SR200-SG

MIL-STD Rugged Computer

User's Manual

User's Manual

Revision Date: : AUG.30, 2016

Safety Information

Electrical safety

- To prevent electrical shock hazard, disconnect the power cable from the electrical outlet before relocating the system.
- When adding or removing devices to or from the system, ensure that the power cables for the devices are unplugged before the signal cables are connected. If possible, disconnect all power cables from the existing system before you add a device.
- Before connecting or removing signal cables from the motherboard, ensure that all power cables are unplugged.
- Seek professional assistance before using an adapter or extension cord. These devices could interrupt the grounding circuit.
- Make sure that your power supply is set to the correct voltage in your area.
- If you are not sure about the voltage of the electrical outlet you are using, contact your local power company.
- If the power supply is broken, do not try to fix it by yourself. Contact a qualified service technician or your local distributor.

Operation safety

- Before installing the motherboard and adding devices on it, carefully read all the manuals that came with the package.
- Before using the product, make sure all cables are correctly connected and the power cables are not damaged. If you detect any damage, contact your dealer immediately.
- To avoid short circuits, keep paper clips, screws, and staples away from connectors, slots, sockets and circuitry.
- Avoid dust, humidity, and temperature extremes. Do not place the product in any area where it may become wet.
- Place the product on a stable surface.
- If you encounter any technical problems with the product, contact your local distributor

Statement

- All rights reserved. No part of this publication may be reproduced in any form or by any means, without prior written permission from the publisher.
- All trademarks are the properties of the respective owners.
- All product specifications are subject to change without prior notice

Specifications

System	
High Performance Processor	Intel® 4th Gen Core™ i7-4700EQ (Frequency 2.4GHz, Turbo Boost up to 3.4GHz), Quad-Core, 8 Thread Support, 6MB SmartCache. Build-in HD Graphics 4600 for excellent 3D, Turbo Boost Technology 2.0, VPro and Hyper-Threading support.
Memory type	1 x DDR3 XR-DIMM™ up to 8GB
Chipset	Intel® QM87 Chipset providing integrated USB 3.0 and supporting 4th generation Intel® Core™ processor families
Expansion Slot	1 x Full-size mPCIe with SIM card holder 1 x Full-size mPCIe/mSATA
Display	
GPU	NVIDIA GTX950M
Display Port	Resolution up to 3840 x 2160
DVI-I	Resolution up to 1920 x 1200
Storage	
uSSD	Onboard uSSD SATAIII 64GB
mSATA	1 x mSATA Solid State Disk (SSD) - up to 512GB Capacity.
Ethernet	
Ethernet	2 x Intel Gigabit Ethernet LAN Interfaces (10/100/1000Mbps)
Rear I/O	
Display Port	2 x DisplayPort connectors
DVI-	1 x DVI-I connector (With cover)
Ethernet	2 x RJ45 Gigabit Ethernet LAN
Audio	2 x 3.5mm Audio Jacks (1 x MIC, 1 x Line-Out)
Serial Port	1 x DB9 connector (RS-232/422/485)
USB Port	2 x USB3.0 standard-A connectors
Front I/O	
Button	1 x Power Button
DC-IN	4P Rugged Terminal connector

Indicator LED	Power, HDD, LAN (Link/Active/Speed)

Front I/O

USB Port	2 x USB3.0 standard-A connectors
DisplayPort	4 x DisplayPort connectors from GPU

Applications, Operating System

Applications	Commercial and Military Platforms Requiring Compliance to MIL-STD-810G Embedded Computing, Process Control, Intelligent Automation and manufacturing applications where Harsh Temperature, Shock, Vibration, Altitude, Dust and EMI Conditions. Used in all aspects of the military
Operating System	Windows 7 , Windows 8 , Windows 8.1 , Windows 10 Ubuntu13.04, Ubuntu13.10, Ubuntu14.04, Fedora 20

Physical

Dimension	308 x 149 x 76mm
Weight	4.3 Kg (9.47 lbs)
Chassis	Aluminum Alloy, Corrosion Resistant.
Cooling	Aluminum Alloy, Corrosion Resistant
Finish	Anodic aluminum oxide (Color Iron gray)
Ingress Protection	Dust Proof (Similar to IP50)

Environmental

MIL-STD-810G Test	Method 507.5, Procedure II (Temperature & Humidity) Method 516.6 Shock-Procedure V Non-Operating (Mechanical Shock) Method 516.6 Shock-Procedure I Operating (Mechanical Shock) Method 514.6 Vibration Category 24/Non-Operating (Category 20 & 24, Vibration) Method 514.6 Vibration Category 20/Operating (Category 20 & 24, Vibration) Method 501.5, Procedure I (Storage/High Temperature) Method 501.5, Procedure II (Operation/High Temperature) Method 502.5, Procedure I (Storage/Low Temperature) Method 502.5, Procedure II (Operation/Low Temperature) Method 503.5, Procedure I (Temperature shock)
Reliability	No Moving Parts; Passive Cooling. Designed & Manufactured using ISO 9001/2000 Certified Quality Program
EMC	CE and FCC compliance
Green Product	RoHS, WEEE compliance

Revision History

Revision	Date (yyyy/mm/dd)	Changes
V1.0	2016/08/30	Initial release

Packing list

- ☐ SR200-SG MIL-STD Rugged Computer
- ☐ XR-DIMM up to 8 GB RAM ***optional***

Accessories Kit

- ☐ Terminal block 4 PIN x 1pcs
- ☐ CD (Driver + User's Manual)
- ☐ Active Thermal Kit ***optional***

If any of the above items is damaged or missing, please contact your local distributor.

Ordering information

Model Number	Description
SR200-SG	Intel® QM87 MIL-STD Fanless Rugged System with Intel® Core i7-4700EQ Processor, NVIDIA GT950M GPU, 9V to 36V DC-in, Wide Temp -20 to 60°C

Table of contents

Safety Information 1
Specifications 2
Revision History 4
Packing list 4
Accessories Kit 4
Ordering information 4
Table of contents 5
Chapter 1: Product Introduction 7
1.1 Key Features 7
1.2 Front Panel Components 9
1.3 Rear Panel Components 9
1.4 Mechanical Dimensions 10
1.5 Active Thermal Kit Installation 11
1.5.1 Installation Guide 11
Chapter 2: Jumpers and Connectors 13
2.1 Front Panel Connector Pin Definitions 13
2.2 Rear Panel Connector Pin Definitions 15
2.3 Internal Connector and Jumper Setting 17
Chapter 3: AMI BIOS UTILITY 19
3.1 Starting 19
3.2 Navigation Keys 19
3.3 Main Menu 20
3.4 Advanced Menu 21
3.4.1 PCI Subsystem Settings 22
3.4.2 ACPI Settings 23
3.4.3 CPU configuration 24
3.4.4 SATA Configuration 29
3.4.5 Intel Rapid Start Technology 33
3.4.6 PCH-FW Configuration 34
3.4.7 Intel Anti-Theft Technology Configuration 35
3.4.8 AMT Configuration 36
3.4.9 USB Configuration 38
3.4.10 IT8786 Super IO Configuration 39

3.4.11 IT8786 HW Monitor 41
3.4.12 Serial Port Console Redirection 42
3.4.13 Network Stack 43
3.4.14 Intel I210 Gigabit Network Connection 44
3.5 Chipset 45
3.5.1 PCH IO configuration 45
3.5.2 System AGENT SA 53
3.6 Boot 56
3.7 Security 57
3.8 Save and Exit 58

Chapter 1: Product Introduction

1.1 Key Features

System	
CPU	Intel® Core™ i7 Haswell , BGA type Core i7-4700EQ (4C x 2.4/1.7 GHz), 6M Cache (47W)
Chipset	Intel® QM87 PCH
Ethernet Chipset	Intel® I210IT & i217-LM GbE
Memory	1 x DDR3 1600 XR-DIMM 8 GB with ECC
Expansion Slot	2 x mPCIe (1 x colay with mSATA)
Storage Device	Onboard uSSD SATAIII 64 GB
Front I/O	
Power Button	Power Button with dual color LED backlight
Power LED	1 x Green LED
HDD LED	1 x Red LED
LAN LED	2 x Red LED, 2 Green LED
USB	2 x USB 3.0
DisplayPort	4 (From MXM Graphic Module)
Power	1 x Terminal Block
Rear I/O	
Ethernet	2 x RJ45
COM	1 x RS232/422/485 with 5V/12V selectable
USB	2 x USB 3.0
DVI-I	1 (Default CLOSED)
DisplayPort	2 (From motherboard)
Audio	1 x MIC, 1 x Line out
Display	
Display Interface	DP x 4 - Resolution Up to 3840 x 2160
GPU	NVIDIA GT950M (MXM Module)
Notice: Because of the GPU limitation, DP1 and DP2 **CANNOT** display in the same time. The system supports total 5 displays output at the same time (3 from MXM card, 2 from motherboard).	
Mechanical & Environment	
Power Requirements	9V to 36V DC-in, AT/ATX mode supports with power delay on/off Power consumption : Under 120 Watt while system fully loading
Dimension (W x H x D)	308 x 149 x 76 mm (12.13" x 5.87" x 2.99")
Operating Temp.	-20 to 60°C (ambient with air flow)
Storage Temp.	-40 to 85°C
Relative Humidity	5% to 95%, non-condensing
Serial Interface & Signals	
Serial Standards	1x RS-232/422/485 port, Jumper-selectable (DB9 male)
RS-232	TxD, RxD, DTR, DSR, RTS, CTS, DCD, GND
RS-422	TxD+, TxD-, RxD+, RxD-, GND
RS-485-4w	TxD+, TxD-, RxD+, RxD-, GND
RS-485-2w	Data+, Data-, GND

Standards and Certifications	
MIL-STD-810G Test Method 507.5, Procedure II (Temperature & Humidity) Method 514.6, Procedure I (Category 20 & 24, Vibration) Method 516.6, Procedure I (Mechanical Shock) Method 501.5, Procedure I (Storage/High Temperature) Method 501.5, Procedure II (Operation/High Temperature) Method 502.5, Procedure I (Storage/Low Temperature) Method 502.5, Procedure II (Operation/Low Temperature) Method 503.5, Procedure I (Temperature shock)	
EMC	CE and FCC compliance
Green Product	RoHS, WEEE compliance

Specifications are subject to change without notice

1.2 Front Panel Components

1	DP1 DP2
2	Grounding Screw
3	2 x USB 3.0 (Type A)
4	System/ LAN LED
5	Power Button
6	Power Input (9~36V DC in)
7	DP3 DP4

1.3 Rear Panel Components

1	Audio jack (1 x MIC, 1 x Line out)
2	LAN port, 2 x RJ45
3	2 x DisplayPort
4	1 x DVI-I
5	1 x RS232/422/485 with 5V/12V selectable
6	2 x USB 3.0

1.4 Mechanical Dimensions

1.5 Active Thermal Kit Installation

The active thermal kit for SR200 is an optional accessory for more safe and steady application.

1.5.1 Installation Guide

Step 1. Align thermal kit by grooves on top side of system.

Step 2. Pick screws from accessory box and use screwdriver to fix thermal kit.

Step 3. Plug USB cable of thermal kit into USB port as a power supply.

Chapter 2: Jumpers and Connectors

This chapter describes the jumpers and connectors on the systems' motherboard.

2.1 Front Panel Connector Pin Definitions

Status Indicators

LED1: LAN1 LED STATUS

LED1	Light	Dark	Flash
GREEN	Link	Un-link	Activity
RED	1000M	100M	NA

LED2: LAN2 LED STATUS

LED2	Light	Dark	Flash
GREEN	Link	Un-link	Activity
RED	1000M	100M	NA

LED3: POWER/HDD LED

LED2	Light	Dark	Flash
GREEN	Power On	Power Off	NA
RED	NA	HDD un-access	HDD access

USB3.0 CN19: USB*2

LOWER USB		UPPER USB	
PIN	DEFINITION	PIN	DEFINITION
1	USB_VCC2	10	USB_VCC3
2	USBD0-	11	USBD1-
3	USBD0+	12	USBD1+
4	GND	13	GND
5	USB_SSRX3N_C	14	USB_SSRX4N_C
6	USB_SSRX3P_C	15	USB_SSRX4P_C
7	GND	16	GND
8	USB3TN3	17	USB3TN4
9	USB3TP3	18	USB3TP4

DP1,2,3,4: DISPLAY PORT

PIN	DEFINITION	PIN	DEFINITION
1	DPC_LANEP0	2	GND
3	DPC_LANEN0	4	DPC_LANEP1
5	GND	6	DPC_LANEN1
7	DPC_LANEP2	8	GND
9	DPC_LANEN2	10	DPC_LANEP3
11	GND	12	DPC_LANEN3
13	DDIC_DDC_AUX_SEL	14	GND
15	DPC_AUXP	16	GND
17	DPC_AUXN	18	DPC_DET
19	GND	20	DPC_PWR

POWER BUTTON

Orange Backlight	Blue Backlight
Power Off	Power On

POWER

DC IN: DC Adapter Power Input

PIN	DEFINITION
1	GND
2	GND
3	+VIN
4	+VIN

2.2 Rear Panel Connector Pin Definitions

LAN1: Intel i217LM
LAN2: Intel i210IT

LAN1		LAN2	
PIN	DEFINITION	PIN	DEFINITION
1	D0+	1	D0+
2	D0-	2	D0-
3	D1+	3	D1+
4	D2+	4	D2+
7	D2-	7	D2-
8	D1-	8	D1-
9	D3+	9	D3+
10	D3-	10	D3-

COM1: RS232/422/485 with 5V/12V selectable

Pin	RS-232	RS-422	Half Duplex RS-485
1	DCD#	TX-	D-
2	RXD	TX+	D+
3	TXD	RX+	NA
4	DTR#	RX-	NA
5	GND	GND	GND
6	DSR#	NA	NA
7	RTS#	NA	NA
8	CTS#	NA	NA
9	RI# (Define by JP12)	RI# (Define by JP12)	RI# (Define by JP12)

DP5,6: DISPLAY PORT

PIN	DEFINITION	PIN	DEFINITION
1	DPC_LANEP0	2	GND
3	DPC_LANEN0	4	DPC_LANEP1
5	GND	6	DPC_LANEN1
7	DPC_LANEP2	8	GND
9	DPC_LANEN2	10	DPC_LANEP3
11	GND	12	DPC_LANEN3
13	DDIC_DDC_AUX_SEL	14	GND
15	DPC_AUXP	16	GND
17	DPC_AUXN	18	DPC_DET
19	GND	20	DPC_PWR

DVI: DVI-I

PIN	DEFINITION	PIN	DEFINITION
1	TMDS Data2-	13	NC
2	TMDS Data2+	14	+5V Power
3	GND	15	GND
4	NC	16	Hot Plug Detect
5	NC	17	TMDS Data0-
6	DDC Clock	18	TMDS Data0+
7	DDC Data	19	GND
8	Analog VSYNC	20	NC
9	TMDS Data1-	21	NC
10	TMDS Data1+	22	GND
11	GND	23	TMDS Clock+
12	NC	24	TMDS Clock-
C1	Analog Red	C2	Analog Green
C3	Analog Blue	C4	Analog HYNC
C5	Analog GND0	C6	Analog GND1

USB3.0 CN18: USB*2

LOWER USB		UPPER USB	
PIN	DEFINITION	PIN	DEFINITION
1	USB_VCC0	10	USB_VCC1
2	USBD2-	11	USBD3-
3	USBD2+	12	USBD3+
4	GND	13	GND
5	USB_SSRX1N_C	14	USB_SSRX2N_C
6	USB_SSRX1P_C	15	USB_SSRX2P_C
7	GND	16	GND
8	USB3TN1	17	USB3TN2
9	USB3TP1	18	USB3TP2

MIC 1: Audio Jacks Connector

PIN	DEFINITION
5	MIC_L
4	GND
3	NC
2	MIC1_R
1	GND

Line out: Audio Jacks Connector

PIN	DEFINITION
5	FRONT_L
4	GND
3	NC
2	FRONT_R
1	GND

2.3 Internal Connector and Jumper Setting

MCARD1: Mini PCIE Card Slot<COLAY M SATA>

PIN	DEFINITION	PIN	DEFINITION
1	WAKE#	2	3.3VAUX
3	COEX1	4	GND
5	COEX2	6	1.5V
7	CLKREQ#	8	UIM_PWR
9	GND	10	UIM_DATA
11	REFCLK-	12	UIM_CLK
13	REFCLK+	14	UIM_RESET
15	GND	16	UIM_VPP
17	Reserved	18	GND
19	Reserved	20	W_Disable#
21	GND	22	PERST#
23	PERn0	24	+3.3Vaux
25	PERp0	26	GND
27	GND	28	1.5V
29	GND	30	SMB_CLK
31	PETn0	32	SMB_DATA
33	PETp0	34	GND
35	GND	36	USB_D-
37	GND	38	USB_D+
39	+3.3VAUX	40	GND
41	+3.3VAUX	42	LED_WWAN#
43	GND	44	LED_WLAN#
45	Reserved	46	LED_WPAN#
47	Reserved	48	1.5V
49	Reserved	50	GND
51	Reserved	52	3.3VAUX

JV2,3: COM1 RS232/422/485 jumper setting

No.	Function Description	JV3	JV2	Location
1	Loopback	1 2 3	1 2 3	
2	RS232 (Default)	1 2 3	1 2 3	
3	RS485 Half-Duplex	1 2 3	1 2 3	
4	RS485/422 Full Duplex	1 2 3	1 2 3	

JV4: COM1 RS422/485 receiver termination

Jumper	Function description	Setting
1-2	Disable RS422/485 receiver termination (default)	
2-3	Enable RS422/485receiver termination	
Default setting: 1-2		

JP12: COM1P9SEL pin function select

Jumper	Function description	Setting
1-2	COM_RI(Default)	
3-4	5VS	
5-6	12V	

Chapter 3: AMI BIOS UTILITY

This chapter provides users with detailed descriptions on how to set up a basic system configuration through the AMI BIOS setup utility.

3.1 Starting

To enter the setup screens, perform the following steps:

- Turn on the computer and press the <Del> key immediately.
- After the <Del> key is pressed, the main BIOS setup menu displays. Other setup screens can be accessed from the main BIOS setup menu, such as the Chipset and Power menus.

3.2 Navigation Keys

The BIOS setup/utility uses a key-based navigation system called hot keys. Most of the BIOS setup utility hot keys can be used at any time during the setup navigation process.
Some of the hot keys are <F1>, <F10>, <Enter>, <ESC>, and <Arrow> keys.

Some of the navigation keys may differ from one screen to another.

Left/Right	The Left and Right <Arrow> keys moves the cursor to select a menu.
Up/Down	The Up and Down <Arrow> keys moves the cursor to select a setup screen or sub-screen.
+– Plus/Minus	The Plus and Minus <Arrow> keys changes the field value of a particular setup setting.
Tab	The <Tab> key selects the setup fields.
F1	The <F1> key displays the General Help screen.
F10	The <F10> key saves any changes made and exits the BIOS setup utility.
Esc	The <Esc> key discards any changes made and exits the BIOS setup utility.
Enter	The <Enter> key displays a sub-screen or changes a selected or highlighted option in each menu.

3.3 Main Menu

The Main menu is the screen that first displays when BIOS Setup is entered, unless an error has occurred.

You could setup these items on the Main menu:
System Language: Choose the system default language.
System Date: Set the date. Use Tab to switch between date elements.
System Time: Set the time. Use Tab to switch between time elements.

Access Level
Displays the access level of the current user in the BIOS.

3.4 Advanced Menu

This section allows you to configure and improve your system and allows you to set up some system features according to your preference.

3.4.1 PCI Subsystem Settings

PCI, PCI-X and PCI Express settings.

PCI Common Settings

PCI Latency Timer: Value to be programed into PCI Latency Timer Register.

VGA Palette Snoop: Enable or disable VGA Palette Registers Snooping.

PERR# Generation: Enables or Disables PCI Device to Generate PERR#.

SERR# Generation: Enables or Disables PCI Device to Generate SERR#.

PCI Express Settings

Change PCI Express Devices Settings.

PCI Express Device Register Settings

Relaxed Ordering: Enables or Disables PCI Express Device Relaxed Ordering.

Extended Tag: If ENABLED allows Device to use 8-bit Tag field as a requester.

No Snoop: Enabled or Disables PCI Express Device No Snoop option.

Maximum Payload: Set Maximum Payload of PCI Express Device or allow System BIOS to select the value.

Maximum Read Request: Set Maximum Read Request Size of PCI Express Device or allow System BIOS to select value.

PCI Express Link Register Settings

ASPM Support: Set the ASPM level: Force L0s - Force all links to L0s state: AUTO - BIOS auto configure: DISABLE- Disables ASPM. **WARNING:** Enabling ASPM may cause some PCI-E devices to fail.

Extended Synch: If ENBLED allows generation of extended synchronization patterns.

Link Training Retry
Defines number of retry attempts software will take to retrain the link if previous training attempt was unsuccessful.

Link Training Time out (uS)
Defines number of Microseconds software will wait before polling "Link training" bit in link status register. Value range from 10 to 10000 uS.

Unpopulated Links
In order to save power, software will disable unpopulated PCI Express Links. If this option save to "Disable Link".

Restore PCIE Registers
On non-PCI Express aware OS's some device may not be correctly reinitial after S3. Enableling this restore PCI Express device configurations on S3 resume.
Warning: Enabling this may cause issues with other hardware after S3 resume.

3.4.2 ACPI Settings

System ACPI Parameters.

Enable ACPI Auto Configuration
Enable/disable 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 ACPI sleep state the system will enter when the suspend button is pressed.

Lock Legacy Resources
Enable or disable lock of legacy resource.

S3 Video Repost
Enable or disable S3 Video Repost.

3.4.3 CPU configuration

CPU Configuration Parameters.

```
Aptio Setup Utility - Copyright (C) 2012 American Megatrends, Inc.
Advanced

Hyper-threading                    [Enabled]        This limit is for 1 core
Active Processor Cores             [All]            active. 0 means using the
Overclocking lock                  [Disabled]       factory-configured value.
Limit CPUID Maximum                [Disabled]
Execute Disable Bit                [Enabled]
Intel Virtualization Technology    [Enabled]
Hardware Prefetcher                [Enabled]
Adjacent Cache Line Prefetch       [Enabled]
CPU AES                            [Enabled]
Boot performance mode              [Turbo Performance]
EIST                               [Enabled]
Turbo Mode                         [Enabled]
Energy Performance                 [Performance]
    Package power limit lock       [Enabled]        →←: Select Screen
    Cpu Power Limit1               0                ↑↓: Select Item
    Cpu Power Limit1 Time          0                Enter: Select
    Cpu Power Limit2               0                +/-: Change Opt.
    Platform power limit lock      [Enabled]        F1: General Help
    Cpu Power Limit3               0                F2: Previous Values
    Cpu Power Limit3 Time          0                F3: Optimized Defaults
    Cpu Power Limit3 Duty Cycle    0                F4: Save & Exit
    DDR Power Limit1               0                ESC: Exit
    DDR Power Limit1 Time          0
    DDR Power Limit2               0
    1-Core Ratio Limit             0

Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

```
Aptio Setup Utility - Copyright (C) 2012 American Megatrends, Inc.
Advanced

    2-Core Ratio Limit             0                Lock the Config TDP Control
    3-Core Ratio Limit             0                register
    4-Core Ratio Limit             0
VR Current value lock              [Enabled]
VR Current value                   0
CPU C states                       [Enabled]
  Enhanced C1 state                [Enabled]
  CPU C3 Report                    [Enabled]
  CPU C6 report                    [Enabled]
    C6 Latency                     [Short]
  CPU C7 report                    [CPU C7s]
    C7 Latency                     [Long]
  C1 state auto demotion           [Enabled]
  C3 state auto demotion           [Enabled]        →←: Select Screen
  Package C state demotion         [Disabled]       ↑↓: Select Item
  C1 state auto undemotion         [Enabled]        Enter: Select
  C3 state auto undemotion         [Enabled]        +/-: Change Opt.
  Package C state undemotion       [Disabled]       F1: General Help
  C state Pre-Wake                 [Enabled]        F2: Previous Values
CFG lock                           [Enabled]        F3: Optimized Defaults
Package C State limit              [AUTO]           F4: Save & Exit
LakeTiny Feature                   [Disabled]       ESC: Exit
ACPI CTDP BIOS                     [Disabled]
Configurable TDP Level             [TDP NOMINAL]
Config TDP Lock                    [Disabled]

Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

Hyper-threading
Enable for windows XP and Linux(OS optimized for Hyper-Threading Technology) and Disabled for other OS (OS not optimized for Hyper-Threading Technology). When Disabled only one thread per enabled core is enabled.

Active Processor Cores
Number of cores to enable in each processor package.

Overclocking lock
FLEX_RATIO(194) MSR.

Limit CPUID Maximum
Disable for Windows XP.

Execute Disable Bit
XD can prevent certain classes of malicious buffer overflow attecks when combined with a supporting OS.

Intel Virtualization Technology
When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.

Hardware Prefetcher
Enable the mid level cache(L2) streamer prefetcher.

Adjacent Cache Line Prefetcher
Enable the mid level cache(L2) prefetching of adjacent cache lines.

CPU AES
Enable/disable CPU advanced encryption standard instruction.

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

EIST
Enable/Disable Intel speed step.

Turbo Mode
Enable/Disable CPU turbo mode

Energy performance
Optimize between performance and power savings.

Package power limit lock: When enabled PACKAGE_POWER_LIMIT MSR will be locked and a reset will be required to unlock the register.
CPU Power limit1: CPU power limit1 value
CPU Power limit1 time: Time window which the power limit1 is maintained
CPU Power limit2: CPU power limit2 value
Platform power limit lock: When enable, PLATFORM_POWER_LIMIT MSD will be locked and a reset will be required to unlock the register.
CPU Power Limit3: CPU Power Limit3 value
CPU Power Limit3 Time: Time window which the power limit3 is maintained
CPU Power Limit3 Duty Cycle: Specify the duty cycle in percentage that the CPU is required to maintain over the configured Power Limit3 time windows.
DDR Power Limit1: DDR Power limit1 value
DDR Power Limit1 Time: Time window which the DDR Power Limit1 is maintained.
DDR Power Limit2: DDR Power limit2 value
1-Core Ratio Limit: This limit is for 1 core active. 0 means using the factory-configured value.
2-Core Ratio Limit: This limit is for 2 cores active. 0 means using the factory-configured value.
3-Core Ratio Limit: This limit is for 3 cores active. 0 means using the factory-configured value.
4-Core Ratio Limit: This limit is for 4 cores active. 0 means using the factory-configured value.

VR Current value lock
Locks VR Current value from further writes until a reset.

VR Current value
Voltage regulator current limit. 0 means AUTO.

CPU C States
Enable or disable CPU C states.
Enhanced C1 State: Enhanced C1 State
CPU C3 Report: Enable /disable CPU C3 report to OS
CPU C6 Report: Enable /disable CPU C6 report to OS
C6 Latency: Configure short/long latency for C6
CPU C7 Report: Enable /disable CPU C7 report to OS
C7 Latency: Configure short/long latency for C7
C1 state auto demotion: processor will conditionally demote C3/C6/C7 requests to C1 based on uncore auto-demote information.
C3 state auto demotion: processor will conditionally demote C6/C7 requests to C3 based on uncore auto-demote information.
Package C state demotion: enable package C state demotion
C1 state auto undemotion: undemotion from demoted C1.
C3 state auto undemotion: undemotion from demoted C1.
Package C state undemotion: enable package C state undemotion
C state Pre-wake: Enable or disable C state Pre-Wake feature.

CFG lock
Configure MSR 0xE2[15], CFG lock bit.

Package C State limit
C0/C1, C2, C3, C6, C7, C7s, AUTO

LakeTiny Feature
Enable/Disable LakeTiny for C state configuration.

ACPI CTDP BIOS
Enable/Disable ACPI CTDP BIOS support.

Configurable TDP level
Allows reconfiguration of TDP levels base on current power and thermal delivery capabilities of the system.

Configure TDP lock
Lock the Config TDP control register.

TCC activation offset
Offset from the factory TCC activation temperature.

Intel TXT(LT) Support
Only Disable

ACPI T state
Enable/Disable ACPI T state support.

CPU DTS
Disabled: ACPI thermal management uses EC reported temperature value.
Enabled: ACPI thermal management uses DTS SMM mechanism to obtain CPU temperature values.
Out of Spec: ACPI Thermal Management uses EC reported temperature values and DTS SMM is used to handle Out of spec.

Debug interface
Enable/Disable CPU debug feature.

Debug interface lock
Lock CPU debug interface setting.

IOUT OFFSET Sign
0 positive offset. 1 negative offset.

IOUT OFFSET
VR IOUT OFFSET configuration 0~625.

IOUT SLOPE
VR IOUT SLOPE configuration range 0~1023.

3.4.4 SATA Configuration

This section is used to configure the SATA drives.

SATA Controller(s)
Enable or disable SATA device.

SATA Mode Selection
Determines how SATA controller(s) operate. The options are: IDE, AHCI, RAID

SATA Test Selection
Enable or disable Test Mode

Aggressive LPM Support
Enable PCH to aggressively enter link power state.

SATA Controller Speed
Indicates the maximum speed the SATA controllers can support. The options are default, Gen1, Gen2, Gen3.

Software Feature Mask Configuration

RADI OROM/RST driver will refer to the SWFW configuration to enable or disable the storage features.

RAID0: Enable or disable RAID0 feature.
RAID1: Enable or disable RAID1 feature.
RAID10: Enable or disable RAID10 feature.
RAID5: Enable or disable RAID5 feature.
Intel Rapid Recovery Technology: Enable or disable Intel Rapid Recovery Technology.
OROM UI and Banner: If enabled, then the OROM UI is shown. Otherwise, no OROM banner or information will be displayed if all disks and RAID volumes are Normal.
HDD unlock: If enabled, indicates that the HDD password unlock in the OS is enabled.
LED Locate: If enabled, indicates that the LED/SGPIO hardware is attached and ping yo locate features is enabled on the OS.
IRRT Only on eSATA: If enabled, then only IRRT volumes can span internal and eSATA drives. If disabled, then any RAID volume can span internal and eSATA drives.
Smart Response Technology: Enabled or disable Smart Response Technology.
OROM UI Delay: If enabled, indicates the delay of the OROM UI Splash Screen in a normal status. The options are 2 seconds, 4 seconds, 6 seconds, 8 seconds.

Serial ATA Port 0

Port 0: Enable or disable SATA port
Hot Plug: Designates this port as Hot Pluggable.
External SATA: External SATA support.
SATA device type: Identify the SATA port is connected to Solid State Drive or Hard Disk Drive.
Spin Up Device: On an edge detec from 0 to 1, the PCH starts a COMRESET initialization sequence to the device.

Serial ATA Port 1

Port 1: Enable or disable SATA port
Hot Plug: Designates this port as Hot Pluggable.
External SATA: External SATA support.
SATA device type: Identify the SATA port is connected to Solid State Drive or Hard Disk Drive.
Spin Up Device: On an edge detec from 0 to 1, the PCH starts a COMRESET initialization sequence to the device.

Serial ATA Port 2

Port 2: Enable or disable SATA port

Hot Plug: Designates this port as Hot Pluggable.

External SATA: External SATA support.

SATA device type: Identify the SATA port is connected to Solid State Drive or Hard Disk Drive.

Spin Up Device: On an edge detec from 0 to 1, the PCH starts a COMRESET initialization sequence to the device.

Serial ATA Port 3

Port 3: Enable or disable SATA port

Hot Plug: Designates this port as Hot Pluggable.

External SATA: External SATA support.

SATA device type: Identify the SATA port is connected to Solid State Drive or Hard Disk Drive.

Spin Up Device: On an edge detec from 0 to 1, the PCH starts a COMRESET initialization sequence to the device.

Serial ATA Port 4

Port 4: Enable or disable SATA port

Hot Plug: Designates this port as Hot Pluggable.

External SATA: External SATA support.

SATA device type: Identify the SATA port is connected to Solid State Drive or Hard Disk Drive.

Spin Up Device: On an edge detec from 0 to 1, the PCH starts a COMRESET initialization sequence to the device.

Serial ATA Port 5

Port 5: Enable or disable SATA port

Hot Plug: Designates this port as Hot Pluggable.

External SATA: External SATA support.

SATA device type: Identify the SATA port is connected to Solid State Drive or Hard Disk Drive.

Spin Up Device: On an edge detec from 0 to 1, the PCH starts a COMRESET initialization sequence to the device.

3.4.5 Intel Rapid Start Technology

Enable or disable Intel Rapid Start Technology

3.4.6 PCH-FW Configuration

Configure Management Engine Technology Parameters.

MDES BIOS Status Code
Enable/Disable MDES BIOS Status Code.

Firmware Update Configuration
Configure Management Engine Technology Parameters.

Me FW Image Re-Flash: Enable/Disable Me FW Image Re-Flash function.

3.4.7 Intel Anti-Theft Technology Configuration

Disabling Intel AT allow user to login to platform. This is strictly for testing only. This does not disable Intel AT services in ME.

Intel Anti-Theft Technology
Enable/Disable Intel AT in BIOS for testing. On

Enter Intel AT Suspend Mode
Only Disabled

3.4.8 AMT Configuration

Configure Active Management Technology Parameters.

Intel AMT
Enable/Disable Intel Active Management Technology BIOS Extension.
Note: iAMT H/W is always enabled.
This option just controls the BIOS extension execution. If enabled, this requires additional firmware in the SPI device.

BIOS Hotkey Pressed
OEMFlag Bit 1: Enable/Disable BIOS hotkey press.

MEBx Selection Screen
OEMFlag Bit 2: Enable/Disable MEBx selection screen.

Hide Un-Configure ME Confirmation
OEMFlag Bit 6: Hide Un-Configure ME without password Configuration prompt.

MEBx Debug Message Output
OEMFlag Bit 14: Enable MEBx debug message output.

Un-Configure ME
OEMFlag Bit 15: Un-Configure ME without password.

Amt Wait Timer
Set Timer to wait before sending ASF_GET_BOOT_OPTIONS.

Disable ME
Set ME to Soft Temporary Disabled.

ASF
Enable/Disable Alert Specification Format.

Activate Remote Assistance Process
Trigger CIRA boot.

USB Configure
Enable/Disable USB Configure function.

PET Progress
User can Enable/Disable PET Events progress to receive PET events or not.

WatchDog
Enable/Disable WatchDog Timer.

3.4.9 USB Configuration

USB Configuration Parameters.

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.

USB3.0 Support
Enable/Disable USB3.0 (XHCI) Controller support.

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

EHCI Hand-off
This is a workaround for OSes without EHCI hand-off support. The EHCI ownership change should be claimed by EHCI driver.

USB Mass Storage Driver Support
Enable/Disable USB Mass Storage Driver Support.

USB hardware delays and time-outs:

USB transfer time-out: The time-out value for Control, Bulk, and Interrupt transfers. The options are 1 sec, 5 sec, 10 sec, 20 sec.

Device reset time-out: USB mass storage device Start Unit command time-out. The options are 10 sec, 20 sec, 30 sec, 40 sec.

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 Hub port the delay is taken from Hub descriptor. The options are Auto, manual.

3.4.10 IT8786 Super IO Configuration

System Super IO Chip Parameters.

Serial Port 1 Configuration

Set Parameters of Serial Port 0 (COMA).

Serial Port: Enable or Disable Serial Port (COM).

Device Settings: IO=3F8h, IRQ=4

Change Settings: Select an optimal setting for Super IO device.

Serial Port 2 Configuration

Set Parameters of Serial Port 1 (COMB).

Serial Port: Enable or Disable Serial Port (COM).

Device Settings: IO=2F8h, IRQ=3

Change Settings: Select an optimal setting for Super IO device.

Serial Port 3 Configuration

Set Parameters of Serial Port 2 (COMC).

Serial Port: Enable or Disable Serial Port (COM).
Device Settings: IO=3E8h, IRQ=7
Change Settings: Select an optimal setting for Super IO device.

Serial Port 4 Configuration

Set Parameters of Serial Port 3 (COMD).

Serial Port: Enable or Disable Serial Port (COM).
Device Settings: IO=2E8h, IRQ=7
Change Settings: Select an optimal setting for Super IO device.

Serial Port 5 Configuration

Set Parameters of Serial Port 4 (COME).

Serial Port: Enable or Disable Serial Port (COM).
Device Settings: IO=2F0h, IRQ=7
Change Settings: Select an optimal setting for Super IO device.

Serial Port 6 Configuration

Set Parameters of Serial Port 5 (COMF).

Serial Port: Enable or Disable Serial Port (COM).
Device Settings: IO=2E0h, IRQ=7
Change Settings: Select an optimal setting for Super IO device.

3.4.11 IT8786 HW Monitor

Monitor hardware status.

3.4.12 Serial Port Console Redirection

Console Redirection
Console Redirection Enable or Disable.

Console Redirection Setting
The Settings specify how the host computer and the remote computer will exchange data. Both computers should have the same or compatible setting.

Out-of-Band Mgmt Port: Microsoft Windows Emergency Management Service allows for remote management of a Windows Server OS through a serial port. The options are COM0 (Disabled), COM1(Pci Bus0, Dev0, Func0) (Disabled)

Terminal Type: VT-UTF8 is the preferred terminal type for out-of-band management. The next best choice is VT100+ and then VT100. See above, in Console Redirection Settings page, for more Help with Terminal Type/Emulation. The options are VT100, VT100+, VT-UTF8, ANSI.

Bits per second: selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds. The options are 9600, 19200, 57600, 115200.

Flow Control: Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a "stop" signal can be sent to stop the data flow. Once the buffers are empty, a "star" signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals. The options are None, Hardware RTS/CTS, Software Xon/xoff

Data bits: 8

Parity: None

Stop bits: 1

3.4.13 Network Stack

Network stack settings

Network Stack

Enable/Disable UEFI network stack

3.4.14 Intel I210 Gigabit Network Connection

Configure Gigabit Ethernet device parameters.

PORT CONFIGURATION MENU

NIC Configuration: Configure Boot Protocol, wake on LAN, Link Speed, and VLAN.

Blink LEDs: Identify the physical network port by blinking the associated LED.

PORT CONFIGURATION INFORMATION

Link Status: Link Status.

Virtual MAC Address: Programmatically assignable MAC address for port.

3.5 Chipset

This section gives you functions to configure the system based on the specific features of the chipset. The chipset manages bus speeds and access to system memory resources.

3.5.1 PCH IO configuration

PCI Express Configuration

PCI Express Configuration settings

PCIE Root Port Function Swapping: Enable or disable PCI Express PCI Express Root Port Function Swapping.

Subtractive Decode: Enable or disable PCI Express Subtractive Decode.

PCI Express Root Port1

PCI Express Root Port1 setting. Only enabled

ASPM Support: Set the ASPM Level: Force L0s – Force all links to L0s State: AUTO – BIOS auto configure : DISABLE – Disables ASPM. The options are Disabled, L0s, L1, L0SL1, Auto

L1 Substates: PCI Express L1 Substates setting. The options are Disabled, L1.1, L1.2, L1.1 & L1.2

URR: Enable or disable PCI Express Unsupported Request Reporting.

FER: Enable or disable PCI Express Device Fatal Error Reporting.

NFER: Enable or disable PCI Express Device Non-Fatal Error Reporting.

CER: Enable or disable PCI Express Device Correctable Error Reporting.

CTO: Enable or disable PCI Express Completion Timer TO.

SEFE: Enable or disable Root PCI Express System Error on Fatal Error.

SENFE: Enable or disable Root PCI Express System Error on Non-Fatal Error.

SECE: Enable or disable Root PCI Express System Error on Correctable Error.

PME SCI: Enable or disable PCI Express PME SCI.

Hot Plug: Enable or disable PCI Express Hot Plug.

PCIe Speed: Select PCI Express port speed.

Detect Non-Compliance Device: Detect Non Compliance PCI Express Device. If enable, it will take more time at POST time.

Extra Bus Reserved: Extra Bus Reserved (0-7) for bridges behind this Root Bridge.

Reseved Memory: Reserved Memory Range for this Root Bridge.

Prefetchable Memory: Prefetchable Memory Range for this Root Bridge.

Reserved I/O: Reserved I/O (4K/8K/12K/16K/.../48K) Range for this Root Bridge.

PCIE LTR: PCIE Latency Reporting Enable/Disable.

PCIE LTR Lock: PCIE LTR configuration lock.

Snoop Latency Ocerride: Snoop Latency Ocerride for PCH PCIE.

Non Snoop Latency Ocerride: Non Snoop Latency Ocerride for PCH PCIE.

PCI Express Root Port2

control the PCI Express Root port, the options are enabled/disabled.

ASPM Support: Set the ASPM Level: Force L0s – Force all links to L0s State: AUTO – BIOS auto configure: DISABLE – Disables ASPM.

L1 Substates: PCI Express L1 Substates setting.

- **URR:** Enable or disable PCI Express Unsupported Request Reporting.
- **FER:** Enable or disable PCI Express Device Fatal Error Reporting.
- **NFER:** Enable or disable PCI Express Device Non-Fatal Error Reporting.
- **CER:** Enable or disable PCI Express Device Correctable Error Reporting.
- **CTO:** Enable or disable PCI Express Completion Timer TO.
- **SEFE:** Enable or disable Root PCI Express System Error on Fatal Error.
- **SENFE:** Enable or disable Root PCI Express System Error on Non-Fatal Error.
- **SECE:** Enable or disable Root PCI Express System Error on Correctable Error.
- **PME SCI:** Enable or disable PCI Express PME SCI.
- **Hot Plug:** Enable or disable PCI Express Hot Plug.

PCIe Speed: Select PCI Express port speed.

Detect Non-Compliance Device: Detect Non Compliance PCI Express Device. If enable, it will take more time at POST time.

Extra Bus Reserved: Extra Bus Reserved (0-7) for bridges behind this Root Bridge.

Reseved Memory: Reserved Memory Range for this Root Bridge.

Prefetchable Memory: Prefetchable Memory Range for this Root Bridge.

Reserved I/O: Reserved I/O (4K/8K/12K/16K/.../48K) Range for this Root Bridge.

PCIE LTR: PCIE Latency Reporting Enable/Disable.

PCIE LTR Lock: PCIE LTR configuration lock.

Snoop Latency Ocerride: Snoop Latency Ocerride for PCH PCIE.

Non Snoop Latency Ocerride: Non Snoop Latency Ocerride for PCH PCIE.

PCI Express Root Port3

control the PCI Express Root port, the options are enabled/disabled

ASPM Support: Set the ASPM Level: Force L0s – Force all links to L0s State: AUTO – BIOS auto configure: DISABLE – Disables ASPM.

L1 Substates: PCI Express L1 Substates setting.

- **URR:** Enable or disable PCI Express Unsupported Request Reporting.
- **FER:** Enable or disable PCI Express Device Fatal Error Reporting.
- **NFER:** Enable or disable PCI Express Device Non-Fatal Error Reporting.
- **CER:** Enable or disable PCI Express Device Correctable Error Reporting.
- **CTO:** Enable or disable PCI Express Completion Timer TO.
- **SEFE:** Enable or disable Root PCI Express System Error on Fatal Error.
- **SENFE:** Enable or disable Root PCI Express System Error on Non-Fatal Error.
- **SECE:** Enable or disable Root PCI Express System Error on Correctable Error.
- **PME SCI:** Enable or disable PCI Express PME SCI.
- **Hot Plug:** Enable or disable PCI Express Hot Plug.

PCIe Speed: Select PCI Express port speed.

Detect Non-Compliance Device: Detect Non-Compliance PCI Express Device. If enable, it will take more time at POST time.

Extra Bus Reserved: Extra Bus Reserved (0-7) for bridges behind this Root Bridge.

Reseved Memory: Reserved Memory Range for this Root Bridge.

Prefetchable Memory: Prefetchable Memory Range for this Root Bridge.

Reserved I/O: Reserved I/O (4K/8K/12K/16K/.../48K) Range for this Root Bridge.

PCIE LTR: PCIE Latency Reporting Enable/Disable.

PCIE LTR Lock: PCIE LTR Configuration Lock.

Snoop Latency Ocerride: Snoop Latency Ocerride for PCH PCIE.

Non Snoop Latency Ocerride: Non Snoop Latency Ocerride for PCH PCIE.

PCI Port 4 is assigned to LAN

PCI Express Root Port5:
control the PCI Express Root port, the options are enabled/disabled

ASPM Support: Set the ASPM Level: Force L0s – Force all links to L0s State: AUTO – BIOS auto configure: DISABLE – Disables ASPM.

L1 Substates: PCI Express L1 Substates setting.

- **URR:** Enable or disable PCI Express Unsupported Request Reporting.
- **FER:** Enable or disable PCI Express Device Fatal Error Reporting.
- **NFER:** Enable or disable PCI Express Device Non-Fatal Error Reporting.
- **CER:** Enable or disable PCI Express Device Correctable Error Reporting.
- **CTO:** Enable or disable PCI Express Completion Timer TO.
- **SEFE:** Enable or disable Root PCI Express System Error on Fatal Error.
- **SENFE:** Enable or disable Root PCI Express System Error on Non-Fatal Error.
- **SECE:** Enable or disable Root PCI Express System Error on Correctable Error.
- **PME SCI:** Enable or disable PCI Express PME SCI.
- **Hot Plug:** Enable or disable PCI Express Hot Plug.

PCIe Speed: Select PCI Express port speed.

Detect Non-Compliance Device: Detect Non-Compliance PCI Express Device. If enable, it will take more time at POST time.

Extra Bus Reserved: Extra Bus Reserved (0-7) for bridges behind this Root Bridge.

Reseved Memory: Reserved Memory Range for this Root Bridge.

Prefetchable Memory: Prefetchable Memory Range for this Root Bridge.

Reserved I/O: Reserved I/O (4K/8K/12K/16K/.../48K) Range for this Root Bridge.

PCIE LTR: PCIE Latency Reporting Enable/Disable.

PCIE LTR Lock: PCIE LTR Configuration Lock.

Snoop Latency Ocerride: Snoop Latency Ocerride for PCH PCIE.

Non Snoop Latency Ocerride: Non Snoop Latency Ocerride for PCH PCIE.

PCI Express Root Port6

control the PCI Express Root port, the options are enabled/disabled

ASPM Support: Set the ASPM Level: Force L0s – Force all links to L0s State: AUTO – BIOS auto configure: DISABLE – Disables ASPM.

L1 Substates: PCI Express L1 Substates setting.

- **URR:** Enable or disable PCI Express Unsupported Request Reporting.
- **FER:** Enable or disable PCI Express Device Fatal Error Reporting.
- **NFER:** Enable or disable PCI Express Device Non-Fatal Error Reporting.
- **CER:** Enable or disable PCI Express Device Correctable Error Reporting.
- **CTO:** Enable or disable PCI Express Completion Timer TO.
- **SEFE:** Enable or disable Root PCI Express System Error on Fatal Error.
- **SENFE:** Enable or disable Root PCI Express System Error on Non-Fatal Error.
- **SECE:** Enable or disable Root PCI Express System Error on Correctable Error.
- **PME SCI:** Enable or disable PCI Express PME SCI.
- **Hot Plug:** Enable or disable PCI Express Hot Plug.

PCIe Speed: Select PCI Express port speed.

Detect Non-Compliance Device: Detect Non-Compliance PCI Express Device. If enable, it will take more time at POST time.

Extra Bus Reserved: Extra Bus Reserved (0-7) for bridges behind this Root Bridge.

Reseved Memory: Reserved Memory Range for this Root Bridge.

Prefetchable Memory: Prefetchable Memory Range for this Root Bridge.

Reserved I/O: Reserved I/O (4K/8K/12K/16K/.../48K) Range for this Root Bridge.

PCIE LTR: PCIE Latency Reporting Enable/Disable.

PCIE LTR Lock: PCIE LTR Configuration Lock.

Snoop Latency Ocerride: Snoop Latency Ocerride for PCH PCIE.

Non Snoop Latency Ocerride: Non Snoop Latency Ocerride for PCH PCIE.

PCI Express Root Port7

control the PCI Express Root port, the options are enabled/disabled

ASPM Support: Set the ASPM Level: Force L0s – Force all links to L0s State: AUTO – BIOS auto configure: DISABLE – Disables ASPM.

L1 Substates: PCI Express L1 Substates setting.

- **URR:** Enable or disable PCI Express Unsupported Request Reporting.
- **FER:** Enable or disable PCI Express Device Fatal Error Reporting.
- **NFER:** Enable or disable PCI Express Device Non-Fatal Error Reporting.
- **CER:** Enable or disable PCI Express Device Correctable Error Reporting.
- **CTO:** Enable or disable PCI Express Completion Timer TO.
- **SEFE:** Enable or disable Root PCI Express System Error on Fatal Error.
- **SENFE:** Enable or disable Root PCI Express System Error on Non-Fatal Error.
- **SECE:** Enable or disable Root PCI Express System Error on Correctable Error.
- **PME SCI:** Enable or disable PCI Express PME SCI.
- **Hot Plug:** Enable or disable PCI Express Hot Plug.

PCIe Speed: Select PCI Express port speed.

Detect Non-Compliance Device: Detect Non-Compliance PCI Express Device. If enable, it will take more time at POST time.

Extra Bus Reserved: Extra Bus Reserved (0-7) for bridges behind this Root Bridge.

Reseved Memory: Reserved Memory Range for this Root Bridge.

Prefetchable Memory: Prefetchable Memory Range for this Root Bridge.

Reserved I/O: Reserved I/O (4K/8K/12K/16K/.../48K) Range for this Root Bridge.

PCIE LTR: PCIE Latency Reporting Enable/Disable.

PCIE LTR Lock: PCIE LTR Configuration Lock.

Snoop Latency Ocerride: Snoop Latency Ocerride for PCH PCIE.

Non Snoop Latency Ocerride: Non Snoop Latency Ocerride for PCH PCIE.

PCI Express Root Port8

control the PCI Express Root port, the options are enabled/disabled

ASPM Support: Set the ASPM Level: Force L0s – Force all links to L0s State: AUTO – BIOS auto configure: DISABLE – Disables ASPM.

L1 Substates: PCI Express L1 Substates setting.

- **URR:** Enable or disable PCI Express Unsupported Request Reporting.
- **FER:** Enable or disable PCI Express Device Fatal Error Reporting.
- **NFER:** Enable or disable PCI Express Device Non-Fatal Error Reporting.
- **CER:** Enable or disable PCI Express Device Correctable Error Reporting.
- **CTO:** Enable or disable PCI Express Completion Timer TO.
- **SEFE:** Enable or disable Root PCI Express System Error on Fatal Error.
- **SENFE:** Enable or disable Root PCI Express System Error on Non-Fatal Error.
- **SECE:** Enable or disable Root PCI Express System Error on Correctable Error.
- **PME SCI:** Enable or disable PCI Express PME SCI.
- **Hot Plug:** Enable or disable PCI Express Hot Plug.

PCIe Speed: Select PCI Express port speed.

Detect Non-Compliance Device: Detect Non-Compliance PCI Express Device. If enable, it will take more time at POST time.

Extra Bus Reserved: Extra Bus Reserved (0-7) for bridges behind this Root Bridge.

Reseved Memory: Reserved Memory Range for this Root Bridge.

Prefetchable Memory: Prefetchable Memory Range for this Root Bridge.

Reserved I/O: Reserved I/O (4K/8K/12K/16K/.../48K) Range for this Root Bridge.

PCIE LTR: PCIE Latency Reporting Enable/Disable.

PCIE LTR Lock: PCIE LTR Configuration Lock.

Snoop Latency Ocerride: Snoop Latency Ocerride for PCH PCIE.

Non Snoop Latency Ocerride: Non Snoop Latency Ocerride for PCH PCIE.

USB Configuration

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

XHCI Mode: Mode of operation of xHCI controller.

BTCG: Enabling/disabling trunk clock gating.

USB Ports Per-Port Disable Control: Control each of the USB ports (0~13) disabling.

PCH Azalia Configuration.

Azalia: Control Detection of the Azalia device.

- Disabled=Azalia will be unconditionally disabled.
- Enabled=Azalia will be unconditionally Enabled.
- Auto=Azalia will be enabled if present, disabled otherwise.

Azalia Docking Support: Enable or disable Azalia Docking Support of Audio Controller.

Azalia PME: Enable or disable Power Management capability of Audio Controller.

PCH LAN Controller

Enable or disable onboard NIC.

Wake on LAN: Enable or disable integrated LAN to wake the system. (The Wake On LAN cannot be disabled if ME is on at Sx state.)

SLP_LAN# Low on DC Power: Enable/Disable SLP_LAN# Low on DC Power.

Board Capability
Board Capability-SUS_PWR_DN_ACK->Send Disabled to PCH, DeepSx->Show DeepSx Policies.

GP27 Wake From DeepSx
Wake from DeepSx by the assertion of GP27 pin.

PCIE Wake From DeepSx
Wake from DeepSx by the assertion of PCIE.

Serial IRQ Mode
Configure Serial IRQ Mode.

SLP_S4 Assertion Width
Select a minimum assertion width of the SLP_S4# signal.

Port 80h Redirection
Control where the Port 80h cycles are sent.

3.5.2 System AGENT SA

VT-d
Check to enable VT-d function on MCH.

Graphics Configuration

Graphics Turbo IMON Current: Graphics turbo IMON current values supported (14-31).

Primary Display: select which of AUTO/IGFX/PEG/SG graphics device should be primary display or select SG for switchable GFX

Primary PEG: Select Auto/PEG1/PEG2 Graphics device should be Primary PEG.

Primary PCIE: Select Auto/PCIE1/PCIE2/PCIE3/PCIE4PCIE5/PCIE6/PCIE7 Graphics device should be Primary PCIE.

Internal Graphics: Keep IGD enabled based on the setup options

Aperture Size: Select the Aperture Size.

DVMT Pre-Allocated: Select DVMT 5.0 Pre-Allocated (fixed) Graphics memory size used by the internal graphics device.

DVMT Total Gfx Mem: Select DVMT5.0 total graphic memory size used by the internal graphics device.

Gfx Low Power Enable: this option is applicable for SFF only.

Panel Power Enable: Enable/Disable forcing of Panel Power in the BIOS.

LCD Control

Primary IGFX Boot Display: Select the Video Device which will be activated during POST. This has no effect if external graphics present. Secondary boot display selection will appear based on your selection. VGA modes will be supported only on primary display.

LCD Panel Type: Select LCD panel used by Internal Graphics Device by selecting the appropriate setup item.

SDVO-LFP Panel Type: Select SDVO panel used by Internal Graphics Device by selecting the appropriate setup item.

Panel Scaling: Select the LCD panel scaling option used by the Internal Graphics Device.

Backlight control: backlight control setting

Panel Color Depth: select the LFP panel color depth.

LCD Control

Primary IGFX Boot Display: Select the Video Device which will be activated during POST. This has no effect if external graphics present. Secondary boot display selection will appear based on your selection. VGA modes will be supported only on primary display.

LCD Panel Type: Select LCD panel used by Internal Graphics Device by selecting the appropriate setup item.

SDVO-LFP Panel Type: Select SDVO panel used by Internal Graphics Device by selecting the appropriate setup item.

Panel Scaling: Select the LCD panel scaling option used by the Internal Graphics Device.

Backlight control: backlight control setting

Panel Color Depth: select the LFP panel color depth.

Memory Configuration

DIMM profile: Select DIMM timing profile that should be used.

Memory Frequency Limiter: maximum memory frequency selections in Mhz.

DDR Reset Wait Time: The value of ns to wait for switch DDR voltage, minimum 20ns.

ECC Support: Enable or disable DDR Ecc support

Max TOLUD: Maximum Value of TOLUD. Dynamic assignment would adjust TOLUD automatically based on largest MMIO length of installed graphic controller.

GT- Power Management Control

RC6 (render standby): check to enable render standby support.

GT OverClocking Support: enable or disable GT overclocking support

3.6 Boot

This section is used to configure the boot features.

Setup Prompt Timeout
Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.

Bootup NumLock State
Select the keyboard NumLock state.

Quiet Boot
Enables or disables Quiet Boot option.

Fast Boot
Enables or disables boot with initialization of a minimal set of devices required to launch active boot option. Has no effect for BBS boot options.

Boot option priorities
Boot Option #1: Sets the system boot order.

Hard Drive BBS Priorities
Set the order of the legacy devices in this group

CSM16 Parameters

Set the order of the legacy devices in this group

GateA20 Active: UPON REQUEST – GA20 can be disabled using BIOS serices.ALWAYS-do not allow disabling GA20; this option is useful when any RT code is executed above 1MB.

Option ROM Messages: Set display mode for option ROM.

INT19 Trap Response: BIOS reaction on INT19 trapping by option ROM: IMMEDIATE-execute the trap right away; POSTPONES-execute the trap during legacy boot.

CSM Parameters

OpROM execution, boot options filter, etc.

3.7 Security

Use the Security Menu to establish system passwords

Administrator Password

Set Administartor Password.

User Password

Set User Password.

HDD Security Configuration

Set HDD Password.

3.8 Save and Exit

This screen provides functions for handling changes made to the BIOS settings and the exiting of the Setup program.

Save Changes and Exit
Exit system setup after saving the changes.

Discard Changes and Exit
Exit system setup without saving any changes.

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

Discard Changes and Reset
Reset system setup without saving any changes.

Save Options

Save Changes: Save Changes done so far to any of the setup options.
Discard Changes: Discard Changes done so far to any of the setup options.

Restore Defaults
Restore/Load Default values for all the setup options.

Save as User Defaults
Save the changes done so far as User Defaults.

Restore user Defaults
Restore the User Defaults to all the setup options.

Launch EFI Shell from filesystem device
Attempts to launch EFI Shell application (Shellx64.efi) from one of the available filesystem devices.