IOPMP TG Meeting

September 15th, 2022

Agenda

- Disclosure:
- TG Charter
- Meeting
- Atomicity issues on programming IOPMP

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 a free and 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 free, 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

People

- Chair: Paul
  - Affiliation: Andes Technology
  - Interest: Parallel Algorithm, SoC, and Platform/Processor Security
  - Worked for: Faraday Technology, Realtek Semiconductor, Cadence Design System
  - Email: scku@andestech.com
- Vice-chair: Channing

TG Charter (Approved)

- Over half year discussion with the Security Committee and TSC:
  - IOPMP spec has been requested urgently in the RISC-V processor and platform market.
  - We want to expedite the first (non-ISA) spec delivered by limiting it to essential goals.
  - People don't want to run a long TG. That is, once we finish this stage, we can initiate subsequent discussions to add advanced features later.
  - Approved charter: https://github.com/riscv-admin/iopmp/blob/main/CHARTER.md
- Items included in the first version:
  1) rules, memory domains, IDs for I/O agents, and the mappings of one another,
  2) protection of IOPMP settings,
  3) solution to the atomicity issue on programming an IOPMP,
  4) register definitions and their reset states, and
  5) reactions to an access violation (may include the AIA supporting).

Not Included in the Version

1) the error handling of speculative accesses,
2) the mitigation of denial-of-service and side-channel attacks,
3) supporting NoC,
4) the interactions with the caches and the cache manipulation operations,
5) changing the ID of an I/O agent dynamically, or
6) supporting multiple VMs in a hart with different permissions.

ISA spec

- I know you must have many other brilliant ideas, and we may have them in the future version(s)!

Biweekly Meeting

- 8:00am ~ 9:00am UTC, every other Thursday from this week
- Policies from Best Practice:
  - Everyone should have identifiable names (first and last name and company/individual)
    - e.g., “Paul Ku (Andes)”
  - Do as much in email without meetings as you can take items offline as appropriate.
    - Conduct discussions on the group’s email list.
    - Spec issues go in github issues.
    - Cross group things go in Jira.

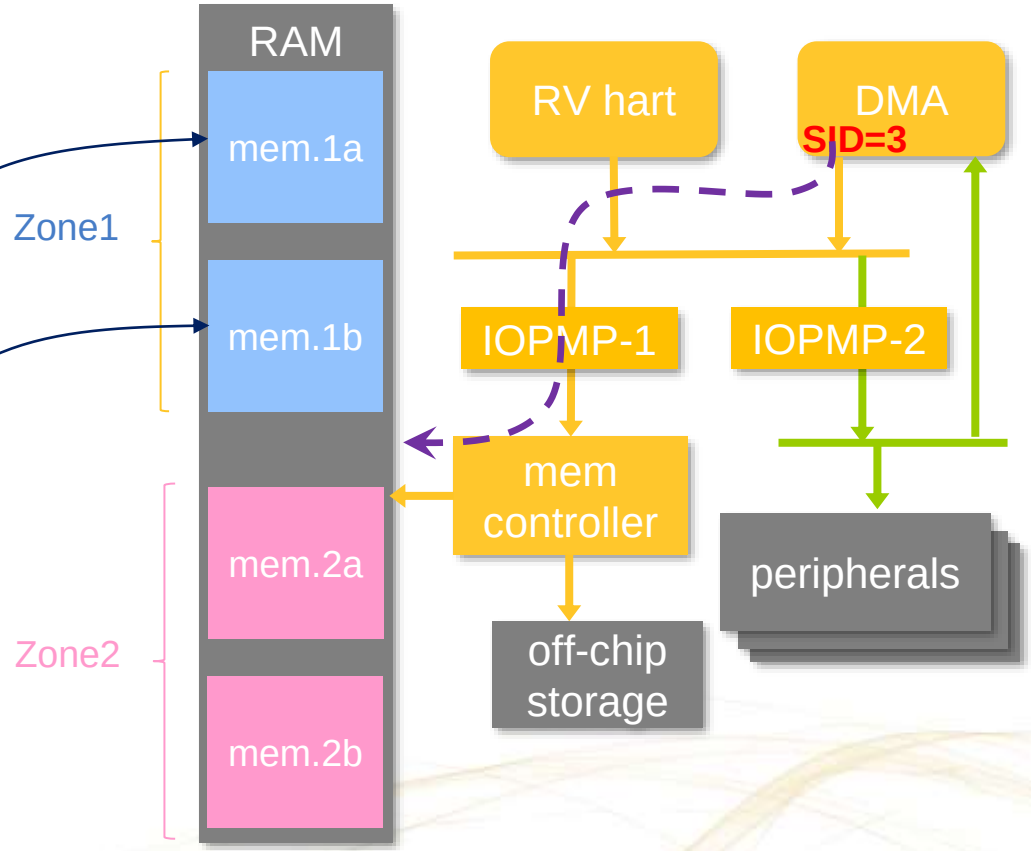
Atomicity Issues

- On programming multiple rules in the run-time, there could be a moment that IOPMP works under incomplete settings. → It could transiently create a security hole.
- An example described here (in Mandarin): https://www.bilibili.com/video/BV16K411f7k2?share_source=copy_web&vd_source=73dda4d670cd64091fc98c08f02adc31

DMA Belonging to Zone1

- Zone1 has mem.1a & mem.1b.
- Zone2 has mem.2a & mem.2b.

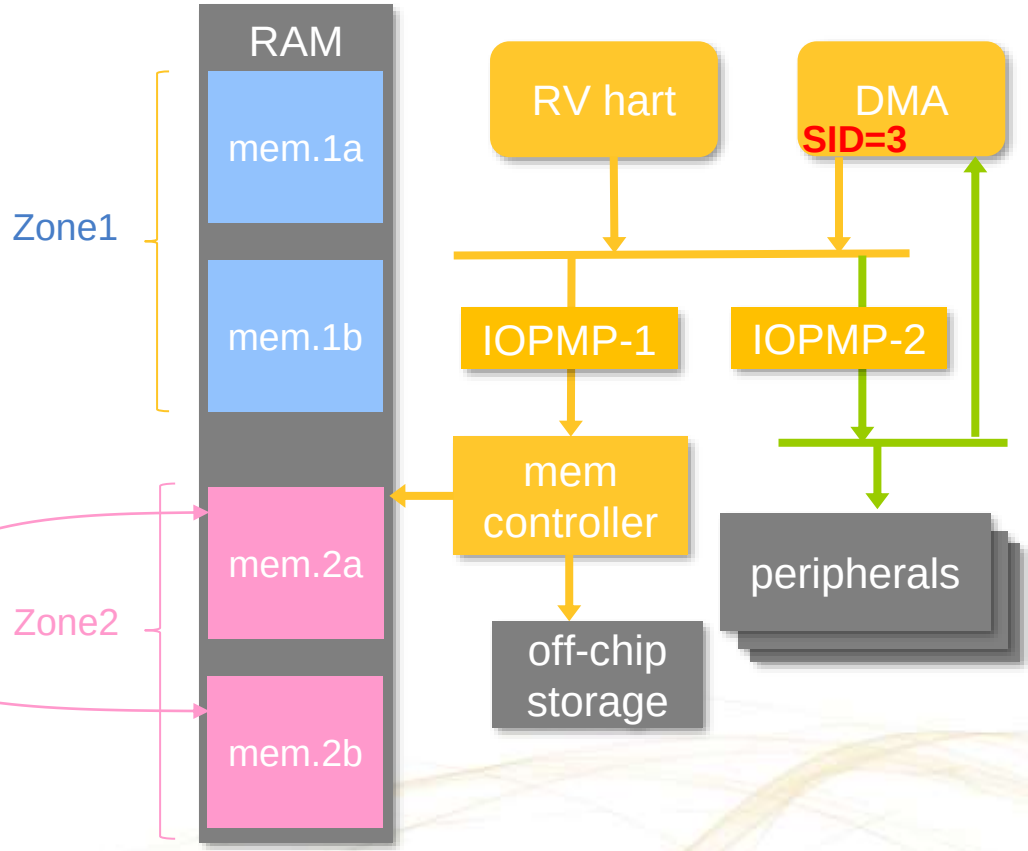
- IOPMP-1 setting:
  - For SID=3 (before)
    [entry-7] read+write in mem.1a
    [entry-8] read+write in mem.1b



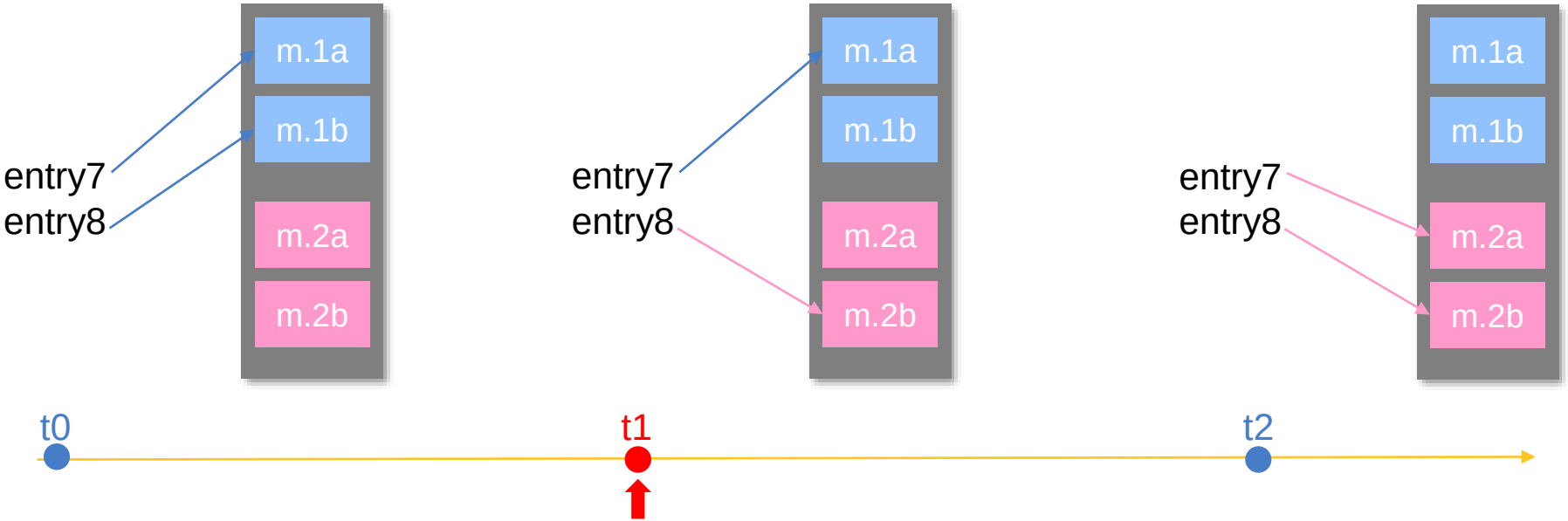
Change DMA's Access Regions

- Zone1 has mem.1a & mem.1b.
- Zone2 has mem.2a & mem.2b.

- IOPMP-1 setting:
  - For SID=3 (before)
    [entry-7] read+write in mem.1a
    [entry-8] read+write in mem.1b
  - For SID=3 (after)
    [entry-7] read+write in mem.2a
    [entry-8] read+write in mem.2b



Trigger DMA-Transfer in between Switch



A vulnerability:
DMA can access both zones at t1.

Thank You