Corn Ern Over	[Disable]	+/-: Change Opt.
LOs Support	[Disable]	F1: General Help
PM ACPI Mode	[Disable]	F2: Previous Values
Gen3 Eq Mode	[Auto]	F3: Optimized Defaults
Gen3 Spec Mode	[Auto]	F4: Save & Exit
Gen3 Phase2 Mode	[Hardware Adaptive]	ESC: Exit
Gen3 DN Tx Preset	[Auto]	
Gen3 DN Rx Preset Hint	[Auto]	
Gen3 UP Tx Preset	[Auto]	•

Figure 3.39 Socket 0 PcieD03F0 – Port 3A

In auto mode the BIOS will remove the EXP port if there is no device or errors on that device or device is not HP capable. Disable is used to disable the port and hide its CFG space.

IOAT Configuration

	Aptio Setup Utility – Copyright IntelRCSetup	(C) 2017 American	Megatrends, Inc.
Enable IOAT No Snoop Disable TPH	[Disable] [Disable] [Enable]		Control to enable/disable IOAT devices ++: Select Screen t: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
	Version 2.18.1260. Copyright (C) 2017 American Mu	egatrends, Inc.

Figure 3.40 IOAT Configuration

Chapter 3 BIOS Operation

- Enable IOAT

Control to enable ot disable IIOAT devices.

No Snoop

No Snoop enable or disable for each CB device.

- Disable TPH
 - TLP Processing Hint disable.
- IIO General Configuration

Aptio Setup Uti. IntelRCSetup	lity – Copyright (C) 2017 An	merican Megatrends, Inc.
TXT DPR memory setting	[3M DPR]	Allows selection of the TXT DPR size in sustem
IIO 0		
IIO IOAPIC	[Enable]	
		++: Select Screen
		↑↓: Select Item Enter: Select
		+/−: Change Opt. F1: General Help
		F2: Previous Values F3: Optimized Defaults
		F4: Save & Exit ESC: Exit
Version 2.18.12	260. Copyright (C) 2017 Amer	rican Megatrends, Inc.

Figure 3.41 IIO General Configuration

- TXT DPR memory setting

Allow selection of the TXT DPR size in system.

- IIO 0

User Defined

- IIO IOAPIC

Enable or disable the IIO IOAPIC.

Intel VT for Directed I/O (VT-d)

Aptio Setup Utility – IntelRCSetup	Copyright	(C) 2017 American	Megatrends, Inc.
Intel VT for Directed I/O (VT-d)			Enable/Disable Azalea VCp Optimizations
VTd Azalea VCp Optimizations Intel VT for Directed I/O (VT-d) ACS Control Interrupt Remapping Coherency Support (Non-Isoch) Coherency Support (Isoch)	(Disable) (Enable) (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 2.18.1260. C	opyright (C) 2017 American Me	egatrends, Inc.

Figure 3.42 Intel VT for Directed I/O (VT-d)

- Vtd Azalea VCp Optimizations

Enable or disable Azalea VCp Optimizations.

- Intel VT for Directed I/O (VT-d)
 Enable or disable Intel Virtualization Technology for Directed I/O (VT-d) by reporting the I/O device assignment to VMM through DMAR ACPI Tables.
- ACS Control

Enable: Programs ACS only to Chipset PCIe Root Ports Bridges. Disable: Programs ACS to all PCIe bridges.

- Interrupt Remapping

Enable or disable VT-F Interrupt Remapping support.

- Coherency Support (Non-Isoch)
 Enable or disable non-Isoch VT-D Engine Coherency support.
- Coherency Support (Isoch)
 Enable or disable Isoch VT-D Engine Coherency support.

IIO South Complex Configuration

Aptio Setup Utility - IntelRCSetup	Copyright (C) 2017 American	Megatrends, Inc.	
IIO South Complex Configuration		Force Enable / Disable SC GbE physical function 0	
SC GbE PFO (10GbE) SC GbE PF1 (10GbE)	[Auto] [Auto]		
		<pre>++: Select Screen tl: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>	
Version 2.18.1260. Copyright (C) 2017 American Megatrends, Inc.			

Figure 3.43 IIO South Complex Configuration

- SC GbE PF0 (10GbE)
 Force Enable or disable SC GbE physical function 0.
- SC GbE PF1 (10GbE)
 Force Enable or disable SC GbE physical function 1.

3.2.3.12 PCH Configuration



Figure 3.44 PCH Configuration

PCH Devices

Aptio Setup Utility - IntelRCSetup	Copyright (C) 2017 American	Megatrends, Inc.	
Board Capability DeepSx Power Policies GP27 Wake From DeepSx SMBUS Device PCH Server Error Reporting Mode (S PCH Display Serial IRQ Mode High Precision Timer Boot Time with HPET Timer External SSC Enable - CK420 PCH state after G3 PCH CRID	[DeepSx] [Disabled] [Disabled] [Enabled] [Disabled] [Continuous] [Disabled] [Disabled] [Disabled] [S5] [Disabled]	Board Capability – SUS_PWR_DN_ACK –> Send Disabled to PCH, DeepSx –> Show DeepSx Policies	
		<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 2.18.1260. Copyright (C) 2017 American Megatrends, Inc.			

Figure 3.45 PCH Devices
- Board Capability

Board Capability – SUS_PWR_DN_ACK ? Send Disable to PCH, DeepSx - >Show DeepSx Policies.

- DeepSx Power Policies
 Configure the DeepSx Mode configuration.
- GP27 Wake From DeepSx

Wake from DeepSx by the assertion of DP27 pin.

- SMbus Device
 Enable or disable SMBus Device.
- PCH Server Error Reporting Mode (SERM)
 - When enable MCH is final target of all final target to all errors.
- PCH Display
 Enable or disable PCH Display.
- Serial IRQ Mode
 Configure Serial IRQ Mode.
- High Precision Timer
 Enable or disable the High Precision event Timer.
- Boot Time with HPET Timer
 Boot time calculation with High Precision Event Timer enabled.
- External SSC Enable CK420
 Enable Spread Spectrum only affects external clock generator.
- PCH state after G3 Select S0/S5 for ACPI state after a G3.
- PCH CRID

Enable or disable PCH's CRID.

PCH Express Configuration

Aptio Setup Utility IntelRCSetup) – Copyright (C) 2017 America	an Megatrends, Inc.
Subtractive Decode PCIe-USB Glitch W/A	[Disabled] [Disabled]	PCIe-USB Glitch W/A for bad USB device(s) connected behind PCIE/PEG Port.
 PCI Express Root Port 0 PCI Express Root Port 1 PCI Express Root Port 2 PCI Express Root Port 3 PCI Express Root Port 4 PCI Express Root Port 5 PCI Express Root Port 6 PCI Express Root Port 7 (Intel i2 	210 Giga Lan)	
		<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 2.18.1260.	Copyright (C) 2017 American	Megatrends, Inc.

Figure 3.46 PCH Express Configuration

- PCIe-USB Glitch W/A

PCIe-USB Glitch W/A for bad USB device(s) connected behind PCIE/PEG Port.

PCI Express Root Port 0 ~ 7

Select one of the PCI Express Root Port, press <enter> into the table to change the setting.

PCH SATA Configuration

Aptio Setup Utility - IntelRCSetup	Copyright (C) 2017 American	Megatrends, Inc.
PCH SATA Configuration		Enable or Disable SATA
SATA Controller Configure SATA as SATA test mode ▶ SATA Mode options SATA AHCI LPM Support Aggressive Link Power Mana	[Enabled] [AHCI] [Disabled] [Enabled] [Enabled]	
SATA Port O Software Preserve Port O Spin Up Device SATA Device Type SATA Port 1 Software Preserve Port 1 Spin Up Device SATA Device Type	[Not Installed] Unknown [Enabled] [Disabled] [Hard Disk Drive] [Not Installed] Unknown [Enabled] [Disabled] [Hard Disk Drive]	++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.18.1260. Cc	ppyright (C) 2017 American M	egatrends, Inc.

Figure 3.47 PCH SATA Configuration

Press <enter> into each option to select SATA devices and settings. Select configuration SATA as AHCI or IDE, default by AHCI.

USB Configuration

Aptio Setup Utility IntelRCSetup	– Copyright (C) 2017 Americar	Megatrends, Inc.
Subtractive Decode PCIe–USB Glitch W/A	[Disabled] [Disabled]	PCIE–USB Glitch W/A for bad USB device(s) connected behind PCIE/PEG Port.
 PCI Express Root Port 0 PCI Express Root Port 1 PCI Express Root Port 2 PCI Express Root Port 3 PCI Express Root Port 4 PCI Express Root Port 5 PCI Express Root Port 6 PCI Express Root Port 7 (Intel 121) 	0 Giga Lan)	
		<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 2.18.1260.	Copyright (C) 2017 American ⊧	legatrends, Inc.

Figure 3.48 USB Configuration

- USB Precondition

Precondition work on USB host controller and root ports for faster enumeration.

- xHCI Mode

Mode of operation of xHCI controller.

- Trunk Clock Gating (BTCG)
 Enable or disable BTCG.
- USB Ports Per-Port Disable Control
 Control each of the USB ports (0~13) disabling.
- xHCI Idle L1

Enabled xHCI Idle L1. Disabled to workaround USB3 hot plug will fail after 1 hot plug removal. Please put the system to G3 for the new settings to take effect.

Security Configuration

Aptio Setup Utility - IntelRCSetup	Copyright (C) 2017 American	Megatrends, Inc.
Security Configuration GPIO Lockdown RTC Lock BIOS Lock Host Flash Lock-Down Gbe Flash Lock-Down	[Disabled] [Enabled] [Enabled] [Enabled] [Disabled]	Enable/Disable the PCH GPIO Lockdown feature.
		<pre>++: Select Screen f1: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
Version 2.18.1260. Co	pyright (C) 2017 American M	egatrends, Inc.

Figure 3.49 Security Configuration

- GPIO Lockdown

Enable or disable the PCH GPIO Lockdown feature.

- RTC 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.
- Host Flash Lock-Down
 Enable or disable Host flash lock-down.
- GbE Flash Lock-Down
 Enable or disable GbE flash lock-down.

3.2.3.13 Miscellaneous Configuration

Aptio Setup Utility – Copyright (C) 2017 Americar <mark>IntelRCSetup</mark>	n Megatrends, Inc.
Miscellaneous Configuration Fan PWM Offset [4096B] PCIE Max Read Request Size [4096B] PCIE Latency Tolerance Reporting [Enable] PCI Minimum Secondary Bus Number 1 PCIE Extended Tag Enable [Enable] PCIE AtomicOp Request Support [Disable] Breakpoint Type [None] BIOS Guard [Disabled] Serial Debug Message Level [Disable] Trace Messages [Disabled] Training Messages [Disabled] RC Promote Warnings [Enabled] RC Promote MRC Warnings [Enabled] Active Video [Offboard Device] TargetVGA Vga From CPU 0	Specify fan speed offset ++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.18.1260. Copyright (C) 2017 American ⊧	legatrends, Inc.

Figure 3.50 Miscellaneous Configuration

Fan PWN Offset

Specify fan speed offset.

PCIe Max Read Request Size
 Set Max Read Request Size

3.2.3.14 Server ME Configuration

Aptio Setup Utility - IntelRCSetup	Copyright (C) 2017 American	Megatrends, Inc.
General ME Configuration Operational Firmware Version ME Firmware Type Recovery Firmware Version ME Firmware Features ME Firmware Status #1 ME Firmware Status #2 Current State Error Code Altitude MCTP Bus Owner Server ME General Configuration	06:3.0.3.27 SPS 06:3.0.3.27 SiEn+NM+PECIProxy+ICC 0x000F0345 0xB800C000 Operational No Error 80000000 0	The altitude of the platform location above the see level, expressed in meters. The hex number is decoded as 2's complement signed integer. Provide the 80000000 value if the altitude is unknown. ++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.18.1260. Co	pyright (C) 2017 American M	egatrends, Inc.

Figure 3.51 Server ME Configuration

Altitude

The altitude of the platform location above the see level, expressed in meters. The hex number is decoded as 2's complement signed integer. Provide the 80000000 value if the altitude is unknown.

MCTP Bus Owner

MCTP bus owner location on PCIe: [15:8] bus, [7:3] device, [2:0] function. If all zero sending bus owner is disabled.

3.2.3.15 Runtime Error Logging

Aptio Setup Utility - IntelRCSetup	· Copyright ((C) 2017 American	Megatrends, Inc.
Runtime Error Logging			System Error enabling and
System Errors S/W Error Injection Support Clear McBankErrors System Poison IIO Error Enable PCH Error Enable Enable Cloaking Whea Settings : Memory Error Enabling : Memory Error Enabling : PCI/PCI Error Enabling :	[Enable] [Disable] [Disable] [Jisable] [yes] [Jisable]		++: Select Screen ++: Select Screen +: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.18.1260. C	opyright (C)	2017 American Me	egatrends, Inc.

Figure 3.52 Runtime Error Logging

Press <enter> to view or change the runtime error log configuration.

System Errors

System Error enabling and logging setup option.

S/W Error Injection Support

When Enable S/W Error Injection is supported by unlocking MSR 0x790.

Clear McBankErroes

Enable or disable clearing McBank errors on warm reset.

System Poison

Enable or disable core, uncore and IIO poison.

Chapter 3 BIOS Operation

3.2.3.16 Reserve Memory

Aptio Setup Utility IntelRCSetup	– Copyright (C) 2017 Americ	an Megatrends, Inc.
Reserve Memory Range Start Address Reserve TAGEC Memory	[Disabled] 100000 [Disable]	Sets aside an empty memory page that is hidden from the OS ++: Select Screen
		T4: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.18.1260.	Copyright (C) 2017 American	Megatrends, Inc.

Figure 3.53 Reserve Memory

- Reserve Memory Range Sets aside an empty memory page that is hidden from the OS.
- Reserve TAGEC Memory Reserve 16M for TAGEC.

3.2.4 Server Mgmt

Select the IntelRCSetup tab from the SOM-5992 setup screen to enter the BIOS Setup screen. You can select the items by highlighting it using by the <Arrow> keys.

Aptio Setup Util Main Advanced IntelRCSetup	ity – Copyright (C) 2017 Ameri Server Mgmt <mark>Security Boot</mark>	can Megatrends, Inc. Event Logs Save & Exit
BMC Self Test Status BMC Device ID BMC Device Revision BMC Firmware Revision IPMI Version BMC Support Wait For BMC FRB-2 Timer Olicy OS Watchdog Timer OS Wtd Timer Policy OS Wtd Timer Policy System Event Log BMC self test log BMC network configuration View System Event Log BMC User Settings	PASSED 32 1 1.3 2.0 [Enabled] [Enabled] [Enabled] [6 minutes] [Do Nothing] [Disabled] [10 minutes] [Reset]	Enable/Disable interfaces to communicate with BMC ++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
version 2.18.12	60. copyrignτ (c) 2017 America	in Megatrends, Inc.

Figure 3.54 Server Mgmt

BMC Support

Enable or disable interfaces to communicate with the BMC.

Wait For BMC

Enable or disable to wait BMC response for specified time out. In PILOTII, BMC starts ar the same time when BIOS starts during AC power on. It takes around 30 seconds to initialize host to BMC interfaces.

FRB-2 Timer

Enable or disable FRB-2 timer (POST timer)

FRB-2 Timer Timeout

Enter values between 3 to 6 min for FRB-2 timer expiration value.

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

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

OS Wtd Timer Policy

3.2.4.1 System Event Log

Press <Enter> to change the SEL event log configuration.

Aptio Setup Utility – Serve	Copyright (C) 2017 American r Mgmt	Megatrends, Inc.
Enabling/Disabling Options		Change this to enable or
SEL Components	[Enabled]	disable all features of System Event Logging during boot.
Erasing Settings		
Enase SEL	[No]	
When SEL is Full	[Do Nothing]	
Custom EFI Logging Options		
Log EFI Status Codes	[Ennon code]	
NOTE: All values changed here do not until computer is restarted.	take effect	
		1. Select Item
		Enter: Select
		+/-: Change Opt.
		F1: General Help
		F2: Previous Values
		F3: Optimized Defaults
		F4: Save & Exit
		ESC: Exit
Version 2.18.1260. Copyright (C) 2017 American Megatrends, Inc.		

Figure 3.55 System Event Log

SEL Components

Change this to enable or 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 code or only progress code or both.

3.2.4.2 BMC self test log

Logs the report returned by BMC self test command.



Figure 3.56 BMC self test log

Erase Log

Choose Yes or No, to erase log on every reset.

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

3.2.4.3 BMC network configuration

Check configuration BMC network parameters.

Aptio Setup Utility – Serve	Copyright (C) 2017 American r Mgmt	Megatrends, Inc.
BMC network configuration жананананананананананан Configure IPV4 support жананананананананананан		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 sour Station IP address Subnet mask Station MAC address	[Unspecified] StaticAddress 0.0.0.0 0.0.0.0 00-0b-ab-00-0a-1a	parameters during BIOS phase
Router IP address Router MAC address	0.0.0.0 00-00-00-00-00	++: Select Screen
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx		I∔: Select Item Enter: Select +/-: Change Opt. F1: General Help
Lan channel 1		F2: Previous Values F3: Optimized Defaults
IPV6 is not supported in BMC.		F4: Save & Exit ESC: Exit
Version 2.18.1260. Co	pyright (C) 2017 American M	egatrends, Inc.

Figure 3.57 BMC network configuration

Configuration Address source

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

3.2.4.4 BMC User Settings

Press <Enter> to select the BMC user setting in this page to add or delete user information.



Figure 3.58 BMC User Settings

3.2.5 Security

Select the Security tab from the SOM-5992 setup screen to enter the BIOS Setup screen. You can select the items by highlighting it using the <Arrow> keys. All Plug and Play BIOS Setup options are described in this section. The Plug and Play BIOS Setup screen is shown below.

Aptio Setup Main Advanced IntelRCSe	<mark>Utility – Copyright (C) 2017 An</mark> tup Server Mgmt <mark>Security Boo</mark>	merican Megatrends, Inc. Dt Event Logs Save & Exit
Password Description		Set Administrator Password
If ONLY the Administrator' then this only limits acce only asked for when enteri If ONLY the User's passwor is a power on password and boot or enter Setup. In Se have Administrator rights. The password length must b in the following range: Minimum length	s password is set, ss to Setup and is ng Setup. d is set, then this must be entered to tup the User will e 3	
Maximum length	20	
Administrator Password User Password ▶ Secure Boot menu		<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>

Figure 3.59 Security

Administration Password

Press <enter> and user is able to set the Administration Password.

User Password

Press <enter> and user is able to set the User Password.

Secure Boot menu

Press <enter> to start Customizable Secure Boot settings.

3.2.6 Boot

Select the Boot tab from the SOM-5992 setup screen to enter the BIOS Setup screen. You can select the items by highlighting it using by the <Arrow> keys.



Figure 3.60 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 Enable or disable Quiet Boot option.
- Boot Option #1
 Sets the system boot order.
- New Boot Option Policy Controls the placement of newly detected UEFI boot options.

3.2.7 Event Logs

Select the Event Logs tab from the SOM-5992 setup screen to enter the BIOS Setup screen. You can select the items by highlighting it using the <Arrow> keys.

Aptio Setup Utility – Copyright (C) 2017 American Main Advanced IntelRCSetup Server Mgmt Security Boot <mark>Ever</mark>	Megatrends, Inc. It Logs <mark>Save & Exit</mark>
 Change Smbios Event Log Settings View Smbios Event Log 	Press <enter> to change the Smbios 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 2.18.1260. Copyright (C) 2017 American Me	gatrends, Inc.

Figure 3.61 Event Logs

Change Smbios Event Log Settings
 Press <enter> to change the smbios event Log configuration.

 View Smbios Event Log

Press <enter> to change the smbios event Log records.

3.2.8 Save & Exit



Figure 3.62 Save & Exit

3.2.8.1 Save Changes and Exit

When users have completed system configuration, select this option to save changes, exit BIOS setup menu and reboot the computer if necessary to take effect of all system configuration parameters.

3.2.8.2 Discard Changes and Exit

Select this option to quit Setup without making any permanent changes to the system configuration.

3.2.8.3 Save Changes and Reset

When users have completed system configuration, select this option to save changes, exit BIOS setup menu and reboot the computer to take effect of all system configuration parameters.

3.2.8.4 Discard Changes and Reset

Select this option to quit Setup without making any permanent changes to the system configuration and reboot the computer.

3.2.8.5 Save Changes

When users have completed system configuration, select this option to save changes without exiting the BIOS setup menu.

3.2.8.6 Discard Changes

Select this option to discard any current changes and load the previous system configuration.

3.2.8.7 Restore Defaults

The SOM-5992 automatically configures all setup items to optimal settings when users select this option. Optimal Defaults are designed for maximum system performance, but may not work best for all computer applications. In particular, do not use the optimal defaults if the user's computer is experiencing system configuration problems.

3.2.8.8 Save as User Defaults

When users have completed system configuration, select this option to save changes as default without exiting the BIOS setup menu.

3.2.8.9 Restore User Defaults

The users can select this option to restore user defaults.



S/W Introduction & Installation

Sections include: ■ S/W Introduction ■ Driver Installation ■ Advantech iManager

4.1 S/W Introduction

The mission of Advantech Embedded Software Services is to "Enhance quality of life with Advantech platforms and Microsoft Windows embedded technology." We enable Windows Embedded software products on Advantech platforms to more effectively support the embedded computing community. Customers are freed from the hassle of dealing with multiple vendors (Hardware suppliers, System integrators, Embedded OS distributor) for projects. Our goal is to make Windows Embedded Software solutions easily and widely available to the embedded computing community.

4.2 **Driver Installation**

To install the drivers on a windows-based operation system, please connect to internet and browse the website http://support.advantech.com.tw and download the drivers that you want to install and follow Driver Setup instructions to complete the installation.

4.2.1 Windows Driver Setup

To install the drivers on a windows-based OS, please connect to the internet and go to http://support.advantech.com.tw to download the drivers that you want to install and follow Driver Setup instructions to complete the installation.

4.2.2 Other OS

To install the drivers for other OS, please connect to internet and browse the browse the website http://support.advantech.com.tw to download the setup file.

4.3 Advantech iManager

Advantech's platforms come equipped with iManager, a micro controller that provides embedded features for system integrators. Embedded features have been moved from the OS/BIOS level to the board level, to increase reliability and simplify integration.

iManager runs whether the operating system is running or not; it can count the boot times and running hours of the device, monitor device health, and provide an advanced watchdog to handle errors as they happen. iManager also comes with a secure & encrypted EEPROM for storing important security keys or other customer information. All the embedded functions are configured through the API and provide corresponding utilities to demonstrate. These APIs comply with PICMG EAPI (Embedded Application Programmable Interface) specifications and makes these embedded features easier to integrate, speed development schedules, and provide customer's with software continuity while upgrading hardware. More details of how to use the APIs and utilities, please refer to the Advantech iManager 2.0 Software API User Manual.

Control



General Purpose Input/Output is a flexible parallel interface defeat Purpose inpurviupur is a revole parale interact that allows a variety of custom connections. It allows users to monitor the level of algoral input or set the output status to switch on/off a device. Our API also provides Programmable GPIO, which allows developers to dynamically set the GPIO input or output status



SMBus is the System Management Bus defined by Intel® Corporation in 1995. It is used in personal computers and servers for low-speed system management communications. The SMBus API allows a developer to interface a embedded system environment and transfer serial messages using the SMBus protocols, allowing multiple simultaneous device



PC is a bi-directional two wire bus that was developed by Phillips for use in their televisions in the 1980s. The PC API allows a developer to interface with an embedded system environment and transfer serial messages using the PC protocols, allowing multiple simultaneous device cont

Display



The Brightness Control API allows a developer to interface with an embedded device to easily control brightness.





The Backlight API allows a developer to control the backlight (screen) on/off in an embedded device.

Monitor



A watchdoo timer (WDT) is a device that performs a specific operation after a certain period of time if something goes wrong and the system does not recover on its own. A watchdog timer can be programmed to perform a warm boot (restarting the system) after a certain number of seconds.



The Hardware Monitor (HWM) API is a system health supervision API that inspects certain condition indexes, such as fan speed, temperature and voltage



The Hardware Control API allows developers to set the PWM (Pulse Width Modulation) value to adjust fan speed or other devices; it can also be used to adjust the LCD brightness.

Power Saving



Make use of Intel SpeedStep technology to reduce power power consumption. The system will automatically adjust the CPU Speed depending on system loading.



Refers to a series of methods for reducing power consumption in



computers by lowering the clock frequency. These APIs allow the user to lower the clock from 87.5% to 12.5%.



Pin Assignment

This appendix gives you the information about the hardware pin assignment of the SOM-5992 CPU System on Module.

Sections include:

■ SOM-5992 Type 7 Pin Assignment

A.1 SOM-5992 Type 7 Pin Assignment

This section gives SOM-5992 pin assignment on COM Express connector which compliant with COM Express R3.0 Type 7 pin-out definitions. More details about how to use these pins and get design reference. Please contact to Advantech for design guide, checklist, reference schematic, and other hardware/software supports.

SOM-5992 ROW A, B			
A1	GND(FIXED)	B1	GND(FIXED)
A2	GBE0_MDI3-	B2	GBE0_ACT#
A3	GBE0_MDI3+	B3	LPC_FRAME#
A4	GBE0_LINK100#	B4	LPC_AD0
A5	GBE0_LINK1000#	B5	LPC_AD1
A6	GBE0_MDI2-	B6	LPC_AD2
A7	GBE0_MDI2+	B7	LPC_AD3
A8	GBE0_LINK#	B8	LPC_DRQ0#
A9	GBE0_MDI1-	B9	LPC_DRQ1#
A10	GBE0_MDI1+	B10	LPC_CLK
A11	GND(FIXED)	B11	GND(FIXED)
A12	GBE0_MDI0-	B12	PWRBTN#
A13	GBE0_MDI0+	B13	SMB_CK
A14	-	B14	SMB_DAT
A15	-	B15	SMB_ALERT#
A16	SATA0_TX+	B16	SATA1_TX+
A17	SATA0_TX-	B17	SATA1_TX-
A18	SUS_S4#	B18	SUS_STAT#
A19	SATA0_RX+	B19	SATA1_RX+
A20	SATA0_RX-	B20	SATA1_RX-
A21	GND(FIXED)	B21	GND(FIXED)
A22	PCIE_TX15+	B22	PCIE_RX15+
A23	PCIE_TX15-	B23	PCIE_RX15-
A24	SUS_S4#	B24	PWR_OK
A25	PCIE_TX14+	B25	PCIE_RX14+
A26	PCIE_TX14-	B26	PCIE_RX14-
A27	BATLOW#	B27	WDT
A28	(S)ATA_ACT#	B28	RSVD
A29	RSVD	B29	RSVD
A30	RSVD	B30	RSVD
A31	GND(FIXED)	B31	GND(FIXED)
A32	RSVD	B32	SPKR
A33	RSVD	B33	I2C_CK
A34	BIOS_DIS0#	B34	I2C_DAT
A35	THRMTRIP#	B35	THRM#
A36	PCIE_TX13+	B36	PCIE_RX13+
A37	PCIE_TX13-	B37	PCIE_RX13-
A38	GND	B38	GND
A39	PCIE_TX12+	B39	PCIE_RX12+
A40	PCIE_TX12-	B40	PCIE_RX12-
A41	GND(FIXED)	B41	GND(FIXED)
A42	USB2-	B42	USB3-
A43	USB2+	B43	USB3+

A44	USB 2 3 OC#	B44	USB 0 1 OC#
A45	USB0-	B45	USB1-
A46	USB0+	B46	USB1+
A47	VCC_RTC	B47	-
A48	RSVD	B48	-
A49	GBE0_SDP	B49	SYS_RESET#
A50	LPC SERIRQ	B50	CB RESET#
A51	GND(FIXED)	B51	GND(FIXED)
A52	PCIE_TX5+	B52	PCIE_RX5+
A53	PCIE_TX5-	B53	PCIE_RX5-
A54	GPI0	B54	GPO1
A55	PCIE_TX4+	B55	PCIE_RX4+
A56	PCIE_TX4-	B56	PCIE_RX4-
A57	GND	B57	GPO2
A58	PCIE_TX3+	B58	PCIE_RX3+
A59	PCIE_TX3-	B59	PCIE_RX3-
A60	GND(FIXED)	B60	GND(FIXED)
A61	PCIE_TX2+	B61	PCIE_RX2+
A62	PCIE_TX2-	B62	PCIE_RX2-
A63	GPI1	B63	GPO3
A64	PCIE_TX1+	B64	PCIE_RX1+
A65	PCIE_TX1-	B65	PCIE_RX1-
A66	GND	B66	WAKE0#
A67	GPI2	B67	WAKE1#
A68	PCIE_TX0+	B68	PCIE_RX0+
A69	PCIE_TX0-	B69	PCIE_RX0-
A70	GND(FIXED)	B70	GND(FIXED)
A71	PCIE_TX8+	B71	PCIE_RX8+
A72	PCIE_TX8-	B72	PCIE_RX8-
A73	GND	B73	GND
A74	PCIE_TX9+	B74	PCIE_RX9+
A75	PCIE_TX9-	B75	PCIE_RX9-
A76	GND	B76	GND
A77	PCIE_TX10+	B77	PCIE_RX10+
A78	PCIE_TX10-	B78	PCIE_RX10-
A79	GND	B79	GND
A80	GND(FIXED)	B80	GND(FIXED)
A81	PCIE_TX11+	B81	PCIE_RX11+
A82	PCIE_TX11-	B82	PCIE_RX11-
A83	GND	B83	GND
A84	NCSI_IX_EN	B84	VCC_5V_SBY
A85	GPI3	B85	VCC_5V_SBY
A86	RSVD	B86	VCC_5V_SBY
A87	RSVD	B87	VCC_5V_SBY
A88	PCIE_CK_REF+	B88	BIOS_DIS1#
A89		889	
A90	GND(FIXED)	890	
A91	SPI_POWER	891	
A92	SPI_MISU	892	
A93		893	
A94	SPI_ULK	894	
A95	SPI_MOSI	B95	NCSI_TXD1

A96	TPM_PP	B96	NCSI_TXD0
A97	-	B97	SPI_CS#
A98	SER0_TX	B98	NCSI_ARB_IN
A99	SER0_RX	B99	NCSI_ARB_OUT
A100	GND(FIXED)	B100	GND(FIXED)
A101	SER1_TX	B101	FAN_PWMOUT
A102	SER1_RX	B102	FAN_TACHIN
A103	LID#	B103	SLEEP#
A104	VCC_12V	B104	VCC_12V
A105	VCC_12V	B105	VCC_12V
A106	VCC_12V	B106	VCC_12V
A107	VCC_12V	B107	VCC_12V
A108	VCC_12V	B108	VCC_12V
A109	VCC_12V	B109	VCC_12V
A110	GND(FIXED)	B110	GND(FIXED)

SOM-5992 ROW C, D			
C1	GND(FIXED)	D1	GND(FIXED)
C2	GND	D2	GND
C3	USB_SSRX0-	D3	USB_SSTX0-
C4	USB_SSRX0+	D4	USB_SSTX0+
C5	GND	D5	GND
C6	USB_SSRX1-	D6	USB_SSTX1-
C7	USB_SSRX1+	D7	USB_SSTX1+
C8	GND	D8	GND
C9	USB_SSRX2-	D9	USB_SSTX2-
C10	USB_SSRX2+	D10	USB_SSTX2+
C11	GND(FIXED)	D11	GND(FIXED)
C12	USB_SSRX3-	D12	USB_SSTX3-
C13	USB_SSRX3+	D13	USB_SSTX3+
C14	GND	D14	GND
C15	-	D15	-
C16	-	D16	-
C17	-	D17	-
C18	GND	D18	GND
C19	PCIE_RX6+	D19	PCIE_TX6+
C20	PCIE_RX6-	D20	PCIE_TX6-
C21	GND(FIXED)	D21	GND(FIXED)
C22	PCIE_RX7+	D22	PCIE_TX7+
C23	PCIE_RX7-	D23	PCIE_TX7-
C24	-	D24	-
C25	GND	D25	GND
C26	-	D26	-
C27	-	D27	-
C28	GND	D28	GND
C29	-	D29	-
C30	-	D30	-
C31	GND(FIXED)	D31	GND(FIXED)
C32	-	D32	-
C33	-	D33	-
C34	-	D34	-

C35	10G_PHY_RST_01	D35	10G_PHY_CAP_01
C36	10G_LED_SDA	D36	RSVD
C37	10G_LED_SCL	D37	RSVD
C38	10G_SFP_SDA1	D38	10G_SFP_SCL1
C39	10G_SFP_SDA0	D39	10G_SFP_SCL0
C40	10G_SDP0	D40	10G_SDP1
C41	GND(FIXED)	D41	GND(FIXED)
C42	10G_KR_RX1+	D42	10G_KR_TX1+
C43	10G_KR_RX1-	D43	10G_KR_TX1-
C44	GND	D44	GND
C45	10G_PHY_MDC_SCL1	D45	10G_PHY_MDIO_SDA1
C46	10G_PHY_MDC_SCL0	D46	10G_PHY_MDIO_SDA0
C47	10G_INT0	D47	10G_INT1
C48	GND	D48	GND
C49	10G_KR_RX0+	D49	10G_KR_TX0+
C50	10G_KR_RX0-	D50	10G_KR_TX0-
C51	GND(FIXED)	D51	GND(FIXED)
C52	PEG_RX0+	D52	PEG_TX0+
C53	PEG_RX0-	D53	PEG_TX0-
C54	GND	D54	RSVD
C55	PEG_RX1+	D55	PEG_TX1+
C56	PEG_RX1-	D56	PEG_TX1-
C57	-	D57	GND
C58	PEG_RX2+	D58	PEG_TX2+
C59	PEG_RX2-	D59	PEG_TX2-
C60	GND(FIXED)	D60	GND(FIXED)
C61	PEG_RX3+	D61	PEG_TX3+
C62	PEG_RX3-	D62	PEG_TX3-
C63	RSVD	D63	RSVD
C64	RSVD	D64	RSVD
C65	PEG_RX4+	D65	PEG_TX4+
C66	PEG_RX4-	D66	PEG_TX4-
C67	RAPID_SHUTDOWN	D67	GND
C68	PEG_RX5+	D68	PEG_TX5+
C69	PEG_RX5-	D69	PEG_TX5-
C70	GND(FIXED)	D70	GND(FIXED)
C71	PEG_RX6+	D71	PEG_TX6+
C72	PEG_RX6-	D72	PEG_TX6-
C73	GND	D73	GND
C74	PEG_RX7+	D74	PEG_TX7+
C75	PEG_RX7-	D75	PEG_TX7-
C76	GND	D76	GND
C77	RSVD	D77	RSVD
C78	PEG_RX8+	D78	PEG_TX8+
C79	PEG_RX8-	D79	PEG_TX8-
C80	GND(FIXED)	D80	GND(FIXED)
C81	PEG_RX9+	D81	PEG_TX9+
C82	PEG_RX9-	D82	PEG_TX9-
C83	RSVD	D83	RSVD
C84	GND	D84	GND
C85	PEG_RX10+	D85	PEG_TX10+
C86	PEG_RX10-	D86	PEG_TX10-
			•

C87	GND	D87	GND
C88	PEG_RX11+	D88	PEG_TX11+
C89	PEG_RX11-	D89	PEG_TX11-
C90	GND(FIXED)	D90	GND(FIXED)
C91	PEG_RX12+	D91	PEG_TX12+
C92	PEG_RX12-	D92	PEG_TX12-
C93	GND	D93	GND
C94	PEG_RX13+	D94	PEG_TX13+
C95	PEG_RX13-	D95	PEG_TX13-
C96	GND	D96	GND
C97	RSVD	D97	RSVD
C98	PEG_RX14+	D98	PEG_TX14+
C99	PEG_RX14-	D99	PEG_TX14-
C100	GND(FIXED)	D100	GND(FIXED)
C101	PEG_RX15+	D101	PEG_TX15+
C102	PEG_RX15-	D102	PEG_TX15-
C103	GND	D103	GND
C104	VCC_12V	D104	VCC_12V
C105	VCC_12V	D105	VCC_12V
C106	VCC_12V	D106	VCC_12V
C107	VCC_12V	D107	VCC_12V
C108	VCC_12V	D108	VCC_12V
C109	VCC_12V	D109	VCC_12V
C110	GND(FIXED)	D110	GND(FIXED)



Watchdog Timer

This appendix gives you the information about the watchdog timer programming on the SOM-5992 CPU System on Module.

Sections include:

■ Watchdog Timer Programming

B.1 Programming the Watchdog Timer

Trigger Event	Note
IRQ	IRQ5, 7, 14 (BIOS setting default disable)**
NMI	N/A
SCI	Power button event
Power Off	Support
H/W Restart	Support
External WDT	Support

 ** WDT new driver support automatically selects available IRQ. Only Win XP, Win7 and Win8 support it.

In other OS, for details, please refer to iManager & Software API User Manual For details, please refer to iManager & Software API User Manual:



Programming GPIO

This Appendix gives the illustration of the General Purpose Input and Output pin setting. Sections include: ■ System I/O Ports

C.1 GPIO Register

GPIO Byte Mapping	H/W Pin Name
BIT0	GPO0
BIT1	GPO1
BIT2	GPO2
BIT3	GPO3
BIT4	GPI0
BIT5	GPI1
BIT6	GPI2
BIT7	GPI3

For details, please refer to iManager & Software API User Manual.



System Assignments

This appendix gives you the information about the system resource allocation on the SOM-5992 CPU System on Module.

- Sections include:
- System I/O ports
- DMA Channel Assignments
- Interrupt Assignments
- 1st MB Memory Map

D.1 System I/O Ports

Table D.1: System I/O ports

Addr.Range(Hex)	Device	
0000-000F	Direct memory access controller	
0000-000F	PCI Express Root Complex	
0010-001F	Motherboard resources	
0040-0043	System timer	
0050-0053	System timer	
0061-0061	System speake	
0062-0062	Microsoft ACPI-Compliant Embedded Controller	
0066-0066	Microsoft ACPI-Compliant Embedded Controller	
0070-0071	System CMOS/real time clock	
0072-0073	Motherboard resource	
0074-0077	System CMOS/real time clock	
0080-0080	Motherboard resources	
0081-0083	Direct memory access controller	
0084-0086	Motherboard resources	
0087-0087	Direct memory access controller	
0088-0088	Motherboard resources	
0089-008B	Direct memory access controller	
008C-008E	Motherboard resources	
008F-008F	Direct memory access controller	
0090-009F	Motherboard resources	
0092-0092	Motherboard resources	
00C0-00DF	Direct memory access controller	
0020-003D	Programmable interrupt controller	
00A0-00BD	Programmable interrupt controller	
00F0-00F0	Numeric data processor	
02F8-02FF	Communications Port (COM2)	
03F8-03FF	Communications Port (COM1)	
029C-029D	Motherboard resources	
03B0-03BB	Intel(R) 8 Series/C220 Series PCI Express Root Port #8 - 8C1E	
03B0-03BB	PCI standard PCI Express to PCI/PCI-X Bridge	
03C0-03DF	Intel(R) 8 Series/C220 Series PCI Express Root Port #8 - 8C1E	
03C0-03DF	PCI standard PCI Express to PCI/PCI-X Bridg	
04D0-04D1	Programmable interrupt controller	
0400-047F	Motherboard resources	
0500-0573	Motherboard resources	
00580-059F	Motherboard resources	
0600-061F	Motherboard resources	
0800-081F	Motherboard resources	
0880-0883	Motherboard resources	
D000-DFFF	Intel(R) 8 Series/C220 Series PCI Express Root Port #8 - 8C1E	
D000-DFFF	PCI standard PCI Express to PCI/PCI-X Bridge	
D000-DFFF	ASPEED Graphics Family(WDDM)	
F020-F03F	tandard SATA AHCI Controller	
Table D.1: System I/O ports		
-----------------------------	--	--
F040-F043	Standard SATA AHCI Controller	
F050-F057	Standard SATA AHCI Controller	
F060-F063	Standard SATA AHCI Controller	
F070-F077	Standard SATA AHCI Controller	
1000-FFFF	PCI Express Root Complex	
E000-EFFF	Intel(R) Xeon(R) E7 v4/Xeon(R) E5 v4/Xeon(R) E3 v4/Xeon(R) D PCI Express Root Port 1 - 6F03	

D.2 DMA Channel Assignments

Table D.2: DMA Channel Assignments		
Channel	Function	
4	Direct memory access controller	

D.3 Interrupt Assignments

Table D.3: Interrupt Assignments		
Interrupt#	Interrupt Source	
IRQ 0	System timer	
IRQ 7	Communications Port (COM2)	
IRQ 8	System CMOS/real time clock	
IRQ 10	PCI Simple Communications Controller	
IRQ 11	Communications Port (COM1)	
IRQ 13	Numeric data processor	
IRQ 16	Standard SATA AHCI Controller	
IRQ 16	Intel(R) 8 Series/C220 Series PCI Express Root Port #1 - 8C10	
RQ 18	Intel(R) 8 Series/C220 Series USB EHCI #1 - 8C26	
IRQ 19	Intel(R) 8 Series/C220 Series PCI Express Root Port #8 - 8C1E	
IRQ 19	Intel SD Host Controller	
IRQ 26	Intel(R) Xeon(R) E7 v4/Xeon(R) E5 v4/Xeon(R) E3 v4/Xeon(R) D PCI Express Root Port 1 - 6F03	
IRQ 26	Intel(R) Xeon(R) E7 v4/Xeon(R) E5 v4/Xeon(R) E3 v4/Xeon(R) D PCI Express Root Port 1 - 6F02	
IRQ 32	Intel(R) Xeon(R) E7 v4/Xeon(R) E5 v4/Xeon(R) E3 v4/Xeon(R) D PCI Express Root Port 2 - 6F04	
IRQ 32	Intel(R) Xeon(R) E7 v4/Xeon(R) E5 v4/Xeon(R) E3 v4/Xeon(R) D PCI Express Root Port 2 - 6F06	
IRQ 40	Intel(R) Xeon(R) E7 v4/Xeon(R) E5 v4/Xeon(R) E3 v4/Xeon(R) D PCI Express Root Port 3 - 6F08	
IRQ 81~191	Microsoft ACPI-Compliant System	
IRQ 256~511	Microsoft ACPI-Compliant System	
IRQ 4294967293	Intel(R) USB 3.0 eXtensible Host Controller - 0100 (Microsoft)	
IRQ 4294967294	PCI standard PCI Express to PCI/PCI-X Bridge	
IRQ 4294967247~ 4294967256	Intel(R) I210 Gigabit Network Connection #2	

D.4 1st MB Memory Map

Table D.4: 1st MB Memory Map			
Device			
Intel(R) 8 Series/C220 Series PCI Express Root Port #8 - 8C1E			
PCI standard PCI Express to PCI/PCI-X Bridge			
ASPEED Graphics Family(WDDM)			
Intel(R) 8 Series/C220 Series PCI Express Root Port #8 - 8C1E			
PCI standard PCI Express to PCI/PCI-X Bridge			
PCI Express Root Complex			
Standard SATA AHCI Controller			
PCI Simple Communications Controller			
Intel(R) I210 Gigabit Network Connection #2			
Intel(R) I210 Gigabit Network Connection #2			
High precision event timer			
Intel(R) Xeon(R) E7 v4/Xeon(R) E5 v4/Xeon(R) E3 v4/ Xeon(R) D PCI Express Root Port 2 - 6F04			
ASPEED Graphics Family(WDDM)			
Intel(R) 8 Series/C220 Series USB EHCI #1 - 8C26			
Intel(R) Xeon(R) E7 v4/Xeon(R) E5 v4/Xeon(R) E3 v4/ Xeon(R) D PCI Express Root Port 2 - 6F06			
Intel(R) Xeon(R) E7 v4/Xeon(R) E5 v4/Xeon(R) E3 v4/ Xeon(R) D PCI Express Root Port 2 - 6F06			
PCI Simple Communications Controller			
Intel(R) Xeon(R) E7 v4/Xeon(R) E5 v4/Xeon(R) E3 v4/ Xeon(R) D I/O APIC - 6F2C			
Advanced programmable interrupt controller			
PCI Express Root Complex			
Intel(R) Xeon(R) E7 v4/Xeon(R) E5 v4/Xeon(R) E3 v4/ Xeon(R) D PCI Express Root Port 1 - 6F03			
Trusted Platform Module 2.0			
Motherboard resources			
Intel(R) USB 3.0 eXtensible Host Controller - 0100 (Microsoft)			
Intel(R) 8 Series/C220 Series PCI Express Root Port #8 - 8C1E			



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 of the publisher.

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

© Advantech Co., Ltd. 2017