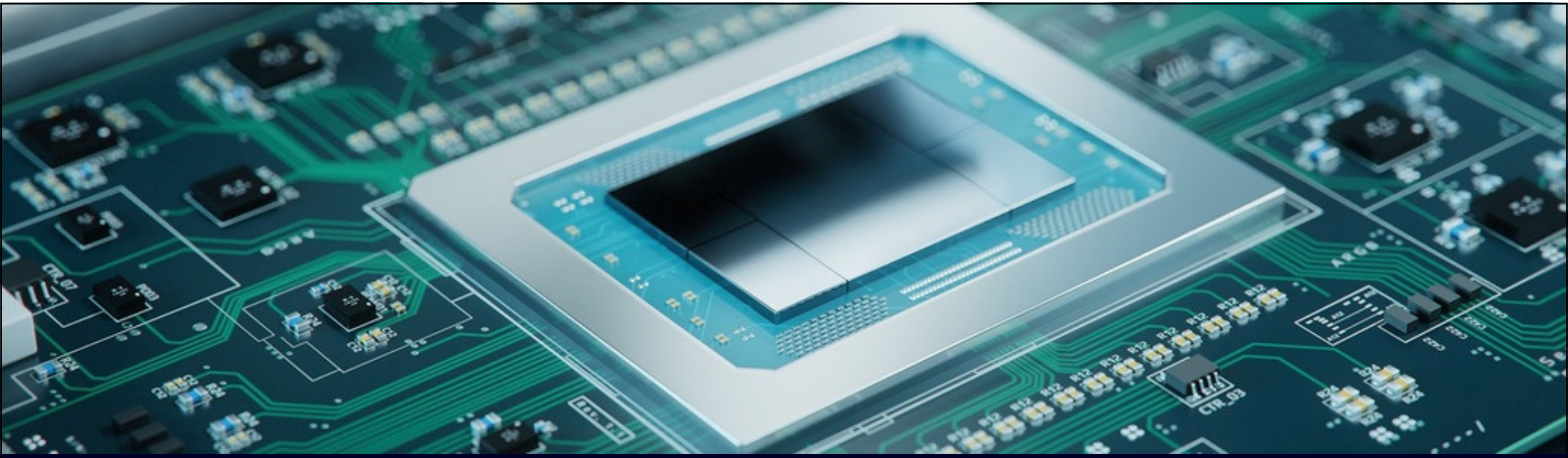


Leveraging FPGA Optimized EC
Security, Safety and Assurance

IC Verification Solutions / DVT

SIEMENS

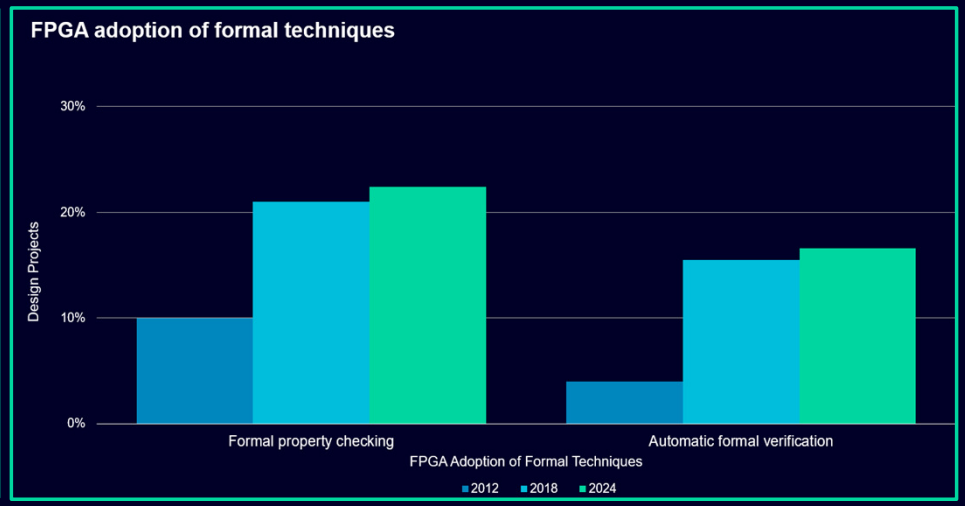
FPGA Equivalence Checking
Verifying Implementation

The need for absolute assurance

- Safety critical designs (mil/aero, automotive, medical, etc.) are severely impacted by functional escapes

87%

FPGA design projects having non-trivial escapes into production



Absolute Assurance

Source: Wilson Research Group and Siemens EDA, 2022 Functional Verification Study

SIEMENS

Security and Safety Implementation Issue Detection
Unique solutions needed for compliance

Security Compliance
- Functional trojans change functionality
  - Intentionally hard to trigger
- EC addresses multiple Threat Descriptions for DoD Microelectronics: FPGA Level of Assurance Best Practices
  - Supports Level of Assurance (LOA) 1, 2, and 3

Safety Compliance
- Independent verification of the build tool chain
- Improves Tool Detection levels
- Reduces risk
- Successful adoption in:
  - Aerospace
  - Automotive
  - Nuclear

A&D
DoD FPGA LoAs - AFMAN 91-119 - DO-254

Automotive
ISO 26262

Industrial
IEC 61508

Nuclear
IEC 61513, IEC 62566

SIEMENS

Security, Safety, and Assurance Focused Implementation Verification

Extending equivalence from RTL through the bitstream

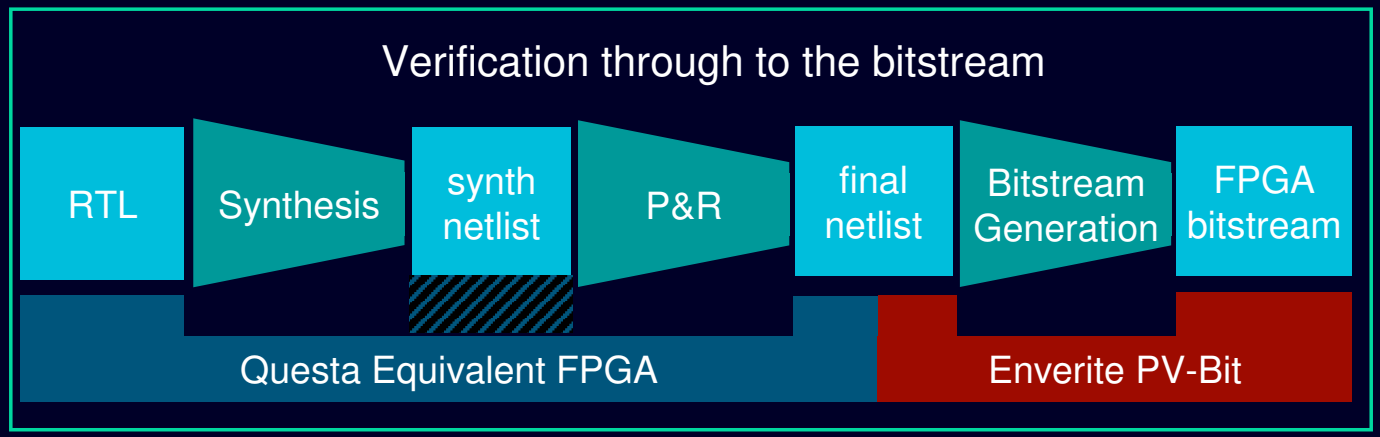
Industry-first solution:

- Absolute Assurance for security and safety critical FPGAs
- Combines Siemens Questa Equivalent FPGA and Graf Research Enverite PV-Bit in a unified flow

Absolute Assurance

Provides Evidence Based Assurance (EBA) for:

- DoD FPGA LoAs and AFMAN 91-119 guidance
- Aerospace, automotive, industrial, and nuclear safety certifications



SIEMENS

Example Security and Safety Concerns

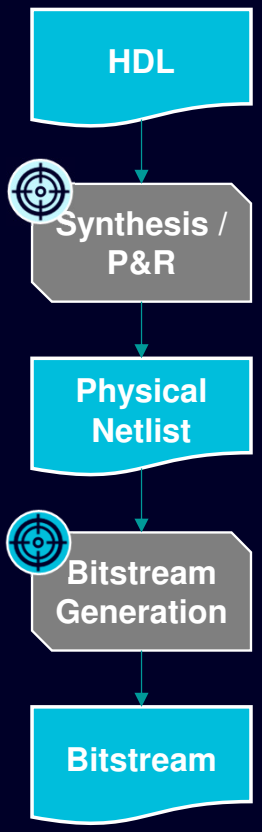
Security Concern Example
Hardware Trojan Horse

Hardware Trojan Horse A (HTH-A)[1,2]

- Leaks encryption key using clever encoding scheme via power side channel (AES-T1100)
- Inserted into physical netlist
- ***Questa Equivalent FPGA detects HTH-A in the netlist***

Hardware Trojan Horse B (HTH-B)[3]

- Weakens the crypto engines, enabling man-in-the-middle attacks on comm systems
- Inserted into bitstream via tool for auto-detecting cryptographic primitives in FPGA bitstreams
- ***Enverite PV-Bit detects HTH-B in the bitstream***



Safety Concern
Errors in Build Flow

HDL Synthesis Errors

- Example: HDL synthesis error produces an improper finite state machine encoding
- ***Questa Equivalent FPGA detects in the netlist***

Bitstream Generation Errors

- Example: Routing fragments are activated that should be off
- ***Enverite PV-Bit detects in the bitstream***

Graf Research
UNLEASHING INNOVATION

1. L. Lin, M. Kasper, T. Güneysu, C. Paar and W. Burleson, "Trojan Side-Channels: Lightweight Hardware Trojans through Side-Channel Engineering," 11th International Workshop Cryptographic Hardware and Embedded Systems (CHES), 2009.
2. H. Salmani, M. Tehranipoor, and R. Karri, "On Design vulnerability analysis and trust benchmark development", IEEE Int. Conference on Computer Design (ICCD), 2013.
3. P. Swierczynski, M. Fyrbiak, P. Koppe and C. Paar, "FPGA Trojans Through Detecting and Weakening of Cryptographic Primitives," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Aug. 2015

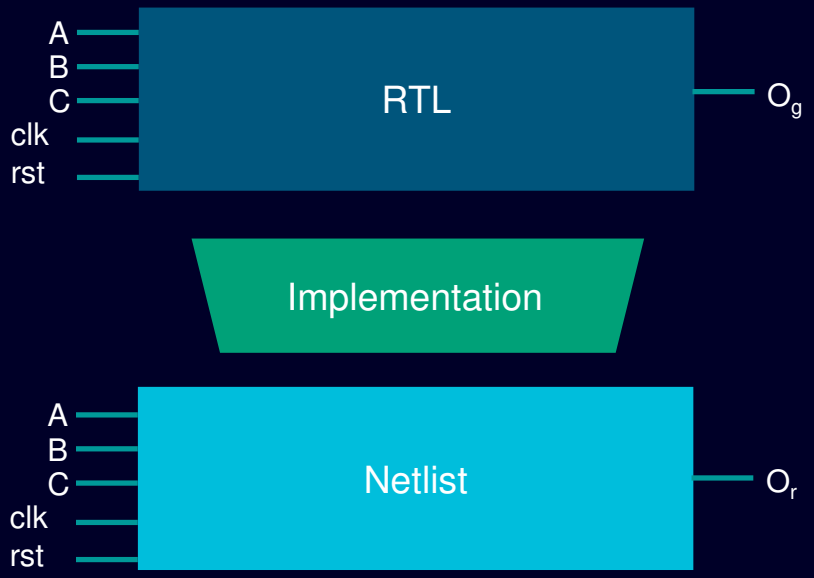
Questa Equivalent FPGA

Providing absolute assurance for FPGAs from RTL through P&R

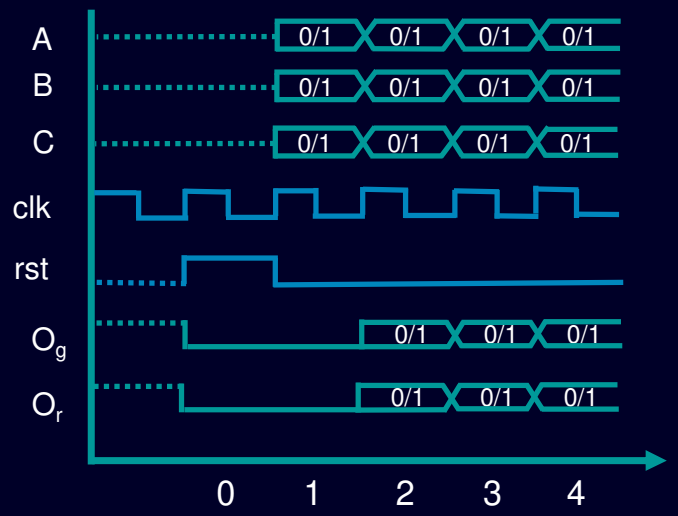
SIEMENS

Simulation vs. Logical Equivalence Check

There are $(2^{\#inputs})^{depth}$ input sequences for simulation



Equivalent FPGA formally proves identical function for **all** possible inputs



SIEMENS

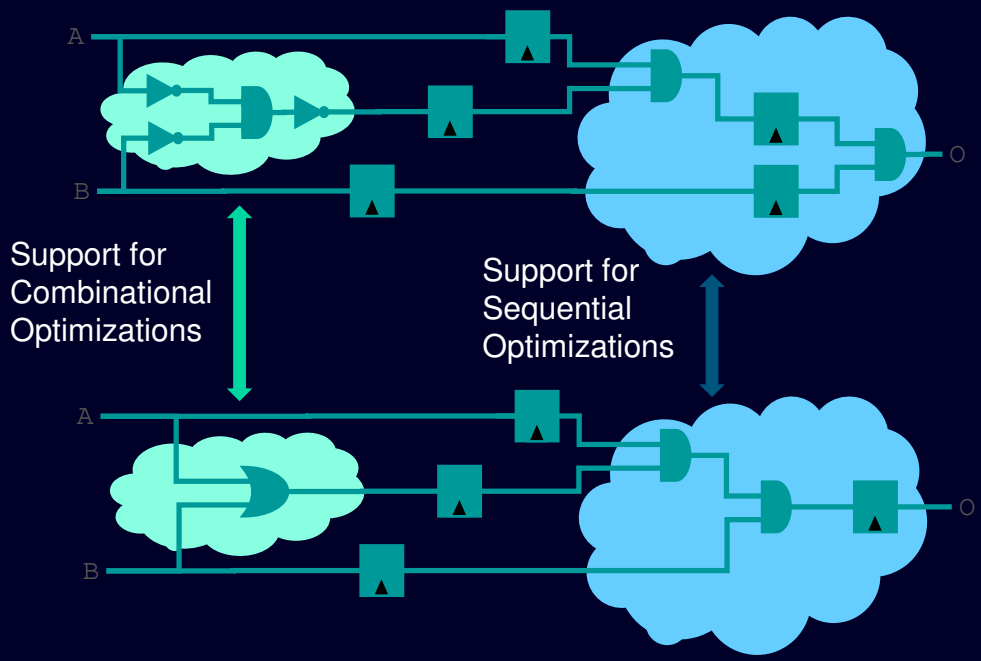
FPGA Implementation Verification

Sequential optimization support

- Modern FPGAs utilize increasingly complex design optimizations
- Critical capability for FPGA success
- Unique to Equivalent FPGA

FPGA optimization examples

- FSM re-encoding
- RAM/ROM inferencing (macro and distributed)
- DSP inferencing
- Pipelining and retiming
- Register duplication/merging
- SRL inference and SRL to RAM conversion

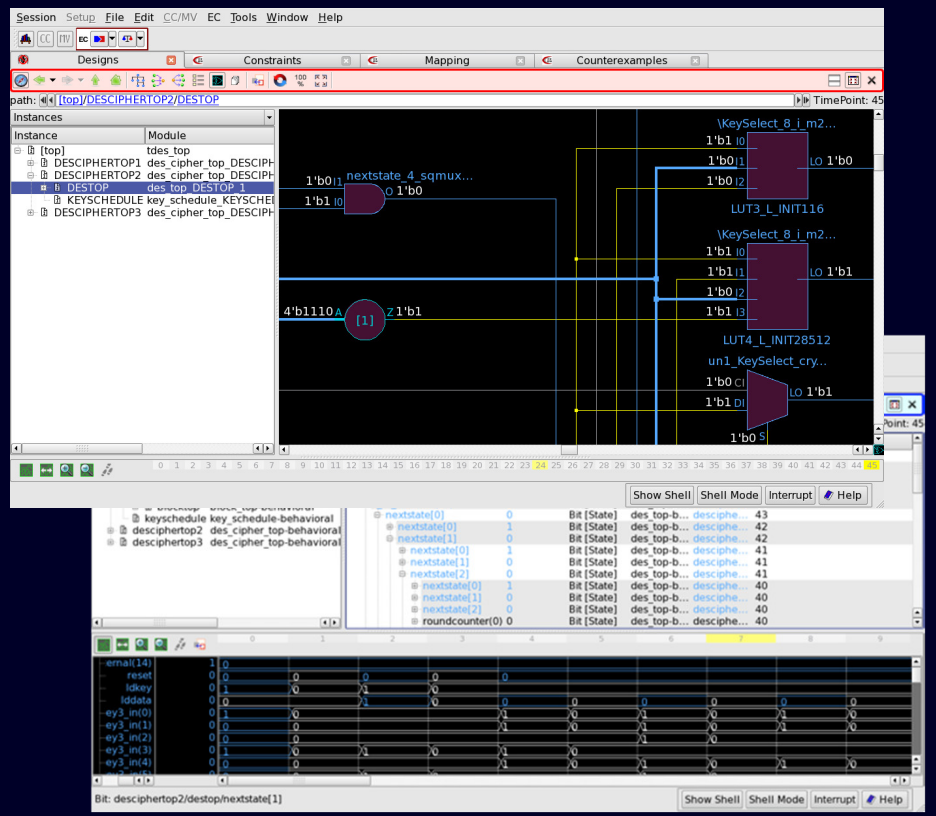


SIEMENS

Counter-example Resolution
Focuses on source of any miscompares

- Quickly identify and resolve issues faster than simulation

- Ease-of-use features include:
  - GUI visualization
  - Auto reset and clock detection
  - TCL scripting
  - Counter-example trace generation



SIEMENS

Questa Equivalent FPGA ISO-26262 Safety Certification

FPGA Tool Qualification

- ISO-26262 certification from SGS TÜV SAAR
- Download directly from Siemens Support Center

"*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

SIEMENS

Unique FPGA Vendor Collaboration and Support

We are **the vendor recommended FPGA EC solution**.

Altera, AMD-Xilinx, and Microchip are long-term partners using Equivalent FPGA for:

- QA
- FPGA product introductions
- Implementation tool and flow development

Only solution with direct integration for Vivado, Quartus, and Libero including benefits such as:

- automated script generation
- mapping/implementation guidance

SIEMENS

Enverite PV-Bit: Verify the Bits that Fly

SIEMENS

Enverite PV-Bit Verification Overview

Graf Research
UNLEASHING INNOVATION

Enables an end user to independently verify their FPGA bitstream without reverse engineering

Automated Evaluation of Bitstream and Netlist Equivalency

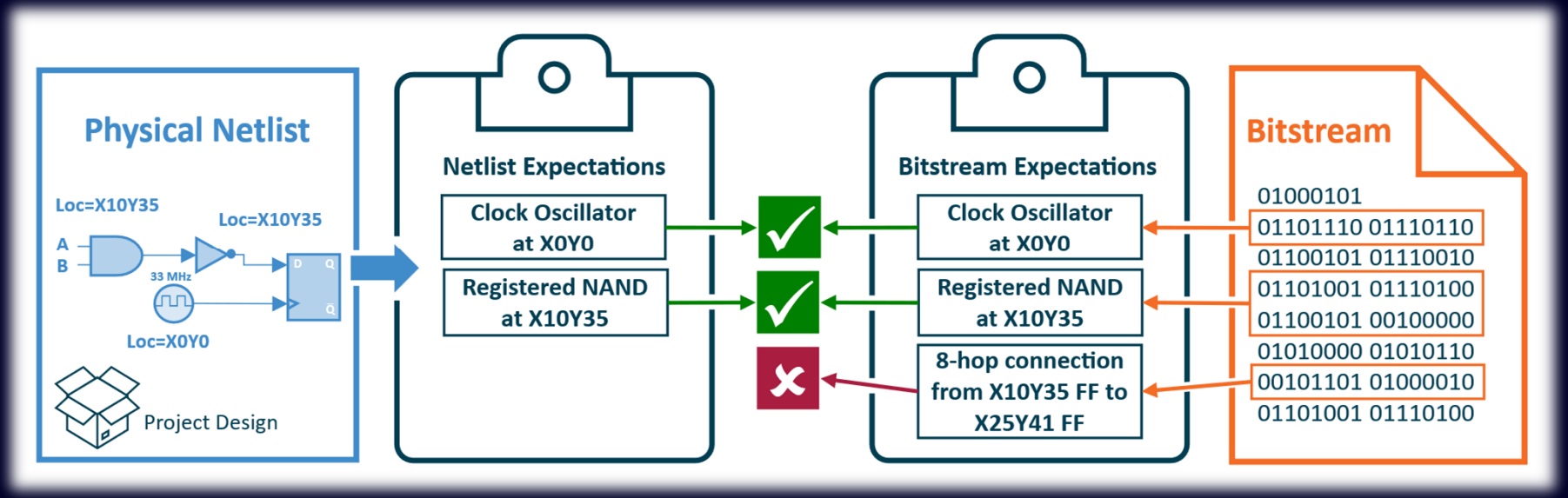
Designed for the Typical End-User

Respects FPGA Vendor Bitstream

Respects Third Party Vendor IP

Enverite PV-Bit Verification Process

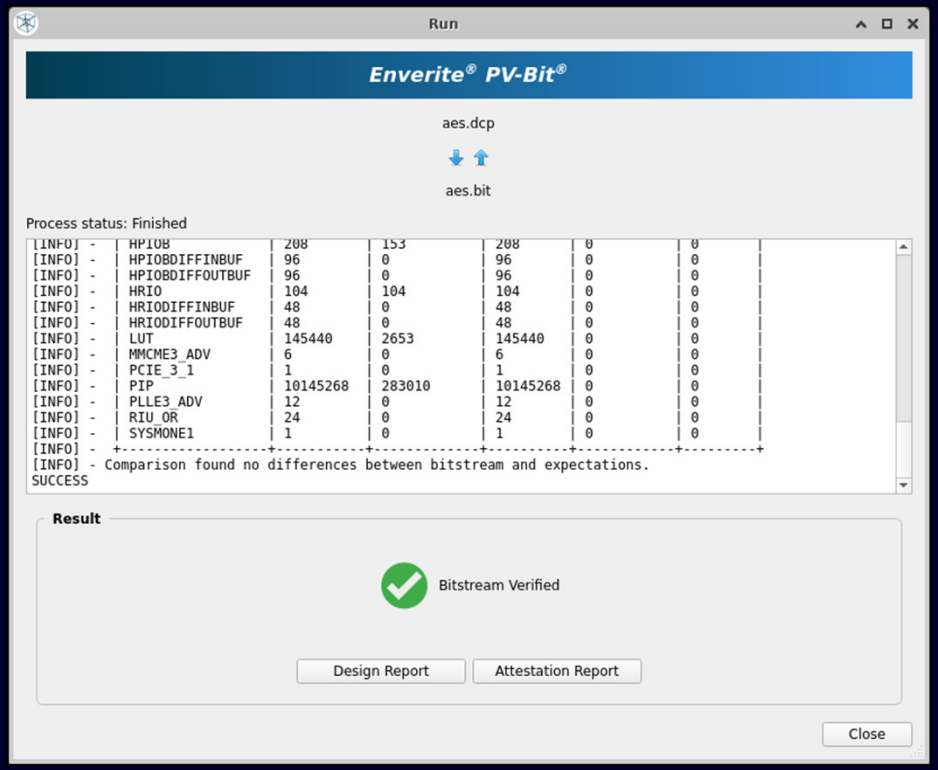
A Physical Equivalency Check in a Properties Domain



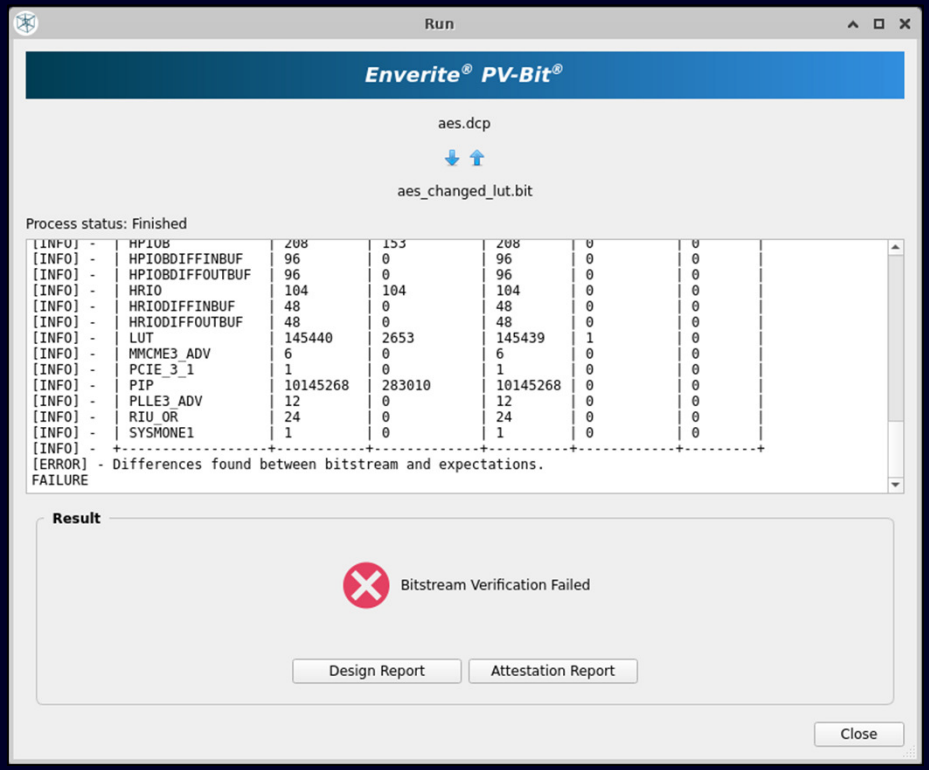
Graf Research
UNLEASHING INNOVATION

SIEMENS

Enverite PV-Bit Design Report



Equivalent



Mismatch

Graf Research UNLEASHING INNOVATION | SIEMENS

Summary

SIEMENS

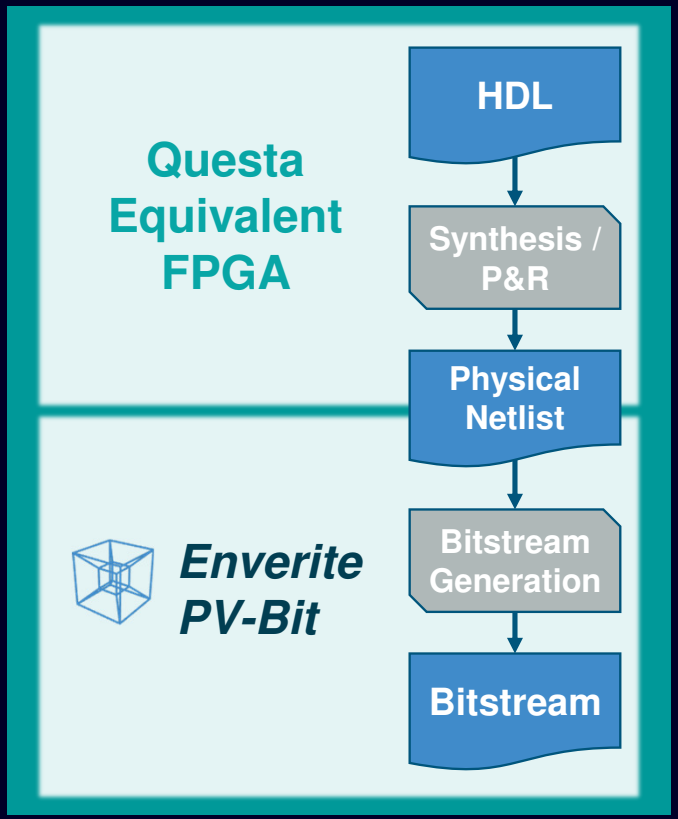
EC from RTL to Bitstream Conclusions
Industry-first solution for verifiable safety and security compliance

Cohesive FPGA assurance flow

- **Establish a strong foundation through verified RTL**

- **Maintain Absolute Assurance throughout implementation**
  - **Questa Equivalent FPGA**
    - Incremental flow to pinpoint functional issues: RTL to synth and synth to P&R
    - Stimulus-free verification through formal proofs

  - **Enverite PV-Bit**
    - Translate assurance claims for FPGAs from the netlist to the bitstream
    - Ensure the P&R netlist is physically and logically equivalent to the bitstream



SIEMENS

Disclaimer

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

Contact

Published by Siemens 2025

Yassine Eben Aimine
Product Architect, Formal Tools

E-mail yassine.eben_aimine@siemens.com

For information regarding Enverite PV-Bit, contact: marketing@grafresearch.com

SIEMENS