System architecture standards from Arm-based servers to PCs

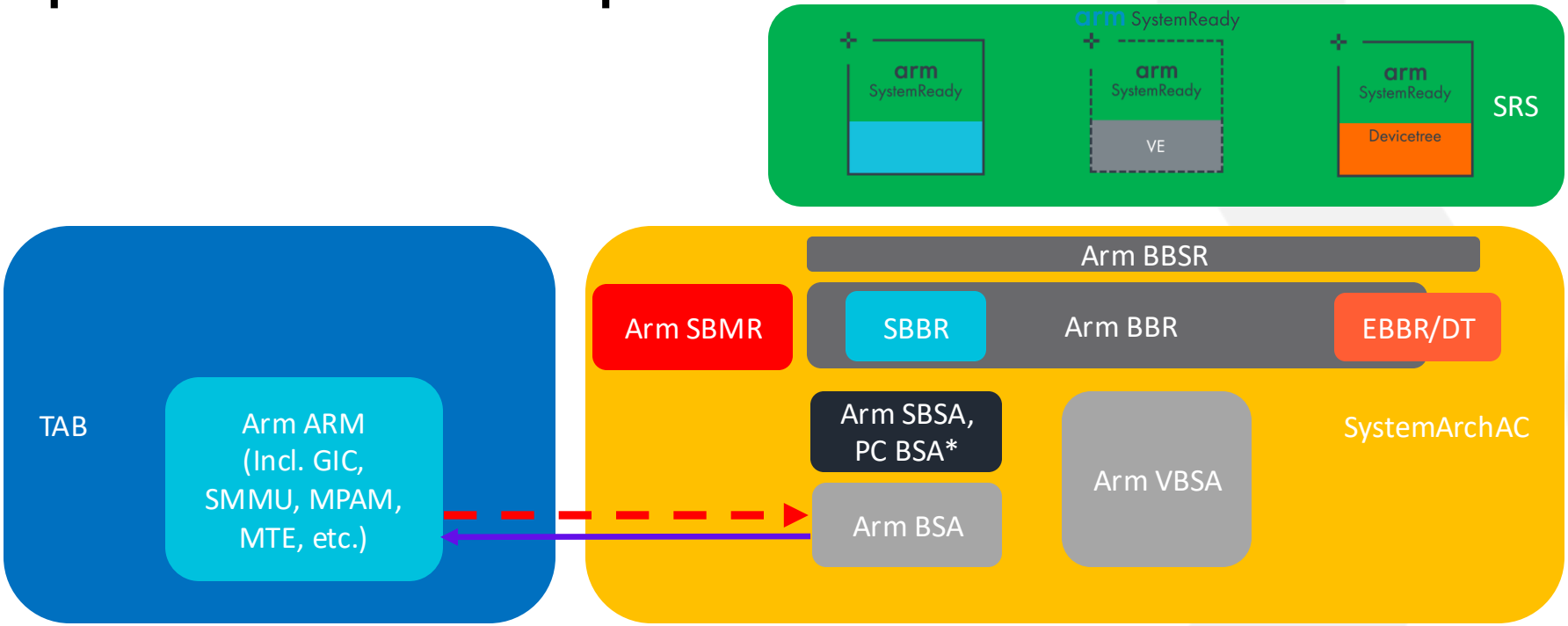
Dong Wei, Arm Fellow

Agenda

1. Arm system architecture
2. Arm System Architecture Advisory Committee (SystemArchAC)
3. Arm system architecture specifications
4. Compliance program
5. System manageability
6. Call to action

Arm system architecture

Specification relationships

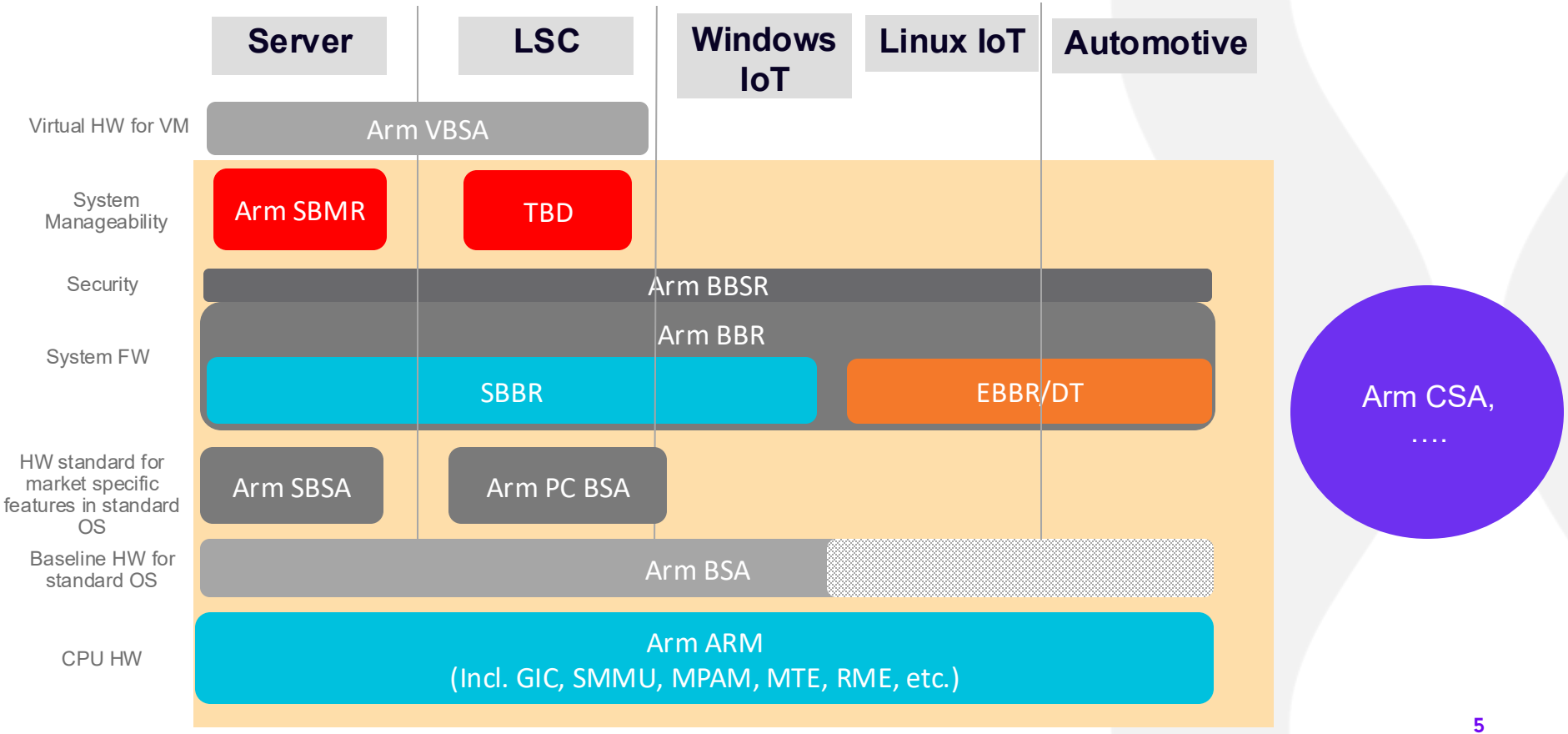


* PC BSA currently is not part of SystemArchAC nor SystemReady

CPU architecture

PE requirements and system architecture requirements for standard OSes

System architecture - market segment view

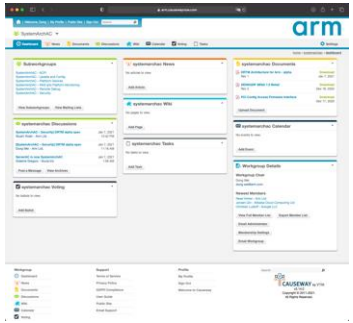


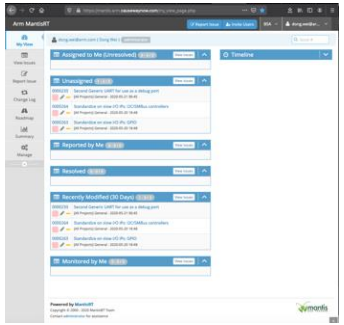
Arm System Architecture Advisory Committee (SystemArchAC)

SystemArchAC

Where BSA/SBSA/VBSA/BBR/BBSR/SBMR Specifications are Developed

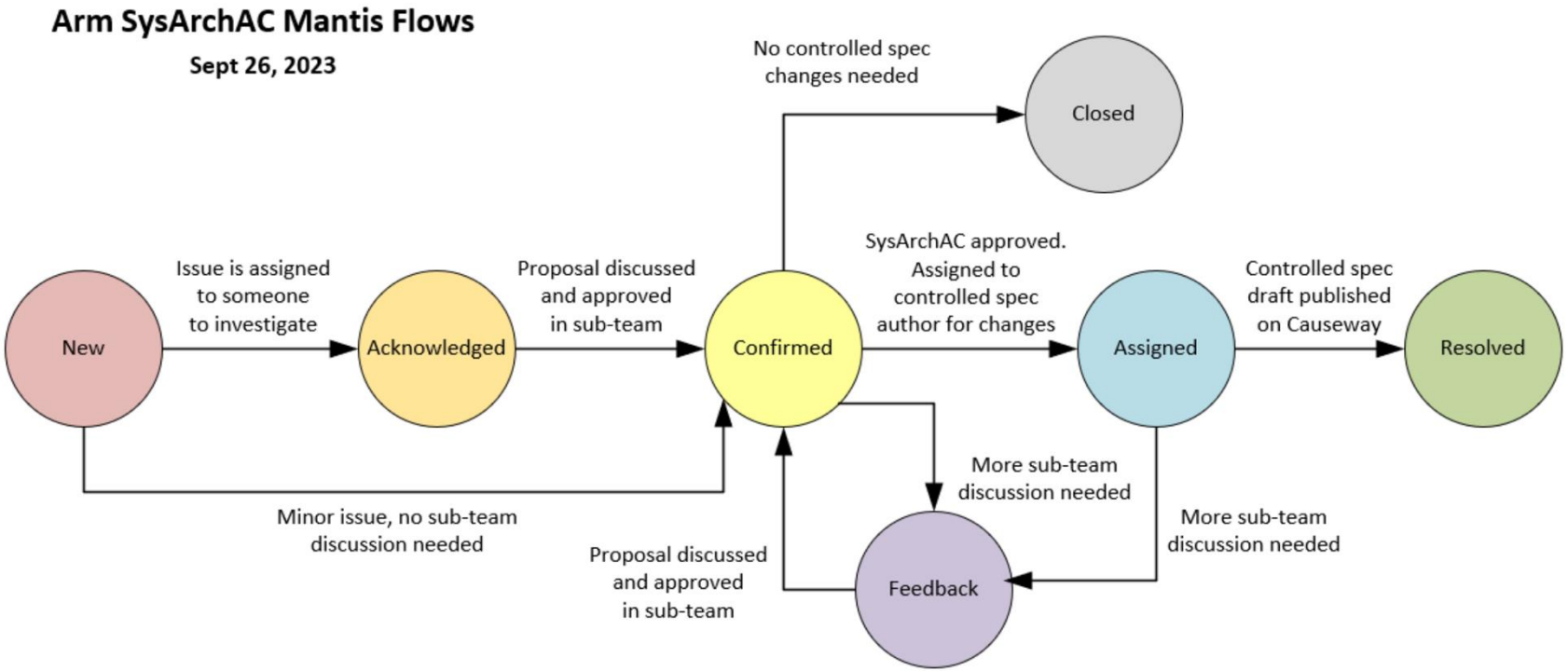
Facility: Causeway/Mantis





- 70+ companies
- Silicon Providers, OS Vendors, IP Providers, OEMs, ODMs, Firmware Vendors, IHVs, ISVs, Hyperscalers
- Standards approach for maximum compatibility and consistency
- Current subteams: ACPI, FF-A, Management, RAS, Remote Debug, SBSA/SBBR, VE, Security, UCIe, Update & Config, IO (PCI SIG members/CXL Promoters/Contributors), Rich IoT Edge

ECR approval flow



Arm system architecture specifications

Key specifications

Hardware baseline (BSA – Base System Architecture)

- Common standard architecture for 64-bit A-profile applicable to all market segment
- Defining a minimal set of CPU and system architecture necessary for a standard OS (not customized).
- BSA v1.1 (Nov 2024)

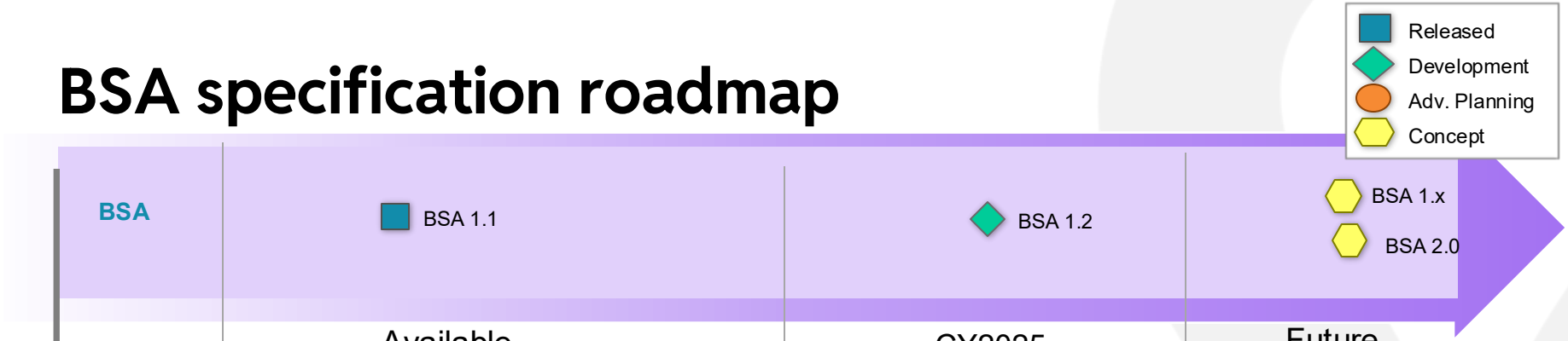
Firmware (BBR – Base Boot Requirements)

- Expands to include common firmware interfaces, but recognizes that different software stacks will require different recipes
- BBR v2.1 (April 2024)
- BBR v2.2 (May 2025)

Virtual environment(VBSA – Virtual BSA)

- Specifies requirements and run-time features that a base virtual environment needs to install, boot and run an operating system
- VBSA v1.0 (Feb 2025)

BSA specification roadmap



Available

BSA 1.1

(Nov 2024)

Errata for BSA 1.0

- Require SVE2 for Armv9
- Recommend PTM
- Remove CBSA reference
- Remove LPI for Timer/WD/UART
- Timer rules clarification
- PAuth errata
- FEAT_LSE errata
- PMU Errata
- GIC related errata
- PCIe related errata
- SMMU related errata
- Update for FEAT_CSV2_3
- SM3 and SM4 crypto as needed
- Heterogenous systems support
- Relax UART to be conditional

"Future Requirements" for BSA

- Require FEAT_LSE
- Recommend FEAT_LRCPC
- Cleanup separation between BSA and SBSA: Move rules in BSA 1.x used only in SBSA L5+ to "BSA Future Requirements"

New Content

Move SBSA Appendix "Support for Secure Firmware" to BSA

CY2025

BSA 1.2

(CY2025)

Errata, as needed

- Approved so far: PCIe (835), (750), (846), Memory (810), (822), SMMU (817)

Future Requirements, as needed

- Breakpoints rule for virtualization (852)
- Potentially move some requirements from SBSA to BSA that are common across PC and servers

Future

BSA 1.x

- Continue releasing Errata and Future Requirements, as needed

BSA 2.0

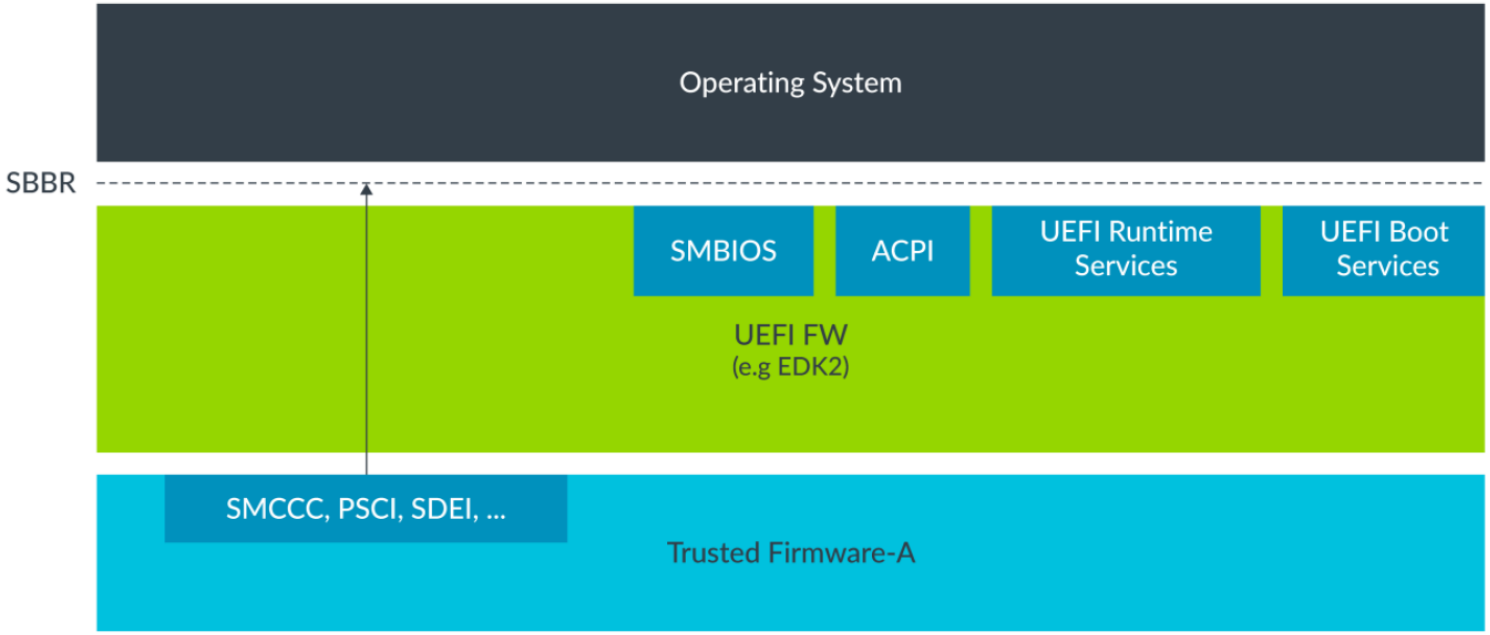
- Based on all the approved Future Requirements from BSA 1.x
- Release when enough new requirements, and ecosystem readiness

BBR specification roadmap

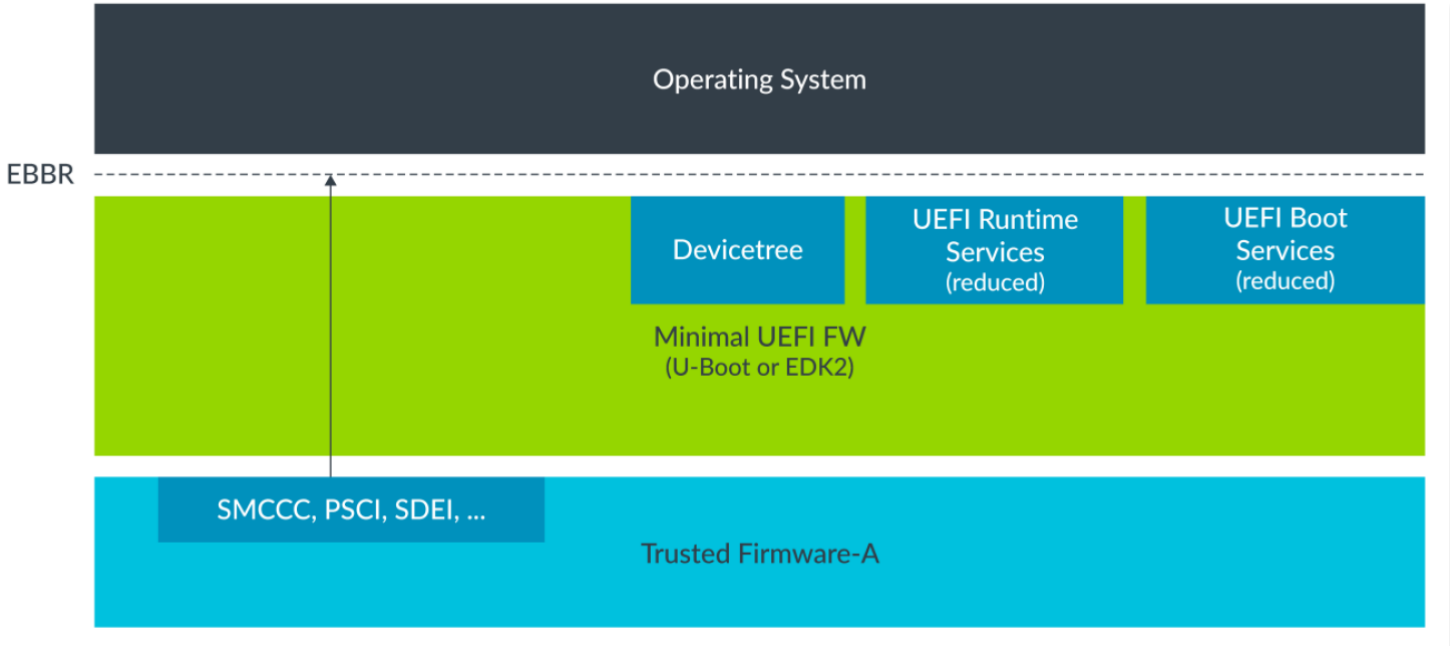
- Released
- Development
- Adv. Planning
- Concept

BBR	BBR 2.1	BBR 2.2	BBR 2.3	BBR 2.4
	Available	CY2025	CY2026	CY2027
	BBR 2.1 (April 2024)	**BBR 2.2** (May 2025) • Errata, as needed • PC BSA v1.0/VBSA v1.0 related firmware requirements	**BBR 2.3** (2026) • Errata, as needed • PC BSA.next related firmware requirements • May merge with BBSR	**BBR 2.4** (2027) • Errata, as needed • PC BSA.next+ related firmware requirements

BBR recipe – SBBR (Servers, PCs, Windows IoT)



BBR recipe - EBBR



BBR related Arm FW specifications

SMCCC & FF-A ABIs

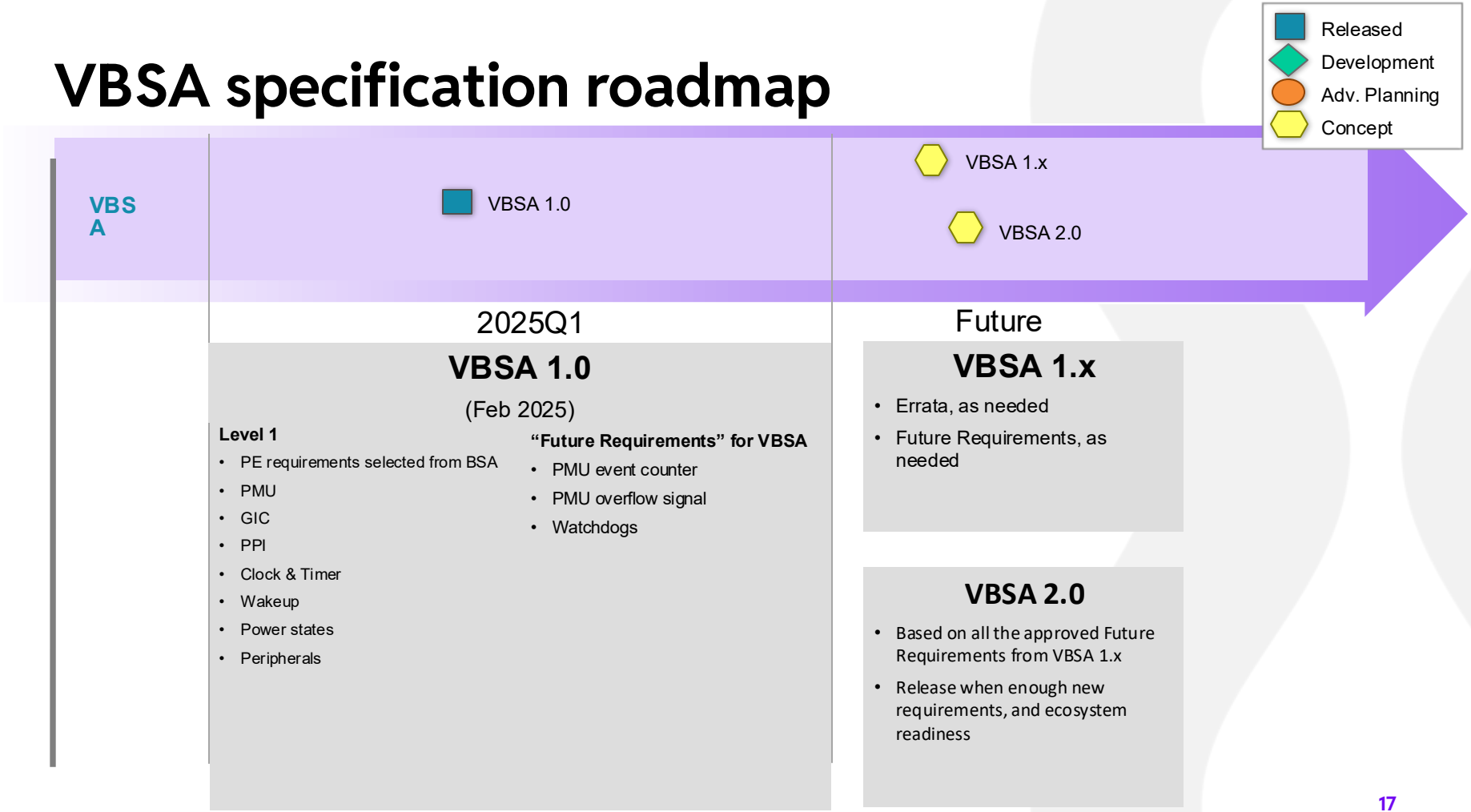
Document	Title	Version	Released	URL
DEN0028	SMC Calling Convention (SMCCC)	1.6 G BET0	Jan 2025	https://developer.arm.com/documentation/den0028/
DEN0022	Power State Coordination Interface (PSCI)	1.3 F.b	Oct 2024	https://developer.arm.com/documentation/den0022/
DEN0054	Software Delegated Exception Interface (SDEI)	C REL	Jan 2023	https://developer.arm.com/documentation/den0054/
DEN0113	DRTM Architecture for Arm	1.1	Oct 2024	https://developer.arm.com/documentation/den0113/
DEN0098	TRNG Firmware Interface	1.0 REL0	Jan 2022	https://developer.arm.com/documentation/den0098/
DEN0118	Secure FW Update ABI	1.0 A EAC1	Oct 2024	https://developer.arm.com/documentation/den0118/
DEN0100	SMC Errata ABI	1.0 EAC1	Oct 2022	https://developer.arm.com/documentation/den0100/
~~DEN0115~~	~~PCIe Config Access ABI~~	~~1.0 Beta 1~~	~~May 2021~~	https://developer.arm.com/documentation/den0115/
DEN0060	Management Mode Interface (MM)	1.0 Issue A	Dec 2016	https://developer.arm.com/documentation/den0060/
DEN0077	Arm Firmware Framework (FF-A)	1.3 ALP1	Nov 2024	https://developer.arm.com/documentation/den0077/
DEN0140	FF-A Memory Management Protocol	1.3 ALP1	Nov 2024	https://developer.arm.com/documentation/den0140/latest/
DEN0143	FF-A SP Lifecycle	1.2 ALP0	Dec 2023	https://developer.arm.com/documentation/den0143/latest/

BBR related Arm FW specifications

ACPI

Document	Title	Version	Released	URL
DEN0049	IO Remapping Table (IORT)	Issue E.f	April 2024	https://developer.arm.com/documentation/den0049/
DEN0085	ACPI for Arm RAS Extensions (AEST)	2.0 BET1	May 2024	https://developer.arm.com/documentation/den0085/
DEN0117	ACPI for CoreSight PMU (APMT)	1.0	Jan 2022	https://developer.arm.com/documentation/den0117/
DEN0065	ACPI for MPAM (MPAM)	3.0 ALP	Dec 2023	https://developer.arm.com/documentation/den0065/
DEN0067	ACPI for CoreSight	1.3	April 2024	https://developer.arm.com/documentation/den0067
DEN0093	ACPI for Arm Components (AGDI)	1.2 BET1	Oct 2024	https://developer.arm.com/documentation/den0093/
DEN0048	ARM Functional Fixed Hardware (FFH)	1.2	Sep 2022	https://developer.arm.com/documentation/den0048/

VBSA specification roadmap



Other specifications

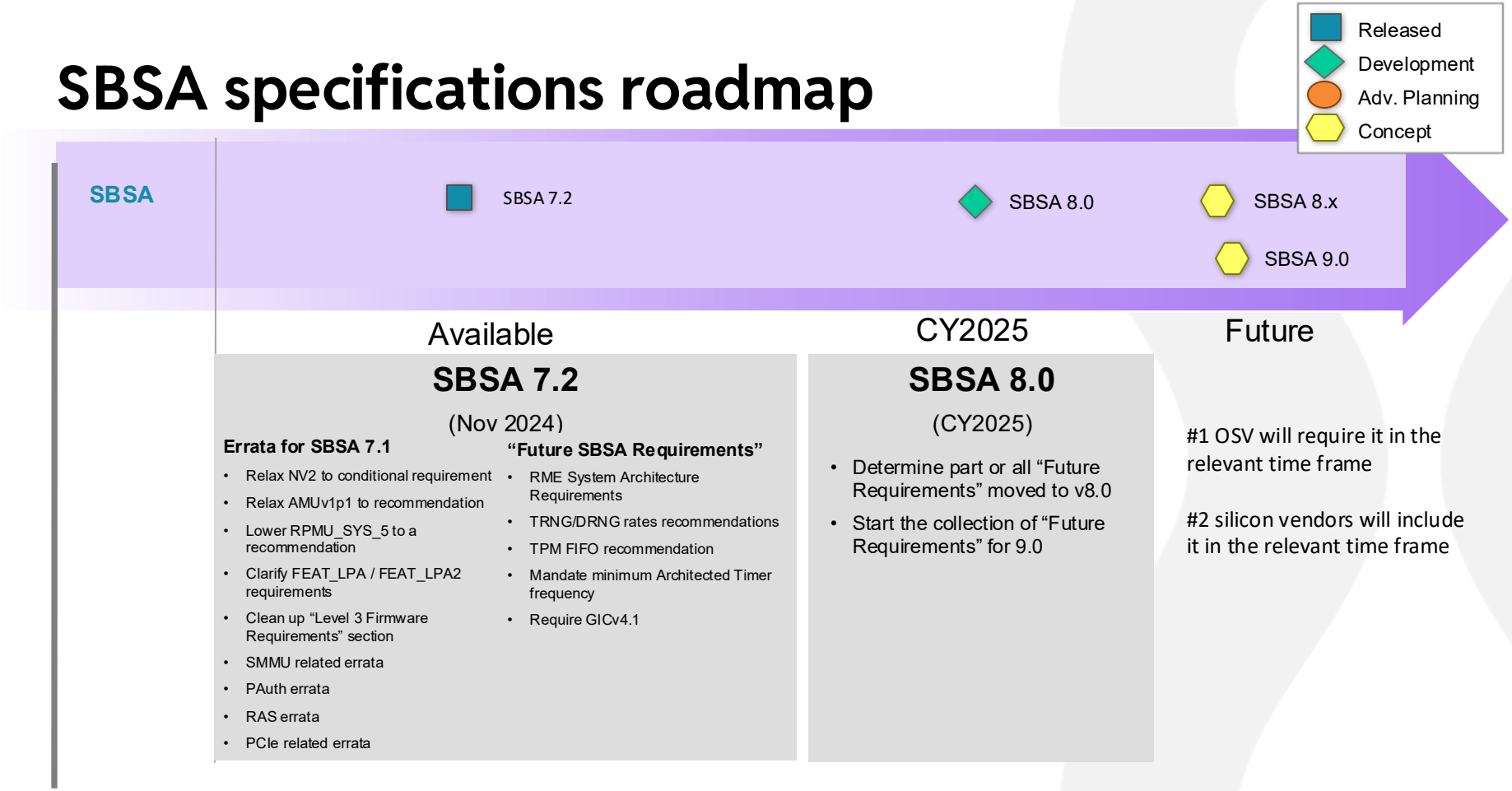
Hardware Supplements (xBSA)

- Provides market segment specific hardware requirements
- Server BSA for server requirements
  - SBSA v7.2 (Nov 2024)
- PC BSA for PC requirements
  - PC BSA v1.0 (Nov 2024)

BBSR (Base Boot Security Requirements)

- Secure Boot and Firmware Update
- V1.3 (March 2024)
- Maintenance Mode
- May merge with BBR in the future

SBSA specifications roadmap



PC BSA specifications roadmap

- Released
- Development
- Adv. Planning
- Concept

PC BSA

PC BSA 1.0	PC BSA.next	PC BSA.next+	PC BSA.next++
Available	CY2025	CY2026	Future

PC BSA 1.0

(Nov 2024)

- Leverage from SBSA L3/4 to form PC BSA L1
- Target device: support minimal power/thermal management features
- Not fully power optimized Windows customer shippable Arm PCs (developer kits, PC kiosks)
- Achieve CPU/Cluster and certain shallow platform states w/o device dependencies
- S0, S4, S5 and D0-3, No S3
- PEP is still expected if more granular and optimized power/thermal management

PC BSA.next

(Nov 2025)

- Leverage from SBSA L5+
- Target device: L1 plus minimal unoptimized S0idle (_SxW, _SxD, etc)
- Somewhat power optimized Windows customer shippable Arm PCs
- GIC and device wake, _RDI support
- Power capping
- Thermal management modifications
- PEP is still expected if more granular and optimized power/thermal management

PC BSA.next+

(Nov 2026)

- Target device: support complete S0idle and wake capabilities
- Standard Windows shippable Arm PC devices
- S0, S0idle, S4, S5 and D0-3 support
- Fine graine runtime device management
- Resource dependencies: _RDI for component idle resource dependencies
- Clock, device performance, device sub-component idle and performance management
- Power capping complete solution
- EC interfaces
- Debug transport power management
- Platform telemetry reporting

#1 OSV will require it in the relevant time frame

#2 silicon vendors will include it in the relevant time frame

Compliance Programs

Compliance check

System Architecture Compliance Suite (ACS)

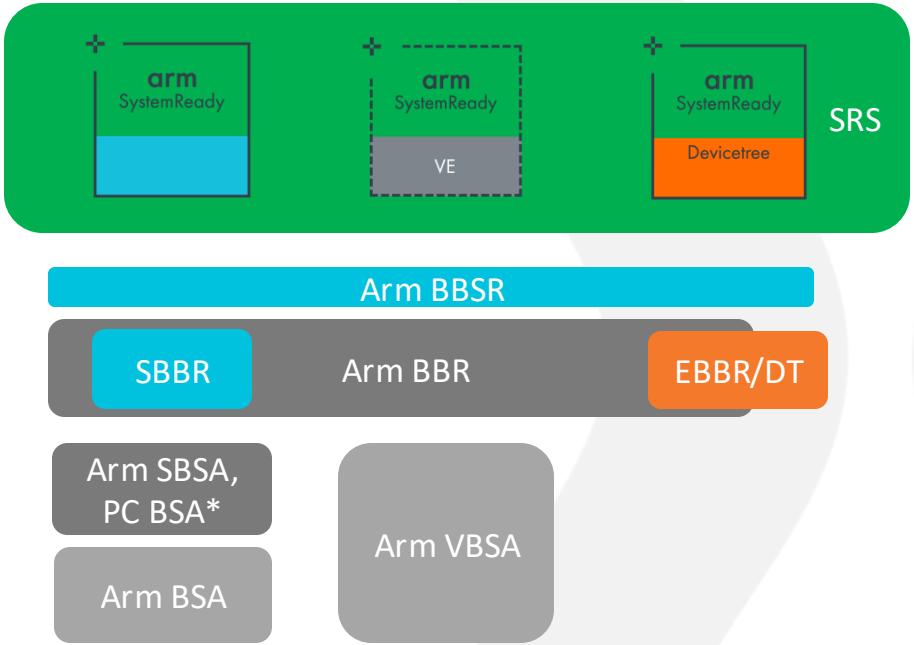
- Verify that the DUT is compliant with the system architecture specifications
- Encourage partner certifications to include the use of ACS
  - e.g. Microsoft WHCP/HLK, Nvidia NVSSVT, Redhat Certified, SUSE Yes Certification

Presilicon Program

- Helps silicon vendors achieve BSA/xBSA compliance prior to taping out
- Provides tools (such as the pre-silicon BSA/xBSA ACS), and, above all, a framework with specific steps for silicon vendors to take to become compliant

arm SystemReady

- Moving from Certification to Compliance
  - No longer accept new certification request
  - Certification ends on June 30, 2025
- Certification
  - Arm tests, reviews logs and approves
  - Arm needs access to the hardware (can be remotely)
- Compliance
  - Vendor tests, reviews logs and self-declare compliance
  - Arm can selectively collaborate on "pathfinding" projects: new SoC's CRB only



* PC BSA currently is not part of SystemArchAC nor SystemReady

Arm SystemReady Supporters

ISVs

Canonical, Microsoft, ORACLE, Parallels (Enabled by Alludo), Red Hat, SUSE, vmware

SiPs

AMPERE, ASPEED, BROADCOM, CIX, FUJITSU, MARVELL, MEDIATEK, nuvoTon, NVIDIA, NXP, Qualcomm, RENESAS, Rockchip 瑞芯微电子, SANECHIPS, SIPEARL (The Silicon Pearl), socionext (for better quality of experience), ST, AMD XILINX

CSPs

Alibaba Cloud, aws, Baidu 百度, Google Cloud, Meta, Microsoft Azure, ORACLE CLOUD Infrastructure

OEMs/ODMs

AAEON (an ASUS company), ADLINK TECHNOLOGY INC., ADVANTECH (Enabling an Intelligent Planet), AMD XILINX, ARDUINO, ASRock Rack, ASUS, ASUS IoT, AVANTEK COMPUTER, COMPAL, Compulab, congatec, CyberTAN, DIGI, DELL Technologies, EUROTECH (Imagine. Build. Succeed.), Foxconn Industrial Internet, GIGA COMPUTING, Google, HAWKEYE TECH, Hewlett Packard Enterprise, 华辰连科 HuachenLink, inspur, kontron (S&T Group), Lanner, Lenovo, 联泰集群 LTHPC, NEXCOM, NORCO, PEGATRON, PHYTEC, QCT, radxa, Raspberry Pi, Scalys, SECO, 天固信安 SKYSOLIDISS, SolidRun (Embedded Edge Computing), SUPERMICRO, Rxi 日海飞信, Toradex (Swiss. Embedded. Computing.), Variscite, WINSYSTEMS, wiwynn, Xsight

EDAs

cadence, SYNOPSYS

IFVs

9ELEMENTS Cyber Security, ami, BYOSOFT 百数软件, insyde, phoenix, PureSoftware

Communities

AlmaLinux, Linaro, OpenAnolis 龙蜥社区, OPEN Compute Project, OpenGCC, Rocky Linux, yocto PROJECT PARTICIPANT

Test Labs

GlobalLogic (A Hitachi Group Company), iol (University of New Hampshire InterOperability Laboratory), ITRI (Industrial Technology Research Institute)

System manageability

Arm server management standard

- Server Base Manageability Requirements (SBMR) https://developer.arm.com/documentation/den0069/
- HW / FW requirements for system management of Arm servers
- SBMR 2.1 (Nov 2024)
- Co-developed with the Arm ecosystem partners in the SystemArchAC (similar to BSA, SBSA, SBBR, BBSR , ..)
- Builds on top of prevalent management industry standards:
  - DMTF (Redfish, MCTP, PLDM, SPDM)
  - OCP (HW Mgmt, HW Mgmt Module / DC-SCM, HW Fault Mgmt)
  - IPMI (for minimum legacy compatibility)

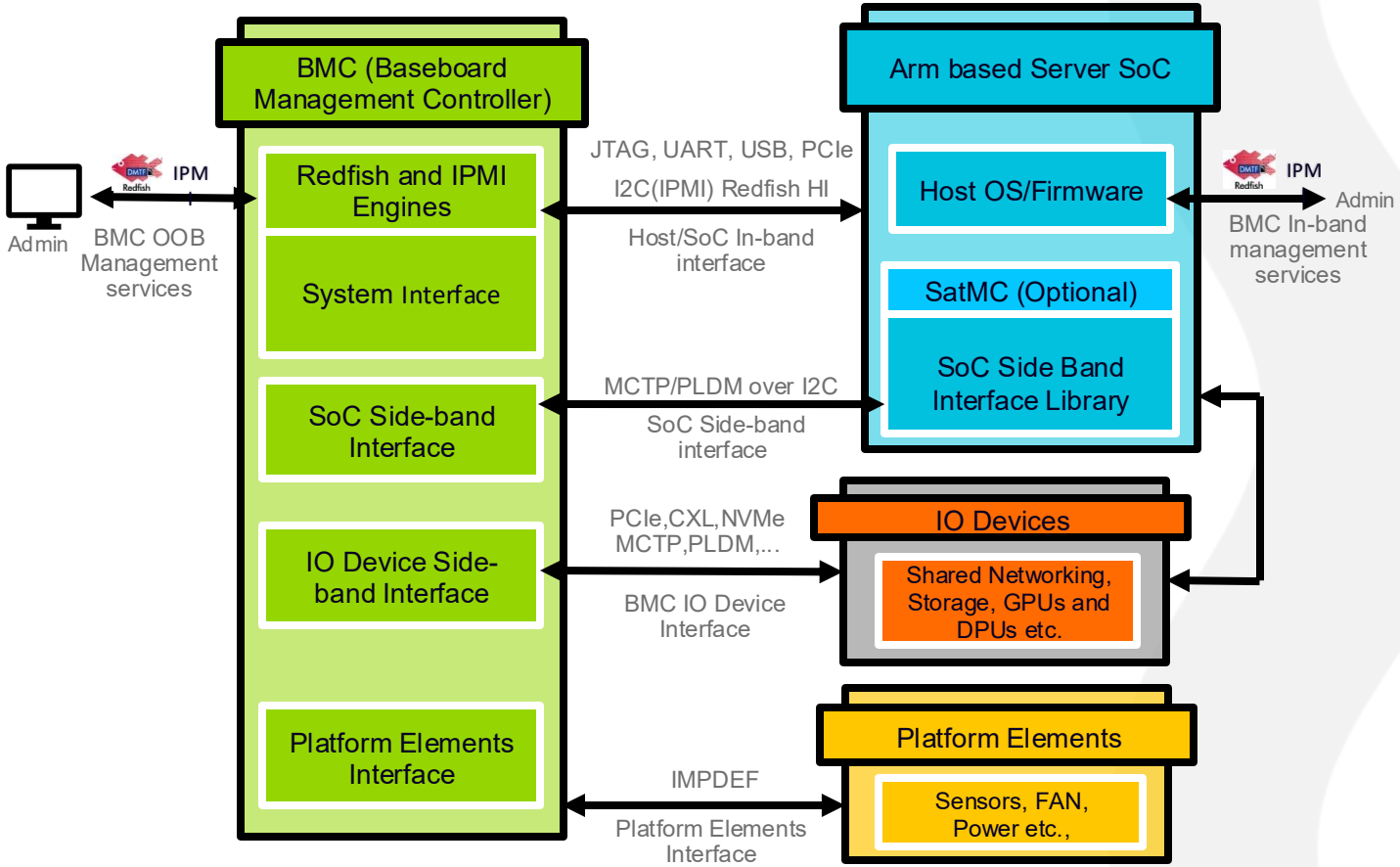
- **SBMR Goal**: *Help guide the Arm server designers to provide common manageability functions that match the industry expectations and capabilities and increase the interoperability in the Arm infrastructure ecosystem.*

Redfish

- IPMI -
Intelligent Platform Management Interface Specification Second Generation
v2.0

HW MANAGEMENT

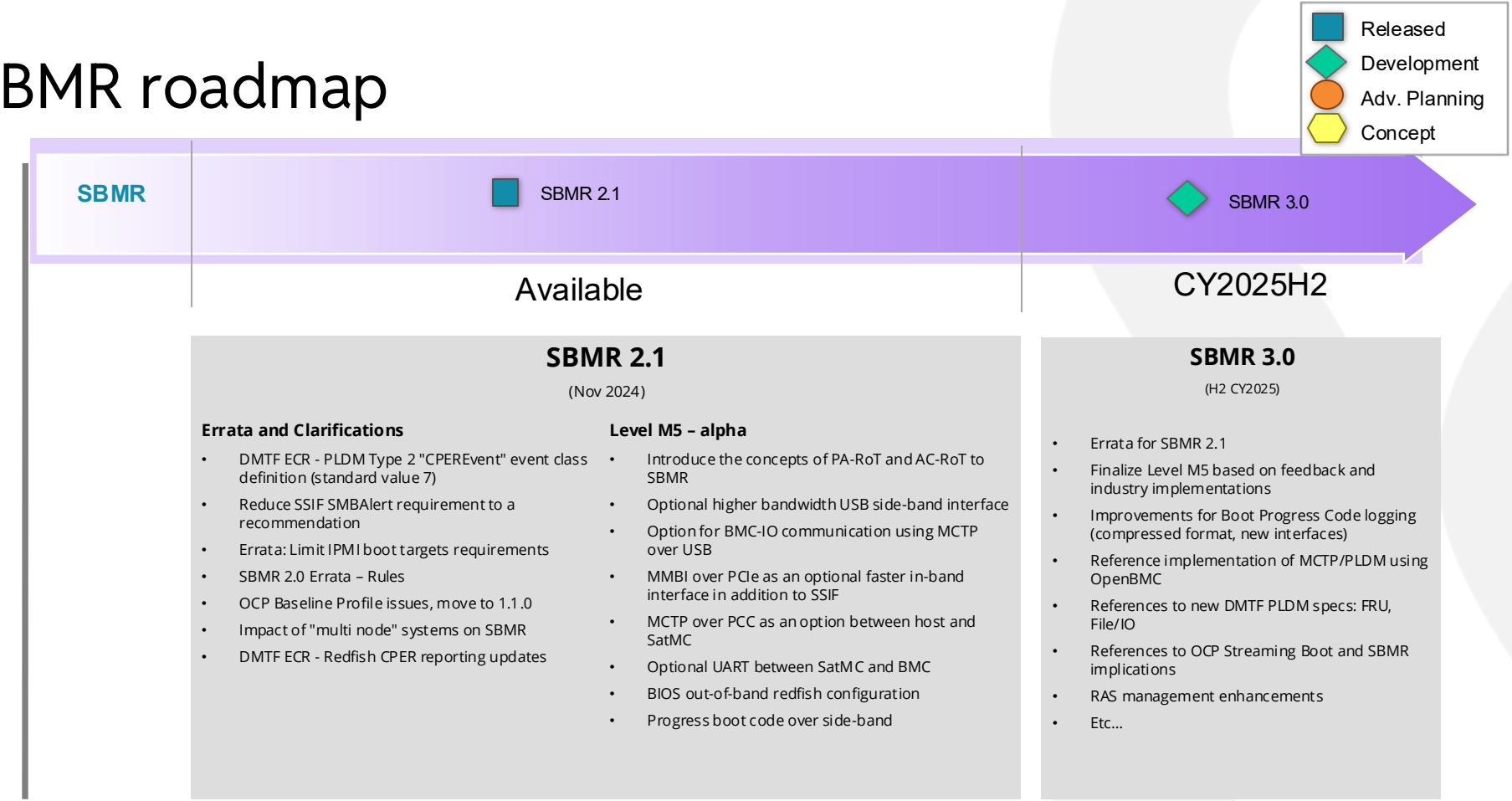
SBMR architecture



SBMR compliance levels

	Level	Out-of-band Interface	SoC Side-band Interface	Host/SoC In-band Interface	BMC-IO Device Interface	BMC Platform Element Interface	Host to SatMC Interface
SBMR 1.0/1.1	~~M0~~	~~IMPLEMENTATION DEFINED~~	~~IMPLEMENTATION DEFINED~~	~~IMPLEMENTATION DEFINED~~	~~IMPLEMENTATION DEFINED~~	~~IMPLEMENTATION DEFINED~~	~~IMPLEMENTATION DEFINED~~
	M1	**Required:** IPMI	IMPLEMENTATION DEFINED	**Required:** IPMI SSIF	IMPLEMENTATION DEFINED	IMPLEMENTATION DEFINED	IMPLEMENTATION DEFINED
	M2/ M2.1	**Required:** Redfish **and** IPMI	IMPLEMENTATION DEFINED	**Required:** IPMI SSIF, **and** Redfish Host Interface	**Conditional Requirement:** NC-SI	IMPLEMENTATION DEFINED	IMPLEMENTATION DEFINED
SBMR 2.0	**M3**	**Required**: Redfish	**Required:** MCTP/PLDM over I2C/SMBus or a higher bandwidth interface	**Required:** IPMI SSIF and Redfish Host Interface	**Conditional Requirement:** NC-SI **Recommended:** MCTP/PLDM for PCIe devices, and NVMe-MI over MCTP, using I2C/SMBus or a higher bandwidth interface.	IMPLEMENTATION DEFINED. Refer to OCP and IPMI specs for guidance	IMPLEMENTATION DEFINED
	M4	**Required:** Redfish	**Required**: MCTP/PLDM over I3C	**Required**: IPMI SSIF and Redfish Host Interface	**Conditional Requirement:** NC-SI **Conditional Requirement:** MCTP/PLDM for PCIe devices, and NVMe-MI over MCTP, using I3C or PCIe VDM, with I2C as fallback **Recommended**: CXL FM and CCI over MCTP for CXL devices, using I2C or PCIe VDM, with I2C as fallback	IMPLEMENTATION DEFINED. Refer to OCP and IPMI specs for guidance **Recommended:** PLDM/MCTP	IMPLEMENTATION DEFINED
SBMR 2.1	**M5a (WIP)**	**Required:** Redfish	**Required**: MCTP/PLDM over I3C, USB, or PCIe VDM, with I2C as fallback	**Required**: IPMI SSIF and Redfish Host Interface **Recommended**: MCTP Host Interface over MMBI	**Conditional Requirement:** NC-SI **Conditional Requirement:** MCTP/PLDM for PCIe devices, and NVMe-MI over MCTP, using I3C, USB or PCIe VDM, with I2C as fallback **Recommended**: CXL FM and CCI over MCTP for CXL devices, using I3C, USB or PCIe VDM, with I2C as fallback	IMPLEMENTATION DEFINED. Refer to OCP and IPMI specs for guidance **Recommended:** PLDM/MCTP	MCTP/PLDM over PCC

SBMR roadmap



SBMR 2.1

(Nov 2024)

Errata and Clarifications

- DMTF ECR - PLDM Type 2 "CPEREvent" event class definition (standard value 7)
- Reduce SSIF SMBAlert requirement to a recommendation
- Errata: Limit IPMI boot targets requirements
- SBMR 2.0 Errata – Rules
- OCP Baseline Profile issues, move to 1.1.0
- Impact of "multi node" systems on SBMR
- DMTF ECR - Redfish CPER reporting updates

Level M5 – alpha

- Introduce the concepts of PA-RoT and AC-RoT to SBMR
- Optional higher bandwidth USB side-band interface
- Option for BMC-IO communication using MCTP over USB
- MMBI over PCIe as an optional faster in-band interface in addition to SSIF
- MCTP over PCC as an option between host and SatMC
- Optional UART between SatMC and BMC
- BIOS out-of-band redfish configuration
- Progress boot code over side-band

SBMR 3.0

(H2 CY2025)

- Errata for SBMR 2.1
- Finalize Level M5 based on feedback and industry implementations
- Improvements for Boot Progress Code logging (compressed format, new interfaces)
- Reference implementation of MCTP/PLDM using OpenBMC
- References to new DMTF PLDM specs: FRU, File/IO
- References to OCP Streaming Boot and SBMR implications
- RAS management enhancements
- Etc…

Manageability Compliance (SBMR-ACS)

- New open-source test suite for SBMR Compliance
  - https://github.com/ARM-software/sbmr-acs
- Automated HW Management compliance testing
  - Based on openbmc-test-automation and robot framework
  - Leverage other open-source tools (redfish-service-validator, redfish-interop-validator, redfish-finder , …)
  - Applies to any Arm server implementation (OpenBMC or other FW)
  - In-band (IB) and out-of-band (OOB)
  - Redfish, Redfish Host Interface, IPMI-over-LAN, IPMI Host Interface, USB/PCIe, KVM, UART (console redirection), …
  - Including compliance testing for OCP HW Management Profiles
- **Planned for contribution to OCP GitHub**
- Ongoing collaborating with Arm server partners to verify their implementations

Commercial Laptop Remote Management

Generally found on business or commercial laptops:

- In-band
  - Microsoft Intune
- Out-of-Band (OOB)
  - Option 0: No OOB remote management (same as consumer laptops)
  - Option 1: Keep this proprietary
  - Option 2: Standards-based approach
    - DMTF DASH?
    - Redfish?
    - PC BMR?
    - May need collaboration with NIC vendors

Call to action

Call to action

1. Join SystemArchAC to review and contribute to BSA/SBSA/BBR/BBSR/SBMR development
2. Review PC BSA (use page 10 links to provide feedback)
3. Identify areas for future collaborations

Thank You!