framatome

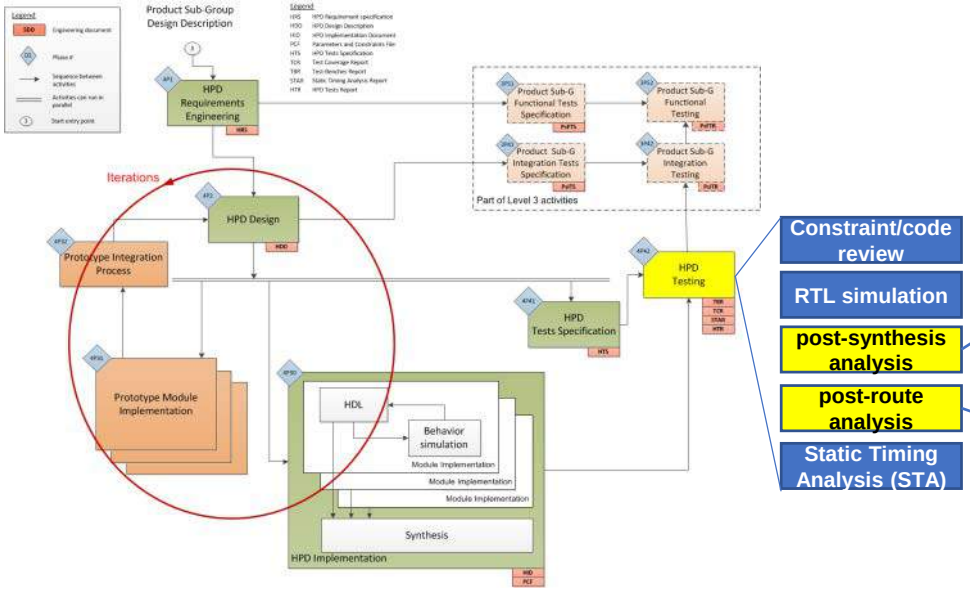
Using Sequential Equivalence Checking to Verify Implementation of FPGAs for NPP Applications

Hayder Haouaneb, Framatome

Vlada Kalinic, OneSpin Solutions

Budapest, 14/10/2019

Equivalence Checking in the V&V flow



HPD lifecycle

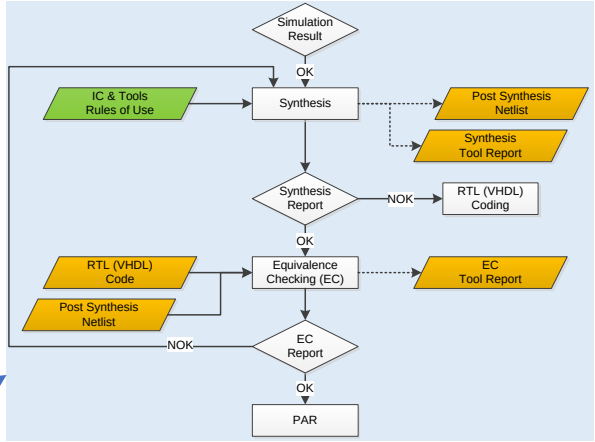
Constraint/code review

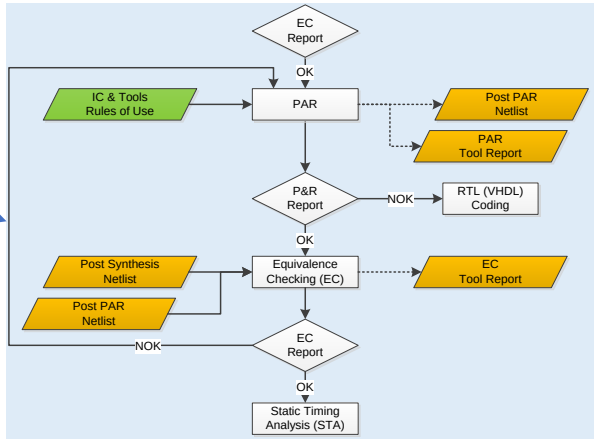
RTL simulation

post-synthesis analysis

post-route analysis

Static Timing Analysis (STA)





Post Route Analysis

Alternative Method, Equivalence Checking

An alternative method to post-route dynamic timing simulation is to use a tool that checks that RTL and physical description level are mathematically equivalent.

Standard IEC 62566 [1], Section 8.4.2.2 requires the HPD development process to “produce timing information to supplement the RTL description by back-annotation in order to precisely simulate the temporal behavior taking into account all delays associated with gates and wires”, similar see Section 8.4.8. In addition, standard IEC 62566 [1], Section 9.7.2 requires tests “after the implementation phase to confirm that the post route description complies with the timing constraints, taking account of the timing information provided by the tools and libraries”, similar see Section 9.7.3.

However, according to standard IEC 62566 [1], Section 8.4.4.2 and 8.4.4.3, a dynamic timing analysis is not mandatory. The post-route analysis can be done by demonstrating that the post-route description is mathematically equivalent to the RTL description, and post-route description complies with the timing constraints.

Post Route Analysis

The Equivalence Checking is motivated by :

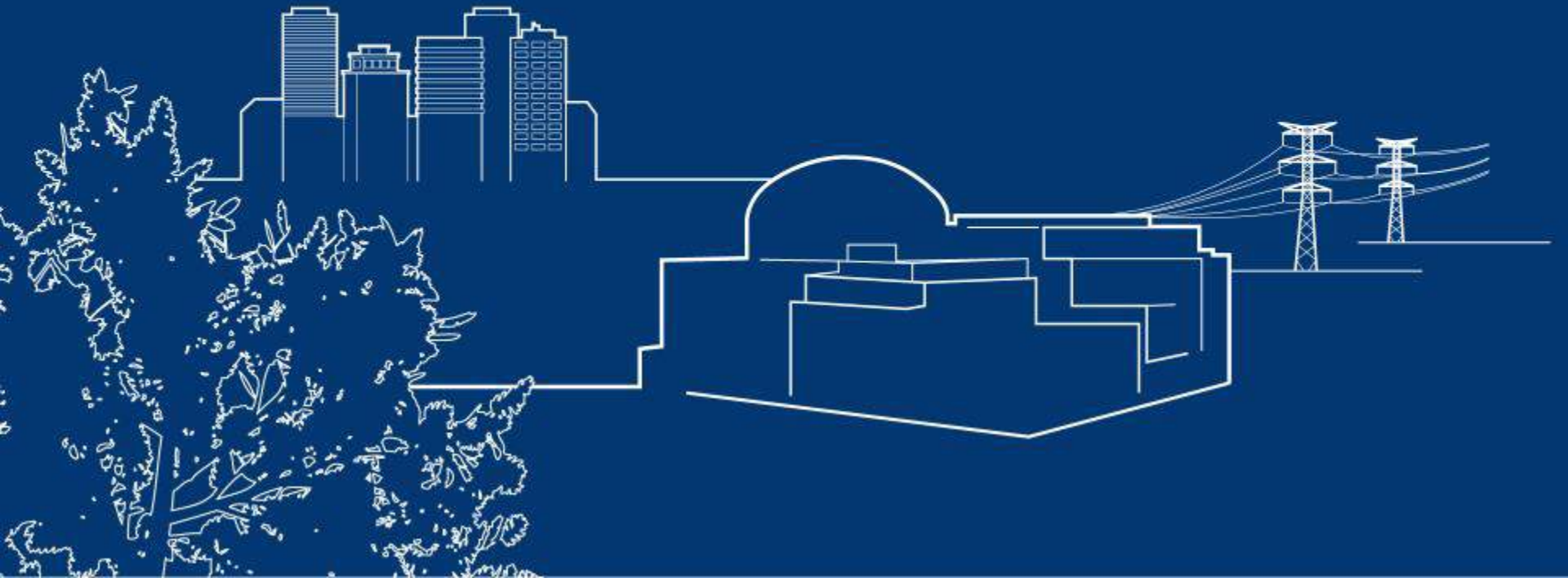
1. Exhaustive tests: Post-route dynamic timing simulation is not exhaustive and might not discover errors introduced by the place-and-route tool.
2. Tools independence: HPD Verification tools used to check the output of HPD development tools are required to be independent from the HPD development tools ➔ Systematic errors included within the HPD development tool can also be included within the HPD verification tool.
3. Complexity: Systematic errors are difficult to find by simulations of the HPD netlist. The excitation of these errors is often by unexpected corner cases.

DESIGN FLOW ISSUES
bus connection ordering
coincident read discrepancies
wrong FSM re-encoding
non-driven or unconnected wires
incorrectly coded pipeline
incorrect BRAM parameter settings
clock gating for low power issues
PAR connection issues

Alternatively or complementarily, the post-route analysis can be done by demonstrating that

- **the post-route description is mathematically equivalent to the RTL description, and**
- **post-route description complies with the timing constraints.**

framatome



Implementation Verification using Equivalence Checking

How to assure (and convince your certification agency) that the FPGAs in your NPP follow your specification

Hayder Haouaneb, Framatome

Vlada Kalinic, OneSpin Solutions

Budapest, 16/10/2019

Modern FPGA Design Flow Issues

New architectures present new challenges

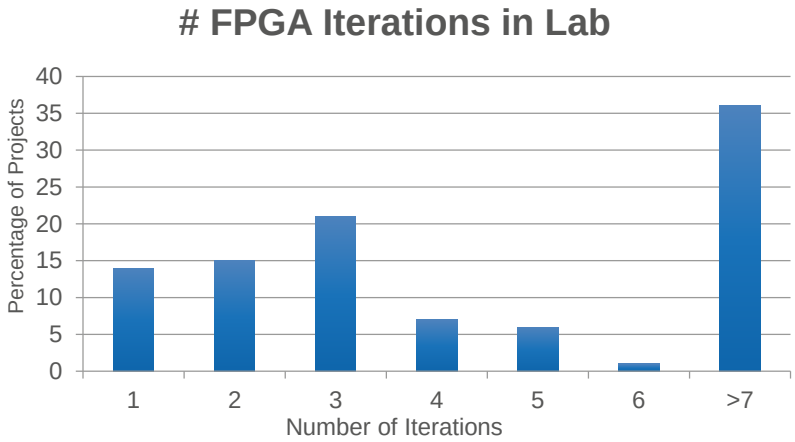
- FPGA requires advanced optimizations

- Systematic error probability increases
  - Created by design flow refinement automation
  - Hard to find, require days of debug
  - Requires many complex tests to discover
  - May cause damaging field issues
  - Limits use of powerful optimizations

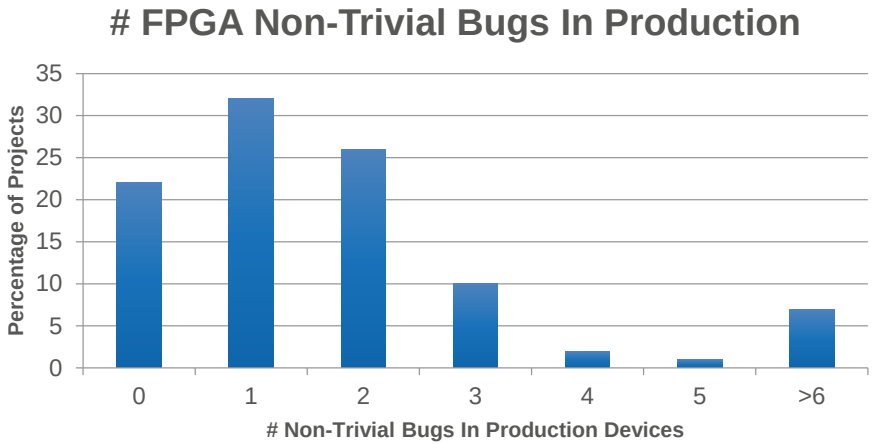
- Prototype-based testing no longer viable
  - Excluding systematic errors require many additional tests
  - Errors often triggered by unexpected corner cases
  - Safety-critical regulations mandate formal techniques

FPGA Iterations and Production Bugs

Time wasted and production higher than expected



78% of projects have non-trivial bugs in production devices



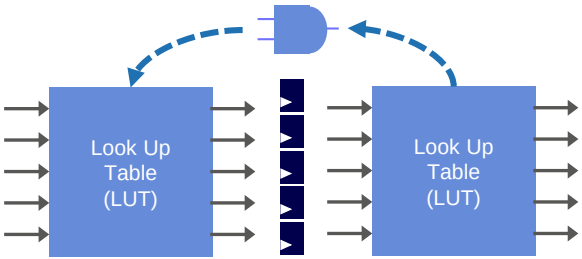
Source: Wilson Research 2016

 |

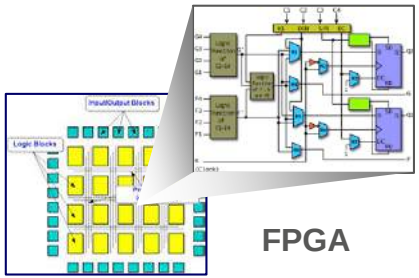
FPGA Synthesis Optimization

Key factor in design performance

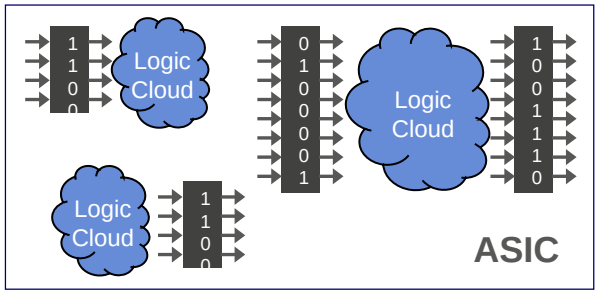
- FPGA Specifics
  - Fixed interconnect grid, LUTs, shift registers, block RAMs, configurable DSP blocks, etc.
  - Many timing, fan-out, capacity restrictions
  - Synthesis maximizes utilization by register duplication, retiming, and other sequential optimizations



FPGA synthesis tools balance logic between LUTs to improve QoR



Fixed Pre-Manufactured Structure



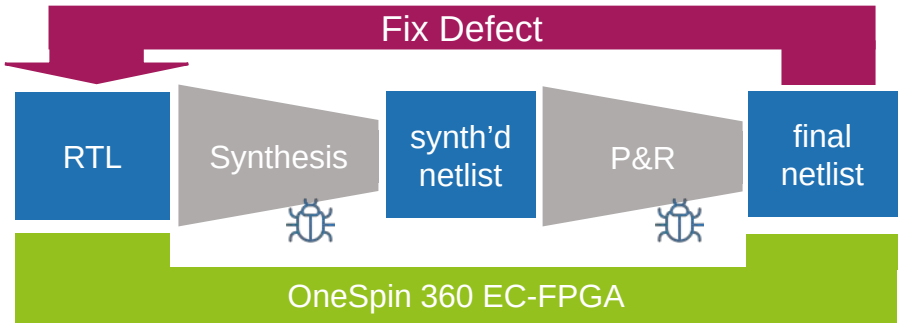
Fully Flexible Interconnect and Logic

FPGA Implementation Verification

Sequential equivalence checking: reliable and trusted FPGAs

- Accelerates design flow, reduces testing
- Enables aggressive optimization usage
- Significant post-production risk reduction
- Detects functional Trojans

FPGA Implementation Flow

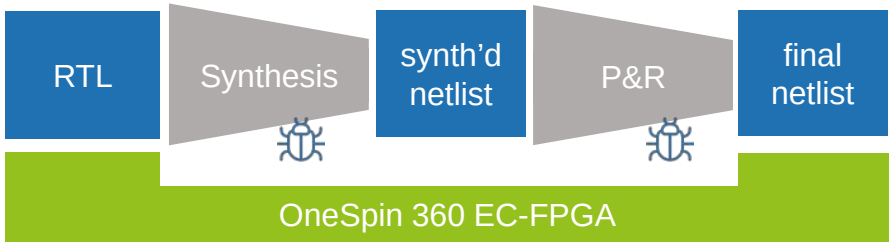


Eliminate Lengthy Test and Debug Loop

 |

FPGA Design Flow Bug Examples

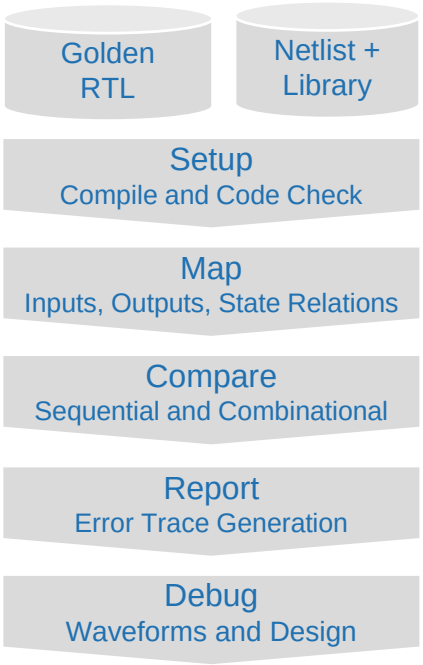
Issues Found on Real-World Designs



Examples of Encountered Defects

- Bus Connection Ordering
- Coincident Read Discrepancies
- Wrong FSM Re-Encoding
- Undriven or Unconnected Wires
- Incorrectly Coded Pipeline
- Incorrect Block RAM Parameter Settings
- Clock Gating for Low Power Issues
- P&R Connection Issues
- Unspecified Added Logic

Core Equivalence Checking Technology



Comprehensive Front End

- Supports vast range of SystemVerilog and VHDL

Easy Setup

- Spots in-depth code issues
- Handles complex blocks to minimize black-boxing, etc.

Powerful Mapping Algorithms

- Reduces the need for side files or synthesis hints
- Handles retimed registers

Advanced Proof Engines

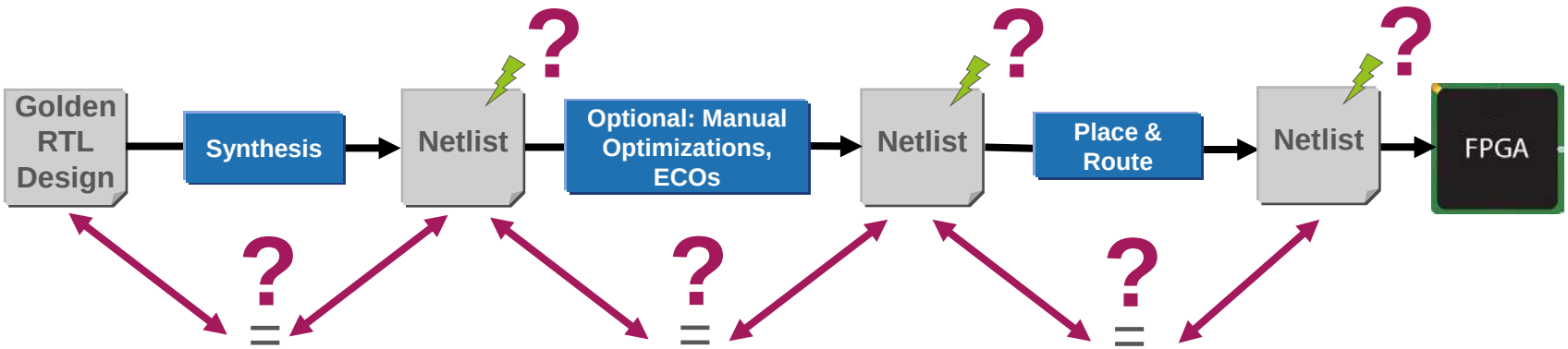
- Improves capacity, performance
- Enables sequential proofs

Intuitive Debugging

- Full inspection, driver trace, etc.
- Shows errors on diagram
- Provides wave trace to error

Synthesis and Verification Challenges

Synthesis and manual optimizations are error prone



Critical issues:

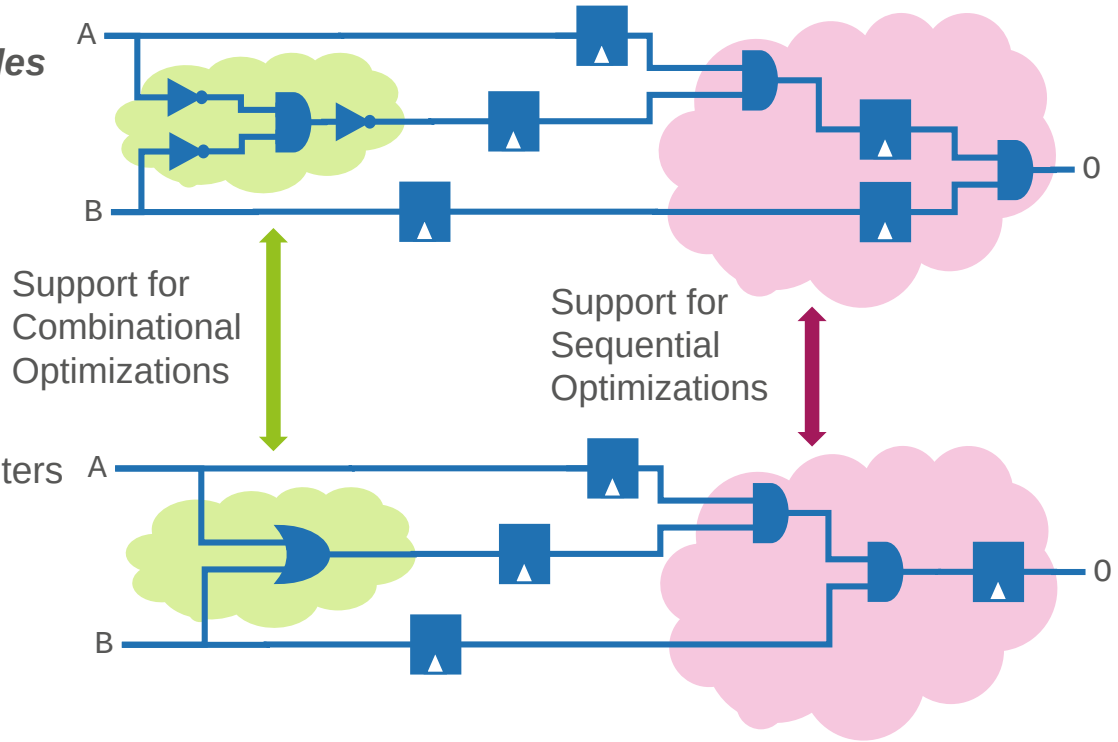
Incorrect wiring, user-directed logic optimizations (pragmas et. al.), logic retiming, pipelining, arithmetic optimizations, state initialization …

FPGA Implementation Verification

360 EC-FPGA Supports Sequential Optimizations

Specialized FPGA Optimization Examples

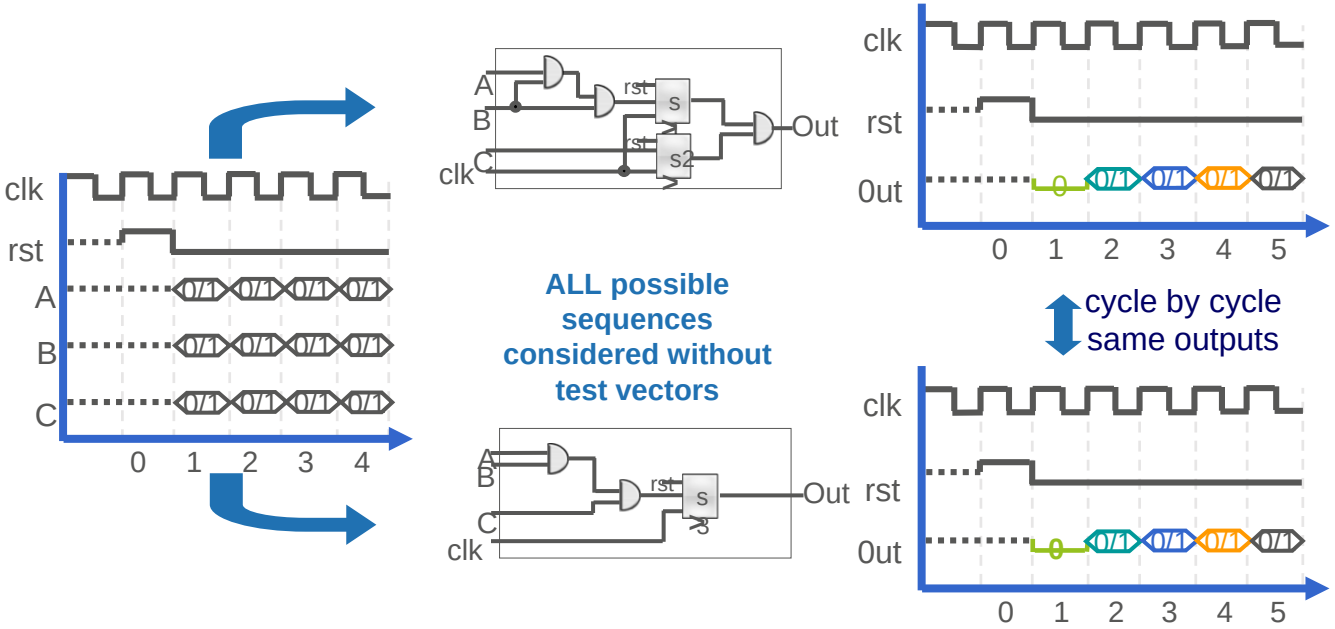
- Constants register removal
- Register duplication/merging
- TMR
- Fixed gated clocks
- Tri-state pushing
- FSM re-encoding
- FSM safe or unknown encoding
- SRL, including resettable shift registers
- Distributed block RAM/ROM
- Pipelining Retiming
- IO cell, bus resolution schemes
- Power optimization



Optimization Support Results

Designs guaranteed to be **sequentially equivalent**

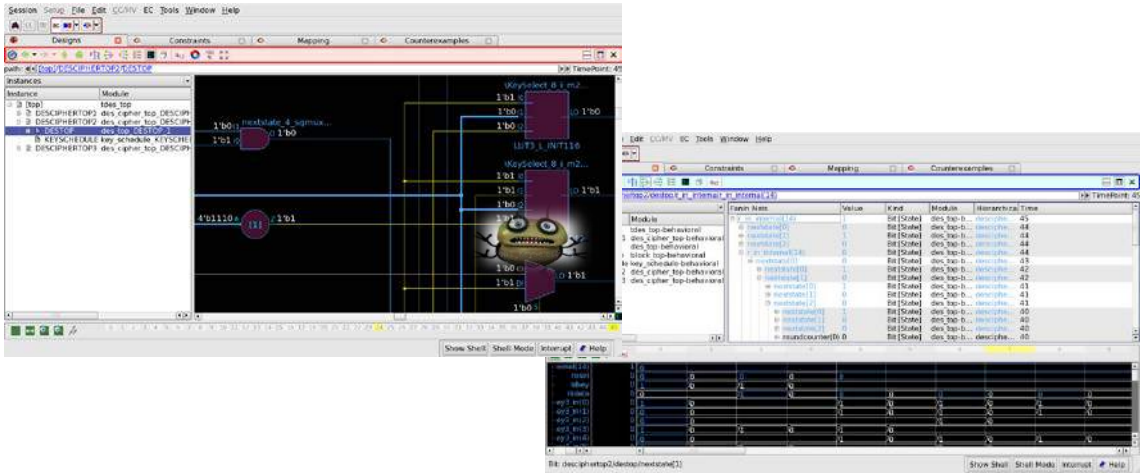
Corresponding outputs values proven to be identical for **ALL** possible input sequences



Ease of Use and Rapid Debug

Focuses on source or any miscompares

- Many ease-of-use features, auto reset and clock detection, reduced scripting, advanced GUI debug and visualization, TCL scripting
- Full debug with trace generation for rapid issue resolution
- Support for Verilog, SystemVerilog, VHDL, EDIF



Library Cell Models
Formal Models for Cyclone V

- Independent flow (not depending on the tool)
- Engineered by OneSpin development team using hardware specifications and simulation models supplied by the vendor (Intel FPGA)
- Formal library models included in library distributed with OneSpin 360 EC-FPGA
- Rigorously tested models

Xilinx® Vivado® Flow

Xilinx Device Support
Artix, Kintex, Spartan, and Virtex (up to 7 plus UltraScale/UltraScale+)

- Xilinx long-term OneSpin customer
- Verify the largest FPGA designs
- Close cooperation enabled full support of Vivado optimization and device range

"OneSpin has a powerful Sequential EC tool, **OneSpin 360 EC**, that we at **Xilinx** use extensively. It is a technology that should not be ignored!"

Xilinx Engineer, DeepChip

Synopsys® Synplify® / Microsemi® Libero® Flow

Microsemi Device Support

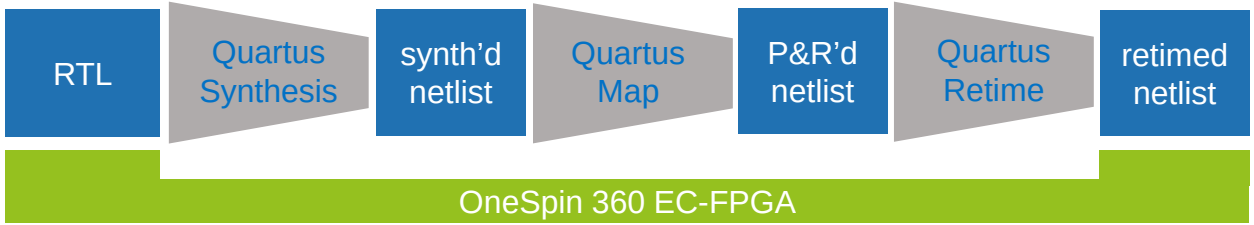
Axcelerator, Fusion/SmartFusion/SmartFusion2, IGLOO/e/2/nano/PLUS, PolarFire/PolarFire SoC, ProASIC3/3E/3L/nano, ProASICPLUS, RTG4

- Full support of Synplify/Libero FPGA implementation flow and Microsemi devices
- Microsemi is 360 EC-FPGA customer
- OneSpin/Synopsys partnership: up-to-date optimization support

"OneSpin Solutions has created innovative formal-based design verification and equivalence checking solutions that are being used to fully vet some of the most safety-critical designs in production today."

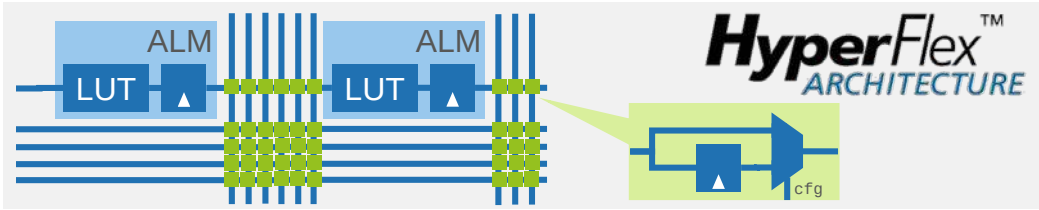
Bruce Weyer, Vice President and Business Unit Manager, Microsemi, Inc.

Intel® Quartus Prime® Flow



- Close partnership with Intel enables full support of Quartus implementation flow
- including leading edge HyperFlex™ retiming technology

Intel Device Support
Arria and Stratix (up to 10),
Cyclone and Max (up to V)



"You can optionally use the third-party OneSpin 360 EC-FPGA* sequential equivalence checking tool to verify the logic equivalence between specific netlists following compilation. The 360 EC-FPGA software can help you to confirm that aggressive Compiler optimizations do not introduce unexpected results."

Intel Third-party Logic Equivalence Checking Tools User Guide

EC-FPGA Certification

Critical for meeting demanding safety standards

- OneSpin EC-FPGA Tool Qualification Kit
  - Based on certification from TÜV SÜD
  - EC-FPGA meets ISO 26262 (TCL3/ASIL D), IEC 61508 (T2/SIL 3) and EN 50128 (T2/SIL 3)
  - Removes the burden of tool qualification from users
  - Supports using state-of-the-art verification technology
- OneSpin EC-FPGA DO-254 Tool Assessment and Qualification Kits
  - Standard compliance, including Design Assurance Level (DAL) A/B

"We achieved IEC 61508 SIL 4 for the fault avoidance measures during development of the functional safety controller vCOSS S-zero®, a challenging endeavor for this type of equipment. We used a number of technologies to meet SIL 4 requirements, but equivalence verification using OneSpin's EC-FPGA and EC-RTL was indispensable."

Masahiro Shiraishi, Chief Engineer at Hitachi

OneSpin EC-FPGA Solution

EC Critical for Modern FPGA Design

- Reduce risk, accelerate schedule, and increase quality

FPGA Sequential Synthesis Drives EC Capability

- Advanced optimizations too risky without EC support

OneSpin Technology Ideal for FPGA Verification

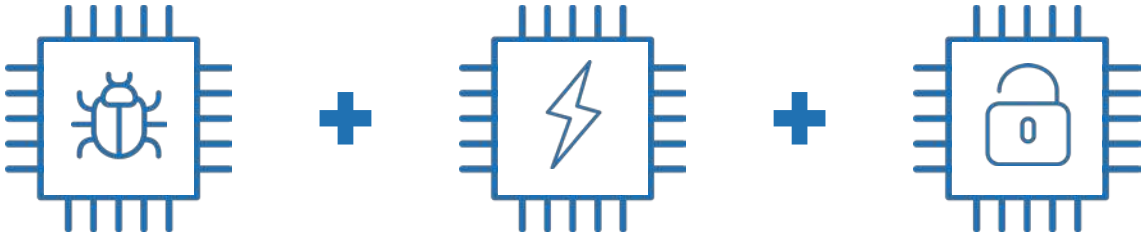
- Close partnerships with all three major vendors

OneSpin for IC Integrity
Visit **https://www.onespin.com**

Functional Correctness

Safety

Trust and Security



Thank You!

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