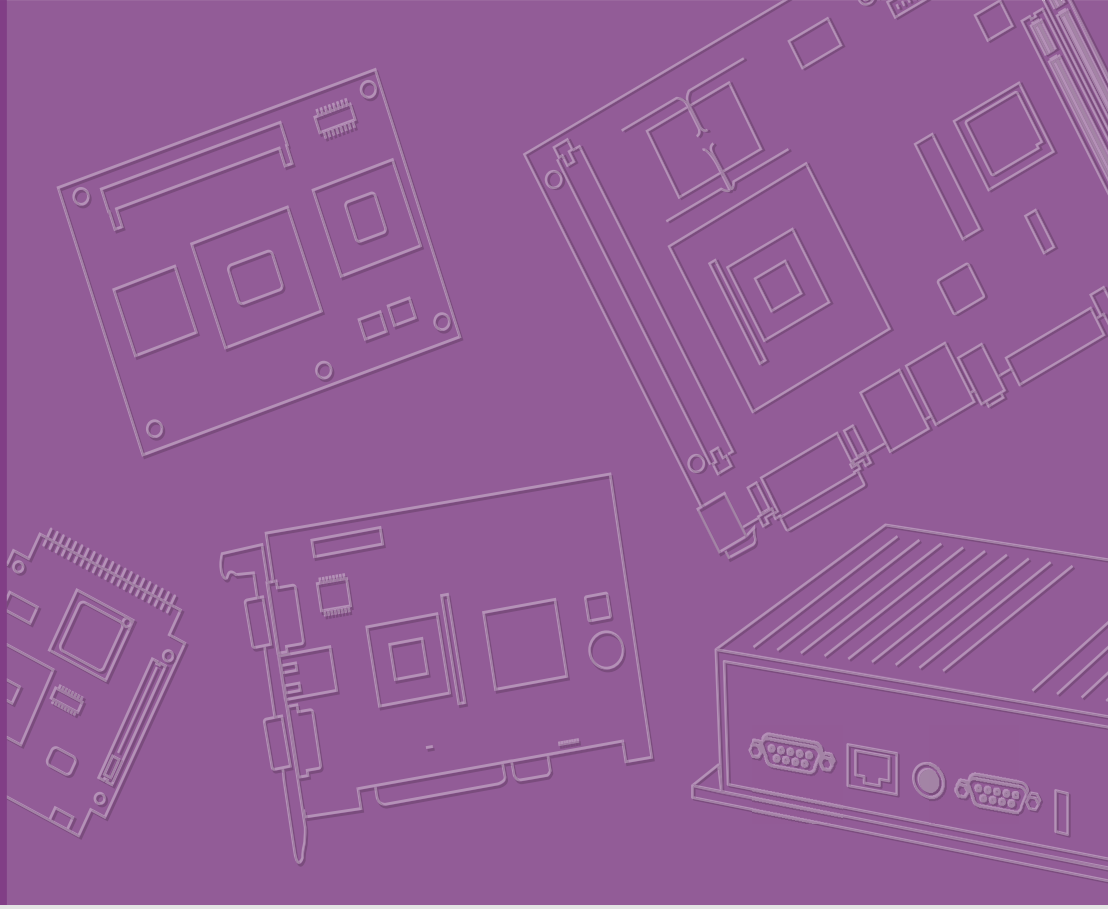


User Manual

SOM-5991

ADVANTECH

Enabling an Intelligent Planet

Copyright

Acknowledgements

Intel and Pentium are trademarks 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 out-of-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. 2006599100 Edition 1

Printed in China December 2016

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 support website at http://www.emacinc.com/support where you can find the latest information about the product.
2. Contact your distributor, sales representative, or technical 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: info@emacinc.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.

- Item 1 x SOM-5991 CPU module
- Box 1 x Heat spreader

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.

Contents

Chapter 1

General Information

This chapter gives background information on the SOM-5991 CPU Computer on Module

Sections include:

- Introduction
- Functional Block Diagram
- Product Specification

1.1 Introduction

SOM-5991, 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 options for optimizing a variety of workloads and infrastructure 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, the SOM-5991 incorporates two 10GBase-KR interfaces, which should help fulfill the ever-increasing service application demands in the area of COM Express. Customers can take advantage of SOM-5991's native 10GBase-KR interfaces to design in 10GbE carrier boards. SOM-5991 and its development board are ready for customers as a reference design.

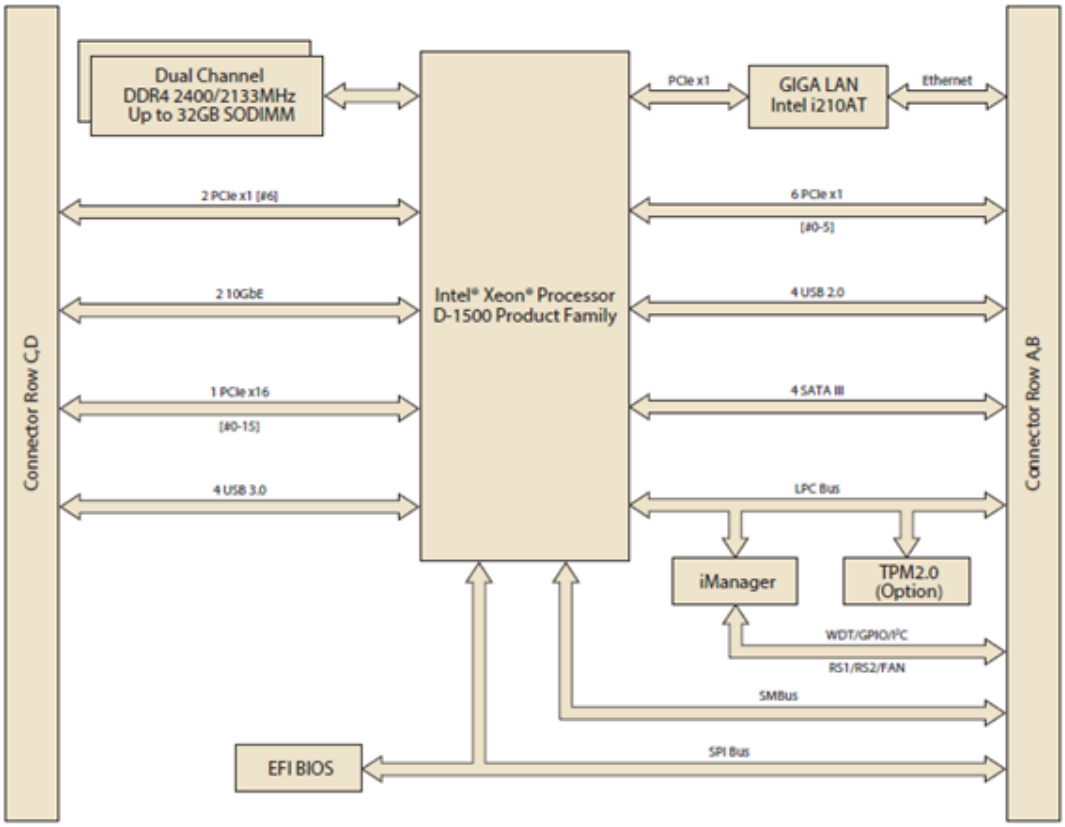
PCIe x16 and 8 PCIe x1 support Non-Transparent Bridge (NTB), which allows redundancy via PCIe. This helps reduce data loss, allowing a secondary system to take over PCIe storage devices if the CPU fails, and it provides high availability for applications providing continuous service.

SOM-5991 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 using a balanced torque design, it is the first COM Express with added a backplane to increase rigidity so the thermal module makes tight contact with the CPU without board bending. This results in highly efficient heat dissipation with outstanding computing performance. Advantech also offers a SOM-5991 pre-assembly thermal solution service that can make system-level assembly easier.

Table 1.1: 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 initialize system components before handing control over to the operating system
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 system 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
TPM	Trusted Platform Module, chip to enhance the security features of a computer system
UEFI	Unified Extensible Firmware Interface
WDT	Watch Dog Timer

1.2 Functional Block Diagram



1.3 Product Specification

1.3.1 Compliance

- PICMG COM.0 (COM Express) Revision 2.1
- Basic Size – 125 x 95mm
- Pin-out Type 6 compatible

1.3.2 Feature List

Feature Type	Connector Row	Feature	Type 6 Define		SOM-5991
			Max.	Min.	
Display	A-B	LVDS Channel A (18/24-bit)	1	0	0
	A-B	LVDS Channel B (18/24-bit)	1	0	0
	A-B	eDP (muxed on LVDS Channel A)	1	0	0
	A-B	VGA	1	0	0
Expansion	A-B	PCI Express x1	6	1	6
	A-B	LPC	1	1	1
Serial	A-B	SMBus	1	1	1
	A-B	I2C Bus	1	1	1
	A-B	Serial Port	2	0	2
	A-B	CAN Bus (muxed on SER1)	1	0	0
I/O	A-B	LAN Port 0 (Gigabit Ethernet)	1	1	1
	A-B	SATA	4	1	4
	A-B	USB2.0	8	4	4
	A-B	USB Client	1	0	0
	A-B	HD Audio	1	0	0
	A-B	SPI Bus	2	1	1
	A-B	General Purpose I/O (GPIO)	8	8	8
	A-B	SDIO (muxed on GPIO)	1	0	0
	A-B	Express Card Support	2	1	2
	A-B	Watchdog Timer Output	1	0	1
	A-B	Speaker Out	1	1	1
	A-B	External BIOS ROM Support	2	0	2
	A-B	Power Button Support	1	1	1
	A-B	Power Good	1	1	1
	A-B	VCC_5V_SBY Contacts	4	4	4
	A-B	Sleep	1	0	1
	A-B	Thermal Protection	1	0	1
	A-B	Lid Input	1	0	1
	A-B	Battery Low Alarm	1	0	1
	A-B	Suspend/Wake Signals	3	0	3
	A-B	Fan PWM / Tachometer	2	0	2
	A-B	Trusted Platform Modules	1	0	1
Display	C-D	Digital Display Interfaces 1 - 3	3	0	0
I/O	C-D	PEG (PCI Express x16)	1	0	1
	C-D	PCI Express x1	2	0	2
	C-D	USB3.0	4	0	4

1.3.3 Processor System

CPU	Std. Freq.	Max. Turbo Freq.	Core/Thread	LLC Cache	TDP(W)
Xeon D-1548	2.0 GHz	2.6 GHz	8/16	12 MB	45 W
Pentium D1508	2.2 GHz	2.6 GHz	2/4	3 MB	25 W

1.3.4 Memory

Dual channels 2 sockets support DDR4 2400MHz up to 32GB (supported ECC)

Maximum support 16G + 16G on each socket

1.3.5 Graphics / Audio

Intel® Xeon® Processor D Family is without graphics. SOM-5991 does not support display and audio. For graphics behavior, it will be defined according to specific user scenario based on system specification. Please contact to Advantech sales or FAE for more detail.

1.3.6 Expansion Interface

1.3.6.1 PCIe x16

Intel Xeon® Processor D natively integrates 1 x16 PCI Express interface supports up to 4 devices at up to Gen3 speeds (8 GHz). SOM-5991 supports 1 PCIe x16, and is configurable to 2 x8, 1 x8 & 2 x4, or 4 x4.

1.3.6.2 PCIe x1

Intel Xeon® Processor D natively integrates 8 PCI Express x1 lanes and up to 8 devices, which support up to Gen2 (5.0 Gb/s). SOM-5991 supports 8 PCIe x1 by default, and is configurable to three options in the following table.

Type 6		Row A,B						Row C,D	
		P0	P1	P2	P3	P4	P5	P6	P7
Default	Config.	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			

1.3.6.3 LPC

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

1.3.6.4 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.

1.3.6.5 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**
  Support 4 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**
  4 ports USB3.0 (5.0 Gbps) and 4 ports USB2.0 (480 Mbps) which are backward compatible to USB1.x. For USB3.0, supports LPM (U0, U1, U2, and U3) manageability to saving power.
- **USB3.0**

Type 6	P0	P1	P2	P3
SoC	P0	P1	P2	P3
Type 6	OC_01	OC_23		
SoC USB_OC#	OC_0	OC_2		

- **USB2.0**

Type 6	P0	P1	P2	P3
SoC	P0	P1	P2	P3
Type 6	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**
  8 programmable general purpose Input or output (GPIO).
- **Watchdog**
  Supports multi-level watchdog time-out output. Provides 1-65535 level, from 100ms to 109.22 minutes interval.
- **Serial port**
  2 ports, 2-wire serial port (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
- **Express Card**
  2 sets of Express Card control signals including card detection and reset, follows PICMG COM Express R2.1 specification.
- **TPM**
  Supports TPM 2.0 module by default.
- **Smart Fan**
  Supports two Fan PWM control signal and two tachometer input for fan speed detection. Provides one on module with connector and the other to carrier board follow by PICMG COM Express R2.1 specification.

- **BIOS**
  BIOS chip is on module by default. Also allows user to place BIOS chip on carrier board with 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 you to go into the BIOS setup menu and load the default setting at the first time of boot up.*

1.3.6.6 Power Management

- **Power Supply**
  Supports both ATX and AT power modes. VSB is for suspend power and can be an option if not requiring standby (suspend-to-RAM) support. RTC Battery may be option 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**
  Power OK from 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 R2.1 specification
- **Wake Event**
  Various wake-up events allow users to apply different scenarios.
  Wake-on-LAN(WOL): Wake to S0 from S3/S4/S5
  USB Wake: Wake to S0 from S3/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 an additional feature to allow the system 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 the on-module controller active. Therefore, only less than 50mW power will be consumed which means the user's battery pack can last longer. With this mode enabled in BIOS, the system (or module) will only allow a power button to boot rather than others such as WOL.

1.3.6.7 Environment

- **Temperature**
  Operating: 0 ~ 60° C (32 ~ 140° F), with an active heat sink under 0.7m/s air flow chamber
  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 EN55022 Class B and FCC Certifications: validate with standard development boards in Advantech chassis

1.3.6.8 MTBF

Please refer to Advantech SOM-5991 Series Reliability Prediction Report No: 16R323A0.

1.3.6.9 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 and browse the website http://www.emacinc.com/support to download the setup file.

1.3.6.10 Advantech iManager

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

1.3.6.11 Power Consumption

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-5991X8-U0A1E	55.5W	48.7W	11.0W	1.97W	0.025W	4.41uA

Hardware Configurations:

1. MB: SOM-5991X8-U0A1E (PCB_A101-3)
2. DRAM: 8GB DDR4 2133MHz *2
3. Carrier board: SOM-DB5900_A101-2

Test Condition:

1. Test temperature: room temperature
2. Test voltage: rated voltage DC +12.0V
3. Test loading:
   3.1 Maximum load mode: According to Intel thermal/power test tools
   3.2 Burn-in mode: Passmark Burn-in Test v8.1 Pro with appropriate load setting
   3.3 Idle mode: DUT power management off and no running any program.
4. OS: Server 2012 R2

1.3.6.12 Performance

For reference performance or benchmark data that compare with other modules, please refer to “Advantech COM Performance & Power Consumption Table”.

1.3.6.13 Selection Guide w/ P/N

Part No.	CPU	Core	Freq.	CPU TDP	LLC	DDR4 SODIMM	Giga LAN	10GBase -KR	PEG x16	PCI2 x1	USB 2.0	USB 3.0	SATA III	LPC	Power	Thermal Solution	Operating Temp.
SOM-5991XB-U0A1E	Xeon D-1548	8	2.0	45W	12MB	ECC/non ECC	1	2	1	8	4	4	4	Yes	AT/ATX	Active	0 ~ 60° C

1.3.6.14 Packing list

Part No.	Description	Quantity
-	SOM-5991 CPU module	1
1960077016N001	Heatspreader	1

1.3.6.15 Development Board

Part No.	Description
SOM-DB5900-00A1E	COMe Devel.Board w/10GB I/O pin-out

1.3.6.16 Optional Accessory

Part No.	Description

1960048820N001	Semi-Cooler 125x95x33.5 mm with 12V Fan
1960075879N001	Cooler 66x60x23 mm with 12V Fan

1.3.6.17 Pin Description

Advantech provides useful checklists for schematic design and layout routing. In schematic checklist, it will specify details about each pin electrical properties and how to connect for different user scenes. 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 advance supports.

Chapter 2

Mechanical Information

This chapter gives mechanical information on the SOM-5991 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-5991 Computer-on-Module. Please be aware off these positions while designing the customer's own carrier board to avoid mechanical problems and thermal solutions contacts for best thermal dispassion performance.

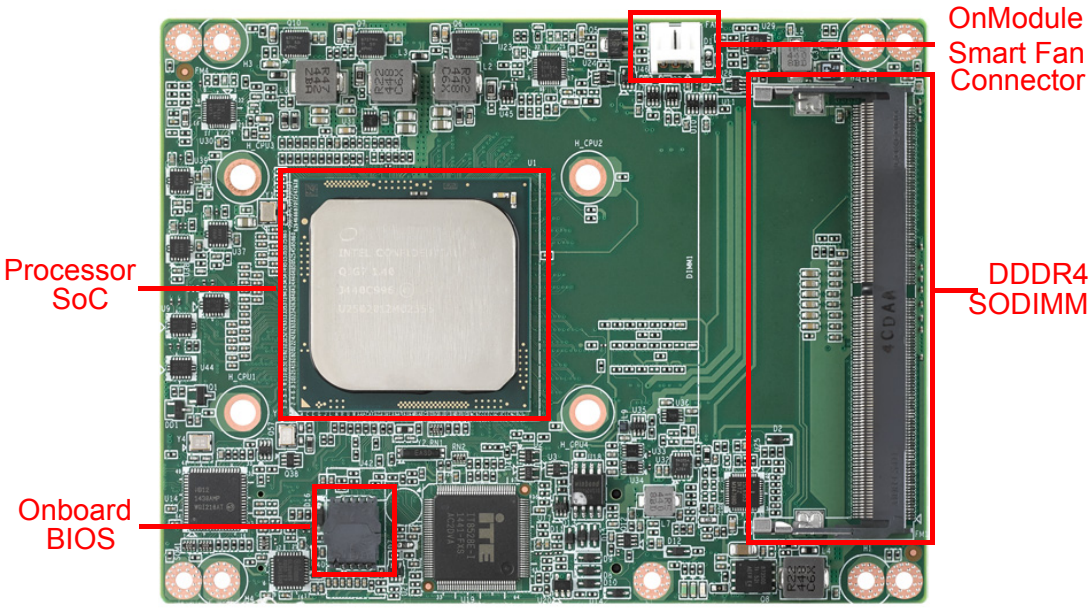


Figure 2.1 Board chips identify – Front

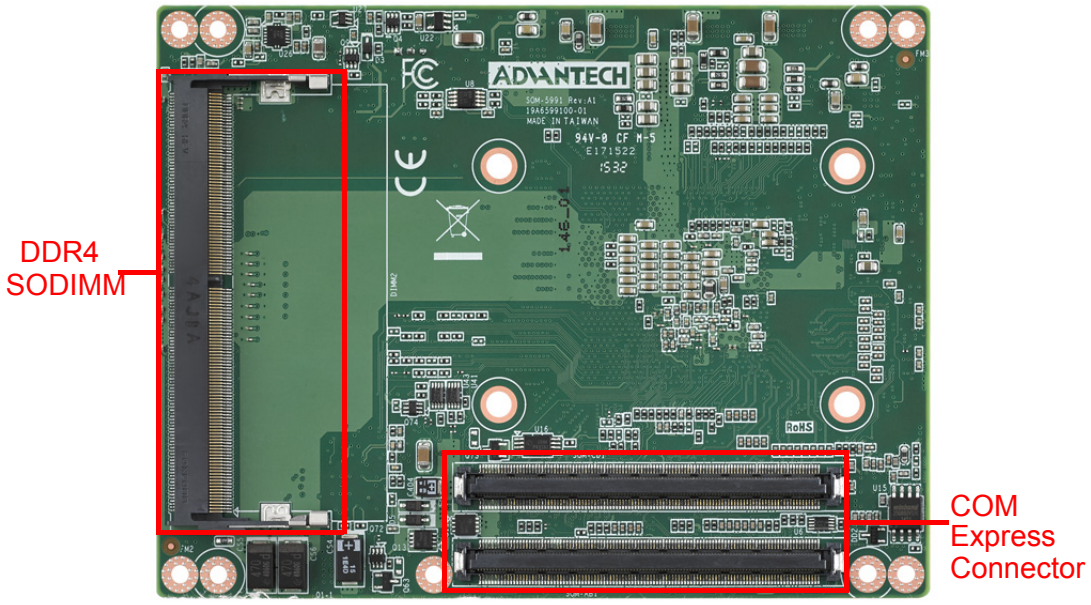
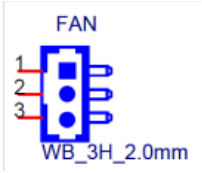


Figure 2.2 Board chips identify – Back

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 detail about 2D/3D models, please contact support services

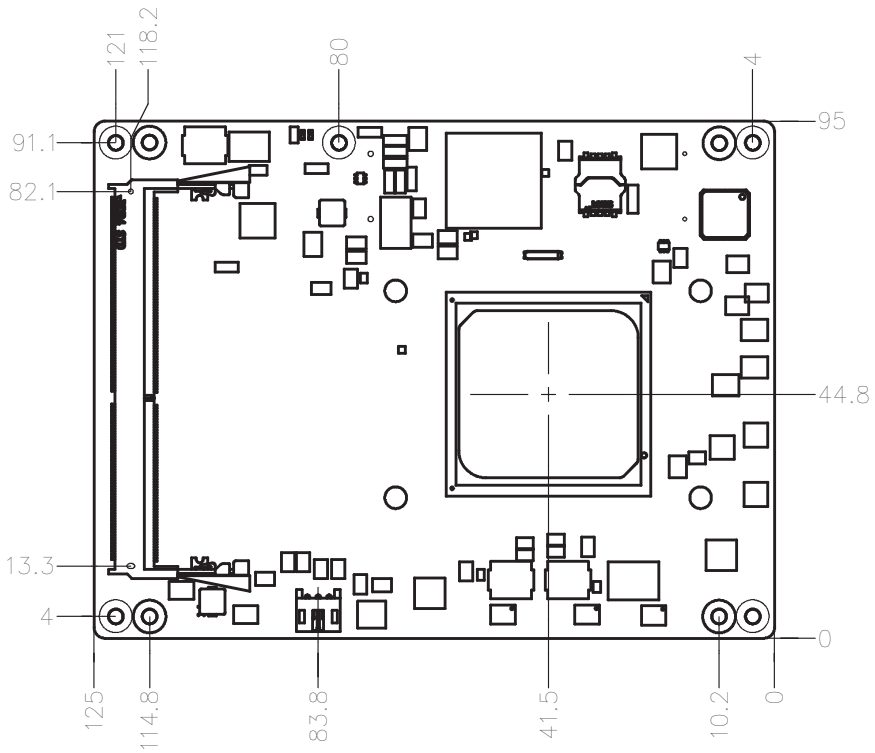


Figure 2.3 Board Mechanical Drawing - Front

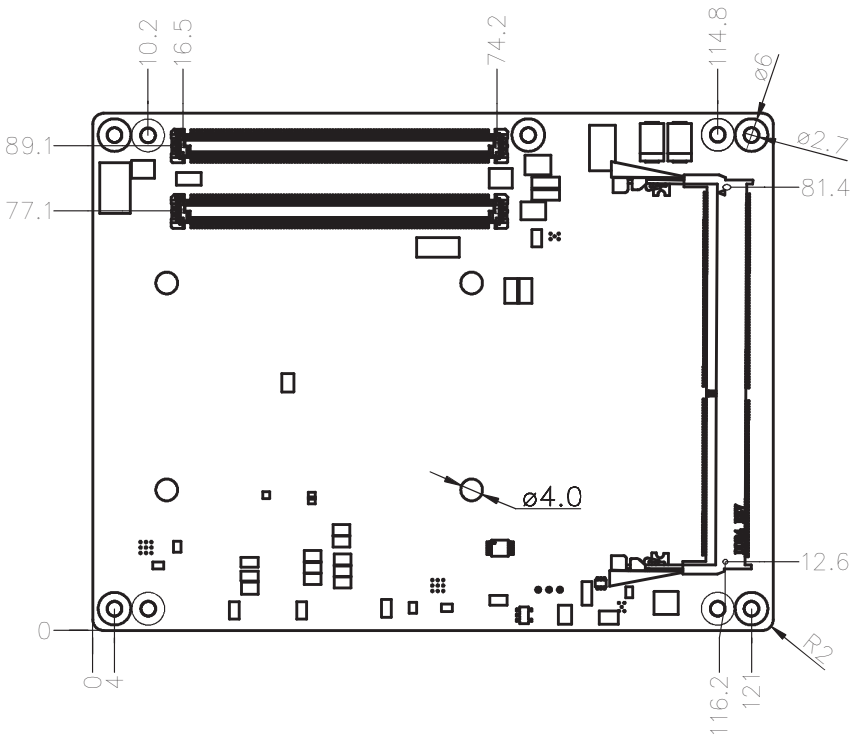


Figure 2.4 Board Mechanical Drawing – Back

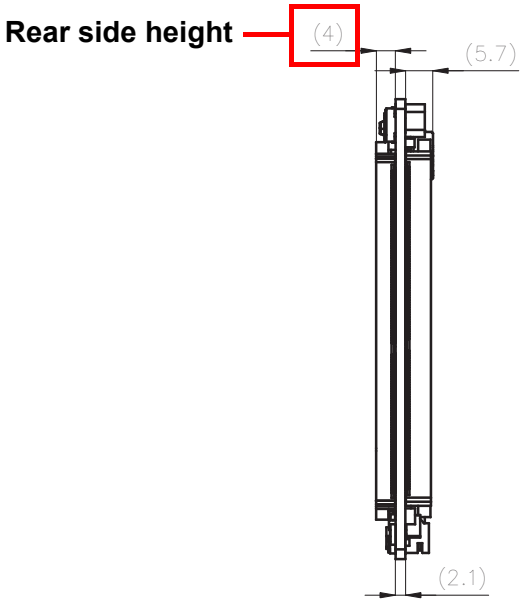


Figure 2.5 Board Mechanical Drawing – Side

2.3 Assembly Drawing

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

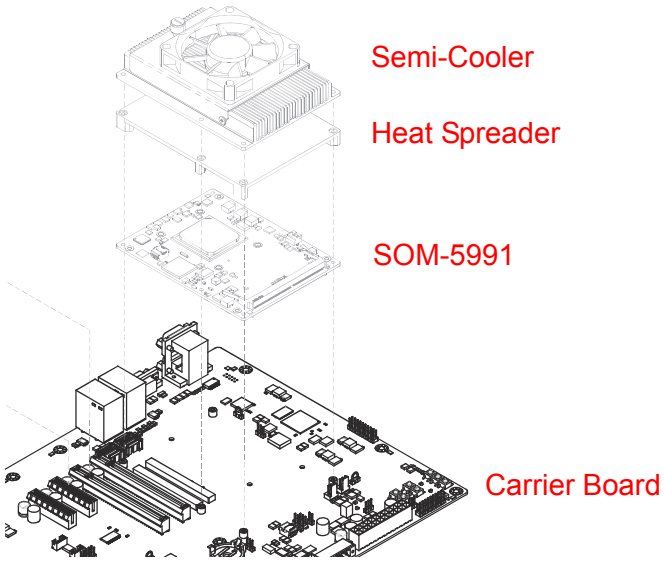
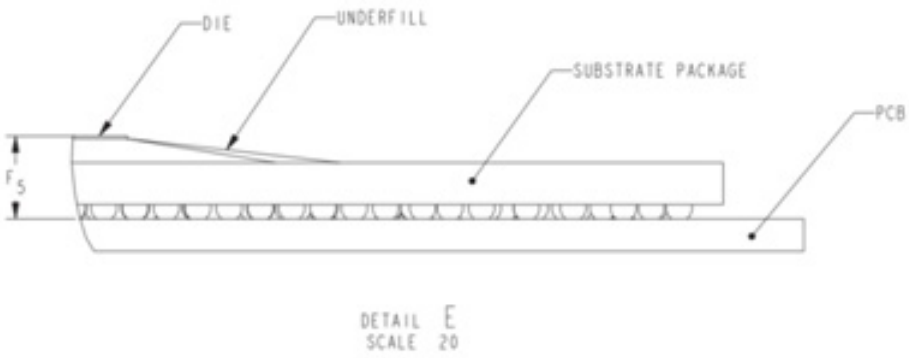


Figure 2.6 Assembly Drawing

There are 4 reserved screw holes for SOM-5991 to be pre-assembled with heat spreader.

2.4 Assembly Drawing

Please 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 REFERENCE BOARD DESIGN)

Figure 2.7 Main Chip Height and Tolerance

Chapter 3

AMI BIOS

This chapter gives BIOS setup information for the SOM-5991 CPU computer-on module

Sections include:

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

3.1 Introduction

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.

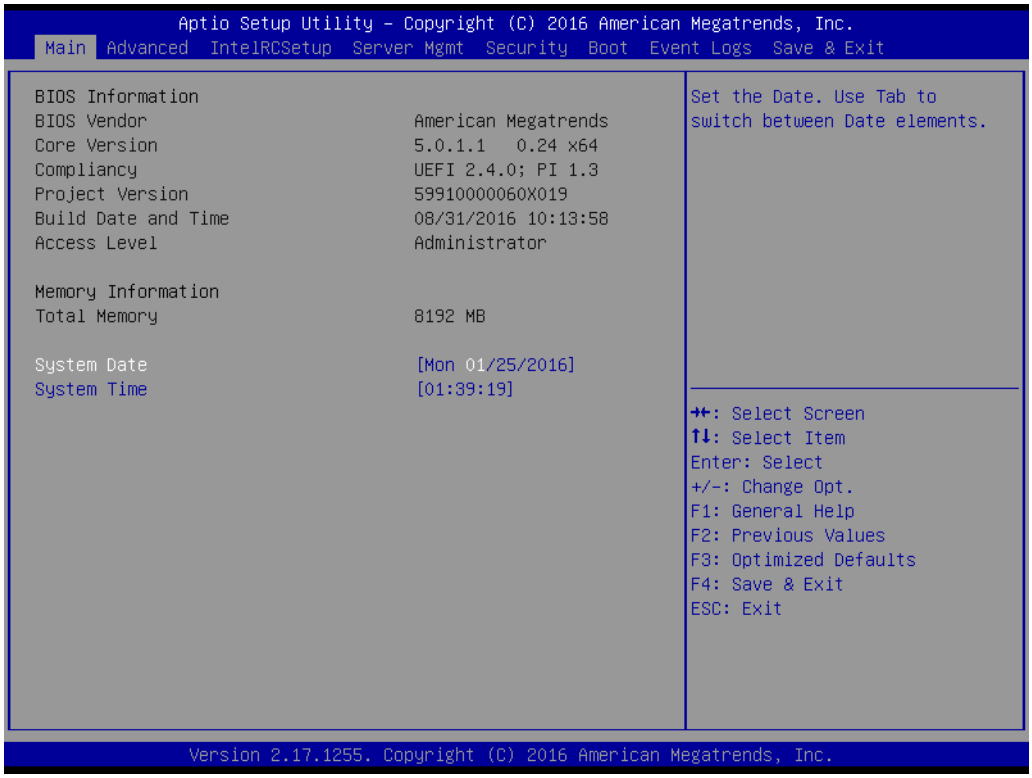


Figure 3.1 Setup program initial screen

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 <DEL> 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.

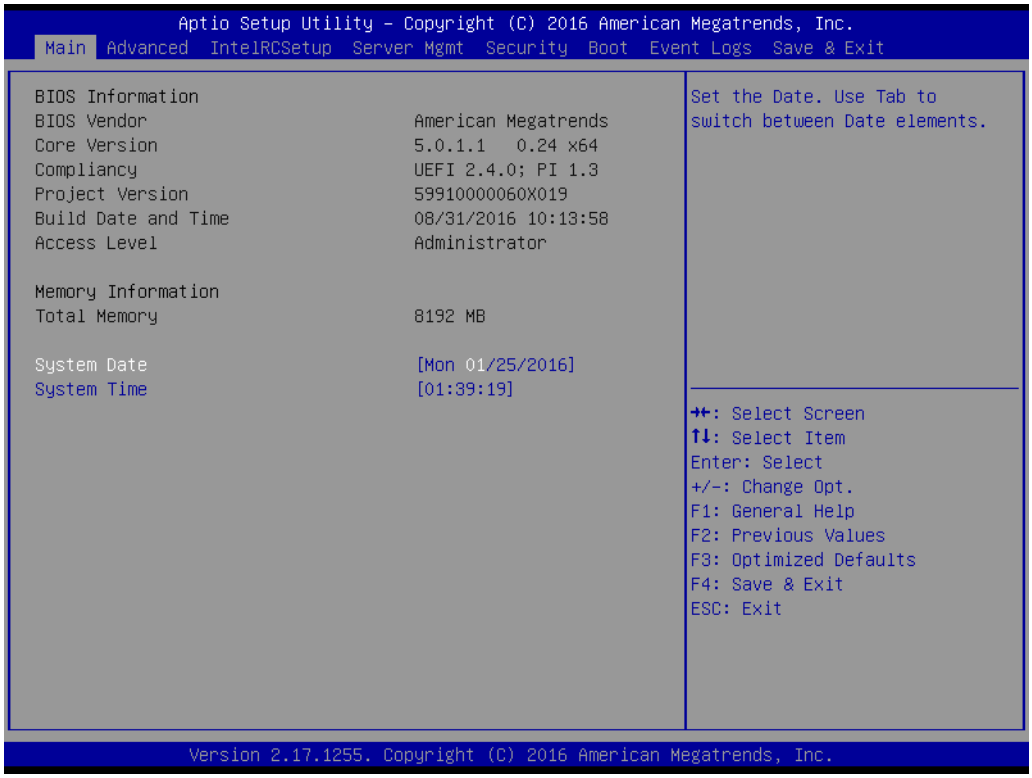


Figure 3.2 Main setup screen

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-5991 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.

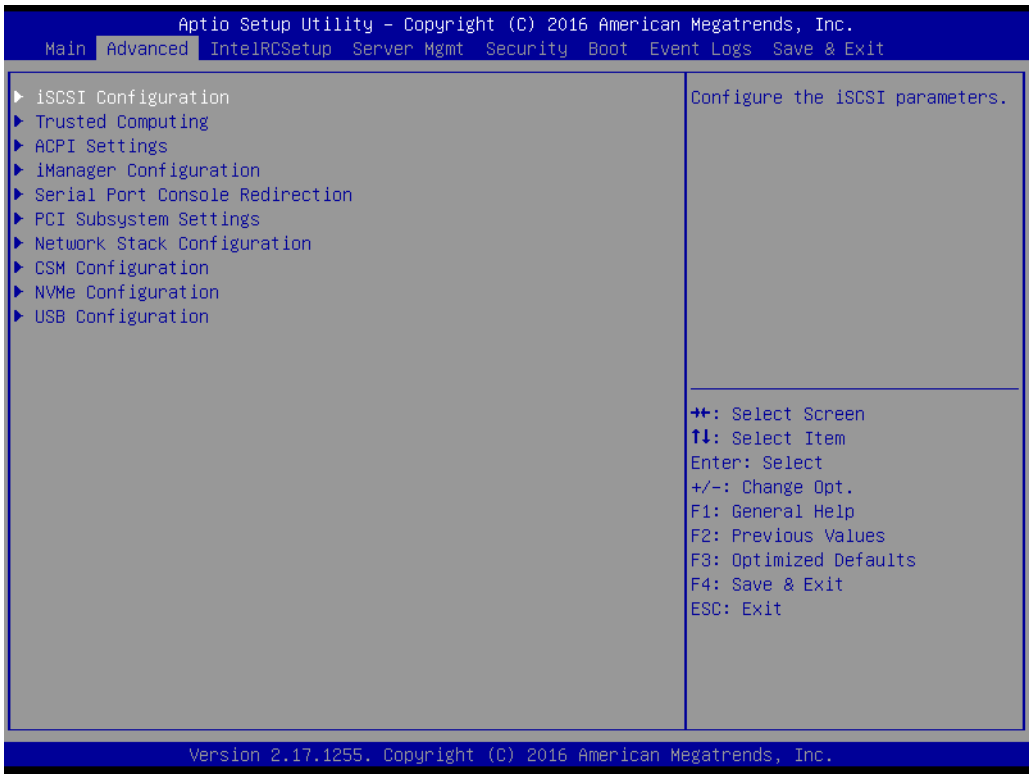


Figure 3.3 Advanced BIOS features setup screen

3.2.2.1 Trusted Computing

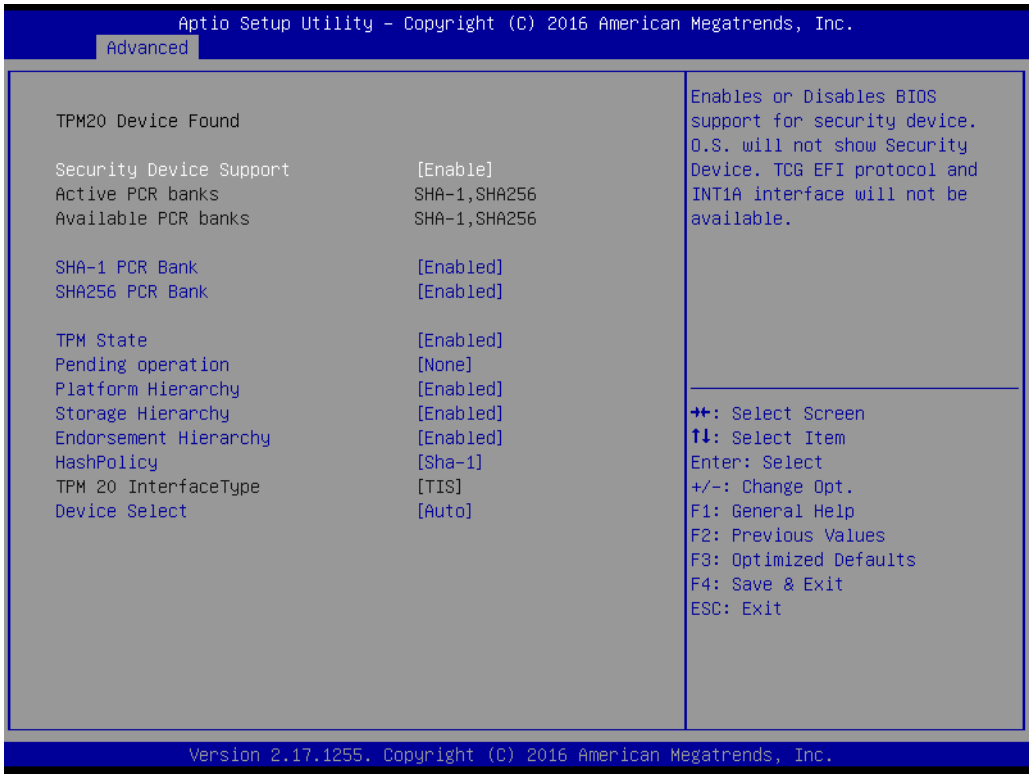


Figure 3.4 Trusted Computing

- **Security Device Support**
  Enable or Disables BIOS support for security device. OS will not show security Device. TCG EFI protocol and INT1A interface will not be available.
- **Device Select**
  Select the device. 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 no found. TPM 2.0 devices will be enumerated.

3.2.2.2 ACPI Settings

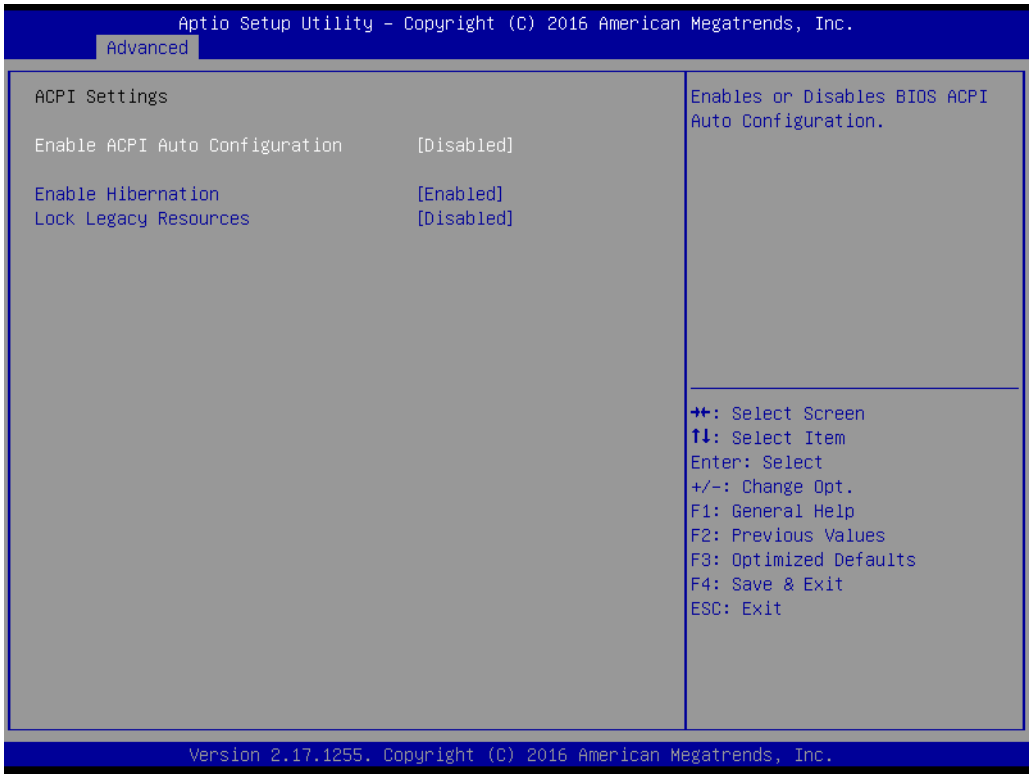


Figure 3.5 ACPI Settings

- **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.
- **ACPI Sleep State**
  Select the highest ACPI sleep state the system will enter when the SUSPEND button is pressed.
- **Lock Legacy Resources**
  Enables or Disables Lock of Legacy Resources

3.2.2.3 iManager Configuration

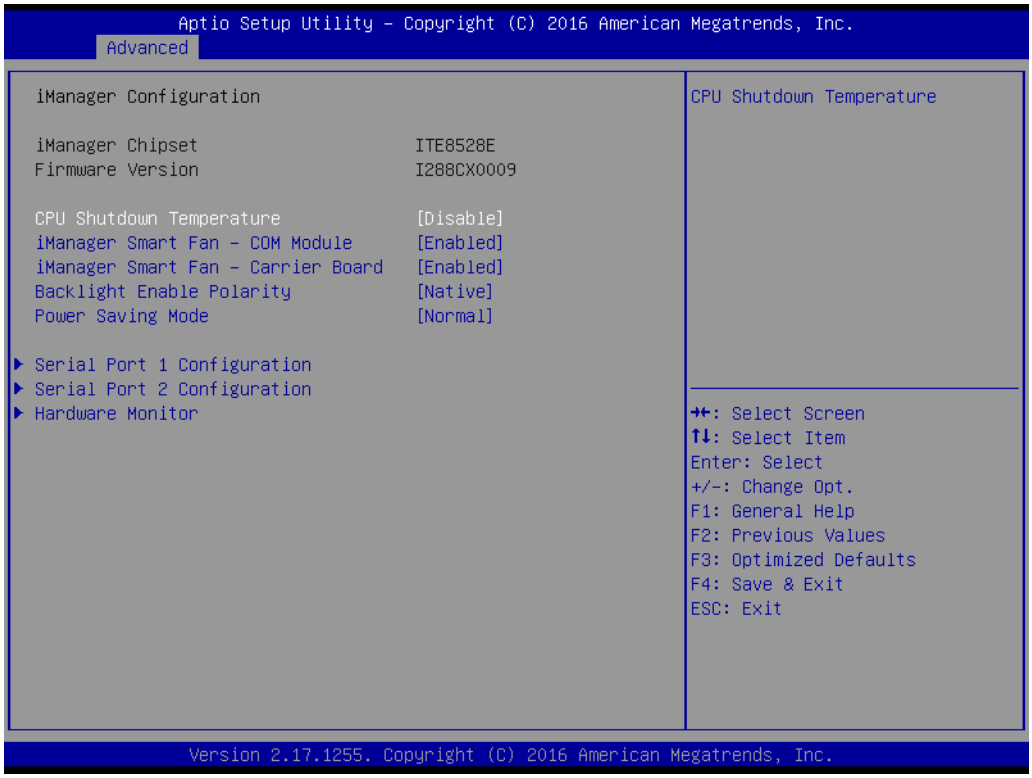


Figure 3.6 iManager Configuration

- **CPU Shutdown Temperature**
  Enable/Disable CPU Shutdown Temperature.
- **iManager Smart Fan – Carrier Board**
  Control iManager Smart FAN Carrier Board function.
- **Backlight Enable Polarity**
  Switch Backlight Enable Polarity for Native or Invert**.**
- **Brightness PWM Polarity**
  Switch Backlight Control Brightness PWM Polarity for Native or Invert.
- **Power Saving Mode**
  Select Ite8528 Power Saving Mode.
- **Serial Port 3 Configuration**
  Set Parameters of Serial Port 3.
- **Serial Port 4 Configuration**
  Set Parameters of Serial Port 4.
- **Hardware Monitor**
  Monitor hardware status.

Serial Port 1 Configuration

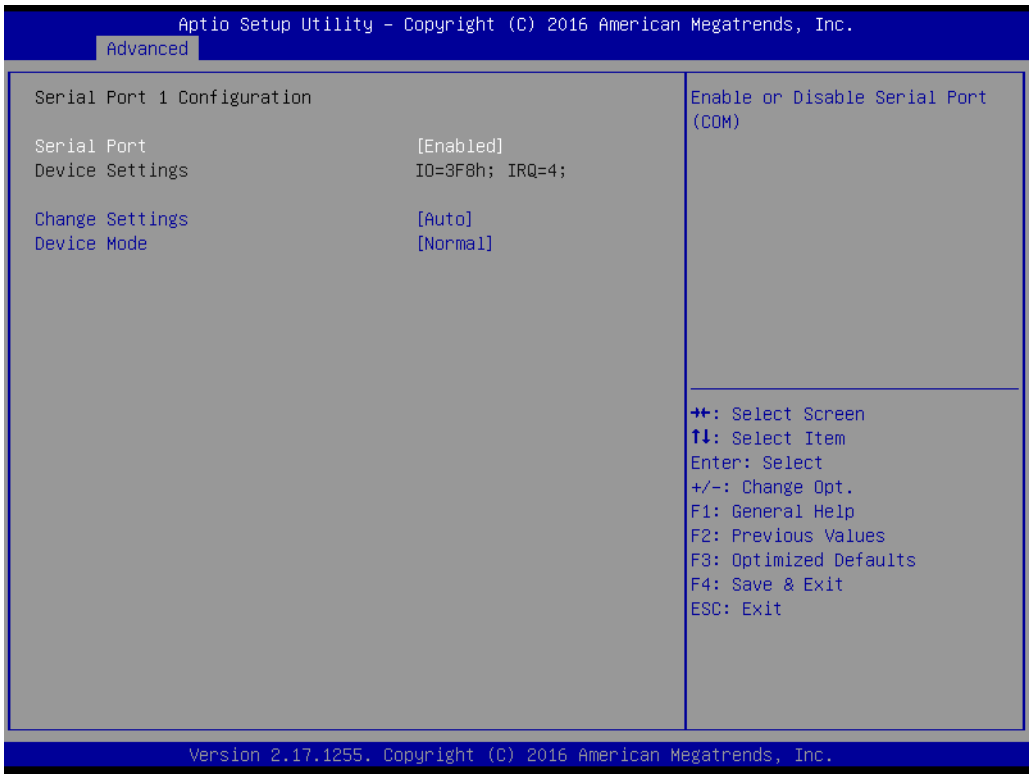


Figure 3.7 Serial Port 1 Configuration

- **Serial Port**
  Enable or Disable Serial Port (COM).
- **Change Settings**
  Select an optimal setting for Super IO device.

Serial Port 2 Configuration

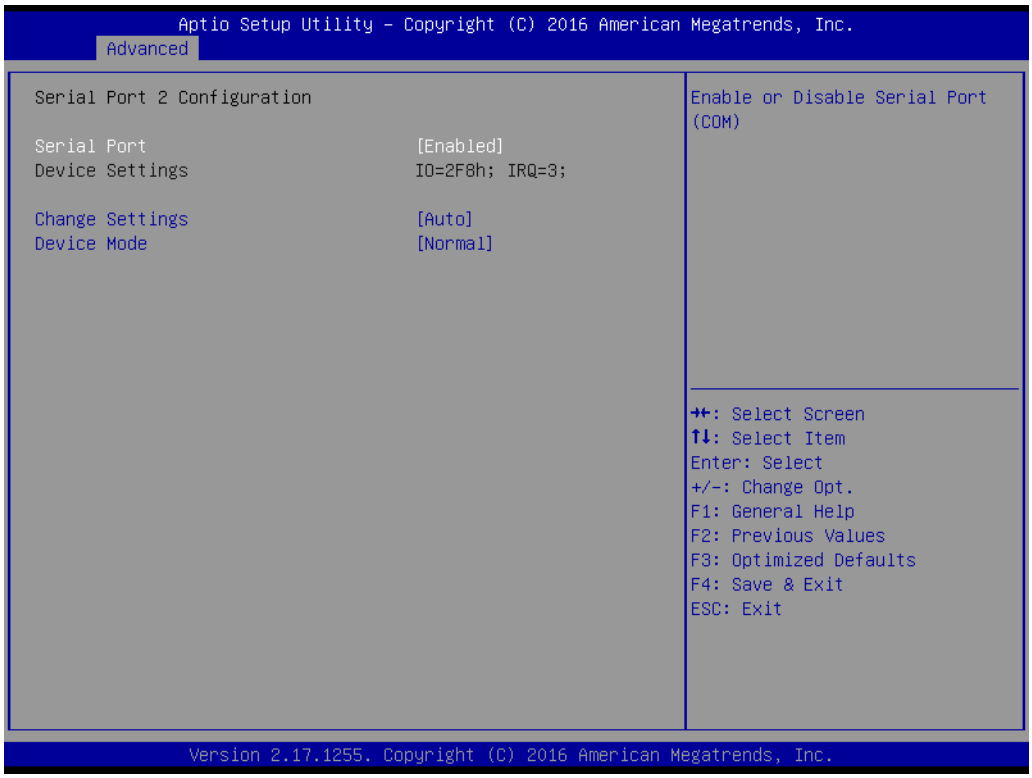


Figure 3.8 Serial Port 2 Configuration

- **Serial Port**
  Enable or Disable Serial Port (COM).
- **Change Settings**
  Select an optimal setting for Super IO device.

Hardware Monitor

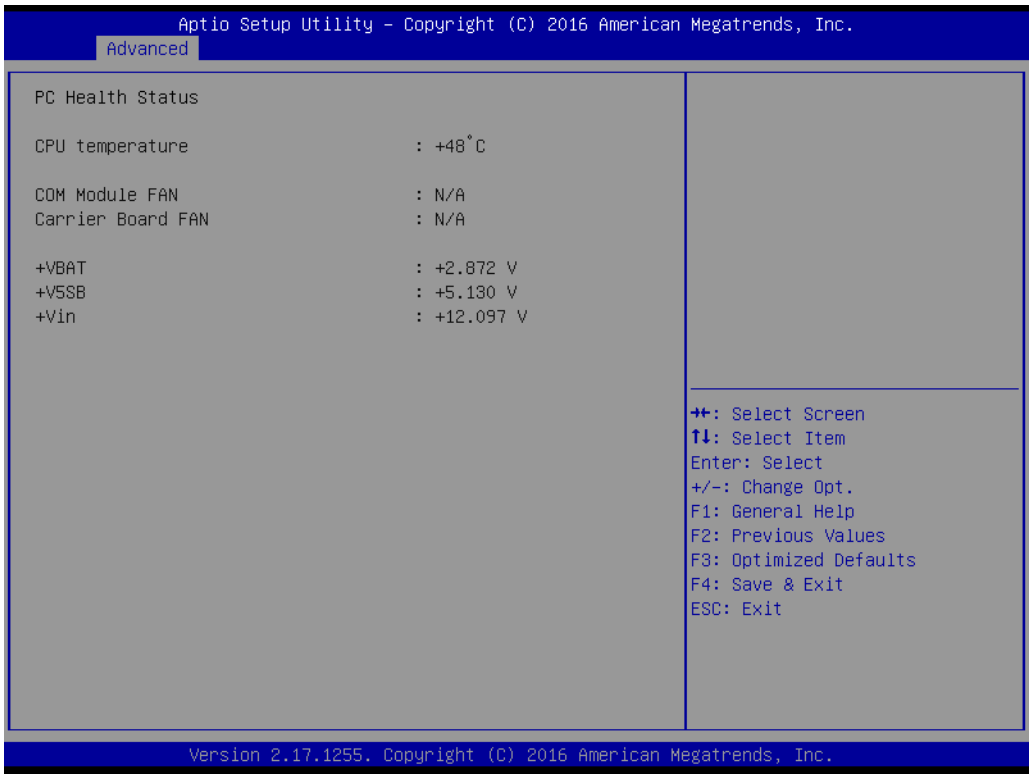


Figure 3.9 Hardware Monitor

- **Hardware Monitor Information**
  This item shows hardware information parameters.

3.2.2.4 Serial Port Console Redirection

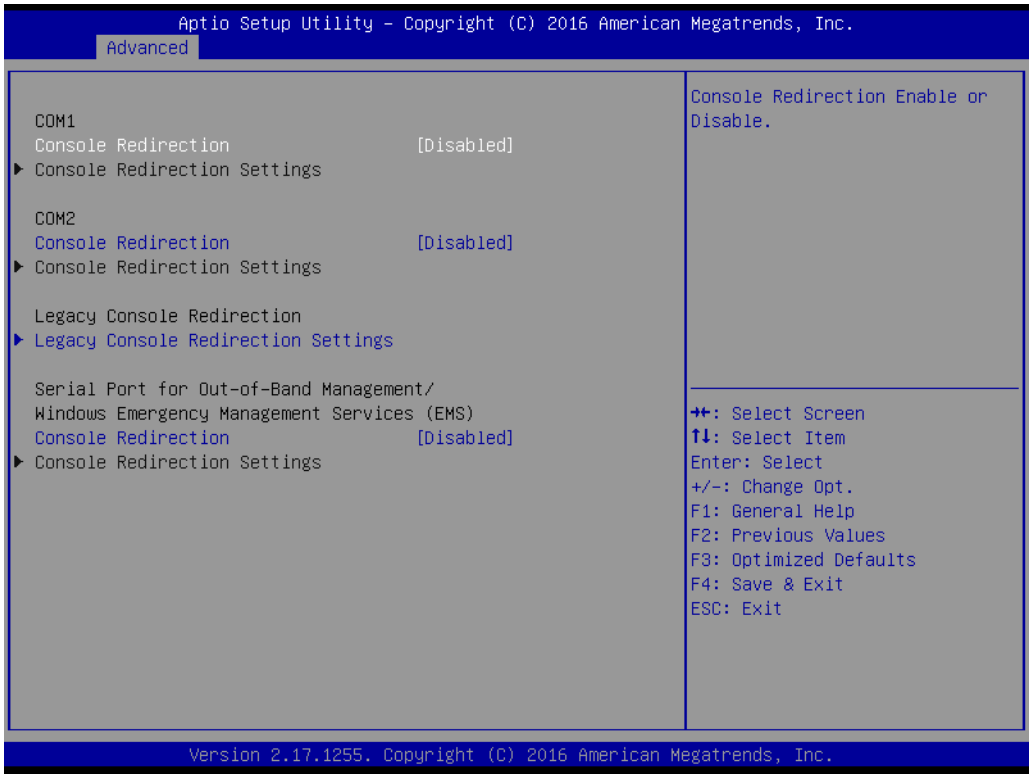


Figure 3.10 Serial Port Console Redirection

- **COM1 Console Redirection**
  Console Redirection Enable or Disable.
- **COM2 Console Redirection**
  Console Redirection Enable or Disable.
- **COM3 Console Redirection**
  Console Redirection Enable or Disable.
- **COM4 Console Redirection**
  Console Redirection Enable or Disable.
- **Serial Port for Out-of-Band Management / Windows Emergency Management Service (EMS) Console Redirection**
  Console Redirection Enable or Disable.

3.2.2.5 PCI Subsystem Settings

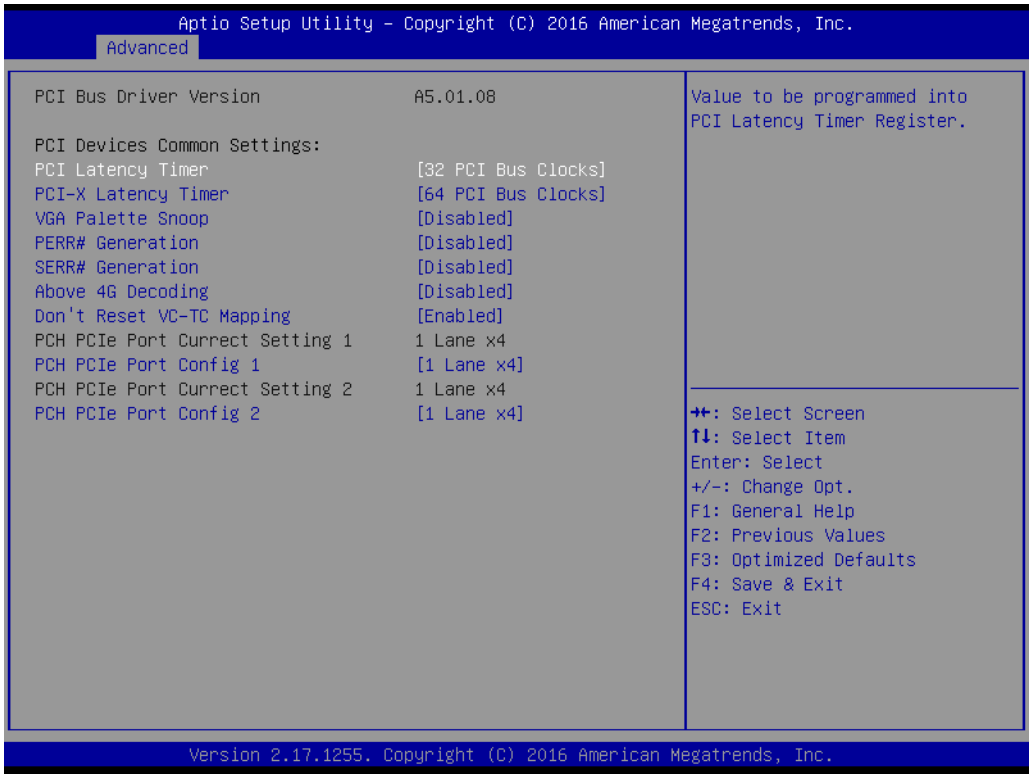


Figure 3.11 PCI Subsystem Settings

- **PCI Latency Timer**
  Press enter to select the PCI Bus clocks.
- **PCI-X Latency Timer**
  Press enter to select the PCI Bus clocks.
- **VGA Palette Snoop**
  Enable or Disable VGA Palette Snoop.
- **PERR# Generation**
  Enable or Disable PERR# Generation.
- **SERR# Generation**
  Enable or Disable SERR# Generation.
- **Above 4G Decoding**
  Enable or Disable Above 4G Decoding.
- **Don’t Reset VC-TC Mapping**
  Enable or Disable Don’t Reset VC-TC Mapping.
- **PCH PCIe Port Current Setting 1**
  PCH PCIe Port Config 1.
  Press enter to select the config.
- **PCH PCIe Port Current Setting 2**
- **PCH PCIe Port Config 2**
  Press enter to select the config.

3.2.2.6 Network Stack Configuration

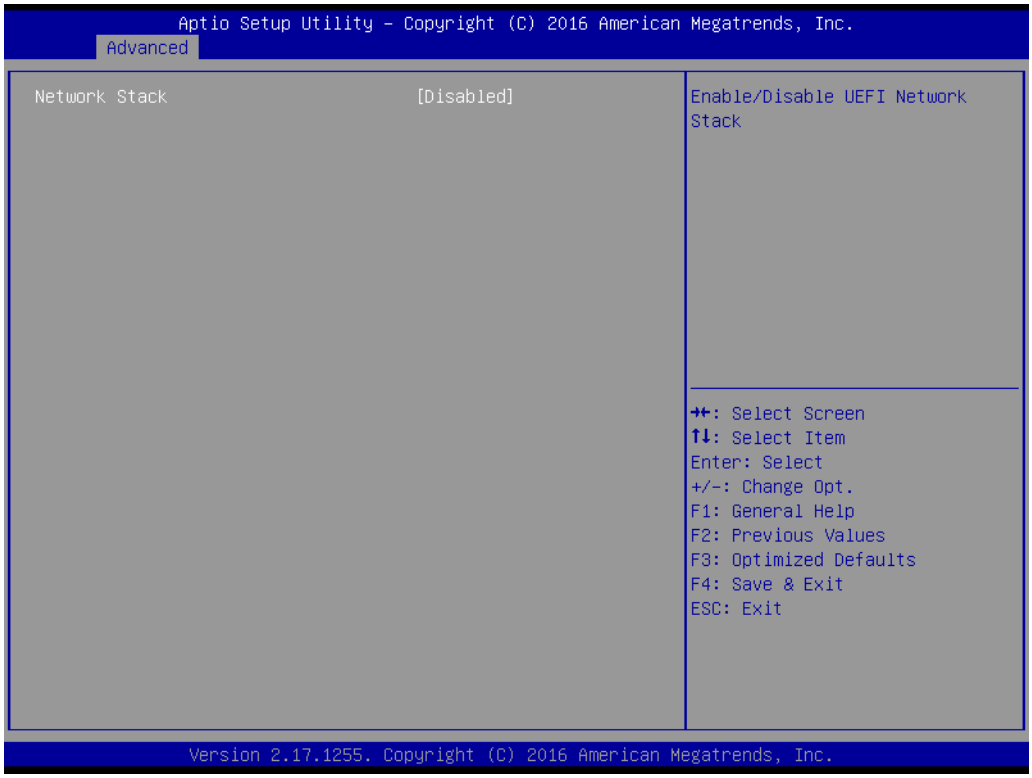


Figure 3.12 Network Stack Configurations

- **Network Stack**
  Enable or Disable Network Stack.
- **Ipc4 PXE Support**
  Enable or Disable Ipc4 PXE support.
- **Ipv6 PXE Support**
  Enable or Disable Ipv6 PXE upport.
- **PXE boot wait time**
- **Media detect count**

3.2.2.7 CSM Configuration

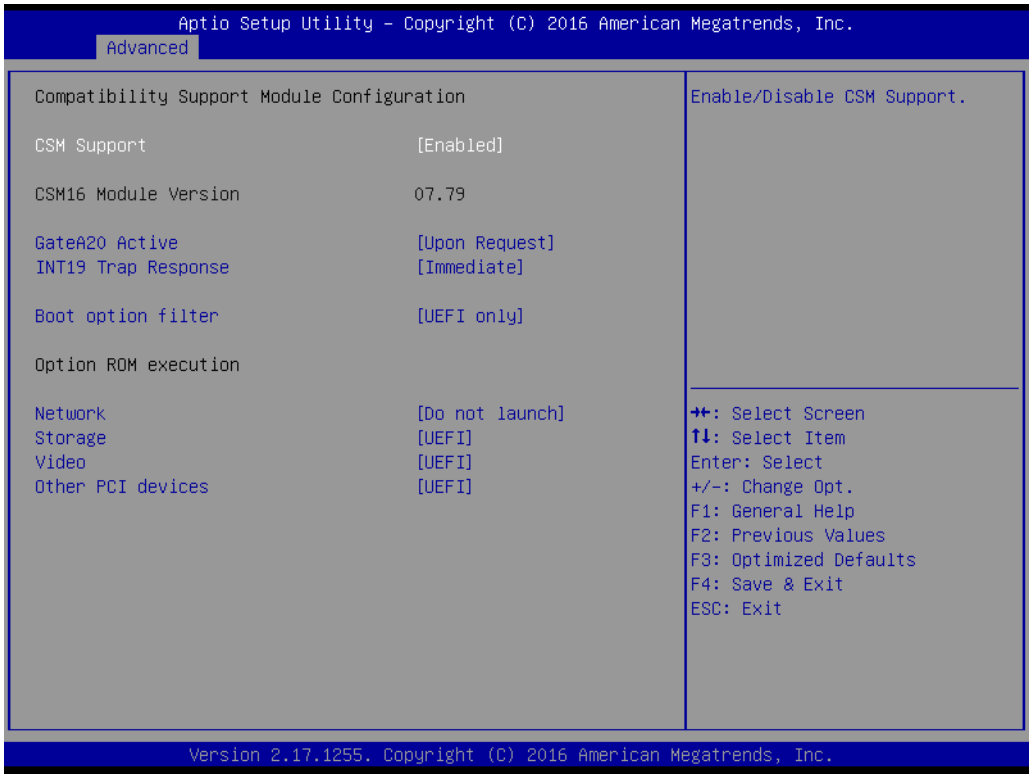


Figure 3.13 CSM Configuration

- **CSM Support**
  Enable or Disable CSM Support.
- **GateA20 Active**
  UPON Request- GA20 can be disabled using BIOS services. Do not allow disabling INT19 Trap Response; 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.

3.2.2.8 NVMe Configuration

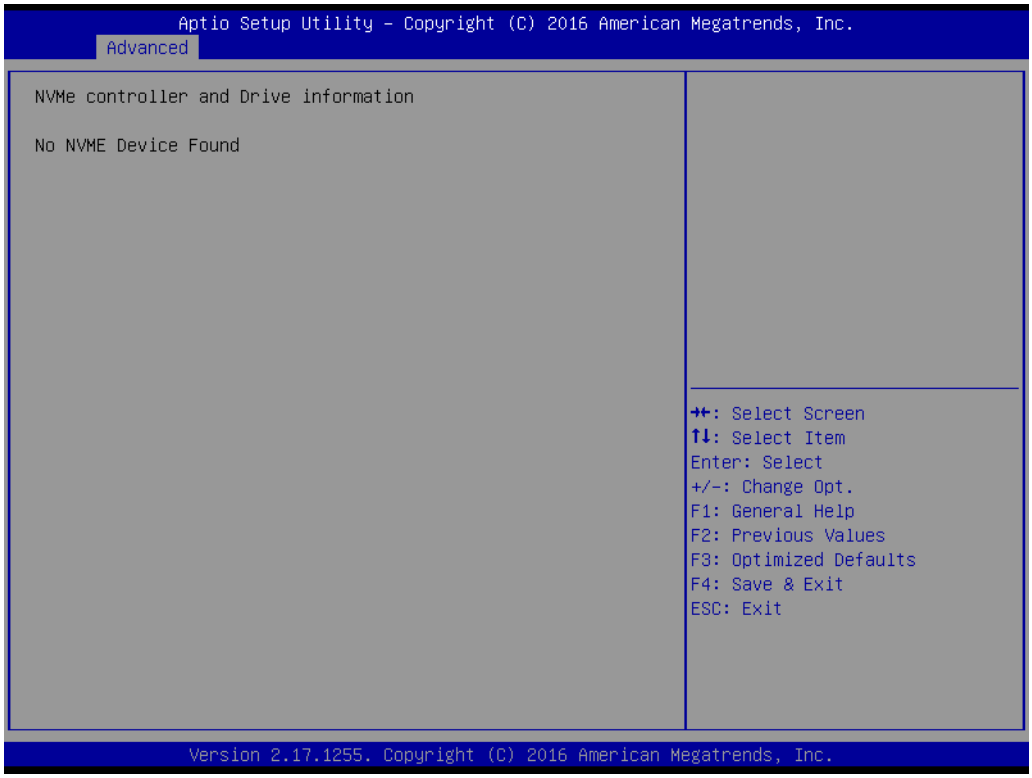


Figure 3.14 NVMe Configuration

- **NVMe Device Options Setting**
  User can adjsut the setting after inserting the NVMe device.

3.2.2.9 USB Configuration

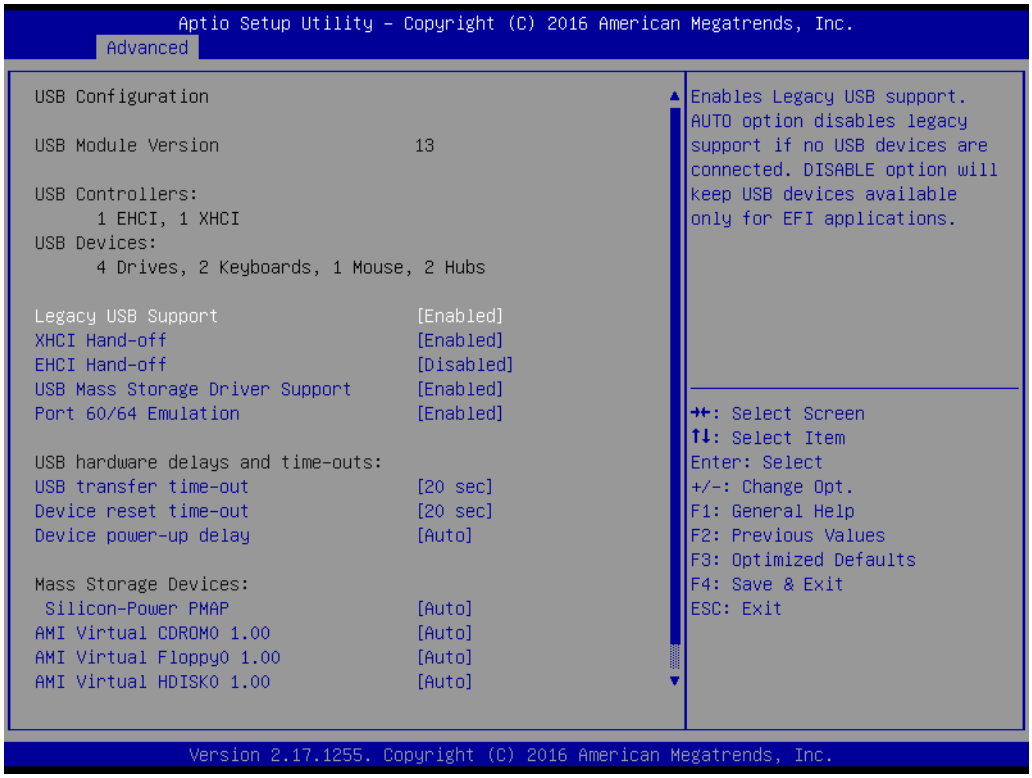


Figure 3.15 USB Configuration

- **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-5991 setup screen to enter the BIOS Setup screen. You can select the items by highlighting it using by 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.

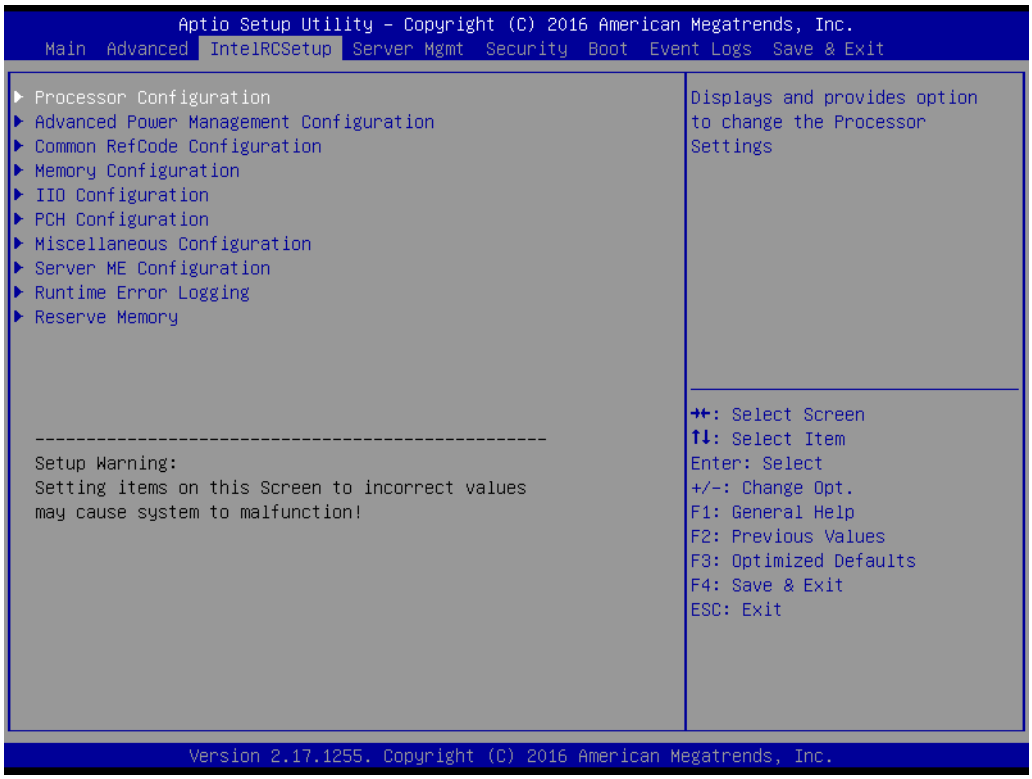


Figure 3.16 Intel RCSetup

- **Processor Configuration**
  Displays and provides options to change the Processor Settings.
- **Advanced Power Management Configuration**
  Displays and provides options to change the Power Management Settings.
- **Common RefCode Configuration**
  Displays and provides options to change the Common RefCode Settings.
- **Memory Configuration**
  Displays and provides options to change the Memory Settings.
- **IIO Configuration**
  Displays and provides options to change the IIO Settings.
- **PCH Configuration**
  Displays and provides options to change the PCH Settings.
- **Miscellaneous Configuration**
- **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

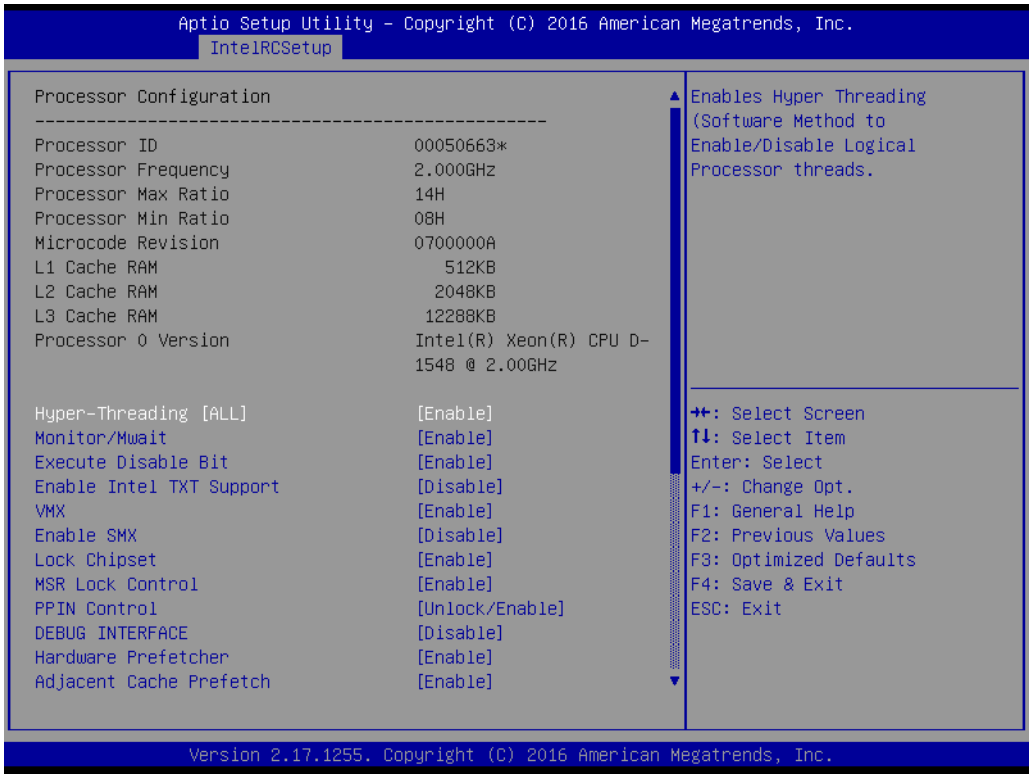


Figure 3.17 Processor Configuration -1

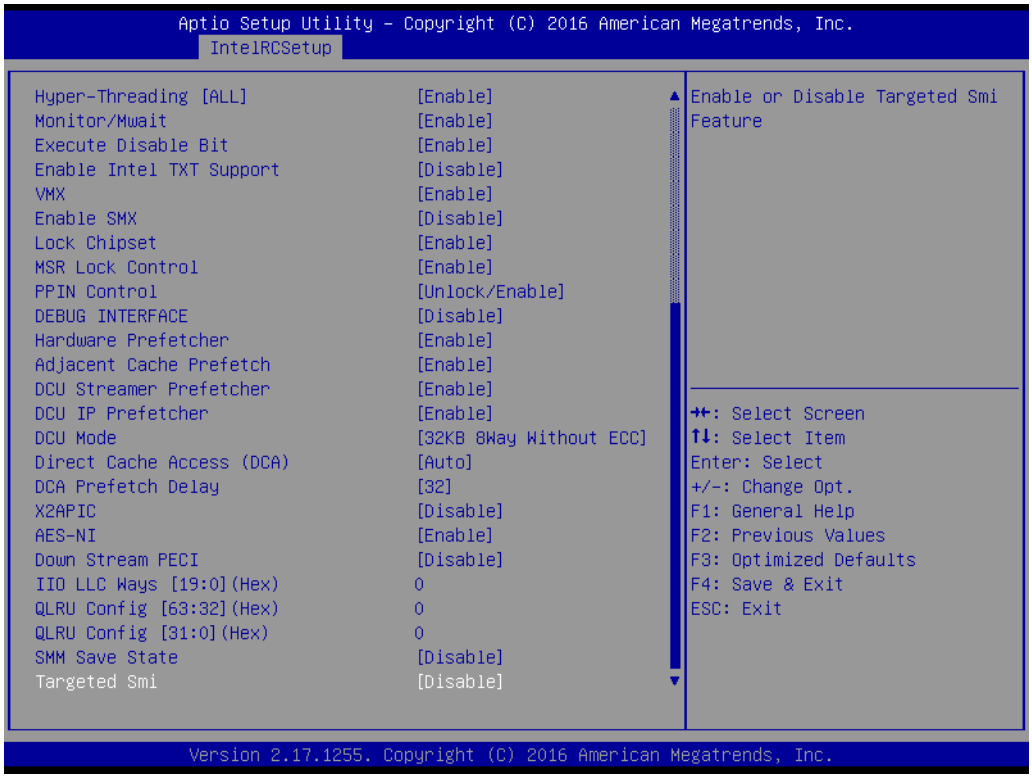


Figure 3.18 Processor Configuration -2

- **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 the Vanderpool Technology, takes effort after reboot.
- **Enable SMX**
  Enables Safer 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 lock bits.
- **PPIN Control**
  Unlock and Enable/Disable PPIN Control.
- **Debug Interface**
  MSR 0C80h bit [0], When set enables te debug 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**
  Enables 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

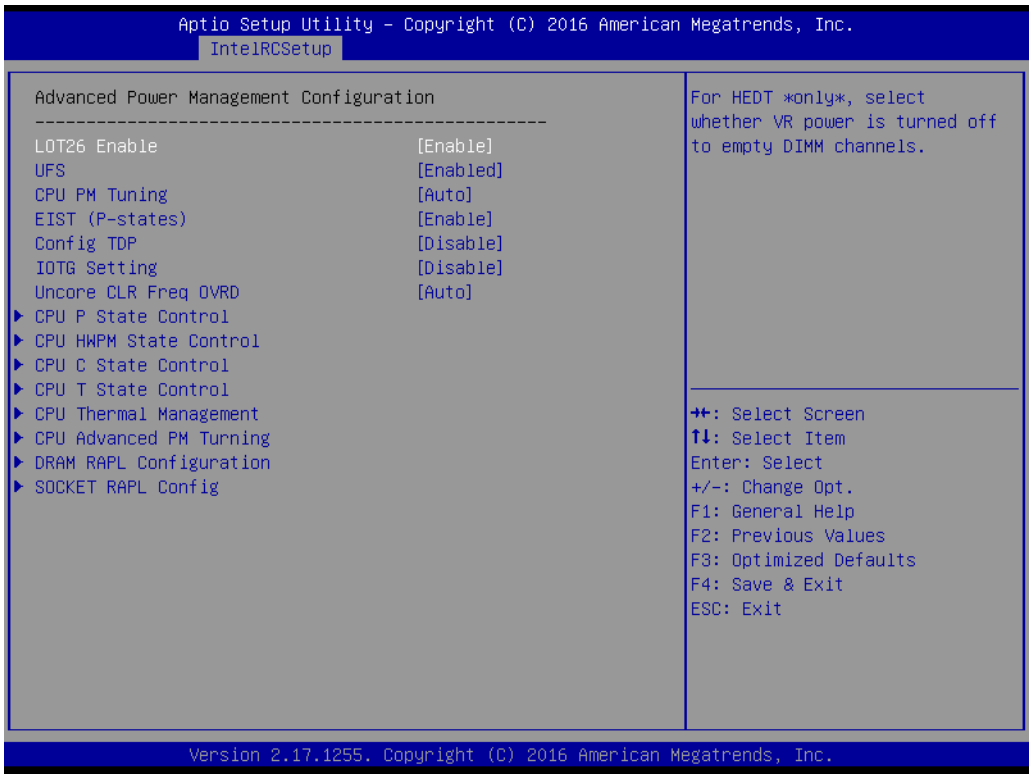


Figure 3.19 Advanced Power Management Configuration

- **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 selected as ‘AUTO’, all bit in MSR 1FCh keeping value as P0.
- **EIST (P-states)**
  When enabled, OS sets CPU frequency according load. When disable, CPU frequency is set at Max non-Turbo.
- **Config TDP**
  Setting in PCU_MISC_CONFIG Bit [28]. Optional 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

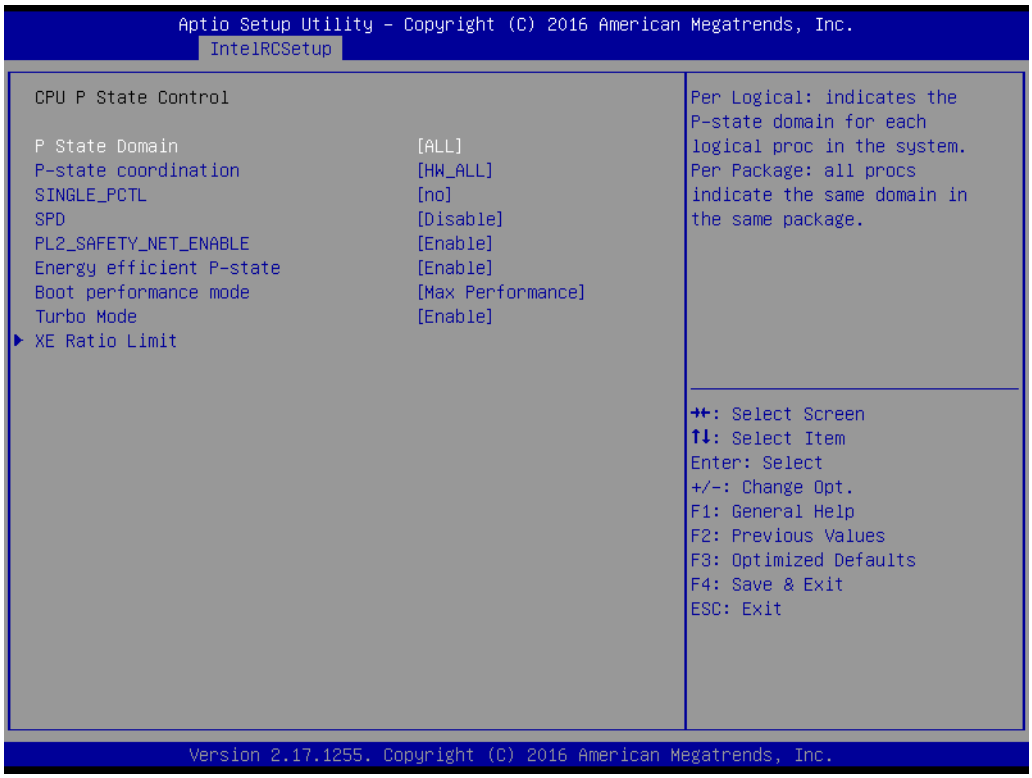


Figure 3.20 CPU P State Control

- **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 exceed CPU defined limits.

XE Ratio Limit

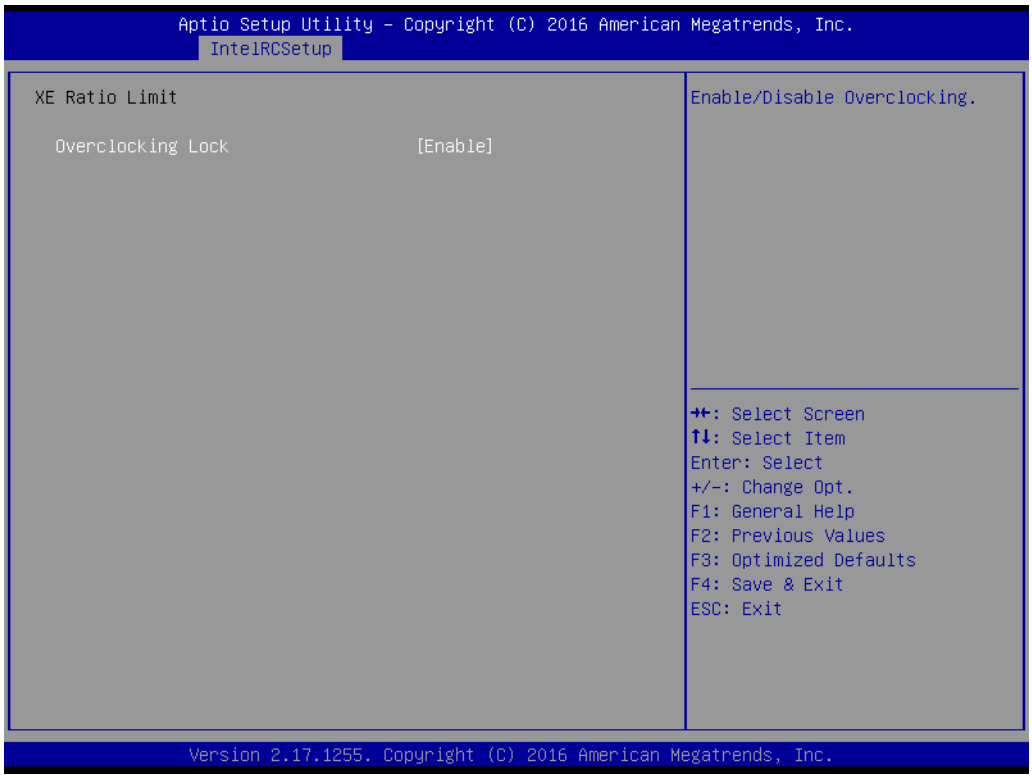


Figure 3.21 XE Ratio Limit

- **Overclocking Lock**
  Enable/Disable Overclocking.

CPU C State Control

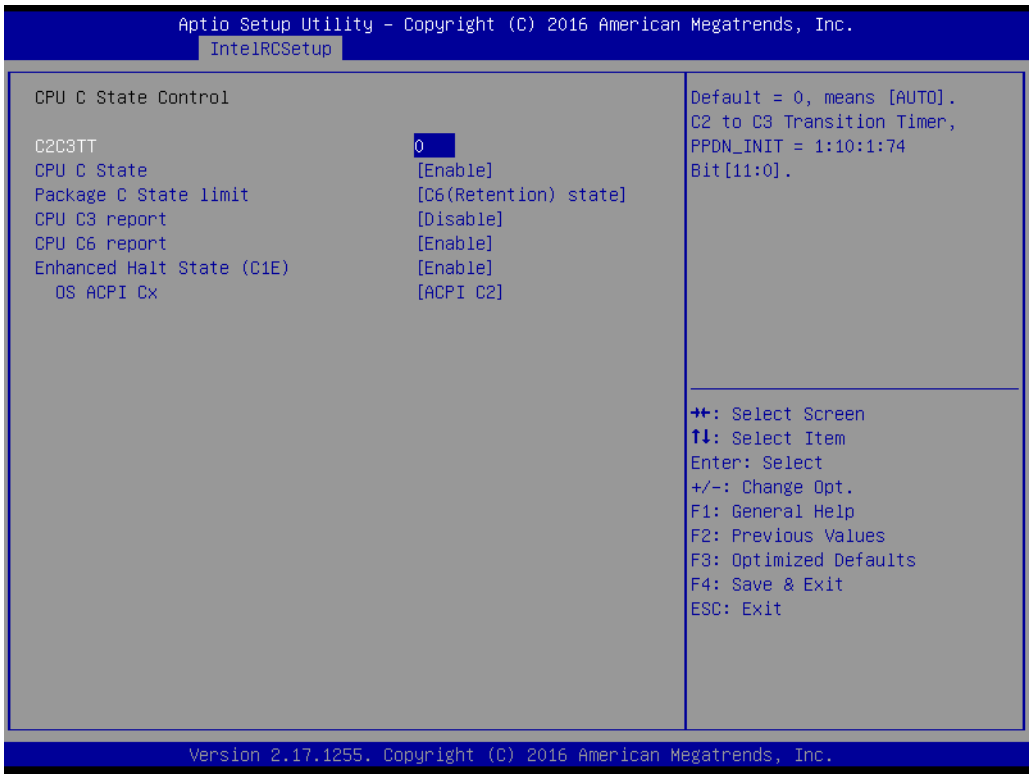


Figure 3.22 CPU C State Control

- **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.

CPU T State Control

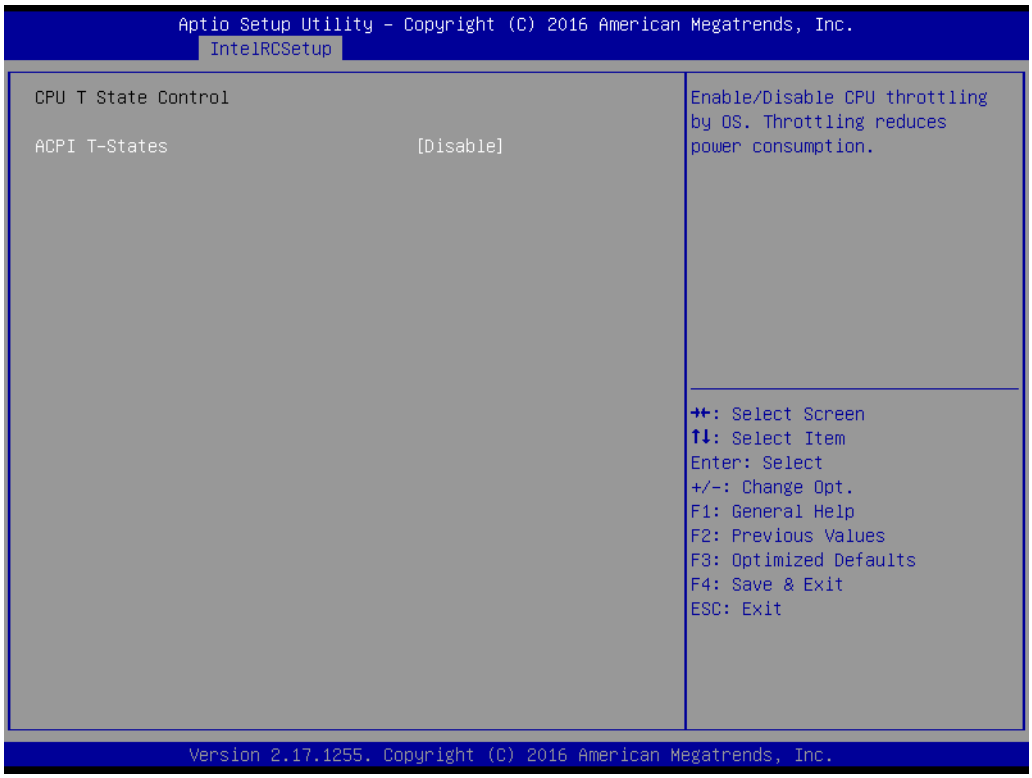


Figure 3.23 CPU T State Control

- **ACPI T-States**
  Enable or Disable CPU throttling by OS. Throttling reduces power consumption.

CPU Thermal Management

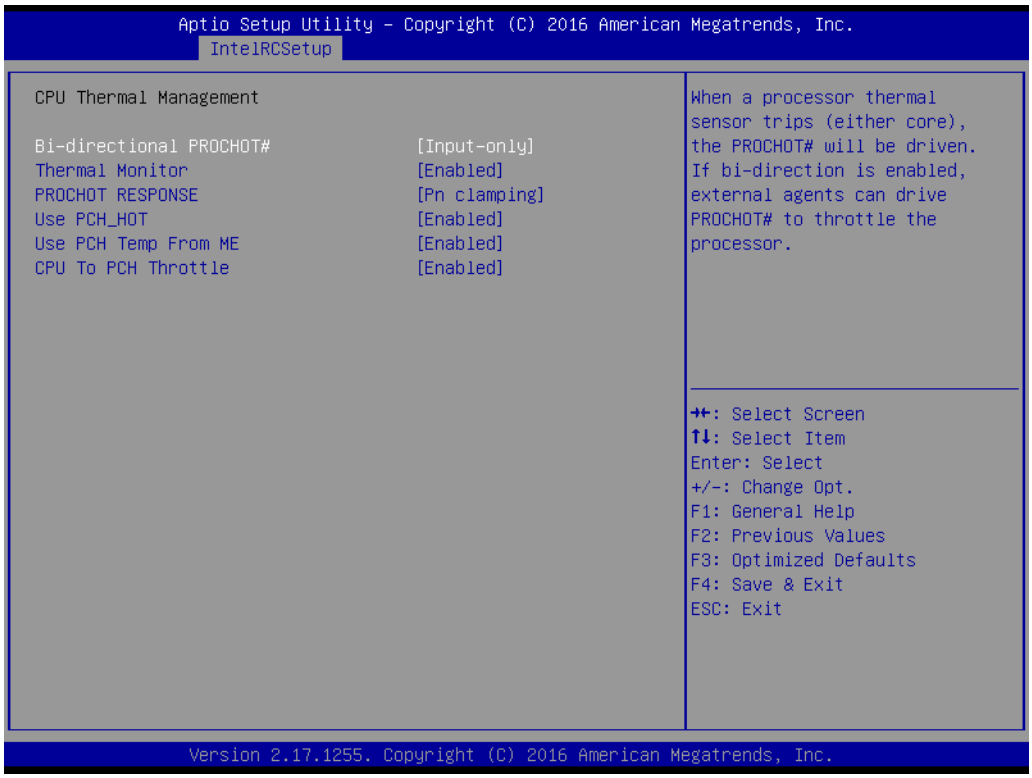


Figure 3.24 CPU Thermal Management

- **Bi-directional PROCHOT#**
  When a processor thermal sensor trips (either core), the PROCHOT# will be driven. IF bi-direction is enabled, external agents can drive PROCHOT# to throttle the processor.
- **Thermal Monitor**
  Enable or Disable Thermal Monitor.
- **PROCHOT PREPONSE**
  Force CPU to throttle to a lower power condition such as Pn/Pm by asserting PROCHOT#. MSR 0xaFC [26]
  =1: go to Pm(min freq) on PROCHOT; =0: go to Pn (max efficient freq).
- **Use PCH_HOT**
  Pcode is allowed to se PCH_HOT pin information for thermal management.
- **Use PCH Temp From ME**
  Pcode is allowed to use PCH Temperature provided by ME.
- **CPU To PCH Throttle**
  Enable Pcode to throttle PCH.

CPU Advanced PM Turning

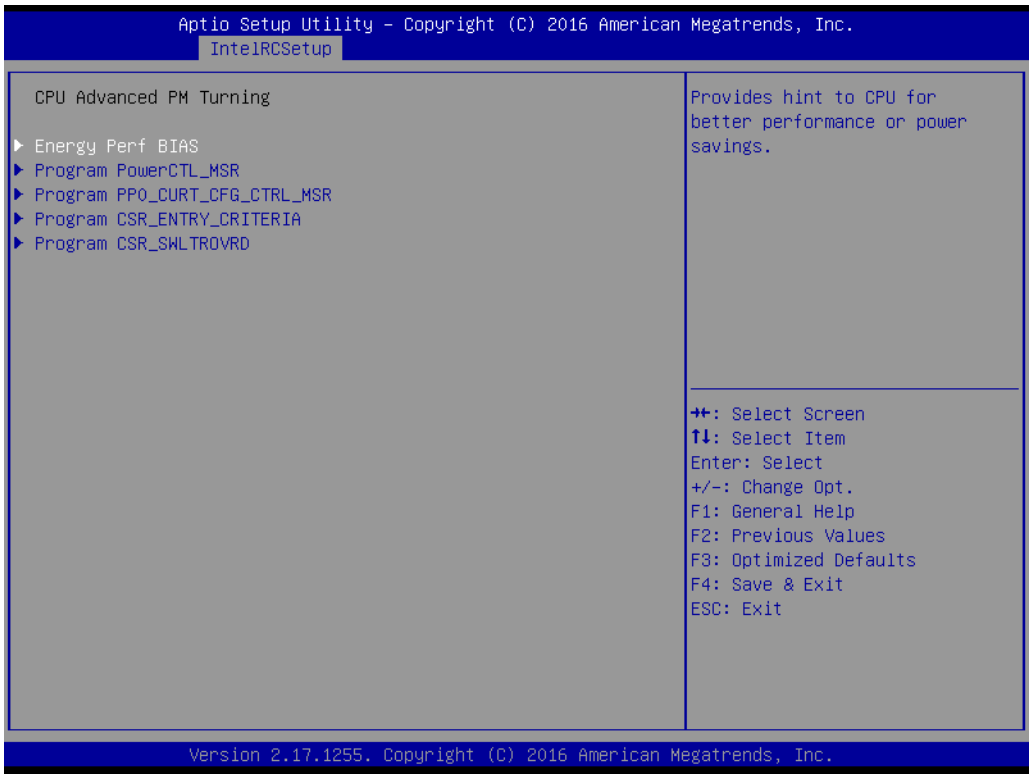


Figure 3.25 CPU Advanced PM Turning

- **Energy Perf BIAS**
  Provides hints to the 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.
- **Program CSR_SWL TROVRD**
  Pregram CSR_SWL TROVRD 1:10:1:0x78 Sub Menu.

DRAM RAPL Configuration

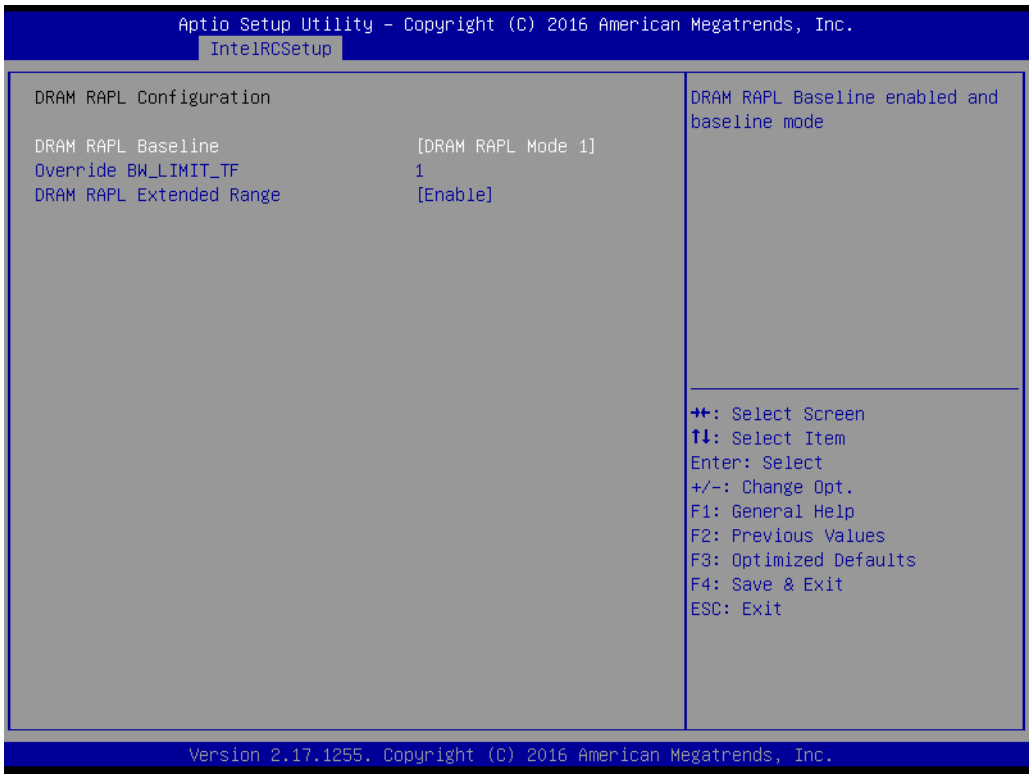


Figure 3.26 DRAM RAPL Configuration

- **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.

SOCKET RAPL Config

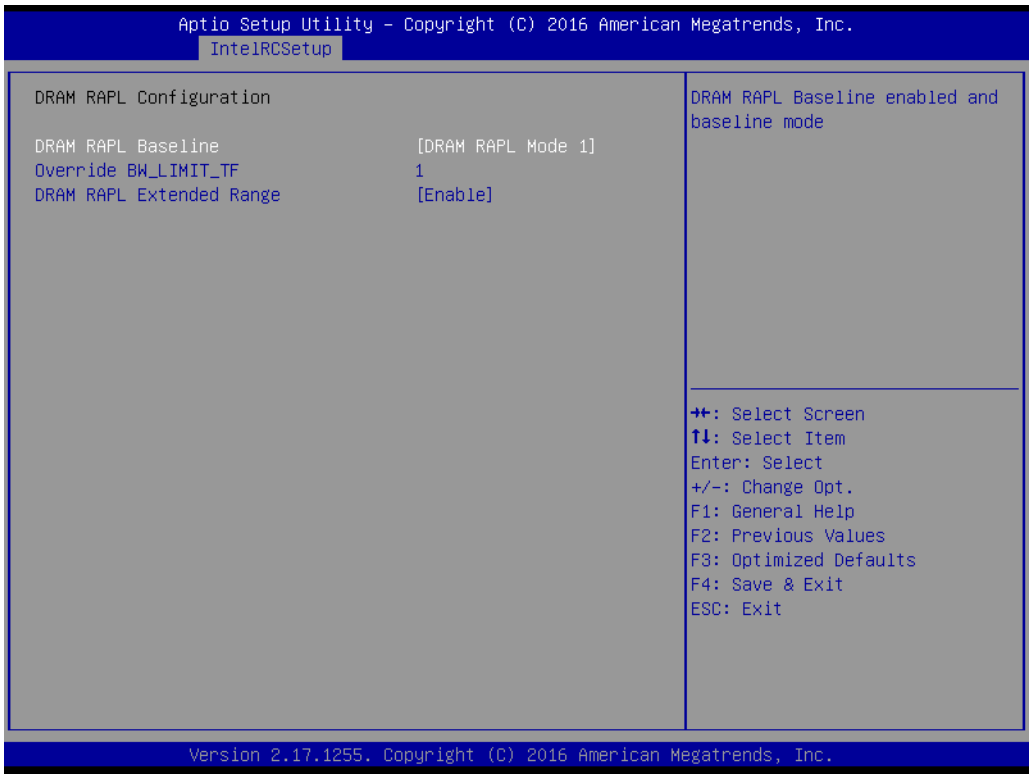


Figure 3.27 SOCKET RAPL Config

- **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 Values.
- **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, allows 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.

3.2.3.3 Common RefCode Configuration

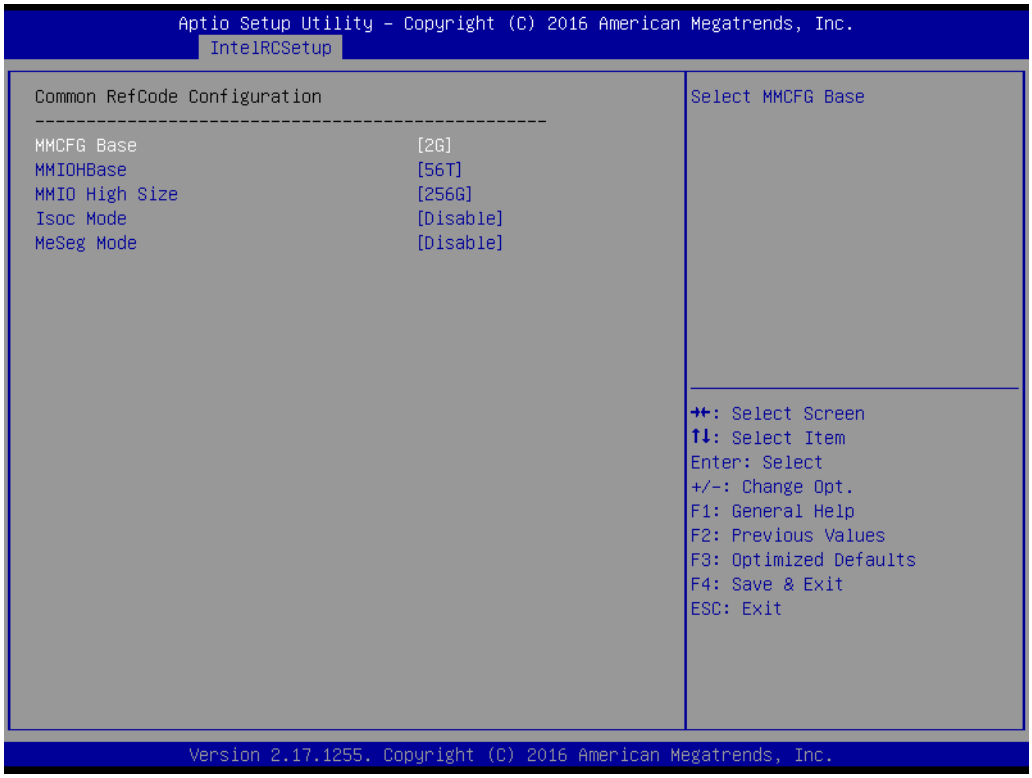


Figure 3.28 Common RefCode Configuration

- **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.

3.2.3.4 Memory Configuration

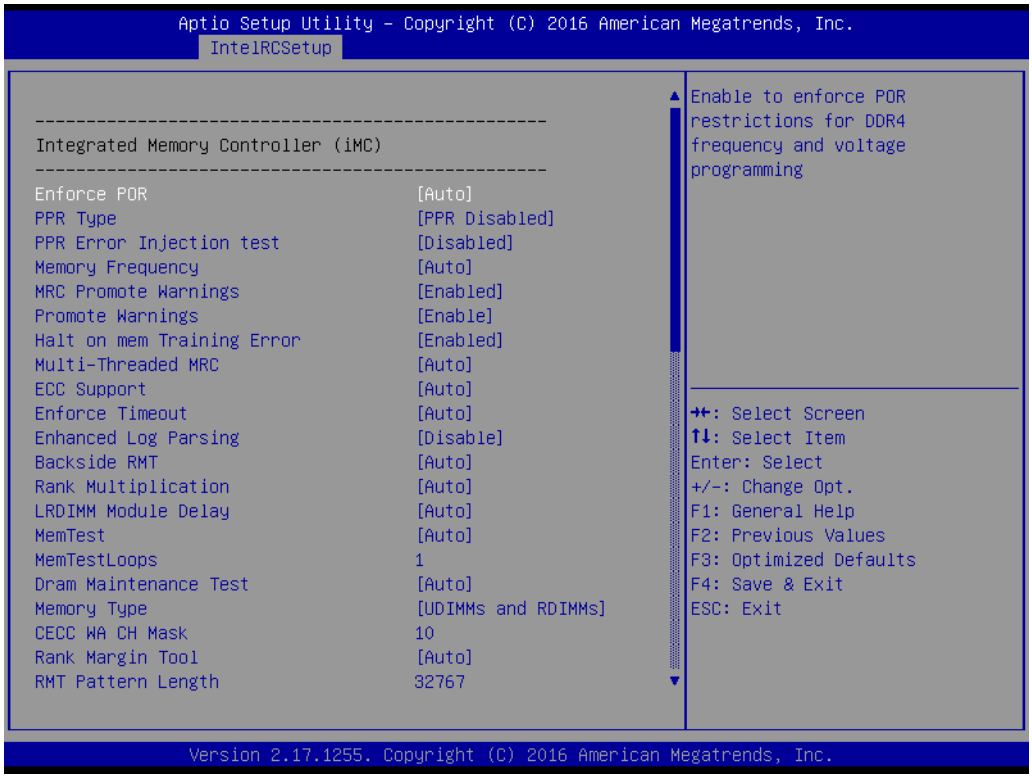


Figure 3.29 Memory Configuration -1

- **Enforce POR**
  Enable to enforce for 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 err inj test.
- **Memory Frequency**
  Maximum Memory Frequency Selections in Mhz. Do not select reserved.
- **MRC Promote Warnings**
  Determines if MRV warnings are promoted to system level 1.
- **Promote Warnings**
  Determines if warnings are promoted to system level 1.
- **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 the 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.

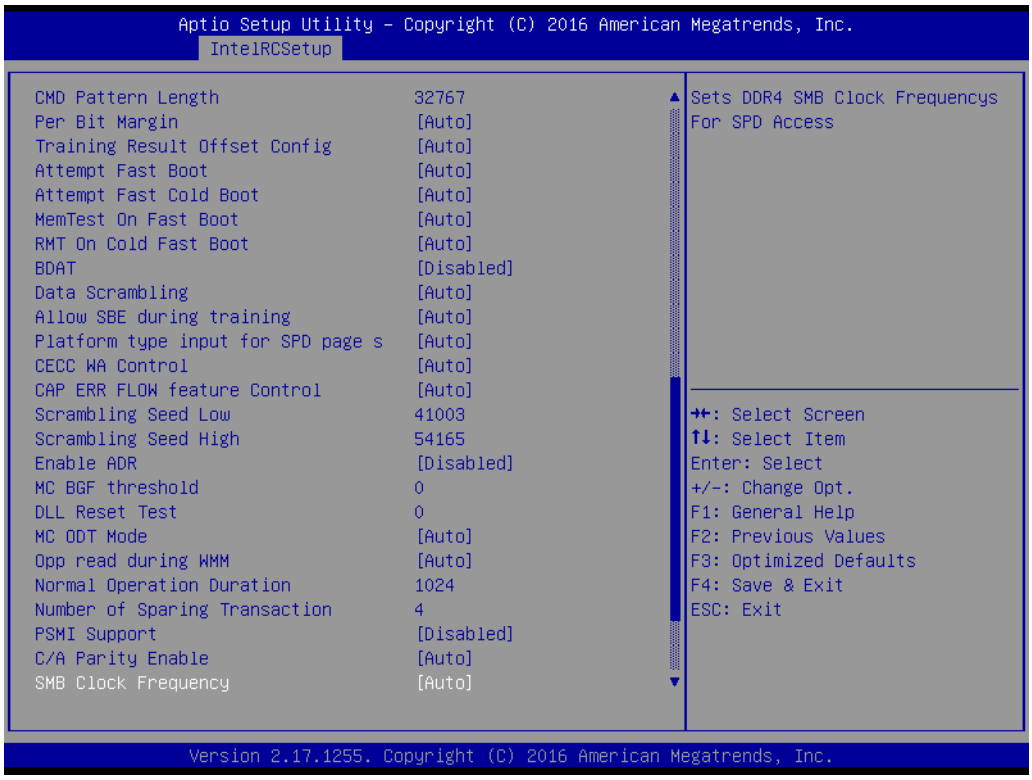


Figure 3.30 Memory Configuration -2

- **Per Bit Margin**
  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 - enable or disable.
- **Platform type input for SPD pages**
  This knob controls the SPD page selection feature. Disabled by Default.

- **CECC WA Control**
  This knob controls the CECC WA. Disabled by Default on L0 and later processor.
- **CAP ERR FLOW feature Control**
  This knob 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**
  Enables 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 loops 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

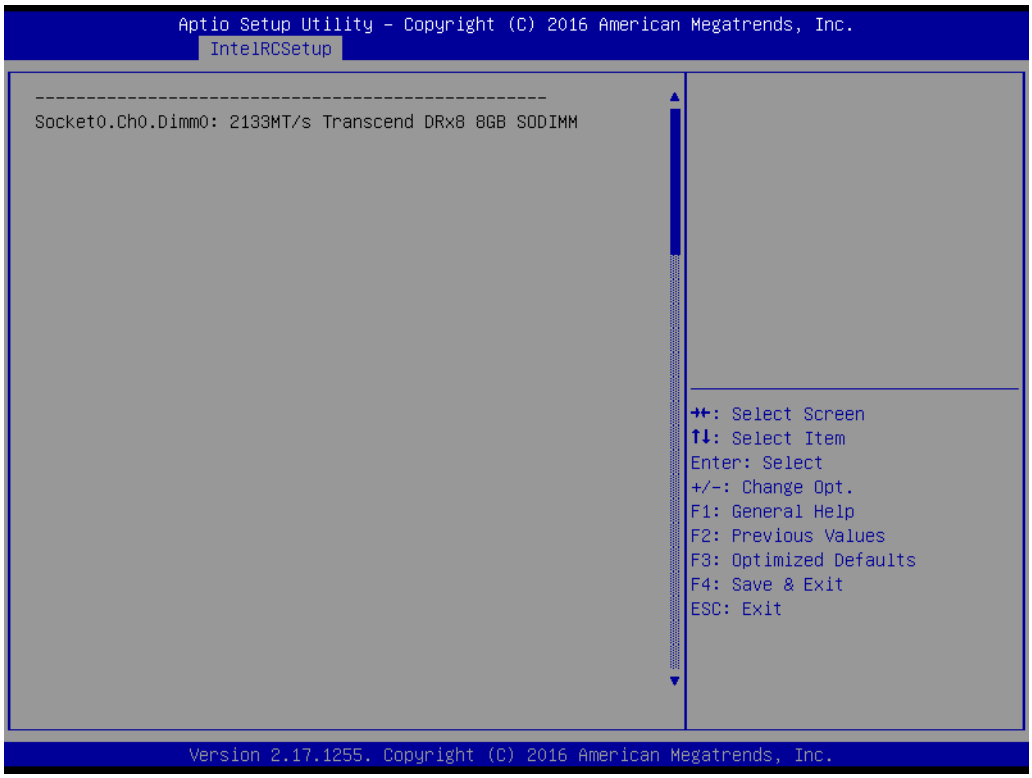


Figure 3.31 Memory Topology

Display memory topology with DIMM population information.

Memory Thermal

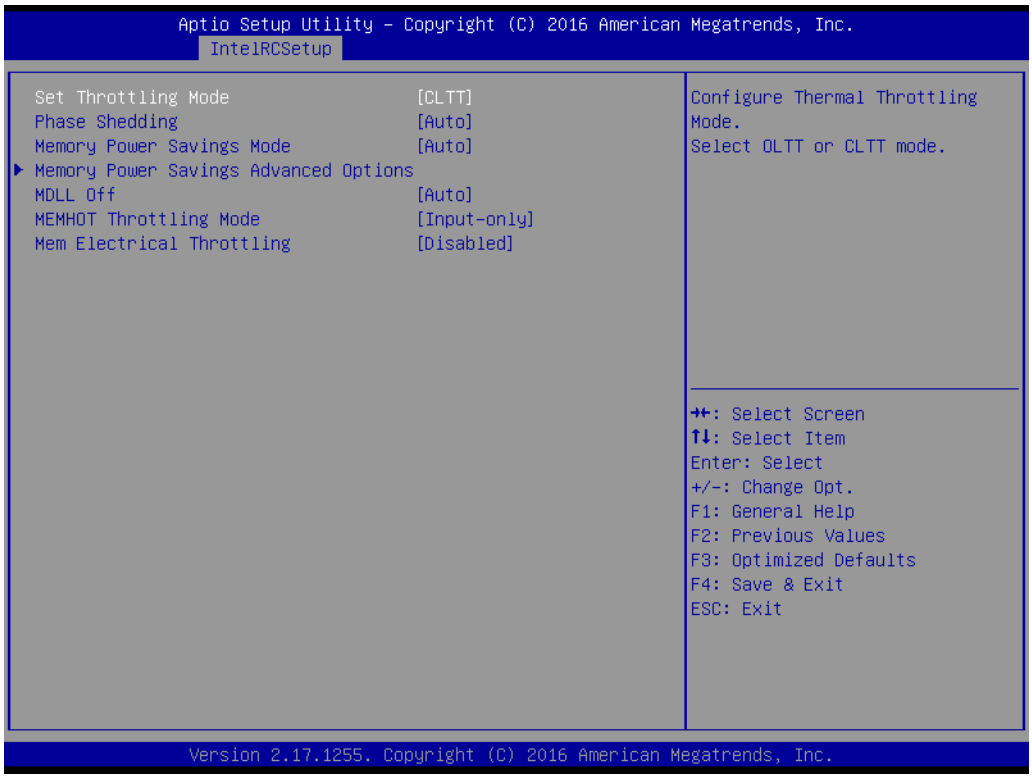


Figure 3.32 Memory Thermal

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.

Memory Power Savings Advanced Options

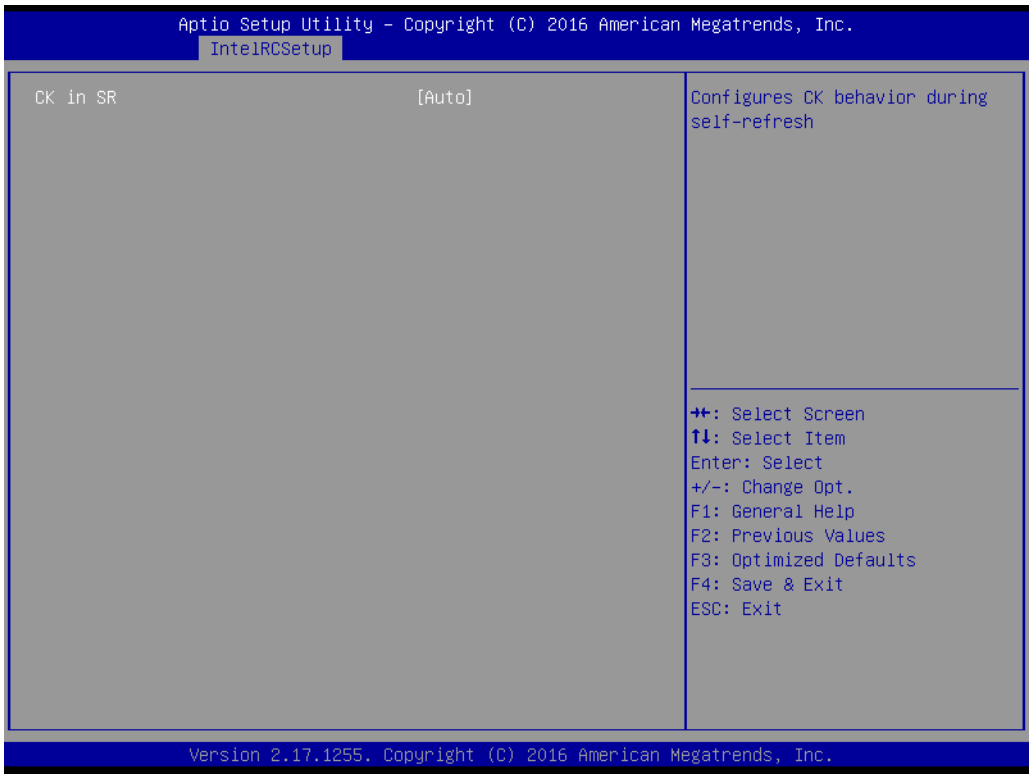


Figure 3.33 Memory Power Savings Advanced Options

Allow user to configure CK behavior during self-refresh.

Memory Timings & Voltage Override

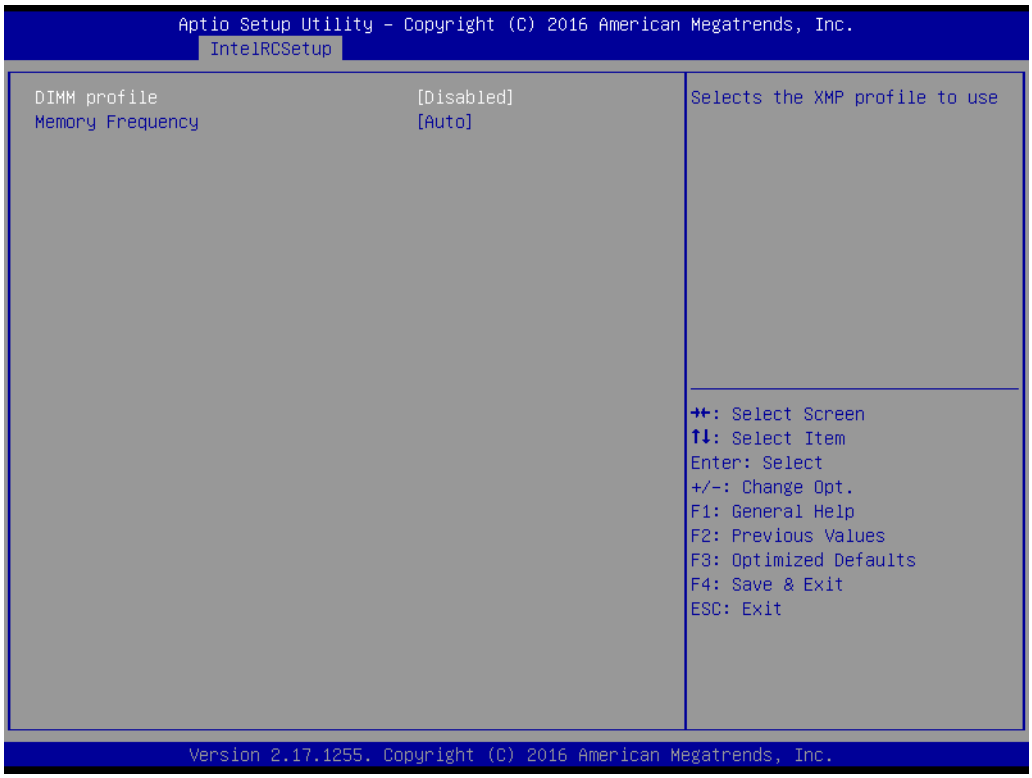


Figure 3.34 Memory Timings & Voltage Override

- **DIMM profile**
  Select the XMP profile to use.
- **Memory Frequency**
  Maximum memory frequency selection in Mhz. Do not select Reserved.

Memory Map

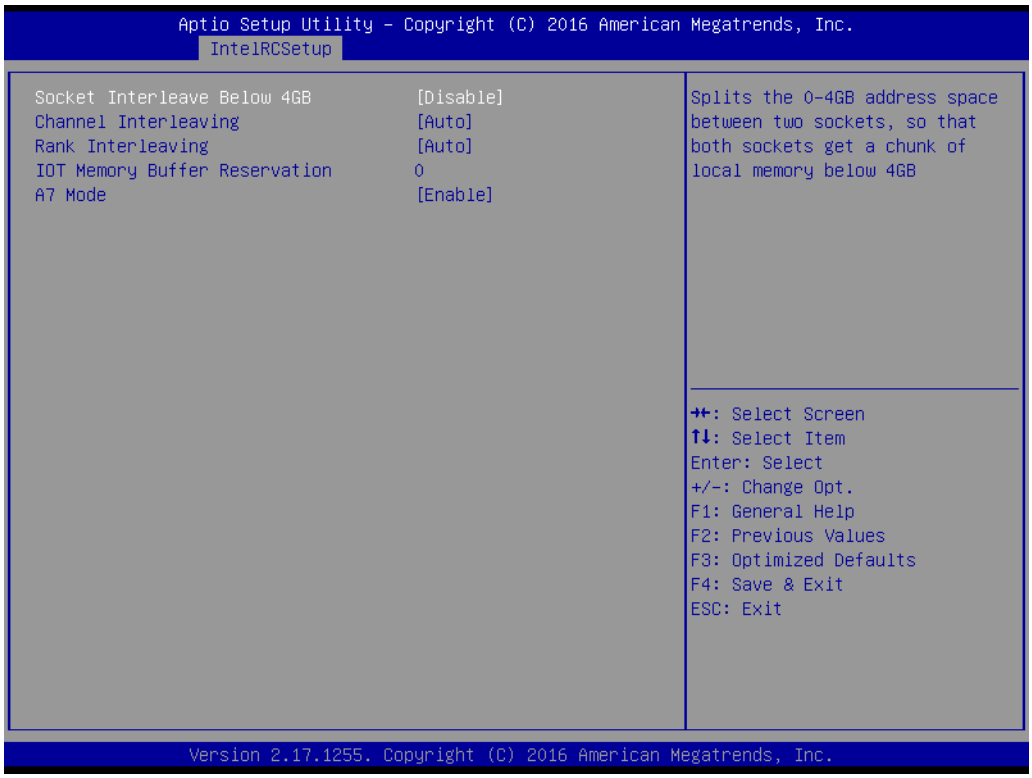


Figure 3.35 Memory Map

- **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

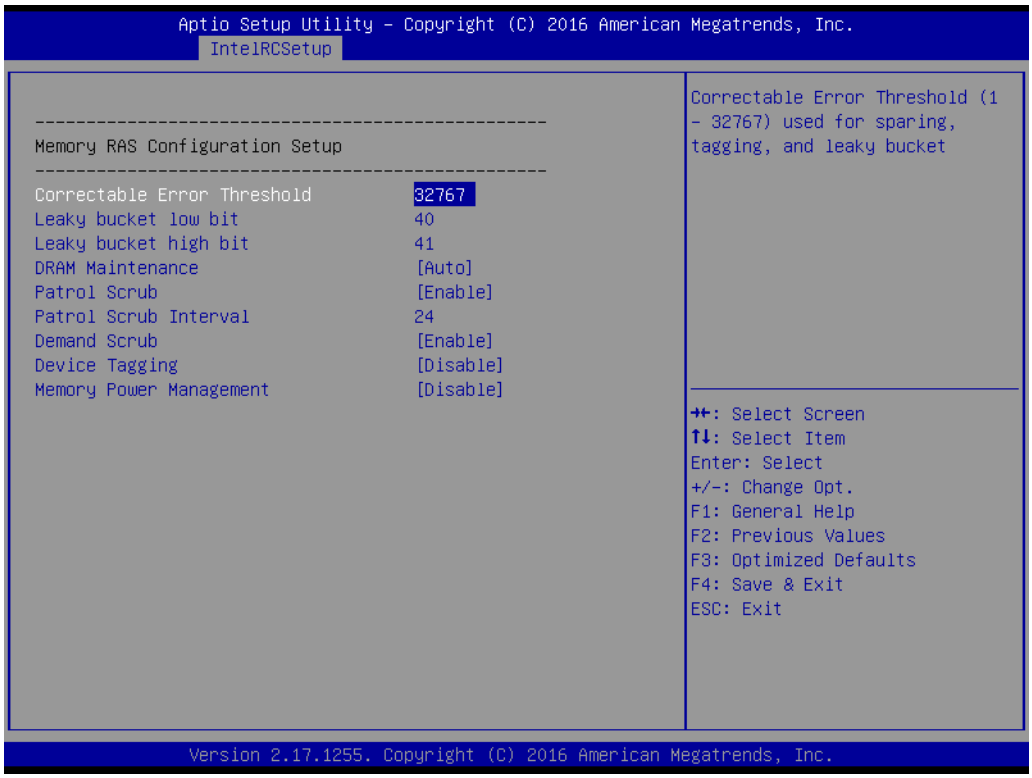


Figure 3.36 Memory RAS Configuration

Display and provide option to change the memory Ras Settings.

3.2.3.5 IIO Configuration

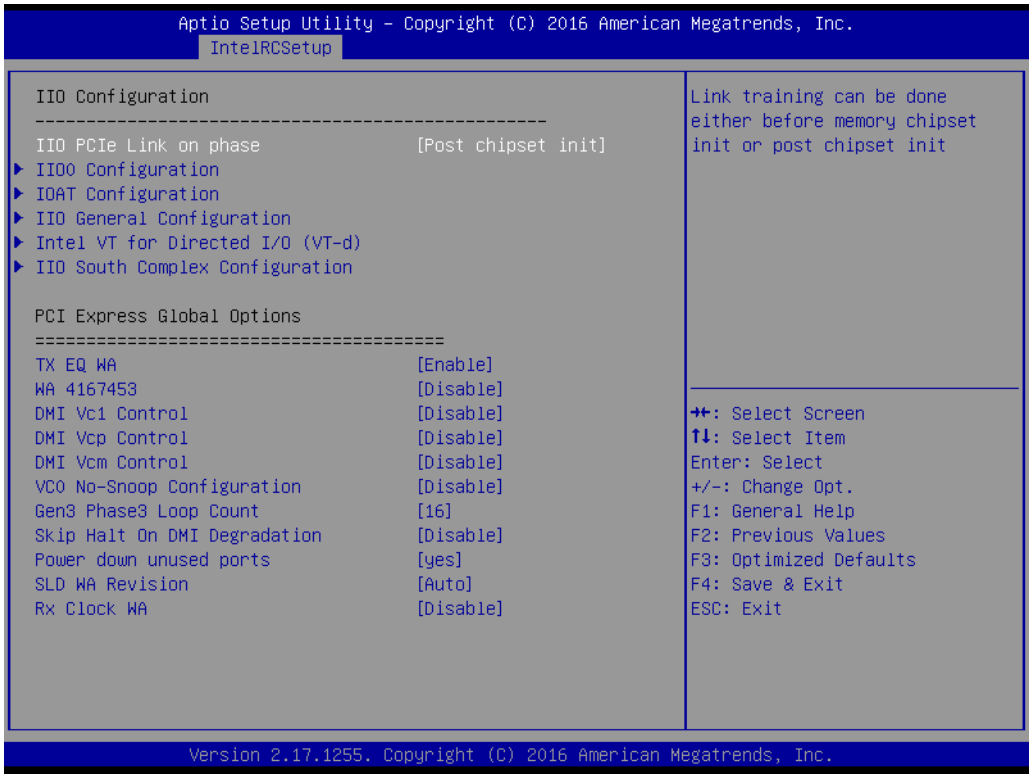


Figure 3.37 IIO Configuration

- **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 as 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

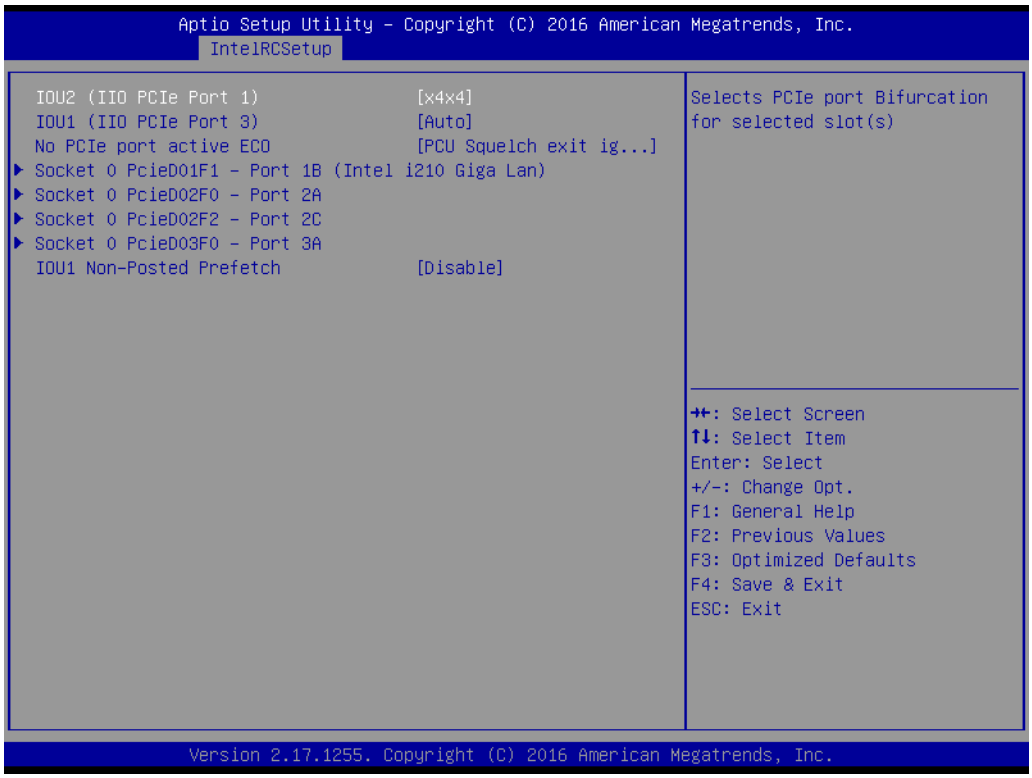


Figure 3.38 IIO Configuration

- **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 PCIe port active ECO**
  Workaround settings when no PCIe port active.

Socket 0 PcieD01F1 – Port 1B (Intel i210 Giga Lan)

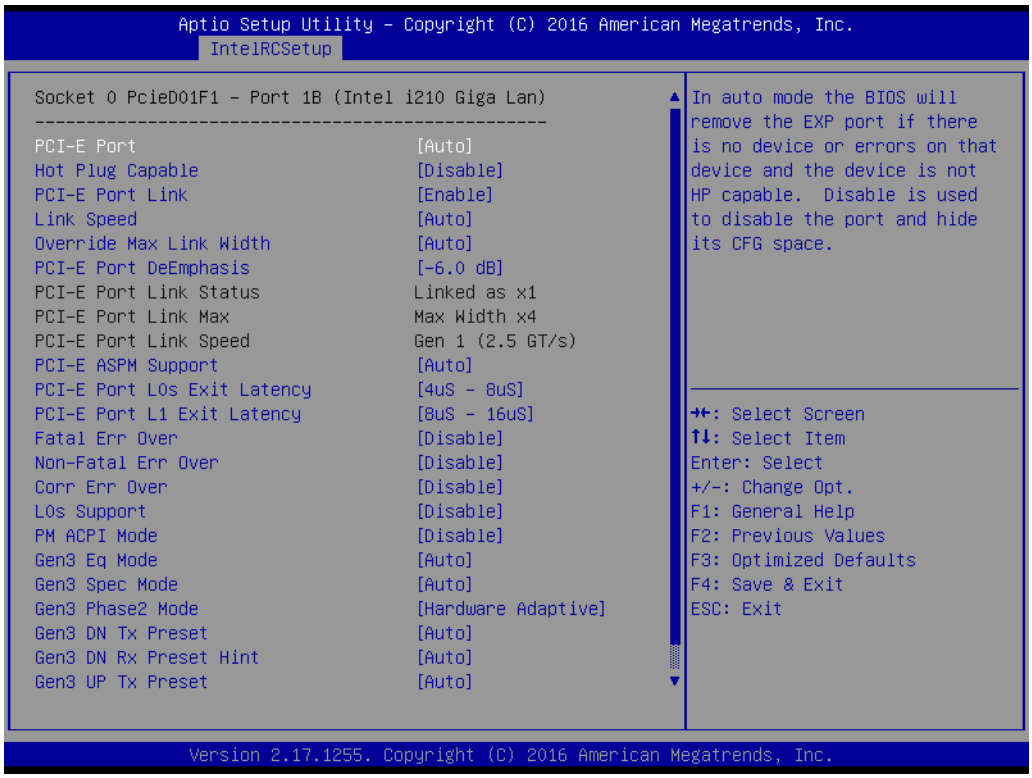


Figure 3.39 Socket 0 PcieD01F1 – Port 1B (Intel i210 Giga Lan)

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 PcieD01F2 – Port 2A

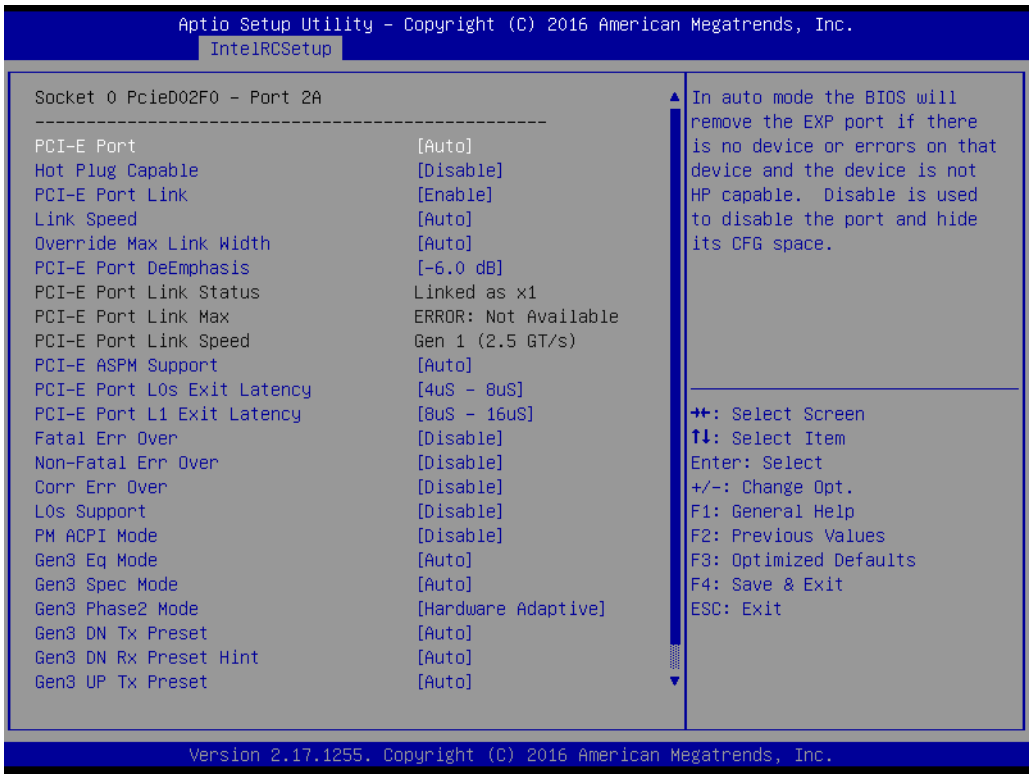


Figure 3.40 Socket 0 PcieD01F2 – Port 2A

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

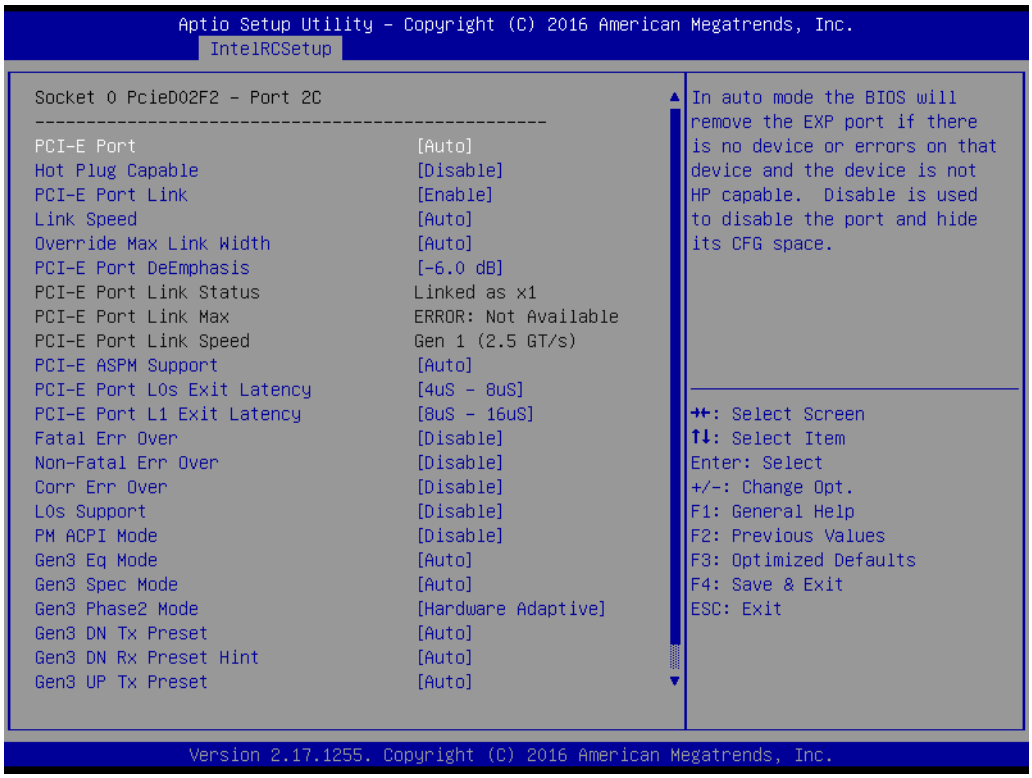


Figure 3.41 Socket 0 PcieD02F2 – Port 2C

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

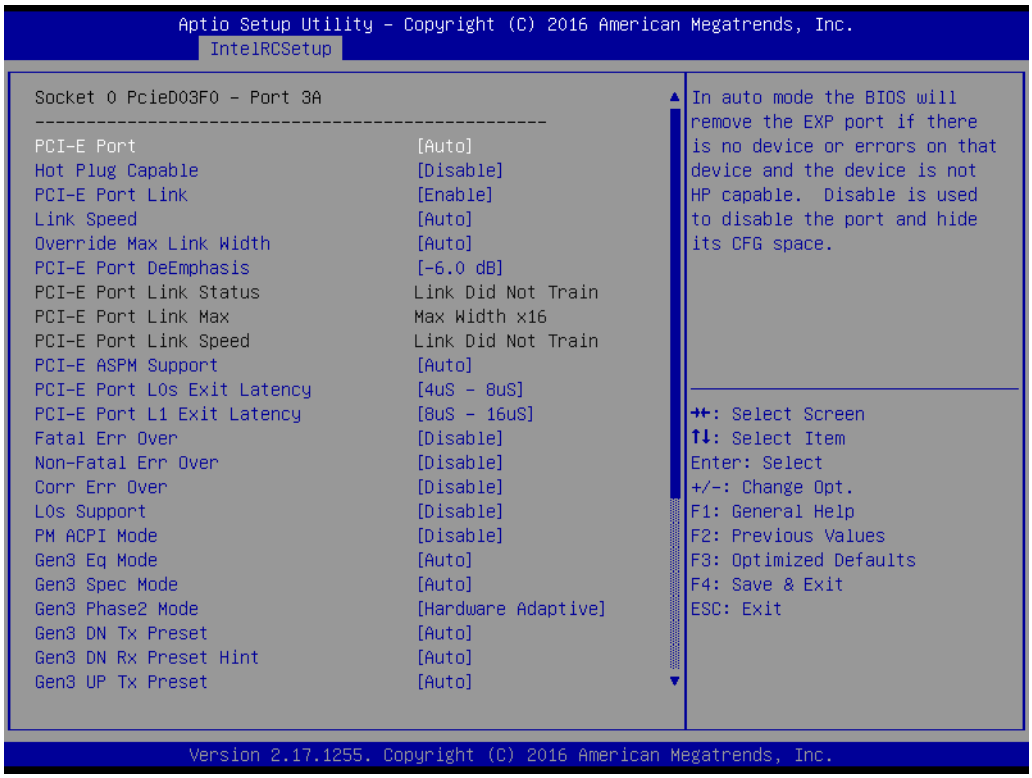


Figure 3.42 Socket 0 PcieD03F0 – Port 3A

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

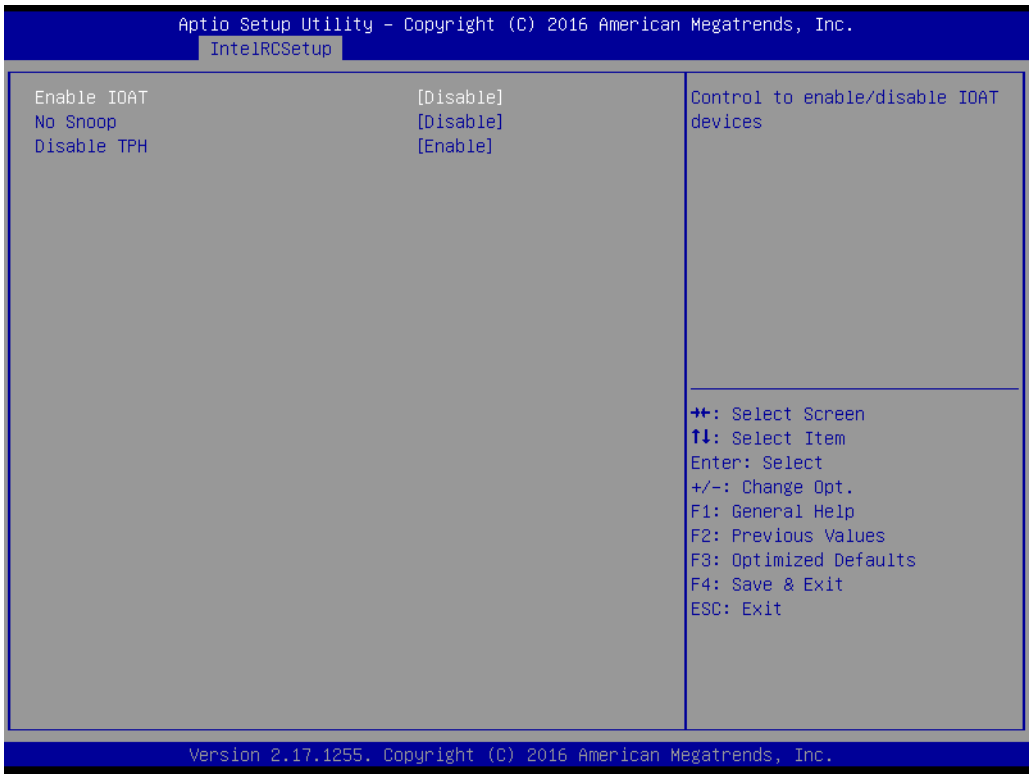


Figure 3.43 IOAT Configuration

- **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

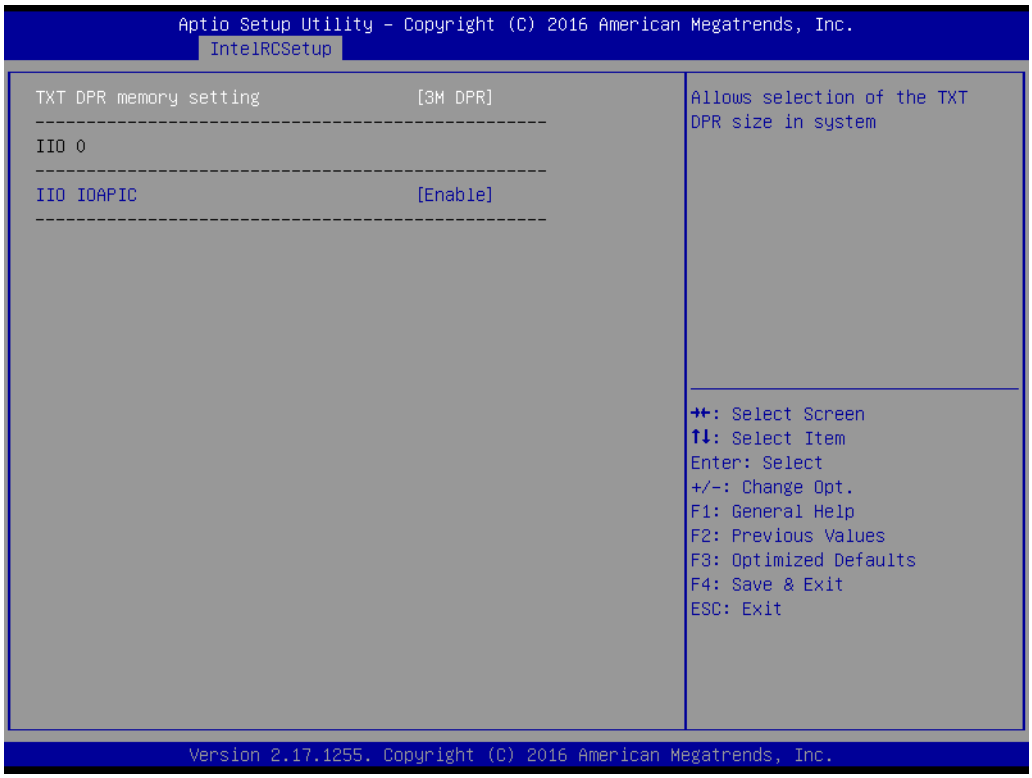


Figure 3.44 IIO General Configuration

- **TXT DPR memory setting**
  Allows selection of the TXT DPR size in system.
- **IIO 0**
- **IIO IOAPIC**
  Enable or Disable the IIO IOAPIC.

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

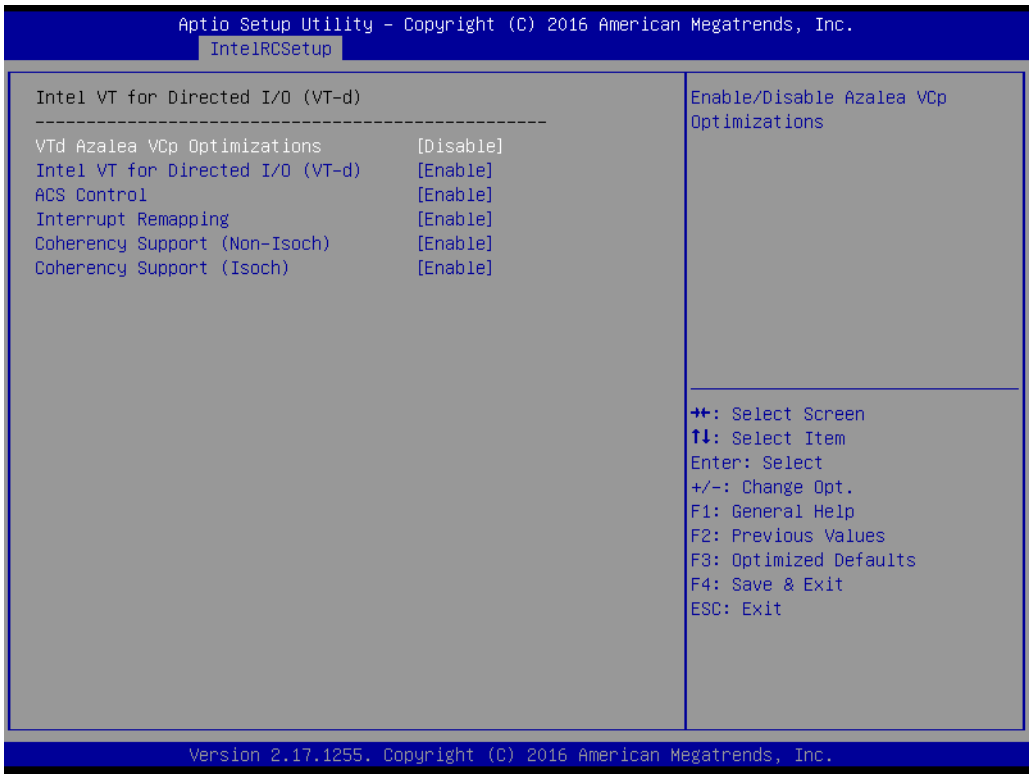


Figure 3.45 Intel VT for Directed I/O (VT-d)

- **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

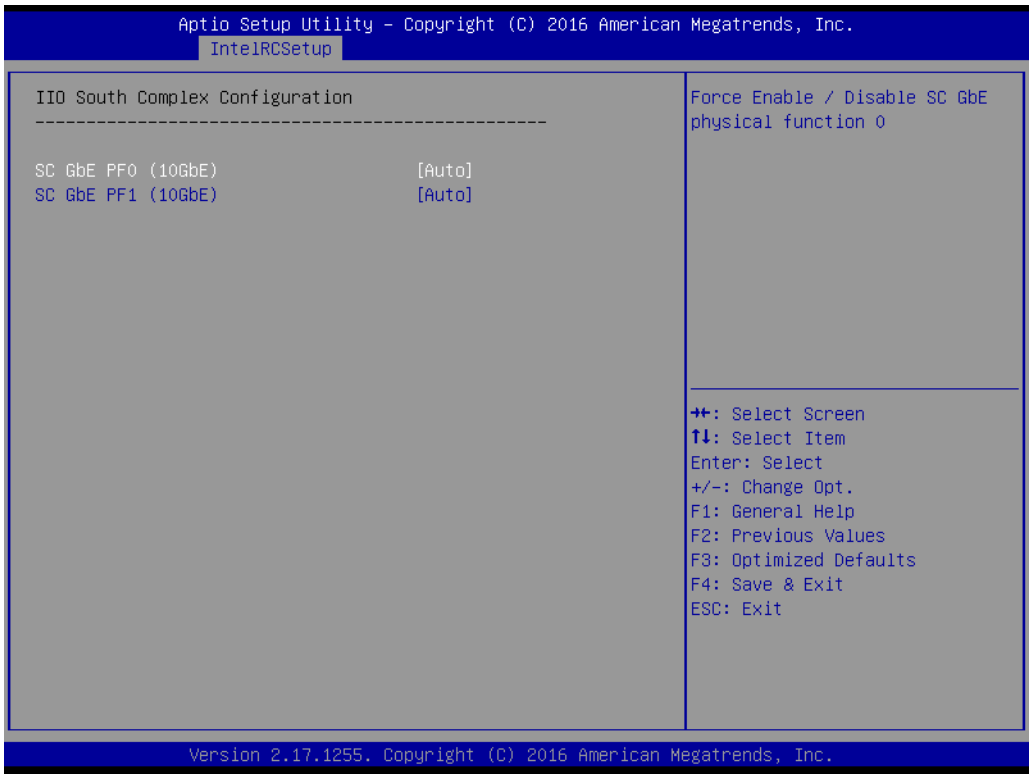


Figure 3.46 IIO South Complex Configuration

- **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.

3.2.3.6 PCH Configuration

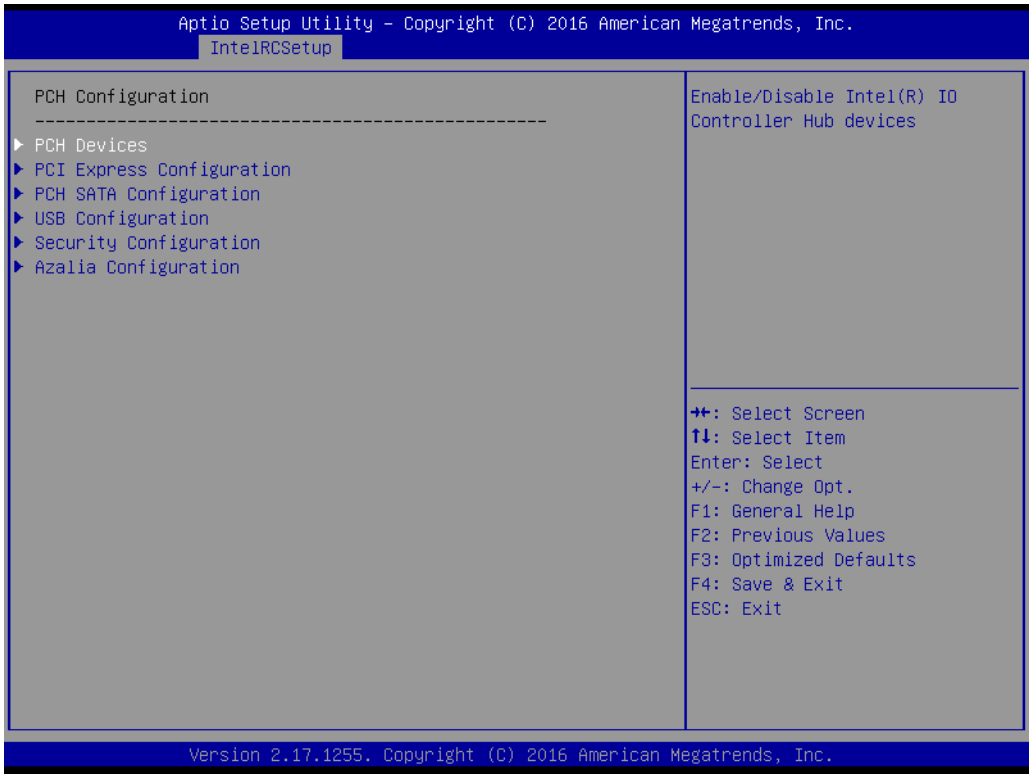


Figure 3.47 PCH Configuration

PCH Devices

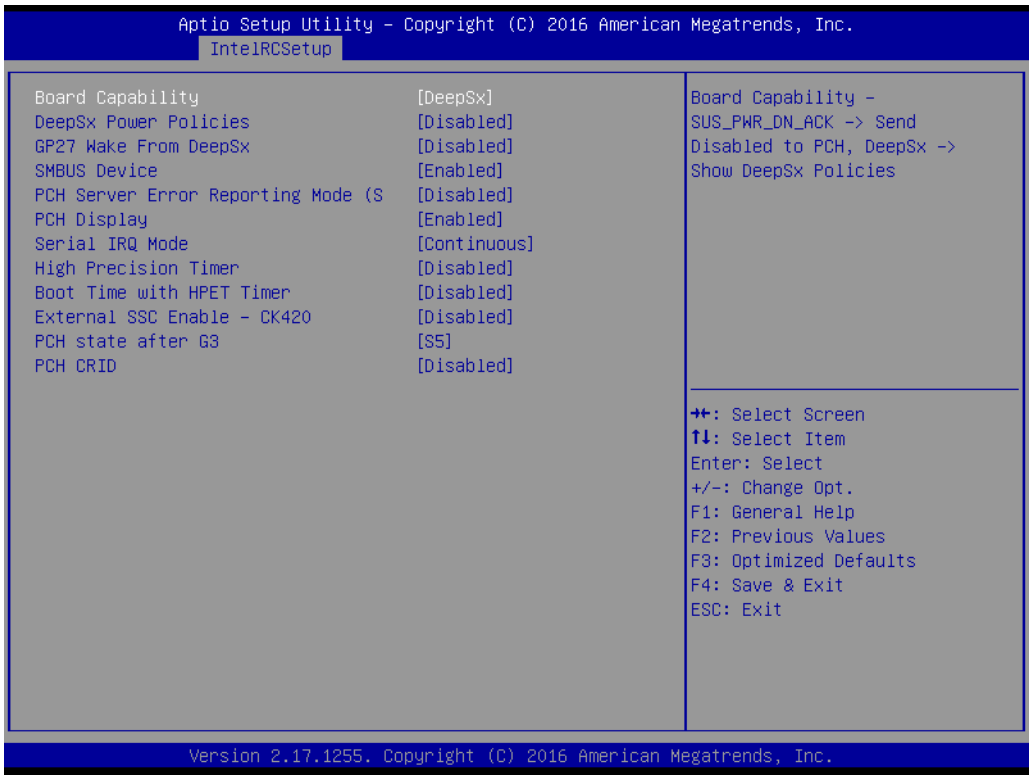


Figure 3.48 PCH Devices

- **Board Capability**
  Board Capability – SUS_PWR_DN_ACK -> Send Disable to PCH, DeepSx ->Show DeepSx Polocies.
- **DeepSx Power Policies**
  Configure the DeepSx Mode confuration.
- **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 erroes.
- **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

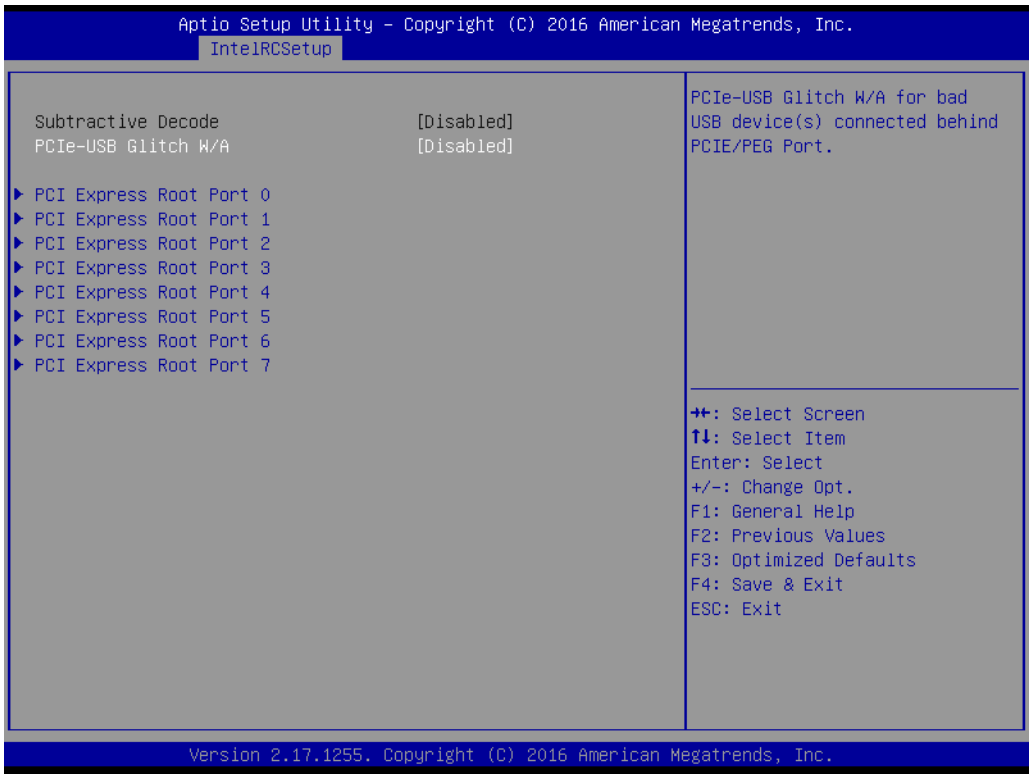


Figure 3.49 PCH Express Configuration

- **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

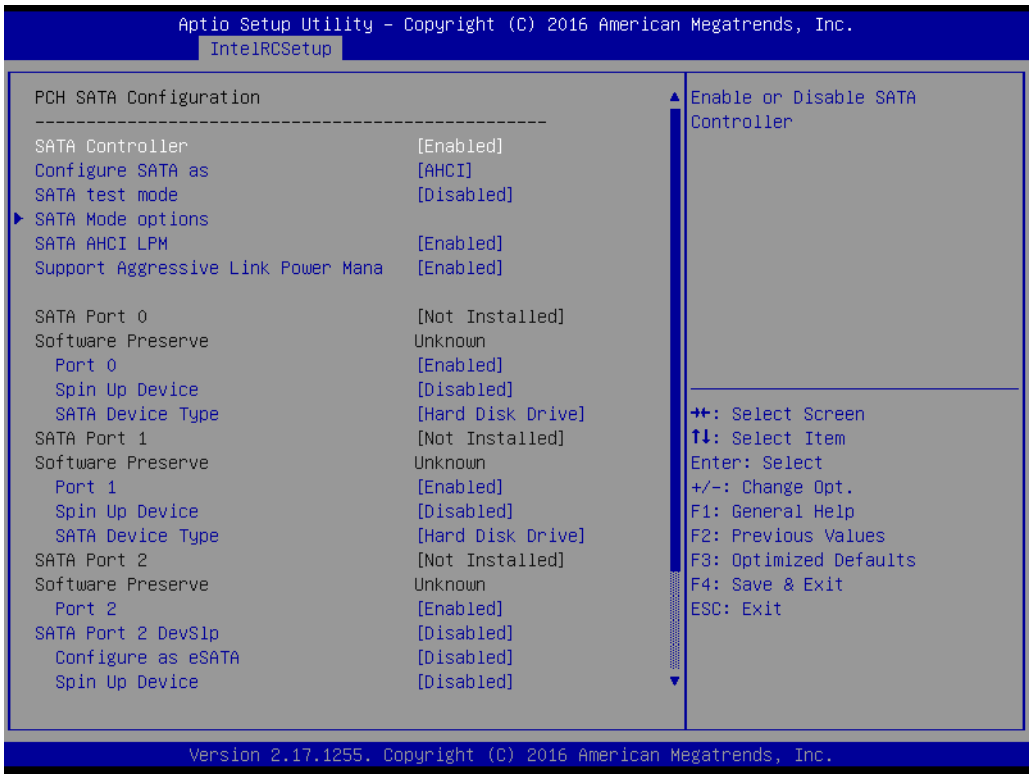


Figure 3.50 PCH SATA Configuration

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

USB Configuration

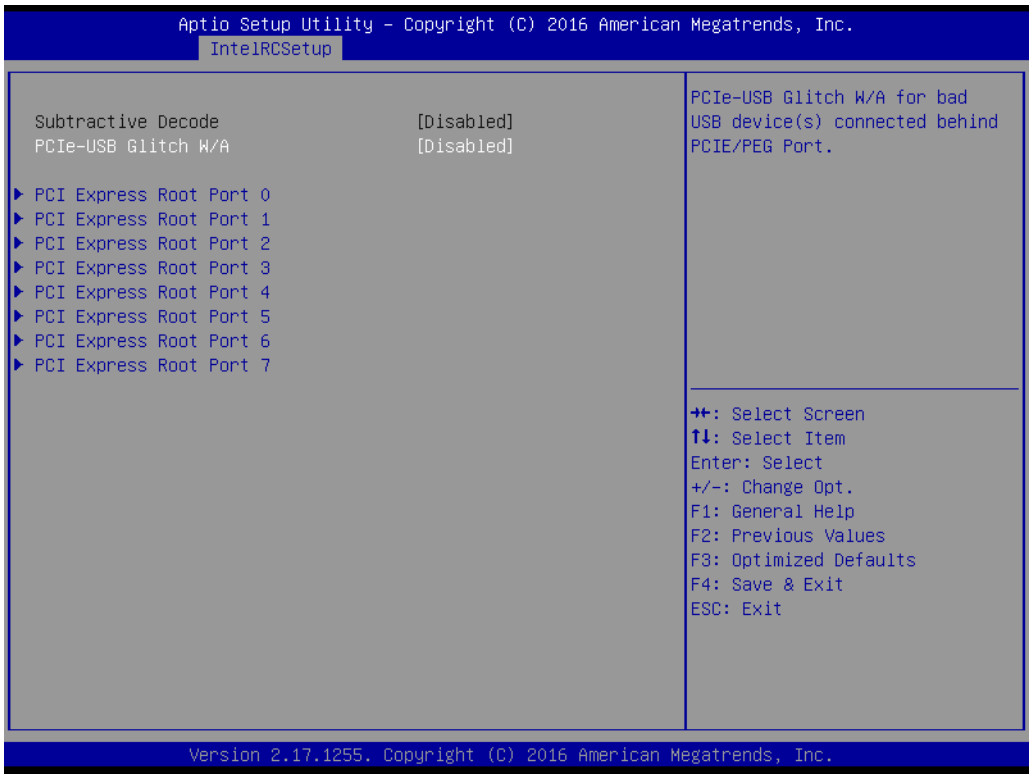


Figure 3.51 USB Configuration

- **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

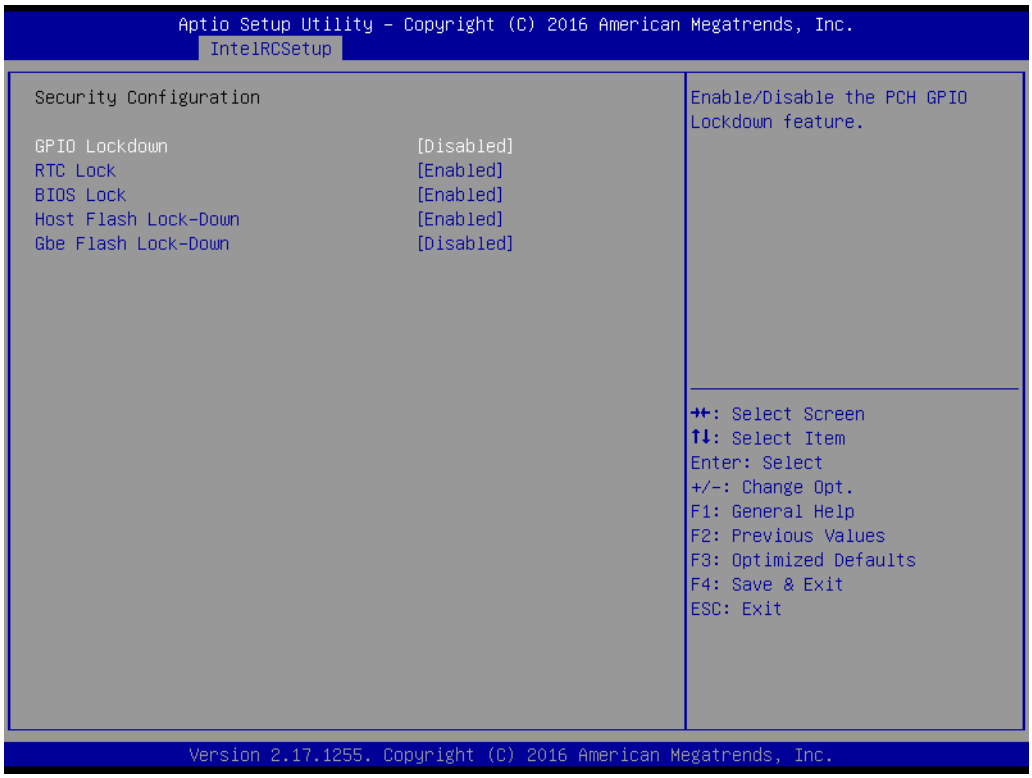


Figure 3.52 Secutiry Configuration

- **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.

Azalia Configuration

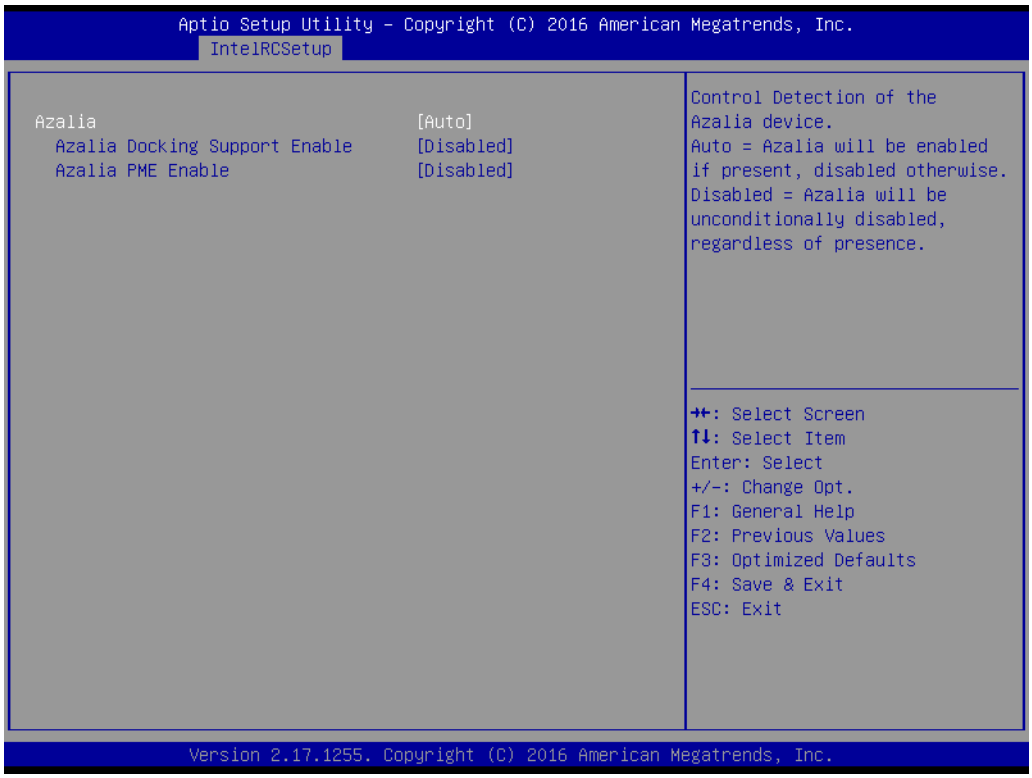


Figure 3.53 Azalia Configuration

Control Detection of the Azalia device.
Auto = Azalia will be enabled if present, disabled otherwise.
Disabled = Azalia will be unconditionally disabled, regardless of presence.

3.2.3.7 Miscellaneous Configuration

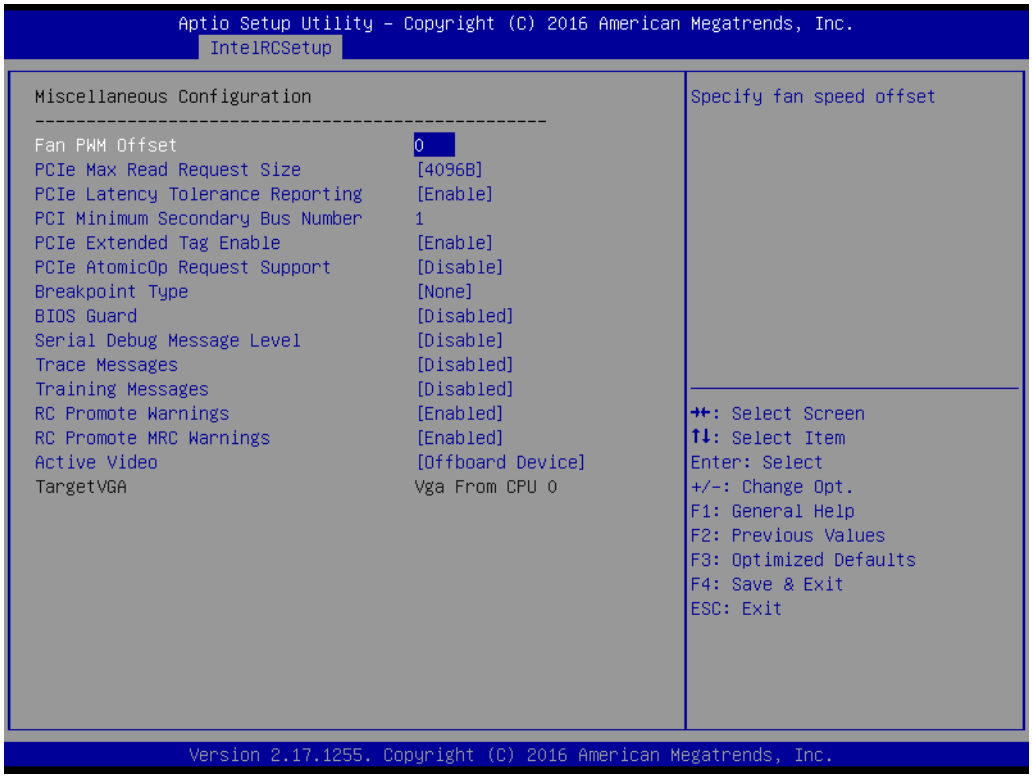


Figure 3.54 Miscellaneous Configuration

- **Fan PWN Offset**
  Specify fan speed offset.
- **PCIe Max Read Request Size**
  Set Max Read Request Size.

3.2.3.8 Server ME Configuration

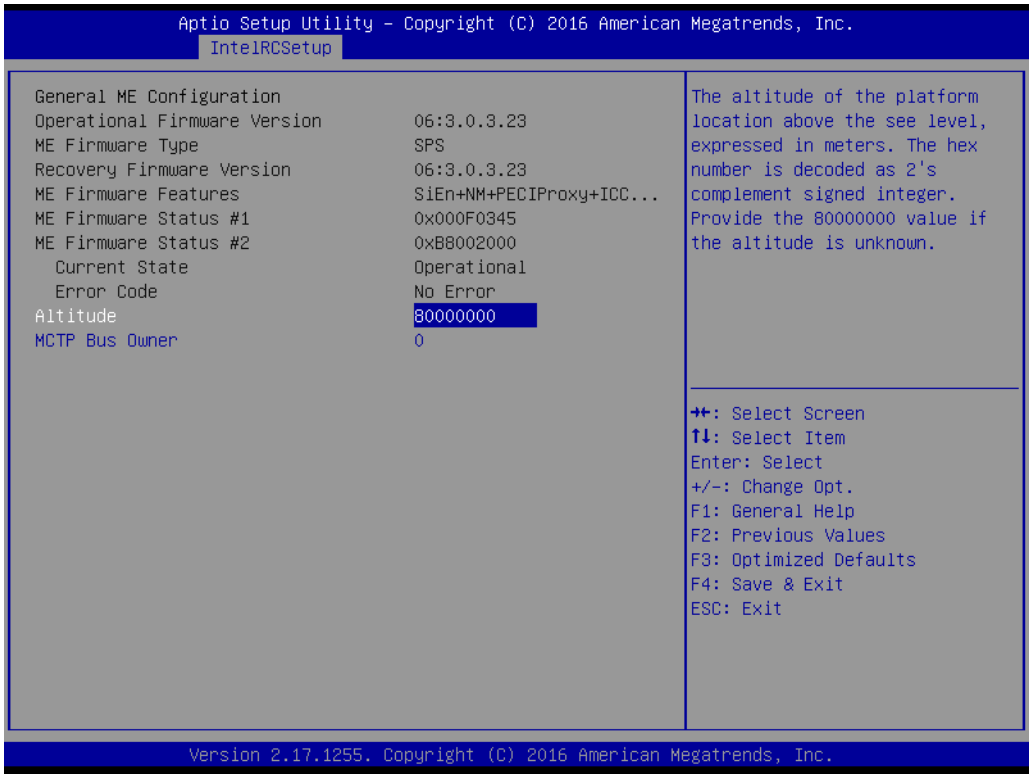


Figure 3.55 Server ME Configuration

- **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.

3.2.3.9 Runtime Error Logging

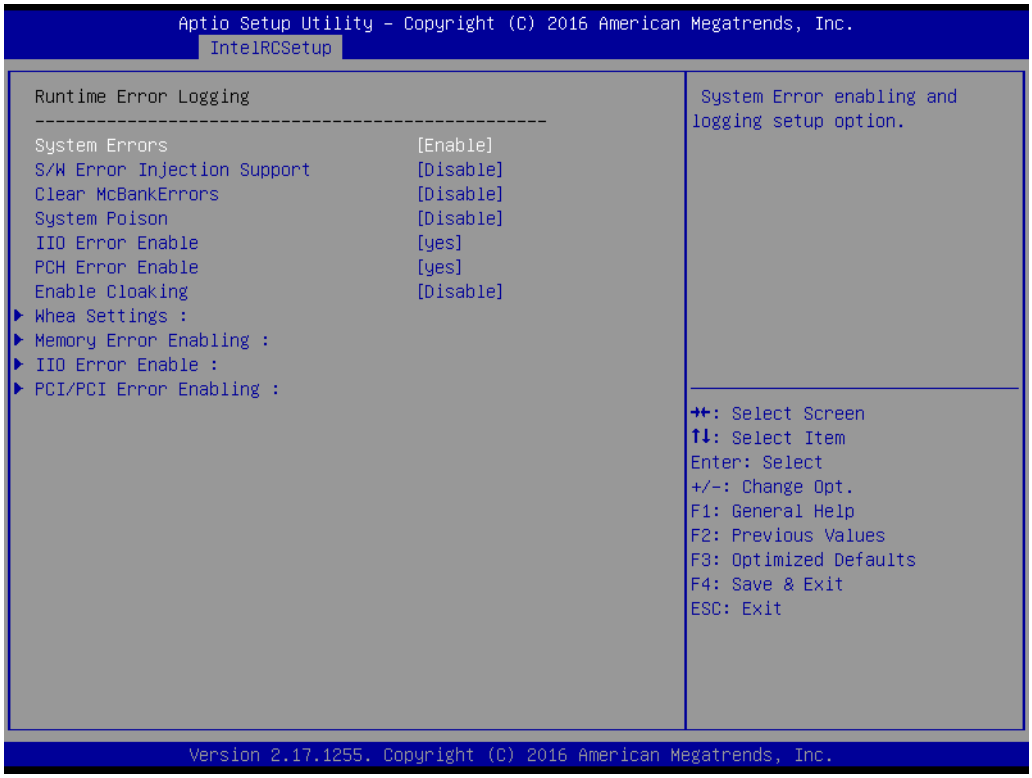


Figure 3.56 Runtime Error Logging

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.

3.2.3.10 Reserve Memory

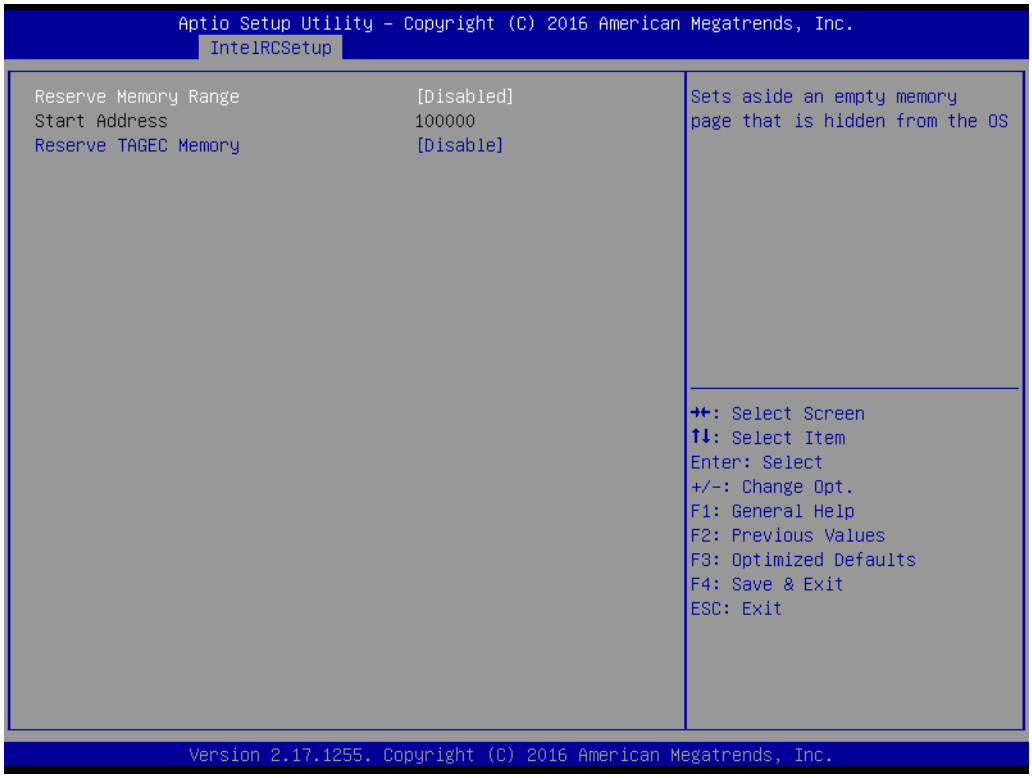


Figure 3.57 Reserve Memory

- **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-5991 setup screen to enter the BIOS Setup screen. You can select the items by highlighting it using by the <Arrow> keys.

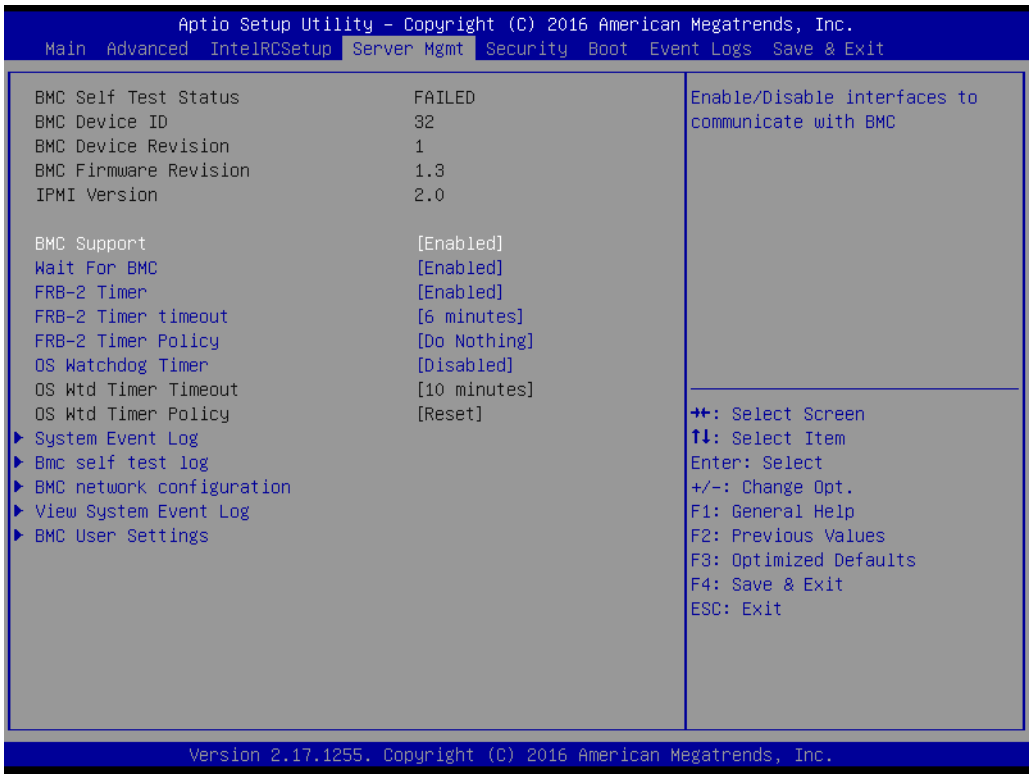


Figure 3.58 Server Mgmt

- **BMC Support**
  Enable or Disable interfaces to communicate with 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 value 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 disables.
- **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.

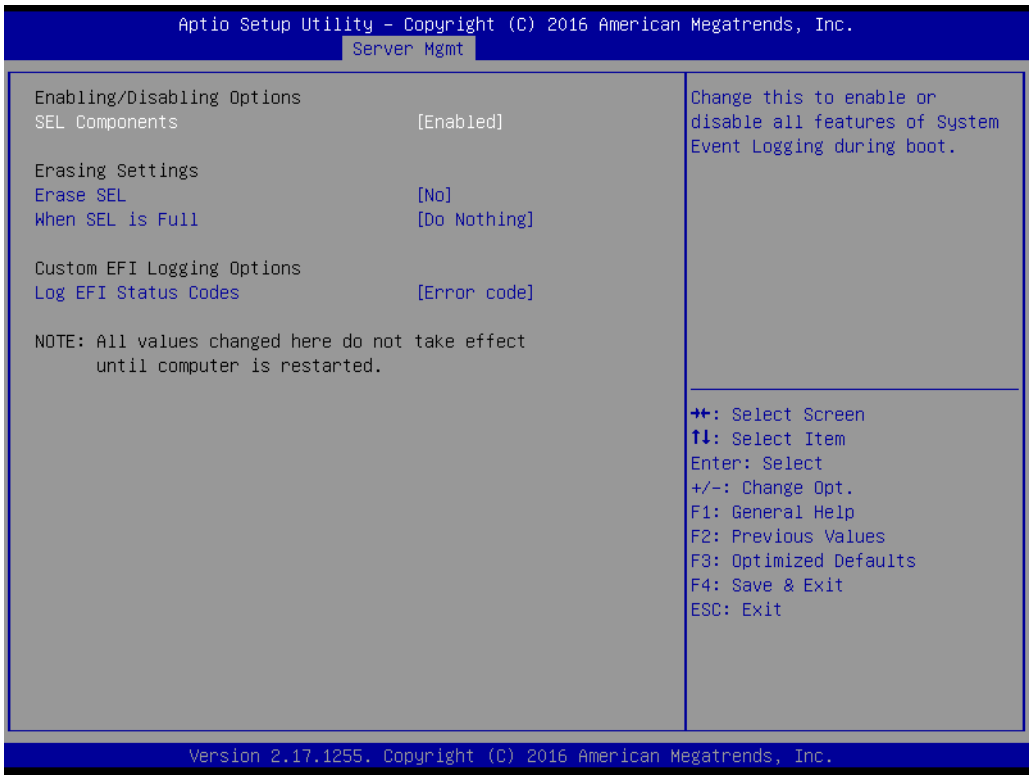


Figure 3.59 System Event Log

- **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.

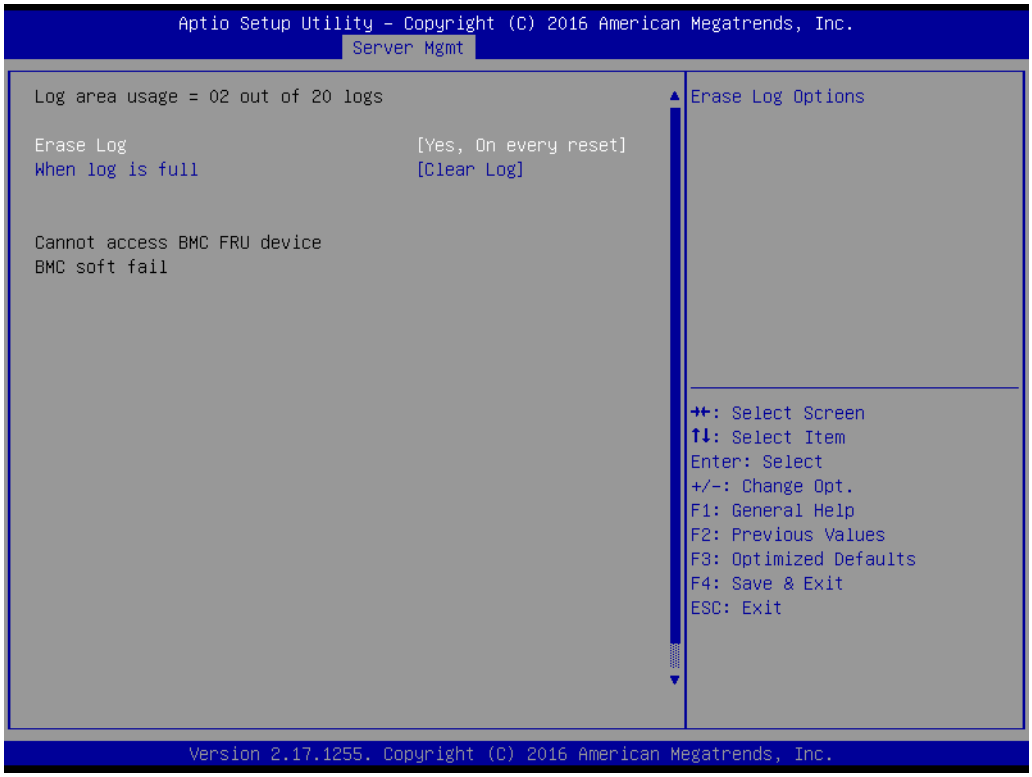


Figure 3.60 BMC self test log

- **Erase Log**
  Choose Yes or No, to erase log on every reset.
- **When log is full**
  Select the action to be taken when log is full.

3.2.4.3 BMC network configuration

Check configuration BMC network parameters.

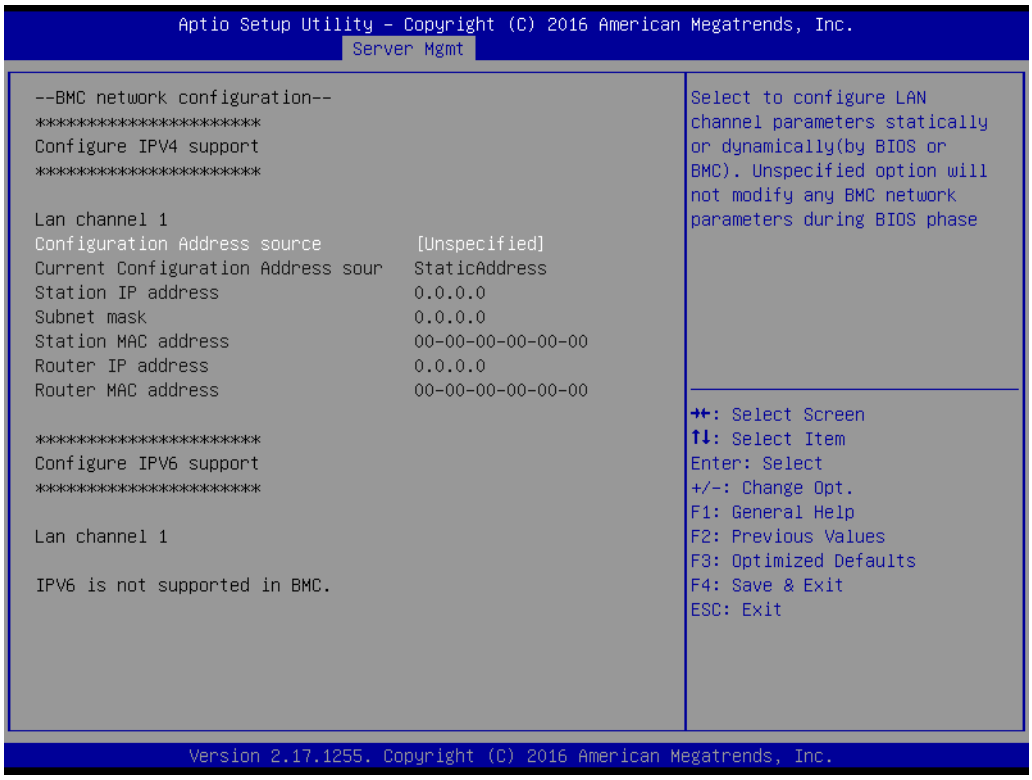


Figure 3.61 BMC network configuration

- **Configuration Address source**

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

3.2.4.4 View System configuration

Press <Enter> to view the system configuration status. You need to wait some time for system reaction.

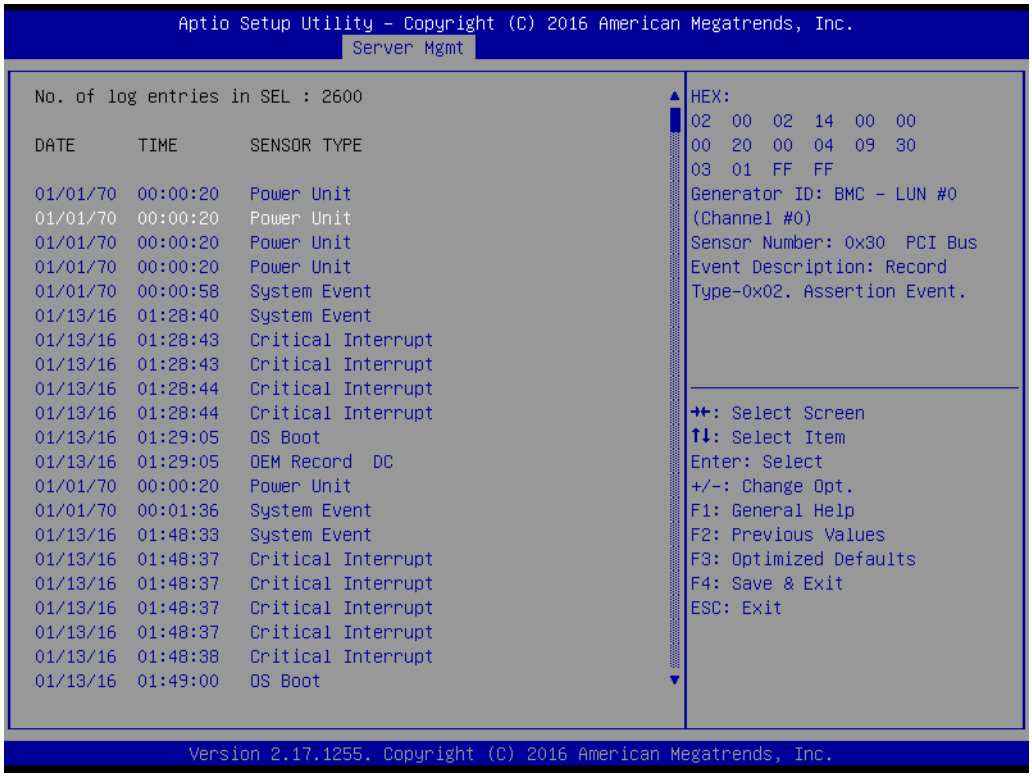


Figure 3.62 View System configuration

3.2.4.5 BMC User Settings

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

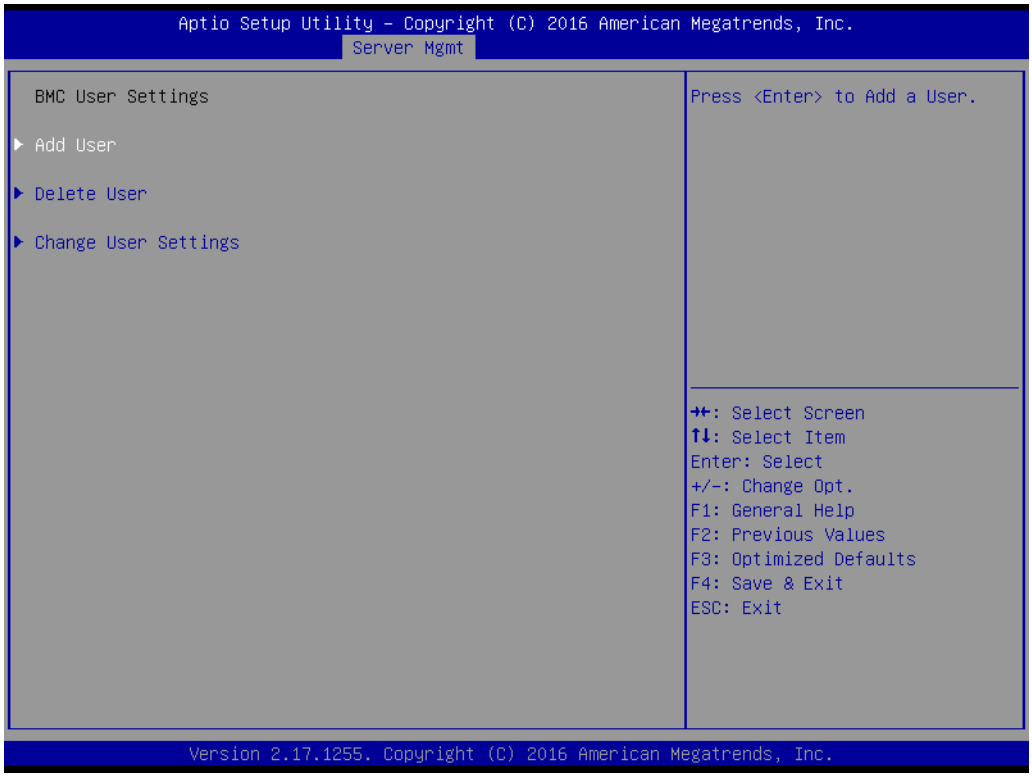


Figure 3.63 BMC User Settings

3.2.5 Security

Select the Security tab from the SOM-5991 setup screen to enter the BIOS Setup screen. You can select the items by highlighting it using by 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.

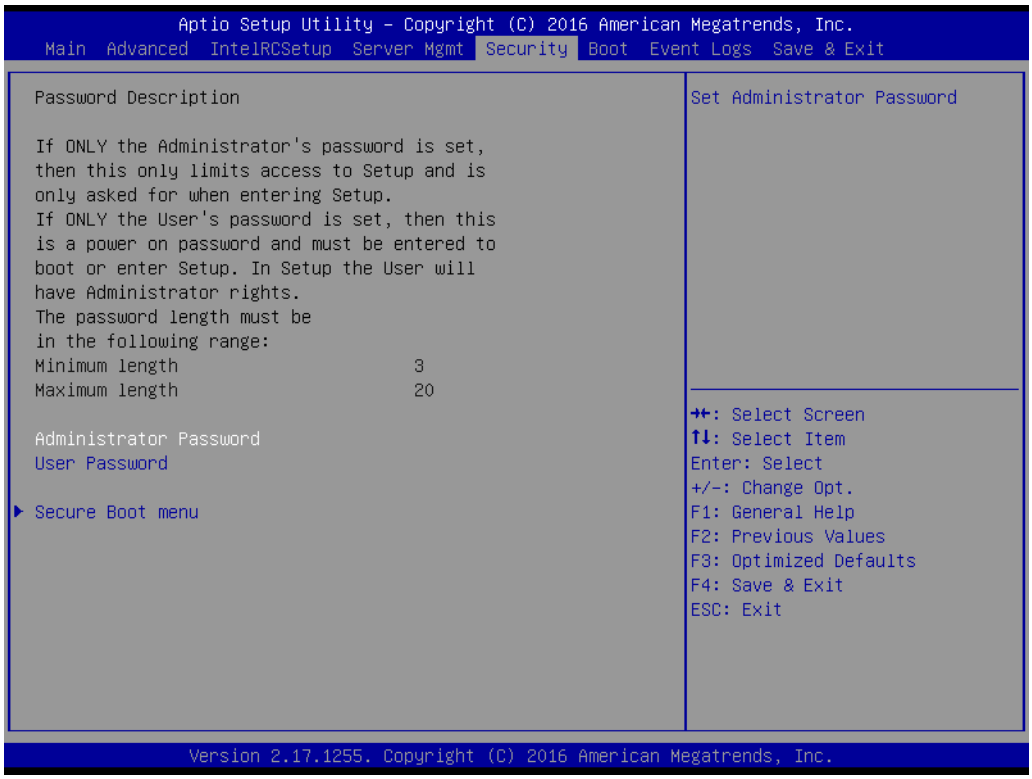


Figure 3.64 Security

- **Administration Password**
  Press <enter> and the user is able to set the Administration Password.
- **User Password**
  Press <enter> and the 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-5991 setup screen to enter the BIOS Setup screen. You can select the items by highlighting it using by the <Arrow> keys.

Figure 3.65 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-5991 setup screen to enter the BIOS Setup screen. You can select the items by highlighting it using by the <Arrow> keys.

Figure 3.66 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 3.67 Save & Exit

- **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 all system configuration parameters.
- **Discard Changes and Exit**
  Select this option to quit Setup without making any permanent changes to the system configuration.
- **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 all system configuration parameters.
- **Discard Changes and Reset**
  Select this option to quit Setup without making any permanent changes to the system configuration and reboot the computer.
- **Save Changes**
  When users have completed system configuration, select this option to save changes without exit BIOS setup menu.
- **Discard Changes**
  Select this option to discard any current changes and load previous system configuration.

- **Restore Defaults**

  The SOM-5991 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.

- **Save as User Defaults**

  When users have completed system configuration, select this option to save changes as user defaults without exit BIOS setup menu.

- **Restore User Defaults**

  Restore the User Defaults to all the setup options.

Chapter 4

S/W Introduction & Installation

- 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

The Intel Chipset Software Installation (CSI) utility installs the Windows INF files that outline to the operating system how the chipset components will be configured.

4.2.1 Windows Driver Setup

To install the drivers on a windows-based operation system, please connect to internet and browse the website http://www.emacinc.com/support and 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 Linux or other OS, please connect to internet and browse the browse the website http://www.emacinc.com/support 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 just as they happen. iManager also comes with a secure & encrypted EEPROM for storing important security key or other customer define information. All the embedded functions are configured through API and provide corresponding utilities to demonstrate. These APIs comply with PICMG EAPI (Embedded Application Programmable Interface) specification and unify in the same structures. It makes these embedded features easier to integrate, speed up developing schedule, and provide the customer's software continuity while upgrade hardware. More detail of how to use the APIs and utilities, please refer to Advantech iManager 2.0 Software API User Manual.

4.3.1 Control

GPIO

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

SMBus

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 control.

PC

PC is a bi-directional two wire bus that was developed by Philips 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 I2C protocols, allowing multiple simultaneous device control.

4.3.2 Display

Brightness Control

The Brightness Control API allows a developer to access embedded devices and easily control brightness.

Backlight

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

4.3.3 Monitor

Watchdog

A watchdog 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.

Hardware Monitor

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

Hardware Control

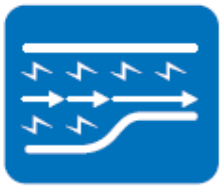
The Hardware control API allows developers to set the PWM (Pulse Width Modulation) value to adjust fan speed or other devices; it can also be used to adjust the LCD brightness.

4.3.4 Power Saving

CPU Speed

Makes use of Intel SpeedStep technology to save power consumption. The system will automatically adjust the CPU speed depending on the system loading.

System Throttling



Refers to a series of methods for reducing power consumption in computers by lowering the clock frequency. This API allows the user to adjust the clock from 87.5% to 12.5%.

Appendix A

Pin Assignment

This appendix gives you the information about the hardware pin assignment of the SOM-5991 CPU System on Module

Sections include:

- SOM-5991 Type 6 Pin Assignment

A.1 SOM-5991 Type 6 Pin Assignment

This section gives SOM-5991 pin assignment on COM Express connector which compliant with COMR.0 R2.1 Type 6 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.

*Remark: Please be aware that the word in blue is the special pin assignment in SOM-5991 for 10GBase-KR.

SOM-5991 Row A,B			
A1	GND	B1	GND
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	B11	GND
A12	GBE0_MDI0-	B12	PWRBTN#
A13	GBE0_MDI0+	B13	SMB_CK
A14	SOM-5991 NC	B14	SMB_DAT
A15	SUS_S3#	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	B21	GND
A22	SATA2_TX+	B22	SATA3_TX+
A23	SATA2_TX	B23	SATA3_TX-
A24	SUS_S5#	B24	PWR_OK
A25	SATA2_RX+	B25	SATA3_RX+
A26	SATA2_RX	B26	SATA3_RX-
A27	BATLOW#	B27	WDT
A28	(S)ATA_ACT#	B28	SOM-5991 NC
A29	SOM-5991 NC	B29	SOM-5991 NC
A30	SOM-5991 NC	B30	SOM-5991 NC
A31	GND	B31	GND
A32	SOM-5991 NC	B32	SPKR
A33	SOM-5991 NC	B33	I2C_CK
A34	BIOS_DIS0#	B34	I2C_DAT
A35	THRMTRIP#	B35	THRM#
A36	SOM-5991 NC	B36	SOM-5991 NC
A37	SOM-5991 NC	B37	SOM-5991 NC
A38	USB_6_7_OC#	B38	USB_4_5_OC#

A39	SOM-5991 NC	B39	USB5-
A40	SOM-5991 NC	B40	USB5+
A41	GND	B41	GND
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	EXCD1_PERST#
A48	EXCD0_PERST#	B48	EXCD1_CPPE#
A49	EXCD0_CPPE#	B49	SYS_RESET#
A50	LPC_SERIRQ	B50	CB_RESET#
A51	GND	B51	GND
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	B60	GND
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	B70	GND
A71	SOM-5991 NC	B71	SOM-5991 NC
A72	SOM-5991 NC	B72	SOM-5991 NC
A73	SOM-5991 NC	B73	SOM-5991 NC
A74	SOM-5991 NC -	B74	SOM-5991 NC -
A75	SOM-5991 NC	B75	SOM-5991 NC
A76	SOM-5991 NC	B76	SOM-5991 NC
A77	SOM-5991 NC	B77	SOM-5991 NC
A78	SOM-5991 NC	B78	SOM-5991 NC
A79	SOM-5991 NC	B79	SOM-5991 NC
A80	GND	B80	GND
A81	SOM-5991 NC	B81	SOM-5991 NC
A82	SOM-5991 NC	B82	SOM-5991 NC
A83	SOM-5991 NC	B83	SOM-5991 NC
A84	SOM-5991 NC	B84	VCC_5V_SBY
A85	GPI3	B85	VCC_5V_SBY
A86	KB_RST#	B86	VCC_5V_SBY

A87	RSVD	B87	VCC_5V_SBY
A88	PCIE_CLK_REF+	B88	BIOS_DIS1#
A89	PCIE_CLK_REF-	B89	SOM-5991 NC
A90	GND	B90	GND
A91	SPI_POWER	B91	SOM-5991 NC
A92	SPI_MISO	B92	SOM-5991 NC
A93	GPO0	B93	SOM-5991 NC
A94	SPI_CLK	B94	SOM-5991 NC
A95	SPI_MOSI	B95	SOM-5991 NC
A96	TPM_PP	B96	SOM-5991 NC
A97	TYPE10#	B97	SPI_CS#
A98	SER0_TX	B98	RSVD
A99	SER0_RX	B99	RSVD
A100	GND	B100	GND
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	B110	GND
SOM-5991 Row C,D			
C1	GND	D1	GND
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	D11	GND
C12	USB_SSRX3-	D12	USB_SSTX3-
C13	USB_SSRX3+	D13	USB_SSTX3+
C14	GND	D14	GND
C15	LAN_MDC	D15	SOM-5991 NC
C16	LAM_MDIO	D16	SOM-5991 NC
C17	RSVD	D17	RSVD
C18	RSVD	D18	RSVD
C19	PCIE_RX6+	D19	PCIE_TX6+
C20	PCIE_RX6-	D20	PCIE_TX6-
C21	GND	D21	GND
C22	PCIE_RX7+	D22	PCIE_TX7+
C23	PCIE_RX7-	D23	PCIE_TX7-

C24	SOM-5991 NC	D24	RSVD
C25	SOM-5991 NC	D25	RSVD
C26	LAN_KR_RX0_P	D26	LAN0_KR_TX0_P
C27	LAN_KR_RX0_N	D27	LAN0_KR_TX0_N
C28	RSVD	D28	RSVD
C29	LAN_KR_RX1_P	D29	LAN0_KR_TX1_P
C30	LAN_KR_RX1_N	D30	LAN0_KR_TX1_N
C31	GND	D31	GND
C32	SOM-5991 NC	D32	SOM-5991 NC
C33	SOM-5991 NC	D33	SOM-5991 NC
C34	SOM-5991 NC	D34	SOM-5991 NC
C35	RSVD	D35	RSVD
C36	SOM-5991 NC	D36	SOM-5991 NC
C37	SOM-5991 NC	D37	SOM-5991 NC
C38	LAN0_PORT0_LED1	D38	LAN0_PORT0_LED0
C39	LAN0_PORT0_SDP0	D39	LAN0_PORT0_I2C_CLK
C40	SOM-5991 NC	D40	LAN0_PORT0_I2C_DATA
C41	GND	D41	GND
C42	LAN0_PORT1_SDP0	D42	LAN0_PORT1_I2C_CLK
C43	SOM-5991 NC	D43	LAN0_PORT1_I2C_DATA
C44	LAN1_PORT1_LED1	D44	LAN0_PORT1_LED0
C45	RSVD	D45	RSVD
C46	SOM-5991 NC	D46	SOM-5991 NC
C47	SOM-5991 NC	D47	SOM-5991 NC
C48	RSVD	D48	RSVD
C49	SOM-5991 NC	D49	SOM-5991 NC
C50	SOM-5991 NC	D50	SOM-5991 NC
C51	GND	D51	GND
C52	PEG_RX0+	D52	PEG_TX0+
C53	PEG_RX0-	D53	PEG_TX0-
C54	TYPE0# SOM-5991 NC	D54	PEG_LANE_RV#
C55	PEG_RX1+	D55	PEG_TX1+
C56	PEG_RX1-	D56	PEG_TX1-
C57	TYPE1# SOM-5991 NC	D57	TYPE2#
C58	PEG_RX2+	D58	PEG_TX2+
C59	PEG_RX2-	D59	PEG_TX2-
C60	GND	D60	GND
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	RSVD	D67	GND
C68	PEG_RX5+	D68	PEG_TX5+
C69	PEG_RX5-	D69	PEG_TX5-
C70	GND	D70	GND
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	D80	GND
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	D90	GND
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	PEG_ENABLE#
C98	PEG_RX14+	D98	PEG_TX14+
C99	PEG_RX14-	D99	PEG_TX14-
C100	GND	D100	GND
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	D110	GND

Appendix B

Watchdog Timer

This appendix gives you the information about the watchdog timer programming on the SOM-5991 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
WDT Pin Activate	Support

** WDT new driver support automatically select available IRQ number from BIOS, and then set to EC. Only Win8.1 and Win10 support it.

In other OS, it will still use IRQ number from BIOS setting as usual.

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

Appendix C

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

Appendix D

System Assignments

This appendix gives you the information about the system resource allocation on the SOM-5991 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

Addr. Range (Hex)	Device
0xF4000000-0xF80FFFFF	Intel(R) 8 Series/C220 Series PCI Express Root Port #8 - 8C1E
0xF4000000-0xF80FFFFF	PCI standard PCI Express to PCI/PCI-X Bridge
0xF4000000-0xF80FFFFF	ASPEED Graphics Family(WDDM)
0xA0000-0xBFFFF	Intel(R) 8 Series/C220 Series PCI Express Root Port #8 - 8C1E
0xA0000-0xBFFFF	PCI standard PCI Express to PCI/PCI-X Bridge
0xA0000-0xBFFFF	PCI Express Root Complex
0xF8612000-0xF86127FF	Standard SATA AHCI Controller
0xF8615000-0xF861500F	PCI Simple Communications Controller
0xF8200000-0xF82FFFFF	Intel(R) I210 Gigabit Network Connection #2
0xF8300000-0xF8303FFF	Intel(R) I210 Gigabit Network Connection #2
0xFED00000-0xFED003FF	High precision event timer
0xF8500000-0xF85FFFFF	Intel(R) Xeon(R) E7 v4/Xeon(R) E5 v4/Xeon(R) E3 v4/Xeon(R) D PCI Express Root Port 2 - 6F04
0xF8000000-0xF801FFFF	ASPEED Graphics Family(WDDM)
0xF8613000-0xF86133FF	Intel(R) 8 Series/C220 Series USB EHCI #1 - 8C26
0xF8400000-0xF84FFFFF	Intel(R) Xeon(R) E7 v4/Xeon(R) E5 v4/Xeon(R) E3 v4/Xeon(R) D PCI Express Root Port 2 - 6F06
0xFBA00000-0xFBEFFFFF	Intel(R) Xeon(R) E7 v4/Xeon(R) E5 v4/Xeon(R) E3 v4/Xeon(R) D PCI Express Root Port 2 - 6F06
0xF8616000-0xF861600F	PCI Simple Communications Controller
0xF8617000-0xF8617FFF	Intel(R) Xeon(R) E7 v4/Xeon(R) E5 v4/Xeon(R) E3 v4/Xeon(R) D I/O APIC - 6F2C
0xFEC00000-0xFECFFFFF	Advanced programmable interrupt controller
0x90000000-0xFBFFBFFF	PCI Express Root Complex
0xF8100000-0xF83FFFFF	Intel(R) Xeon(R) E7 v4/Xeon(R) E5 v4/Xeon(R) E3 v4/Xeon(R) D PCI Express Root Port 1 - 6F03
0xFED40000-0xFED44FFF	Trusted Platform Module 2.0
0xFED1C000-0xFED3FFFF	Motherboard resources
0xFED45000-0xFED8BFFF	Motherboard resources
0xFF000000-0xFFFFFFFF	Motherboard resources

Table D.4: 1st MB Memory Map	
0xFEE00000-0xFEEFFFFF	Motherboard resources
0xFED12000-0xFED1200F	Motherboard resources
0xFED12010-0xFED1201F	Motherboard resources
0xFED1B000-0xFED1BFFF	Motherboard resources
0xF8600000-0xF860FFFF	Intel(R) USB 3.0 eXtensible Host Controller - 0100 (Microsoft)
0xF4000000-0xF80FFFFF	Intel(R) 8 Series/C220 Series PCI Express Root Port #8 - 8C1E