MBC8240

8240-xxx

No. 87-508240-000 Revision A

BIOS and Trenton Smart System Management

TECHNICAL REFERENCE

Aptio® 4.x Test Setup Environment (TSE)

For use with MBC8240

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

Dual and Quad Core

PROCESSOR-BASED

Modular Blade Card

WARRANTY

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

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

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

RETURN POLICY

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

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

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

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

Trenton Systems, Inc.
2350 Centennial Drive
Gainesville, GA 30504
Attn: Repair Department

Contact Trenton Systems for our complete service and repair policy.

TRADEMARKS

IBM, PC/AT, VGA, EGA, OS/2 and PS/2 are trademarks or registered trademarks of International Business Machines Corp.
AMI, Aptio, AMIBIOS, MegaRAC SP-X and YAFU 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.
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

CARD Handling Precautions

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

To protect your processor card (CARD) from electrostatic damage, be sure to observe the following precautions when handling or storing the board:

- Keep the CARD in its static-shielded bag until you are ready to perform your installation.
- Handle the CARD by its edges.
- Do not touch the I/O connector pins.
- Do not apply pressure or attach labels to the CARD.
- 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 CARD 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 MBC8240 and feature the Aptio® 4.x BIOS from American Megatrends, Inc. (AMI) with a ROM-resident setup utility called the Aptio® Text Setup Environment or TSE. The TSE allows you to select to the following categories of options:

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

Each of these options allows you to review and/or change various setup features of your system. Details are provided in the following chapters of this manual. Additional copies of the Trenton MBC8240 BIOS and hardware technical reference manuals are available under the **Downloads** tab on the MBC8240 web page.

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: Portions 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 CARD 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 MBC8240 implementation of the Aptio TSE BIOS utility. Contact Trenton Technical support for any questions regarding the CARDs' implementation of Aptio TSE.

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

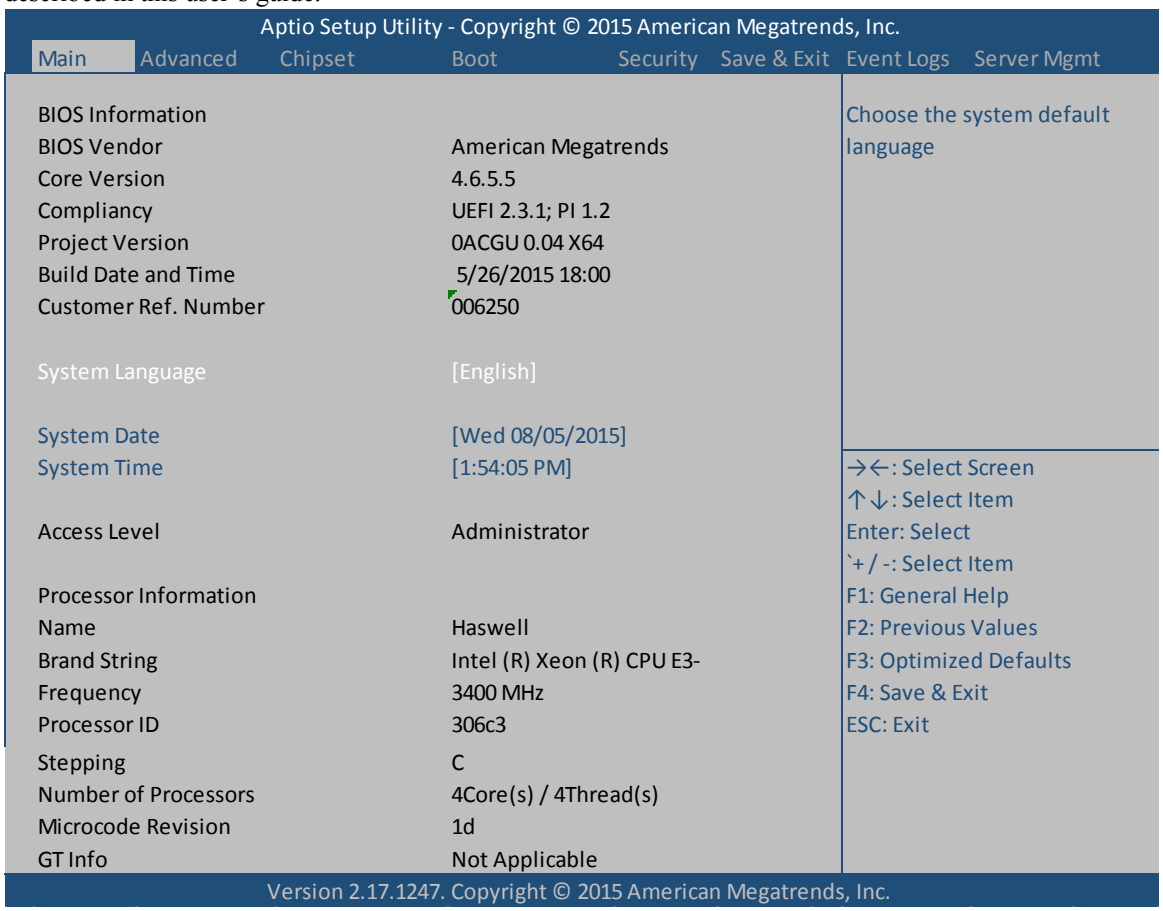
Step	Description
1	Install the CARD into a system with a compatible midplane setup such as the Trenton MPI8241 or TMI8254with the proper system power connections made to the midplane and a mouse, keyboard and monitor connected to the CARD
2	Power on the system with the CARD
3	Press the <Delete> or <ESC> key on your keyboard when you see the following text prompt: Press DEL or F2 to enter Setup
4	After you press the <Delete>/<ESC> 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 <ESC> keys are used to invoke the Aptio TSE screen. There are a few cases that other keys are used (<F1>, <F10>, <F11>).

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 MBC8240 BIOS modifications. Contact Trenton Technical support for any questions regarding the CARDs' implementation of Aptio TSE.

Navigation

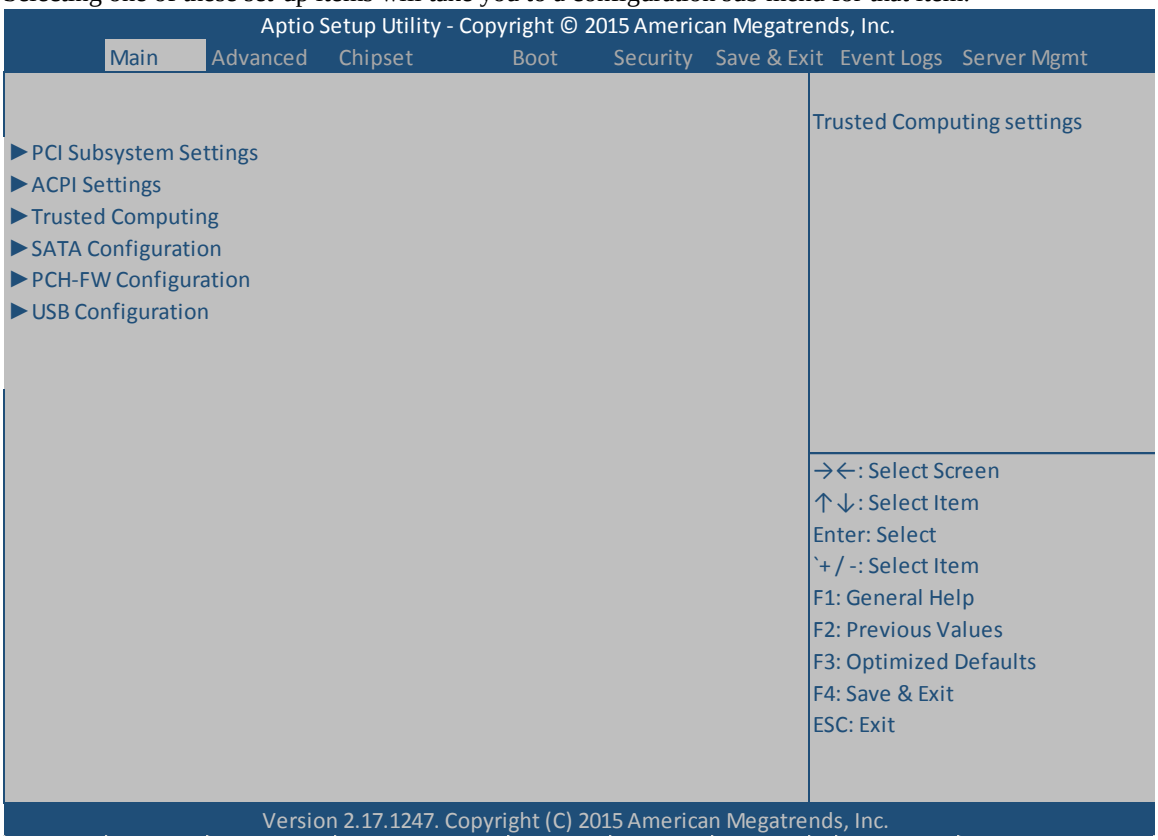
The Aptio® TSE keyboard-based navigation can be accomplished using a combination of the keys.(<FUNCTION> keys, <ENTER>, <ESC>, <ARROW> keys, etc.).

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

Chapter 2 Advanced Setup

Introduction

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



PCI Sub-System Settings

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

Option	Description
PCI Subsystem Settings	
PCI Bus Driver Version	V2.05.02 (This is a static message, informational only, no user selectable option)
PCI 64bit Resources Handling	
Above 4G Decoding	**Disabled**/Enabled ***(bold** = default setting)* – The system design needs to support 64-bit PCI decoding for this setting to be meaningful. Enabling the setting allows the CARD to decode the 64-bit capable devices connected to the CARD the 4G-address space. Use caution when enabling this system BIOS parameter.

ACPI Settings

The Advanced Configuration and Power Interface allows the Operating System to control certain elements of the computer hardware for power control and communication processes.

Option	Description
ACPI Settings	
Enable ACPI Auto Configuration	**Disabled**/Enabled – Enables or disables BIOS ACPI Auto Configuration
Enable Hibernation	**Disabled**/Enabled – Enables or disables system ability to Hibernate (OS/S4 Sleep State). This option may not be effective with some operating systems
ACPI Sleep State	**Suspend Disabled/**S3 only (Suspend to RAM)/Both S1 and S3 available for OS to choose from – Select ACPI sleep state the system will enter when the SUSPEND button is pressed
Lock Legacy Resources	**Disabled**/Enabled – Enables or disables lock of legacy resources
S3 Video Repost	**Disabled**/Enabled – Enable or disable S3 video repost

Trusted Computing

The Advanced Configuration and Power Interface allows the Operating System to control certain elements of the computer hardware for power control and communication processes.

Option	Description
Security Device Support	**Enable**/Disable – Enables or disables BIOS support for security devices. Operating system will not show Security Device. TCG EFI protocol and INT1A interface will not be available.
TPM20 Device Found	This is a static, user-information field.
Hash Policy	[Sha-1] This is a static, user information field that depicts the current encryption scheme in use by the security device.

SATA Configuration

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

Option	Description
SATA Controller(s)	Disabled/**Enabled (bold** = default setting) - Short operational descriptions for each sub-menu setting can be found in the upper left corner of the BIOS set-up screen.
SATA Mode Selection	IDE/**AHCI**/RAID
SATA Test Mode	**AHCI**/RAID

Aggressive LPM Support	Disabled/**Enabled** (Enables PCH to aggressively enter link power state)
Serial ATA Port n (n= 0,1,2,3,4 or 5)	Software Preserve: Static diagnostic message, message depends on SATA drive connection upon boot, **Unknown** can be expected if no drive is present during system boot. **SUPPORTED** will be reported if the target drive supports Software Preserve. **UNSUPPORTED** will be reported if the target drive does not support Software Preserve.
	Port 0: Disabled/**Enabled –** Enables or disables operation of specific SATA port.
	Hot Plug: **Disabled**/Enabled -- Enables or disables Hot Plug capability.
	Mechanical Presence Switch: **Disabled**/Enabled – Controls reporting of mechanical presence switches for this port. Note: This capability requires additional hardware support.
	External SATA: **Disabled**/Enabled – Enables or disables reporting of External SATA capability of this port.
	SATA Device Type: **Hard Disk Drive**/Solid State Drive – Selects between magnetic and solid state storage drive types.
	Spin Up Device: **Disabled**/Enabled – Upon an edge detection from 0 to 1, the PCH starts a COMRESET initialization sequence for the device.

Platform Controller Hub (PCH-FW Configuration)

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

Option	Description
ME FW Version	9.1.20.1035 (This is a static message, informational only, no user selectable option.)
►Firmware Update Configuration	Me FW Image Reflash: **Disabled**/Enabled – Enables or disables the Management Engine firmware re-flash function.

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	10 Drives, 2 Keyboards , 2 Mice, 2 Hubs – Status message that is variable based on the USB devices connected to the system and read by the BIOS on boot-up
Legacy USB Support	Disabled/**Enabled/**Auto – Enables Legacy USB support. Auto option disables legacy USB support if no USB devices are connected. Disable option will keep the USB devices available only for EFI applications.
XHCI Hand-off	Disabled/**Enabled** – Enables or disables this workaround for Operating Systems without XHCI hand-off support. The XCHI ownership changes should be claimed by a XHCI driver.
EHCI Hand-Off	**Disabled**/Enabled – Enables or disables this workaround for Operating Systems without EHCI hand-off support. The EHCI ownership changes should be claimed by anEHCI driver.
USB Mass Storage Driver Support	Disabled/**Enabled** – Enables or disables USB Mass Storage Driver support.
USB Hardware Delays and Timeouts	The following sub-menu selections are used to configure data transfer delays and timeouts needed for the USB storage devices used in the system design: USB Transfer Timeout: 1 sec, 5 sec, 10 sec, **20sec** Device Reset Timeout: 10sec, **20sec**, 30sec, 40sec Device Power-Up Delay: ***Auto***, *Manual* -- If manual is selected the available options in seconds are 1-40secs with 5secs as the default value Device power-up delay in seconds: **5**
Mass Storage Devices	The following sub-menu selections are used to configure the USB Mass Storage Devices attached via USB. AMI Virtual CDROM0 1.00 – **Auto**/Disabled AMI Virtual Floppy0 1.00 – **Auto**/Disabled AMI Virtual HDisk0 1.00 – **Auto**/Disabled AMI Virtual CDROM1 1.00 – **Auto**/Disabled AMI Virtual CDROM2 1.00 – **Auto**/Disabled AMI Virtual CDROM3 1.00 – **Auto**/Disabled

	AMI Virtual Floppy1 1.00 – **Auto**/Disabled AMI Virtual Floppy2 1.00 – **Auto**/Disabled AMI Virtual Floppy3 1.00 – **Auto**/Disabled AMI Virtual HDisk1 1.00 – **Auto**/Disabled

This page intentionally left blank

Chapter 3 Chipset Configuration Setup

Introduction

The term "chipset" is a bit of a misnomer for the Trenton MBC8240. The "chipset" on this CARD is a single component called a "Platform Controller Hub" or PCH. Some of the traditional "chipset" functions have migrated into the Haswell processor's micro-architecture. The MBC8240 features the Intel® C226 PCH. This platform controller hub merges the former South Bridge chipset component functionality with the North Bridge functionality not handled by the Haswell processor. The following sections cover the new set-up parameters for the single chip Intel® C226 PCH and are labeled: PCH-IO Configuration and System Agent (SA) Configuration

PCH-IO Configuration

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

Option	Description
Intel PCH RC Version	1.1.0.1 **(**Static message – informational only, no user configuration settings)
Intel PCH SKU Name	C226 **(**Static message – informational only, no user configuration settings)
Intel PCH Rev ID	05/c2 **(**Static message – informational only, no user configuration settings)
►USB Configuration (submenu)	USB Precondition: ***Disabled****/Enabled* XHCI Mode: **Smart Auto**/Auto/Enabled/Disabled BTCG: Disabled/**Enabled** EHCI1: Disabled/**Enabled** EHCI2: Disabled/**Enabled** USB Ports Per-Port Disable Control: **Disabled**/Enabled (If enabled then the following selections become visible) USB Port #0 Disable: *Disabled/****Enabled*** USB Port #1 Disable: *Disabled/****Enabled*** USB Port #2 Disable: *Disabled/****Enabled*** USB Port #3 Disable: *Disabled/****Enabled*** USB Port #4 Disable: *Disabled/****Enabled*** USB Port #5 Disable: *Disabled/****Enabled*** USB Port #6 Disable: *Disabled/****Enabled*** USB Port #7 Disable: *Disabled/****Enabled*** USB Port #8 Disable: *Disabled/****Enabled*** USB Port #9 Disable: *Disabled/****Enabled*** USB Port #10 Disable: *Disabled/****Enabled*** USB Port #11 Disable: *Disabled/****Enabled*** USB Port #12 Disable: *Disabled/****Enabled*** USB Port #13 Disable: *Disabled/****Enabled***
►BIOS Security Configuration (submenu)	BIOS Security Configuration SMI Lock: Disabled/**Enabled –** Enables or disables SMI Lock functionality. BIOS Lock: **Disabled**/Enabled – Enables or disables BIOS Lock functionality. GPIO Lock: **Disabled**/Enabled – Enables or disables GPIO Lock functionality. BIOS Interface Lock: Disabled/**Enabled –** Enables or disables BIOS Interface Lock functionality. RTC Lock: Disabled/**Enabled** – Enables or disables bytes 38h-3Fh in the upper and lower 128 byte bank of RTC RAM lockdown.
Restore AC Power Loss	Power Off/Power On/**Last State**

System Agent (SA) Configuration

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

Option	Description
VT-d Capability	Supported **(**Static message – informational only, no user configuration settings)
VT-d	Disabled/**Enabled –** Enable to allow the VT-d function on MCH.

This page intentionally left blank

Chapter 4 Boot Setup

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

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

Option	Description
Setup Prompt Timeout	**5 (bold** = default setting) A numeric value of 5 is the default setting with a range of 1 to 65355 entered is in seconds being valid inputs. A value of 65355 or FFFFh means an indefinite wait period
Bootup NumLock State	The default setting is ***On*** with an option to turn the setting *Off*. The *On* setting enables the keyboard to automatically enabled at system boot and allows the immediate use of the 10-key numeric keypad located on the right side of the keyboard. In the Off setting, the NumLock keyboard key will need to be pressed to use the 10-key numeric pad.
Quiet Boot	**Disabled**/Enabled – Prevents system speaker from alerting user to BIOS errors upon boot
Fast Boot	**Disabled**/Enabled – Enables or disables Fast Boot capability
Boot Option Priorities	Boot Option Priorities Boot Option #1: P4:ST3160316AS (UEFI: Built-In EFI Shell, P4:ST3160316AS, Disabled) Boot Option #2: UEFI: Built-In EFI Shell (UEFI: Built-In EFI Shell, P4:ST3160316AS, Disabled) Note: ST3160316AS is the boot drive identifier in this particular test lab set-up. Your particular boot drive identifier will be different.
►CD/DVD ROM Drive BBS Priorities	Boot Option #1 [P2: HL-DT-ST DVDRAM…] Boot Option #2 [AMI Virtual CDROM0 …] Boot Option #3 [AMI Virtual CDROM1 …] Boot Option #4 [AMI Virtual CDROM2 …] Boot Option #5 [AMI Virtual CDROM3 …] Note: HL_DT_ST DVDRAM is the optical drive identifier in this particular test lab set-up. Your particular boot drive identifier will be different.
►Hard Drive BBS Priorities	Boot Option #1 [P1: WDC WD5000BPKT-…] Boot Option #2 [AMI Virtual HDisk0 …] Boot Option #3 [AMI Virtual HDisk1 …] Note: WDC WD5000BPKT is the hard drive identifier in this particular test lab set-up. Your particular boot drive identifier will be different.
►Floppy Drive BBS Priorities	Boot Option #1 [AMI Virtual Floppy0 …]
►CSM16 Parameters	CSM16 Module Version: 07:70 **(**Static message – informational only, no user configuration settings) *The following are special purpose BIOS settings and should remain in the default positions. Contact Trenton's technical support team if you need to use these BIOS settings.* GateA20 Active: **Upon Request** (**Upon Request**, Always) Option ROM Messages: **Force BIOS** (**Force BIOS**, Keep Current) INT19 Trap Response: **Immediate** (**Immediate**, Postponed)
►CSM Parameters	Launch CSM: Disabled/**Enabled** Boot option filter: **UEFI and Legacy** (**UEFI and Legacy**, Legacy Only, UEFI Only) Launch PXE OpROM policy: **Do Not Launch** (**Do Not Launch**, UEFI Only, Legacy Only) Launch Storage OpROM policy: **Legacy Only** (Do Not Launch, UEFI Only, **Legacy Only**) Launch Video OpROM policy: **Legacy Only** (Do Not Launch, UEFI Only, **Legacy Only**, Legacy First, UEFI First) Other PCI device ROM priority: **UEFI OpROM** (**UEFI OpROM**, Legacy OpROM)

This page intentionally left blank

Chapter 5 Security

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

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

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

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

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

Option	Description
Administrator Password	This option allows the user to set an administrative level password for the BIOS. BIOS access passwords must be between 3 and 20 characters in length.
User Password	This option allows the user to set a user level password for the BIOS.
HDD Security Configuration	This option allows the user to identify and secure a system's HDD such as the one we used in our test lab set-up: P1: WDCWD5000 BP
HDD Password	This option allows the user to set a user level password for a system's HDD: Security Supported: Yes Security Enabled: No Security Locked: No HDD User Pwd Status: Not Installed HDD Master Pwd Status: Installed Set User Password

This page intentionally left blank

Chapter 6 Saving and Exiting BIOS Setup and Restoring Defaults

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

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

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

Save Configuration Changes and Exit Now?

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

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

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

Discard Changes and Exit Setup Now?

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

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

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

Save Configuration Changes and Exit Now?

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

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

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

Discard Configuration Changes and Exit Now?

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

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

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

The following menu options for BIOS defaults are available:

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

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

Restore Defaults?

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

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

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

Save as User Defaults?

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

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

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

Restore User Defaults?

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

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

UEFI: Built-In EFI Shell

P4: ST3160316AS (system configuration dependent)

This page intentionally left blank

Chapter 7 Event Logs

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

Option	Description
►Change Smbios Event Log Settings	Smbios Event Log: Disabled/**Enabled** Erasing Settings Erase Event Log: **No** (**No**, Yes Next Reset, Yes Every Reset) When Log Is Full: **Do Nothing** (**Do Nothing**, Erase Immediately) Smbios Event Log Standard Settings Log System Boot Event: **Enabled** (Disabled, **Enabled**) MECI: **1** METW: **60** Custom Options Log OEM Codes: **Enabled** (Disabled, **Enabled**) Convert OEM Codes: **Disabled** (**Disabled**, Enabled)
►View Smbios Event Log – Displays current Smbios event log entries. Below is an example log from our engineering test bed. Date Time Error Code Severity 11/04/15 00:00:15 Smbios 0x16 N/A	

This page intentionally left blank

Chapter 8 Server Management

Server Mgmt

This menu provides information and options relating to the management and maintenance of the MBC8240.

Option	Description
BMC Self Test Status	This header is non-selectable. It informs the user if the BMC Self Test was successful or not. The two possible statuses are: 1) PASSED 2) FAILED
BMC Support	**Enabled** (Enabled, Disabled) -- Enables or disables communication with the BMC.
Wait for BMC	**Enabled** (Enabled, Disabled) – Waits for BMC response for the specified time out. In PILOTII, the BMC starts at the same time when BIOS starts during AC power ON. Its takes around 30 seconds to initialize Host to BMC interfaces.
FRB-2 Timer	Controls the operation of the Fault Resistant Booting timer. FRB level 2 is intended to recover from a watchdog timeout during POST. **Disabled** (Enabled, Disabled)
FRB-2 Timer Timeout	This option allows the end user to manually select a timeout for the FRB-2 Timer. Will not be selectable if "FRB-2 Timer" is set to 'Disabled' **6 Minutes** (3 minutes, 4 minutes, 5 minutes, 6 minutes)
FRB-2 Timer Policy	This option allows the end user to select the operating rules under which the FRB-2 Timer performs its function. Will not be selectable if "FRB-2 Timer" is set to 'Disabled' **Reset** (Do Nothing, Reset, Power Down)
OS Watchdog Timer	Controls the operation of the Operating System Watchdog Timer. **Disabled** (Enabled, Disabled)
OS Wtd Timer Timeout	This option allows the end user to select a timeout for the OS Watchdog Timer. Will not be selectable if "OS Watchdog Timer" is set to 'Disabled' **10 minutes** (5 minutes, 10 minutes, 15 minutes, 20 minutes)
OS Wtd Timer Policy	This option allows the end user to select the operating rules under which the OS Watchdog Timer performs its function. Will not be selectable if "OS Watchdog Timer is set to 'Disabled' **Reset** (Do Nothing, Reset Power Down) ,
Serial Mux	Controls operation of the onboard serial multiplexer. **Disabled** (Enabled, Disabled)
BMC self test log	Erase **No** (Yes, clear on every reset, no) When log is full **Clear Log** (Do not log anymore, clear log)
System Event Log	Enabling/Disabling Options Sel components **Enabled** (Enabled, disabled) Erasing Settings Erase sel **No** (No, Yes next reset, Yes every reset) When sel is full **Do Nothing** (Erase immediately, Do Nothing) Custom EFI Logging Options **Both** (Disabled, Error Code, Progress Code, Both)
View FRU information	No user-selectable options. Provides information about the Field Replaceable Units currently installed in the system.
BMC network configuration	Provides configuration options for Channels 1 and 2 of the BMC network. Channel 1 Configure address source **Unspecified** (Unspecified, Static, Dynamic-obtained by BMC, Dynamic-loaded by BIOS, Dynamic-BMC running other protocol) Channel 2 Configure address source **Unspecified** (Unspecified, Static, Dynamic-obtained by BMC, Dynamic-loaded by BIOS, Dynamic-BMC running other protocol)

Chapter 9 Trenton Smart System Management

The Smart System Management (SSM) software embedded in the MBC8240 is accessible via the dedicated management Ethernet LAN (Port 0/Lnk 0). This dedicated interface provides full Ethernet 10/100/1000Base-T bandwidth and, optionally, isolation of these functions to a specific LAN. Trenton's SSM is built upon the industry standard Intelligent Platform Management Interface (IPMI) and its related sub-components including:

• Intelligent Platform Management Bus (IPMB)
• IPMI Platform Management FRU Information Storage Definition
• Intelligent Chassis Management Bus (ICMB)

Trenton SSM's implementation of IPMI provides seamless and efficient out-of-band management and control capability from any compatible device worldwide, regardless of the power-on state and is operating system-agnostic. A short list of Trenton SSM application software functionality includes:
• Fan speed monitoring
• Fan condition & status
• Alarm monitoring
• FRU management
• Voltage monitoring
• SBC present
• Remote messaging (i.e. call home)
• Poll for processor & memory health

The "intelligence" behind Trenton SSM is the Baseboard Management Controller (BMC). It is driven by firmware that is capable of being upgraded locally or remotely. Management can be done inside a Linux or Windows® operating system environment locally or remotely, via software issued under license from AMI, for AMI's Yet Another Firmware Upgrade Flash (YAFUFLash) tool.

Additionally, the Yet Another Firmware Upgrade Keyboard Controller Style, (YAFUKCS) allows the firmware to be flashed locally in a UEFI environment.

YAFUFlash (Yet Another Firmware Upgrade Flash) Windows Environment Instructions
Open the command prompt and enter **YafuFlash\[Windows Path]**

For help and examples, use the following flags, i.e: **Yafuflash [HELP FLAG]**

Help Flags	**Usage**
-?	Displays the utility usage
-h	Displays the utility usage
-V	Displays version number of the tool
-e	Lists examples of tool usage

To execute a flash upgrade, enter
Yafuflash [OPTION(S)] [MEDIUM] [NAME OF NEW FIRMWARE IMAGE FILE]
Where OPTIONS=possible options and MEDIUM=the medium used to flash.

Option Flag	**Usage**
-info	Displays information about existing Firmware and new Firmware
-force-boot	Option to force the bootloader to upgrade during a full upgrade
-preserve-config	Option to preserve the configuration module during a full upgrade
-quiet	Option to show minimum flash progress details during upgrade
-i	Option to interactive upgrade (This will allow upgrade of only required modules)**
-full	Performs a full upgrade in interactive upgrade mode.
-ignore-platform-check	Allows flashing of a different image to the target platform

-ignore-diff-image	Skips user interaction if the selected image is different from the target image
-ignore-same-image	Skips user interaction if the selected image is the same from the target image
-ignore-module-location	Skips user interaction if the selected image contains different module locations
-ignore-boot-version	Skips users interaction if the boot loader version is different and '-force-boot' option is not given
-ignore-reselect-image	Skips reselecting the active image
-ignore-non-preserve-config	Skips the 'restore to default factor' setting if the image shares the same configuration area
-img-section-info	Displays information about current firmware sections
-img-info	Displays information about current firmware versions
-img-select	Option to specify the image to be updated 0 – Inactive Image 1 – Image 1 2 – Image 2 3 – Both Images
-replace-publickey	Replaces the Public Key in existing firmware
-version-cmp-flash	Skips flashing modules if the versions are the same
-preserve-XXX	Option to preserve 'XXX' configuration. Will prompt for other already preserved configurations to be preserved or not. 'XXX' may be: 'sdr' 'fru' 'sel' 'ipmi' 'auth' 'net' 'ntp' 'snmp' 'ssh' 'kvm' or 'syslog'
-preserve-XXX -ignore-existing-overrides	Option to preserve only 'XXX' configuration. Must be used with at least one '-preserve-XXX' option.
-ignore-non-preserve-config	If the images of both flash share the same configuration area, this option will skip restring factory default settings
-split-img	Flashes the split image
-flash-XXX	Option to flash specific section in non-interactive mode. If it is a split image, the split-image is required along with this option where 'XXX' falls in boot, conf, root, osimage
-preserve-extlog	Option to preserve extended log. This option will be enabled only if the extended log feature is supported
-d	Option to specify SPI devices. This option will be enabled only if dual image feature is supported. <bit0> - BMC <bit1> - BIOS <bit2> - CPLD

Note: '-preserve-config' and '-force-boot' options cannot be used in an interactive upgrade
******: Interactive upgrade is not a default option. This option can be enabled in YafuFlash, if the software is built with the 'Enable/Disable Interactive Upgrade YafuFlash' option is selected..
Possible mediums include:

Medium Flag	**Usage**
-cd	Flash via USB
-nw -ip	Flash via Network (-nw –ip [IP ADDRESS OF TARGET])
-kcs	Keyboard Controller Style **Note:** KCS Medium can only be used in a DOS environment.

Note: When utilizing the network medium, additional flags to set HOST NAME, USER NAME and PASSWORD can be employed as necessary by using the flag structure
-nw –ip [IP address] –u [user name] –p [password] –host [host name]

YAFUFlash (Yet Another Firmware Upgrade Flash) Linux Environment Instructions
Open Terminal and go to **YafuFlash/Linux** path.
Run **./YafuFlash**

For help and examples, use the following flags, i.e: **./Yafuflash [HELP FLAG]**

Help Flags	**Usage**
-?	Displays the utility usage
-h	Displays the utility usage
-V	Displays version number of the tool
-e	Lists examples of tool usage

To execute a flash upgrade, enter
./Yafuflash [OPTION(S)] [MEDIUM] [NAME OF NEW FIRMWARE IMAGE FILE]
Where OPTIONS=possible options and MEDIUM=the medium used to flash.

Option Flag	**Usage**
-info	Displays information about existing Firmware and new Firmware
-force-boot	Option to force the bootloader to upgrade during a full upgrade
-preserve-config	Option to preserve the configuration module during a full upgrade
-quiet	Option to show minimum flash progress details during upgrade
-i	Option to interactive upgrade (This will allow upgrade of only required modules)**
-full	Performs a full upgrade in interactive upgrade mode.
-ignore-platform-check	Allows flashing of a different image to the target platform
-ignore-diff-image	Skips user interaction if the selected image is different from the target image
-ignore-same-image	Skips user interaction if the selected image is the same from the target image
-ignore-module-location	Skips user interaction if the selected image contains different module locations
-ignore-boot-version	Skips users interaction if the boot loader version is different and '-force-boot' option is not given
-ignore-reselect-image	Skips reselecting the active image
-ignore-non-preserve-config	Skips the 'restore to default factor' setting if the image shares the same configuration area
-img-section-info	Displays information about current firmware sections
-img-info	Displays information about current firmware versions
-img-select	Option to specify the image to be updated 0 – Inactive Image 1 – Image 1 2 – Image 2 3 – Both Images
-replace-publickey	Replaces the Public Key in existing firmware
-version-cmp-flash	Skips flashing modules if the versions are the same
-preserve-XXX	Option to preserve 'XXX' configuration. Will prompt for other already preserved configurations to be preserved or not. 'XXX' may be: 'sdr' 'fru' 'sel' 'ipmi' 'auth' 'net' 'ntp' 'snmp' 'ssh' 'kvm' or 'syslog'
-preserve-XXX -ignore-existing-overrides	Option to preserve only 'XXX' configuration. Must be used with at least one '-preserve-XXX' option.
-ignore-non-preserve-config	If the images of both flash share the same configuration area, this option will skip restring factory default settings
-split-img	Flashes the split image

-flash-XXX	Option to flash specific section in non-interactive mode. If it is a split image, the split-image is required along with this option where 'XXX' falls in boot, conf, root, osimage
-preserve-extlog	Option to preserve extended log. This option will be enabled only if the extended log feature is supported
-d	Option to specify SPI devices. This option will be enabled only if dual image feature is supported. <bit0> - BMC <bit1> - BIOS <bit2> - CPLD

Note: '-preserve-config' and '-force-boot' options cannot be used in an interactive upgrade
******: Interactive upgrade is not a default option. This option can be enabled in YafuFlash, if the software is built with the 'Enable/Disable Interactive Upgrade YafuFlash' option is selected.
Possible mediums include:

Medium Flag	**Usage**
-cd	Flash via USB
-nw -ip	Flash via Network (-nw –ip [IP ADDRESS OF TARGET])
-kcs	Keyboard Controller Style **Note:** KCS Medium can only be used in a DOS environment.

Note: When utilizing the network medium, additional flags to set HOST NAME, USER NAME and PASSWORD can be employed as necessary by using the flag structure
-nw –ip [IP address] –u [user name] –p [password] –host [host name]

YAFUFlash (Yet Another Firmware Upgrade Flash) DOS Environment Instructions
Copy **Yafuflash.exe** into the DOS machine
Run the **Yafuflash** utility

For help and examples, use the following flags, i.e: **Yafuflash [HELP FLAG]**

Help Flags	Usage
-?	Displays the utility usage
-h	Displays the utility usage
-V	Displays version number of the tool
-e	Lists examples of tool usage

To execute a flash upgrade, enter
Yafuflash [OPTION(S)] [MEDIUM] [NAME OF NEW FIRMWARE IMAGE FILE]
Where OPTIONS=possible options and MEDIUM=the medium used to flash.

Option Flag	Usage
-info	Displays information about existing Firmware and new Firmware
-force-boot	Option to force the bootloader to upgrade during a full upgrade
-preserve-config	Option to preserve the configuration module during a full upgrade
-quiet	Option to show minimum flash progress details during upgrade
-i	Option to interactive upgrade (This will allow upgrade of only required modules)**
-full	Performs a full upgrade in interactive upgrade mode.
-ignore-platform-check	Allows flashing of a different image to the target platform
-ignore-diff-image	Skips user interaction if the selected image is different from the target image
-ignore-same-image	Skips user interaction if the selected image is the same from the target image
-ignore-module-location	Skips user interaction if the selected image contains different module locations
-ignore-boot-version	Skips users interaction if the boot loader version is different and '-force-boot' option is not given
-ignore-reselect-image	Skips reselecting the active image
-ignore-non-preserve-config	Skips the 'restore to default factor' setting if the image shares the same configuration area
-img-section-info	Displays information about current firmware sections
-img-info	Displays information about current firmware versions
-img-select	Option to specify the image to be updated 0 – Inactive Image 1 – Image 1 2 – Image 2 3 – Both Images
-replace-publickey	Replaces the Public Key in existing firmware
-version-cmp-flash	Skips flashing modules if the versions are the same
-preserve-XXX	Option to preserve 'XXX' configuration. Will prompt for other already preserved configurations to be preserved or not. 'XXX' may be: 'sdr' 'fru' 'sel' 'ipmi' 'auth' 'net' 'ntp' 'snmp' 'ssh' 'kvm' or 'syslog'
-preserve-XXX -ignore-existing-overrides	Option to preserve only 'XXX' configuration. Must be used with at least one '-preserve-XXX' option.
-ignore-non-preserve-config	If the images of both flash share the same configuration area, this option will skip restring factory default settings
-split-img	Flashes the split image

-flash-XXX	Option to flash specific section in non-interactive mode. If it is a split image, the split-image is required along with this option where 'XXX' falls in boot, conf, root, osimage
-preserve-extlog	Option to preserve extended log. This option will be enabled only if the extended log feature is supported
-d	Option to specify SPI devices. This option will be enabled only if dual image feature is supported. <bit0> - BMC <bit1> - BIOS <bit2> - CPLD

******: Interactive upgrade is not a default option. This option can be enabled in YafuFlash, if the software is built with the 'Enable/Disable Interactive Upgrade YafuFlash' option is selected..
Possible mediums include:

Medium Flag	Usage
-kcs	Keyboard Controller Style **Note:** KCS Medium can only be used in a DOS environment.

Note: When utilizing the network medium, additional flags to set HOST NAME, USER NAME and PASSWORD can be employed as necessary by using the flag structure
-nw –ip [IP address] –u [user name] –p [password] –host [host name]

YAFUKCS (Yet Another Firmware Upgrade Keyboard Controller Style) Flash Instructions
Using a USB storage device, copy **Yafukcs_uefi\obj\Yafukcs.efi** and **the new image file** to the root of the drive. Boot the machine to a BIOS UEFI Shell prompt.
To execute a flash upgrade, enter
Yafukcs.efi [OPTION(S)] [NAME OF NEW FIRMWARE IMAGE FILE]
Where OPTIONS=possible options and MEDIUM=the medium used to flash.

Help Flag	Usage
-h	Display the utility usage
-info	Display information about current firmware and new firmware
-force-boot	FORCES Bootloader upgrade during full upgrade
-preserve-config	Attempts to preserve the Configuration Module's data during full upgrade

YAFU Error Codes

Error Code	Macro	Definition
0x00	-	Normal Response/Success
0x01	YAFU_FW_MOD_NOT_FOUND	Firmware module not found
0x02	YAFU_GREATER_IMAGE_SIZE	Image size is greater
0x03	YAFU_GET_DUAL_IMAGE_FAILED	Dual image configurations failed
0x04	YAFU_IMAGE_CHKSUM_VERIFY_FAILED	Image checksum verification failed
0x05	YAFU_FILE_OPEN_ERR	Cannot open file
0x06	YAFU_INVALID_NAME	Invalid Name Given Invalid Host Name Invalid Publickey File Name Invalid IP Address
0x07	YAFU_NAME_LONG	Parameter Size Exceeds Public Key File Nam Exceeds IP Address Size Exceeds Host Name Size Exceeds Username Size Exceeds Password Size Exceeds
0x08	YAFU_CC_IMAGE_SIZE_INVALID	Invalid image size
0x09	YAFU_COMMAND_TIMEOUT_ERR	Command timeout exception

This page intentionally left blank

Appendix A BIOS Messages

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

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

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

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

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

PEI Beep Codes

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

DXE Beep Codes

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

BIOS Status Codes

As the POST (Power On Self Test) routines are performed during boot-up, test codes are displayed on Port 80 POST code LEDs 0, 1, 2, 3, 4, 5, 6 and 7. These LED are located on the top of the CARD, 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 MBC8240 and CARDs. 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.

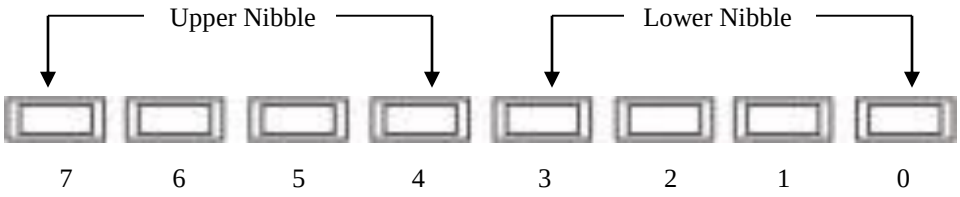
BIOS Status POST Code LEDs

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 CARD, 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 MBC8240 and CARDs. 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



MBC8240 POST Code LEDs

Status Code Ranges

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

SEC Status Codes

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

SEC Beep Codes

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

PEI Status Codes

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

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

PEI Beep Codes

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

DXE Status Codes

Status Code	Description
0x60	DXE Core is started
0x61	NVRAM initialization
0x62	Installation of the South Bridge Runtime Services
0x63	CPU DXE initialization is started
0x64	CPU DXE initialization (CPU module specific)
0x65	CPU DXE initialization (CPU module specific)
0x66	CPU DXE initialization (CPU module specific)
0x67	CPU DXE initialization (CPU module specific)
0x68	PCI host bridge initialization
0x69	North Bridge DXE initialization is started
0x6A	North Bridge DXE SMM initialization is started
0x6B	North Bridge DXE initialization (North Bridge module specific)
0x6C	North Bridge DXE initialization (North Bridge module specific)
0x6D	North Bridge DXE initialization (North Bridge module specific)
0x6E	North Bridge DXE initialization (North Bridge module specific)
0x6F	North Bridge DXE initialization (North Bridge module specific)
0x70	South Bridge DXE initialization is started
0x71	South Bridge DXE SMM initialization is started
0x72	South Bridge devices initialization
0x73	South Bridge DXE Initialization (South Bridge module specific)
0x74	South Bridge DXE Initialization (South Bridge module specific)
0x75	South Bridge DXE Initialization (South Bridge module specific)
0x76	South Bridge DXE Initialization (South Bridge module specific)
0x77	South Bridge DXE Initialization (South Bridge module specific)
0x78	ACPI module initialization
0x79	CSM initialization
0x7A – 0x7F	Reserved for future AMI DXE codes
0x80 – 0x8F	OEM DXE initialization codes

0x90	Boot Device Selection (BDS) phase is started
0x91	Driver connecting is started
0x92	PCI Bus initialization is started
0x93	PCI Bus Hot Plug Controller Initialization
0x94	PCI Bus Enumeration
0x95	PCI Bus Request Resources
0x96	PCI Bus Assign Resources
0x97	Console Output devices connect
0x98	Console input devices connect
0x99	Super IO Initialization
0x9A	USB initialization is started
0x9B	USB Reset
0x9C	USB Detect
0x9D	USB Enable
0x9E – 0x9F	Reserved for future AMI codes
0xA0	IDE initialization is started
0xA1	IDE Reset
0xA2	IDE Detect
0xA3	IDE Enable
0xA4	SCSI initialization is started
0xA5	SCSI Reset
0xA6	SCSI Detect
0xA7	SCSI Enable
0xA8	Setup Verifying Password
0xA9	Start of Setup
0xAA	Reserved for ASL (see ASL Status Codes section below)
0xAB	Setup Input Wait
0xAC	Reserved for ASL (see ASL Status Codes section below)
0xAD	Ready To Boot event
0xAE	Legacy Boot event
0xAF	Exit Boot Services event
0xB0	Runtime Set Virtual Address MAP Begin
0xB1	Runtime Set Virtual Address MAP End
0xB2	Legacy Option ROM Initialization
0xB3	System Reset
0xB4	USB hot plug
0xB5	PCI bus hot plug
0xB6	Clean-up of NVRAM
0xB7	Configuration Reset (reset of NVRAM settings)
0xB8 – 0xBF	Reserved for future AMI codes
0xC0 – 0xCF	OEM BDS initialization codes

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

DXE Beep Codes

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

ACPI/ASL Status Codes

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

OEM-Reserved Status Code Ranges

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