RISC-V®

DTPM SIG

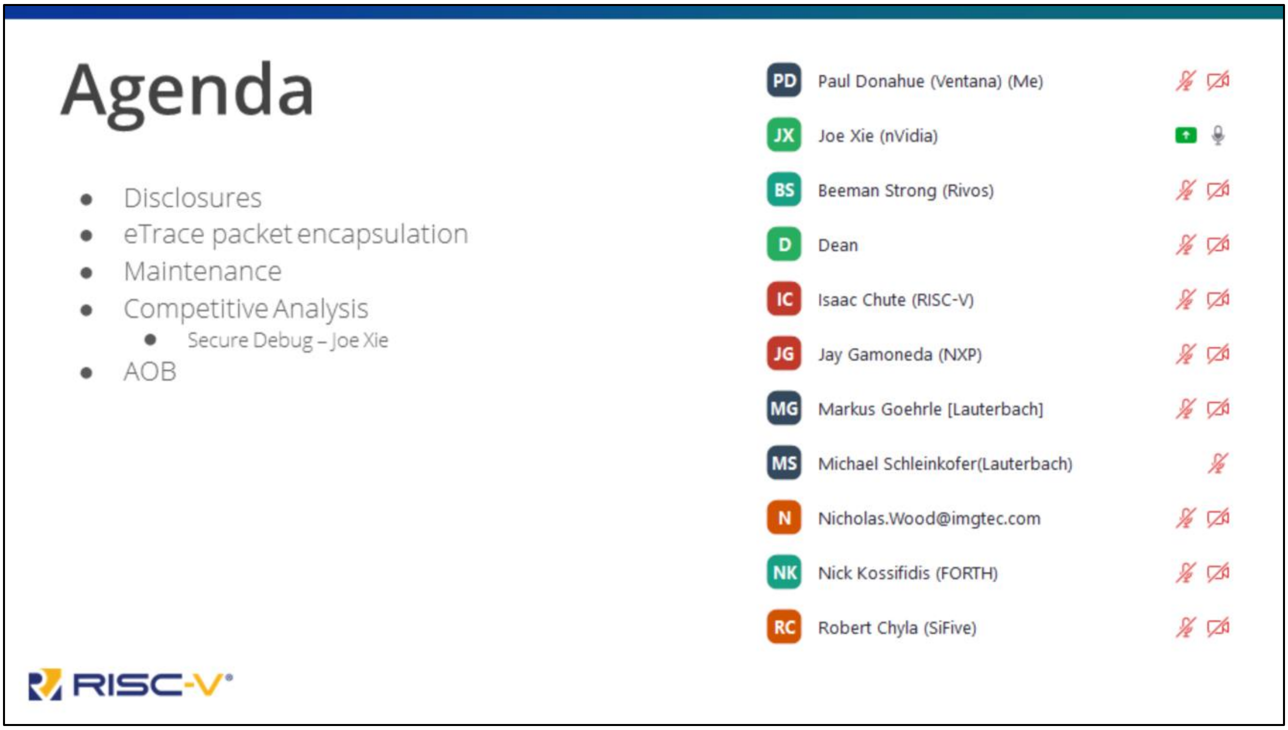
E-Trace-Encap TG

13-Sep-2023

Meeting minutes are in the speaker notes for the relevant slide

RISC-V®

Disclosures



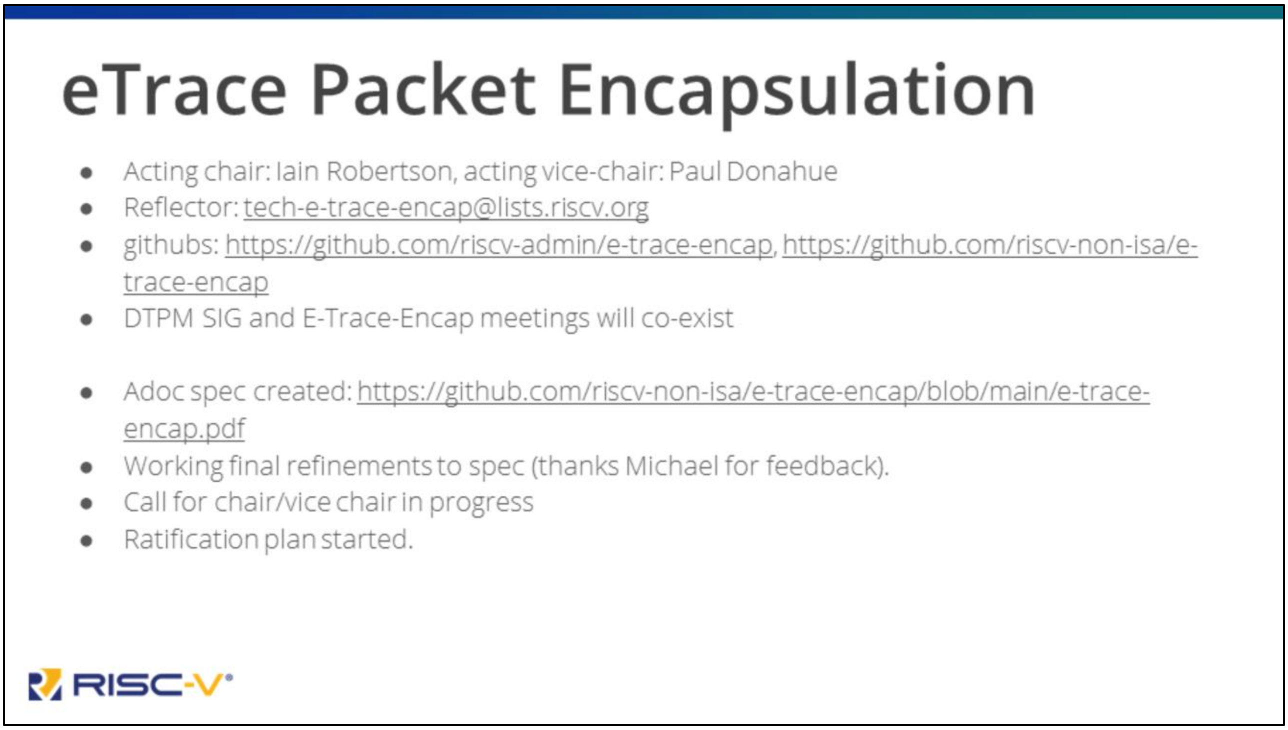
Agenda

- Disclosures
- eTrace packet encapsulation
- Maintenance
- Competitive Analysis
  - Secure Debug – Joe Xie
- AOB

PD	Paul Donahue (Ventana) (Me)
JX	Joe Xie (nVidia)
BS	Beeman Strong (Rivos)
D	Dean
IC	Isaac Chute (RISC-V)
JG	Jay Gamoneda (NXP)
MG	Markus Goehrle [Lauterbach]
MS	Michael Schleinkofer(Lauterbach)
N	Nicholas.Wood@imgtec.com
NK	Nick Kossifidis (FORTH)
RC	Robert Chyla (SiFive)

RISC-V

Attendees: see screenshot on the agenda slide

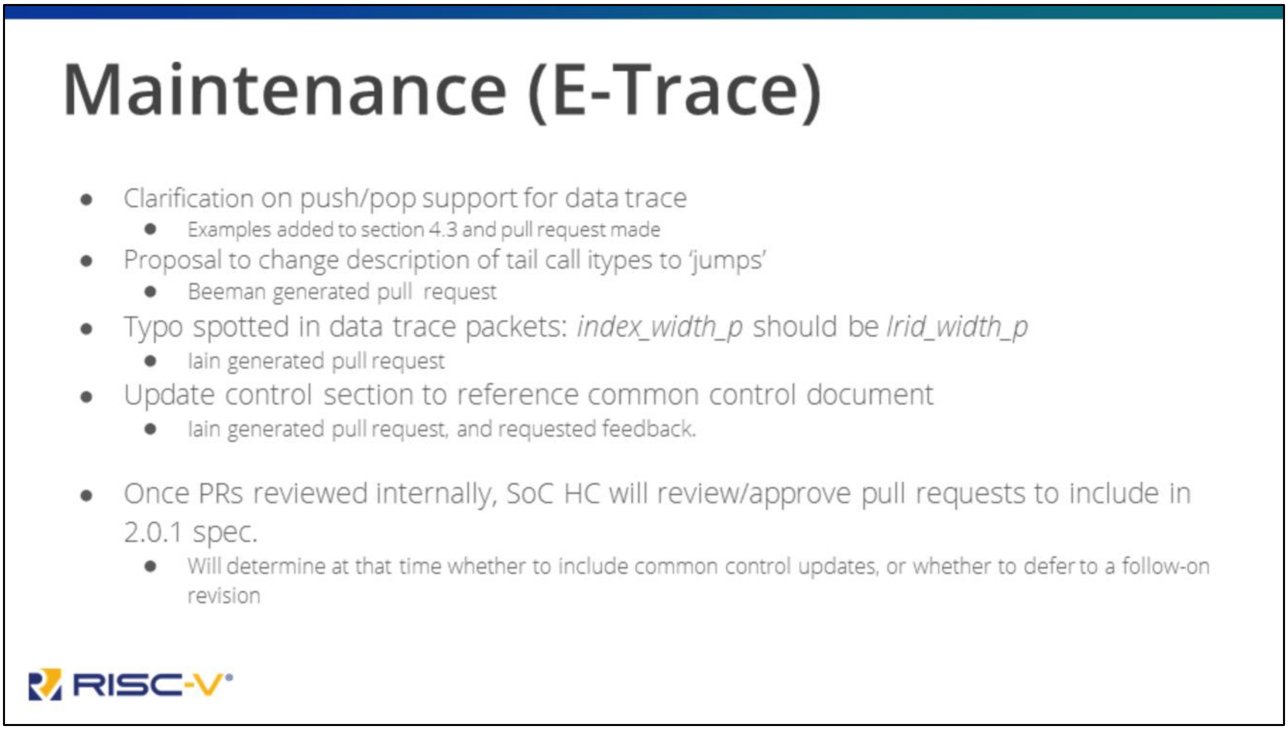


eTrace Packet Encapsulation

- Acting chair: Iain Robertson, acting vice-chair: Paul Donahue
- Reflector: tech-e-trace-encap@lists.riscv.org
- githubs: https://github.com/riscv-admin/e-trace-encap, https://github.com/riscv-non-isa/e-trace-encap
- DTPM SIG and E-Trace-Encap meetings will co-exist

- Adoc spec created: https://github.com/riscv-non-isa/e-trace-encap/blob/main/e-trace-encap.pdf
- Working final refinements to spec (thanks Michael for feedback).
- Call for chair/vice chair in progress
- Ratification plan started.

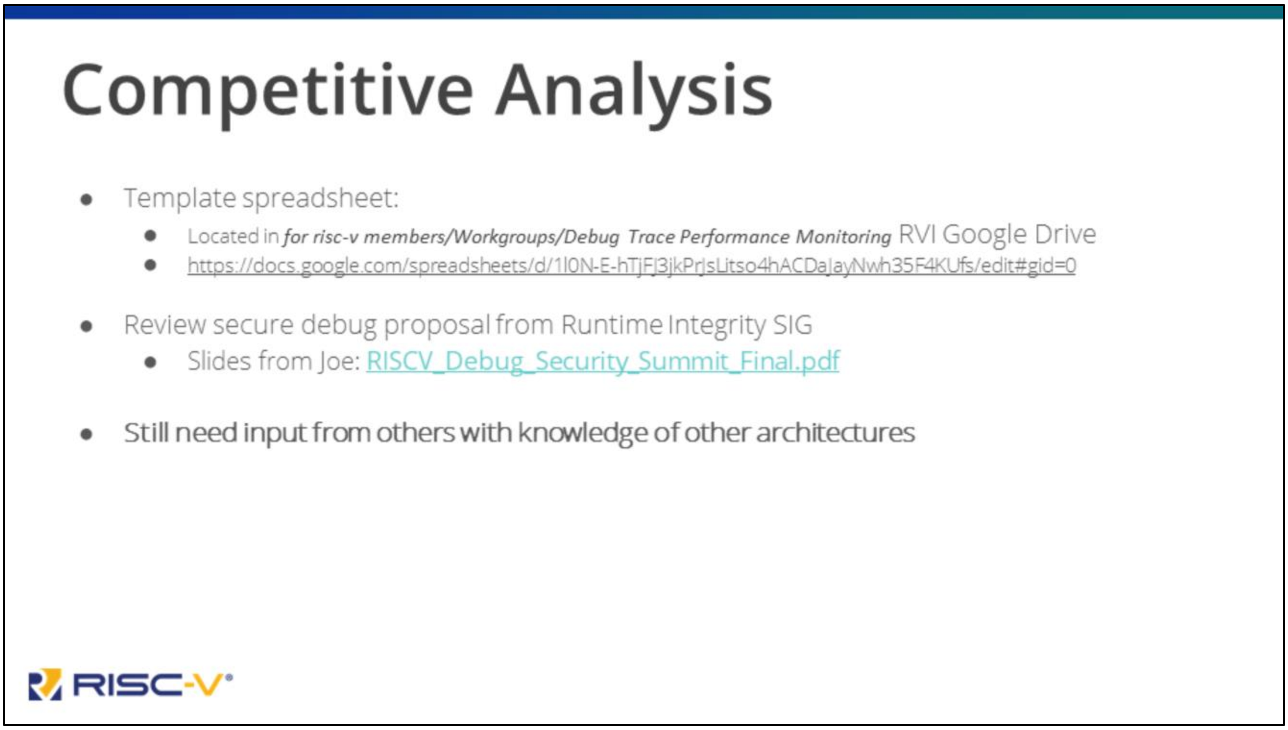
- E-trace packet encapsulation
  - Spec created, in refinement
  - Ratification plan WIP



Maintenance (E-Trace)

- Clarification on push/pop support for data trace
  - Examples added to section 4.3 and pull request made
- Proposal to change description of tail call itypes to 'jumps'
  - Beeman generated pull request
- Typo spotted in data trace packets: *index_width_p* should be *lrid_width_p*
  - Iain generated pull request
- Update control section to reference common control document
  - Iain generated pull request, and requested feedback.
- Once PRs reviewed internally, SoC HC will review/approve pull requests to include in 2.0.1 spec.
  - Will determine at that time whether to include common control updates, or whether to defer to a follow-on revision

- E-trace spec maintenance
  - Several PRs, to be integrated in v2.0.1
  - Some question about version name: Control section may be more substantial change. 2.1.0 or 2.0.1?



Competitive Analysis

- Template spreadsheet:
  - Located in ***for risc-v members/Workgroups/Debug Trace Performance Monitoring*** RVI Google Drive
  - https://docs.google.com/spreadsheets/d/1l0N-E-hTjFJ3jkPrJsLitso4hACDaJayNwh35F4KUfs/edit#gid=0
- Review secure debug proposal from Runtime Integrity SIG
  - Slides from Joe: RISCV_Debug_Security_Summit_Final.pdf
- Still need input from others with knowledge of other architectures

- Secure Debug discussion
  - Security model diagram doesn’t include H extension, for simplicity
  - Problem that debug mode can write PMPs, e.g.
  - Need a way to debug bootloader firmware post-production, self-hosted can run in this environment
  - Want to protect firmware secrets from OS debugger, minimize TCB
  - Reviewed ARM secure debug interface, including new v9 additions (realm and root debug)
  - Does RISC-V allow multi-user debug? Multiple sessions at once? Some disagreement. Could have multiple domains.
  - Authentication module in ARM is undefined, could be a DM-like structure, or even software (RoT)
    - SiFive uses WorldGuard
  - ARM accesses in debug state behave like non-debug, depend on priv mode for access
  - Sent proposal to debug list, how to progress?
    - Should DTPM spin off a new TG, or handle under Smmtt?
      - Smmtt only covers supervisor needs, and is setup late
    - Concern about overhead of forming a TG, and approval process

AI: Joe Xie will draft a proposed charter for a new TG that DTPM will propose to SoC HC. Refinements to the draft charter and other details to be worked out via the mailing list.

Future Meetings / AOB

- 2nd Wednesday of each month
- AOB

Thank You