

» User Guide «

CP6003-SA/RA/RC uEFI BIOS

Doc. ID: 1045-9149, Rev. 2.0
March 13, 2012



Revision History

Publication Title:		CP6003-SA/RA/RC uEFI BIOS User Guide
Doc. ID:		1045-9149
Rev.	Brief Description of Changes	Date of Issue
1.0	Initial issue based on the uEFI BIOS version R11	20-Sep-2011
2.0	General update based on the uEFI BIOS version R12, added description for the CP6003-RA/RC	13-Mar-2012

Imprint

Kontron Modular Computers GmbH may be contacted via the following:

MAILING ADDRESS

Kontron Modular Computers GmbH
 Sudetenstraße 7
 D - 87600 Kaufbeuren Germany

TELEPHONE AND E-MAIL

+49 (0) 800-SALESKONTRON
 sales@kontron.com

For further information about other Kontron products, please visit our Internet web site: www.kontron.com.

Disclaimer

Copyright © 2012 Kontron AG. All rights reserved. All data is for information purposes only and not guaranteed for legal purposes. Information has been carefully checked and is believed to be accurate; however, no responsibility is assumed for inaccuracies. Kontron and the Kontron logo and all other trademarks or registered trademarks are the property of their respective owners and are recognized. Specifications are subject to change without notice.



Table of Contents

1. Starting uEFI BIOS Setup	9
1.1 Main Setup Menu	10
1.2 Navigation	11
2. Main Setup	15
2.1 BIOS Information	15
2.2 Trusted Computing	16
2.2.1 TPM Configuration	16
2.2.1.1 TPM Support	16
2.2.1.2 TPM State	17
2.2.2 Pending TPM Operation	17
2.2.3 Current TPM Status Information	17
2.3 Serial Port Console Redirection	18
2.3.1 COM0	18
2.3.1.1 Console Redirection	18
2.3.1.2 Console Redirection Settings	18
2.3.2 COM1	19
2.3.2.1 Console Redirection	19
2.3.2.2 Console Redirection Settings	19
2.3.3 Serial Port for Out-of-Band Management/Windows EMS	19
2.3.3.1 Console Redirection	19
2.3.3.2 Out-of-Band Mgmt Port	19
2.3.3.3 Data Bits	20
2.3.3.4 Parity	20
2.3.3.5 Stop Bits	20
2.3.3.6 Terminal Type	20
2.3.4 Console Redirection Settings	21
2.3.4.1 Terminal Type	21
2.3.4.2 Bits per second	21
2.3.4.3 Data Bits	22



2.3.4.4	Parity	22
2.3.4.5	Stop Bits	22
2.3.4.6	Flow Control	22
2.3.4.7	Recorder Mode	22
2.3.4.8	Resolution 100x31	23
2.3.4.9	Legacy OS Redirection	23
2.4	System Language	23
2.5	System Date	23
2.6	System Time	23
2.7	Access Level	24
3.	Boot Setup	27
3.1	Boot Configuration	27
3.1.1	Setup Prompt Timeout	27
3.1.2	Bootup NumLock State	28
3.1.3	Quiet Boot	28
3.1.4	CSM16 Module Version	28
3.1.5	GateA20 Active	28
3.1.6	Option ROM Messages	28
3.1.7	Interrupt 19 Capture	29
3.2	Boot Option Priorities	29
3.2.1	Boot Option #1..4	29
3.2.2	Hard Drive/Network Device/CD/DVD ROM Drive/Floppy Drive etc. ..	29
4.	Security Setup	33
4.1	Administrator Password	34
4.2	User Password	34
4.3	HDD Security Configuration	34
4.4	Remember the Password	34
5.	Save & Exit	37
5.1	Save Changes and Exit	37



5.2	<i>Discard Changes and Exit</i>	37
5.3	<i>Save Changes and Reset</i>	37
5.4	<i>Discard Changes and Reset</i>	38
5.5	<i>Save Changes (Save Options)</i>	38
5.6	<i>Discard Changes (Save Options)</i>	38
5.7	<i>Restore Defaults (Save Options)</i>	38
5.8	<i>Save as User Defaults (Save Options)</i>	38
5.9	<i>Restore User Defaults (Save Options)</i>	38
5.10	<i>Boot Override</i>	38
6.	<i>The uEFI Shell</i>	41
6.1	<i>Introduction, Basic Operation</i>	41
6.1.1	<i>Shell Startup</i>	41
6.2	<i>Kontron Shell Commands</i>	42
6.2.1	<i>kboardconfig uEFI Shell Command</i>	43
6.2.2	<i>kboardinfo uEFI Shell Command</i>	46
6.2.3	<i>kboot uEFI Shell Command</i>	48
6.2.4	<i>kbootnsh uEFI Shell Command</i>	49
6.2.5	<i>kclearnvram uEFI Shell Command</i>	50
6.2.6	<i>kclsp uEFI Shell Command</i>	50
6.2.7	<i>kflash uEFI Shell Command</i>	51
6.2.8	<i>kipmi uEFI Shell Command</i>	52
6.2.9	<i>kmkramdisk uEFI Shell Command</i>	55
6.2.10	<i>kpassword uEFI Shell Command</i>	56
6.2.11	<i>kresetconfig uEFI Shell Command</i>	57
6.2.12	<i>kwdt uEFI Shell Command</i>	58
6.3	<i>uEFI Shell Scripting</i>	60
6.3.1	<i>Startup Scripting</i>	60
6.3.2	<i>Create a Startup Script</i>	60
6.3.3	<i>Examples of Startup Scripts</i>	60
6.3.3.1	<i>Automatic Booting from USB Flash Drive</i>	60
6.3.3.2	<i>Switch On Clock Spreading Prior to Booting from Harddrive</i>	60
6.3.3.3	<i>Execute Shell Script on Other Harddrive</i>	60



6.3.3.4 *Enable Watchdog and Control PXE Boot* 61
 6.3.3.5 *Handling the Startup Script in the Flash Bank* 62

7. *Updating the uEFI BIOS* 65
 7.1 *uEFI BIOS Fail-Over Mechanism* 65
 7.2 *Updating Procedure* 65
 7.3 *uEFI BIOS Recovery* 65
 7.4 *Determining the Active Flash* 65





Chapter

1

Starting uEFI BIOS Setup



This page has been intentionally left blank.





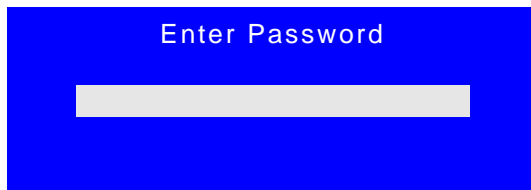
1. Starting uEFI BIOS Setup

The CP6003-SA/RA/RC is provided with a Kontron-customized, pre-installed and configured version of Aptio® (referred to as uEFI BIOS in this manual), AMI's next generation BIOS firmware based on the Unified Extensible Firmware Interface (uEFI) specification and the Intel® Platform Innovation Framework for EFI.

This uEFI BIOS provides a variety of new and enhanced functions specifically tailored to the hardware features of the CP6003-SA/RA/RC. To take advantage of these functions, the uEFI BIOS comes with an uEFI Shell, which provides quick and easy access to the individual function settings for control or modification of the uEFI BIOS configuration, and a Setup program, which allows the accessing of various menus that provide functions or access to sub-menus with more specific functions of their own. The individual menus and the configurable functions are described in this guide.

To start the uEFI BIOS Setup program, follow the steps below:

1. Power on the board.
2. Wait until the first characters appear on the screen (POST messages or splash screen).
3. Press the <F2> key.
4. If the uEFI BIOS is password-protected, a window such as the one below will appear:



Enter either the User password or the Administrator password (refer to Chapter 4, Security Setup, for further information), press <RETURN>, and proceed with step 2.

5. A Setup menu with the following token attributes will appear.
The currently active menu and the currently active uEFI BIOS Setup item are highlighted in white.



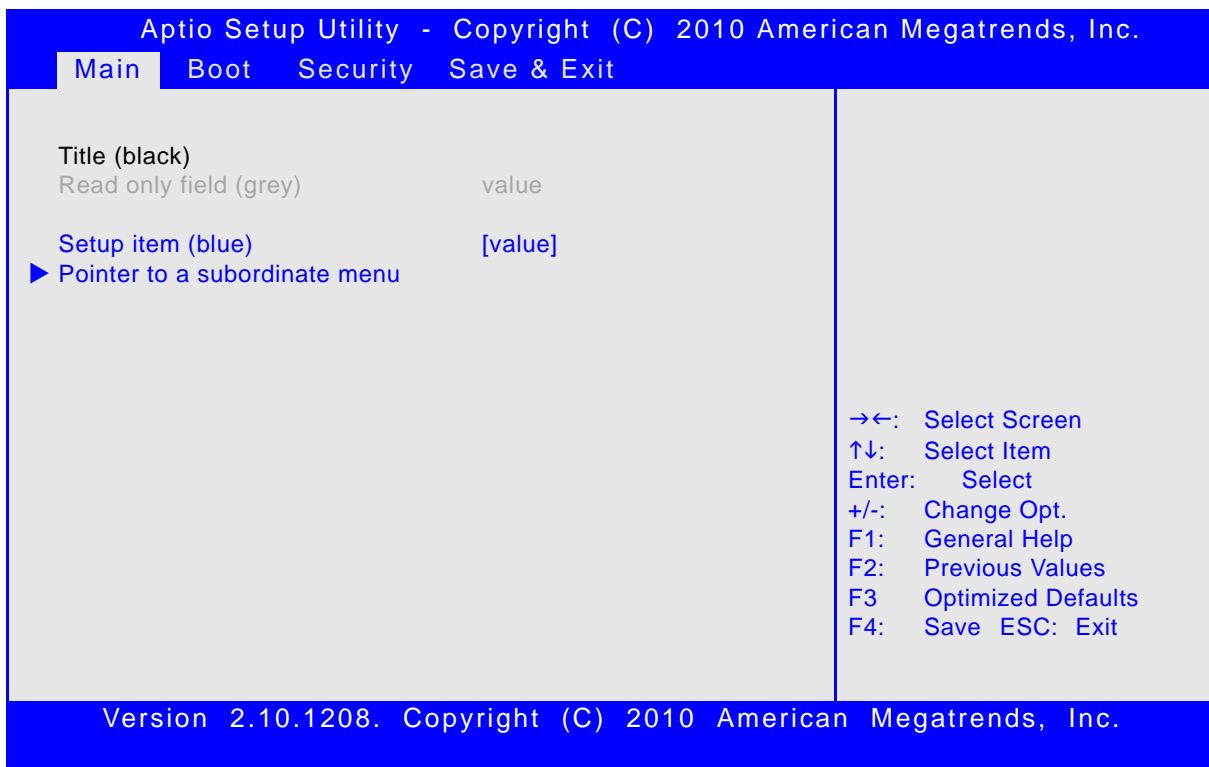
1.1 Main Setup Menu

The Main setup menu is the first screen that appears after starting the Setup program.

At the top of this screen and all of the other major screens, there is a setup menu selection bar, which permits access to all of the other major setup menus. These menus are selected via the left-right arrow keys.

All setup menu screens have two main frames. The left frame displays all the functions that can be configured. They are displayed in blue. Functions displayed in gray provide information about the status or the operational configuration.

The right frame displays the key legend. Above the key legend there is an area reserved for a text message. When a function is selected in the left frame, it is displayed in white. Often a text message will accompany it.





1.2 Navigation

The CP6003-SA/RA/RC uEFI BIOS setup program uses a hot key-based navigation system. A hot key legend is located in the right frame on most setup screens. The following table provides information concerning the usage of these hot keys.

HOT KEY	DESCRIPTION
<F1>	The <F1> key is used to invoke the General Help window.
<F2>	The <F2> key is used to restore the previous values.
<F3>	The <F3> key is used to load the defaults.
<F4>	The <F4> key is used to save the current settings and exit the uEFI BIOS Setup.
→ ← Left/Right	The <i>Left and Right</i> <Arrow> keys are used to select a major Setup screen. For example: Main Screen, Boot Screen, Security Screen, etc.
↑ ↓ Up/Down	The <i>Up and Down</i> <Arrow> keys are used to select a Setup function or a sub-screen.
+ - Plus/Minus	The <i>Plus and Minus</i> <Arrow> keys are used to change the field value of a particular Setup function, for example, system date and time.
<ESC>	The <ESC> key is used to exit a menu or the uEFI BIOS Setup. Pressing the <ESC> key in a sub-menu causes the next higher menu level to be displayed. When the <ESC> key is pressed in a major Setup menu, the uEFI BIOS Setup is terminated without saving any changes made.
<Enter>	The <Enter> key is used to execute a command or select a menu.



This page has been intentionally left blank.





Chapter **2**

Main Setup



This page has been intentionally left blank.



2. Main Setup

Upon entering the uEFI BIOS Setup program, the Main setup screen is displayed. This screen lists the main setup sub-screens and provides very basic system information as well as functions for setting the system time and date. In addition, the remaining major setup menus can be accessed from this screen. This screen can also be selected from any other major setup screen by using the Main tab.

Aptio Setup Utility - Copyright (C) 2010 American Megatrends, Inc.

Main Boot Security Save & Exit

BIOS Information
 BIOS Vendor American Megatrends
 Core Version 4.6.4.0
 Compliance UEFI 2.1
 Project Version B3C01 12.00 x64
 Build Date and Time 12/19/2011 14:09:54

▶ Trusted Computing
 ▶ Serial Port Console Redirection

System Language [English]

System Date [Fri 02/10/2012]
 System Time [10:33:17]

Access Level Administrator

→←: Select Screen
 ↑↓: Select Item
 Enter: Select
 +/-: Change Opt.
 F1: General Help
 F2: Previous Values
 F3: Optimized Defaults
 F4: Save ESC: Exit

Version 2.10.1208. Copyright (C) 2010 American Megatrends, Inc.

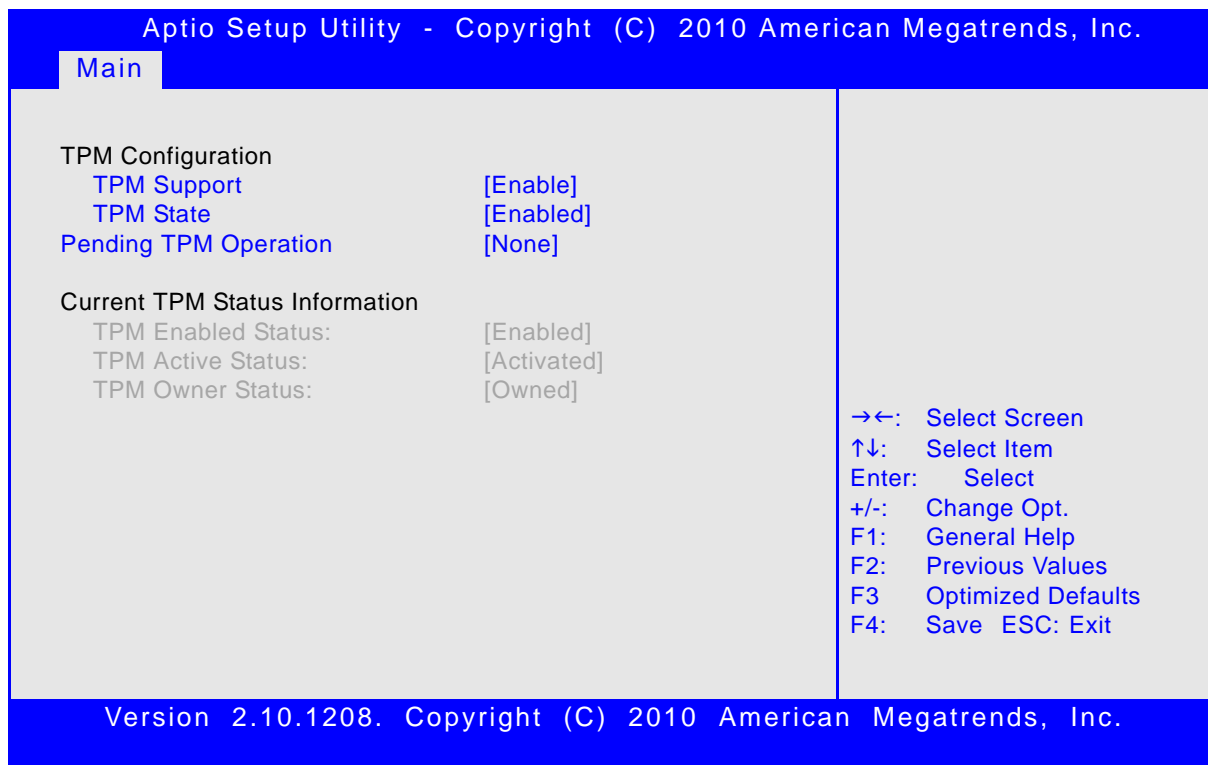
2.1 BIOS Information

This function provides display-only information concerning the uEFI BIOS.

Information about the running uEFI BIOS version is reflected in the display-only function Project Version (parameter "12.00" indicates revision 12).

2.2 Trusted Computing

This screen provides functions for specifying the TPM configuration settings and TPM displaying status information.



Aptio Setup Utility - Copyright (C) 2010 American Megatrends, Inc.

Main

TPM Configuration

TPM Support [Enable]

TPM State [Enabled]

Pending TPM Operation [None]

Current TPM Status Information

TPM Enabled Status: [Enabled]

TPM Active Status: [Activated]

TPM Owner Status: [Owned]

→←: Select Screen
 ↑↓: Select Item
 Enter: Select
 +/-: Change Opt.
 F1: General Help
 F2: Previous Values
 F3: Optimized Defaults
 F4: Save ESC: Exit

Version 2.10.1208. Copyright (C) 2010 American Megatrends, Inc.

2.2.1 TPM Configuration

2.2.1.1 TPM Support

This function is used to provide the Trusted Platform Module (TPM) functionality to the OS.

Note: Trusted Platform Module support is available on request.

SETTING	DESCRIPTION
Disable	Use this setting to disable TPM support. If this setting is used, TPM is not present for the OS, regardless whether the function TPM State is enabled or not.
Enable	Use this setting to enable TPM support.

Default setting: Disable



2.2.1.2 TPM State

This function is used to select the TPM State command to be issued to the TPM after POST.

Note: This function is available only when the function TPM Support is set to Enable.

SETTING	DESCRIPTION
Disabled	Use this setting to disable the TPM after POST. If this setting is used, the TPM is present for the OS but its functionality is locked.
Enabled	Use this setting to enable the TPM after POST.

Default setting: Disabled

2.2.2 Pending TPM Operation

This function is used to select a TPM command to be issued once against the TPM during the next boot.

Note: This function is available only when the function TPM Support is set to Enable.

SETTING	DESCRIPTION
None	Use this setting to prevent the system from issuing any TPM commands.
Enable Take Ownership	Use this setting to allow the system to issue an Enable Take Ownership command during the next boot. If this setting is used, the Take Ownership command is enabled, which allows the OS to take ownership of the TPM.
Disable Take Ownership	Use this setting to allow the system to issue a Disable Take Ownership command during the next boot. If this setting is used, the Take Ownership command is disabled, which prevents the OS from taking ownership of the TPM.
TPM Clear	Use this setting to allow the system to issue a TPM Clear command during the next boot. If this setting is used, the TPM is reset to the factory default. Warning: Use of this setting also deletes any keys and passwords stored within the TPM. Always ensure that encryption software such as Microsoft BitLocker, etc. are deactivated prior to selecting this setting.

Default setting: None

2.2.3 Current TPM Status Information

This is a display-only function providing status information about the TPM.

FUNCTION	DESCRIPTION
TPM Enabled Status	Displays if the TPM device is enabled.
TPM Active	Displays if the TPM has been activated by the OS.
TPM Owner Status	Displays if the OS has taken ownership of the TPM device.

2.3 Serial Port Console Redirection

This screen provides information about functions for specifying the Serial Port Console Redirection configuration settings. Console redirection can be used to remotely operate system settings and the uEFI console.

Aptio Setup Utility - Copyright (C) 2010 American Megatrends, Inc.

Main

COM0
 Console Redirection [Enabled]
 ▶ Console Redirection Settings

COM1
 Console Redirection [Disabled]
 ▶ Console Redirection Settings

Serial Port for Out-of-Band Management/
 Windows Emergency Management Services (EMS)
 Console Redirection [Disabled]
 Out-of-Band Mgmt Port [COM0]
 Data Bits 8
 Parity None
 Stop Bits 1
 Terminal Type [VT-UTF8]

→←: Select Screen
 ↑↓: Select Item
 Enter: Select
 +/-: Change Opt.
 F1: General Help
 F2: Previous Values
 F3: Optimized Defaults
 F4: Save ESC: Exit

Version 2.10.1208. Copyright (C) 2010 American Megatrends, Inc.

2.3.1 COM0

On the CP6003-SA/RA, the COM0 port (serial port 0) corresponds to the serial port on the front panel (hardware designation COMA). On the CP6003-RC, the COM0 port (serial port 0) corresponds to the serial port on the rear I/O (hardware designation COMA).

2.3.1.1 Console Redirection

SETTING	DESCRIPTION
Disabled	Use this setting to disable console redirection for the serial port 0.
Enabled	Use this setting to enable console redirection for the serial port 0.

Default setting: Enabled

2.3.1.2 Console Redirection Settings

For information about this function, refer to Chapter 2.3.4 in this manual.



2.3.2 COM1

The COM1 port (serial port 1) corresponds to the RS-422 serial port on the RIO connector (J3) of the CP6003-SA/RA/RC (hardware designation COMB).

2.3.2.1 Console Redirection

SETTING	DESCRIPTION
Disabled	Use this setting to disable console redirection for the serial port 1.
Enabled	Use this setting to enable console redirection for the serial port 1.

Default setting: Disabled

2.3.2.2 Console Redirection Settings

For information about this function, refer to Chapter 2.3.4 in this manual.

2.3.3 Serial Port for Out-of-Band Management/Windows Emergency Management Services (EMS)

The following functions control the presence and content of the ACPI serial port redirection table (SPCR). This table is mainly used by the Windows server variants to provide Windows Emergency Management Services (EMS). This functionality is totally independent from serial redirection of other console output.

OoB Management or EMS makes it possible to control selected components of (Windows) servers, even when a server is not connected to the network or the network is not available. In short: EMS allows for remote management of a Windows Server OS through a serial port

2.3.3.1 Console Redirection

SETTING	DESCRIPTION
Disabled	Use this setting to prevent the system from adding the SPCR table to the ACPI tables.
Enabled	Use this setting to add the SPCR table to the ACPI tables. The OS can further use the information provided for serial redirection services.

Default setting: Disabled

2.3.3.2 Out-of-Band Mgmt Port

This function is used to select the serial port intended for use with Out-of-Band Management. This functionality is independent from serial redirection of other console output.

SETTING	DESCRIPTION
COM0	Use this setting to specify that the serial port 0 is to be used with Out-of-Band Management.
COM1	Use this setting to specify that the serial port 1 is to be used with Out-of-Band Management.

Default setting: COM0



2.3.3.3 Data Bits

This is a display-only function providing information about the frame width for the Out-of-Band Management.

2.3.3.4 Parity

This is a display-only function providing information about the parity for Out-of-Band Management.

2.3.3.5 Stop Bits

This is a display-only function providing information about the number of stop bits for Out-of-Band Management.

2.3.3.6 Terminal Type

SETTING	DESCRIPTION
VT100	Use one of these settings to select the terminal type for out-of-band management.
VT100+	
VT-UTF8	
ANSI	

Default setting: VT-UTF8



2.3.4 Console Redirection Settings

This screen provides information about functions for specifying the Console Redirection configuration settings for the serial ports 0 and 1, and a PCI serial port. Each serial port can be independently configured.

Aptio Setup Utility - Copyright (C) 2010 American Megatrends, Inc.

Main

<p>COM0 Console Redirection Settings</p> <p>Terminal Type [ANSI] Bits per second [115200] Data Bits [8] Parity [None] Stop Bits [1] Flow Control [None] Recorder Mode [Disabled] Resolution 100x31 [Disabled] Legacy OS Redirection [80x24]</p>	<p>→←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save ESC: Exit</p>
---	---

Version 2.10.1208. Copyright (C) 2010 American Megatrends, Inc.

2.3.4.1 Terminal Type

SETTING	DESCRIPTION
VT100	Use one of these settings to select the terminal type to be emulated.
VT100+	
VT-UTF8	
ANSI	

Default setting: ANSI

2.3.4.2 Bits per second

SETTING	DESCRIPTION
9600	Use one of these settings to select the baud rate of the serial port.
19200	
57600	
115200	

Default setting: 115200

2.3.4.3 Data Bits

SETTING	DESCRIPTION
7	Use one of these settings to specify the number of data bits per frame.
8	

Default setting: 8

2.3.4.4 Parity

SETTING	DESCRIPTION
None	Use one of these settings to select the parity for the serial port.
Even	
Odd	
Mark	
Space	

Default setting: None

2.3.4.5 Stop Bits

SETTING	DESCRIPTION
1	Use one of these settings to specify the number of stop bits for the serial port.
2	

Default setting: 1

2.3.4.6 Flow Control

SETTING	DESCRIPTION
None	Use one of these settings to specify the type of flow control to be used for this serial port.
Hardware RTS/CTS	
Software Xon/Xoff	

Default setting: None

2.3.4.7 Recorder Mode

Use this setting to specify whether display formatting characters are to be transmitted along with data or if only data is to be transmitted.

SETTING	DESCRIPTION
Disabled	Use this setting to specify normal terminal operation.
Enabled	Use this setting to specify that only text will be sent. Use this to capture terminal data

Default setting: Disabled

2.3.4.8 Resolution 100x31

SETTING	DESCRIPTION
Disabled	Use this setting the disable extended terminal resolution.
Enabled	Use this setting the enable extended terminal resolution.

Default setting: Disabled

2.3.4.9 Legacy OS Redirection

SETTING	DESCRIPTION
80x24	Use one of these settings to select the number of rows and columns for legacy OS redirection.
80x25	

Default setting: 80x24

2.4 System Language

SETTING	DESCRIPTION
English	Use this function to select the system language. Currently, only English is supported.

2.5 System Date

SETTING	DESCRIPTION
<WD MM/DD/YYYY>	Use this function to change the system date. Select System Date using the Up and Down <Arrow> keys. Enter the new values through the keyboard or press +/- to increment/decrement values. Use "Tab" to switch between date elements.

2.6 System Time

SETTING	DESCRIPTION
<HH:MM:SS>	Use this function to change the system time. Select System Time using the Up and Down <Arrow> keys. Enter the new values through the keyboard or press +/- to increment/decrement values. Use "Tab" to switch between time elements.

Note: The time is in 24-hour format. For example, 5:30 A.M. appears as 05:30:00, and 5:30 P.M. as 17:30:00.



2.7 Access Level

This function provides display-only information concerning the uEFI BIOS Setup accessibility for the current Setup session. Depending on the type of password protection used, one of the following settings is displayed:

SETTING	DESCRIPTION
Administrator	This setting indicates that read/write access to all setup options is available.
User	This setting indicates that only a limited subset of all setup options is modifiable.

Note: If no password is set, the access setup is Administrator.



Chapter **3**

Boot Setup



This page has been intentionally left blank.





3. Boot Setup

Select the Boot tab to enter the Boot Setup screen. This screen lists the sub-screens for boot configuration and boot device priority.

Aptio Setup Utility - Copyright (C) 2010 American Megatrends, Inc.

Boot

<p>Boot Configuration</p> <p>Setup Prompt Timeout 1</p> <p>Bootup NumLock State [On]</p> <p>Quiet Boot [Disabled]</p> <p>CSM16 Module Version 07.64</p> <p>GateA20 Active [Upon Request]</p> <p>Option ROM Messages [Force BIOS]</p> <p>Interrupt 19 Capture [Disabled]</p> <p>Boot Option Priorities</p> <p>Boot Option #1 [Built-in EFI Shell]</p> <p>Boot Option #2 [SanDisk uSSD 5000 ...]</p> <p>Boot Option #3 [P0: ...]</p> <p>Boot Option #4 [P1: ...]</p> <p>Hard Drive BBS Priorities</p> <p>Network Device BBS Priorities</p> <p>CD/DVD ROM Drive BBS Priorities</p> <p>Floppy Drive BBS Priorities</p> <p>BEV Device BBS Priorities</p>	<p>→←: Select Screen</p> <p>↑↓: Select Item</p> <p>Enter: Select</p> <p>+/-: Change Opt.</p> <p>F1: General Help</p> <p>F2: Previous Values</p> <p>F3: Optimized Defaults</p> <p>F4: Save ESC: Exit</p>
---	--

Version 2.10.1208. Copyright (C) 2010 American Megatrends, Inc.

3.1 Boot Configuration

3.1.1 Setup Prompt Timeout

This integer function is used to set an additional time the POST should wait for the operator to press the key to enter setup. The time is entered in seconds.

SETTING	DESCRIPTION
1	Use one of these settings to specify the setup prompt timeout.
⋮	
65535	

Default setting: 1



3.1.2 Bootup NumLock State

This function is used to set the state of the keyboard's numlock function after POST.

SETTING	DESCRIPTION
On	Use this setting to switch on the keyboard's numlock function after POST.
Off	Use this setting to switch off the keyboard's numlock function after POST.

Default setting: On

3.1.3 Quiet Boot

This function is used to display either POST output messages or a splash screen during boot-up.

SETTING	DESCRIPTION
Disabled	Use this setting to display POST output messages during boot-up.
Enabled	Use this setting to display a splash screen during boot-up.

Default setting: Disabled

3.1.4 CSM16 Module Version

This function provides display-only information concerning the CSM Module and is intended for internal use only.

3.1.5 GateA20 Active

This function is used to enable or disable GateA20.

SETTING	DESCRIPTION
Upon Request	Use this setting to disable GA20 in the uEFI BIOS.
Always	Use this setting to prevent the system from disabling GA20.

Default setting: Upon Request

3.1.6 Option ROM Messages

This function is used to control the messages of the loaded PCI option ROMs.

SETTING	DESCRIPTION
Force BIOS	Use this setting to force to a BIOS-compatible output. This will show the option ROM messages.
Keep Current	Use this setting to keep the current video mode. This will suppress option ROM messages. Option ROMs requiring interactive inputs may not work properly in this mode.

Default setting: Force BIOS



3.1.7 Interrupt 19 Capture

This function is used to specify if legacy PCI option ROMs are allowed to capture software interrupt 19h.

SETTING	DESCRIPTION
Disabled	Use this setting to prevent legacy PCI option ROMs from capturing software interrupt 19h.
Enabled	Use this setting to allow legacy PCI option ROMs to capture software interrupt 19h.

Default setting: Disabled

3.2 Boot Option Priorities

3.2.1 Boot Option #1..4

These functions are used to form the boot order and are dynamically generated. They represent either a legacy BBS (BIOS Boot Specification) class of devices or a native uEFI boot entry. Press Return on each option to select the BBS class / uEFI boot entry desired.

3.2.2 Hard Drive/Network Device/CD/DVD ROM Drive/Floppy Drive/BEV Device BBS Priorities

These functions lead to sub-menus that allow configuring the boot order for a specific device class. These options are visible only if at least one device for this class is present. These functions are dynamically generated.



This page has been intentionally left blank.





Chapter **4**

Security Setup



This page has been intentionally left blank.





4. Security Setup

Select the Security tab to enter the Security Setup screen. This screen provides information about the passwords and functions for specifying the security settings.

Aptio Setup Utility - Copyright (C) 2010 American Megatrends, Inc.

Security

<p>Password Description</p> <p>If ONLY the Administrator's password is set, then this only limits access to Setup and is only asked for when entering Setup.</p> <p>If ONLY the User's password is set, then this is a power on password and must be entered to boot or enter Setup. In Setup the User will have Administrator rights.</p> <p>The password must be 3 to 20 characters long.</p> <p style="margin-top: 20px;">Administrator Password User Password</p> <p style="margin-top: 20px;">HDD Security Configur HDD 0:ST9120822SB</p>	<p>→←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save ESC: Exit</p>
--	--

Version 2.10.1208. Copyright (C) 2010 American Megatrends, Inc.

The following modes of security are provided:

SETTING	DESCRIPTION
No password is set	Booting the system as well as entering the Setup is unsecured.
Only Administrator password is set	Booting the system is unsecured. If no valid Administrator password is entered, only limited access to Setup is provided.
Only User password is set	The User password is required for booting the system as well as for entering the Setup menu. On every start-up, the user will be asked for the password.
Both User and Administrator passwords are set	Either the User or the Administrator password is required for booting the system as well as for entering the Setup menu. If the User password is entered here, limited access to the Setup is granted. Entering the Administrator password provides full access to all Setup entries.

Note: The CP6003-SA/RA/RC provides no factory-set passwords.



4.1 Administrator Password

This function is used to set, change or delete the Administrator password. If there is already a password installed, the system asks for this first. To clear a password, simply enter nothing and acknowledge by pressing Return. To set a password, enter it twice and acknowledge by pressing Return.

Note: The password is case-sensitive.

4.2 User Password

This function is used to set, change or delete the User password. If there is already a password installed, the system asks for this first. To clear a password, simply enter nothing and acknowledge by pressing Return. To set a password, enter it twice and acknowledge by pressing Return.

Note: The password is case-sensitive.

4.3 HDD Security Configuration

This function is not fully supported on the CP6003-SA/RA/RC.

Warning! Before using this function, contact Kontron for assistance. Failure to comply with the instruction above may result in an irreparable disk lockout.

4.4 Remember the Password

It is highly recommended to keep a record of all passwords in a safe place. Forgotten passwords may lead to being completely locked out of the system. Booting may not be possible, and in worst case the uEFI BIOS Setup program will also not be accessible.

If the system cannot be booted because neither the User password nor the Administrator password are known, refer to the respective chapters providing information about clearing the uEFI BIOS settings in the board's user guide or contact Kontron for further assistance. Information about clearing the uEFI BIOS settings for the CP6003-SA is provided in the CP6003-SA User Guide, Chapter 4.1, for the CP6003-RA in the CP6003-RA/RC User Guide, Chapter 4.1, and for the CP6003-RC in the CP6003-RA/RC User Guide, Chapter 4.2.



Chapter

5

Save & Exit

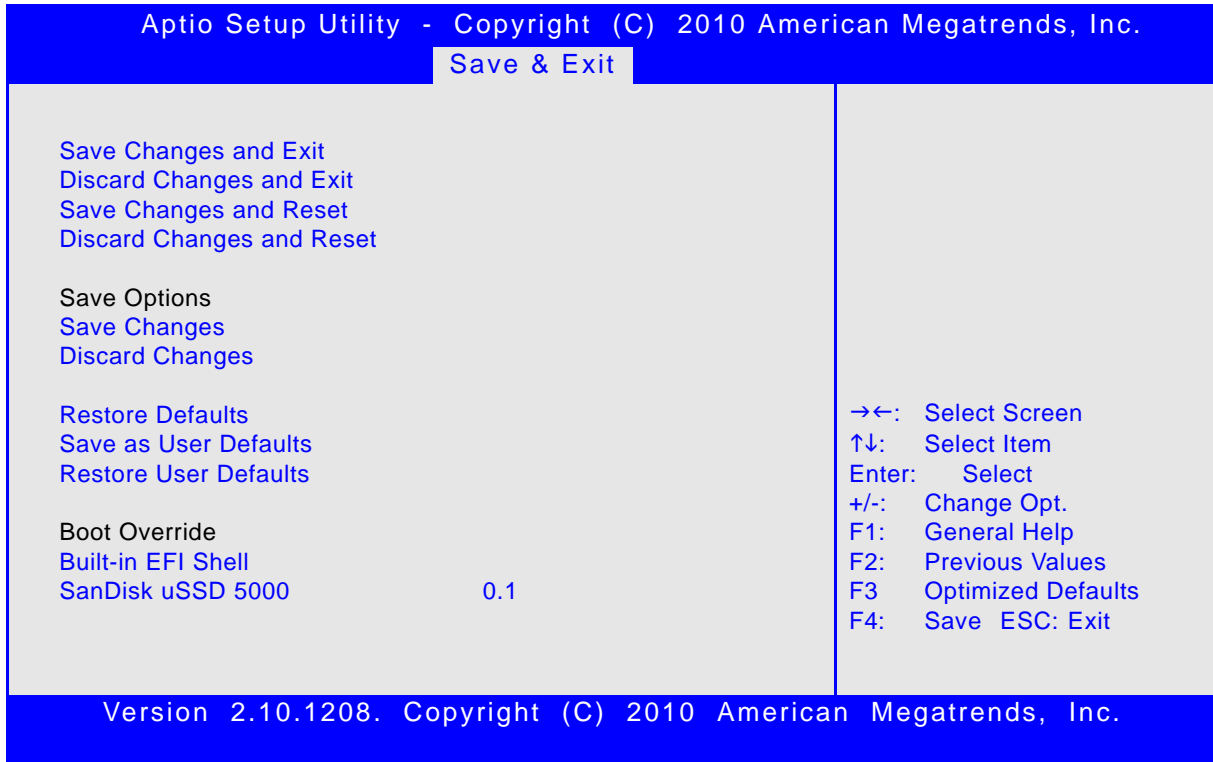


This page has been intentionally left blank.



5. Save & Exit

Select the Save & Exit tab to enter the Save & Exit menu screen. This screen provides functions for handling changes made to the uEFI BIOS settings and the exiting of the Setup program.



5.1 Save Changes and Exit

This function is used to save all changes made within the Setup to flash. This function continues the boot process as long as no option was altered that requires a reboot.

Note: The Setup will ask for confirmation prior to executing this command.

5.2 Discard Changes and Exit

This function is used to discard all changes made within the Setup. This function continues the boot process.

Note: The Setup will ask for confirmation prior to executing this command.

5.3 Save Changes and Reset

This function is used to save all changes made within the Setup to flash. This function performs a reboot afterwards.

Note: The Setup will ask for confirmation prior to executing this command.



5.4 Discard Changes and Reset

This function is used to discard all changes made within the Setup. This function performs a reboot afterwards.

Note: The Setup will ask for confirmation prior to executing this command.

5.5 Save Changes (Save Options)

This function is used to save all changes made within the Setup to flash. This function returns to Setup.

Note: The Setup will ask for confirmation prior to executing this command.

5.6 Discard Changes (Save Options)

This function is used to discard all changes made within the Setup. This function returns to Setup.

Note: The Setup will ask for confirmation prior to executing this command.

5.7 Restore Defaults (Save Options)

This function is used to restore all tokens to factory default.

Note: The Setup will ask for confirmation prior to executing this command.

5.8 Save as User Defaults (Save Options)

This function is used to save all current settings as user default. The current setup state can later be restored using Restore User Defaults.

Note: The Setup will ask for confirmation prior to executing this command.

5.9 Restore User Defaults (Save Options)

This function is used to restore all tokens to settings previously stored by Save as User Defaults.

Note: The Setup will ask for confirmation prior to executing this command.

5.10 Boot Override

This group of functions includes a list of tokens, each of them corresponding to one device within the boot order. Select a drive to immediately boot that device regardless of the current boot order. If booting to uEFI Shell this way, an exit from the shell returns to Setup.



Chapter

6

The uEFI Shell



This page has been intentionally left blank.





6. The uEFI Shell

The Kontron uEFI BIOS features a built-in and enhanced version of the uEFI Shell. For a detailed description of the available standard shell scripting refer to the EFI Shell User's Guide. For a detailed description of the available standard shell commands, refer to the Shell Command Manual 1.0. Both documents can be downloaded from the EFI and Framework Open Source Community homepage (<https://efi-shell.tianocore.org>) under the "Documents and Files" section.

Please note that not all shell commands described in the Shell Command Manual 1.0 are provided by the Kontron uEFI BIOS.

6.1 Introduction, Basic Operation

The uEFI Shell forms an entry into the uEFI boot order and is the first boot option by default. It is simply started by putting the uEFI Shell first in boot and running the board as usual.

6.1.1 Shell Startup

If the shell is executed, it displays its signon message followed by a list of detected devices. The output produced by the device mapping table can vary depending on the board's configuration.

```
EFI Shell version 2.00 [4.631]
Current running mode 1.1.2
Device mapping table
fs0      :Removable HardDisk - Alias hd33b0b0b blk0
          Acpi(PNP0A03,0)/Pci(1D|7)/Usb(1, 0)/Usb(1, 0)/HD(Part1,Sig17731773)
fs1      :Removable BlockDevice - Alias f33b0c0 blk1
          Acpi(PNP0A03,0)/Pci(1D|7)/Usb(1, 0)/Usb(2, 0)
blk0     :Removable HardDisk - Alias hd33b0b0b fs0
          Acpi(PNP0A03,0)/Pci(1D|7)/Usb(1, 0)/Usb(1, 0)/HD(Part1,Sig17731773)
blk1     :Removable BlockDevice - Alias f33b0c0 fs1
          Acpi(PNP0A03,0)/Pci(1D|7)/Usb(1, 0)/Usb(2, 0)
blk2     :HardDisk - Alias (null)
          Acpi(PNP0A03,0)/Pci(1F|2)/Ata(Primary,Master)/HD(Part1,SigC811D18D)
blk3     :BlockDevice - Alias (null)
          Acpi(PNP0A03,0)/Pci(1F|2)/Ata(Primary,Master)
blk4     :Removable BlockDevice - Alias (null)
          Acpi(PNP0A03,0)/Pci(1D|7)/Usb(1, 0)/Usb(1, 0)
```

Press the ESC key within 5 seconds to skip startup.nsh, and any other key to continue.

If the ESC key is pressed before the 5-second timeout has elapsed, the shell prompt is shown:

```
Shell>
```



6.2 Kontron Shell Commands

The Kontron uEFI implementation provides the following additional commands related to the specific HW features of the Kontron system:

- **kboardconfig**
- **kboardinfo**
- **kboot**
- **kbootnsh**
- **kclearnvram**
- **kclsp**
- **kflash**
- **kipmi**
- **kmkramdisk**
- **kpassword**
- **kresetconfig**
- **kwdt**

The following chapters provide information concerning these Kontron-specific commands. Where “RESPONSE” information is provided in “USAGE”, the value indicated in brackets is the currently selected setting. Where “SETTINGS” information is provided, the value indicated in brackets is the default setting. The uEFI Shell commands are case-sensitive.

6.2.1 kboardconfig uEFI Shell Command

kboardconfig

FUNCTION:	Configure non-volatile board settings
SYNTAX:	<pre>kboardconfig</pre> <pre>kboardconfig [-? <device> <setting>]</pre> <p>where:</p> <ul style="list-style-type: none"> ? Show online help <device> Specify device from list <setting> Select configuration type
DESCRIPTION:	The kboardconfig command is used to configure non-volatile board settings.
USAGE:	<p>Show all possible configurations</p> <p>COMMAND / RESPONSE:</p> <pre>Shell> kboardconfig Control nonvolatile board settings Example: kboardconfig Pxe: PXE boot device ([disabled] all gbe_a gbe_b rear_a rear_b gbe_e) StorageOprom: Launch Storage PCI OPROM (disabled [enabled]) PrimaryDisplay: Select primary display device ([auto] igd peg pci) Vga: VGA port configuration (auto [front] rear disabled) SataMode: Determines how SATA controller(s) operate (ide [ahci] raid) WrProtSata: Onboard SATA flash write protection ([disabled] enabled)!!! WARNING: CONTACT KONTRON BEFORE USING THIS FUNCTION !!! WrProtEeprom: System EEPROM write protection ([disabled] enabled) WrProtSpi: SPI boot flash write protection ([disabled] enabled) IntelVirtualization: Intel VT-x ([disabled] enabled) HyperThreading: Enable Hyper-Threading technology (disabled [enabled]) CpuTurbo: Enable CPU turbo mode (disabled [enabled]) C3State: Enable CPU C3-state report to OS (disabled [enabled]) C6State: Enable CPU C6-state report to OS (disabled [enabled]) C7State: Enable CPU C7-state report to OS (disabled [enabled])</pre> <p>Show allowed settings e.g. for "PrimaryDisplay":</p> <pre>Shell> kboardconfig PrimaryDisplay PrimaryDisplay: Select primary display device PrimaryDisplay == auto Allowed options: auto, igd, peg, pci</pre>

kboardconfig (continued)

SETTINGS:

pxe: Select PXE boot device
[disabled]: No PXE boot available
all: Try all Ethernet devices round robin for PXE boot
gbe_a: CP6003-SA: try only front GbE A port
 CP6003-RA: try either front GbE B port or rear LPc port
 CP6003-RC: try only rear LPc port
gbe_b: CP6003-SA: try only front GbE B port
 CP6003-RA: try either front GbE A port or rear LPd port
 CP6003-RC: try only rear LPd port
rear_a: CP6003-SA/RA/RC: try only rear PICMG 2.16 LPa port
rear_b: CP6003-SA/RA/RC: try only rear PICMG 2.16 LPb port
gbe_e: CP6003-SA: try only front GbE E port
 CP6003-RA: try only front GbE C port
 CP6003-RC: function not supported

StorageOprom: Launch storage PCI option ROMs
disabled: Do not launch storage PCI option ROMs. This includes the onboard RAID option ROM.
[enabled]: Launch storage option ROMs, if present

PrimaryDisplay: Select primary display device
[auto]: Automatically detect primary display device
igd: Use internal graphics, if enabled
peg: Try to use video on the PCIe graphics port, if present
pci: Try to use video on the PCI(e) bus first

Vga: VGA port configuration (CP6003-SA)
auto: Automatically detect devices. HDMI/DVI on rear I/O takes precedence over front VGA if devices are connected to both front and rear.
[front]: Try to use front VGA if available
rear: Try to use device connected to rear I/O if available
disabled: Disable graphic output
 Note: "Auto" operation may fail if the monitor cable in use does not correctly follow the VESA standard. For further information, refer to the CP6003-SA User Guide, Chapter "Analog VGA Connector".
 Note: This function is not relevant on the CP6003-RA/RC as the VGA port is statically routed to rear I/O.

SETTINGS:

SataMode: Determines how SATA controllers operate
ide: SATA ports operate as two IDE controllers
[ahci]: SATA ports operate as one 6-port AHCI controller
raid: SATA ports form a RAID device

**kboardconfig (continued)**

WrProtSata: Enable/Disable onboard SATA flash write protection [disabled]: Do not write protect the onboard SATA flash enabled: The onboard SATA flash is write-protected after POST. OS needs to be prepared to work with write-protected flash. For further information, refer to the operating system's documentation.
WrProtEeprom: Enable/Disable system EEPROM write protection [disabled]: Do not write protect the system EEPROM enabled: System EEPROM is write-protected after POST
WrProtSpi: Enable/Disable SPI boot flash write protection [disabled]: Do not write protect the SPI boot flash enabled: The SPI boot flash is write-protected after POST
IntelVirtualization: Enable/Disable Intel® VT-X technology
HyperThreading: Enable/Disable Hyper-Threading Technology
CPUTurbo: Enable/Disable CPU Turbo Boost Technology
C3State: Enable/Disable CPU C3 state report to OS
C6State: Enable/Disable CPU C6 state report to OS
C7State: Enable/Disable CPU C7 state report to OS



6.2.2 kboardinfo uEFI Shell Command

kboardinfo

FUNCTION:	Show board identification data
SYNTAX:	<code>kboardinfo</code>
DESCRIPTION:	The kboardinfo command shows a summary of board-specific identification data. It is especially useful for support queries because it contains this data in a concentrated form.
USAGE:	<p>Show board identification data</p> <p>COMMAND / RESPONSE:</p> <pre> Shell> kboardinfo KOMaOEMF rev.: 3 Board ID: 0xB3C0 Hardware rev.: 0x0 Logic rev.: 0x1 Boot flash: Standard SPI boot flash In system slot: No Geographic address: 5 Material number: Hardware index: Serial number: EFI article name: SK-EFI-B3C01 EFI material number: 1045-6085 EFI index: 12, standard EFI bulid time: 14:09:54 EFI build date: 12/19/2011 CPU rev.: 0x9 Chipset rev.: 0x4 Microcode: 0x12 CPU ID: 0x206A7 CPU Branding: Intel(R) Core(TM) i7-2655LE CPU @ 2.20 GHz RIO Module: 100 </pre>

**kboardinfo (continued)**

USAGE:	KOMaOEMF rev.:	Revision of KOMaOEMF protocol
	Board ID:	Kontron board identification value
	Hardware rev.:	Hardware revision of this board
	Logic rev.:	Logic revision of this board
	Boot flash:	Current boot flash: either “Standard SPI boot flash” or “Recovery SPI boot flash”
	In system slot:	Indicates whether the board is installed in the system slot.
	Geographic Address:	Geographic address of the cPCI backplane slot the board is currently plugged into
	Material number:	Kontron hardware reference number
	Hardware index:	Kontron hardware index
	Serial number:	This board’s unique serial number
	EFI article name:	Kontron uEFI reference name
	EFI material number:	Kontron uEFI reference number
	EFI index:	Version of this uEFI BIOS
	EFI build time:	Build time of this uEFI BIOS
	EFI build date:	Build date of this uEFI BIOS
	CPU rev.:	Chip revision of the CPU
	Chipset rev.:	Chip revision of the Chipset
	Microcode:	Currently loaded microcode
	CPU ID:	CPU ID
	CPU Branding:	CPU identification string
RIO Module:	RIO module identification bit pattern	



6.2.3 kboot uEFI Shell Command

kboot

FUNCTION:	Boot a legacy OS Not to be used for uEFI BootLoaders!
SYNTAX:	<pre>kboot [-? -d -p -p <path> -n <name> -t <type>]</pre> <p>where:</p> <ul style="list-style-type: none"> ? Show online help -d Boot default order -p <path> Specify the path to the device to boot from -n <name> Specify the device name to boot from -t <type> Specify the device type to boot from <p>Available types are:</p> <ul style="list-style-type: none"> floppy harddrive cdrom network usb-floppy usb-harddrive usb-cdrom
DESCRIPTION:	The kboot command boots a legacy OS. Boot device can be selected in a very flexible way. If the requested device is not present, boot returns to shell. The kboot command cannot boot native uEFI-aware operating systems. But since these are bootable from shell by calling their bootloader, this is not necessary either. If a requested device is present but not bootable, uEFI continues to boot with the next bootable device in the boot order.
USAGE:	<p>Show all connected devices:</p> <p>COMMAND / RESPONSE:</p> <pre>fs0:\> kboot _____ BBS_TABLE 00002 network "IBA GE Slot 0100 v1300" 00003 network "IBA GE Slot 0101 v1300" 00004 network "IBA GE Slot 0200 v1300" 00005 network "IBA GE Slot 0201 v1300" 00002 usb-harddrive "SanDisk uSSD 5000 0.1" Device path: Acpi(PNP0A03,0)/Pci(1A 7)/Usb(1,0) 0001 usb-harddrive "KingstonDataTraveler 2.04.10" Device path: Acpi(PNP0A03,0)/Pci(1D 7)/Usb(1,0)</pre> <p>Boot from device containing the string "Kingston":</p> <pre>fs0:\> kboot -n Kingston</pre> <p>Boot from the first device found that is of type floppy:</p> <pre>fs0:\> kboot -t floppy</pre>



6.2.4 kbootnsh uEFI Shell Command

kbootnsh

FUNCTION:	Manage the startup script stored in the flash
SYNTAX:	<pre>kbootnsh [-b][-? -g <filename> -p <filename> -d]</pre> <p>where:</p> <ul style="list-style-type: none"> -b Display output page by page -? Show online help -g <filename> Store the current boot script to disk. If there is no physical disk drive present, the kmkramdisk command may be used. -p <filename> Store the shell script pointed to by filename to flash. Note: The shell script cannot be larger than 400 bytes. -d Delete the current startup script from flash.
DESCRIPTION:	The kbootnsh command manages the flash stored startup script. If the shell is launched by the boot process, it executes a shell script stored in the flash. If the shell script terminates, the shell executes a kboot -d command to continue the boot process. However, the shell script can of course contain any other boot command.
USAGE:	<p>Get current startup script to file named boot.nsh</p> <p>COMMAND / RESPONSE:</p> <pre>Shell> kbootnsh -g boot.nsh</pre> <p>Store file named boot.nsh to flash:</p> <p>COMMAND / RESPONSE:</p> <pre>Shell> kbootnsh -p boot.nsh</pre> <p>Delete startup script:</p> <p>COMMAND / RESPONSE:</p> <pre>Shell> kbootnsh -d</pre>



6.2.5 kclearnvram uEFI Shell Command

kclearnvram

FUNCTION:	Clear the NVRAM to restore the system's default settings
SYNTAX:	<code>kclearnvram</code> No parameters required. For safety reasons this command must be confirmed by pressing "c".
DESCRIPTION:	The kclearnvram command allows to clear the system NVRAM. Since all uEFI settings are stored inside the NVRAM, the default settings are loaded afterwards.

6.2.6 kclsp uEFI Shell Command

kclsp

FUNCTION:	Configure clock spreading
SYNTAX:	<code>kclsp [-? -d -e]</code> where: -? show help -d disable clock spreading -e enable clock spreading
DESCRIPTION:	The kclsp command enables or disables clock spreading on the onboard core clock generator. Clock spreading can be used to reduce system EMI.
USAGE:	Get help: COMMAND / RESPONSE: <code>Shell> kclsp -?</code> <code>Kontron Clock Spreading Configuration for ICS9LPRS365</code> <code>-d disable clock spreading</code> <code>-e enable clock spreading</code> Default setting: disable



6.2.7 kflash uEFI Shell Command

kflash

FUNCTION:	Manage uEFI BIOS update
SYNTAX:	<p>kflash [-p -i -v -s -c -h -?] [-f] [-r] [file]</p> <p>Operation mode:</p> <ul style="list-style-type: none"> -p Program flash -i Show information string and check CRC -v Verify flashed image -s Save current ROM image to file -c Clone flash content to second flash -h Show this help -? Show online help <p>file uEFI BIOS binary file</p> <p>Options:</p> <ul style="list-style-type: none"> -f Force write <p>Expert options: Not recommended for standard use</p> <ul style="list-style-type: none"> -r Raw image mode (.bin, .rom)
DESCRIPTION:	The kflash command is used to program and verify the flash banks holding the uEFI BIOS code. uEFI BIOS binary files must be available from connected mass storage devices, such as USB flash drive or harddisk.
USAGE:	<p>Get help:</p> <p>COMMAND / RESPONSE:</p> <pre>shell> kflash -?</pre> <p>Get help:</p> <p>COMMAND / RESPONSE:</p> <pre>shell> kflash -h</pre> <p>Program the uEFI BIOS into the standard SPI boot flash:</p> <p>COMMAND / RESPONSE:</p> <pre>shell> kflash -p BIOS_file.kf1</pre> <p>Note: This function will select and update the standard SPI boot flash regardless of the DIP switch setting (CP6003-SA/RA) / configuration resistor setting (CP6003-RC) for boot selection.</p> <p>Copy the currently running uEFI BIOS into the inactive SPI boot flash:</p> <p>COMMAND / RESPONSE:</p> <pre>shell> kflash -c</pre> <p>Note: Using this function will overwrite the inactive SPI boot flash. Failures during the process will make the inactive SPI boot flash invalid. In such cases, please execute the function again until the process completes successfully.</p>



6.2.8 kipmi uEFI Shell Command

kipmi

FUNCTION:	Read or configure available MMC parameters
SYNTAX:	<pre>kipmi [-? -b parameters]</pre> <p>where:</p> <ul style="list-style-type: none"> -? show online help -b display output page by page <p>parameters</p> <ul style="list-style-type: none"> fru -- display fru data: [Fru Device ID] ipmb -- ipmb bus settings: ipmb [redundant / single] irq -- get / set KCS IRQ: irq [number] mode -- set ipmi controller mode: mode [bmc / smc] net -- display and change SOL network settings sel -- handle system event log sensor -- show sensor related information raw -- execute raw ipmi command rawsendmessage -- execute raw SendMessage ipmi cmd info -- show information about the device and firmware
DESCRIPTION:	The kipmi command can read event logs or set the MMC IRQ configuration. This shell application can also be used to set up raw command to the MMC.
USAGE:	<p>Display fru data:</p> <p>COMMAND / RESPONSE:</p> <pre>Shell> kipmi fru 0</pre> <p>Display ipmb bus settings:</p> <p>COMMAND / RESPONSE:</p> <pre>Shell> kipmi ipmb</pre> <p>Change IRQ configuration:</p> <p>COMMAND / RESPONSE:</p> <pre>Shell> kipmi irq 10</pre> <p>Show IRQ configuration:</p> <p>COMMAND / RESPONSE:</p> <pre>Shell> kipmi irq</pre>



kipmi (continued)

USAGE:	Set IPMI controller mode: COMMAND / RESPONSE: <code>Shell> kipmi mode</code>
	Set Serial-over-LAN I/O/SOL parameters: COMMAND / RESPONSE: <code>Shell> kipmi net 1</code>
	Display system event log: COMMAND / RESPONSE: <code>Shell> kipmi sel list</code>
	Show sensor related information: COMMAND / RESPONSE: <code>Shell> kipmi sensor list</code>
	Execute raw command. Example: Get self-test results. COMMAND / RESPONSE: <code>Shell> kipmi raw 0x06 0x00 0x04</code>
	Execute raw SendMessage command: COMMAND / RESPONSE: <code>Shell> kipmi rawsendmessage 0x20 0x00 0x06 0x00 0x01</code>
SETTINGS:	fru [<Fru device ID>]: Displays FRU data Options: fru device ID: Numeric FRU device ID. The FRU ID 0 is used by default if no FRU ID is entered.
	ipmb: Displays IPMB bus settings ipmb redundant: Switch IPMB bus to redundant mode ipmb single: Switch IPMB bus to single mode Note: The redundant mode is not available on the CP6003-SA/RA/RC. Please leave this function at single mode.
	irq <number>: Display/Set the IRQ number of the KCS interface Options: 0: KCS uses no IRQ 10: KCS uses IRQ 10 11: KCS uses IRQ 11 The board must be reset for the settings to apply.



kipmi (continued)

SETTINGS:	mode <mode>: Display/Set the IPMI controller operating mode Options: bmc : IPMI controller operates in BMC mode (master) smc : IPMI controller operates in SMC mode (slave)
	net : Set IPMI-over-LAN (IOL) / Serial-over-LAN (SOL) parameters
	sel : Display system event log
	sensor list read : Show board sensor data Options: list : Display an overview of all available board sensors read : Display specific sensor data
	raw [<bytes> <...>]: Execute raw IPMI command Syntax: raw [NetFn] [LUN] [COMMAND] ...
	rawsendmessage [<bytes> <...>]: Execute raw SendMessage command Syntax: rawsendmessage [rsSa] [CHANNEL] [NetFn] [LUN] [COMMAND] ...
	info : Display IPMI firmware information



6.2.9 kmkramdisk uEFI Shell Command

kmkramdisk

FUNCTION:	Create RAMdisk drives
SYNTAX:	<pre>kmkramdisk [-? -s <size> <name>]</pre> <p>where:</p> <p>-? show help</p> <p>-s <size> <name> create a RAMdisk of given size in Megabytes with the mount point name <name></p>
DESCRIPTION:	<p>Creates a RAMdisk of variable size. Can be very useful to perform file operations when no real filesystem is connected to the system.</p> <p>Note: The RAMdisk loses its mount point name after all drives are remapped by the map -r command. The RAMdisk will then be enumerated as any other connected drive and gain a mount point name like "fs0". This is not a bug of the kmkramdisk command but a normal function of the uEFI framework.</p>
USAGE:	<p>Create RAMdisk:</p> <p>COMMAND / RESPONSE:</p> <pre>rd:\> kmkramdisk -s 5 myramdisk Device mapping table myramdisk :BlockDevice - Alias (null) VenMsg'(93B5F448-127A-4B29-B306- 5BE8AAC4826E) Success - Force file system to mount rd:\> myramdisk: myramdisk:\> echo testfile > testfile myramdisk:\> ls Directory of: myramdisk:\ 05/24/08 04:39a 22 testfile 1 File(s) 22 bytes 0 Dir(s)</pre>



6.2.10 kpassword uEFI Shell Command

kpassword

FUNCTION:	Control uEFI Setup and Shell passwords
SYNTAX:	<p><code>kpassword [-u -s]</code></p> <p>Call without parameters to get current password status</p> <p>Parameters:</p> <ul style="list-style-type: none"> -u Install or change User password -s Install or change Superuser password <p>Note: Old passwords must be verified if set. Entering an empty password disables the password.</p>
DESCRIPTION:	The kpassword command is used to get and set the uEFI Shell and Setup passwords. Both User and Superuser (Administrator) passwords can be controlled.
USAGE:	<p>Control EFI setup and shell passwords</p> <p>COMMAND / RESPONSE:</p> <pre>kpassword [-u -s] No password is installed! Enter new USER password --> Retype password --> Done.</pre>



6.2.11 kresetconfig uEFI Shell Command

kresetconfig

FUNCTION:	Control the board reset behavior
SYNTAX:	<p>kresetconfig [-? <parameter>]</p> <p>where:</p> <p>-? Show help</p> <p><parameter> pcislave [on off]</p> <p>Controls if the board shall react on a CPCI backplane reset if it is used as slave board in a peripheral slot. It has no effect if the board is located within a CPCI master slot.</p> <p>Note: This parameter is volatile, and at next start is set to off.</p>
DESCRIPTION:	The kresetconfig command controls the board's reset behavior.
USAGE:	<p>Enable CPCI backplane reset:</p> <p>COMMAND / RESPONSE:</p> <pre>Shell> kresetconfig pcislave on Reset from system master is enabled</pre> <p>Disable CPCI backplane reset:</p> <p>COMMAND / RESPONSE:</p> <pre>Shell> kresetconfig pcislave off Reset from system master is disabled</pre>

6.2.12 **kwdt** uEFI Shell Command**kwdt**

FUNCTION:	Configure the Kontron onboard Watchdog
SYNTAX:	<pre>kwdt [-? -t <timeindex>]</pre> <p>where:</p> <ul style="list-style-type: none"> -? Show help -t <timeindex> Configure the Watchdog with the time related to timeindex and activate it with reset routing <p>Call kwdt -h to obtain a list of time index values and related times</p>
DESCRIPTION:	The kwdt command allows to enable the Kontron onboard Watchdog with reset target before OS boot. This can be used to detect if the OS fails to boot and react by reset. The OS Watchdog driver is required for this functionality to operate.
USAGE:	<p>Get help:</p> <p>COMMAND / RESPONSE:</p> <pre>Shell> kwdt -? -t [time] - set Timer value 0 = 125ms value 1 = 250ms value 2 = 500ms value 3 = 1s value 4 = 2s value 5 = 4s value 6 = 8s value 7 = 16s value 8 = 32s value 9 = 64s value 10 = 128s value 11 = 256s value 12 = 512s value 13 = 1024s value 14 = 2048s value 15 = 4096s</pre>

**kwdt (continued)**

USAGE: Set Watchdog to 16 seconds and activate it

COMMAND / RESPONSE (none):

```
Shell> kwdt -t 7
```

Note: Because there is no application which triggers the Watchdog, the system will be reset after 16 seconds in this case. This command should be invoked from a script, followed by an operating system boot, and the OS then has to start triggering the Watchdog.

Display Watchdog configuration:

COMMAND / RESPONSE:

```
Shell> kwdt
```

Kontron Board Watchdog Configuration:

Watchdog Configuration Register (0x28C): 0x00



6.3 uEFI Shell Scripting

6.3.1 Startup Scripting

If the ESC key is not pressed and the timeout is run out, the uEFI Shell tries to execute some startup scripts automatically. It searches for scripts and executes them in the following order:

1. Kontron flash-stored startup script
2. If there is no Kontron flash-stored startup script present, the uEFI-specified `startup.nsh` script is used. This script must be located on any of the attached FAT formatted disk drives under `\efi\boot\startup.nsh`.
3. If none of the startup scripts is present or the startup script terminates, the default boot order is continued.

6.3.2 Create a Startup Script

Startup scripts can be created using the uEFI Shell built-in editor `edit` or under any OS with a plain text editor of your choice. To create a startup shell script, simply save the script on any FAT-formatted drive attached to the system under the file name `\efi\boot\startup.nsh`. To copy the startup script to the flash use the `kbootnsh` uEFI Shell command.

In case there is no mass storage device attached, the startup script can be generated in a RAM disk and stored in the flash bank.

6.3.3 Examples of Startup Scripts

6.3.3.1 Automatic Booting from USB Flash Drive

Automatic booting is made from a USB flash drive, if present, otherwise the boot is made from the harddrive.

```
kboot -t usb-harddrive
kboot -t harddrive
```

If neither a USB flash drive nor a harddrive is present, the boot order is continued.

6.3.3.2 Switch On Clock Spreading Prior to Booting from Harddrive

```
kclsp -e
kboot -t harddrive
```

If no harddrive is present, the default order is continued.

6.3.3.3 Execute Shell Script on Other Harddrive

This example executes the shell script named `bootme.nsh` located in the root of the first detected disc drive (`fs0`).

```
fs0:
bootme.nsh
```



6.3.3.4 Enable Watchdog and Control PXE Boot

The uEFI Shell provides environment variables used to control the execution flow.

The following sample start-up script shows two uEFI Shell environment variables, `wdt_enable` and `pxe_first`, used to control the boot process and the Watchdog.

```
echo -off
echo "Executing sample startup.nsh..."
if %wdt_enable% == "on" then
    kwdt -t 15
    echo "Watchdog enabled"
endif
if %pxe_first% == "on" then
    echo "forced booting from network"
    kboot -t network
endif
```

To create uEFI Shell environment variables, use the **set** uEFI Shell command as shown below:

```
Shell> set wdt_enable on
Shell> set pxe_first on
Shell> set
    pxe_first : on
    wdt_enable : on
Shell> reset
```



6.3.3.5 Handling the Startup Script in the Flash Bank

In case there is no mass storage device attached, the startup script can be generated in a RAM disk and stored in the flash bank using the following instructions:

4. Press <ESC> during power-up to log into the uEFI Shell.
5. Create a RAM disk and set the proper working directory as shown below:

```
Shell> kmkramdisk -s 3 myramdisk
Shell> myramdisk:
```

6. Enter the sample start-up script mentioned above in this section using the **edit** uEFI Shell command.

```
myramdisk:\> edit boot.nsh
```

7. Save the start-up script to the uEFI flash bank using the **kbootnsh** uEFI Shell command.

```
myramdisk:\> kbootnsh -p boot.nsh
```

8. Reset the board to execute the newly installed script using the **reset** uEFI Shell command.

```
myramdisk:\> reset
```

9. If a script is already installed, it can be edited using the following **kbootnsh** uEFI Shell commands.

```
myramdisk:\> kbootnsh -g boot.nsh
myramdisk:\> edit boot.nsh
```



Chapter

7

Updating the uEFI BIOS



This page has been intentionally left blank.





7. Updating the uEFI BIOS

BIOS updates are typically delivered as an update CD ISO image. This ISO image needs just to be burned to a CD and booted. Follow the menu for updating the uEFI BIOS. For further information refer to the update CD documentation.

7.1 uEFI BIOS Fail-Over Mechanism

The CP6003-SA/RA/RC has two SPI boot flashes programmed with the uEFI BIOS, a standard SPI boot flash and a recovery SPI boot flash. The basic idea behind that is to always have at least one working uEFI BIOS flash available regardless if there have been any flashing errors or not.

7.2 Updating Procedure

An update CD is provided for flashing the latest uEFI BIOS on the standard SPI boot flash. The standard SPI boot flash can also be programmed with the latest uEFI BIOS via the **kflash -p** uEFI Shell command.

Note: To have the same content in both SPI boot flashes, clone the standard SPI boot flash to the recovery SPI boot flash. For further information, please refer to Chapter 6.2.7, kflash uEFI Shell Command.

7.3 uEFI BIOS Recovery

In case of the standard SPI boot flash being corrupted and therefore the board not starting up, the IPMI controller boots the board from the recovery SPI boot flash if the DIP switch SW1 (CP6003-SA) / SW3 (CP6003-RA), switch 2 is set to OFF. On the CP6003-RC, the configuration resistor R759 must be set to Open in order for the IPMI controller to boot the board from the recovery SPI boot flash.

For further information about the boot configuration, refer to the respective chapters in the board's user guide or contact Kontron for further assistance. Information about the boot configuration for the CP6003-SA is provided in the CP6003-SA User Guide, Chapter 4.1, for the CP6003-RA in the CP6003-RA/RC User Guide, Chapter 4.1 and for the CP6003-RC in the CP6003-RA/RC User Guide, Chapter 4.2.

7.4 Determining the Active Flash

Sometimes it may be necessary to check which flash is active. On the AMI Aptio-based uEFI BIOS, the information is available using the **kboardinfo** uEFI Shell command. For further information, refer to Chapter 6.2.2, kboardinfo uEFI Shell Command.



This page has been intentionally left blank.

