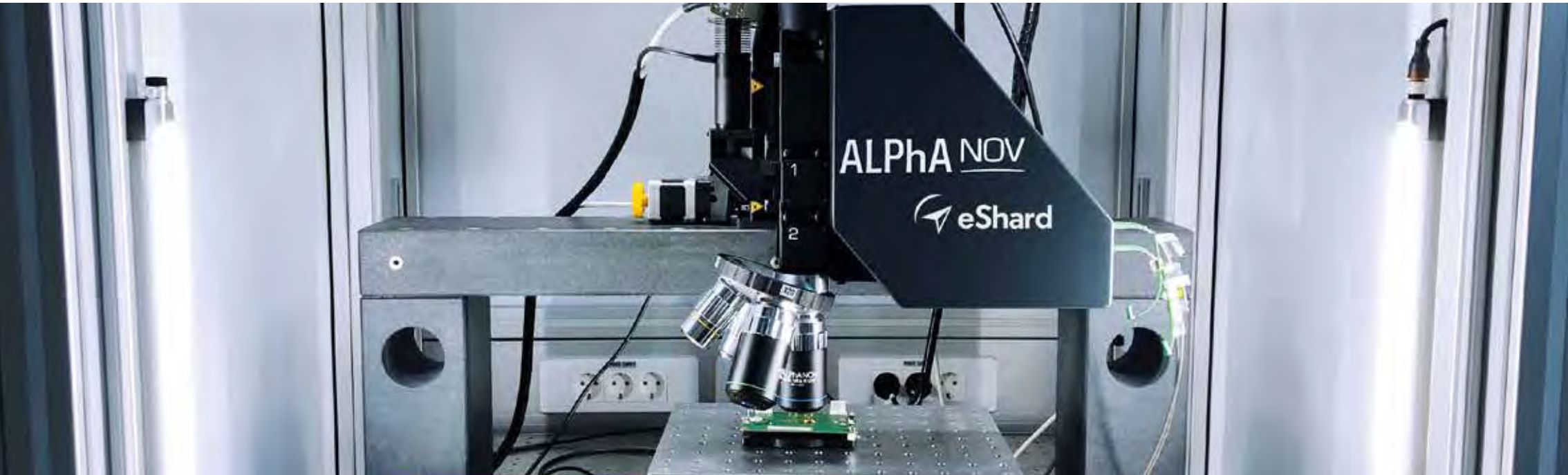
eShard x ALPhA NOV
Optics & Lasers Technology Center

Laser Fault Injection

A COMPLETE GUIDE OF ESHARD'S SOLUTIONS FOR LFI, IN PARTNERSHIP WITH ALPHANOV.



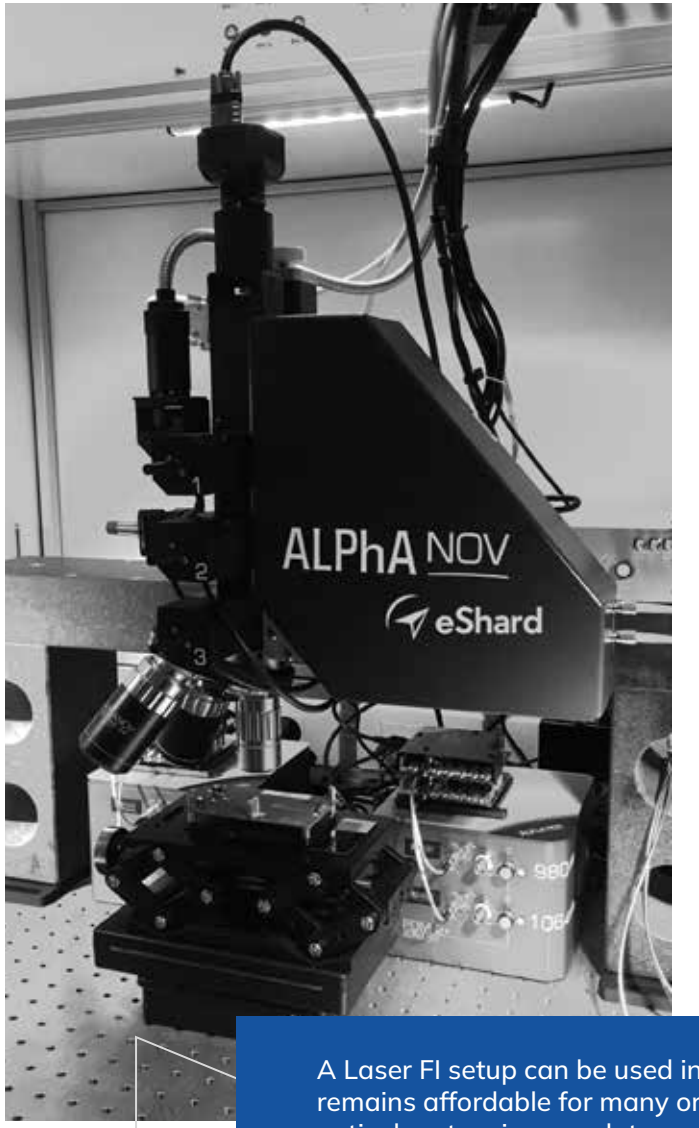
LFI

LASER FAULT INJECTION

An Integrated Circuit hosts and handles extremely valuable assets (cryptography private keys, secrets, sensitive code,...) used for payments, access control, data protection. These assets are physically materialized into the chip itself, with more or less obfuscation layers. With the right technique (methods, tools) and enough time, it may be possible to tamper with them.

The so-called fault injections aim at inducing a valuable logical fault by a physical disruption. It has been demonstrated that a laser pulse focused on a sensitive part of the die may induce such a logical fault. A non-protected device can be compromised by attackers applying Laser FI techniques with laboratory equipment. The laser is powerful and accurate. It is considered as the best way to assess whether chips withstand fault injection.

Mastering the Laser Fault Injection technique is necessary to evaluate the efficiency of counter-measures implemented on a chip against physical perturbations and manage the risks.



WORKFLOW

1. Sample preparation: decapping with chemical and/or mechanical means the package for a direct access to the die. Backside preparation is preferable when infrared lasers are used.

2. Fault campaign: injecting brief but intense laser pulses at different locations of the die with different characteristics (pulse duration, beam size, power level...) to cause local disruptions during the logic execution and build a fault map.

3. Exploitation: exploring the faults from the scan made at the fault campaign step; some parameters may generate exploitable logical faults. They can lead to vulnerability or secret exposure.

A Laser FI setup can be used in a laboratory only, but a basic setup remains affordable for many organizations. A low-end laser and optical system is enough to compromise a non protected chip. However for chips integrating counter-measures against FI, since the bar has been raised, a higher end setup has to be used to qualify the performance of built-in protections.

What makes a LFI *successful?*

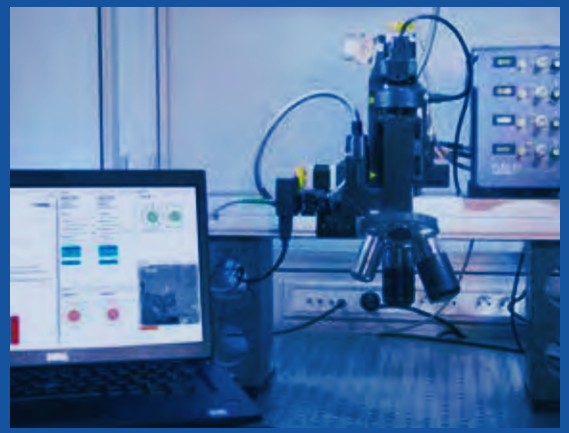
First it is important to have a neat sample preparation and a good laser and optical setup. Faulting from the backside of the chip is a lot easier as the laser avoids all the metal layers and has direct access to the active parts of the die. This requires an infrared laser source. Then everything lies in the ability to combine the different parameters leading to an exploitable fault: the size, intensity, duration, timing and location of the beam. All these variables can make a big difference. Advanced attacks can even combine up to four laser spots at different time and space for doing multiple injections on the same command.

In the identification phase, when the analyst does not know the possibility of a weakness, there is a need for complex fault campaigns combining many parameters with many laser characteristics. Looking for the right set of parameters may be challenging without efficient automation and proper synchronisation with the chip to capture its reaction to the laser injection.
The main objective is to avoid any blind spot in the test coverage.
Professional equipment shall do a comprehensive scan.

Key points for a successful LFI:

- A **high quality** optical and laser system, single or double fault injection;
- A good system for **back side imaging**;
- A side-channel capability to set the **timing**;
- Ability to control the **beam size**;
- A **software** able to reliably control all the hardware equipment;
- Ability to **pulse** when doing a backside imaging;
- Efficient and flexible **scanning** engine;
- Ability to **manage the data** in cartography.

eShard's solutions



Create or upgrade your lab with a turnkey LFI Solution
(page 5)

Challenge a solution in eShard's LFI Lab
(page 6)

Grow your LFI expertise
(page 7)

Create or upgrade your lab with a turnkey

LFI Solution

leveraging **ALPhANOV**'s optical and laser system*

- Optical and laser systems from a world class specialist: ALPhANOV;
- Evolutive setup for both hardware and software: single to double fault injection, and to photoemission;
- Ready to use experimental setup from back side imaging and laser pulsing to exploitation of logical faults.

Key differentiators:

FINE, POWERFUL AND PARAMETRABLE LASER SPOT

ALPhANOV leverages monomode laser source to design the most advanced laser and optical solution in this field.

IMAGING

Back side imaging reaches a strong quality. Simultaneous backside imaging is possible with laser pulbe.

SCALABLE

Ability to scale multiple lasers in space and time. Ability to scale the laser power by stacking up to 4 lasers (PDM+).

NANO OR PICO

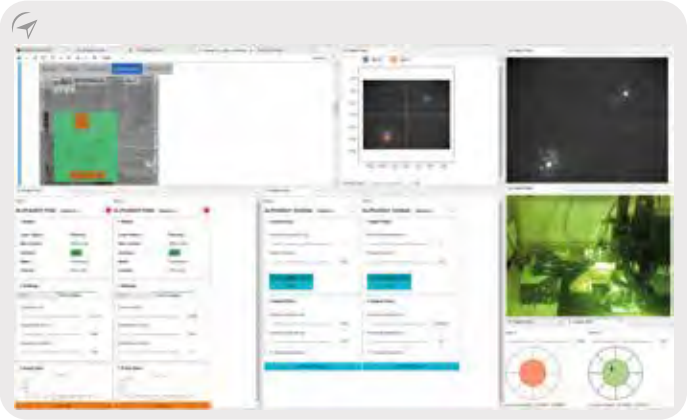
Opt for the latest 1064nm laser technologies with on-demand 60 picosecond pulses.

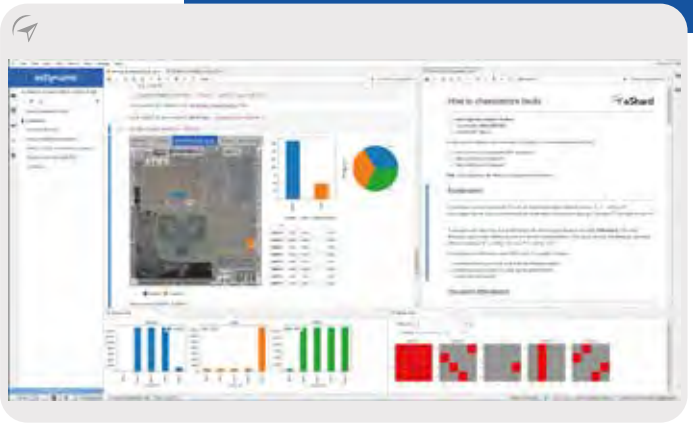
FLEXIBLE

Jupyterlab interface with analysis and attack workflow scripted in Python source code. Hardware equipment API is available.

COLLABORATIVE

Multi-users, remote hardware control, notebook co-edition, scanning features, heatmap creation.





Overview of the Software Environment

With such a solution, you can empower your experts in:

- ✓ Exploring the practicals of Laser FI technique;
- ✓ Evaluating an IC against Laser FI through a comprehensive scanning;
- ✓ Keeping track of results. Replaying analyses;
- ✓ Implement an end-to-end Laser FI use case for stressing a specific sensitive operation.

*Ask our experts for the fact sheet for more technical informations.

Audience: Semiconductor companies with IC security expertise, Secure products OEM and system vendors, Governmental agencies, Evaluation laboratories, Research centres in IC security.

CHALLENGE A SOLUTION IN
ESHARD & **ALPHANOV**'S

LFI Lab

Key differentiators:

LONG TRACK RECORD

Hands-on experience on different chip technologies: Secure elements, SoC, ASIC and FPGA.

TESTING LAB

High end and efficient testing lab based on eShard and ALPhANOV's Laser FI solution.

COLLABORATIVE

Continuous project scope review and adjustment. Resulting notebooks can be replayed in your lab premises for further analyses.

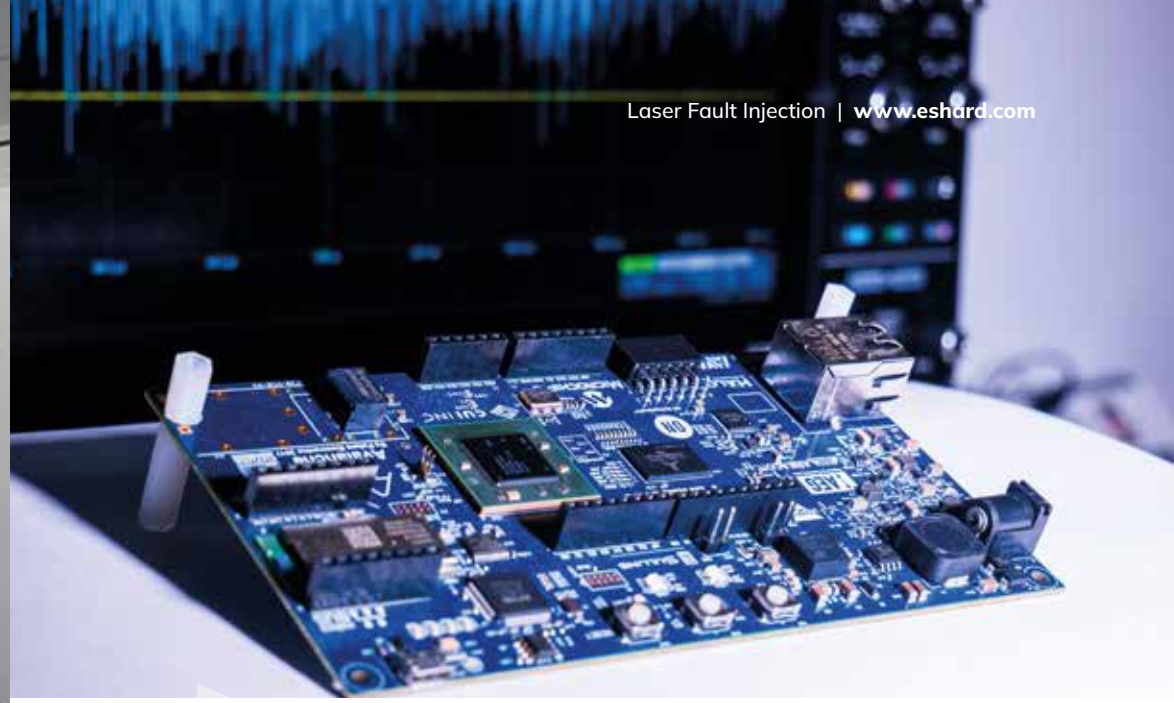
Audience: Any industry and governmental and academic institution that needs to outsource a hardware product evaluation with Laser FI for lack of expertise or resource reasons.

GROW YOUR

Expertise

WITH ESCOACHING

- Setup the laser bench and learn about safety procedures
- Characterize a chip susceptibility to laser pulse and launch a test campaign
- Implement a practical laser fault injection from back to back



AND WITH

STARTER KITS

Laser Fault Injection implemented on a complex and not outdated SoC: a hardware-based cryptography engine.

Know-how material implements the workflow: from the lab setup, the fault campaign to the secret key extraction.

Ideal as a training material, an internal benchmark or a showcase.

Audience: Hardware security analysts who want to learn practical knowledge about Laser FI or increase their competencies in this field.

Book a demo with our experts

We would like to know more about your business and projects in order to present you a more in-depth view of our solutions, tailored to your needs.

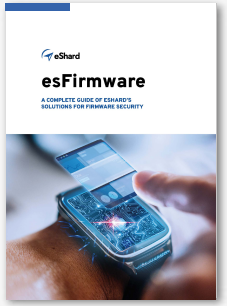
Click or scan to be redirected to the form.

Learn more about our other solutions for Integrated Circuits Security:

ELECTROMAGNETIC FAULT INJECTION

Assess the resistance of your hardware against fault attacks with our turnkey solution.

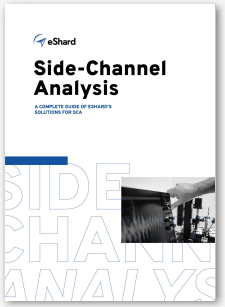
Learn more.



FIRMWARE SECURITY

Assess the security of firmware of IoT devices against logical and physical attacks.

Learn more.



SIDE-CHANNEL ANALYSIS

Our solution includes hardware, software, training for experts in cryptography and physical attacks on hardware products.

Learn more.

eShard

Get in touch

www.eshard.com

contact@eshard.com

/showcase/ic-eshard

@eshard

France HQ
Bâtiment GIENAH
11 avenue de Canteranne
33600 Pessac, France

France R&D
7 rue Gaston de Flotte
13012 Marseille, France

Germany
eShard GmbH
Beethovenallee 21
53173 Bonn