LCIS
Laboratoire de Conception
et d'Intégration des Systèmes

Linksium
technology transfer & startup building
Grenoble Alpes

EDA4SEC

Pre-Silicon Security Evaluation

Johan MARCONOT, David HELY (LCIS)
Gisela SCHACH (Linksium)

Lille, 8 September 2021

Cybersecurity Institute
Université Grenoble Alpes

FIC 2021

GRENOBLE INP
UGA

EDA4SEC

Technology Transfer from the Lab

LCIS

Laboratoire de Conception
et d'Intégration des Systèmes

- Embedded system laboratory from Grenoble Alpes University
- Security from hardware to software, attack and countermeasure
- Solution, tool and methods for the industry needs => EDA4Sec

60
RESEARCHERS

220
PEER-REVIEWED
ARTICLES

13
COLLABORATIVE
PROJECTS

700
CONFERENCE
PAPERS

Linksium

technology transfer & startup building
Grenoble Alpes

- Accelerating innovation from public research
- Funding for emerging technologies from the labs
- Facilitating transfer to industry
- Creating deeptech startups in the Alpes

59
STARTUPS
created

191
TECHNOLOGY TRANSFER
projects

45
M€
invested

165
PATENTS
leveraged by projects

Agenda

1. Hardware security issues in IC conception
2. Focus on fault attack evaluation
3. EDA4Sec : a software tool providing probabilistic analysis and automated countermeasures early in the design flow

Growing Concern in Industry

63% of companies have been targeted in 2019 by hackers through hardware or silicon-level vulnerability

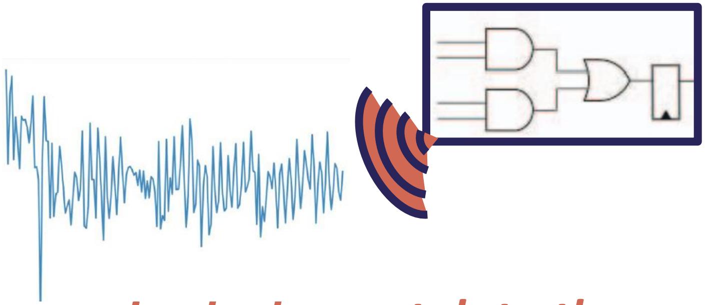
70% are unsatisfied of the silicon-level security offered by their hardware vendors

*Investigation carried out by Forrester, interviews were conducted with decision makers for 307 companies.
https://www.delltechnologies.com/en-us/endpoint-security/index.htm#scroll=off&overlay=/en-us/collaterals/unauth/analyst-reports/solutions/dell-bios-security-the-next-frontier-for-endpoint-protection.pdf

Hardware Attacks

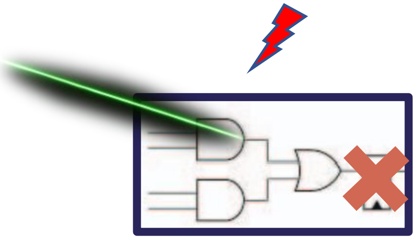
- Over hundred methods to compromise IC security through physical vulnerability are reported today
  - Mainly due to lack of security integration during the IC design flow

Side channel attack



Leaked secret data through power, timing or EM analysis (even photon or heat dissipation)

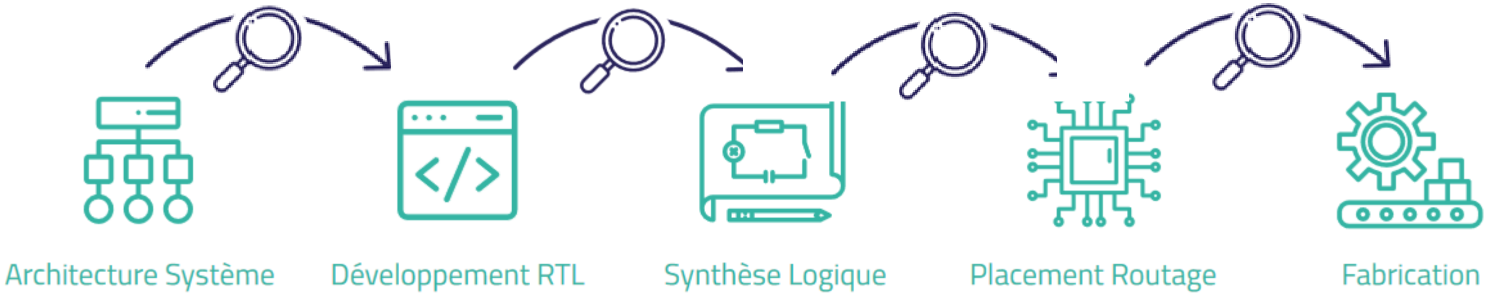
Fault injection attack



Provoke errors in systems' security protocol or critical functions (often exploitable faulty result or behavior)

Security Challenge for Conventional EDA tools

- Functional and parametric verification, performance optimization
  - Provided by conventional tools (Mentor, Synopsys, Defacto)

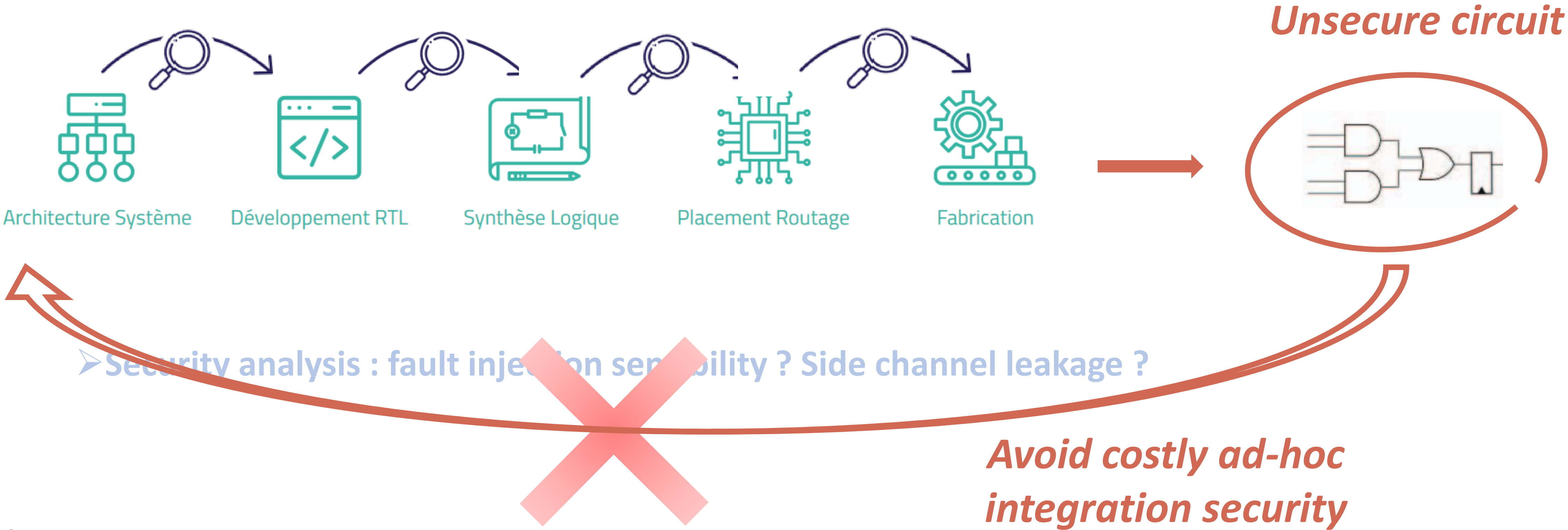


- **Security characterization against real-world vulnerabilities**
  - **Fault injection sensibility ? Side channel leakage ?**

**Electronic Design Automation*

Security Challenge for Conventional EDA tools

- Functional and parametric verification, performance optimization
  - Provide by classic tools (Mentor, Synopsys, Defacto)



Unsecure circuit

- **Security analysis : fault injection sensibility ? Side channel leakage ?**

Avoid costly ad-hoc integration security

**Electronic Design Automation*

Agenda

1. Hardware security issues in IC conception

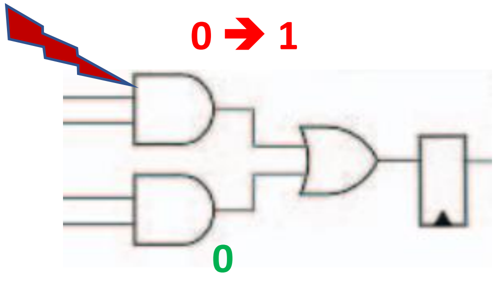
2. Focus on fault attacks evaluation

3. EDA4Sec : a software tool providing probabilistic analysis and automated countermeasures early in the design flow

Fault Attack Problems

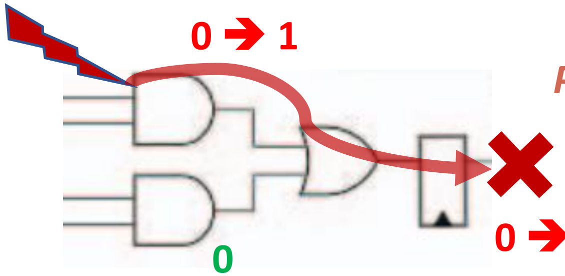
- One fault, at the right moment onto a critical signal can break IC security
  - Several means : laser, clock glitch, power glitch, EM…

Fault injection impacting an output value



Fault Attack Problems

- One fault, at the right moment onto a critical signal can break IC security
  - Several means : laser, clock glitch, power glitch, EM…



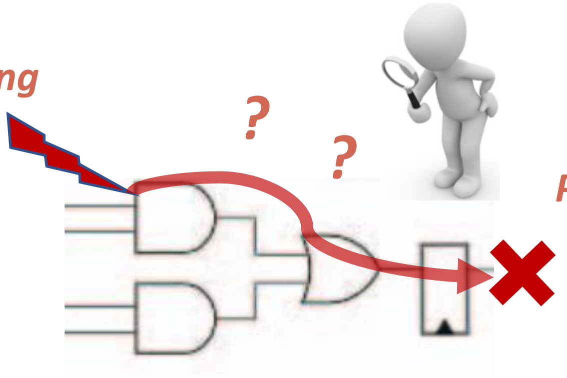
Fault injection impacting an output value

Propagation to the register (flip flop)

- Modify the status of **critical** register used in security protocol : authentication, right access management, ciphering…

Fault Attack Problems

- One fault, at the right moment onto a critical signal can break IC security
  - Several means : laser, clock glitch, power glitch, EM…



Fault injection impacting an output value

Propagation to the register (flip flop)

- Modify the status of **critical** register used in security protocol : authentication, right access management, ciphering…
- Can be **undetected** during algorithm execution

Fault Attack Problems

- One fault, at the right moment onto a critical signal can break IC security
  - Several means : laser, clock glitch, power glitch, EM…

Fault injection impacting

Propa
regist

Which logic part is sensitive to fault injection ?

Is there a risk of fault propagation ? What is the impact of the attack ?

- Modify the status of critical register used i n,
  t, ciphering…
  g algorithm execu

Which registers are manipulating critical data ?

How to detect the errors due to fault injection ?

Fault Attack Problems

- One fault, at the right moment onto a critical signal can break IC security
  - Several means : laser, clock glitch, power glitch, EM…

Fault injection impacting

Propa
regist

Which logic part is sensitive to fault injection ?

Is there a risk of fault propagation ? What is the impact of the attack ?

- Modify the status of critical register used i n,
t, ciphering…
g algorithm execu

Which registers are manipulating critical data ?

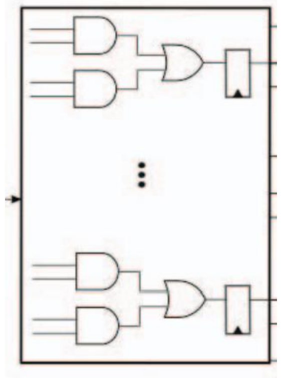
How to detect the errors due to fault injection ?

Fault Attack Evaluation : Current Solutions

- Simulator tool evaluate the random fault scenario impacts
  - As a current practice in EDA software
  - Identify and observe the fault effects

Sig0 :
00110101

Sig1 :
10101110



✗

✓

Fault list establishment

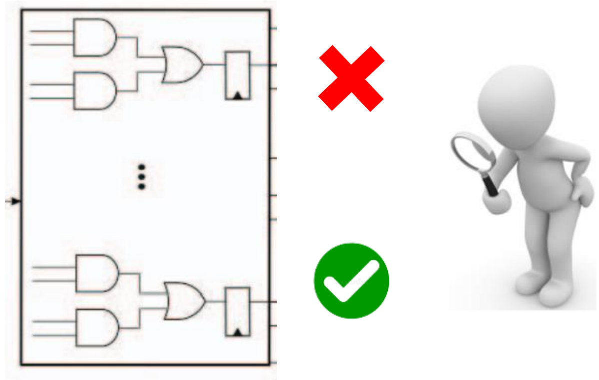
- Fault condition (input signal, fault type)
- Impacted outputs

Fault Attack Evaluation : Current Solutions

- Simulator tool evaluate the random fault scenario impacts
  - As a current practice in EDA software
  - Identify and observe the fault effects

Sig0 :
00110101

Sig1 :
10101110



Fault list establishment

- Fault condition (input signal, fault type)
- Impacted outputs

Challenge

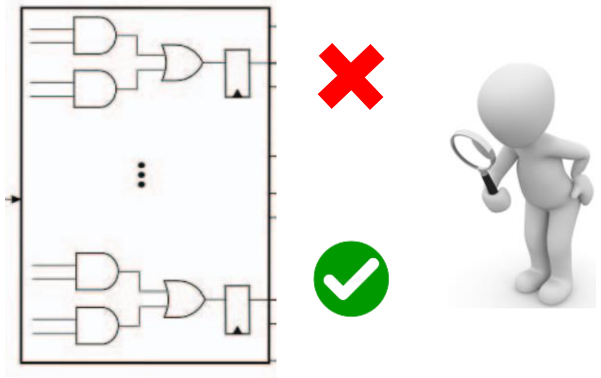
- Very time consuming for large design
- Lack of sensitivity metrics to characterize the faults

Fault Attack Evaluation : Current Solutions

- Simulator tool evaluate impacts of random fault scenario
  - As a current practice in EDA software
  - Identify and observe the fault effects

Sig0 :
00110101

Sig1 :
10101110



Fault list establishment

- Fault condition (input signal, fault type)
- Impacted outputs

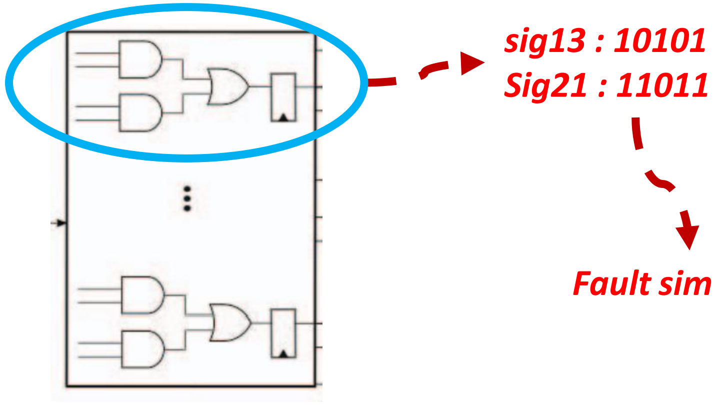
Challenge

- Very time consuming for large design
- Lack of sensitivity metrics to characterize the faults

- Formal engine can verify fault propagation
  - Initially used to property design verification

Fault perimeter is exhaustively evaluated by the formal engine

Sig0 : 00000
Sig1 : 00001
….
SigX : 11111



Verified faults

sig13 : 10101
Sig21 : 11011

Fault simulator

Optimized fault evaluation

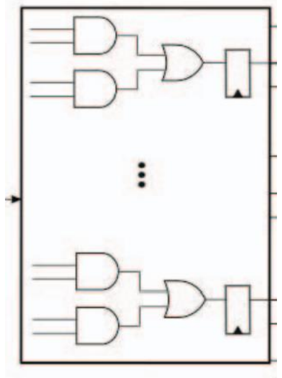
- Exhaustive and correct fault list
- Still face the same challenge for sensitivity

Fault Attack Evaluation : Current Solutions

- Simulator tool evaluate impacts of random fault scenario
  - As a current practice in EDA software
  - Identify and observe the fault effects

Sig0 : 00110101

Sig1 : 10101110



Fault list establishment

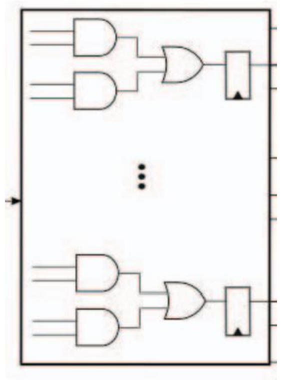
- Fault condition (input signal, fault type)
- Impacted outputs

Challenge

- Formal engine can verify fault propagation
  - Initially used to property design verification

Fault perimeter exhaustively evaluated by formal engine

Sig0 : 00000
Sig1 : 00001
….
SigX : 11111



Verified faults

sig13 : 10101
Sig21 : 11011

Fault simulator

uation

orrect fault list

e challenge for sensitivity

But which logic part is sensitive to fault injection ?

Agenda

1. Security issues in IC conception

2. Focus on fault injections (analysis)

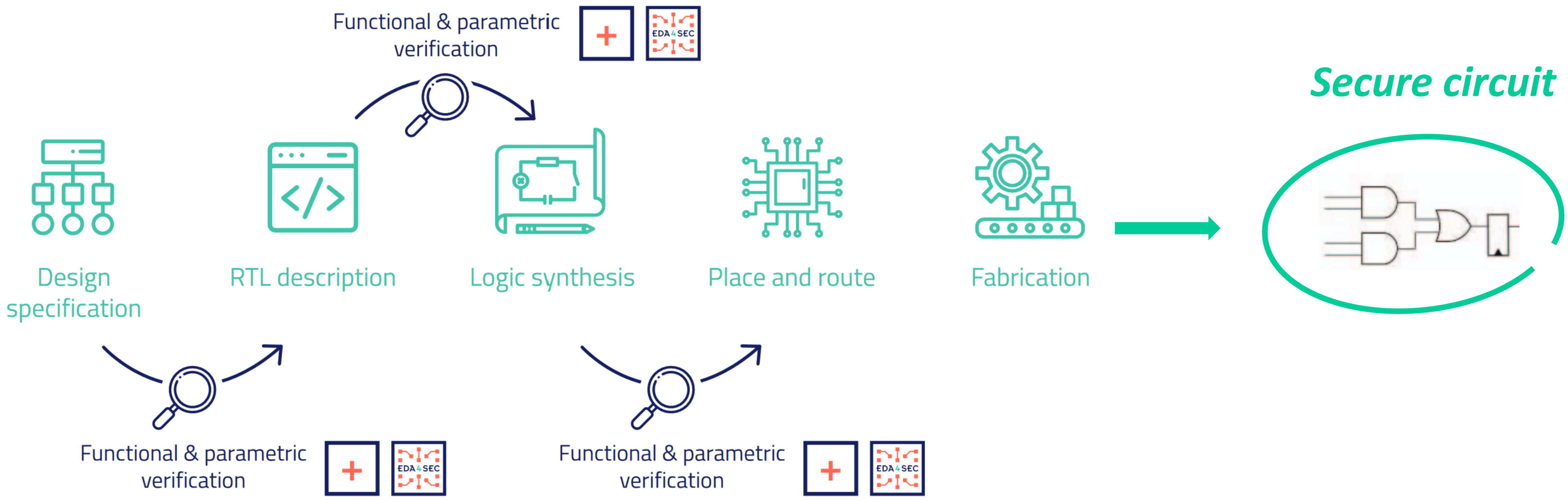
3. EDA4SEC : a software tool providing probabilistic analysis and automated countermeasures early in the design flow

Pre-Silicon Security Evaluation

RESPECTING THE DESIGN FLOW REQUIREMENTS

- Offers structural analysis to identify potential hardware security vulnerabilities
- Positions IC on a sensitivity score
- Runs at various abstraction levels from RTL to gate levels
- Compatible with common EDA design tools

Pre-Silicon Security Evaluation



Functional & parametric verification +

Design specification

RTL description

Logic synthesis

Place and route

Fabrication

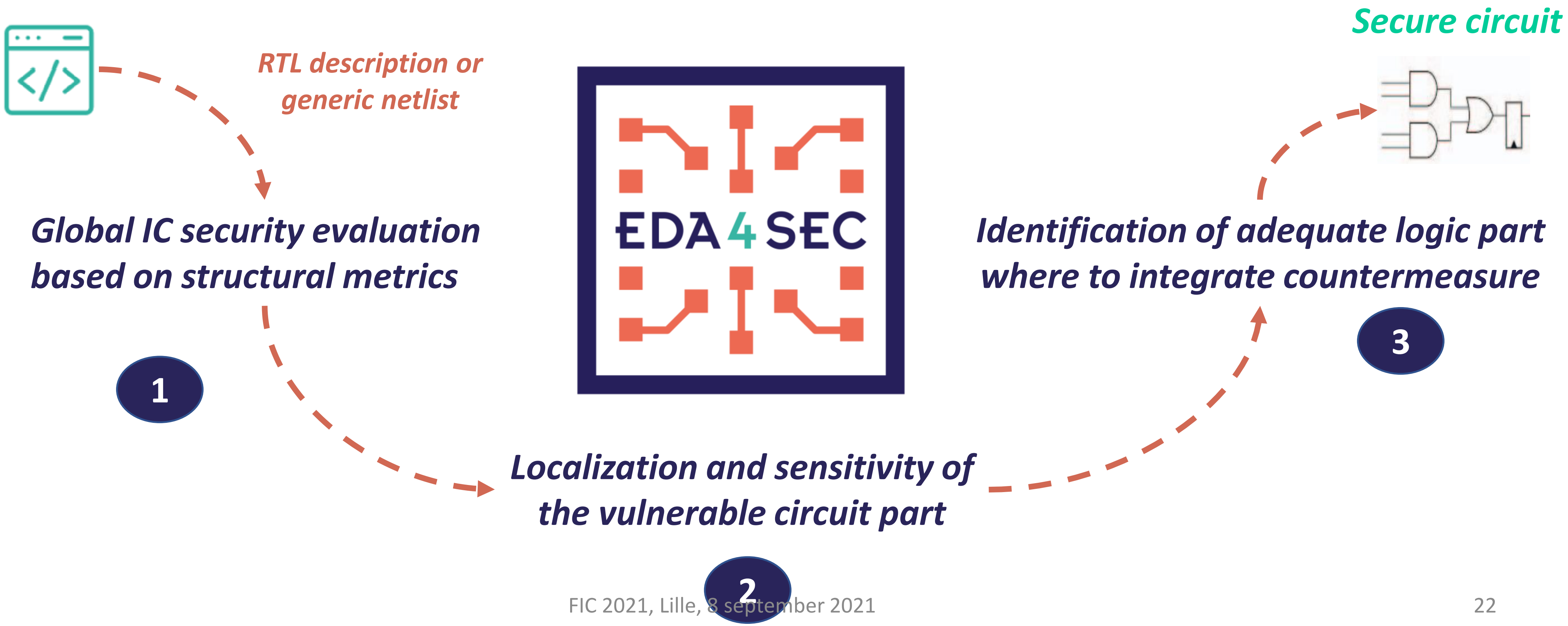
Secure circuit

Functional & parametric verification +

Functional & parametric verification +

Pre-Silicon Security Evaluation

- A software plugin to analyze IC sensitivity to fault injection and localize its vulnerabilities



RTL description or generic netlist

1 *Global IC security evaluation based on structural metrics*

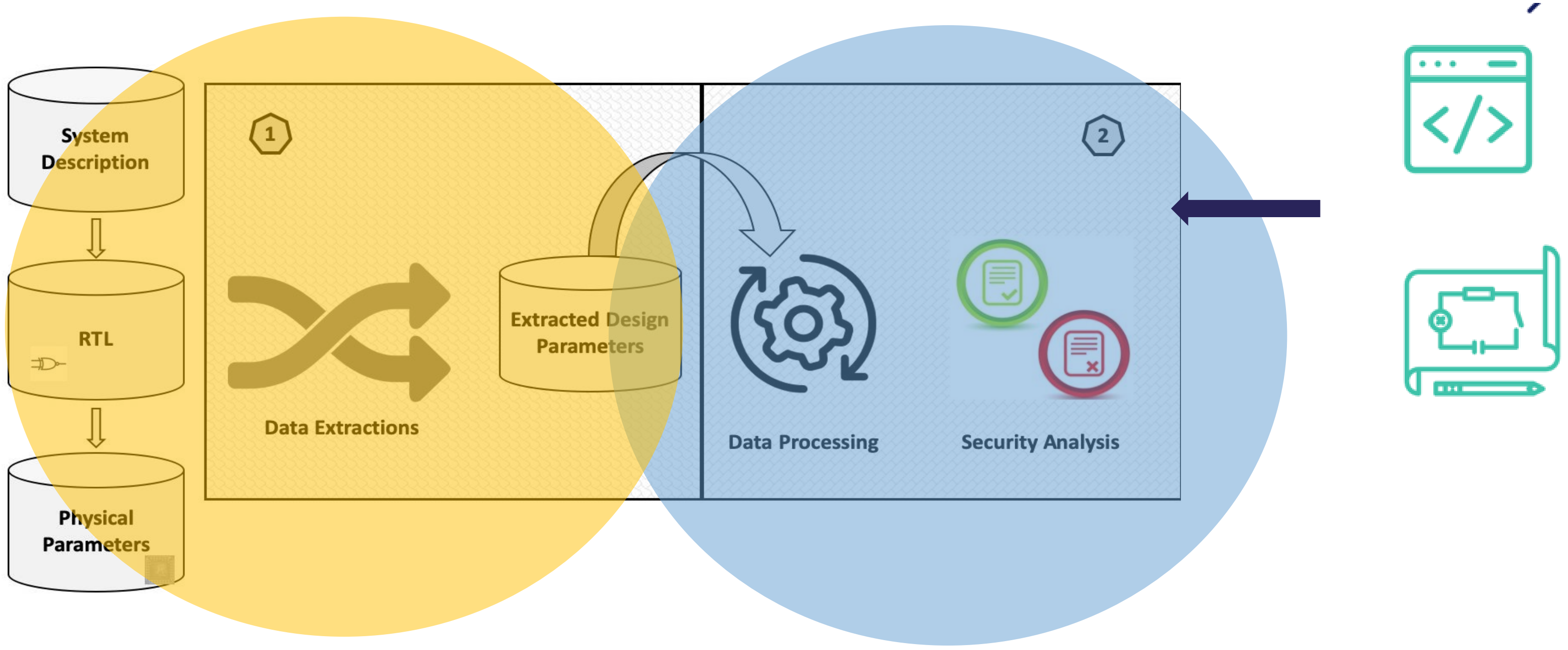
2 *Localization and sensitivity of the vulnerable circuit part*

3 *Identification of adequate logic part where to integrate countermeasure*

Secure circuit

1 – Global IC Security Evaluation

- EDA4Sec focuses on structural metrics provided by EDA tools to analyze the design



VHDL or Verilog design

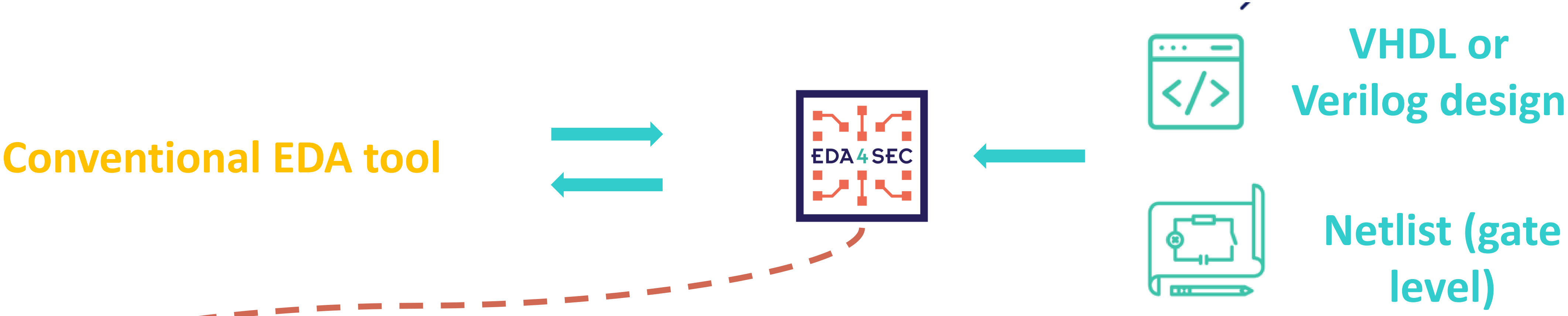
Netlist (gate level)

EDA conventional tools: Synopsys, Mentor, Defacto

EDA4Sec

1 – Global IC Security Evaluation

- EDA4Sec performs the evaluation on the whole IC design (100 % of the circuit)



Conventional EDA tool

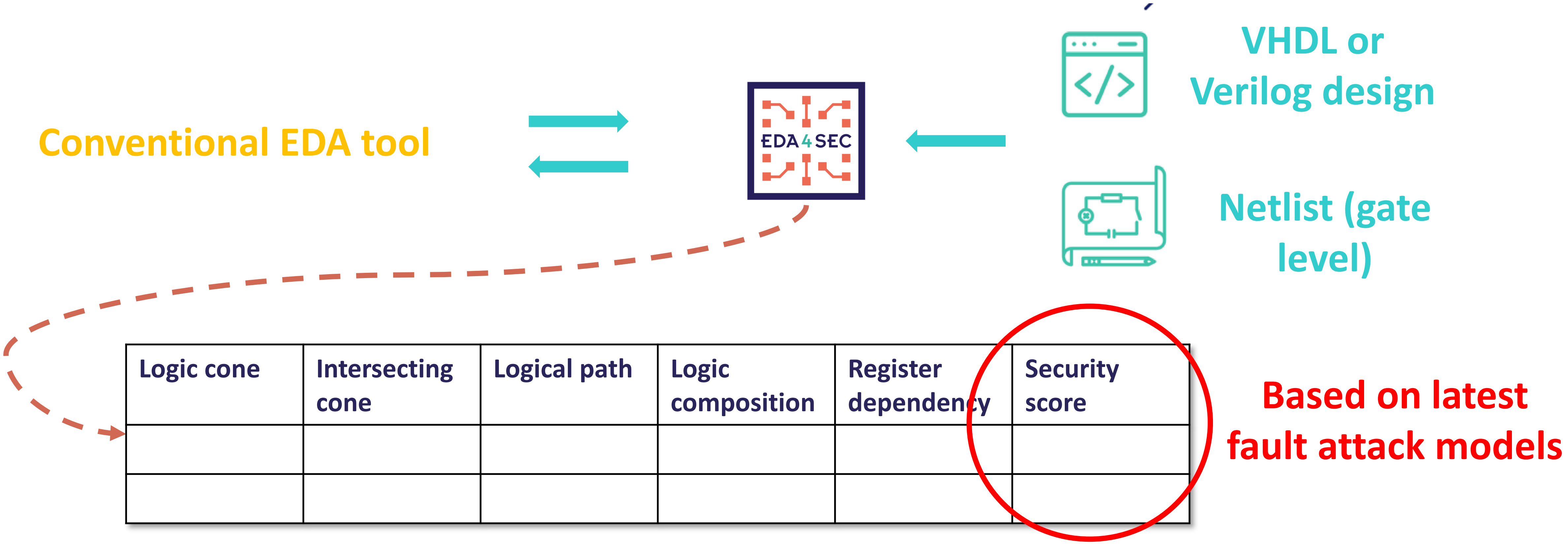
VHDL or Verilog design

Netlist (gate level)

Logic cone	Intersecting cone	Logical path	Logic composition	Register dependency	Security score

1 – Global IC Security Evaluation

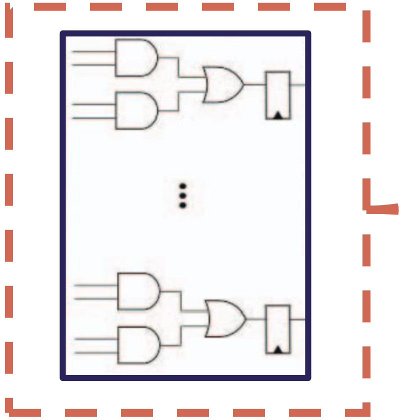
- ➢ EDA4Sec integrates the recent fault attack model to compute security metrics

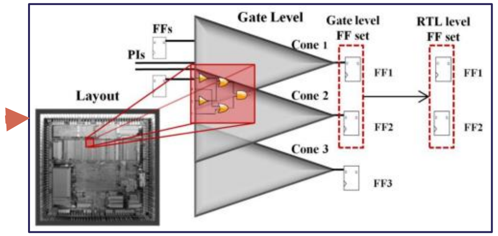


Logic cone	Intersecting cone	Logical path	Logic composition	Register dependency	Security score

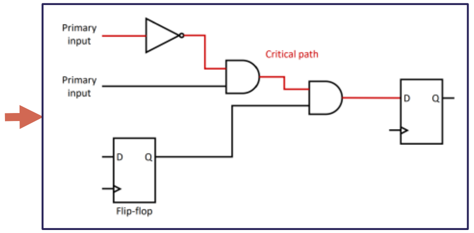
1 – Global IC Security Evaluation

- EDA4Sec performs sensitivity evaluation faced to laser fault injection and clock glitching…





Register ID	Intersection
R1	17 %
R2	11 %
R3	37 %
….	…

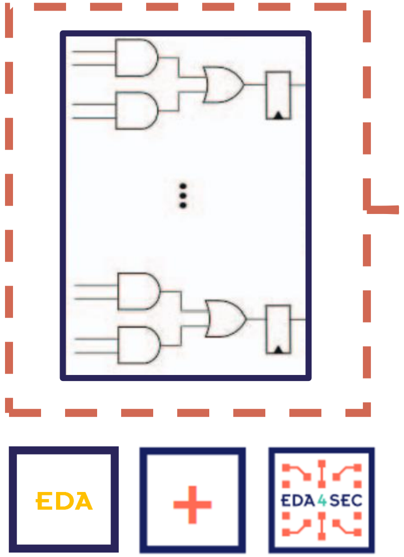


Path ID	Length path
P1	21
P2	39
P3	33
….	….

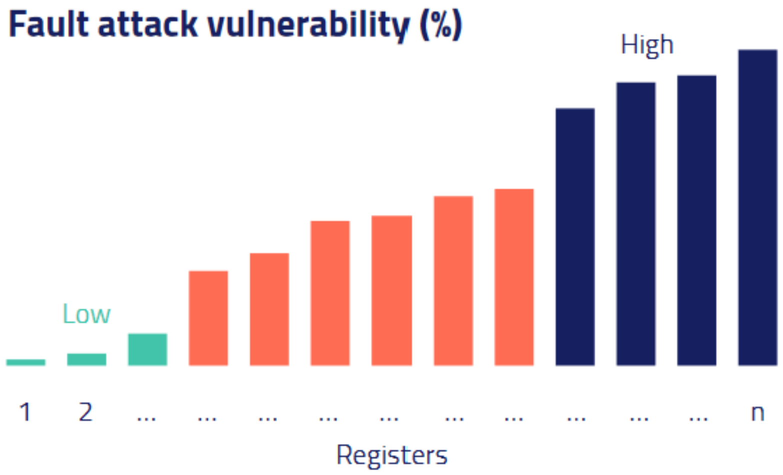
Global IC Security Metric	
Intersection	14 %
Length path	25

2 – Localization and Sensitivity of the Vulnerable Parts of the IC Design

- EDA4Sec provides a full security report and graphic charts to the designer

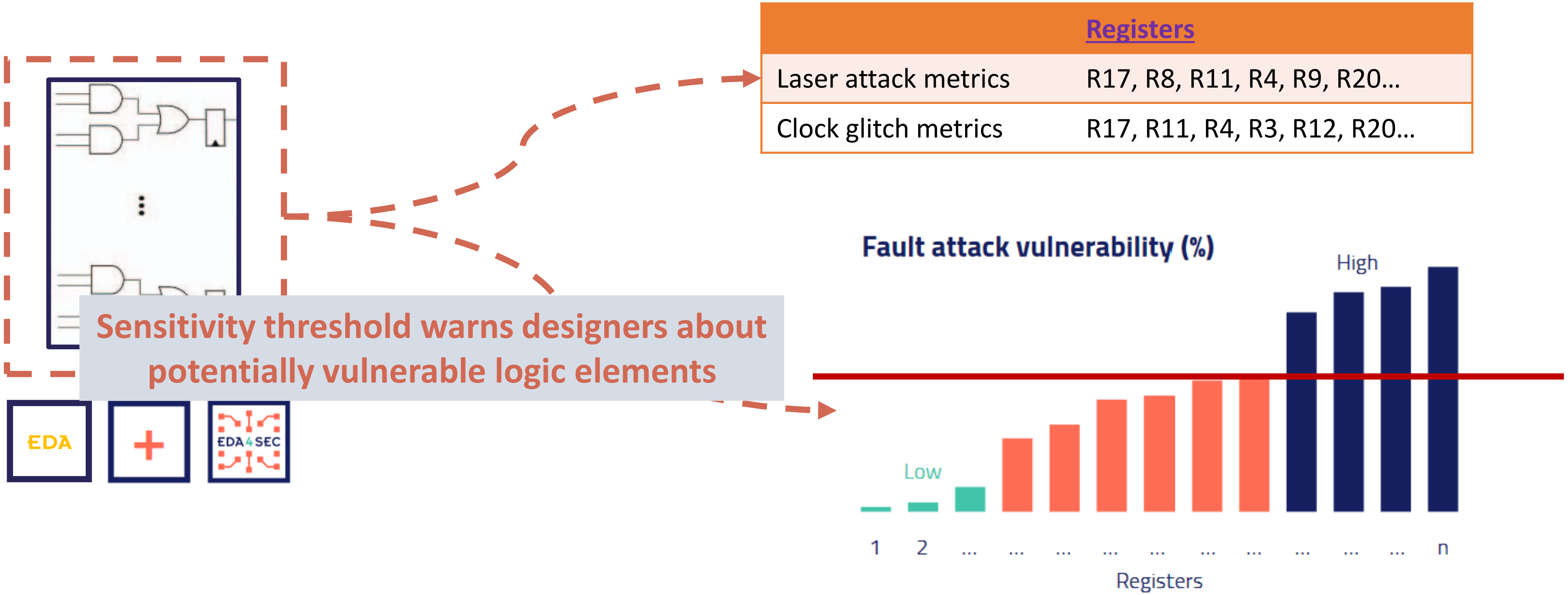


	Registers
Laser attack metrics	R17, R8, R11, R4, R9, R20…
Clock glitch metrics	R17, R11, R4, R3, R12, R20…



2 – Localization and sensitivity of the vulnerable part of the IC design

- ➢ EDA4Sec provides full security report and graphic interface to the designers

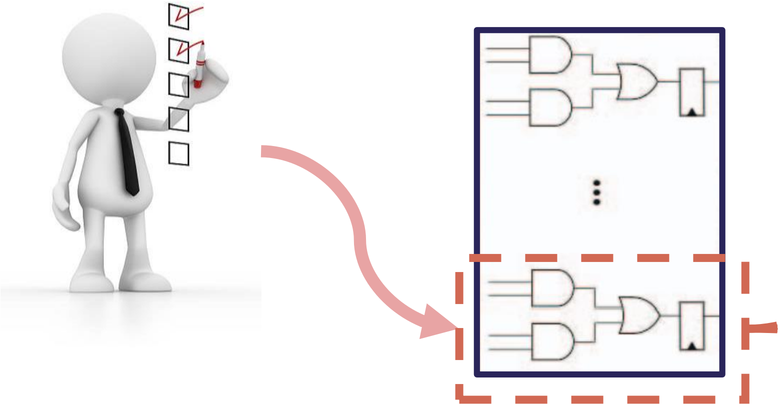


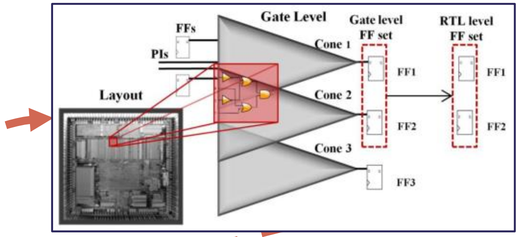
	Registers
Laser attack metrics	R17, R8, R11, R4, R9, R20…
Clock glitch metrics	R17, R11, R4, R3, R12, R20…

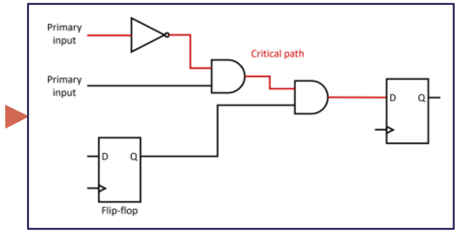
Sensitivity threshold warns designers about potentially vulnerable logic elements

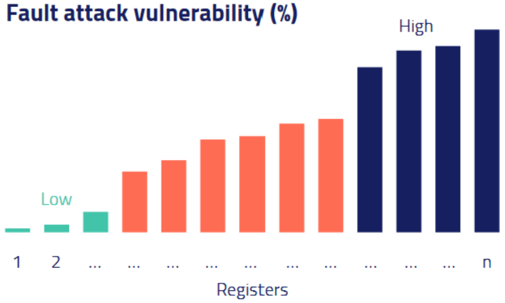
2 – Localization and sensitivity of the vulnerable part of the IC design

- ➢Designer can visualize the sensitivity metrics of any specific register and decides if he wants to improves its security





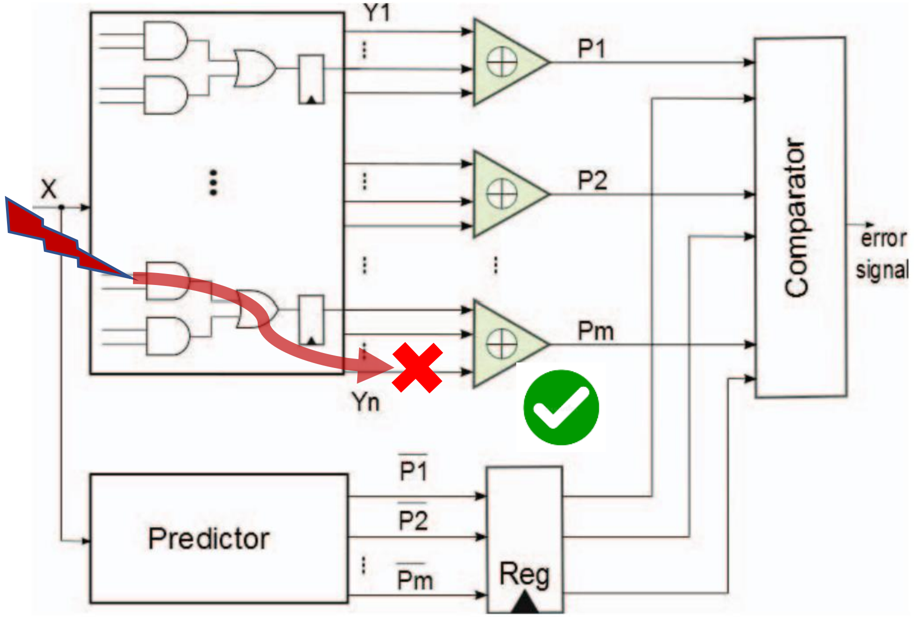




Specific register list		
R17	R11	R4
R20	R8	R9

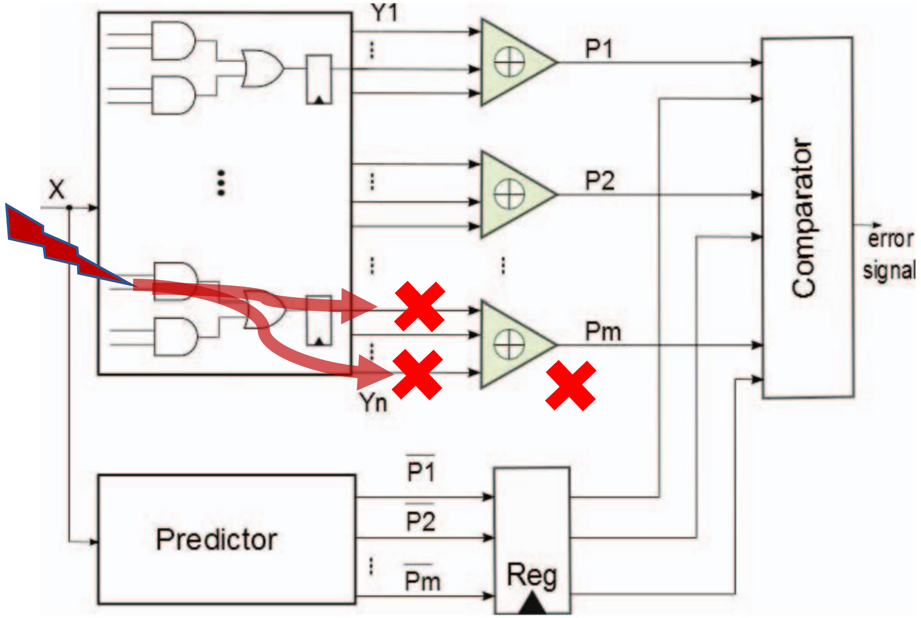
3 – Automated Countermeasure Insertion

- EDA4Sec provides support to integrate an efficient error detection scheme
  - For instance, an approach with parity checksum to this design



3 – Automated Countermeasure Insertion

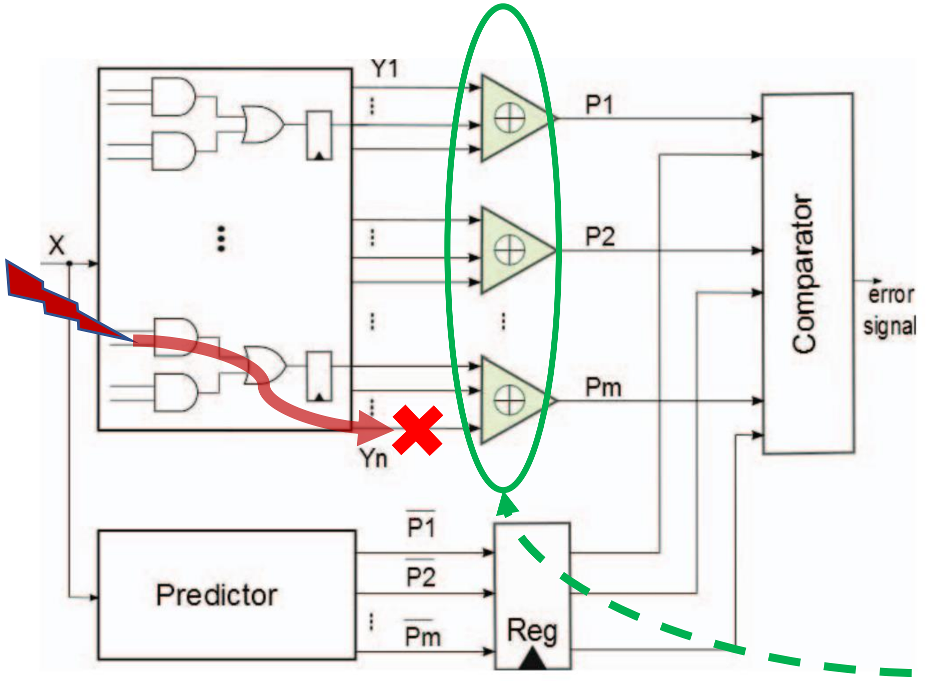
- EDA4Sec provides support to integrate an efficient error detection scheme
    - In this design, the challenge is to find the right combination of register bit parity



Independent register groups ????

3 – Automated Countermeasure Insertion

- EDA4Sec identifies the adequate register groups



Independant register group		
R17	R11	R4
R20	R8	R9

Benefits of EDA4Sec

- **EDA4sec brings benefits to designers who want to integrate security**

	Fault simulator	Formal verification engine	Global EDA4sec analysis
Exhaustivity	- -	+ +	+ +
Vulnerability identification	+ / -	+ / -	+ +
Calculation time	- -	- -	+ +
Risk evaluation	- -	- -	+ +
Countermeasure support	- -	- -	+ +
Easy integration into the design flow	+ +	- -	+ +

Next steps

We are looking for industrial partners …

- ➢Security evaluation of your IC design
- ➢Compatibility test of your EDA tools
- ➢Comparing methods to evaluate security
- ➢Software available for technology transfer

Next steps

We are looking for industrial partners …

- ➢Security evaluation of your IC design
- ➢Compatibility test of your EDA tools
- ➢Comparing methods to evaluate security
- ➢Software available for technology transfer

We are moving forward to deployment of testing platform and new attack models…

Contact us

David Hély

Assistant professor

+33 (0)6 78 40 74 90

David.hely@lcis.Grenoble-inp.fr

Johan Marconot

Research Engineer

+33 (0)7 55 68 84 41

Johan.marconot@lcis.Grenoble-inp.fr

Gisela SCHACH

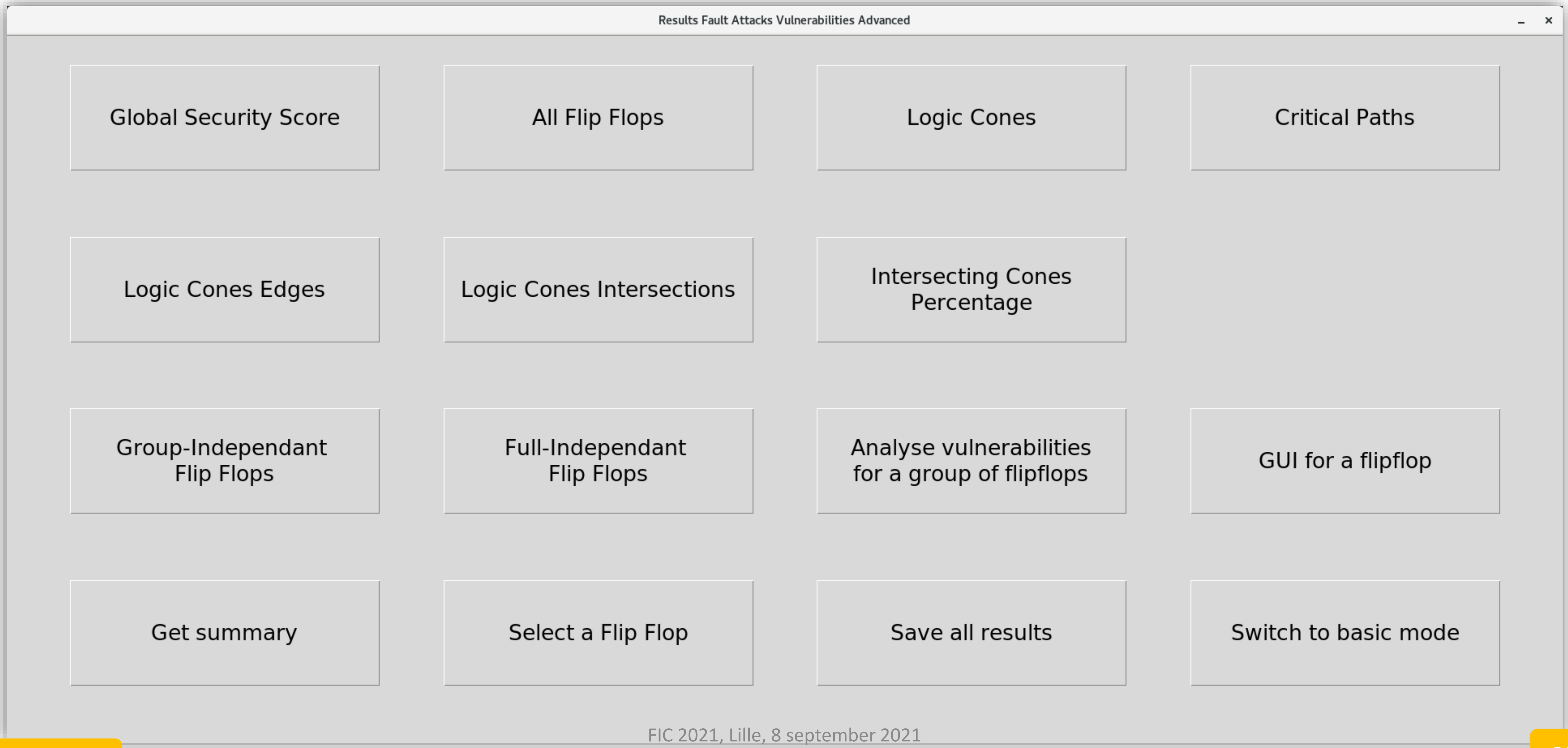
Innovation project manager

+33 (0)6 33 63 44 99

Gisela.Schach@linksium.fr

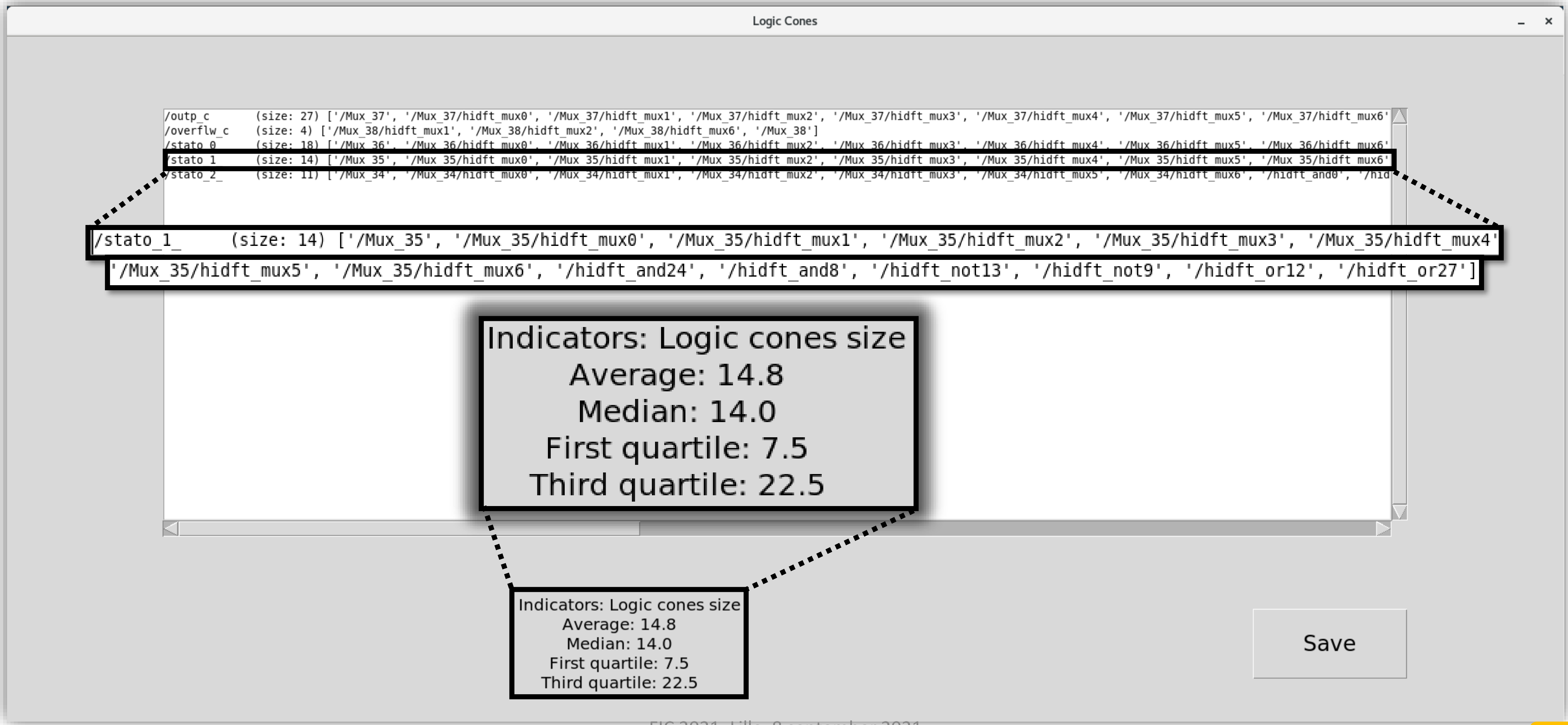
Slides annexes

Fenêtre de résultats – mode avancé



Results Fault Attacks Vulnerabilities Advanced

Fenêtre de résultats – cônes logiques



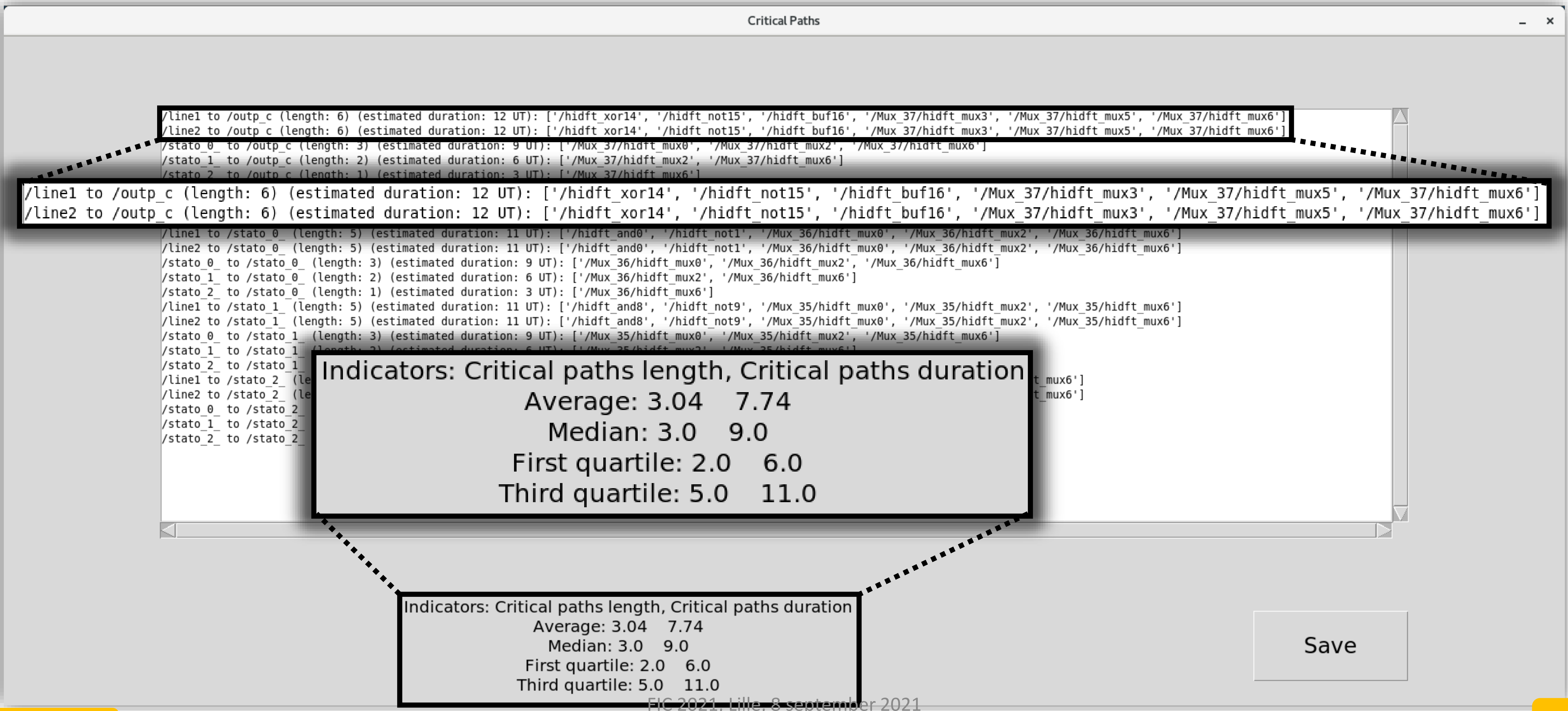
```
/outp_c       (size: 27) ['/Mux_37', '/Mux_37/hidft_mux0', '/Mux_37/hidft_mux1', '/Mux_37/hidft_mux2', '/Mux_37/hidft_mux3', '/Mux_37/hidft_mux4', '/Mux_37/hidft_mux5', '/Mux_37/hidft_mux6'
/overflw_c    (size: 4) ['/Mux_38/hidft_mux1', '/Mux_38/hidft_mux2', '/Mux_38/hidft_mux6', '/Mux_38']
/stato_0      (size: 18) ['/Mux_36', '/Mux_36/hidft_mux0', '/Mux_36/hidft_mux1', '/Mux_36/hidft_mux2', '/Mux_36/hidft_mux3', '/Mux_36/hidft_mux4', '/Mux_36/hidft_mux5', '/Mux_36/hidft_mux6'
/stato_1      (size: 14) ['/Mux_35', '/Mux_35/hidft_mux0', '/Mux_35/hidft_mux1', '/Mux_35/hidft_mux2', '/Mux_35/hidft_mux3', '/Mux_35/hidft_mux4', '/Mux_35/hidft_mux5', '/Mux_35/hidft_mux6'
/stato_2_     (size: 11) ['/Mux_34', '/Mux_34/hidft_mux0', '/Mux_34/hidft_mux1', '/Mux_34/hidft_mux2', '/Mux_34/hidft_mux3', '/Mux_34/hidft_mux5', '/Mux_34/hidft_mux6', '/hidft_and0', '/hid
```

```
/stato_1_     (size: 14) ['/Mux_35', '/Mux_35/hidft_mux0', '/Mux_35/hidft_mux1', '/Mux_35/hidft_mux2', '/Mux_35/hidft_mux3', '/Mux_35/hidft_mux4'
'/Mux_35/hidft_mux5', '/Mux_35/hidft_mux6', '/hidft_and24', '/hidft_and8', '/hidft_not13', '/hidft_not9', '/hidft_or12', '/hidft_or27']
```

Indicators: Logic cones size
Average: 14.8
Median: 14.0
First quartile: 7.5
Third quartile: 22.5

Indicators: Logic cones size
Average: 14.8
Median: 14.0
First quartile: 7.5
Third quartile: 22.5

Fenêtre de résultats – chemin critique



```
/line1 to /outp_c (length: 6) (estimated duration: 12 UT): ['/hidft_xor14', '/hidft_not15', '/hidft_buf16', '/Mux_37/hidft_mux3', '/Mux_37/hidft_mux5', '/Mux_37/hidft_mux6']
/line2 to /outp_c (length: 6) (estimated duration: 12 UT): ['/hidft_xor14', '/hidft_not15', '/hidft_buf16', '/Mux_37/hidft_mux3', '/Mux_37/hidft_mux5', '/Mux_37/hidft_mux6']
/stato_0_ to /outp_c (length: 3) (estimated duration: 9 UT): ['/Mux_37/hidft_mux0', '/Mux_37/hidft_mux2', '/Mux_37/hidft_mux6']
/stato_1_ to /outp_c (length: 2) (estimated duration: 6 UT): ['/Mux_37/hidft_mux2', '/Mux_37/hidft_mux6']
/stato_2_ to /outp_c (length: 1) (estimated duration: 3 UT): ['/Mux_37/hidft_mux6']
/line1 to /stato_0_ (length: 5) (estimated duration: 11 UT): ['/hidft_and0', '/hidft_not1', '/Mux_36/hidft_mux0', '/Mux_36/hidft_mux2', '/Mux_36/hidft_mux6']
/line2 to /stato_0_ (length: 5) (estimated duration: 11 UT): ['/hidft_and0', '/hidft_not1', '/Mux_36/hidft_mux0', '/Mux_36/hidft_mux2', '/Mux_36/hidft_mux6']
/stato_0_ to /stato_0_ (length: 3) (estimated duration: 9 UT): ['/Mux_36/hidft_mux0', '/Mux_36/hidft_mux2', '/Mux_36/hidft_mux6']
/stato_1_ to /stato_0_ (length: 2) (estimated duration: 6 UT): ['/Mux_36/hidft_mux2', '/Mux_36/hidft_mux6']
/stato_2_ to /stato_0_ (length: 1) (estimated duration: 3 UT): ['/Mux_36/hidft_mux6']
/line1 to /stato_1_ (length: 5) (estimated duration: 11 UT): ['/hidft_and8', '/hidft_not9', '/Mux_35/hidft_mux0', '/Mux_35/hidft_mux2', '/Mux_35/hidft_mux6']
/line2 to /stato_1_ (length: 5) (estimated duration: 11 UT): ['/hidft_and8', '/hidft_not9', '/Mux_35/hidft_mux0', '/Mux_35/hidft_mux2', '/Mux_35/hidft_mux6']
/stato_0_ to /stato_1_ (length: 3) (estimated duration: 9 UT): ['/Mux_35/hidft_mux0', '/Mux_35/hidft_mux2', '/Mux_35/hidft_mux6']
/stato_1_ to /stato_1_ (length: 2) (estimated duration: 6 UT): ['/Mux_35/hidft_mux2', '/Mux_35/hidft_mux6']
/stato_2_ to /stato_1_
/line1 to /stato_2_ (le                                                                              t_mux6']
/line2 to /stato_2_ (le                                                                              t_mux6']
/stato_0_ to /stato_2_
/stato_1_ to /stato_2_
/stato_2_ to /stato_2_
```

```
/line1 to /outp_c (length: 6) (estimated duration: 12 UT): ['/hidft_xor14', '/hidft_not15', '/hidft_buf16', '/Mux_37/hidft_mux3', '/Mux_37/hidft_mux5', '/Mux_37/hidft_mux6']
/line2 to /outp_c (length: 6) (estimated duration: 12 UT): ['/hidft_xor14', '/hidft_not15', '/hidft_buf16', '/Mux_37/hidft_mux3', '/Mux_37/hidft_mux5', '/Mux_37/hidft_mux6']
```

```
Indicators: Critical paths length, Critical paths duration
Average: 3.04    7.74
Median: 3.0    9.0
First quartile: 2.0    6.0
Third quartile: 5.0    11.0
```

```
Indicators: Critical paths length, Critical paths duration
Average: 3.04    7.74
Median: 3.0    9.0
First quartile: 2.0    6.0
Third quartile: 5.0    11.0
```