Formal Verification of PULPino and Other RISC-V SoCs

11-12 June 2019, Zurich

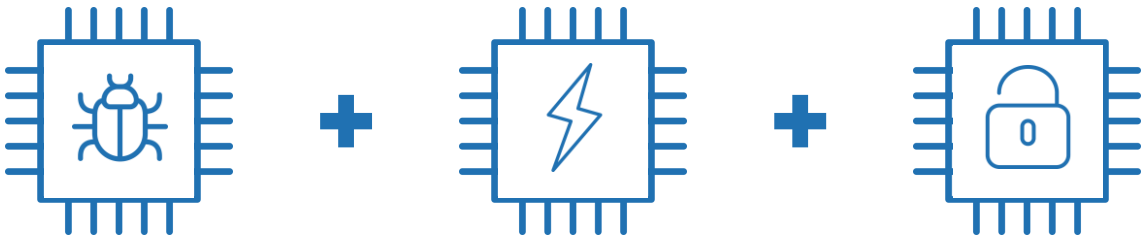
Nicolae Tusinschi | nicolae.tusinschi@onespin.com

Product Specialist Design Verification | **OneSpin Solutions**

IC Integrity

Reliable, safe, secure, and trusted SoCs/ASICs/FPGAs

Functional Reliability + **Functional Safety** + **Trust & Security**



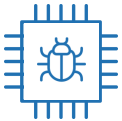
OneSpin provides certified **IC Integrity Verification Solutions** to develop reliable, safe, secure, and trusted integrated circuits.

Leading-Edge Formal Technology

Targeting Critical Hardware Verification Challenges

Functional Reliability

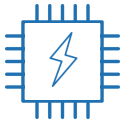
Rigorous coverage-driven functional verification from block to chip, leveraging formal technology



- Design Exploration
- Protocol Violations
- Integrate Formal/Sim Coverage
- End-to-End User Assertions
- HLS/SystemC Verification
- Synthesis/P&R Errors

Functional Safety

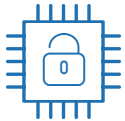
Safety analysis and higher diagnostic coverage to meet strict certification requirements



- FMEDA of Complex SoCs
- Failure Mode Distribution
- Avoid Excessive Fault Simulations
- Measure Diagnostic Coverage
- ISO 26262 Compliance
- Tool Qualification

Trust and Security

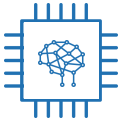
Automated detection of RTL Trojans and hardware vulnerabilities to adversary attacks



- Denial of Service
- Data Leakage
- Privileges Escalation
- Data Integrity/Confidentiality
- Hardware Backdoors
- Hardware Trojans

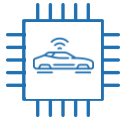
OneSpin 360® Formal Platform

Heterogeneous Computing



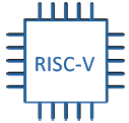
Thorough verification of complex SoC platforms used for 5G wireless, IoT, and AI applications

Automotive and Industrial



Systematic bug elimination and metrics on proper handling of random errors in the field

RISC-V



Proof of compliance to instruction set architecture (ISA) with no gaps or inconsistencies

OneSpin Solutions and Services

RISC-V Background

"The Free and Open RISC ISA"

- Developed at the University of California, Berkeley

- Supported by RISC-V Foundation
  - More than 200 members, including OneSpin
    - Hardware vendors, software vendors, and universities
  - Many events held worldwide every year

- Instruction Set Architecture (ISA) designed for flexibility
  - Implementable on a wide range of microarchitectures
  - Significant body of supporting software already available
  - Designed to allow user extensibility

- Free, open-source, and royalty-free
  - Anyone can design, manufacture, and sell RISC-V chips and software

RISC-V Outlook

Great potential if challenges are overcome

Challenges

Must compete with older, well-established ISAs

- RISC-V IP core providers must verify compliance
- Core integrators need to confirm compliance

High safety, security, and trust requirements

- Must ensure core is free of hardware Trojans and malicious logic

Requirements

Third-party compliance verification

Instruction Set Architecture (ISA) captured with standard SystemVerilog Assertions (SVA)

100% formal proof for core's implementation of all instructions against the ISA specification

Proof that core does what it is supposed to do and does *not* do what it is *not* supposed to do

Formal trust verification that core contains no hardware Trojans or other unintended functionality

Functional Verification of RISC-V Cores

Does the RTL precisely implement the RISC-V ISA spec?

RISC-V processor cores are hard to verify

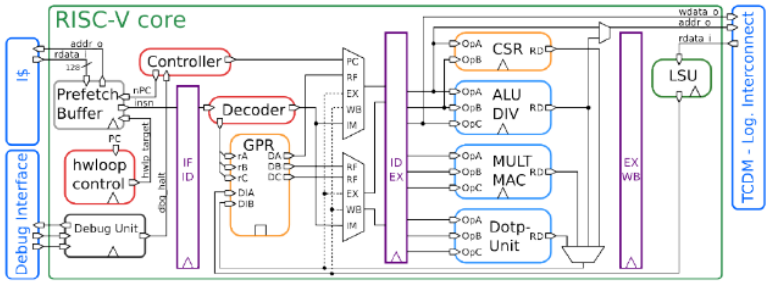
- Complex microarchitectures to achieve power/price/performance targets
- Branch prediction, forwarding, out-of-order execution …

Formal verification

- Exhaustive analysis finds corner-case bugs
- The only technology with potential to prove absence of bugs or missing functionality

Challenges

- Complexity issues lead to bounded proofs
- Hard to write good quality, reusable assertions



OneSpin RISC-V Integrity Verification Solution

Industry's first formal RISC-V compliance solution

RISC-V ISA formalized as SystemVerilog Assertions (SVA)

- Decoupled from microarchitectural details

Enables 100% unbounded formal proof for implementation of all instructions against ISA specification

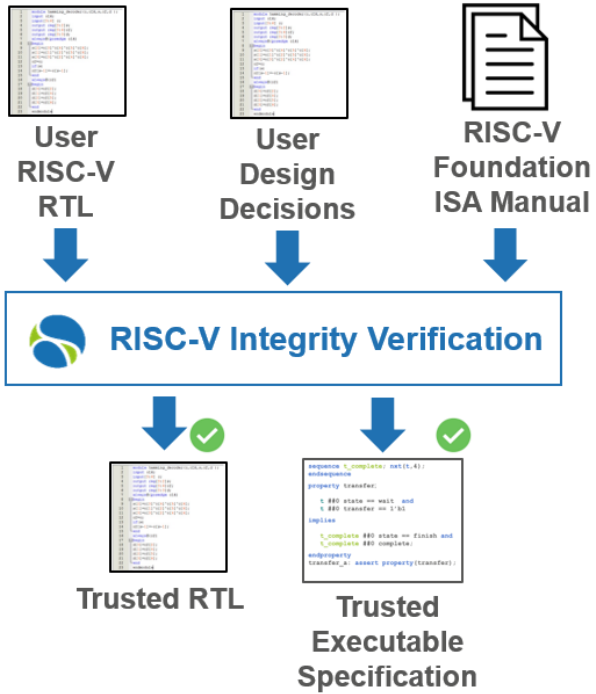
- Guarantees that core is fully compliant

Enables verification of entire core implementation

- Leverages user-provided microarchitectural details

Detects any extra functionality beyond the ISA specification

- Formally verifies trust



 |

OneSpin's GapFreeVerification™

Proof that RISC-V assertions cover all possible core behavior

RISC-V ISA expressed using OneSpin's Operational Assertions

- Standard SystemVerilog assertions following a strict template
- Assertions define results for each instruction
- Assertions cover instruction decode to completion

Enables automated unbounded proof of all assertions

Unexamined logic cause failure of completeness proof

- Formal check of core's RTL against the RISC-V ISA
- Reveals any hidden logic that impacts core's functionality

RISC-V Integrity Verification Solution in Use

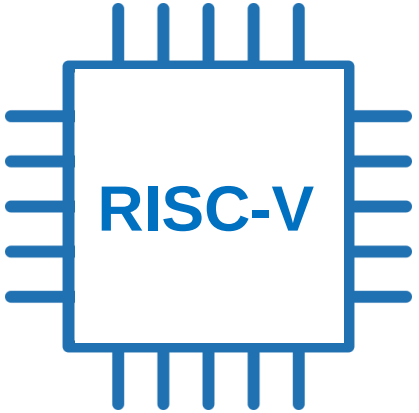
Solid experience on open-source RISC-V designs

Solution architected for easy use

- Defined process to map to new implementation

Solution has been verified on Rocket Core implementation

Solution has been verified on PULPino SoC Platform

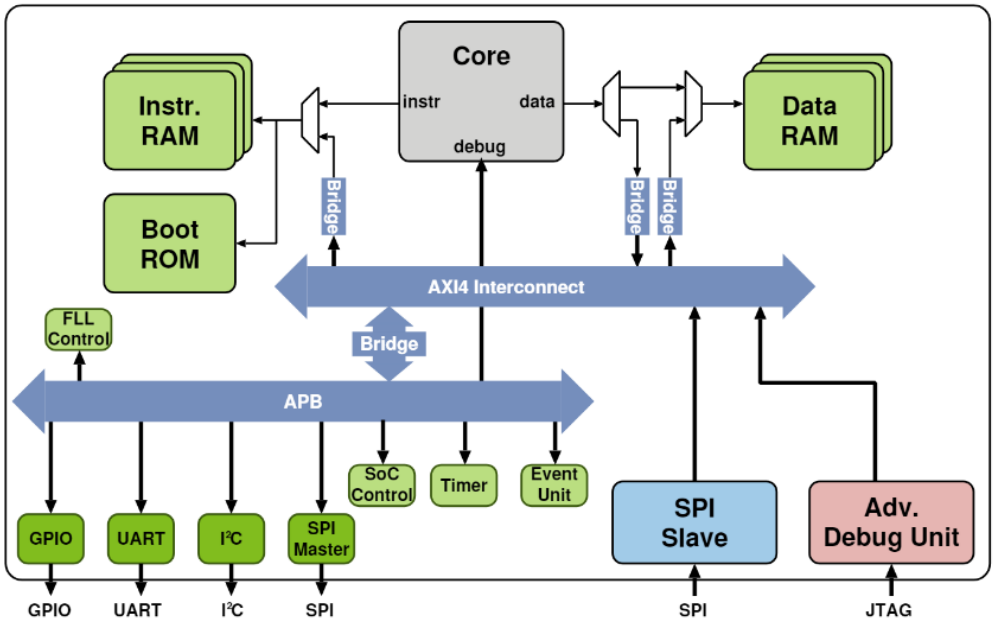


Additional results have been presented at conferences:

- “Complete Formal Verification of RISC-V Processor IPs for Trojan-Free Trusted ICs” at Government Microcircuit Applications & Critical Technology Conference (GOMACTech) March 25-28 in Albuquerque, New Mexico
- “Unbounded Formal Verification of RISC-V CSRs with Interval Property Checking” at Design Automation Conference (DAC) June 2-6 in Las Vegas, Nevada

Parallel Ultra Low Power (PULP) Platform

Open-source project started by ETH Zürich and University of Bologna



PULPino Platform

Part of the PULP project

Single-core SoC platform

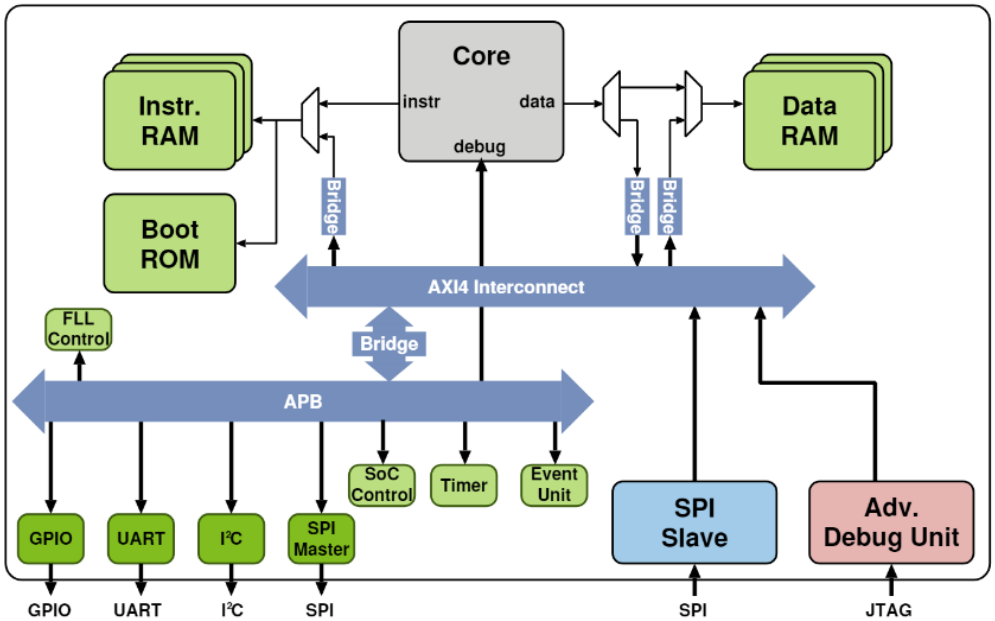
Built for two open-source **RISC-V** cores

Rich set of peripherals

https://github.com/pulp-platform/pulpino

PULPino Integrity Verification

Covering the entire RISC-V SoC



Uses OneSpin's suite of formal apps

Examples

- Floating-point unit (FPU) verification
- AMBA protocol compliance
- I²C protocol compliance
- Safe RTL inspection
- Reachability analysis
- Interconnect verification
- X-propagation

PULPino Integrity Verification

Selection of findings

Floating-Point Unit

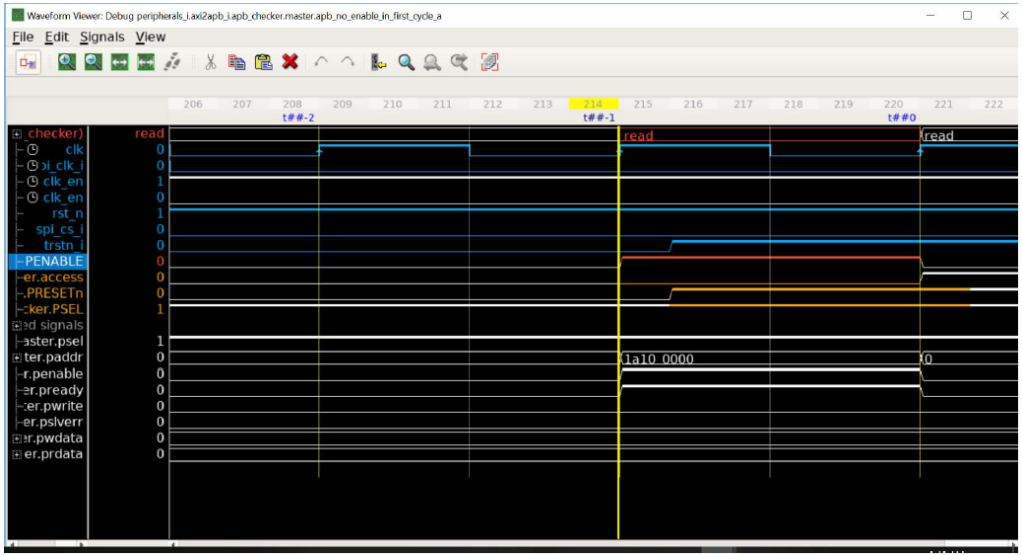
- Addition (-0 + -0) delivers incorrect result
- **Bug confirmed by PULP**

Safe RTL Inspection

- ***unique*** case violation results in unexpected instruction decode
- **Bug confirmed and fixed by PULP**

APB Interface

- PENABLE signal violates address phase protocol



Sample trace showing APB protocol violation

Thank you!

For questions or more information on OneSpin's RISC-V Integrity Verification Solution, get in touch:

nicolae.tusinschi@onespin.com