Marvell ThunderX2™ (CN99XX)

Aptio® V support for Marvell's latest ThunderX2™ family of ARM64 SOC

APTIO® V FOR ARM64

Aptio® V for ARM64 is the "next generation of UEFI BIOS supporting ARM64", featuring support for the latest Marvell ThunderX2™ family of ARM64 SOC's. AMI is enabling two reference platforms from Marvell, Borg and Saber. This allows AMI to provide comprehensive support to all the ThunderX2™ family.

Aptio® V for ARM64 firmware is intended for eco-system partners to develop production hardware, enabling customers to develop ThunderX2™ features based on their specific hardware and/or applications.

AMI ADVANTAGE

Firmware developed for the Marvell ThunderX2™ CRB (Customer Reference Platform) allows developers to accelerate their development cycle for those OEMs / ODMs, who are building ThunderX2™ platforms and developing their firmware stack to deploy ThunderX2™:

- Easy migration from x86 to ARM64
- Build structure has been improved by AMI for Aptio V and customer usability
- Superior development environment
- Superior tools for ARM64
- Full featured BIOS including highly customized BDS (Boot Device Selection) flow
- Production ready code, no IP licensing issues that comes with open source

The chipset support package for ThunderX2 SOC development will use the same source project for both CRB platforms (Borg & Saber).

OEM EMODULE CAPABILITIES

Creating an OEM eModule allows a customer to hook many portions of the BIOS for consistent changes across multiple projects. Reusing the OEM eModule in projects can almost completely customize the behavior of the BIOS for the OEM on all subsequent projects.

- Add custom drivers to the code
- Add custom interrupts
- Modify SDL parameters
- Change SMBIOS
- Change logos
- Change TSE behaviors
- Custom PCI handling
- Modify BDS and boot order behaviors
- NVRAM reset and defaults behaviors

Key Aptio Features:

- **Full UEFI 2.6 and EDK II Support**
- **Multi-processor**
- **Full ACPI Support 6.1**
- **ARM64 TrustZone Technology Support**
- **SMBIOS 3.0 Support**
- **PCIe AHCI and NVMe SSD Boot**
- **TSE (Text-based Setup Engine) including Graphical Themes**
  - **Allows easy customization of BIOS setup to provided feature rich OEM brandable versions.**
- Operating System Support includes
  - Red Hat Enterprise Linux Server for ARM Development Preview 7.4
  - CentOS 7.3 for AArch64 (64-bit ARM)
  - Ubuntu 17.10
  - SUSE Linux
- UEFI Network Stack
  - IPv4 & IPv6 Support
  - UEFI iSCSI & PXE Boot
- Boot to Linux image stored on a SD card
- Boot to Linux image stored on a USB card
- USB Mass Storage Boot - HDD, CD-ROM, DVD, FLASH
- Variable storage on SPI
- Serial Console
- Power Management
- Diagnostic tests
- IPMI Support for BMC Server Management
  - Set power on policy - always on / off
  - IP configuration
  - Boot progress report to BMC / UEFI progress codes
- TPM 2.0
- RAS (Phase 1 -DRAM Handling)
- VeB
  - GUI development studio, VeB, created by AMI, specifically for BIOS development
    - VeB groups files into logical components related to specific technologies
    - VeB helps make common platform level changes without editing source
    - Build process is configured through VeB so no need to edit complicated configuration files directly
  - Project management is controlled by the VeB with built in source control capabilities
  - SBSA/SBBR test suite cycle

RAS CAPABILITIES

Reliability, availability, and serviceability (RAS) is a computer engineering term involving performing consistently to specifications, continuing to functionally work, and the ability to respond to failure. RAS support:

- DRAM handling
- PCI configuration display (EFI Shell)
- Unified firmware for launching diagnostics
- GPIO enablement for general purpose pins
- CCPI2 error handling
- PCIe error handling
- SW GPIO notification to BMC of errors
- SOC error handling
- ARM RAS extensions

ARM64 PROJECT SOLUTIONS WITH AMI

AARCH64 NATIVE OPTION ROMS

Spring 2015 UEFI Plugfest was the first official AARCH64 Option ROMs testing platform opened for ARM64. AMI was the only IBV in attendance with support for ARM64 SoC's, providing multiple SoC's for validation and testing at this event:

- Though limited availability AMI was able to test and validate the limited cards provided.
  - Validated and tested such cards from vendors such as Aspeed

CONSOLE

In the available AARCH64 designs, the Super I/O chips and graphical (VGA) controllers are not available in the hardware. Therefore, the primary console is the serial port. To use the serial port as the main console, the AMI Serial Redirection Module (Terminal) must be in the project.

Additionally, AMI has included an Aspeed Graphics Output Protocol (GOP) in our Aptio® V for ARM64 source code package that enables a UEFI driver

The ultimate goal of GOP is to to support graphic console output in the pre-OS phase, replace legacy VGA BIOS and eliminate VGA HW functionality.

GETTING STARTED WITH AMI APTIO FOR ARM64

AMI provides a complete Getting Started Guide with instructions to setting up your Linux or Windows build environment. This document is designed as a reference for engineers starting development on an ARM64 based platform. The document will go through the steps needed for creating a new ARM based project based on the Marvell ThunderX2™ CRB platform.

APTIO® V AND AMI BMC SOLUTION

Working with Aptio® V BIOS and BMC combined provides greater manageability and this allows greater customization of OEM IPMI commands.

- Highly customized solution that provides many features that are not easily developed with a separate BIOS and BMC solution
- Extends customer IP
- BIOS provides platform knowledge and BMC provides the out-of-band manageability
- Extends the overall manageability scope
- Multiple runtime interfaces between BIOS and BMC

ROM UTILITIES AVAILABLE FOR ARM64:

- AMIBCP
  - Edit setup strings and option defaults
  - Edit BIOS strings and static SMBIOS data
- MMTool
  - Add, remove and replace option ROMs
- ChangeLogo
  - Change BIOS splash logos
- AMISDE
  - Record setup options to a spreadsheet
  - Used to archive configurations for testing and release control
- AFU Firmware Update
  - UEFI Shell and Linux support

American Megatrends

American Megatrends Inc. | ami.com
5555 Oakbrook Parkway, Bldg. 200
Norcross GA 30093 | 770.246.8600

AptioV

For more information: http://ami.com/products/