presented by

Arm SystemReady and the UEFI Firmware Ecosystem

UEFI 2021 Virtual Plugfest

January 26, 2021

Dong Wei (Arm)

Samer El-Haj-Mahmoud (Arm)

Presenters

Dong Wei is an Arm Fellow and is responsible for the Arm SystemReady program and other related standards. He is the Chief Executive of the UEFI Forum and a Board member of PCI-SIG and CXL Consortium.

Samer El-Haj-Mahmoud is a Senior Principal Architect at Arm, working on Arm SystemReady and firmware architecture. He contributes to industry standards such as UEFI, ACPI, CXL, and DMTF Redfish as well as the TianoCore open-source firmware project.

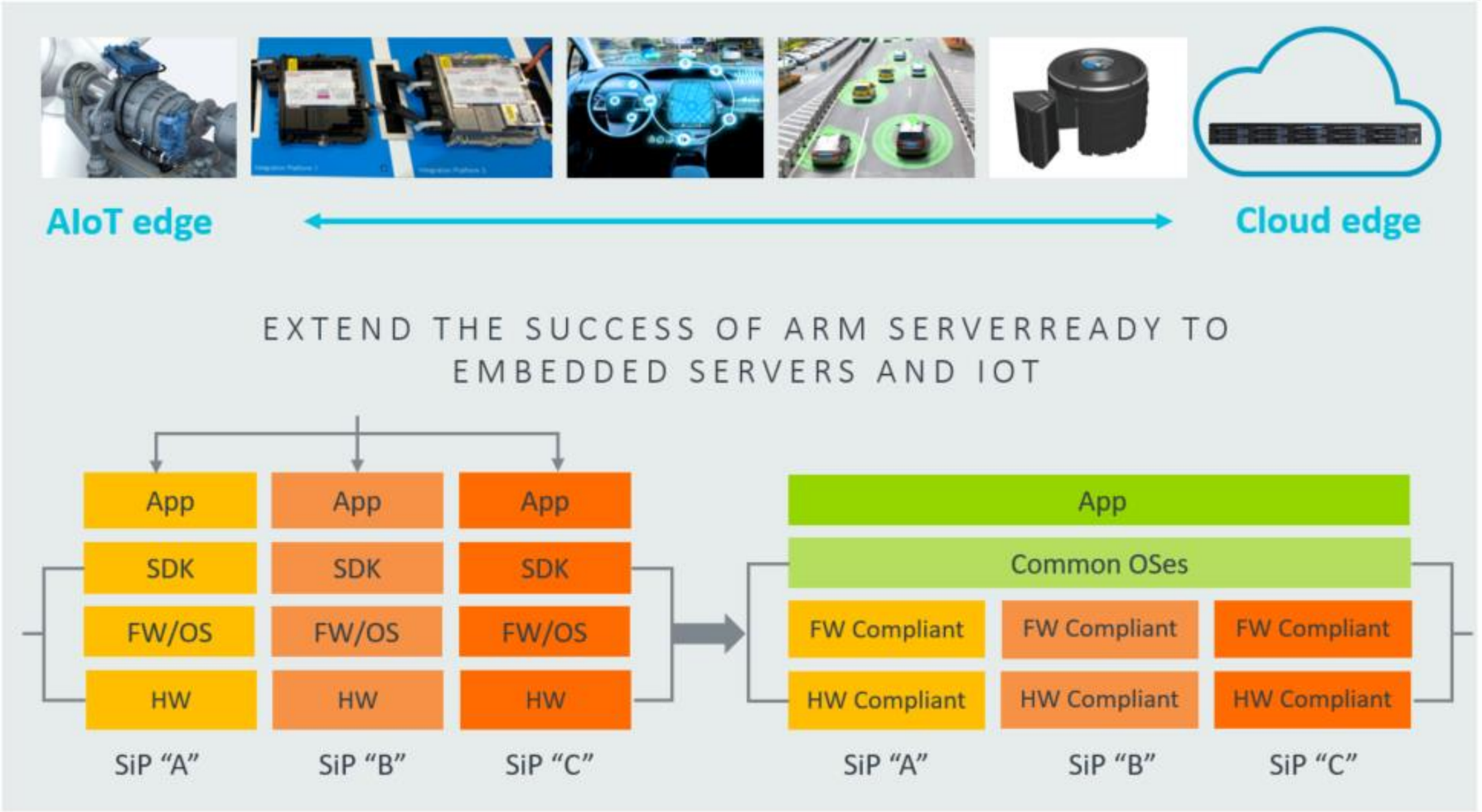
Agenda

- Arm SystemReady
- Arm UEFI Firmware Ecosystem
- Devices Showcase

arm SystemReady

Arm SystemReady

arm
SystemReady



Vision: "Software Can Just Work on Arm-based Devices"

Arm SystemReady

Making all Arm-based infrastructure consistent

Hardware Requirements

***BSA** - Base System Architecture*

- Documents minimal set of CPU and System architecture necessary for an OS to boot and run. Includes aspects such as PCIe integration etc.
- Add segment-specific xBSA hardware requirements (e.g. **SBSA** for servers)

Firmware Requirements

***BBR** – Base Boot Requirements*

- Expand to include common firmware interfaces, but recognize that different software stacks will require different recipes

Certification

***ACS** - Architectural Compliance Suites*

- WIP, Restructured for SystemReady.
- Existing ACS v2.5 used for now, with new versions available in the future

https://developer.arm.com/architectures/system-architectures/arm-systemready

Base Boot Requirements (BBR)

BBR Interfaces

- PSCI, SMCCC (Common)
- UEFI (for SBBR recipe)
- ACPI (for SBBR recipe)
- Exceptions (if needed)
- SMBIOS
- DeviceTree (reference DT Spec)

BBR Recipes Tailored to Various OSes

SBBR

- Same requirements as current SBBR “Servers” specification
- PSCI, SMCCC, UEFI, ACPI, SMBIOS
- More complete OS support

EBBR

- PSCI, SMCCC, UEFI

LBBR

- PSCI, SMCCC, LinuxBoot, ACPI, SMBIOS

EBBR Spec

- UEFI Requirements for embedded systems
- Subset of SBBR. BBR spec refers to EBBR spec as needed (for EBBR recipe)
- Includes reduced UEFI requirements for embedded systems
- Open community spec development https://github.com/ARM-software/ebbr
- Join the discussion on Linaro Boot Architecture mailing list

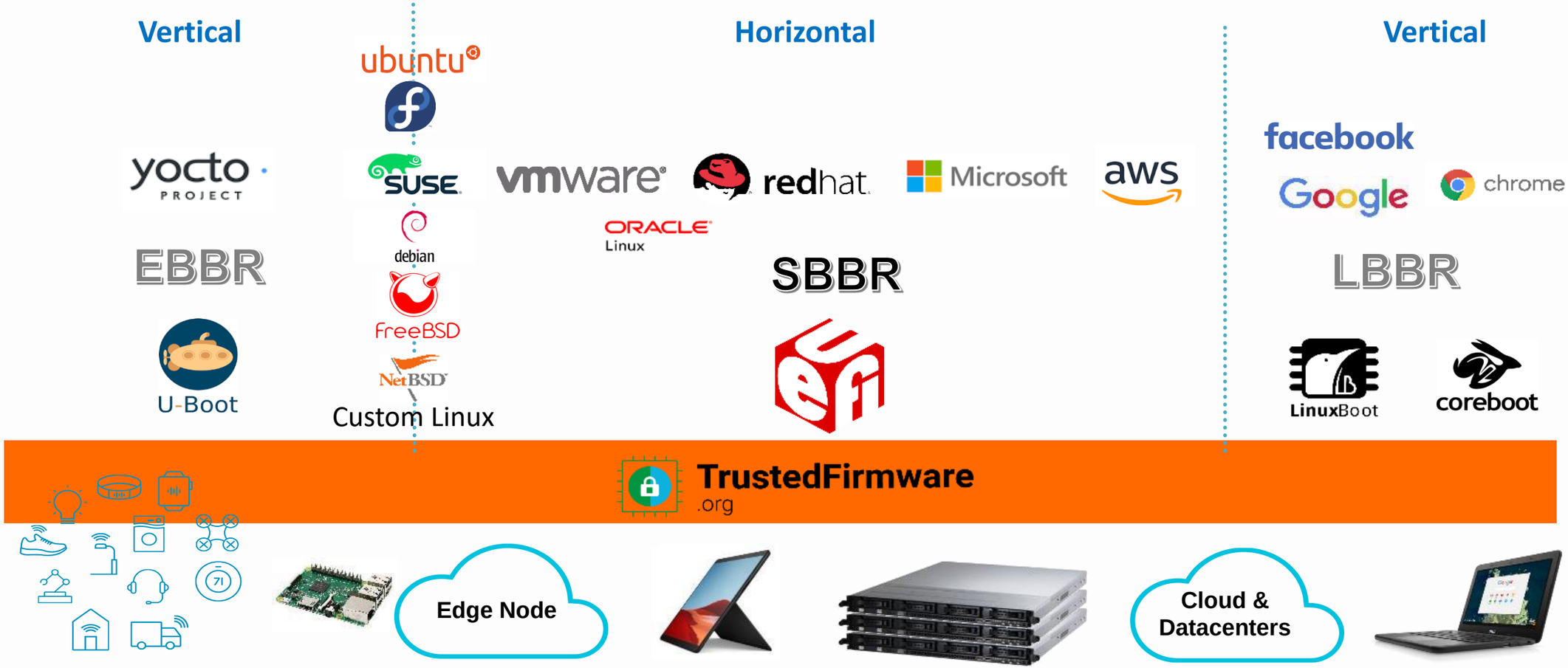
https://developer.arm.com/documentation/den0044/latest

BBSR (Base Boot Security Requirements)

- Additional requirements for security interfaces for UEFI (SBBR or EBBR) based systems
  - UEFI Authenticated Variables
  - UEFI Secure Boot
  - UEFI secure firmware update using Capsule Updates
  - TPMs and Measured Boot
- Additional SystemReady “Security Option” Certification

https://developer.arm.com/documentation/den0107/latest

System Firmware Landscape



arm SystemReady

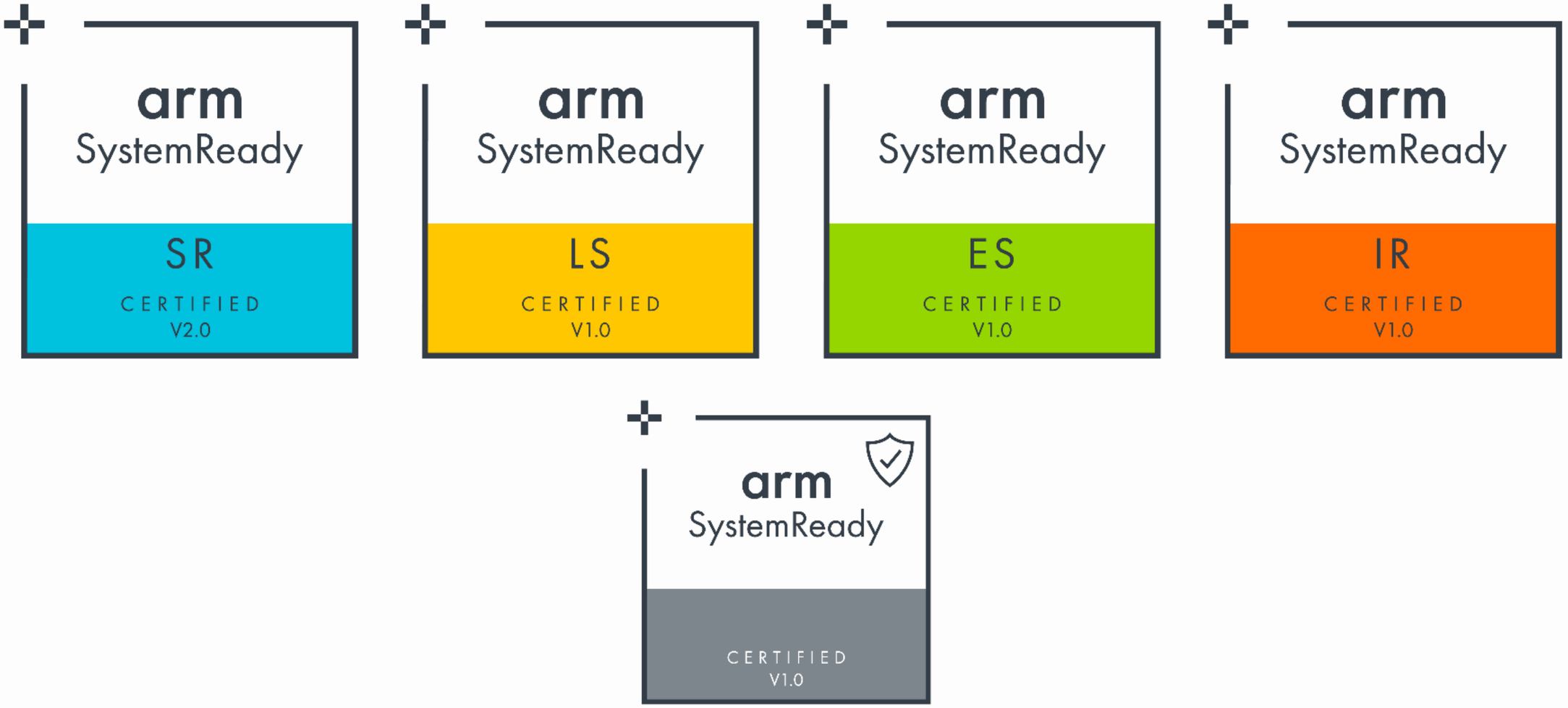
One program, Multiple Bands

Certification	Description	Specifications			
SystemReady SR	ServerReady	BSA	SBSA	BBR(SBBR)	
SystemReady LS	LinuxBoot Server Ready	BSA	SBSA	BBR(LBBR)	
SystemReady ES	Embedded Server Ready	BSA	-	BBR(SBBR)	
SystemReady IR	IOT Ready	BSA	-	BBR(EBBR)	
Security	Security Option	BSA	-	BBR(SBBR or EBBR)	BBSR

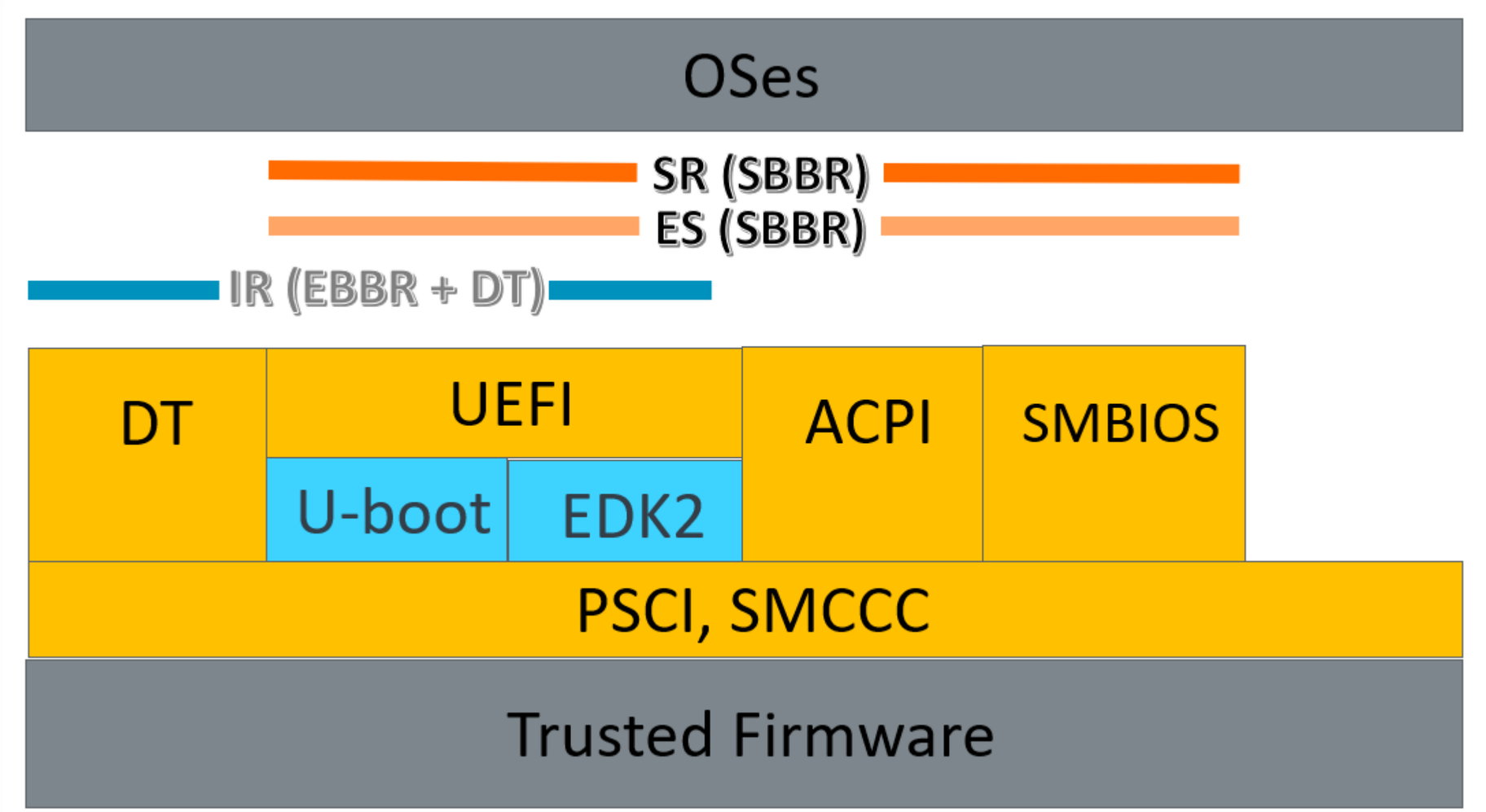
https://developer.arm.com/architectures/system-architectures/arm-systemready

arm SystemReady

One program, Multiple Bands



Firmware Interfaces for SR, ES, IR



arm SystemReady

	LS (LinuxBoot Server Ready)	**IR (IoT Ready)**	**ES (Embedded Server Ready)**	**SR (ServerReady)**
Firmware Spec	ACPI +SMBIOS	UEFI + Devicetree	UEFI + ACPI + SMBIOS	UEFI + ACPI + SMBIOS
Platform Hardware	64bit Arm	32bit/64bit Arm	64bit Arm	64bit Arm
OS/Hypervisor	Linux	Linux, etc.	Generic, off-the-shelf w/ exceptions: RAS, virtualization, etc.	Generic, off-the-shelf
OS Distro *(examples)*	Linux	Fedora, openSUSE, Ubuntu, Debian Under investigation: OpenWRT, QNX, VxWorks, Integrity, Yocto, Wind River, Mentor	Windows IoT Enterprise, VMware ESXi, RHEL, SLES, Ubuntu, CentOS, Fedora, openSUSE, Debian, FreeBSD, NetBSD	VMware ESXi, Windows Client/Server, RHEL, SLES, Ubuntu, CentOS, Fedora, openSUSE, Debian, FreeBSD, NetBSD
Hardware Compliance Levels	**BSA+SBSA** Levels 3 through 6	**BSA** + No BSA requirements for 32-bit + waivers for existing HW initially	**BSA** + waivers for existing HW initially	**BSA+SBSA** Levels 3 through 6
BBR Recipe	**LBBR**	**EBBR**	**SBBR**	**SBBR**
Certification	**Arm SystemReady LS** + System Compatibility List	**Arm SystemReady IR** + System Certification List	**Arm SystemReady ES** + System Certification List	**Arm SystemReady SR** + System Certification List

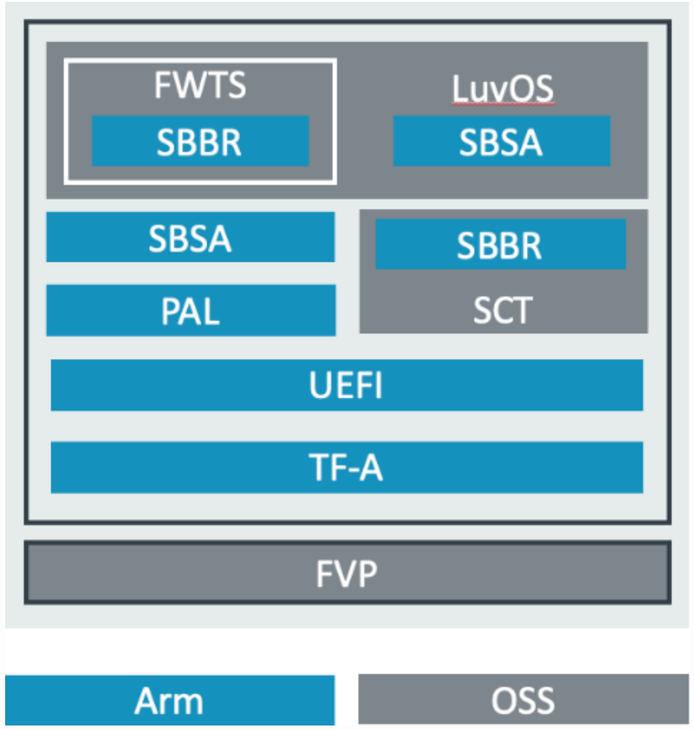
Can support UEFI SecureBoot and Secure Firmware Update via UEFI Capsule Service across (**BBSR**)

Architectural Compliance Suite (ACS)

ACS for SystemReady SR

ACS v3.0 available

Tests for SBBR + SBSA compliance

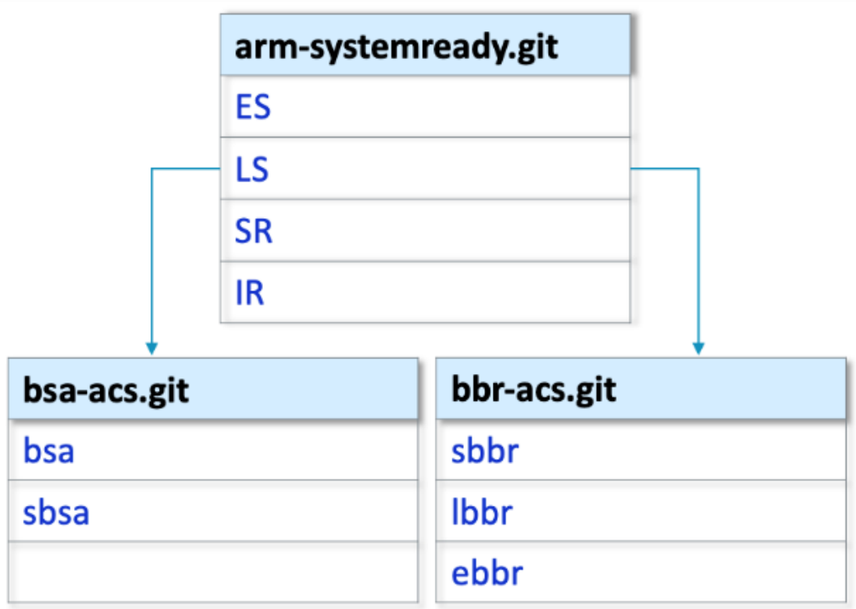


https://github.com/arm-software/arm-enterprise-acs

ACS for SystemReady ES and IR

ACS Development WIP (ETA: Q2 CY2021)

Use ACS v2.5 w/ SBSA Level 3 to certify ES now



https://github.com/ARM-software/arm-systemready

BBSR ACS

- Extend ACS test suites to cover BBSR security requirements
  - **UEFI Authenticated Variables**: Leverage existing SCT and FWTS test cases
  - **UEFI Secure Boot**: New SCT and manual tests to ensure correct behavior of LoadImage() and SetVariable() with PK/KEK/db/dbx/SecureBoot/SetupMode
  - **Capsule Updates**: New manual and automated tests, leveraging UEFI tool CapsuleApp, Linux fwupdmgr, FWTS esrtdump
  - **TPMs and Measured Boot**: Test TCG2 UEFI Protocol (SCT), and Linux TPM2 support (using tpm2-tools, and FWTS tpmevlogdump)

Arm Aarch64 UEFI Driver

- Arm based BBR compliant systems require UEFI drivers to be in UEFI AArch64 native format
- Some ecosystem partners already providing AArch64 binaries
- Call to more to make available for support on Arm SystemReady compliant systems

https://developer.arm.com/architectures/system-architectures/software-standards/uefi-drivers

Arm UEFI Firmware Ecosystem

Arm and TianoCore

- Open-source community project with implementations of UEFI standards: UEFI, PI, ACPI, SMBIOS, UEFI Shell, etc..
  - Including Arm SBBR specification
- Growing Arm community (maintainers, contributors)
  - Complete and partial Arm64 platforms, silicon drivers, libraries, and support code
- https://github.com/tianocore/ : edk2 , edk2-platforms , edk2-non-osi , uefi-sct (test suite)

Arm and U-Boot

- “Universal Bootloader” open-source firmware, with support for multiple architectures (including Arm/Arm64)
  - https://github.com/u-boot/u-boot
- Portable, easy to port/debug. Many (100s) boards up-streamed.
- Suitable for embedded / edge devices (predominantly vertically integrated ecosystem)

U-Boot and UEFI

- U-Boot implements a UEFI layer that follows the EBBR specification, allowing standard OS bootloader (like GRUB) to load and boot a standard OS
- UEFI compliance testing using UEFI SCT (Results) and FWTS (Results) show very good progress towards complete EBBR compliance
  - Most boot and runtime services, some UEFI protocols
  - Support for booting UEFI Shell and Linux standard UEFI boot loaders (Grub, etc..)
- UEFI Secure Boot and secure Capsule Updates has been recently added to U-Boot
- Reference presentation in OSFC 2020 by Heinrich Schuchardt

Arm and LinuxBoot

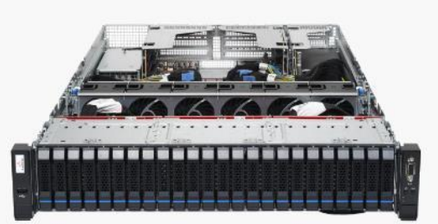
- LinuxBoot is an alternative firmware stack (used by hyperscale datacenters) that relies on the Linux kernel as the Normal World firmware component.
- Re-uses existing Linux drivers code (without the need to write DXE/UEFI drivers)
- On Arm64 systems, LinuxBoot could be loaded directly from TF-A
- https://linuxboot.org/
- https://github.com/linuxboot/linuxboot
- Google/Facebook leading ongoing work to implement UEFI ABI on top of LinuxBoot.
  - Join the discussions on OSFC slack server **#efi-boot-support** channel
  - Current proposal relies on UefiPayloadPkg from EDK2
  - Alternative is to implement UEFI ABI directly in Linux, just like the U-Boot approach

SystemReady Devices Showcase

Ampere Altra Mt Jade

- **Arm SystemReady SR v2.0 certified**
- Ampere Computing Altra Mt Jade Dual Socket Rack Server
- Choice for evaluating benefit of Arm compute in enterprise server roles. Cloud native, high performance scalable CPU
- Firmware options both open-source and commercial
  - UEFI EDK2 (upstreaming patches under review in edk2-devel)
  - OpenBMC FW (upstreaming patches under review)
  - LinuxBoot FW
- UEFI Firmware upstreaming to TianoCore WIP

AMPERE™



arm SystemReady SR CERTIFIED V2.0

https://amperecomputing.com/altra/

Raspberry Pi 4 Model B

- **Arm SystemReady ES v1.0 certified**
- Choice for evaluating benefit of Arm in an IoT, edge gateway, or low-end developer box roles
- Open-source firmware community project (leadership from Arm, VMware, Akeo Consulting, and others in the developer community)
- Opensource community:
  - UEFI project on Github
  - UEFI EDK2 FW (upstream)
  - TF-A FW (upstream)
  - Discord community
- Porting to other flavors (CM4, RPi 400) TBD/WIP
- Reference: UEFI Forum Webinar (by Arm and VMware)

https://rpi4-uefi.dev/

NXP Layerscape LX 2160A RDB

- **Arm SystemReady ES v1.0 certified**
- Choice for evaluating benefit of Arm in mobile edge compute, edge gateway, embedded/edge server, NFV, 5G, switching, …
- UEFI EDK2 FW (upstream)
- UEFI EDK2 FW (NXP repo)
- TF-A FW:
- UEFI Firmware upstreaming to TianoCore WIP

https://www.nxp.com/design/qoriq-developer-resources/layerscape-lx2160a-reference-design-board:LX2160A-RDB

Solidrun HoneyComb LX2K

- Arm SystemReady Certification **In Progress**
- Based on NXP Layerscape LX2160A
- Choice for evaluating benefit of Arm in a Micro-server, Workstation, or Edge gateway role.
- UEFI EDK2 FW
- TF-A FW
- UEFI FW Build script
- Discord community
- UEFI FW upstreaming WIP

SolidRun
Embedded Edge Computing

https://www.solid-run.com/nxp-lx2160a-family/honeycomb-workstation/

NXP LS1046A FRWY / RDB

- Arm SystemReady Certification **In Progress**
- Choice for evaluating benefit of Arm in high performance IoT, edge gateway, enterprise access point, etc…
- UEFI EDK2 FW (upstream)
- UEFI EDK2 FW
- TF-A FW
- UEFI Firmware upstreaming to TianoCore WIP

https://www.nxp.com/design/qoriq-developer-resources/ls1046a-freeway-board:FRWY-LS1046A

SBSA QEMU

- Virtualization environment for Armv8-A, with support for Arm SBSA specifications
  - Available as “sbsa-ref” machine
  - Supports SBSA HW such as GICv3, generic timer, watchdog, etc..
- Choice as an environment for developing firmware and testing operating systems and compliance testing
- Linaro working on completing SBSA and SBBR support and testing compliance with the ACS test suite
- Upstreamed to:
  - QEMU
  - UEFI EDK2 FW
  - TF-A FW
- Testing results: sbsa-acs and UEFI SCT tests

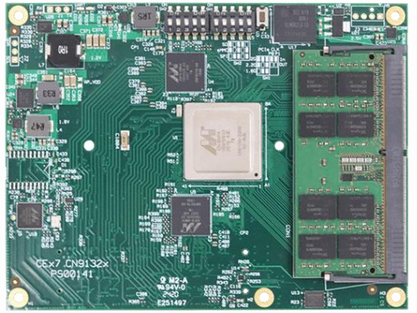
Marvell Octeon TX2 CN913x

- Work done by SemiHalf to for UEFI+ACPI support in EDK2
  - Firmware already available upstream
  - Boots most standard distros (Linux, ESXi, BSDs).
  - Testing with ACS test suites for more complete BSA+SBBR compliance
- EDK2 FW (upstream)
- TF-A FW (upstream)
- Reference presentation in OSFC 2020 by Marcin Wojtas

MARVELL

Semihalf

SolidRun
Embedded Edge Computing



Questions?

More Questions?

Following today's webinar, join the live, interactive WebEx Q&A for the opportunity to chat with the presenter

Visit this link to attend: http://bit.ly/3pjpf0O
Meeting number (access code): 126 003 8932
Meeting password: UEFIForum (83343678 from phones and video systems)

Thanks for attending the UEFI 2021 Virtual Plugfest

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

presented by