

DE LA RECHERCHE À L'INDUSTRIE



INSPIRING INNOVATION | INNOVANTE PAR TRADITION



TRUDEVICE



Analysis of a fault injection mechanism related to voltage glitches using an on-chip voltmeter

Loïc ZUSSA

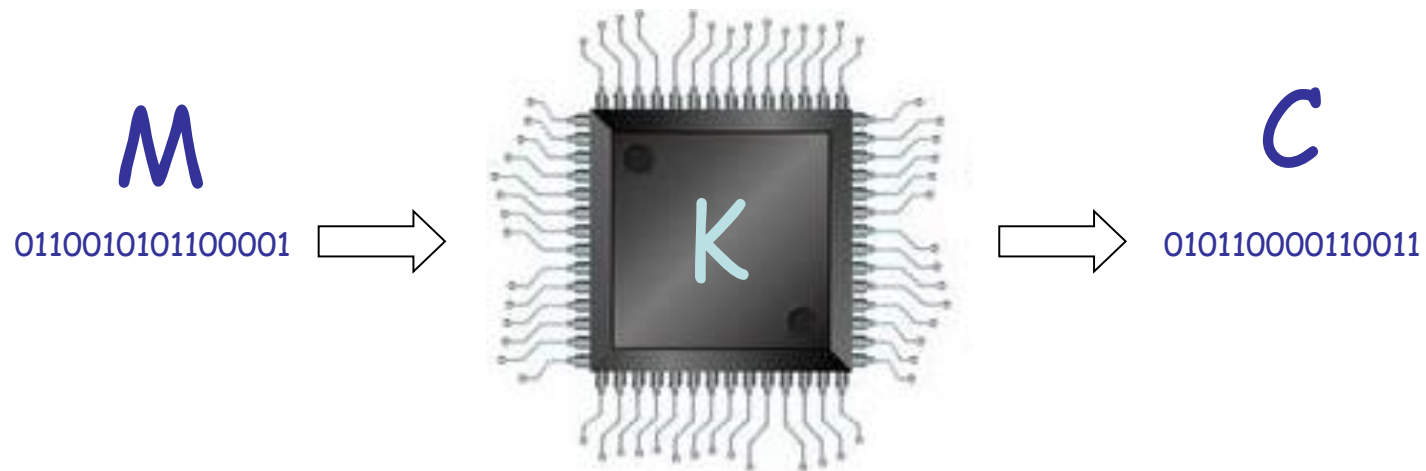
Jean-Max DUTERTRE

Jessy CLEDIERE

Bruno ROBISSON



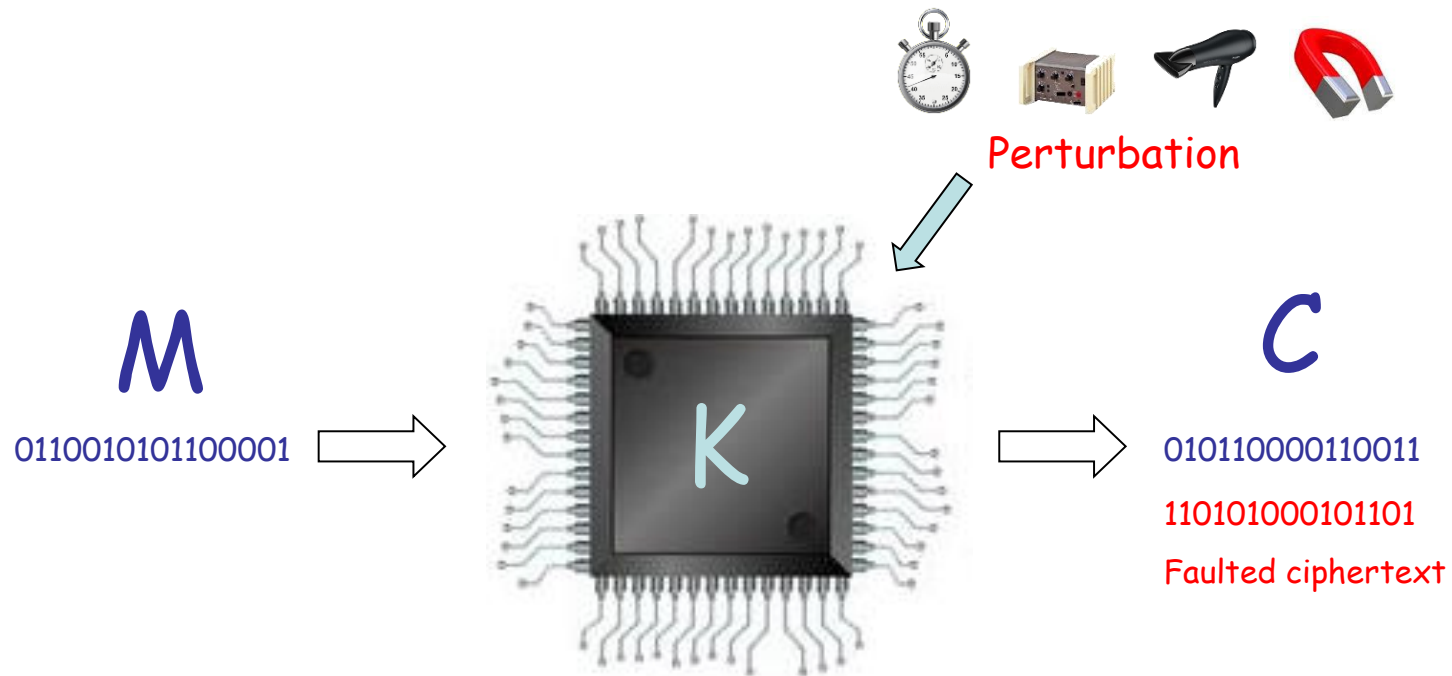
Thesis works





Thesis works

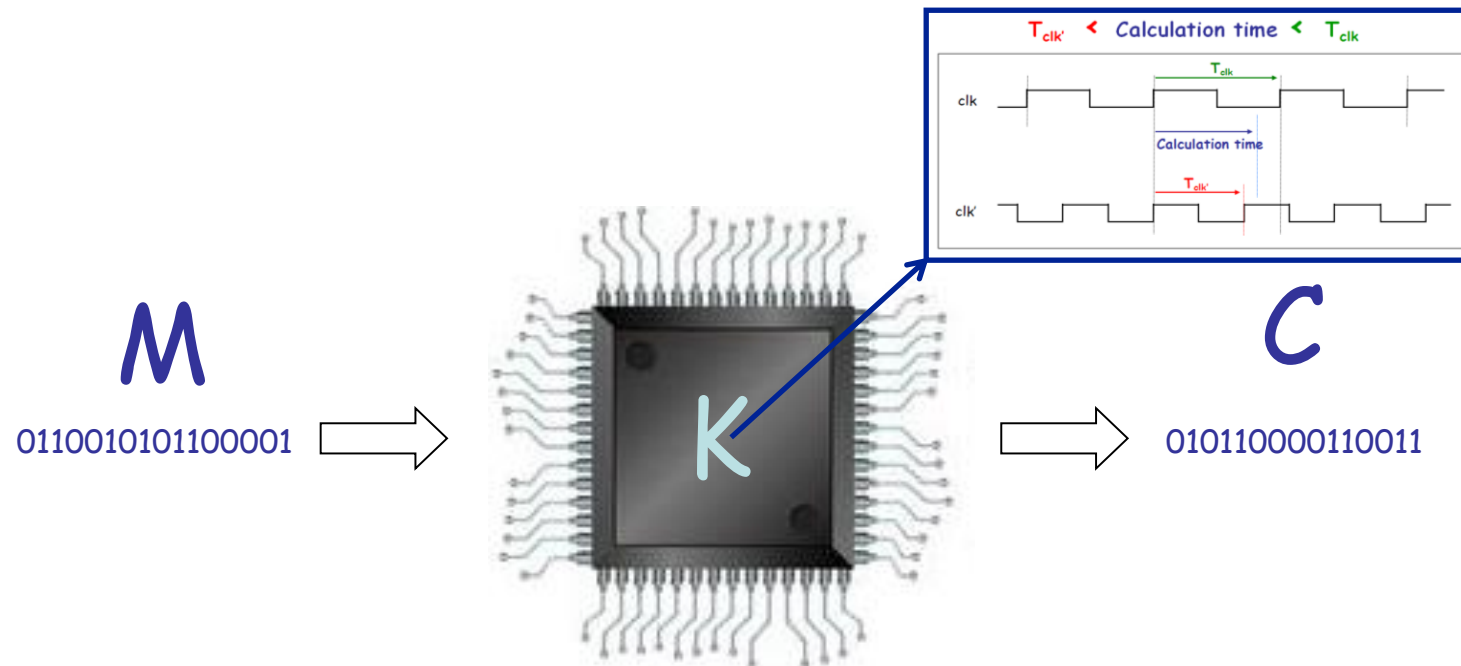
- **Non-invasive** fault injections





Thesis works

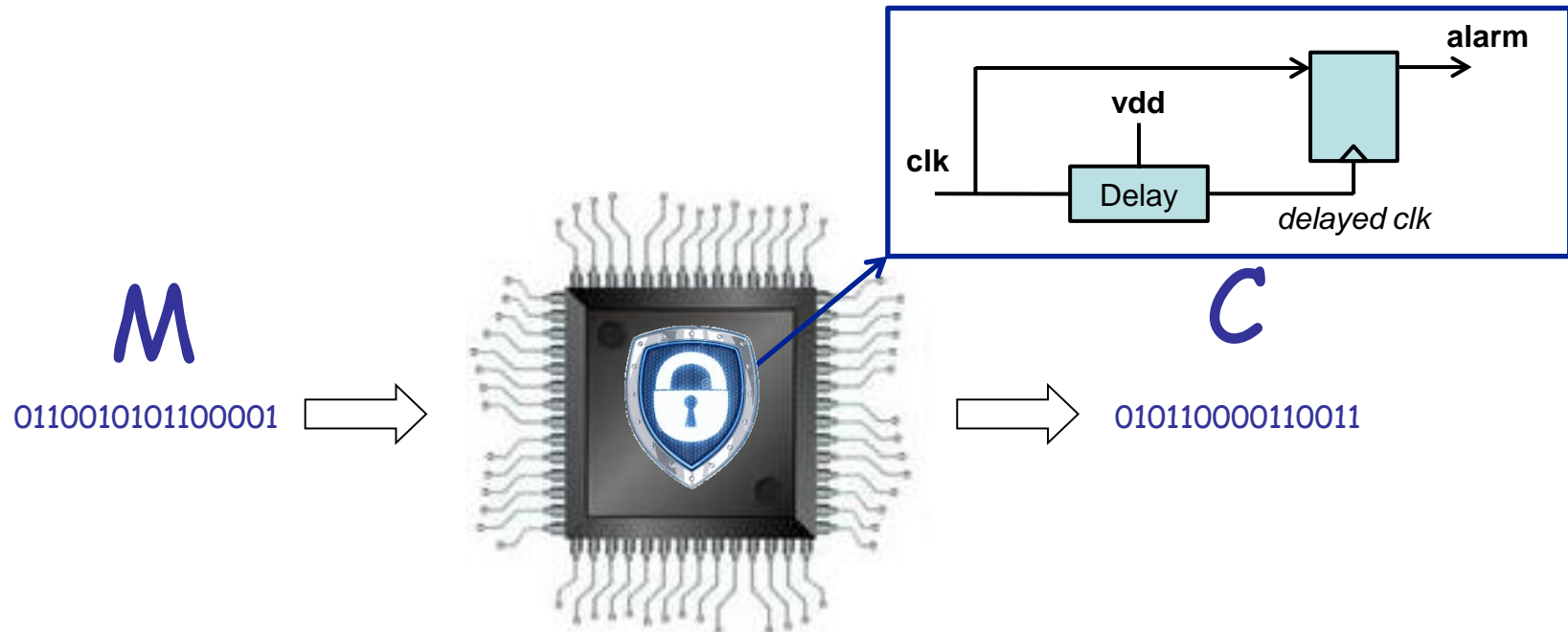
- **Non-invasive** fault injections
- Analysis of an injection mechanism: **timing constraints violation**





Thesis works

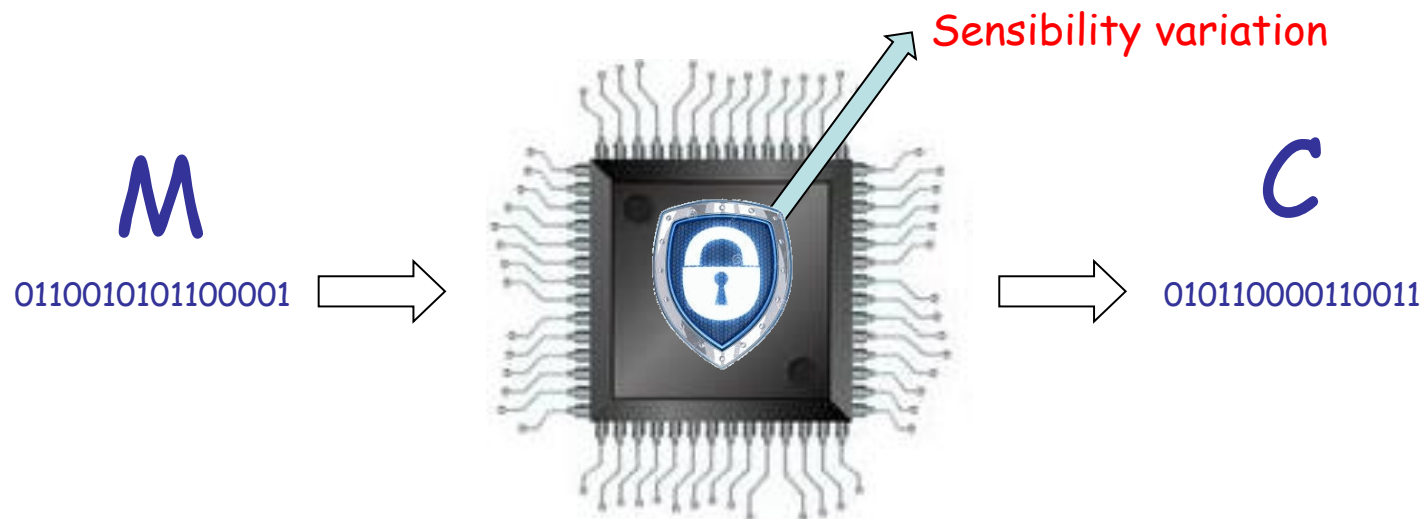
- **Non-invasive** fault injections
- Analysis of an injection mechanism: **timing constraints violation**
- Design, analysis and improvement of a **counter-measure**





Thesis works

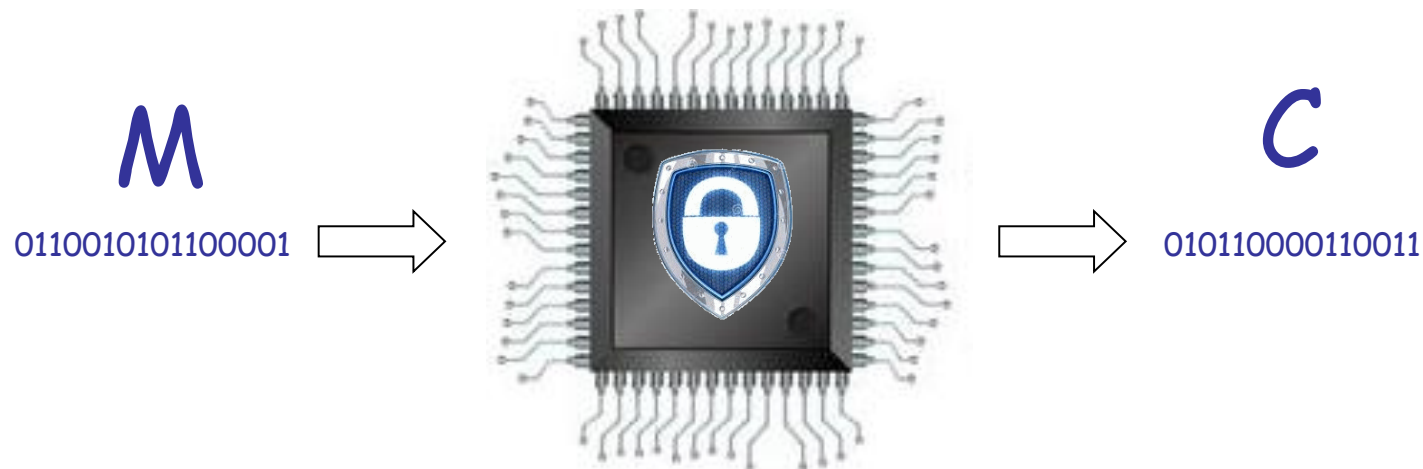
- **Non-invasive** fault injections
- Analysis of an injection mechanism: **timing constraints violation**
- Design, analysis and improvement of a **counter-measure**
- Study of **new vulnerabilities** induced by the **counter-measure** (side channel)





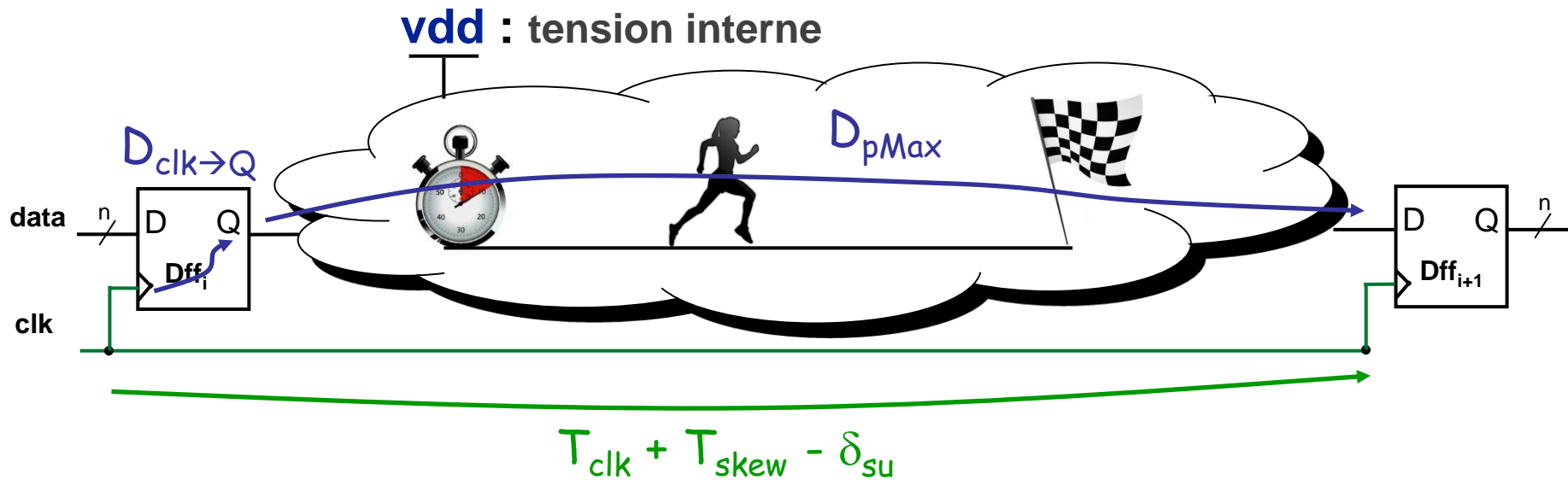
In this presentation

- **Non-invasive** fault injections
- Analysis of an injection mechanism: **timing constraints violation**
- Design, analysis and improvement of a **counter-measure**
- Study of **new vulnerabilities** induced by the **counter-measure** (side channel)





Timing constraints



$D_{clk \rightarrow Q}$: required time for register's output to be updated

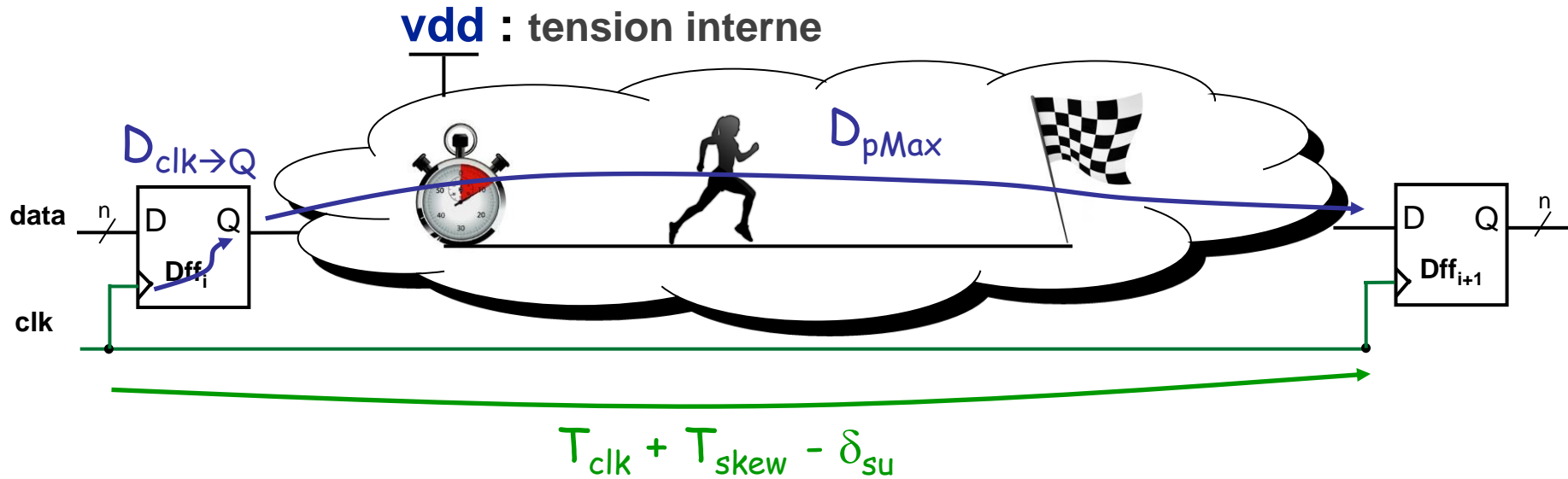
D_{pMax} : data propagation time through the logic

T_{clk} : clock period T_{skew} : little phase distance between two clocks

δ_{su} : setup time : the data have to be stable during this amount of time before the next clock rising edge



Timing constraints violation



$$T_{clk} > D_{clk \rightarrow Q} + D_{pMax} - T_{skew} + \delta_{su}$$

If D_{pMax} increase a fault could be injected :

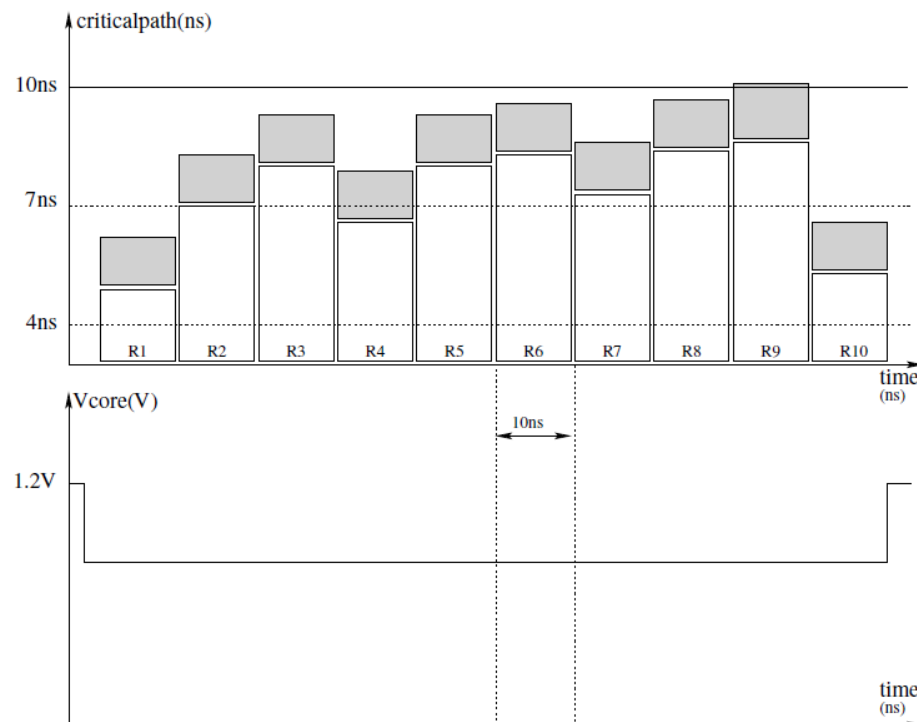
$$T_{clk} < D_{clk \rightarrow Q} + D_{pMax} - T_{skew} + \delta_{su}$$



Static injections

Static under-powering leads to **timing constraint violation** by increasing the calculation times of all the calculation rounds

- Identical faults injected on an **AES** using overclocking and underpowering



Note :

Underpowering the circuit make the **calculation times longer**

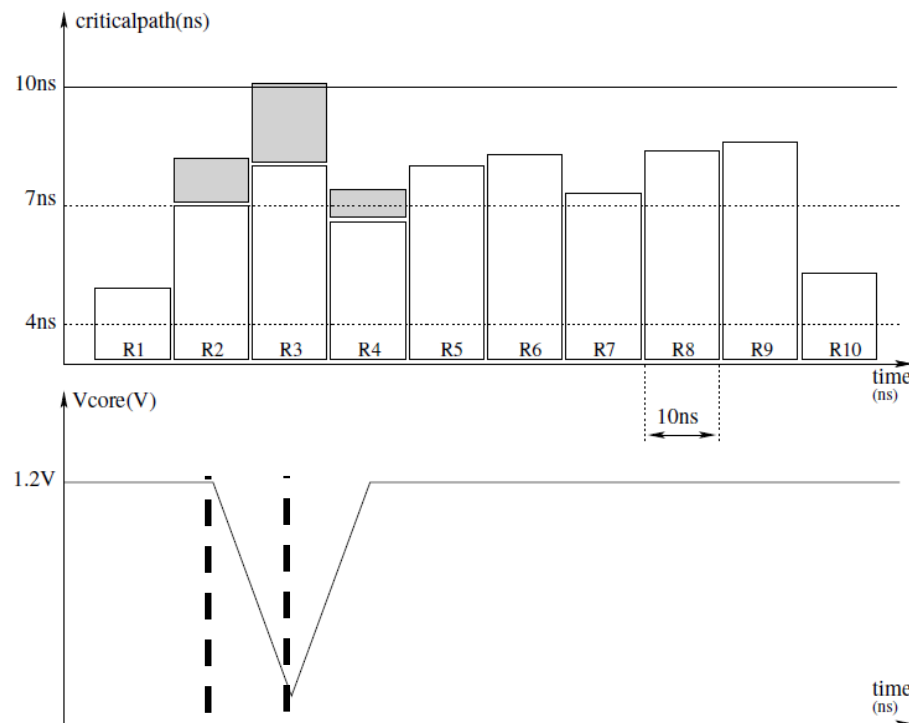
A fault is injected in the most critical one due to timing constraint violation



Dynamic injections

Transient under-powering also leads to **timing constraint violation** by increasing the calculation time of **a specific round**

- Identical faults injected on an **AES** using clock and negative voltage glitches



Note :

Most of the time a fault is injected in the targeted round due to timing constraint violation



Low temporal accuracy
due to signal filtering



Motivations

Transient over-powering also leads to **FAULTS injection**
But it **seems inconsistent** with **timing constraint violation**



On-chip Voltmeter :

- To observe the voltage **inside the circuit**
- To understand the **fault injection mechanism related to positive voltage glitches**

“Sensing nanosecond-scale voltage attacks and natural transients in FPGAs” - FPGA 2013

ZICK Kenneth M. ; SRIVASTAV, Meeta ; ZHANG, Wei



Agenda

- **Voltmeter**
Principle and implementation
- **Internal disturbances observation**
Fault injection characterization
- **Internal disturbances shaping**
Fault injection improvement
- **Conclusion**

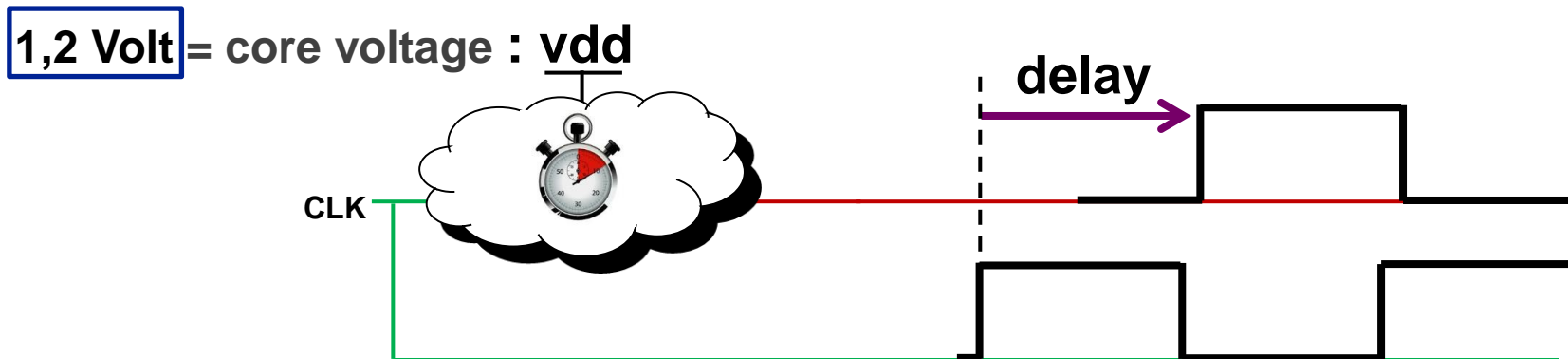




A delay-meter

Propagation times increase when the **core voltage decreases**

Measuring a propagation time **is equivalent** to measuring the core voltage

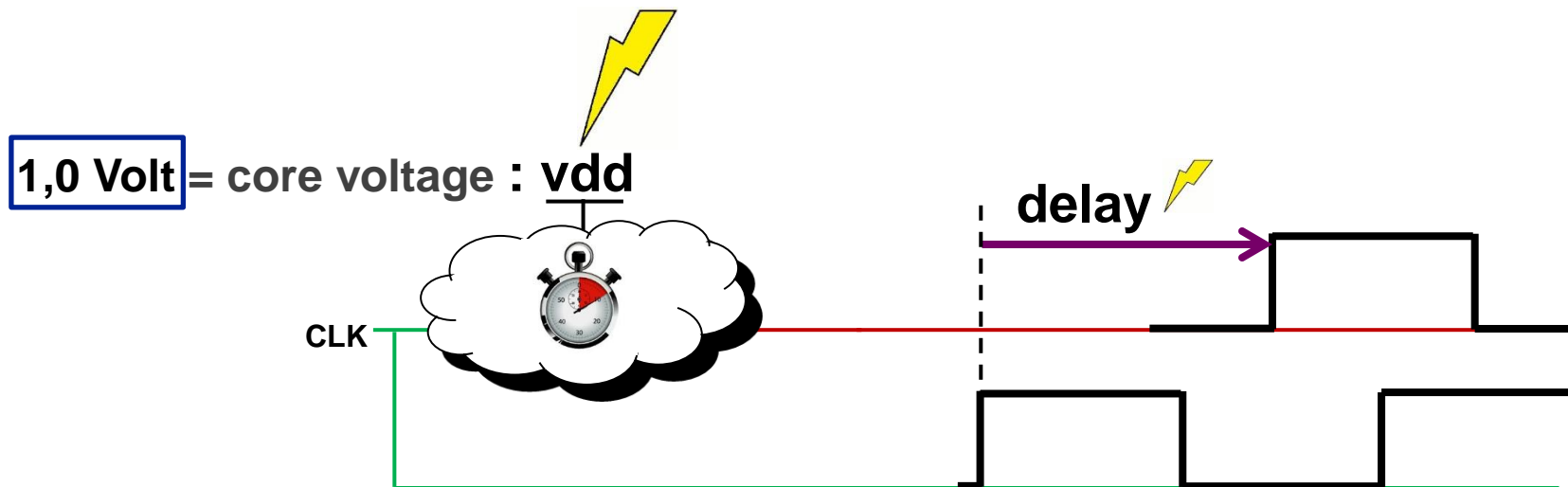




A delay-meter

Propagation times increase when the **core voltage decreases**

Measuring a propagation time **is equivalent** to measuring the core voltage

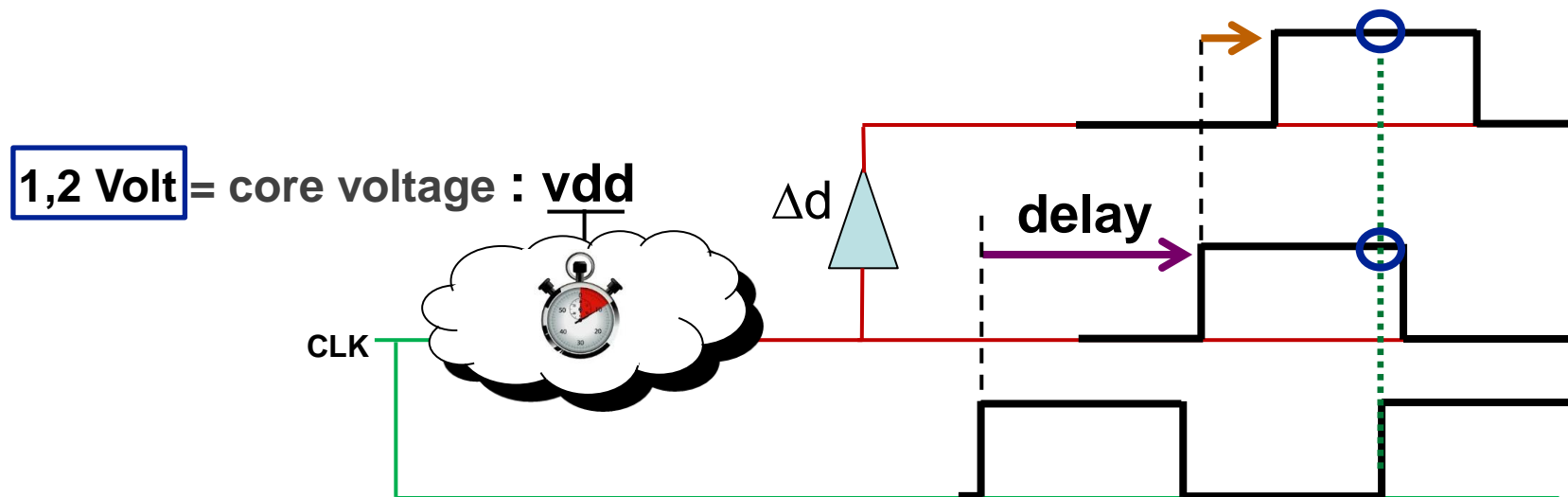




Time to digital converter

The **time-to-digital converter** measures a **phase distance** between two signals

$$\text{delay} + 1 * \Delta d < \text{clock period}$$



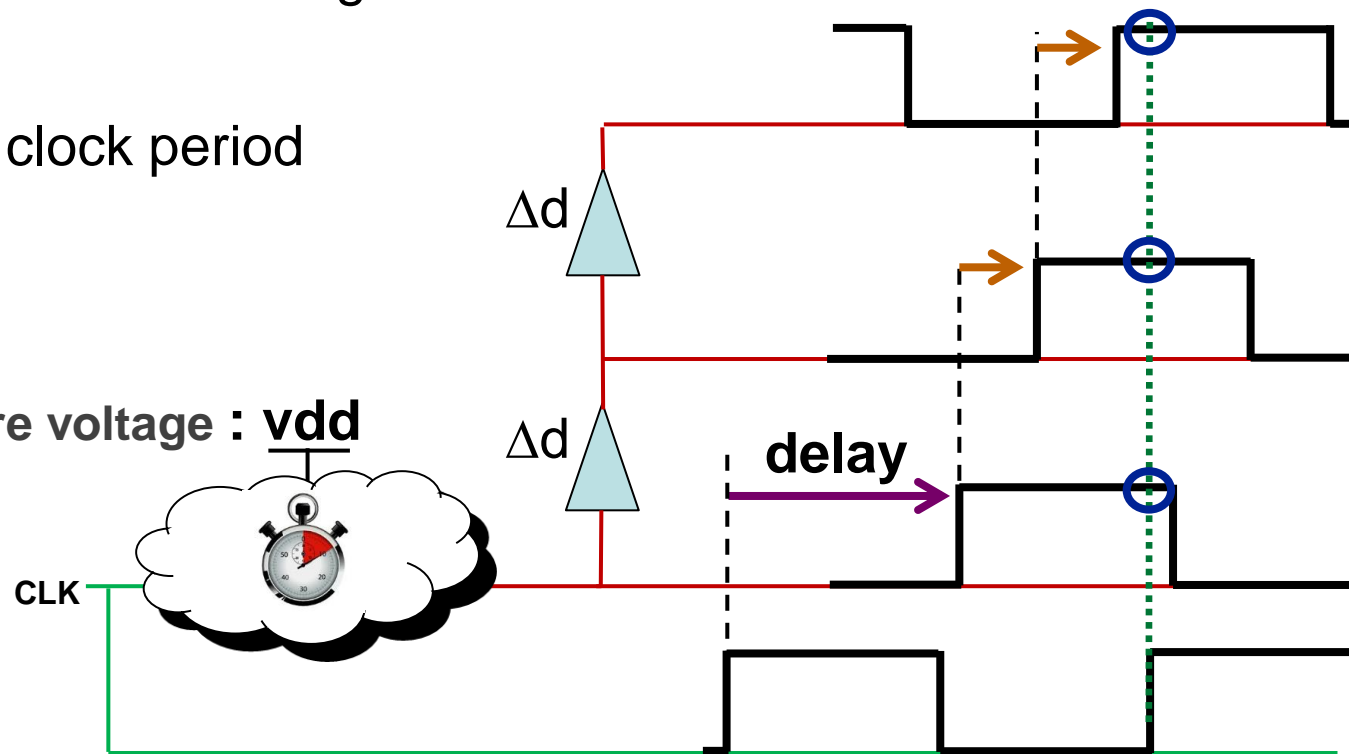


Time to digital converter

The **time-to-digital converter** measures a **phase distance** between two signals

$$\text{delay} + 2 * \Delta d < \text{clock period}$$

1,2 Volt = core voltage : **vdd**



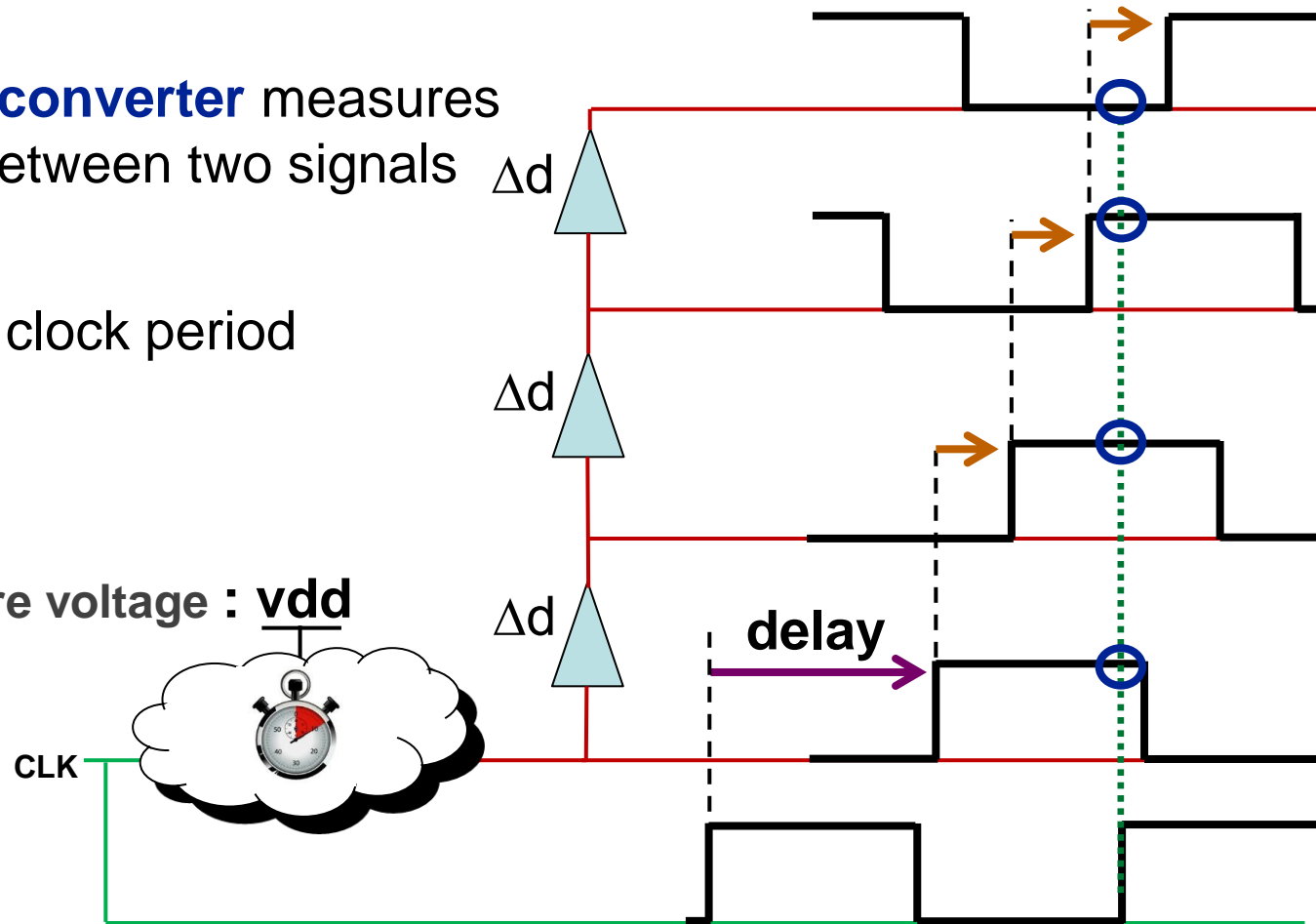


Time to digital converter

The **time-to-digital converter** measures a **phase distance** between two signals

delay + 3 * Δd > clock period

1,2 Volt = core voltage : vdd



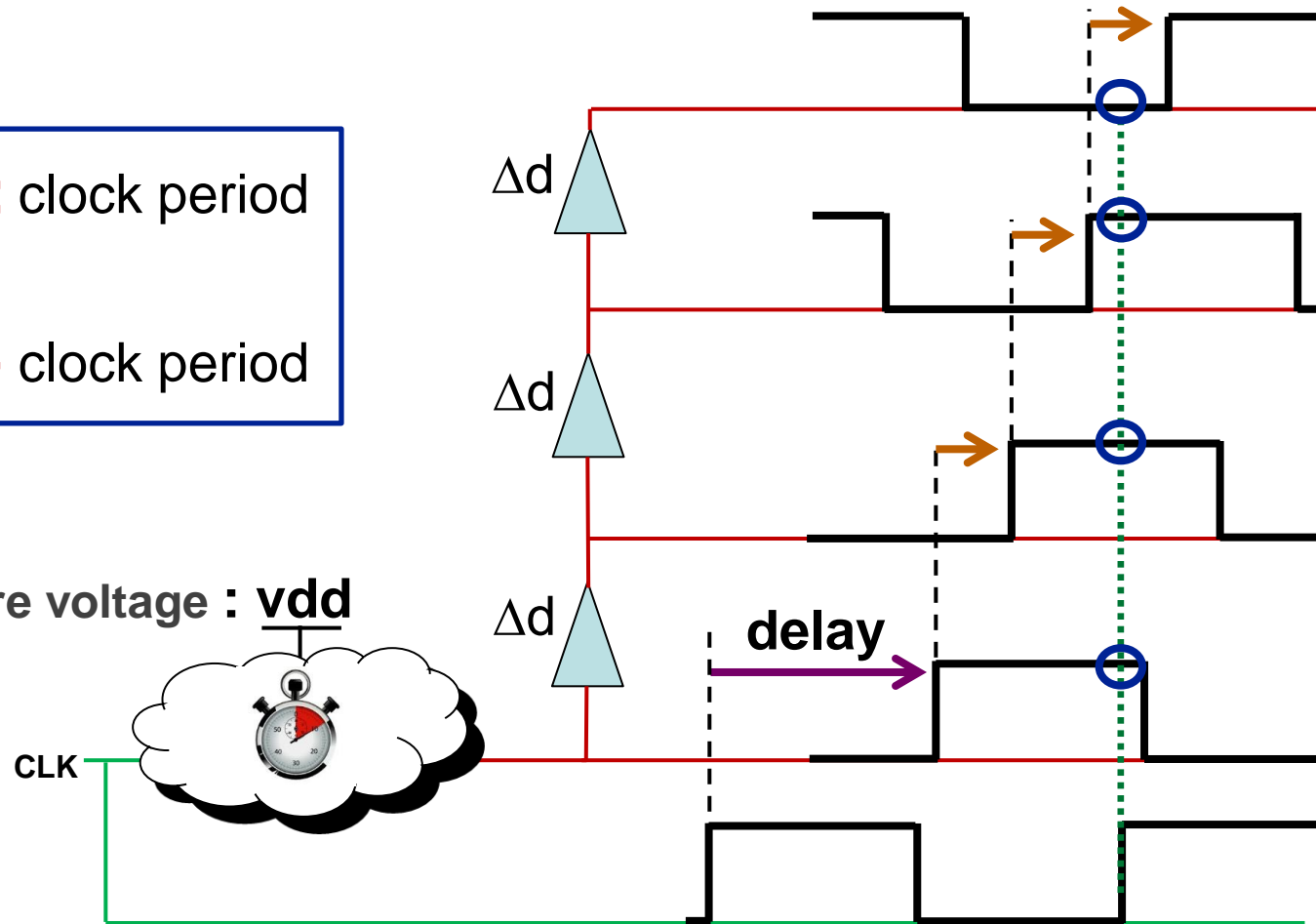


When undergoing a glitch injection

$\text{delay} + 2 * \Delta d < \text{clock period}$

$\text{delay} + 3 * \Delta d > \text{clock period}$

code = '1110' = core voltage : vdd





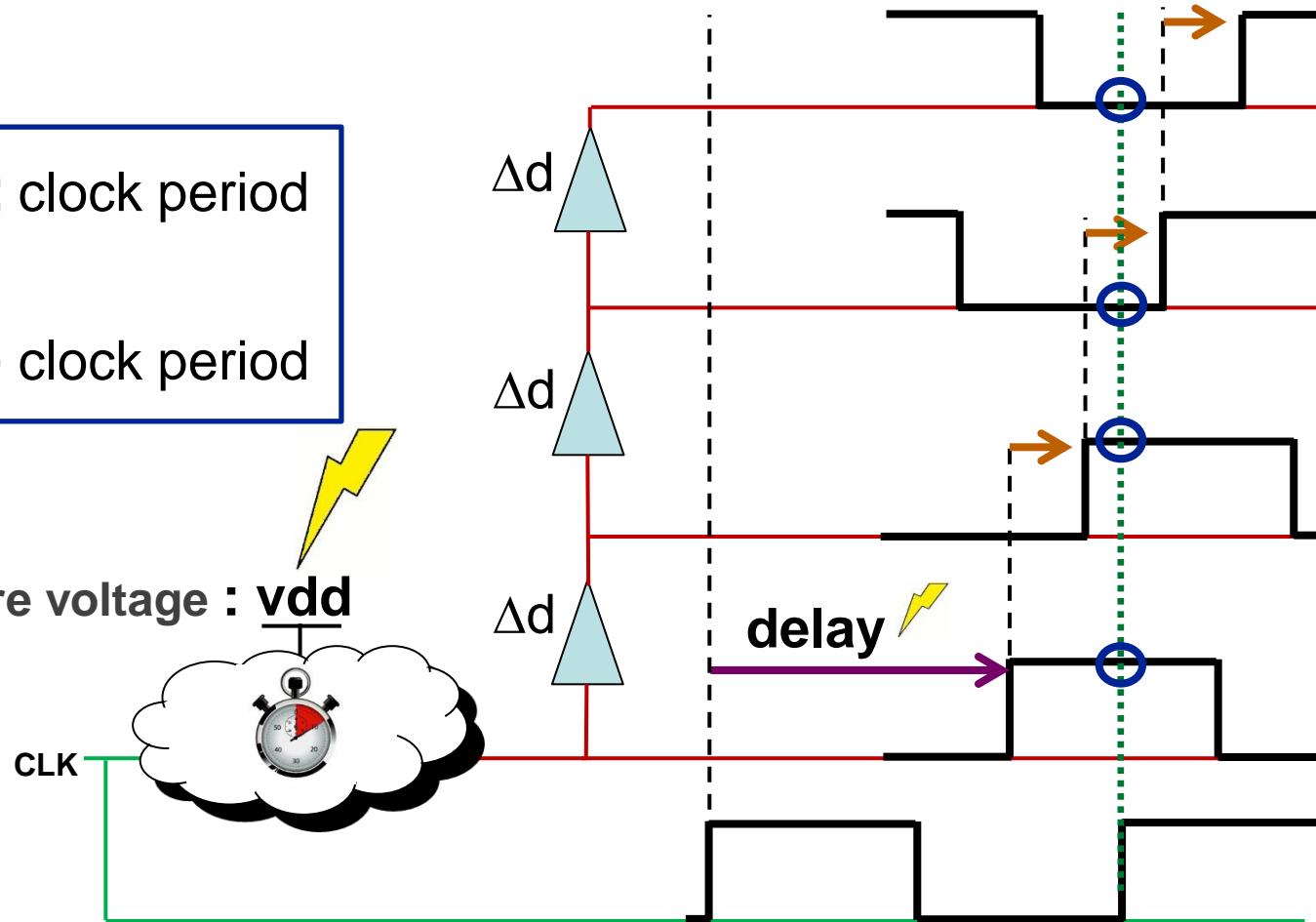
When undergoing a glitch injection

$\text{delay} + 1 * \Delta d < \text{clock period}$

$\text{delay} + 2 * \Delta d > \text{clock period}$

code = '1100'

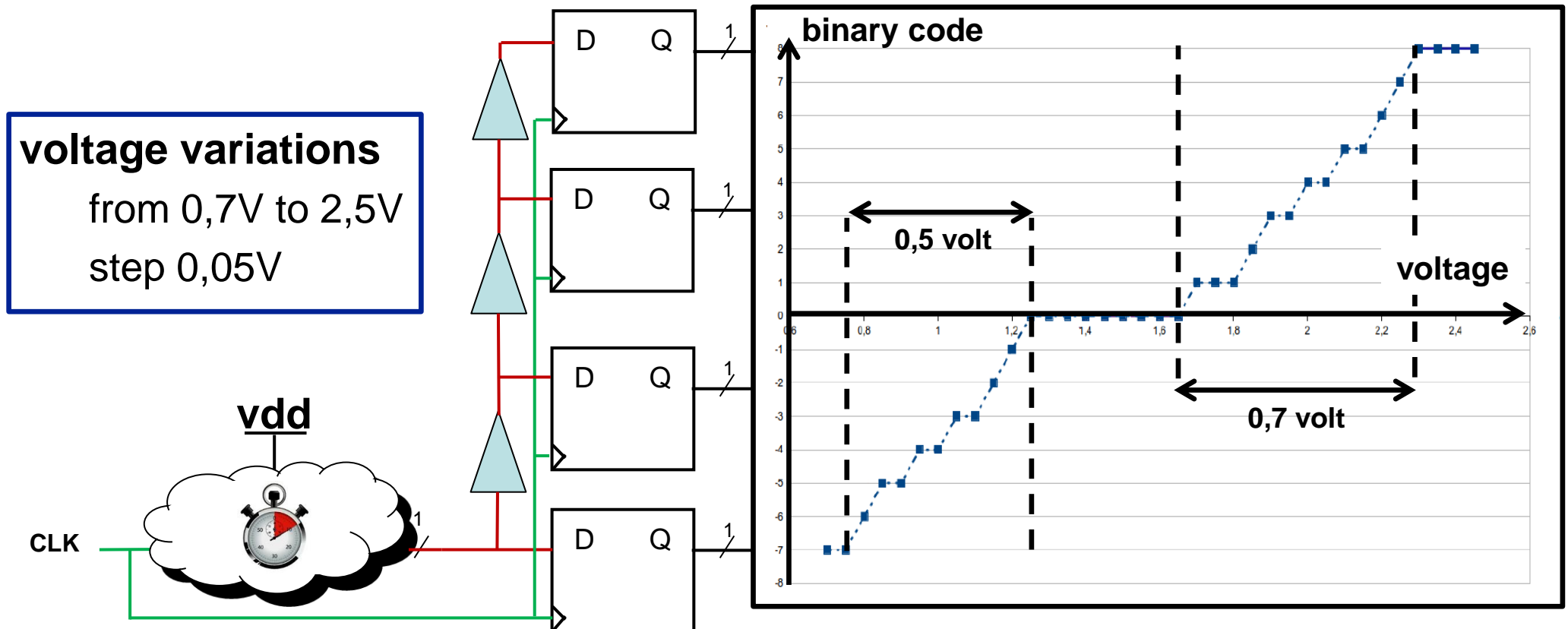
1,0 Volt = core voltage : vdd



Voltmeter



Library : voltage \leftrightarrow code



2 “linear” zones => resolution ~ 0,07V
1 “blind” zone



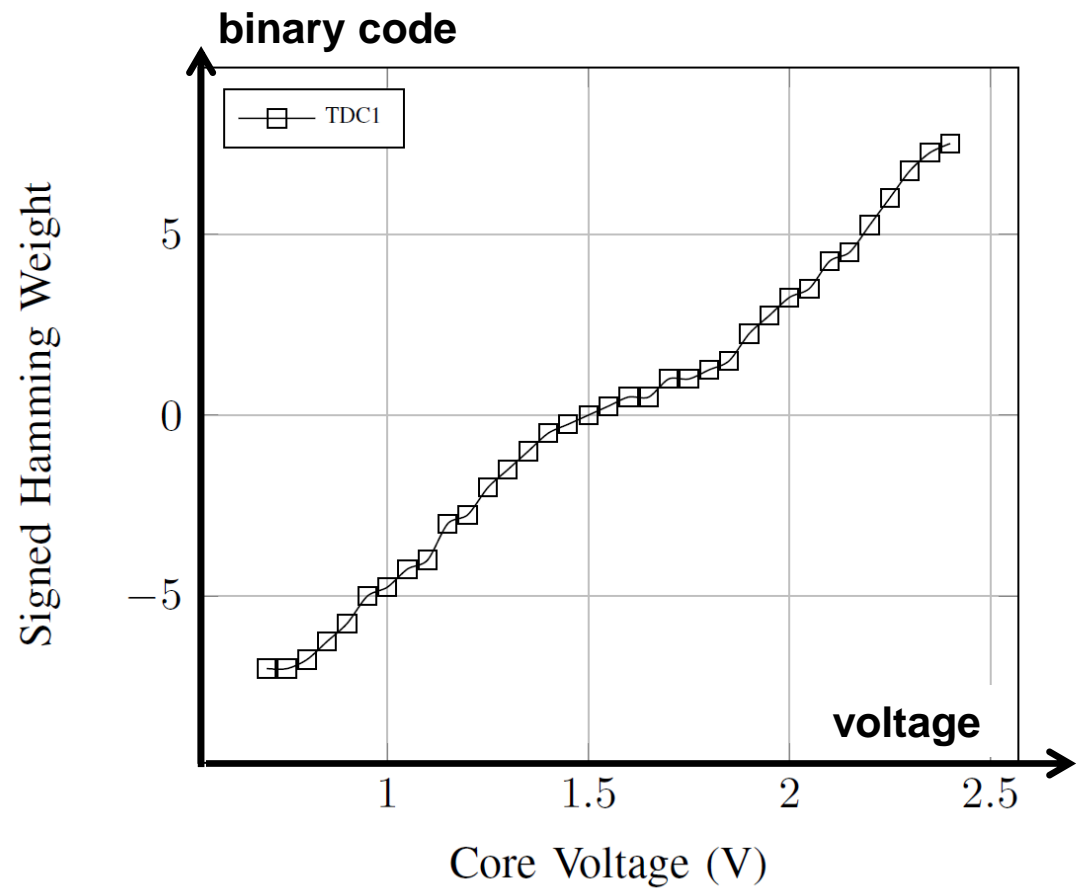
Library : voltage \leftrightarrow code

4 voltmeters implemented :

different delays due to
within-die **process**
variations

Only one “linear” zones
=> **resolution improving**

No “blind” zone

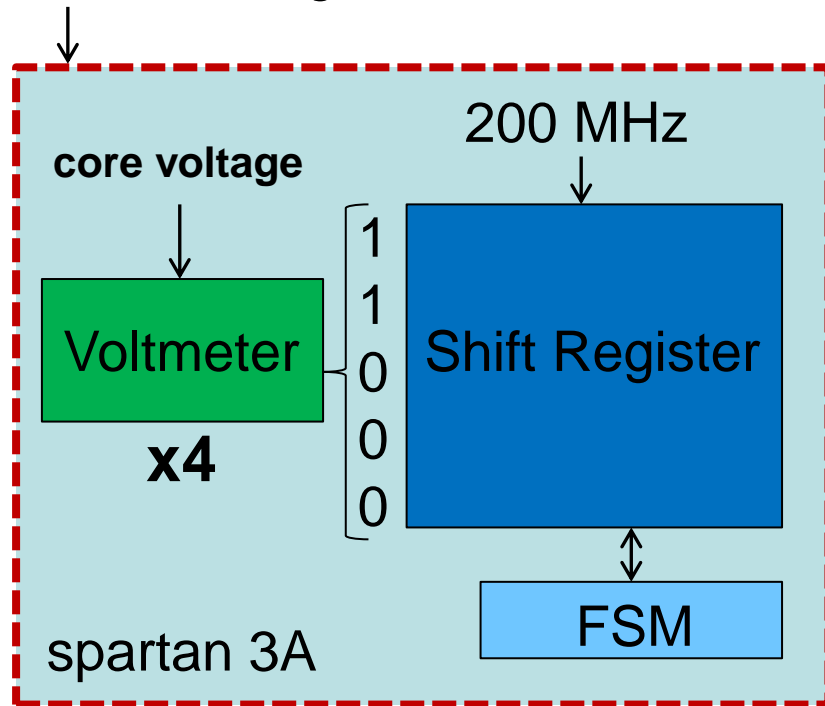


Experimental setup



Acquisition setup

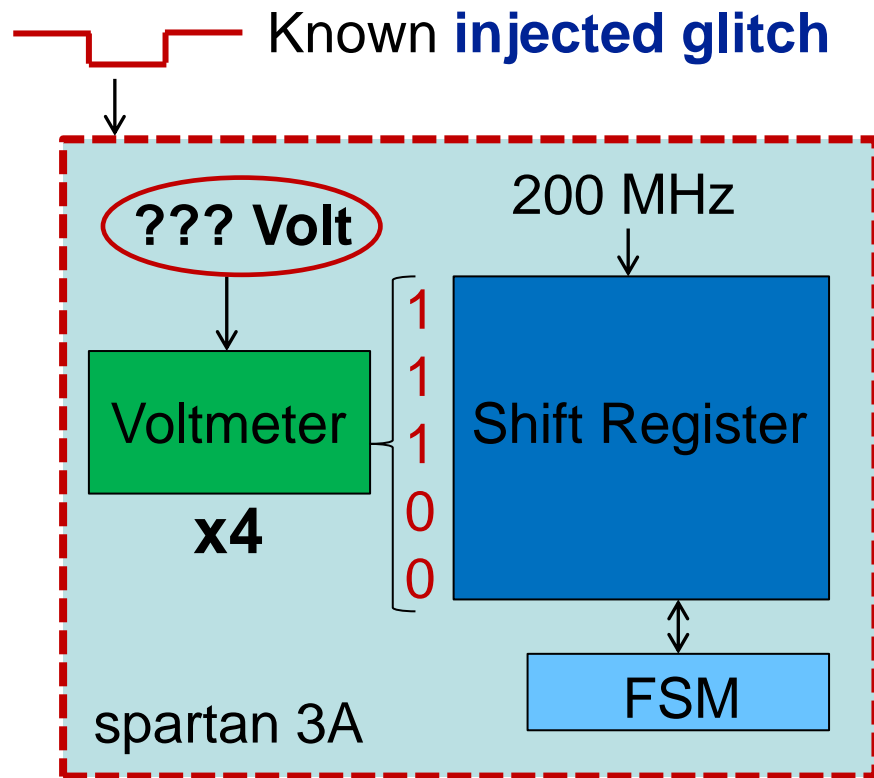
nominal voltage



Experimental setup



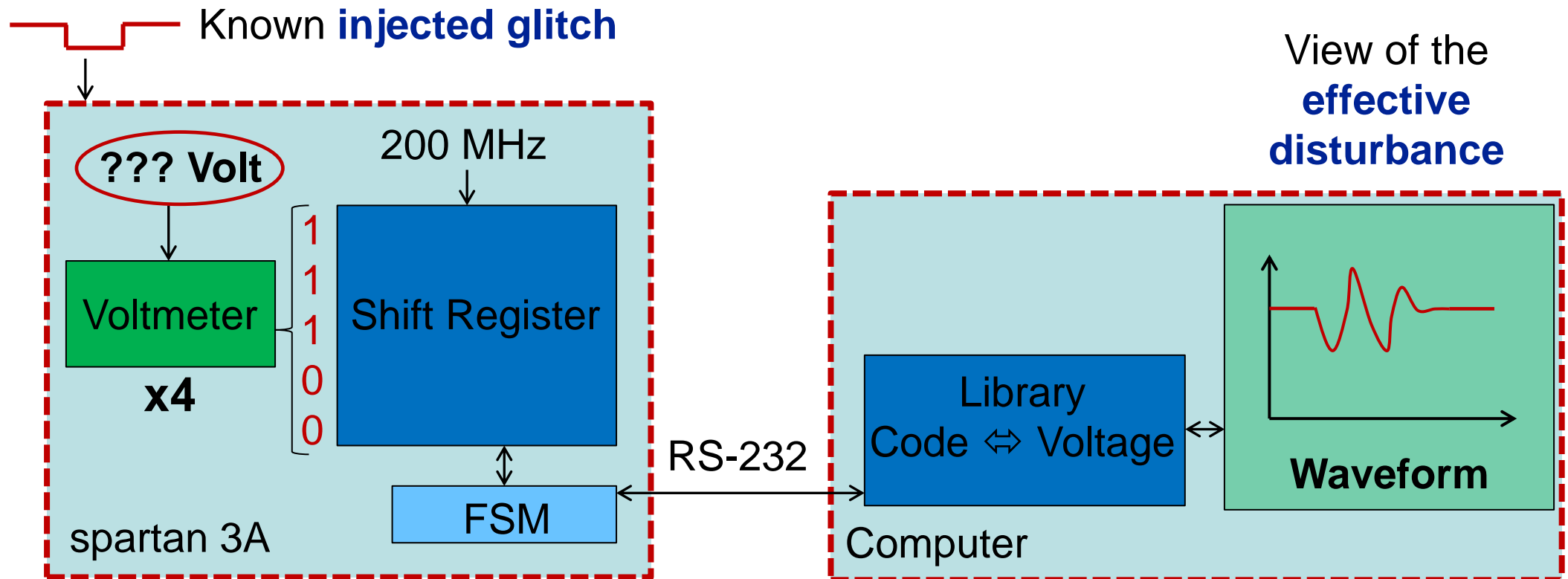
Acquisition setup



Experimental setup



Acquisition setup



Experimental setup



www.emse.fr

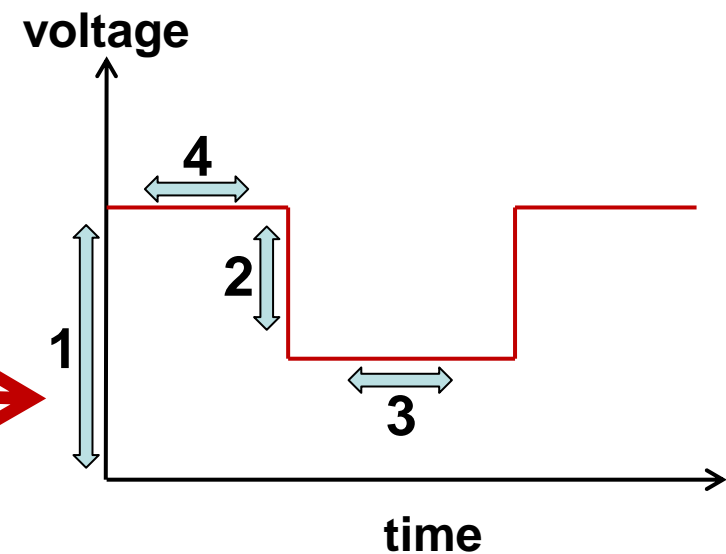
INSPIRING INNOVATION | INNOVANTE PAR TRADITION

Glitches injection setup



Pulse generator variables :

1. DC offset (Volts)
2. Amplitude (Volts)
3. Width (ns)
4. Delay (ns)



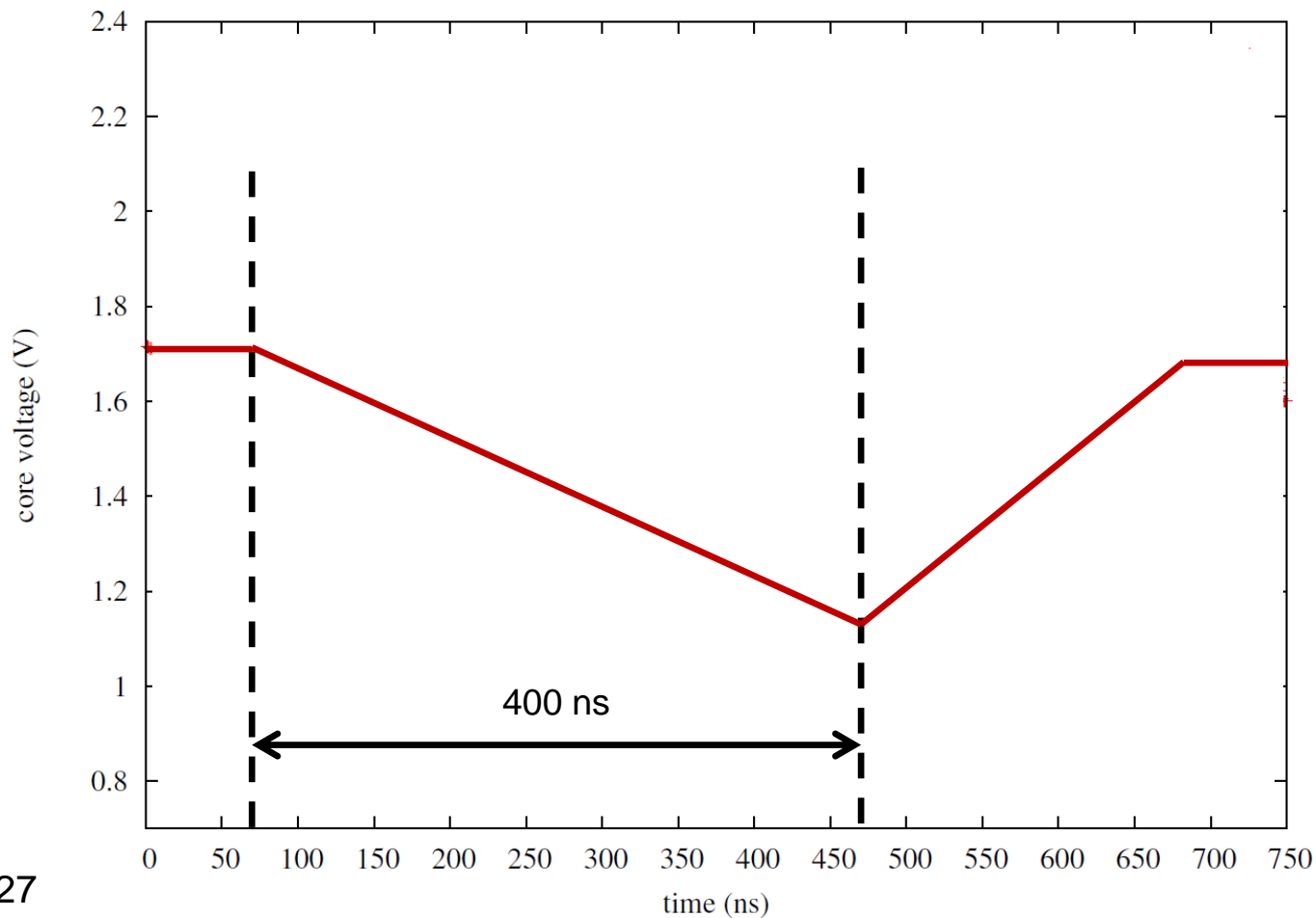
Experimental results



Negative voltage glitch : what I expected

amplitude : -14V

width : 400ns



Expectation :

Filtered signal due to the **input capacitances**

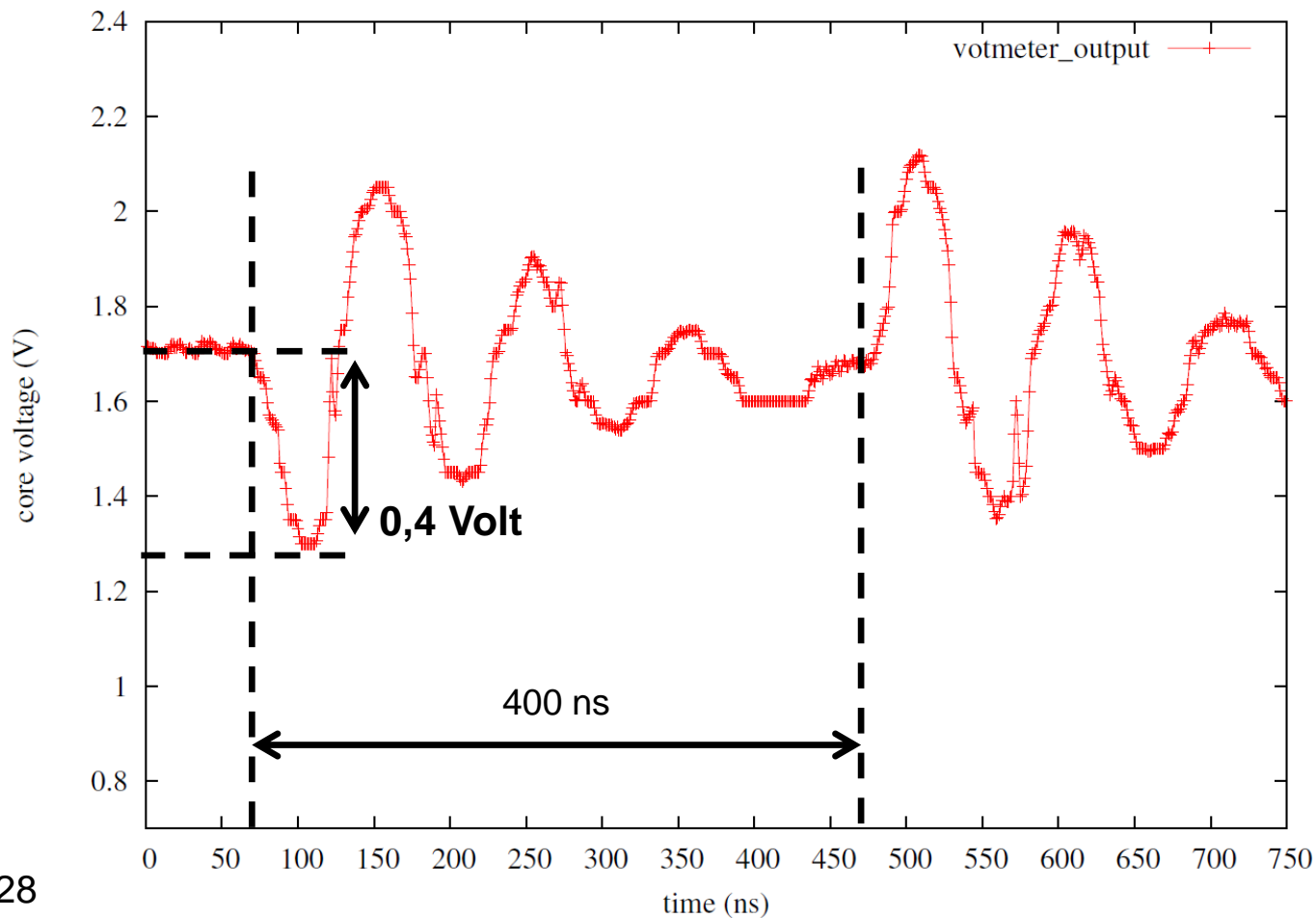
Experimental results



Negative voltage glitch : what it is !

amplitude : -14V

width : 400ns



Observation :

2 sets of **damping oscillations**

Effective disturbances are **due to the rising/falling edges** of the injected voltage

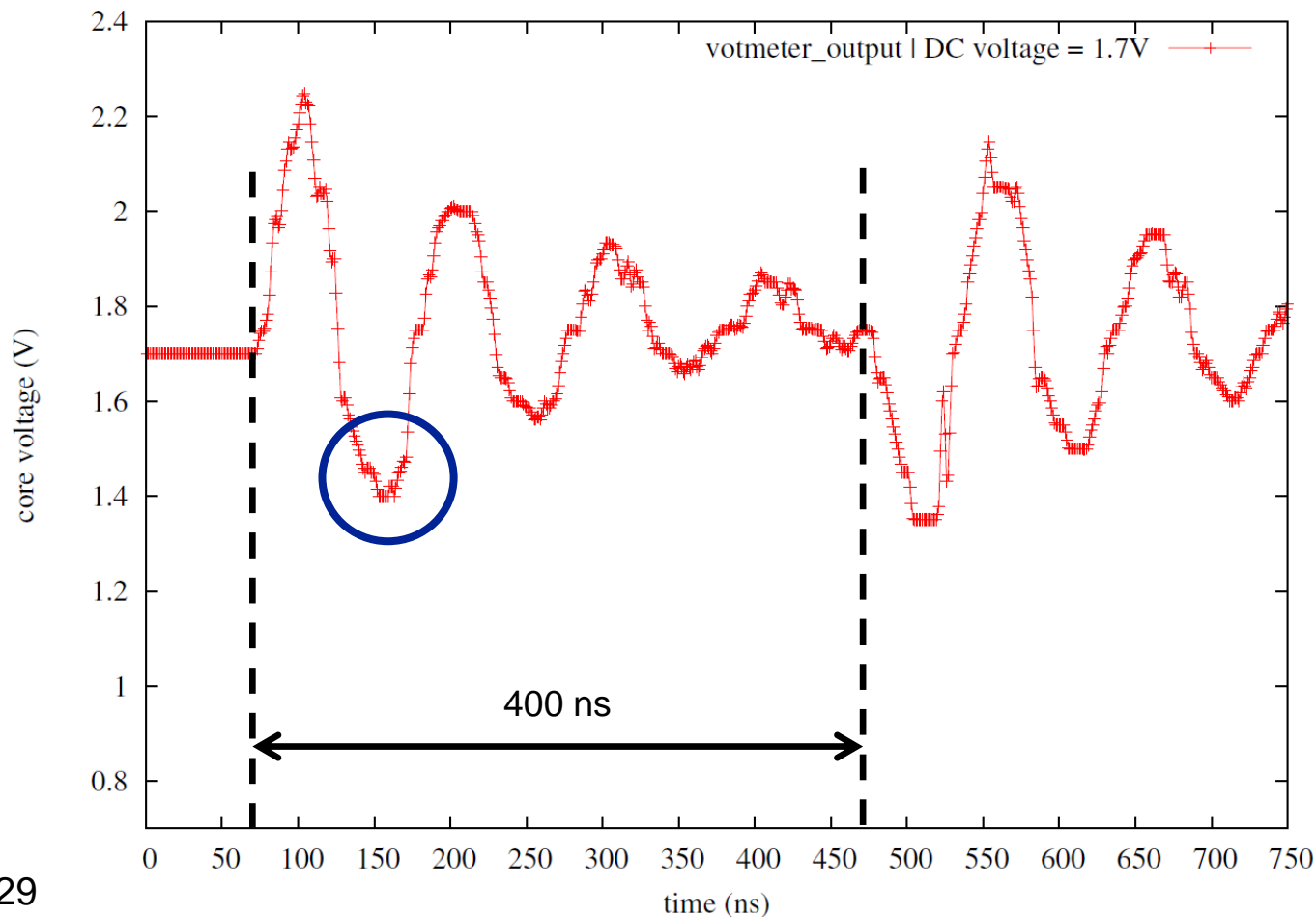
Experimental results



Positive voltage glitch

amplitude : +14V

width : 400ns



Observation :

Positive glitches

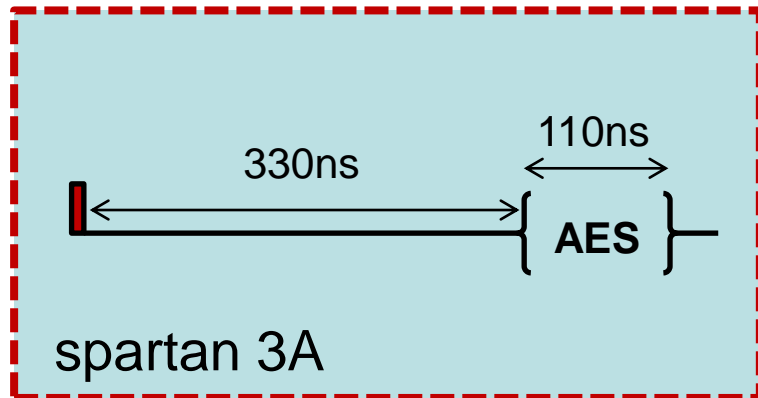
injection also produce **negative disturbances** due to the **rising/falling edges** of the injected voltage

Fault injection

mechanism could also be related to **timing constraint violation ?**



Fault injection target



Target

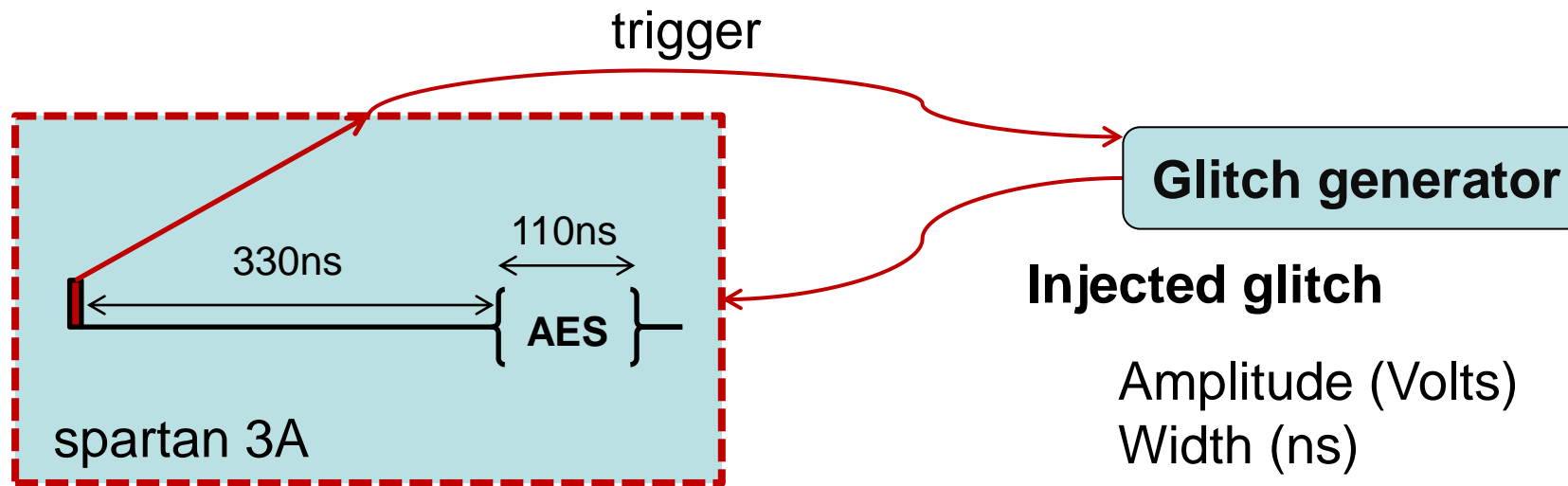
AES 128bit - 100MHz

Fault injection synchronization

Trig signal 330 ns before the
AES calculation



Fault injection protocol



Injected glitch

Amplitude (Volts)

Width (ns)

Variables

DC offset from 1,4 to 1,1 Volts

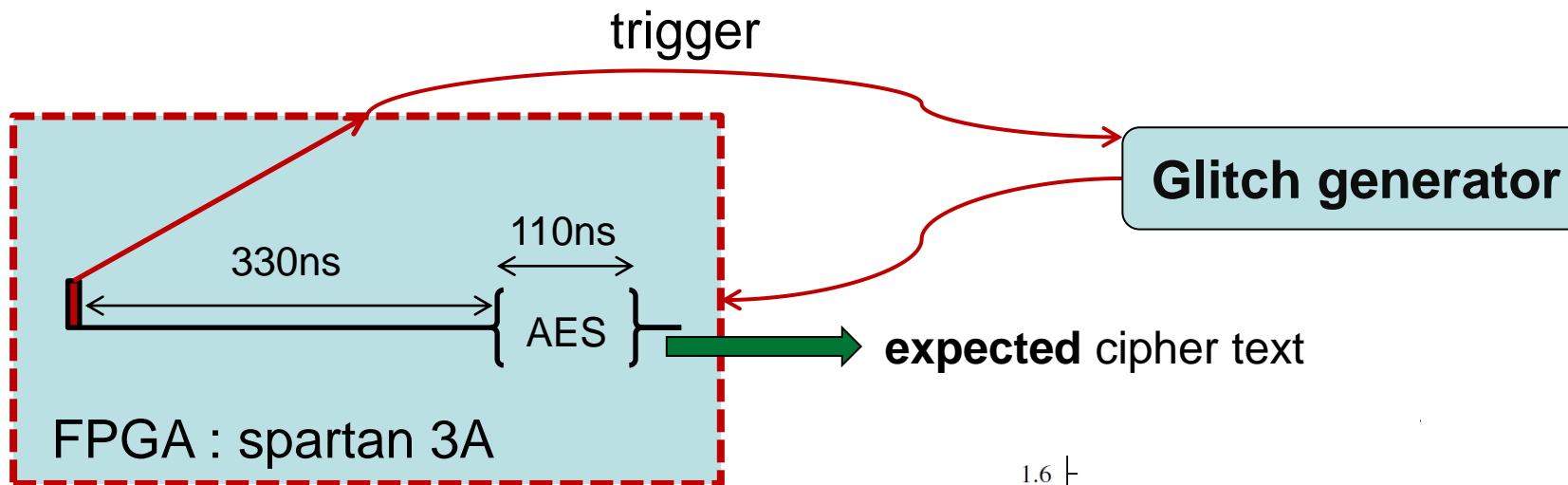
Delay from 170 to 330 ns

AES 128bit : 11 rounds - 100MHz

Characterization



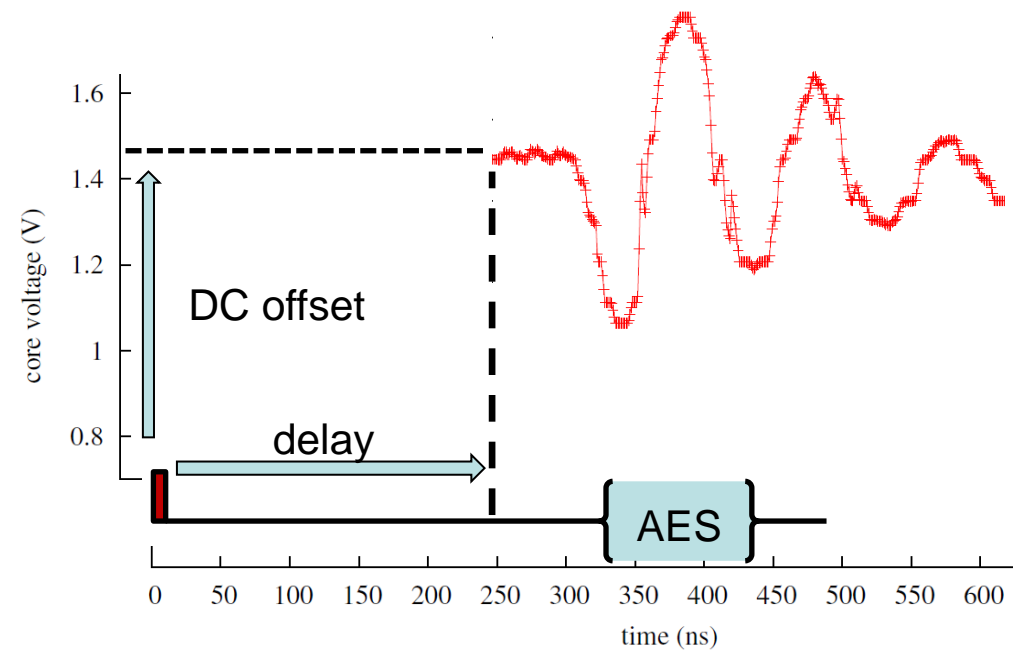
Fault injection protocol



AES 128bit : 11 rounds - 100MHz

DC offset from 1,4 to 1,1 Volts

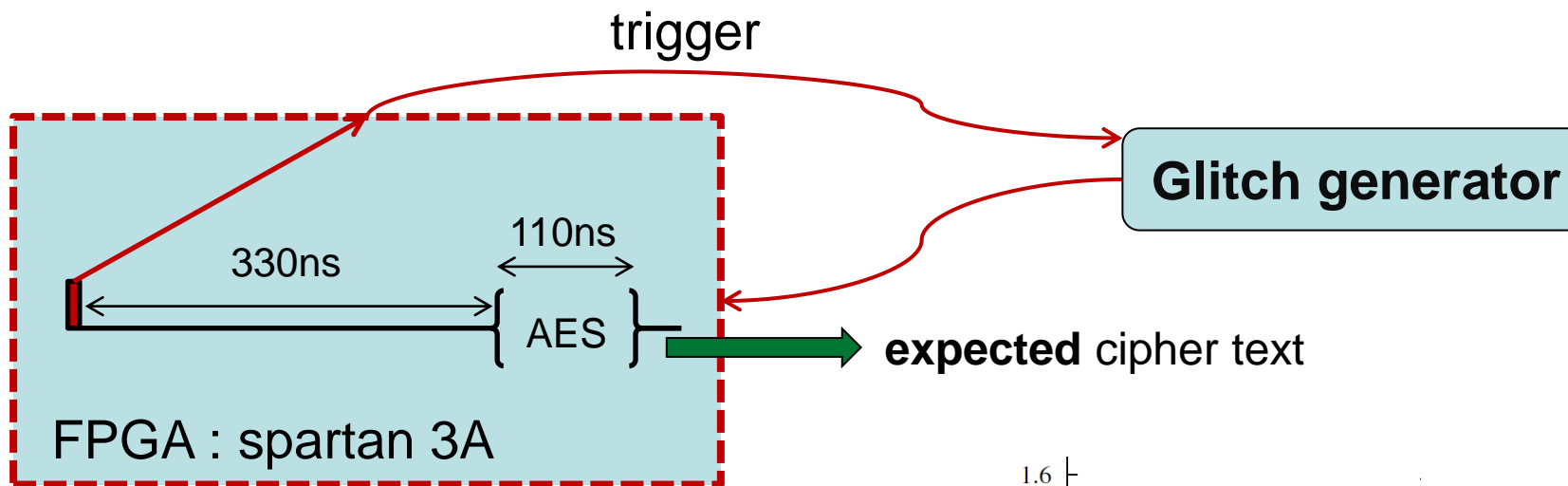
Delay from 170 to 330 ns



Characterization



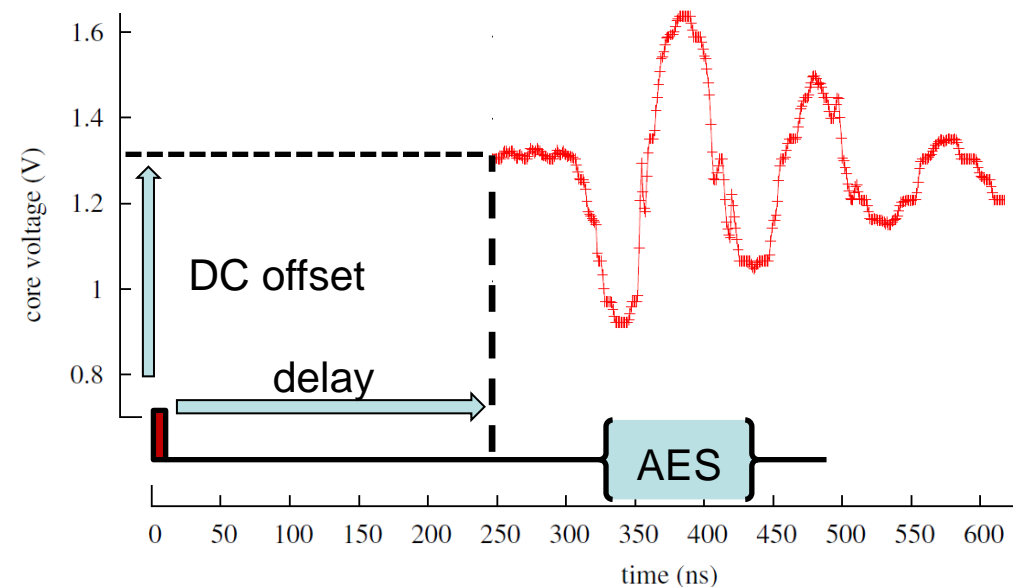
Fault injection protocol



AES 128bit : 11 rounds - 100MHz

DC offset from 1,4 to 1,1 Volts

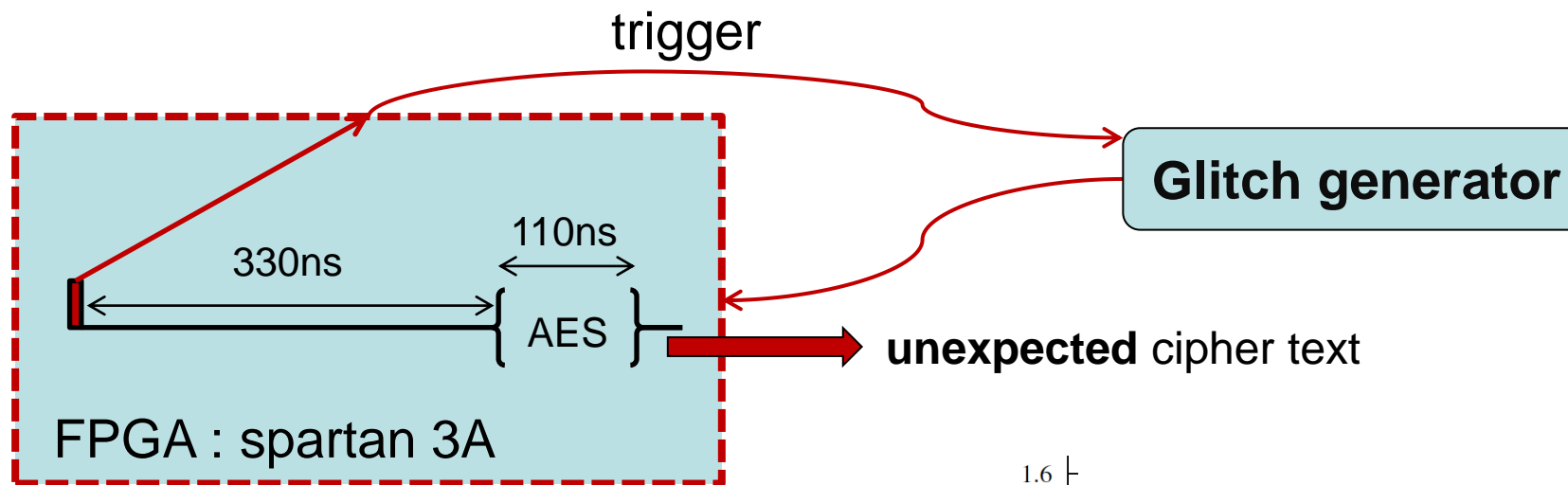
Delay from 170 to 330 ns



Characterization



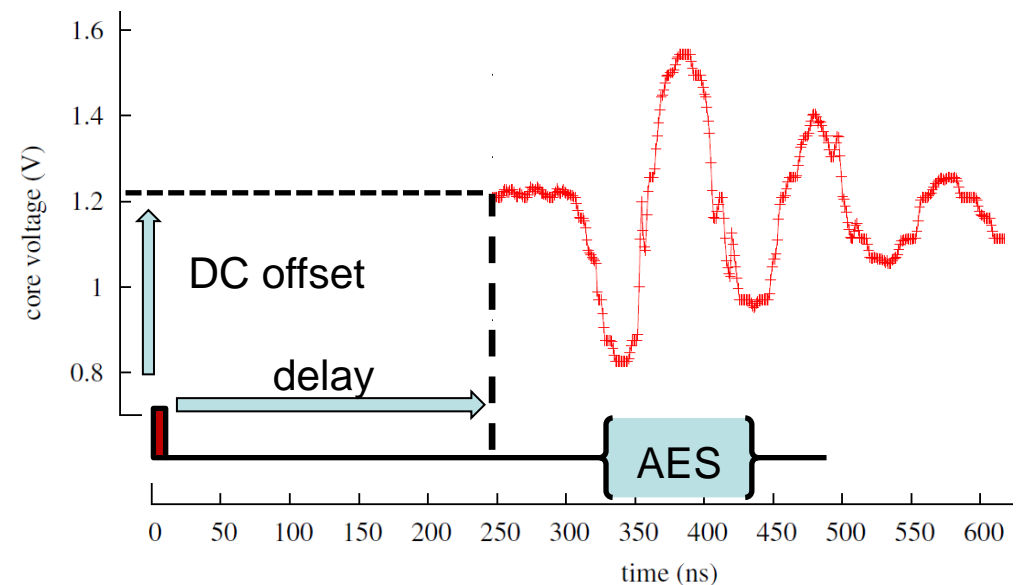
Fault injection protocol



AES 128bit : 11 rounds - 100MHz

DC offset from 1,4 to 1,1 Volts

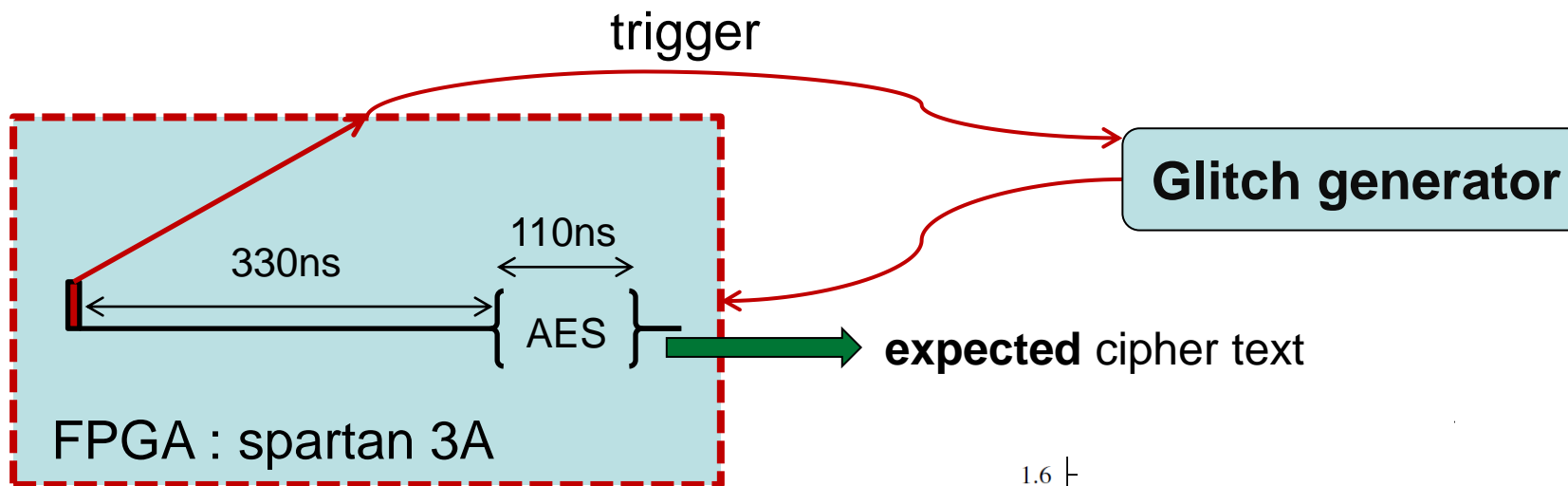
Delay from 170 to 330 ns



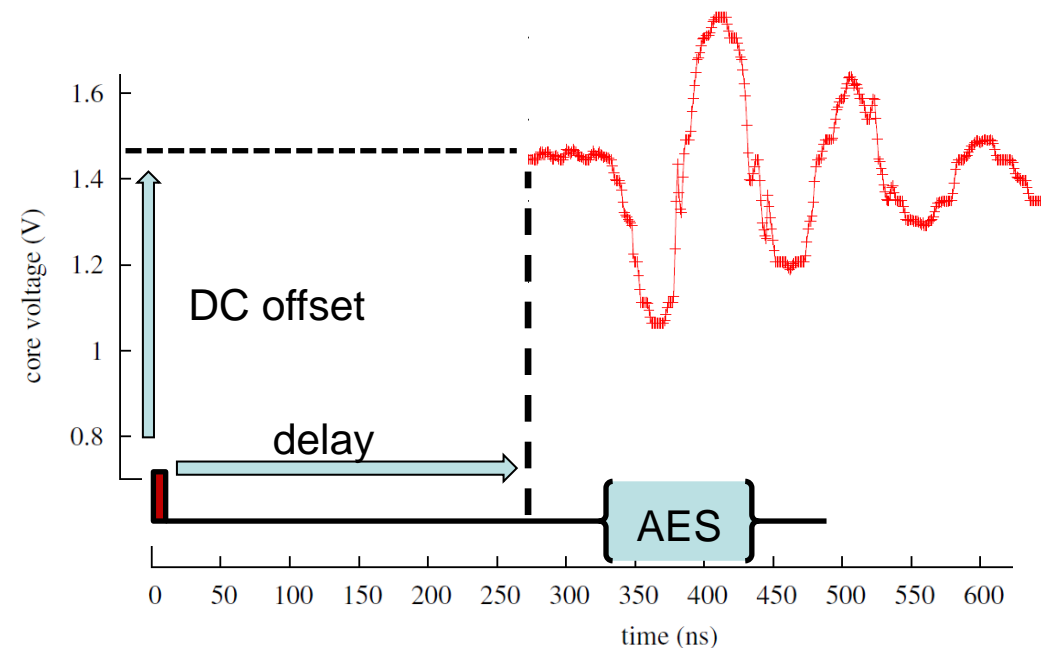
Characterization



Fault injection protocol



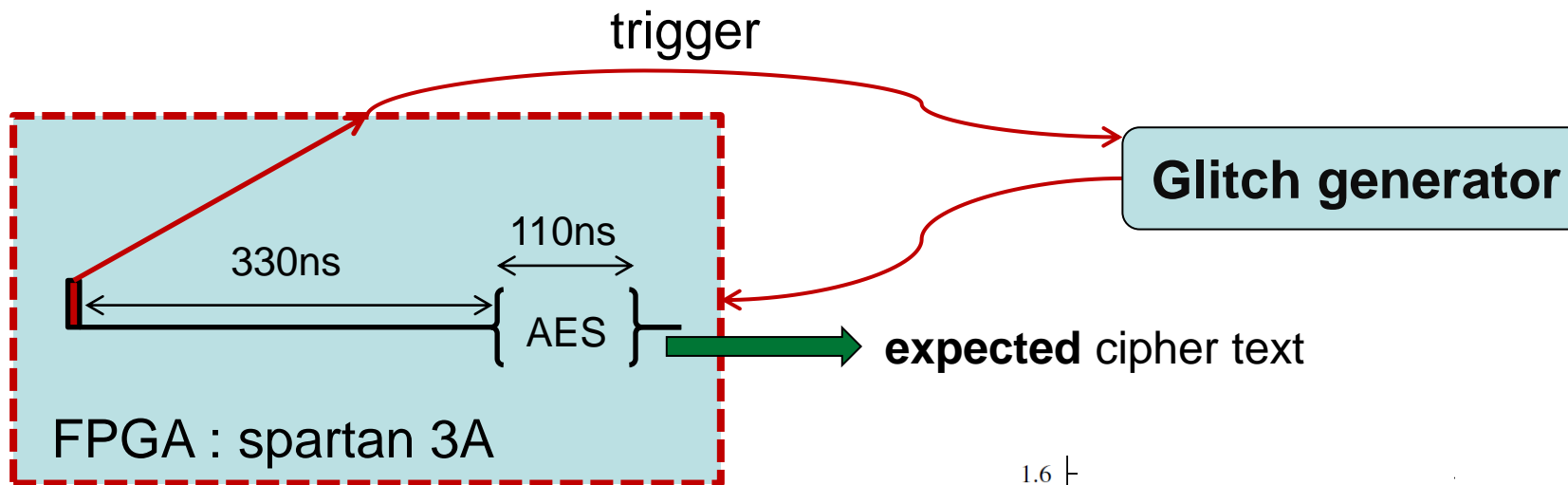
AES 128bit : 11 rounds - 100MHz
DC offset from 1,4 to 1,1 Volts
Delay from 170 to 330 ns



Characterization



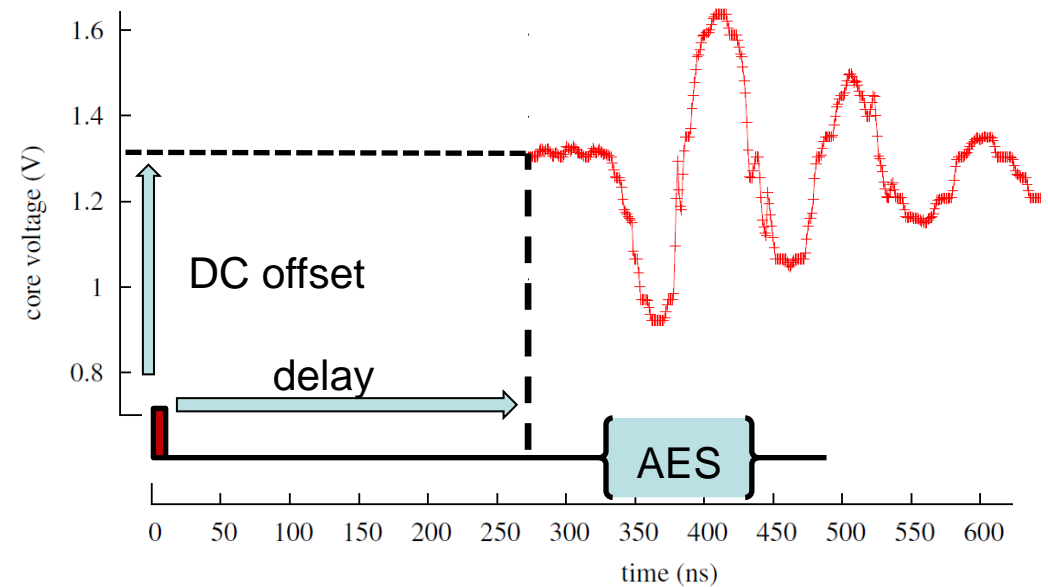
Fault injection protocol



AES 128bit : 11 rounds - 100MHz

DC offset from 1,4 to 1,1 Volts

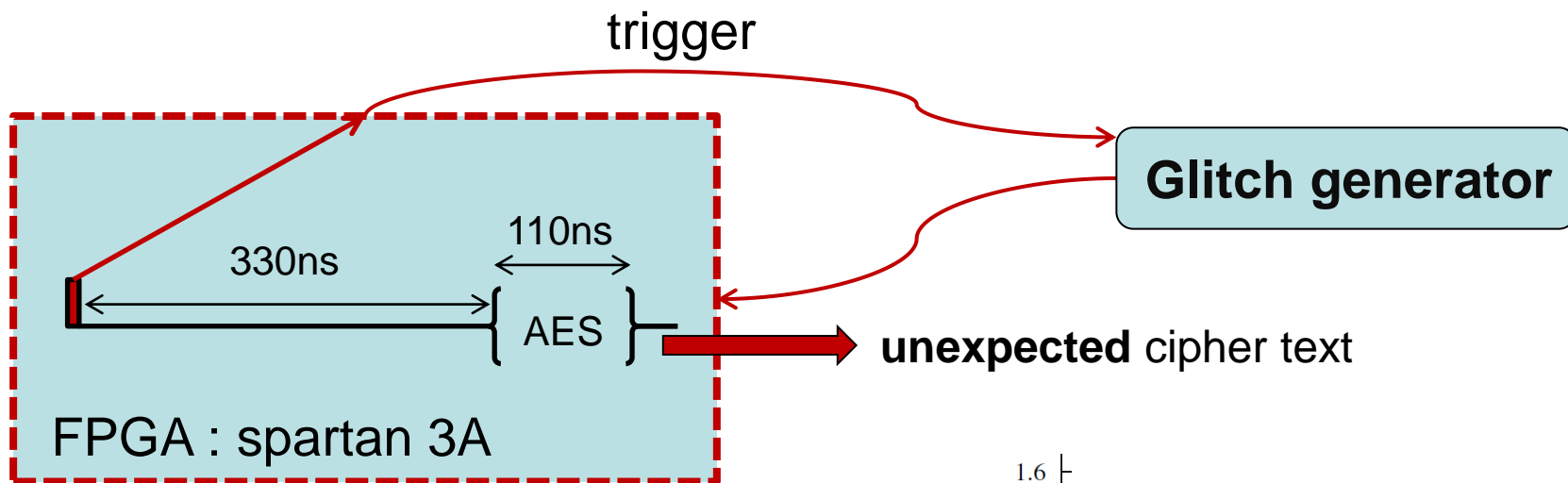
Delay from 170 to 330 ns



Characterization



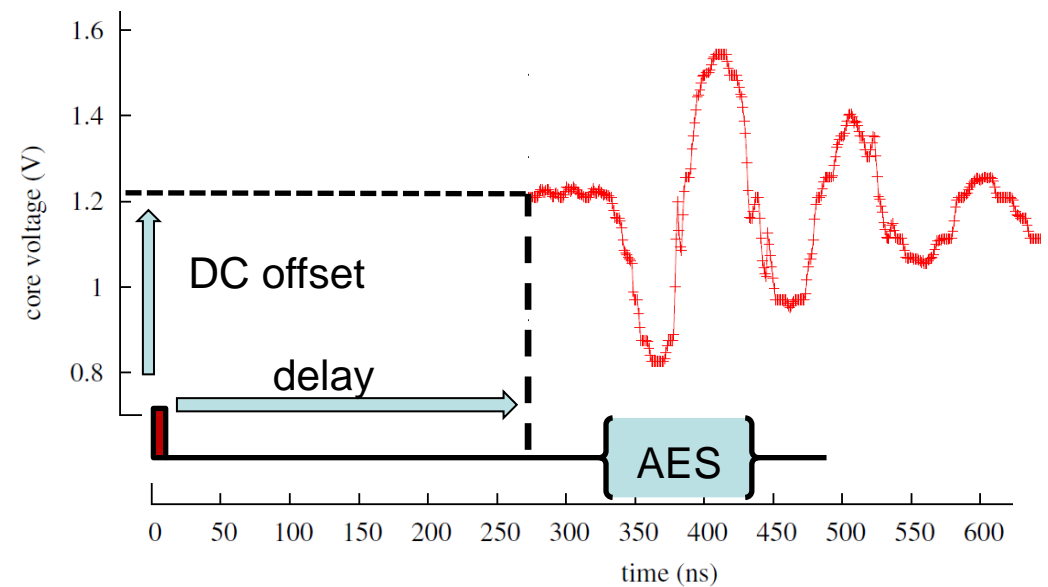
Fault injection protocol



AES 128bit : 11 rounds - 100MHz

DC offset from 1,4 to 1,1 Volts

Delay from 170 to 330 ns



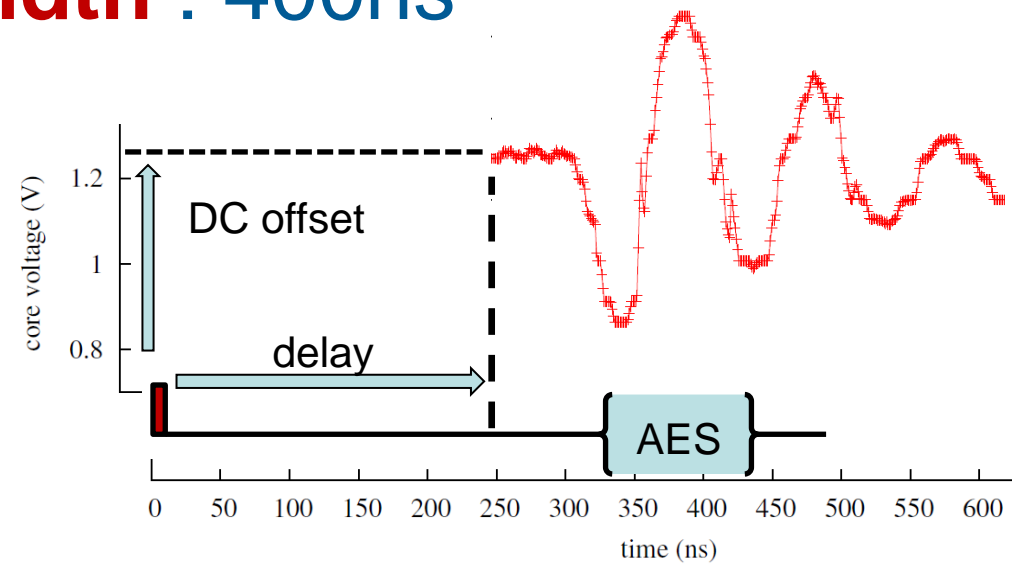
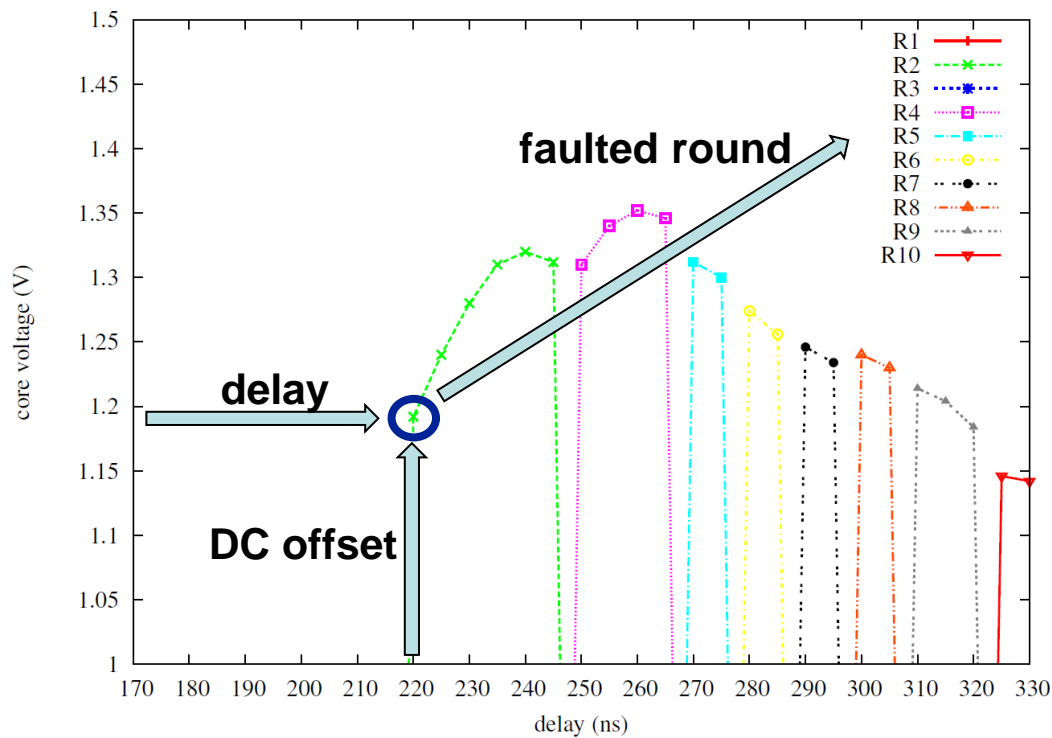
Experimental results



Negative voltage glitch characterization

amplitude : -14V

width : 400ns



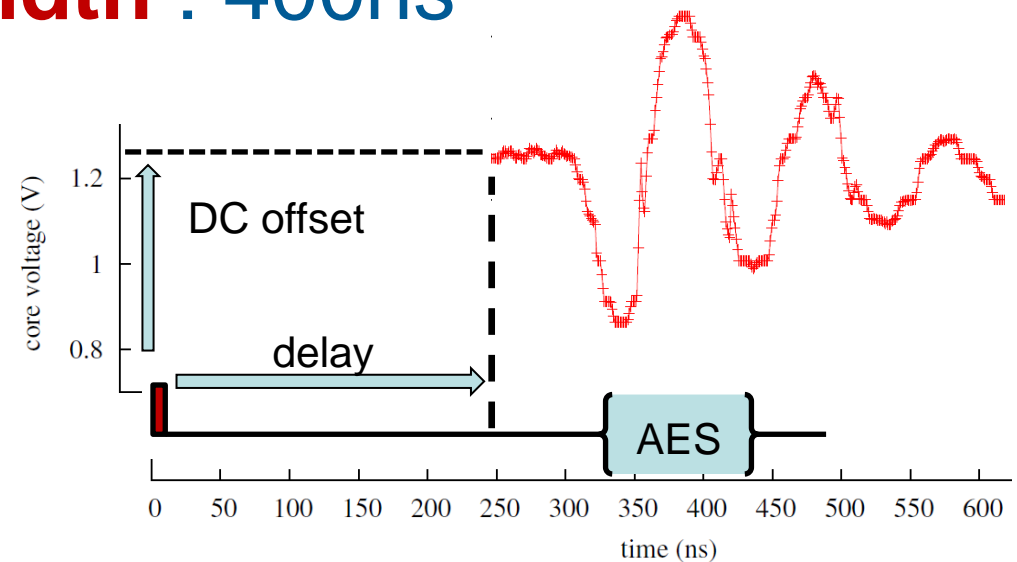
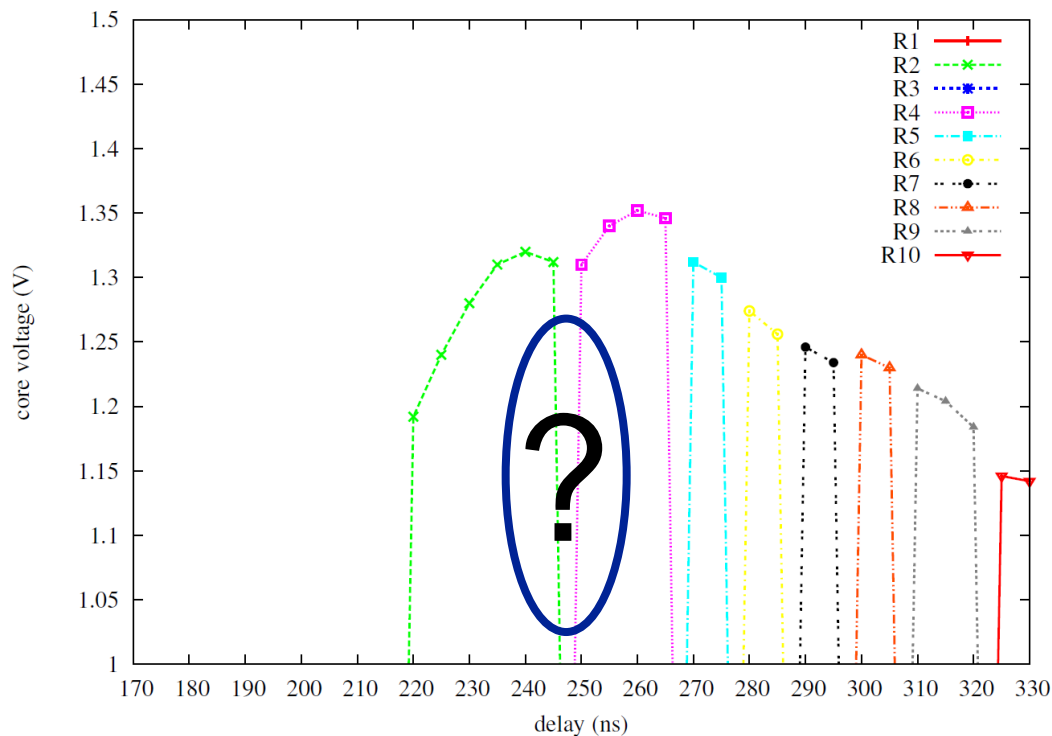
Experimental results



Negative voltage glitch characterization

amplitude : -14V

width : 400ns



Observation :

R3 wasn't faulted

The **negative disturbance is too large**
Faults were injected in R2 or R4 first

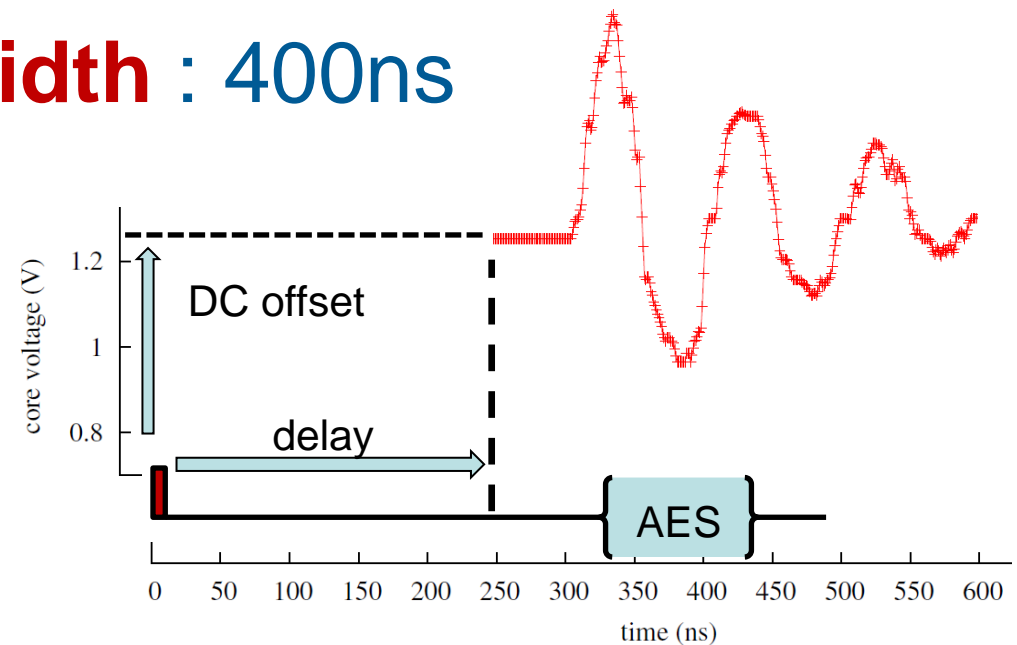
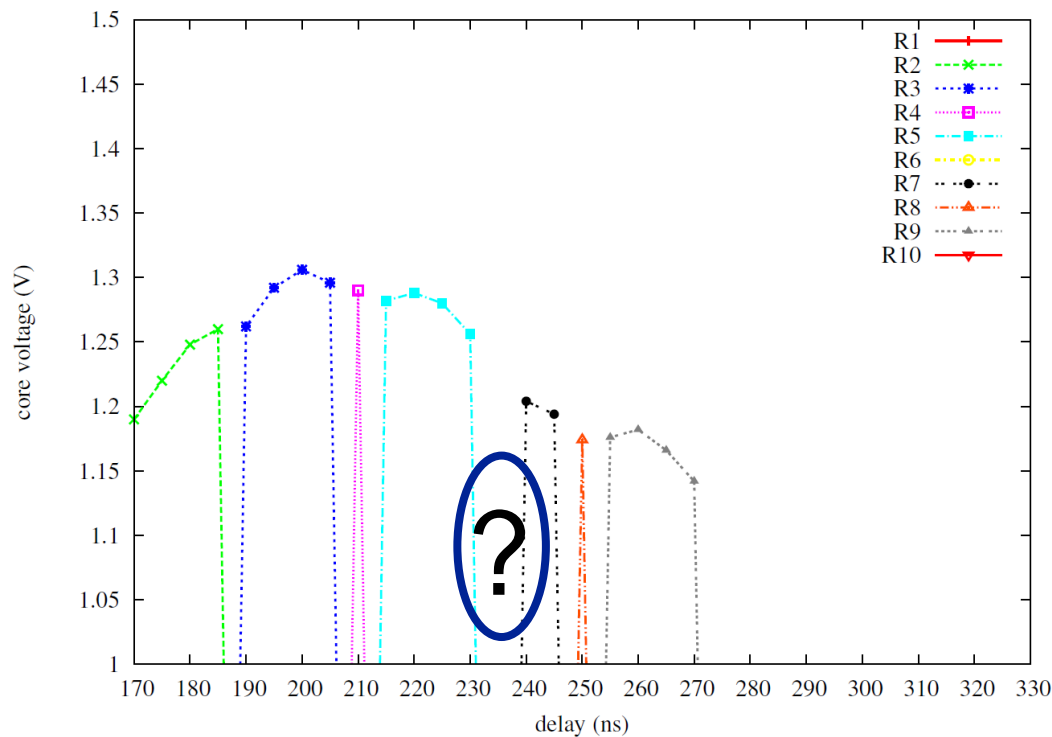
Experimental results



Positive voltage glitch characterization

amplitude : +14V

width : 400ns



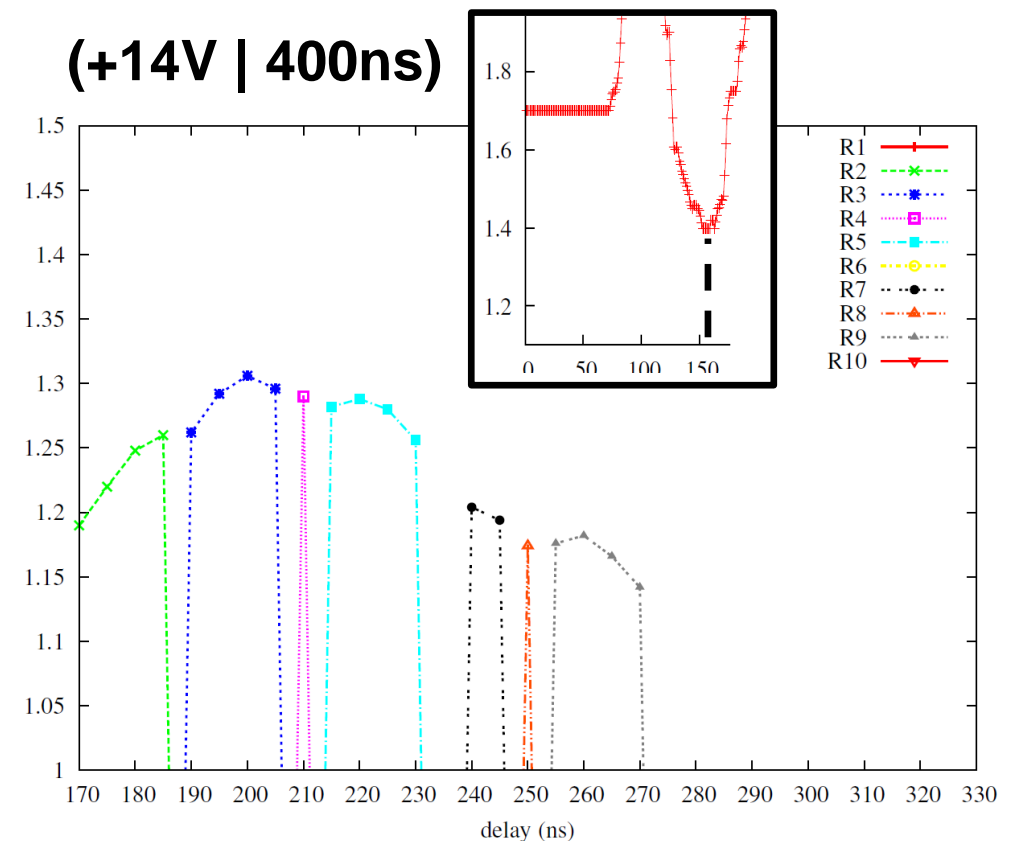
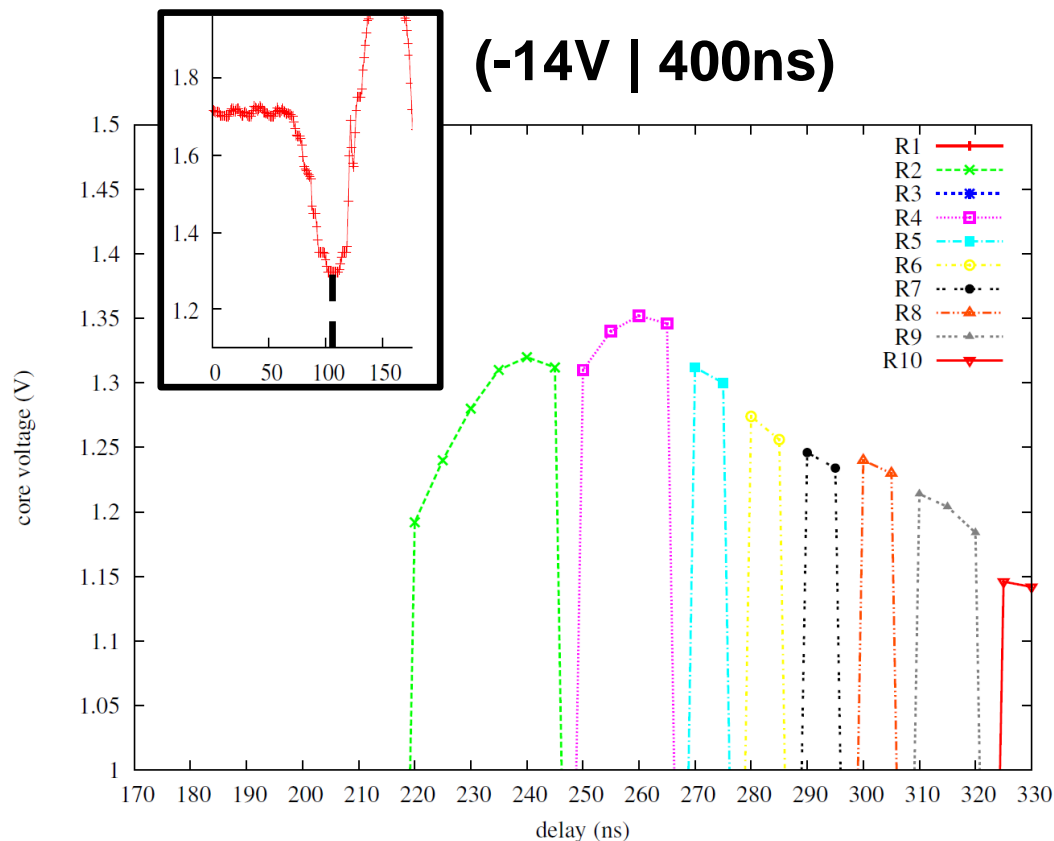
Observation :

R3 was faulted BUT R6 wasn't !

Experimental results



Injected faults comparison



⇒ Same injected faults

⇒ Different temporal accuracy

⇒ Same fault injection mechanism

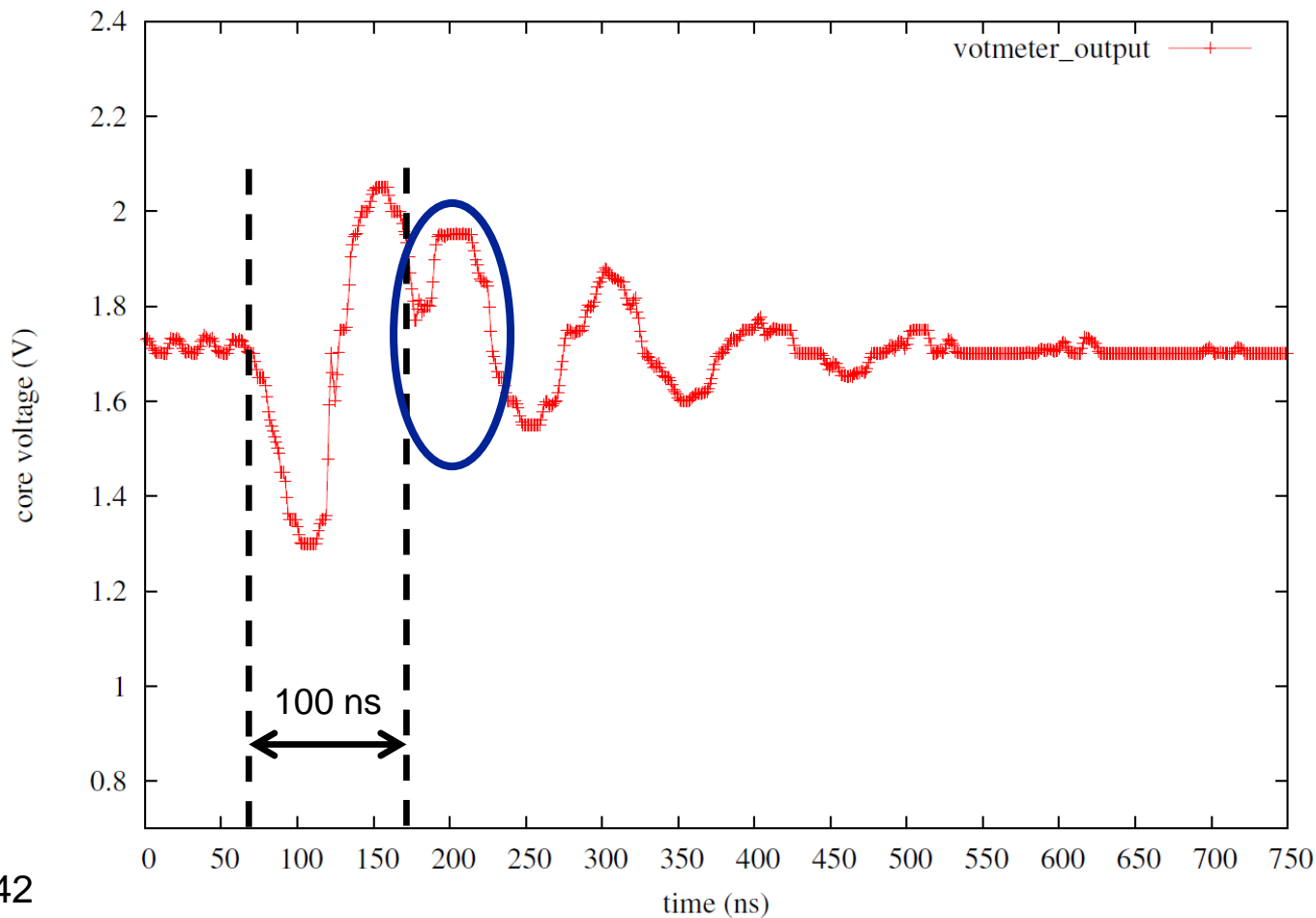
Glitch shaping



Offsetting

amplitude : -14V

width : 100ns



Observation :

Positive oscillations
due to the rising edge

COMPENSATE

negative oscillations
due to the falling edge

➤ **Only one significant
negative spike**

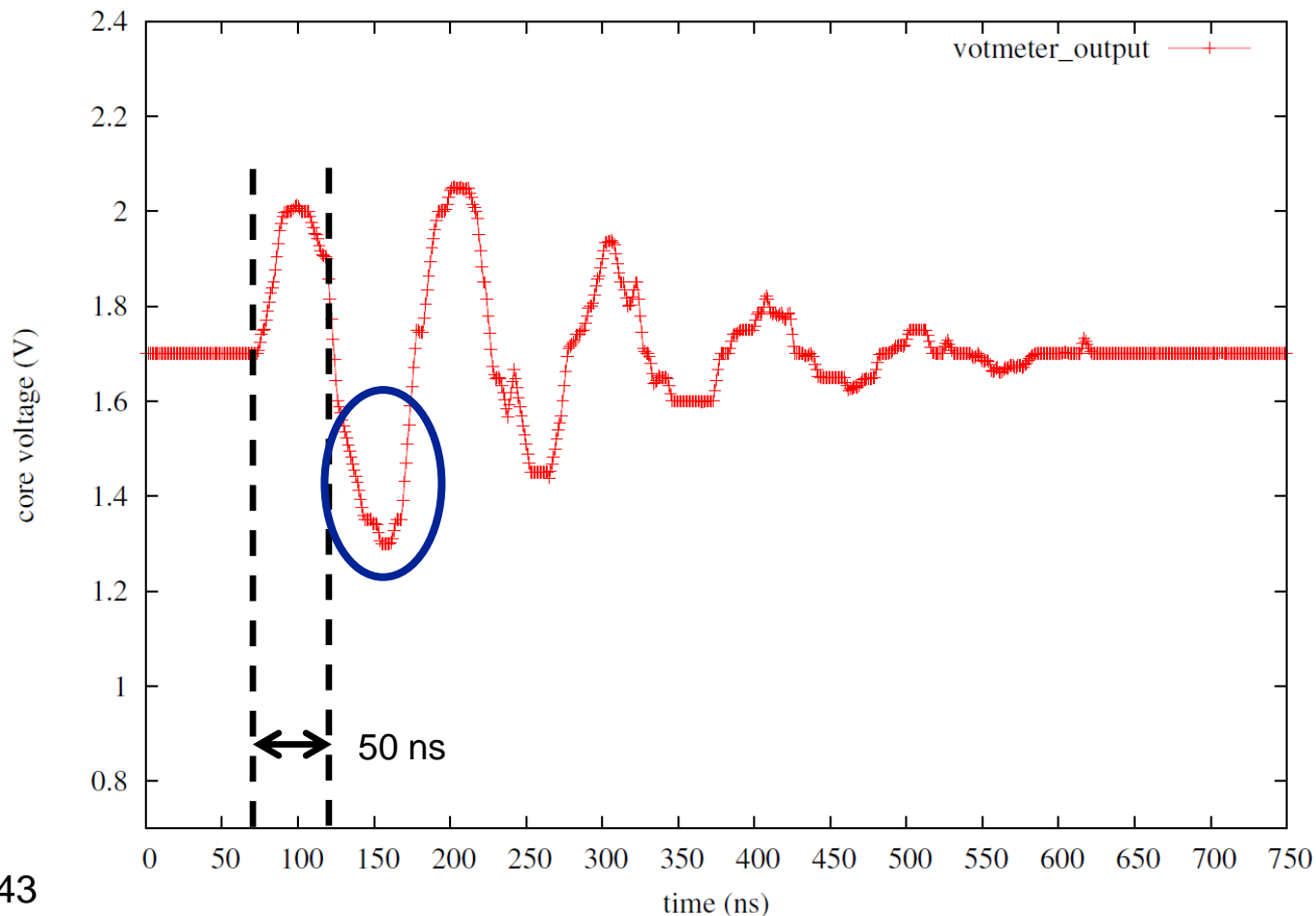
Glitch shaping



Addition

amplitude : +8V

width : 50ns



Observation :

Negative oscillations
due to the rising edge
and due to the falling
edge are

SYNCHRONIZED

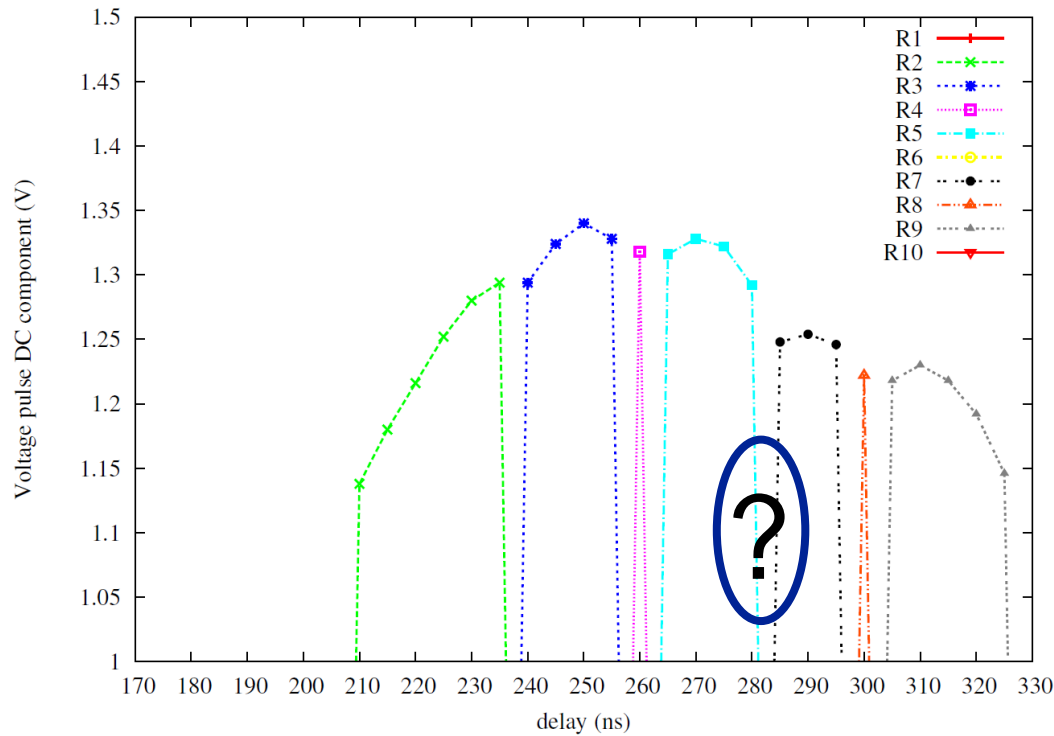
➤ **More efficient glitch
injection**

Glitch shaping



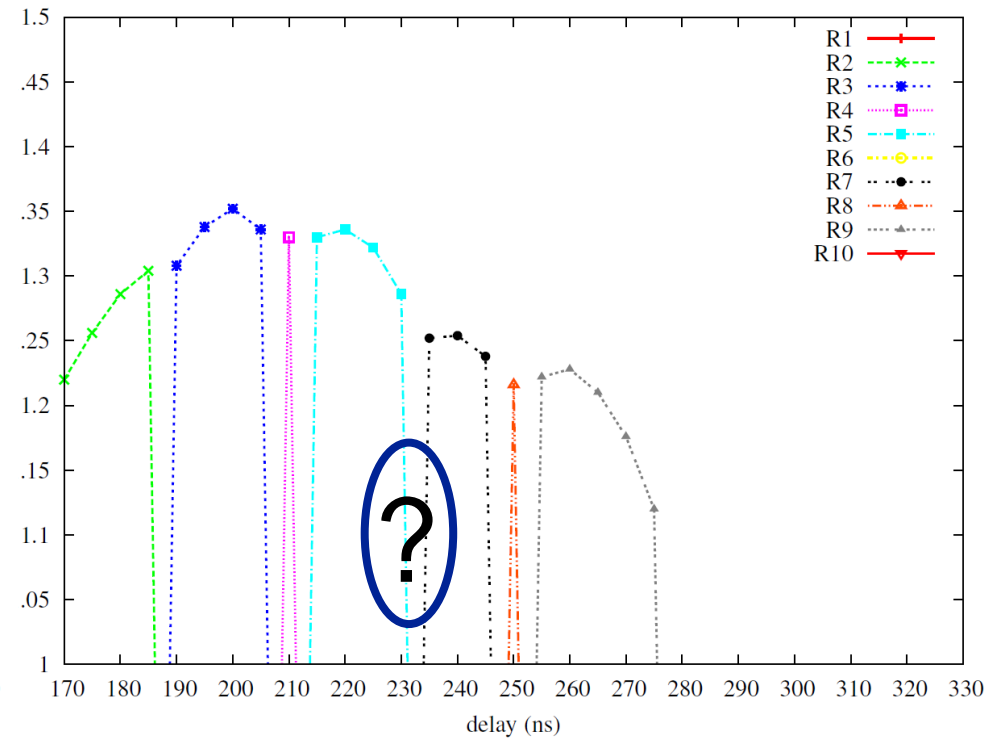
Injected faults comparison

(-14V | 100ns) : compensation



⇒ Same injected faults

(+8V | 50ns) : synchronization



⇒ Same temporal accuracy

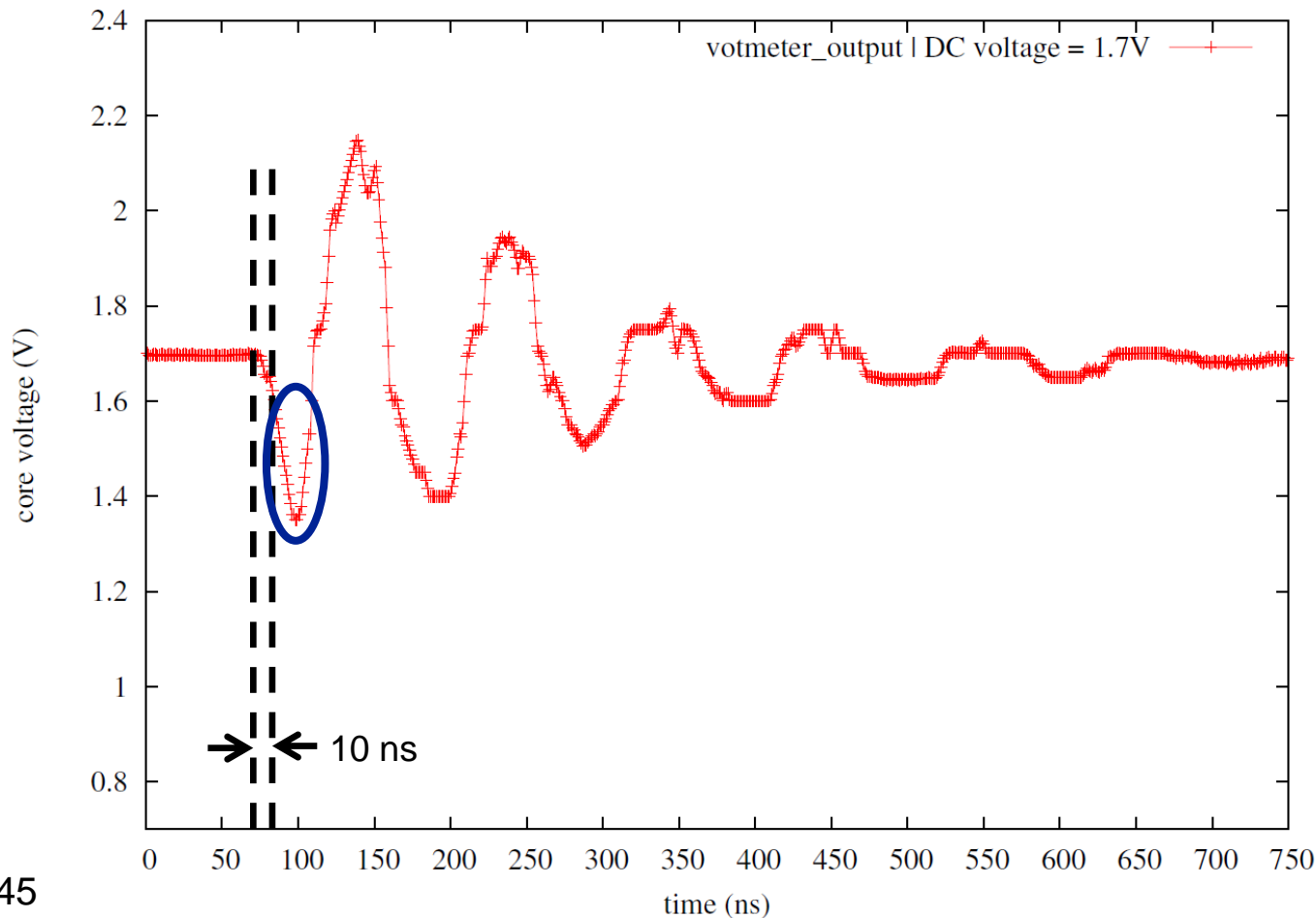
Glitch shaping



Sharpening

amplitude : -22V

width : 10ns



Observation :

Negative oscillation
due to the falling edge is

SHORTEN

by the **positive oscillation** due to the rising edge

➤ **More accurate glitch injection**

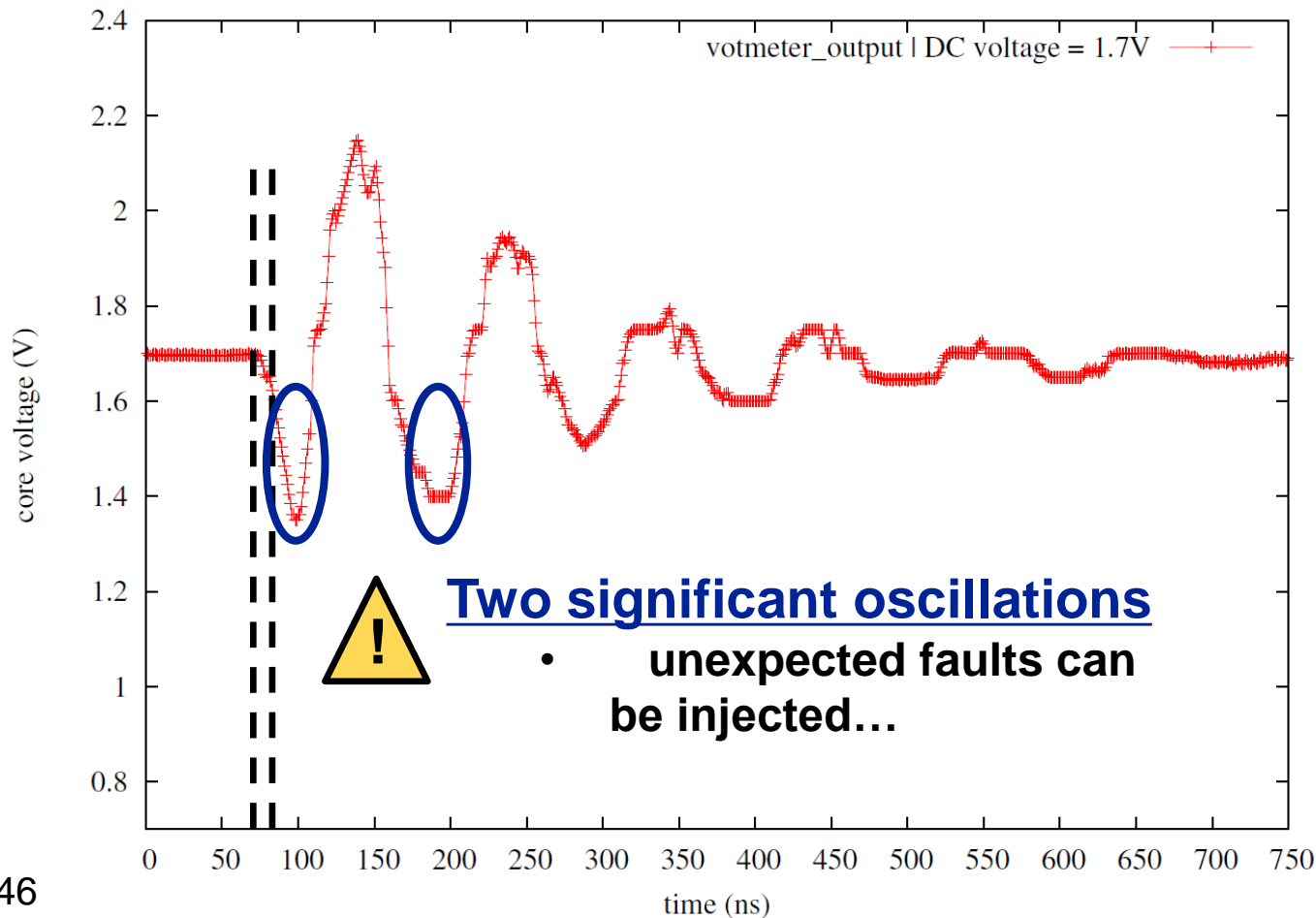
Glitch shaping



Sharping

amplitude : -22V

width : 10ns



Observation :

Negative oscillation due to the falling edge is

SHARPED

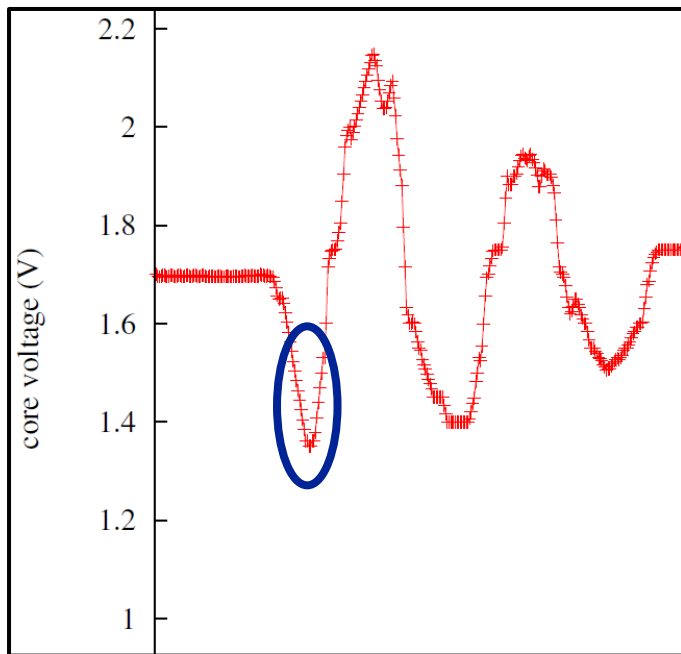
by the **positive oscillation** due to the rising edge

➤ **More accurate glitch injection**

Glitch shaping

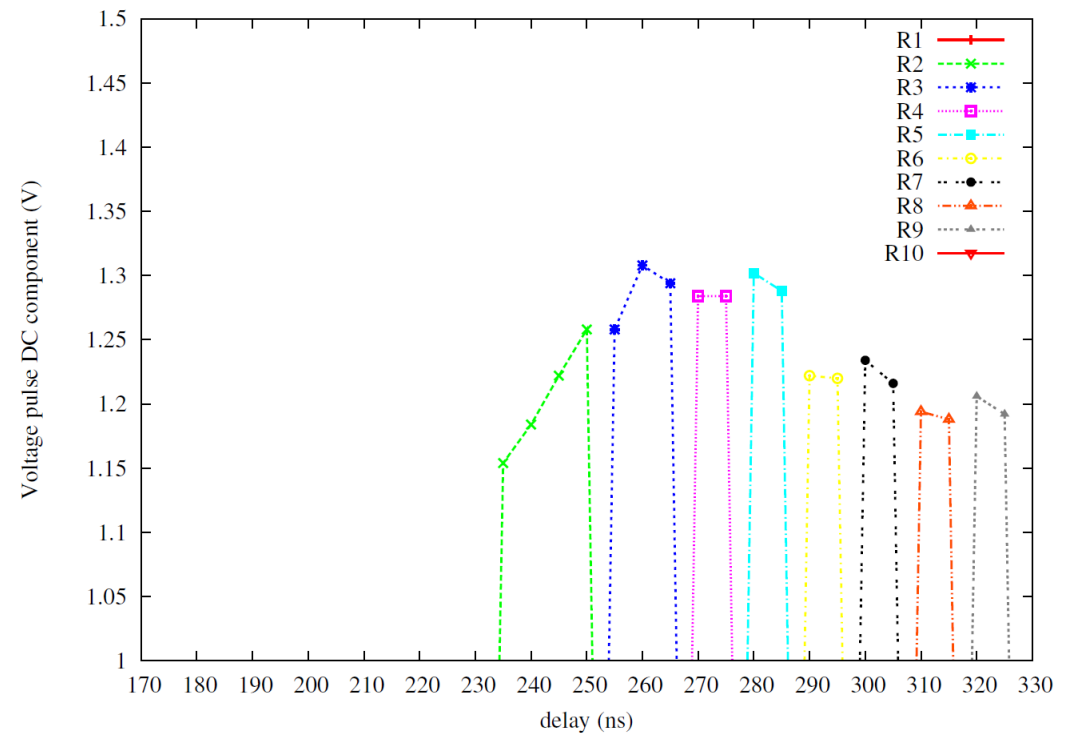


Injected faults comparison



⇒ Same injected faults

(-22V | 10ns) : sharpening

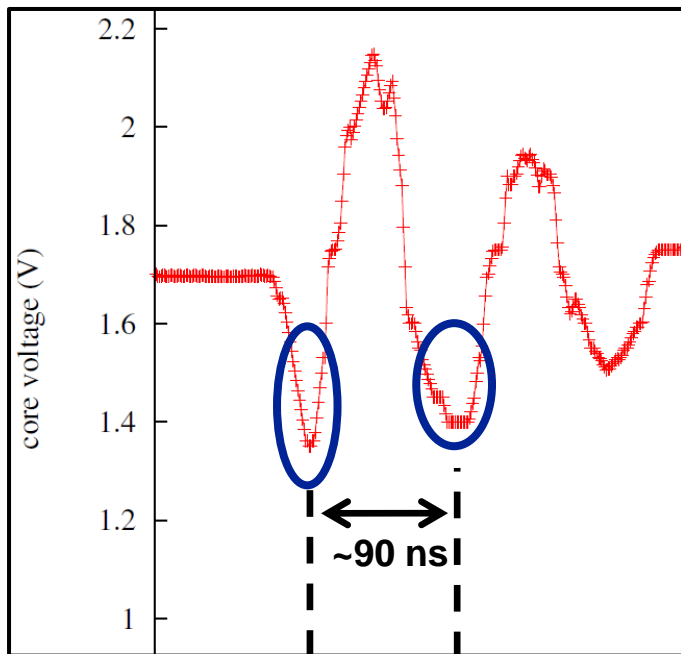


⇒ Very good temporal accuracy

Glitch shaping

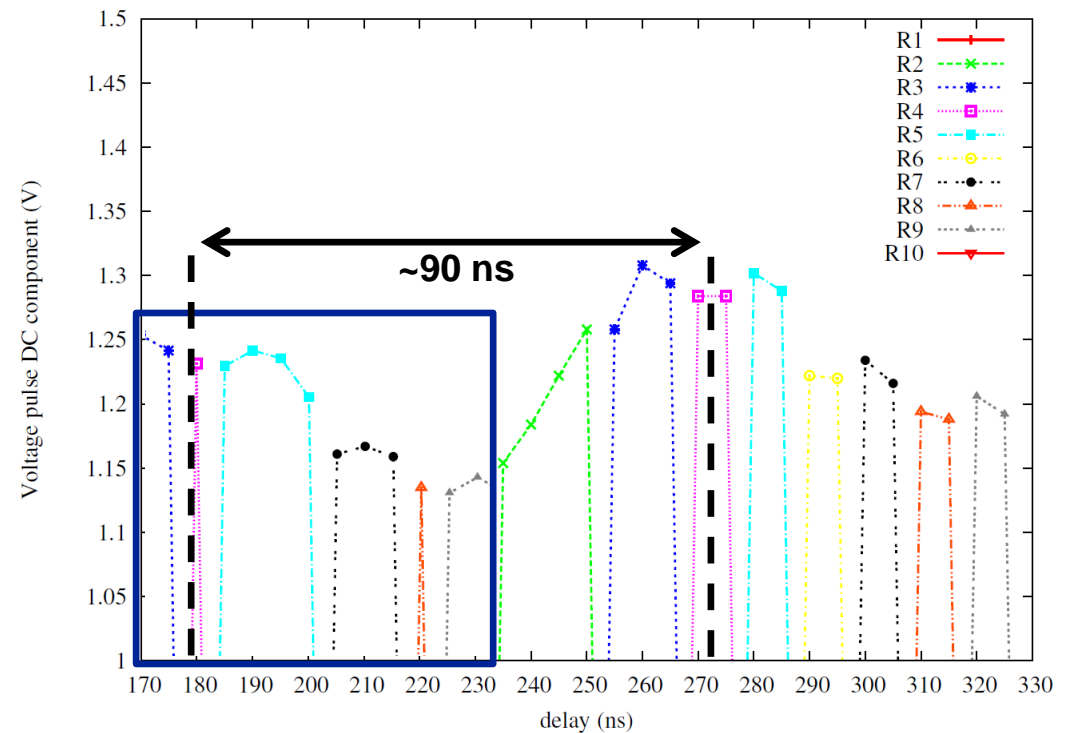


Injected faults comparison



⇒ Same injected faults

(-22V | 10ns) : sharpening



⇒ Very good temporal accuracy

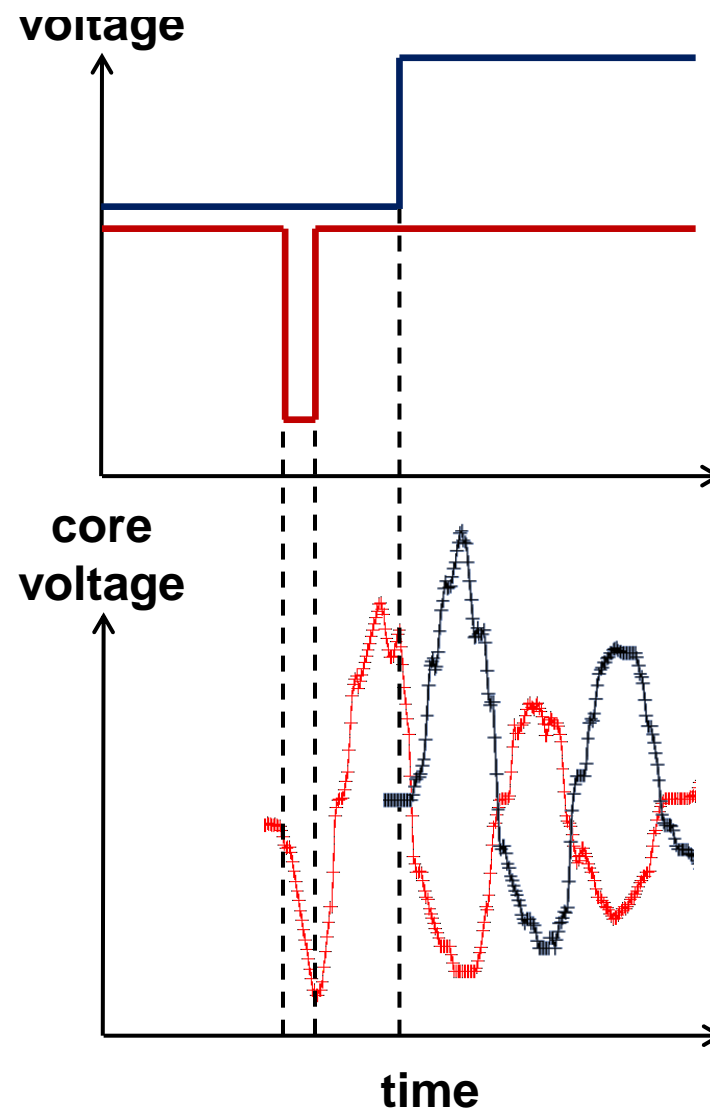
Glitch shaping



Fault injection mechanism



- A **short glitch** to **shorten** the first oscillation
- A **long glitch** to **compensate** the remaining oscillations





Fault injection mechanism & glitch shaping

Effective disturbances are **damping oscillations** due to the **rising** and **falling edges** of the injected glitch

Negative and **positive** glitches share the same fault injection mechanism : **timing constraint violation**

Damping oscillations due to the **rising** and **falling edges** of one or several injected glitches **can be “superimposed”** to shape the effective disturbance

Questions & Contact



www.emse.fr

INSPIRING INNOVATION | INNOVANTE PAR TRADITION

ZUSSA Loïc

PhD Student

Secure integrated circuits and physical fault injections

Download PDF version



zussa@emse.fr

loic.zussa.fr

880 route de Mimet 13541 Gardanne - FRANCE