presented by

ARM®

UEFI Forum ARM Update

UEFI Spring Plugfest – March 29-31, 2016
Presented by Mitch Ishihara

Agenda

- Economics
- Status Overview
  - Specifications
- Resources
- Call to Action

Economics

Economics

What are the ARM numbers?

Silicon with ARM IP shipped in 2015	: 14.8 Bu
Cumulative total shipped	: 75+ Bu
Processor + GPU licenses	: 1375+
Licensees	: 400+
Foundry partners	: 5+
Process technology	: 10 – 250 nm
Connected community members[1]	: 1300+

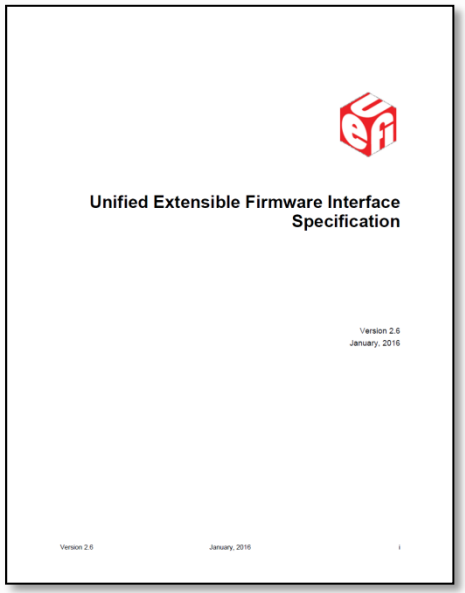
[1] Important for a collaborative business model

Economics (1300+)

Specifications

Status Overview

UEFI Specification Updates



New: Published in UEFI Specification 2.6

- Common Platform Error Record (CPER)
  - Firmware first hardware error handling

Published in UEFI Specification 2.5 errata A and 2.6

- 4KB and 64KB page attributes for AArch64
  - Clarification that mixed attribute mappings within a larger page are not allowed
- AArch64 bindings alignment checking
  - Data alignment fault checking disabled

ACPI Specification Updates

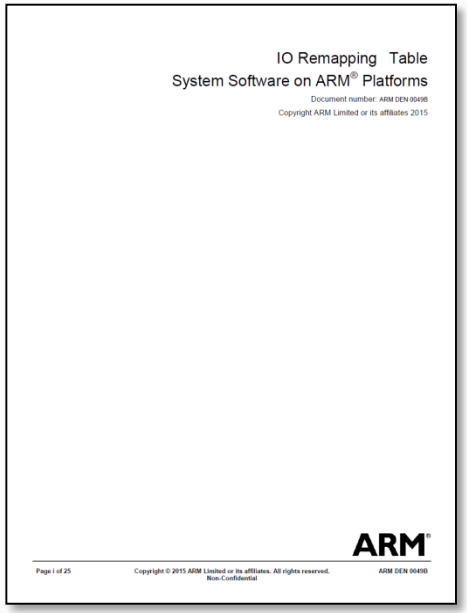
ACPI 6.0 adopted April 2015 addressing the following for ARM:

- ✓ Low Power Idle Table (LPIT)
- ✓ IO topology and SMMU
  - I/O Remapping Table (IORT)
- ✓ GIC Interrupt Translation Service (ITS)
  - MADT GIC ITS Structure
- ✓ …and others

ACPI 6.1 adopted January 2016 addressing the following for ARM:

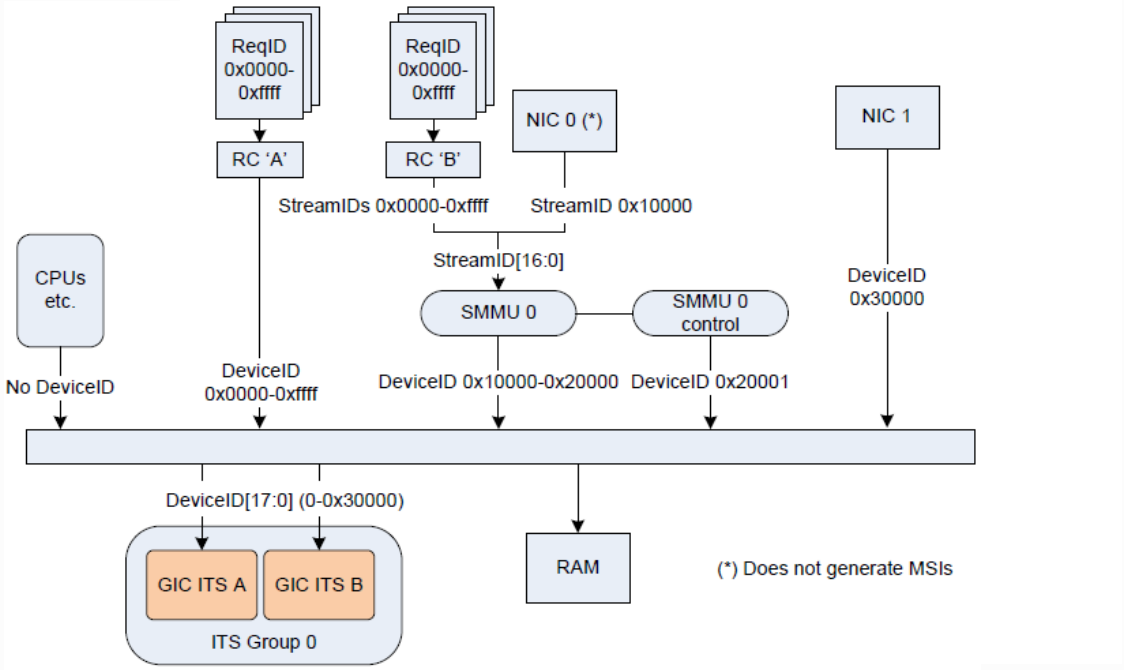
- ✓ ARM ACPI Platform Error Interfaces (APEI) extensions

ARM ACPI Companion Specs


IO Remapping Table
System Software on ARM® Platforms
Document number: ARM DEN 0049B
Copyright ARM Limited or its affiliates 2015
ARM
Page 1 of 25
Copyright © 2015 ARM Limited or its affiliates. All rights reserved.
Non-Confidential
ARM DEN 0049B

Input Output Remapping Table (IORT)

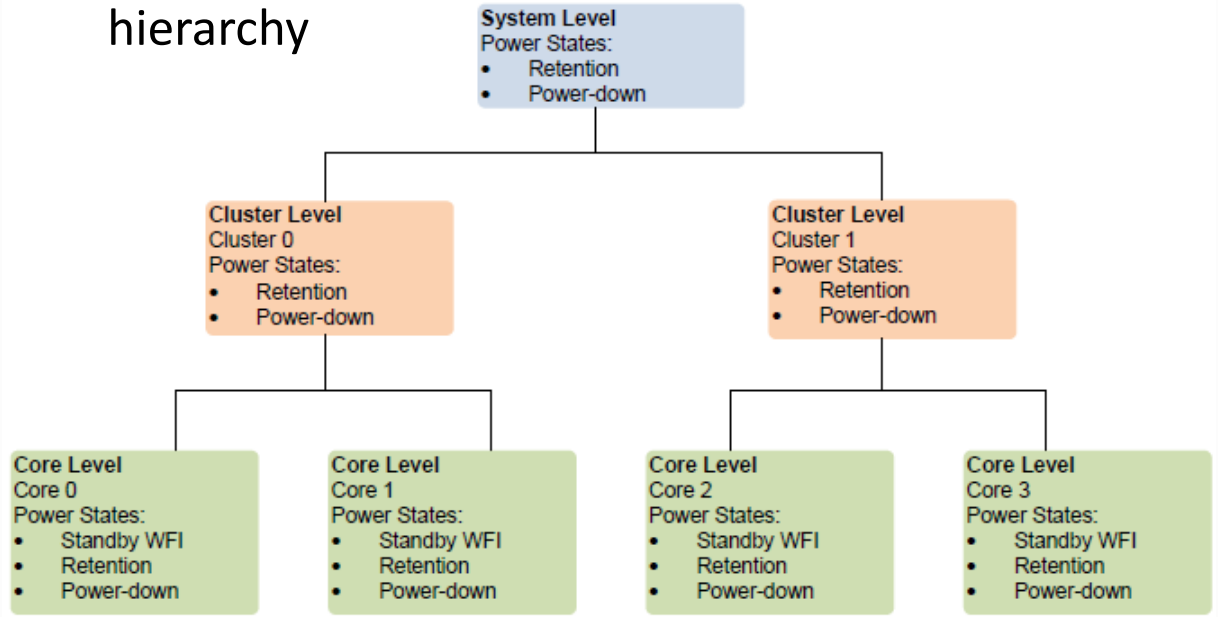
- Provides an ACPI description for IO Topology, SMMU, GIC ITS



ARM ACPI Companion Specs

ARM Functional Fixed Hardware (FFH) Specification

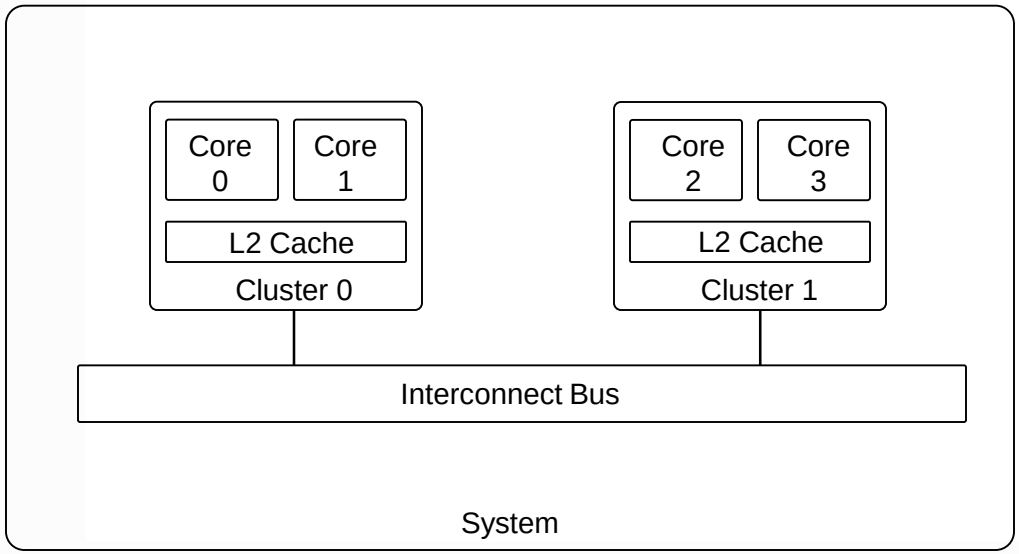
- Idle Management and Low Power Idle (LPI) states
- Alignment with Low Power Idle (LPI) states introduced in ACPI 6.0
- OS managed power states of power domain hierarchy



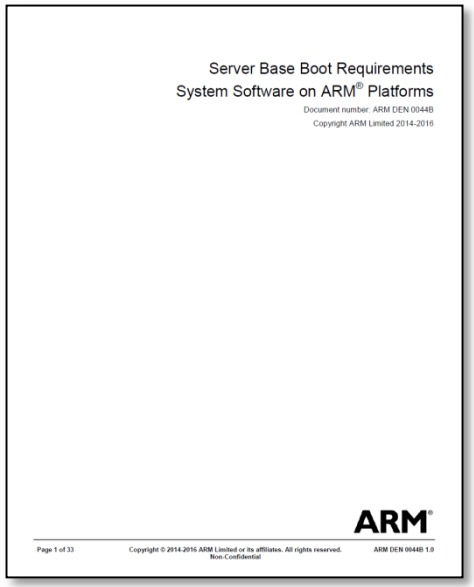
ARM ACPI Companion Specs

ARM Functional Fixed Hardware (FFH) Specification

- Idle Management and Low Power Idle (LPI) states
- Alignment with Low Power Idle (LPI) states introduced in ACPI 6.0
- OS managed power states of power domain hierarchy



ARM Specification Updates



ARM boot architecture

- Published ARM Server Base Boot Requirements (SBBR) v1.0
  - Targets SBSA-compliant 64-bit ARMv8-A servers
  - UEFI Specification 2.5
    - Boot services, Runtime services, protocols
  - ACPI Specification 6.0
    - ACPI Tables: mandatory, recommended, optional
    - ACPI Methods and Objects
  - SMBIOS 3.0.0
- Updated SBBR review cycle to follow
  - UEFI Specification 2.6
  - ACPI Specification 6.1

PI Specification Updates

- Active work on ARM Management Mode extensions to Volume 4 PI Specification
- Join the PIWG and sub-team

Resources

Resources

ARM Server Base Boot Requirements (SBBR)

- http://infocenter.arm.com/help/topic/com.arm.doc.den0044b/index.html

ARM Functional Fixed Hardware Specification

- http://infocenter.arm.com/help/topic/com.arm.doc.den0048a/index.html

IO Remapping Table

- http://infocenter.arm.com/help/topic/com.arm.doc.den0049b/index.html

Call to Action

Call to Action

Join the PIWG and ABST sub-team

- Active work on ARM Management Mode extensions to Volume 4 PI Specification

PCIe Option ROM: Support for any architecture

- Three options:
  1. EBC Option ROM image and UEFI EBC VM interpreter
     - True cross architecture solution - a single image

  2. Native port to targeted architecture(s)
     - Requires multiple additional images, multiple SKUs, additional validation

  3. Emulation of x86 Option ROM image
     - Could be a fragile solution and require a lot of PlugFests!

- Compiler for EFI Byte Code
  - Intel® C Compiler for EFI Byte Code
  - Open source (LLVM) C Compiler for EFI Byte Code (long-term solution?)

Summary

Summary

- UEFI firmware first hardware error handling
  - Common Platform Error Record (CPER)
- Tightening of UEFI Specification AArch64 bindings
- Active work on ARM Management Mode extensions to PI Specification Volume 4
- ACPI Specification and ARM companion specs
  - ARM ACPI Platform Error Interfaces (APEI) extensions
  - ACPI MADT GIC Interrupt Translation Service (ITS) Structure
  - ARM I/O Remapping Table (IORT)
  - ACPI Low Power Idle Table (LPIT)
  - ARM Functional Fixed Hardware (FFH) Specification
- ARM Server Base Boot Requirements (SBBR) v1.0
- PCIe Option ROM: Support for any architecture

Thanks for attending the
UEFI Spring Plugfest 2016

For more information on the Unified EFI Forum and UEFI Specifications, visit
http://www.uefi.org

presented by

ARM®