Unbounded Formal Verification of RISC-V CSRs with Interval Property Checking

Nicolae Tusinschi | nicolae.tusinschi@onespin.com
Product Specialist Design Verification | OneSpin Solutions

12 – 13 March 2019, Taiwan
Functional Verification of RISC-V Cores

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

RISC-V processor cores are hard to verify

• Complex micro architectures to achieve PPA targets
• Brach prediction – Forwarding – Out-of-order execution …

Formal verification

• Exhaustive verification finds corner-case bugs
• The only technology that can prove bug absence

Challenges

• Complexity issues lead to bounded proofs
• Hard to write good quality, reusable assertions
Interval Property Checking (IPC)  
Reusable SystemVerilog assertions achieving unbounded proofs

Anatomy of an IPC assertion
• Does not start from reset but from a generic valid state
• Limited number of cycles (interval) to reach generic valid state
• Decouple ISA spec requirements from micro architectural details

Application to the RISC-V Rocket core
• Poster shows a selection of results
• Instructions, interrupts, exceptions that access CSRs

Part of a comprehensive solution
• RISC-V integrity verification solution
• Prove bug absence for the entire core
• Prove absence of hidden, malicious logic
Thank you!

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

nicolae.tusinschi@onespin.com