IOPMP Task Group Meeting

March 2, 2023

Video link

Agenda

- IOPMP TG 2023 plan
- Any updates from the Runtime Integrity SIG?
- Lock MDCFG and static IOPMP entries
- The section about the atomicity issues
- Reactions to violation

Only RISC-V Members May Attend

- Non-members are asked to please leave except for Joint Working Groups (JWG).
- Members share IP protection by virtue of their common membership agreement. Non-members being present jeopardizes that protection. Joint working groups (JWG) agree that any IP discussed or worked on is fully open source and unencumbered as per the policy.
- It is easy to become a member. Check out riscv.org/membership
- If you need work done between non-members or or other orgs and RISC-V, please use a joint working group (JWG).
    - used to allow non-members in SIGs but the SIGs purpose has changed.
- Please put your name and company (in parens after your name) as your zoom name. If you are an individual member just use the word “individual” instead of company name.
- Non-member guests may present to the group but should only stay for the presentation. Guests should leave for any follow on discussions.

Antitrust Policy Notice

RISC-V International meetings involve participation by industry competitors, and it is the intention of RISC-V International to conduct all its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.

Examples of types of actions that are prohibited at RISC-V International meetings and in connection with RISC-V International activities are described in the RISC-V International Regulations Article 7 available here: https://riscv.org/regulations/

If you have questions about these matters, please contact your company counsel.

Collaborative & Welcoming Community

RISC-V is an open ISA enabling a new era of processor innovation through open standard collaboration. Born in academia and research, RISC-V ISA delivers a new level of extensible software and hardware freedom on architecture, paving the way for the next 50 years of computing design and innovation.

We are a transparent, collaborative community where all are welcomed, and all members are encouraged to participate. We are a continuous improvement organization. If you see something that can be improved, please tell us. help@riscv.org

We as members, contributors, and leaders pledge to make participation in our community a harassment-free experience for everyone.

https://riscv.org/community/community-code-of-conduct/

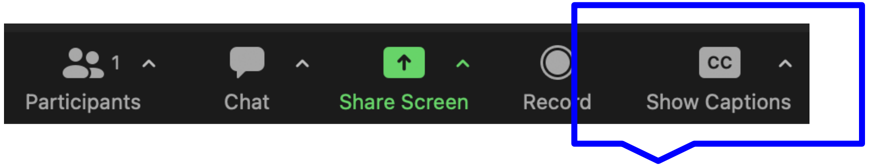
Conventions

- **For one hour meetings, please start at 5 after the start time** in order to allow people going to other meetings have time for a short break between meetings. 30 minute meetings start on time.
- Unless it is a scheduled agenda topic, we don’t solve problems or detailed topics in most meetings unless specified in the agenda because we don’t often have enough time to do so and it is more efficient to do so offline and/or in email. We identify items and send folks off to do the work and come back with solutions or proposals.
- If some policy, org, extension, etc. can be doing things in a better way, help us make it better. Do not change or not abide by the item unilaterally. Instead let's work together to make it better.
- Please conduct meetings that accommodates the virtual and broad geographical nature of our teams. This includes meeting times, repeating questions before you answer, at appropriate times polling attendees, guide people to interact in a way that has attendees taking turns speaking, …
- Where appropriate and possible, meeting minutes will be added as speaker notes within the slides for the Agenda

Zoom Translated Captions

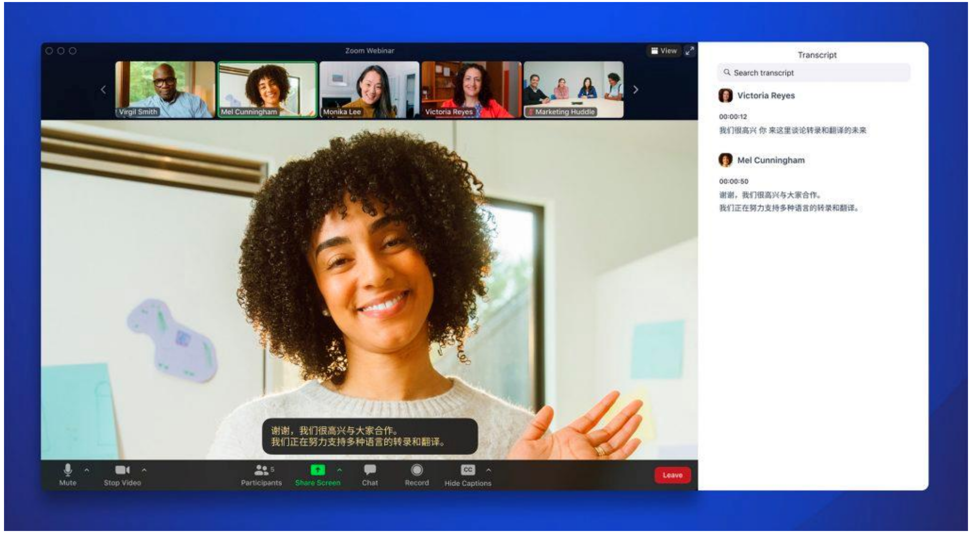
Step 1: Select **Show Captions** in the Zoom Meeting Window

- Tip: For smaller windows, this may be under More > Captions



Step 2: Ensure Speaking language is set to English. Under **Translate To**, select your desired output language.

Step 3 (optional): Under the Captions menu, select **View Full Transcript** (this will enable to you see captions in their full context)



谢谢，我们很高兴与大家合作。
我们正在努力支持多种语言的转录和翻译。

Transcript

Search transcript

Victoria Reyes

00:00:12

我们很高兴 你 来这里谈论转录和翻译的未来

Mel Cunningham

00:00:50

谢谢，我们很高兴与大家合作。
我们正在努力支持多种语言的转录和翻译。

Questions? Please email help@riscv.org

Zoom currently supports caption translation for 12 languages: Chinese Mandarin – Simplified (beta), Dutch, English, French, German,

IOPMP TG 2023 Plan

- Updated Plan
  - Plan Target Date: **Q3**’23
  - Freeze Target Date: Q3’23
  - Ratification Target Date: Q4’23
- The gap to freeze the IOPMP spec:
  - On-going items:
    - Atomicity
    - Locked configuration
    - Static configuration
  - To discussion:
    - Reaction to violation
    - Reset
    - Register definition
  - Any more items?
- New spec repo!

Agenda

- IOPMP TG 2023 plan
- Any updates from the Runtime Integrity SIG?
- Lock MDCFG and static IOPMP entries
- The section about the atomicity issues
- Reactions to violation

Agenda

- Ratification plan update
- Any updates from the Runtime Integrity SIG?
- Lock MDCFG and static IOPMP entries
- The section about the atomicity issues
- Reactions to violation

Agenda

- IOPMP TG 2023 plan
- Any updates from the Runtime Integrity SIG?
- Lock MDCFG and static IOPMP entries
- The section about the atomicity issues: drafting
- Reactions to violation

Agenda

- IOPMP TG 2023 plan
- Any updates from the Runtime Integrity SIG?
- Lock MDCFG and static IOPMP entries
- The section about the atomicity issues:
- Reactions to violation

Bus-Side Reactions to Violation Access

- On an illegal access, an IOPMP must/could react on the bus:
  - On an illegal **write** access:
    - IOPMP intercepts the transaction. Downstream can’t observe the transaction. Just like nothing happened. [could]
    - No memory is changed. [must]
    - It doesn’t mean nothing is observed in downstream! EX: the write command can still go through the IOPMP, but disable all byte lanes later, e.g. keeping WSTRB=0. [could] [speculation, lower latency]
  - On an illegal **read** access:
    - IOPMP stops the access. Downstream can’t observe the transaction. [could]
    - No real data should be returned to the transaction issuer. [must]
    - Return a forged data? [could]
    - Return a bus error [could]
    - The read command can still go through the IOPMP but the real data is not returned. [could] [speculation, idempotent device, lower latency]

System-Wide Reactions to Violation Access

- On an illegal access, an IOPMP could react system-wide:
  - Record [programmable]
  - Interrupt [programmable]
  - Reset [programmable]

What to Record an Illegal Access

- Record of an illegal access:
    - Must record:
        - Address
        - # of bytes
        - Direction: read/write/execute
        - SID
    - Could record:
        - MD index?
        - Entry index?
        - Thread ID? (AWID, ARID)
        - Customized fields: A[RW]PROT, A[RW]CACHE, A[RW]LOCK, …

When to Record an Illegal Access

- Reading back an record of illegal access takes more than one cycle/transaction.
    - Only one record.
    - The record and its refreshment should be atomic. No half-half.
- First-illegal mode:
    - Record the first illegal access and then pause automatically.
    - The record will not be refreshed until an explicit re-enable.
    - Usage: SW notices an illegal, it reads back the record and then re-enable the recorder.
- Sampling mode:
    - Refresh and overwrite the record on every illegal access unless an explicit pause.
    - Usage: once SW wants to sample, it pauses the recorder. Once SW reads back the record completely, it should explicitly resume the recorder.

Thank You

RISC-V®