THD8141

8141-xxx

No. 87-508144-000 Revision A

BIOS SETUP

TECHNICAL REFERENCE

Aptio® 4.x Test Setup Environment (TSE)

For use with THD8141

Intel® Xeon® E3-1275 v3
Intel® Xeon® E3-1225 v3
Intel® Xeon® E3-1268L v3
Intel® Core™ i7-4790S
Intel® Core™ i5-4590S
Intel® Core™ i3-4330TE
(Haswell)

Quad and Dual Core

PROCESSOR-BASED

SHB

WARRANTY

The following is an abbreviated version of Trenton Systems' warranty policy for PICMG® 1.3 products. For a complete warranty statement, contact Trenton or visit our website at: www.trentonsystems.com/about-us/company-policies/.

Trenton PICMG® 1.3 products are warranted against material and manufacturing defects for five years from date of delivery to the original purchaser. Buyer agrees that if this product proves defective Trenton Systems, Inc. is only obligated to repair, replace or refund the purchase price of this product at Trenton Systems' discretion. The warranty is void if the product has been subjected to alteration, neglect, misuse or abuse; if any repairs have been attempted by anyone other than Trenton Systems, Inc.; or if failure is caused by accident, acts of God, or other causes beyond the control of Trenton Systems, Inc. Trenton Systems, Inc. reserves the right to make changes or improvements in any product without incurring any obligation to similarly alter products previously purchased.

In no event shall Trenton Systems, Inc. be liable for any defect in hardware or software or loss or inadequacy of data of any kind, or for any direct, indirect, incidental or consequential damages arising out of or in connection with the performance or use of the product or information provided. Trenton Systems, Inc.'s liability shall in no event exceed the purchase price of the product purchased hereunder. The foregoing limitation of liability shall be equally applicable to any service provided by Trenton Systems, Inc.

RETURN POLICY

A Return Material Authorization (RMA) number, obtained from Trenton Systems prior to return, must accompany products returned for repair. The customer must prepay freight on all returned items, and the customer is responsible for any loss or damage caused by common carrier in transit. Items will be returned from Trenton via Ground, unless prior arrangements are made by the customer for an alternative shipping method

To obtain an RMA number, call us at (800) 875-6031 or (770) 287-3100. We will need the following information:

Return company address and contact
Model name and model # from the label on the back of the product
Serial number from the label on the back of the product
Description of the failure

An RMA number will be issued. Mark the RMA number clearly on the outside of each box, include a failure report for each board and return the product(s) to our Utica, NY facility:

Trenton Systems, Inc.
1001 Broad Street
Utica, NY 13501
Attn: Repair Department

Contact Trenton Systems for our complete service and repair policy.

TRADEMARKS

IBM, PC/AT, VGA, EGA, OS/2 and PS/2 are trademarks or registered trademarks
of International Business Machines Corp.
AMI, Aptio and AMIBIOS are trademarks of American Megatrends Inc.
Intel, Xeon, Intel Core, Intel AMT 7.0, Intel TXT Intel Hyper-Threading Technology and Intel Virtualization Technology are trademarks or registered trademarks of Intel Corporation.
MS-DOS and Microsoft are registered trademarks of Microsoft Corp.
PICMG, SHB Express and the PICMG logo are trademarks or registered trademarks
of the PCI Industrial Computer Manufacturers Group.
PCI Express is a trademark of the PCI-SIG
All other brand and product names may be trademarks or registered trademarks
of their respective companies.

LIABILITY DISCLAIMER

This manual is as complete and factual as possible at the time of printing; however, the information in this manual may have been updated since that time. Trenton Systems, Inc. reserves the right to change the functions, features or specifications of their products at any time, without notice.

E-mail: Support@TrentonSystems.com
Web: www.TrentonSystems.com

TRENTON Systems, Inc.
2350 Centennial Drive • Gainesville, Georgia 30504
Sales: (800) 875-6031 • Phone: (770) 287-3100 • Fax: (770) 287-3150

This page intentionally left blank

Table of Contents

SHB HANDLING PRECAUTIONS

WARNING: This product has components which may be damaged by electrostatic discharge.

To protect your system host board (SHB) from electrostatic damage, be sure to observe the following precautions when handling or storing the board:

- Keep the SHB in its static-shielded bag until you are ready to perform your installation.
- Handle the SHB by its edges.
- Do not touch the I/O connector pins.
- Do not apply pressure or attach labels to the SHB.
- Use a grounded wrist strap at your workstation or ground yourself frequently by touching the metal chassis of the system before handling any components. The system must be plugged into an outlet that is connected to an earth ground.
- Use antistatic padding on all work surfaces.
- Avoid static-inducing carpeted areas.

RECOMMENDED BOARD HANDLING PRECAUTIONS

This SHB has components on both sides of the PCB. Some of these components are extremely small and subject to damage if the board is not handled properly. It is important for you to observe the following precautions when handling or storing the board to prevent components from being damaged or broken off:

- Handle the board only by its edges.
- Store the board in padded shipping material or in an anti-static board rack.
- Do not place an unprotected board on a flat surface.

This page intentionally left blank

Chapter 1 Starting Aptio® TSE

Introduction

The THD8141 and feature the Aptio® 4.x BIOS from American Megatrends, Inc. (AMI) with a ROM-resident setup utility called the Aptio® Text Setup Environment or TSE. The TSE allows you to select to the following categories of options:

- Main Menu
- Advanced Setup
- Chipset Setup
- Boot Setup
- Security Setup
- Save & Exit Setup
- Event Logs Setup

Each of these options allows you to review and/or change various setup features of your system. Details are provided in the following chapters of this manual. Additional copies of the Trenton THD8141 BIOS and hardware technical reference manuals are available under the **Downloads** tab on the THD8141 or web pages.

Aptio Text Setup Environment (TSE) is a text-based basic input and output system. The purpose of Aptio TSE is to empower the user with complete system control at boot. This document explains the basic navigation of Aptio TSE.

NOTE: The contents of this document were provided as a courtesy from American Megatrends, Inc or AMI and describe the standard look and feel of the Aptio TSE interface. Trenton Systems, Inc. is the manufacturer of the SHB hardware and during production may have made subtle changes to some of the settings described in this document. Therefore, some of the options that are described in this document may not exist or may have been modified for use in the THD8141 implementation of the Aptio TSE BIOS utility. Contact Trenton Technical support for any questions regarding the SHBs' implementation of Aptio TSE.

Starting Aptio TSE

To enter the Aptio TSE screens, follow the steps below:

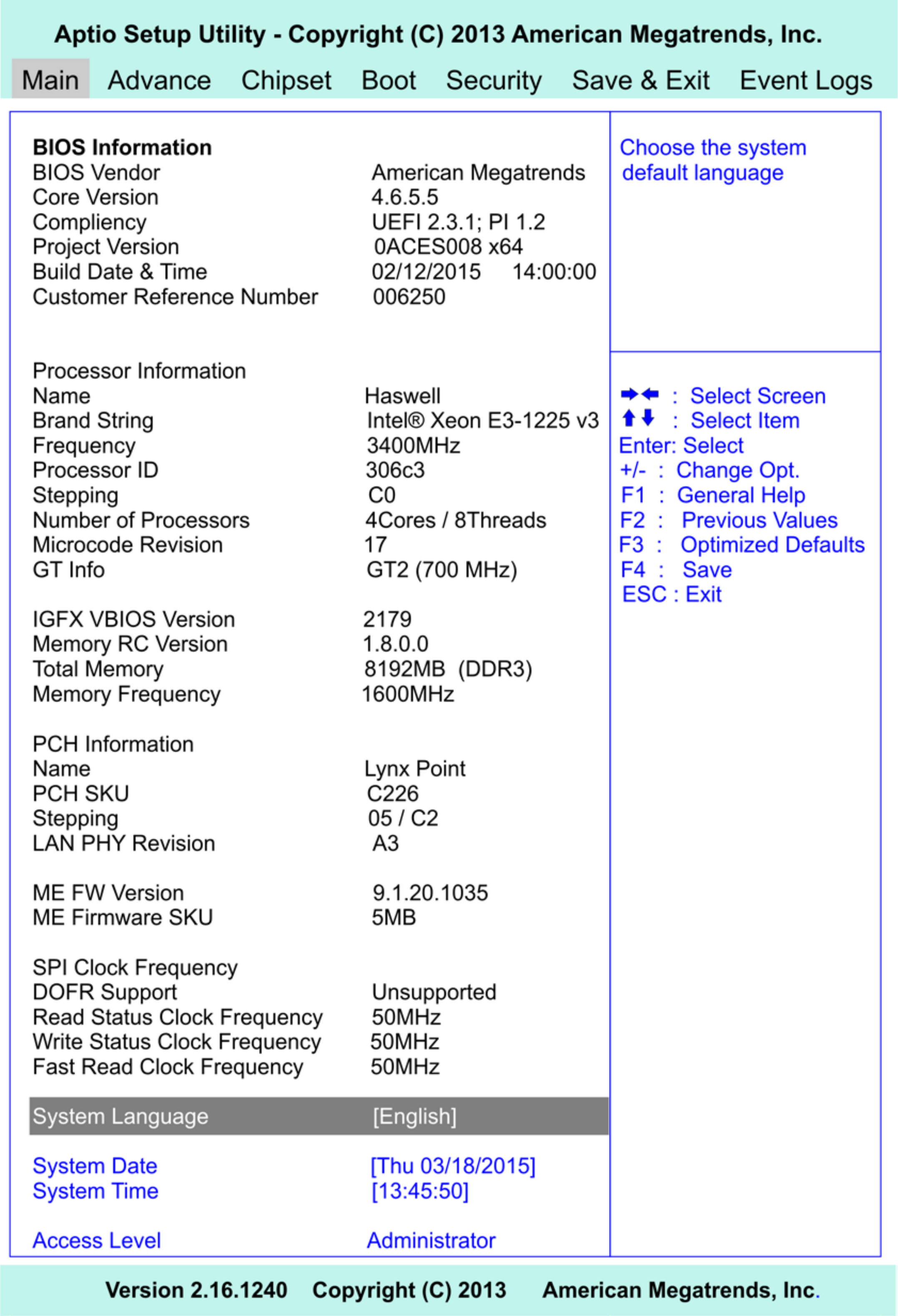
Step	Description
1	Install the SHB in a PICMG 1.3 backplane with the proper system power connections made to the backplane and a mouse, keyboard and monitor connected to the SHB
2	Power on the system with the SHB
3	Press the <Delete> or <F2> key on your keyboard when you see the following text prompt: **Press DEL or F2 to enter Setup**
4	After you press the <Delete>/<F2> key, the Aptio TSE main BIOS setup menu displays. You can access the other setup screens from the main BIOS setup menu, such as the Chipset and Power menus.

NOTE: In most cases, the <Delete> or <F2> keys are used to invoke the Aptio TSE screen. There are a few cases that other keys are used (<F1>, <F10>, …).

NOTE: The user can press the <TAB> key during boot to switch from the boot splash screen (logo) to see the keystroke messages.

Aptio® TSE Setup Menu

The Aptio TSE BIOS setup menu is the first screen that you can navigate. Each BIOS setup menu option is described in this user's guide.



```
BIOS Information
BIOS Vendor                     American Megatrends
Core Version                    4.6.5.5
Compliency                      UEFI 2.3.1; PI 1.2
Project Version                 0ACES008 x64
Build Date & Time               02/12/2015    14:00:00
Customer Reference Number       006250

Processor Information
Name                            Haswell
Brand String                    Intel® Xeon E3-1225 v3
Frequency                       3400MHz
Processor ID                    306c3
Stepping                        C0
Number of Processors            4Cores / 8Threads
Microcode Revision              17
GT Info                         GT2 (700 MHz)

IGFX VBIOS Version              2179
Memory RC Version               1.8.0.0
Total Memory                    8192MB  (DDR3)
Memory Frequency                1600MHz

PCH Information
Name                            Lynx Point
PCH SKU                         C226
Stepping                        05 / C2
LAN PHY Revision                A3

ME FW Version                   9.1.20.1035
ME Firmware SKU                 5MB

SPI Clock Frequency
DOFR Support                    Unsupported
Read Status Clock Frequency     50MHz
Write Status Clock Frequency    50MHz
Fast Read Clock Frequency       50MHz

System Language                 [English]

System Date                     [Thu 03/18/2015]
System Time                     [13:45:50]

Access Level                    Administrator
```

Choose the system default language

There may be slight differences in the screen shots illustrated in this manual due to Trenton THD8141 BIOS modifications. Contact Trenton Technical support for any questions regarding the SHBs' implementation of Aptio TSE.

Navigation

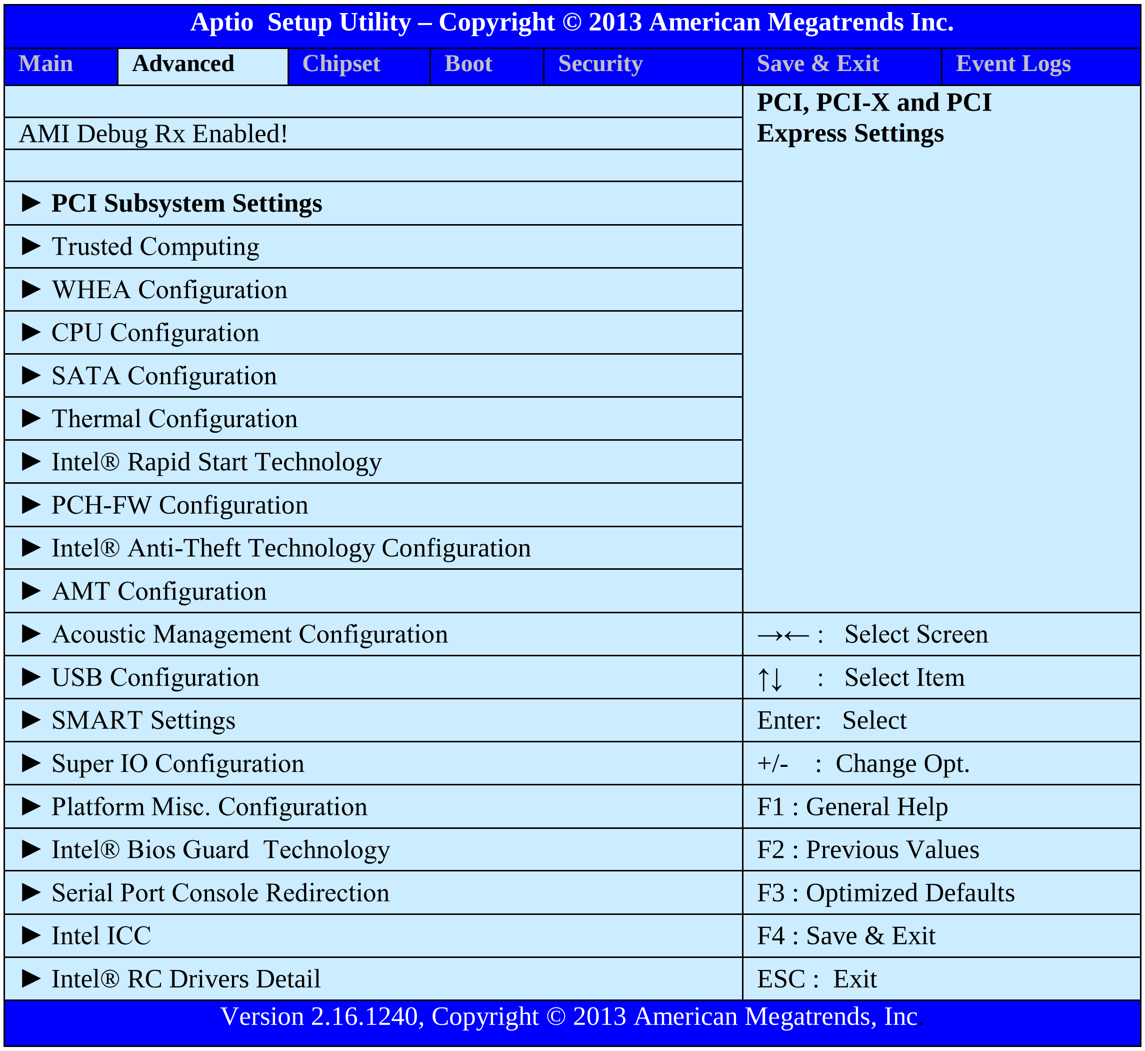
The Aptio® TSE keyboard-based navigation can be accomplished using a combination of the keys.(<FUNCTION> keys, <ENTER>, <ESC>, <ARROW> keys, etc.).

Key	**Description**
ENTER	The *Enter* key allows the user to select an option to edit its value or access a sub menu.
→← Left/Right	The *Left and Right* <Arrow> keys allow you to select an Aptio TSE screen. For example: Main screen, Advanced screen, Chipset screen, and so on.
↑↓ Up/Down	The *Up and Down* <Arrow> keys allow you to select an Aptio TSE item or sub-screen.
+- Plus/Minus	The *Plus and Minus* <Arrow> keys allow you to change the field value of a particular setup item. For example: Date and Time.
Tab	The <Tab> key allows you to select Aptio TSE fields.
ESC	The <Esc> key allows you to discard any changes you have made and exit the Aptio TSE. Press the <Esc> key to exit the Aptio TSE without saving your changes. The following screen will appear: Press the <Enter> key to discard changes and exit. You can also use the <Arrow> key to select *Cancel* and then press the <Enter> key to abort this function and return to the previous screen.
Function keys	When other function keys become available, they are displayed in the help screen along with their intended function.

Chapter 2 Advanced Setup

Introduction

Select the *Advanced* menu item from the Aptio TSE screen to enter the Advanced BIOS Setup screen. You can select any of the items in the left frame of the screen, such as PCI Sub-System Settings, ACPI Settings, CPU Configuration, SATA Configuration, USB Configuration, Intel TXT Configuration and a SuperIO configuration. Selecting one of these set-up items will take you to a configuration sub menu for that item.



Aptio Setup Utility – Copyright © 2013 American Megatrends Inc.

Main	**Advanced**	Chipset	Boot	Security	Save & Exit	Event Logs

	PCI, PCI-X and PCI Express Settings
AMI Debug Rx Enabled!	
▶ **PCI Subsystem Settings**	
▶ Trusted Computing	
▶ WHEA Configuration	
▶ CPU Configuration	
▶ SATA Configuration	
▶ Thermal Configuration	
▶ Intel® Rapid Start Technology	
▶ PCH-FW Configuration	
▶ Intel® Anti-Theft Technology Configuration	
▶ AMT Configuration	
▶ Acoustic Management Configuration	→← : Select Screen
▶ USB Configuration	↑↓ : Select Item
▶ SMART Settings	Enter: Select
▶ Super IO Configuration	+/- : Change Opt.
▶ Platform Misc. Configuration	F1 : General Help
▶ Intel® Bios Guard Technology	F2 : Previous Values
▶ Serial Port Console Redirection	F3 : Optimized Defaults
▶ Intel ICC	F4 : Save & Exit
▶ Intel® RC Drivers Detail	ESC : Exit

Version 2.16.1240, Copyright © 2013 American Megatrends, Inc

PCI Sub-System Settings

A number of PCI Express, PCI-X and PCI device settings are available for configuration with this BIOS parameter. Specific device availability depends on what the BIOS can see during the system boot process. This setting is used to optimize the operations of off-board cards or devices that interact with the SHB and the SHB's BIOS. Listed below are all the available BIOS settings for board's PCI bus driver and the PCI Express link interfaces.

Option	Description
PCI Subsystem Settings	
PCI Bus Driver Version	V2.05.02 (This is a static message, informational only, no user selectable option)
PCI 64bit Resources Handling	
Above 4G Decoding	**Disabled**/Enabled ***(bold** = default setting)* – The system design needs to support 64-bit PCI decoding for this setting to be meaningful. Enabling the setting allows the SHB to decode the 64-bit capable devices connected to the SHB the 4G-address space. Use caution when enabling this system BIOS parameter.
PCI Common Settings	
PCI Latency Timer	Timer value selections available: **32 PCI Bus Clocks**, 64 PCI Bus Clocks, 96 PCI Bus Clocks, 128 PCI Bus Clocks, 160 PCI Bus Clocks, 192 PCI Bus Clocks, 224 PCI Bus Clocks, 248 PCI Bus Clocks
VGA Pallet Snoop	**Disabled**/Enabled
PERR# Generation	**Disabled**/Enabled
SERR# Generation	Disabled/Enabled
PCI Express Settings	There are several sections associated with this BIOS parameter setting as shown below. Short operational descriptions for each setting can be found in the upper left corner of the BIOS set-up screen. PCI Express Device Register Settings Relaxed Ordering: **Disabled**/*Enabled* **(bold** = default setting) Extended Tag: **Disabled**/Enabled No Snoop: Disabled/**Enabled** Maximum Payload: **Auto**, 128 Bytes, 256 Bytes, 512 Bytes, 1024 Bytes, 2048Bytes, 4096 Bytes Maximum Read Request: **Auto**, 128 Bytes, 256 Bytes, 512 Bytes, 1024 Bytes, 2048Bytes, 4096 Bytes PCI Express Link Register Settings ASPM Support: **Disabled/**Enabled/Force L0s WARNING: Enabling ASPM may cause some PCI-E devices to fail Extended Sync: **Disabled**/Enabled Clock Power Management: **Disabled**/Enabled Link Training Retry: Disabled, 2, 3, **5** Link Training Timeout: 10 – 1000 usec with **100 usec** being the default value Unpopulated Links: **Keep Link On**, Disabled Restore PCIE Registers: **Disabled**/Enabled

WHEA Configuration

This BIOS parameter enables the Windows Hardware Error Architecture which provides support for hardware error reporting and recovery available in Windows Server 2008 and other more recent Microsoft operating systems.

Option	Description
WHEA Support	Disabled/**Enabled (bold** = default setting)

CPU Configuration

The parameters for the specific Haswell processor installed on your SHB are displayed on the top portion of this sub-menu. The lower portion of this screen contains processor features that you may elect to enable or disable based on the unique requirements of your system. Here is a partial listing of some of these CPU parameters.

Option	Description
CPU Configuration	
	Intel® Xeon® E5-1225 v3 CPU * 3.20GHz (status message based on installed processor)
CPU Signature	306c3 (status message based on installed processor)
Microcode Patch	17 (status message based on installed processor)
Max CPU Speed	3200MHz (status message based on installed processor)
Min CPU Speed	800MHz (status message based on installed processor)
CPU Speed	3400MHz (status message based on installed processor)
Processor Cores	4 (status message based on installed processor)
Intel HT Technology	Supported (status message based on installed processor)
Intel VT-x Technology	Supported (status message based on installed processor)
Intel SMX Technology	Supported (status message based on installed processor)
64-bit	Supported (status message based on installed processor)
EIST Technology	Supported (status message based on installed processor)
CPU C3 state	Supported (status message based on installed processor)
CPU C6 state	Supported (status message based on installed processor)
CPU C7 state	Supported (status message based on installed processor)
L1 Data Cache	32kb x4 (status message based on installed processor)
L1 Code Cache	32kb x4 (status message based on installed processor)
L2 Cache	256kb x4 (status message based on installed processor)
L3 Cache	8192 x4 (status message based on installed processor)
Intel® Hyper-Threading	Disabled/**Enabled (bold** = default setting) This option allows the user to enable or disable Intel® Hyper-Threading support on the Intel® Xeon® E5-1275 v3 processor. **NOTE:** The Intel® Xeon® E5-1225 v3 and the Intel® Core™ i5-4590S embedded Haswell processors do not support Intel® Hyper-Threading.
Active Processor Cores	**All**, 1, 2. 3 With this setting you may use all of the available cores available in the Intel® Intel® Xeon® E5-1275 v3 processor or on use a subset of the available CPU execution cores. The default setting for this option is “ALL” and the number of cores to select depends on the specific processor installed on the SHB.
Overclocking lock	**Disabled**/Enabled
Limit CPUID Maximum	**Disabled**/Enabled
Execute Disable Bit	Disabled/**Enabled**
Intel Virtualization Technology	Disabled/**Enabled** This option allows the user to enable or disable Intel® Virtualization Technology support on the Intel® Core™ i7-3770 processor. Other Haswell or Haswell processors may or may not support Virtualization Technology
Hardware Prefetcher	Disabled/**Enabled**
Adjacent Cache Line Prefetch	Disabled/**Enabled**
CPU AES	Disabled/**Enabled**
Boot performance mode	Max Non-Turbo Performance/Max Battery/**Turbo Performance**
EIST	Disabled/**Enabled**
Turbo Mode	Disabled/**Enabled**
Energy Performance	**Performance**/Balanced Performance/Balanced Energy/Energy Efficient
Package power limit lock	Disabled/**Enabled**
Cpu Power Limit1	**0** [acceptable range 0 – 255]
Cpu Power Limit1 Time	**0** [acceptable range 0 – 255]
Cpu Power Limit2	**0** [acceptable range 0 – 255]
Platform power limit lock	Disabled/**Enabled**
Cpu Power Limit3	**0** [acceptable range 0 – 255]
Cpu Power Limit3 Time	**0** [acceptable range 0 – 255]
Cpu Power Limit3 Duty Cycle	**100** [acceptable range 0 – 100]
DDR Power Limit1	**0** [acceptable range 0 – 255]
DDR Power Limit1 Time	**0** [acceptable range 0 – 255]

DDR Power Limit2	**0** [acceptable range 0 – 255]
1-Core Ratio Limit	**0** [acceptable range 0 – 255]
2-Core Ratio Limit	**0** [acceptable range 0 – 255]
3-Core Ratio Limit	**0** [acceptable range 0 – 255]
4-Core Ratio Limit	**0** [acceptable range 0 – 255]
VR Current value lock	Disabled/**Enabled**
VR Current value	**0** [acceptable range 0 – 255]
CPU C states	Disabled/**Enabled**
Enhanced C1 state	Disabled/**Enabled**
CPU C3 Report	Disabled/**Enabled**
CPU C6 report	Disabled/**Enabled**
C6 Latency	**Short**/Long
CPU C7 report	Disabled/CPU 7/**CPUc7s**
C7 Latency	Short/**Long**
C1 state auto demotion	Disabled/**Enabled**
C3 state auto demotion	Disabled/**Enabled**
Package C state demotion	**Disabled**/Enabled
C1 state auto undemotion	Disabled/**Enabled**
C3 state auto undemotion	Disabled/**Enabled**
Package C state undemotion	**Disabled**/Enabled
C state Pre-Wake	Disabled/**Enabled**
CFG lock	Disabled/**Enabled**
Package C State limit	C0/C1,C2,C3,C6, C7, C7s,**Auto**
LakeTiny Feature	**Disabled**/Enabled
TCC Activation offset	**0** (Offset form factor TCC activation temperature)
Intel TXT(LT) Support	**Disabled**/Enabled
ACPI T State	**Disabled**/Enabled
CPU DTS	**Disabled**/Enabled
IOUT OFFSET Sign	**0** [acceptable range 0 – 255]
IOUT OFFSET	**0** [acceptable range 0 – 255]
IOUT SLOPE	**512** [acceptable range 0 – 1023]
Debug Interface	**Disabled**/Enabled
Debug Interface Lock	**Disabled**/Enabled

SATA Configuration

This is where you can set the parameters for the SATA devices that SHB's BIOS senses during the boot process. All SATA ports support SATA 3.0, SATA 2.0 and SATA 1.0 devices. As a reminder, SATA 3.0 devices support a maximum data transfer rate of 600MB/s data transfers, while SATA 2.0 = 300MB/s and SATA 1.0 = 150MB/s data transfers. What follows is a list of SATA port configuration parameters.

Option	Description
SATA Controller(s)	Disabled/**Enabled (bold** = default setting) - Short operational descriptions for each sub-menu setting can be found in the upper left corner of the BIOS set-up screen.
SATA Mode Selection	IDE/**AHCI**/RAID
SATA Mode Selection	**AHCI**/RAID
Aggressive LPM Support	Disabled/**Enabled** (Enables PCH to aggressively enter link power state)
SATA Controller Speed	**Default**/Gen1/Gen2/Gen3
►Software Feature Mask Configuration (sub-menu)	RAID0: Disabled/**Enabled**
	RAID1: Disabled/**Enabled**
	RAID10: Disabled/**Enabled**
	RAID5: Disabled/**Enabled**
	Intel Rapid Recovery Technology: *Disabled/**Enabled***
	OROM UI and BANNER: *Disabled/**Enabled***
	HDD Unlock: Disabled/**Enabled**
	LED Locate: Disabled/**Enabled**
	IRRT Only on eSATA: *Disabled/**Enabled***
	Smart Response Technology: *Disabled/**Enabled***
	OROM UI Delay: **2seconds**/4seconds/6seconds/8seconds
Serial ATA Port n (n= 0,1,2,3,4 or 5)	Software Preserve: Static diagnostic message, message depends on SATA drive connection upon boot, **Unknown** can be expected if no drive is present during system boot
	Port 0: Disabled/**Enhanced**
	Hot Plug: **Disabled**/Enhanced
	External SATA: **Disabled**/Enhanced
	SATA Device Type: **Hard Disk Drive**/Solid State Drive
	Spin Up Device: **Disabled**/Enhanced

Thermal Configuration

Thermal over-temp conditions are sensed in a number of locations on the SHB. This BIOS setup screen allows you to choose temperature thresholds and how you would like these potential error conditions to be reported in order for the system to take any necessary corrective actions.

Option	Description
Automatic Thermal Reporting	Disabled/**Enabled (bold** = default setting)
Critical Trip Point	**POR** – POR is the Plan of Record temperature value for the ACPI critical trip point. This is temperature limit in which the ACPI will shut down the O/S if the POR value is exceeded. The POR value varies by processor, but 74°C is a typical Tcase maximum temperature rating for processors like the Intel$^{®}$ Xeon$^{®}$ E5-1275 v3.
Active Trip Point 0	Disabled, 15C, 23C, 31C, 39C, 47C, 55C, 63C, **71C**, 79C, 87C, 5C, 103C, 111C, 119C
Active Trip Point 0 Fan Speed	**100**, 0[fan off]-100[maximum fan speed] (valid range input)
Active Trip Point 1	Disabled, 15C, 23C, 31C, 39C, 47C, **55C**, 63C, 71C, 79C, 87C, 5C, 103C, 111C, 119C
Active Trip Point 1 Fan Speed	**75**, 0-100 (valid range input)
Passive Trip Point	**95C**, This is the ACPI trip point where the O/S will begin throttling the processor
Passive TC1 Value	**1**, 1-16 (valid range input)
Passive TC2 Value	**5**, 1-16 (valid range input)
Passive TSP Value	**10**, 2-32 (valid range input in tenths of a second where the O/S will read the CPU temp)
PCH Thermal Device	**Disabled**/Enabled

Intel® Rapid Start Technology Configuration

The system default for this feature is disabled. The following BIOS parameters become visible if you elect to enable the feature.

Option	Description
Intel(R) Rapid Start Technology	**Disabled**/Enabled **(bold** = default setting) Static message - No valid iFFS partition found.
Entry on S3 RTC Wake	**Disabled**/Enabled
Entry After	Immediately, 1minute, 2minutes, 3mins., 5mins., **10mins.**, 15mins., 30mins., 1hr., 2hrs.
Active Page Threshold Support	**Disabled**/Enabled
Active Memory Threshold	**0:** Value in MB, when set to 0 this is the automatic mode and the BIOS will check if the partition size is large enough at S3 entry
Hybrid Hard Disk Support	**Disabled**/Enabled
RapidStart Display Save/Restore	**Disabled**/Enabled
RapidStart Display Type	**BIOS/Save Restore**, DeskTop/Save Restore
RapidStart enable NVME support	**Disabled**/Enabled
RapidStart whole memory check	Disabled/Enabled
RapidStart scan zero page	Disabled/**Enabled**
RapidStart performance monitor	**Disabled**/Enabled
RapidStart store search type	**Intel AHCI/RAID controller**, PCIE AHCI/NVRAM controller

Platform Controller Hub (PCH) Firm Ware (FW) Configuration

This menu configures the operational parameters for the management engine technology features of the boards' PCH. Note: Status messages may vary based on a specific SHB build.

Option	Description
ME FW Version	9.1.20.1035 (status message)
ME Firmware Mode	Normal mode, (status message)
ME Firmware Type	Full SKU Firmware (status message)
ME Firmware SKU	5MB (status message)
PTT Capability/State	(status message)
MDES BIOS Status Code	**Disabled**/Enabled
►Firmware Update Configuration (submenu)	
Me FW Image Re-Flash	**Disabled**/Enabled

Intel® Anti-Theft Technology (TXT) Configuration

With this BIOS setup screen you can enable or disable the Intel Anti-Theft Technology features supported by the SHB.

Option	Description
Intel Anti-Theft Technology	Disabled/**Enabled (bold** = default setting)
Enter Intel(R) AT Suspend Mode	**Disabled**/Enabled

AMT Configuration

The processor's Intel Advanced Management Technology or AMT is *Enabled* by default. The configuration settings available when Intel AMT is *Enabled* are listed below.

Option	Description
Intel AMT	Disabled/**Enabled (bold** = default setting)
BIOS Hotkey Pressed	**Disabled**/Enabled
MEBx Selection Screen	Disabled/Enabled
Hide Un-Configure ME Confirmation Prompt	Disabled/Enabled
MEBx Debug Message Output	Disabled/Enabled
Un-Configure ME	Disabled/Enabled
Amt Wait Timer	**0**, (0-65535 is the acceptable range for this setting)
ASF	Disabled/**Enabled**
Activate Remote Assistance Process	Disabled/**Enabled**
USB Configure	Disabled/**Enabled**
PET Progress	Disabled/**Enabled**
AMT CIRA Timeout	**0**, (fixed)
WatchDog	**Disabled**/Enabled
OS Timer	**0**, (0-65535 is the acceptable range for this setting/only visible if watchdog is enabled)
BIOS Timer	**0**, (0-65535 is the acceptable range for this setting/only visible if watchdog is enabled)

Acoustic Management Configuration

Option	Description
Automatic Acoustic Management	**Disabled/**Enabled **(bold** = default setting)
Serial ATA Port n (n= 0,1,2,3,4 or 5)	Port is Empty (Status message)
	Acoustic Mode: **Bypass**/Quite/Max Performance
	Acoustic Mode: **Not Supported**
	Acoustic Mode: **Not Available**

USB Configuration

The top portion of the menu screen lists the USB devices detected by the BIOS. The lower portion has several sub-menu selections available where you can set the parameters for the USB devices.

Option	Description
USB Devices	1 Keyboard, 2 Hubs – Status message that is variable based on the USB devices connected to the system and read by the BIOS on boot-up
Legacy USB Support	Disabled/**Enabled/**Auto
XHCI Hand-off	Disabled/**Enabled**
EHCI Hand-Off	**Disabled**/Enabled
USB Mass Storage Driver Support	Disabled/**Enabled**
USB Hardware Delays and Timeouts	The following sub-menu selections are used to configure data transfer delays and timeouts needed for the USB storage devices used in the system design: USB Transfer Timeout: 1 sec, 5 sec, 10 sec, **20sec** Device Reset Timeout: 10sec, **20sec**, 30sec, 40sec Device Power-Up Delay: ***Auto***, *Manual* -- If manual is selected the available options in seconds are 1-40secs with 5secs as the default value Device power-up delay in seconds: **5**

SMART Settings

Option	Description
SMART Self Test	**Disabled**/Enabled **(bold** = default setting)

Super IO Configuration

The one Super IO component on the THD8141 supports the SHB's PS/2 mouse and keyboard ports as well as Serial Port 1 and Serial Port 2. Later BIOS revisions support a second Super I/O chip located on an optional IOB33 or MPE40* module. These later BIOS revisions enable an option module to plug into the SHBs' P20A in the case of the IOB33, or P20A and P20B for the MPE40. These I/O Expansion connectors provide additional device I/O and display monitor connectivity to the system designer. The Super IO Configuration submenu that will be displayed will depend on the SHB's BIOS revision and if an IOB33 or MPE40 is connected to P20A/P20B. This Advanced Setup sub-menu allows you to configure the system ports connected to the board's Super I/O component(s).

Option	**Description**
Super IO Configuration	LPC47B272 **(**status message)
SIO Chip Location	**IOB** When Present**/IOB/OnBoard (**bold** = default setting)

*The MPE40 option module is in development. Contact Trenton for latest availability status.

**The IOB notation may also be used by the BIOS when an MPE40 is installed on the THD8141.

►Floppy Disk Controller Configuration (Super IO sub-menu)

When available, this option will be the first sub-menu seen on the Super IO configuration page and allow you to enable or disable the floppy drive controller on your platform.

Option	**Description**
Disabled	*Set this value to prevent the BIOS from detecting the onboard floppy drive controller.*
Enabled (default)	*Set this value to allow the BIOS to use the onboard floppy drive controller to control selected floppy drive operational parameters. This is the default setting.*
	Device settings Reset Required (status message)
Change Settings	***Auto****, IO-3F0h;IRQ=6;DMA=2, IO=3F0h; IRQ=3,4,5,6,7,10,12;DMA=1,2,3; IO=370h; IRQ=3,4,5,6,7,10,12;DMA=1,2,3*
Device Mode	***Read Mode****, Write Protect*

NOTE: Floppy port functionality is not supported in the current THD8141 BIOS revision.

►Serial Port 0 Configuration (Super IO sub-menu)

This option specifies the base I/O port address and Interrupt Request address of serial port 1 located on header connector P7 on the THD8141. The Optimal setting is *3F8/IRQ4*, but you do have the ability to change this setting with the Change Settings parameter. The Fail-Safe default setting is *Auto*.

Option	**Description**
Serial Port	Disabled/**Enabled**
	Device settings IO=3F8h; IRQ=4 (status message)
Change Settings	**Auto --** IO=3F8h IRQ4 -- IO=3F8h; IRQ3, 4, 5, 6, 7, 10, 11, 12 -- IO=2F8h; IRQ3, 4, 5, 6, 7, 10, 11, 12 -- IO=3E8h; IRQ3, 4, 5, 6, 7, 10, 11, 12 -- IO=2E8h; ; IRQ3, 4, 5, 6, 7, 10, 11, 12
Device Mode	**Normal**, High Speed

►Serial Port 1 Configuration (Super IO sub-menu)

These BIOS setup parameters are for the SHB's serial port 2 available on header connector P14. Most of the BIOS settings are identical to the ones described in the Serial Port 0 Configuration section.

Option	**Description**
Serial Port	Disabled/**Enabled**
	Device settings IO=2F8h; IRQ=3 (status message)
Change Settings	**Auto** -- IO=2F8h; IRQ3 -- IO=3F8h; IRQ3, 4, 5, 6, 7, 10, 11, 12 -- IO=2F8h; IRQ3, 4, 5, 6, 7, 10, 11, 12 -- IO=3E8h; IRQ3, 4, 5, 6, 7, 10, 11, 12 -- IO=2E8h; IRQ3, 4, 5, 6, 7, 10, 11, 12
Device Mode	**Normal**, High Speed

►Parallel Port Address (Super IO sub-menu)

This option specifies the I/O address used by the parallel port. The Optimal setting is *378h*. The Fail-Safe setting is *Auto*.

Option	Description
Parallel Port	Disabled/**Enabled**
	Device settings IO=378h; IRQ=5 (status message)
Change Settings	**Auto --** IO=378h; IRQ5 -- IO=378h; IRQ3, 4, 5, 6, 7, 10, 11, 12 -- IO=3BCh; IRQ3, 4, 5, 6, 7, 10, 11, 12 -- IO=378h -- IO=278h -- IO=3BCh
Device Mode	**STD Printer Mode**, SPP Mode, EPP-1.9 and SPP Mode, EPP-1.7 and SPP Mode, ECP Mode, ECP Mode and EPP 1.9 Mode, ECP and EPP 1.7 Mode

The Device Mode parameter enables you to select either the standard printer mode (STD) or a variation of the SPP, EPP or SCP parallel printer mode of operation. Any application still using a parallel printer will likely use the *STD Printer Mode*.

Platform Misc. Configuration

Option	Description
Native PCIE Enable	**Disabled**/Enabled **(bold** = default setting)
Native ASPM	**Disabled**/Enabled **(**only visible if native PCIe is enabled)
ACPI Debug	Disabled/Enabled
PTID Support	Disabled/Enabled
PECI Access Method	Direct I/O or ACPI

Intel® BIOS Guard Technology

Option	Description
Intel BIOS Guard Support	Disabled/**Enabled (bold** = default setting)

Serial Port Console Redirection

Option	Description
COM0	
Console Redirection	**Disabled**/Enabled **(bold** = default setting)
Console Redirection Settings	(Status message, settings specify how the host and the remote computers will communicate, both devices must have compatible serial port settings)
COM1	
Console Redirection	**Disabled**/Enabled
Console Redirection Settings	(Status message, settings specify how the host and the remote computers will communicate, both devices must have compatible serial port settings)
Console Redirection	Disabled/**Enabled** ►Console Redirection Settings Submenu Out-of-Band Mgmt Port: ***COM0*** Terminal Type: VT100/VT100+/**VT-UTF8**/ANSI Bits per second: 9600/19200/57600/**115200** Flow Control: **None**, Hardware CTS/RTS, Hardware Xon/Xoff Data Bits Parity Stop Bits

NOTE: The THD8141 BIOS does not currently support serial port console redirect and IDE-R functionality in Intel® AMT applications.

Enabled (Intel ICC)

The BIOS parameters listed for the **Enabled** function offer several operational settings related to how to implement the ICC or Integrated Clock Control function in the SHB's ME (Management Engine) firmware.

Option	Description
Use Watchdog Timer for ICC	**Disabled**/Enabled **(bold** = default setting)
Turn off unused PCI/PCIe clocks	Disabled/**Enabled**
ICC Locks after EOP	Default/**All Locked**/All Unlocked
ICC Profile	0
Clock Manipulation	
ICC Overclocking Lib	

Intel RC Drivers Version Detail

The BIOS parameters listed below are informational only and list the version string for each particular driver. The information below may vary as a function of the board build.

Option	Description
Intel CPU RC Version	**1.1.0.0 (**Static message – informational only, no user configuration settings)
Intel SA RC Version	**1.1.0.0 (**Static message – informational only, no user configuration settings)
Intel PCH RC Version	**1.1.0.0 (**Static message – informational only, no user configuration settings)
Intel ME RC Version	**1.1.0.0 (**Static message – informational only, no user configuration settings)
Intel RST RC Version	**1.1.0.0 (**Static message – informational only, no user configuration settings)

This page intentionally left blank

Chapter 3 Chipset Configuration Setup

Introduction

The term "chipset" is a bit of a misnomer for the Trenton THD8141. The "chipset" on this SHB is a single component called a "Platform Controller Hub" or PCH. Some of the traditional "chipset" functions specifically the system memory interfaces and the A0, A2, A3 and PCI Express Expansion links to a PICMG 1.3 backplane have migrated up into the Haswell processor's micro-architecture. The THD8141 features the Intel® C226 PCH and this platform controller hub merges the former South Bridge chipset component functionality with the North Bridge functionality not handled by the Haswell processor. The following sections cover the new set-up parameters for the single chip Intel® C226 PCH and are labeled: PCH-IO Configuration and System Agent (SA) Configuration

PCH-IO Configuration

Several system I/O and PCI Express configurations are included in this area of the BIOS. Once selected, several static messages and sub-menus of the PCH-IO configuration become visible.

Option	Description
Intel PCH RC Version	1.1.0.1 **(**Static message – informational only, no user configuration settings)
Intel PCH SKU Name	C226 **(**Static message – informational only, no user configuration settings)
Intel PCH Rev ID	05/c2 **(**Static message – informational only, no user configuration settings)
►PCI Express Configuration (submenu)	PCI Express Clock Gating: *Disabled/**Enabled*** DMI Link ASPM Control: *Disabled/**Enabled*** DMI Link Extended Synch Control: **Disabled**/Enabled Subtractive Decode: **Disabled**/Enabled Subtractive Decode: 0 [0 - 7] ►PCI Express Root Port 1 ►PCI Express Root Port 2 ►PCI Express Root Port 3 ►PCI Express Root Port 4 ►PCI Express Root Port 5 ►PCI Express Root Port 6 ►PCI Express Root Port 7 PCIE Port 8 is assigned: *Static Message, no user configuration settings* PCIe ports 1 through 8 sub-menu configuration settings if available PCI Express Root Port: *Disabled/**Enabled*** ASPM Support: *Disabled/L0s/L1/L0sL1/**Auto*** L1 Substates: Disabled/L1.1/L1.2/**L1.1 & L1.2** URR: **Disabled**/Enabled FER: **Disabled**/Enabled NFER: **Disabled**/Enabled CER: **Disabled**/Enabled CTO: **Disabled**/Enabled SEFE: **Disabled**/Enabled SENFE: **Disabled**/Enabled SECE: **Disabled**/Enabled PME SCI: Disabled/**Enabled** Hot Plug: **Disabled**/Enabled PCIe Speed: **Auto**/Gen1/Gen2 Detect Non-Compliance Device: **Disabled**/Enabled (only visible if PCIe Speed = Auto) Extra Bus Reserved: **0** (Acceptable values = 0 – 7) Reserved Memory: **10** (Acceptable values = 1 – 20) Prefetchable Memory: **10** (Acceptable values = 1 – 20) Reserved I/O: **4** (Acceptable values = 4 – 20) PCIE LTR: Disabled/**Enabled** PCIELTR Lock: Disabled/**Enabled** Snoop Latency: Ocerride: *Disabled/Manual/**Auto***
►USB Configuration (submenu)	USB Precondition: ***Disabled**/Enabled* XHCI Mode: **Smart Auto**/Auto/Enabled/Disabled BTCG: Disabled/**Enabled**

	EHCI1: Disabled/**Enabled** EHCI2: Disabled/**Enabled** USB Ports Per-Port Disable Control: **Disabled**/Enabled (If enabled then the following selections become visible) USB Port #0 Disable: *Disabled/**Enabled*** USB Port #1 Disable: *Disabled/**Enabled*** USB Port #2 Disable: *Disabled/**Enabled*** USB Port #3 Disable: *Disabled/**Enabled*** USB Port #4 Disable: *Disabled/**Enabled*** USB Port #5 Disable: *Disabled/**Enabled*** USB Port #6 Disable: *Disabled/**Enabled*** USB Port #7 Disable: *Disabled/**Enabled*** USB Port #8 Disable: *Disabled/**Enabled*** USB Port #9 Disable: *Disabled/**Enabled*** USB Port #10 Disable: *Disabled/**Enabled*** USB Port #11 Disable: *Disabled/**Enabled*** USB Port #12 Disable: *Disabled/**Enabled*** USB Port #13 Disable: *Disabled/**Enabled***
►PCH Azalia Configuration (submenu)	Azalia: Disabled/Enabled/**Auto** Azalia Docking Support: **Disabled**/Enabled (only visible if Azalia = Auto or Enabled) Azalia PME: **Disabled**/Enabled (only visible if Azalia = Auto or Enabled)
►BIOS Security Configuration (submenu)	BIOS Security Configuration SMI Lock: Disabled/**Enabled** BIOS Lock: **Disabled**/Enabled GPIO Lock: **Disabled**/Enabled BIOS Interface Lock: Disabled/**Enabled** RTC Lock: Disabled/**Enabled**
Toggle EC	**Disabled**/Enabled
PCH LAN Controller	Disabled/**Enabled (bold** = default setting)
Wake on LAN	**Disabled**/Enabled
Wake of WLAN Enable	Disabled/**Enabled**
Wake of WLAN Enable From DeepSx	**Disabled**/Enabled
DeepSx Power Policies	**Disabled,** Enabled in S5, Enabled in S4-S5
GP27 Wake From DeepSx	**Disabled**/Enabled
PCIE Wake From DeepSx	**Disabled**/Enabled
EC Turbo Control Mode	**Disabled**/Enabled
CLKRUN# Logic	Disabled/**Enabled**
Serial IRQ Mode	**Quite**/Continuous
SB CRID	**Disabled**/Enabled
SLP_S4 Assertion Width	Disabled/1-2 seconds/2-3 seconds/3-4 seconds/**4-5 seconds**
Restore AC Power Loss	Power Off/Power On/**Last State**
Port 80h Redirection	**LPC Bus**/PCIE Bus
NFC Device	**Disabled**/Enabled

System Agent (SA) Configuration

Several system additional PCI Express configurations as well as graphics and memory configurations are included in this area of the BIOS. Once selected, several static messages and sub-menus of the System Agent (SA) configuration become visible.

Option	Description
System Agent Bridge Name	Haswell **(**Static message – informational only, no user configuration settings)
System Agent RC Version	1.1.0.0 **(**Static message – informational only, no user configuration settings)
VT-d Capability	Supported **(**Static message – informational only, no user configuration settings)
VT-d	Disabled/**Enabled (bold** = default setting)
CHAP Device (B0:D7:F0)	**Disabled**/Enabled
Thermal Device (B0:D4:F0)	**Disabled**/Enabled
CPU SA Audio Device (B0:D3:F0)	Disabled/**Enabled**
Enable NB CRID	Disabled/**Enabled**
X2ACPI Opt Out	Disabled/**Enabled**
►Graphics Configuration	IGFX VBIOS Version: 2179 (Status Message, result depends on board configuration) IGfx Frequency: 700MHz (Status Message, result depends on board configuration) Graphics Turbo IMON Current: **31** (**bold** = default setting, supported values = 14 to 31) Skip External Gfx Card: **Disabled**/Enabled Primary Display: **Auto/**IGFX/PEG/PCIE Primary PEG: **Auto**/PEG11/PEG12 Primary PCIE: **Auto**/PCIE1/PCIE2/PCIE3/PCIE4/PCIE5/PCIE6/PCIE7 Internal Graphics: **Auto/** Disabled/Enabled Aperture Size For HAS: 128MB/**256MB/**512MB/1024MB/2048MB/4096MB CD Clk Frequency: 337.5MHz/450MHz/**540MHz**/675MHz/Auto DVMT Pre-Allocated: **32MB/**64MB/96MB/128MB/160MB/192MB/224MB/256MB/288MB 320MB/352MB/384MB/416MB/448MB/480MB/512MB/1024MB/2016MB ALS Support: Disabled/**Enabled** DVMT Total Gfx Mem: **128MB**/256MB/MAX) Gfx Low Power Mode: Disabled/**Enabled** Panel Power Enable: **Disabled**/Enabled ►LCD Control Primary IGFX Boot Display: **VBIOS Default** (**VBIOS Default**, CRT, EFP, LFP, EFP3, EFP2, LFP2) LCD Panel Type: **VBIOS Default** (**VBIOS Default**, 640x480 LVDS, 800x600 LVDS, 1024x768 LVDS1, 1280x1024 LVDS, 1400x1050(RB) LVDS1, 1400x1050 LVDS2,1600x1200 LVDS, 1366x768 LVDS, 1680x1050 LVDS, 1920x1200 LVDS, 1440x900 LVDS, 1600x900 LVDS, 1024x768 LVDS2, 1280x800 LVDS,1920x1080 LVDS, 2048x1536 LVDS) SDVO-LFP Panel Type: **VBIOS Default** (**VBIOS Default**, 1024x768 SVDO-LFP, 1280x1024 SVDO-LFP, 1400x1050 SVDO-LFP, 1600x1200 SVDO-LFP) Panel Scaling: **Auto** (**Auto**, Off, Force Scaling) Backlight Control: **PWM Normal** (PWM Inverted, **PWM Normal**, GMBUS Inverted, GMBUS Normal) BIA: **Auto** (**Auto**, Disabled, Level 1, Level 2, Level 3, Level 4, Level 5) Spread Spectrum clock Chip: ***Off*** *(**Off**, Hardware, Software)* TV1 Standard: **VBIOS Default** (**VBIOS Default**, NTSC_M, NTSC_M_J, NTSC_433, PAL_B, PAL_G, PAL_D, PAL_H, PAL_I, PAL_M, PAL_N, SECAM_L, SECAM_B, SECAM_D, SECAM_G, SECAM_H, SECAM_K, DTV_STD_SMPTE_240M_1080i59, HDTV_STD_SMPTE_240M_1080i60, HDTV_STD_SMPTE_295M_1080i50, HDTV_STD_SMPTE_295M_1080p50, HDTV_STD_SMPTE_296M_720p50, HDTV_STD_SMPTE_296M_720p60, HDTV_STD_CEAEIA_7702A_480p60, HDTV_STD_CEAEIA_7702A_480i60)

	TV2 Standard: **VBIOS Default** (**VBIOS Default**, NTSC_M, NTSC_M_J, NTSC_433, PAL_B, PAL_G, PAL_D, PAL_H, PAL_I, PAL_M, PAL_N, SECAM_L, SECAM_B, SECAM_D, SECAM_G, SECAM_H, SECAM_K, DTV_STD_SMPTE_240M_1080i59, HDTV_STD_SMPTE_240M_1080i60, HDTV_STD_SMPTE_295M_1080i50, HDTV_STD_SMPTE_295M_1080p50, HDTV_STD_SMPTE_296M_720p50, HDTV_STD_SMPTE_296M_720p60, HDTV_STD_CEAEIA_7702A_480p60, HDTV_STD_CEAEIA_7702A_480i60) Active LFP: **eDP Port-A** (No LVDS, Int_LVDS, SDV0 LVDS, **eDP Port-A**, eDP Port-D) Panel Color Depth: **18 Bit** (**18 Bit**, 24 Bit)
►DMI Configuration	DMI: x4 GEN2 (Status Message, result depends on board configuration) DMI Vc1 Control: **Disabled**/Enabled **(bold** = default setting) DMI Vcp Control: Disabled/**Enabled** DMI Vcm Control: Disabled/**Enabled** DMI Link ASPM Control: **L0sL1** (Disabled, L0s, L1, **L0sL1**) DMI Extended Synch Control: **Disabled**/Enabled DMI Gen 2: Disabled/**Enabled** DMI De-emphasis Control: **-6db/-**3.5db DMI IOT: **Disabled**/Enabled
►NB PCIe Configuration	PEG0: x16 GEN2 (Status Message, result depends on board configuration) PEG0 - Gen X: **Auto** (**Auto**, GEN1, GEN2, GEN3) **(bold** = default setting) PEG1 - Gen X: **Auto** (**Auto**, GEN1, GEN2, GEN3) **(bold** = default setting) PEG2 - Gen X: **Auto** (**Auto**, GEN1, GEN2, GEN3) **(bold** = default setting) Run-time C7 Allowed: Disabled/**Enabled** Enable PEG: **Auto** (**Auto**, Enabled, Disabled) Detect Non-Compliance Device: **Disabled**/Enabled Program PCIe ASPM after OpROM: **Disabled**/Enabled PEG0 De-emphasis Control: ***-6dB (-6dB***, *-3.5dB)* PEG1 De-emphasis Control: ***-6dB (-6dB***, *-3.5dB)* PEG2 De-emphasis Control: ***-6dB (-6dB***, *-3.5dB)* PEG Sampler Calibrate: **Disabled** (Auto, Enabled, **Disabled**) Swing Control: **Full** (Reduced, Half, **Full**) Gen3 Equalization: Disabled/**Enabled** Gen3 Eq Phase 2: **Enabled** (Auto, **Enabled**, Disabled) PEG Gen3 Root Port Preset Value for each Lane: **4** (1 – 11 acceptable values for each of the 16 lanes) PEG Gen3 Endpoint Preset Value each Lane: **4** (1 – 11 acceptable values for each of the 16 lanes) PEG Gen3 Endpoint Hint Value each Lane: **2** (0-7 acceptable values for each of the 16 lanes) Gen3 Eq Preset Search: Disabled/**Enabled** Always re-search Gen3 Eq Preset: **Disabled**/Enabled Allow PERST# GPIO Usage: Disabled/**Enabled** Preset Search Dwell Time: **1000** (dwell time in ms) Timing Margin Steps: **2** (acceptable range = 1 to 255) Timing Start Margin: **15** (acceptable range = 4 to 255) Voltage Margin Steps: **2** (acceptable range = 1 to 255) Voltage Start Margin: **20** (acceptable range = 4 to 255) Favor Timing Margin: **Disabled**/Enabled Error Target: **1** (acceptable range = 1 to 65535) Generate BDAT PEG Margin Data: **Disabled**/Enabled PEG PCIe Compliance Testing Mode: **Disabled**/Enabled PEG RxCEM LoopBack Mode: **Disabled**/Enabled PEG Lane number for Test: **0** (acceptable range = 0 to 15) PCIe Gen3 RxCTLEp Setting: **2** (acceptable range = 0 to 15)
►Memory Configuration	Memory Information Memory RC Version: 1.8.0.0 (Status Message, result depends on board configuration) Memory Frequency: 1600MHz (Status Message, result depends on board configuration) Total Memory: 8192MB (DDR3) (Status Message, result depends on board configuration) Memory Voltage: 1.5V (Status Message, result depends on board configuration) DIMM#0: 4096MB (DDR3) (Status Message, result depends on board configuration) DIMM#1: Not Present (Status Message, result depends on board configuration)

	DIMM#2: 4096MB (DDR3) (Status Message, result depends on board configuration) DIMM#3: Not Present (Status Message, result depends on board configuration) CAS Latency (tCL): 11 (Status Message, result depends on board configuration) Minimum delay time CAS to RAS (tRCDmin): 11 **(**Static message – informational only, no user configuration settings) Row Precharge (tRPmin): 11 **(**Static message – informational only, no user configuration settings) Active to Precharge (tRASmin): 28 **(**Static message – informational only, no user configuration settings) XMP Profile 1: Not Supported **(**Static message – informational only, no user configuration settings) XMP Profile 2: Not Supported **(**Static message – informational only, no user configuration settings) DIMM profile: **Default DIMM Profile** (**Default DIMM Profile**, Custom Profile, XMP Profile 1, XMP Profile 2) **(bold** = default setting) Memory Frequency Limiter: **Auto** (**Auto**, 1067, 1333, 1600, 2133, 2400, 2667, 2933, 3200) ECC Support: Disabled/**Enabled** Max TOLUD: **Dynamic** (**Dynamic**, 1GB, 1.25GB, 1.5GB, 1.75GB, 2GB, 2.25GB, 2.5GB, 2.75GB, 3GB, 3.25GB) Enh Interleave Support: Disabled/**Enabled** RI Support: Disabled/**Enabled** DLL Weak Lock Support: Disabled/**Enabled** Mc Lock: Disabled/**Enabled** Ch Hash Support: Disabled/Enabled/**Auto** Ch Hash Mask: 12494 Ch Hash Interleaved Bit: BIT06/**BIT07**/BIT08/BIT09 NMode Support: **Auto** (**Auto**, 1N Mode, 2N Mode) Memory Scrambler: Disabled/**Enabled** RMT Crosser Support: **Disabled**/Enabled BDAT ACPI Table Support: **Disabled**/Enabled MRC Fast Boot: Disabled/**Enabled** DIMM Exit Mode: **Auto (Auto**, Slow Exit, Fast Exit) Power Down Mode: **Auto** (No Power Down, APD, PPD, PPD-DLLoff, **Auto**) Memory Remap: Disabled/**Enabled** Channel A DIMM Control: **Enable Both DIMMS** (**Enable Both DIMMS**, Disable DIMM0, Disable DIMM1, Disable Both DIMMS) Channel B DIMM Control: **Enable Both DIMMS** (**Enable Both DIMMS**, Disable DIMM0, Disable DIMM1, Disable Both DIMMS) GDXC Support: **Disabled**/Enabled ►Custom Profile Control (Sub-menu below main Memory Configuration is visible when DIMM Profile selection is set to Custom) Memory Timing Information: **(**Static message – informational only) Memory Frequency: **(**Static message – informational only) Memory Voltage: **(**Static message – informational only) CAS Latency (tCL): **(**Static message – informational only) CAS to RAS (tRCDmin): **(**Static message – informational only) Row Precharge (tRPmin): **(**Static message – informational only) Active to Precharge (tRASmin): **(**Static message – informational only) Write Recovery (tWRmin): **(**Static message – informational only) Refresh Recovery (tRFCmin): **(**Static message – informational only) Row Active to Row Active (tRRDmin): **(**Static message – informational only) Internal Write to Read Command (tWTRmin): **(**Static message – informational only) Internal Read to Precharge Command (tRTPmin): **(**Static message – informational only) Four Activate Window (tFAWmin): **(**Static message – informational only) Memory Timing Configuration Memory Frequency Limiter: 1066/**1333**/1600/1867/2133/2400/2667/2933/3200 DDR3 Voltage Selection: **Auto**/DDR3/DDR3L/DDR3LP tCL: 4 tRCD: 3 tRP: 3

	tRAS: 9 tWR: 5 tRFC: 15 tRRD: 4 tWTR: 3 tRTP: 4 tRC: 15 tFAW: 10 tCWL value: 5 tREFI value: 1
►Memory Thermal Configuration	Memory Thermal Configuration ►Memory Power and Thermal Throttling (sub-menu) DDR PowerDown and idle counter: **BIOS**/PCODE **(bold** = default setting) Refresh 2x Support: **Disabled**/Enabled for WARM or HOT/Enabled for HOT only LPDDR Thermal Sensor: Disabled/**Enabled** SelfRefresh Enable: Disabled/**Enabled** SelfRefresh IdleTimer: **512** Throttler CKEMin Defeature: **Disabled**/Enabled Throttler CKEMin Timer: 48 ►Dram Power Meter (sub-menu) User Power Weights Enable: **Disabled**/Enabled Energy Scale Fact: 4 Idle Energy Ch0Dimm0: 10 PowerDown Energy Ch0Dimm0: 6 Activate Energy Ch0Dimm0: 172 Read Energy Ch0Dimm0: 212 Write Energy Ch0Dimm0: 221 Idle Energy Ch0Dimm1: 10 PowerDown Energy Ch0Dimm1: 6 Activate Energy Ch0Dimm1: 172 Read Energy Ch0Dimm1: 212 Write Energy Ch0Dimm1: 221 Idle Energy Ch1Dimm0: 10 PowerDown Energy Ch1Dimm0: 6 Activate Energy Ch1Dimm0: 172 Read Energy Ch1Dimm0: 212 Write Energy Ch1Dimm0: 221 Idle Energy Ch1Dimm1: 10 PowerDown Energy Ch1Dimm1: 6 Activate Energy Ch1Dimm1: 172 Read Energy Ch1Dimm1: 212 Write Energy Ch1Dimm1: 221 ►Memory Thermal Reporting (sub-menu) Lock Thermal Management Registers: **Disabled**/Enabled Extern Therm Status: **Disabled**/Enabled Closed Loop Therm Manage: **Disabled**/Enabled Open Loop Therm Manage: **Disabled**/Enabled Thermal Threshold Settings Warm Threshold Ch0 Dimm0: 255 Warm Threshold Ch0 Dimm1: 255 Hot Threshold Ch0 Dimm0: 255 Hot Threshold Ch0 Dimm1: 255 Warm Threshold Ch1 Dimm0: 255 Warm Threshold Ch1 Dimm1: 255 Hot Threshold Ch1 Dimm0: 255 Hot Threshold Ch1 Dimm1: 255

	Thermal Throttle Budget Settings Warm Budget Ch0 Dimm0: 255 Warm Budget Ch0 Dimm1: 255 Hot Budget Ch0 Dimm0: 255 Hot Budget Ch0 Dimm1: 255 Warm Budget Ch1 Dimm0: 255 Warm Budget Ch1 Dimm1: 255 Hot Budget Ch1 Dimm0: 255 Hot Budget Ch1 Dimm1: 255 ►Memory RAPL (sub-menu) RAPL Power Floor Ch0: 0 RAPL Power Floor Ch1: 0 RAPL PL Lock: **Disabled**/Enabled RAPL PL 1 Enable: **Disabled**/Enabled RAPL PL 1 Power: 0 RAPL PL 1 WindowX: 0 RAPL PL 1 WindowY: 0 RAPL PL 2 Enable: **Disabled**/Enabled RAPL PL 2 Power: 222 RAPL PL 2 WindowX: 1 RAPL PL 2 WindowY: 10 ►Memory Thermal Manage: **Disabled**/Enabled
►GT - Power Management Control	GT Info: GT2 (700 MHz) **(**Static message – informational only, no user configuration settings) RC6(Render Standby): Disabled/**Enabled (bold** = default setting) GT OverClocking Support: **Disabled**/Enabled (If enabled the following two selections appear) GT OverClocking Frequency: 22 GT OverClocking Voltage: 0

This page intentionally left blank

Chapter 4 Boot Setup

Introduction

Select the *Boot Setup* menu item from the Aptio TSE screen to enter the BIOS Setup screen. The Boot menu option allows you to access the following the following boot setup features.

Boot Configuration

Set this value to instruct the system on how long it needs to wait for the setup activation key and turn On/Off the Bootup NumLock State.

Option	Description
Setup Prompt Timeout	**5 (bold** = default setting) A numeric value of 5 is the default setting with a range of 1 to 65355 entered is in seconds being valid inputs. A value of 65355 or FFFFh means an indefinite wait period
Bootup NumLock State	The default setting is ***On*** with an option to turn the setting *Off*. The *On* setting enables the keyboard to automatically enabled at system boot and allows the immediate use of the 10-key numeric keypad located on the right side of the keyboard. In the Off setting, the NumLock keyboard key will need to be pressed to use the 10-key numeric pad.
Quiet Boot	**Disabled**/Enabled
Fast Boot	**Disabled**/Enabled SATA Support: **HDD Only** (Last Boot HDD Only, All SATA Devices, **HDD Only**) VGA Support: **EFI Driver** (Auto, **EFI Driver**) USB Support: **Full Initial** (Disabled, **Full Initial**, Partial Initial) PS2 Devices Support: **Enabled** (Disable/**Enabled**) NetWork Stack Driver Support: ***Enabled*** *(Disable/**Enabled**)*
Driver Option Priorities	Driver Option Priorities Boot Option #1: **P4:ST3160316AS** (UEFI: Built-In EFI Shell, **P4:ST3160316AS**, Disabled) Boot Option #2: **UEFI: Built-In EFI Shell** (**UEFI: Built-In EFI Shell**, P4:ST3160316AS, Disabled) *Note: ST3160316AS is the boot drive identifier in this particular test lab set-up. Your particular boot drive identifier will be different*.
►CSM16 Parameters	CSM16 Module Version: 07:70 **(**Static message – informational only, no user configuration settings) *The following are special purpose BIOS settings and should remain in the default positions. Contact Trenton's technical support team if you need to use these BIOS settings.* GateA20 Active: **Upon Request** (**Upon Request**, Always) Option ROM Messages: **Force BIOS** (**Force BIOS**, Keep Current) INT19 Trap Response: **Immediate** (**Immediate**, Postponed)
►CSM Parameters	Launch CSM: Disabled/**Enabled** Boot option filter: **UEFI and Legacy** (**UEFI and Legacy**, Legacy Only, UEFI Only) Launch PXE OpROM policy: **Do Not Launch** (**Do Not Launch**, UEFI Only, Legacy Only) Launch Storage OpROM policy: **Legacy Only** (Do Not Launch, UEFI Only, **Legacy Only**) Launch Video OpROM policy: **Legacy Only** (Do Not Launch, UEFI Only, **Legacy Only**, Legacy First, UEFI First) Other PCI device ROM priority: **UEFI OpROM** (**UEFI OpROM**, Legacy OpROM)

This page intentionally left blank

Chapter 5 Security

Two Levels of Password Protection

Security Setup provides both an Administrator and User password. If you use both passwords, the Administrator password must be set first.

The system can be configured so that all users must enter a password every time the system boots or when Setup is executed, using either or either the Supervisor password or User password.

The Administrator and User passwords activate two different levels of password security. If you select password support, you are prompted for a one to six character password. Type the password on the keyboard. The password does not appear on the screen when typed. Make sure you write it down. If you forget it, you must drain NVRAM and reconfigure.

Remember the Password

Keep a record of the new password when the password is changed. If you forget the password, you must erase the system configuration information in NVRAM. See (Deleting a Password) for information about erasing system configuration information.

Security Configuration

The *Security* setup menu item allows the user to do the following:

Option	Description
Administrator Password	This option allows the user to set an administrative level password for the BIOS. BIOS access passwords must be between 3 and 20 characters in length.
User Password	This option allows the user to set a user level password for the BIOS.
HDD Security Configuration	This option allows the user to identify and secure a system's HDD such as the one we used in our test lab set-up: ST3160316AS
HDD Password	This option allows the user to set a user level password for a system's HDD: Security Supported: Yes Security Enabled: No Security Locked: No HDD User Pwd Status: Not Installed HDD Master Pwd Status: Installed Set User Password

This page intentionally left blank

Chapter 6 Saving and Exiting BIOS Setup and Restoring Defaults

Introduction
There are four methods of saving BIOS changes and leaving Aptio TSE listed at the top of this screen:

Save Changes & Exit
When you have completed the system configuration changes, select this option to save your BIOS changes and leave Aptio TSE. You will need to reboot the computer for the new system configuration parameters to take effect.

Select Save Changes & Exit from the Exit menu and press <Enter>.

Save Configuration Changes and Exit Now?

[YES] [NO] appears in the window. Select *YES* to save changes and exit.

Discard Changes & Exit
Select this option to quit Aptio TSE without making any permanent changes to the system configuration.

Select Discard Changes & Exit from the Exit menu and press <Enter>.

Discard Changes and Exit Setup Now?

[YES] [NO] Select *YES* to discard changes and exit.

Save Changes & Reset
When you have completed the system configuration changes, select this option to save the BIOS changes, leave Aptio TSE and reset the computer so the new system configuration parameters can take effect.

Select Save Changes & Reset from the Exit menu and press <Enter>.

Save Configuration Changes and Exit Now?

[YES] [NO] appears in the window. Select *YES* to save changes and reset.

Discard Changes & Reset
Choose this option if you decide to discard your BIOS changes, but what to reset the system upon leaving Aptio TSE.

Select Discard Changes & Reset from the Exit menu and press <Enter>.

Discard Configuration Changes and Exit Now?

[YES] [NO] appears in the window. Select *YES* to discard changes and reset.

Save Options
The following two screen options allow save or discard BIOS changes without leaving Aptio TSE:

Save Changes	[YES]	[NO]
Discard Changes	[YES]	[NO]

The following menu options for BIOS defaults are available:

Restore Defaults
Aptio TSE automatically sets all Aptio TSE options to a complete set of factory default settings when you select this option.

Select restore defaults from the Exit menu and press <Enter>.

Restore Defaults?

[YES] [NO] appears in the window. Select *YES* to load restore defaults.

Save as User Defaults
With this option the BIOS changes done so far by the user are saved as User Defaults.

Select save as user defaults from the Exit menu and press <Enter>.

Save as User Defaults?

[YES] [NO] appears in the window. Select *YES* to save user defaults.

Restore User Defaults
Aptio TSE automatically sets all Aptio TSE options to a complete set of user default settings when you select this option.

Select restore user defaults from the Exit menu and press <Enter>.

Restore User Defaults?

[YES] [NO] appears in the window. Select *YES* to load restore user defaults.

Boot Overide
Select this option to allow a system boot override from either a specific device connected to the SHB or from the BIOS' EFI Shell. A sample board configuration yields the following boot override selections:

UEFI: Built-In EFI Shell

P4: ST3160316AS (system configuration dependent)

This page intentionally left blank

Chapter 7 Event Logs

Event Logs

This BIOS menu allows you the view the contents of the SHB's Smbios Event Log for system troubleshooting and diagnostic purposes. There are a wide variety of possible event log messages that can be displayed depending on system activity and the events that the BIOS is setup to capture and display.

Option	Description
►Change Smbios Event Log Settings	Smbios Event Log: Disabled/**Enabled** Erasing Settings Erase Event Log: **No** (**No**, Yes Next Reset, Yes Every Reset) When Log Is Full: **Do Nothing** (**Do Nothing**, Erase Immediately) Smbios Event Log Standard Settings Log System Boot Event: **Enabled** (Disabled, **Enabled**) MECI: **1** METW: **60** Custom Optiona Log OEM Codes: **Enabled** (Disabled, **Enabled**) Convert OEM Codes: **Disabled** (**Disabled**, Enabled)
►View Smbios Event Log	

This page intentionally left blank

Appendix A BIOS Messages

Introduction
A status code is a data value used to indicate progress during the boot phase. These codes are outputed to I/O port 80h on the SHB. Aptio 4.x core outputs checkpoints throughout the boot process to indicate the task the system is currently executing. Status codes are very useful in aiding software developers or technicians in debugging problems that occur during the pre-boot process.

Aptio Boot Flow
While performing the functions of the traditional BIOS, Aptio 4.x core follows the firmware model described by the Intel Platform Innovation Framework for EFI (“the Framework”). The Framework refers the following “boot phases”, which may apply to various status code descriptions:

- Security (SEC) – initial low-level initialization
- Pre-EFI Initialization (PEI) – memory initialization[1]
- Driver Execution Environment (DXE) – main hardware initialization[2]
- Boot Device Selection (BDS) – system setup, pre-OS user interface & selecting a bootable device (CD/DVD, HDD, USB, Network, Shell, …)

[1] Analogous to “bootblock” functionality of legacy BIOS
[2] Analogous to “POST” functionality in legacy BIOS

BIOS Beep Codes
The Pre-EFI Initialization (PEI) and Driver Execution Environment (DXE) phases of the Aptio BIOS use audible beeps to indicate error codes. The number of beeps indicates specific error conditions.

PEI Beep Codes

# of Beeps	Description
1	Memory not Installed
1	Memory was installed twice (InstallPeiMemory routine in PEI Core called twice)
2	Recovery started
3	DXEIPL was not found
3	DXE Core Firmware Volume was not found
7	Reset PPI is not available
4	Recovery failed
4	S3 Resume failed

DXE Beep Codes

# of Beeps	Description
4	Some of the Architectural Protocols are not available
5	No Console Output Devices are found
5	No Console Input Devices are found
1	Invalid password
6	Flash update is failed
7	Reset protocol is not available
8	Platform PCI resource requirements cannot be met

BIOS Status Codes

As the POST (Power On Self Test) routines are performed during boot-up, test codes are displayed on Port 80 POST code LEDs 0, 1, 2, 3, 4, 5, 6 and 7. These LED are located on the top of the SHB, just above the board's battery socket. The POST Code LEDs and are numbered from right (position 1 = LED0) to left (position 8 – LED7).

The POST code checkpoints are the largest set of checkpoints during the BIOS pre-boot process. The following chart is a key to interpreting the POST codes displayed on LEDs 0 through 7 on the THD8141 and SHBs. Refer to the board layout in the *Specifications* chapter for the exact location of the POST code LEDs.

The HEX to LED chart in the POST Code LEDs section will serve as a guide to interpreting specific BIOS status codes.

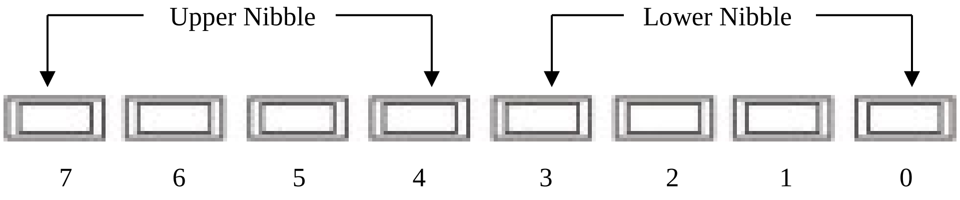
BIOS Status POST Code LEDs

As the POST (Power On Self Test) routines are performed during boot-up, test codes are displayed on Port 80 POST code LEDs 0, 1, 2, 3, 4, 5, 6 and 7. These LED are located on the top of the SHB, just above the board's battery socket. The POST Code LEDs and are numbered from right (position 1 = LED0) to left (position 8 – LED7).

The POST code checkpoints are the largest set of checkpoints during the BIOS pre-boot process. The following chart is a key to interpreting the POST codes displayed on LEDs 0 through 7 on the THD8141 and SHBs. Refer to the board layout in the *Specifications* chapter for the exact location of the POST code LEDs.

Upper Nibble (UN)				
Hex. Value	LED7	LED6	LED5	LED4
0	Off	Off	Off	Off
1	Off	Off	Off	On
2	Off	Off	On	Off
3	Off	Off	On	On
4	Off	On	Off	Off
5	Off	On	Off	On
6	Off	On	On	Off
7	Off	On	On	On
8	On	Off	Off	Off
9	On	Off	Off	On
A	On	Off	On	Off
B	On	Off	On	On
C	On	On	Off	Off
D	On	On	Off	On
E	On	On	On	Off
F	On	On	On	On

Lower Nibble (LN)				
Hex. Value	LED3	LED2	LED1	LED0
0	Off	Off	Off	Off
1	Off	Off	Off	On
2	Off	Off	On	Off
3	Off	Off	On	On
4	Off	On	Off	Off
5	Off	On	Off	On
6	Off	On	On	Off
7	Off	On	On	On
8	On	Off	Off	Off
9	On	Off	Off	On
A	On	Off	On	Off
B	On	Off	On	On
C	On	On	Off	Off
D	On	On	Off	On
E	On	On	On	Off
F	On	On	On	On



THD8141 POST Code LEDs

Status Code Ranges

Status Code Range	Description
0x01 – 0x0F	SEC Status Codes & Errors
0x10 – 0x2F	PEI execution up to and including memory detection
0x30 – 0x4F	PEI execution after memory detection
0x50 – 0x5F	PEI errors
0x60 – 0xCF	DXE execution up to BDS
0xD0 – 0xDF	DXE errors
0xE0 – 0xE8	S3 Resume (PEI)
0xE9 – 0xEF	S3 Resume errors (PEI)
0xF0 – 0xF8	Recovery (PEI)
0xF9 – 0xFF	Recovery errors (PEI)

SEC Status Codes

Status Code	Description
0x0	Not used
Progress Codes	
0x1	Power on. Reset type detection (soft/hard).
0x2	AP initialization before microcode loading
0x3	North Bridge initialization before microcode loading
0x4	South Bridge initialization before microcode loading
0x5	OEM initialization before microcode loading
0x6	Microcode loading
0x7	AP initialization after microcode loading
0x8	North Bridge initialization after microcode loading
0x9	South Bridge initialization after microcode loading
0xA	OEM initialization after microcode loading
0xB	Cache initialization
SEC Error Codes	
0xC – 0xD	Reserved for future AMI SEC error codes
0xE	Microcode not found
0xF	Microcode not loaded

SEC Beep Codes

There are no SEC Beep codes associated with this phase of the Aptio BIOS boot process.

PEI Status Codes

Status Code	Description
Progress Codes	
0x10	PEI Core is started
0x11	Pre-memory CPU initialization is started
0x12	Pre-memory CPU initialization (CPU module specific)
0x13	Pre-memory CPU initialization (CPU module specific)
0x14	Pre-memory CPU initialization (CPU module specific)
0x15	Pre-memory North Bridge initialization is started
0x16	Pre-Memory North Bridge initialization (North Bridge module specific)
0x17	Pre-Memory North Bridge initialization (North Bridge module specific)
0x18	Pre-Memory North Bridge initialization (North Bridge module specific)
0x19	Pre-memory South Bridge initialization is started
0x1A	Pre-memory South Bridge initialization (South Bridge module specific)
0x1B	Pre-memory South Bridge initialization (South Bridge module specific)
0x1C	Pre-memory South Bridge initialization (South Bridge module specific)
0x1D – 0x2A	OEM pre-memory initialization codes
0x2B	Memory initialization. Serial Presence Detect (SPD) data reading
0x2C	Memory initialization. Memory presence detection
0x2D	Memory initialization. Programming memory timing information
0x2E	Memory initialization. Configuring memory
0x2F	Memory initialization (other).
0x30	Reserved for ASL (see ASL Status Codes section below)
0x31	Memory Installed
0x32	CPU post-memory initialization is started
0x33	CPU post-memory initialization. Cache initialization
0x34	CPU post-memory initialization. Application Processor(s) (AP) initialization
0x35	CPU post-memory initialization. Boot Strap Processor (BSP) selection
0x36	CPU post-memory initialization. System Management Mode (SMM) initialization
0x37	Post-Memory North Bridge initialization is started
0x38	Post-Memory North Bridge initialization (North Bridge module specific)
0x39	Post-Memory North Bridge initialization (North Bridge module specific)
0x3A	Post-Memory North Bridge initialization (North Bridge module specific)
0x3B	Post-Memory South Bridge initialization is started
0x3C	Post-Memory South Bridge initialization (South Bridge module specific)
0x3D	Post-Memory South Bridge initialization (South Bridge module specific)
0x3E	Post-Memory South Bridge initialization (South Bridge module specific)
0x3F-0x4E	OEM post memory initialization codes
0x4F	DXE IPL is started

PEI Error Codes	
0x50	Memory initialization error. Invalid memory type or incompatible memory speed
0x51	Memory initialization error. SPD reading has failed
0x52	Memory initialization error. Invalid memory size or memory modules do not match.
0x53	Memory initialization error. No usable memory detected
0x54	Unspecified memory initialization error.
0x55	Memory not installed
0x56	Invalid CPU type or Speed
0x57	CPU mismatch
0x58	CPU self test failed or possible CPU cache error
0x59	CPU micro-code is not found or micro-code update is failed
0x5A	Internal CPU error
0x5B	reset PPI is not available
0x5C-0x5F	Reserved for future AMI error codes
S3 Resume Progress Codes	
0xE0	S3 Resume is stared (S3 Resume PPI is called by the DXE IPL)
0xE1	S3 Boot Script execution
0xE2	Video repost
0xE3	OS S3 wake vector call
0xE4-0xE7	Reserved for future AMI progress codes
0xE0	S3 Resume is stared (S3 Resume PPI is called by the DXE IPL)
S3 Resume Error Codes	
0xE8	S3 Resume Failed in PEI
0xE9	S3 Resume PPI not Found
0xEA	S3 Resume Boot Script Error
0xEB	S3 OS Wake Error
0xEC-0xEF	Reserved for future AMI error codes
Recovery Progress Codes	
0xF0	Recovery condition triggered by firmware (Auto recovery)
0xF1	Recovery condition triggered by user (Forced recovery)
0xF2	Recovery process started
0xF3	Recovery firmware image is found
0xF4	Recovery firmware image is loaded
0xF5-0xF7	Reserved for future AMI progress codes
Recovery Error Codes	
0xF8	Recovery PPI is not available
0xF9	Recovery capsule is not found
0xFA	Invalid recovery capsule
0xFB – 0xFF	Reserved for future AMI error codes

PEI Beep Codes

# of Beeps	Description
1	Memory not Installed
1	Memory was installed twice (InstallPeiMemory routine in PEI Core called twice)
2	Recovery started
3	DXEIPL was not found
3	DXE Core Firmware Volume was not found
7	Reset PPI is not available
4	Recovery failed
4	S3 Resume failed

DXE Status Codes

Status Code	Description
0x60	DXE Core is started
0x61	NVRAM initialization
0x62	Installation of the South Bridge Runtime Services
0x63	CPU DXE initialization is started
0x64	CPU DXE initialization (CPU module specific)
0x65	CPU DXE initialization (CPU module specific)
0x66	CPU DXE initialization (CPU module specific)
0x67	CPU DXE initialization (CPU module specific)
0x68	PCI host bridge initialization
0x69	North Bridge DXE initialization is started
0x6A	North Bridge DXE SMM initialization is started
0x6B	North Bridge DXE initialization (North Bridge module specific)
0x6C	North Bridge DXE initialization (North Bridge module specific)
0x6D	North Bridge DXE initialization (North Bridge module specific)
0x6E	North Bridge DXE initialization (North Bridge module specific)
0x6F	North Bridge DXE initialization (North Bridge module specific)
0x70	South Bridge DXE initialization is started
0x71	South Bridge DXE SMM initialization is started
0x72	South Bridge devices initialization
0x73	South Bridge DXE Initialization (South Bridge module specific)
0x74	South Bridge DXE Initialization (South Bridge module specific)
0x75	South Bridge DXE Initialization (South Bridge module specific)
0x76	South Bridge DXE Initialization (South Bridge module specific)
0x77	South Bridge DXE Initialization (South Bridge module specific)
0x78	ACPI module initialization
0x79	CSM initialization

0x7A – 0x7F	Reserved for future AMI DXE codes
0x80 – 0x8F	OEM DXE initialization codes
0x90	Boot Device Selection (BDS) phase is started
0x91	Driver connecting is started
0x92	PCI Bus initialization is started
0x93	PCI Bus Hot Plug Controller Initialization
0x94	PCI Bus Enumeration
0x95	PCI Bus Request Resources
0x96	PCI Bus Assign Resources
0x97	Console Output devices connect
0x98	Console input devices connect
0x99	Super IO Initialization
0x9A	USB initialization is started
0x9B	USB Reset
0x9C	USB Detect
0x9D	USB Enable
0x9E – 0x9F	Reserved for future AMI codes
0xA0	IDE initialization is started
0xA1	IDE Reset
0xA2	IDE Detect
0xA3	IDE Enable
0xA4	SCSI initialization is started
0xA5	SCSI Reset
0xA6	SCSI Detect
0xA7	SCSI Enable
0xA8	Setup Verifying Password
0xA9	Start of Setup
0xAA	Reserved for ASL (see ASL Status Codes section below)
0xAB	Setup Input Wait
0xAC	Reserved for ASL (see ASL Status Codes section below)
0xAD	Ready To Boot event
0xAE	Legacy Boot event
0xAF	Exit Boot Services event
0xB0	Runtime Set Virtual Address MAP Begin
0xB1	Runtime Set Virtual Address MAP End
0xB2	Legacy Option ROM Initialization
0xB3	System Reset
0xB4	USB hot plug
0xB5	PCI bus hot plug
0xB6	Clean-up of NVRAM
0xB7	Configuration Reset (reset of NVRAM settings)

0xB8 – 0xBF	Reserved for future AMI codes
0xC0 – 0xCF	OEM BDS initialization codes
DXE Error Codes	
0xD0	CPU initialization error
0xD1	North Bridge initialization error
0xD2	South Bridge initialization error
0xD3	Some of the Architectural Protocols are not available
0xD4	PCI resource allocation error. Out of Resources
0xD5	No Space for Legacy Option ROM
0xD6	No Console Output Devices are found
0xD7	No Console Input Devices are found
0xD8	Invalid password
0xD9	Error loading Boot Option (LoadImage returned error)
0xDA	Boot Option is failed (StartImage returned error)
0xDB	Flash update is failed
0xDC	Reset protocol is not available

DXE Beep Codes

# of Beeps	Description
4	Some of the Architectural Protocols are not available
5	No Console Output Devices are found
5	No Console Input Devices are found
1	Invalid password
6	Flash update is failed
7	Reset protocol is not available
8	Platform PCI resource requirements cannot be met

ACPI/ASL Status Codes

Status Code	Description
0x01	System is entering S1 sleep state
0x02	System is entering S2 sleep state
0x03	System is entering S3 sleep state
0x04	System is entering S4 sleep state
0x05	System is entering S5 sleep state
0x10	System is waking up from the S1 sleep state
0x20	System is waking up from the S2 sleep state
0x30	System is waking up from the S3 sleep state
0x40	System is waking up from the S4 sleep state
0xAC	System has transitioned into ACPI mode. Interrupt controller is in PIC mode.
0xAA	System has transitioned into ACPI mode. Interrupt controller is in APIC mode.

OEM-Reserved Status Code Ranges

Status Code	Description
0x5	OEM SEC initialization before microcode loading
0xA	OEM SEC initialization after microcode loading
0x1D – 0x2A	OEM pre-memory initialization codes
0x3F – 0x4E	OEM PEI post memory initialization codes
0x80 – 0x8F	OEM DXE initialization codes
0xC0 – 0xCF	OEM BDS initialization codes