# Securing Custom Computing Devices: Observations from the Lab and the Market

**Prepared for SCCM 2025**

September 2, 2025

**Jonathan Graf, PhD; CEO**

jon@grafresearch.com

Enverité®
By Graf Research

# Securing Custom Computing Devices: Observations from the Lab and the Market

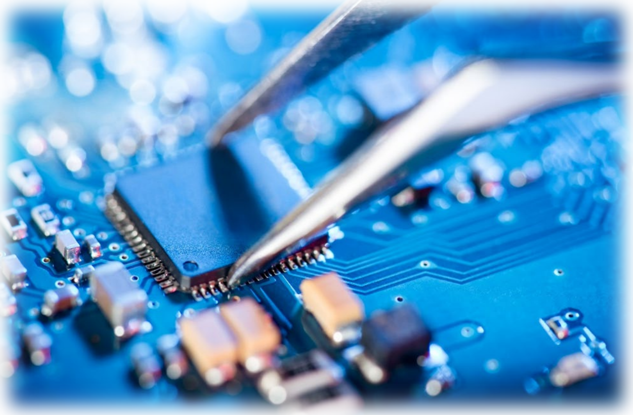
Dr. Jonathan Graf, CEO of Graf Research, will share how Graf Research is ***developing a new generation of configurable computing tools*** for electronic design automation and verification—tools that create independent, trustworthy views of FPGA configuration and silicon correctness.

Among these innovations is a method for bitstream equivalence checking, Enverité PV-Bit, which confirms whether an FPGA bitstream truly matches the intended gate-level netlist. Another is Ensofic, a silicon attestation platform that combines soft sensors with machine learning to evaluate both the reliability and authenticity of an FPGA, including the ability to spot counterfeit devices.

The talk will also cover what it takes to turn ***research prototypes into practical, commercial-grade solutions*** ready for deployment in high-stakes industries like aerospace, automotive, defense, and energy. Drawing on hands-on experience with deployed commercial solutions, Dr. Graf will outline key lessons learned and show how these projects have inspired unexpected new applications. The result is a clear picture of challenges and how the security of custom computing machines can advance rapidly in the years ahead.

# Graf Research R&D Areas

- Microelectronics Trust & Assurance
- Machine Learning
- Digital Signal Processing
- Software Defined Radio
- FPGA Design & Verification
- Circuit Analysis
- Anti-Tamper Technologies
- Laboratory Automation



# Enverité by Graf Research

EDA for FPGA Design Assurance

**PV-Bit®**

Evaluates the equivalence of an FPGA bitstream and its physical netlist

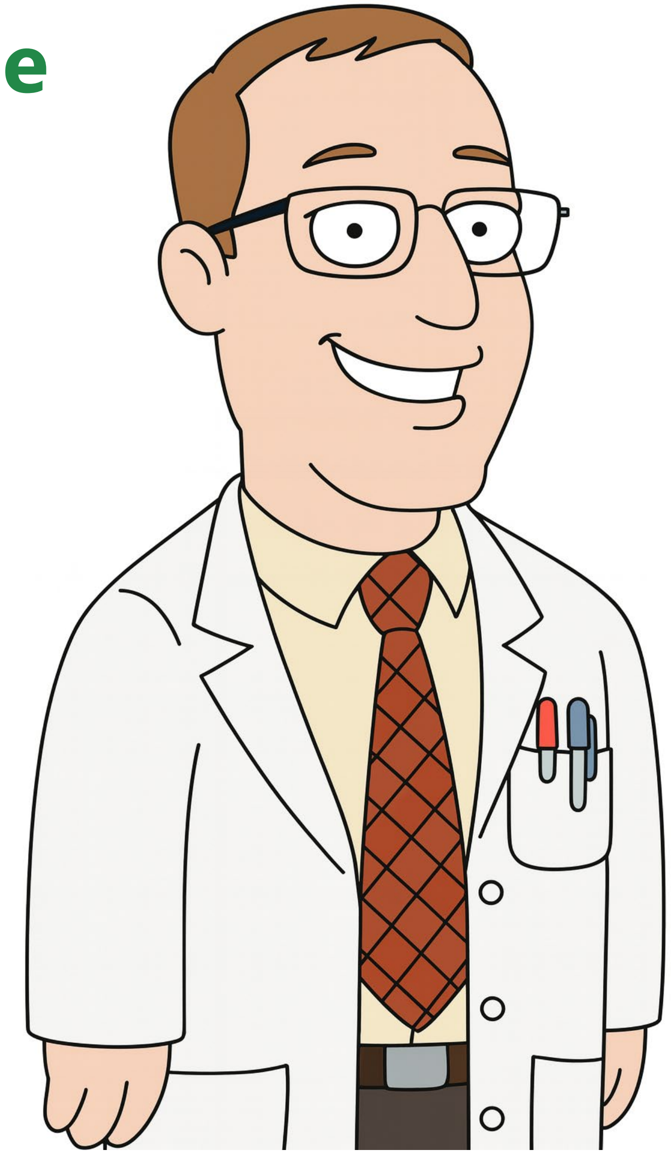
**Trace®**

Creates and verifies a tamper-evident auditable digital thread as a design traverses the build flow

**Not-Yet-Announced In-Development Tool**

Come to the AMD Security Working Group in Colorado, D.C., or ***Munich*** this Fall to see this tool demonstrated!

## PhD Side



## CEO Side

#1
NEW YORK TIMES
AND
WALL STREET
JOURNAL
BESTSELLER
WITH A SPECIAL NEW AFTERWORD BY THE AUTHOR
jack
STRAIGHT FROM THE GUT
JACK WELCH
WITH JOHN A. BYRNE
"Jack is the Tiger Woods of management."
—WARREN BUFFETT, CHAIRMAN, BERKSHIRE HATHAWAY

# Agenda

Two SCCM Challenges and Two Graf Research technologies from the PhD and CEO perspective

### Challenge 1 : Verify Bitstream Contents

- FPGA Bitstream Equivalence Checking Software

Enverité® PV-Bit®

### Challenge 2 : Find Counterfeit FPGAs

- Counterfeit FPGA detection through soft sensors and machine learning

Ensof(IC)™

CHALLENGE 1

# Verify Bitstream Contents

Enverité®
By Graf Research

# Previous: Verify through Reverse Engineering

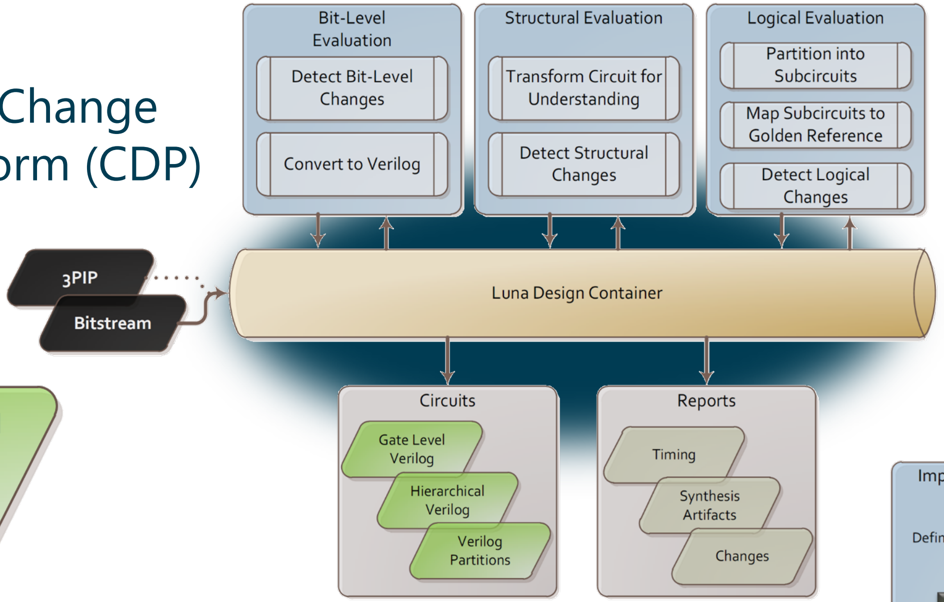
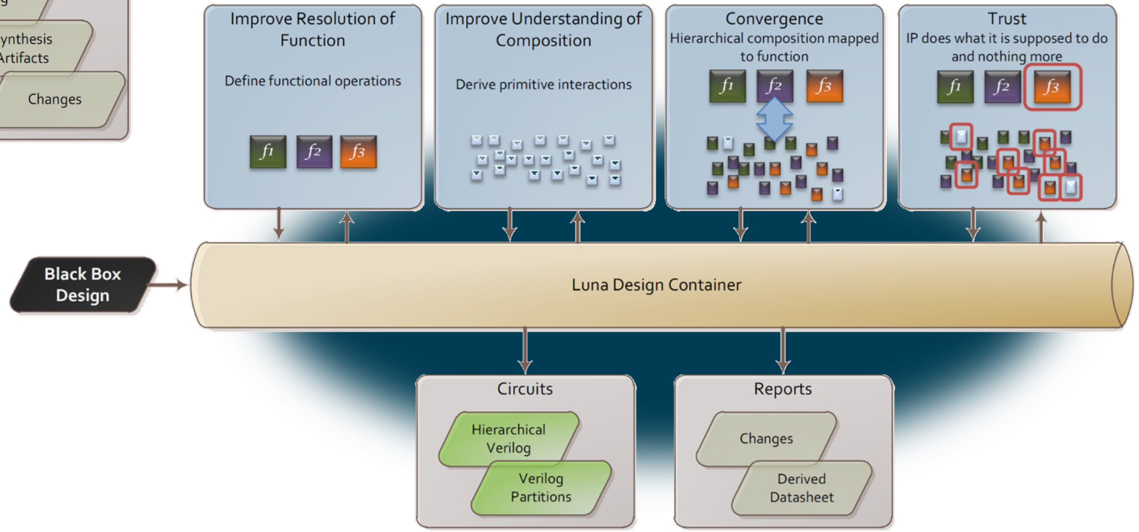


Fig. 3. Luna's Change Detection Platform (CDP)



Improve Resolution of Function
Define functional operations
Improve Understanding of Composition
Derive primitive interactions
Convergence
Hierarchical composition mapped to function
Trust
IP does what it is supposed to do and nothing more
f1
f2
f3
Black Box Design
Luna Design Container
Circuits
Hierarchical Verilog
Verilog Partitions
Reports
Changes
Derived Datasheet

Fig. 4. Luna's Functional Derivation Platform (FDP)

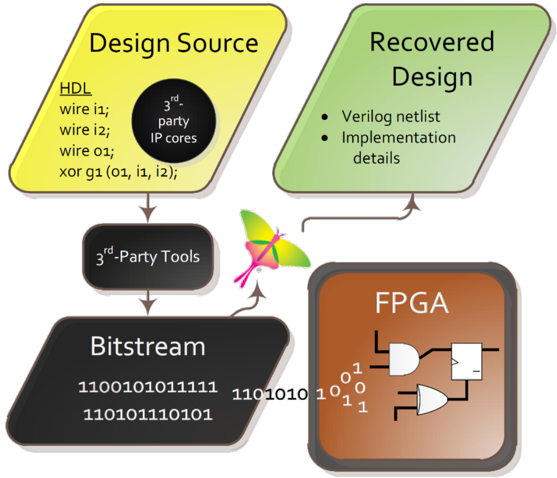
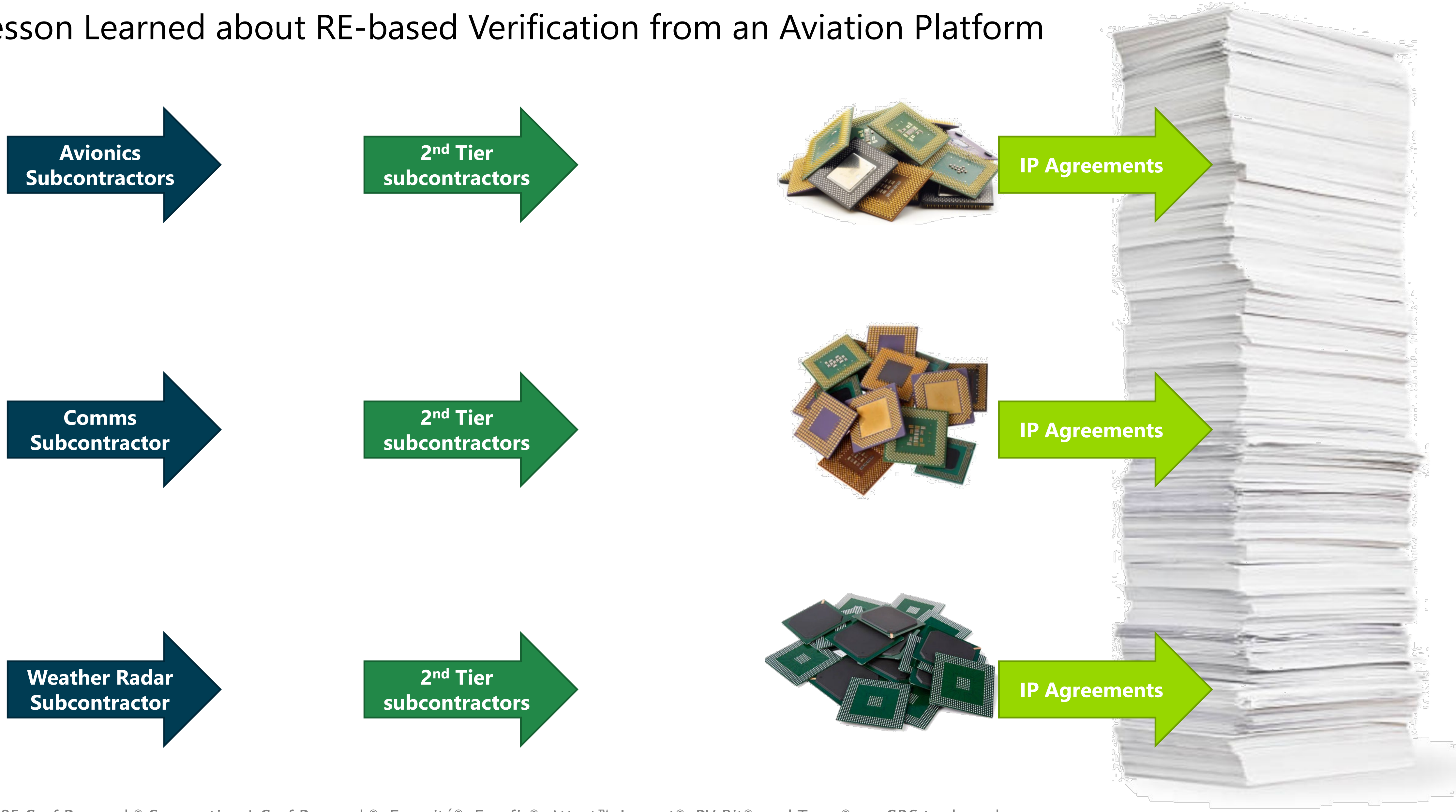


Fig. 1. Recovering design details from a bitstream

J. Graf, S. Harper, L. Lerner, "The Integrity of FPGA Designs: Capabilities Enabled by Unlocking Bitstreams and 3rd-Party IP," GOMAC 2012
J. Graf, S. Harper, L. Lerner, "Ensuring Design Integrity through Analysis of FPGA Bitstreams and IP Cores," ERSA 2012 Keynote

# Verify the Bits the Fly?

Hard Lesson Learned about RE-based Verification from an Aviation Platform



Avionics Subcontractors

2nd Tier subcontractors

IP Agreements

Comms Subcontractor

2nd Tier subcontractors

IP Agreements

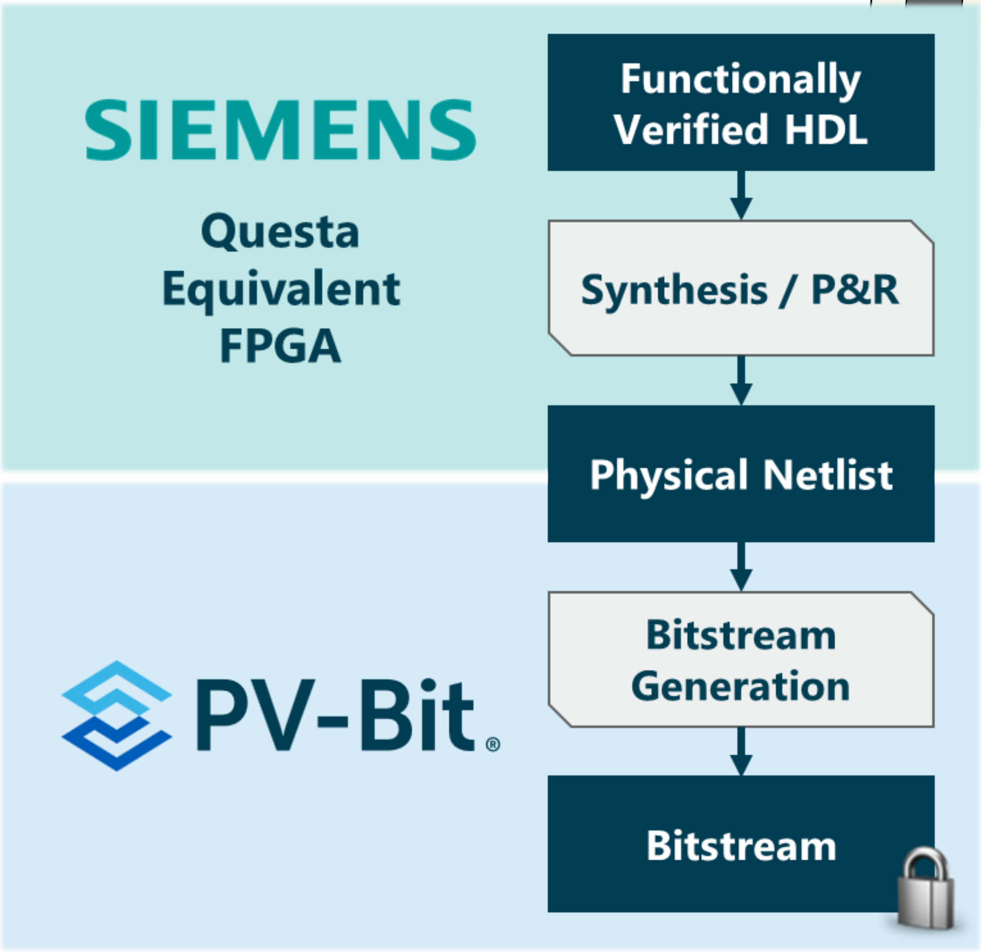
Weather Radar Subcontractor

2nd Tier subcontractors

IP Agreements

# New: HDL-to-Bitstream Equivalence Checking

- Ensures **unintended errors and/or malicious modifications have NOT been inserted** during the design build flow
- Pairing **Questa Equivalent FPGA** with **Enverité PV-Bit** creates a verification toolchain that performs HDL-to-bitstream equivalence checking
  0. Precondition: HDL is functionally verified
  1. Questa Equivalent FPGA: Verifies the logical equivalence between the HDL and Physical Netlist
  2. Enverite PV-Bit: Verifies the physical and logical equivalence between the Physical Netlist and Bitstream



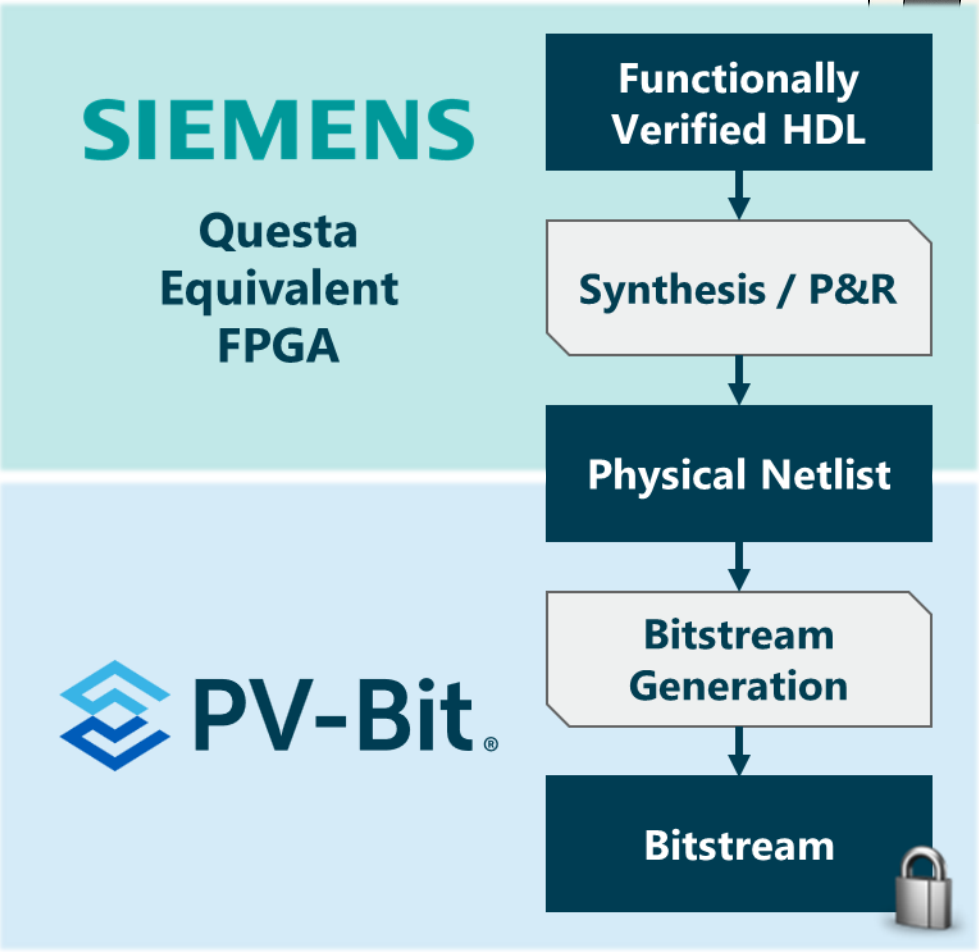
# New: HDL-to-Bitstream Equivalence Checking

Automated Evaluation of Physical and Logical Equivalence

Designed for the Typical End User

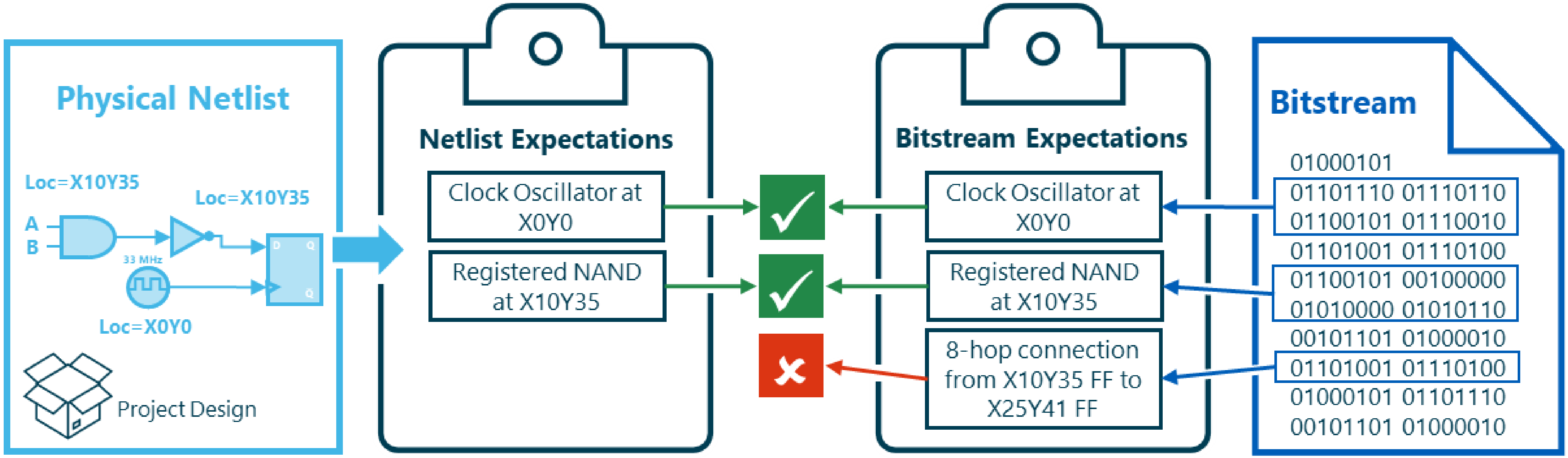
Respects FPGA Vendor Bitstream

Respects Third Party Vendor IP



# Enverité PV-Bit Verification Process

A Logical and Physical Equivalence Check in the Properties Domain



Physical Netlist

Project Design

Netlist Expectations

- Clock Oscillator at X0Y0
- Registered NAND at X10Y35

✓

✓

✗

Bitstream Expectations

- Clock Oscillator at X0Y0
- Registered NAND at X10Y35
- 8-hop connection from X10Y35 FF to X25Y41 FF

Bitstream

```
01000101
01101110 01110110
01100101 01110010
01101001 01110100
01100101 00100000
01010000 01010110
00101101 01000010
01101001 01110100
01000101 01101110
00101101 01000010
```

AMD | altera | LATTICE SEMICONDUCTOR | MICROCHIP

AMD, Lattice, Altera, and Microchip logos are registered trademarks of their respective corporations

# Lessons Learned

Make what the SCCM market wants, not just what it needs

Make your SCCM solution work with, not against, the interest of Silicon Valley

Bootstrap – VCs are often not patient enough for SCCM solutions

CHALLENGE 2

# Find Counterfeit FPGAs

Enverité®
By Graf Research

# Pre-existing Solutions

Image credit : Battelle

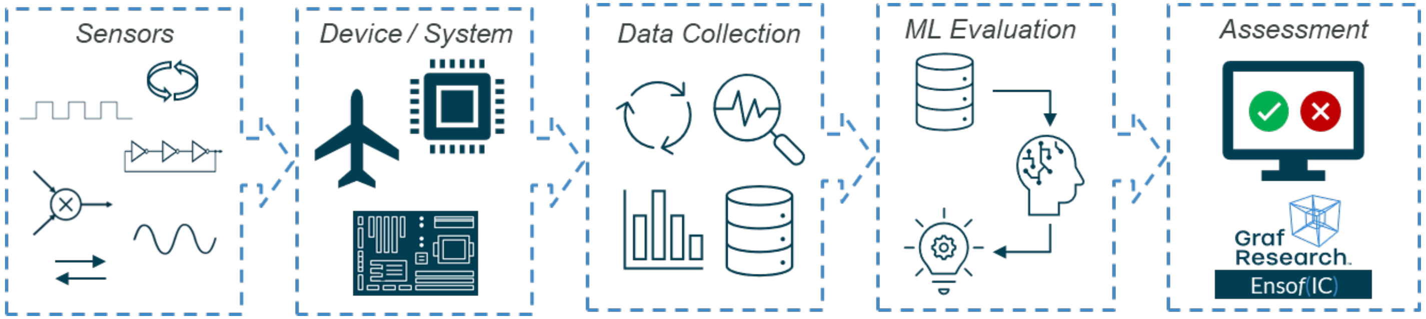
# EnsofIC Tool Suite

- EnsofIC Foundation
  - Soft sensors to extract knowledge from FPGAs
  - Support for AMD Xilinx and Altera devices
  - Techniques readily extendable to other vendors and device types
  - Broadly applicable throughout the supply chain
- Attest
  - Platform for detecting counterfeit FPGAs without external equipment
  - Non-destructive, at-rest or at-boot
- Inspect
  - Platform for analyzing characteristics of FPGA silicon
  - Data transformations, analyses, visualizations, and reporting

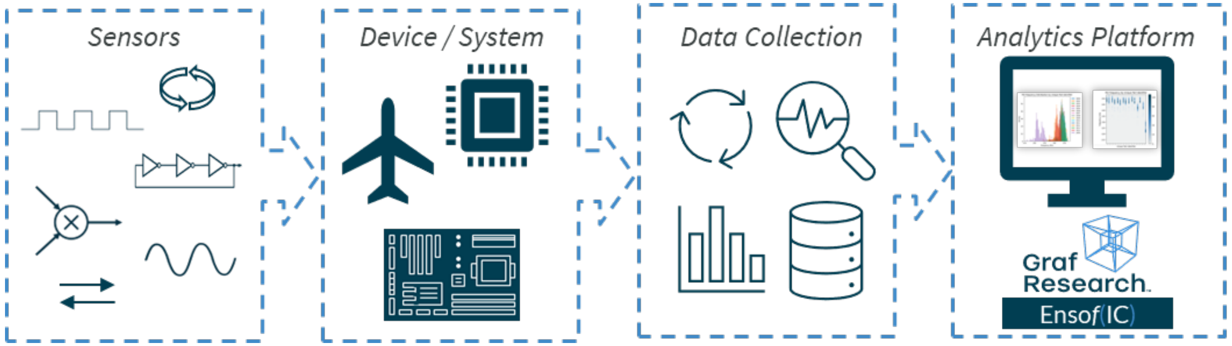
*Patent Pending: US 2024/0362133 A1*

# EnsofIC Attest & Inspect

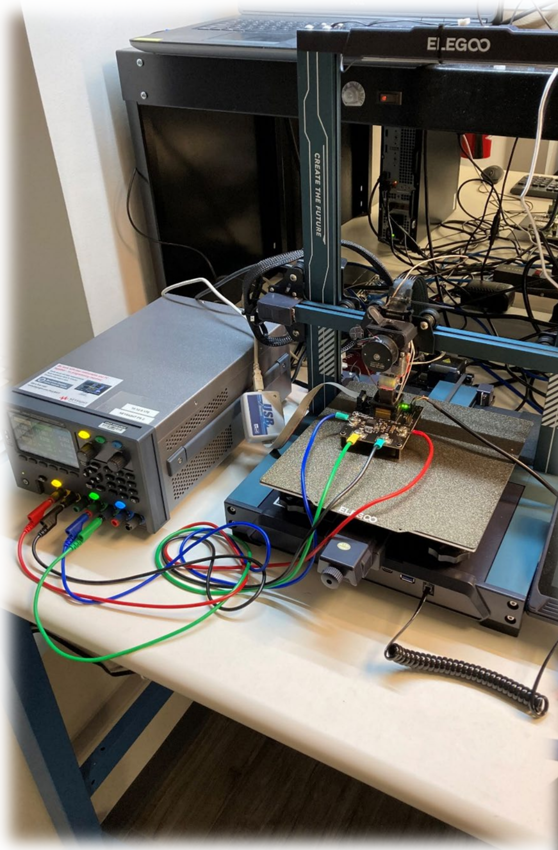
- **Attest**: For a ***user of any skill*** who simply wants to ***quickly ascertain*** whether a device is ***genuine or counterfeit***
  - Genuine / counterfeit classification
  - Focused on repackaged counterfeits
  - ID devices as quickly as possible
  - Abstracts–away raw sensor data

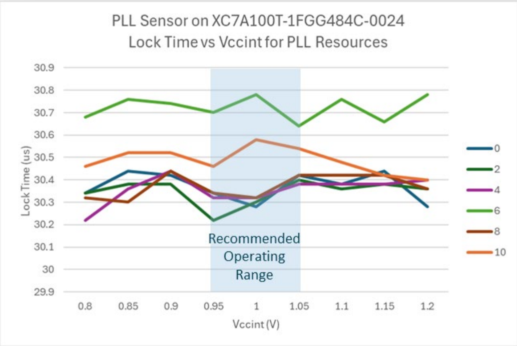


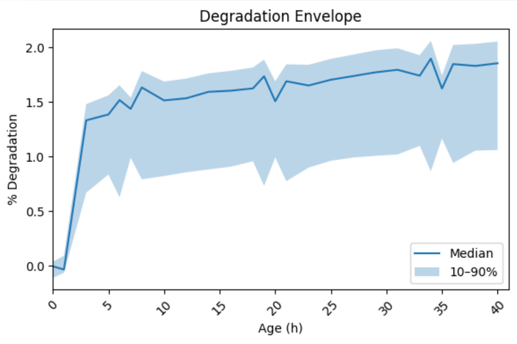
- **Inspect**: For an ***analyst or engineer*** who wants a powerful suite of sensors that can ***interrogate the FPGA silicon***, producing ***data that can be analyzed*** in both currently recognized and future/extensible ways
  - In-depth analytics using statistics, transformations, and visualizations
  - Examine inter- and intra-device relationships
  - Directly access to raw sensor data
  - Extensible to new analytics and sensors

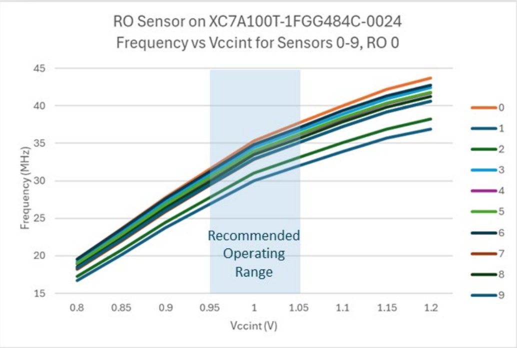


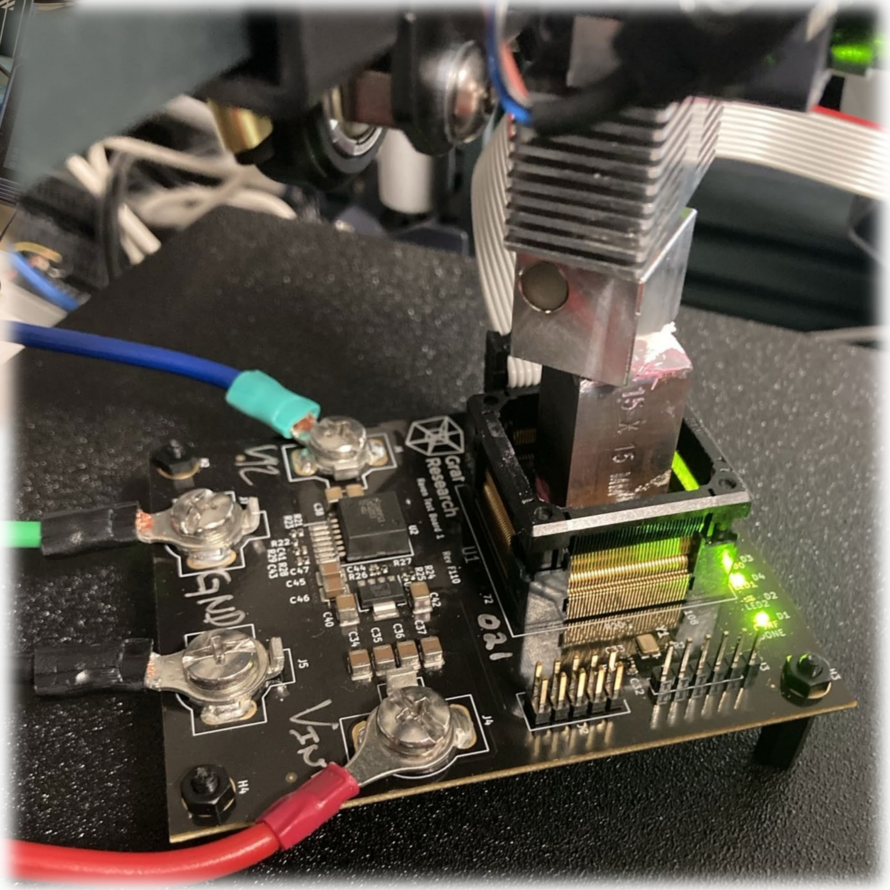
*Patent Pending: Application No. 63/462,604*

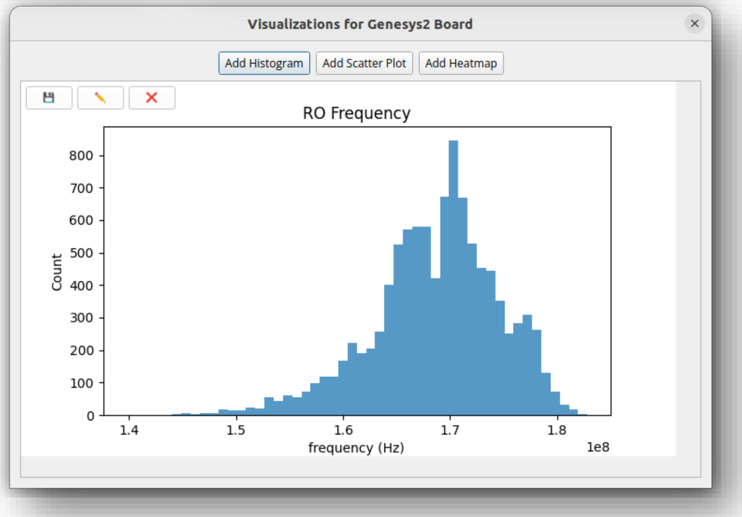


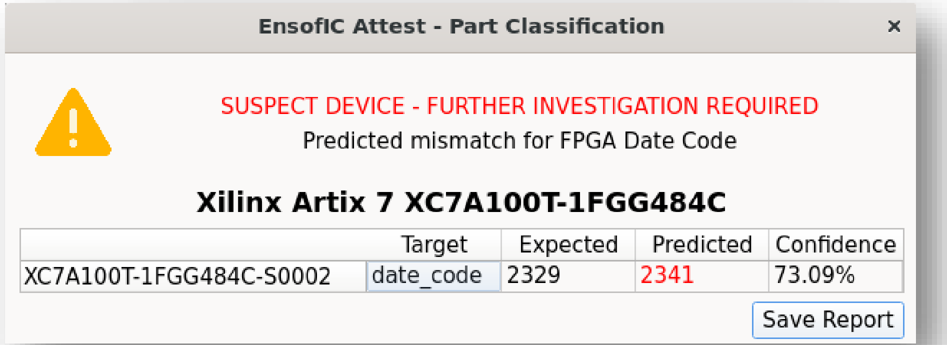












EnsofIC Attest - Part Classification

SUSPECT DEVICE - FURTHER INVESTIGATION REQUIRED

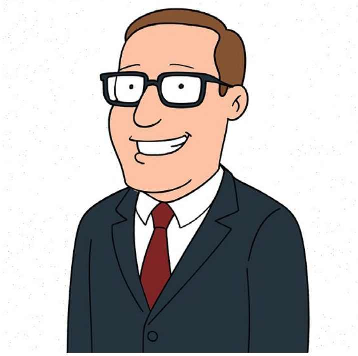
Predicted mismatch for FPGA Date Code

**Xilinx Artix 7 XC7A100T-1FGG484C**

| | Target | Expected | Predicted | Confidence |
|---|---|---|---|---|
| XC7A100T-1FGG484C-S0002 | date_code | 2329 | 2341 | 73.09% |

Save Report

# Lessons Learned



Meet the customer at their need

Be Apple, not Microsoft

Restate your technology in the language of the customer need

# Additional Principles

Enverité®
By Graf Research

# Additional Lessons Learned

| | | |
|---|---|---|
| Incremental is not interesting | Grow organically<br>(one degree principle) | Stick to your values<br>(Values — Graf Research) |
| Don’t make fragile solutions | Don’t be a one-trick pony | Hire your SCCM classmates |
| Pay attention to who is paying for SCCM solutions | Be fair | Have grit and hustle |

# For more…

### At FPL 2025

- **Booth & Industrial Talk**
- **Demo of Enverité PV-Bit** finding a hardware Trojan in a bitstream (Wednesday)

### PV-Bit Reading

- https://www.grafresearch.com/pvbit
- **J. Graf**, E. Drinkert, S. Harper, M. Winslow, A. Cook, A. A. Sohanghpurwala, T. Dunham, and W. Tabada, **"Accelerating Recertification of FPGA-Based Avionics Systems via Bitstream Equivalence Checking,"** in *Proc. 44th AIAA/IEEE Digital Avionics Systems Conf. (DASC)*, Sept. 2025.
- A. Sohanghpurwala, D. Gibson, S. Harper, **J. Graf**, and T. Dunham, **"PV-Bit: Private Verification of FPGA Bitstreams Via Bitstream Equivalence Checking,"** in *Proc. IEEE Secure Development Conf. (SecDev)*, Indianapolis, IN, USA, Oct. 2025.

### EnsofIC Reading

- **W. Batchelor**, J. Koiner, C. Crofford, K. Paar, M. Winslow, M. Taylor, S. Harper, **"Attest: Non-Destructive Identification of Counterfeit FPGA Devices,"** in *Proc. IEEE Physical Assurance and Inspection of Electronics (PAINE)*, Huntsville, AL, USA, 2023.
- **W. Batchelor,** C. Crofford, M. Winslow, M. Taylor, K. Paar, J. Koiner, S. Harper, **"Towards Synthetic Data Generation for Characterization of FPGAs,"** in *GOMACTech 2025 Proc.*, Mar. 2025.
- **W. Batchelor**, C. Crofford, J. Koiner, M. Winslow, M. Taylor, K. Paar, S. Harper. **"Counterfeit FPGA Characterization and Classification with Soft Sensors and Machine Learning"** in *Proc. Ground Vehicle Systems Engineering and Technology Symp. (GVSETS)*, NDIA, Novi, MI, USA, Aug. 12–14, 2025.