



CORE-V[®]



OPENHW[®]

RISC-V Cores

How we help to secure

Florian 'Flo' Wohlrab flo@openhwgroup.org

T [@FlorianWoh](https://twitter.com/FlorianWoh) T [@openhwgroup](https://twitter.com/openhwgroup)

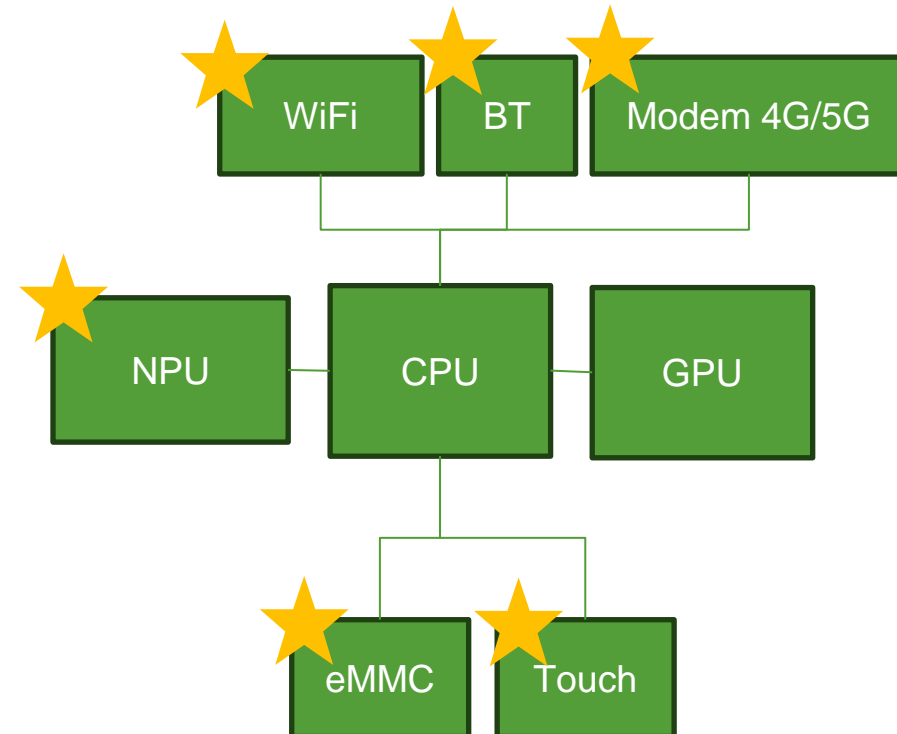
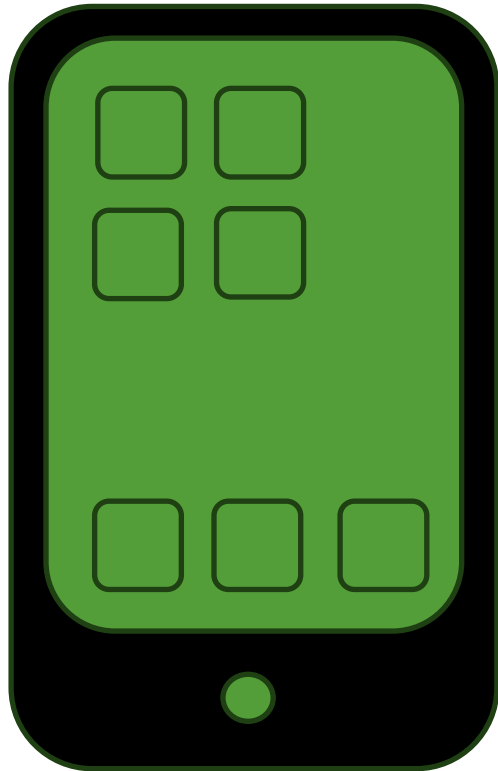
www.openhwgroup.org



Agenda

- Do we need to Secure RISC-V Cores?
- Who is the OpenHW Group and why we are here
- How we add security
- CVE2: A Secure Core, ready for integration

There is no RISC-V in real world...



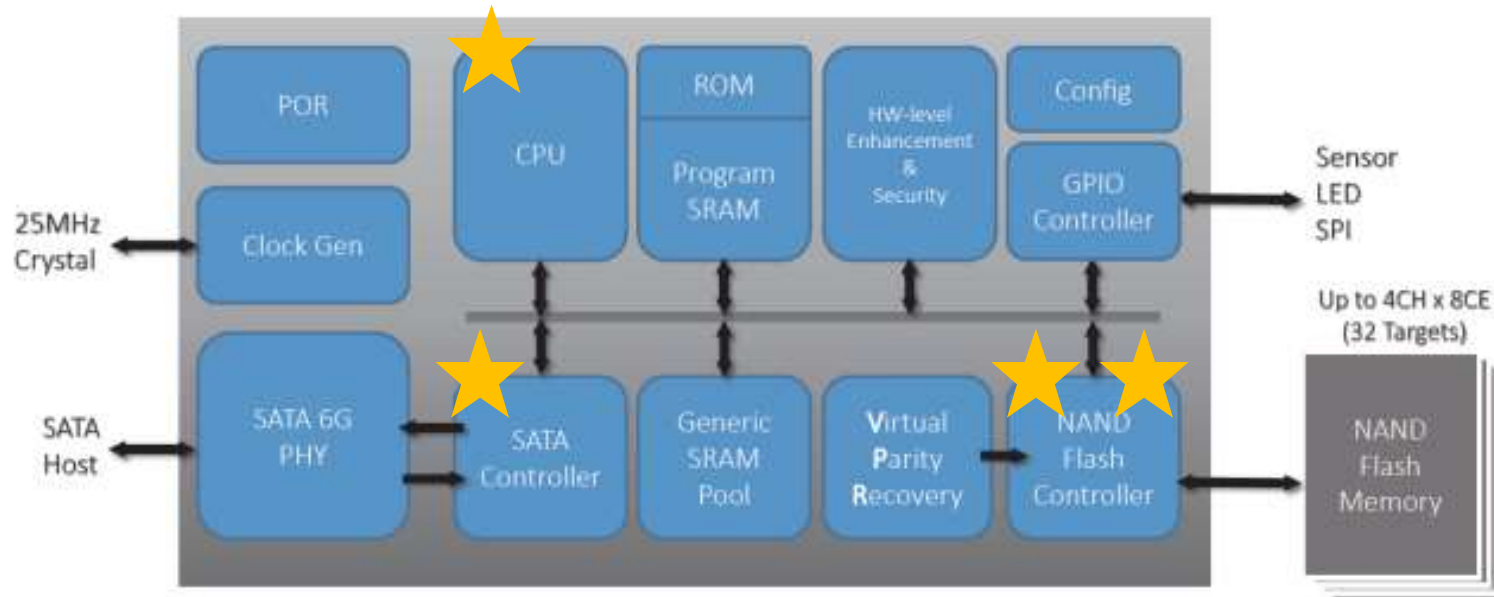
★ = RISC-V already today by some manufacturers, sometimes multiple Cores

Does RISC-V need to be secure?

- SSD's shipped in high volume with RISC-V

→ isn't that a great attack vector?

Block Diagram



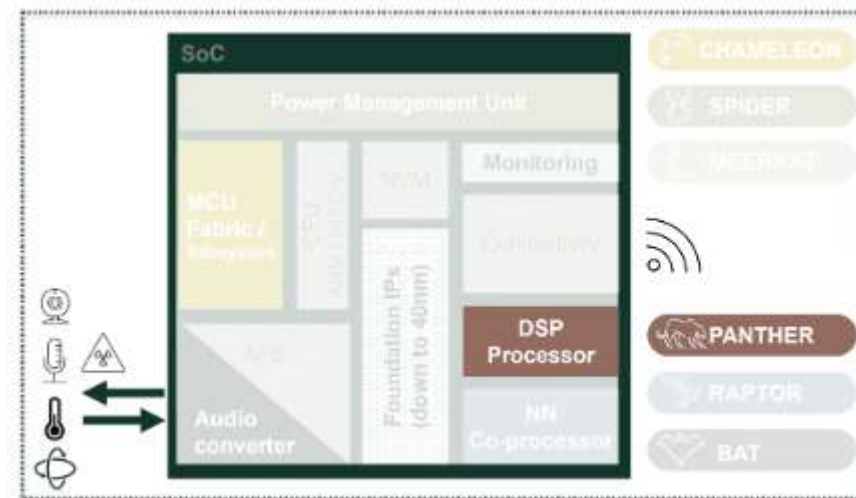
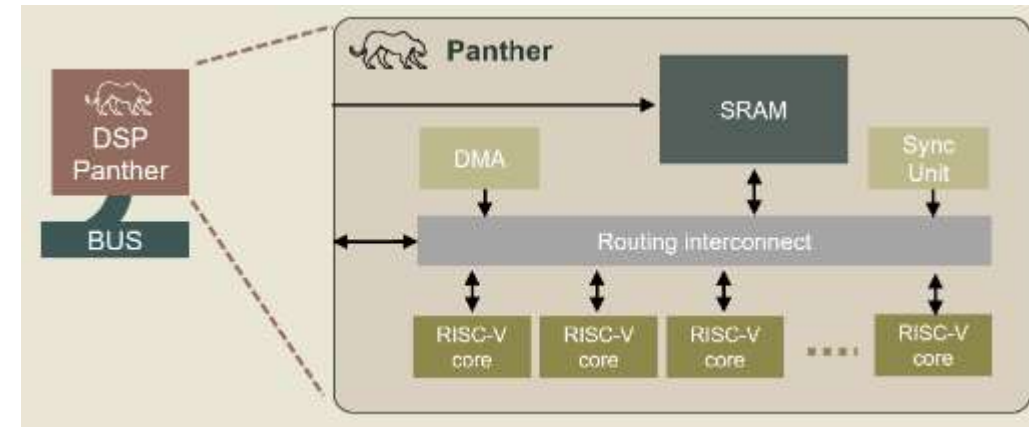
No one is using Open Source Cores

FALSE

- Many use, very few talk about it...
- Especially ASIC design houses use

Applications:

- IoT
- SSD
- AI
- Audio
- Connectivity



Can you design a commercial chip, shipping hundred of millions of it?

- Writing RISC-V Cores is easy
- Documenting it is more work
- Verifying it is a lot of work
- Keeping it up to date ...



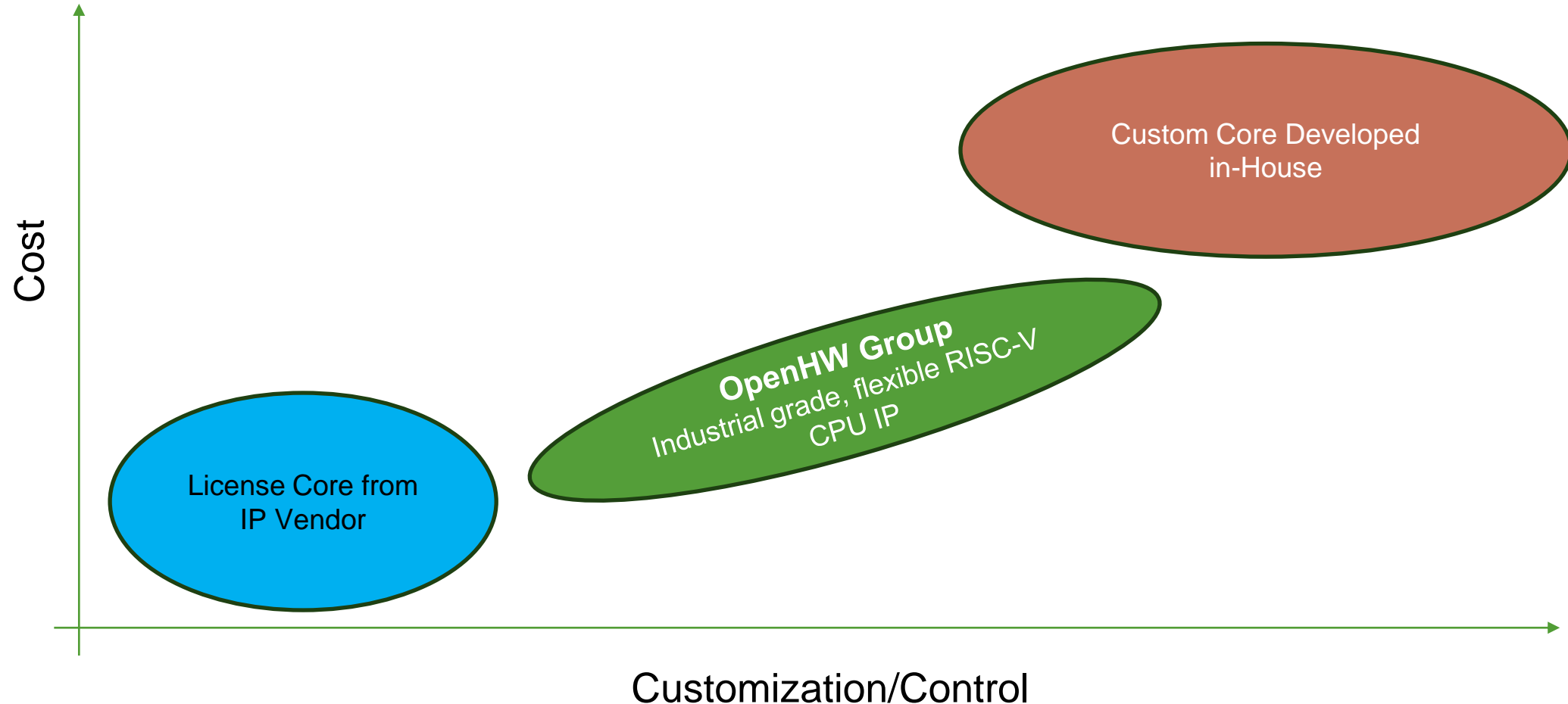
- ASICs are normally target by Millions, targeting best case various different end customers, with various different (undefined) use-cases

Why OpenHW Group is here

Why OpenHW Group is here Integrate RISC-V in your next SoC



- Buy vs. Make? Or can there be more flexibility?



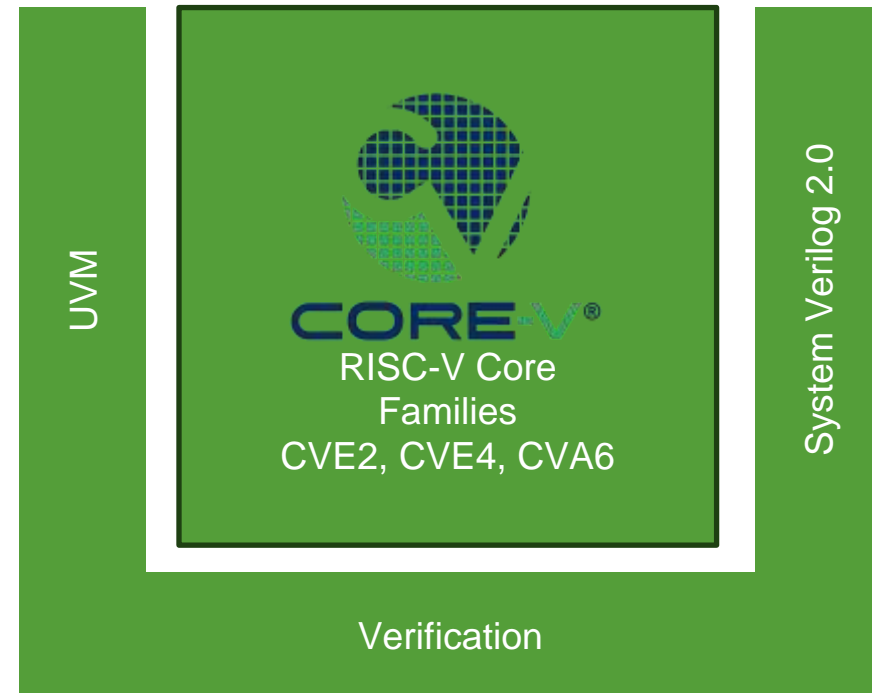
OpenHW Group deliverables

- License:
 - Apache 2.0/Solderpad
- Cores:
 - System Verilog



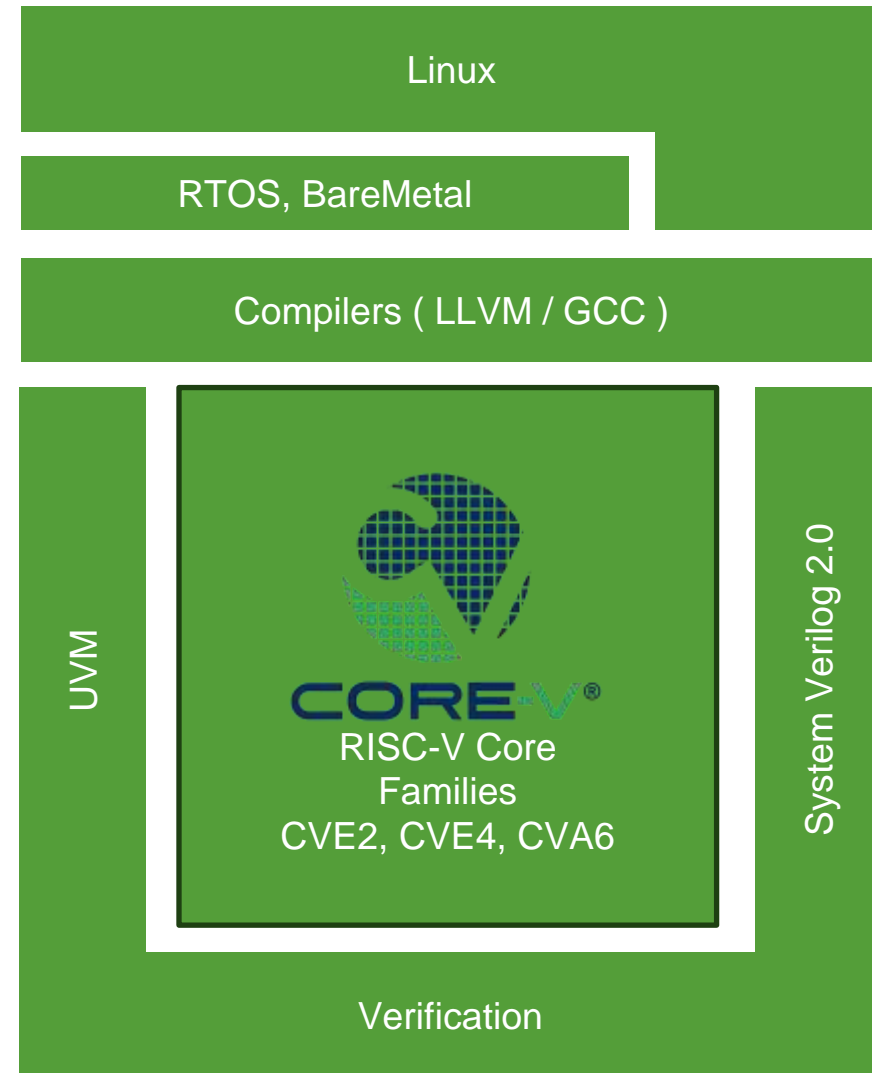
OpenHW Group deliverables

- License:
 - Apache 2.0/Solderpad
- Cores:
 - System Verilog
- Testbenches
 - UVM, System Verilog, a little python and tcl
- Tools
 - Siemens Mentor Questa, Cadence, Synopsys, Imperas,...



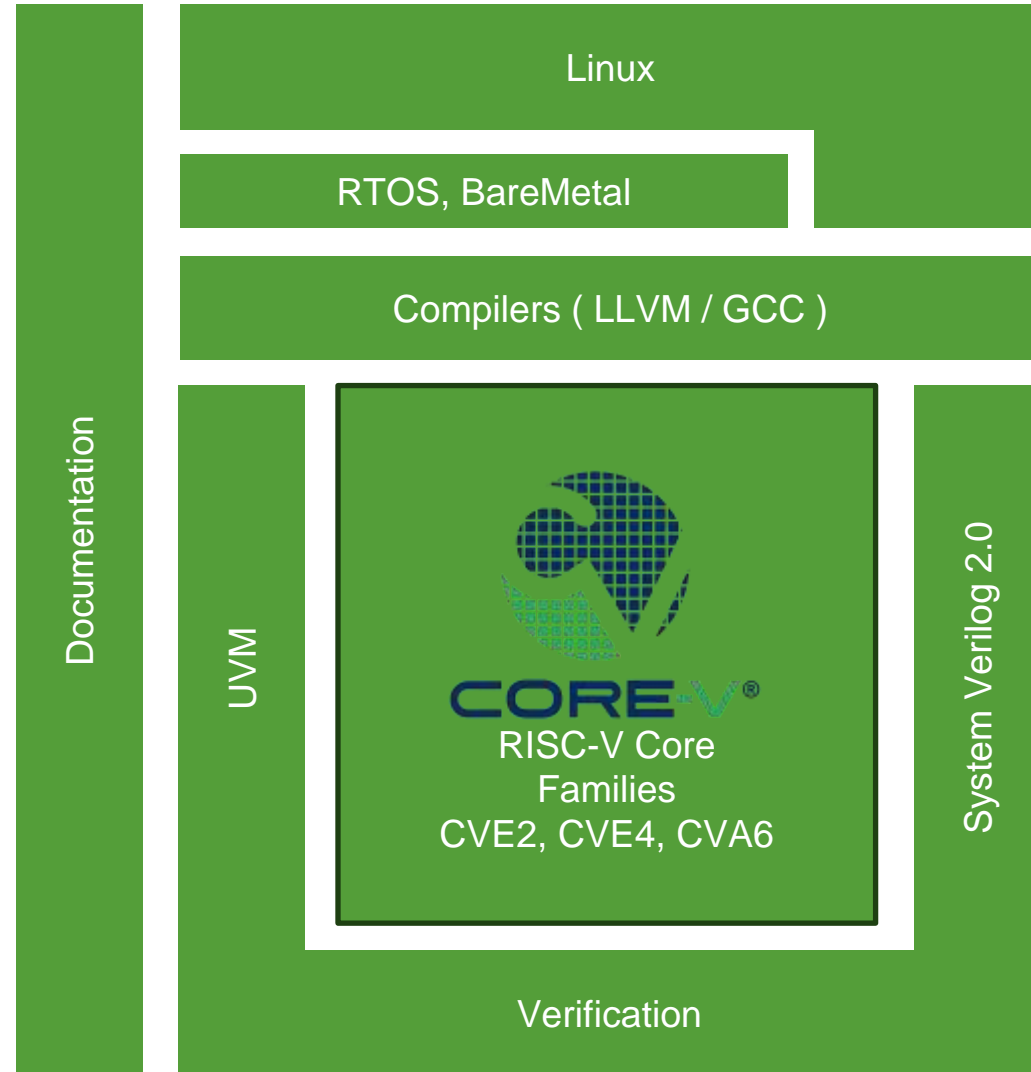
OpenHW Group deliverables

- License:
 - Apache 2.0/Solderpad
- Cores:
 - System Verilog
- Testbenches
 - UVM, System Verilog, a little python and tcl
- Tools
 - Siemens Mentor Questa, Cadence, Synopsys, Imperas,...



OpenHW Group deliverables

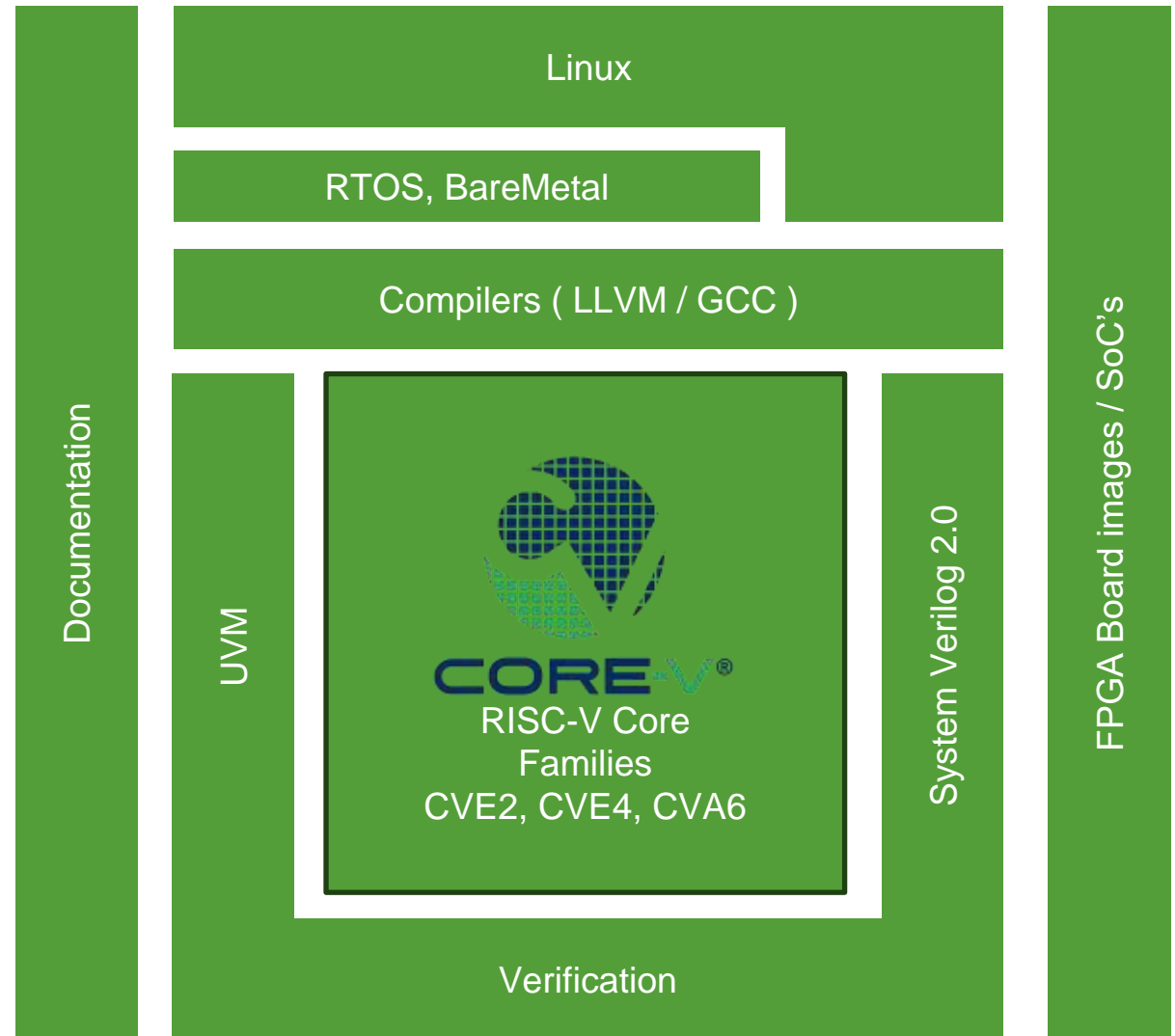
- License:
 - Apache 2.0/Solderpad
- Cores:
 - System Verilog
- Testbenches
 - UVM, System Verilog, a little python and tcl
- Tools
 - Siemens Mentor Questa, Cadence, Synopsys, Imperas,...



OpenHW Group deliverables



- License:
 - Apache 2.0/Solderpad
- Cores:
 - System Verilog
- Testbenches
 - UVM, System Verilog, a little python and tcl
- Tools
 - Siemens Mentor Questa, Cadence, Synopsys, Imperas,...

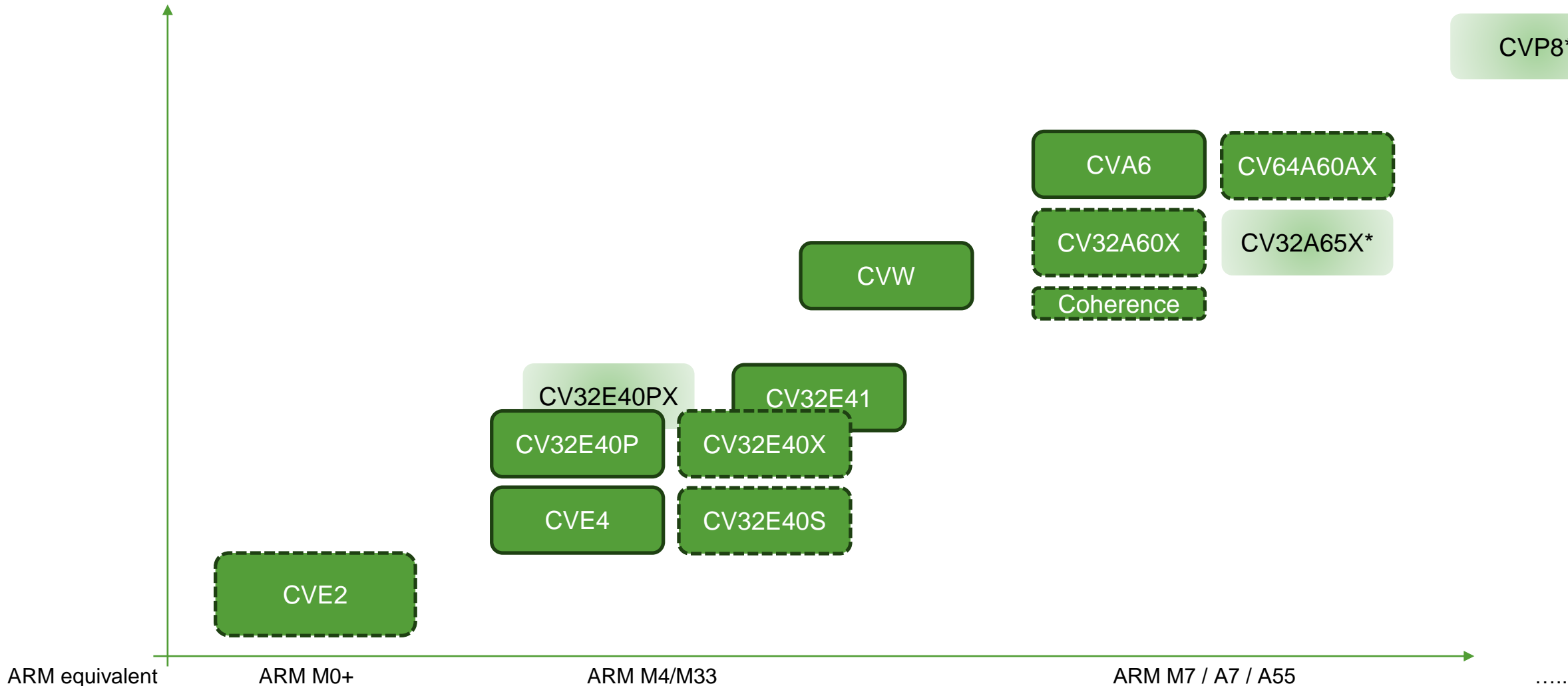


OpenHW RISC-V Roadmap

- ready
- In Develop.
- Planning*



CVP8*



Who are the OpenHW Group?

- Global, non-profit Organization (registered in Canada)
- Host and curate high quality RISC-V Cores (and related IP) for industrial usage
- Provide infrastructure, coordination and support
- Develop, Verify, Document - in line with industry best practice
- Driven by Members (Industry, Academia, Research)



OPENHW^{GROUP}
— PROVEN PROCESSOR IP —

Industry Members

100+ Members & Partners



ETH zürich

bluespec

BSC Barcelona Supercomputing Center
Centro Nacional de Supercomputación

PULP
Parallel Ultra Low Power



Universidade do Minho

FUTUREWEI
Technologies

SILICON LABS



PlanV

ALDEC
THE DESIGN VERIFICATION COMPANY

aLearn-Tec
adding value to open source HW

AMIO EDA

ASHLING

aws

beagleboard.org

BTA DESIGN SERVICES
your project, our team

CAES

CIRCUIT SUTRA
TECHNOLOGIES

codasip

CRYPTO QUANTIQUE

DATUM Empaiot.

ECSPEC **ESPRESSIF** **EMBECOSM**

CIRRUS LOGIC

GF

GREEN WAVES
TECHNOLOGIES

GroupGets

DOLPHIN
DESIGN

em em microelectronic

10x
ENGINEERS

Silicon Assurance

Jade
design automation

KALRAY

lpf **metrics** **MU** **NXP**
ELECTRONICS

OPERSYS

QuickLogic **Rumble Development** **SECURE THINGZ**

SIEMENS THALES imperas whalemicro

Alibaba Group
阿里巴巴集团

ZEROJNY LABS





OPENHW^{GROUP}
— PROVEN PROCESSOR IP —

Academic Members

100+ Members & Partners



ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA



Universidade do Minho



OPENHW^{GROUP}
— PROVEN PROCESSOR IP —



OPENHW GROUP
PROVEN PROCESSOR IP

Partner Ecosystem

100+ Members & Partners



AMD
XILINX

aws **cādence**



RvA
中国开放指令生态 (RISC-V) 联盟
China RISC-V Alliance

ayenne
GLOBAL, LLC

DIGILENT
A National Instruments Company



EUROPRACTICE

ECLIPSE
FOUNDATION

FOSSi
Foundation

GroupGets

LiP

OpenUK **ORCRO**



RISC-V **SYNOPSYS**

Accounting, Legal, Banking

BDO

MOORCROFTS
CORPORATE LAW

NORTON ROSE FULBRIGHT



OPENHW GROUP
PROVEN PROCESSOR IP

Open-Source Collaboration in the Semiconductor Industry

How do you organize that over multiple Companies?

Open-Source Collaboration in the Semiconductor Industry



- Open source enable a lot of more possibility's to handle things in different ways
 - RISC-V Spec: implement your own Core, get hands on, compare with others, learn
 -
- Industrial grade, open source Cores
 - Industry can deploy for products
 - Academia and Research can use the same Core
- Industry Partners and Academia collaborate
 - e.g.: Industry partner wondering if he can accelerate function X with dedicated HW accelerator, University can help to evaluate

Working Groups & Task Groups

- Board of Directors approves elected Chairs of Working Groups and has final approval of working group recommendations
 - Technical Working Group
 - Cores Task Group
 - Verification Task Group
 - SW Task Group
 - HW Task Group
 - **Safety & Security Task Group**
 - Marketing Working Group
 - University Outreach Task Group
 - OpenHW Asia Working Group
 - OpenHW Europe Working Group
- Together with internal OpenHW Group engineering staff, member company development engineers (FTEs / ACs) establish and execute [OpenHW Group projects](#)
- 20+ active projects across CORE-V RTL, Verification, GCC / LLVM, IDE, RTOS, FPGA, SoC, etc. with more projects in the pipeline



Technical Working Group (TWG)





- Co-Chair: Jérôme Quévremont, Thales Research & Technology

THALES

- Drive the overall technical direction, development roadmap and project execution for all technology related activities within the OpenHW Group and oversee the Task Groups
 - TWG is essentially the OpenHW Group company's "R&D / Engineering Organization"
- OpenHW Group engineering release methodology is based on the Eclipse Development Process
 - All OpenHW Group Platinum / Gold / Silver members are also Solutions members of the Eclipse Foundation

ECLIPSE
FOUNDATION

Cores Task Group

- Chair: Arjan Bink, Silicon Laboratories  
- Vice-Chair: Jérôme Quévremont, Thales Research & Technology
- Define and develop feature and functionality roadmap and the open-source IP for the cores within the OpenHW Group.
- Initial contribution of open-source RISC-V cores mainly from [ETH Zurich PULP Platform](#)  
- The OpenHW Group is the [official committer for these repositories](#)

Verification Task Group



- Chair: Jean-Roch Coulon, Thales Silicon Security
- Vice-Chair: -----



- Develop best in class verification test bench environments for the cores and IP blocks developed within the OpenHW Group.

SW Task Group



- Chair: Paolo Savini, Embecosm
- Vice-Chair: Yunhai Shang, Alibaba T-Head
- Define, develop and support SW tool chain, operating system ports and firmware for the cores and IP developed within the OpenHW Group
- SW TG active projects include: GCC / LLVM, IDEs, FreeRTOS, HAL, CORE-V MCU SDK, etc.



SW Task Group



- Compilers are fully up streamed for CV32E40Pv2
 - GNU Tools/GCC 14.1 to be fully up streamed for CVE4 by Apr 2024
 - Clang/LLVM 18 to be fully up streamed for CVE4 by Jan 2024
- Features include:
 - Core awareness
 - Xpulp integration
 - native HWloop support



SW Task Group



- QEMU



- RTOS support
 - FreeRTOS => 10.3.0
 - Zephyr 2.4, 2.5,...



- Linux OS Support

- Linux Kernel 6.2 Support
- uBoot and OpenSPI
- buildroot
- Fedora and RedHat working on Linux Support



HW Task Group

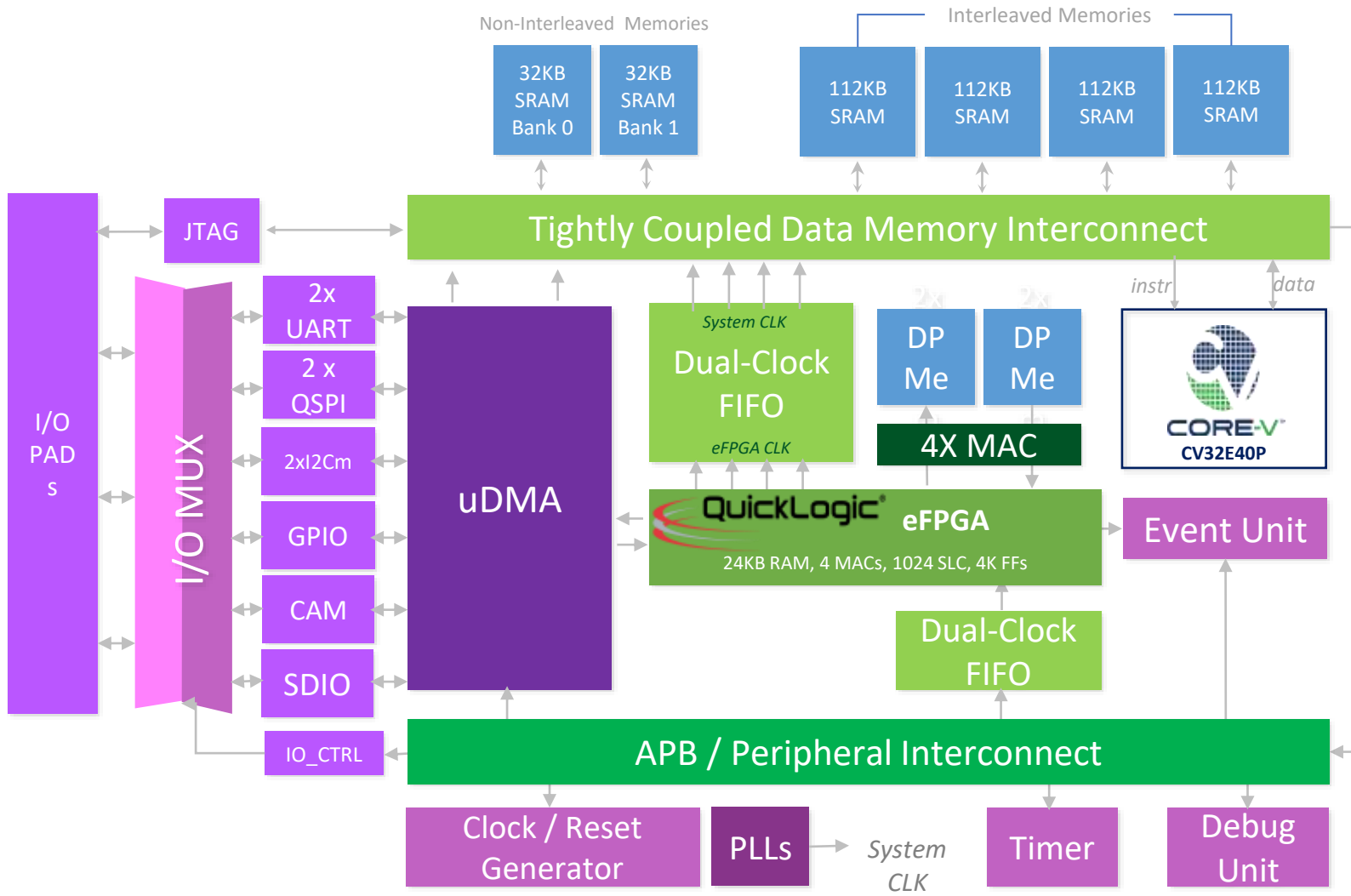
- Chair: Tim Saxe, QuickLogic
- Vice-Chair:-----

- define, develop and support SoC and FPGA based evaluation / development platforms for the cores and IP developed within the OpenHW Group.





CORE-V[®] MCU Tapeout 1st half 2023



- Real Time Operating System (e.g. FreeRTOS) capable
~400+MHz CV32E4 MCU
- Embedded FPGA fabric with hardware accelerators from QuickLogic
- Multiple low power peripheral interfaces (SPI, GPIO, I2C, HyperRAM, CAMIF, etc) for interfacing with sensors, displays, and connectivity modules
- Built in 22FDX with





TRISTAN Overview

“Together for **RISc-V Technology and ApplicationNs**”

TRISTAN is a **36 month** KDT-JU (Key-Digital Technology Joint Undertaking) program under the Horizon-Europe calls via a **public-private partnership** focused on research and innovation to reinforce the EU’s strategic autonomy in the electronic components and systems sector

There are **46 participants** in TRISTAN and several are part of OpenHW Group ecosystem

THALES



NXP

SIEMENS

ETH zürich



GREENWAVES
TECHNOLOGIES

codasip

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA



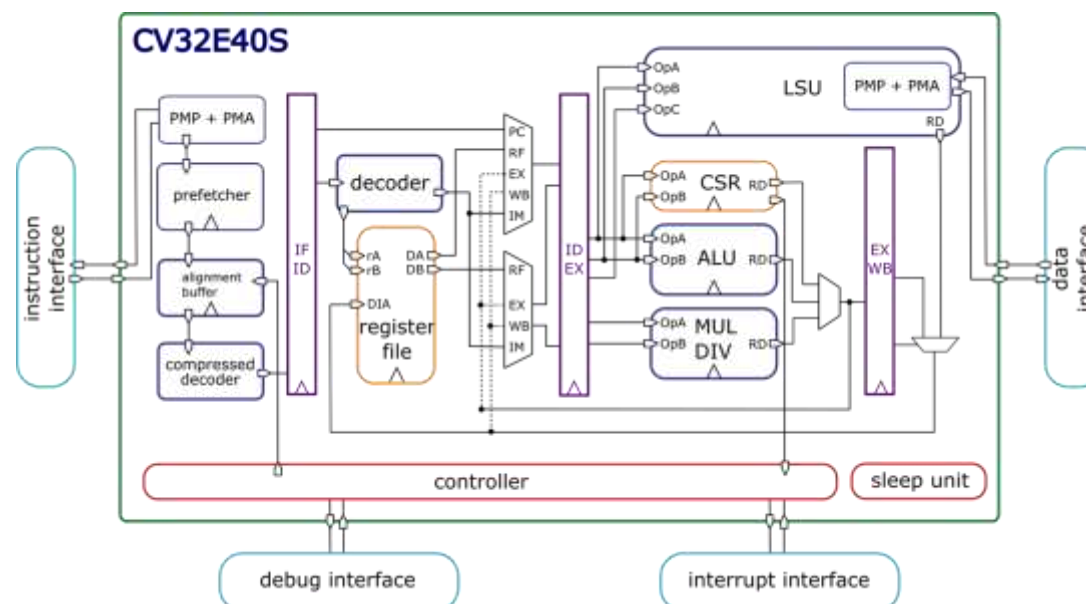
OPENHW
GROUP
PROVEN PROCESSOR IP

CV32E40S – PA / TRL 4

- 4-stage, in-order, single-issue
- RV32[I | E][M | Zmmul]

Zca_Zcb_Zcmp_Zcmt
 [Zba_Zbb_Zbc_Zbs_Zkt_Zbkc]
 ZicsrZifencei**Xsecure**

- M/U-mode, CLINT or CLIC, OBI, ePMP, PMA, bus error
- **Xsecure**: Custom Security Extensions
- Project goal: industrial grade (TRL 5)



CV32E40S - Security



- Xsecure extension:
 - Security Alerts
 - Data Independent timing
 - Dummy instruction insertion
 - Random instruction for hint
 - Register File in ECC
 - Hardened PC/CSR's

Check our Manual:



Examples of community collaboration (excerpts only)

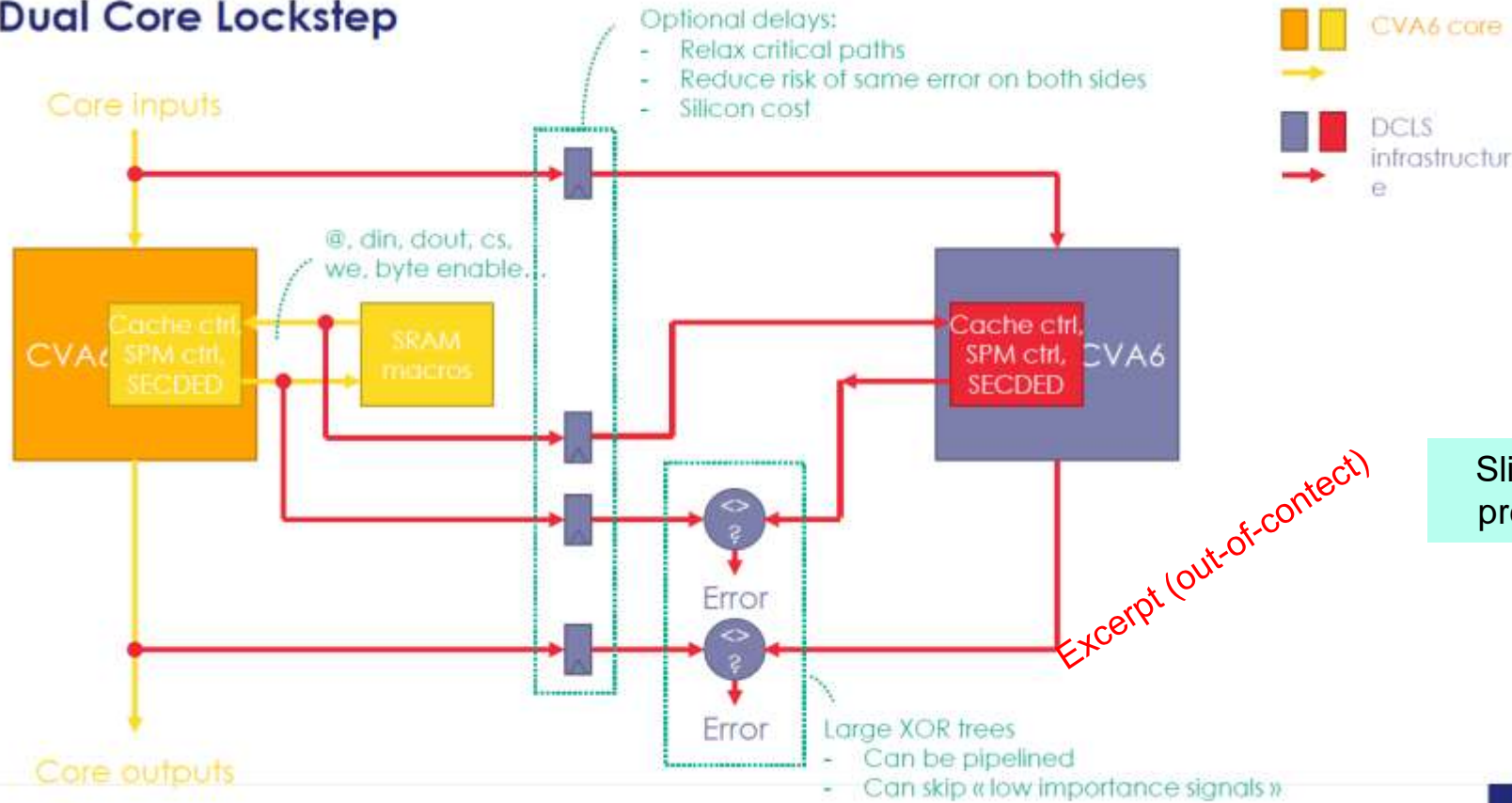
ECC

- An ECC project for CVA6 needed
- Parity
 - Cheap, but no correction capabilities
 - Useful if data is read-only (instruction caches) or replicated (write-through data caches): upon an error, invalidate and fetch again
- SECDED
 - Expensive (impacts latency), but provides error correction capabilities
 - Useful if data can be modified (write-back caches): upon an error, correct it
- ECC codes can be used for end-to-end protection
 - Send data to other cores, memory, etc. along with ECC code

Approach for CVA6 by Thales



Dual Core Lockstep



Slide taken from: Sebastien Jacq's presentation in April-2024 meeting

Possible Approach for CVA6 by Thales



- Characteristics
 - Do not replicate caches (rely on SECDED)
 - Compare all activity reaching caches (including accesses that hit in caches)
- Pros/cons
 - (pro) Lower area cost than full core replication with caches
 - (pro) Errors can be anticipated w.r.t. full core replication since we don't have to wait until data is evicted from cache
 - (cons) Some parts of the cache may remain unprotected (e.g., decoding logic leading to accessing wrong row/column)
 - (cons) Some errors that could be masked are reported already
 - (cons) Hard faults in parts of the cache may not allow operation due to lacking any sort of redundancy

Excerpt (out-of-context)



Let us be your Core Provider



- OpenHW as a platform to host. Maintain and verify high quality, industrial grade Cores
- Academia an Industry to work together
- Fully open Cores (RTL, Verification) challenge our RTL!
- Security is important, lets work together





OPENHW^{GROUP}[®]
— PROVEN PROCESSOR IP —

and



CORE-V[®]



- OpenHW Group & CORE-V Family of open-source RISC-V cores for use in high-volume production SoCs
 - Visit www.openhwgroup.org for details
 - Learn more at [OpenHW TV](#)
- Follow us on Twitter [@openhwgroup](#) & [LinkedIn OpenHW Group](#)
- Talk to us: flo@openhwgroup.org

Overview RISC-V Cores

CVE2 / CVE4 / CVA6

TRL Levels as Utilized by OpenHW



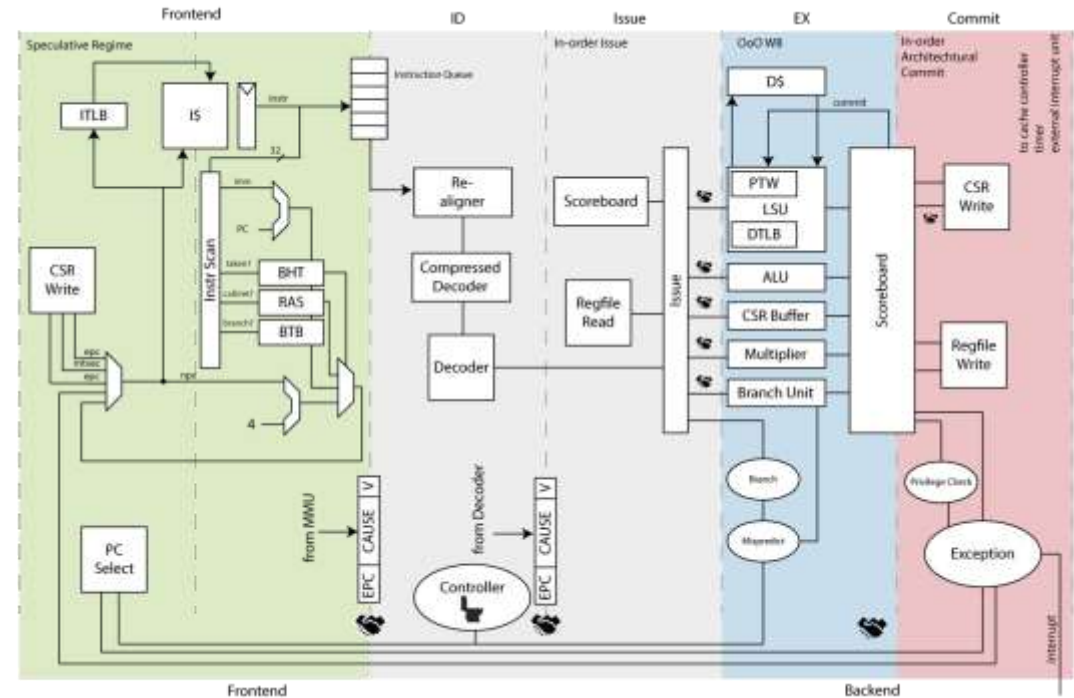
TRL = Technical Readiness Level

TRL	OpenHW Utilization
1-Basic Principles Observed	<ul style="list-style-type: none">• OpenHW research projects may target TRL-1 as project output, e.g. to develop novel approaches to core or accelerator architecture
2-Concept Formulation	<ul style="list-style-type: none">• Core IP or accelerator development projects are typically initiated as TRL-2 concepts, identifying principles and applications of the IP• The OpenHW Project Concept Gate output includes a TRL-2 description of the Core IP
3- Proof of Concept	<ul style="list-style-type: none">• Core IP or accelerator development projects will pass through TRL-3 as the (RTL) design completes.• Proof of concept is shown by core compilation and demonstration of basic operations (e.g. Linux booted, coremark results, hello-world)
4- Component Prototype	<ul style="list-style-type: none">• Core IP or accelerator projects will pass through TRL-4 as they produce preliminary PPA results (via synthesis scripts for FPGA or ASIC) and/or run preliminary application code, such as an accelerator running machine learning code.
5- Subsystem Designed and Tested	<ul style="list-style-type: none">• Core IP projects reach TRL-5 as they complete full verification. The OpenHW RTL Freeze checklist process verifies that the design is fully ready for industrial adoption.
6-Functional (Alpha) Prototype	<ul style="list-style-type: none">• OpenHW IP that is integrated into an MCU system or other device reaches TRL-6 as prototype Silicon is fabricated and demonstrated on a development board or other platform.
7-Field Demonstration Prototype	<ul style="list-style-type: none">• OpenHW IP that is integrated into an MCU system or other device reaches TRL-7 as prototype Silicon is fabricated, deployed and demonstrated in the field.

CVA6



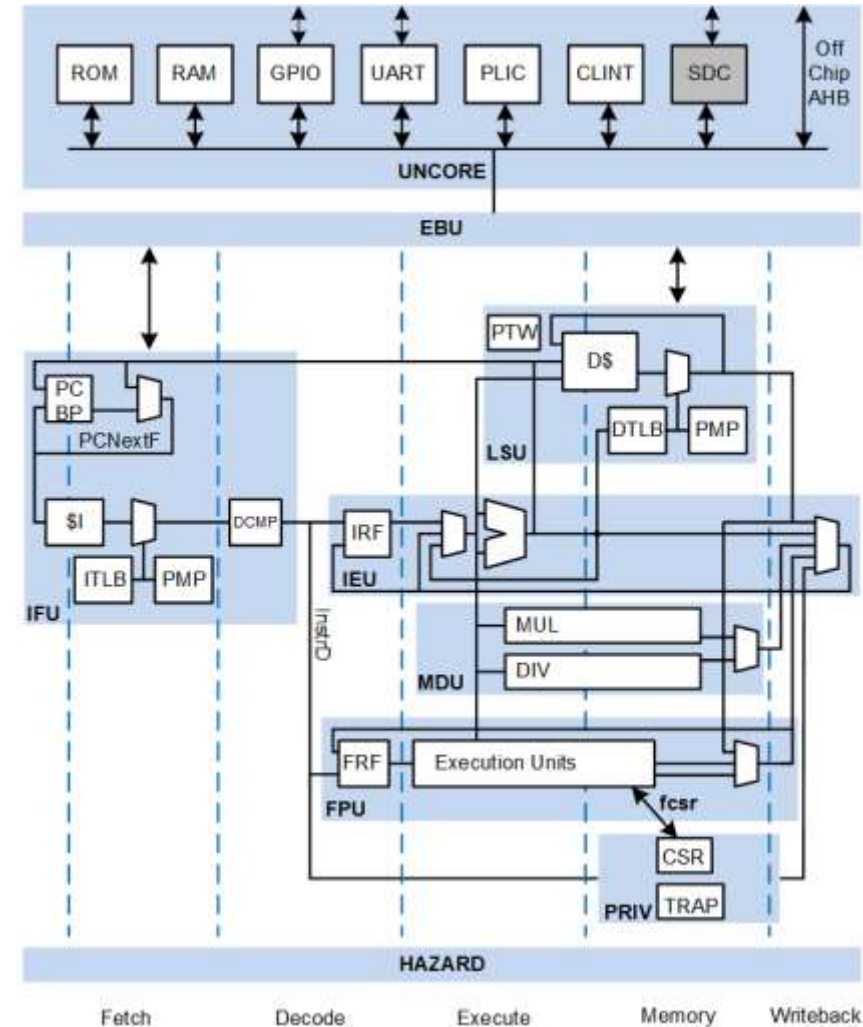
- 6-stage, in-order, single-issue
- RV{32 | 64}IMAC[FD][V]Zicsr
- M/S/U-mode, CLIC, AXI
- Flexible application core
 - Linux-compatible thanks to MMU
 - 32 or 64 bit (CV32A6, CV64A6) from same RTL (64b from ETH, 32b from Thales)
 - L1 caches
- Project goal: industrial grade (TRL 5)
 - Currently drafting specifications, entry point for next stages



CVW – PC / TRL 4

- 5-stage, single-issue, in-order
- RV{32,64}{I,E}[M][F[Zfh][D][Q]][A][C]
- Cache
 - none, associativity, capacity
- Branch Prediction
 - none, 2b BHT, GSHARE
- MMU and TLB
 - entries, sv32/sv39/sv48
- M, S, U Privileged support
- CLIC (and PLIC support)
- Targets both FPGA and ASIC

- Project goal: optimized CPU but still TRL 4



CVW – preliminary PPA



- **CV32WG**
 - COREMARK/MHz: **2,54**

Technology	Frequency	Area	Comments
28nm	~1GHz	N.A.	Biggest configuration

Upcoming Textbook:
RISC-V System-on-Chip Design
by Harris, Stine, Thompson, and Harris

