



RISC-V Server Feature in SpacemiT SoCs

Lv 'Zetalog' Zheng

RISC-V Server IP Racks

- **Server SoC Platform – V100**
 - 64-core X100
 - Support CPU/IO virtualization
 - Support BMC/UEFI server firmware environment
 - Support RISC-V compliant RAS and perf features
 - Support trusted computing
- **High Performance CPU – X100**
 - SPEC CPU@ 2006 scores > 9/GHz
 - 2.5GHz@12nm
 - AI computers and AI robots
- **High Performance CPU – X200**
 - SPEC CPU@ 2006 scores > 16/GHz
 - 3.2GHz@7nm
 - Super AI computers, cloud computing and advanced automotive chips



RISC-V Server SoC Compliance

Segment	Required	Supported
timers		All compliant
AIA		All compliant
IOMMU	SHOULD support MRIF	No MRIF support
	SHOULD support DBG	No DBG support
PCIe	MUST support ACS I/O request blocking	No ACS enhanced capability
	SHOULD support P2P VDM routing between RCs	No P2P VDM routing between RCs except MCTP routing
	MAY support P2P VDM routing between EPs	No P2P VDM routing between EPs
	MAY support PTM	No PTM support
RAS		All compliant
QoS	SHOULD support CBQRI	No CBQRI support

- Compliant to RISC-V Server SoC Specification v1.0, 2025-02-21: Ratified
- Support all but one PCIe 6.0 MUST feature
- Support most SHOULD features and lots of MAY features
- Significant compliance to virtualization, manageability (RAS), security, performance requirements

Segment	Required	Supported
Manageability		All compliant
Performance Monitoring	SHOULD support requester average latency counting	Only support target latency counting
	SHOULD support local/remote filter	No local/remote filter
	SHOULD support PCIe flit performance measurement	No PCIe flit performance measurement
Security	SHOULD support PCIe IDE	No PCIe IDE
	SHOULD support off-chip DRAM encryption	No off-chip DRAM encryption

Contents

- 01 Virtualization**
- 02 Manageability**
- 03 Security**
- 04 Performance**
- 05 Other features**

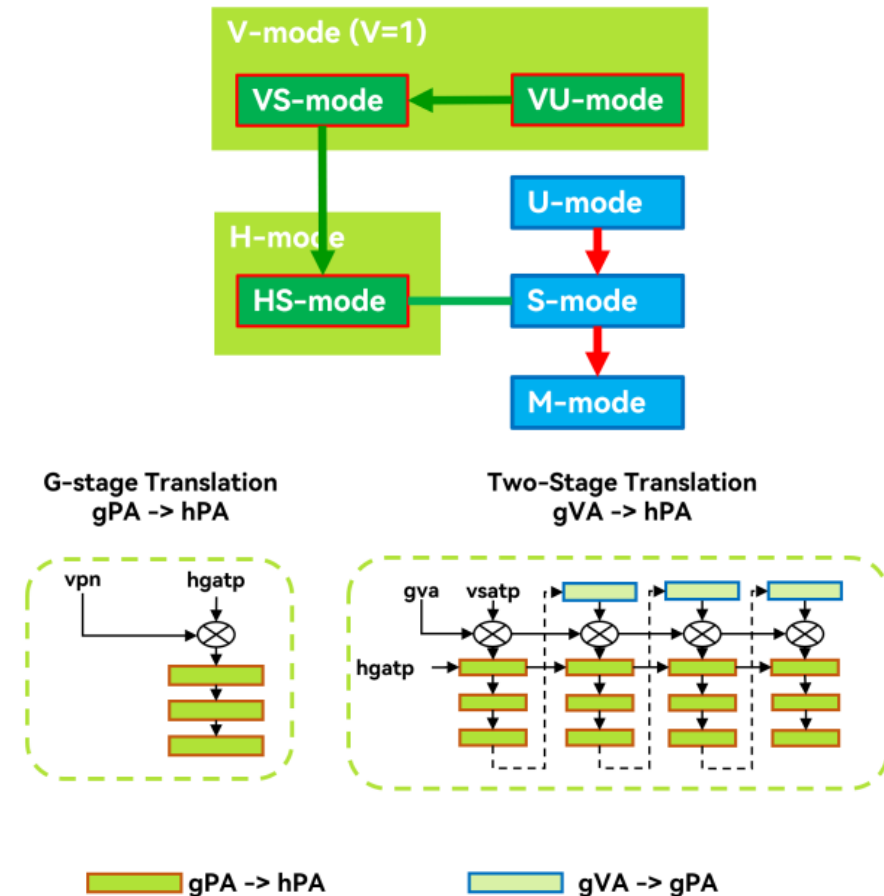
01

Virtualization

CPU Virtualization – RVH



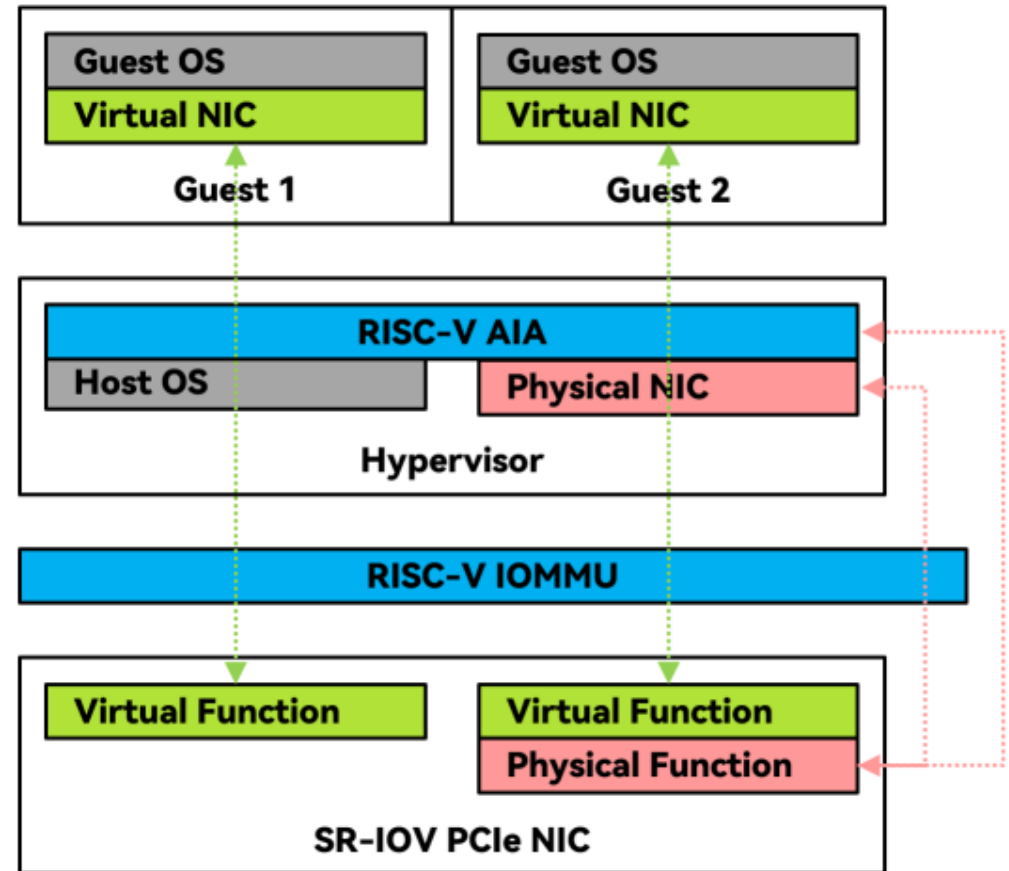
- Hypervisor extended S (HS) mode
 - HS-mode CSR, time delta HPM
 - Guest page/virtual instruction fault/HS-mode ECALL
 - VSEI/VSTI/VSSI
- Virtualization Mode (V)
 - Virtualized supervisor (VS) mode/Virtualized user (VU) mode
 - VS-mode background CSR
 - ECALL from VS-mode/VU-mode
- Address translations
 - hgatp pointing to G-stage translation table
 - vsatp pointing to VS-stage translation table
 - PTW/TLB with GPA support
- Instructions
 - HS-mode system barrier
 - Guest memory access



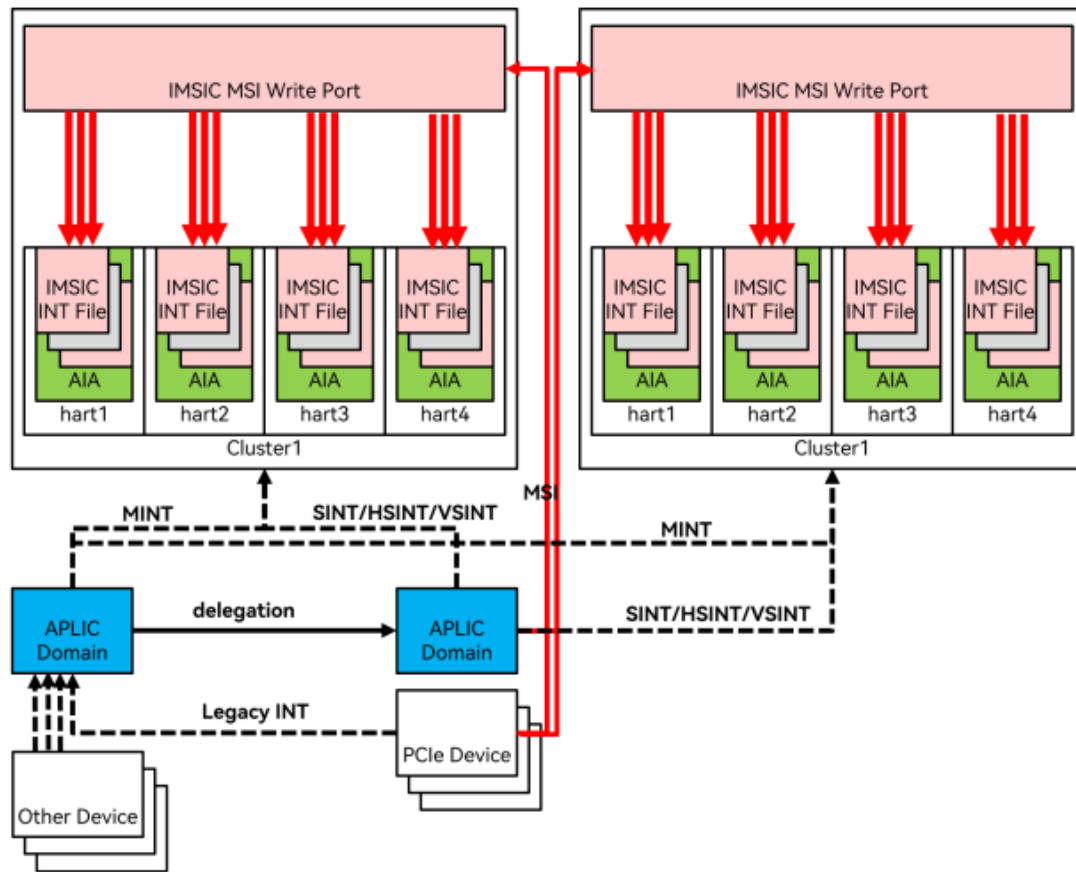
IO Virtualization Overview



- IO virtualization – AIA
- IO virtualization – IOMMU
- IO virtualization – SR-IOV
 - Support PCIe physical function assignment of host OS
 - Support PCIe virtual function assignment of guest OS

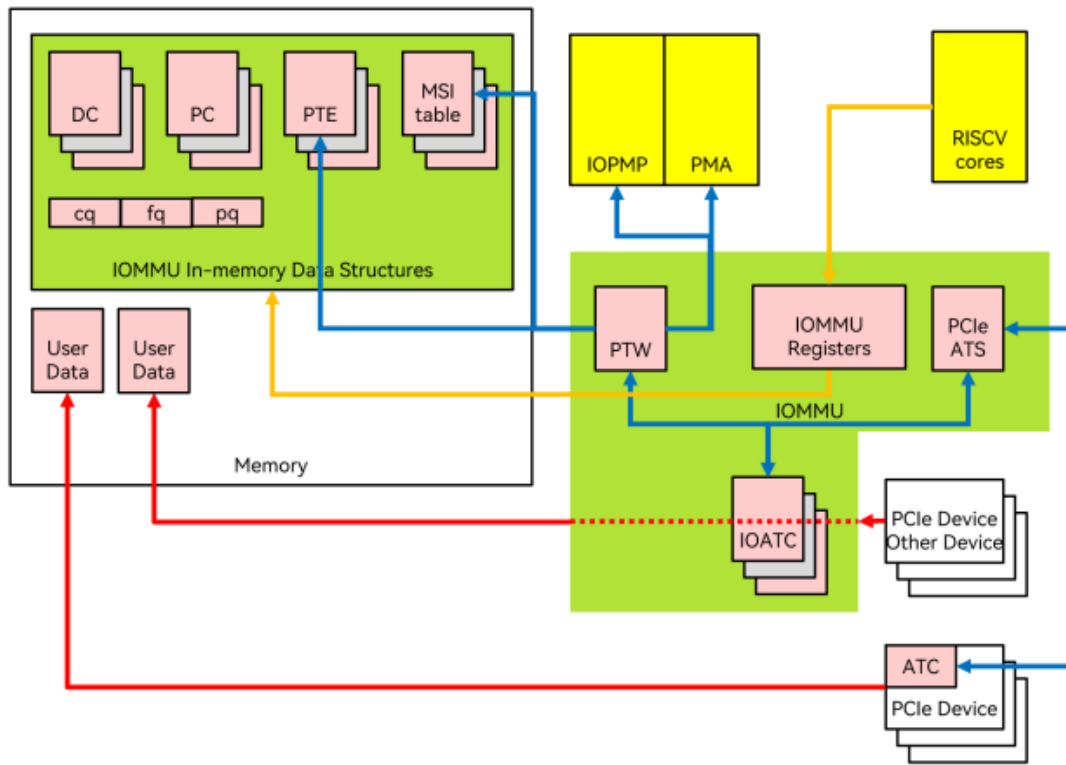


IO Virtualization – AIA



- AIA v1.0 compliant
 - Major IRQ priority
 - Virtual interrupt, VTI
 - GEILEN ≥ 8
 - WSI and MSI support
 - 1023 APLIC interrupt sources
 - 2048 IMSIC interrupt sources
- Prioritized platform IRQs:
 - RAS CE, RAS NE, NMI, debug and trace, etc.
- MSI support
- PCIe interrupt routing
- IRQ virtualization and remapping
- Interrupt domain
- GSI/IPI support

IO Virtualization – IOMMU



- IOMMU v1.0 Compliant **T100**

- **24-bit DDI**, **20-bit PDI**, 44-bit DMA
- Sv39/Sv48 S1 + Sv39x4 Sv48x4 S2 support
- PCIe ATS/T2GPA/PRI support
- Support MSI flat, Svpbmt/Svnapot
- **Support HPM and RAS RERI**
- Support IOPMP/PMA check

- Interrupt remapping and virtualization
- DMA remapping, memory protection
- Pointer-is-a-Pointer in heterogenous computing (accelerators)
- Nested address translation in Guest OS
- Translation Cache in PCIe device
- Demand Paging from PCIe device



02

Manageability

Manageability Overview

- **BMC features**

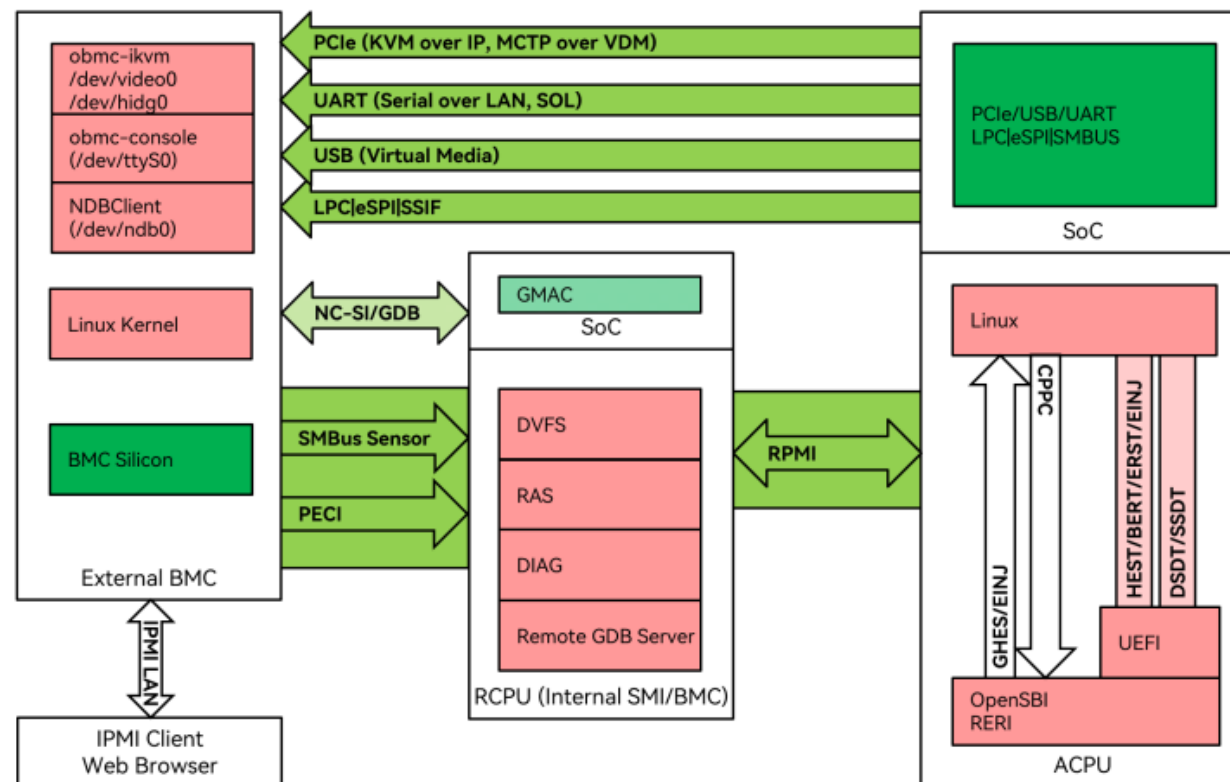
- LPC
- eSPI
- KCS
- SSIF
- SOL
- KVM
- MCTP
- PECE

- **DVFS ACPI compliance**

- CPPC

- **DVFS RISC-V compliance**

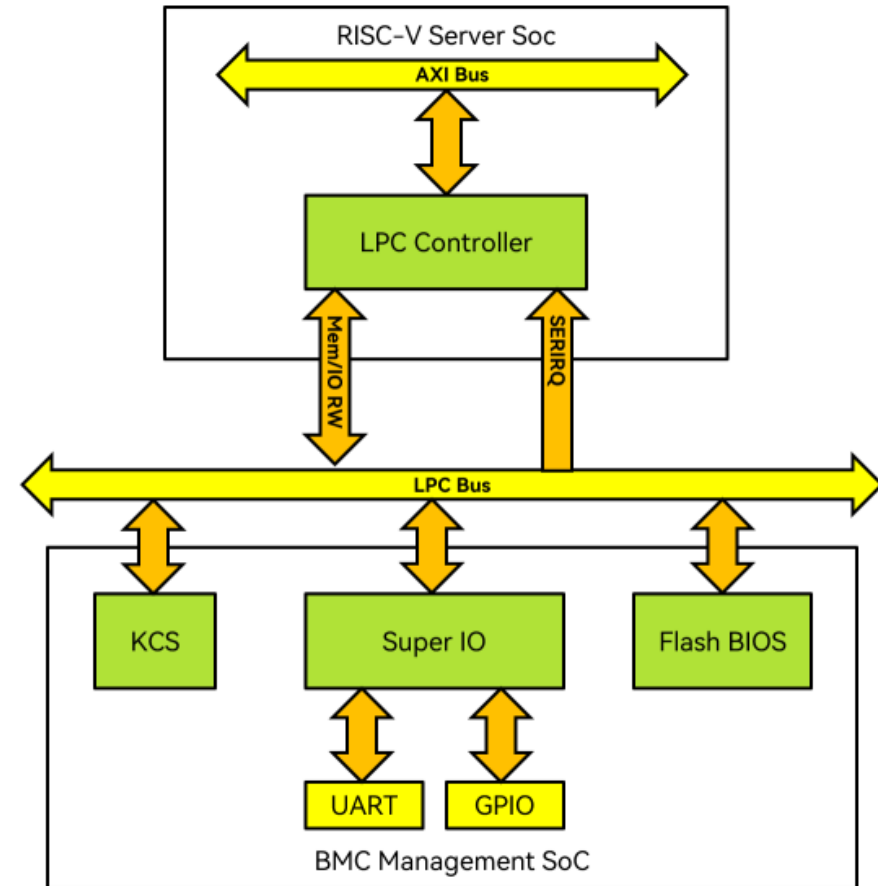
- RPMI



BMC Feature – LPC



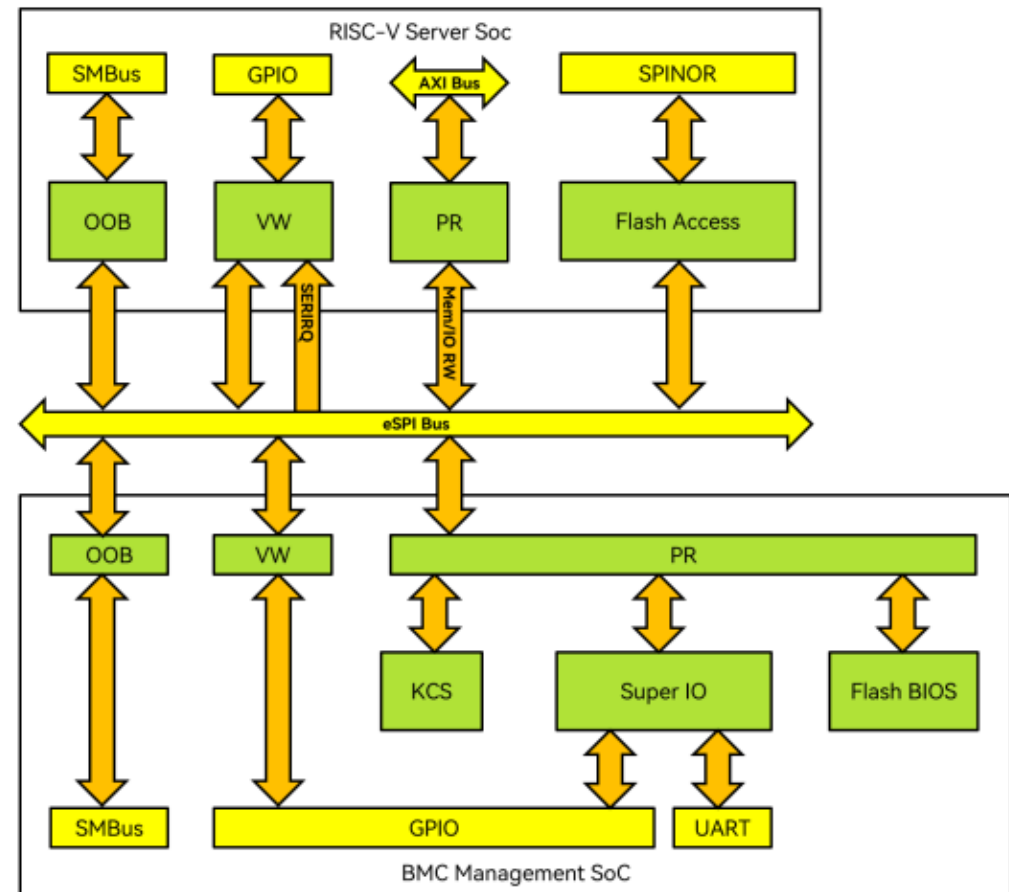
- Intel Low PIN Count Interface 1.1
- Support I/O, memory and firmware read/write cycle
- Support 1/2/4 bytes firmware read/write cycle
- Support 17 ~ 32 IRQ slots SERIRQ interface
- Support AXI4 64-bit address, 32-bit data width, 64KB bridged I/O space and 32MB bridged memory space



BMC Feature – eSPI



- Enhanced Serial Peripheral Interface (eSPI) revision 1.0
- Support PR/OOB/VW/flash access channels
- Support 20/25/33/50/66MHz IO frequency
- Support 1x/2x/4x eSPI I/O mode
- Support AXI4 64-bit address, 32-bit data width, burst 16, 64KB bridged I/O space and 32MB bridged memory space
- Support 16*4-byte PR FIFO size
- Support 0-23 VW IRQ, up to 16-bit GPIO
- Support interrupt for system event 2~7
- Support up to 16 VW count per transfer
- Support up to 128-byte OOB and flash access transfer size



BMC Feature – KCS/SSIF

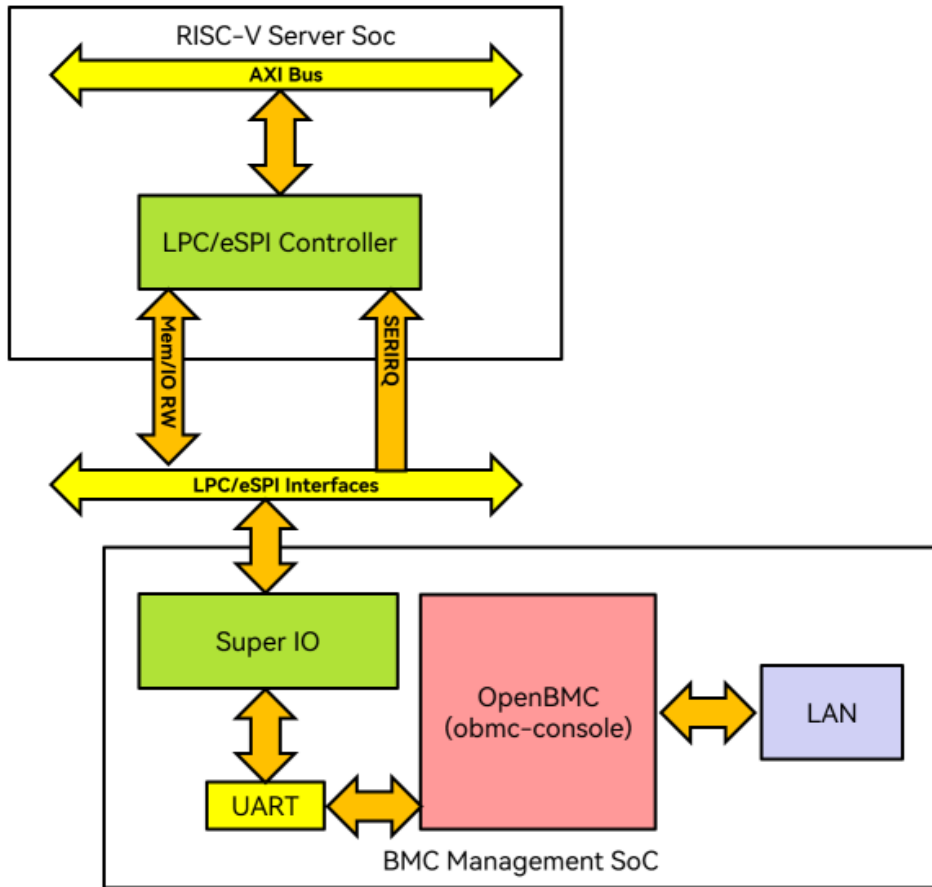
- Support traditional non-x86 platform IPI0001 PnP device returning _IFT 0x04 SSIF via SMBus
- Support IPI0001 PnP device returning _IFT 0x01 KCS IPMI system interface KCS via LPC I/O and eSPI PR channel
- Support ACPI IPMI operation region in system definition tables
- Support accesses to BMC power meters

```
[ 5.429923] riscv-aplic RSCV0002:00: 511 interrupts forwarded to MSI base 0x0000005586000000
[ 5.468665] IPMI message handler: version 39.2
[ 5.481225] ipmi device interface
[ 5.670716] ipmi_si: IPMI System Interface driver
[ 5.688403] ipmi_si IPI0001:00: ipmi_platform: probing via ACPI
[ 5.706054] ipmi_si IPI0001:00: ipmi_platform: [mem 0x53fe00ca2 window] register 1 spacing 1 irq 13
[ 82.322779] Freeing initrd memory: 18476K
[ 82.424998] ipmi_si: Adding ACPI-specified kcs state machine
[ 82.444542] ipmi_si: Trying ACPI-specified kcs state machine at mem address 0x53fe00ca2, slave address 0x0, irq 13
[ 83.084217] ipmi_si IPI0001:00: The BMC does not support clearing the recv irq bit, compensating, but the BMC needs to be fixed.
[ 83.628675] ipmi_si IPI0001:00: Using irq 13
[ 83.759773] ipmi_si IPI0001:00: Error clearing flags: c1
[ 84.498262] ipmi_si IPI0001:00: IPMI message handler: Found new BMC (man_id: 0x00a741, prod_id: 0x424f, dev_id: 0x00)
[ 87.328451] ipmi_si IPI0001:00: IPMI kcs interface initialized
[ 89.942581] Serial: 8250/16550 driver, 4 ports, IRQ sharing disabled
[ 90.031293] serial8250 RSCV0003:00: error -ENXIO: IRQ index 0 not found
```

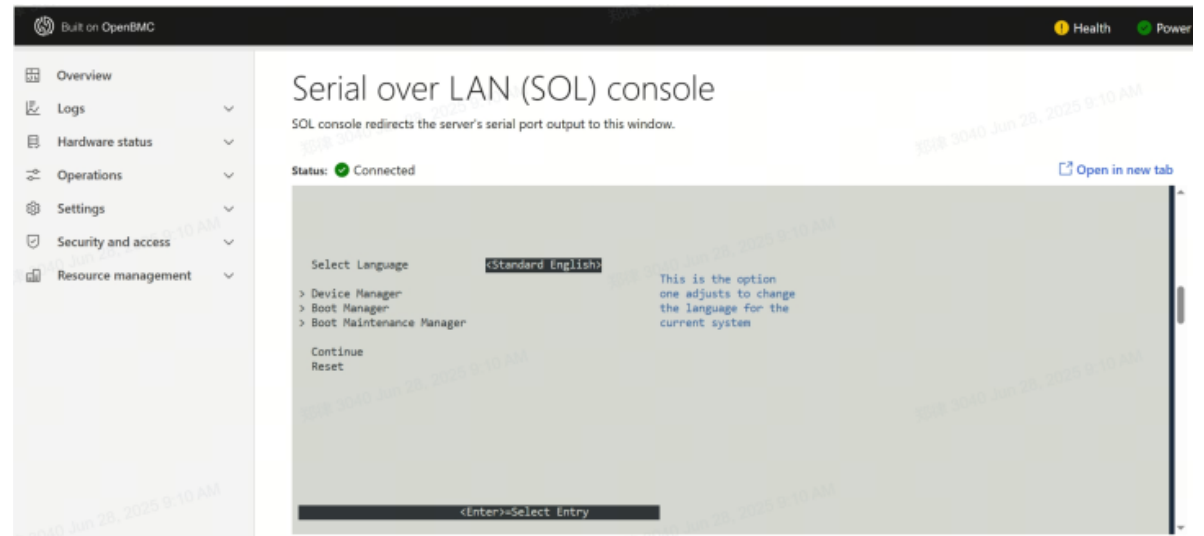
```
sdfirm> kcs xfer 2 63 0x6 0x1
00000000 00000000000000106 0000000000000000 |.....|
00000010 00000000000000000 0000000000000000 |.....|
Command success 'kcs - 0'
```



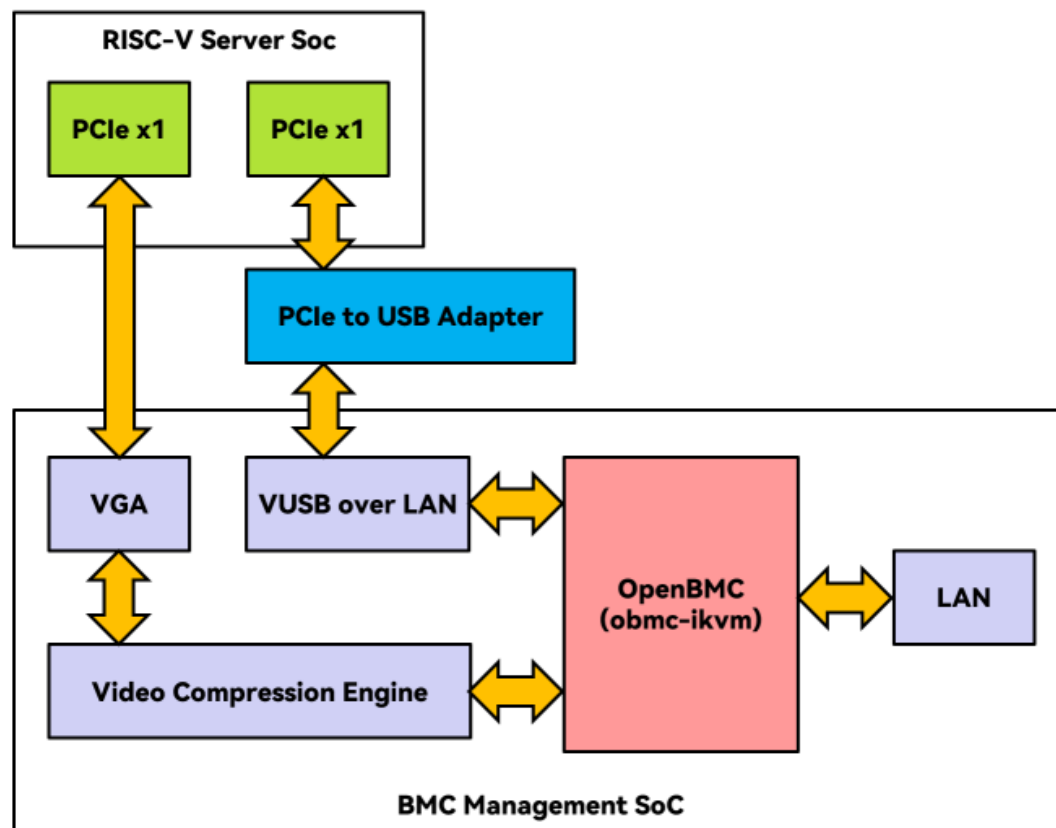
BMC Feature – SOL



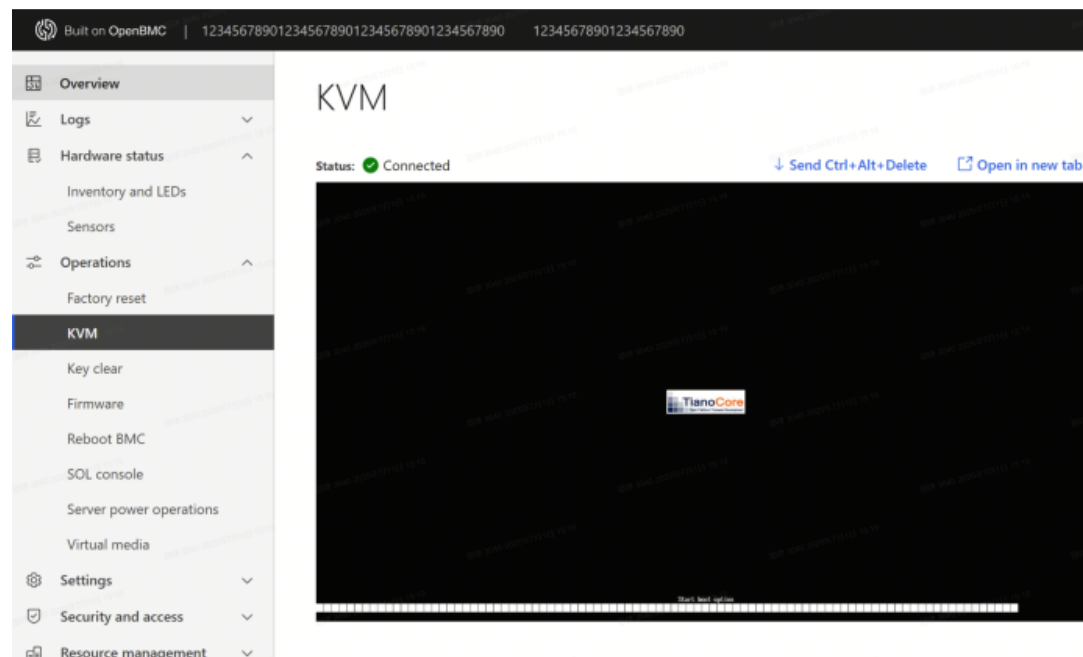
- Support remote OS install, BIOS setup, etc. using CUI
- Enable BMC IPMI SOL (serial over LAN) console using LPC/eSPI adapters
- Support super IO peripherals in UEFI
- Support UART based on SIO/SERIRQ in UEFI



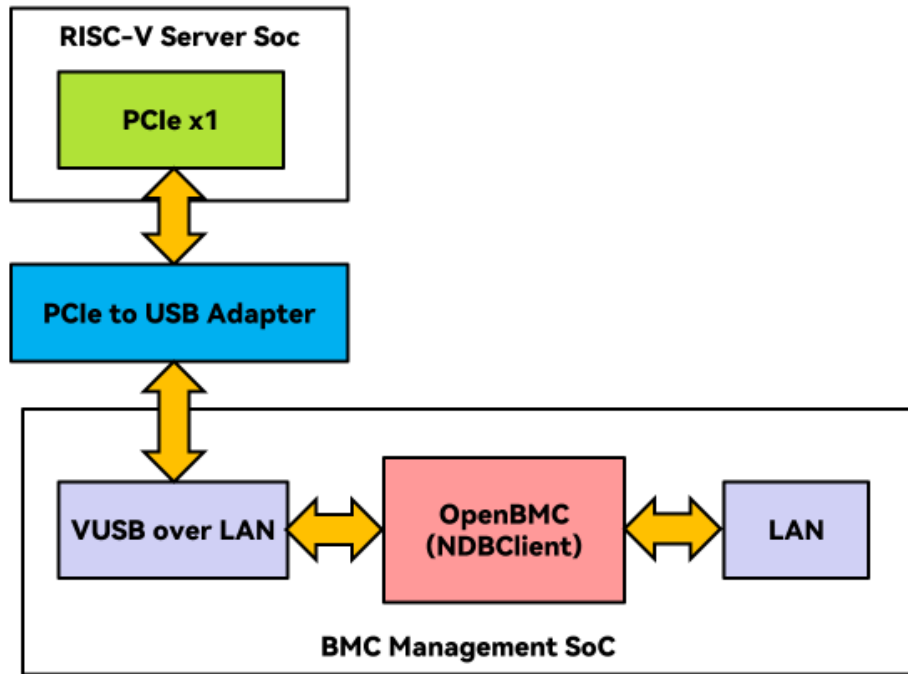
BMC Feature – KVM



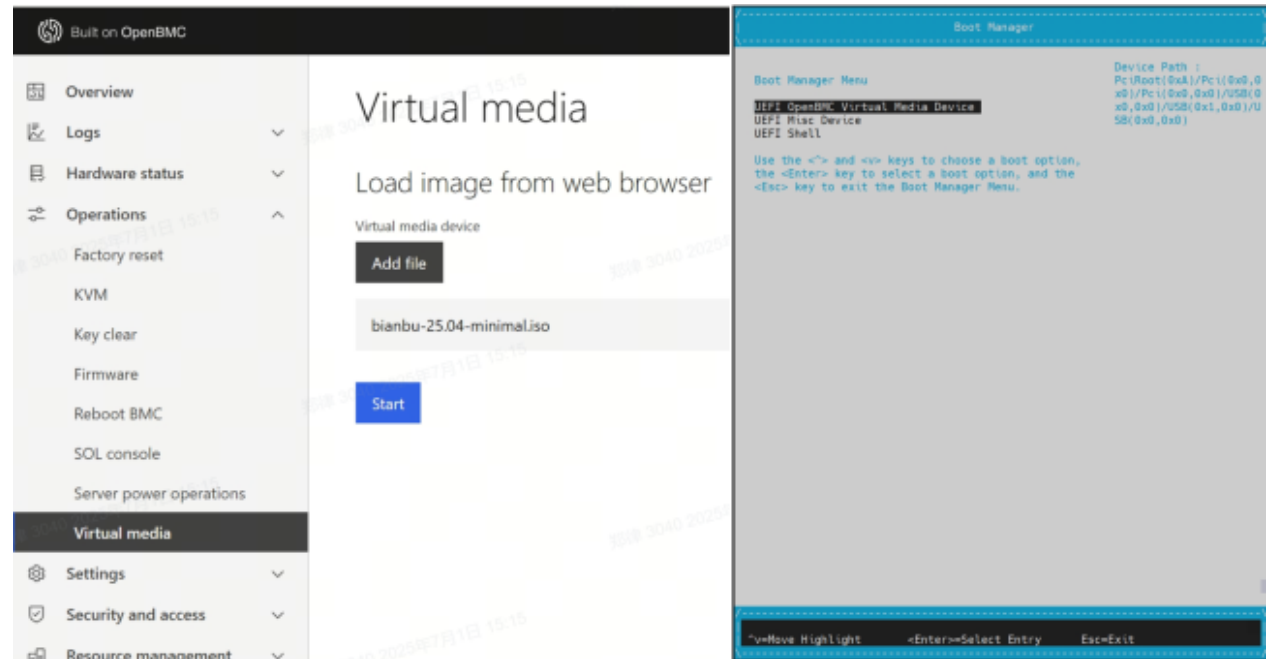
- Support remote OS install, BIOS setup, etc. using GUI
- Enable BMC KVM (keyboard, video, mouse) over IP using dedicated PCIe adapters
- Support USB over LAN protocol using virtual USB
- Support graphics compression into YUV420/YUV444



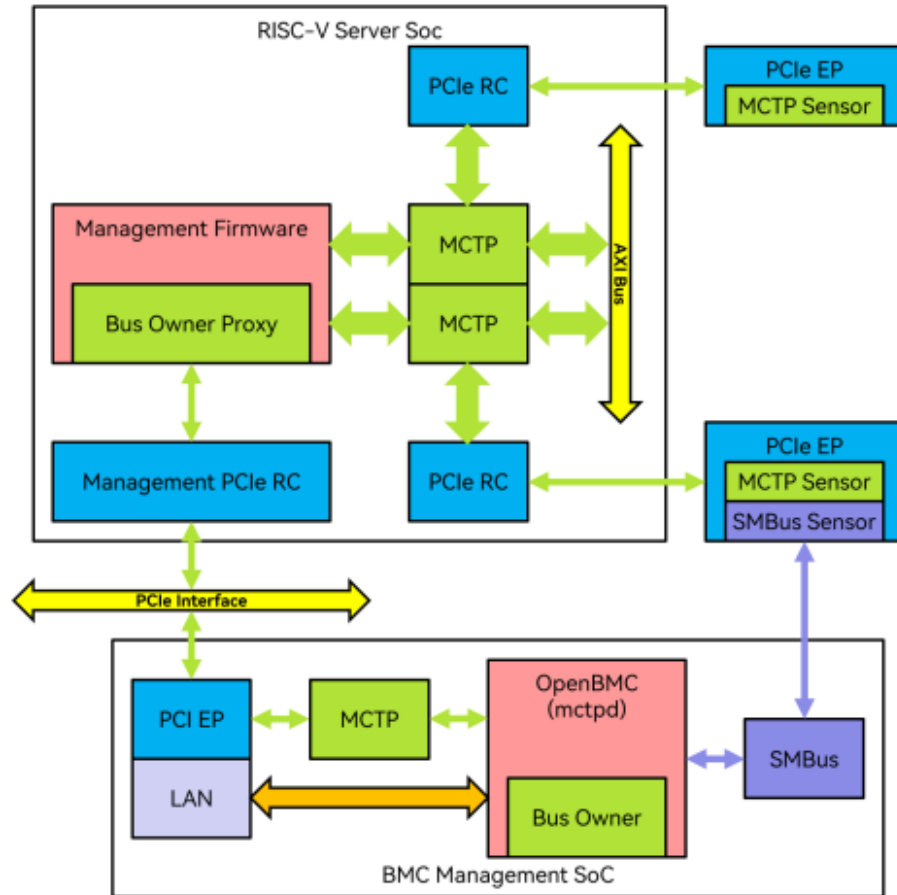
BMC Feature – Virtual Media



- Support remote operating system installation along with SOL and KVM
- Enable BMC USB virtual media using dedicated PCIe adapters
- Support USB over LAN protocol using virtual USB



BMC Feature – MCTP



```

mctp[10] rcv size: 20
get data:
410132808 01 10 00 73 7f 10 00 01 b4 1a 00 00 c8 08 ff 01 |...s.....|
410132818 00 80 0b 00 |....|

rcv mctp command[11]: Prepare Endpoint Discovery ctrl->rq: 1
tx status: 0x9
mctp[0] send done, size: 20
j_mctp[0] send size: 20

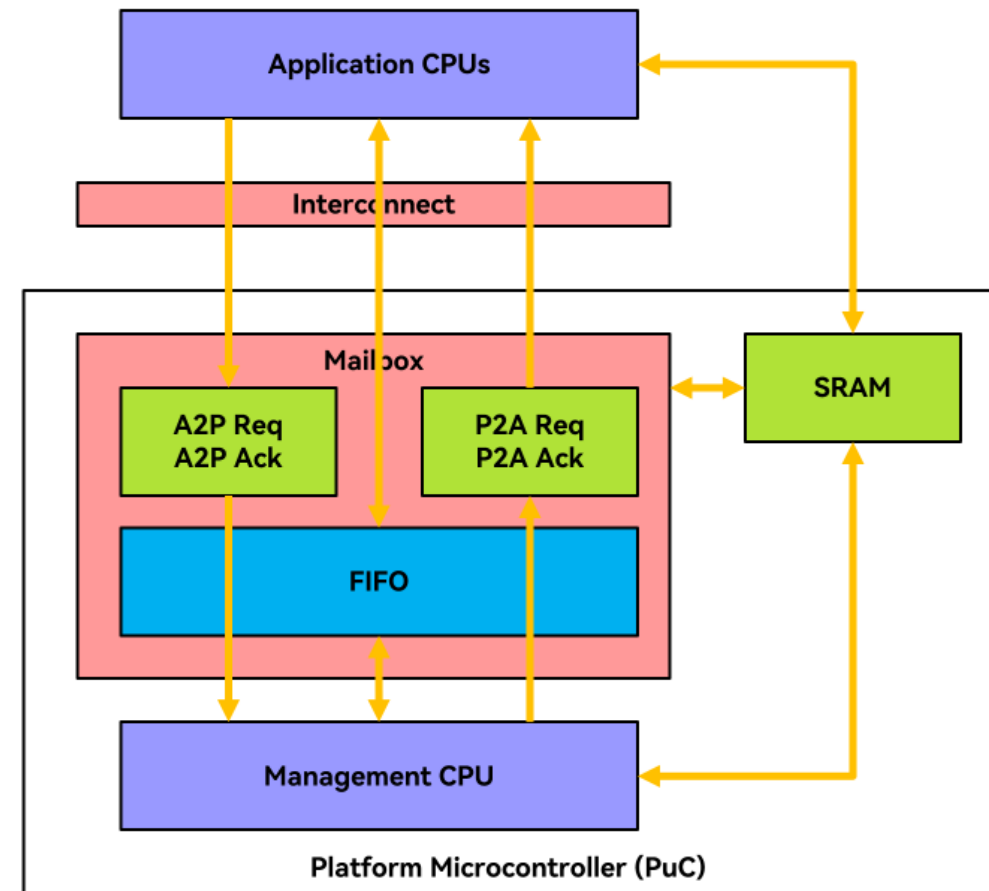
mctp[0] rcv size: 20
get data:
410132808 01 00 00 70 7f 00 00 01 b4 1a 00 00 c0 00 08 01 |...p.....|
410132818 00 00 0b 00 |....|

rcv mctp command[11]: Prepare Endpoint Discovery ctrl->rq: 0
tx status: 0x9
mctp[10] send done, size: 20
j_mctp[10] send size: 20
-----
mctppcie0 Link encap:UNSPEC HWaddr 00-00-30-30-30-30-00-30-00-00-00-00-00-00-00-00
UP RUNNING MTU:1024 Metric:1
RX packets:3 errors:0 dropped:0 overruns:0 frame:0
TX packets:3 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1100
RX bytes:432 (432.0 B) TX bytes:64 (64.0 B)
    
```

- Management firmware programs PCIe VDM routing to/from AXI memory between RCs
- Management firmware acts as MCTP bus owner proxy and BMC acts as MCTP bus owner and bridge
- Demonstration:
 - MCTP EP discovery request and response
 - MCTP probed interface on BMC evaluation board

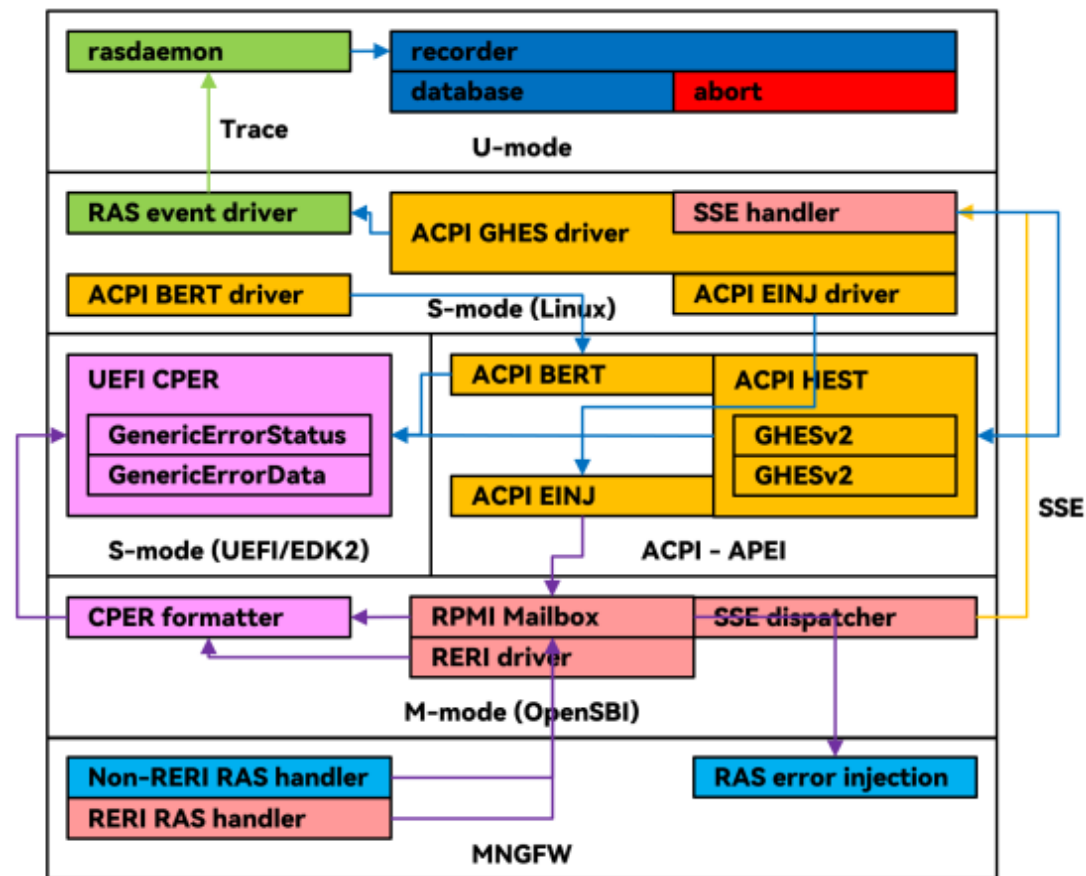
RISC-V Feature – RPMI

- RISC-V RPMI compliant mailbox
 - Support secure/non-secure world specific mailbox slots
 - Support 16KB per-world external SRAM based message channels
 - Support per-world P2A/A2P REQ/ACK doorbell interrupts
- Additional FIFO based mailbox
 - Support secure/non-secure world specific mailbox slots
 - Support up to 16 mailbox slots and up to 8 users per-world
 - Support 8*32-bit FIFO based message per-channel (slot)



RAS Overview

- RAS ACPI/APEI compliance
 - BERT
 - HEST
 - EINJ
- RAS EFI compliance
 - CPER
- RAS RISC-V compliance
 - RERI
 - RPMI
 - SSE
- Hardware RAS sources
 - CPU
 - IOMMU
 - DDR
 - PCIe
 - ECC SRAM



RAS Feature – ACPI/APEI

- Support pre-silicon stubbed EFI memory descriptor, system table and memory mapping embedded in SBI firmware
- Support pre-silicon lightweight ACPI tables embedded in SBI firmware
- Support compile time ACPI table modification via preprocessor
- Support runtime ACPI table modification via EFI SDTs (system definition tables) protocol in SBI firmware
 - Support SBI bootstrap fixup of ACPI data tables and SDTs
 - Support partial goods fixup of ACPI processor and interrupts in xSDTs
- Support automatic APEI/HEST table generation directly from RERI and other errors indirectly reported via RPM1

```
SOF FIRM
acpi_bios: 000000000030958 - 000000000030990
acpi_bios: installing [FACP] at 0000000001201f88
acpi_bios: skipping [RSD ] at 0000000001201f00
acpi_bios: skipping [XSDT] at 0000000001201f24
acpi_bios: skipping [FACP] at 0000000001201f88
acpi_bios: skipping [DSDT] at 000000000120209c
acpi_bios: installing [RHCT] at 00000000012029de
acpi_bios: installing [APIC] at 00000000012030a2
acpi_bios: installing [SPCR] at 0000000001203bbc
acpi(0): [NS-0000000000c8050-\_] INIT
acpi(0): [NS-0000000000c80a8-\_SB_] INIT
acpi(0): [NS-0000000000c8050-2-\_] INC(object)
acpi(0): [NS-0000000000c8100-\_TZ_] INTT
```

```
0.000000] SBI specification v2.0 detected
0.000000] SBI implementation ID=0x1 Version=0x10004
0.000000] SBI TIME extension detected
0.000000] SBI IPI extension detected
0.000000] SBI DBCN extension detected
0.000000] efi: EFI v2.3 by SpacemiT
0.000000] efi: ACPI 2.0-0x1201f00
0.000000] ACPI: Early table checksum verification disabled
0.000000] ACPI: RSDP 0x0000000001201f00 00002c (v02 SPACET)
0.000000] ACPI: XSDT 0x0000000001201f24 000044 (v01 SPACET SERVER 00000001 INTL 20250404)
0.000000] ACPI: FACP 0x0000000001201f88 000114 (v06 SPACET SERVER 00000000 00000000)
0.000000] ACPI: DSDT 0x000000000120209c 000942 (v02 SPACET SERVER 00000001 INTL 20250404)
0.000000] ACPI: RHCT 0x00000000012029de 0006c4 (v01 SPACET SERVER 00000001 INTL 20250404)
0.000000] ACPI: APIC 0x00000000012030a2 000b1a (v07 SPACET SERVER 00000001 INTL 20250404)
0.000000] ACPI: SPCR 0x0000000001203bbc 00005a (v04 SPACET SERVER 00000000 INTL 20250404)
0.000000] ACPI: SPCR: console: uart,mio32,0x53c00000
0.000000] earlycon: uart0 at MMIO32 0x0000000053c00000 (options '')
0.000000] printk: legacy bootconsole [uart0] enabled
0.000000] DF: reserved mem: 0x0000000000000000..0x0000000000000000 (2048 KiB) nonrap non-reusable mmode_pmp000
0.000000] Zone ranges:
0.000000] DMA32 [mem 0x0000000000000000-0x0000000000000000]
0.000000] Normal empty
```



RAS Feature – CPU RERI

RERI Errors	CPER Error Type	CPER Error Severity	CPER Other Info
L2Cache SnoopFilter ECC Error (CE/UUE)	0x00: Unknown	2 – Corrected 1 - Fatal	Processor Type: RISC-V Processor ISA: RISC-V 64
L2Cache TAG ECC Error (CE/UUE)	0x01: Cache Error	2 – Corrected 1 - Fatal	
L2Cache DATA ECC Error (CE/UDE)	0x01: Cache Error	2 – Corrected 0 - Recoverable	
CoreX IFU Consume Poison (UUE)	0x00: Unknown	1 - Fatal	
CoreX ICACHE TAG Parity Error (CE)	0x01: Cache Error	2 - Corrected	
CoreX ICACHE DATA Parity Error (CE)	0x01: Cache Error	2 - Corrected	
CoreX jTLB TAG Parity Error (CE)	0x02: TLB Error	2 - Corrected	
CoreX jTLB DATA Parity Error (CE)	0x02: TLB Error	2 - Corrected	
CoreX LSU Consume Poison (UUE)	0x00: Unknown	2 – Corrected 1 - Fatal	
CoreX DCACHE TAG ECC Error (CE/UUE)	0x01: Cache Error	2 – Corrected 1 - Fatal	
CoreX DCACHE DATA ECC Error (CE/UCE)	0x01: Cache Error	2 – Corrected 0 - Recoverable	



RAS Feature – IOMMU RERI

Errors	CPER Error Type	CPER Error Severity	CPER Other Info
IOATS Configuration cache (CFGC) data parity and CRC	0x02: TLB Error	2 - Corrected	Control register Status register
IOATS Configuration cache (CFGC) tag parity and CRC	0x02: TLB Error	2 - Corrected	
IOATS 1 st stage level- X page table walk cache (PTWC SL X) data parity and CRC	0x02: TLB Error	2 - Corrected	
IOATS 1 st stage level- X page table walk cache (PTWC SL X) tag parity and CRC	0x02: TLB Error	2 - Corrected	
IOATS 2 nd stage level- X page table walk cache (PTWC GL X) data parity and CRC	0x02: TLB Error	2 - Corrected	
IOATS 2 nd stage level- X page table walk cache (PTWC GL X) tag parity and CRC	0x02: TLB Error	2 - Corrected	
IOATC Main TLB (MTLB) data parity and CRC	0x02: TLB Error	2 - Corrected	
IOATC Main TLB (MTLB) tag parity and CRC	0x02: TLB Error	2 - Corrected	



RAS Feature – DDR

DDR Errors	CPER Error Type	CPER Error Severity	CPER Other Info
Derate temperature limit error	0 - Unknown	3 – Informational	
Command error	0 - Unknown	0 - Recoverable	
Control update error	0 - Unknown	1 – Fatal	
Refresh management alert	0 - Unknown	3 – Informational	
ECC CE	2 - Single-bit ECC	2 – Corrected	
ECC UE	3 - Multi-bit ECC	1 – Fatal	
DDR write CRC error	8 - Parity Error	0 – Recoverable	Physical address Physical address mask
DDR write CRC err max reached error	8 - Parity Error	1 – Fatal	Bank Row
DDR write CRC retry limit error	8 - Parity Error	1 – Fatal	Column Rank
DDR read CRC max reached error	8 - Parity Error	1 – Fatal	Bit position Chip identification
DDR read retry limit error	8 - Parity Error	1 – Fatal	
CA parity retry limit reached error	8 - Parity Error	1 – Fatal	
CA parity FATL error	8 - Parity Error	1 – Fatal	
Write Buffer CHI Port X RAM Y parity error	8 - Parity Error	0 – Recoverable 1 – Fatal	
Read Buffer CHI Port X RAM Y parity error	8 - Parity Error	0 – Recoverable 1 – Fatal	



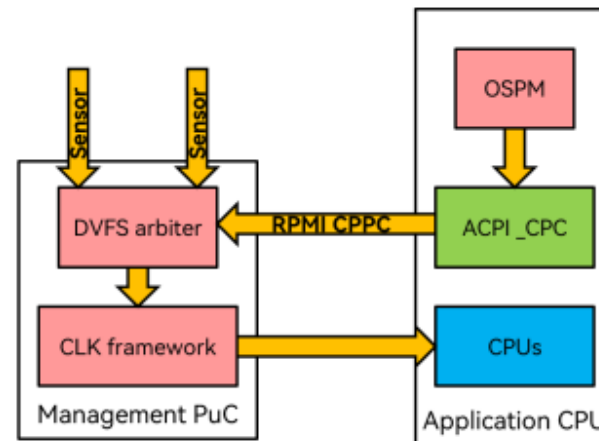
RAS Feature – Others

Module	Error	CPER Error Type	CPER Error Severity	CPER Other Info
PCIe	PCIe advanced error reporting CE	PCIe AER Capability: <ul style="list-style-type: none"> Physical Layer Data Link Layer Transaction Layer 	2 – Corrected	Port Type Device ID Command Status Device Serial Number Capability Structure
	PCIe advanced error reporting UE		1 – Fatal	
SRAM	SEC event	2 - Single-bit ECC	2 – Corrected	Physical address Physical address mask Bit position
	DED event	3 - Multi-bit ECC	1 – Fatal	
BUS	SnoopFilter tag ECC (SECDED)	Corrected Error (CE) Deferred Error (DE)	2 – Corrected 0 – Recoverable	Error status Error addresses
	LLC tag ECC (SECDED)	Corrected Error (CE) Uncorrected Error (UE)	2 – Corrected 1 - Fatal	
	LLC data ECC (SECDED)	Corrected Error (CE) Deferred Error (DE)	2 – Corrected 0 – Recoverable	
	Error request type detect	Deferred Error (DE)	0 – Recoverable	
	AXI/ACE lite write data poison detect	Uncorrected Error (UE)	1 – Fatal	
	AXI/ACE lite write data error	Deferred Error (DE)	0 – Recoverable	
	AXI/ACE lite write response error (BRESP)	Uncorrected Error (UE)	1 – Fatal	



DVFS Feature – ACPI cpufreq

```
[ 70.596095] riscv-aplic RSCV0002:00: 511 interrupts forwarded to MSI base 0x00
00000558600000
[ 70.632310] ACPI CPPC: Parsed CPC struct for CPU: 0
[ 70.666634] suspend: HSM suspend not available
[ 70.692352] ACPI CPPC: Parsed CPC struct for CPU: 1
[ 70.712284] suspend: HSM suspend not available
[ 70.765939] ACPI CPPC: Parsed CPC struct for CPU: 4
[ 70.786472] suspend: HSM suspend not available
[ 70.814879] ACPI CPPC: Parsed CPC struct for CPU: 5
[ 70.835528] suspend: HSM suspend not available
[ 70.857715] ACPI CPPC: Checking ACPI CPC validity
[ 70.865554] ACPI CPPC: CPU2 CPC descriptor is NULL
[ 70.873616] ERST DBG: ERST support is disabled.
[ 70.880993] SBI CPPC extension detected
[ 70.886813] SBI MPXY extension not available
[ 73.854227] Serial: 8250/16550 driver, 1 ports, IRQ sharing disabled
[ 73.907865] printk: legacy console [ttyS0] disabled
[ 73.926049] HISI0031:00: ttyS0 at MMIO 0x53c000000 (irq = 11, base_baud = 6250
00) is a 16550A
[ 73.939818] printk: legacy console [ttyS0] enabled
[ 73.939818] printk: legacy console [ttyS0] enabled
[ 73.952866] printk: legacy bootconsole [uart0] disabled
[ 73.952866] printk: legacy bootconsole [uart0] disabled
[ 74.016096] suspend: HSM suspend not available
[ 74.455415] CPPC Cpuufreq: Initializing CPPC CPUfreq driver
[ 74.463094] CPPC Cpuufreq: Registering CPUfreq driver
[ 74.472168] CPPC Cpuufreq: Initializing CPU0
[ 74.478716] CPPC Cpuufreq: CPU0 performance caps - lowest: 40, lowest_nonlinear
: 40, nominal: 104, highest: 104
[ 74.490338] CPPC Cpuufreq: CPU0 frequency range - min: 1000000 kHz, max: 200000
0 kHz
[ 74.499437] CPPC Cpuufreq: CPU0 using independent policy
[ 74.505989] CPPC Cpuufreq: CPU0 fast_switch: disabled, dvfs_from_any_cpu: enabl
ed
[ 74.514817] CPPC Cpuufreq: CPU0 setting initial performance to 104 (freq: 20000
00 kHz)
[ 74.525120] CPPC Cpuufreq: CPU0 initialization completed successfully
```



- Support ACPI CPPC (collaborative processor performance control)
- OS PM invokes `_CPC` control method in system definition tables
- RISC-V specific RPMI channel is used to send/receive CPPC request/response
- PuC firmware arbitrates frequency requests ceiling/floor, manipulates power and frequency using PID algorithm
- PuC firmware invokes clock tree management framework to manipulate CPU frequency dynamically

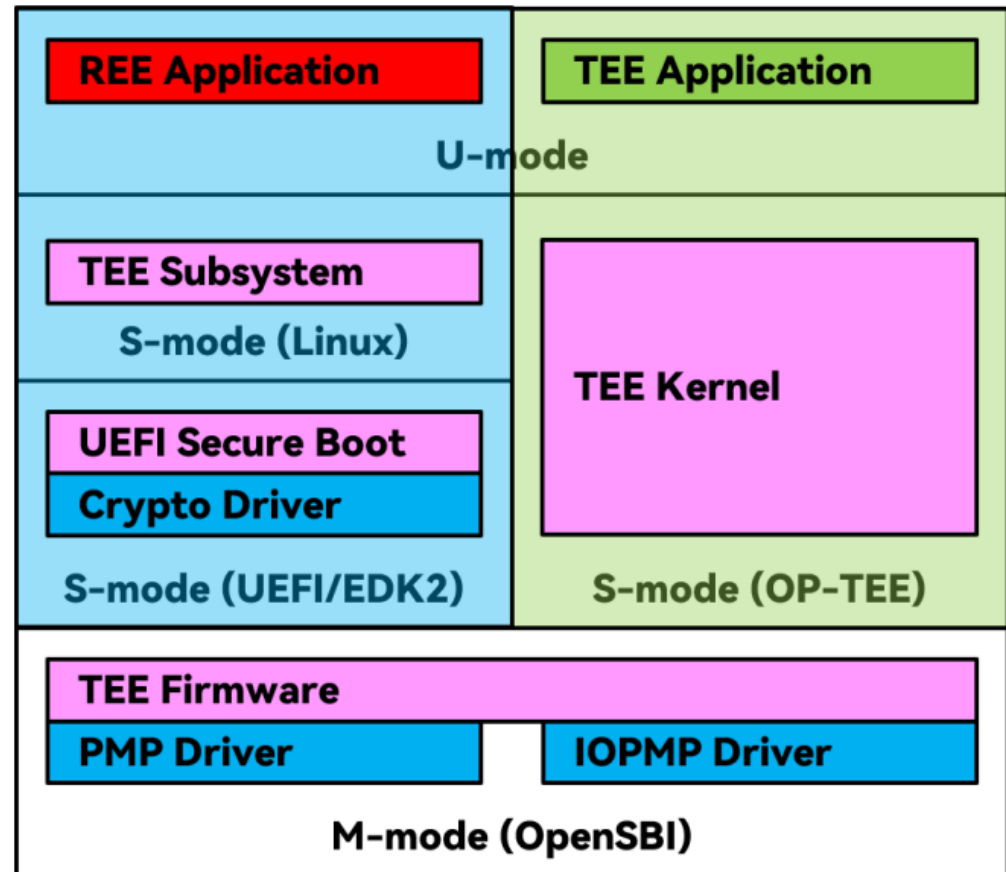


03

Security

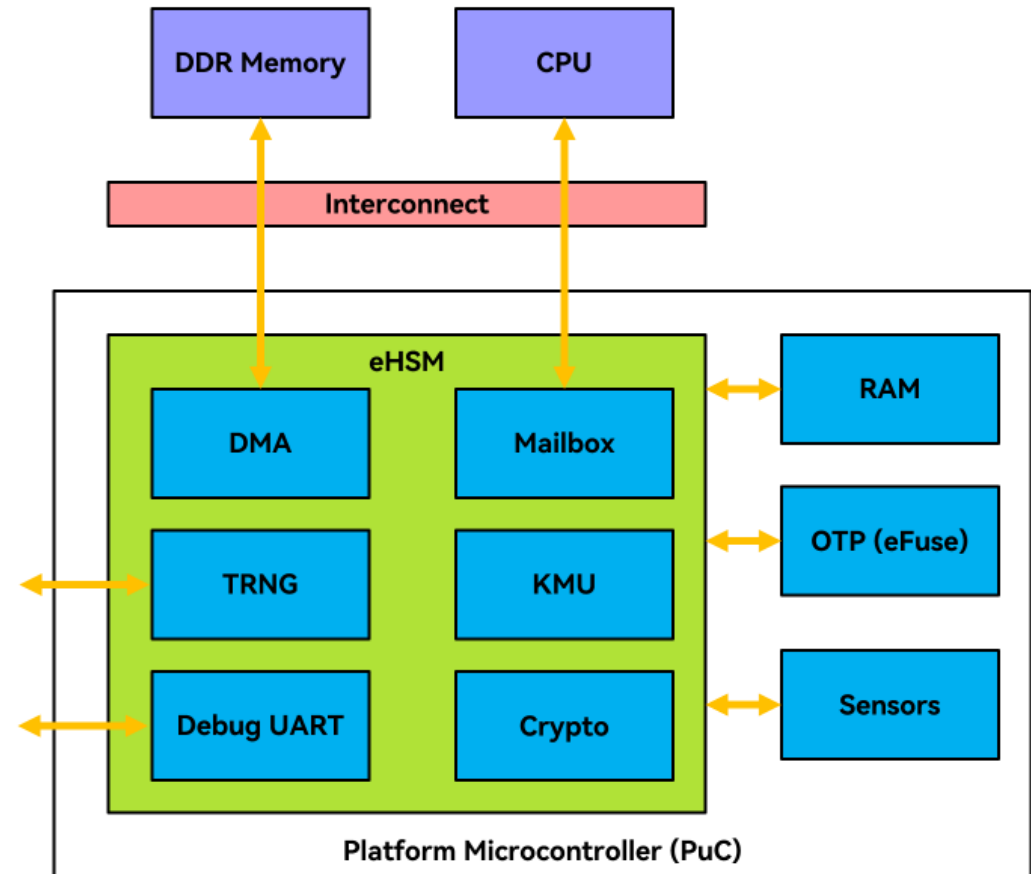
Security – PMP/IOPMP

- Support CPU secure enclave via up to 16 entries of PMP
- Support I/O secure enclave via IOPMP instantiated for each I/O subsystem, each instantiated IOPMP
 - Support up to 32 entries
 - Support up to 64 MD and totally up to 1024 entries
 - Support up to 1024 device IDs
- Support GP-TEE compliant TEE OS (OP-TEE)
- Support secure boot in UEFI and OpenSBI



Security – eHSM

- OSCCA (Office of the State Commercial Cryptographic Administration) Chinese commercial cryptography scheme - level 1 compliance
- Support running up to 600MHz frequency
- Support security algorithm of hashing, symmetric and asymmetric encryption
- Support key management utility (KMU) to store keys in OTP/RAM
- Support TRNG
- Support security sensors
 - Active shield
 - Temperature sensor
- Support secure debugging



04

Performance

Performance Monitors – CPU HPM

X100 Event			
Stalled-backend	Stalled-frontend	Branch-instructions	L1Dcache-loads
L1Dcache-stores	L1Dache-prefetches	Icache-accesses	Icache-prefetches
L2-loads	L2-stores	L2-prefetches	DTLB-loads
DTLB-stores	DTLB-prefetches	ITLB-accesses	Branch-misses
L1Dcache-load-misses	L1Dcache-store-misses	L1Dcache-prefetch-misses	L2-load-misses
L2-store-misses	L2-prefetch-misses	DTLB-load-misses	DTLB-store-misses
DTLB-prefetch-misses	ITLB-load-misses		



Performance Monitors – IOMMU HPM

IOATS Events	
Untranslated requests	Page table walk cache requests
Translated requests	Configuration cache misses
DTI_ATS translation requests	Page table walk cache misses
DTI_TBU translation requests	All translation requests
Device directory walks	All translations buffered
Process directory walks	Configuration cache lookups
1 st stage page table walks	1 st stage level-X page table walk cache lookups
2 nd stage page table walks	1 st stage level-X page table walk cache misses
DTI_ATS page requests (PRI)	2 nd stage level-X page table walk cache lookups
Configuration cache requests	2 nd stage level-X page table walk cache misses

IOATC Events	
Untranslated (ATST=0) requests	Write transactions unissued of write buffer full
Translated (ATST=1) requests	Write transactions using write buffer
TLB misses	Write transactions not using write buffer
All translation requests	Main TLB (MTLB) lookups
Transactions issued	Main TLB (MTLB) misses
Transactions unissued of slot drain	Micro TLB (uTLB) lookups
Transactions unissued of token drain	



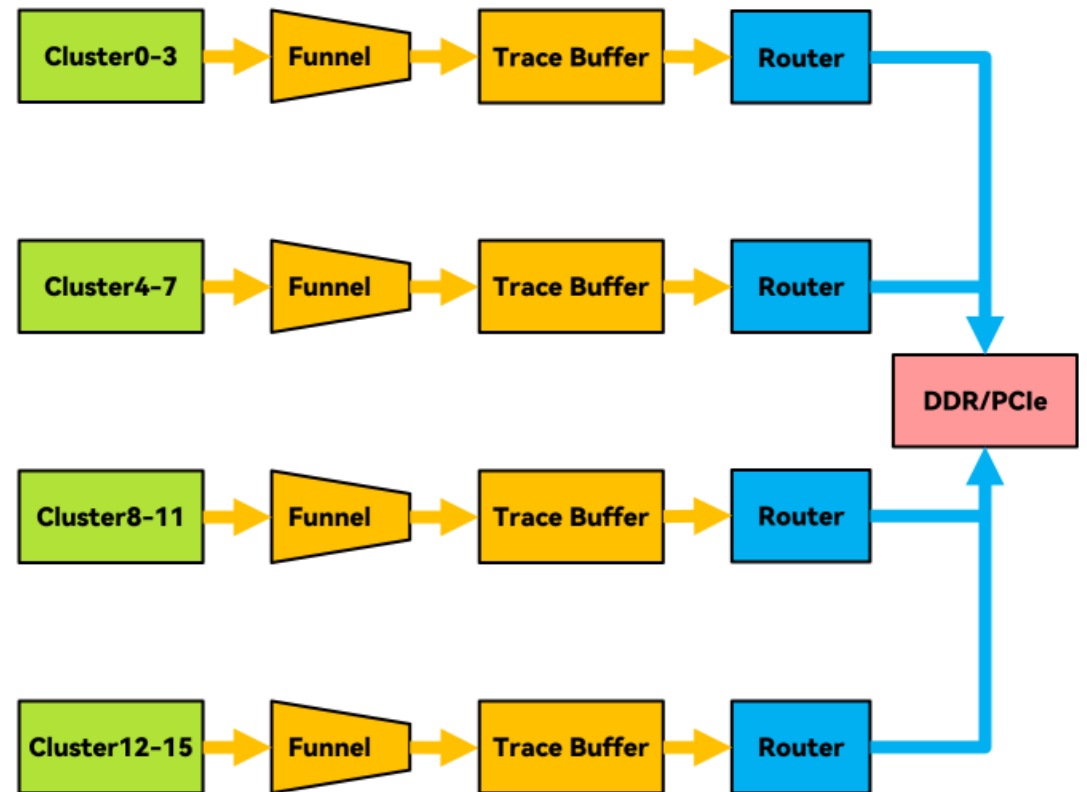
Performance Monitors - DDR

DPM Events	
Effective reads	Write combines
Effective writes	Visible window limitation reached reads
Bypass reads	Visible window limitation reached writes
Bypass activations	Scheduler allocations
DFI read data cycles	Scheduler starvations
DFI write data cycles	Channel based command counting
Type specific op counting	CHI requests dropped
Prioritized transactions when critical	WAR hazards
Precharges	RAW hazards
Read transitions	WAW hazards
Write transitions	



Tracers – CPU N-Trace

- Support RISC-V Nexus based trace (N-Trace) encoder and control interfaces
- Support APB and JTAG DP accesses of N-Trace control interfaces
- Support up to 312.5MHz CPU trace source frequency
- Support up to 300MHz trace channel frequency
- Support 32 depth FIFO based trace buffer
- Support routing trace data to memory and PCIe trace peripherals
- Support trace timestamping

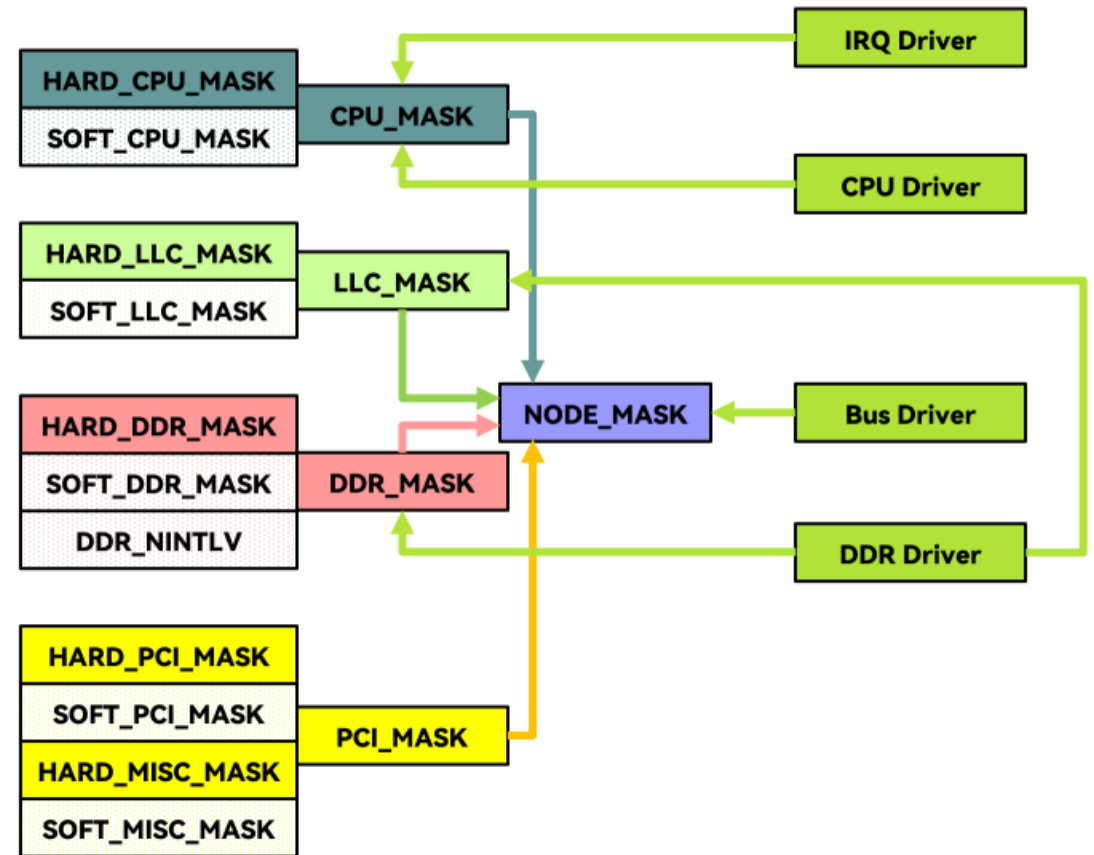


05

Other Features

Yield – Partial Goods

- Support ATE software calibration of CPU/LLC/DDR masks
- Support ATE hardware eFuse of CPU/LLC/DDR masks
- Support hardware integration of Big-Little CPU cores
- Support automatic hardware bus nodes enumeration
- Support pre-silicon various hardware simulation configurations



Yield – Partial Goods

- Support automatic software adaption of DDR interleave and cache groups configurations
- Support automatic software adaption of CPU clock and power gating
- Support automatic software fixup of device tree CPUs and interrupts
- Support automatic software fixup of ACPI firmware CPUs and interrupts
- Support Big-Little architecture to integrate community opensource cores



```
n100: CPU_MASK: 1000000000000013
n100: DDR_MASK: 00000000FFFFFFF01
n100: LLC_MASK: 00000000FFFFFFF
n100: HW_CPU_MASK0: 00000000FFFFFFfec
n100: HW_CPU_MASK1: 00000000eFFFFFFF
n100: HW_DDR_MASK: 00000000000000fe
n100: HW_LLC_MASK: 0000000000000000
n100: HW_PCIE_MASK: 00000000000000ff8
n100: SW_CPU_MASK0: 0000000000000000
n100: SW_CPU_MASK1: 0000000000000000
n100: SW_DDR_MASK: 0000000000000000
n100: SW_LLC_MASK: 0000000000000000
n100: SW_PCIE_MASK: 0000000000000000
n100: NODE_MASK_0: 0000000057d42a00
n100: NODE_MASK_1: 00000000ac57d57d
root@sdfirm:~# grep -E '^hart|^mvendorid|^marchid' /proc/cpuinfo
hart : 0
mvendorid : 0x710
marchid : 0x8000000058000002
hart isa : rv64imafdcvh_zicbom_zicboz_zca_zcd_zve32f_zve32x_zve64d_zve64f_zve64x_smaia_smstateen_ssaia_sscopmf_svpbmt
hart : 1
mvendorid : 0x710
marchid : 0x8000000058000002
hart isa : rv64imafdcvh_zicbom_zicboz_zca_zcd_zve32f_zve32x_zve64d_zve64f_zve64x_smaia_smstateen_ssaia_sscopmf_svpbmt
hart : 4
mvendorid : 0x710
marchid : 0x8000000058000002
hart isa : rv64imafdcvh_zicbom_zicboz_zca_zcd_zve32f_zve32x_zve64d_zve64f_zve64x_smaia_smstateen_ssaia_sscopmf_svpbmt
hart : 60
mvendorid : 0x0
marchid : 0x19
hart isa : rv64imafdcvh_zicbom_zicboz_zca_zcd_zve32f_zve32x_zve64d_zve64f_zve64x_smaia_smstateen_ssaia_sscopmf_svpbmt
root@sdfirm:~#
```



Bootstrap – TCM

- Boot EFI BIOS to DDR address space while still can have DDR driver in the BIOS
 - Configure TCM as memory located in the very first segment of DDR memory regions
 - Reconfigure TCM as CPU cache and leave memory regions for DDR
 - DDR driver runs between TCM initialization and finalization
- Run post-silicon tests by using TCM while DDR is not available
 - Run rich-featured ATE functional test patterns using TCM while can still save silicon area with limited SRAM
 - Reduce TTM during post-silicon validation by running operating system tests using TCM prior to DDR availability

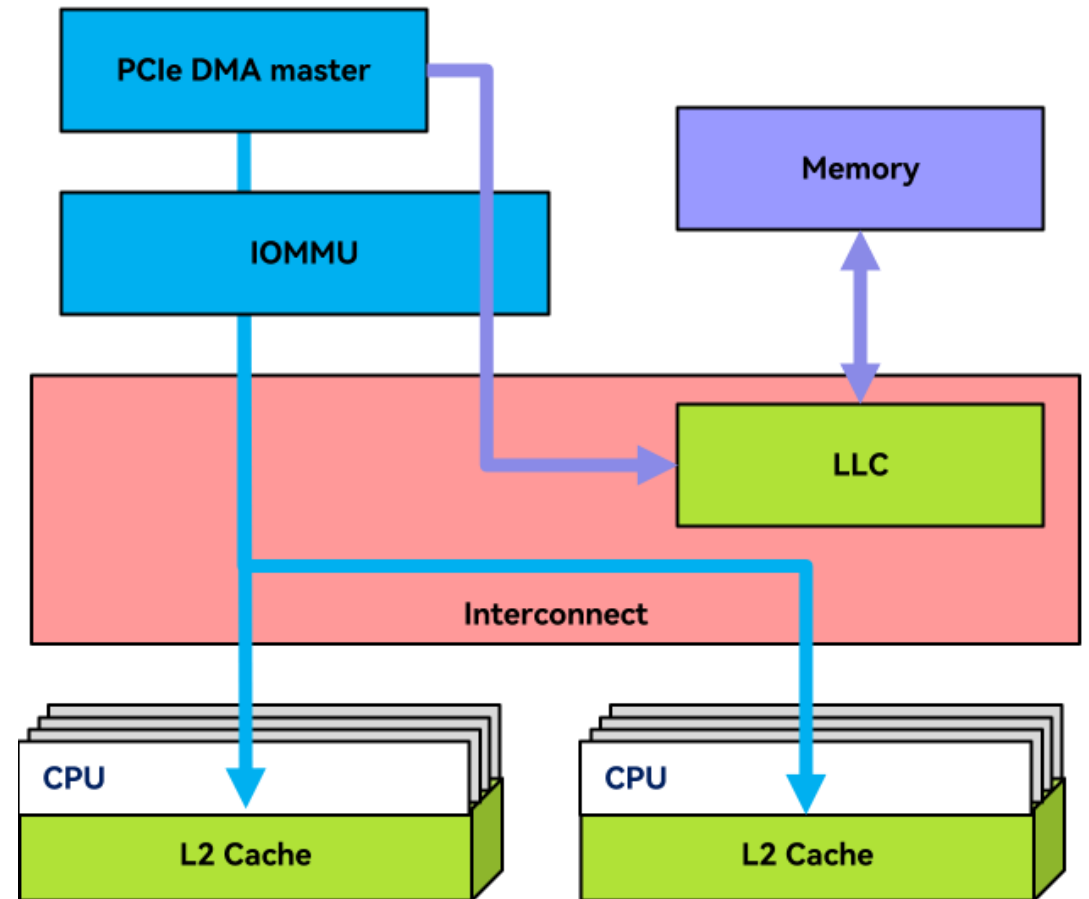
```
partial_good(0): Applying partial goods: 0x33.
[TCM_INIT] TCM initialized.
[TCM_INIT] CHIP_INIT_OCM flag set.
boot(spi): Booting bbl.bin to entry=0x1000...
00000200 45 46 49 20 50 41 52 54 00 00 01 00 5c 00 00 00 |EFI PART....\...|
00000210 61 e6 a1 95 00 00 00 00 01 00 00 00 00 00 00 00 |a.....|
boot(spi): Booting bbl.bin from addr=0x100000, size=0x1808778...
[TCM_EXIT] TCM finalized.
cru: E cluster0_clk
cru: E cpu_clk
cru: E cpu_sub_rstn
cru: E c0_core0_rst_n
cru: E cluster0_clk
cru: E cpu_sub_rstn
cru: E c0_core1_rst_n
cru: E cluster1_clk
cru: E cpu_sub_rstn
cru: E c1_core0_rst_n
lru: E c
uSpatecrelm_icTl k-
tSpacrcue:m iET cKpluM_asturbi_xr sStyns
)em cBriun:a rEy cIln_tceorrfaeic_er s(ts_BnI
Loader
6.2.0-36-generic - 1.0.0.0

[ 0.000000] Linux version 6.12.0-sdfirm (lijoey@SW-Station) (riscv64-unknown-
linux-gnu-gcc (g09b62c20e09) 13.2.1 20240423, GNU ld (GNU Binutils) 2.42) #1 SMP
Sun May 25 09:57:47 CST 2025
[ 0.000000] Machine model: riscv-spacemit
[ 0.000000] SBI specification v1.0 detected
[ 0.000000] SBI implementation ID=0x1 Version=0x10004
[ 0.000000] earlycon: sbi0 at I/O port 0x0 (options '')
[ 0.000000] printk: legacy bootconsole [sbi0] enabled
[ 0.000000] OF: reserved mem: 0x0000000000001000..0x0000000000100fff (1024 Ki
B) nomap non-reusable mmode_pmp@1000
```



Data Plane – Cache Stashing

- Support CHI snoop style dataless cache stashing transactions directed to L2 cache in X100 CPU cluster
 - SnpUniqueStash
 - SnpMakeInvalidStash
 - SnpStashShared
 - SnpStashUnique
- Support pass-through CHI dataless cache stashing transactions in T100 IOMMU
 - WriteUniquePtIStash
 - WriteUniqueFullStash
 - StashOnceShared
 - StashOnceUnique
- Support CHI dataless cache stashing transactions in PCIe controllers
 - WriteUniquePtIStash (TH=1)





Thanks

以RISC-V架构数智未来
RISC-V ARCHITECTURE FOR INTELLIGENT FUTURE

进迭时空（杭州）科技有限公司

SPACEMIT (Hangzhou) Technology Co., Ltd

PHONE: 0571-89000775

WEBSITE: www.spacemit.com

ADDRESS: Room 701, Block b, Future Center, Wuchang Street, Yuhang District, Hangzhou City, Zhejiang Province

