RISC-V Summit China 2024

SBI 安全服务API 规范RISC-V安全实现

Yong Li (yong.li@intel.com)

Aug.23 2024

Legal Notices and Disclaimers

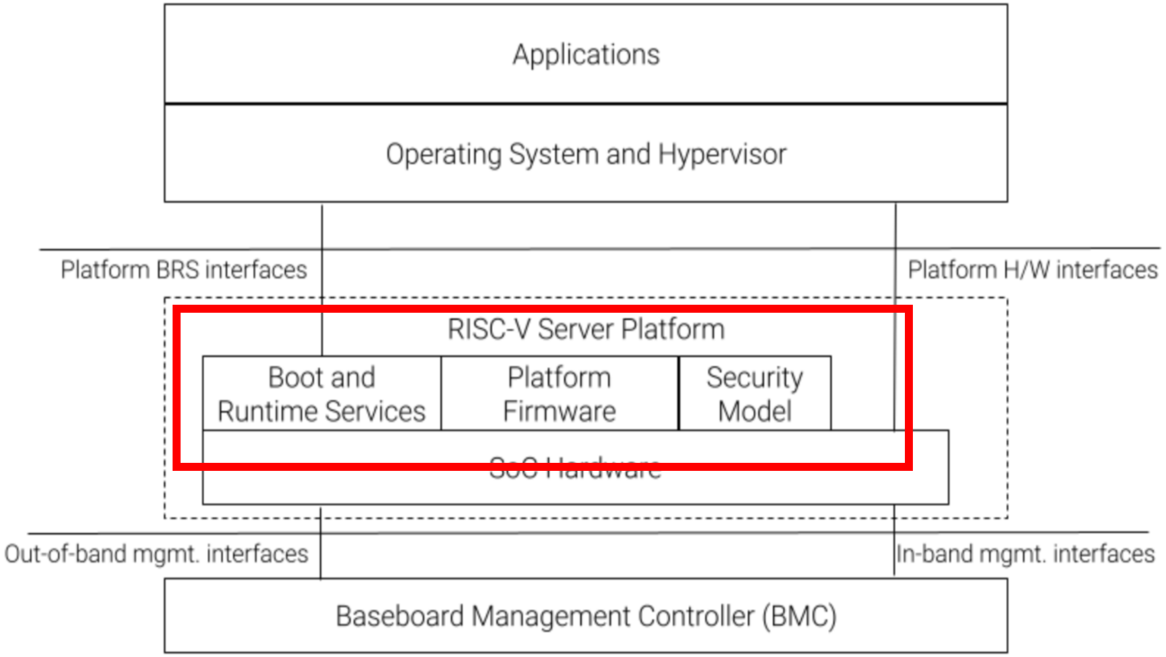
Statements in this document that refer to future plans or expectations are forward-looking statements. These statements are based on current expectations and involve many risks and uncertainties that could cause actual results to differ materially from those expressed or implied in such statements. For more information on the factors that could cause actual results to differ materially, see our most recent earnings release and SEC filings at www.intc.com.

All product plans and roadmaps are subject to change without notice. Any forecasts of goods and services needed for Intel's operations are provided for discussion purposes only. Intel will have no liability to make any purchase in connection with forecasts published in this document. Code names are often used by Intel to identify products, technologies, or services that are in development and usage may change over time. No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

This document contains information on products and/or processes in development.

RISC-V Platform

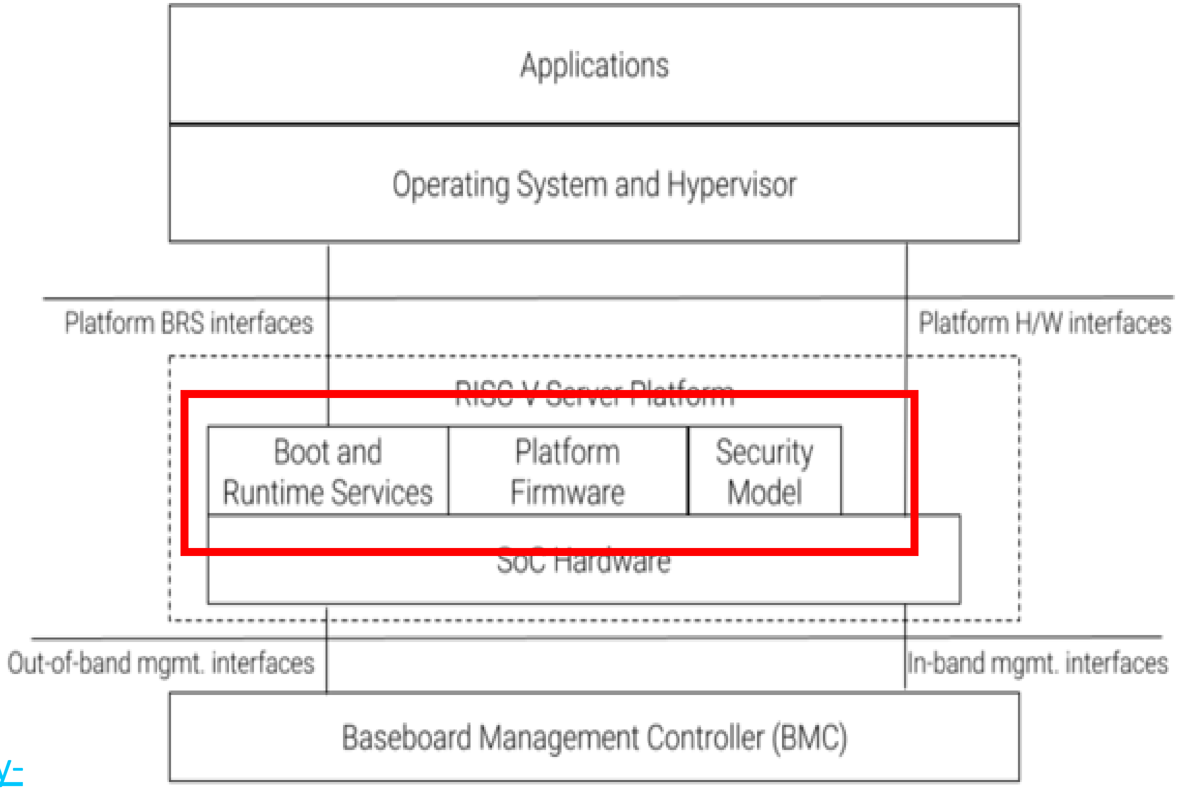
- Boot and Runtime Services (BRS)
  - 定义操作系统启动和运行的环境
- Platform Firmware (PRS)
  - 定义Firmware的实现，包括SBI，UEFI，Device Tree，ACPI
- Platform Security
  - 定义平台的安全模型和需求



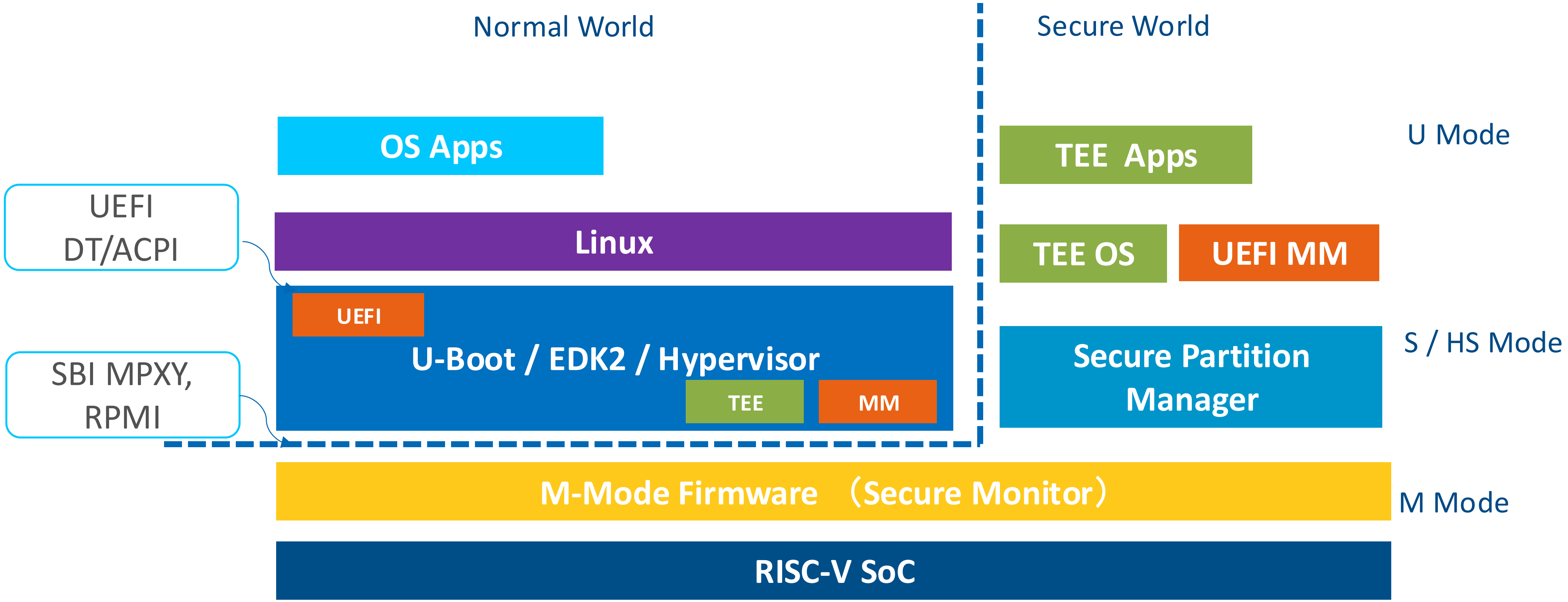
Components of a RISC-V Server Platform

RISC-V Platform

- Boot and Runtime Services (BRS)
  - BRS 规范
    - https://github.com/riscv-non-isa/riscv-brs
- Platform Firmware (PRS)
  - SBI 规范
    - https://github.com/riscv-non-isa/riscv-sbi-doc
  - RPMI 规范
    - https://github.com/riscv-non-isa/riscv-rpmi
- Platform Security
  - Security Model 规范
    - https://github.com/riscv-non-isa/riscv-security-model

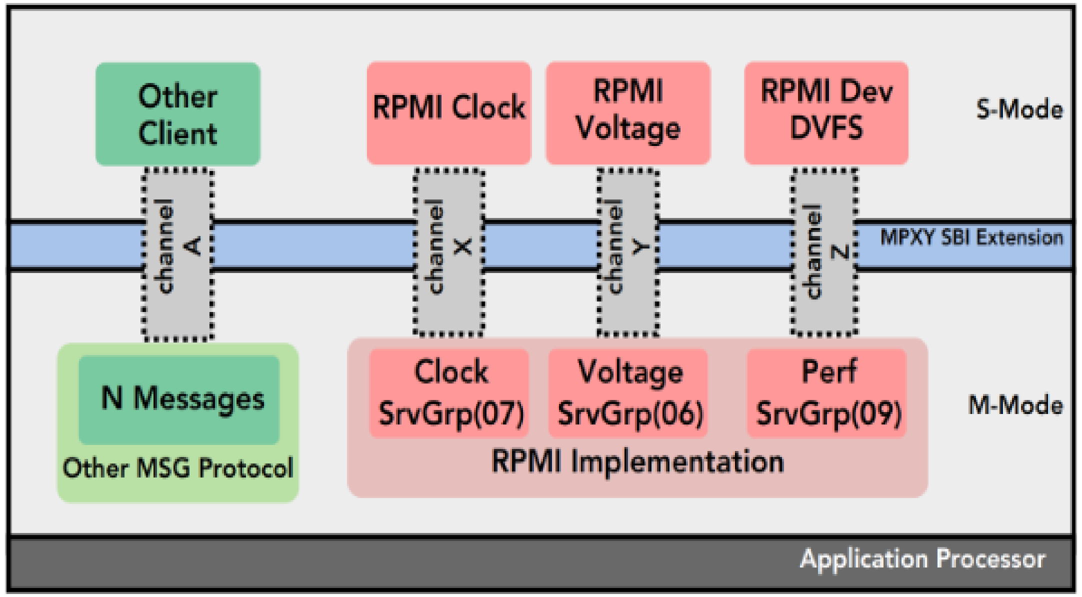


RISC-V的安全软件栈



RISC-V SBI 的消息代理扩展 - MPXY

- 多个S-Mode模式的客户端共享相同的SBI代理接口，包括Domain, Secure 分区， 和虚拟机
- 方便系统扩展多个客户端
- 也可以作为HS-Mode模式跟客户端通信的传输中介
- 包含 ARM SMCCC 功能



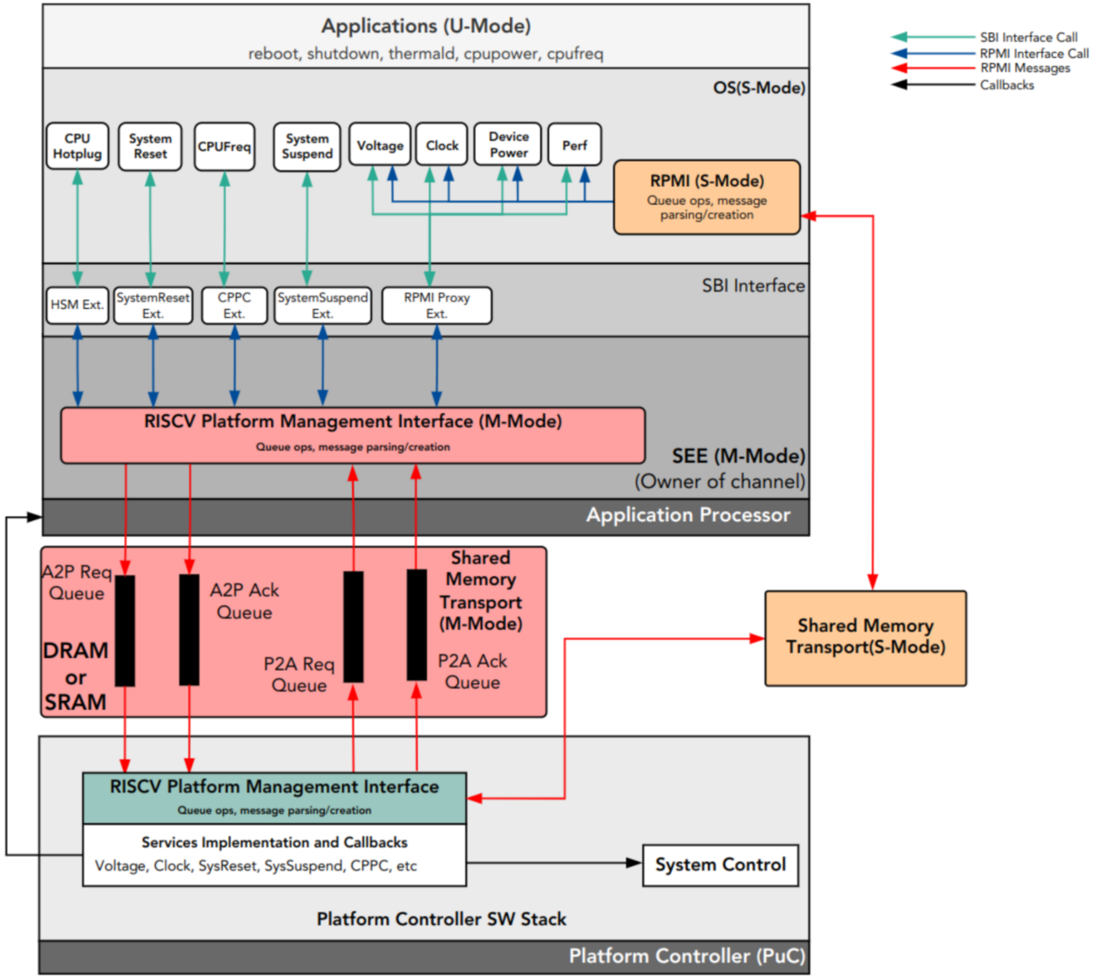
RISC-V 平台管理规范 - RPMI

- **定义了系统管理与控制服务，使用**PuC（Platform Microcontroller)

- **可**扩展安全服务

- **定**义传输层的协议

- 类似于 ARM SCMI

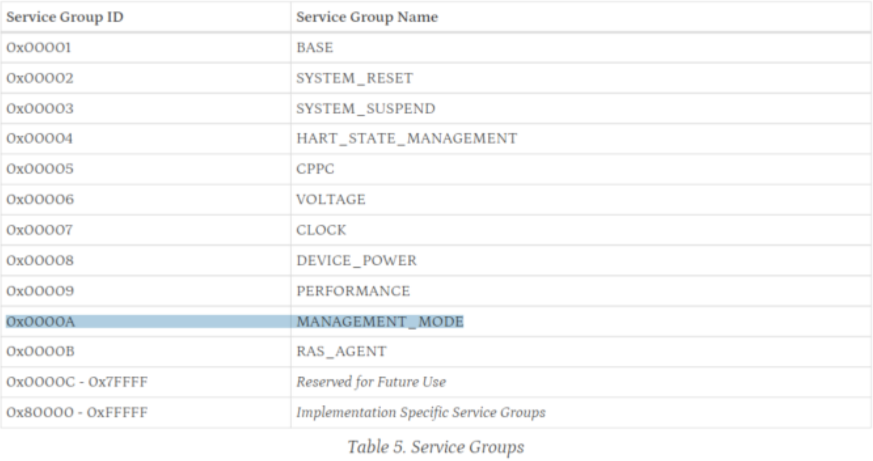


Applications (U-Mode)
reboot, shutdown, thermald, cpupower, cpufreq
OS(S-Mode)
CPU Hotplug
System Reset
CPUFreq
System Suspend
Voltage
Clock
Device Power
Perf
RPMI (S-Mode)
Queue ops, message parsing/creation
SBI Interface
HSM Ext.
SystemReset Ext.
CPPC Ext.
SystemSuspend Ext.
RPMI Proxy Ext.
RISCV Platform Management Interface (M-Mode)
Queue ops, message parsing/creation
SEE (M-Mode)
(Owner of channel)
Application Processor
A2P Req Queue
A2P Ack Queue
P2A Req Queue
P2A Ack Queue
Shared Memory Transport (M-Mode)
DRAM or SRAM
Shared Memory Transport(S-Mode)
RISCV Platform Management Interface
Queue ops, message parsing/creation
Services Implementation and Callbacks
Voltage, Clock, SysReset, SysSuspend, CPPC, etc
System Control
Platform Controller SW Stack
Platform Controller (PuC)
SBI Interface Call
RPMI Interface Call
RPMI Messages
Callbacks

PRS 和RPMI 规范中的安全接口定义 – 进行中

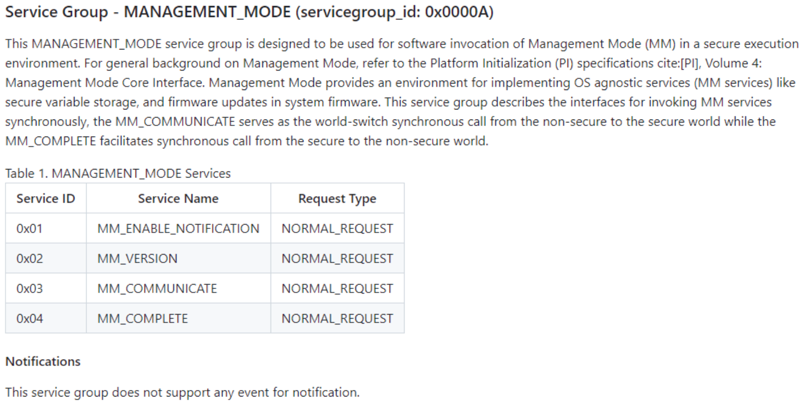
- 在MPXY 规范中增加 UEFI MM 和TEE 的 协议ID
  - https://github.com/riscv-non-isa/riscv-sbi-doc

- 在RPMI 中增加 UEFI MM and TEE 消息协议规范
  - https://github.com/riscv-non-isa/riscv-rpmi



Service Group ID	Service Group Name
0x00001	BASE
0x00002	SYSTEM_RESET
0x00003	SYSTEM_SUSPEND
0x00004	HART_STATE_MANAGEMENT
0x00005	CPPC
0x00006	VOLTAGE
0x00007	CLOCK
0x00008	DEVICE_POWER
0x00009	PERFORMANCE
0x0000A	MANAGEMENT_MODE
0x0000B	RAS_AGENT
0x0000C - 0x7FFFF	*Reserved for Future Use*
0x80000 - 0xFFFFF	*Implementation Specific Service Groups*

Table 5. Service Groups



Service Group - MANAGEMENT_MODE (servicegroup_id: 0x0000A)

This MANAGEMENT_MODE service group is designed to be used for software invocation of Management Mode (MM) in a secure execution environment. For general background on Management Mode, refer to the Platform Initialization (PI) specifications cite:[PI], Volume 4: Management Mode Core Interface. Management Mode provides an environment for implementing OS agnostic services (MM services) like secure variable storage, and firmware updates in system firmware. This service group describes the interfaces for invoking MM services synchronously, the MM_COMMUNICATE serves as the world-switch synchronous call from the non-secure to the secure world while the MM_COMPLETE facilitates synchronous call from the secure to the non-secure world.

Table 1. MANAGEMENT_MODE Services

Service ID	Service Name	Request Type
0x01	MM_ENABLE_NOTIFICATION	NORMAL_REQUEST
0x02	MM_VERSION	NORMAL_REQUEST
0x03	MM_COMMUNICATE	NORMAL_REQUEST
0x04	MM_COMPLETE	NORMAL_REQUEST

Notifications

This service group does not support any event for notification.

RISC-V UEFI Secure Boot 和 OP-TEE 的实现

- 基于RISC-V Virt 实现的UEFI Secure Boot原型 （Also verified on VF2）
  - https://wiki.riseproject.dev/display/HOME/EDK2_00_15+-+StandaloneMmPkg+RPMI+MM+support
  - https://wiki.riseproject.dev/display/HOME/SBI_00_05+-+OpenSBI+RPMI+MM+Support

- 基于RISC-V Virt 实现的OP-TEE 原型(From Andes)
  - https://wiki.riseproject.dev/display/HOME/OPTEE_00_01+-+OP-TEE+support

RISE
RISC-V Software Ecosystem

Call for action

- MPXY/RPMI 规范计划在2025初获得批准

- 参与 MPXY/RPMI 规范的讨论和贡献 -- Lead by Leyfoon Tan, Rahul Pathak
  - https://lists.riscv.org/g/tech-prs
  - https://lists.riscv.org/g/tech-rpmi

- 参与 标准化平台 **和** BRS规范的讨论和贡献 -- Lead by Warkentin, Andrei, Haibo Xu
  - https://lists.riscv.org/g/tech-server-platform
  - https://lists.riscv.org/g/tech-brs

- 参与 RISE **社区的安全相关**项目， 包括UEFI **和** TEE -- Lead by Sunil V L
  - https://wiki.riseproject.dev/display/HOME/Firmware+WG

RISE
RISC-V Software Ecosystem

RISE

RISC-V Software Ecosystem

- https://riseproject.dev

RISE is focused on positive and transparent collaborations with upstream projects to deliver commercial-ready software for various use cases

How: Align on highest priorities & avoid (accidental) duplication of work

Goal: Accelerate open source SW for RISC-V architecture

https://www.intel.com/content/www/us/en/developer/articles/community/rising-to-the-challenge-risc-v-software-readiness.html

Finding more interesting topics from Intel on RISC-V summit China 2024

Topic	When & Where
UXL 软件栈和 RISC-V 的初步探索	August 22 16:45 主会场A
LLVM 工具链 RISC-V 构建实现及其性能优化现状分析与未来展望	August 23 9:40 主会场A
GCC RVV 自动向量化及其应用	August 23 10:00 主会场A
Enhancing RISC-V Security with SBI Secure Service APIs	August 23 10:40 主会场B
Enabling Hardware Sampling Based PGO for RISC-V Platform	August 23 11:40 主会场A
利用 WASM 技术解决多种 ISA 的挑战	August 23 14:20 主会场B
HVP: Hardware Accelerated RISC-V Android Emulator	August 23 14:50 主会场A
Leverage BRS standard to improve RISC-V SW compatibility	August 23 17:30 主会场A
Soft-ISA: kernel built-in emulation engine to extend RISC-V silicon ISA capability	August 23 17:40 主会场A

intel®