

UEFI ARM Update

Presented by Mitch Ishihara



UEFI Plugfest – October 2014

Agenda



Economics Objectives **Status Overview Specifications** Implementation Testing Technology Resources





Economics

Economics

What are the ARM numbers?

Processors shipped in 2013 Processors shipped in total Processor licenses Semiconductor partners Process technology

Connected community members

- : **10+ Bu** (~8.7 Bu`12)
- : **50+ Bu**
- : **1000+** (850'12)
- : 310+ (290'12)
- : 10 250 nm
- : **1000+** (950'12)





Economics (1000+)

SILICON PARTNERS

DESIGN SUPPORT PARTNERS

Stereon CCar Care Anyka Steeling Withoutan Amarkam manager Launan Ing State Anator II Carlies Granz DY BOUARE TH 🦷 🔬 🖓 🖓 MREXYCON & Shine Par Provide PDTi Mbelite EATThink Ersycare Settware 032013 Ramon Computer ESTEREL ENEA Arctarus denes! Continuenter to NSW @ conciss NSC Discussion HOYA 2 🗱 🛋 🖓 SUBARTE 🕅 👘 📩 cādence an 🖄 💭 🖓 SUBARTE 🕅 🗰 LEVIE TAKET PLa denar & TARADAY 2005 CREMERY ALTORS & Hox-Rays & Augmentum nesys Bills Totalphase Scode red ALDEC) Life Dear House Control Sectories Plat Home Ci Absint COUNDOS VIERAN Dorado CALANS EXTERNAL CROSSWARE A MathWorks () I III MULTORE EMPROY COMPANY BRANCON DECEMBER CONTRACTOR CONTRACTOR CONTRACTOR ROSTNA (ATLAS NEGMOTE DOWNSATORIES () TRUESHIE FRETARTS TRATERTE CERTIS CALVERO SALVERO SALVERO Tektronix Markin Soft Interstreament 1117 ANNY AVOID BOTTON MAR OVICE COCKED TOPPAN CONTINUED COMPANIES COMPANIES ACCORE SLOW TOWERS OFFICE COLOR STREET TOPPAN

APTCORE SLOS ICHARGE CLERKE COLOR STREWTON DE BOUNDATY DIRECT MYIR QUARE ORED Amon Savoite Carlos Mill Ovice aborron Toppins Frances Millin Ovice aborron Toppins

software, training and consortia partners

👔 😳 certicom. 💷 🕅 Prestant. MARAE & ANACON 🔤 🧞 🦛 Sara enbedded 🕬 CALLER CONTROL altzem ⊶ PiXSonic. genesi @etokey Sembitel ⊕reizevotke MONTELINE BUILD GOAL Detakey GAME SELECT O PLDC expressiogle DIS Additionable Statistics & Marphoine. AdaCore BLOOMBASE & Keylemon **E**123 est embien ANID CouthIT Panel A Autore Multicore howers master mage The state and scorts TMC De Laurer Breather Courtes In Crocke Valence TURES III UR STARPHIC ASIC ESPICO TATA Contract Contrac NP 🖲 xandros againten diatsor Finder 🕬 10000 Xon theore xively incube & DDC-I ARICENT GROUP atimesys: It' memohe dinsyde war ATTREE D SoftRISC .cod EXTERN Of Mandelive MRETECH & YOU! @ weight Wins Chis Section of Change Cloring Cloring Control Cont Tradicio Contanto de la contractorian conference international la contractorian conference international conference inter Geometics & Electron Commence Street Barrier Barr CLOSE 24 JANE 24 JAN 25 K BY BR DE STORES Separa SpectraCore Tetalo C (Crantin Construction Construction) + CFADAN CARGE NICKA 4000 MERSION CONTRACTION OF CONTRACT OF CO

Induces CALICEDA WAVE CALC ZTE中兴 SIGNOBLE REALIZED CONTRACTOR CONT Disretiz (Ash # Street and Street Starten Sydaap TWEND SERVER ONALOW (O REAL AND MOBILEXE CIVITION Remaining the second of the se Sunner Section Section 2010 Contraction Co

The UEFI Forum



Objectives

Why UEFI on ARM?



Driving forces for UEFI on ARM

- Processor and system complexity increasing
- Support existing partners' ARM processor-based UEFI solutions
- Help standardize boot process for ARM processor-based platforms
- Improve hardware-software interface for OS that targets the ARM architecture

Advantages to ARM partners and OEMs

- Write once per platform, saving costs in boot loader development
- UEFI specification peer reviewed and published
- Tested UEFI drivers available from 3rd party peripherals providers
- Provides an environment for manufacturing tests

ARM UEFI Vision



Provide standard ARM architectural support

- Correctness in implementation within ARMv7-A and ARMv8-A architectures
- Future Proof through standardization (rather than proprietary) reference software
- Focus on reducing fragmentation and overall partner support costs

Provide reference ports of UEFI for ARM development platforms

Support BIOS (and other) partners' UEFI development

Directly and through organizations such as Linaro

ARM UEFI Engineering



UEFI support for the ARM Architecture

- Maintain ARM packages and docs in Tianocore EDK2 repository
- Implement support for new ARM architectures, CPUs and system IP
- Implement common UEFI features or applications for ARM
- Maintain SCT for ARM and validate on standard platforms
- Align with relevant ARM Platform Design Documents (PDDs)

UEFI support for ARM platforms

- Porting for new ARM development platforms
- Maintained within EDK2 (for standard platforms) or other neutral repository

Help partners with UEFI platform code management and development

Juno ARM Development Platform



Cortex-A57 and Cortex-A53 big.LITTLE

Reference firmware

ARM Trusted Firmware UEFI Tianocore EDK2

UEFI support booting any rich OS







Status Overview

The UEFI Forum

UEFI Specification Updates



Approved UEFI Specification 2.4 AArch64 binding clarifications and omissions errata

- Boot configuration requirements (modes, registers, and bit settings)
- Memory alignment restriction to enable 64K page mappings at runtime.
- Functionality to allow use of runtime Services from either EL1 or EL2 exception levels.
- Fixes and runtime usability improvements for AArch64 systems.
- Queued for publication in next update to UEFI Specification



Unified Extensible Firmware Interface Engineering Change Request (ECR)

Draft for Review

Title: AArch64 binding clarifications and errata.

Document: XXXXXXX

Sponsor: Jason Parker, ARM Submission for Review Date: 4 July 2014 Review Approval Date: x/xx/200x Submission for Technical Editing Date: x/xx/200x Submission for Draft Review Date: x/xx/200x Verification Date: x/xx/200x Verifier: firstname lastname, company

ACPI Specification Updates

ACPI 5.1 adopted July 22nd addressing the following for ARM:

✓ Virtualization support for GICv2m, GICv3 for alignment with SBSA

- Improved GIC Architecture description and compatible with SBSA Level 1
- ✓ Added PSCI support
- ✓ Added platform/system memory mapped Generic Timer support
 - Alignment with SBSA Level 1
- ✓ Added support for SBSA Level 1 Generic Watchdog Timer
- Support for clock management and other Device Specific Data features of an SoC

Active ACPI work on support for:

- o Idle management
- CPU topology
- SMMU or IO topology
- o GIC Interrupt Translation Service



Advanced Configuration and Power Interface Specification

> Revision 5.1 [July, 2014]

ARM Specification Updates

ARM boot architecture

Published ARM Server Base Boot Requirements

- Targets SBSA-compliant 64-bit ARMv8 servers
- Defines base firmware requirements for out-ofbox OS or hypervisor support
- UEFI Specification 2.4B or later
 - Boot services, Runtime services, protocols
- ACPI Specification 5.1 or later
 - ACPI Tables: mandatory, recommended, optional
 - ACPI Methods and Objects



Server Base Boot Requirements System Software on ARM[®] Platforms Document number: ARM DEN 0044A Copyright ARM Limited 2014

Copyright @ 2014 ARM Limited. All rights reserve

Page 1 of 32

EDK2 Implementation Updates



- Pushed and stabilized AArch64 code into the EDK2 repository
- Juno support (AArch64 platform, ACPI support)
- Enabled VirtIo support on ARM Fixed Virtual Platform models
- Android FastBoot support
- UEFI Runtime Services support
 - Documentation: <u>http://tianocore.sourceforge.net/wiki/ArmPkg/Runtime</u>
- Optimization (size & speed)

Future Tianocore EDK2

- Enabling LLVM tool chain
- More optimization!



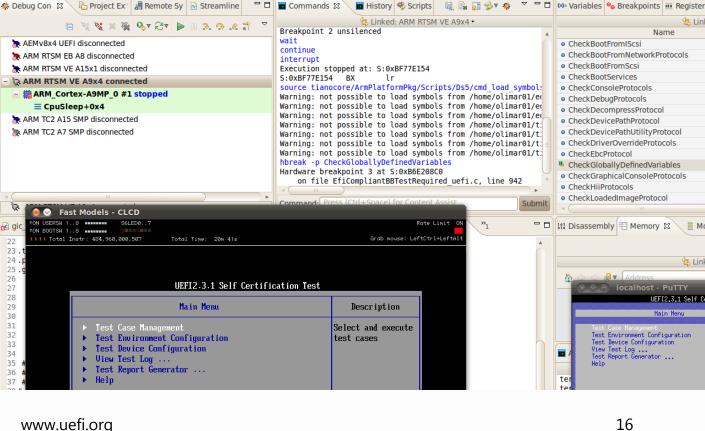
SCT Implementation Updates

SCT "new code base"

- Aligned with EDK2
- Enables both EDK Shell and UEFI Shell 2.0
- Defect fixes
- Optimization (size & speed)

UEFI v2.4B SCT "release candidate"

 Test and send feedback to UTWG



DS-5 Debug - /home/olimar01/tianocore/Build/ArmVExpress-RTSM-A9x4/DEBUG ARMLINUXGCC/ARM/MdePkg/Library/BaseCpuLib/BaseCpuLib/OUTPUT/Arm/Cpu

23. 24.

25.0 26

27

28

29

30 31

32

33

34

35

36

37

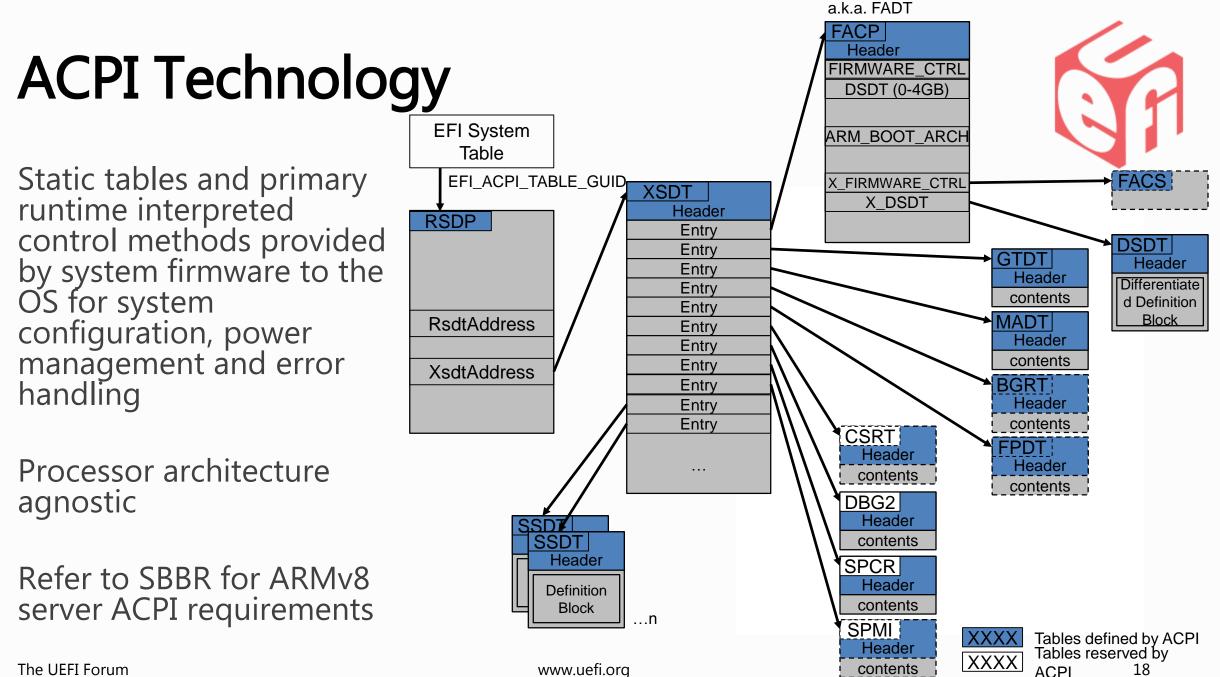
le Edit Navigate Search Project Run Window Help

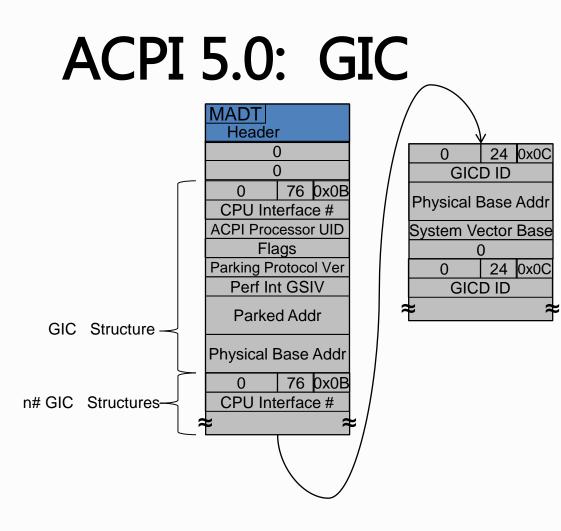
📑 🖬 💼 📄 👘 🛛 🔊 🔊 🖓 🔻 🖉 🖓 🛪 🏷 🖓 🗸 🖓



New Features in ACPI 5.1 for ARM

Technology





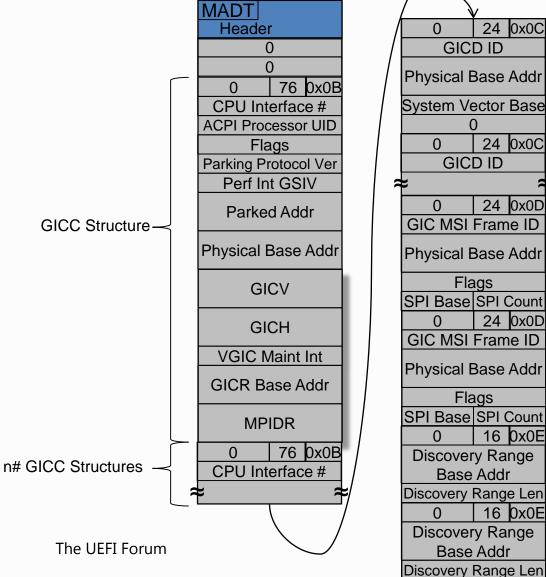
Basic ARM Generic Interrupt Controller

Architecture support

Missing support for alignment with SBSA

New Features in ACPI 5.1: GIC





24 0x0C GICD ID Physical Base Addr System Vector Base 24 0x0C GICD ID 24 0x0D GIC MSI Frame ID Physical Base Addr Flags SPI Base SPI Count 24 0x0D GIC MSI Frame ID Physical Base Addr Flags SPI Base SPI Count 16 0x0E **Discovery Range** Base Addr Discovery Range Len 16 Dx0E **Discovery Range** Base Addr

Updated Generic Interrupt Controller support GIC Support has been extended to cover:

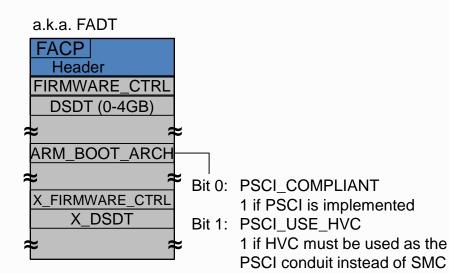
- GICv2 virtualization
- GICv2m (optionally required in SBSA Level 1)
- Partial support for GICv3
 - Redistributors are supported
 - Interrupt Translation Service work in progress
- Improved consistency with "ARM ARM" language

Now called GICC and GICD structures of the MADT

To do: Add ITS support

New Features in ACPI 5.1: PSCI





Support for PSCI

PSCI discoverability is provided by a new ARM Boot Flags field in FADT

MADT provides ways of identifying every core

- Enables the use of PSCI for:
 - Secondary core boot
 - Dynamic addition/removal of cores (hot-plug)
- Creates a path for use in idle management

To do: Use of PSCI in idle management. This will be worked on as part of the more generic idle management support for ARM

Power State Coordination Interface (PSCI) <u>http://infocenter.arm.com/help/topic/com.arm.doc.</u> <u>den0022b/index.html</u>

ACPI 5.0: Generic Timer



Limited support for the Generic Timer Architecture

GTDT described timers that were implemented at the time and cannot describe:

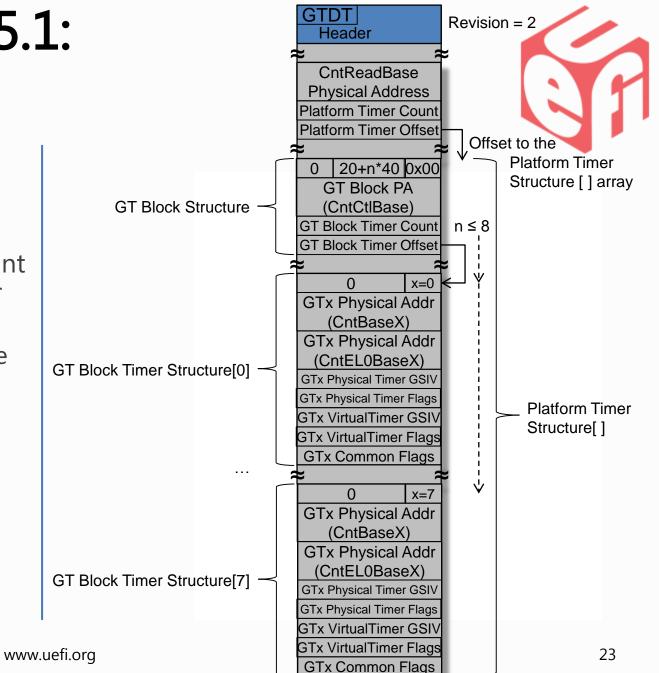
- Always-on per processor timers
- Memory-mapped platform timers
- Platform watchdog timers

Revision = 1

New Features in ACPI 5.1: Generic Timer

Extended support for Generic Timer Architecture

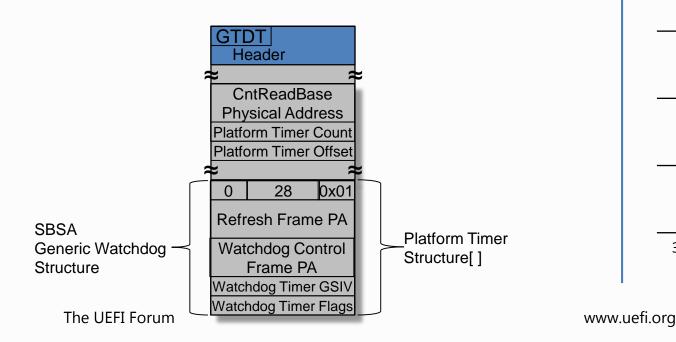
- It is now possible to describe platform memory mapped timers that are compliant with the ARMv7 or ARMv8 Generic Timer Architecture
 - Covered by extension to the GTDT table in the Platform Timer Structure[]
 - Secure or non-secure via GTx Common Flags
 - Always-on Capability via GTx Common Flags
- This is a requirement for SBSA Level 1 systems



New Features in ACPI 5.1: Generic Watchdog Timer

Support for SBSA Level 1 Generic Watchdog Timer

• Covered by extension to the GTDT table in the Platform Timer Structure[]



Watchdog Timer Flags			Reserved ST TIP TIM
i lago		31	3 2 1 0
Bit	Name		Description
0 Timer Int		errupt Mode	Indicates the mode of the timer interrupt
			1: Edge triggered 0: Level Triggered
1	Timer Inte	errupt Priority	Indicates the polarity of the timer interrupt
			1: Active low 0: Active high
2 Secure Tim		mer	Indicates whether the timer is secure or non-secure
			1: Secure 0: Non-secure
31:3	Reserved		Must be zero

New Features in ACPI 5.1: Cache Coherency Attribute (_CCA)



A device identification object specifies whether a device and its descendants support hardware managed cache coherency

_CCA returns

- 0 The device does not have hardware managed cache coherency Software managed to ensure stale or invalid data is not accessed from the caches
- 1 The device has hardware managed cache coherency

Allows platform designers to provide hardware cache coherency support on an asneeded basis for cost and performance reasons, without requiring new drivers to have knowledge of the platform

Provides flexibility in the firmware to indicate to the OS what support is provided in the platform

Optional Features in ACPI 5.1: Device Specific Data (_DSD)



An optional object used to describe device properties to device drivers

_DSD returns a variable-length package of Device Data Descriptor structures UUID and Data Structure tuples

UUIDs may be created by governing bodies (e.g. PCI SIG, UEFI Forum), OEMs or hardware vendors UUID and data structure pairs are published via <u>http://www.uefi.org/acpi</u>

This method will help us to provide more generic solutions in clock control or other bespoke features



Resources

The UEFI Forum

Resources

SCT

- How to contribute: <u>http://tianocore.sourceforge.net/wiki/ArmPkg/HowToContributeSct</u>
- Documentation to build/run/debug SCT: <u>http://tianocore.sourceforge.net/wiki/ArmPkg/Sct</u>
- GitHub source: <u>https://github.com/UEFI/UEFI-SCT/</u>
- UEFI SCT 2.4B ARM+AArch64 for Taipei Plugfest 2014 <u>http://www.uefi.org/sites/default/files/resources/UEFI-SCT-ARM-AARCH64-</u> <u>TaiPeiPlugfest2014.zip</u>

ARM Server Base Boot Requirements (SBBR)

• <u>http://infocenter.arm.com/help/topic/com.arm.doc.den0044a/index.html</u>





Summary

Summary



UEFI provides an OS agnostic boot loader that grows and shrinks depending upon requirements

UEFI Forum specifications written down and peer-reviewed

ARMv8-A AArch64 support for UEFI today

- Tightening of UEFI Specification AArch64 bindings
- ARM pushed and stabilized AArch64 code into the EDK2 repository

Testing UEFI v2.4B SCT underway for Q1 2015 release

ACPI Specification progresses for ARM in 2014

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

presented by





