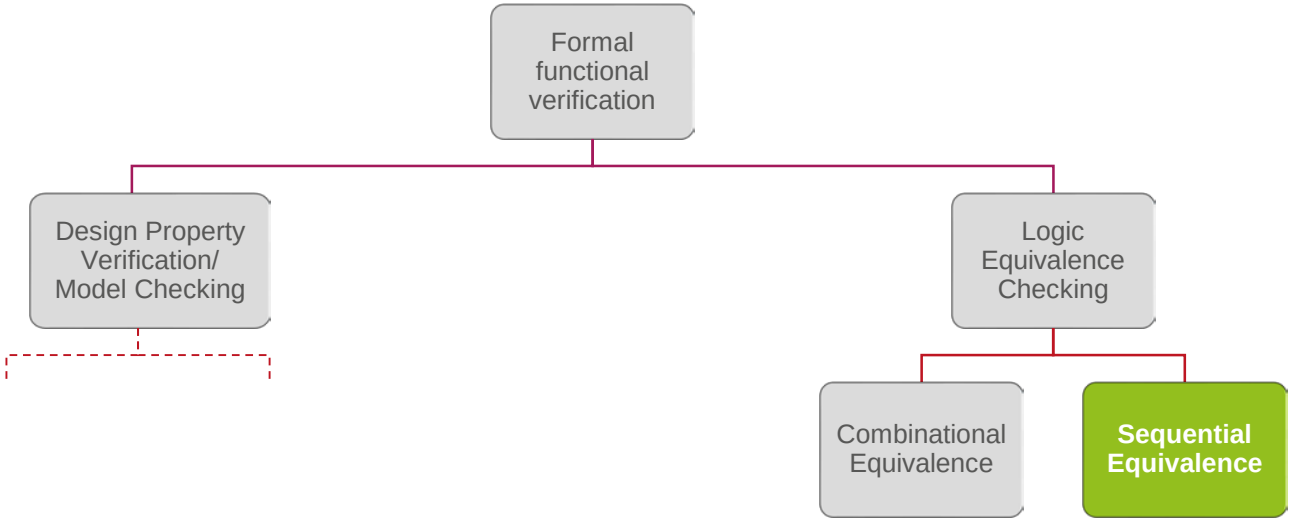
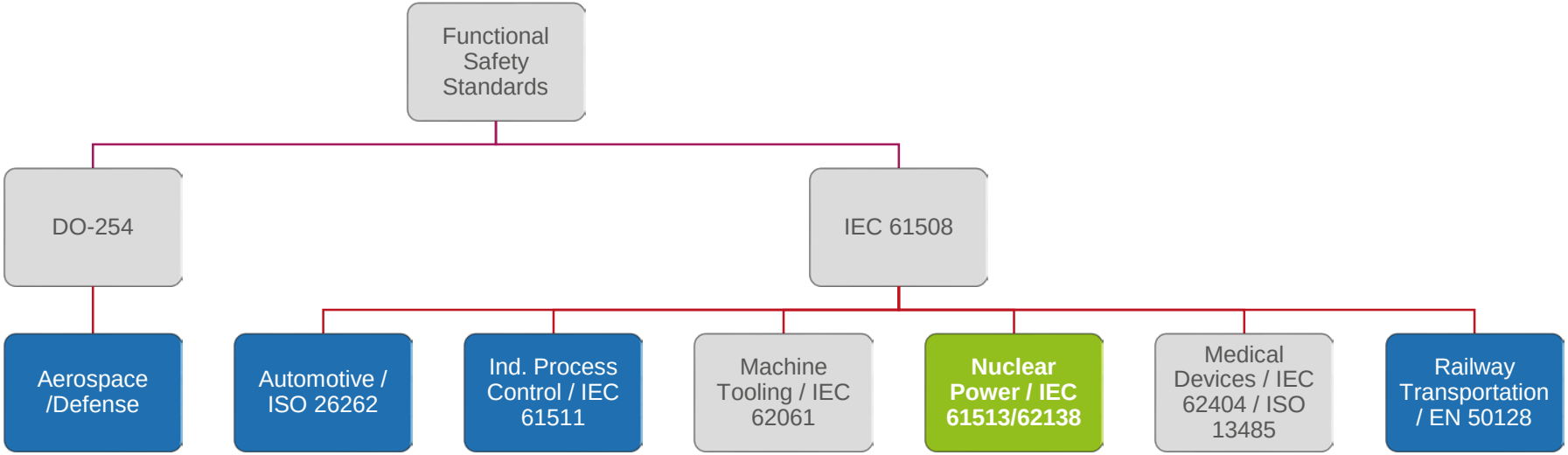
Ensuring a Rigorous Design Flow for NPP FPGA Designs

Formal verification



OneSpin develops exclusively formal tools building on advanced model checking and equivalence checking solutions

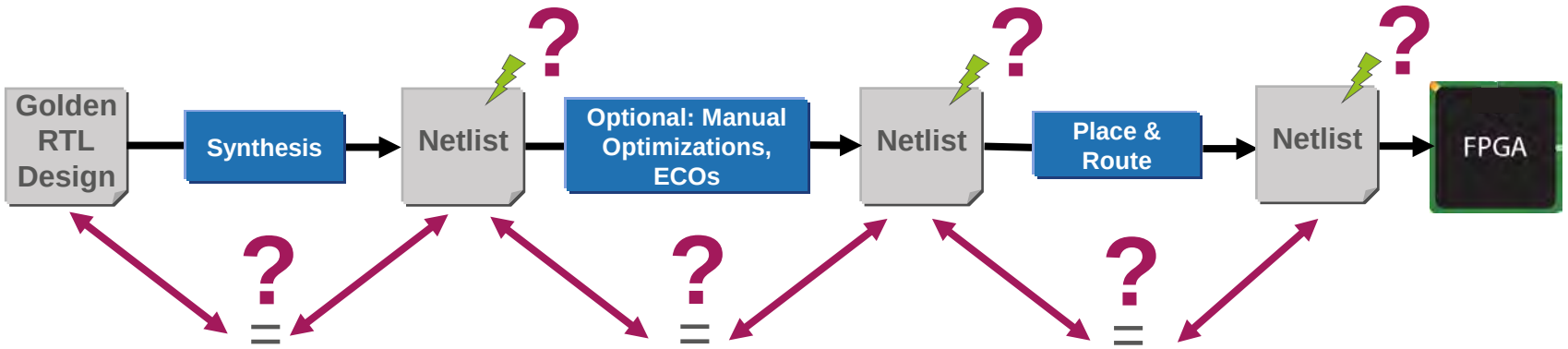
OneSpin Multiple Safety Applications



OneSpin works with multiple companies on various safety applications covering several standards
Heavily involved in the Automotive, Aeronautical, Industrial and Transportation sectors, as well as NPP

NPP Synthesis & 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, …

Modern FPGA Design Flow Issues

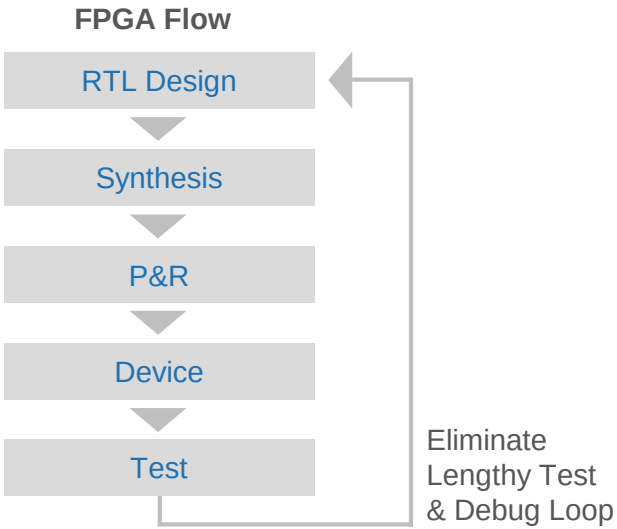
FPGA Requires Advanced Optimizations

Systematic Error Probability Increases

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

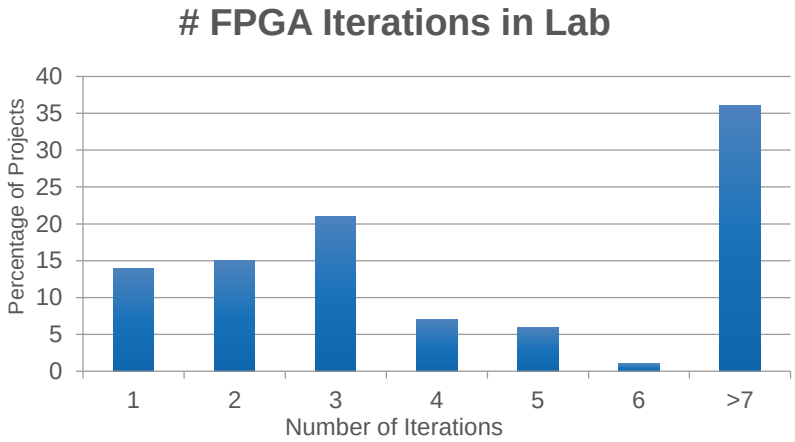
Prototype-Based Testing No longer Viable

- Excluding systematic errors require lots of additional tests
- Errors often triggered by unexpected corner cases
- Safety Critical regulations mandate formal techniques

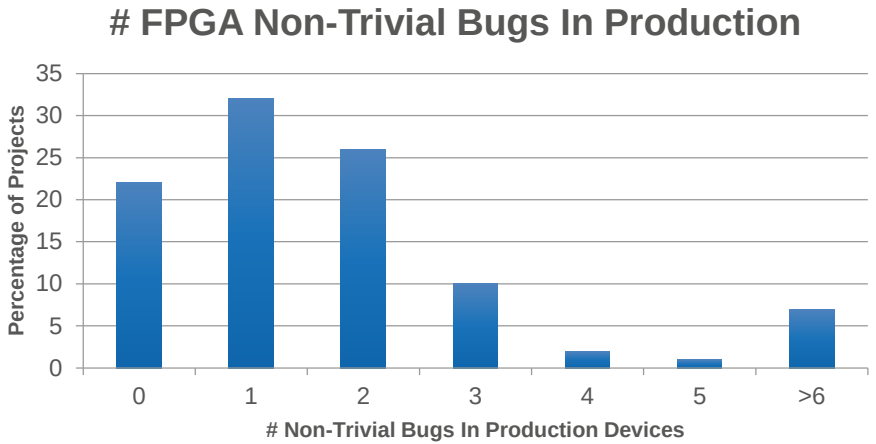


FPGA Iterations & Production Bugs

Time wasted and production higher than expected



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



Source: Wilson Research 2016

Why? FPGA Synthesis Optimization

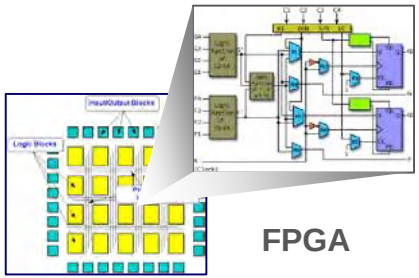
Key Factor in Design Performance

FPGA Specifics

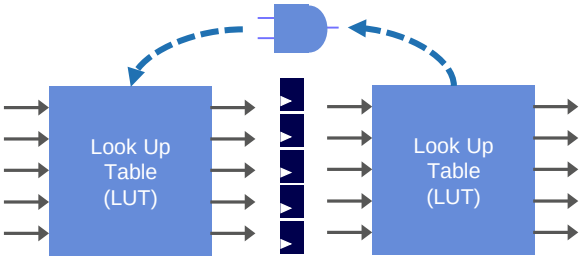
Fixed interconnect grid, LUTs, Shift-Registers, Block RAMs and configurable DSP blocks etc.

Many timing, fan-out, capacity restrictions

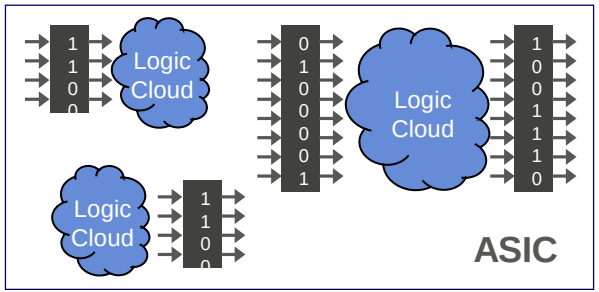
Synthesis maximizes utilization by register duplication, retiming and other sequential optimizations



Fixed Pre-Manufactured Structure



FPGA synthesis tools balance logic between LUTs to improve QoR

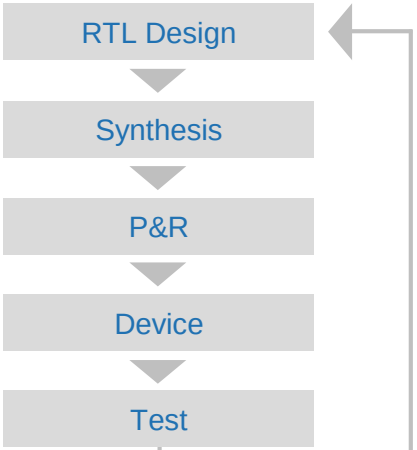


Fully Flexible Interconnect and Logic

Example Real FPGA Design Flow Bugs

Example Design Flow Issues Encountered

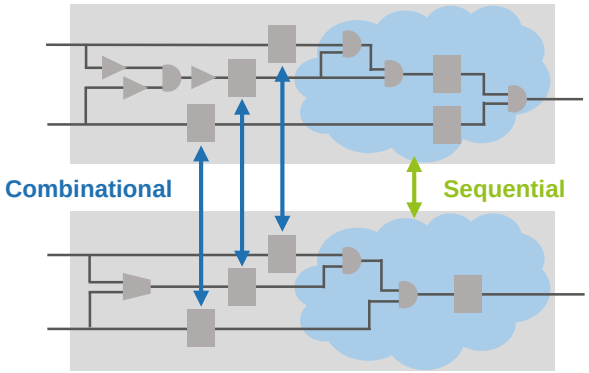
- Bus connection ordering
- Coincident read discrepancies
- Wrong FSM re-encoding
- Undriven or unconnected wires
- Incorrectly coded pipeline
- Incorrect BRAM parameter settings
- P&R connection issues
- Additional, unspecified logic added

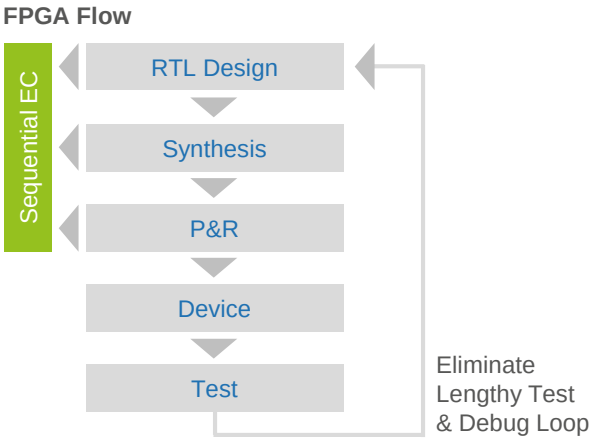


FPGA Implementation Verification

Increasing FPGA QoR with sequential equivalence checking

- Eliminate flow bugs, accelerate FPGA bring-up process
- Use aggressive optimizations with confidence
- Reduce “needle in the haystack”, post product bug risk



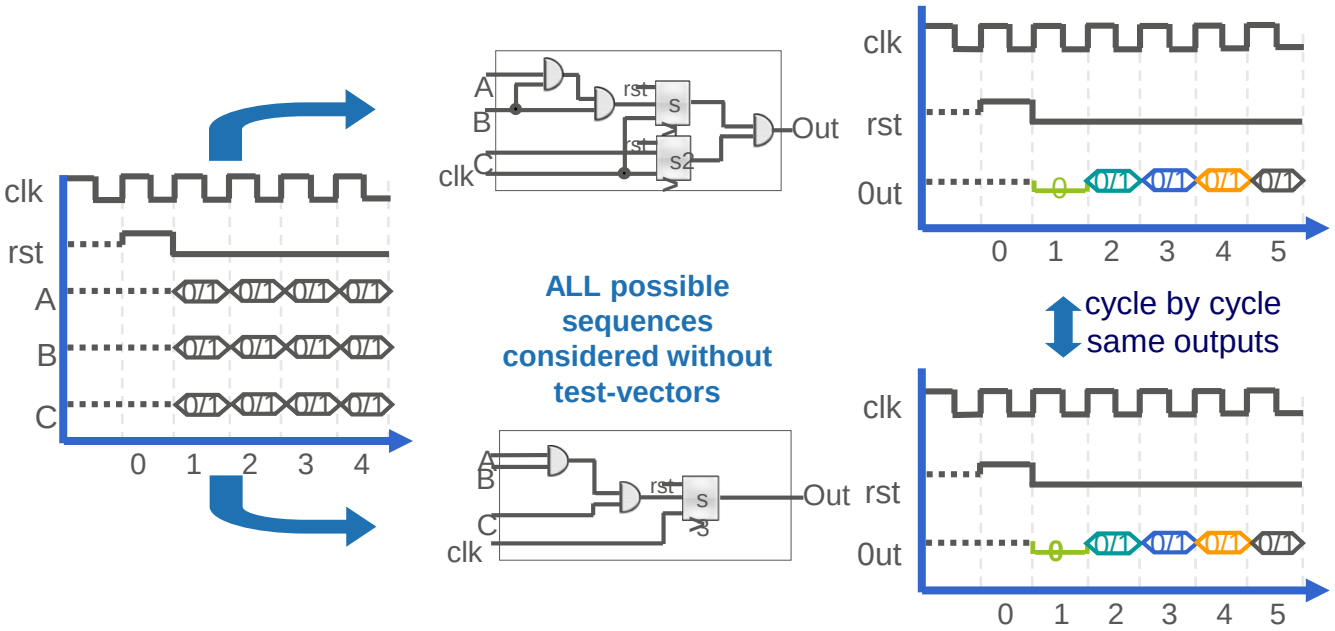


Sequential EC Critical for FPGA

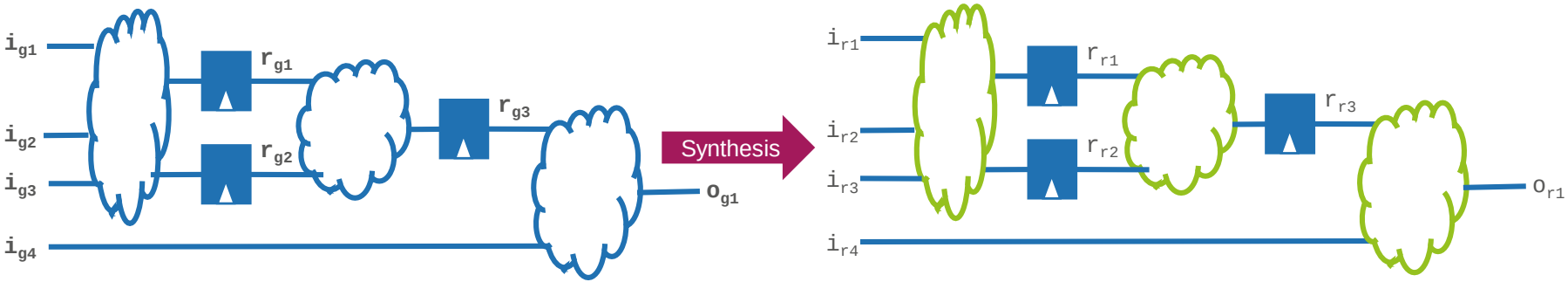
Regular Combinatorial EC Will Not Do!

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

⇨ Designs guaranteed to be **sequentially equivalent**



Equivalence Checking Paradigms



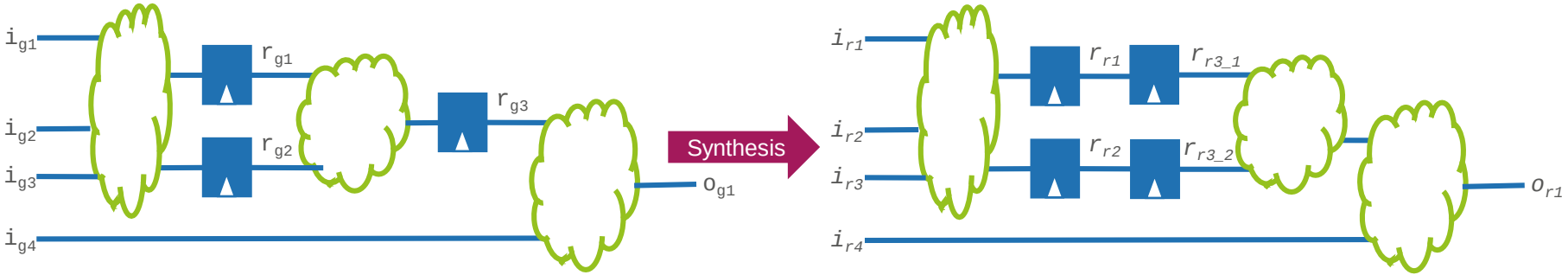
Combinational Proof Obligation:

$$i_{g1}=i_{r1} \quad i_{g2}=i_{r2} \quad i_{g3}=i_{r3} \quad i_{g4}=i_{r4} \quad r_{g1}=r_{r1} \quad r_{g2}=r_{r2} \quad r_{g3}=r_{r3} \Rightarrow r'_{g1}=r'_{r1} \quad r'_{g2}=r'_{r2} \quad r'_{g3}=r'_{r3} \quad o_{g1}=o_{r1}$$

where r_g', r_r' are the next state

Combinational proof techniques can resolve this proof obligation efficiently.

Equivalence Checking Paradigms



Sequential Proof Obligation:

$i_{g1}=i_{r1}$ $i_{g2}=i_{r2}$ $i_{g3}=i_{r3}$ $i_{g4}=i_{r4}$ $r_{g1}=r_{r1}$ $r_{g2}=r_{r2}$ ⇒ $r'_{g1}=r'_{r1}$ $r'_{g2}=r'_{r2}$ $o_1=o_{r1}$

Sequential proof techniques can resolve this sequential proof obligation.

360 EC-FPGA Optimization Support

Combinational, multi-cycle sequential, arithmetic transforms and specialized FPGA optimizations all necessary

Specialized FPGA Optimization Examples

Constants register removal

Register duplication/merging

TMR

Fixed gated clocks

Tri-state pushing

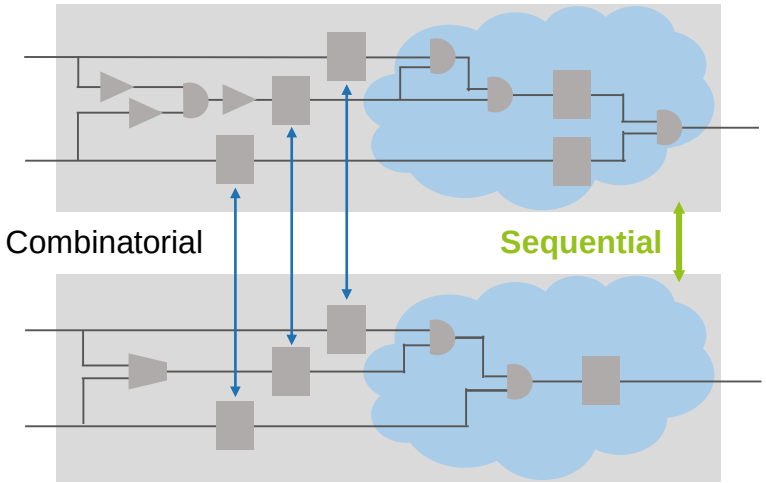
FSM re-encoding

FSM safe or unknown encoding

SRL incl. resettable shift registers

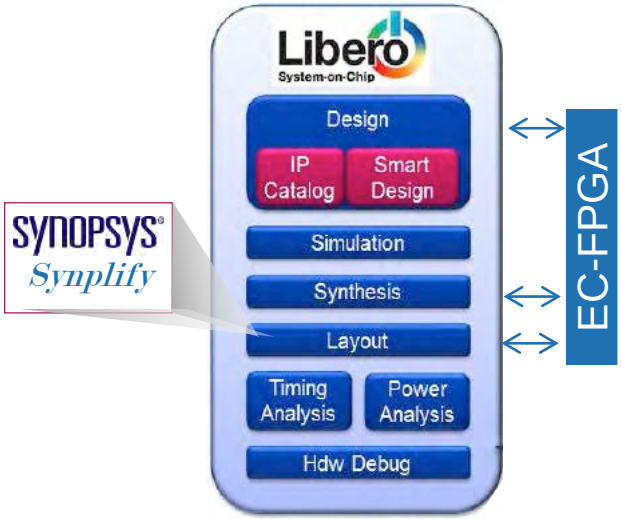
Distributed block RAM/ROM

Pipelining/Retiming



MicroSemi® Libero® (with Synplify®) Flow

Safety Critical FPGA Assurance



Microsemi

Full support of Libero flow and Microsemi devices

Microsemi is EC-FPGA customer

OneSpin Synplify partnership:
up-to-date optimization support

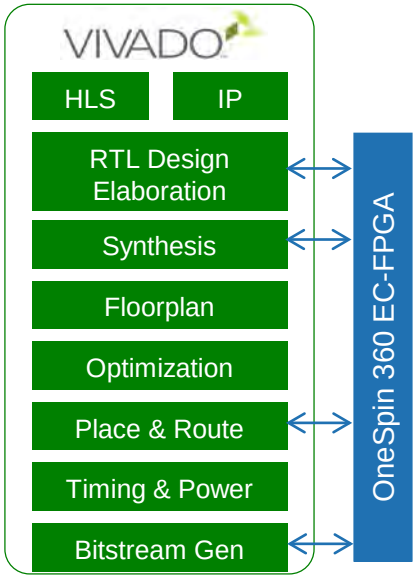
Multiple Safety Critical customers

Microsemi Device Support
Upto and including latest-generation PolarFire FPGA devices

"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. We believe that by including equivalence checking as part of the design flow, we will better meet our customers' stringent requirements for high-reliability designs." ***Bruce Weyer, Vice President and Business Unit Manager, Microsemi, Inc.***

Xilinx® Vivado® Flow

Large Design QoR



XILINX®

Xilinx significant OneSpin customer

Validate the largest FPGA designs

Close cooperation allows full optimization support

Full support of Vivado flow and device range

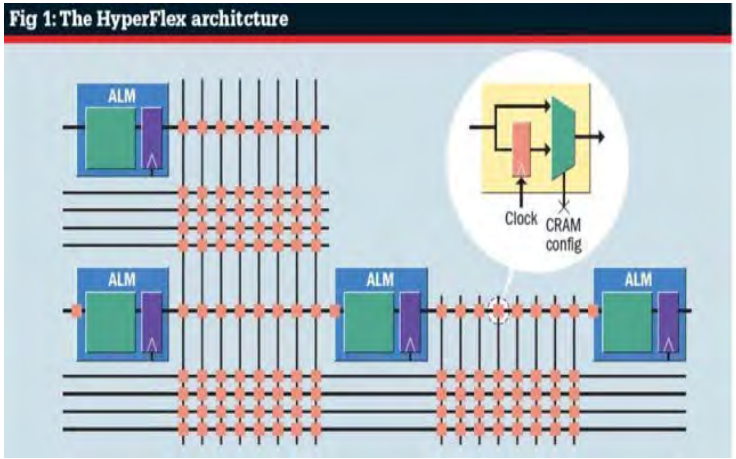
Xilinx Device Support

From Artix7, upto latest generation UltraScale+ device family

"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, Oct 2015

Altera® Quartus® Flow

Latest retimed HyperFlex™ architecture



HyperFlex: registers + retiming everywhere

HyperFlex™ ARCHITECTURE

ALTERA® now part of Intel

Close partnership with Altera

- OneSpin customer

Currently revamping Altera device support with next-generation Quartus®

- Delivery: late 2017

Focus on Stratix10 and Arria10 families

"It proves that the post Intel HyperFlex FPGA Architecture-optimized netlist is equivalent to the post fitter netlist. A third-party tool that you can refer to is the 360-EC FPGA solution by OneSpin."
What's New in Intel® Quartus® Prime Design Software

360 EC-FPGA NPP Case Study

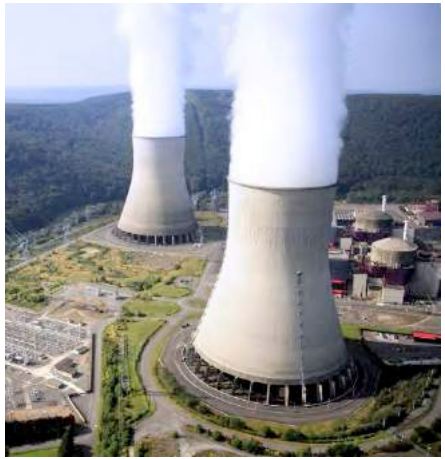
Verification for Safety Critical Design

Westinghouse using OneSpin 360 EC-FPGA on instrumentation for nuclear power stations

Exacting verification requirements to meet SIL safety standards

Close cooperation between OneSpin, Microsemi and Synopsys Synplify teams

360 EC-FPGA also used in automotive, aeronautical, defense & medical applications



"The Microsemi ProASIC3 FPGA is a core component of the Advanced Logic System (ALS), and use of the OneSpin 360 Equivalence Checker is an integral part of our FPGA development process for nuclear safety systems."
Erik Matusek, Safety System Platform Manager, Westinghouse Electric Company, LLC

OneSpin 360 EC-FPGA used on the most safety critical verification projects in the world

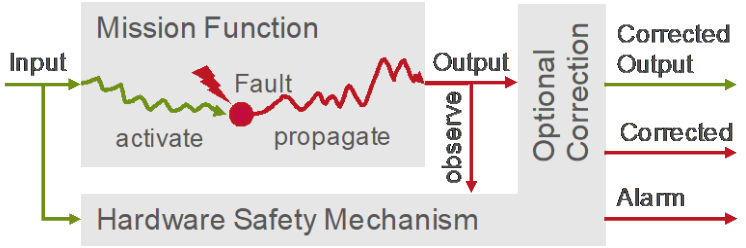
TÜV-Süd Certification Roadmap and Status

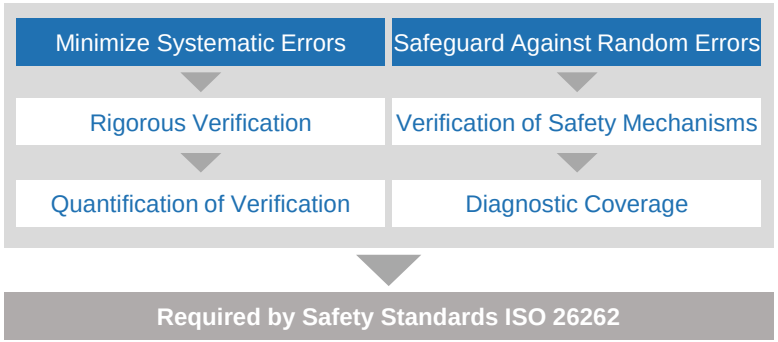
- November 2017
  - Concept phase assessment process completed by TÜV-Süd
- January 2018
  - Certification for EC-FPGA
  - Evaluation of tool development process for all OneSpin tools completed

Automotive Safety Critical Verification

Meeting tough functional safety standards, e.g. ISO 26262

- Efficient verification of functional safety mechanism leveraging fault injection
- Precise diagnostic coverage with formal fault analysis accelerating existing methodologies
- Rigorous systematic verification flow





Powerful Solutions Require Strong Technology and Apps

Unique, Powerful Verification Solutions

Advanced Design Verification

Agile Design Evaluation

Metric-Driven Verification

Block Integ. Validation

Innovative Specialized Solutions

FPGA Impl. Verification

Safety Critical Verification

C++/SysC Des. Verification

Automated Inspection
Design Exploration
Sequential EC RTL-RTL
Assertion Verification
Operational Assertions
Observation Coverage
DV Apps
X-Prop
Connect
Register
Scoreboard
Protocol Comp.
Activation
SystemC/C++ Arithmetic
Sequential EC FPGA
Fault Propagation
Fault Injection
Security Verification
Specification Verification

Proof Engines
Formal Model
Adv. Debug
LaunchPad

SystemVerilog . VHDL . SystemC . SVA . PSL

High Performance, Comprehensive Technology Platform

OneSpin FPGA EC Solutions

EC Critical for Modern FPGA Design

- Reduce risk, accelerate schedule increase quality

FPGA Sequential Synth Drives EC Capability

OneSpin Technology Ideal for FPGA Verification

For more information please visit

www.onespin.com