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

### What are the ARM numbers?

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Silicon with ARM IP shipped in 2015</td>
<td>14.8 Bu</td>
</tr>
<tr>
<td>Cumulative total shipped</td>
<td>75+ Bu</td>
</tr>
<tr>
<td>Processor + GPU licenses</td>
<td>1375+</td>
</tr>
<tr>
<td>Licensees</td>
<td>400+</td>
</tr>
<tr>
<td>Foundry partners</td>
<td>5+</td>
</tr>
<tr>
<td>Process technology</td>
<td>10 – 250 nm</td>
</tr>
<tr>
<td>Connected community members&lt;sup&gt;1&lt;/sup&gt;</td>
<td>1300+</td>
</tr>
</tbody>
</table>

<sup>1</sup> Important for a collaborative business model
Economics (1300+)
**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
Input Output Remapping Table (IORT)
- Provides an ACPI description for IO Topology, SMMU, GIC ITS
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

ARM Server Base Boot Requirements (SBBR)


ARM Functional Fixed Hardware Specification

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

IO Remapping Table

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®