ERROL

Laser Optics Research & Production

Christian Hubert & Marie-George Côme, PhD

March 2017

ERROL
Laser Optics Research & Production

Our Team

Christian HUBERT

Sandra ESTEVES

Marie-George CÔME, PhD

Technological Monitoring

Production

Engineering

Expertise

Software

Assembly

Laser

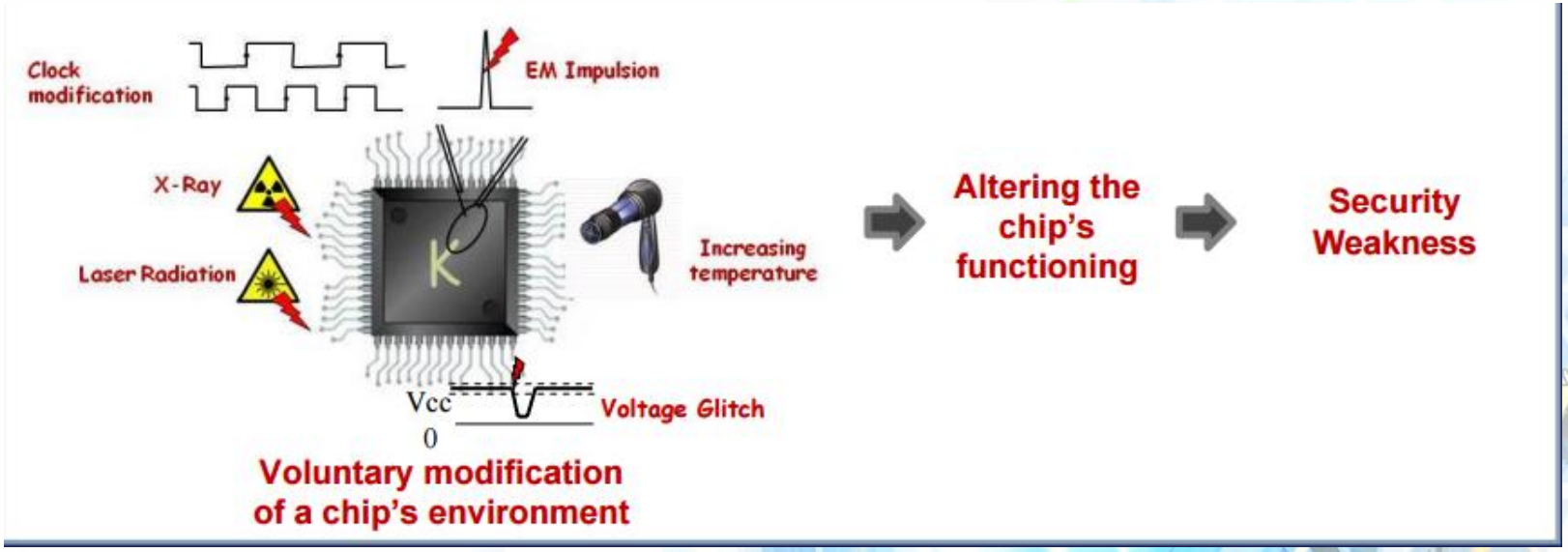
CAD Design

ERROL
Laser Optics Research & Production

InfraRed (IR) Laser Bench Solution For Security Evaluation In 2017

Smart card are design to protect both the confidentiality and the integrity of sensitive information

Attacks:



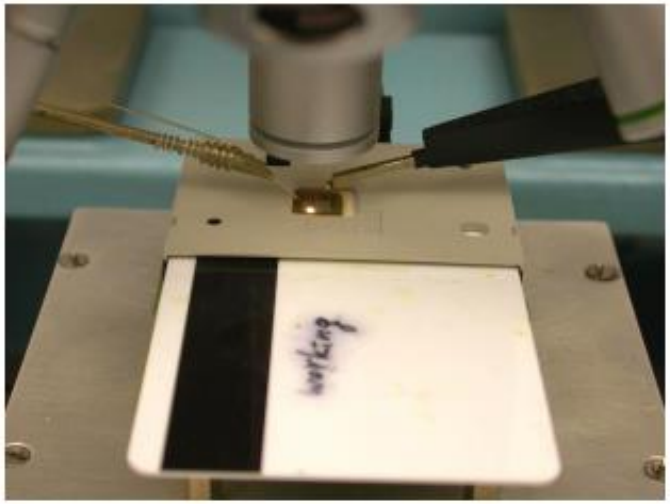
- Semiconductor transistor: more sensitive to ionizing radiation
- Middle sixties: it was found that coherent light causes some similar phenomena

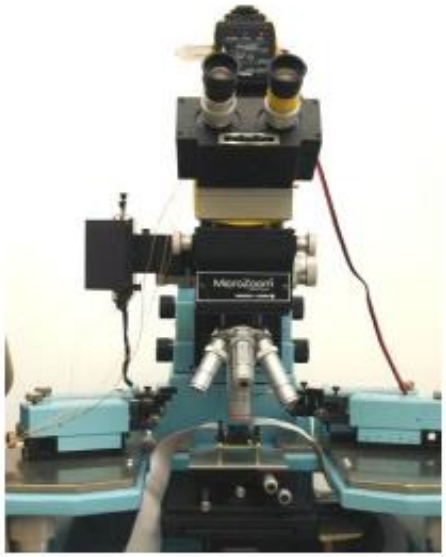
Laser = Light Amplification by Stimulated Emission of Radiation

Optical fault injection attacks

- By exposing a transistor to the focused light from a flash lamp or a laser beam it can be made to conduct

Early 2001





- Original setup involved optical microscope with a photoflash and Microchip PIC16F84 microcontroller programmed to monitor its SRAM (memory array)

Laser Fault Injection

- Laser fault injection consists in exposing the device to an intense light for a brief period to cause faults and errors in the operation of an integrated circuit

Number of reason why:

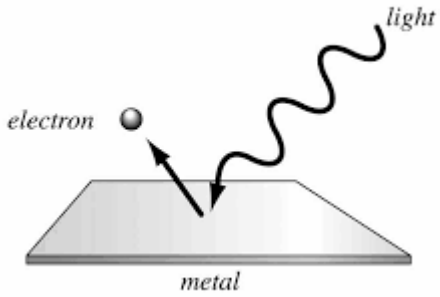
- Light emitted from laser beams = an advantageous technique of inducing faults in an integrated circuit.

Among other things, lasers are nowadays pretty cheap and easy to access compared with other material

Laser Fault Injection

a Near Infrared (NIR) laser beam is focused through the silicon substrate on the active region to induce a current caused by the photoelectric effect. Depending on the spot size and the feature size of the target, multiple or even single transistors can be targeted causing multiple or single bit errors on the device

Photoelectrical Effect



Potentially, any part of the silicon can be attacked provided the pulse location matches with processed operation

Laser Fault Injection

- Why this attack is so powerful :

- Geometric accuracy:
  - Possibility to focus the laser on a very specific part of the device up to 1~2um (in general ~40um square)
- Time accuracy:
  - Possibility to select precisely the moment where the pulse should be sent ~nanoseconds precision
- Generate temporary faults:
  - the device remains functional after the fault is sent, attack is reproducible

The effects of this method of fault injection can be isolated within a specified area and thus the manner in which faults are induced in the chip can be efficiently controlled

Laser Fault Injection

Choice of the wavelength

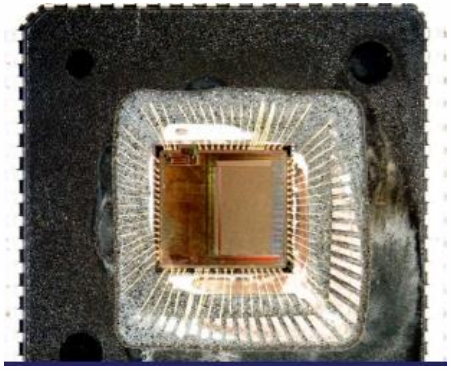
- A smartcard microcontroller is generally made of several layers

Depending on the laser wavelength both front and back side of the device can be perturbed:

- From 400nm to 1200nm silicon might be perturb by the laser pulses
- The penetration depth increase exponentially with the laser wavelength
    - Green light (~500nm) efficient on front side
    - IR (~1000nm) efficient on backside

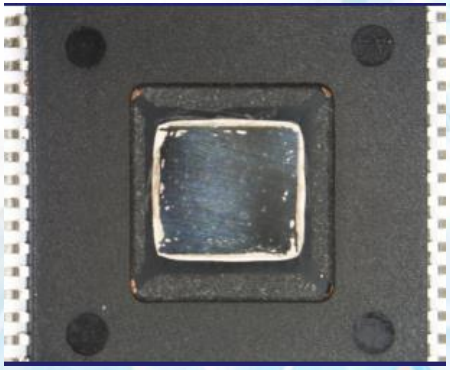
Laser Fault Injection

Front side or Backside attack ?



- Green wavelength (~ 532nm)
- Good visibility of the chip's layout
- Accurate targeting is difficult because of its multiple metal layers and potential shielding which reflect most of the light

- As technology progresses the number of metal interconnects on a chip grows while its size reduce ⇔ more difficult
- Any invasive attacks will require sophisticated and expensive equipment



- Infrared wavelength (~ 1064nm)
- Seems not to have much visibility of the layout
- Reflective problem of metallic surfaces can be resolved

- Low-cost approach used without any special treatment

Laser Fault Injection

- Typical laser source : pulsed nanosecond laser with selectable wavelength
- Focused with optical microscope or single lens
- The target device is mounted on an automated table
- The whole surface of the device can be scanned while pulses are sent on top of the devices

Combined with backside infrared imaging:

- microscopes with IR optics ⇔ better image quality
- scientific camera must be used with better IR QE
- resolution is limited to ~0.6µm by the wavelength of IR laser
- view is not obstructed y multiple metal layers
- Locating Flash and active areas is easy via laser scanning

Defence technologies: Tamper protection

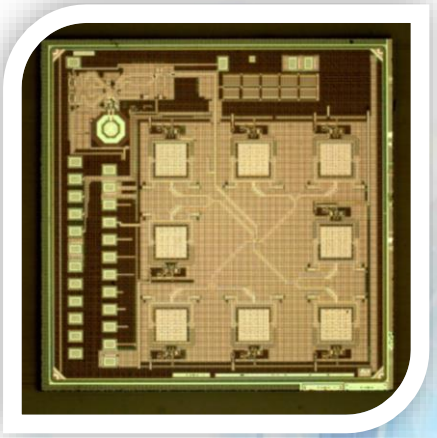
Powerful attacks have forced chip manufacturers to rethink their design and bring better protection ⇔ Complexity of the design on the modern chip

➢ Chip fabrication technology

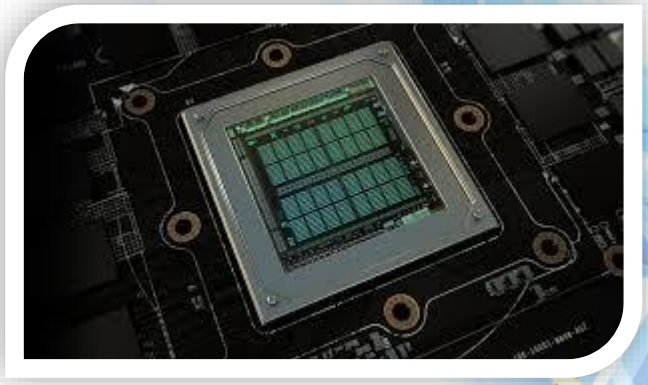
- planarisation as a part of modern chip fabrication process ⇔ 0.5 μm or smaller feature size
- glue logic design makes reverse engineering much harder
- multiple metal layers block any direct access
- small size of transistors makes attacks less feasible
- chips operate at higher frequency and consume less power

Semiconductor device fabrication

10 µm – 1971
6 µm – 1974
3 µm – 1977
1.5 µm – 1982
1 µm – 1985
800 nm – 1989
600 nm – 1994
350 nm – 1995
250 nm – 1997
180 nm – 1999
130 nm – 2001
90 nm – 2004
65 nm – 2006
45 nm – 2008
32 nm – 2010
22 nm – 2012
14 nm – 2014
10 nm – 2017
7 nm – *~2018*
5 nm – *~2020*



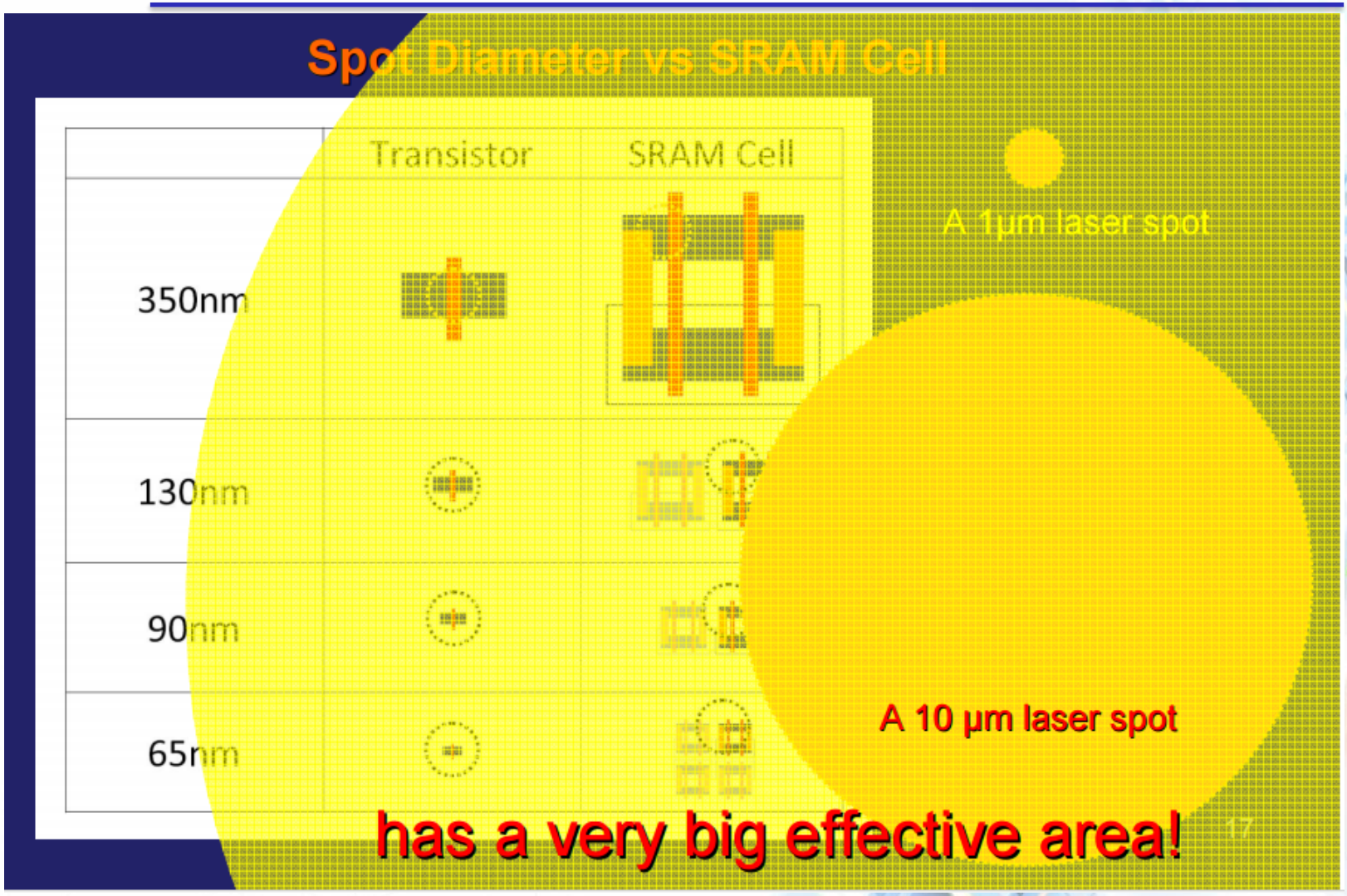
2001
131 nm devices



2017
10 nm devices
Highest level
of design

⇔ New challenges

Laser Fault Injection



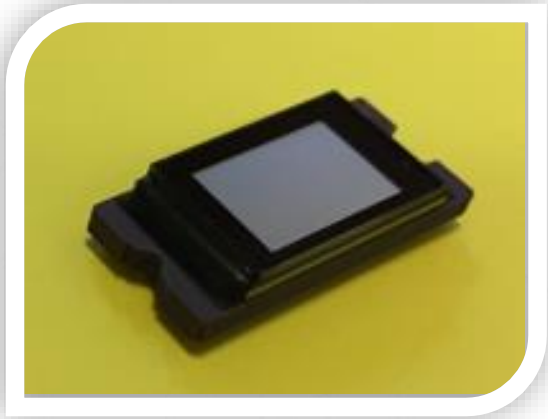
How to make a multi-points laser fault injection

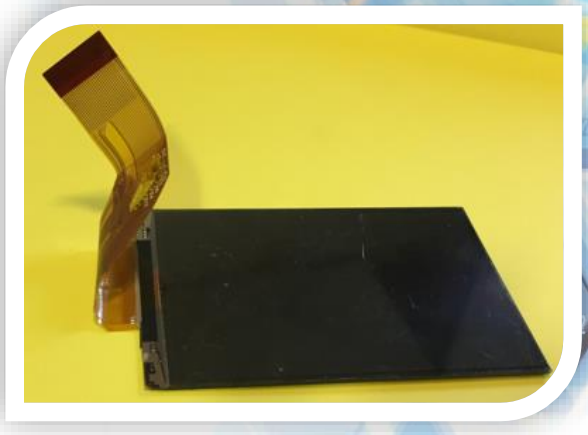
ERROL
Laser Optics Research & Production

GALVO SCANNER

AOD SCANNER

DLP SCANNER





SLM SCANNER

AOD SCANNER	DLP SCANNER	SLM SCANNER	GALVO SCANNER
Field and Compensation			
350 x 500 µm 25x	1000 x 1500 µm 25x	1000 x 1500 µm 25x	3000 x 3000 µm 25x
Imaging scanning capability			
10 kHz 100 kHz/line 50 µs Multi-points	Video Raster 50 kHz/line 500 µs Multi-points	120 Hz 120 Hz refreshment Simultaneous Multi-points	2kHz/line x axis 2kHz/line y axis 250µs Multi-points
Multi spots same time			
Not possible	Not possible	**Possible**	Not possible
Solutions			
Expensive Ex: chip 30 k€	Low cost Ex: chip 3k€	Expensive Ex: chip 35k€	Low Cost Ex: chip 2k€
Single λ laser	Low power laser	High Power Laser	Multi scanners Max 6 lasers High power lasers

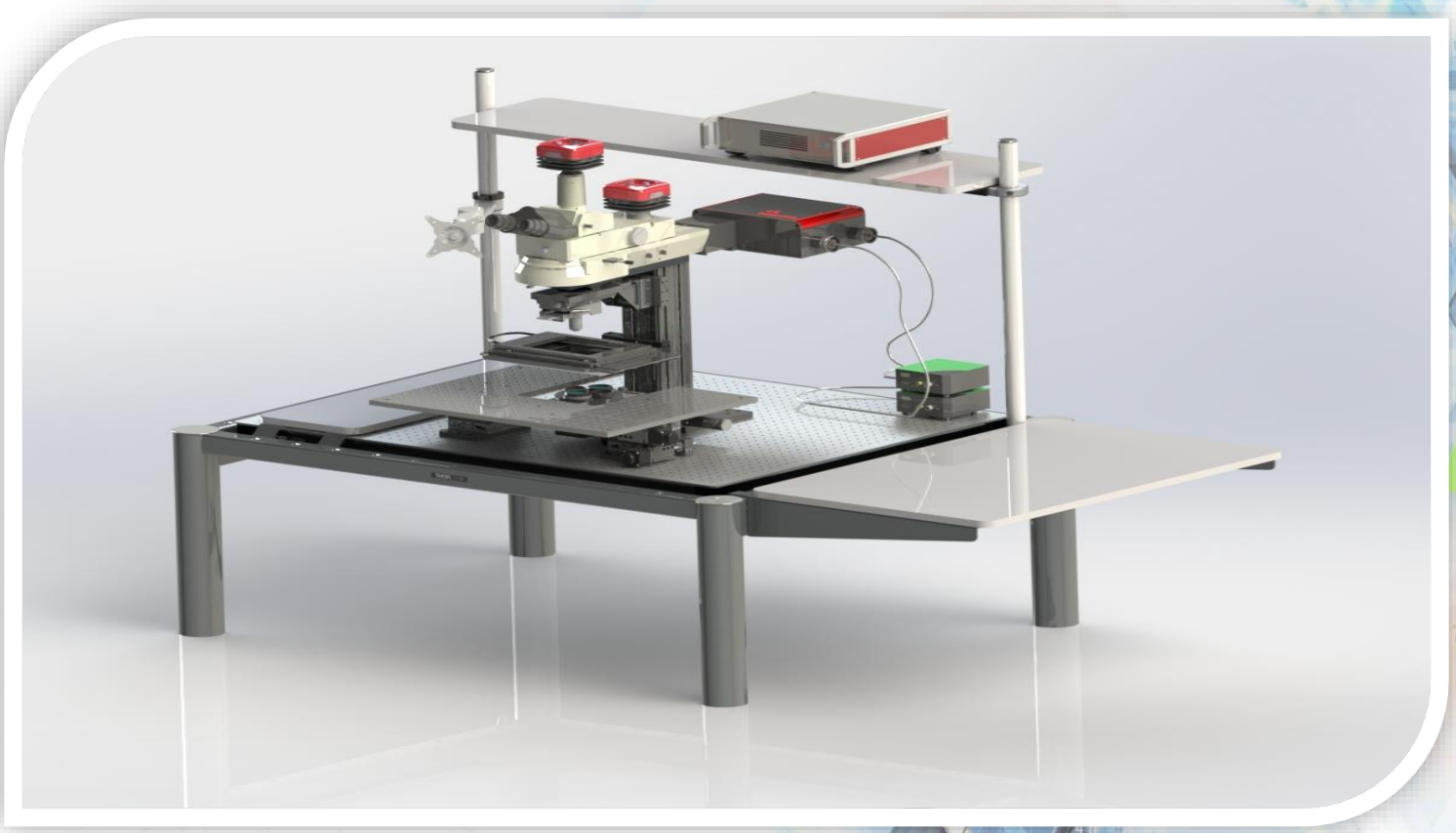
ERROL
Laser Optics Research & Production

Smart Card InfraRed (IR) Laser Bench solution

Protecting chips against laser fault attacks is one of the main security challenges in the smart card industry.
With our solution, a user can perform advanced laser fault attacks that meet the highest international standards to assess if a smart card is secured against laser attacks.

Our solution

Station Smart Card_2017



Our solution / Set Up

- 1 IR camera
- Cross mark on the main camera
  - numerical target
- Motorized stage XYZ
  - XY axis resolution 40 nm
  - Z < 10 nm

Our solution / Laser source

- Laser Pulse Width Range: 1ns to CW
- Wavelength: 1064nm and 975nm

- Power: 1W per diode source
  if multiple diode sources ⇔ 2W

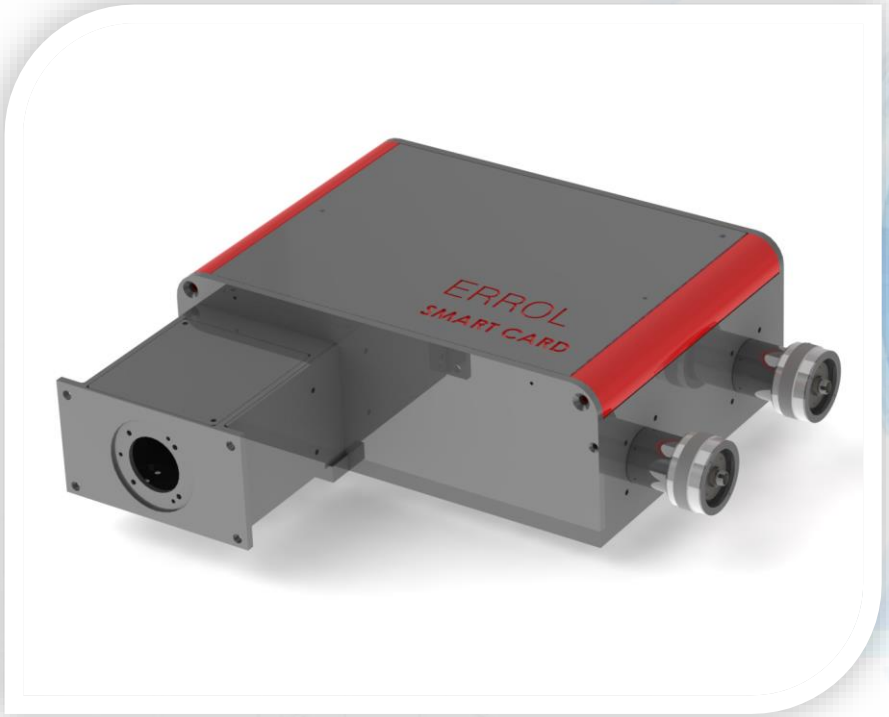
Optical requirements:

- Wavelength range: 700 nm to 1300 nm

- Beam diameter:
  - 0.595 µm per beam @ 975 nm
  - Possibility to increase the beam > 1 µm with electrical lens without changing the visual focus
  - Instant and global power feedback
  - With data recording
  - Low noise high speed with minimal transient when the laser source is changed
  - Probing point

Multi-points laser injection by multiscanners head

- 3 coaxial simultaneous beams (see figure 1)
- Power variation per pulse position totally independent



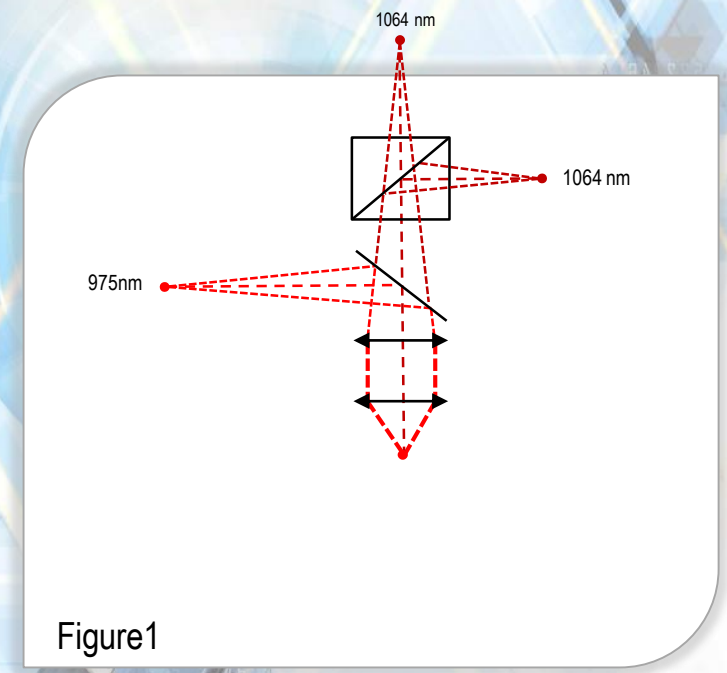
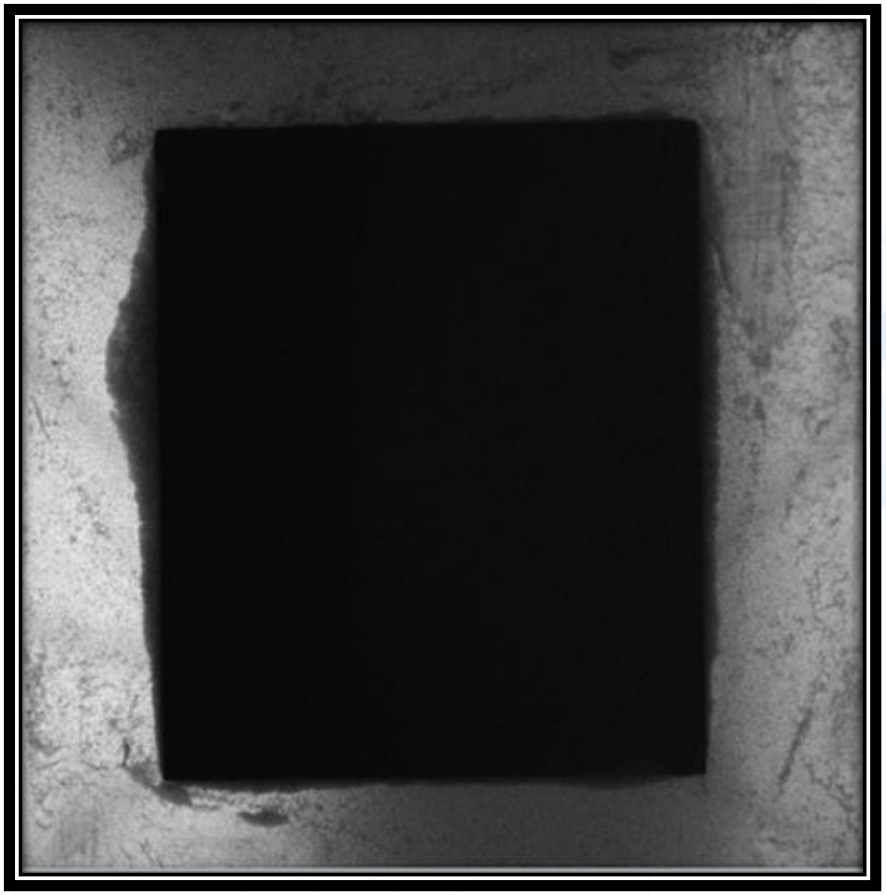
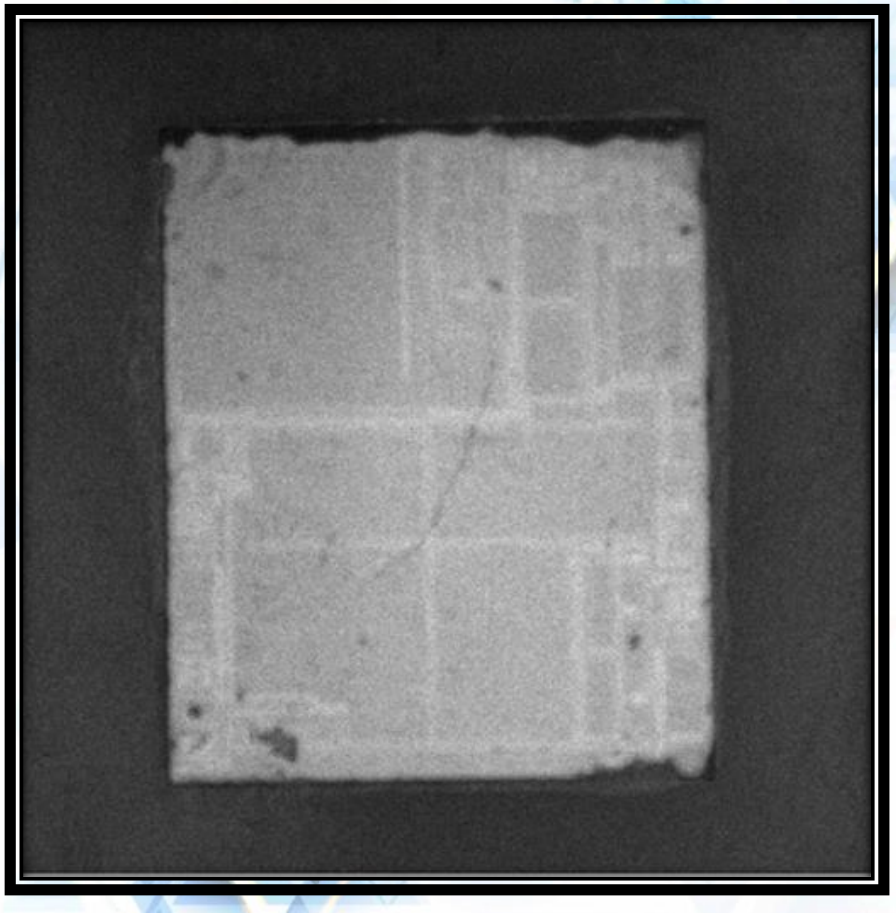


Figure1

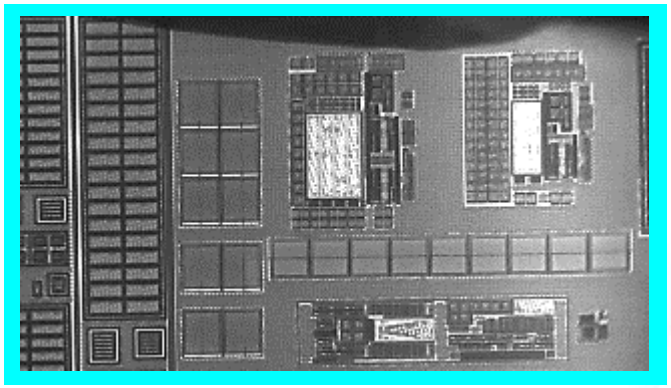
Our solution / Backside infrared imaging

Currently found on workstations:



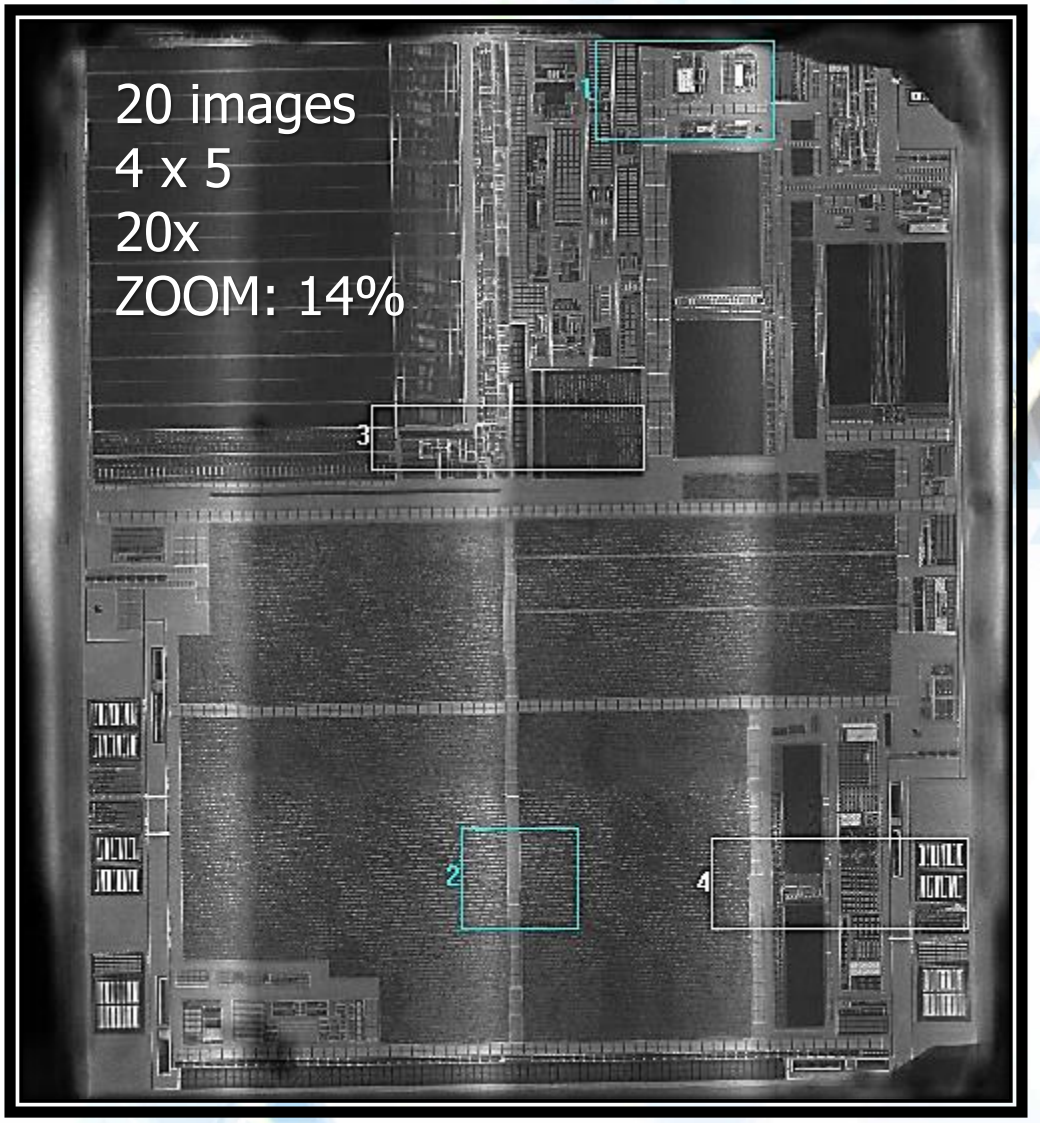


Our solution / One step ahead

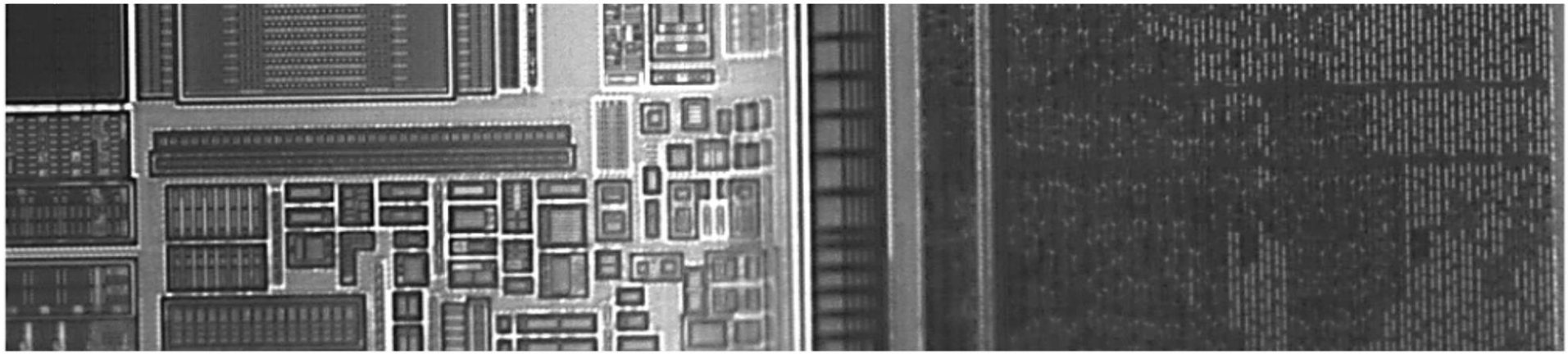


ROI 1 - ZOOM: 50%

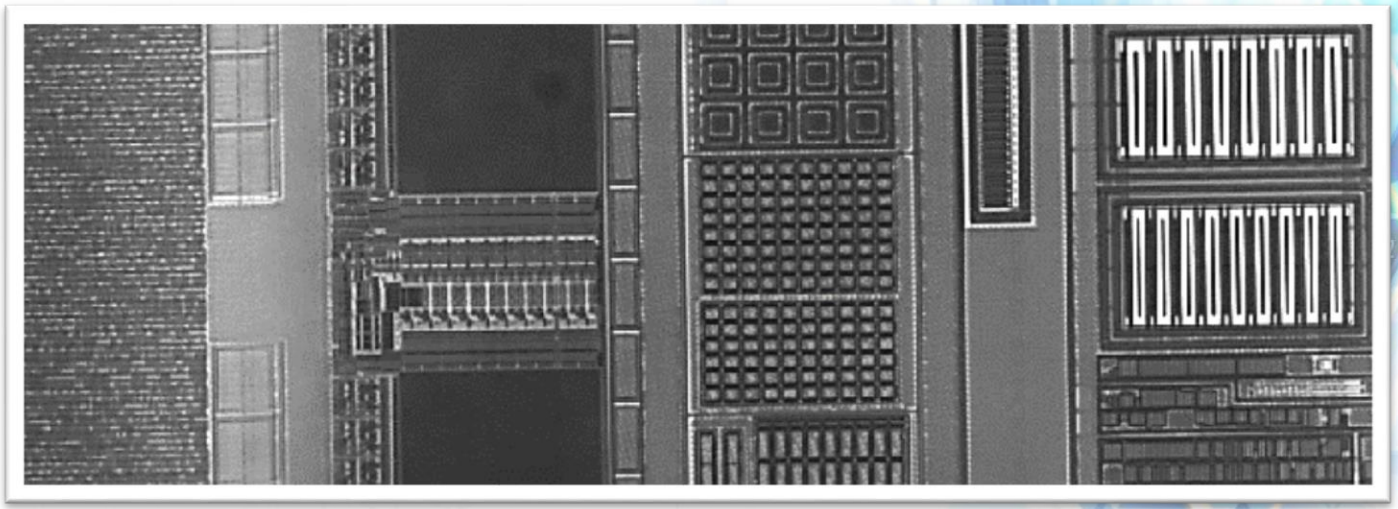
ROI 2 - ZOOM: 75%



Our solution / One step ahead – 2 ROIs

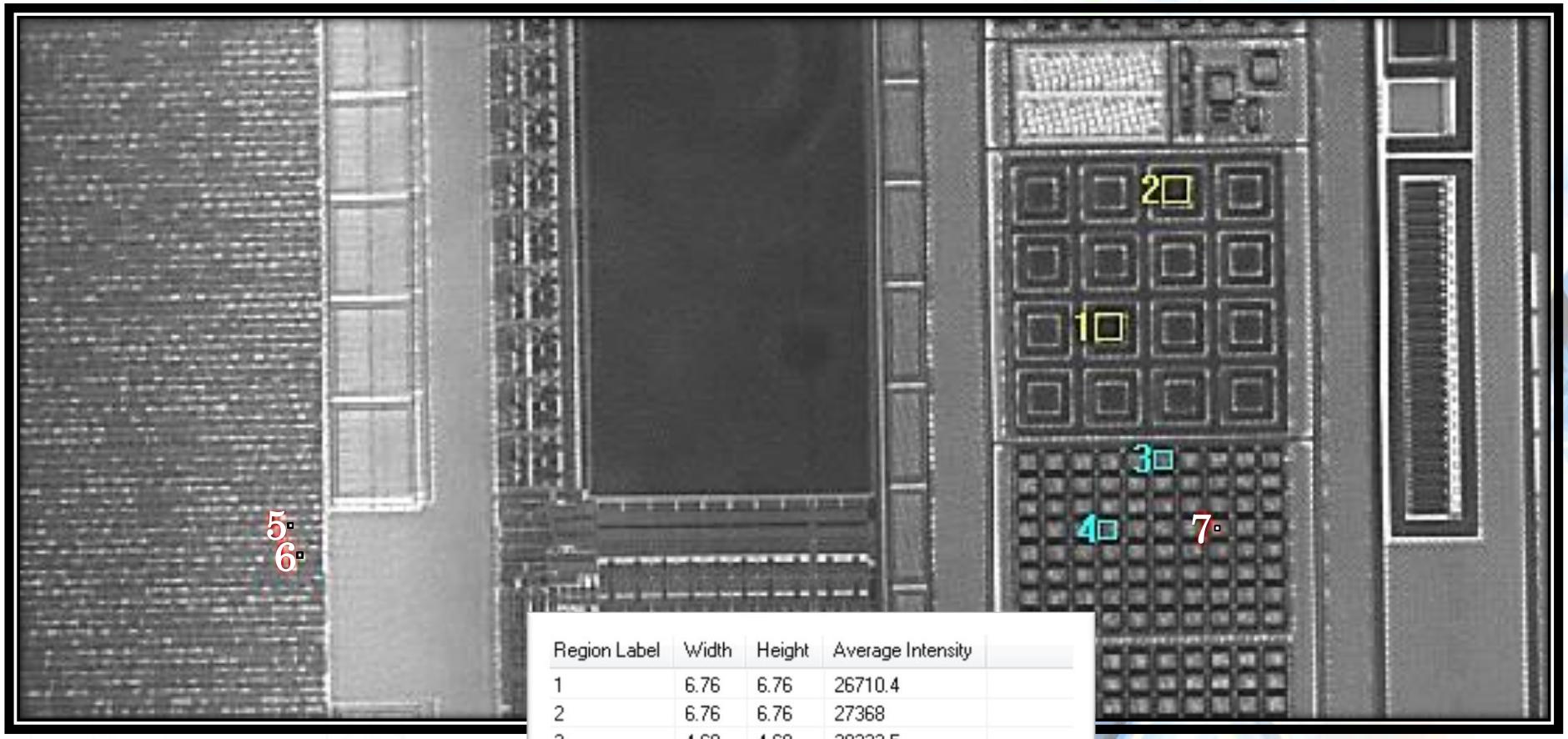


ROI 3 - ZOOM: 100%



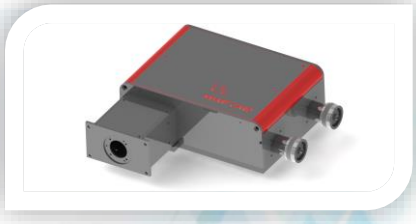
ROI 4 - ZOOM: 75%

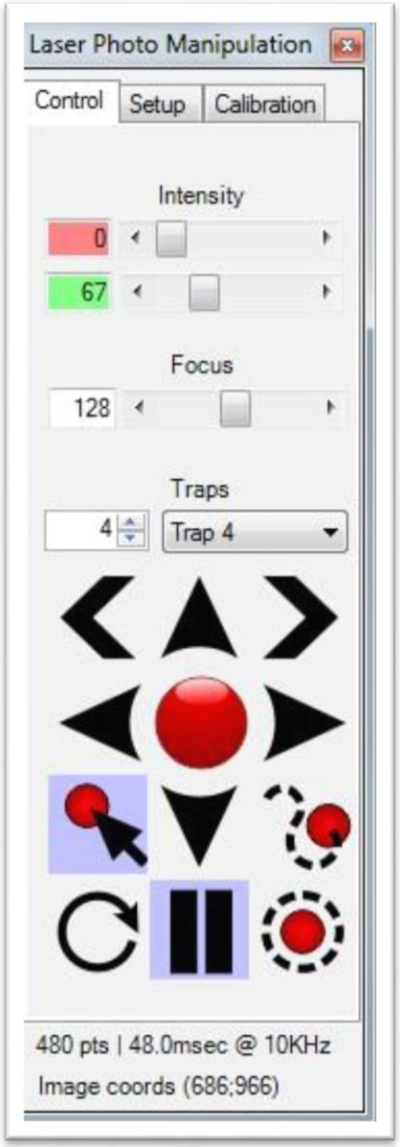
Our solution / See more

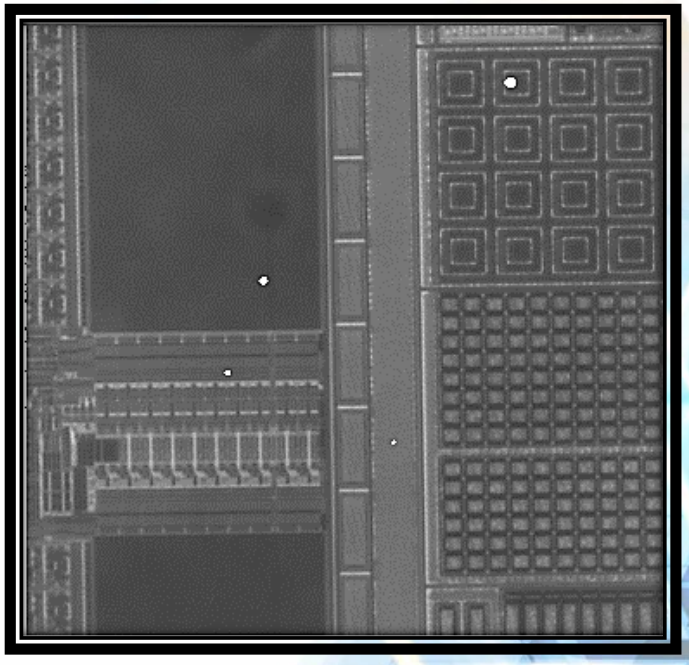


Region Label	Width	Height	Average Intensity
1	6.76	6.76	26710.4
2	6.76	6.76	27368
3	4.68	4.68	29222.5
4	4.68	4.68	29350.8
5	1.04	1.04	33983
6	1.04	1.04	37564.3
7	1.04	1.04	32939

Multi-points laser injection

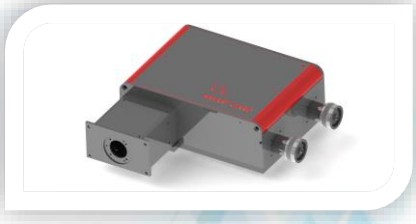






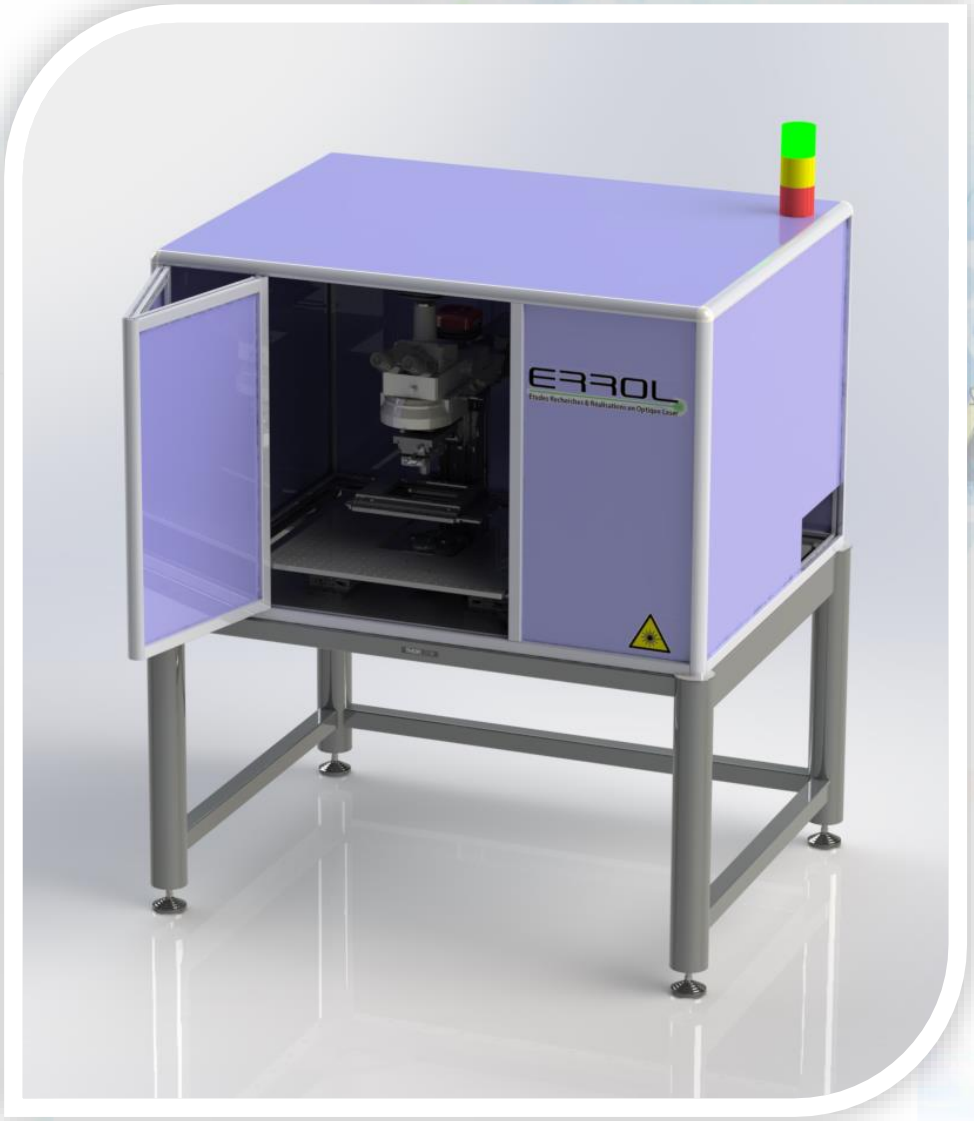
4 independant laser points

Multi-points laser injection



- Up to 3 simultaneous Targeted Laser Actions
- Superimpose all laser optical paths (no commutation delays and positioning issue)
- the ability to manage and modify the position and focalization of several laser light in real time (up to 3 lasers)
- Independent lasers control (intensities, focus, paths)
- ROIs visualization
- Ability to combine the fastest full field of view laser action with the fastest acquisition routines
- Eanable to cope with any demanding acquisition protocoles
- Easy to use interface to manage the lasers, set-up ROIs and plan the experiment

Our solution / Backside infrared imaging



- Instant and global temperature feedbacks
- with data recording

Key Features

- Supports back-side attacks
- Heavy stable base for high magnifications

- Ultra precise XYZ stage
- Fast Automated Z-axis
- Spot sizes down to 595 nm
- Fast multi-time glitching
- Accurate digital scaling
- Multi-spots
- Real time IR navigation
- Automatic scanning of a chip's surface with integrated motorized XYZ
- Camera inspection of laser spot and location on chip area
- High repetition accuracy on motorized axes
- IEC60825-14 approved safety enclosure
- Support Training adapted to your needs of Today and Tomorrow

Benefits

- Reliable and Accurate quantitative data
  - No compromise in quality
  - Wide range of high performance objectives
  - Best possible Image Quality
  - Accuracy
  - Reproducibility
- Better efficiency, Time saving
- Safety of Investment
  - Open solution
  - Most performant technology available Today / Ready for Tomorrow
  - Compatibiliy with multiple accessories
  - Upgradability

Christian Hubert
Technical Director
ERROL
Laser Optics Research & Production

64 Rue Bourdignon
94100 Saint-Maur Des Fossés

Mobile: 00 33 6 63 66 88 91

E-mail: Errol.laser@gmail.com

Accuracy

Marie-George Côme, PhD
Application Specialist
High-end solution integration expert / Consultant

IMAGXCELL
SAVE TIME FOR SCIENCE

Mobile : 33 7 68 04 75 06
E-mail: Marie-George.Come@Imagxcell.com