



TSB7053

7053-xxx

No. 87-007056-002 Revision A

BIOS SETUP

TECHNICAL REFERENCE

Aptio® 4.x Test Setup Environment (TSE)

For use with TSB7053

Intel® Xeon® E3-1200-series

Intel® Core™ i7-2600

Intel® Core™ i5-2400

Intel® Core™ i3-2120

(Sandy Bridge)

Dual and Quad Core

PROCESSOR-BASED

SHB



WARRANTY

The following is an abbreviated version of Trenton Technology's warranty policy for PICMG® 1.3 products. For a complete warranty statement, contact Trenton or visit our website at www.TrentonTechnology.com.

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 Technology Inc. is only obligated to repair, replace or refund the purchase price of this product at Trenton Technology's 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 Technology Inc.; or if failure is caused by accident, acts of God, or other causes beyond the control of Trenton Technology Inc. Trenton Technology 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 Technology 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 Technology 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 Technology Inc.

RETURN POLICY

Products returned for repair must be accompanied by a Return Material Authorization (RMA) number, obtained from Trenton Technology prior to return. Freight on all returned items must be prepaid by the customer, and the customer is responsible for any loss or damage caused by common carrier in transit. Items will be returned from Trenton Technology 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 Technology Inc.
- 1001 Broad Street
- Utica, NY 13501
- Attn: Repair Department

Contact Trenton 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 Technology Inc. reserves the right to change the functions, features or specifications of their products at any time, without notice.

Copyright © 2011 by Trenton Technology Inc. All rights reserved.

E-mail: Support@TrentonTechnology.com

Web: <http://www.trentontechnology.com/>



TRENTON Technology 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

CHAPTER 1	STARTING APTIO® TSE	1-1
	Introduction.....	1-1
	Starting Aptio TSE.....	1-1
	Press DEL or F2 to enter Setup.....	1-1
	Aptio® TSE Setup Menu	1-2
	Navigation	1-2
CHAPTER 2	ADVANCED SETUP	2-1
	Introduction.....	2-1
	Launch PXE OpROM Configuration.....	2-1
	Launch Storage OpROM Configuration	2-1
	PCI Sub-System Settings.....	2-1
	ACPI Settings.....	2-1
	Trusted Computing.....	2-1
	WHEA Configuration	2-1
	CPU Configuration.....	2-1
	SATA Configuration	2-2
	Serial ATA Modes – Disabled, IDE, ACHI or RAID.....	2-2
	Serial ATA Port X.....	2-2
	Thermal Configuration	2-2
	Intel Trusted Execution Technology (TXT) Configuration	2-2
	Intel IGD SWSCI OpRegion Configuration	2-2
	USB Configuration.....	2-2
	Super IO Configuration	2-2
	Floppy Disk Controller Configuration.....	2-3
	Serial Port 0 Configuration	2-3
	Serial Port 1 Configuration	2-3
	Parallel Port Address	2-4
	AMT Configuration	2-4
	Serial Port Console Redirection.....	2-4
CHAPTER 3	CHIPSET CONFIGURATION SETUP	3-1
	Introduction.....	3-1
	North Bridge Configuration	3-1
	South Bridge Configuration.....	3-2
	ME Subsystem Configuration.....	3-2
	Chipset Reference Board.....	3-2
CHAPTER 4	BOOT SETUP	4-1
	Introduction.....	4-1
	Boot Configuration	4-1
	Quit Boot	4-1
CHAPTER 5	SECURITY	5-1
	Two Levels of Password Protection	5-1
	Remember the Password.....	5-1
	Security Setup.....	5-1
CHAPTER 6	SAVING AND EXITING BIOS SETUP AND RESTORING DEFAULTS	6-1
	Introduction.....	6-1
	1 - Save Changes & Exit.....	6-1
	2 - Discard Changes & Exit.....	6-1
	3 - Save Changes & Reset	6-1
	4 - Discard Changes & Reset.....	6-1
	Restore Defaults	6-2
	Save as User Defaults	6-2
	Restore User Defaults	6-2
	Boot Override	6-2
CHAPTER 7	EVENT LOG	7-1
	Change SMBIOS Event Log Settings.....	7-1
	View SMBIOS Event Log.....	7-1
	View SYSTEM Event Log	7-1

APPENDIX A BIOS MESSAGES A-1

- Introduction..... A-1
- Aptio Boot Flow A-1
- BIOS Beep Codes A-1
- PEI Beep Codes A-1
- DXE Beep Codes..... A-2
- BIOS Status Codes A-3
- BIOS Status POST Code LEDs A-3
- Status Code Ranges..... A-4
- SEC Status Codes A-4
- SEC Beep Codes..... A-4
- PEI Beep Codes A-7
- DXE Status Codes A-7
- DXE Beep Codes..... A-9
- ACPI/ASL Status Codes A-10
- OEM-Reserved Status Code Ranges A-10

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 TSB7053 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
- Boot Setup
- Security Setup
- Chipset Setup
- Exit

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 TSB7053 / BIOS and hardware technical reference manuals are available under the **Downloads** tab on the [TSB7053](#) 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 Technology 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 TSB7053 / 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:

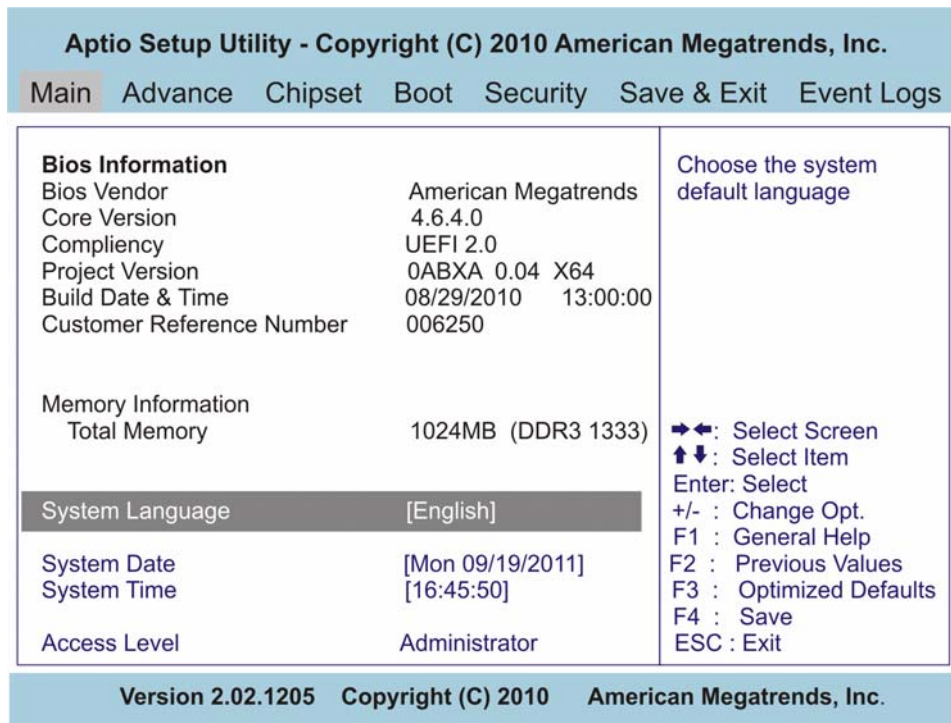
Step	Description
1	Install the SHB in a PICMG 1.3 backplane with the proper system power connections made to the backplane and a mouse, keyboard and monitor connected to the SHB
2	Power on the system with the SHB
3	Press the <Delete> or <F2> key on your keyboard when you see the following text prompt: 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.



There may be slight differences in the screen shots illustrated in this manual due to Trenton TSB7053 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 <i>Enter</i> key allows the user to select an option to edit its value or access a sub menu.
→← Left/Right	The <i>Left and Right</i> <Arrow> keys allow you to select an Aptio TSE screen. For example: Main screen, Advanced screen, Chipset screen, and so on.
↑↓ Up/Down	The <i>Up and Down</i> <Arrow> keys allow you to select an Aptio TSE item or sub-screen.
+/- Plus/Minus	The <i>Plus and Minus</i> <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 <i>Cancel</i> 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.

This page intentionally left blank

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.

Launch PXE OpROM Configuration

With this selection, you can enable or disable the system's Boot From LAN capability of the SHB which allows system ROM storage settings for legacy networks.

Launch Storage OpROM Configuration

With this selection, you can enable or disable the system's ROM storage settings for legacy mass storage devices.

PCI Sub-System Settings

Various PCI Express 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.

ACPI Settings

This is where you set up your system for use with the ACPI soft control states available on the SHB. Various system sleep states and recover modes are available for selection on this sub-menu.

Trusted Computing

This where you must first enable the board's Trusted Platform Module (TPM) if your system is to operated in a Trusted Computing application. When Trusted Computing is enabled, the O/S will not show the TPM until a platform reset is performed.

WHEA Configuration

This BIOS setting enables or disables the Windows Hardware Error Architecture.

CPU Configuration

The parameters for the specific Sandy Bridge 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
Intel® Hyper-Threading	This option allows the user to enable or disable Intel® Hyper-Threading support on the Intel® Xeon® E3-1275 processor. Other Sandy Bridge processors may or may not support Intel Hyper-Threading. By default, this setting is enabled.
Intel® Virtualization	This option allows the user to enable or disable Intel® Virtualization support on the Intel® Xeon® E3-1200 series (i.e. Sandy Bridge) processor. Other Sandy Bridge processors may or may not support Intel Virtualization. By default, this setting is enabled.
Execute Disable Bit	This option allows the user to enable or disable Intel® Execute Disable Bit feature of the Intel® Xeon® E3-1200 series (i.e. Sandy Bridge) processor.
Active Processor Cores	With this setting you may use all of the available cores available in the Intel® Xeon® E3-1200 series (i.e. Sandy Bridge) processor or 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.

SATA Configuration

This is where you can set the parameters for the SATA devices that SHB's BIOS senses during the boot process.

Serial ATA Modes – Disabled, IDE, ACHI or RAID

The selection of the SATA mode will determine most of the remaining SATA configuration selections available on this menu. Use these selections on this menu to configure or to turn on or off the selected onboard SATA ports.

Option	Description
Disabled	All onboard SATA ports disabled
IDE	SATA ports configured for individual SATA drives. The SATA Controller 0 and 1 selections become visible when IDE mode is selected. Most applications will use either the Compatible or Enhanced SATA controller option.
AHCI	AHCI is a variation on IDE in that this SATA mode of operation support hot plug SATA drives using the AHCI control signals. Various settings are available to configure each SATA port for the specific hot plug SATA drive implementation.
RAID	The TSB7053 supports a variety of RAID drive array configurations. Use this setting if your system is using the SHB's on-board software RAID capability.

Serial ATA Port X

This item specifies the number of SATA ports sensed by the BIOS during system startup. An indication of each SATA drive port status will be display along with the individual port settings available for each drive. The specific port settings displayed are a function of the SATA mode selected.

Thermal Configuration

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

Intel Trusted Execution Technology (TXT) Configuration

With this BIOS setup screen you can enable or disable Intel TXT. However, you can only enable Intel TXT if Intel Virtualization Technology is enabled on the CPU Configuration menu and the Secure Mode Extensions (SMX) are enabled on the Intel TXT setup menu.

Intel IGD SWSCI OpRegion Configuration

This menu determines how the two video ports will function on the TSB7053. The IGD – BOOT TYPE setup parameter on this menu is used to determine which video device will be active during POST. The VBIOS default should be used in most applications.

USB Configuration

This is where you can set the parameters for the USB devices that have been sensed SHBs' during the boot process.

Super IO Configuration

The one Super IO component on the TSB7053 supports the SHB's PS/2 mouse and keyboard ports as well as Serial Port 1 and Serial Port 2. A future BIOS revision may be available to support a second Super I/O chip located on an optional IOB33 module. This future BIOS revision will enable an IOB33 to plug into the SHBs' P20 I/O Expansion connector and provide additional IDE floppy and parallel port connectivity to the system designer as well as two additional serial interface ports. The Super IO Configuration submenu that will be displayed will depend on the SHB's BIOS revision and if an IOB33 is connected to P20. This Advanced Setup sub-menu allows you to configure the system ports connected to the board's Super I/O component(s).

Floppy Disk Controller Configuration

When available, this option will 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	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.

Serial Port 0 Configuration

This option specifies the base I/O port address and Interrupt Request address of serial port 1 located on header connector P7 on the TSB7053. 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
Auto	The Aptio BIOS selects the optimum port address and IRQ based on the IO connections sensed during POST. This is the default setting.
3F8h; IRQ4	Set this value to allow the serial port to use 3F8 as its I/O port address and IRQ 4 for the interrupt address. The majority of serial port 1 or COM1 ports on computer systems use IRQ4 and I/O Port 3F8 as the standard setting.
3F8h; IRQ3, 4, 5, 6, 7, 10, 11, 12	Set this value to allow the serial port to use 3F8 as its I/O port address and any one of the listed IRQs for the interrupt address.
2F8h; ; IRQ3, 4, 5, 6, 7, 10, 11, 12	Set this value to allow the serial port to use 2F8 as its I/O port address and any one of the listed IRQs for the interrupt address.
3E8h; ; IRQ3, 4, 5, 6, 7, 10, 11, 12	Set this value to allow the serial port to use 3E8 as its I/O port address and any one of the listed IRQs for the interrupt address.
2E8h; ; IRQ3, 4, 5, 6, 7, 10, 11, 12	Set this value to allow the serial port to use 2E8 as its I/O port address and any one of the listed IRQs for the interrupt address.

The Device Mode setting allows you to select Normal or High Speed serial interface implementations. The default setting is *Normal*.

Serial Port 1 Configuration

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

Parallel Port Address

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
Auto	The Aptio BIOS selects the optimum parallel port address and IRQ based on the IO connections sensed during POST.
378h; IRQ5;	Set this value to allow the parallel port to use 278h as its I/O port address.
378h; IRQ3, 4, 5, 6, 7, 10, 11, 12;	This setting uses parallel port IO address 378h and any one of the listed IRQs for the interrupt address.
278h; IRQ3, 4, 5, 6, 7, 10, 11, 12;	This setting uses parallel port IO address 278h and any one of the listed IRQs for the interrupt address.
3BCh; IRQ3, 4, 5, 6, 7, 10, 11, 12;	This setting uses parallel port IO address 3BCh and any one of the listed IRQs for the interrupt address.
378	Set this value to allow the parallel port to use 378 as its I/O port address. This is the default setting. The majority of parallel ports on computer systems use IRQ7 and I/O Port 378h as the standard setting.
278	Set this value to allow the parallel port to use 278h as its I/O port address.
3BC	Set this value to allow the parallel port to use 3BCh as its I/O port address.

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*.

AMT Configuration

The processor's Intel Advanced Management Technology or AMT is *Enabled* by default. You may disable the AMT capability using this BIOS menu by selecting the *Disabled* option. The configuration settings available when Intel AMT is *Enabled* are listed below.

Option	Description
Unconfigure AMT/ME	This setting allows access to the AMT management engine without a password when <i>Enabled</i> . The Disabled selection requires a password to enter the AMT management engine.
Watchdog Timer	The Enabled setting allows you to enter both Operating System and BIOS watchdog timer values. Valid entries for the watchdog timer values may range from 0 to 9999 (9.999 seconds). The default setting for the watchdog timer setting is <i>Disabled</i> .

Serial Port Console Redirection

The redirection capability of the serial ports is useful for accessing the systems' BIOS remotely using one of the serial ports on the TSB7053. The serial port console redirection BIOS setup parameters are used to ensure that the redirection of the board's VGA output and keyboard parameters used for BIOS selection and modification match those of a remote terminal/keyboard or PC. When *Enabled* there are a number of console redirection setting options available.

Option	Description
Out-of-Band Management Port	This setting enables or disables the Microsoft Windows EMS for remote management of a Windows server operating system via a serial interface port.
Terminal Type, Bits/sec and Flow Control	These three settings are used to set-up the re-directed serial port's interface for the terminal or PC connected to the port.

Chapter 3 Chipset Configuration Setup

Introduction

The term “chipset” is a bit of a misnomer for the Trenton TSB7053. 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 Sandy Bridge processor’s micro-architecture. The TSB7053 features the Intel® C206 PCH and this platform controller hub merges the former South Bridge chipset component functionality with the North Bridge functionality not handled by the Sandy Bridge processor. The following section covers the set-up parameters of what could be thought of as the North Bridge and South Bridge sections of the Sandy Bridge processor and the Intel® C206 PCH.

North Bridge Configuration

The Memory Information at the top of the *North Bridge Configuration* menu lists the memory capacities of each DDR3 DIMM installed on the board and that the BIOS has sensed during POST. The remaining north bridge set-up parameters allow the user to do the following:

Option	Description
Low MMI/O Align	The default setting for Low MMI/O Align is 1024M and this setting optimizes the board’s system memory interface for use with 64-bit operating systems. If you are using a 32-bit operating system you can gain access to additional system memory resources by choosing the 64M setting.
DMI Gen2	The default setting is <i>Enabled</i> and this setting ensures that PCI Express 2.0 link speeds are used between the processor and the PCH using the Intel Direct Media Interface.
VT-d	This option allows the user to enable or disable the Intel® Virtualization Technology for Directed I/O feature of the processor. The default setting is <i>Disabled</i> .
Initiate Graphic Adapter	This setting allows you to select which of the processor’s graphics controllers is to be used as the primary boot device. There are five options: IGD – Processor’s integrated graphics device only PCI/IGD – External PCI graphics card or the CPU’s IGD PCI/PEG – External PCI or PCI Express graphics (PEG) card, PCI first priority PEG/IGD – External PEG or internal IGD [<i>Default</i>] PEG/PCI - External PEG or PCI card, PEG first priority
IGD Memory	This option enables the size of system memory that you would like set aside for use as video memory. Acceptable entries range from <i>Disable</i> i.e. 0 video memory, up to 512M of video memory. The default setting is 64M.
Render Standby	The default setting is <i>Enabled</i> meaning that the processor’s internal graphics device is on standby status during system idle periods. The <i>Disabled</i> option is available for non-video applications.
IGD Multi-Monitor	The IGD used in the Sandy Bridge processor micro-architecture has the capability of supporting one or two video monitors simultaneously. The default condition for this option is <i>Disabled</i> .
PCI Express Port	There are three possible selections for this option: <i>Disabled</i> , <i>Enabled</i> and <i>Auto</i> . <i>Auto</i> is the default setting and offers the most system flexibility and allows the system to use both internal and external PCI Express graphics devices. The <i>Disabled</i> setting implies internal graphics device usage or a PCI graphics card. The <i>Enabled</i> setting means PEG card only system operations.
PEG Force Gen1	The BIOS default setting for this option is <i>Disabled</i> allowing the system to use either a PCIe 2.0 or 1.1 interface to an external PEG device. When this option is <i>Enabled</i> , the processor will expect to see only Gen1 PEG cards.
Detect Non-Compliance Device	The default setting is <i>Disabled</i> , but the user can select <i>Enabled</i> to allow the system to detect non-compliant PCI Express devices.
MRC Message Print	The default setting is <i>Disabled</i> . The <i>Enabled</i> option allows the printing of memory initialization messages.

South Bridge Configuration

The *South Bridge Configuration* menu item allows the user to do the following:

Option	Description
SMBus Controller	This option allows the user to enable or disable the SMBus Controller in the Intel® C206
GbE Controller	This option allows the user to enable or disable the Ethernet Controller in the Intel® C206. Disabling this internal controller shuts down the LAN interface to the PICMG 1.3 backplane. This setting does not affect the operation of the independent Intel® 82580DB Ethernet Controller that drives the two LAN ports on the SHBs I/O plate.
Wake on LAN from S5	This option allows the user to enable or disable wake on LAN feature derived from an ACPI S5 shutdown event
Restore AC Power Loss Settings	This option allows the user to determine how the system will come back up when power is restored after an unplanned power interruption. The options are Power Off, Power On or Last State.
PCI Express Ports Configuration	This option allows the user to Enable, Disable or Automatically turn on the various PCI Express ports inside the Intel® 206 PCH. The default setting is set to Auto and Trenton highly recommends leaving this setting alone. These internal PCIe ports drive on-board components and turning them off will disable critical SHB and system functions
SLP_S4 Assertion Stretch Enable	When <i>Enabled</i> this allows the selection of a minimum assertion width for the SLP_S4 signal. This is the default setting and provides access to the four value choices that may be entered for the assertion width: 1-2, 2-3, 3-4 or 4-5 seconds. The 4 – 5 second assertion width is the default value for the SLP_S4 signal. The assertion width values are hidden if the assertion stretch enable option is set to <i>Disabled</i> .
Deep Sx	This is the deep sleep state setting option. The default value for this option is <i>Disabled</i> since the option is usually associated with mobile devices. There are four possible entries that can be made if the option is <i>Enabled</i> : Enabled in S5 (battery), Enabled in S5, Enabled in S4 and S5 (battery) and Enabled in S4 and S5.
High Precision Event Timer	The default setting is <i>Enabled</i> with an option to disable this timer...
PCI Express Ports Configuration	There are eight potential PCI Express ports available in a standard Intel C206 PCH. The TSB7053 implementation uses these ports for both on-board and off- board PCI Express interfaces. The default setting for each port is <i>Auto</i> , and it should be left in this position. Changing to the <i>Enabled</i> or <i>Disabled</i> option setting can cause unintended system operations.
PCIe Sub Decode	The default value for this option setting is <i>Disabled</i> and should be left in this position. Enabling this option setting allows you to set up a PCIe sub-decode operation on any one of the PCH's eight PCI Express ports. Care must be used if implementing this setting.
USB Configuration	This option allows the user to enable or disable the various USB ports inside the Intel® C206 PCH. The default setting is set to <i>Enabled</i> . These internal USB ports drive the USB interface connections to the SHBs I/O plate and down to edge connector C for use on a PICMG 1.3 backplane, as well as a USB interface to any optional PCI Express Mini-Card connected to board connector P10 located on the back of the TSB7053.

ME Subsystem Configuration

The ME or *Management Engine Subsystem Configuration* menu items provide access to the BIOS software's management engine implementation parameters. The Intel® Management Engine and BIOS Extensions (Bx) come into play in Intel AMT system implementations.

Option	Description
ME Subsystem	System default setting is <i>Enabled</i> .
ME Temporary Disable	System default setting is <i>Disabled</i> .
End of POST Message	System default setting is <i>Enabled</i> .
Execute MEBx	System default setting is <i>Enabled</i> . This allows the BIOS extensions for the ME to run
MEBx Mode	<i>Normal</i> is the defaults setting with optional settings that include <i>Hidden Ctrl + P</i> and <i>Enter MEBx Setup</i> .
Integrated Clock Chip Configuration	System default setting is <i>Disabled</i> .

Chipset Reference Board

This BIOS setting allows you to enable the CIRA (Client Initiated Remote Access) Trigger for use in Intel AMT 7.0 system implementations. The system default setting is *Disabled*.

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	The numeric value of 1 to 65355 entered is in seconds. A value of 65355 or FFFFh means an indefinite wait period
Bootup NumLock State	The default setting is <i>On</i> with an option to turn the setting <i>Off</i> . The <i>On</i> 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 <i>Off</i> setting, the NumLock keyboard key will need to be pressed to use the 10-key numeric pad.

Quite Boot

Set this value to allow the boot up screen options to be modified between POST messages or OEM logo.

Option	Description
Disabled	Set this default value allows the computer system to display the POST messages.
Enabled	Set this value to allow the computer system to display the OEM logo.

The next three BIOS settings on this screen are:

- Gate20 Active -- Default setting = *Upon Request*
- Option ROM Messages -- Default setting = *Force BIOS*
- Interrupt 19 Capture -- Default setting = *Disabled*

These 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.

This page intentionally left blank

Chapter 5 Security

Two Levels of Password Protection

Security Setup provides both a Administrator and a 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 Setup

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.

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:

1 - 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.

2 - 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.

3 - 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.

4 - 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.

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 Override

Select this option to allow a system boot override from either a specific device connected to the SHB or from the BIOS' EFI Shell.

Chapter 7 Event Log

Change SMBIOS Event Log Settings

Use the Aptio TSE menu screen options to set up the system event log reporting format and configuration options for the BIOS.

View SMBIOS Event Log

This read-only menu screen displays the events recorded in the BIOS event log. An event's error code and severity along with the data and time that the event occurred are displayed on this screen.

View SYSTEM Event Log

This read-only menu screen displays the events recorded in the SYSTEM event log. A sensor's event date, time and sensor type are displayed on this screen.

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 outputted 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 initialization¹
- Driver Execution Environment (DXE) – main hardware initialization²
- 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	DXE IPL 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 TSB7053 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.

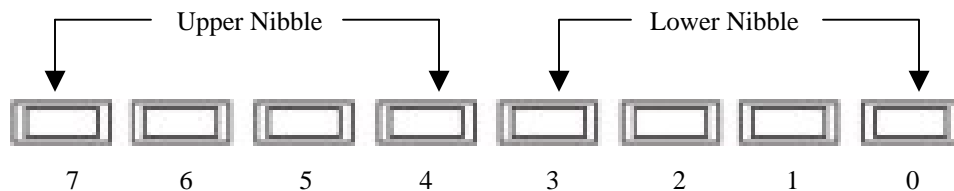
BIOS Status POST Code LEDs

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 TSB7053 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



TSB7053 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 started (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 started (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	DXE IPL 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