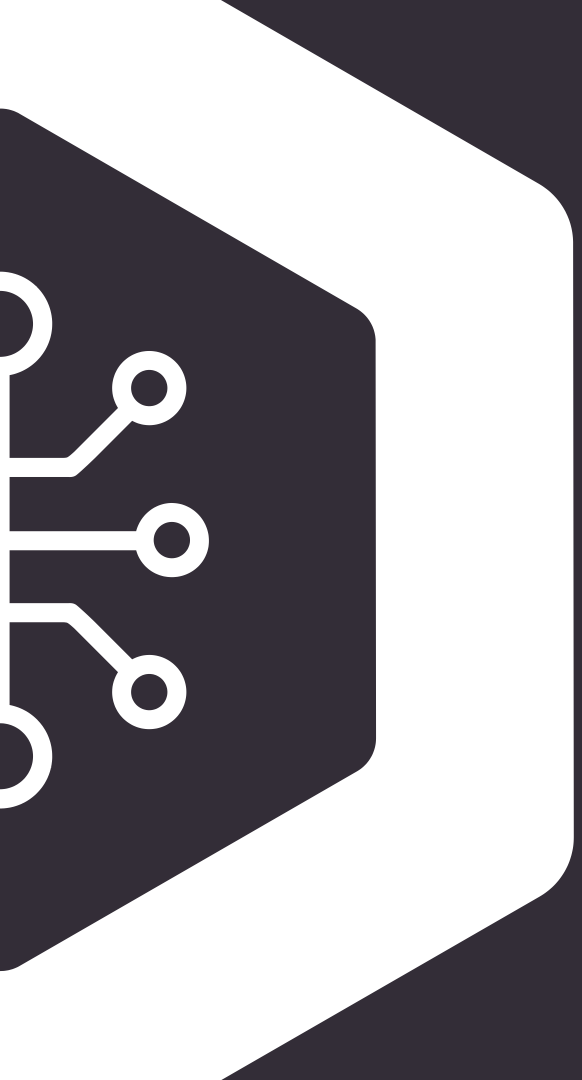


Caliptra: Building Open Source Security IP with Open Source Tools

ORCONF 2023
Munich, 2023-09-15

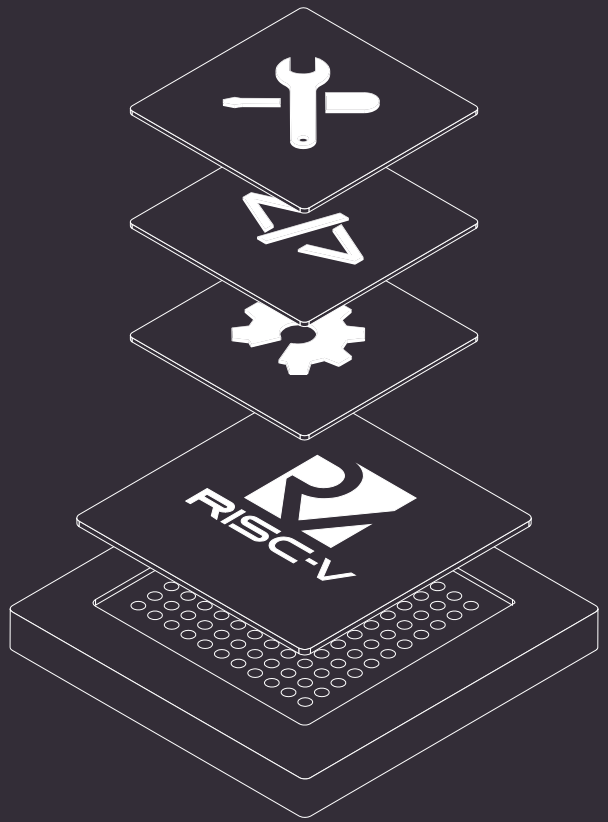
Michael Gielda, mgielda@antmicro.com

antmicro

antmicro

ANTMICRO

- Founded in 2009, dedicated to **commercial adoption of open source** in the hardware space**,** Platinum CHIPS Alliance & Founding RISC-V member
- Long term FOSSi supporter
- Engineering services, software/hardware co-design, tools and R&D
- Developing, adapting and integrating **open source ASIC and FPGA tooling, IP, software, hardware and AI**
- Help customers achieve vertical integration, address niche use cases, increase productivity



antmicro

CALIPTRA

- Open source integrated Root of Trust block
- Collaboration between Google, Nvidia, Microsoft and AMD within CHIPS Alliance (spec lives in OCP, implementation is developed in CHIPS)
- Focused on specific set of features
- By default meant to be integrated with a larger SoC, with concrete plans from several member companies
  - has both Boot Media Integrated/Dependent variants
- Uses VeeR EL2 CPU core
- Reuses a number of OpenTitan peripheral cores

antmicro

CALIPTRA - STATUS

- Moving fast (and trying not to break things)
- Going towards 1.0 RTL release as planned
- Focusing on a small but useful first version, without too many extra features
- Slated to be included in multiple chips coming from main partners (some time from now)

CHIPS MEMBERS INVOLVED WITH CALIPTRA WG

AMD

ami

antmicro

AXIADO

Google

MARVELL

Microsoft

NVIDIA

antmicro

CALIPTRA AND ANTMICRO

- Focus on enabling open source collaboration on the project for both current project partners and external adoption
- Took over cleanup and maintenance of VeeR cores family, primarily EL2, make sure it's on par
- Another goal - enable more open source collaboration around RTL with open source tools:
  - Developer productivity
  - System-level testing and integration
  - Public-facing CI

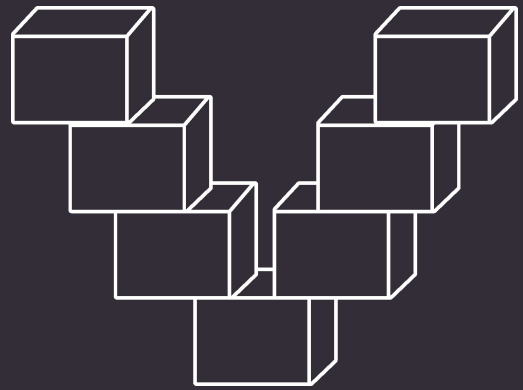
VEER

- Family of open source 32 bit RISC-V CPU cores
- Three options
  - EL2 - tiny and low power core - **this is the one used in Caliptra**
  - EH1 - high performance core
  - EH2 - dual threaded successor to EH1
- All the variants are implemented with SystemVerilog
- RTL is ASIC proven, shipped in millions of devices

antmicro

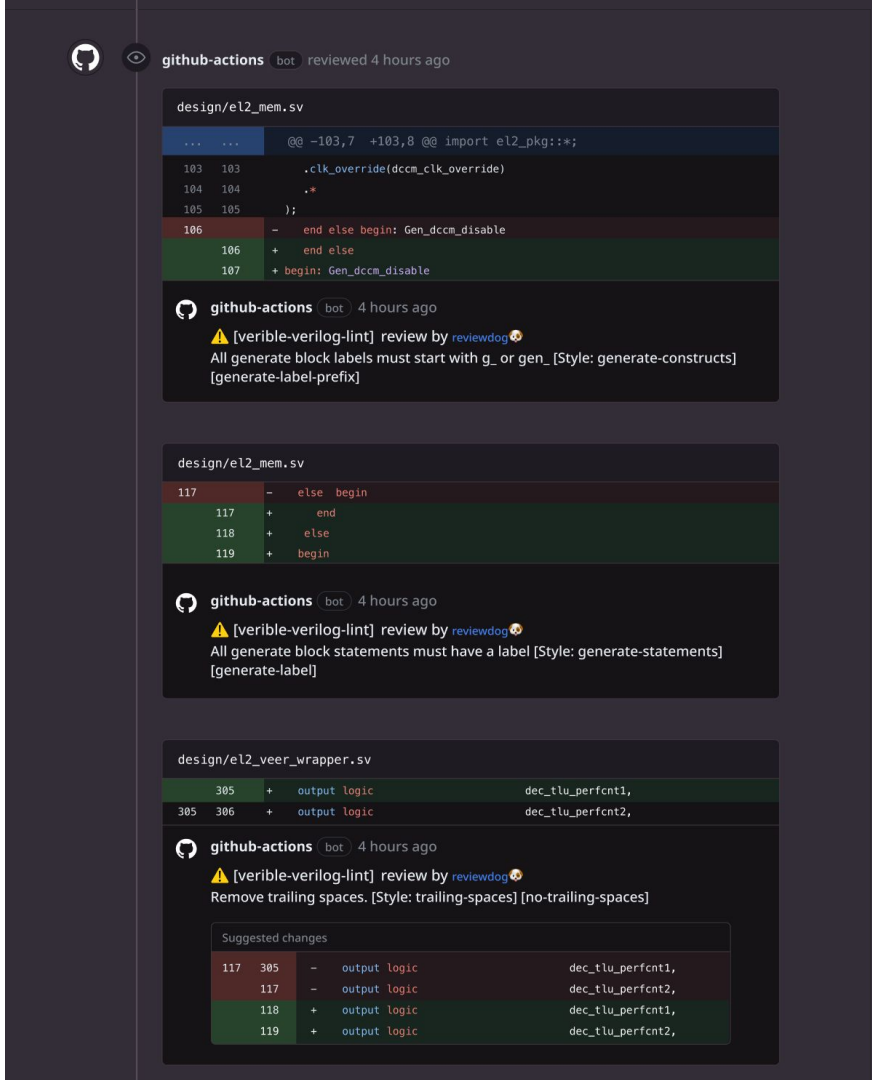
VERIBLE

- SystemVerilog linter, formatter, indexer etc. developed by Google and donated to CHIPS Alliance
- A practical tool used extensively in the wild!
- Now also in Caliptra



VERIBLE GH ACTIONS

- Linter and formatter actions
  - chipsalliance/verible-formatter-action
  - chipsalliance/verible-linter-action
- Both linter and formatter enabled for VeeR EL2 repository

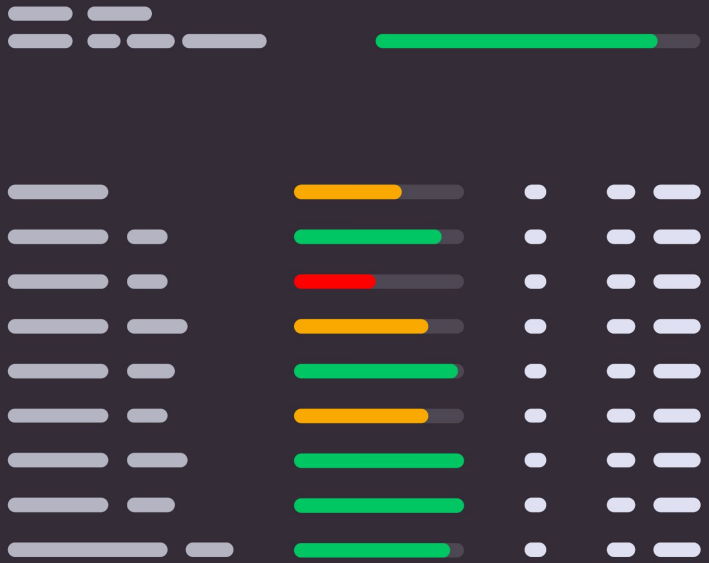


antmicro

CHIPS ALLIANCE

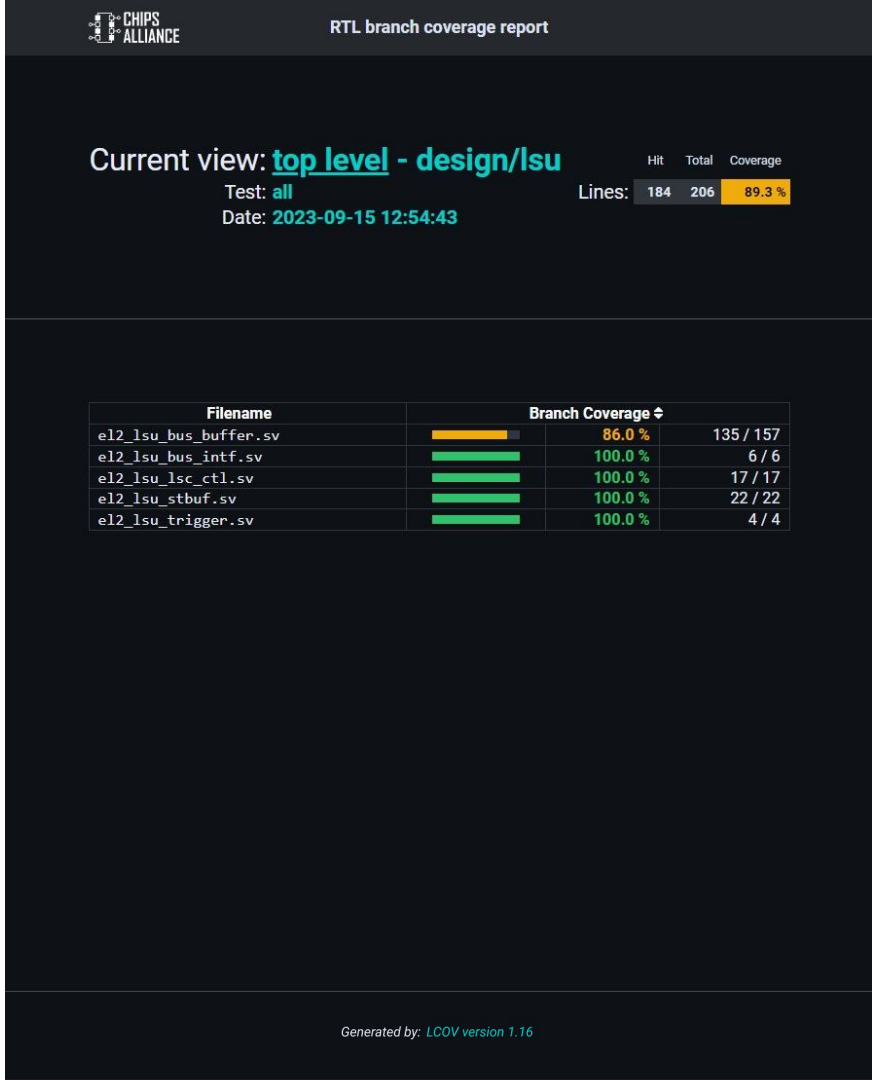
VEER TESTING

- The open source release of VeeR cores family originally only included system level tests
  - A more complex test suite was internal to the original authors and was not released as open source
- One of the main goals is to extend VeeR's publicly available test suite with tests for specific core components
- We added public CI to the VeeR repo running those tests for every commit
- The suite includes code coverage reporting - the CI generates a summary webpage



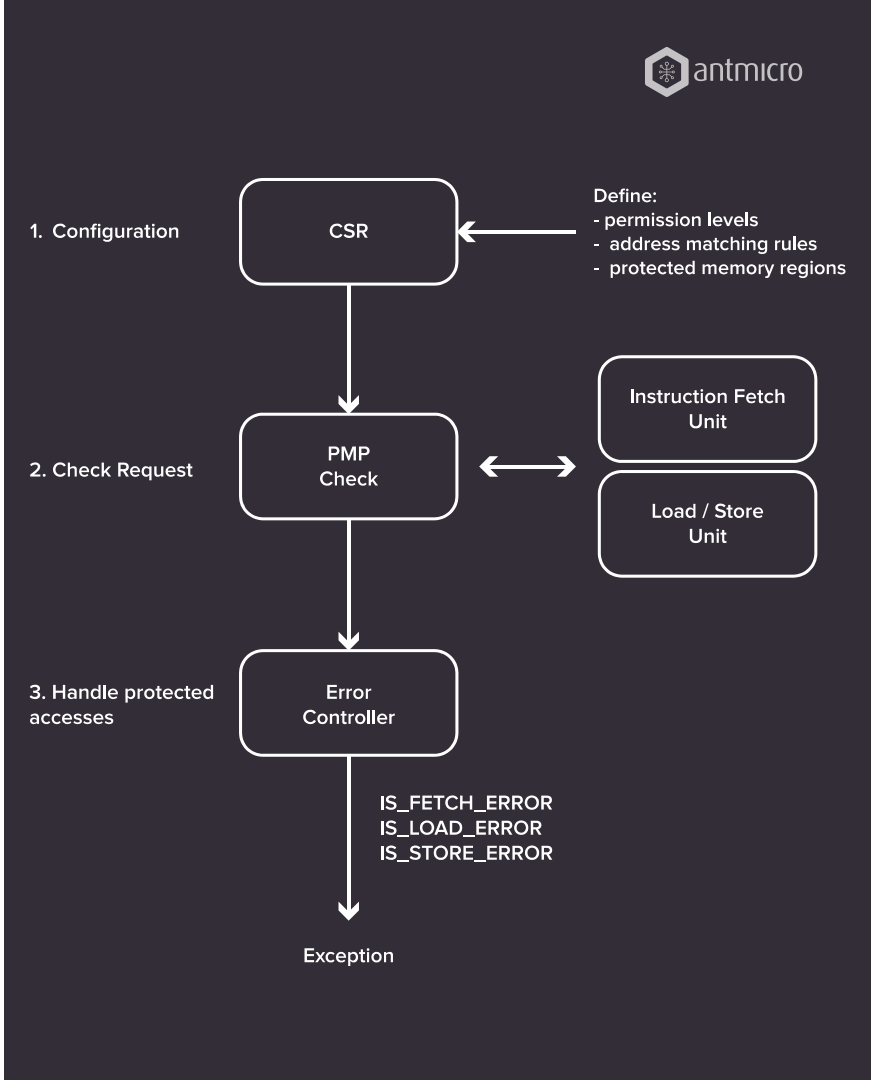
VEER TESTING

- Collecting line and toggle coverage from several types of tests:
  - RISCV-DV
  - RISCOF (RISC-V Architectural Test Framework)
  - UVM (for specific VeeR blocks, i.e. PIC, DEC, EXU, IFU, LSU, etc.)
- Coverage results built within a continuous integration workflow for main branch and PRs



PHYSICAL MEMORY PROTECTION (PMP)

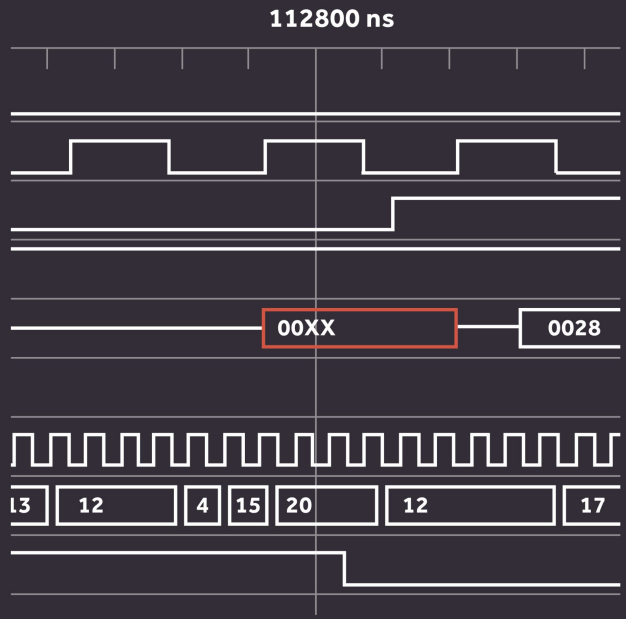
- Originally, in VeeR-EL2 Core only a rudimentary PMP was available. Currently, a RISC-V compliant PMP is being developed.
- Physical Memory Protection is needed to support secure processing and contain faults (PMP violations are precisely trapped at the processor)
- The PMP limits the physical addresses accessible by software:
  - Divide the memory into regions with different levels of privilege
  - Manage protection rules (Read, Write, Execute)
  - Grant or revoke permissions to Supervisor, User and Machine mode



antmicro

JTAG INTEGRATION

- For debugging the core, Caliptra added a JTAG interface, which needed its own end-to-end tests
  - The test connects to a simulated SoC with OpenOCD and runs typical debug scenarios
  - Run in public CI on GitHub with open source tools
- Helped uncover a bug earlier this year which is now covered by a dedicated test



OPEN SOURCE VERIFICATION

- Caliptra's primary use case is integration into bigger SoCs
- The primary testing methodology is UVM based based on widespread use in founding organizations
- UVM simulations are not yet possible with open source tools only
- There is an ongoing effort on enabling UVM simulation in Verilator (see Chris' presentation tomorrow)
- To enable open source collaboration around improving testing coverage, we have been using Cocotb and pyuvm testing which can be run completely open source in CI

antmicro

RISCV-DV

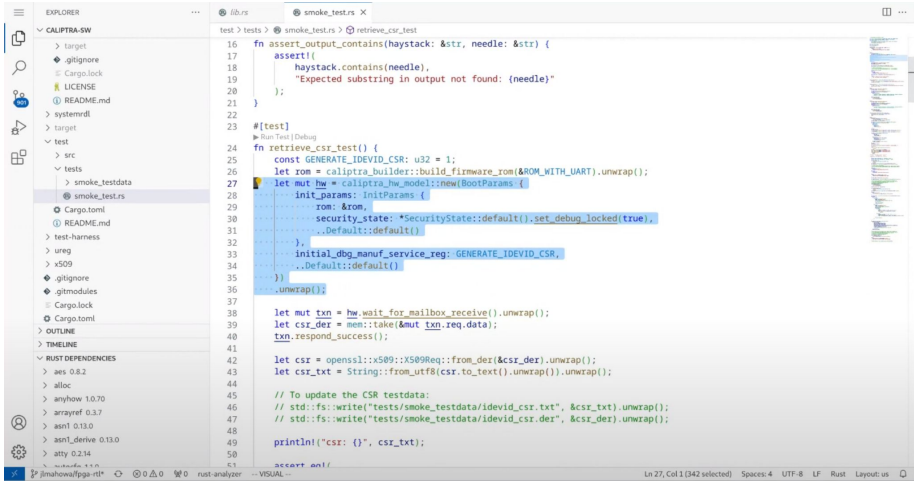
- riscv-dv open source instruction generator for RISC-V processor verification
- By default uses UVM, but also features a Python generator
- To make it work with the current EL2 codebase, VeeR's out of order div/rem block required special handling in the generator
  - We improved trace analyzer and code generator to handle the out-of-order division logic
- fixed support in the Python-based generator, riscv-dv tests are now part of VeeR's public CI
- Also using the VeeR tests in RISC-V DV CI!

```
0x8000bfa8:    01010113  addi sp, sp, 16
0x8000bfac:    00008067  ret
0x8000c0b8:    fff00793  li a5, -1
0x8000c0bc:    00f50e63  beq a0, a5, 28
0x8000c0c0:    00a4dc63  bge s1, a0, 24
0x8000c0d8:    00847413  andi s0, s0, 8
0x8000c0dc:    30042473  csrrs s0, mstatus, s0
0x8000c0e0:    01c12083  lw ra, 28(sp)
0x8000c0e4:    01812403  lw s0, 24(sp)
0x8000c0e8:    01412483  lw s1, 20(sp)
0x8000c0ec:    02010113  addi sp, sp, 32
0x8000c0f0:    00008067  ret
0x8000cac4:    de1f50ef  jal -41504
0x800028a4:    00800793  li a5, 8
0x800028a8:    3007a7f3  csrrs a5, mstatus, a5
0x800028ac:    10500073  wfi
0x80000010:    fb010113  addi sp, sp, -80
```

antmicro

CALIPTRA FIRMWARE VALIDATION

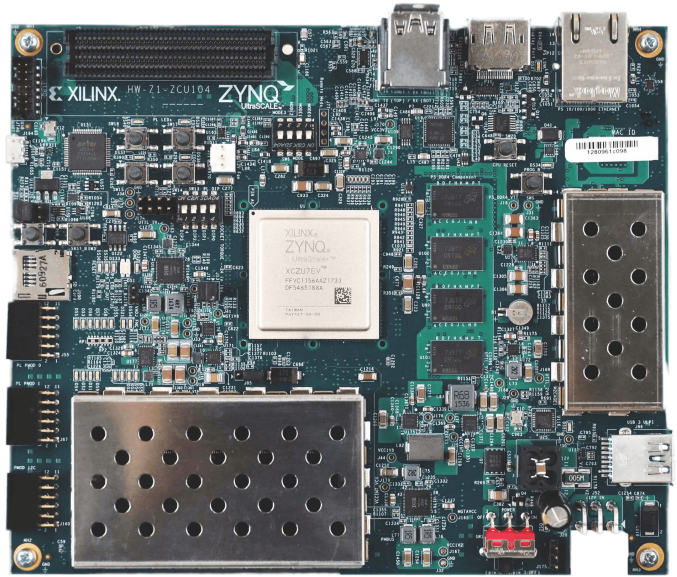
- Rust-based rv32imc interpreter with peripherals
  - can run all integration tests
  - all new firmware tested pre-merge in CI
- Verilator tests
  - direct from RTL but (expectedly) much slower - minutes to compile, hours to run
  - used for several important nightly tests
  - allow outputting signal data into .vcd files for analysis in e.g. GTKwave
- Good test infrastructure
  - test case integration with VS code



antmicro

CALIPTRA FIRMWARE VALIDATION

- FPGA emulation
  - Uses zcu104 (UltraScale+)
  - Tests run on Cortex-A53 Linux
  - Both fast and accurate, but cannot (yet) run all the tests
  - Long compile time

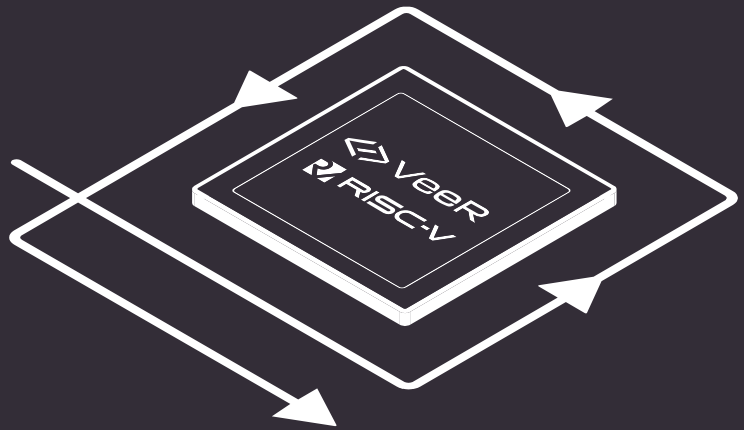


antmicro

RTL2GDS FLOW WITH OPENROAD

- By default Caliptra uses proprietary tools for the digital design, as do its main members
- They are all SystemVerilog shops
- To enable fast turnaround feedback, we have an ongoing effort on getting open source VeeR/Caliptra RTL2GDS flow directly from SV source using Antmicro's SystemVerilog plugin for Yosys through Surelog/UHDM in OpenROAD

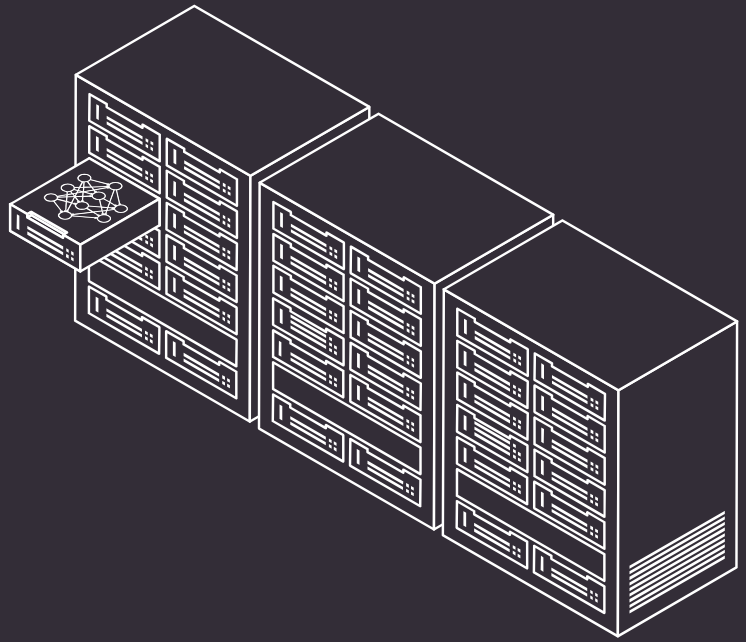
OpenROAD



antmicro

CUSTOM GH RUNNERS

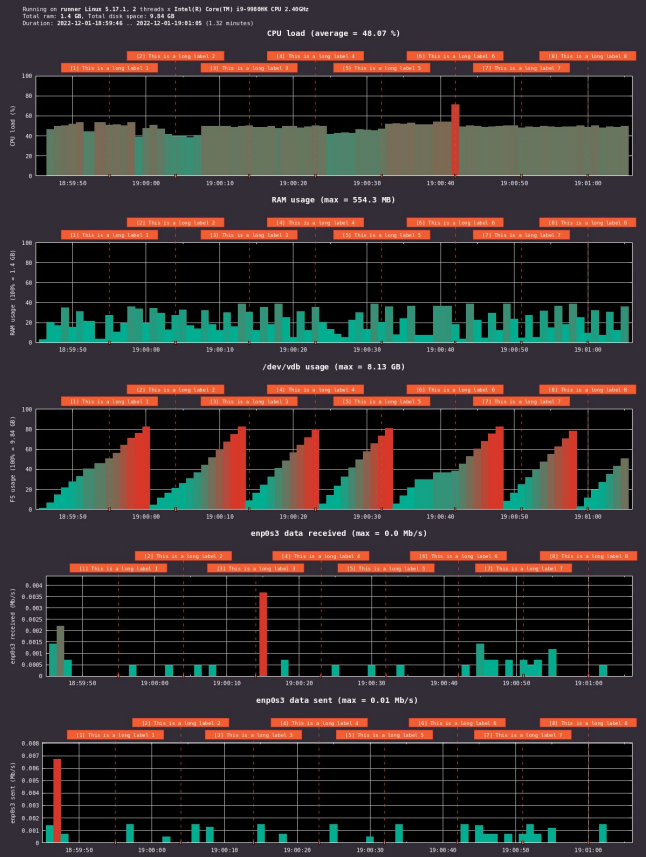
- Since we need more resources than the standard GH runners can provide (long verification jobs etc) as well as we need to allow use of proprietary tools in CI, we're using Antmicro's open source custom GH runners
- Work to structure results between public artifacts and ones we (sadly) cannot share publicly, available to project members
- Infrastructure is open source and available on GitHub, used by a number of CHIPS projects



antmicro

CUSTOM GH RUNNERS - EXECUTION METRICS

- Each job running on our custom runners outputs a performance plot
- Helps developers to better understand how to optimize their builds
- Uses our open source Sargraph tool



antmicro

LEARN MORE

- OCP Summit
  - San Jose, October 17-19
  - Register at opencompute.org

THANK YOU
FOR YOUR ATTENTION!