Designing Standards Compliant Servers with Arm SystemReady and NVIDIA Grace

Scaling Innovation Through Collaboration

OCP GLOBAL SUMMIT

OCTOBER 17-19, 2023
SAN JOSE, CA

Server

SERVER

Designing Standards Compliant Servers with Arm SystemReady and NVIDIA Grace

Samer El-Haj Mahmoud, Distinguished Engineer, Arm

James Bodner, Senior Manager Data Center Firmware, NVIDIA

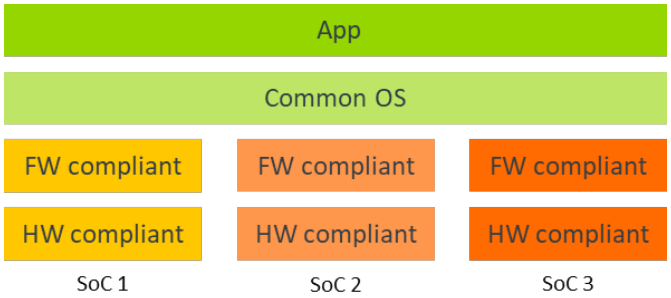
Tim Lewis, CTO, Insyde

OPEN PLATINUM™

Arm SystemReady

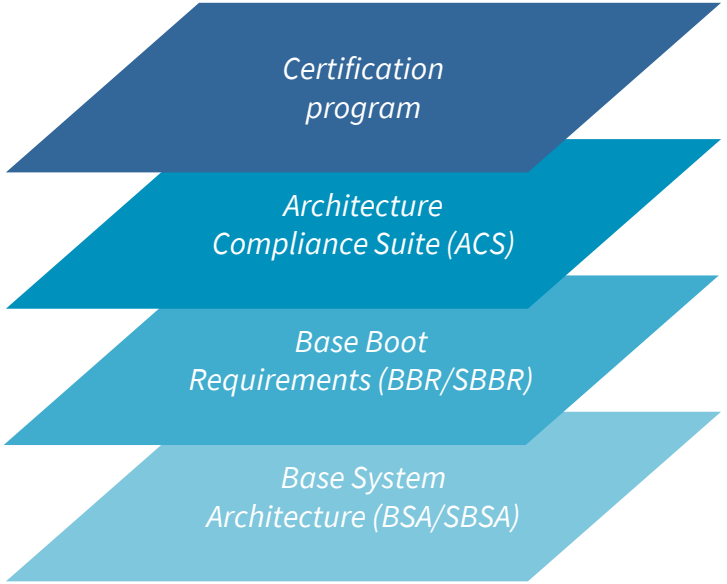
Edge ⟷ Cloud

Vision: “Software Just Works seamlessly across a vibrant, diverse ecosystem of hardware”



Common components like OS, hypervisor, and middleware that just work
Partners can focus on innovating & deploying differentiating layers

arm SystemReady



Specifications enable hardware and firmware compatibility
Certification provides the evidence and confidence

Arm SystemReady Supporters

ISVs

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

SiPs

AMPERE., BROADCOM, CIX, FUJITSU, MARVELL, MEDIATEK, nuvoTon, NVIDIA, NXP, RENESAS, Rockchip 瑞芯微电子, SIPEARL The Silicon Pearl, socionext, AMD XILINX

Hyperscale Cloud Service Providers

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

OEMs/ODMs

AAEON an ASUS company, ADLINK TECHNOLOGY INC., ADVANTECH Enabling an Intelligent Planet, AMD XILINX, ARDUINO, ASUS IoT, AVANTEK COMPUTER, Compulab, congatec, CyberTAN, DIGI, 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, LTHPC 联泰集群, NEXCOM, NORCO, PEGATRON, PHYTEC, radxa, Raspberry Pi, Scalys, SECO, SKYSOLIDISS 天固信安, SolidRun Embedded Edge Computing, SUPERMICRO, Toradex Swiss. Embedded. Computing., Variscite, WINSYSTEMS, wiwynn

EDAs

cadence, SYNOPSYS

IFVs

9ELEMENTS Cyber Security, ami, BYOSOFT, insyde, phoenix technologies, PureSoftware, Semihalf

Communities

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

Test Labs

GlobalLogic A Hitachi Group Company, iol University of New Hampshire InterOperability Laboratory

arm SystemReady

118

Published SystemReady certifications

Software Just Works on Arm

First OCP Experience Center in North America – Hosted by Arm

Broad HW and SW Availability

The experience center supports a variety of silicon from multiple OEM/ODMs. The systems can be tested for compatibility with software offered from various ISVs and OSS developers.

Simple Certification Process

The experience center accelerates datacenter, cloud, and telco deployment-ready hardware by providing easy access to documentation, processes, and systems availability for the Arm ecosystem and OCP Community.

Open Collaboration

Arm and OCP strongly believe in the power of openness. The new experience center is an important opportunity for us to empower vendors to build and deploy compute infrastructure in an open collaborative approach.

Frictionless Developer Experience

Arm has the most fully featured, accessible, and robust development environment for cloud-to-edge developers. The experience center brings a similar environment for the OCP Community.

arm SystemReady

OCP Experience Center
Bedminster, NJ, USA

OPEN Compute Project
SOLUTION PROVIDER®

OPEN ACCEPTED™

OPEN INSPIRED™

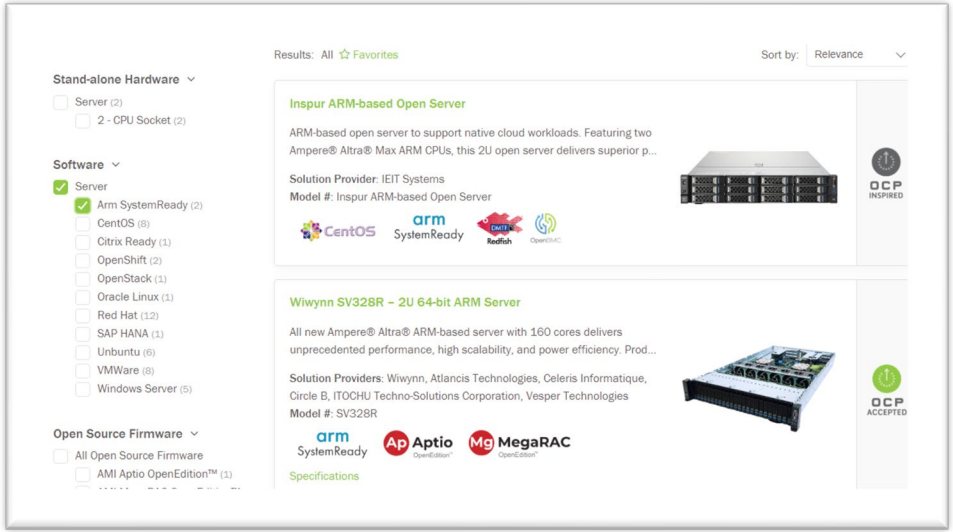
- Collaborate with us: ocp-marketplace@arm.com
- https://www.arm.com/architecture/system-architectures/systemready-certification-program/ocp-experience-center

SystemReady provides “just works” for OCP Accepted™ Arm-based Servers

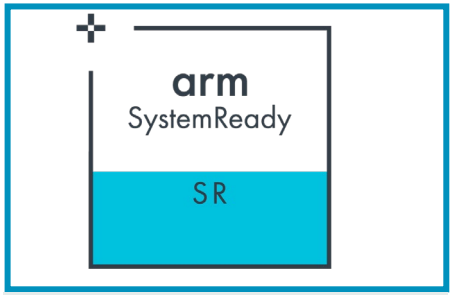
arm SystemReady

OPEN ACCEPTED™

- Arm-based servers are primarily designed for the hyperscalers, data centers, and telcos, aligned with the OCP target market
- Arm SystemReady program provides the user experience of software just works, and ensures higher quality of the Arm-based servers that are OCP Accepted™
- Arm servers submitted to be OCP Accepted™ are now **required** to obtain SystemReady logo first.
  - 2022 OCP Accepted™ Supplier Checklist
  - https://www.opencompute.org/products

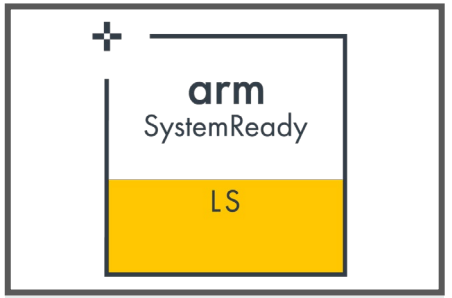


Arm SystemReady for servers



"Just Works" on **server or workstation** Arm SoCs

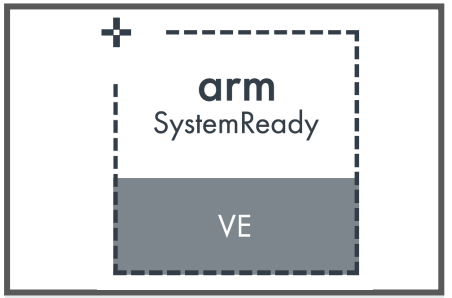
- For the Windows, VMware, Linux, and BSD ecosystem
- Supports existing OSes to run on new hardware and vice versa



"Just Works" for **Linux** on **server** Arm SoCs

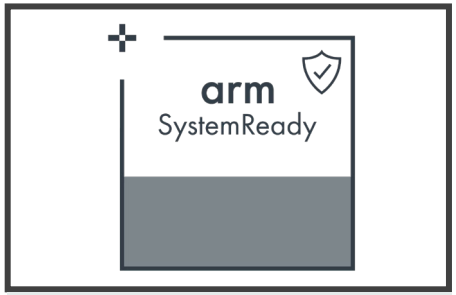
- For hyperscalers' targeting LinuxBoot firmware

Required for OCP Accepted™ servers



"Just Works" for **virtual environments**

- For cloud instances
- For virtual platforms



Security Interface Extension (SIE)

- Optional extension certification for UEFI SecureBoot, TPM, and secure FW updates.
- Recommended for servers. May become required in the future.

Arm Servers Standards

Hardware requirements (**BSA** – Base System Architecture)

- **BSA**: Common standard architecture for 64-bit Arm-v8 and Arm-v9.
- **SBSA**: Server specific hardware requirements
- Covers Arm processor and system architecture, PCIe, CXL.

Firmware (**BBR** – Base Boot Requirements)

- Common firmware interfaces that OSes and hypervisors depend on.
- **SBBR** “recipe” (TF-A, UEFI, ACPI, SMBIOS) for servers and workstations, with generic OS support (Windows, VMware, Enterprise Linux distros).
- **LBBR** “recipe” (LinuxBoot)
- Aligns with OCP OSF.

Security Interfaces (**BBSR** - Base Boot Security Requirements)

- OS-FW security interfaces requirements.
- UEFI Secure Boot , Secure firmware updates, TPM.
- Secure system design guidelines.
- Arm servers compliant with BBSR are REQUIRED to have TPM!

Management (**SBMR** - Server Base Manageability Requirements)

- The “control plane” of the server, (DMTF PMCI/Redfish/SPDM, IPMI).
- Currently not part of SystemReady.
- Aligns with OCP HW Management, HW Fault Management and DC-SCM.

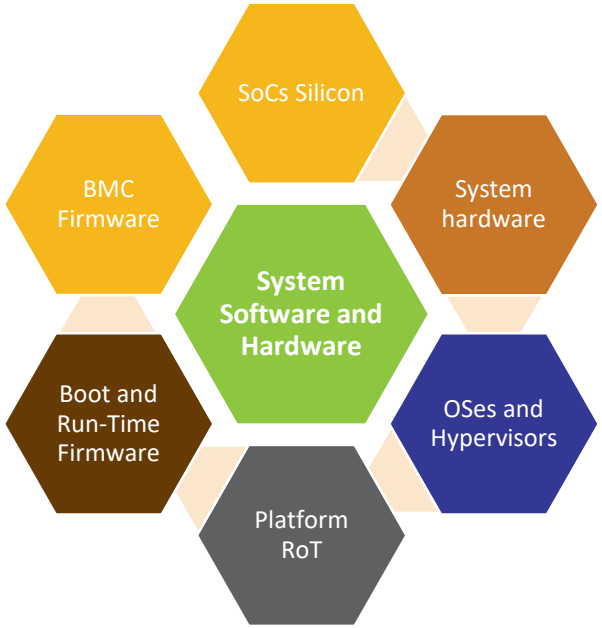
Arm System Architecture Advisory Committee (SystemArchAC)

Arm SystemArchAC

- Consortium of 60+ Companies (Arm partners, hardware and software ecosystem)
- Where Arm system standards are developed

- System Hardware Architectural Requirements
- Boot Firmware Requirements
- Run-time Firmware Requirements
- Manageability Requirements
- Security Requirements
- RAS Requirements
- PCIe, CXL, UCIe Integration Requirements

Impacts



Build on and contribute to industry standards

OPEN Compute Project

DMTF Redfish

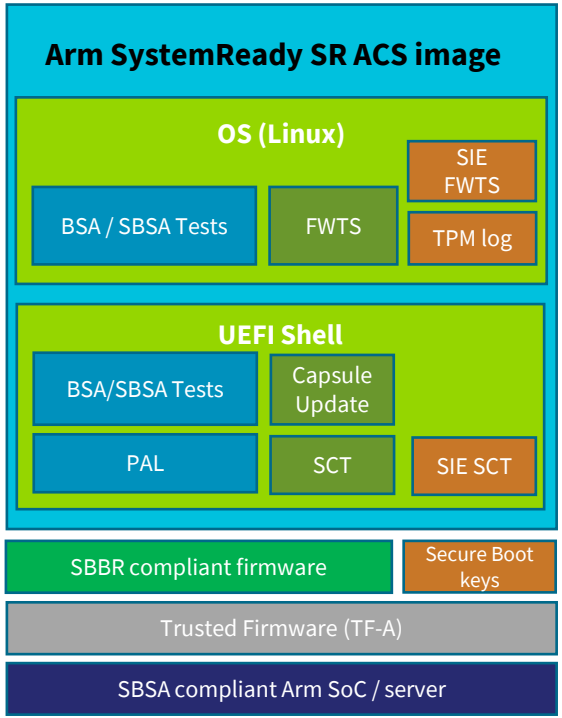
PCI SIG

CXL Compute Express Link

UCIe Universal Chiplet Interconnect Express

TRUSTED COMPUTING GROUP

Arm Architecture Compliance Suite (ACS)

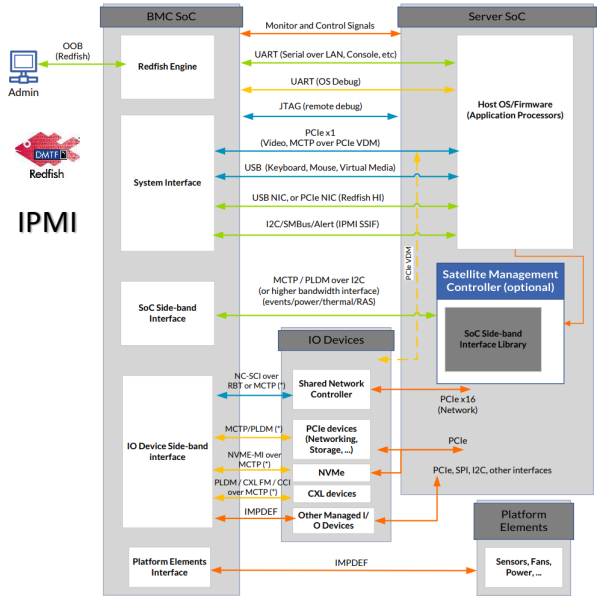


- https://github.com/ARM-software/arm-systemready
- Open-source compliance testing for:
  - Hardware (pre-silicon, silicon and platform)
    - BSA-ACS : https://github.com/ARM-software/bsa-acs
    - SBSA-ACS: https://github.com/ARM-software/sbsa-acs
    - Also available on bare-metal for pre-silicon compliance
  - Firmware (boot- and run-time)
    - BBR-ACS: https://github.com/ARM-software/bbr-acs
  - Security firmware interfaces (UEFI SecureBoot, TPM, Secure FW Update)
    - SIE-ACS, Included in BBR-ACS and SystemReady ACS
- **Contributed to OCP**
  - Scripts to pull Arm SystemReady ACS and its various components

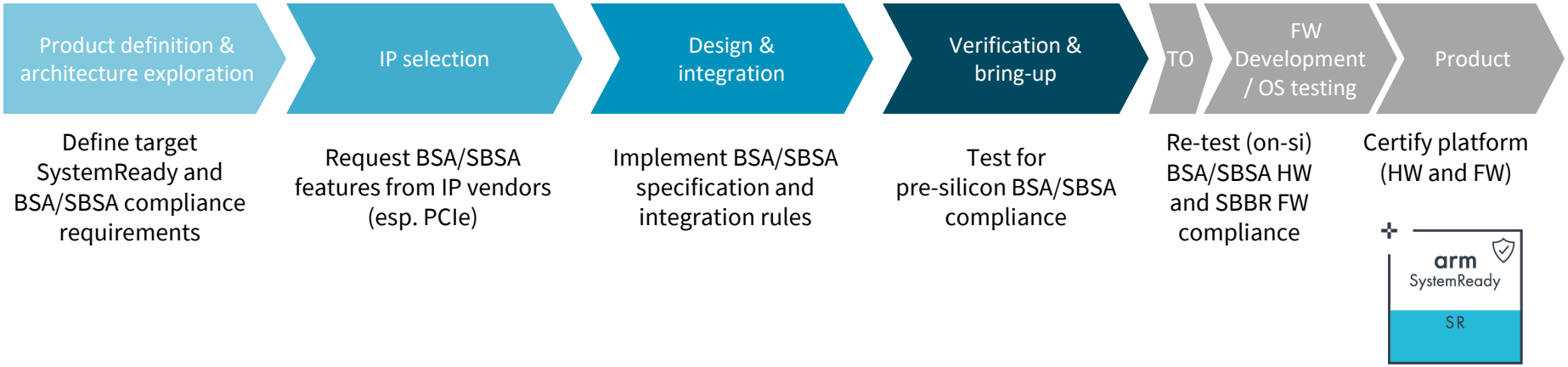
Manageability Compliance (SBMR-ACS)

HW MGMT

- 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
  - 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



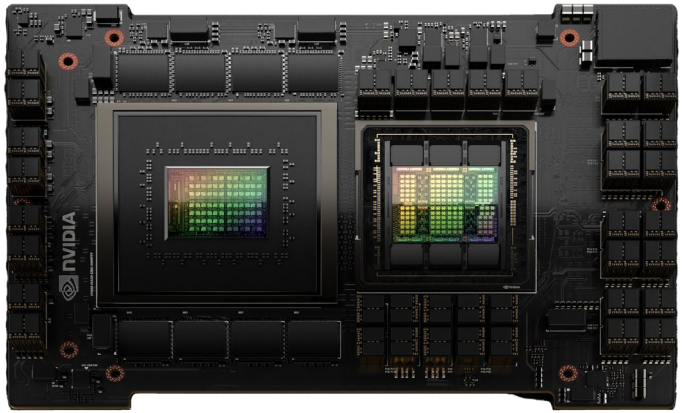
SystemReady Pre-Silicon



Pre-silicon BSA/SBSA compliance is critical to becoming SystemReady

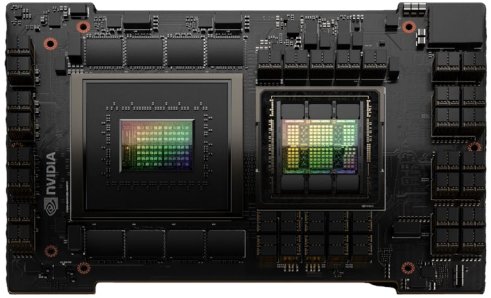
Pre-silicon Exerciser and compliance testing solutions available from Arm EDA partners

NVIDIA Grace GH200 and Grace Superchip



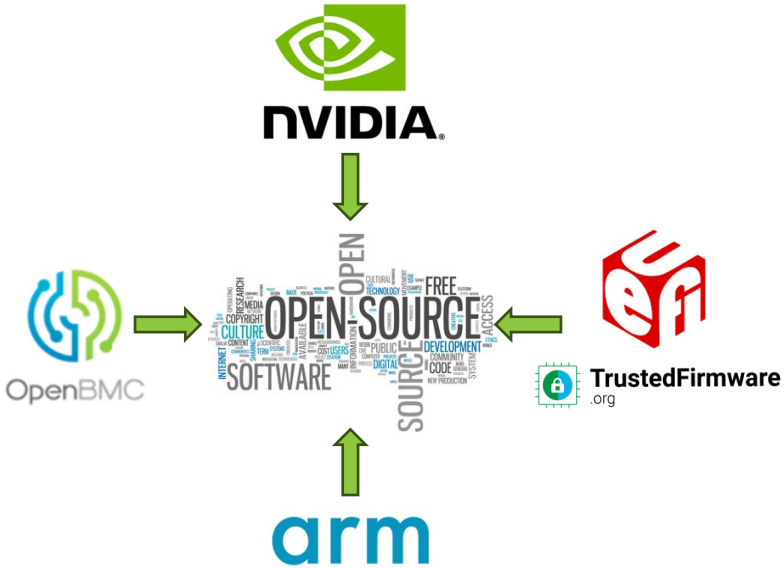
- Up to 144 Core Arm Neoverse V2 with Scalable Vector Extensions (SVE2)
- Hopper GPU with up to 142GB Memory (GH200)
- High-speed C2C interconnect: 900 GB/s alleviates NUMA bottlenecks (7x faster than PCIe Gen5)
- Scalable Coherency Fabric: 3.2 TB/s total bisection bandwidth for faster dataflow among the CPU cores, C2C, and System I/O
- LPDDR5X: 53% more bandwidth at 1/8 power
- Up to 8 x16 PCIe Gen5 PCIe Links

NVIDIA Grace – Build on Standards



- Arm Base System Architecture (BSA) and Server Base System Architecture (SBSA) Compliant – SBSA Level 4.
  - Designed and tested for pre-silicon and post-silicon compliance
- Arm Server Base Management (SBMR) Compliant – Level M3
- Arm Base Boot Requirements Compliant (BBR, SBBR recipe)
- Arm Base Boot Security Requirements Compliant (BBSR)
- Managed via DMTF PLDM Type 2 Sensors and Effectors
- Firmware Update via DMTF PLDM Type 5
- Security - SPDM for Attestation

NVIDIA Grace – Open-Source Firmware



- NVIDIA Reference Firmware built on Open-source and industry standards
- UEFI EDK2 Reference Solution (https://github.com/NVIDIA/edk2)
- BMC Reference Solution based on OpenBMC
- TF-A and Hafnium Open-source

NVIDIA Grace - SystemReady SR + SIE Certifications!

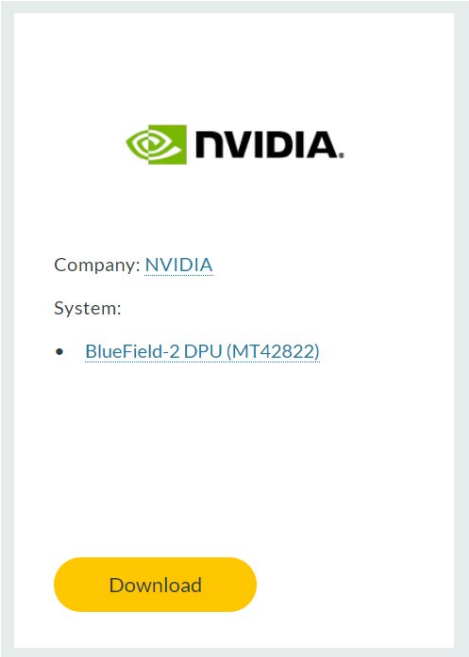
NVIDIA Grace is the industry's first Arm SystemReady SR v2.4 with **Security Interface Extension (SIE)** v1.2 certified system!

"The lifeblood of Arm in my mind has less to do with microarchitecture, and more concerns what the broader ecosystem brings to the table: the ability for NVIDIA to innovate on all aspects of SoC hardware design and deliver products with unique performance and value, while standing on the shoulders of the millions of person-years that have gone into software development, operating systems, drivers, and testing across the decades of Arm-compatible CPUs. Arm SystemReady SR is an incredible extension of this value, and allows us to prove that whatever we're building will let customers take anything from applications and firmware, to entire operating systems with drivers that may have never run before on Grace— and have them fly out-of-the box. More importantly, it protects the investment they make in deploying Arm systems, which they are free to take with them any time— even to other products from other vendors, if they find value there."

Ian Finder, Principal Product Lead, Grace at NVIDIA

NVIDIA BlueField SystemReady Certifications!

arm SystemReady ES CERTIFIED V1.3



NVIDIA BlueField 2 is the industry's first Arm SystemReady ES certified DPU!

"As data centers transform into AI factories, networking infrastructure must evolve to keep up with the spiking efficiency and scalability demands, NVIDIA BlueField DPUs and the DOCA software framework are enabled with Arm architecture to offload, accelerate, and isolate advanced networking, storage, and security services – massively boosting data center efficiency and scale."

John Kim, Director of Networking at NVIDIA

NVIDIA Firmware Ecosystem

OPEN SYS FW

Grace Customized System Design

NVIDIA Reference Design

Reference code

IBV Partner (Insyde)

insyde + OEM Customizations = OEM Grace Firmware Solution based on IBV, leveraging Open-Source

OR

NVIDIA Open-Source (UEFI and OpenBMC) + OEM Customizations = Grace Firmware Solution based on Open FW

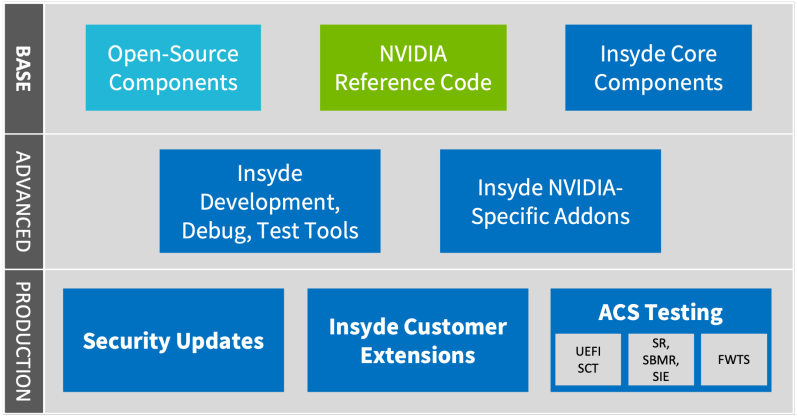
OR

NVIDIA Open-Source (UEFI and OpenBMC) = NVIDIA Grace Firmware Reference Solution based on Open FW

Move Beyond The Basics With Insyde

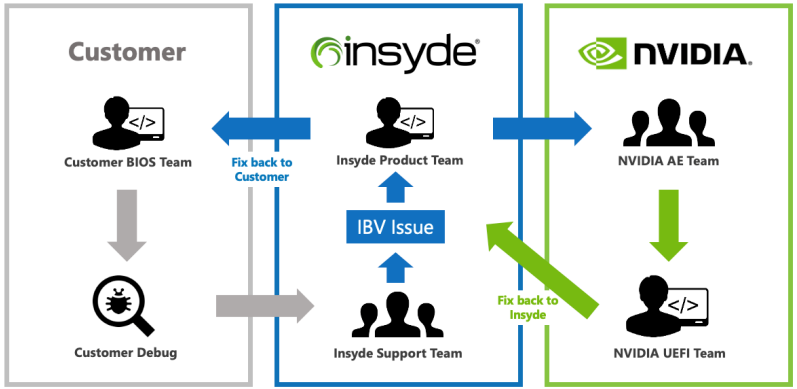
InsydeH2O® on Grace Hopper

- 20+ years of bringing customer requirements to production in EFI/UEFI
- Commonly requested features are ready to go (TPM 2.0, Early Video, Graphical Setup, Logo, Hot Key, Advanced Boot & Console Redirection)
- Comprehensive tool suite makes development (H2OIDE), customization (H2OUVE, H2OSDE) and deployment (H2OFFT) easier
- Security updates before and after first ship
- Arm SystemReady SR and SIE Certified

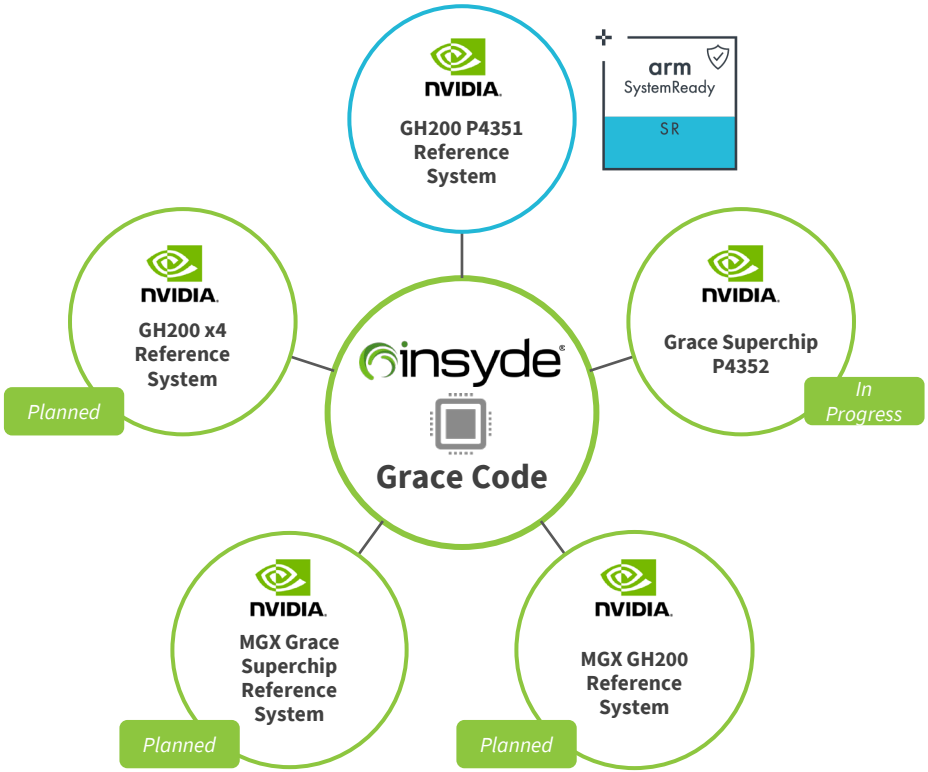


Supervyse® OPF on Grace Hopper

- OpenBMC-based
- NVIDIA Device Ownership Transfer (DOT)
- SPDM for Firmware Integrity Check
- PLDM for Firmware Update, PCIe Devices, DRAM & Grace Power Limiting
- SBMR-ACS Compliant



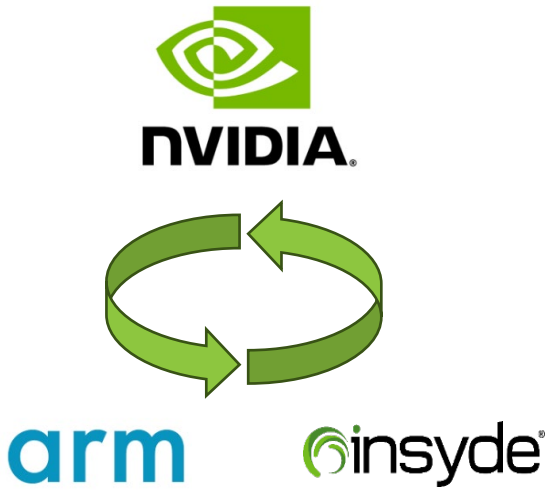
Insyde Certified ARM SystemReady SR-SIE



- InsydeH2O® makes your system ready to go to market
  - Certified SystemReady SR with SIE on NVIDIA GH200 Grace Hopper and Grace Superchip platforms
  - ARM's ACS-SR and SIE ensures compliance with the BSA, SBSA and SBBR standards for servers
- Supervyse® OPF makes your system ready to go to market
  - SBMR 2.0 compliant using SBMR-ACS on NVIDIA GH200 Grace Hopper platform
  - Redfish and IPMI support

insyde H2O BIOS Supervyse® OPF

Arm Datacenter Architecture– Building Trust

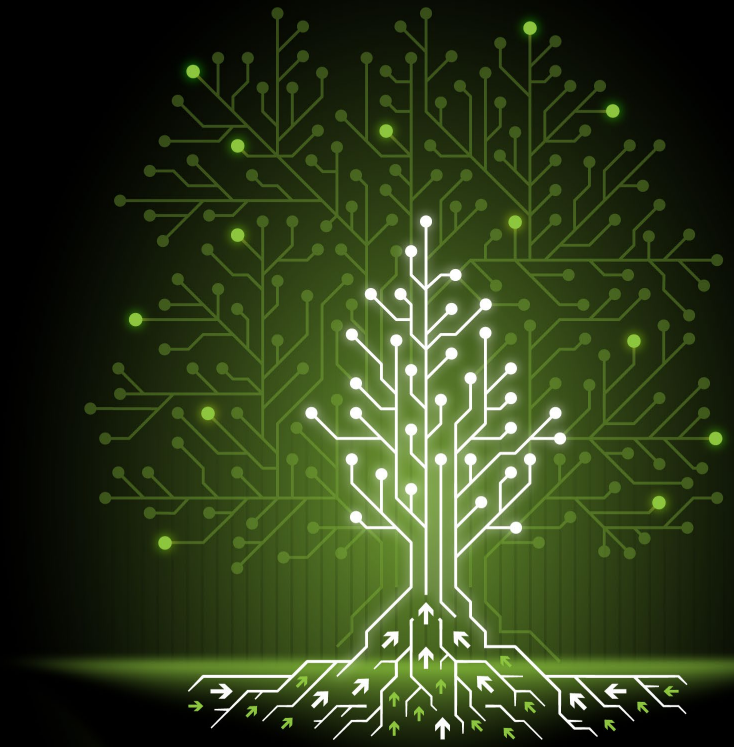


- Arm SystemReady SR Certification and compliance
- Arm SystemReady Security Interface Extension (SIE) compliance
- Arm Server Base Management Requirements (SBMR) compliance

Call to Action

- Join Arm SystemReady! www.arm.com/systemready-certification-program
- Collaborate with us on Arm-hosted OCP Experience Center: ocp-marketplace@arm.com
- Visit Arm booth **(B14)** and attend Arm & NVIDIA sessions @ OCP Global Summit 2023

Thank you!



Scaling Innovation Through Collaboration

OCP GLOBAL SUMMIT

OCTOBER 17-19, 2023
SAN JOSE, CA