Riscure Workshop

LLFI: Lateral Laser Fault Injection Attack

FDTC 2019 - Atlanta

Joaquin Rodriguez, Alex Baldomero, Victor Montilla, and **Jordi Mujal**

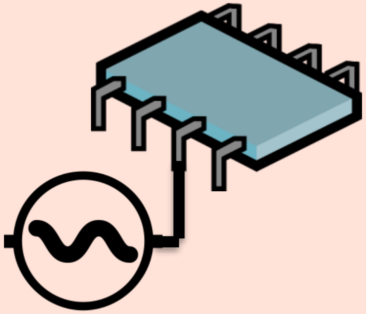
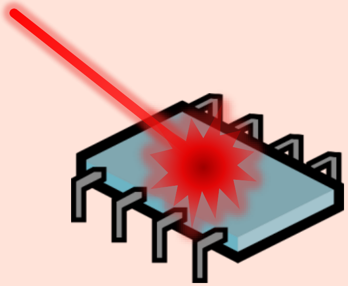
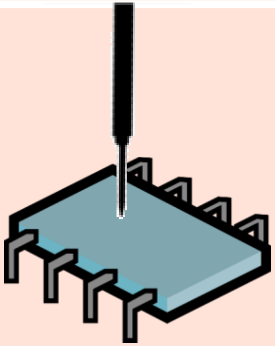
IT Labs
Applus+ Laboratories Barcelona

Agenda

1. Review current packaging techniques and challenges regarding FI
2. Present a new FI technique which is relevant for this topic.

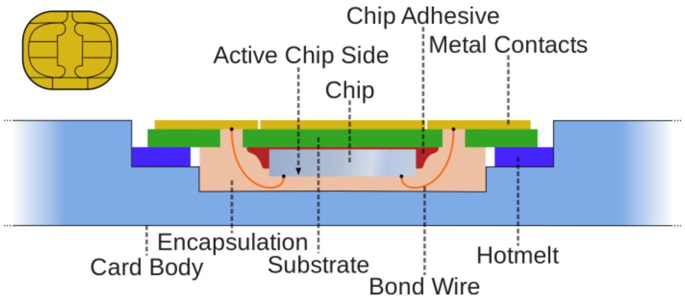
✓

FI Techniques and Sample Access

Power/CLK Glitch FI (PGFI)	Light FI (LFI)	Electromagnetic (EMFI)	Body Biased FI (BBFI)
			
Sample Access: Only Pin acces required	**Sample Access**: Backside – Frontside depackaging required	**Sample Access**: Frontside-Backside (partial?) depackaging required	**Sample Access**: Backside depackaging required

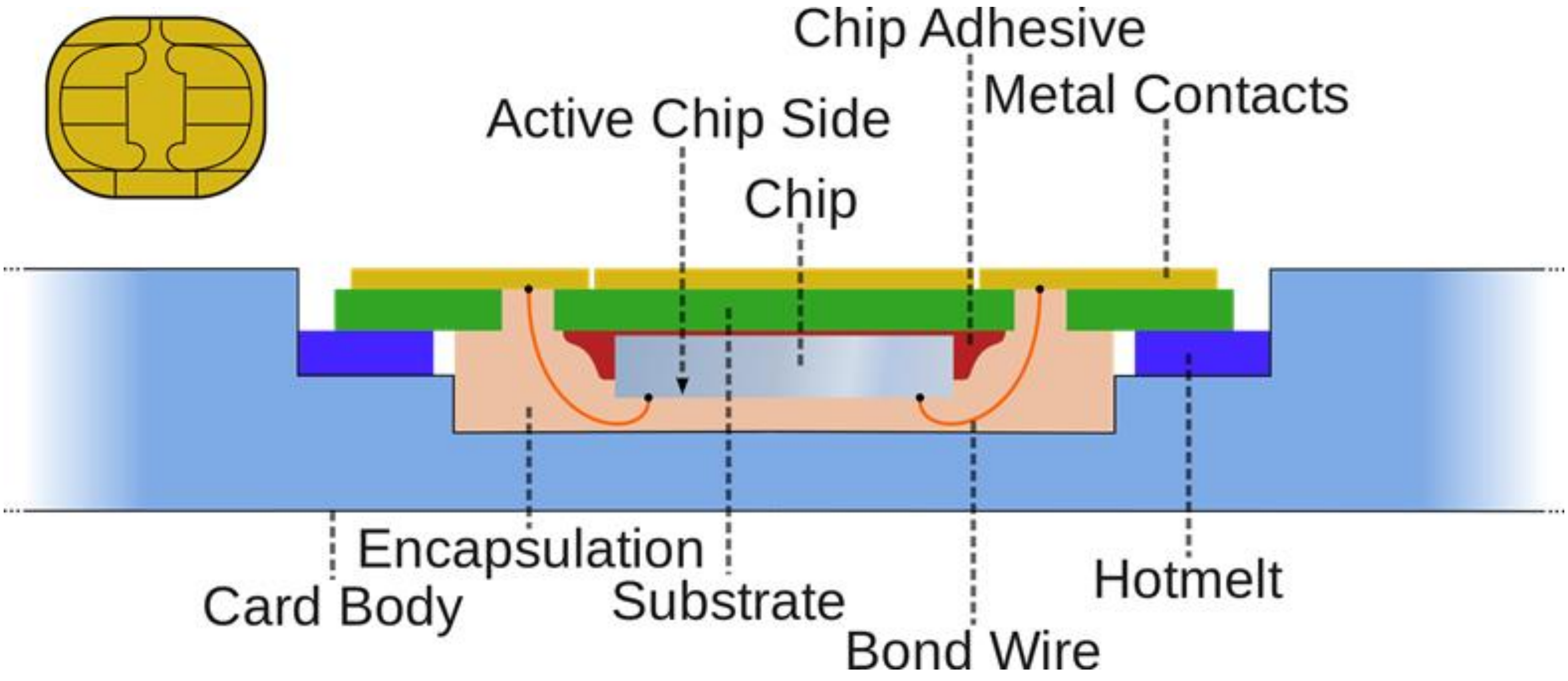
New Form Factors for Secure Elements

New Markets like IoT, Automotive or Mobile are moving the traditional packages where we can find a SE:



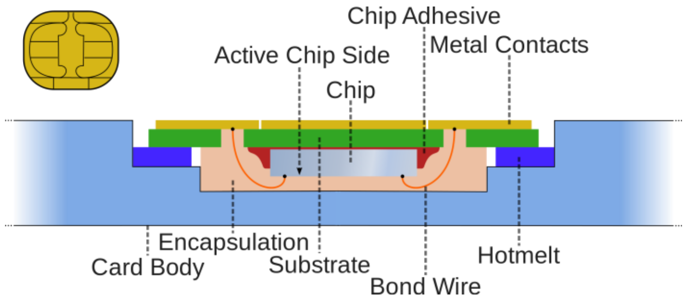
New Form Factors for Secure Elements

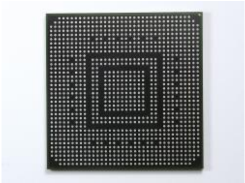
New Markets like IoT, Automotive or Mobile are moving the traditional packages where we can find a SE:



New Form Factors for Secure Elements

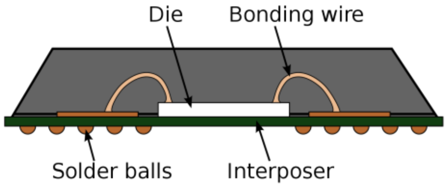
New Markets like IoT, Automotive or Mobile are moving the traditional packages where we can find a SE:

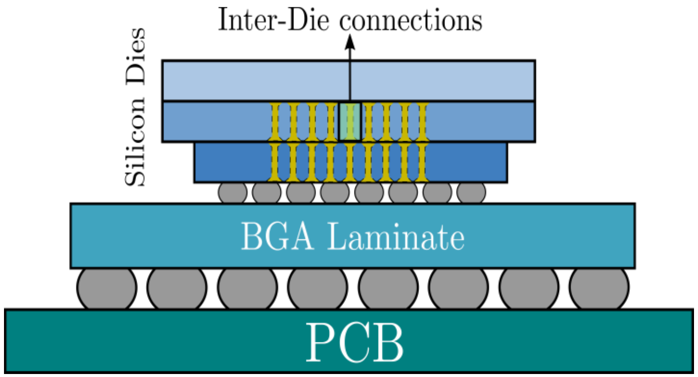




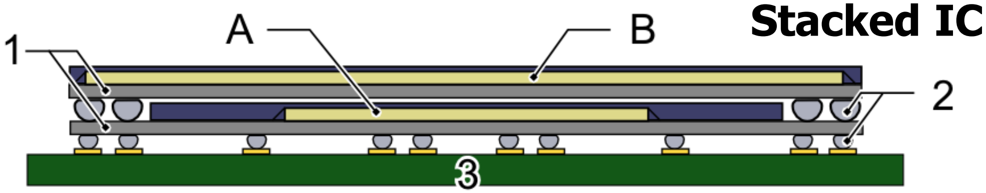
BGA Standard – still Easy?

BGA package sideview





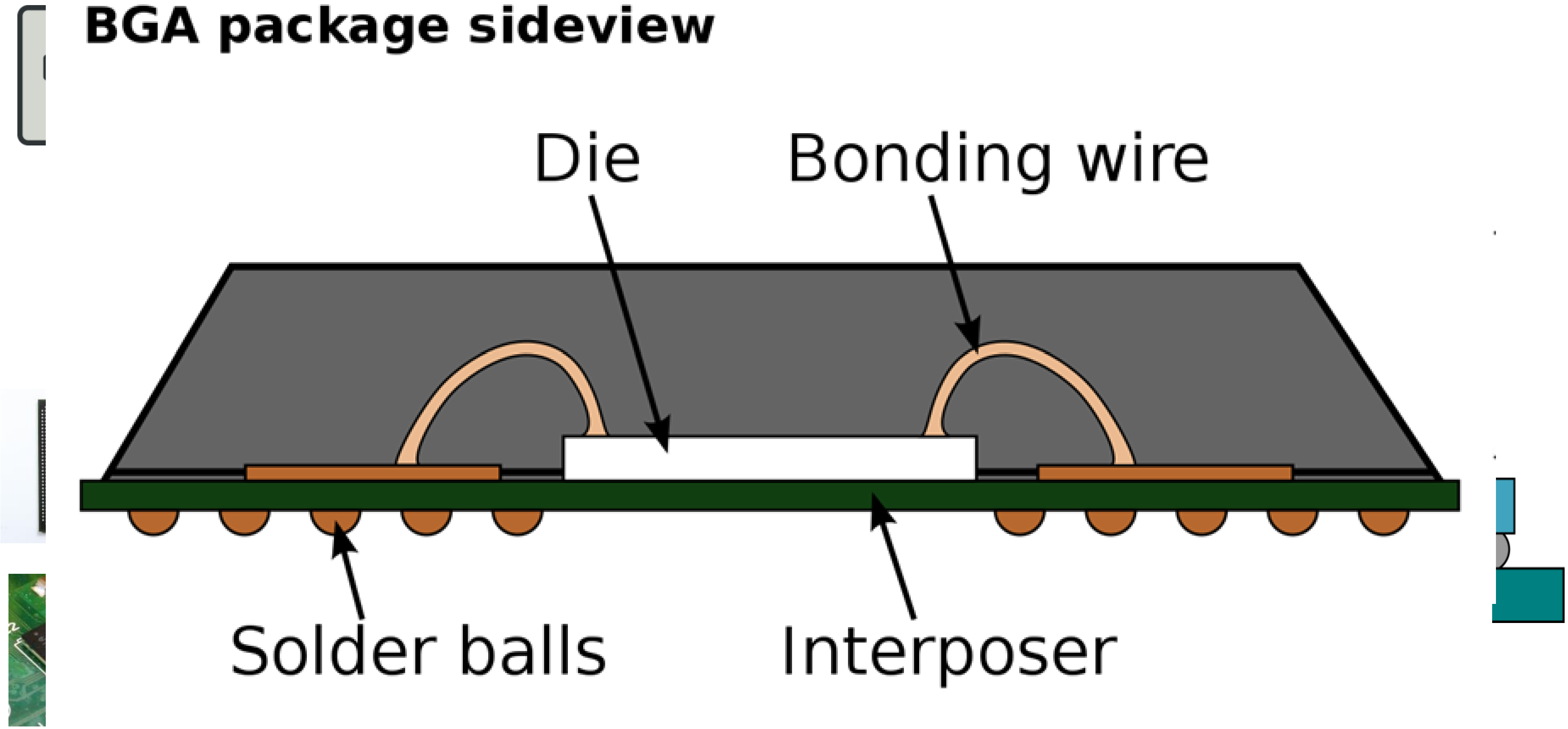
Stacked IC – Difficult?

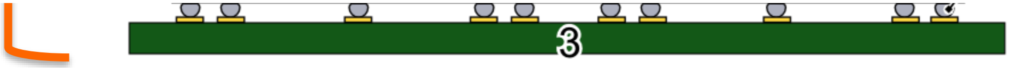


Stacked Packages (POP) –Medium?

New Form Factors for Secure Elements

New Markets like IoT, Automotive or Mobile are moving the traditional packages where we can find a SE:

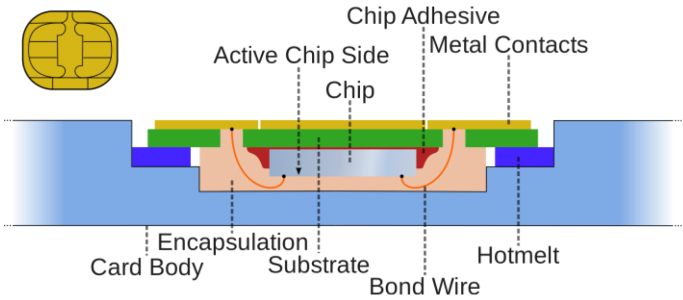


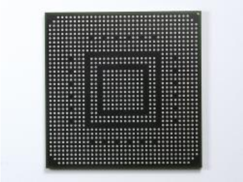


Stacked Packages (POP) –Medium?

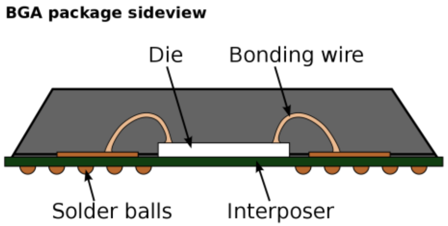
New Form Factors for Secure Elements

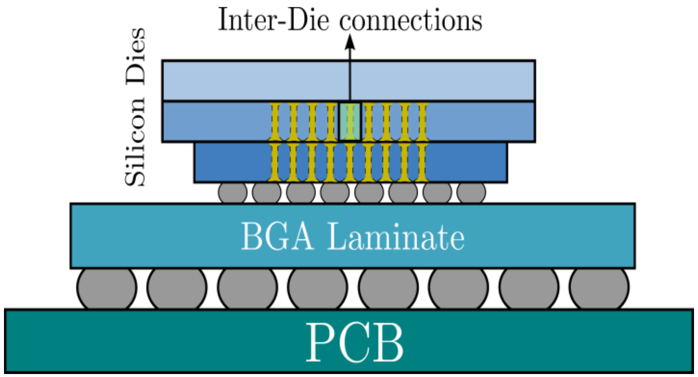
New Markets like IoT, Automotive or Mobile are moving the traditional packages where we can find a SE:



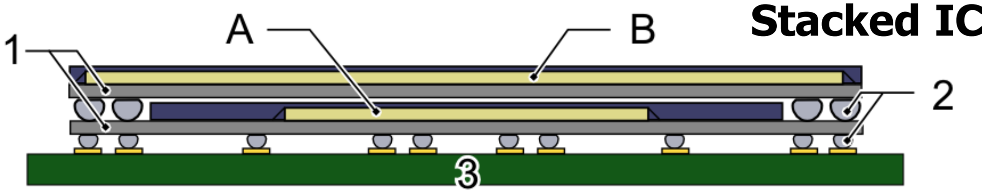


BGA Standard – still Easy?





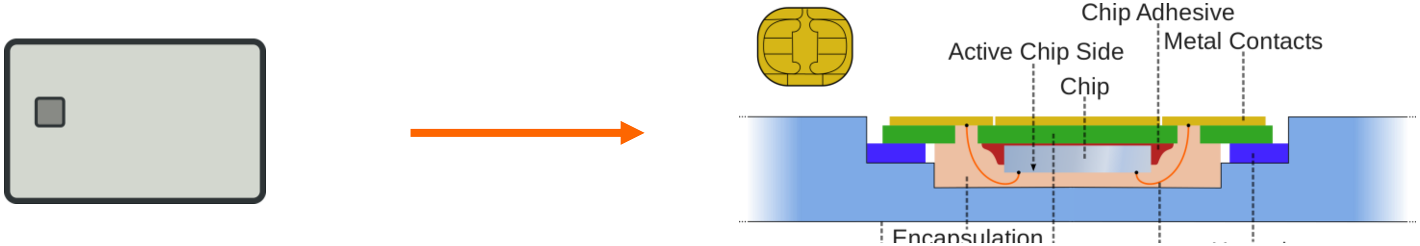
Stacked IC – Difficult?

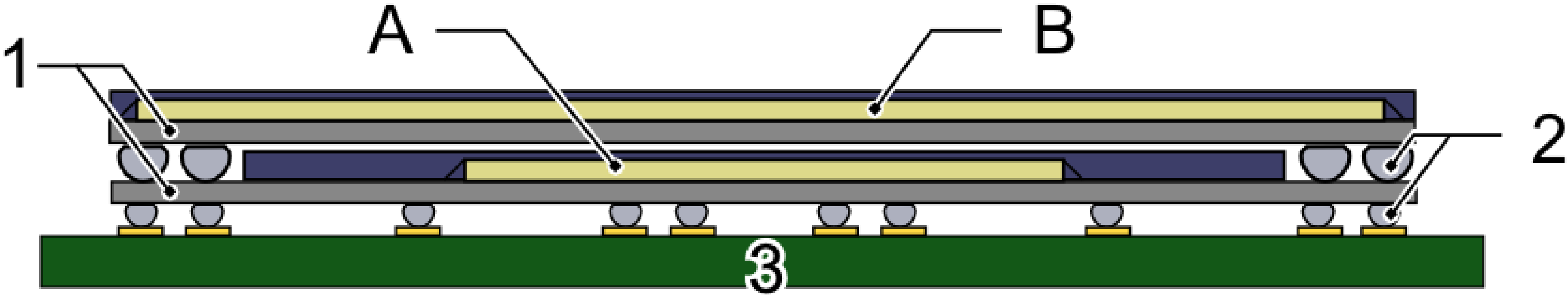


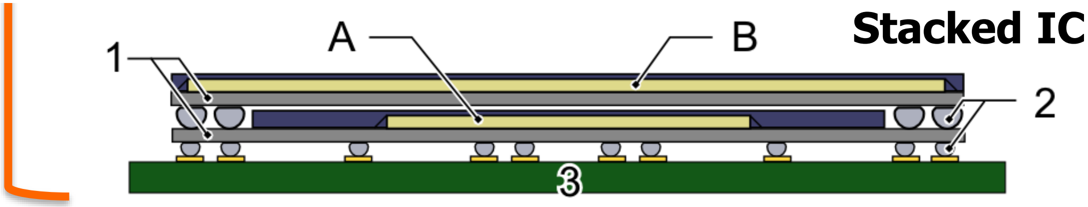
Stacked Packages (POP) –Medium?

New Form Factors for Secure Elements

New Markets like IoT, Automotive or Mobile are moving the traditional packages where we can find a SE:





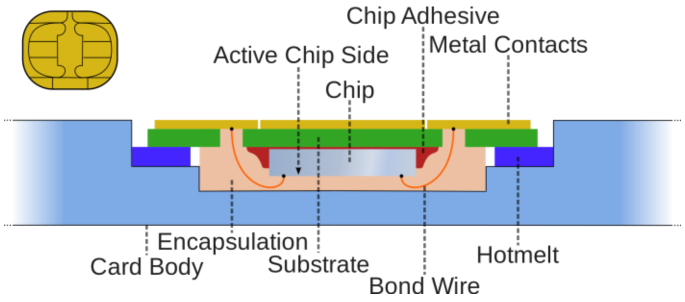


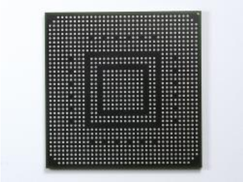
Stacked IC – Difficult?

Stacked Packages (POP) –Medium?

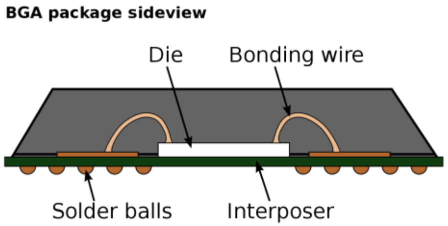
New Form Factors for Secure Elements

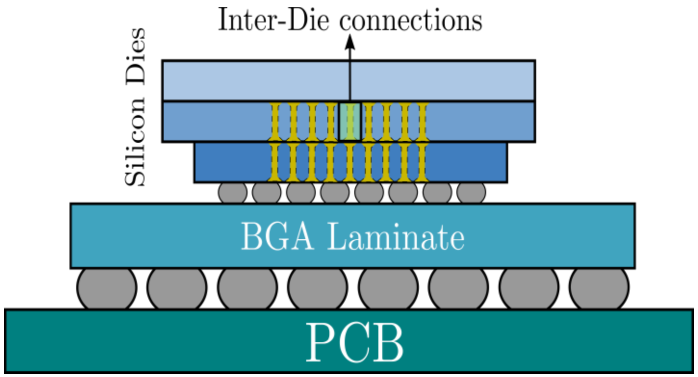
New Markets like IoT, Automotive or Mobile are moving the traditional packages where we can find a SE:



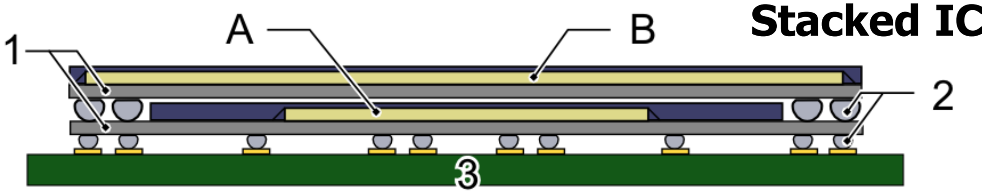


BGA Standard – still Easy?





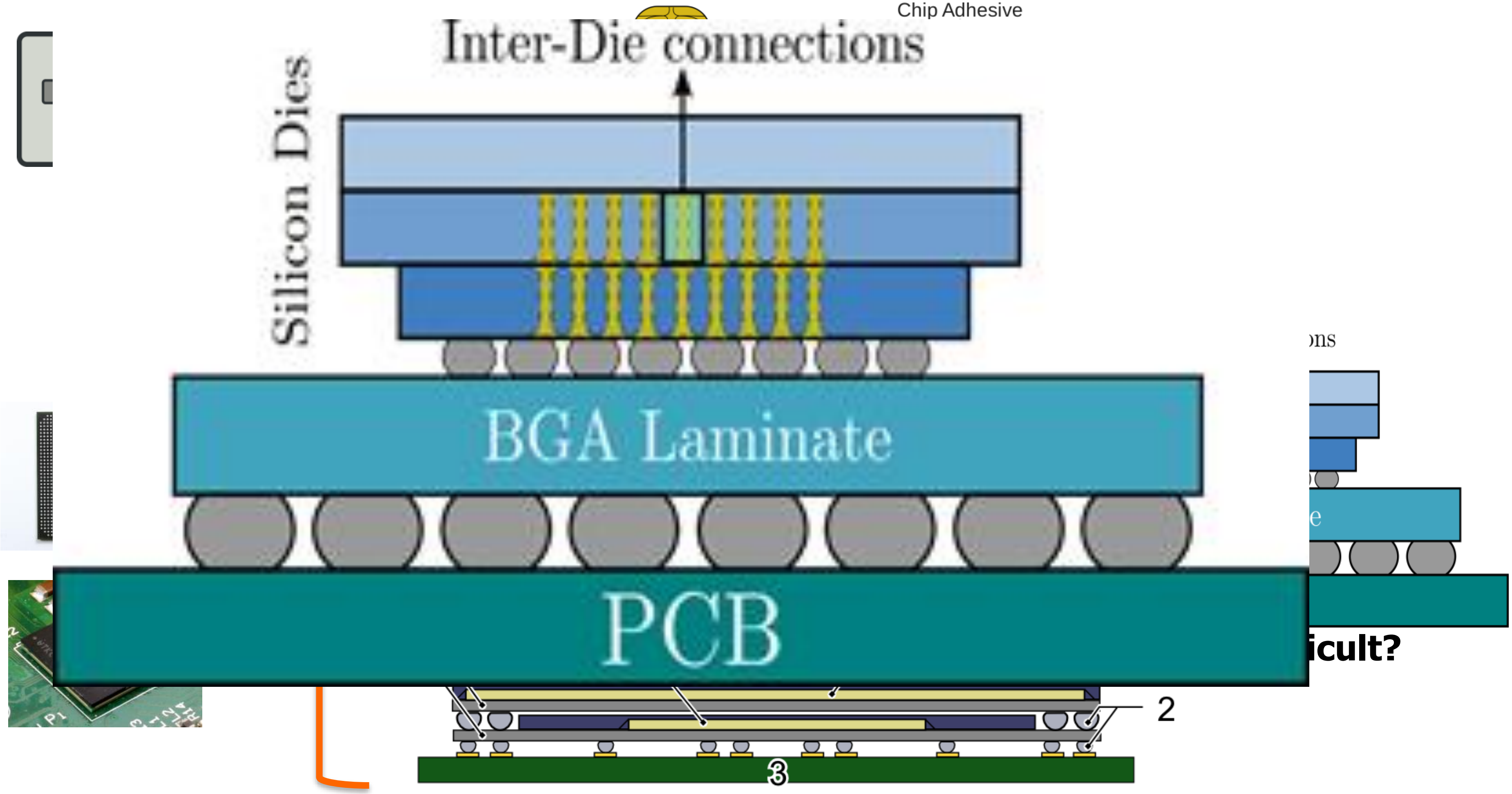
Stacked IC – Difficult?



Stacked Packages (POP) –Medium?

New Form Factors for Secure Elements

New Markets like IoT, Automotive or Mobile are moving the traditional packages where we can find a SE:



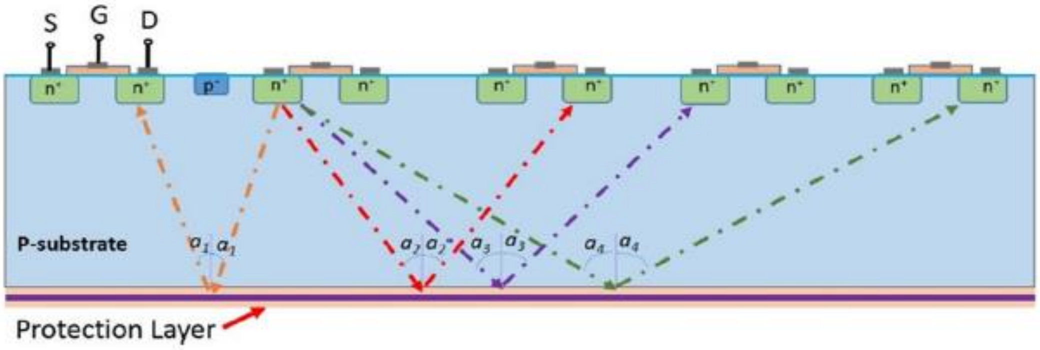
icult?

Stacked Packages (POP) –Medium?

Sample Access and Countermeasures

New countermeasures may come in the future to make some FI attacks more difficult. Some examples of what may be coming:

Figure from



Amini et al., Ic security and quality improvement by protection of chip backside against hardware attacks. Microelectronics Reliability, 88:22–25, 2018. (above figure extra)

Borel et al., A novel structure for backside protection against physical attacks on secure chips or sip. In 2018 IEEE 68th Electronic Components and Technology Conference (ECTC), pages 515–520. IEEE, 2018.

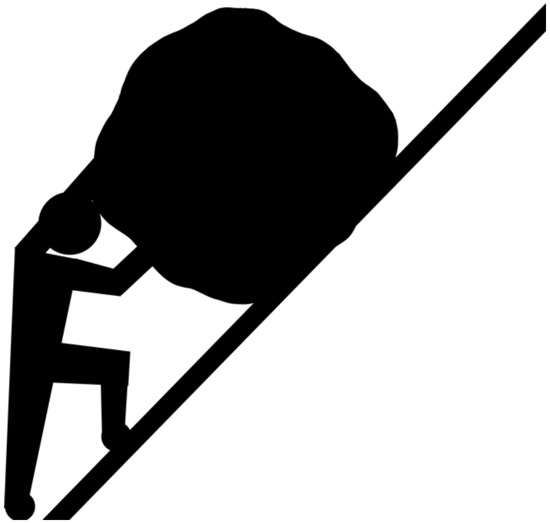
Manich et al., Backside polishing detector: a new protection against backside attacks. In *DCIS'15-XXX Conference on Design of Circuits and Integrated Systems*, 2015

Will be adopted by the industry?

FI sample preparation trend

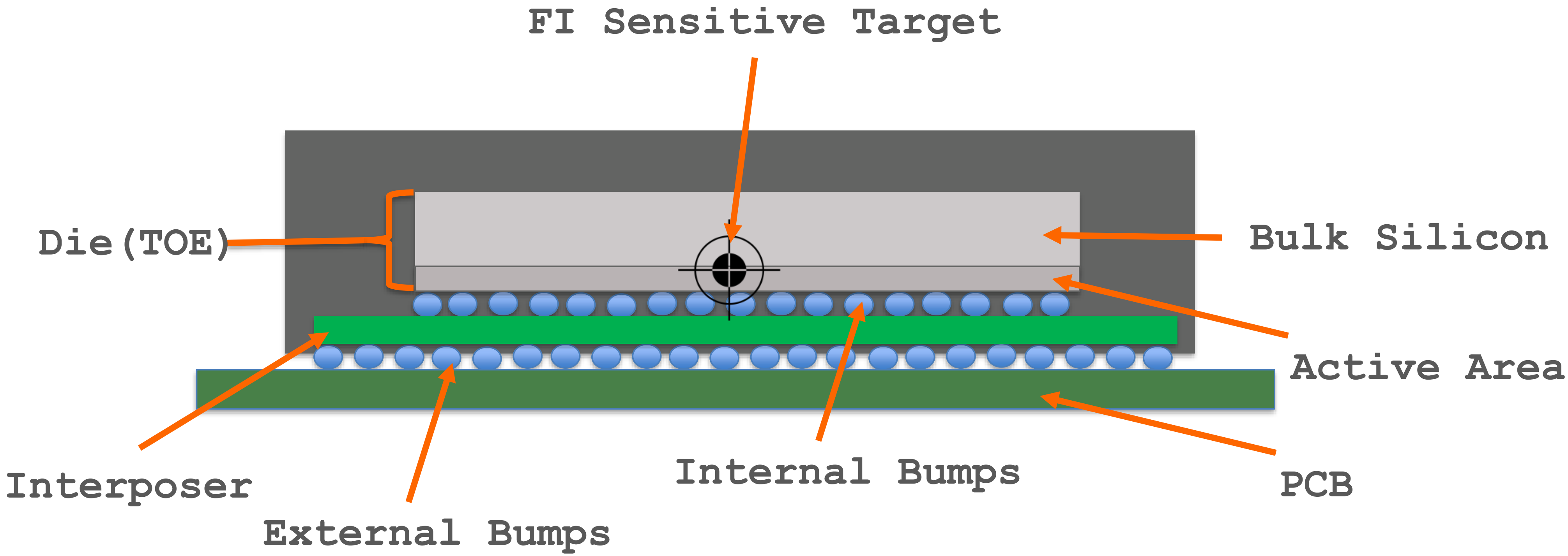
Conclusion:

Clear trend => ↑ effort in sample preparation for FI

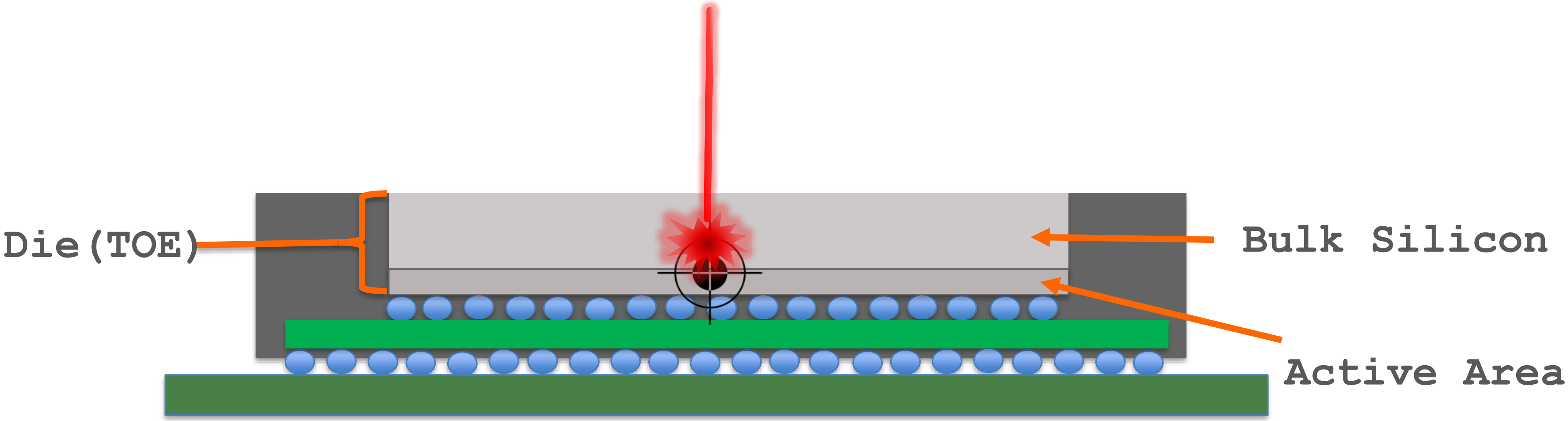


Let’s challenge it!!

Challenge I: LFI on Standard BGA (Flip Chip)

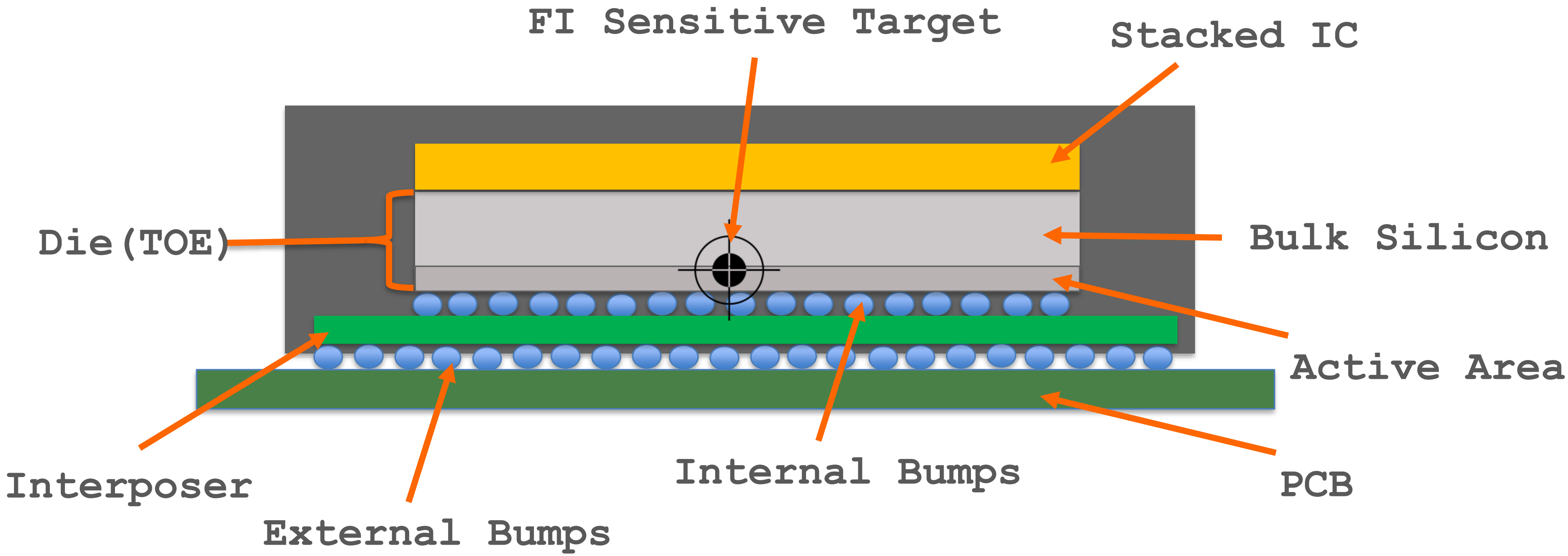


Challenge I: LFI on Standard BGA (Flip Chip)



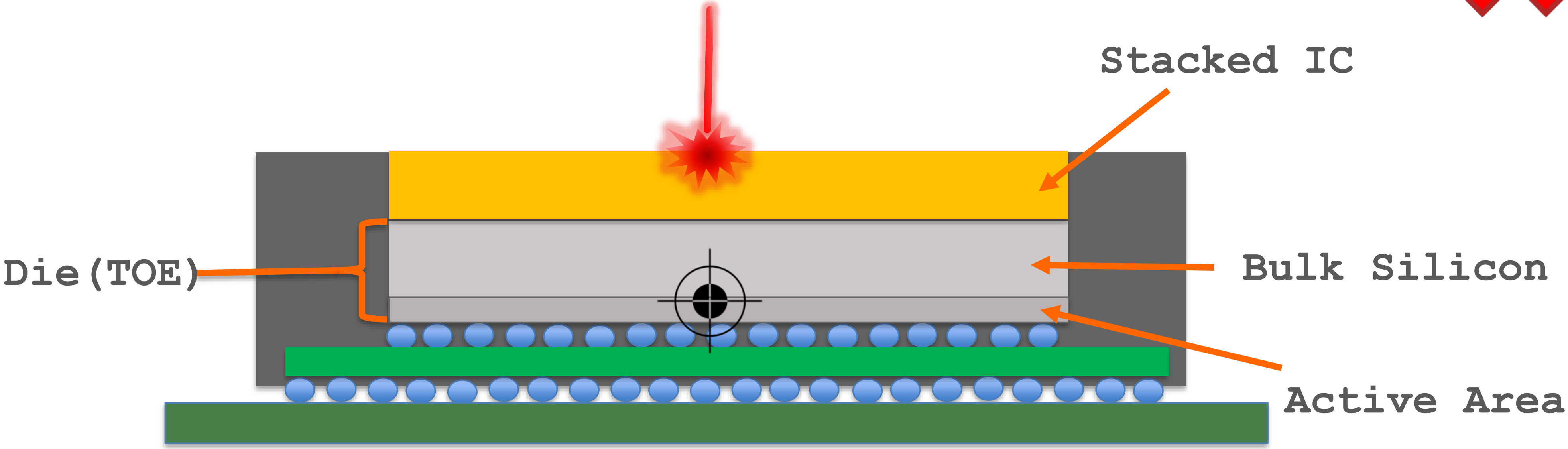
Laser + Polishing Machine => Easy Access ✓

Challenge II: Stacked IC



Challenge II: Stacked IC

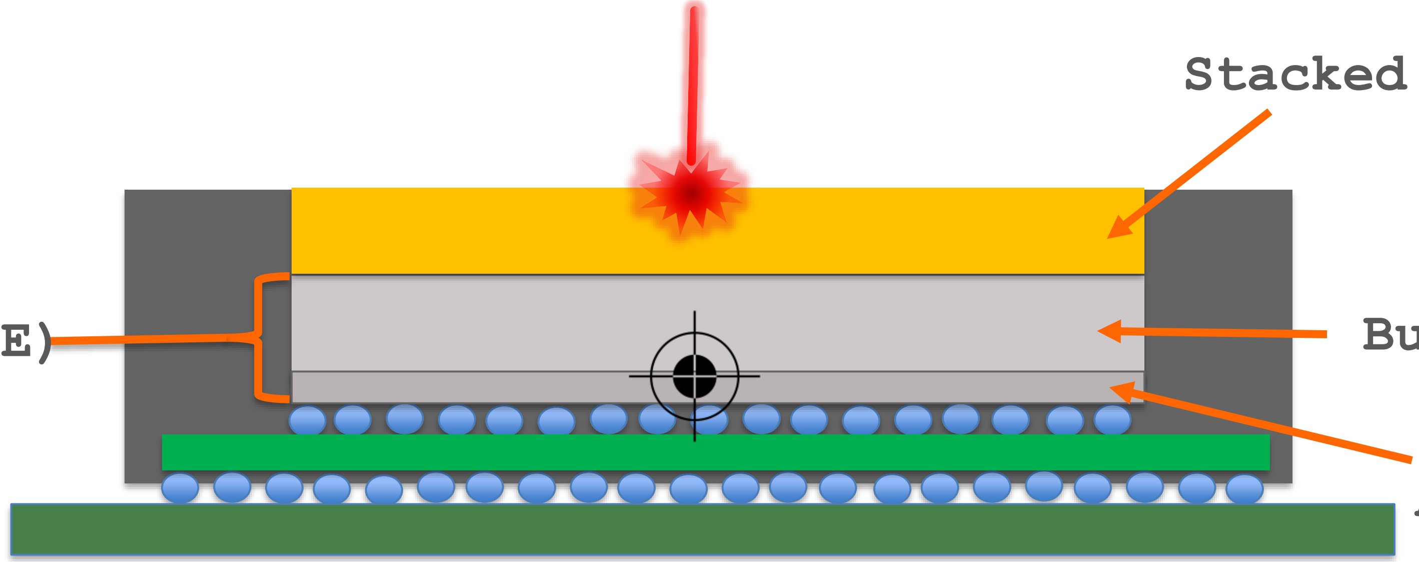
Laser + Polishing Machine => No direct Access ✗



Requires special setup(re-pacakging) => ⬆ more Effort

Challenge II: Stacked IC

Laser + Polishing Machine => No direct Access



Stacked IC

Die(TOE)

Bulk Silicon

Active Area

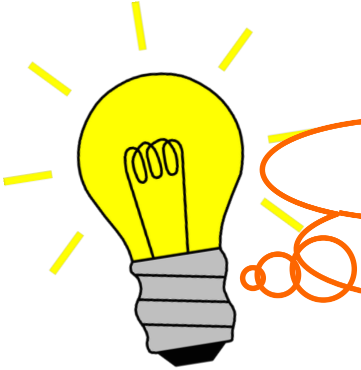
Requires special setup(re-pacakging) => more Effort

Attacker’s mind:

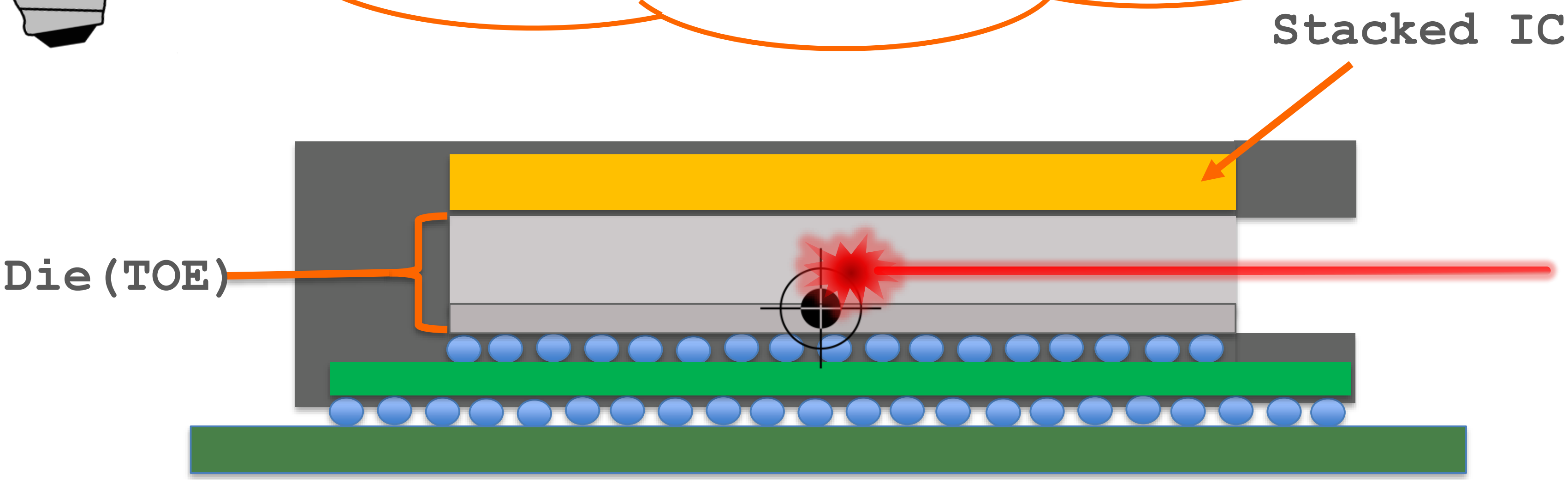
“Principle of minimum effort”
+
“Lateral Thinking”

Is there any (easy) alternative way to attack this configuration?

The idea: Lateral Laser Fault Injection (LLFI)



The edge of the chip is another surface of attack, why not trying Laser there?



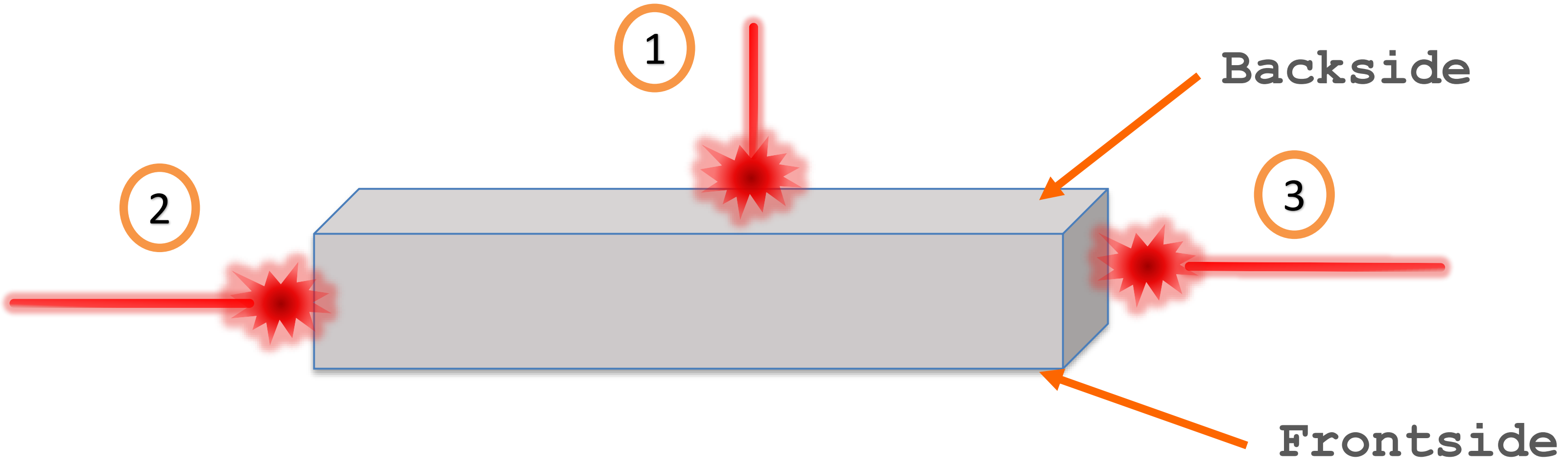
LLFI: Lateral Laser Fault Injection

Proof of concept!

Lateral LFI Proof of Concept on Standard Package

Experimental Testing Objectives:

- LLFI is feasible?
- Difference (backside) LFI vs LLFI?

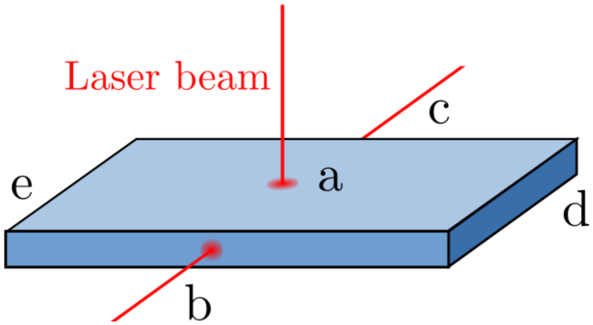


- Two different secure Ics (with standard packaging) were tested for the proof of concept!

Experimental Testing I

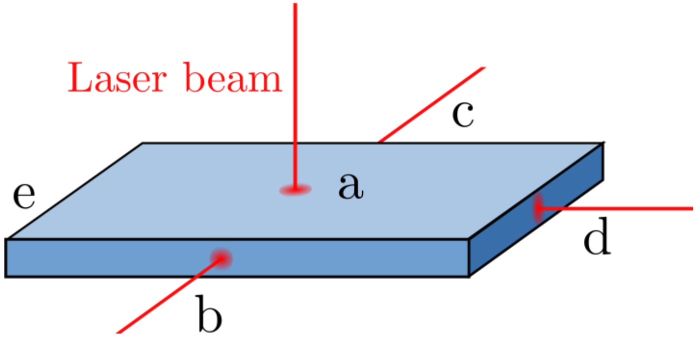
- Standard IC de-packaging techniques* were used (mechanical and chemical)
- Bondings limited Access to all sides

DUT A



2 sides available

DUT B



3 sides available

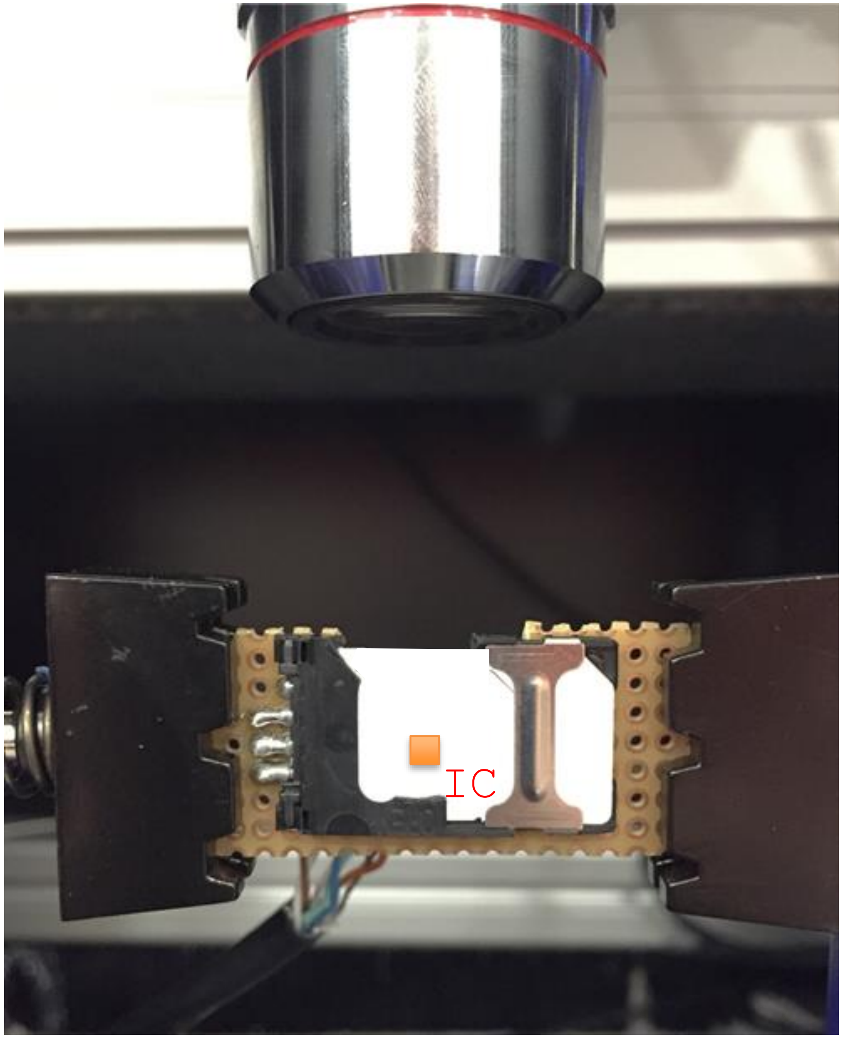
*Philippe Loubet Moundi. Cost effective techniques for chip delayering and in-situ depackaging, 2013.

Experimental Testing II

- DUTs contained an application with password verification
- We sent and incorrect password and we tried to bypass the authentication check:

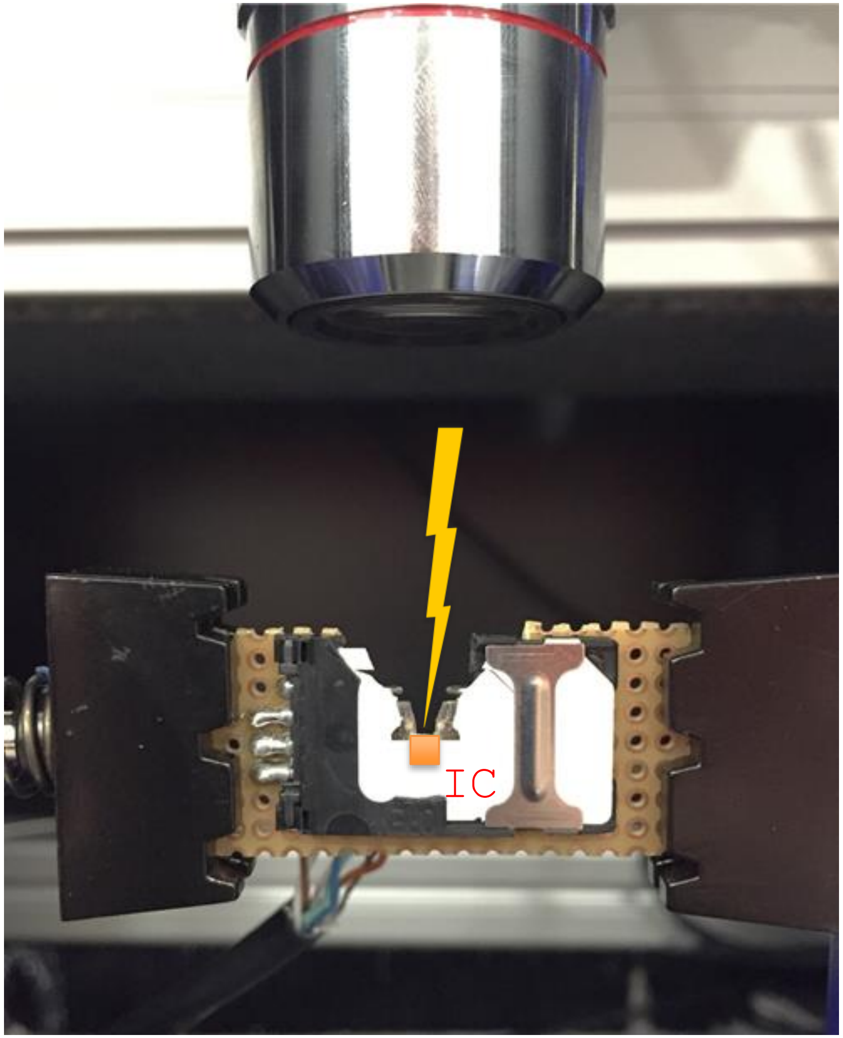
```
If pwd == ref_pwd {
   success_authentication()  //Faulty behavior
   }
 failed_authentication()  // No fault
```

Experimental Setup



- 1064 nm wavelength
- lens with x5 magnification.
- laser spot diameter of 12 µm
- maximum pulse width of 2500 ns
- maximum pulse power of 2 W.
- Special postioning for LLFI (90°)

Experimental Setup

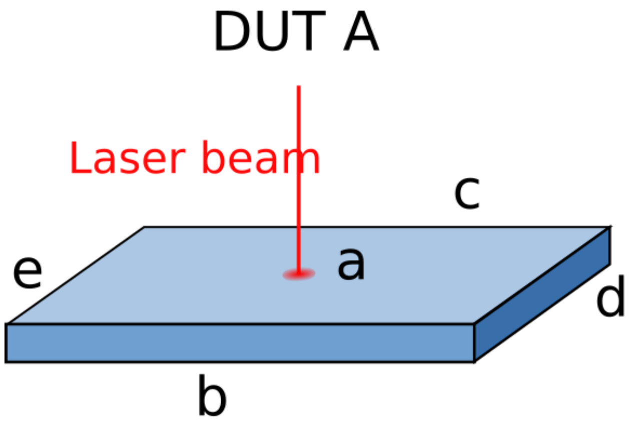


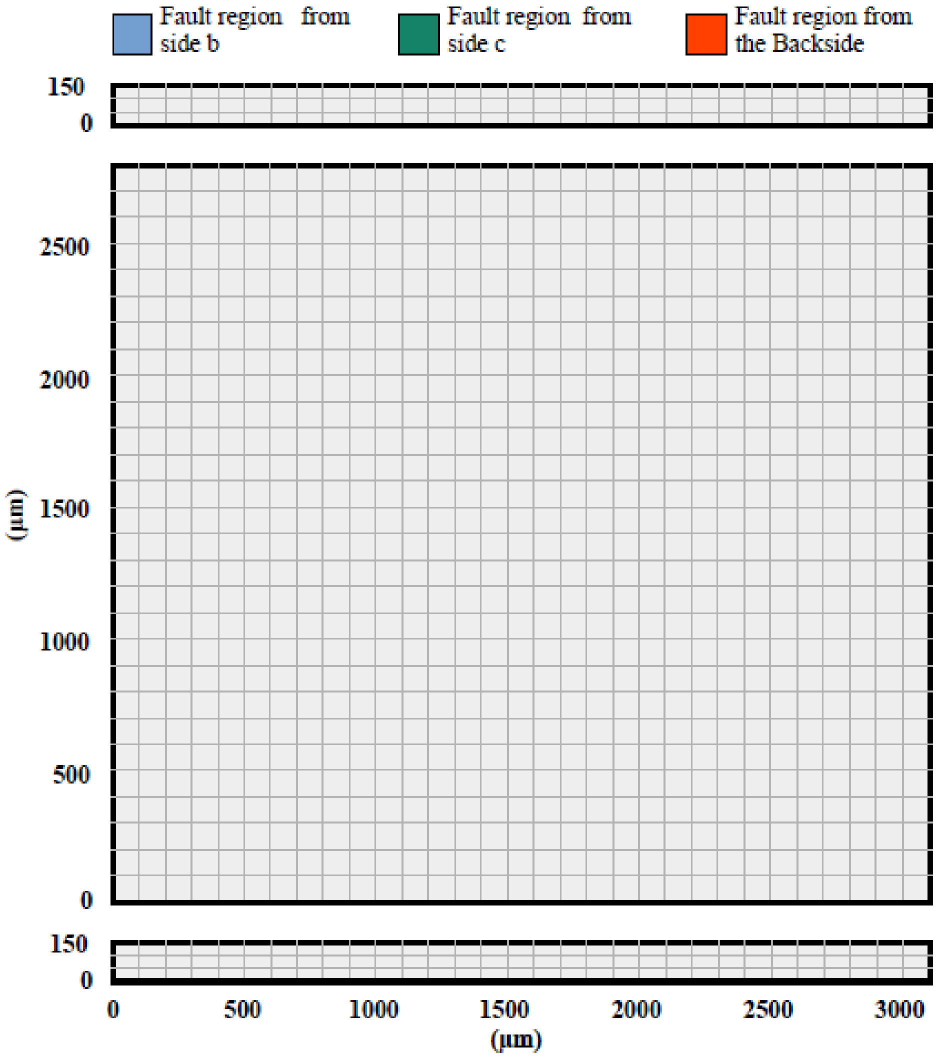
- 1064 nm wavelength
- lens with x5 magnification.
- laser spot diameter of 12 µm
- maximum pulse width of 2500 ns
- maximum pulse power of 2 W.
- Special postioning for LLFI (90°)

Experimental Results:
Spatial Analysis

Experimental Results DUT A: Spatial Analysis

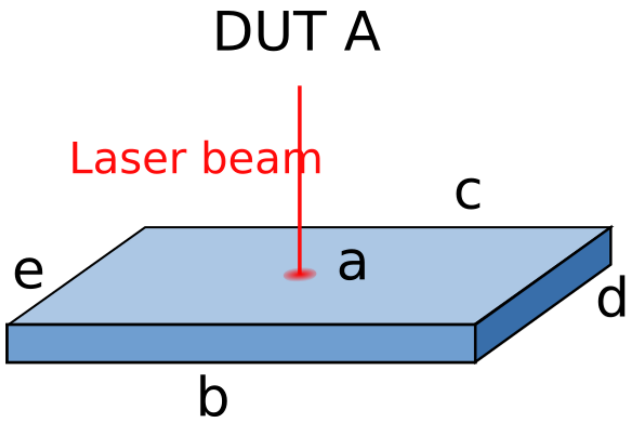
- LFI on Backside



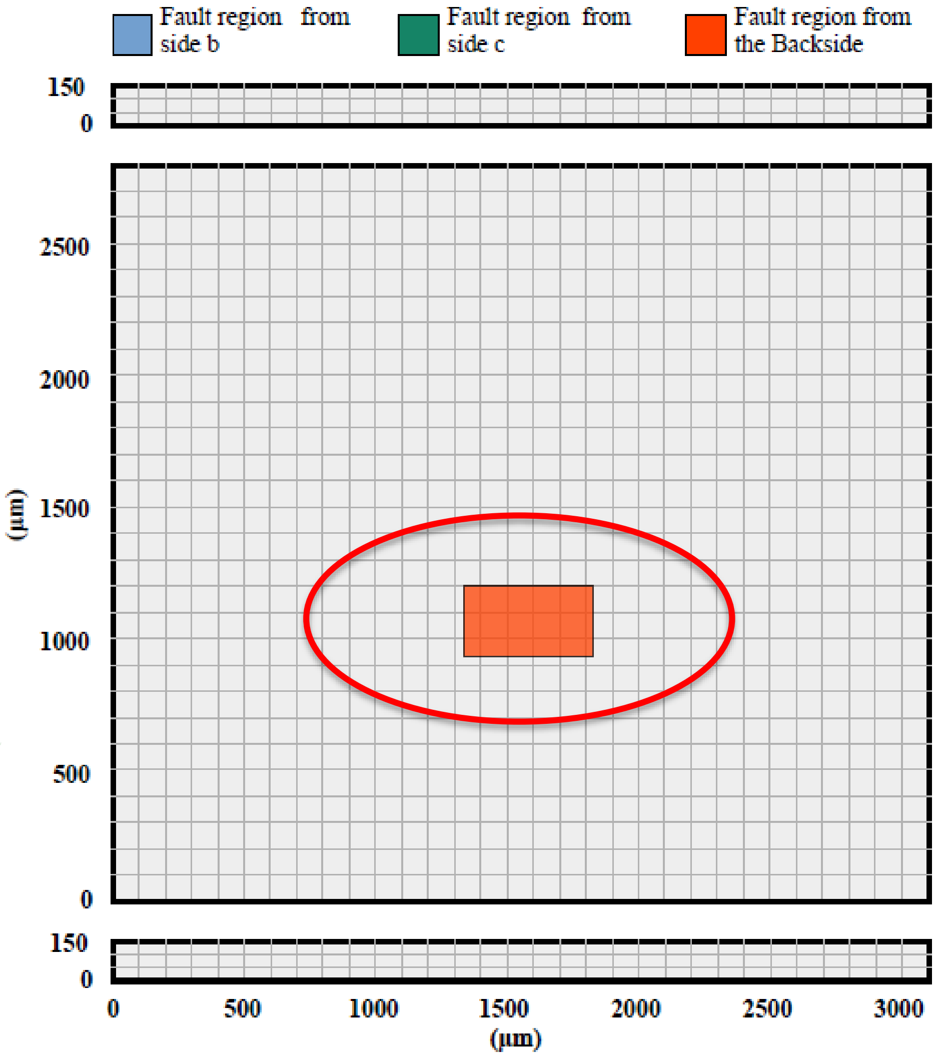


Experimental Results DUT A: Spatial Analysis

- Backside Testing

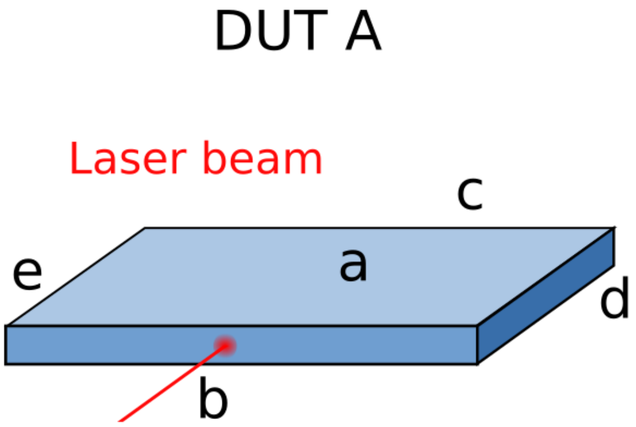


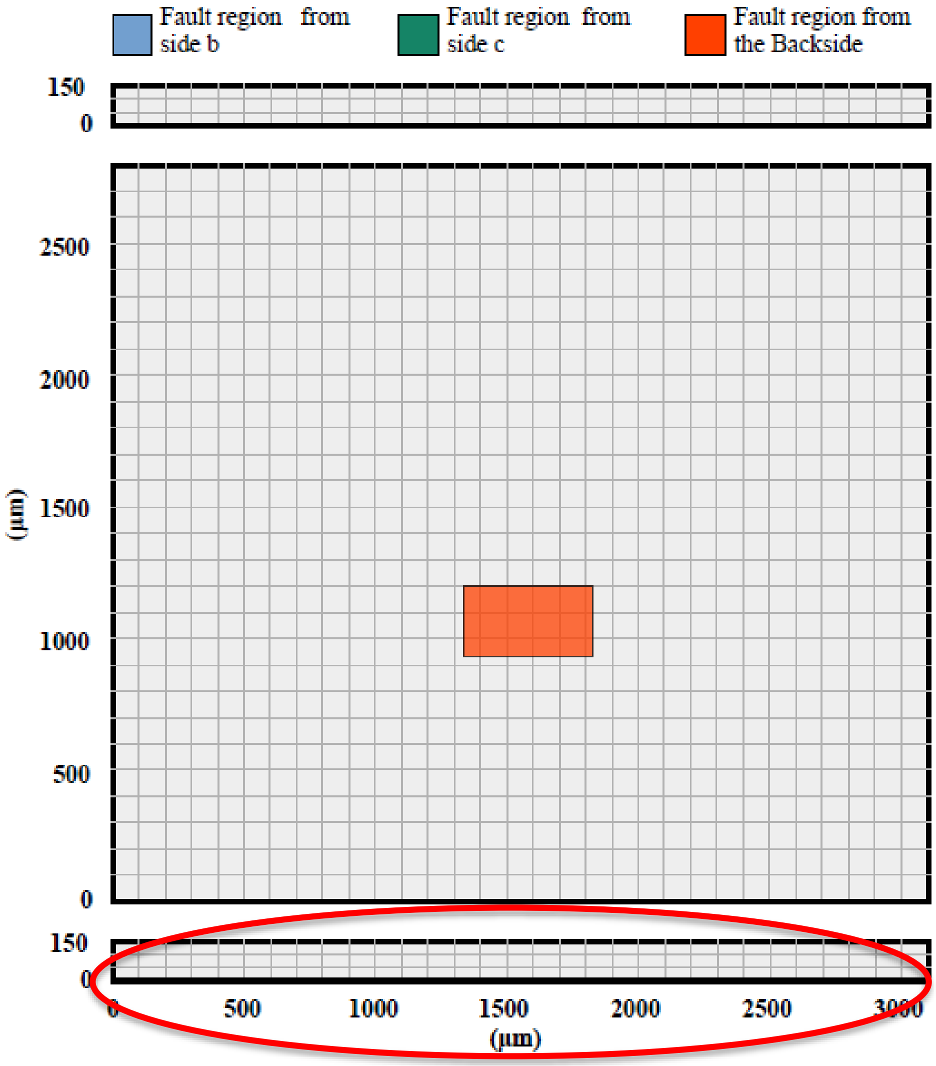
- Successful Faults!!



Experimental Results DUT A: Spatial Analysis

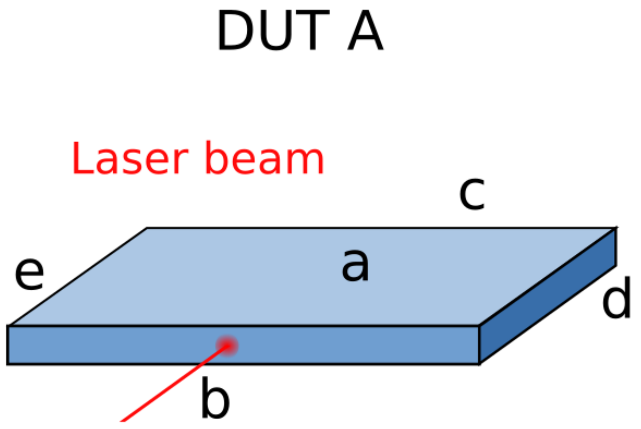
- LFI on side b





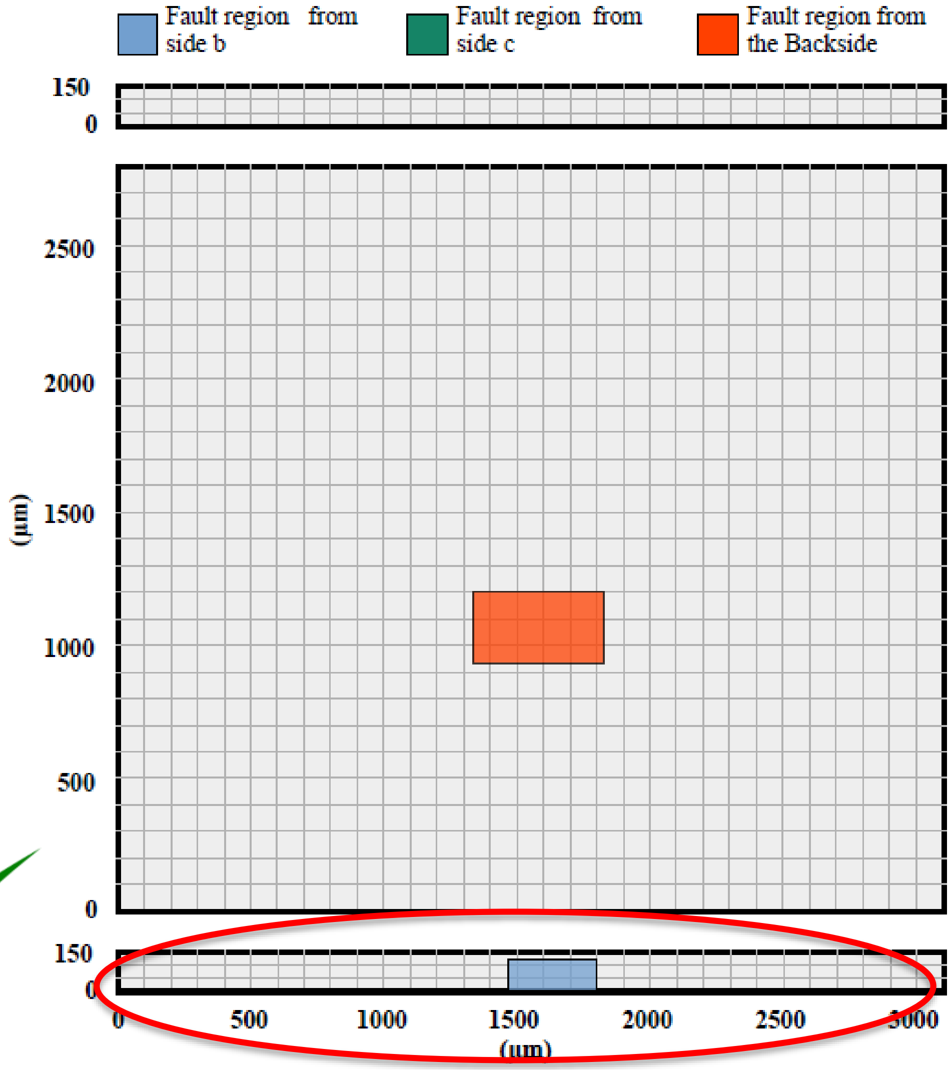
Experimental Results DUT A: Spatial Analysis

- LFI on side b



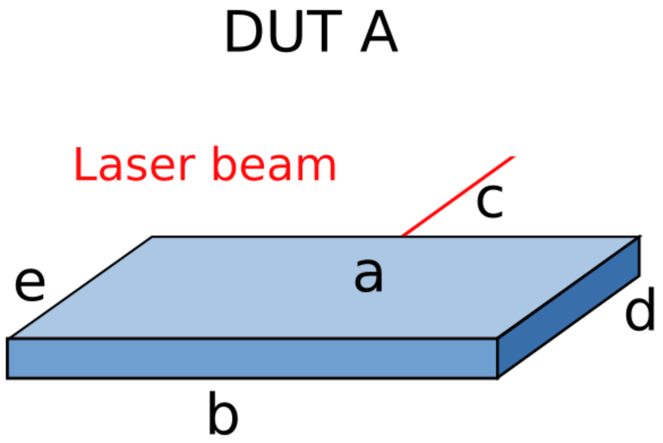
- Successful Faults!!

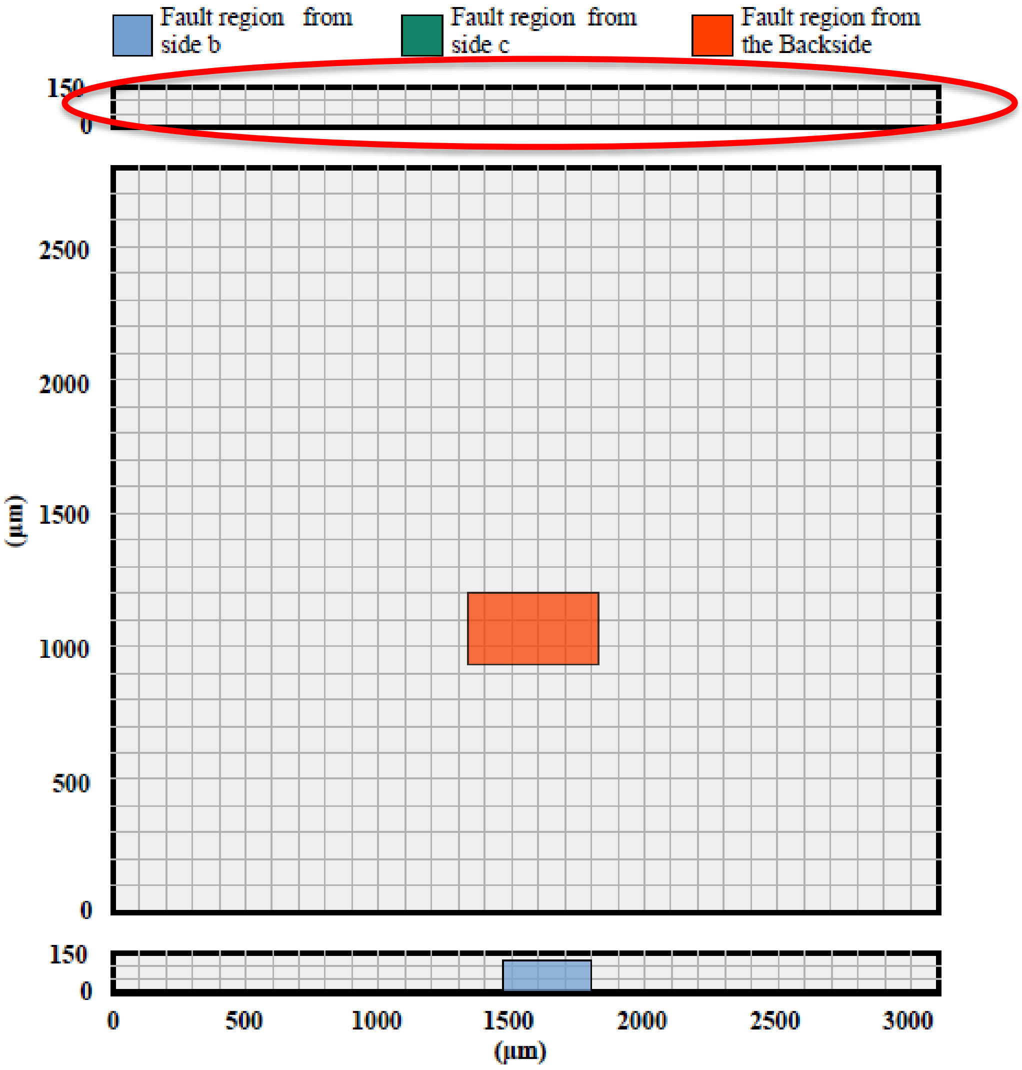
- **First objective achieved!!**



Experimental Results DUT A: Spatial Analysis

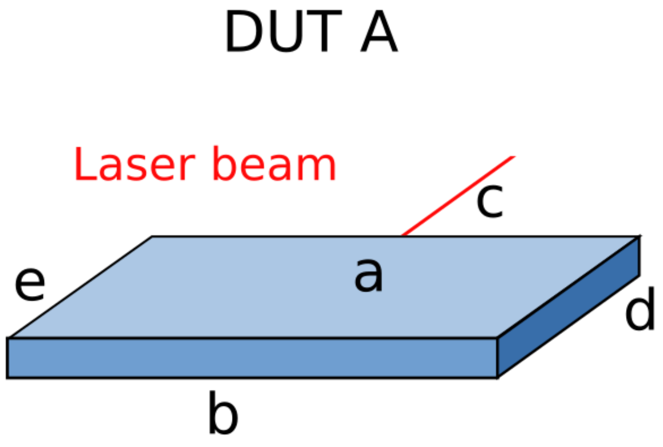
- LFI on side b

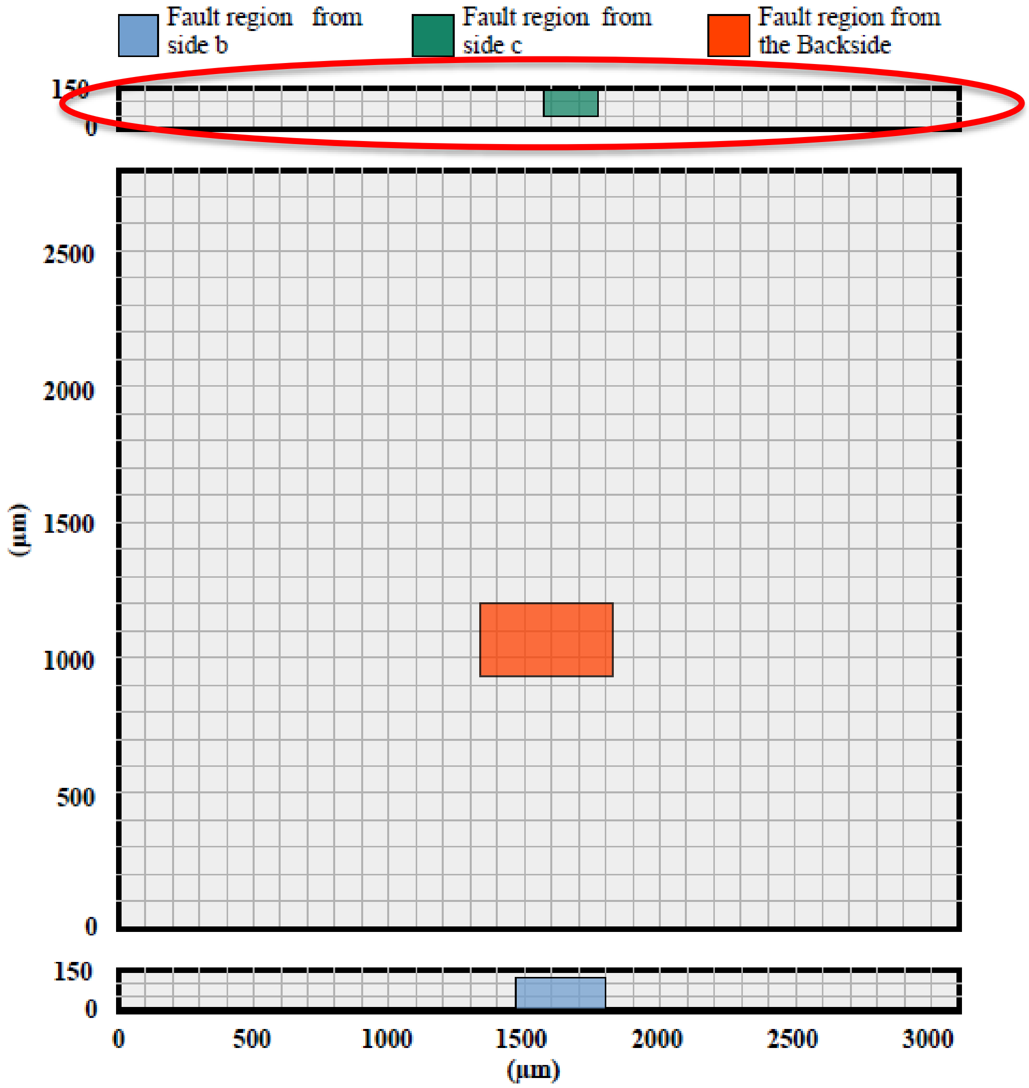




Experimental Results DUT A: Spatial Analysis

- LFI on side b



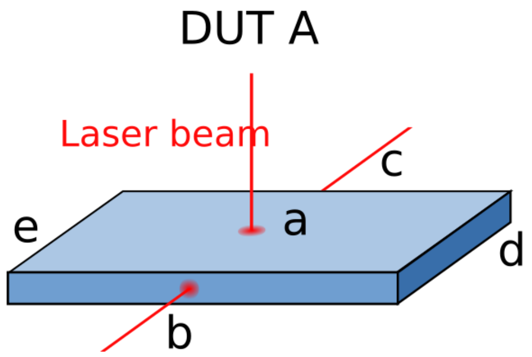


- Successful Faults!!

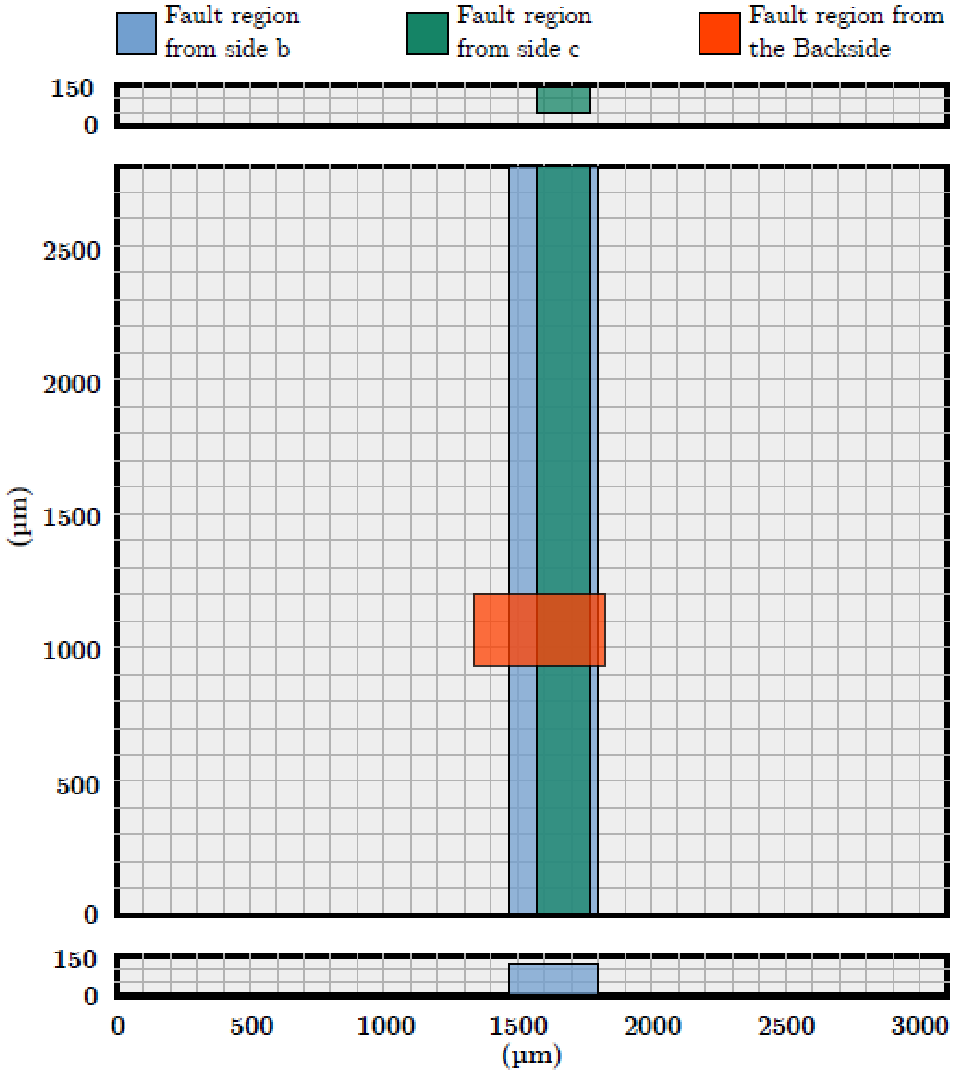
Experimental Results DUT A: Spatial Analysis

- Projected regions are overlapped!!

Same sensitive region?

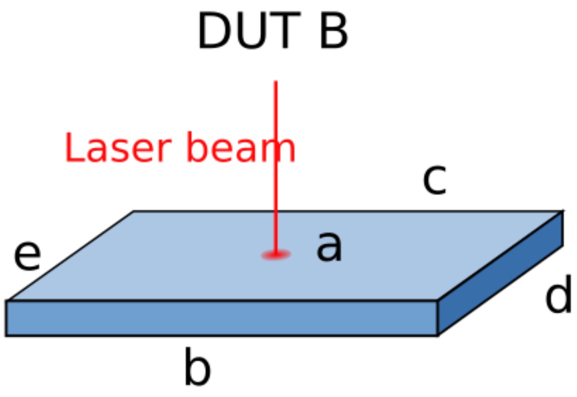


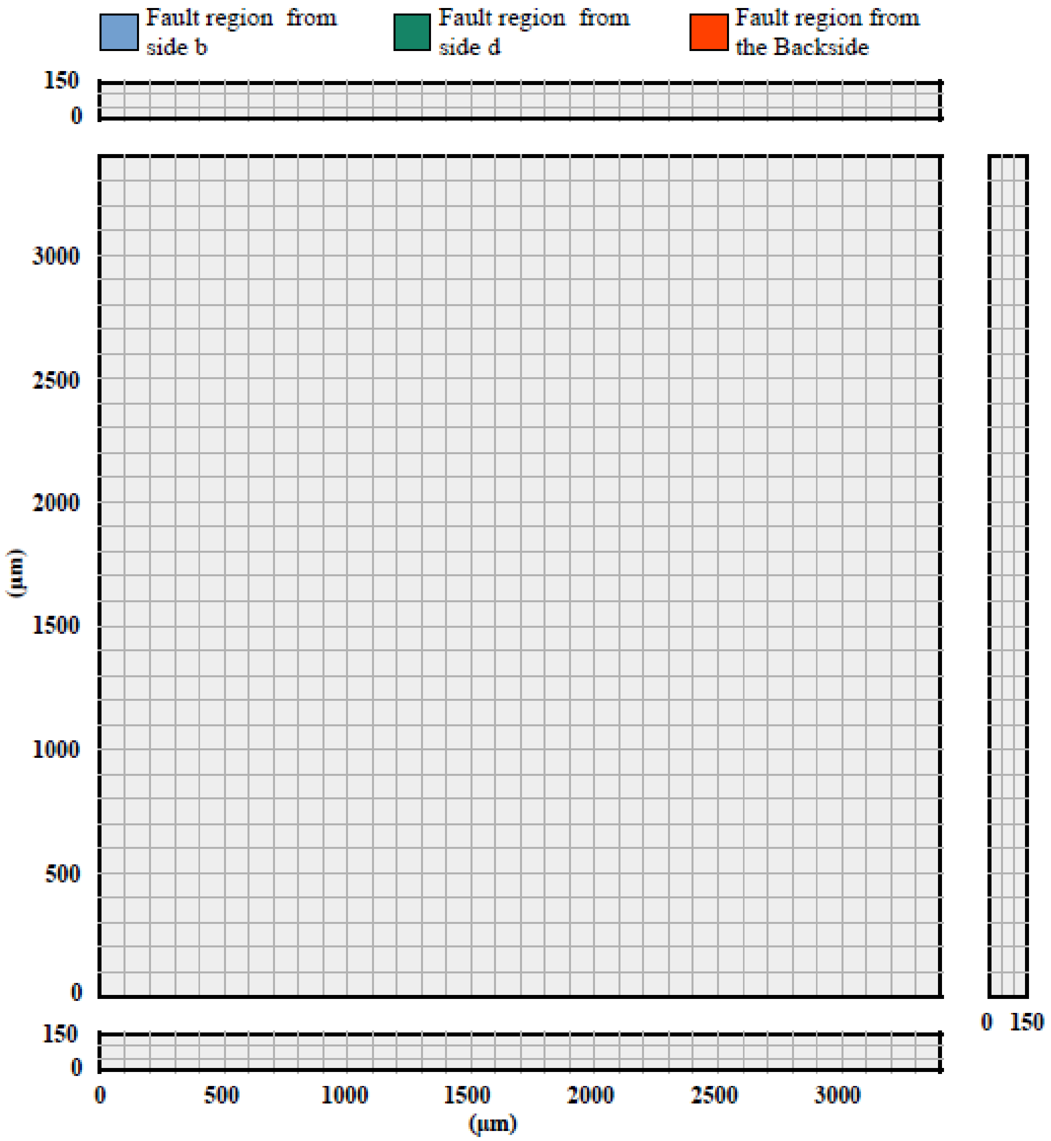
- Backside region larger
- Lateral regions with different size



Experimental Results DUT B: Spatial Analysis

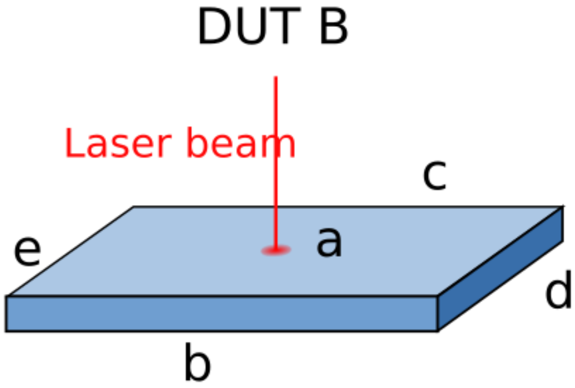
- LFI on Backside



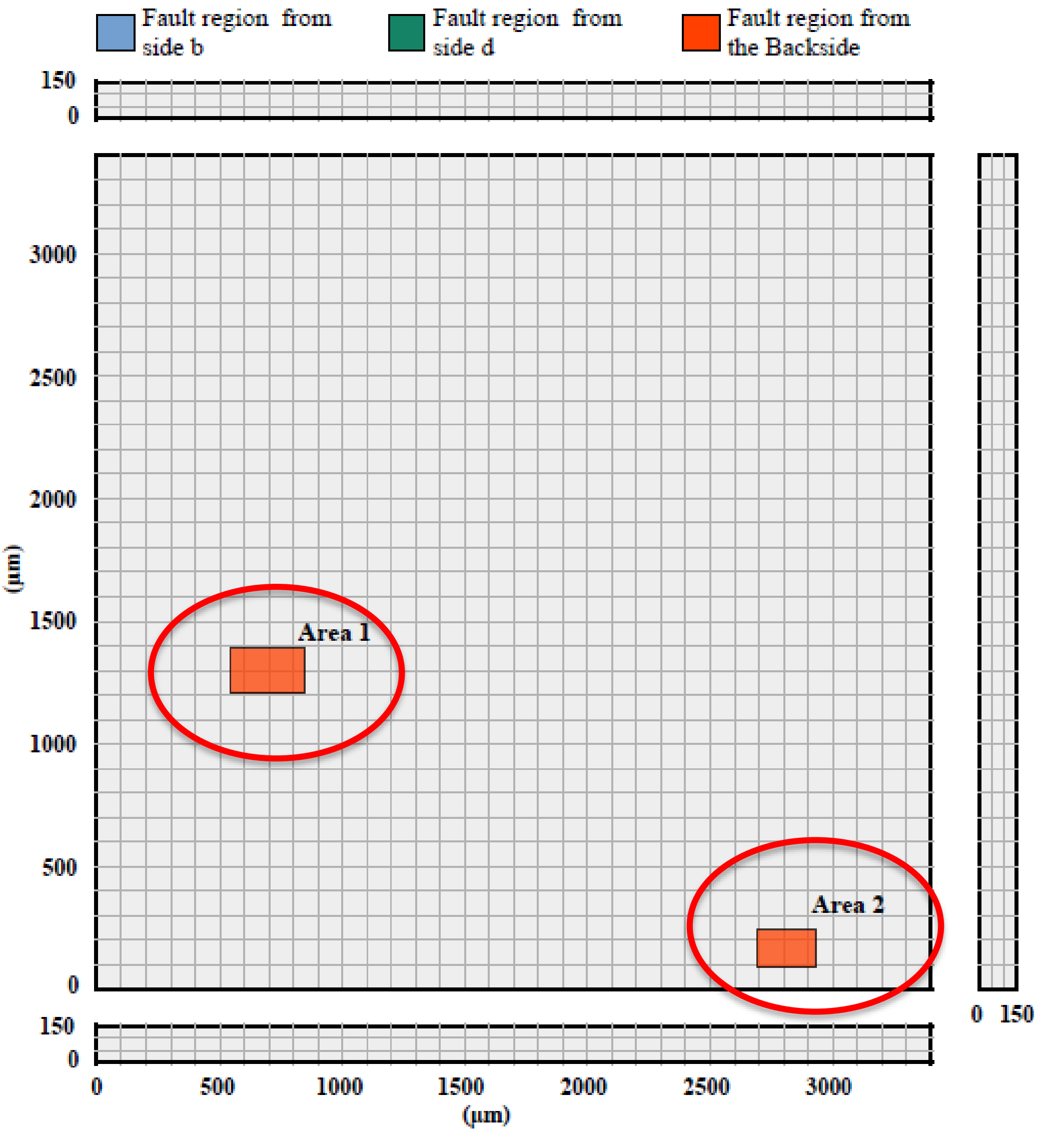


Experimental Results DUT B: Spatial Analysis

- LFI on Backside

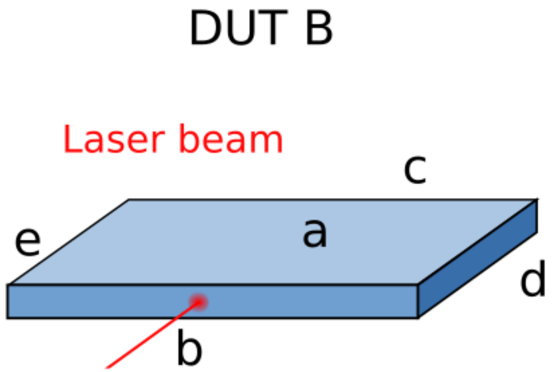


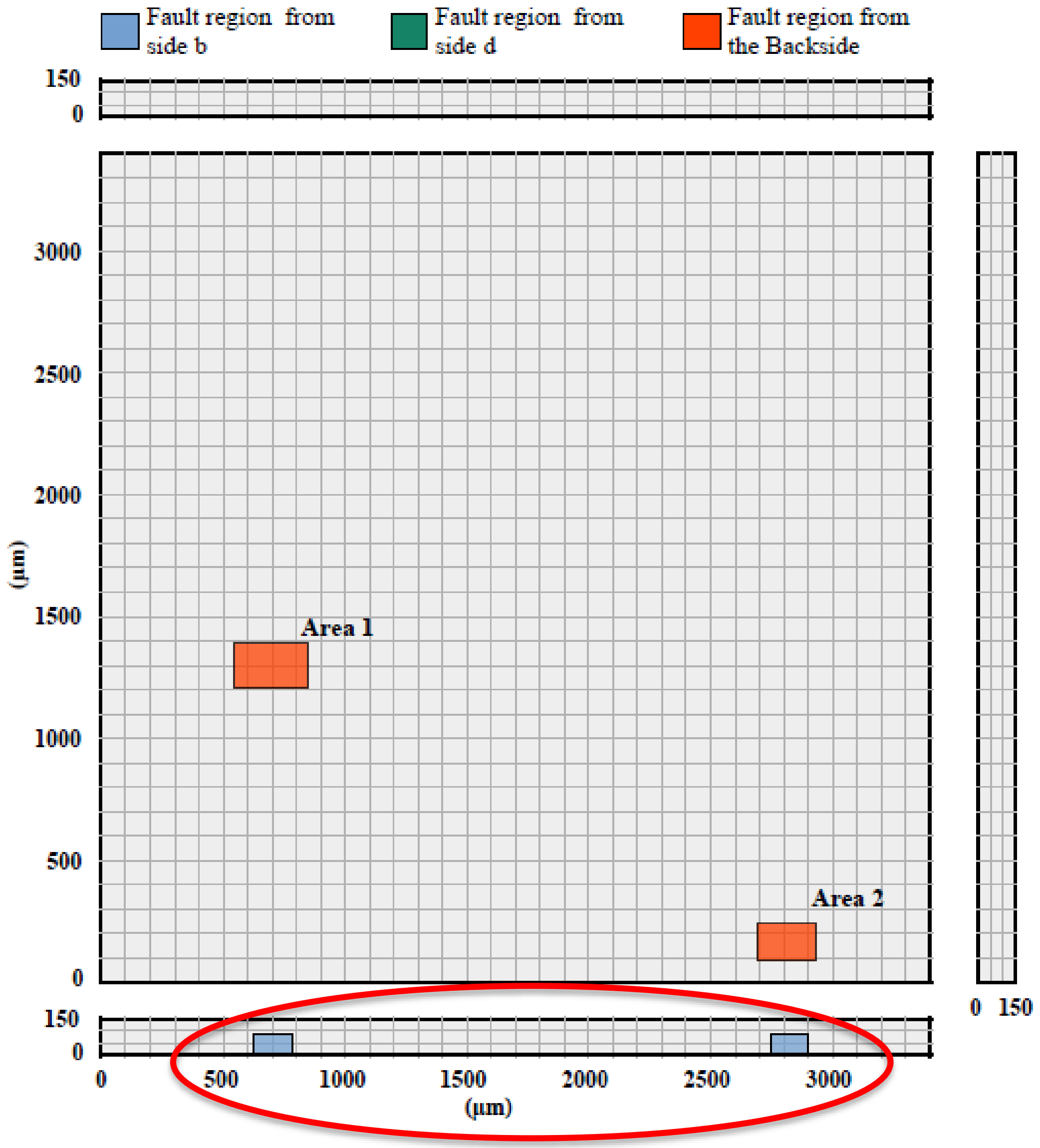
- Successful Faults



Experimental Results DUT B: Spatial Analysis

- LFI on side b

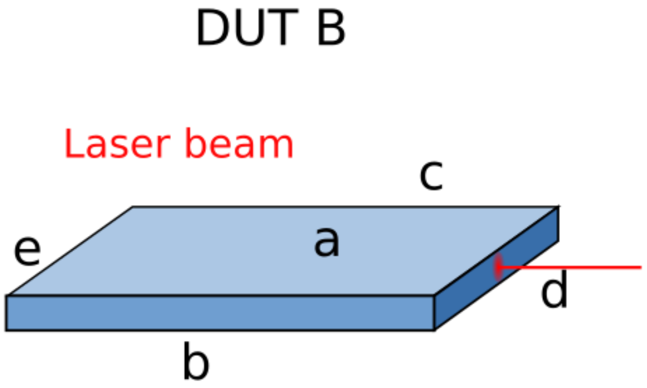


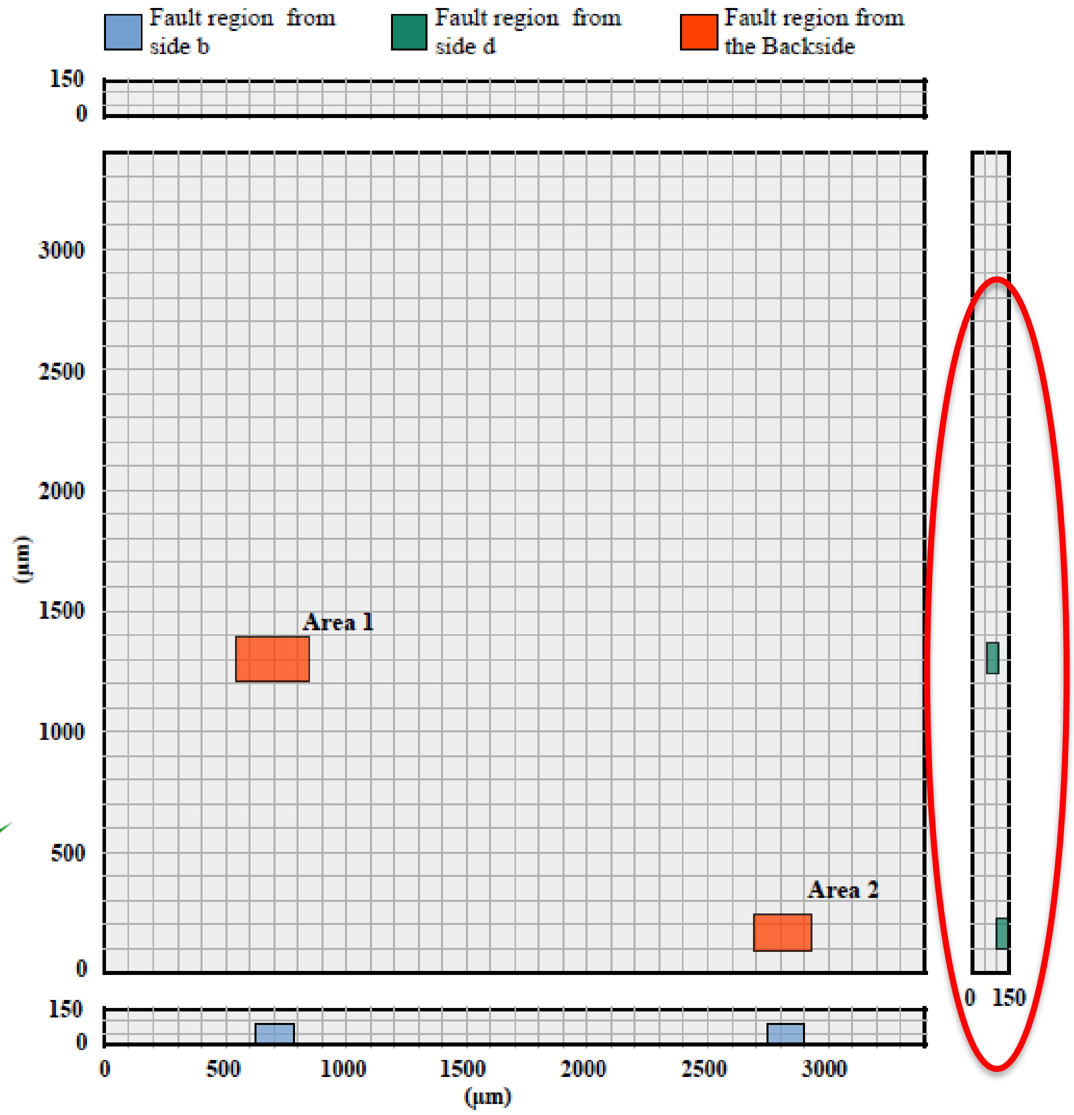


- Successful Faults in both areas!!

Experimental Results DUT B

- LFI on side b

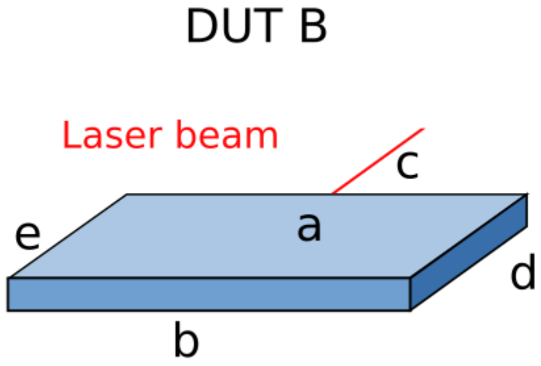




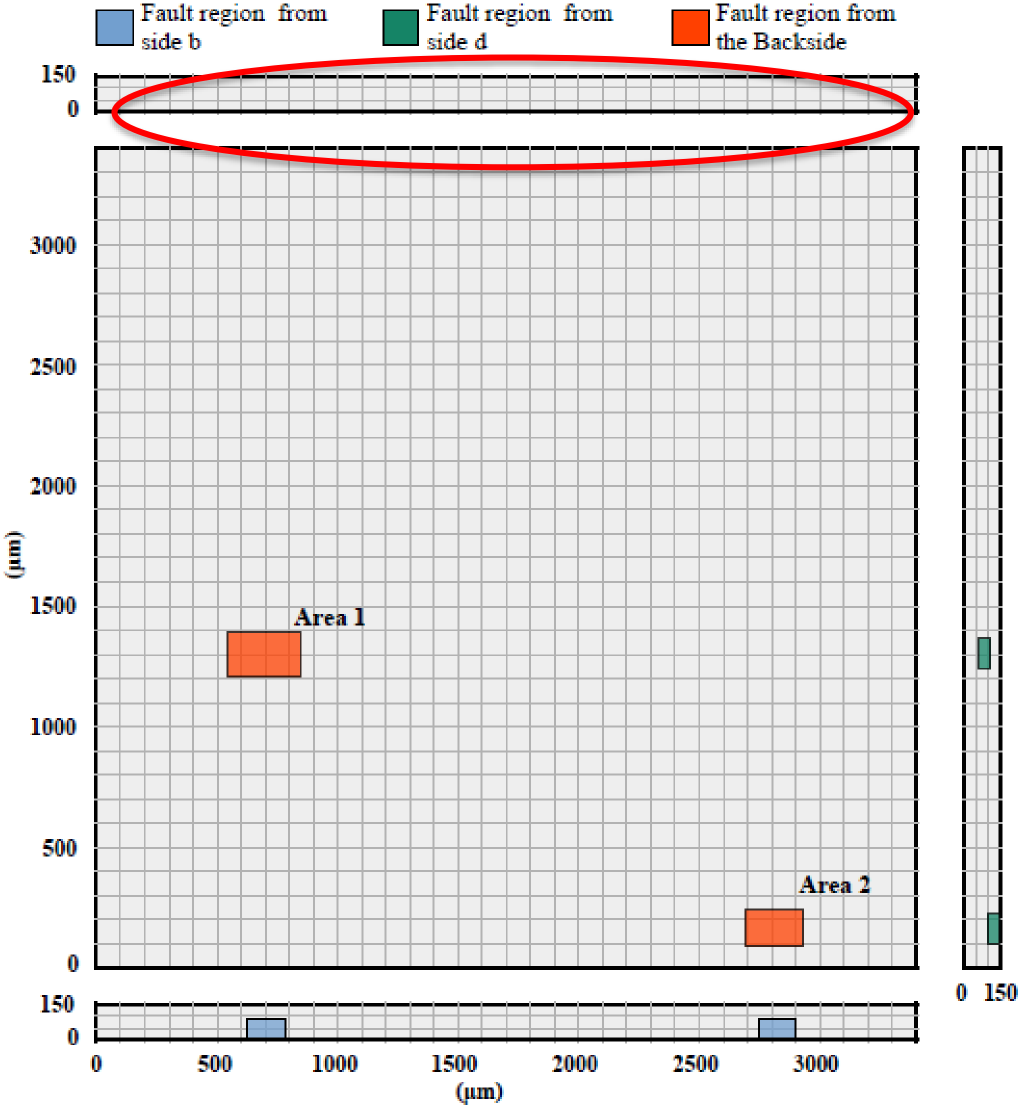
- Successful Faults!!

Experimental Results DUT B

- LFI on side c


DUT B

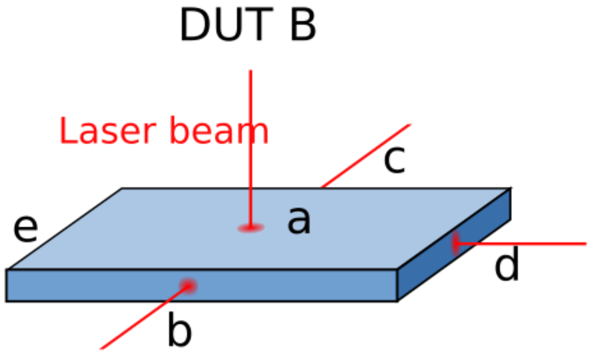
- No Faults ✗



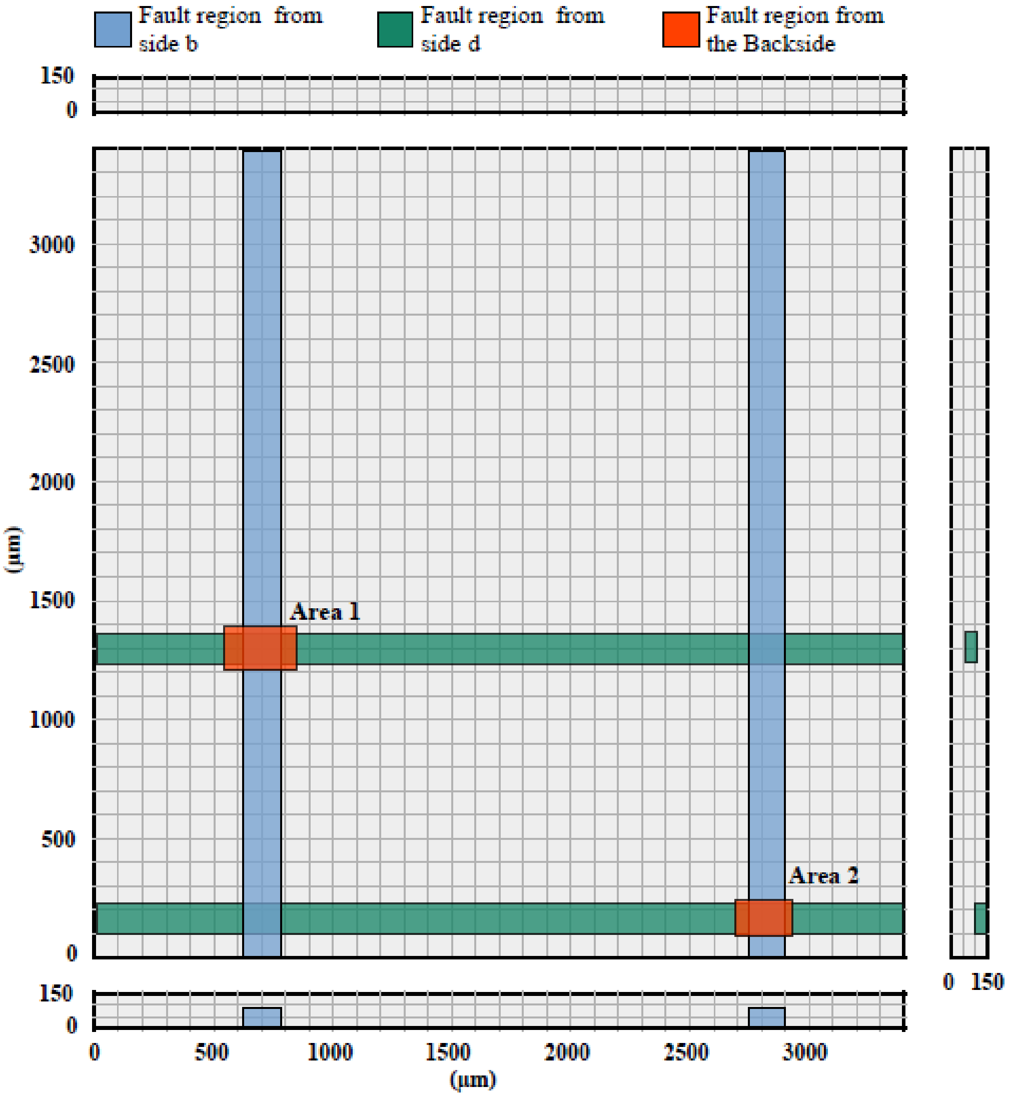
Experimental Results DUT B: Spatial Analysis

- Projected regions are overlapped!!

Same sensitive region?



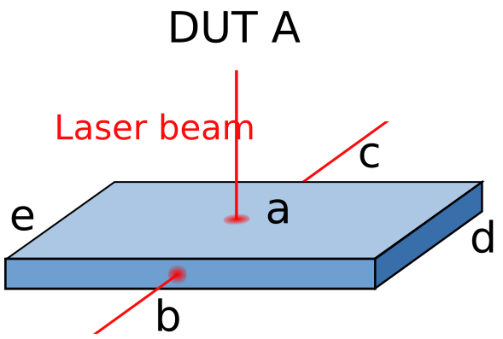
- Backside region larger

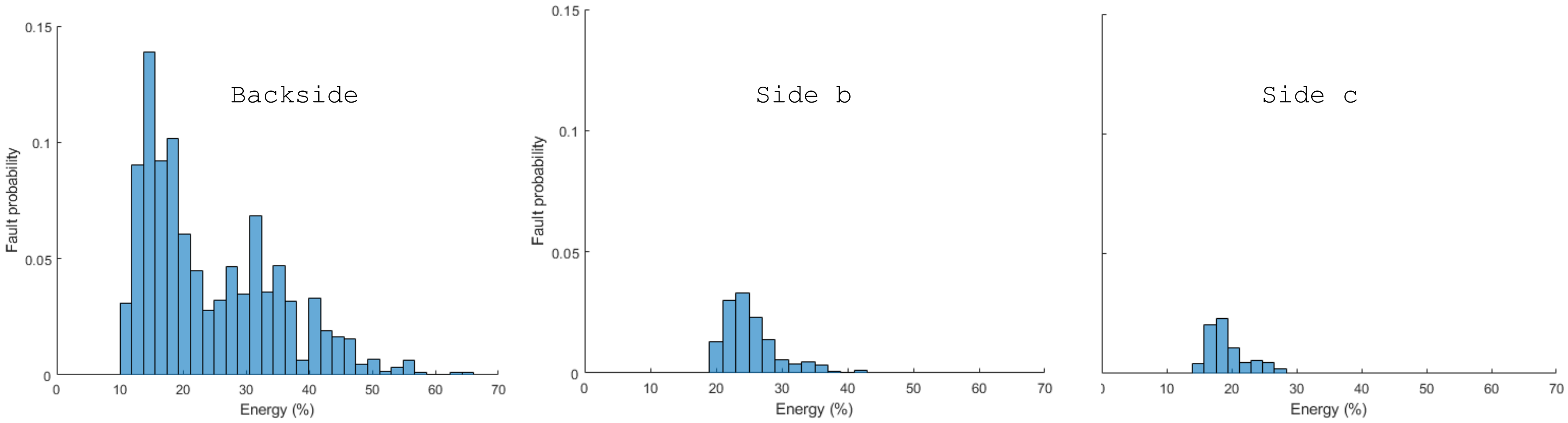


Experimental Results: Energy and Success Rate Analysis

Experimental Results DUT A: Laser Energy Analysis

- Backside requires less minimum energy and has higher probability to get a fault

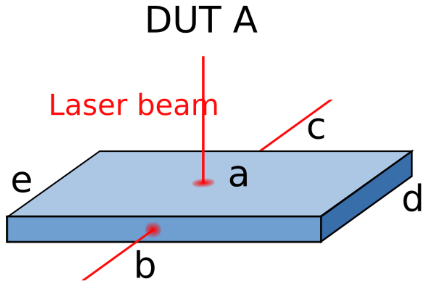


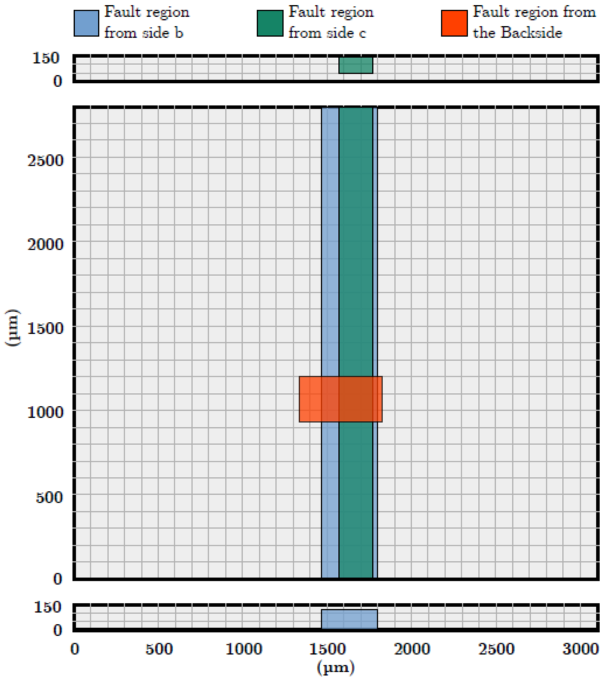


Experimental Results DUT A: Success Rate Analysis

- Success rate is lower for the LLFI
- More distance, less success rate

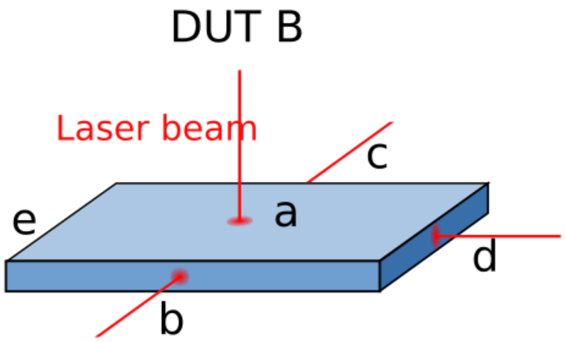
Exposed side	Success rate
Backside (LFI)	17.5%
Side b (LLFI)	5.1%
Side c (LLFI)	4.5%

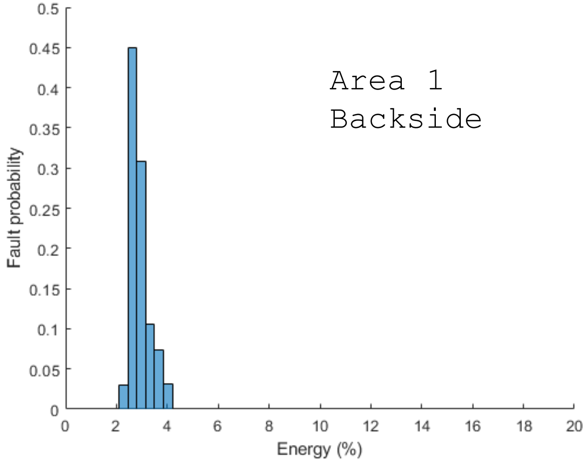


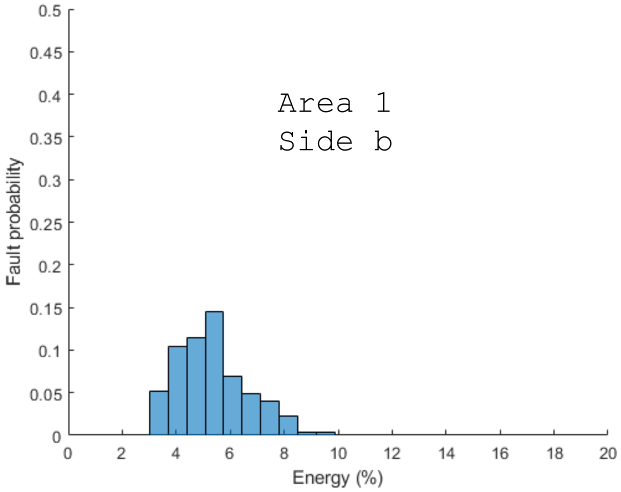


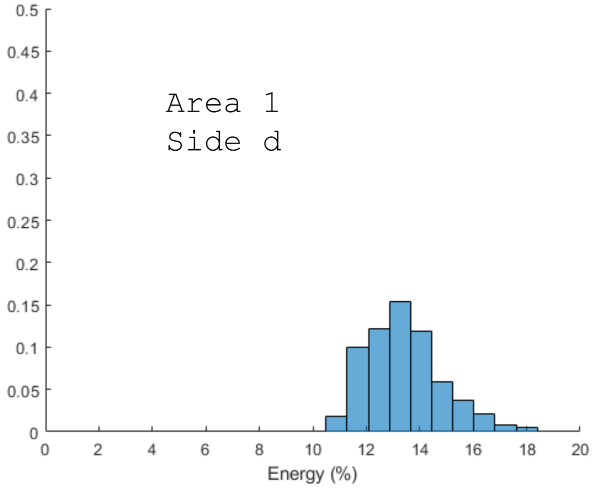
Experimental Results DUT B: Laser Energy Analysis

- Backside requires less minimum energy and has higher probability to get a fault



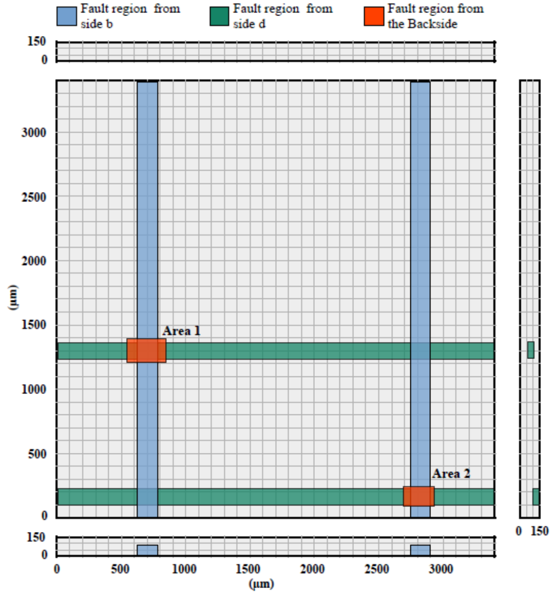




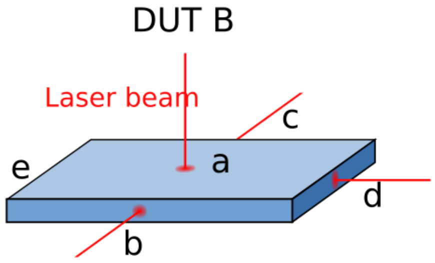


Experimental Results DUT B: Success Rate Analysis

- Success rate lower for the LLFI
- More distance less success rate in area 1. less difference in Area 2.



Exposed side	Success rate, area 1	Success rate, area 2
Backside (LFI)	74.3%	6.6%
Side b (LLFI)	34.1%	2.9%
Side c (LLFI)	0%	0%
Side d (LLFI)	22.1%	2.8%



Experimental Results - Summary

- Experiments showed that LLFI is feasible.

- Faults can be obtained from different sides but sensitive areas converge to the same region as backside => stimulating the same region?

- Not all the sides gave successful results => dependency on distance and circuitry(above) to cross?

- Minimum Energy required for faults is always less for the Backside.

- Fault success rate is better for backside than LLFI. Less distance, better LLFI success rate.

Conclusions

- Most of the **current FI techniques require backside or frontside access**.

- **New packaging techniques and/or countermeasures** will increase the **difficulty** to have **physical access** for FI techniques.

- **LLFI not better** than **backside,** but opens **a new attack surface (the edge)** that needs to be considered when evaluating the security of a chip.

Further Work

- **More experiments** are required in order to **understand** better the behavior of LLFI and **compare** it to backside LFI.

- Interesting to **test** this technique with **3d packaging.**

THANK YOU VERY MUCH FOR YOUR ATTENTION

Questions?

Contact details:

Jordi Mujal (Jordi.Mujal@applus.com)

Applus+ Laboratories
Campus UAB
Ronda de la Font del Carme s/n
08193 Bellaterra, Barcelona
T: +34 93 567 20 00
F: +34 93 567 20 01