State of the Union & The Road Ahead

Spring 2022 RISC-V Week

Mark Himelstein
CTO, RISC-V
What we will discuss today

● 2021
● How we did it?
● 2022
More than 12,000,000,000 RISC-V cores deployed for profit!
16 ratified ISA Specifications Consisting of 44 Extensions!
10 Committees,
17 SIGs
19 Task Groups
How we did it?
Why RISC-V?

- Cost
- Flexibility
- Ecosystem
- Our position in History
- EDA Renaissance
- Pride of Ownership
## Privileged Software HC

<table>
<thead>
<tr>
<th>Components</th>
<th>Interfaces</th>
<th>Operating Systems</th>
<th>Platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypervisors SIG</td>
<td></td>
<td>Operating Systems SIG</td>
<td>Platform SIG</td>
</tr>
<tr>
<td>Platform Security SIG</td>
<td></td>
<td>Android SIG</td>
<td>OS-A SEE TG</td>
</tr>
<tr>
<td>Unified Discovery TG</td>
<td></td>
<td>Linux/Rich OS SIG</td>
<td>OS-A PlatformTG</td>
</tr>
<tr>
<td>AIA TG</td>
<td></td>
<td>RRTOS SIG</td>
<td>RVM-CSIPCT TG</td>
</tr>
<tr>
<td>IOMMU TG</td>
<td></td>
<td>Distro Tools SIG</td>
<td>RVM-CSIPCT TG</td>
</tr>
<tr>
<td>Secure Boot TG</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PLIC VTG</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Components</th>
<th>Interfaces</th>
<th>Operating Systems</th>
<th>Platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Plat &amp; FW Services SIG</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>psABI TG (2022)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>UEFI VTG</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SBI VTG</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ACPI SIG</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SBI SIG</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AP-TEE TG</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**TODO**

**Active**

**Dotted line**
**SOC Infrastructure HC**

- IOMMU TG
- IOPMP TG
- SMPU TG

**TODO**
- Strategy
- Platform Interrupts
- Power Management Infrastructure

- Debug & Trace SIG
  - E-Trace Code
  - Debug 0.1x
  - Debug revision TG
  - E-Trace Data TG
  - Nexus TG

- RAS SIG
  - Functional Safety SIG
  - QoS SIG
  - E2E Data Integrity SIG
  - Error recording, reporting, isolation SIG

- TODO
  - Diagnosability
  - Recoverability
  - Data poisoning containment
  - PCIe error reporting

**Security HC**

- Crypto Vector TG
  - Crypto GOST-R TG
  - Security Model TG

- Security Response SIG
  - Blockchain SIG
  - Control Flow Integrity SIG
  - Microarchitecture Side Channel SIG

- Trusted Computing SIG
  - AP-TEE TG
  - Secure Boot TG

- Memory Safety SIG
  - IOPMP TG
  - SMPU TG
ISA Infrastructure HC

- Formal Specification
- Architecture Tests Strategy
- Architecture Tests SIG
- Simulators SIG
- Documentation SIG
- C/I Regression Tests SIG
- Performance Modeling SIG
- Golden Model SIG

Technology Sectors HC

- Embedded SIG
- Fast Interrupts TG
- Code Size TG
- psABI TG
- Packed SIMD TG
- Debug TG

Implementation Virtual HC

- Data Center SIG
- HPC SIG

TODO
- Networking
- Wireless
- Edge
- Automotive
- Embedded

Final Cost/Benefit/Completeness Checks by SW & Unpriv & Priv Committee chairs

Done

Todo

Active

Dotted line
Backlog

● Profiles

● Platforms
  ○ Supervisor Execution environment
    ■ Dependencies: Discovery, Debug, AIA, PLIC, IOMMU, ACLINT, CLIC, EABI, psABI, Watchdog, Arch Test Requirements

● ISA extensions
  ○ CSR, P, Zc, Zvfh, AIA, bfloat16, security, crypto vector, priv leftovers, Fast Interrupts
  ○ Never ratified but widely used: Ztso, PLIC, Zicntr, Zihpm
Beyond the Backlog

● Automotive
  ○ AGL & Yocto & Realtime
  ○ Functional Safety (ASIL, ISO 26262)

● Datacenter
  ○ Databases
  ○ Accelerators
    ■ Graphics & ML/AI/NLP
    ● Matrix Ops
  ○ Emulation Support
    ■ x86, Arm
  ○ Virtualization
  ○ Smart NICs

● ISA Gaps
  ○ RV32E, RV64E, RV128I
  ○ Software Ecosystem Libraries
  ○ Android

● Security
  ○ uArch
  ○ Robustness
  ○ Security Model
  ○ Ecosystem

● Ecosystem
  ○ 3rd party ISVs (e.g. VMware or OracleDB)
  ○ Libraries (security, graphics, etc.)
  ○ Distros
Rich RISC-V Ecosystem Available Today

HPC          Data Center          IoT          Networking

Applications
Infrastructure
Runtimes
Operating Systems
Hypervisor
Boot

Reliable, Serviceable, Diagnosable
Performant
Secure
Debuggable

Architecture
ISASAIL
Formal Model

CL/Testing
Perf Tools
Simulators
Compilers

Training
Research

Silicon
Soft IP

Compilation
Simulators
Perf Tools

Academia
Research

HPC
Consumer

RTC
DV

Implementation Design & Microarchitecture

OpenSBI

Architectural Tests

Spike
CI/Testing

Infrastructure

Applications

SAIL

HPC          Data Center          IoT          Networking

Performant
Secure
Debuggable

Reliable, Serviceable, Diagnosable

Services

Silicon
Soft IP

Compilers

Academia
Research

Training

HPC
Consumer

RTC
DV

Implementation Design & Microarchitecture

OpenSBI

Architectural Tests

Spike
CI/Testing

Infrastructure

Applications

SAIL

HPC          Data Center          IoT          Networking

Performant
Secure
Debuggable

Reliable, Serviceable, Diagnosable

Services

Silicon
Soft IP

Compilers

Academia
Research

Training

HPC
Consumer

RTC
DV

Implementation Design & Microarchitecture

OpenSBI

Architectural Tests

Spike
CI/Testing

Infrastructure

Applications

SAIL

HPC          Data Center          IoT          Networking

Performant
Secure
Debuggable

Reliable, Serviceable, Diagnosable

Services

Silicon
Soft IP

Compilers

Academia
Research

Training

HPC
Consumer

RTC
DV

Implementation Design & Microarchitecture

OpenSBI

Architectural Tests

Spike
CI/Testing

Infrastructure

Applications

SAIL
Software Stack Examples

- **Storage DB**: ceph, nvme-oF, SPDK, DPDK
- **Network**ing **Switch** Load Balancer: OvS
- **Virtualization**: KVM, visor
- **Guest OS**: Linux
- **Security**: SSL, TLS
- **OpenSSL**: OpenSSL
- **Web Apps**
  - Search: Apache Solr, OpenJDK
- **In-Memory**: Redis
- **Tools**: Memcached
- **Software Stack Examples**
  - PHP
  - MySQL
  - virtio
  - LVM
  - OpenSBI
  - qemu
- **Firmware/BIOS**: OpenSBI
- **RISC-V Platform**: RISC-V
- **Linux**
- **Firmware/BIOS**
- **Virtualization**
- **Security**
ISA Committees Roadmap (Priv & Unpriv)

2021
- Zmmul FT
- Ztso FT
- Code Size (Zce, Zcb) TG
- Temporal hint (Zihintnth) FT
- RV32E/RV64E (predates Foundation)
- Fast Interrupt (Smclic) TG
- I/D coherence (Zjid) J TG
- Pointer Masking (Zjpm) J TG
- New FP instructions (Zfa, Zdm?) FT

2022
- Memory-Wait (Zawrs) FT
- HpmCounter enhancements (Zicntr & Zihpm) FT
- Floating-Point SIG
- Scalar BFloat16 (Zfbfh, Zfbfmin) TG
- Vector Crypto (Zvk)
- Form TG

2023
- Resumable Non-maskable Interrupts (Smrnmi) Fast Track (FT)
- Form SIG
- Vector Phase 2 (Zvfh, ...) TG
- Form TG
- Floating-Point SIG
- SIG Work
- TG Work
- IC Work
Roadmap: Tools & Performance

2021
- Zb[abcs] remedial
- Vectors remedial
- Priv 1.12 remedial

2022
- SIG work
- TG work
- HC work

2023
- ISV outreach
- OS/Linux distribution outreach

Key Areas:
- Performance Modelling Strategy
- Toolchains & Runtimes Coordination, Enablement and Outreach
- Code-Speed Competitive Analysis
- Code-Speed Optimization
- Performance Modelling Coordination
- Trace Formats
- Open-Access Performance Models
- Performance Analysis Tools Outreach & Coordination
- QEMU Coordination
- Performance Modelling Outreach
- PMU Counters
- ISV outreach
Roadmap: Platforms

OS-A Platform Definition
Advanced Interrupt Architecture
RISC-V UEFI Specification
Secure Boot Standardization Requirements
RVM-CSI interoperability goals

Hypervisor Validation & Enablement
Nested Virtualization Validation

Platform Compatibility Test Definitions
RVM-CSI Specification
RVM-CSI Security Model
RVM-CSI AI Use-Cases

OS-A SEE Specification
IOMMU
Secure Boot Specification

RVM-CSI Compatibility Test Kit
RVM-CSI Security Extension
RVM-CSI AI/ML Extension
RVM-CSI AI PCT

RISC-V UEFI Specification
Secure Boot Standardization Requirements
RVM-CSI interoperability goals

Platform Compatibility Test Definitions
RVM-CSI Specification
RVM-CSI Security Model
RVM-CSI AI Use-Cases

OS-A Platform Specification
OS-A PCT

“tech-config” specification
Unified Discovery

2021
2022
2023

SIG work
TG work
HC work
Roadmap: Applications

- Graphics & AI/ML Requirements
- Matrix Multiplication Extension
- WRS Fast-Track
- MP Locks
- Managed Runtimes
- Web Application Stack
- Database Applications

Timeline:
- 2021: SIG work
- 2022: TG work
- 2023: HC work
Security HC - Roadmap

- Security Model
  - AP-TEE
  - Cap-Based TEE?
  - Ecosystem, Reference implementations, etc.
- Application-TEE, Confidential Compute, and Capabilities-Based
  - Security Model
  - Security Incident Response Team
  - Blockchain
    - Scalar Crypto
      - GOST-R Scalar Crypto
    - ePMP
      - Memory Safety
        - M-mode Isolation?
        - Vector Crypto
          - PQC Crypto
        - S-mode MPU
          - Memory Tagging?
          - IOPMP
          - Control Flow Integrity (CFI)
    - uSC TG(s): Temporal Fencing and others (?)
      - Microarchitectural Side Channel (uSC) leakage mitigations
        - Control Flow Integrity (CFI)
    - Sponsor SIG
    - Sponsored TG
    - Blockchain
      - Sponsor SIG
      - Sponsored TG
      - HC work

- 2021
- 2022
- 2023
# Security Planned Specifications

<table>
<thead>
<tr>
<th></th>
<th>CY22-Q1</th>
<th>CY22-Q2</th>
<th>CY22-Q3</th>
<th>CY22-Q4</th>
<th>CY23-Q1</th>
<th>CY23-Q2</th>
<th>CY23-Q3</th>
<th>CY23-Q4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security Model</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(non-ISA)</td>
<td>Inception</td>
<td>Plan</td>
<td>Develop</td>
<td>Freeze</td>
<td>Rat-Ready</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>AP-TEE</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(ISA + non-ISA)</td>
<td>Inception</td>
<td>Plan</td>
<td>Develop</td>
<td>Freeze</td>
<td>Rat-Ready</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CFI</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(ISA)</td>
<td>Inception</td>
<td>Plan</td>
<td>Develop</td>
<td>Freeze</td>
<td>Rat-Ready</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Vector crypto</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(ISA)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>GOST-R scalar crypto</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(ISA)</td>
<td>Inception</td>
<td>Plan</td>
<td>Develop</td>
<td>Freeze</td>
<td>Rat-Ready</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>S-mode MPU</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(ISA)</td>
<td>Inception</td>
<td>Plan</td>
<td>Develop</td>
<td>Freeze</td>
<td>Rat-Ready</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>IOPMP</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(non-ISA)</td>
<td>Inception</td>
<td>Plan</td>
<td>Develop</td>
<td>Freeze</td>
<td>Rat-Ready</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>uSC leakage</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(ISA)</td>
<td>Inception</td>
<td>Plan</td>
<td>Develop</td>
<td>Freeze</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## SoC HC - Roadmap

<table>
<thead>
<tr>
<th></th>
<th>CY22-Q1</th>
<th>CY22-Q2</th>
<th>CY22-Q3</th>
<th>CY22-Q4</th>
<th>CY23-Q1</th>
<th>CY23-Q2</th>
<th>CY23-Q3</th>
<th>CY23-Q4</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAS Register interface</td>
<td>Inception</td>
<td>Plan</td>
<td>Develop</td>
<td>Freeze</td>
<td>Rat-Ready</td>
<td>Freeze</td>
<td>Rat-Ready</td>
<td></td>
</tr>
<tr>
<td>and signaling (Non-ISA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>+ ISA)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quality of Service (QoS)</td>
<td>Inception</td>
<td>Plan</td>
<td>Develop</td>
<td>Freeze</td>
<td>Rat-Ready</td>
<td>Freeze</td>
<td>Rat-Ready</td>
<td></td>
</tr>
<tr>
<td>(Non-ISA + ISA)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IOMMU (TG created)</td>
<td>Develop</td>
<td>Freeze</td>
<td>Rat-Ready</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Non-ISA)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SoC performance</td>
<td>Inception</td>
<td>Plan</td>
<td>Develop</td>
<td>Freeze</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>monitoring and trace</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Non-ISA)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ISA Infra HC Roadmap

2021
- Form SIG

2022
- Form TG
- Simulators SIG: Sail TG
- Form TG: CI/Testing SIG
- Architectural Compatibility Tests SIG

2023
- Form TG: Platforms that tracking the functional and performance regressions of FOSS on RISC-V Arch
- Form SIG: CI Infra / RISC-V Lab (TBD)
- Documentation SIG (TODO, No Actions Yet)
Call To Action!
Join!
Contribute!
Make History!
#riscveverywhere
Thank You!