SECURE-IC
THE SECURITY SCIENCE COMPANY

WHEN IS IT AN ATTACK?
DISTINGUISHING FAULT INJECTION PERTURBATION FROM ENVIRONMENTAL EFFECTS IN FPGA-BASED DIGITAL SENSOR

JAIF 2025

Authors: Idris Raïs-Ali, Khaled Karray, and Sylvain Guilley

Presenter: Idris Raïs-Ali

Date: 01/10/2025

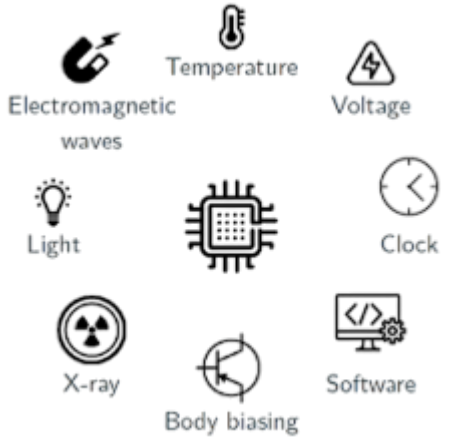
AGENDA

1. FIA countermeasures context and Digital Sensors introduction
2. Calibration
3. Outlooks & Conlusion

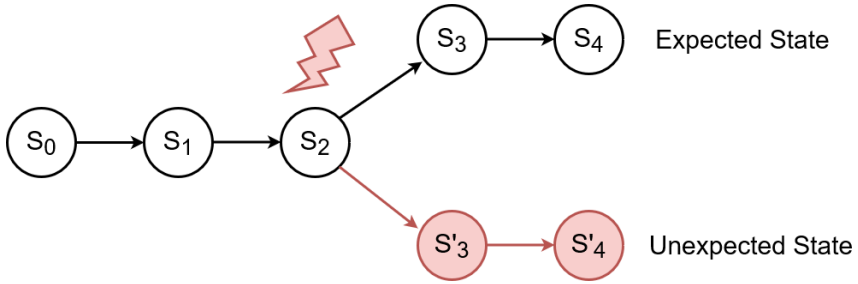
1. FIA COUNTERMEASURES CONTEXT AND DIGITAL SENSORS INTRODUCTION

FAULT INJECTION SAFETY CONTEXT

- Goals:
  - No unwanted FSM state
  - Principle: Detect, Decide and Act
  - Metrics: diagnostic coverage, compliance with a target level
    - SIL in IEC 62443
    - ASIL in ISO 26262



- Requirements:
  - Fast detection
  - Output control
  - Bounded response
  - Robust design and safe FSM default states



⚠ Safety is not Security

CYBERSECURITY: FIPS 140-3 LEVELS

Level	Main Objective	Physical Protection	Key Management	Typical Use Cases
1	Basic security	No special physical requirements	Mandatory cryptographic self-tests	Software libraries, simple crypto modules
2	Tamper-evidence	Tamper-evident coatings, seals, visible protections	Role-based authentication (user/admin)	Smart cards, networking equipment
3	Tamper-resistance	Tamper-resistant enclosure, separation of critical interfaces	Automatic zeroization of keys upon intrusion	Banking HSMs, PKI modules
4	Hostile environment resistance	Active monitoring (voltage, temperature, frequency, radiation, glitching)	Automatic zeroization, protection against fault injection	Military devices, high-security government systems

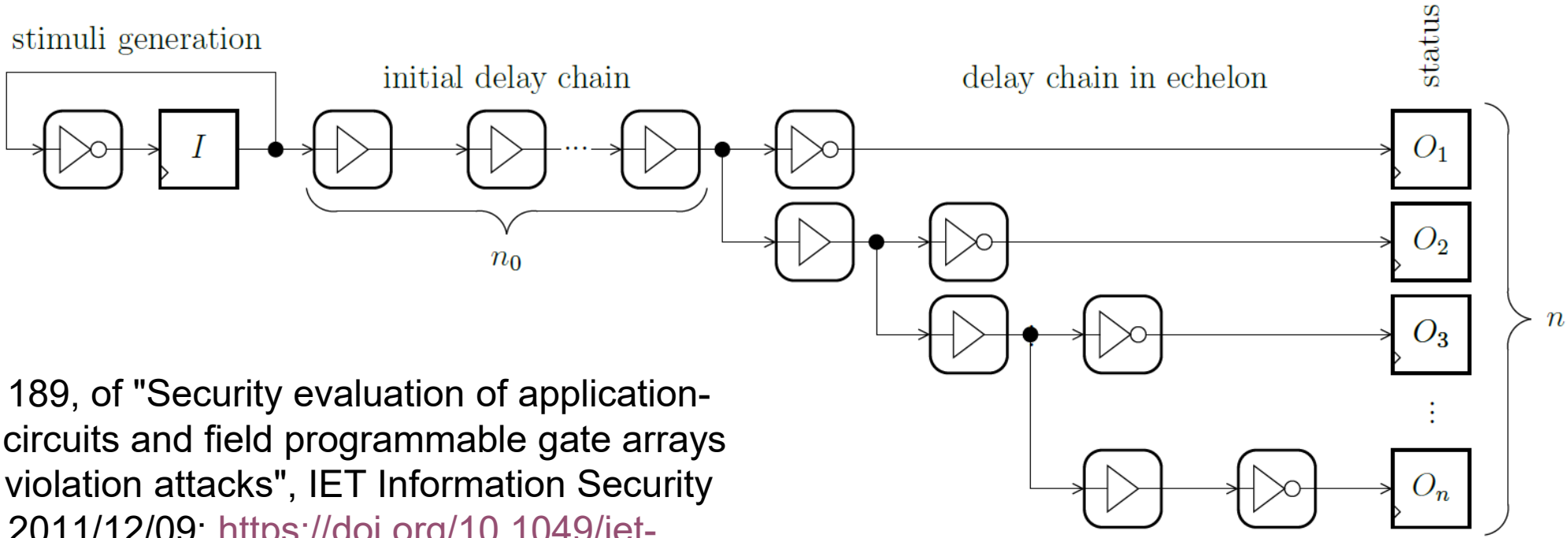
CYBERSECURITY: FIPS 140-3 LEVELS

Level	Main Objective	Physical Protection	Key Management	Typical Use Cases
1	Basic security	No special physical requirements	Mandatory cryptographic self-tests	Software libraries, simple crypto modules
2	Tamper-evidence	Tamper-evident coatings, seals, visible protections	Role-based authentication (user/admin)	Smart cards, networking equipment
3	Tamper-resistance	Tamper-resistant enclosure, separation of critical interfaces	Automatic zeroization of keys upon intrusion	Banking HSMs, PKI modules
4	Hostile environment resistance	Active monitoring (voltage, temperature, frequency, radiation, glitching)	Automatic zeroization, protection against fault injection	Military devices, high-security government systems

DIGITAL SENSOR CONCEPT

- Initial delay chain (length n_0)
- Delay chain with n registers
- Output status $s = (O_1, \ldots, O_n)$

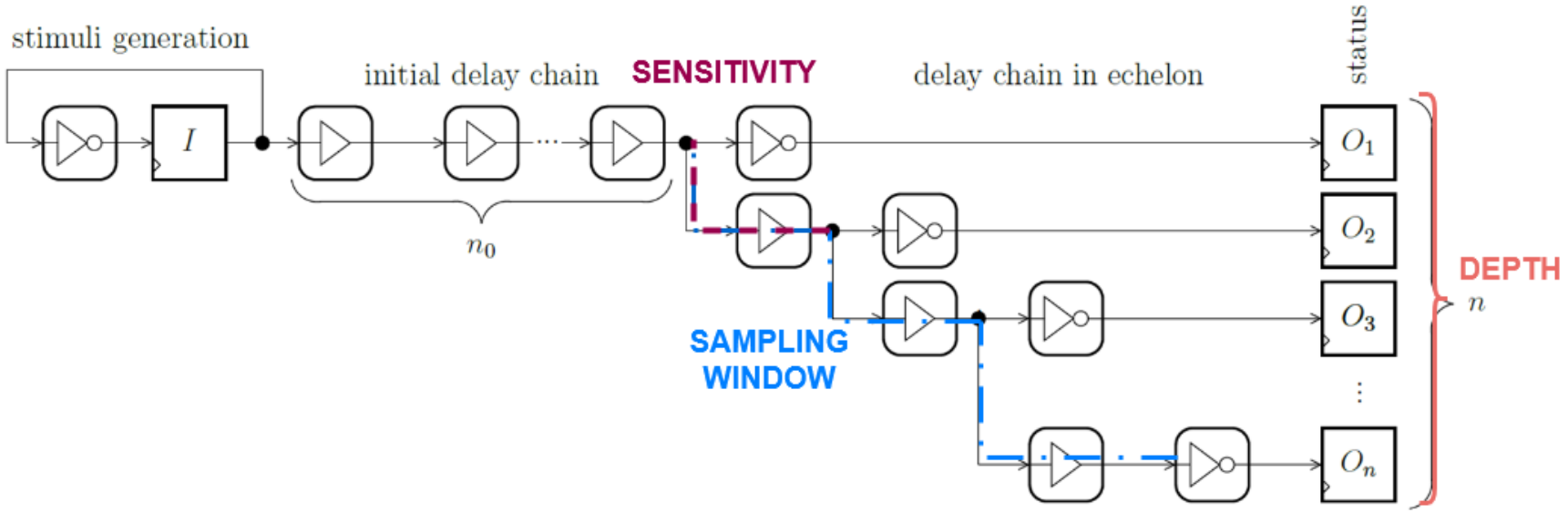
It is a "Time to Digital Converter" (TDC)



See: Fig. 14, page 189, of "Security evaluation of application-specific integrated circuits and field programmable gate arrays against setup time violation attacks", IET Information Security **5**(4), pp. 181~190, 2011/12/09: https://doi.org/10.1049/iet-ifs.2010.0238

2. CALIBRATION

PRE-SILICON CALIBRATION



- Sensitivity s: number of buffers between two following registers
- Sampling Window W: « distance » between the first and the last register
- Depth: Number of registers n
- $W = s \cdot n$

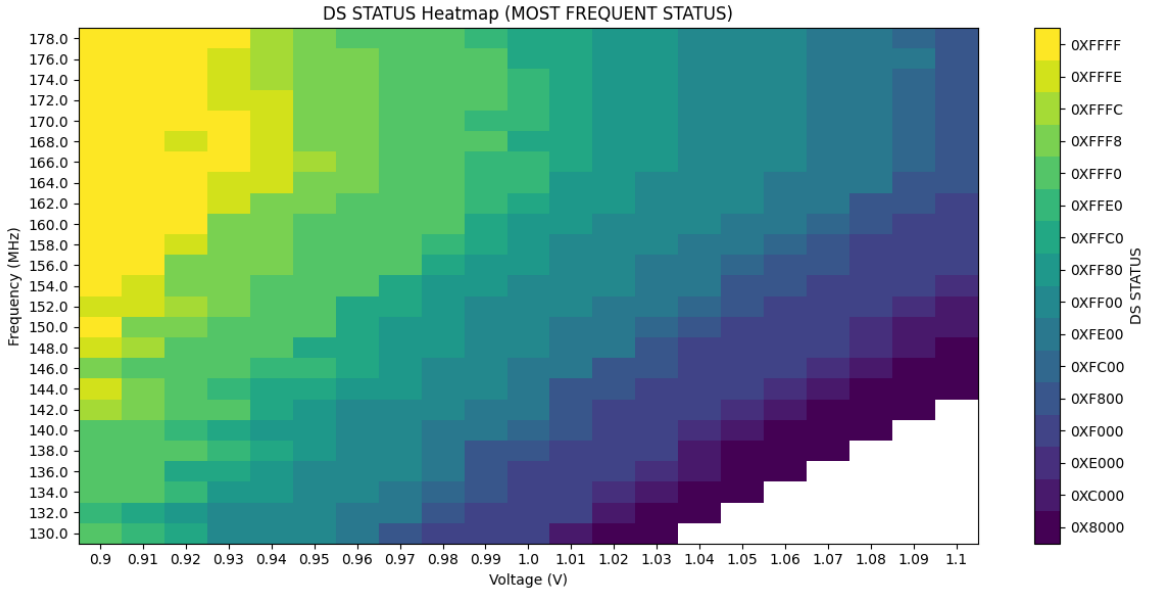
POST-SILICON CALIBRATION 1/4: DEFINITION

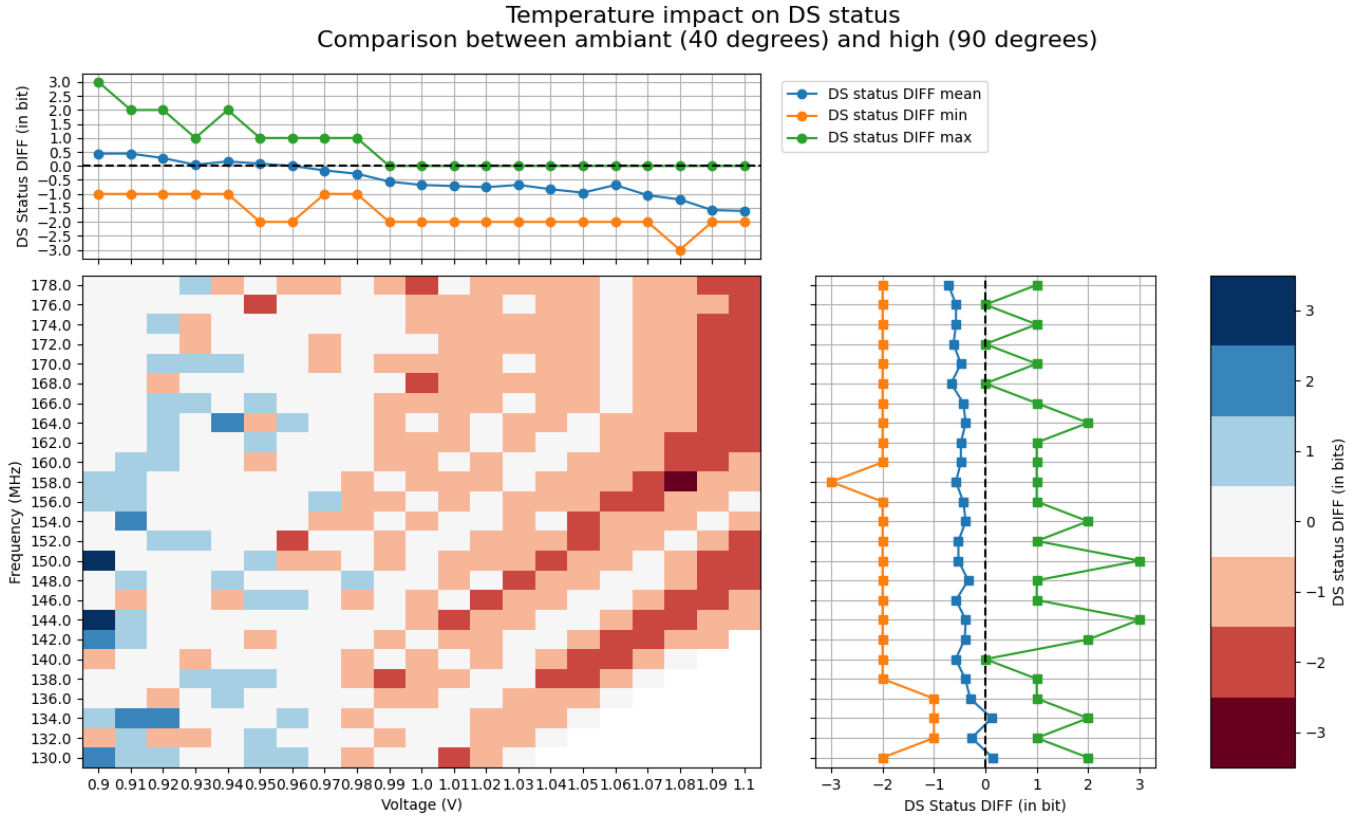
- Trimming procedure:
  - Objective:
    - Compensate calibration uncertainty
      - Process design kit characterization not fully performed (by the foundry)
      - Gap between simulation and reality (models vs reality, simulation accuracy, RC parasitics)
  - Measure propagation delay in delay chains for PVT corner
  - Get extremal delay chain status
  - Apply mask as alarm threshold
- Normal Operation:
  - If delay chain status passes over the threshold, the chain trigs an alarm
  - This alarm is sent to the Anti Tamper Unit (an IP that interprets and executes security policy)
  - Countermeasures are applied based on the security policy

POST-SILICON CALIBRATION 2/4: PVT CONDITION

- Propagation delay is strongly influenced by the environmental PVT conditions.

  … and noise is less of an issue



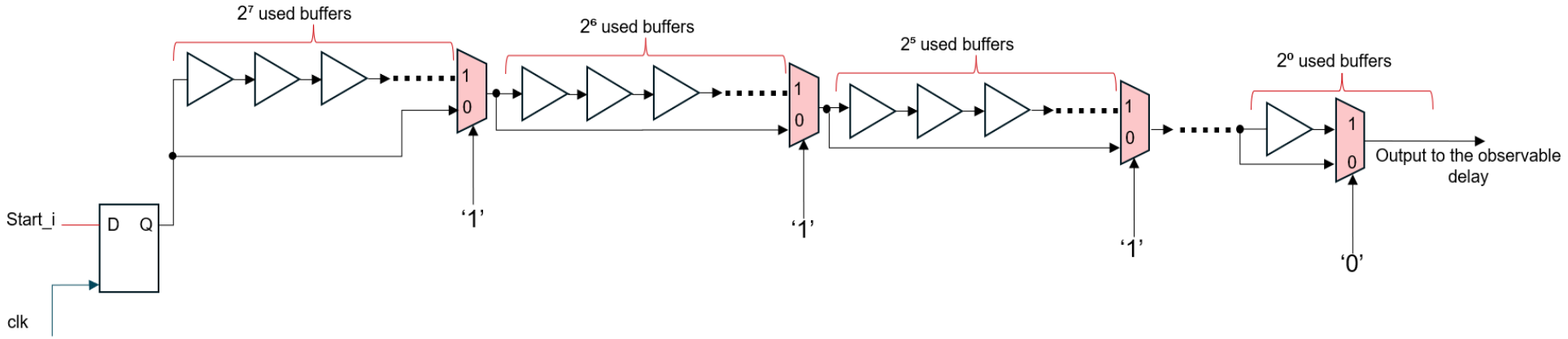


POST-SILICON CALIBRATION 3/4: DYNAMIC FREQUENCY SCALING

(NEW) objectives:

- Change of operational conditions (in the middle of project, in the middle of operations)
- Innacuracy of models/simulations/etc..
- Process design kit not fully characterized (updates requiring recalibration)

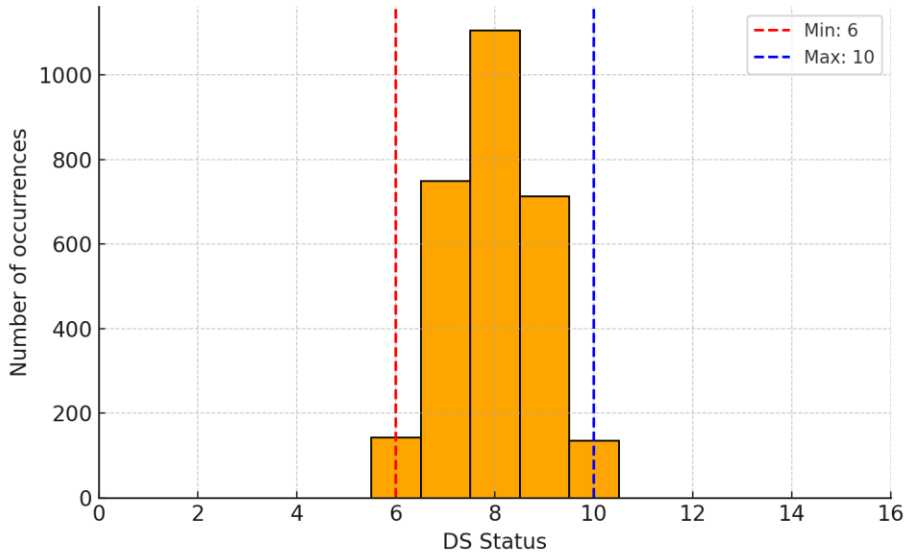
- New Initial delay chain with dynamic configuration.



- Goals:
  - Resize the initial delay chain
  - Precisely control where the signal stops
  - Correct any errors in simulations, noise, or processes

POST-SILICON CALIBRATION 4/4: DOUBLE THRESHOLD

- Objectives:
  - Calibrate based on a reference conditions, not based on worst (worst corner)
  - Adapt sensitivity of sensor, dynamically adapt the security policy.
- Delay chain status varies with PVT conditions
- We now set 2 thresholds:
  - First one under the minimal status value
  - Second one over the maximal status value
- This allows to detect any PVT variations which bypass the nominal functional interval



SECURE-IC
THE SECURITY SCIENCE COMPANY

3. OUTLOOKS & CONCLUSION

OBJECTIVES FOR DEPLOYMENT

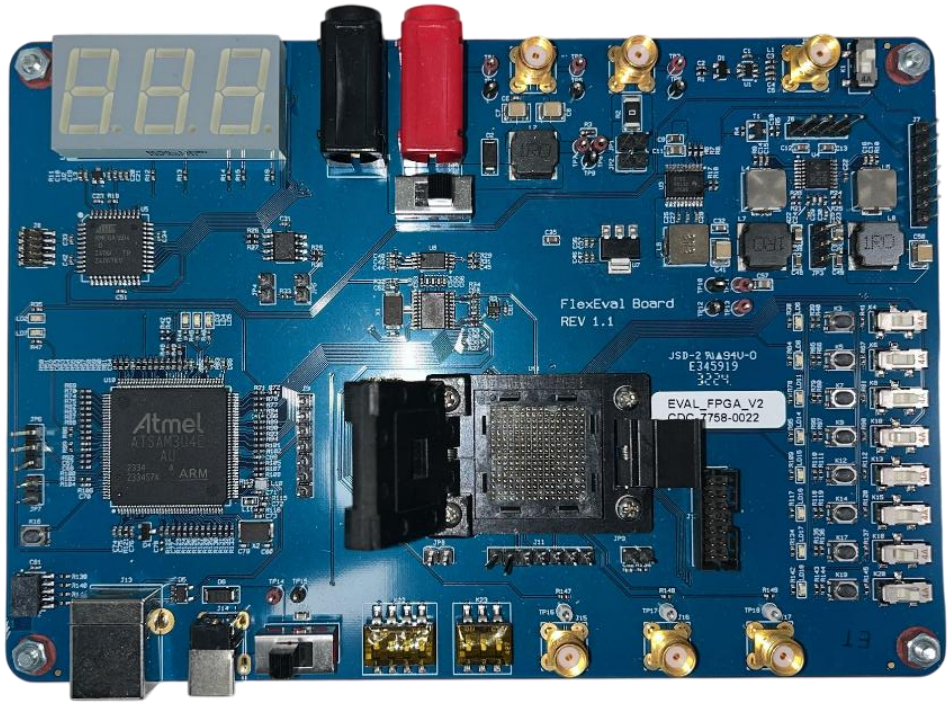
- Confusion matrix

	Attack	No Attack
Alarm	True Positive (TP)	False Positive (FP)
No Alarm	False Negative (FN)	True Negative (TN)

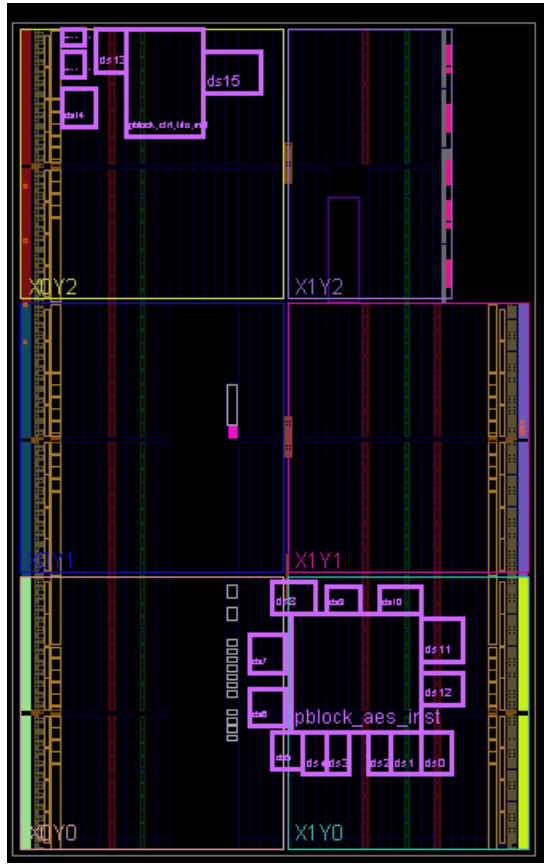
- Goals: Maximise TP and TN (depending on the policy)
- Compliancy to FIPS 140-3 level 4: maximal protection against “environmental attacks”

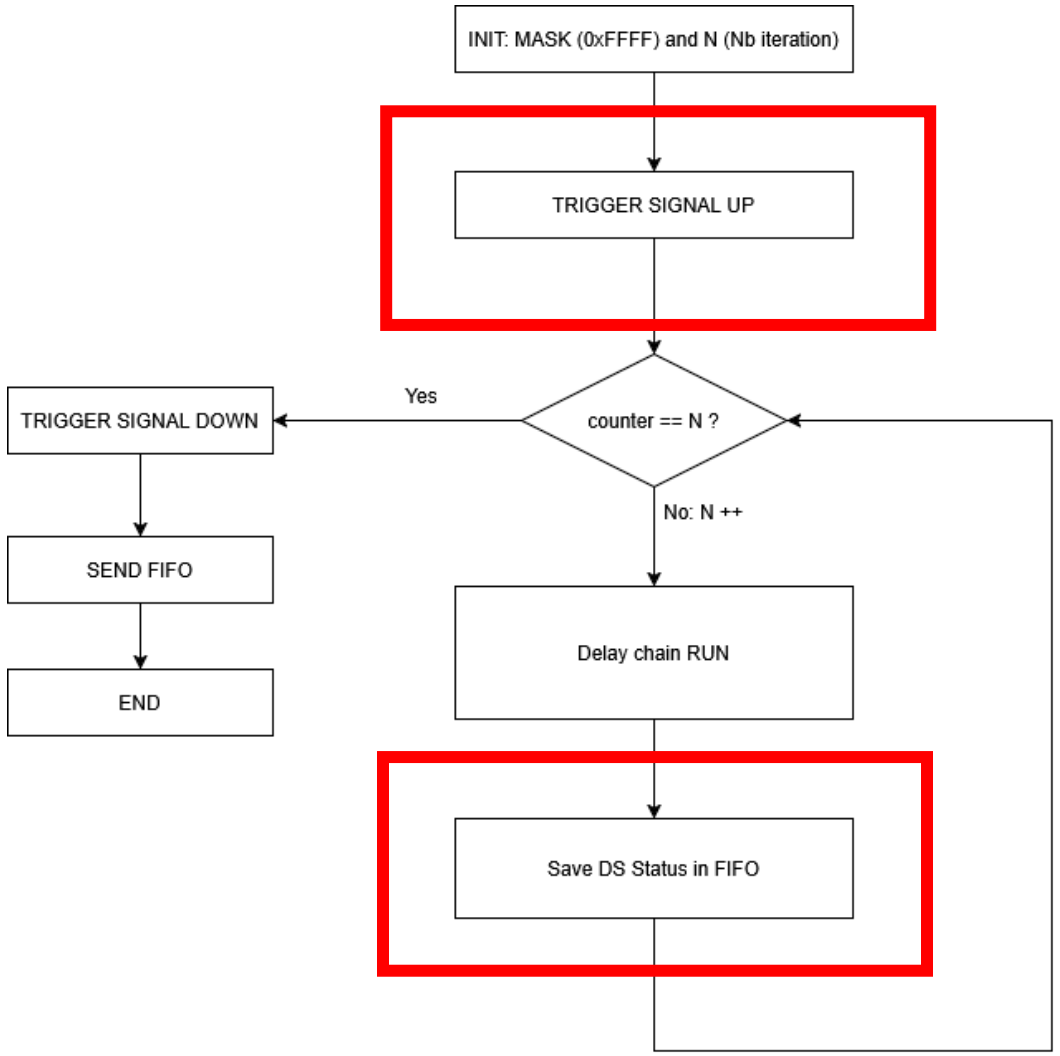
EVALUATION PLATFORM: FLEXEVAL™

- Based on NewAE CW305 (photo)
- AMD Xilinx Artix 7 series
- MCU Atmel SAM series
- Designed for fault injection, side channel and PVT experimentations.
  - Compatible with specific Peltier (thermoelectric) module
  - Monitoring of FPGA operating figures (T, V)



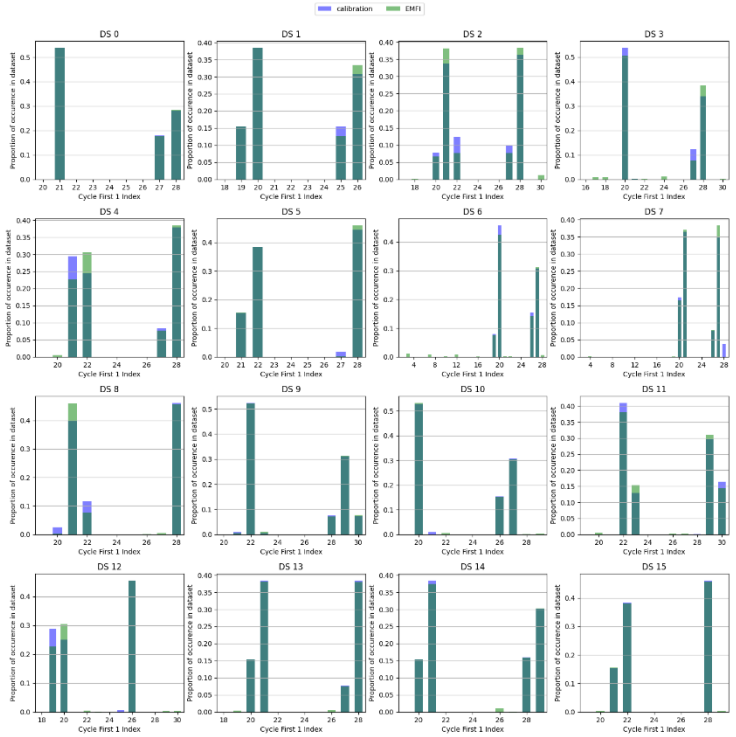
NEW FPGA PLATFORM PROPOSAL

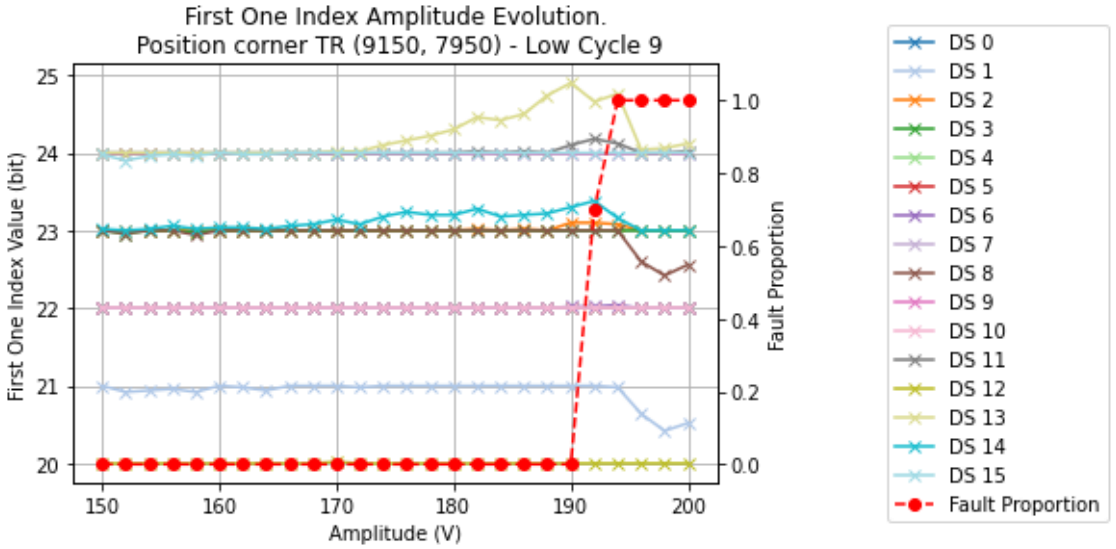




FIA EXPERIMENTATIONS

- Fault injections campaigns (power glitch, clock glitch and EM fault injections)
- Compare delay chain measurements obtained under varying PVT conditions with the measurements during fault injections





SECURE-IC
THE SECURITY SCIENCE COMPANY

THANK YOU FOR YOUR ATTENTION

CONTACTS

EMEA	sales-EMEA@secure-IC.com
APAC	sales-APAC@secure-IC.com
CHINA	sales-CHINA@secure-IC.com
JAPAN	sales-JAPAN@secure-IC.com
TAIWAN	sales-TAIWAN@secure-IC.com
AMERICAS	sales-US@secure-IC.com

FOLLOW US ON SOCIAL MEDIA