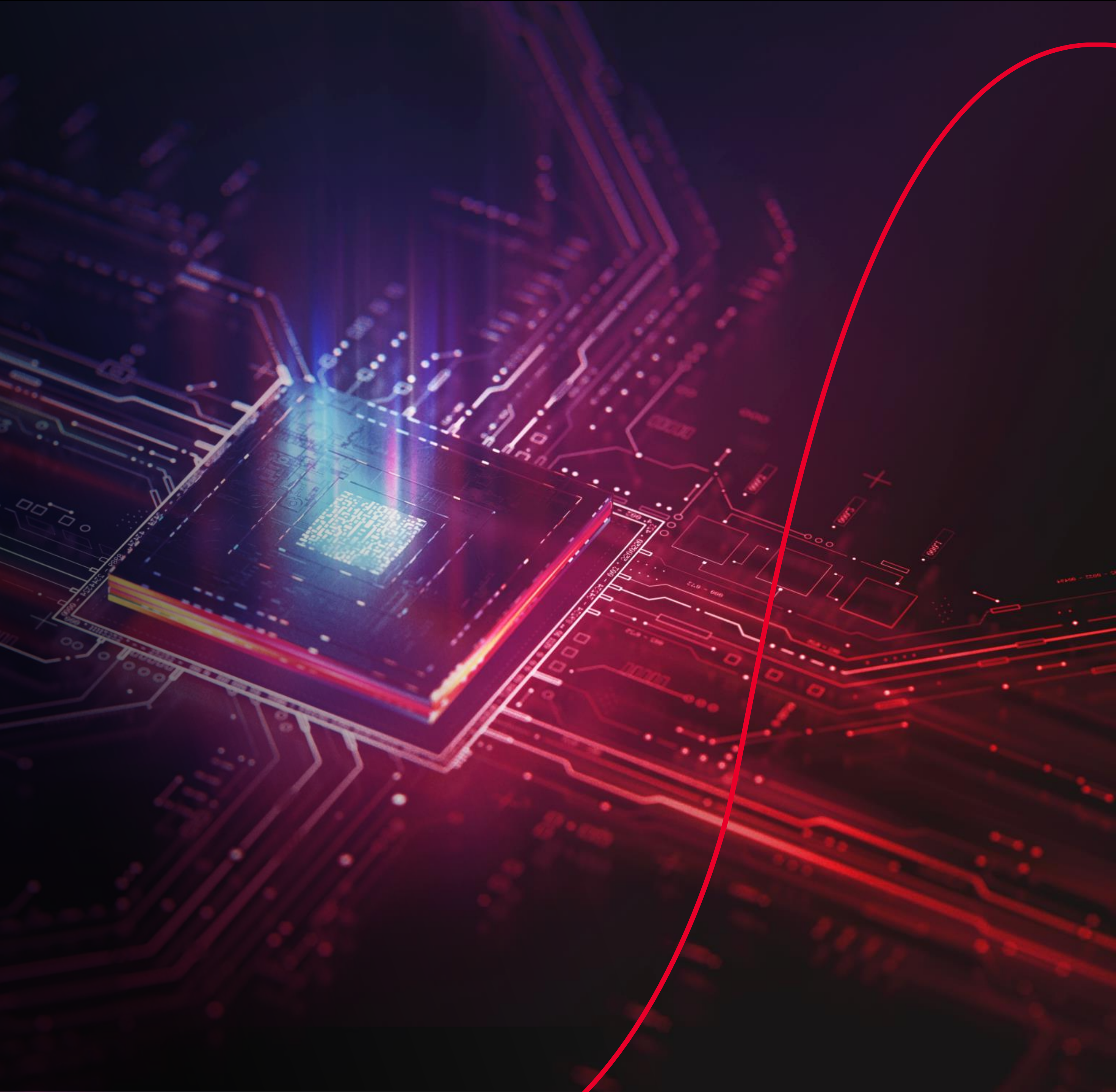
KEYSIGHT

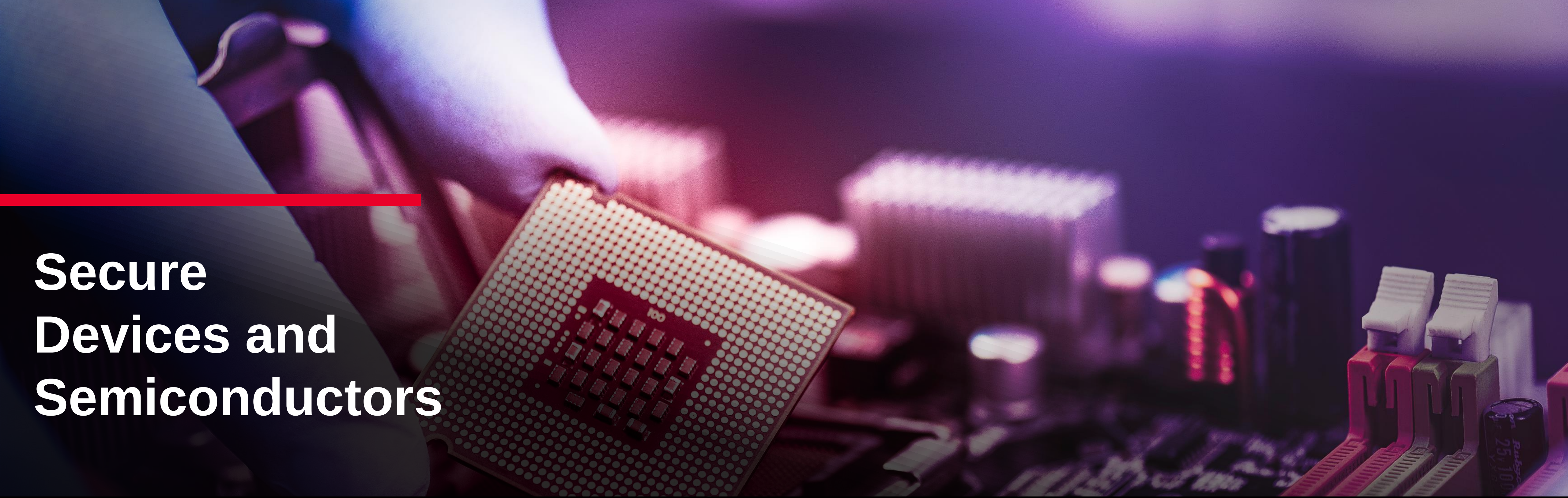
Pre-silicon Identification of Security Vulnerabilities

Doug Carson, Solution Expert
doug.carson@keysight.com

Verification Futures 1/7/2025



Innovators
▶ start here



Secure Devices and Semiconductors

Semiconductor Development

- Secure enclaves in ICs
- Assure cryptography silicon
- Protect foundry supply chain
- Protect sensitive IP

Aerospace and Defense

- Prevent reverse engineering
- Identify supply chain threats
- Secure communications
- Chain of trust in systems

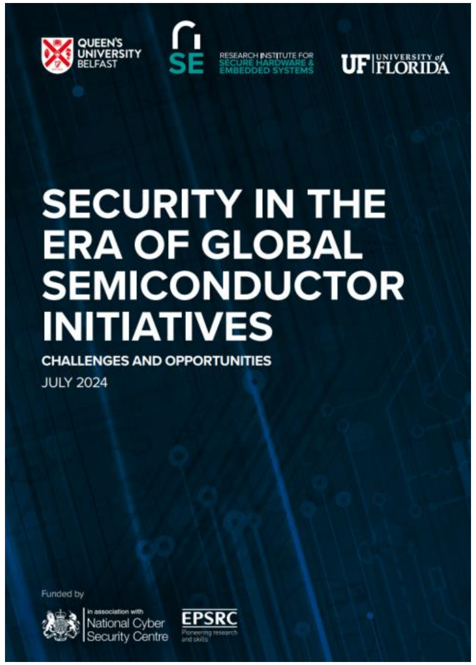
Commercial Communications

- ORAN radio security
- GSMA eSIM security
- Digital wallets on devices
- Secure boot in network equipment and IoT devices

Data Center

- Trusted platform modules
- OCP SAFE certification
- Full lifecycle protection of cryptographic material
- Secure AI models from theft and tampering

Industry View on Semiconductor Challenges



QUEEN'S UNIVERSITY BELFAST

SE RESEARCH INSTITUTE FOR SECURE HARDWARE & EMBEDDED SYSTEMS

UF UNIVERSITY of FLORIDA

SECURITY IN THE ERA OF GLOBAL SEMICONDUCTOR INITIATIVES

CHALLENGES AND OPPORTUNITIES

JULY 2024

Funded by

In association with National Cyber Security Centre

EPSRC Pioneering research and skills

Globalization

Supply Chain Security

Securing the lifecycle

System security

Packaging

Side channels

Complexity

Chiplets & mixed signal

Scaling Up

Secure by design feasibility

Skills shortage

AL and ML

CHIPS for AMERICA

Department for Science, Innovation & Technology

DARPA

U.S. DEPARTMENT OF HOMELAND SECURITY

[dstl] The Science Inside

NIST

intel

AMD

ANALOG DEVICES AHEAD OF WHAT'S POSSIBLE™

Qualcomm

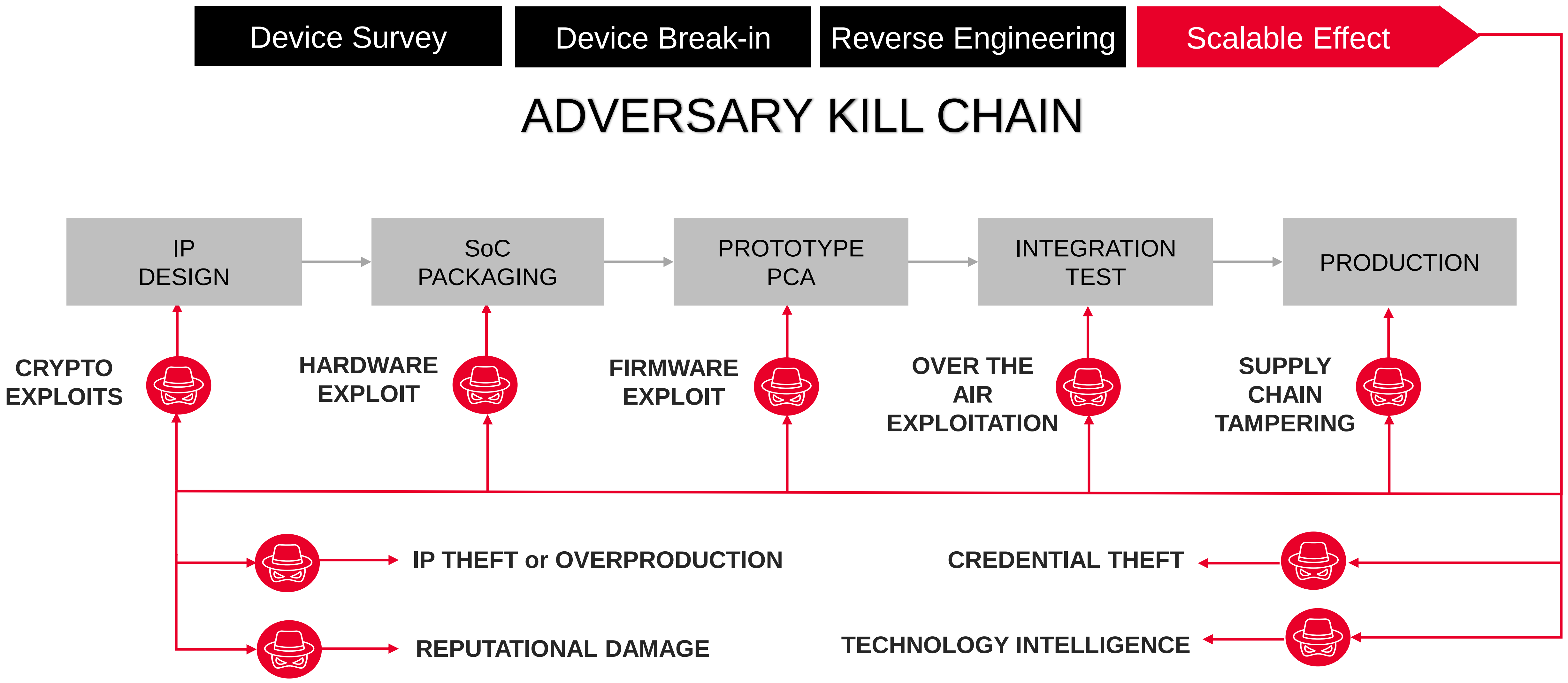
SYNOPSYS

MARVELL

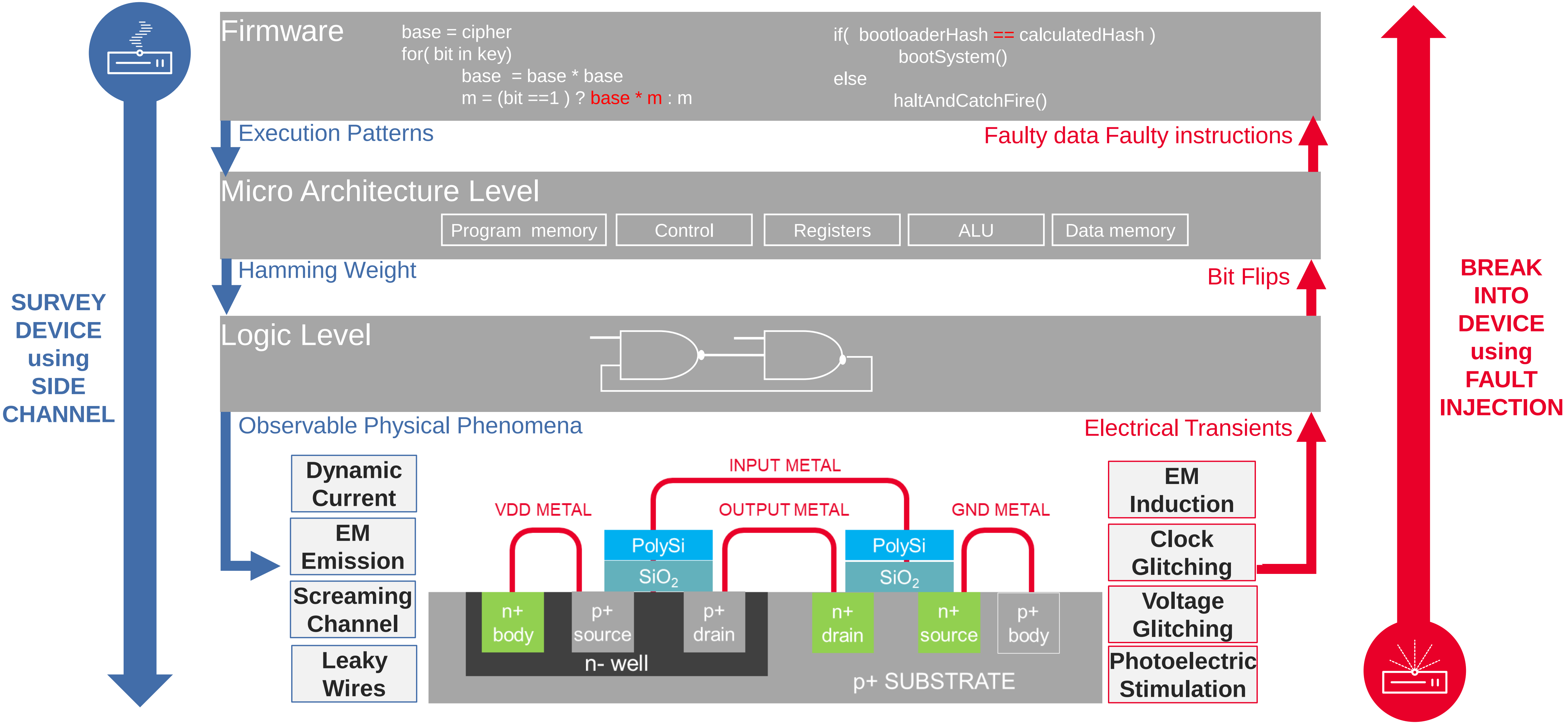
ERICSSON

SEAGATE

Exploiting Hardware Vulnerabilities



How is Hardware Hacked?



SURVEY DEVICE using SIDE CHANNEL

BREAK INTO DEVICE using FAULT INJECTION

Firmware

```
base = cipher
for( bit in key)
        base  = base * base
        m = (bit ==1 ) ? base * m : m
```

```
if(  bootloaderHash == calculatedHash )
        bootSystem()
else
        haltAndCatchFire()
```

Execution Patterns

Faulty data Faulty instructions

Micro Architecture Level

Program memory | Control | Registers | ALU | Data memory

Hamming Weight

Bit Flips

Logic Level

Observable Physical Phenomena

Electrical Transients

- Dynamic Current
- EM Emission
- Screaming Channel
- Leaky Wires

- EM Induction
- Clock Glitching
- Voltage Glitching
- Photoelectric Stimulation

Pre-silicon Opportunities to Break the Hardware Security Kill Chain

> “To know your enemy, you must become your enemy” – Sun Tzu

DISCOVER SIDE CHANNELS

Power leakage

Timing leakage

Electromagnetic leakage

Over the air leakage

IDENTIFY FAULT INJECTION POINTS

Power crowbar glitches

Clocking glitches

Laser fault injection

EM pulse injection

ASSESS VULNERABILITIES

Automated signal acquisition and analysis

Cryptographic test vector leakage assessment

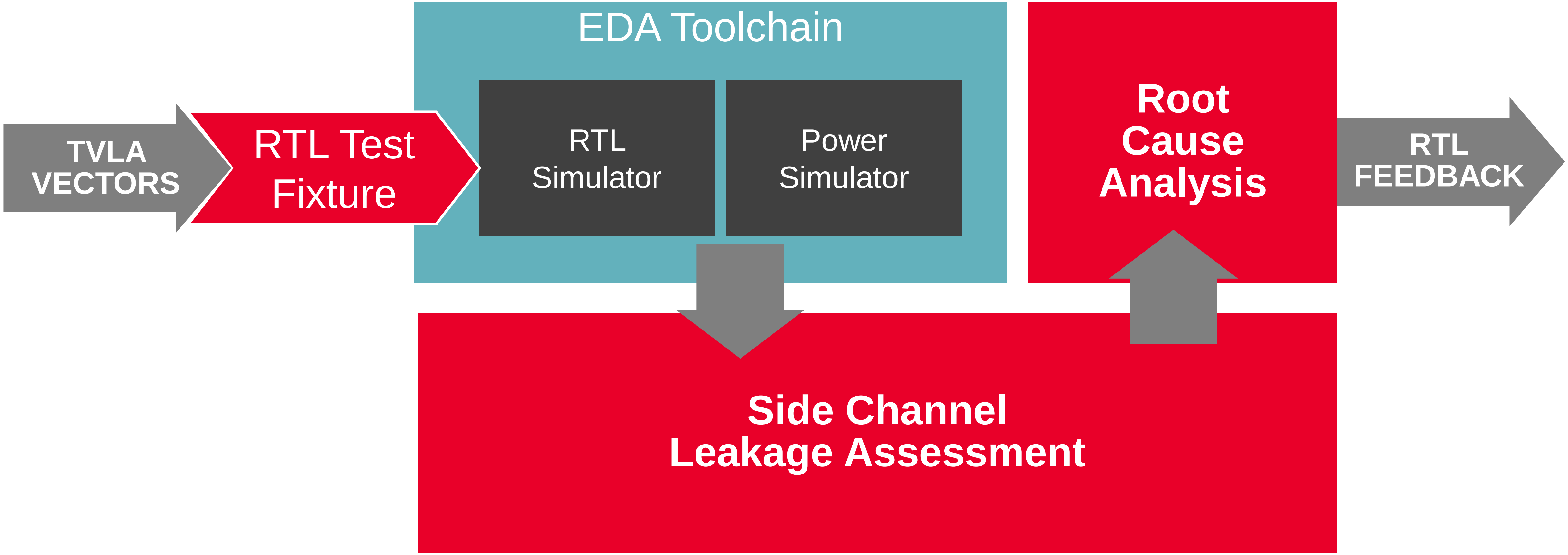
CERTIFY SYSTEM

Assure compliance to industry protection profiles

Traceability of 3rd party devices and subsystems

Pre-Silicon Analysis

Finding leakage at chip design



TVLA VECTORS

RTL Test Fixture

EDA Toolchain

RTL Simulator

Power Simulator

Root Cause Analysis

RTL FEEDBACK

Side Channel Leakage Assessment

Simulation types

RTL simulation

(signal analysis)

- Fast
- Easy to find root cause
- No gate delays

Netlist simulation (signal analysis)

- With/without gate delays
- Specific to cell library
- More realistic

Xilinx netlist simulation

(signal analysis)

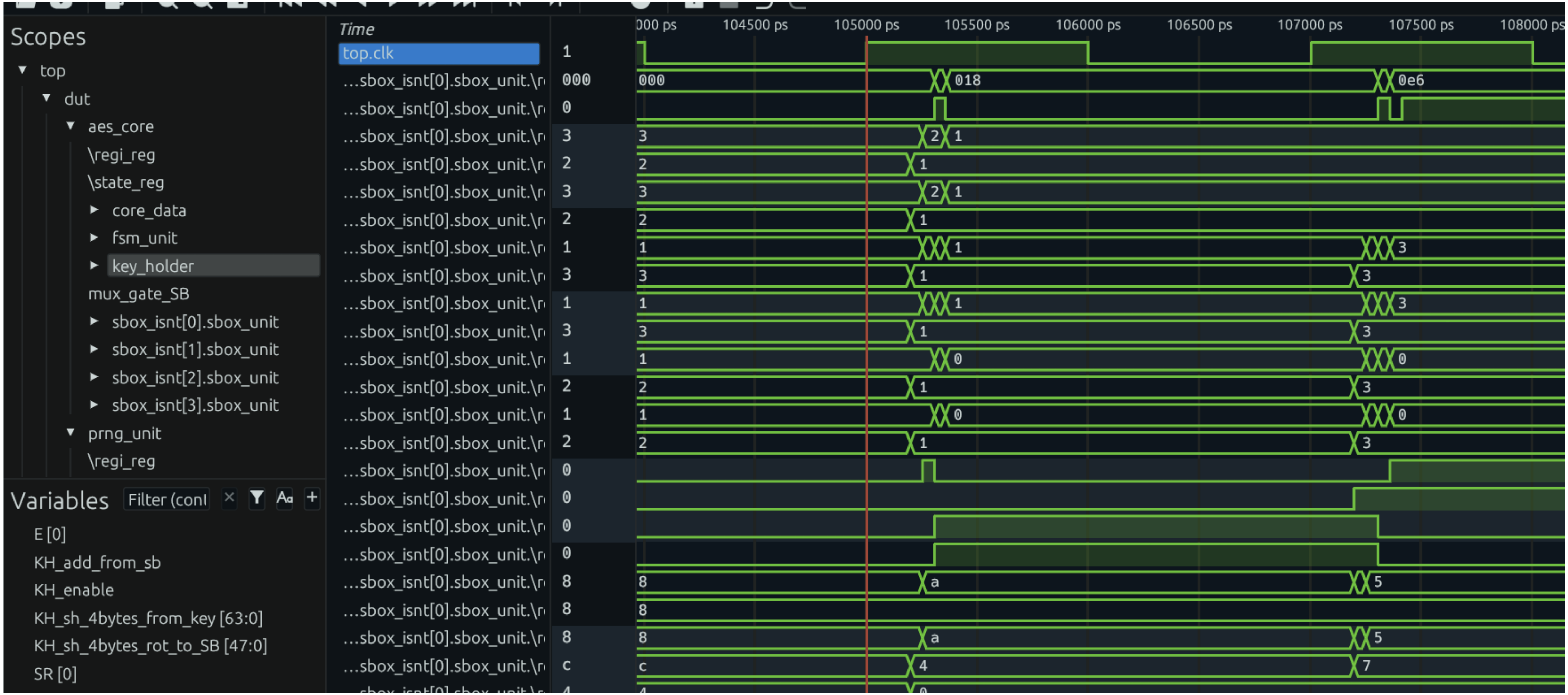
- With/without gate delays
- Specific to FPGA type
- More realistic
- No power simulation possible

Power analysis

- Slow
- Even more realistic

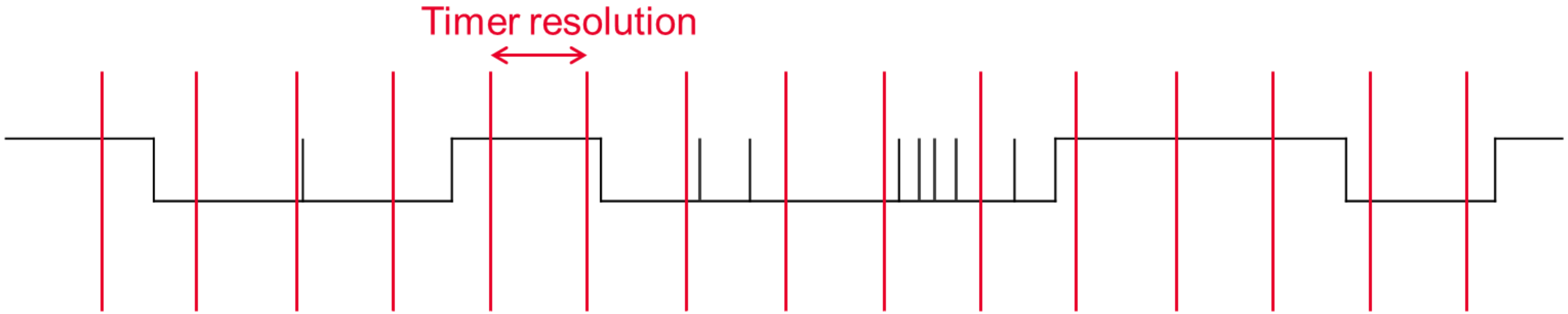
GLITCHES IN RTL SIMULATION

Snippet from VCD file



(C) KEYSIGHT TECHNOLOGIES

TEST CONFIGURATION

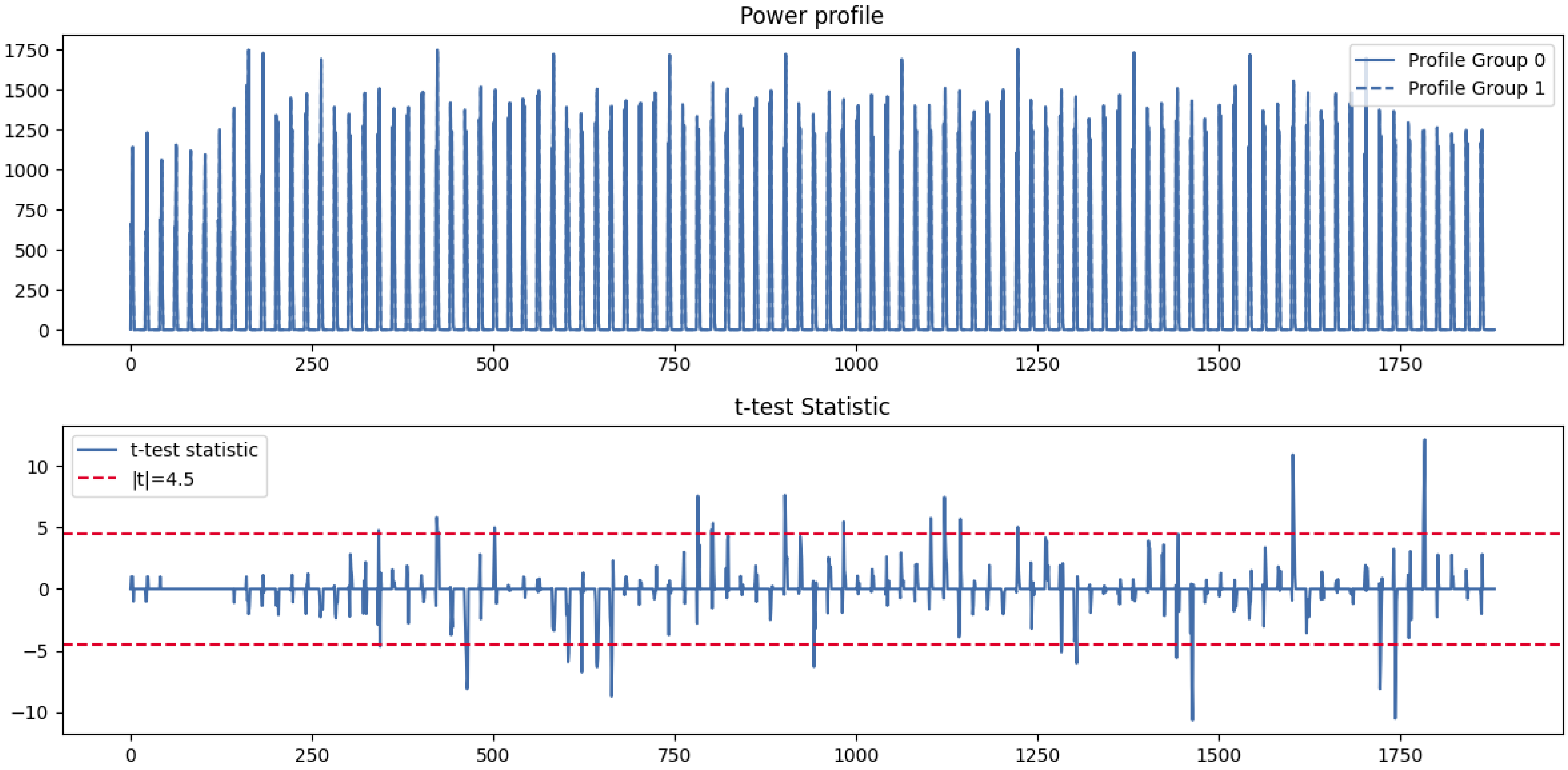


Model (per signal)

Toggle or not	0	1	0	1	1	0	1	1	0	1	1	0	0	1	0	1
Toggle count	0	1	0	2	1	0	1	4	0	8	3	0	0	1	0	1

Analysis using Inspector – Initial Revision

FPGA netlist simulation (including delays)

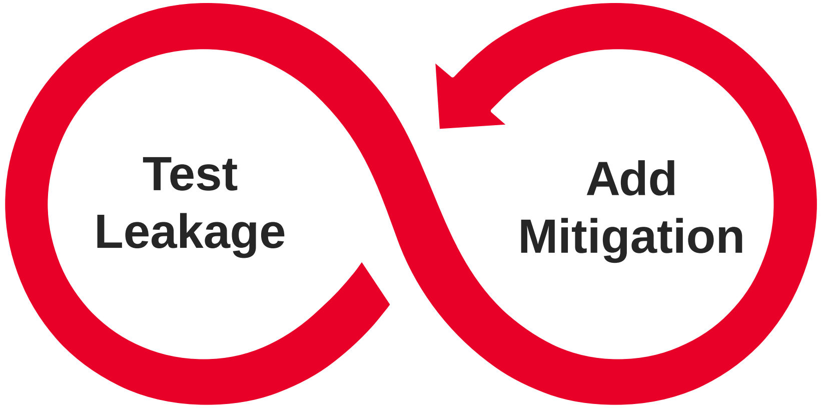


Testing the mitigated design

Countermeasures

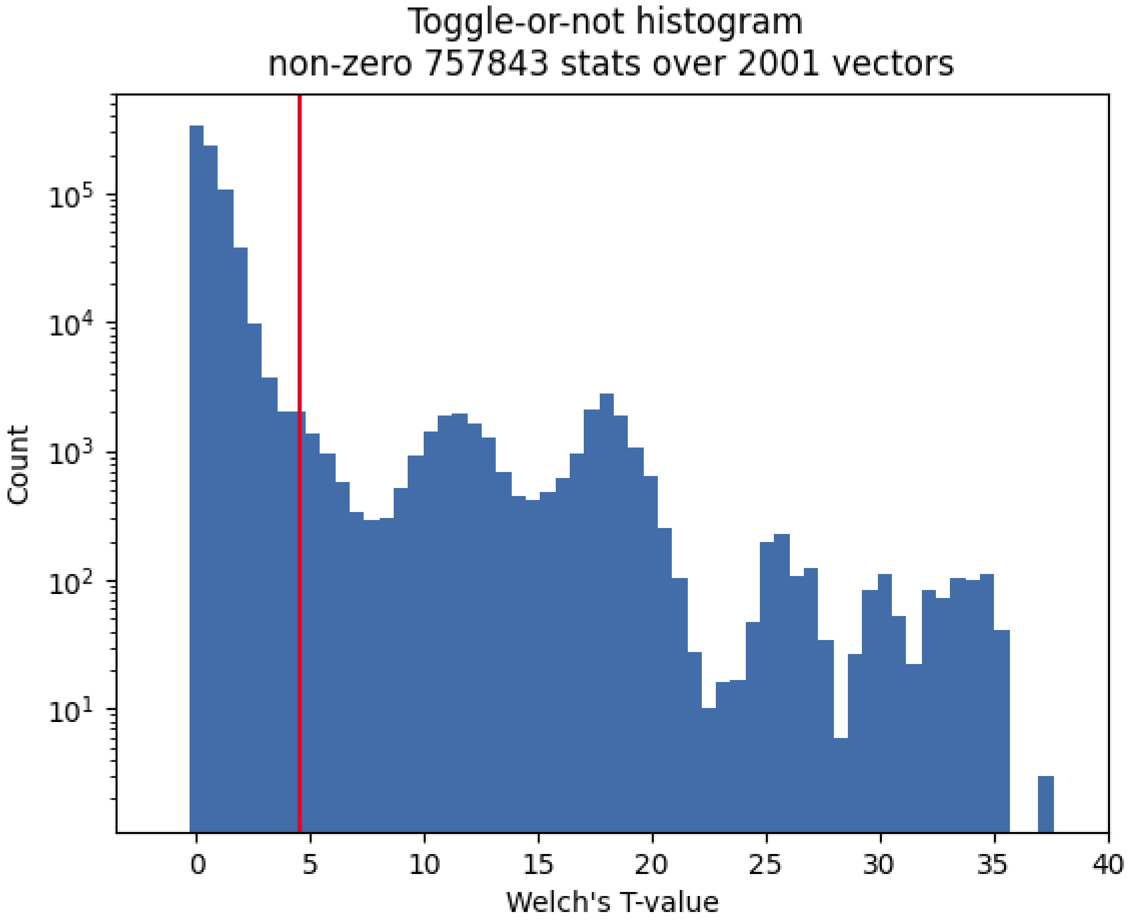
https://opentitan.org/book/doc/security/implementation_guidelines/hardware/index.html#general-module-level-design-guidance

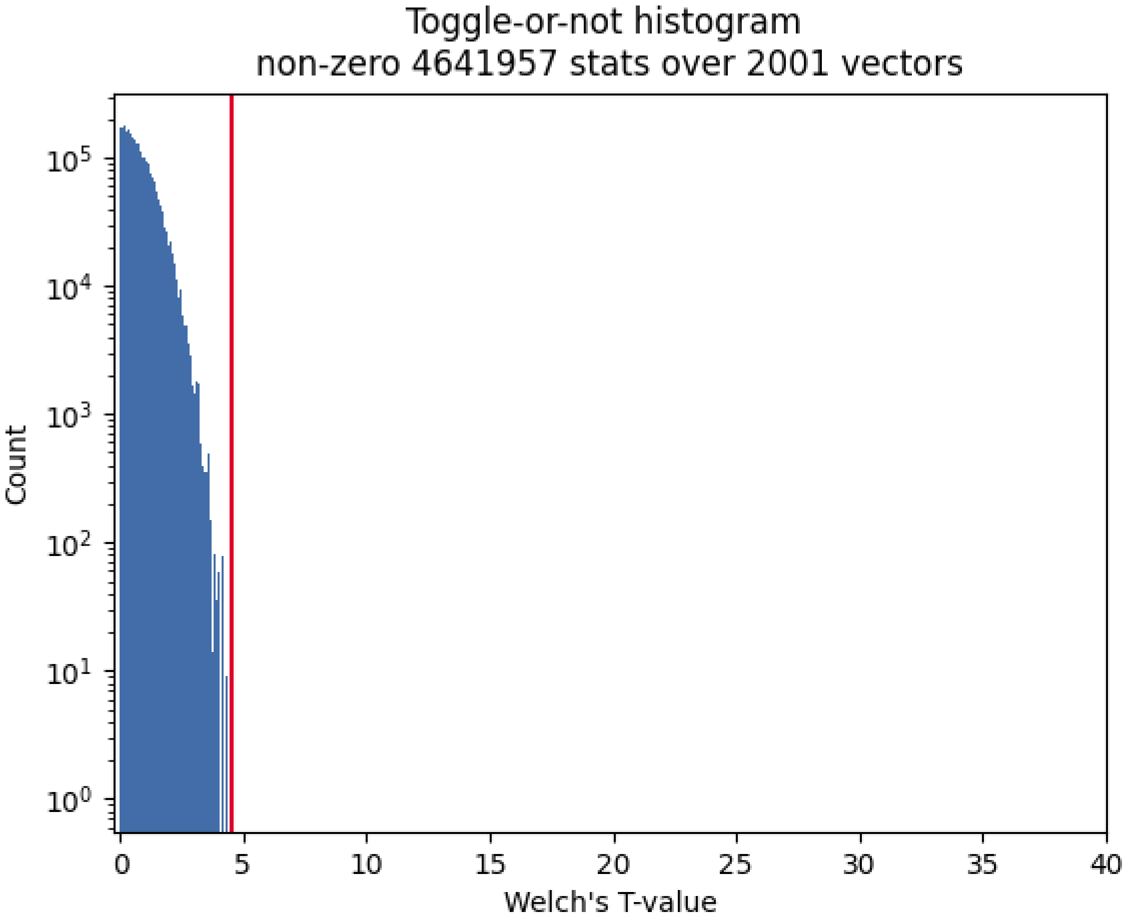
- 32-bit wide datapaths
- Constant time crypto operations
- Blinding and masking of intermediate values
- Increase Hamming weight on state representation
- ECC or dual rail on critical transfers
- Randomness using LFSFs
- Glitch detector circuits



Comparison of Leakage Before and After Testing

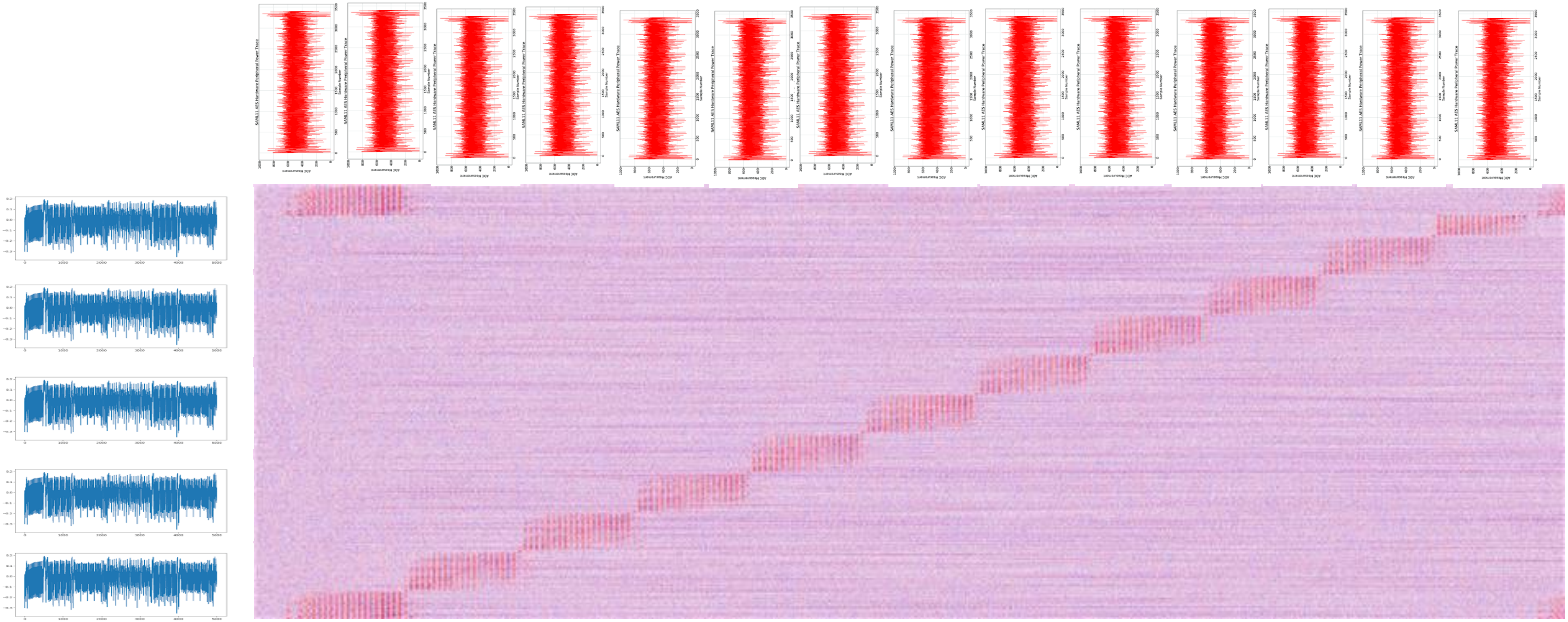
Before (left) vs after (right)





Correlation with physical measurements

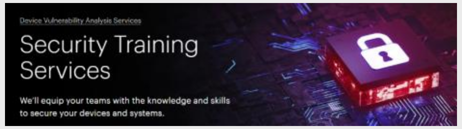
Most leaky signals from simulation



Measurements from FPGA

Keysight Hardware Security Solution Stack

Typical Customer Journey


Device Vulnerability Analysis Services
Security Training Services
We'll equip your teams with the knowledge and skills to secure your devices and systems.

Training & Education Services

Internal Development

OCP S.A.F.E.

GlobalPlatform™ SESIP

MIFARE

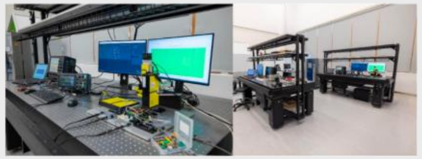
GSMA

EMVCo PARTNER

Certification Services

Security Classified Engineering

ISO
ISO/IEC 17024:2012
Accredited
Personnel Certification Body

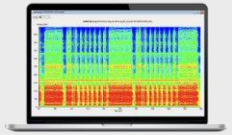


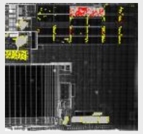
QUALITY MANAGEMENT SYSTEM
ISO 17025
ACCREDITED
LABORATORY

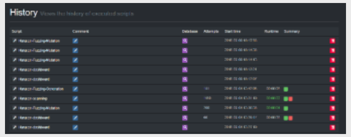
OPEN Compute Project
SOLUTION PROVIDER®

Assessment Services

Proprietary or Legacy Software



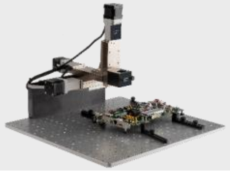




Inspector Orchestration & Automation

Existing Lab Assets

Digitizers
Waveform Generators



Hardware Attack
Test Fixtures
Accessories

Device Under Test

Summary

Device security is a real and growing threat impacting semiconductors, AD systems, communications and data centres

Kill chain is survey, break-in, reverse engineering and scalable effect. Break it by shifting left

Identify power and timing vulnerabilities in simulation to predict side-channel leakage at gate level.

.

Employ countermeasures or check with your IP provider.