



BXT7059 / BXTS7059

7059-xxx

No. 87-0067062-000 Revision C

BIOS SETUP

TECHNICAL REFERENCE

Aptio® 4.x Test Setup Environment (TSE)

For use with BXT7059 or BXTS7059

Intel® Xeon® E5-2400 Series v2

and

Intel® Xeon® E5-2400 Series

10, 8, 6 and 4-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.

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 the discretion of Trenton Systems. 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 Systems 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 Quick Path Interconnect, 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.

Copyright © 2015 by Trenton Systems, Inc. All rights reserved.

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

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
	PCI Sub-System Settings	2-1
	ACPI Settings	2-3
	Trusted Computing Settings	2-3
	WHEA Configuration.....	2-3
	CPU Configuration	2-3
	Runtime Error Logging Configuration.....	2-5
	SATA Configuration.....	2-5
	SAS Configuration	2-5
	Thermal Configuration.....	2-6
	Intel® TXT (LT-SX) Configuration	2-6
	USB Configuration	2-6
	Super IO Configuration.....	2-6
	Floppy Disk Controller.....	2-7
	Floppy Change Settings	2-7
	Floppy Device Mode	2-7
	Serial Port 0 Configuration.....	2-7
	Serial Port 1 Configuration.....	2-7
	Parallel Port Configuration.....	2-8
	AMT Configuration.....	2-8
	Serial Port Console Redirection Configuration.....	2-9
	iSCSI Configuration	2-9
CHAPTER 3	CHIPSET CONFIGURATION SETUP	3-1
	Introduction.....	3-1
	North Bridge Configuration	3-1
	South Bridge Configuration	3-3
	South Bridge Configuration (continued)	3-4
	Intel ME System	3-4
CHAPTER 4	BOOT SETUP	4-1
	Introduction.....	4-1
	Boot Configuration	4-1
	Boot Option Priorities.....	4-1
	CSM16 Parameters	4-1
	CSM Parameters	4-2
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 LOGS	A-1
	Change SMBIOS Event Log Settings.....	A-1
	Change Settings – Enabling/Disabling Options.....	A-1

View SMBIOS Event Log.....A-1

APPENDIX A BIOS MESSAGESA-1

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

SHB HANDLING PRECAUTIONS

WARNING: This product has components that 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 BXT7059 and BXTS7059 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 BXT7059 / BXTS7059 BIOS and hardware technical reference manuals are available under the **Downloads** tab on the [BXT7059](#) or [BXTS7059](#) 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 BXT7059 / BXTS7059 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.

Aptio Setup Utility – Copyright © 2013 American Megatrends Inc.						
Main	Advanced	Chipset	Boot	Security	Save & Exit	Event Logs
BIOS Information					Choose the system default language →← : Select Screen ↑↓ : Select Item Enter: Select +/- : Change Opt. F1 : General Help F2 : Previous Values F3 : Optimized Defaults F4 : Save & Exit ESC : Exit	
BIOS Vendor		American Megatrends				
Core Version		4.6.5.4				
Compliance		UEFI 2.3.1; PI 1.2				
Project Version		0ACADN005 x64				
Build Date & Time		11/14/2013 17:00:00				
Memory Information						
Total Memory		12288 MB (DDR3)				
System Language		[English]				
System Date		[Mon 12/23/2013]				
System Time		[11:07:00]				
Access Level		Administrator				
Version 2.16.1240, Copyright © 2013 American Megatrends, Inc.						

There may be slight differences in the screen shots illustrated in this manual due to Trenton BXT7059 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.
Enter	The <Enter> 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 or SAS Configuration, USB Configuration, and a Super IO configuration if the SHB is equipped with an optional IOB33. Selecting on 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 Subsystem Settings					PCI, PCI-X and PCI Express Settings →← : Select Screen ↑↓ : Select Item Enter: Select +/- : Change Opt. F1 : General Help F2 : Previous Values F3 : Optimized Defaults F4 : Save & Exit ESC : Exit F3 : Optimized Defaults	
▶ ACPI Settings						
▶ Trusted Computing						
▶ WHEA Configuration						
▶ CPU Configuration						
▶ Runtime Error Logging						
▶ SATA Configuration						
▶ SAS Configuration						
▶ Thermal Configuration						
▶ Intel® TXT (LT-SX) Configuration						
▶ USB Configuration						
▶ Super IO Configuration						
▶ AMT Configuration						
▶ Serial Port Console Redirection						
▶ iSCSI Configuration						
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 Bus Driver Version	Informational only – typical data displayed is 2.05.02
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 Sub-System Settings (continued)

Option	Description
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	<p>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.</p> <p>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</p> <p>PCI Express Link Register Settings ASPM Support: Auto/Disabled Extended Sync: Disabled/Enabled</p> <p>Link Training Retry: Disabled, 2, 3, 5 Link Training Timeout: 10 – 1000 usec with 10 usec being the default value Unpopulated Links: Keep Link On, Disabled Restore PCIE Registers: Disabled/Enabled</p>
PCI Express GEN2 Settings	<p>There are several PCIe 2.0/3.0 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.</p> <p>PCI Express Device Register Settings Completion Timeout: Default/Shorter/Longer/Disabled The default setting enables the normal link timeout range of 50us to 50ms. These BIOS selections allow you to vary this setting as needed in your system design. ARI Forwarding: Disabled/Enabled AtomicOp Requester Enable: Disabled/Enabled AtomicOp Egress Blocking: Disabled/Enabled IDO Request Enable: Disabled/Enabled IDO Completion Enable: Disabled/Enabled LTR Mechanism Enable: Disabled/Enabled End-END TLP Prefix Blocking: Disabled/Enabled</p> <p>PCI Express GEN2 Link Register Settings Target Link Speed: Auto, Force to 2.5 GT/s, Force to 5.0 GT/s Clock Power Management: Disabled/Enabled Compliance SOS: Disabled/Enabled Hardware Autonomous Width: Disabled/Enabled Hardware Autonomous Speed: Disabled/Enabled</p>

ACPI Settings

Here are the ACPI soft control states available on the SHB. The standard BIOS default is the S1 only (CPU Stop Clock) sleep state. The SHB hardware and BIOS supports both the S1 and S3 sleep states and these sleep states are available for selection at the operating system level.

Option	Description
Enable ACPI Auto Configuration	Disabled /Enabled (bold = default setting)
Enable Hibernation	Disabled/ Enabled
Lock Legacy Resources	Disabled/Enabled
S3 Video Repost	Disabled /Enabled

Trusted Computing Settings

This is where you tell the BIOS that a security device will be used in the system.

Option	Description
Security Device Support	Disabled /Enabled (bold = default setting)
Current Status Information	Status message, specific message displayed depends on the specific setup. There are three possible status messages: No Security Device Found, SUPPORT TURNED OFF or Reset Required.
TPM Enabled Status	Disabled /Enabled
TPM Active Status	Deactivated/Activated
TPM Owner Status	Owned/Unowned
TCM Enabled Status	Disabled /Enabled
TCM Active Status	Deactivated/Activated
TCM Owner Status	Owned/Unowned

WHEA Configuration

Use this setting to enable or disable the Windows Hardware Error Architecture (WHEA).

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

CPU Configuration

Highlighting and selecting either the socket 0 or socket 1 CPU information line on this menu screen will pull-up a sub-menu that displays the specifics of a processor installed in one of these SHB sockets.

Socket 0 or 1 CPU Information	Description
CPU read by the BIOS upon power up. Here is an example for a processor installed in the CPU 0 socket of the SHB: Intel® Xeon® CPU E5-2448L v2 @ 1.8GHz	
CPU Signature	306e4
Microcode Patch	416
Max CPU Speed	1800 MHz
Min CPU Speed	1200 MHz
Processor Cores	10
Intel HT Technology	Supported
Intel VT-x Technology	Supported
Intel SMX Technology	Supported
L1 Data Cache	32kB x 10
L1 Code Cache	32kB x 10
L2 Cache	256kB x 10
L3 Cache	25600kB

CPU Configuration (continued)

The core speed and 64-bit support status are two parameters for the specific Sandy Bridge-EN / Ivy Bridge-EN processors installed on your SHB that are displayed on the second portion of this CPU configuration main menu.

The lower portion of the main menu 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	Disabled/ Enabled - This option allows the user to enable or disable Intel® Hyper-Threading support on the Intel® Xeon® E5-2400 series (i.e. Sandy Bridge-EN / Ivy Bridge-EN) processor. By default, this setting is enabled. (bold = default setting)
Active Processor Cores	All , 1 through 9 - With this setting you may use all of the available cores in the Intel® Xeon® E5-2400/E5-2400 v2 series (i.e. Sandy Bridge-EN / Ivy Bridge-EN) 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.
Limit CPUID Maximum	Disabled/Enabled – Disabled when using a Windows® XP operating system
Execute Disable Bit	Disabled/Enabled – This option allows the user to enable or disable Intel® Execute Disable Bit feature of the Intel® Xeon® E5-2400/E5-2400 v2 series (i.e. Sandy Bridge-EN / Ivy Bridge-EN) processor.
Hardware Prefetcher	Disabled/ Enabled – This setting activates the L2 streamer prefetcher in processor’s cache
Adjacent Cache Line Prefetch	Disabled/ Enabled
DCU Streamer Prefetcher	Disabled/ Enabled
DCU IP Prefetcher	Disabled/ Enabled
Intel® Virtualization	Disabled/ Enabled - This option allows the user to enable or disable Intel® Virtualization support on the Intel® Xeon® E5-2400 series (i.e. Sandy Bridge-EN / Ivy Bridge-EN) processor. By default, this setting is enabled.
PPIN Support	Disabled/Enabled
CPU Power Management	
Power Technology	Custom/Energy Efficient/ Disable
EIST	Disabled/ Enabled (EIST – Enhanced Intel® Speedstep Technology)
Turbo Mode	Disabled/ Enabled
P-STATE Coordination	HW_ALL/SW_ALL/SW_ANY
CPU C3 Report	Disabled/Enabled
CPU C6 report	Disabled/ Enabled
Package C State limit	C0/C2/C6/C7/No Limit
Energy Performance	Balanced Performance/Balanced Energy/Energy Efficient
Factory long duration Power Limit	70W (Status message only, value is CPU dependent)
Long duration Power Limit	0 is the default value, Acceptable value range is 0-255
Factory long duration Maintained	10s (Status message only)
Long duration Maintained	0 is the default value, Acceptable value range is 0-255
Recommended short duration Power Limit	1.2 * Long Duration (Status message only)
Recommended short duration Power Limit	0 is the default value, Acceptable value range is 0-255

Runtime Error Logging Configuration

Use this menu selection to enable or disable the runtime error logging support feature.

Option	Description
Runtime Error Logging	Disabled/Enabled (bold = default setting) - If enabled the following sub-menu option choices are available: Memory Correctable Error Threshold Value: 10 , 11, 12, 13, 14, 15 PCI Error Logging Support: Disabled/Enabled Poison Support: Disabled [fixed setting] Short operational descriptions for each sub-menu setting can be found in the upper left corner of the BIOS set-up screen.

SATA Configuration

This is where you can set the parameters for the SATA devices that have been sensed by the SHB during the boot process. SATA devices connected to ports P27 or P28 on the SHB may operate at data transfer rate up to 600MB/s. SATA devices connected to P31, P32, P35 or P36 have a maximum data transfer rate of 300MB/s. What follows is a list of SATA port configuration parameters.

Option	Description
SATA Mode	Disabled/ IDE Mode/AHCI Mode/RAID (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.
Serial-ATA Controller 0	Disabled/ Enhanced/Compatible
Serial-ATA Controller 1	Disabled/ Enhanced
Serial-ATA Controller 2	Disabled/ Enhanced (Note: This is the SATA controller for the SATA interface routed to the backplane via board edge connector C)
Aggressive Link Power Management	Disabled/ Enabled
Port 0 through 2 Hot Plug	Disabled/Enabled
External SATA Port 0 through 2	Disabled/Enabled
Staggered Spin Up	Disabled/Enabled – There are three of these option selections available.

If the SATA Mode selection is changed to **RAID** then the following sub-menu options are available:

Option	Description
Port 0 through 2 Hot Plug	Disabled/Enabled

SAS Configuration

SHB ports P31, P32, P36 or P36 also support SAS devices. This sub-menu selection is where you configure the system for SAS drives if there are SAS devices connected and sensed by the SHB during the boot process.

Option	Description
SAS Port # [0 – 7]	Not Present/Disabled/Enabled

Thermal Configuration

This sub-menu is an enable/disable selection for initializing the Intel® C604 thermal subsystem device.

Option	Description
Thermal Management	<p>Disabled/Enabled -- If thermal management is enabled, the ME SMBus Thermal Reporting (Disabled/Enabled) selection becomes active and if enabled the following set-up parameters become visible:</p> <p>PCH Temp Read: Disabled, Enabled</p> <p>CPU Energy Temp Read: Disabled, Enabled</p> <p>CPU Temp Read: Disabled, Enabled</p> <p>Alert Enable Lock: Disabled, Enabled (if enabled, the following selections become visible)</p> <p><i>PCH Alert: Disabled, Enabled</i></p> <p><i>DIMM Alert: Disabled, Enabled</i></p>

Intel® TXT (LT-SX) Configuration

Currently these BIOS parameters are fixed and the configuration states are listed on the TXT sub-menu.

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	Enabled/Disabled/Auto
USB3.0 Support	Enabled/Disabled
XHCI Hand-Off	Enabled/Disabled
EHCI Hand-Off	Disabled/Enabled
USB Mass Storage Driver Support	Enabled/Disabled
Port 60/64 Emulation	Disabled/ Enabled
USB Hardware Delays and Timeouts	<p>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:</p> <p>USB Transfer Timeout: 1 sec, 5 sec, 10 sec, 20sec</p> <p>Device Reset Timeout: 10sec, 20sec, 30sec, 40sec</p> <p>Device Power-Up Delay: Auto, Manual (if manual, the following becomes visible)</p> <p><i>Device Power-Up Delay in Seconds: 1 is the default value, 5 is the optimal value, other values may be entered</i></p>

Super IO Configuration

The only Super IO component available in a system implementation using a BXT7059 or BXTS7059 is located on the optional IOB33 module. An IOB33 can plug into the SHBs' P20 I/O Expansion connector. When an IOB33 is plugged into the SHB, the Super IO Configuration set-up parameters will be displayed. This Advanced Setup sub-menu allows you to configure the system ports connected to the IOB33s' Super I/O component.

NOTE: The following Super IO settings are only valid when an optional Trenton IOB33 I/O Board is installed on the BXT7059 or BXTS7059 SHB.

Floppy Disk Controller

This option allows 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. This is the default setting.

Floppy Change Settings

This option allows you to allow the system to automatically select the optimum IO address and IRQ for the floppy drive or you may select a specific device location.

Option	Description
Change Settings	Auto is the default setting, Optional settings include: 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

Floppy Device Mode

This option allows you to enable or disable write-protection of floppy disks.

Option	Description
Read Write	Set this value to allow writing to floppy disks. This is the default setting.
Write Protect	Set this value to prevent writing to floppy disks.

Serial Port 0 Configuration

This option specifies the base I/O port address and Interrupt Request address of serial port 0. The Optimal setting is *3F8/IRQ4*. The Fail-Safe default setting is *Disabled*.

Option	Description
Serial Port	Enabled/Disabled (bold = default setting) , Setting this value Disabled prevents the IOB33's serial port 0 from accessing any system resources. When this option is set to Disabled, serial port 0 physically becomes unavailable.
Change Settings	Auto is the default setting. Auto enables the system to automatically select the optimum IO address and IRQ for the serial port. There are specific device locations available for selection that include: 3F8h/IRQ=4; 3F8h/IRQ=3,4,5,6,7,10,11,12; 2F8h/IRQ=3,4,5,6,7,10,11,12; 3E8h/IRQ=3,4,5,6,7,10,12; 2E8h/IRQ=3,4,5,6,7,10,11,12
Device Mode	Normal/High Speed

Serial Port 1 Configuration

This option specifies the base I/O port address and Interrupt Request address of serial port 1. The Optimal setting is *3F8/IRQ4*. The Fail-Safe default setting is *Disabled*.

Option	Description
Serial Port	Enabled/Disabled (bold = default setting) , Setting this value Disabled prevents the IOB33's serial port 0 from accessing any system resources. When this option is set to Disabled, serial port 0 physically becomes unavailable.
Change Settings	Auto is the default setting. Auto enables the system to automatically select the optimum IO address and IRQ for the serial port. There are specific device locations available for selection that include: 2F8h/IRQ=3; 3F8h/IRQ=3,4,5,6,7,10,11,12; 2F8h/IRQ=3,4,5,6,7,10,11,12; 3E8h/IRQ=3,4,5,6,7,10,12; 2E8h/IRQ=3,4,5,6,7,10,11,12
Device Mode	Normal/High Speed

Super IO Configuration (continued)**Parallel Port Configuration**

This option enables/disables the parallel port on the IOB33 and is used to configure the I/O address and operating mode for the parallel port. The default setting is AUTO, but you may elect to change this as needed.

Option	Description
Parallel Port	Enable/Disable - Set this value to disable prevent the parallel port from accessing any system resources. When the value of this option is set to Disabled, the printer port becomes unavailable. Enabled is the BIOS default setting
Change Settings	The default setting for this operation is AUTO , which allows the board's BIOS to automatically assign system resources to the IOB33 parallel port. You may also select specific IO address and IRQ setting values from the list below: IO=378h; IRQ=5; IO=378h; IRQ=3,4,5,6,7,10,11,12; IO=278h; IRQ=3,4,5,6,7,10,11,12; IO=3BCh; IRQ=3,4,5,6,7,10,11,12; IO=378h; IO=278h; IO=3BCh; Note: The majority of parallel ports on computer systems use IRQ7 and I/O Port 378H as the standard setting.
Device Mode	Standard (STD) Printer Mode is the default value for this print mode selection. Other parallel printer operating modes available are: SPP Mode EPP-1.9 and SPP Mode EPP-1.7 and SPP Mode ECP Mode ECP-1.9 and SPP Mode ECP-1.7 and SPP Mode The EPP modes enable the parallel port to be used with devices that adhere to the Enhanced Parallel Port (EPP) specification. EPP uses the existing parallel port signals to provide asymmetric bi-directional data transfer driven by the host device. The ECP modes enable the parallel port to be used with devices that adhere to the Extended Capabilities Port (ECP) specification. ECP uses the DMA protocol to achieve data transfer rates up to 2.5 Megabits per second. ECP provides symmetric bi-directional communication.

AMT Configuration

This BIOS menu selection is used to enable/disable Intel AMT 7.0/8.0 support on the SHB. The default setting for the Intel AMT configuration setting is: *Enabled*. The table below lists the board configuration settings related to Intel AMT support.

Option	Description
AMT	Enable/Disable -- Default setting is Enabled .
Un-configure AMT/ME	Enable/Disable -- Default setting is Disabled . When enabled this setting allows you to configure the management engine associated with Intel AMT operations without requiring a password. Use caution when enabling this setting.
Watchdog Timer (WDT)	Enable/Disable -- Default setting is Disabled . When enabled you may input operating system and BIOS time-out values
OS WDT Timer	Input a valid timer value between 0 and 65535 – (Note: The setup parameter is only visible when the WDT value is enabled.)
BIOS WDT Timer	Input a valid timer value between 0 and 65535– (Note: The setup parameter is only visible when the WDT value is enabled.)

Serial Port Console Redirection Configuration

The SHB must have an optional IOB33 installed in order for this BIOS setting to apply. Serial port console redirection is available for use on the IOB33's COM0 and COM1 serial communication ports.

Option	Description
Console Redirection Settings	Use this setting to specify how the system is to re-direct data to the out-of-band management port. Out-of-Band Management Port: COM0, COM1(PCI Bus, DEV0,FUNC0) (Disabled) Terminal Type: VT100, VT100+, VT-UTF8, ANSI Bits per second: 9600, 19200, 57600, 115200 Flow Control: None, Hardware RTS/CTS Data Bits: Fixed at 8 Parity: Fixed at None Stop Bits: Fixed at 1
COM0 Console Redirection	Enabled / Disabled -- Default setting is Enabled . Note: The console redirection settings shown below will be unavailable if the Disabled option is selected.
COM0 Console Redirection Settings	Use this setting to specify how the host computer and the remote computer will exchange data via the COM0 port. Both computers need to have compatible settings. Here are the available COM0 settings: Terminal Type: VT100, VT100+ , VT-UTF8, ANSI Bits per second: 9600, 19200, 38400, 57600, 115200 Data Bits: 7, 8 Parity: None , Even, Odd, Mark, Space Stop Bits: 1, 2 Flow Control: None , Hardware RTS/CTS VT-UTF8Combo Key Support: Disabled, Enabled Recorder Mode: Disabled, Enabled Resolution 100x31: Disabled, Enabled Legacy OS Redirection: 80x24 , 80x25 Putty Keypad: VT100 , LINUX, XTERMR6, SCO, ESCN, VT400 Redirection After BIOS: Always Enable , BootLoader
COM1 Console Redirection	Enabled / Disabled -- Default setting is Enabled . Note: The console redirection settings shown below will be unavailable if the Disabled option is selected.
COM1 Console Redirection Settings	Use this setting to specify how the host computer and the remote computer will exchange data via the COM1 port. Both computers need to have compatible settings. Here are the available COM1 settings: Terminal Type: VT100, VT100+ , VT-UTF8, ANSI Bits per second: 9600, 19200, 38400, 57600, 115200 Data Bits: 7, 8 Parity: None , Even, Odd, Mark, Space Stop Bits: 1, 2 Flow Control: None , Hardware RTS/CTS VT-UTF8Combo Key Support: Disabled, Enabled Recorder Mode: Disabled, Enabled Resolution 100x31: Disabled, Enabled Legacy OS Redirection: 80x24 , 80x25 Putty Keypad: VT100 , LINUX, XTERMR6, SCO, ESCN, VT400 Redirection After BIOS: Always Enable , BootLoader

iSCSI Configuration

Option	Description
iSCSI Initiator Name	Enter a unique name for the iSCSI initiator. After entering a unique name the following iSCSI setup parameters may be entered: Add an attempt, Delete an attempt and Change attempt order

This page intentionally left blank

Chapter 3 Chipset Configuration Setup

Introduction

The term “chipset” is a bit of a misnomer for the Trenton BXT7059 and BXTS7059. The “chipset” on these SHBs is really a single component called a “Platform Controller Hub” or PCH, and the Trenton BXT7059 and BXTS7059 both feature the Intel® C604 PCH. The PCH; developed under the code name Patsburg-B, combines many of the capabilities that were previously contained in individual North Bridge and South Bridge chipset components. The following section covers the set-up parameters of what could be thought of as the North Bridge and South Bridge sections of the Intel® C604 Platform Controller Hub.

North Bridge Configuration

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

Option	Description
Sandy Bridge-EN / Ivy Bridge-EN IOH Configuration	<p>The Input Output Hub (IOH) configuration menu allows the user to view, enable or disable the Intel® Virtualization Technology for Directed I/O feature of the processors. This menu selection is also used to configure the PCI Express links out of the CPUs. Short operational descriptions for each sub-menu setting can be found in the upper left corner of the BIOS set-up screen. The following sub-menu option choices are available for configuration:</p> <p>Intel® VT for Directed I/O Configuration – Disabled/Enabled (bold = default setting)</p> <p>The following configuration choices are available if Intel VT-d is enabled: Coherency Support: Disabled/Enabled ATS Support: Disabled/Enabled</p> <p>Intel® I/O Acceleration Technology (I/OAT): Disabled/Enabled DCA (Direct Cache Access) Support: Disabled/Enabled VGA Priority: Offboard Target VGA: Currently fixed at VGA from CPU0 GEN3 Equalization WA’s (workarounds): Disabled/Enabled – If enabled, the following four parameters become visible: <i>Gen3 Equalization Fail WA: Disabled/Enabled</i> <i>Gen3 Equalization Phase 2/3 WA: Disabled/Enabled</i> <i>Equalization Phase 2/3 Supported: Disabled/Enabled</i> <i>Gen3 Equalization Redoing WA: Disabled/Enabled</i></p> <p>IOH Resource Selection: Auto/Manual No Snoop Optimization: VCO/VCP/VC1 / VC1 MMIOH Size: 1G, 2G, 4G, 8G, 16G, 32G, 64G, 126G MMCFG Base: 0x80000000, 0xA0000000, 0xC0000000</p> <p>PICMG PCIe Port Bifurcation Control: PCH Uplink Link Speed: GEN1, GEN2, GEN3 IOB Link Speed: GEN1, GEN2, GEN3 PICMG/PEX10 Port “Ax”: x4x4x4x4, x4x4x8, x8x4x4, x8x8, x16</p> <p>PICMG PCIe port Data Direct I/O Control: PCH Uplink Port: Disabled/Enabled IOB Port: Disabled/Enabled PICMG/PEX10 Port A0: Disabled/Enabled PICMG/PEX10 Port A1: Disabled/Enabled PICMG/PEX10 Port A2: Disabled/Enabled PICMG/PEX10 Port A3: Disabled/Enabled</p>

	<p>PEX10 PCIe port Bifurcation Control: PICMG/PEX10 Port "Ax": x4x4x4x4, x4x4x8, x8x4x4, x8x8, x16 Port A0 Link Speed: GEN1, GEN2, GEN3 Port A1 Link Speed: GEN1, GEN2, GEN3 Port A2 Link Speed: GEN1, GEN2, GEN3 Port A3 Link Speed: GEN1, GEN2, GEN3</p> <p>PEX10 PCIe port Data Direct I/O Control: PICMG/PEX10 Port A0: Disabled/Enabled PICMG/PEX10 Port A1: Disabled/Enabled PICMG/PEX10 Port A2: Disabled/Enabled PICMG/PEX10 Port A3: Disabled/Enabled</p> <p>Note: The number of link speed selections made visible will vary based on the PCIe port selection; e.g. the x4x4x4x4 option will yield four PCIe link speed selections. No speed selections are seen with the Auto option because the SHB / backplane combination will auto-negotiate link bifurcation and link speed.</p>
<p>QPI Configuration</p>	<p>This option allows the user to view, select or set to auto the link frequency of the Intel® Quick Path Interconnect or Intel QPI between the dual processors on a BXT7059 board. The two status messages listed at the top of this menu indicate the current stat of the QPI interface as a function of the installed processors and previous QPI link settings. Here is an example of two status messages: Current QPI Link Speed – Fast Current QPI Link Frequency – 8.0GT/s</p> <p>Trenton recommends using the QPI link defaults. Isoc: Disabled/Enabled MesegEn: Disabled/Enabled/Auto QPI Link Speed Mode: Slow, Fast QPI Link Frequency Select: Auto, 6.4GT/s, 7.2GT/s, 8.0GT/s QPI LinkOs: Disabled/Enabled QPI LinkOp: Disabled/Enabled QPI Link1: Disabled/Enabled Snoop Mode: Early Snoop, Home Snoop, Home Directory Snoop, Home Directory Snoop with OSB, Auto</p>
<p>Compatibility RID</p>	<p>Disabled/Enabled</p>
<p>Memory Configuration</p>	<p>The upper portion of this BIOS menu lists the specific memory DIMM(s) that are installed in the board and sensed upon start up as well the current memory interface configuration settings or BIOS defaults. Listed below are the available memory configuration parameters: Memory Mode: Independent, Mirroring, Lock Step, Sparing DRAM RAPL BWLIMIT: 0, 1, 8, 16 Perfmon and DEX Devices: Hide, Unhide DRAM RAPL Mode: Disabled, DRAM RAPL MODE0, DRAM RAPL MODE1 NUMA: Disabled/Enabled MPST Support: Disabled/Enabled Enforce POR: Disable/Auto Pdg Length: Standard/Short DDR Speed: Auto, Force DDR3 800, Force DDR3 1066, Force DDR3 1333, Force DDR3 1600, Force DDR3 1866 Channel Interleaving: Auto, 1 Way, 2 Way, 3 Way, 4 Way Rank Interleaving: Auto, 1 Way, 2 Way, 3 Way, 4 Way, 8 Way</p>

	<p>Memory configuration parameters continued: Patrol Scrub: Disabled/Enabled Demand Scrub: Disabled/Enabled Data Scrambling: Disabled/Enabled Device Tagging: Disabled/Enabled Rank Margin: Disabled/Enabled Thermal Throttling: Disabled, OLTT, CLTT OLTT Peak BW %: valid values are between 25 and 100, Default = 50 Altitude: Auto, 300M, 900M, 1500M, 3000M Serial Message Debug Level: Disabled, Minimum, Maximum, Trace, Memory Training</p> <p>DIMM Information: This is an informational menu screen that displays the memory channels and nodes for each processor along with any DIMM information that is read by the BIOS during the boot process.</p>
--	--

South Bridge Configuration

The upper porting of the menu screen provides PCH product code name and the stepping of the particular Intel® C604 PCH this is installed on the board. Accessing the *South Bridge Configuration* option allows the user to do configure the following parameters:

Option	Description
PCH Compatibility RID	Disabled /Enabled is the option parameter choice for this selection. Any option selection listed with bold text indicates that this is the BIOS default setting.
SMBus Controller	This option allows the user to enable or disable the SMBus Controller in the Intel® C604.
SW SMI Timer	Disabled/ Auto
GbE Controller	Disabled/ Enabled - This internal controller provides the LAN interface that is routed via the Intel® 82579LM Ethernet PHY to board’s edge connector C for use on a PICMG 1.3 backplane. This setting does not affect the operation of the independent Intel® i350 Ethernet Controller that drives the two LAN ports on the SHB’s 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
USB WakeOnDev insertion	Disabled /Enabled
Restore AC Power Loss	This option allows the user to determine how the system will come back up when power is restored after an unplanned power interruption. The available options are: Power Off, Power On or Last State.
SLP_S4Assertion Stretch Enable	Disabled/ Enabled The following sub-menu selection is available when this parameter is enabled: SLP_S4 Assertion Width: 1-2 seconds, 2-3 seconds, 3-4 seconds, 4-5 seconds
Deep Sx	This setting supports the deep sleep S4 and S5 states primarily used in mobile devices. The available options include: Disabled , Enabled in S5(Battery), Enabled in S5, Enabled in S4 and S5(Battery), Enabled in S4 and S5
Disable SCU Devices	Disabled /Enabled
Onboard SAS Oprom/Driver	Disabled /Enabled
Onboard SATA RAID Oprom/Driver	Disabled/ Enabled
High Precision Event Timer	Disabled/ Enabled

South Bridge Configuration (continued)	
PCI Express Ports Configuration	<p>These settings are available for configuring the PCI Express links used for component interconnects on the board and for the B0 PCIe link routed to the SHB's edge connector. The default setting for each port is set to Auto and Trenton highly recommends leaving these settings alone. These internal PCIe ports drive on-board components and turning them off will disable critical SHB and system functions</p> <p>The available options include:</p> <p>PCI Express Port 1: Disabled, Enabled, Auto <i>PME SCI: Disabled, Enabled</i></p> <p>PCI Express Port 2: Disabled, Enabled, Auto <i>PME SCI: Disabled, Enabled</i></p> <p>PCI Express Port 3: Disabled, Enabled, Auto <i>PME SCI: Disabled, Enabled</i></p> <p>PCI Express Port 4: Disabled, Enabled, Auto <i>PME SCI: Disabled, Enabled</i></p> <p>PCI Express Port 5: Disabled, Enabled, Auto <i>PME SCI: Disabled, Enabled</i></p> <p>PCI Express Port 6: Disabled, Enabled, Auto <i>PME SCI: Disabled, Enabled</i></p> <p>PCI Express Port 7: Disabled, Enabled, Auto <i>PME SCI: Disabled, Enabled</i></p> <p>PCI Express Port 8: Disabled, Enabled, Auto <i>PME SCI: Disabled, Enabled</i></p>
PCI Sub Decode	<p>Disabled/Enabled – If enabled the following sub-menu selection appears. <i>Port Select: PCI Express Port 1, PCI Express Port 2, PCI Express Port 3, PCI Express Port 4, PCI Express Port 5, PCI Express Port 6, PCI Express Port 7, PCI Express Port 8</i></p>
DMI Vc1 Control	Disabled/ Enabled
DMI Vcp Control	Disabled/ Enabled
DMI Vcm Control	Disabled/ Enabled
USB Configuration	<p>This option allows the user to Enable or Disable the various USB ports inside the Intel® C604 PCH. These internal USB ports drive the USB interface connections to the SHBs I/O plate and down to edge connector C for us on a PICMG 1.3 backplane.</p> <p>The available option parameters include:</p> <p>All USB Devices: Disabled/Enabled</p> <p>EHCI Controller 1: Disabled/Enabled</p> <p>EHCI Controller 2: Disabled/Enabled</p> <p>USB Port #: Disabled/Enabled -- Note: # equals the USB port number of 0 through 13</p>

Intel ME System

The Intel® Management Engine or Intel® ME is a portion of the Intel® C604 firmware stored in the boards SPI devices and is used in conjunction such features Intel® AMT and the PCI Express GEN3 link parameters.

Option	Description
Intel ME Subsystem	<p>Exercise caution if you elect to change the following default parameters:</p> <p>ME Sub System: Disabled/Enabled</p> <p>ME Temporary Disable: Disabled/ Enabled</p> <p>End of Post Message: Disabled/Enabled</p> <p>Execute MEBx: Disabled/Enabled</p>

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

Enter the number of seconds you wish the board to wait for a setup key activation key.

Option	Description
Setup Prompt Timeout	Acceptable values: 0 to 65535 (0xFFFF) and the default value is 1 Note: 65535 means the BIOS will wait indefinitely for a key press
Bootup Numlock State	On/Off – Selects the keyboard numlock state
Quiet Boot	Disabled/Enabled - this default value allows the computer system to display the POST messages. The enabled option is used for displaying a custom OEM logo during POST.
Fast Boot	Disabled/Enabled – this default setting allows the computer system to perform a full boot with a full set of devices. In full configuration mode, all devices are detected and initialized. The enabled option allows the computer system to do a minimal boot. In minimal configuration mode, only the devices that are necessary to boot the system are detected and initialized as defined in the option settings below: <i>VGA Support: Auto/EFI Driver</i> <i>USB Support: Disabled/Full Initial/Partial Initial</i> <i>PS2 Support: Disabled/ Enabled</i> <i>Network Stack Driver Support: Disabled/ Enabled</i>

Boot Option Priorities

The following settings allow you to set the system boot priority of where to pull the BIOS settings from in order to perform a system boot. You can set four priority levels and the number of available options within each priority is based on the devices connected to the SHB. Here is an example of potential boot options.

Option	Description
Boot Option Priorities	Boot Option #1: IBA GE Slot 00C8 v1395 , IBA GE Slot 0900 v1395, IBA GE Slot 0901 v1395, UEFI: Built-In EFI Shell, Disabled Boot Option #2: IBA GE Slot 00C8 v1395, IBA GE Slot 0900 v1395 , IBA GE Slot 0901 v1395, UEFI: Built-In EFI Shell, Disabled Boot Option #1: IBA GE Slot 00C8 v1395, IBA GE Slot 0900 v1395, IBA GE Slot 0901 v1395 , UEFI: Built-In EFI Shell, Disabled Boot Option #1: IBA GE Slot 00C8 v1395, IBA GE Slot 0900 v1395, IBA GE Slot 0901 v1395, UEFI: Built-In EFI Shell , Disabled

Any other devices connected to SHB and the system would show up under each option in the above listing. Other possible boot option devices are: SATA Hard Drive [HD type info], and USB Flash Hub [USB type info].

CSM16 Parameters

These are special purpose BIOS settings and should remain in the default positions.

Option	Description
CSM16 Parameters	Gate20 Active: Upon Request , Always Option ROM Messages: Force BIOS , Keep Current INT19 Trap Response: Intermediate , Postponed

CSM Parameters

The Compatibility Support Module (CSM) parameters are used for BIOS compatibility with non-UEFI compliant operating systems.

Option	Description
Launch CSM	Disabled/ Enabled
Boot Option Filter	UEFI and Legacy , Legacy Only, UEFI Only
Launch PXE OpROM policy	Do not launch, UEFI only, Legacy only , Legacy first, UEFI first
Launch Storage OpROM	Do not launch, UEFI only, Legacy only , Legacy first, UEFI first
Launch Video OpROM policy	Do not launch, UEFI only, Legacy only , Legacy first, UEFI first
Other PCI Device ROM	UEFI OpROM , Legacy OpROM

This page intentionally left blank

Chapter 5 Security

Two Levels of Password Protection

Security Setup provides both a Supervisor and a User password. If you use both passwords, the Supervisor 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 Supervisor and User passwords activate two different levels of password security. If you select password support, you are prompted for a 3-20 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
User Password	This option allows the user to set a user level password for the BIOS.
Admin Password	This option allows the user to set an administrative 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]
(i.e. load previous values)		

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 such as a SATA HDD or from the BIOS' UEFI Shell.

Save configuration and reset?

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

This page intentionally left blank

Chapter 7 Event Logs

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.

Change Settings – Enabling/Disabling Options

Option	Description
Smbios Event Log	Enabled/Disabled
Erasing Settings	
Erase Event Log	No/Yes-Next Reset/Yes-Every Reset
When Log Is Full	Do Nothing/Erase Immediately
Smbios Event Log Standard Settings	
Log System Boot Event	Enabled/Disabled
MECI	1
METW	60
Custom Options	
Log OEM Codes	Enabled/Disabled
Convert OEM Codes	Enabled/Disabled

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 date and time that the event occurred 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 BXT7059 and BXTS7059 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.

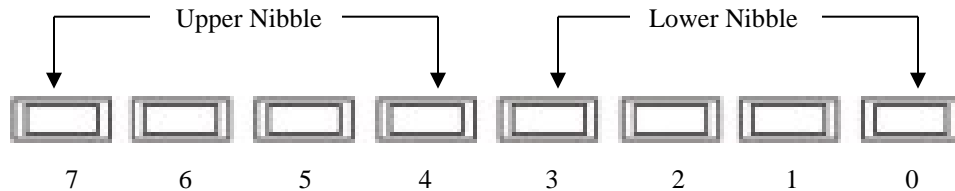
BIOS Status POST Code LEDs

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 BXT7059 and BXTS7059 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



BXT7059 & BXTS7059 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