Cavium ThunderX™

Aptio® V support for Cavium's latest ThunderX™ family of ARM64 SOC

Aptio® V for ARM64 supports

Aptio® V for ARM64 is the "next generation of UEFI BIOS supporting ARM64", featuring support for the latest Cavium ThunderX™ family of ARM64 SoC's. AMI is enabling two reference platforms from Cavium i.e. the Thunder 1K (Single Processor) and the Thunder 2K (Dual Processor) . This allows AMI to provide comprehensive support to all the ThunderX™ family including:

- **ThunderX_CP™**- This family is optimized for private and public cloud web servers and content delivery, web caching and social media data analytics workloads
- **ThunderX_ST™-** This family is optimized for Hadoop, block & object storage, distributed file storage and hot/warm/cold storage type workloads
- **ThunderX_SC™-** This family is optimized for Secure Web frontend, security appliances and Cloud RAN type workloads.
- **ThunderX_NT™-** This family is optimized for media servers, scale-out embedded application and NFV type workloads.

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

AMI Advantage

Firmware developed for the Cavium ThunderX™ CRB (Customer Reference Platform) allows developers to accelerate their development cycle for those OEM's / ODM's, who are building ThunderX™ platforms and developing their firmware stack to deploy ThunderX™ such as-

- 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

Key Aptio Features:

- Full UEFI 2.4 and EDK II Support
- Multi-processor Support
- Full ACPI Support
- ARM TrustZone® Technology Support
- SMBIOS 3.0 Support
- Fully featured BIOS that enables all boot devices of a platform
- UEFI Secure Boot Support
- PCIe AHCI and NVMe SSD Boot
- TSE (Test 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 7.2
  - CentOS 7 for the AArch64 (64-bit ARM)
  - Ubuntu
  - SUSE Linux
- UEFI Network Stack
  - IPv4 & IPv6 Support
  - UEFI iSCSI & PXE Boot
- Native Recovery Support
- IPMI Support
- 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

ROM Utilities Available for ARM:

- 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

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

ARM Project Challenges with AMI Solutions

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.

System Management Mode (SMM) vs. ARM TrustZone®

ARM TrustZone® technology can secure a specific memory region to protect it from software attack. This is similar to SMM (System Management Mode) which is widely available with IA platforms.

An AMI proprietary UEFI driver utilizes ARM TrustZone® to accomplish a SMM simulation. The AMI driver simulates the SMM behaviors and SW SMI functions. The SW SMI dependent UEFI functions can easily migrate to ARM platforms on top of the UEFI driver.

The SW SMI handlers can be reached through one of the following:

- UEFI SMM Communication Protocol
- AFRI is a UEFI variable service based interface

UEFI functions, applications and OS tools can utilize one of the above interfaces to invoke SW SMI handlers.

- For the ARM SoC without TrustZone®, the AMI proprietary driver can still simulate SMM by preserving a runtime memory region as SMRAM.

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 to support graphic console output in the pre-OS phase.

The ultimate goal of GOP is to 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 ARM/ARM64 based platform. The document will go through the steps needed for creating a new ARM based project based on the Cavium ThunderX™ CRB platform.

Aptio® V and AMI BMC Solution Together

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

American Megatrends

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

Aptio V

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