DE LA RECHERCHE À L'INDUSTRIE

INSPIRING INNOVATION | INNOVANTE PAR TRADITION

Ecole Nationale Supérieure des Mines SAINT-ETIENNE

HOST 2014

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

Loïc ZUSSA

Jean-Max DUTERTRE

Jessy CLEDIERE

Bruno ROBISSON

MINISTÈRE DE L'ÉCONOMIE DE L'INDUSTRIE ET DE L'EMPLOI

Context

Thesis subject

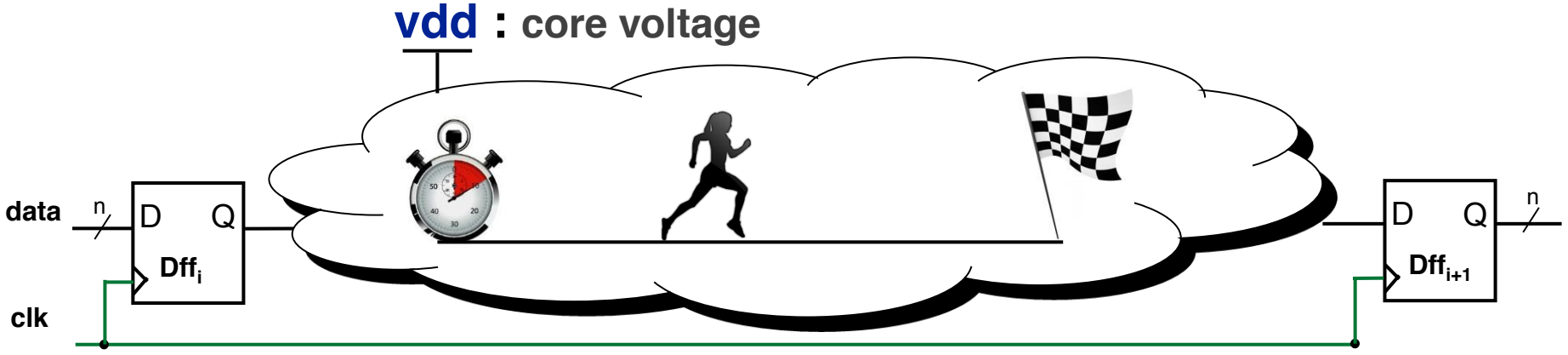
“Cryptanalysis of secure circuits by physical fault injections”

- Analysis of **fault injection** mechanisms related to **non-invasive physical disturbances**

In this presentation

- Analysis of fault **injection mechanism** related to **voltage glitches**
- Injection temporal resolution improving

Previous work



Under-powering a synchronous circuit make its **calculation time longer**

If the **calculation time** is **longer than the clock period** => **faults are injected**

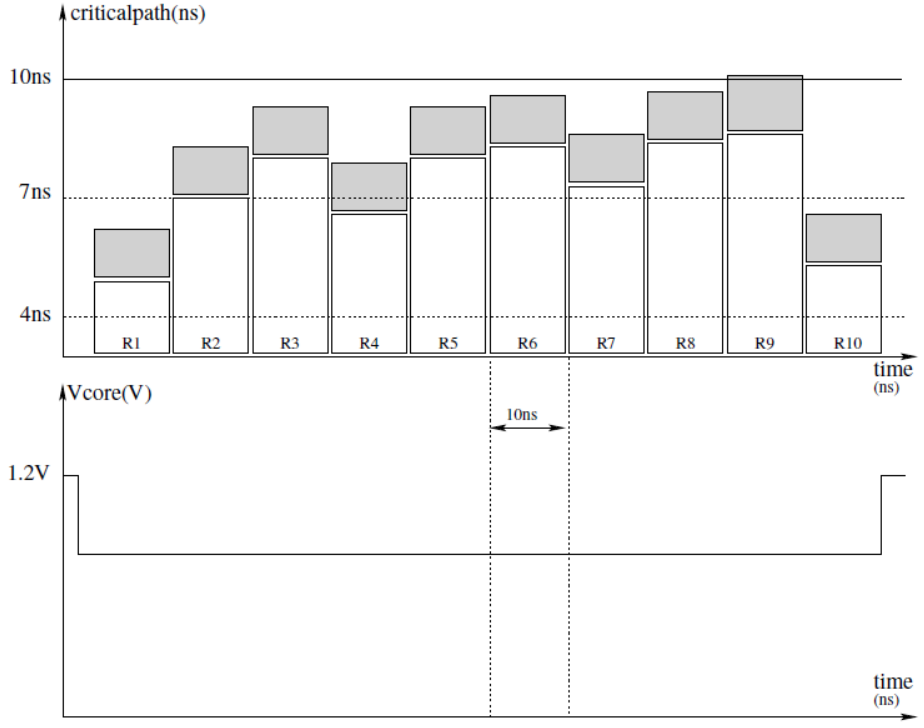
- DFFs sample data which are not up-to-date

The **longest calculation time** is called the **critical time**

Previous work

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 :

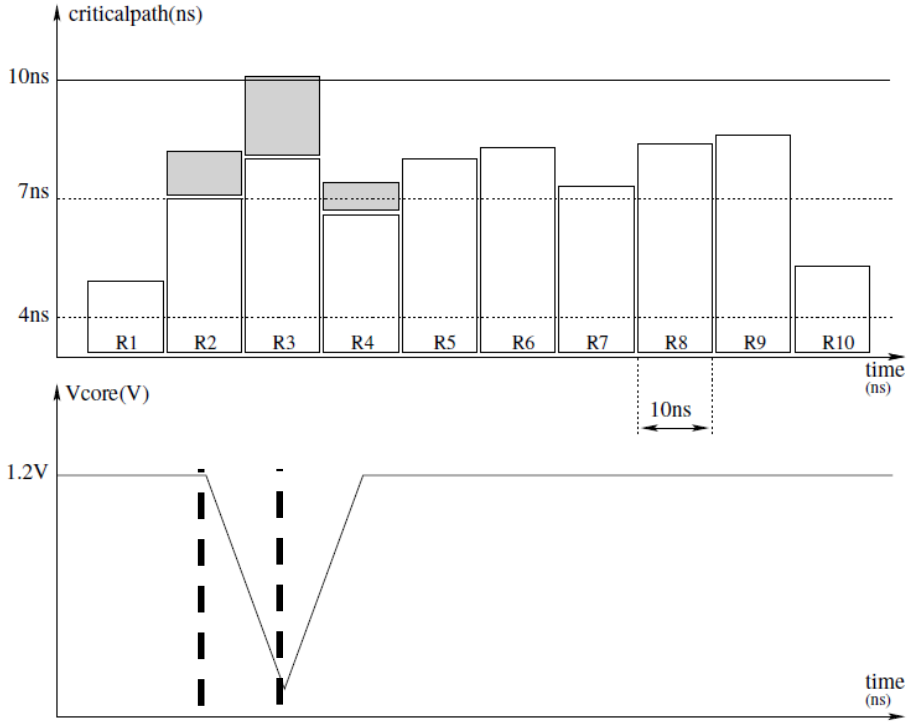
Underpowering the circuit make the **calculation times longer**

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

Previous work

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

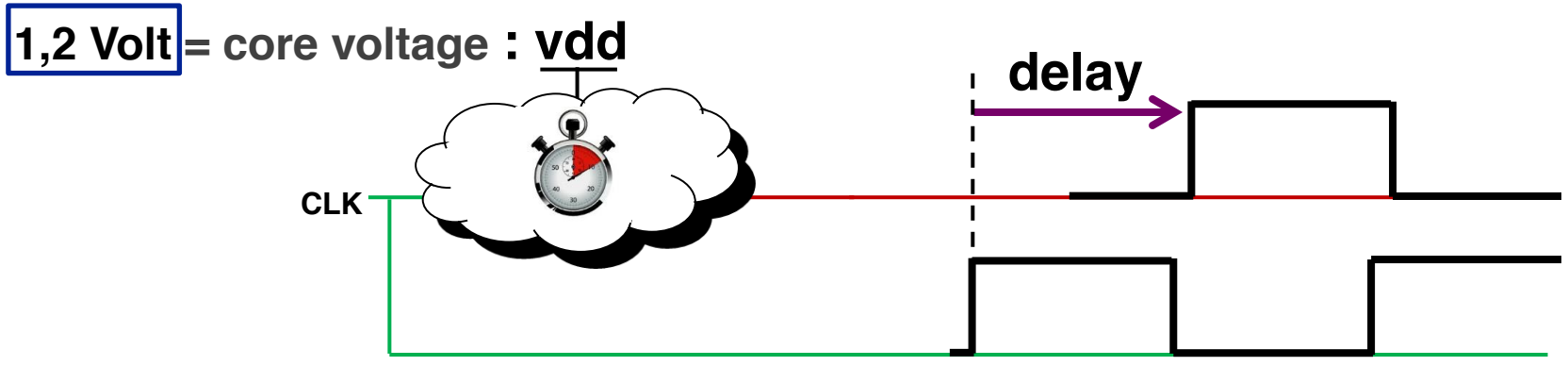
Agenda

- **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**

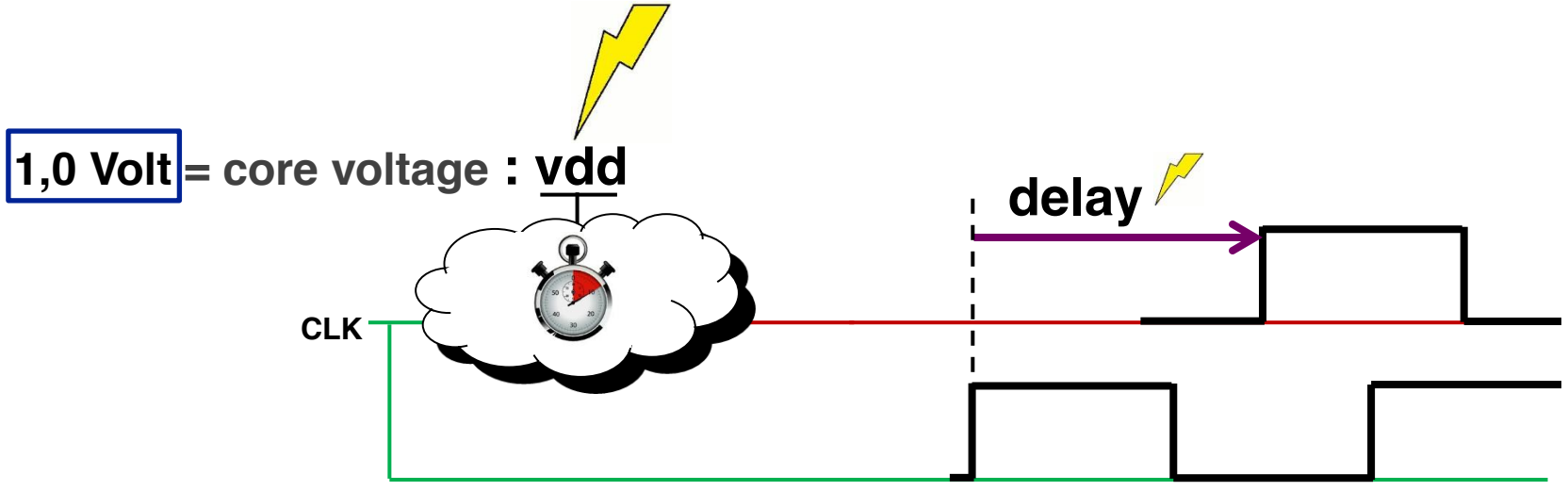
Measuring a propagation time **is equivalent** to measuring the core voltage



A delay-meter

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

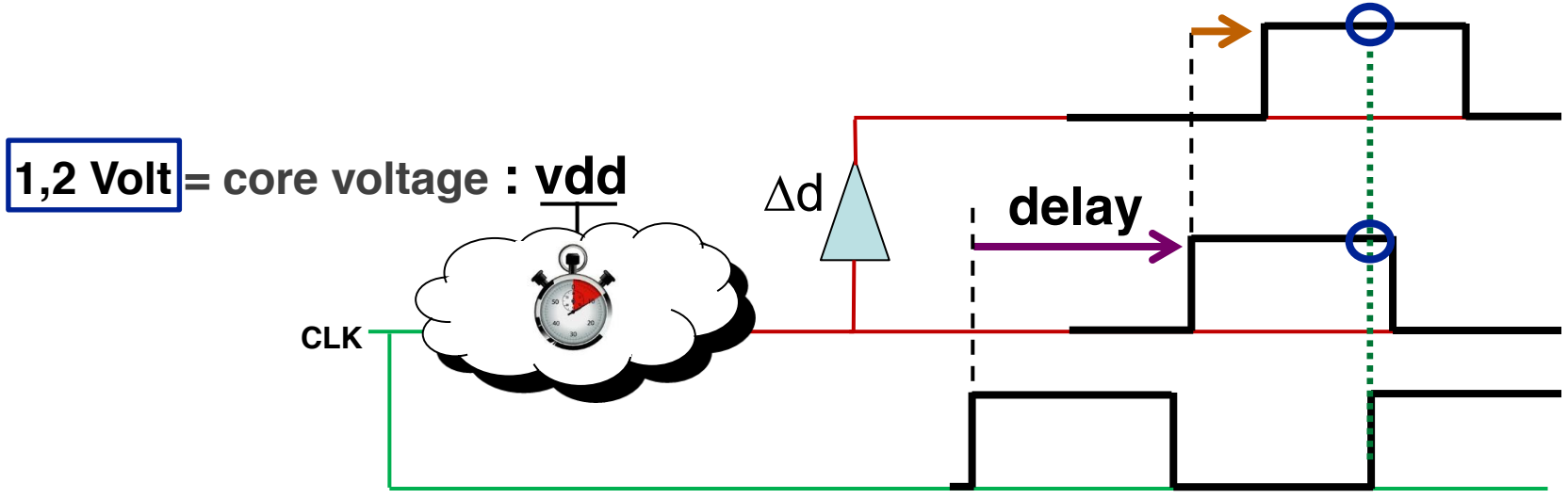
Measuring a propagation time **is equivalent** to measuring the core voltage



Time to digital converter

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

delay + **1** * Δd **<** clock period

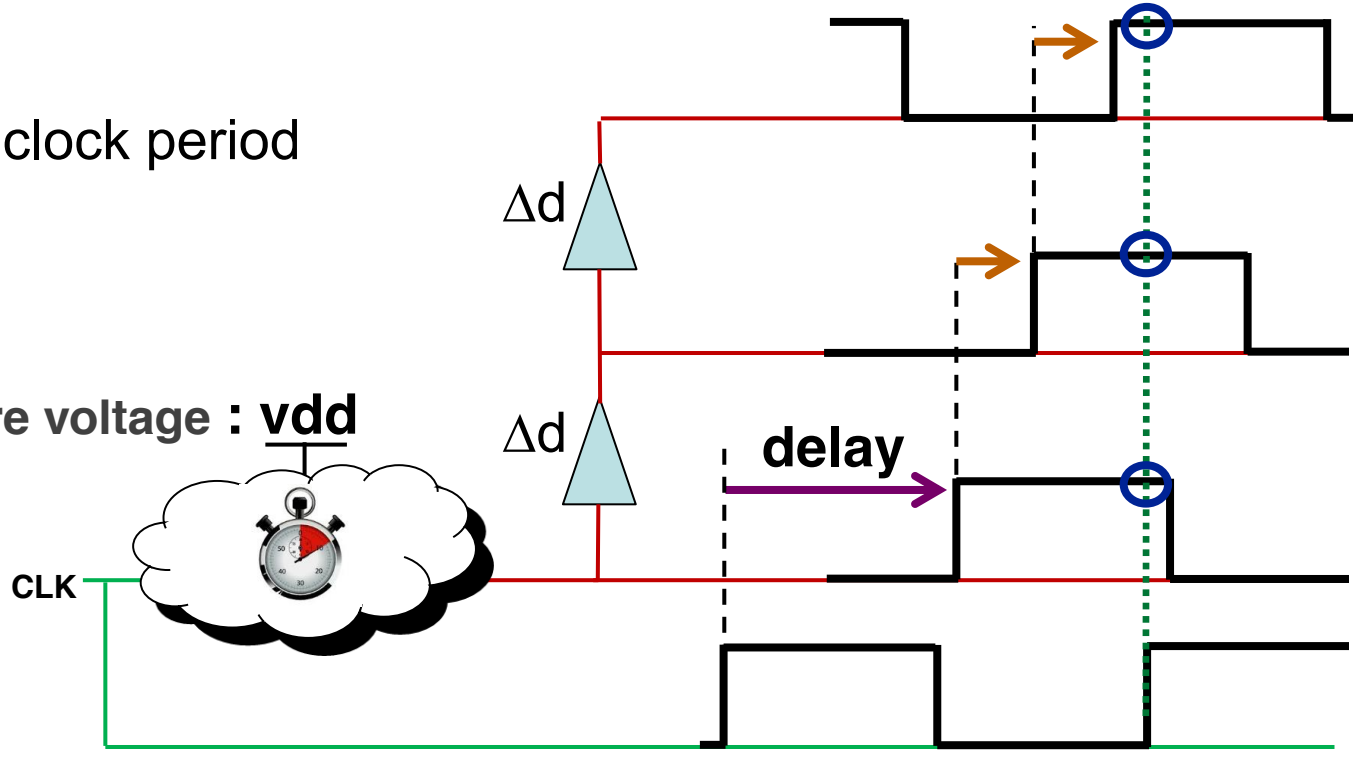


Time to digital converter

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

delay + **2** * Δd **<** clock period

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

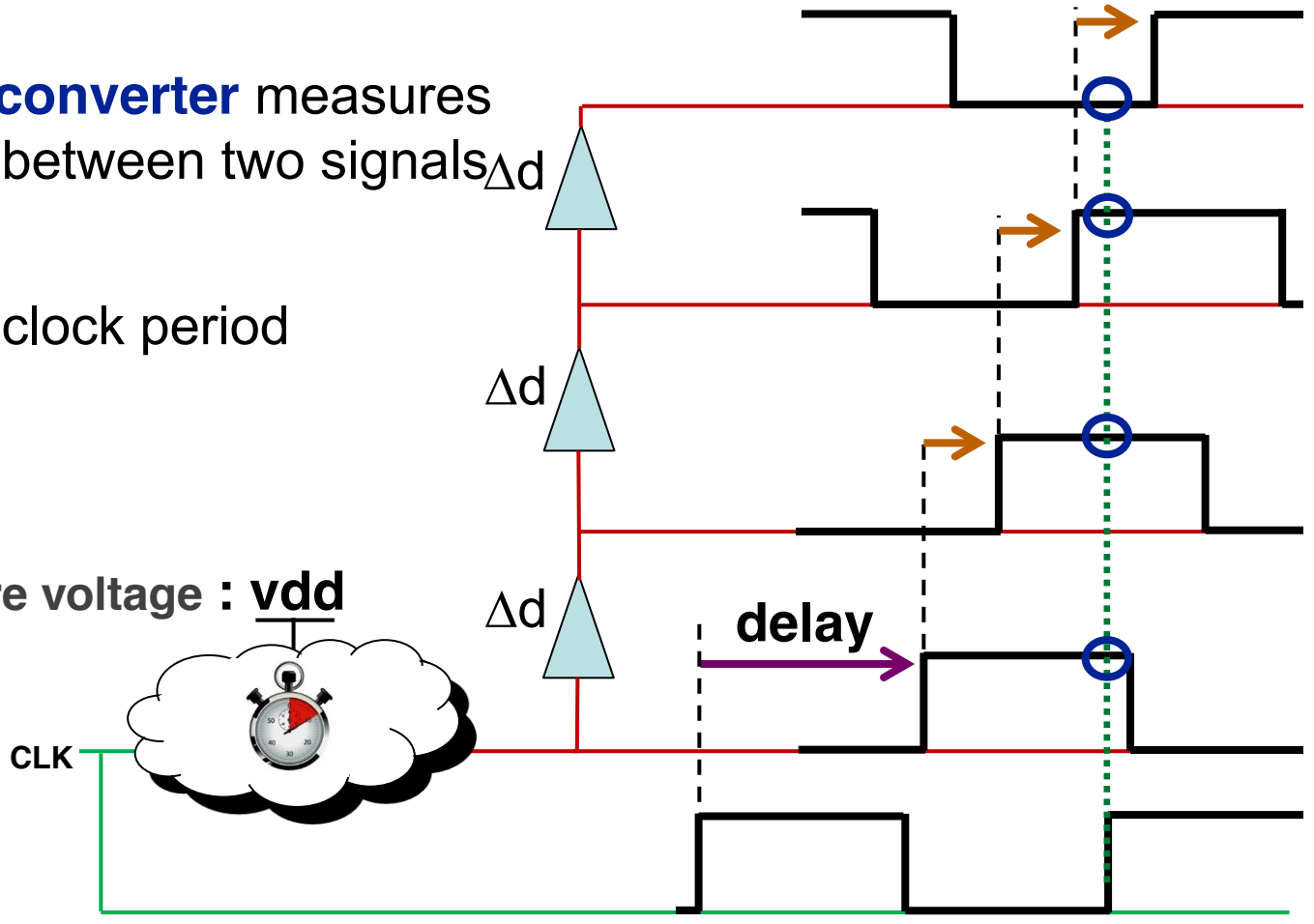


Time to digital converter

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

delay + **3** * Δd **>** clock period

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

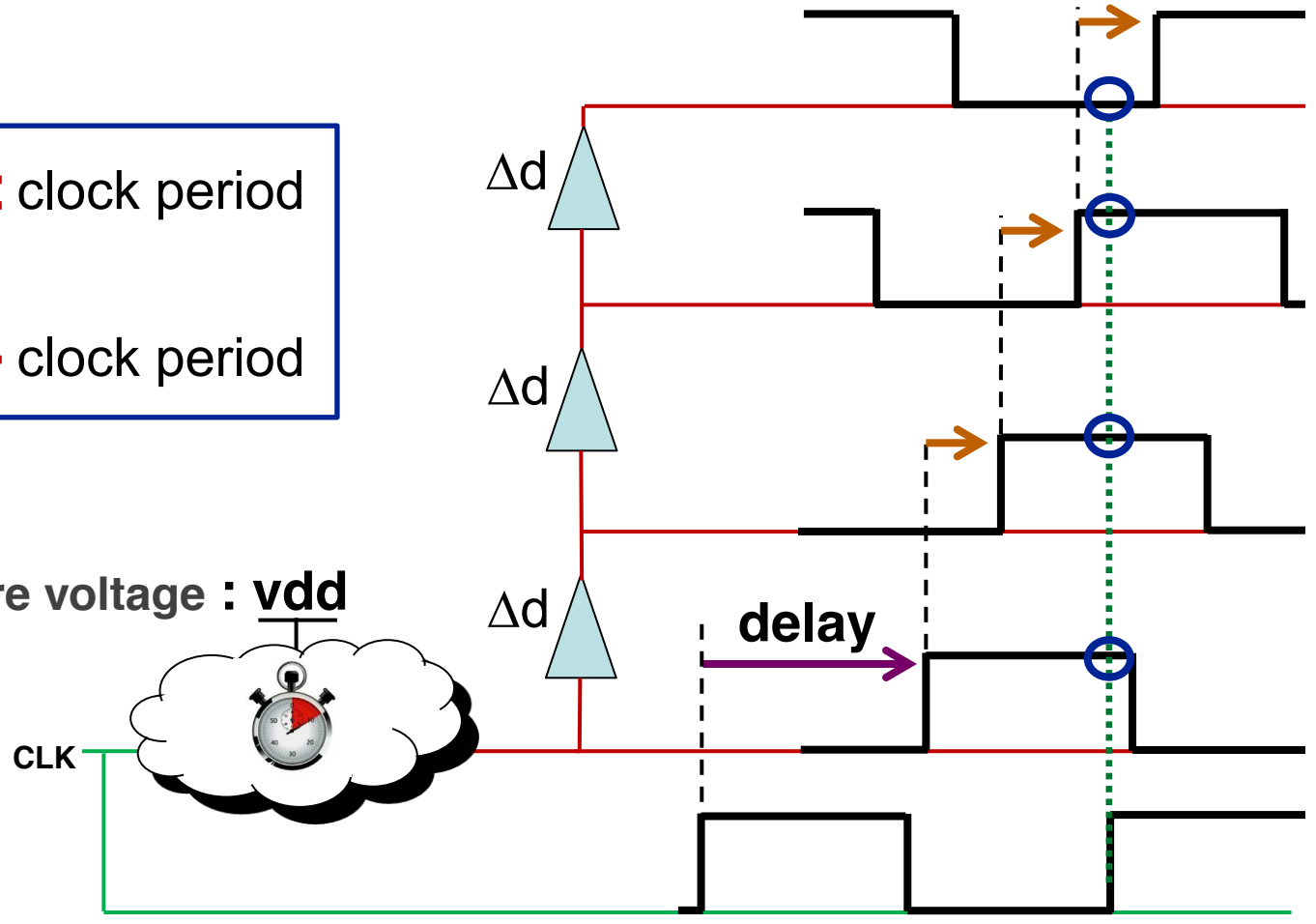


When undergoing a glitch injection

delay + **2** * Δd **<** clock period

delay + **3** * Δd **>** clock period

code = '1110' **1,2 Volt** = core voltage : **vdd**

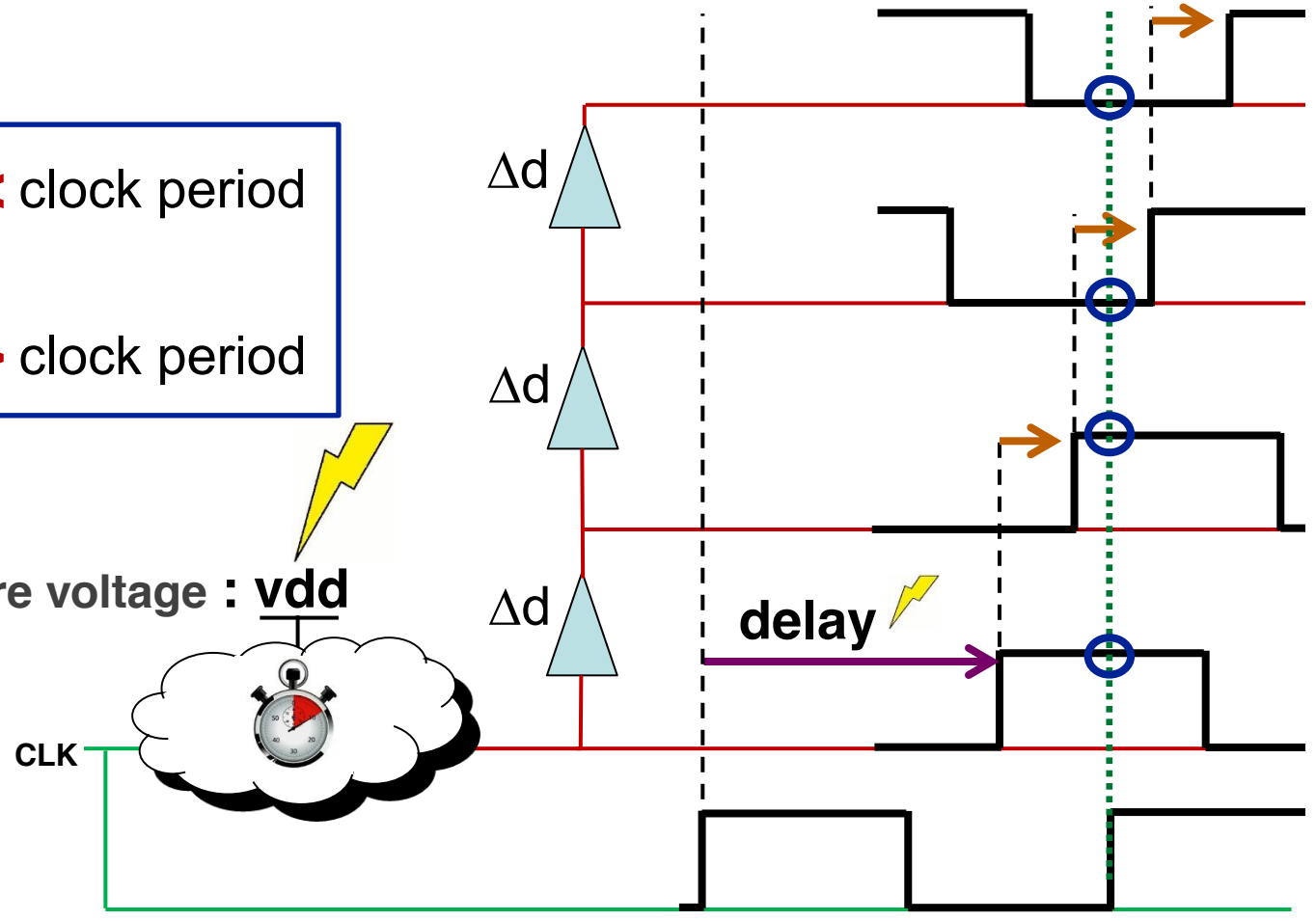


When undergoing a glitch injection

delay + **1** * Δd **<** clock period

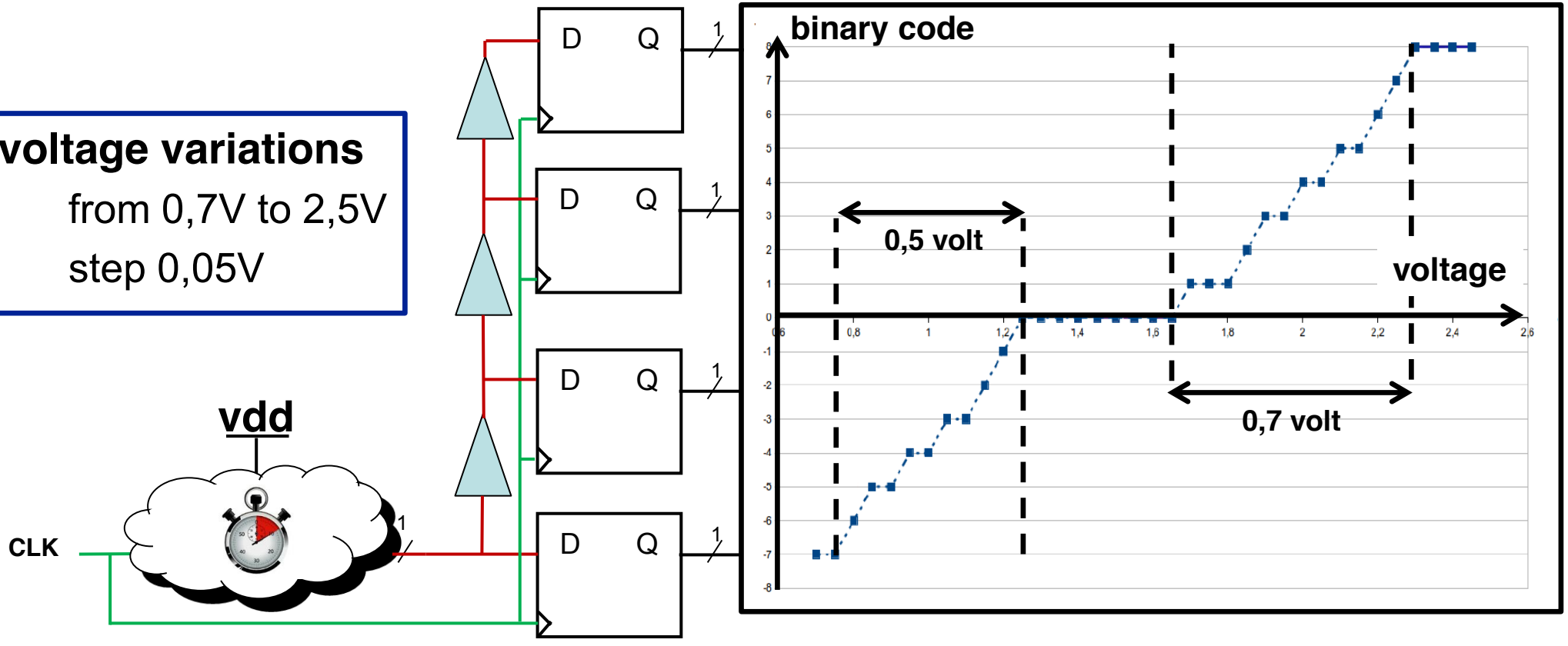
delay + **2** * Δd **>** clock period

code = '1100' **1,0 Volt** = core voltage : **vdd**



Library : voltage <> code

voltage variations
from 0,7V to 2,5V
step 0,05V



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

Library : voltage <> code

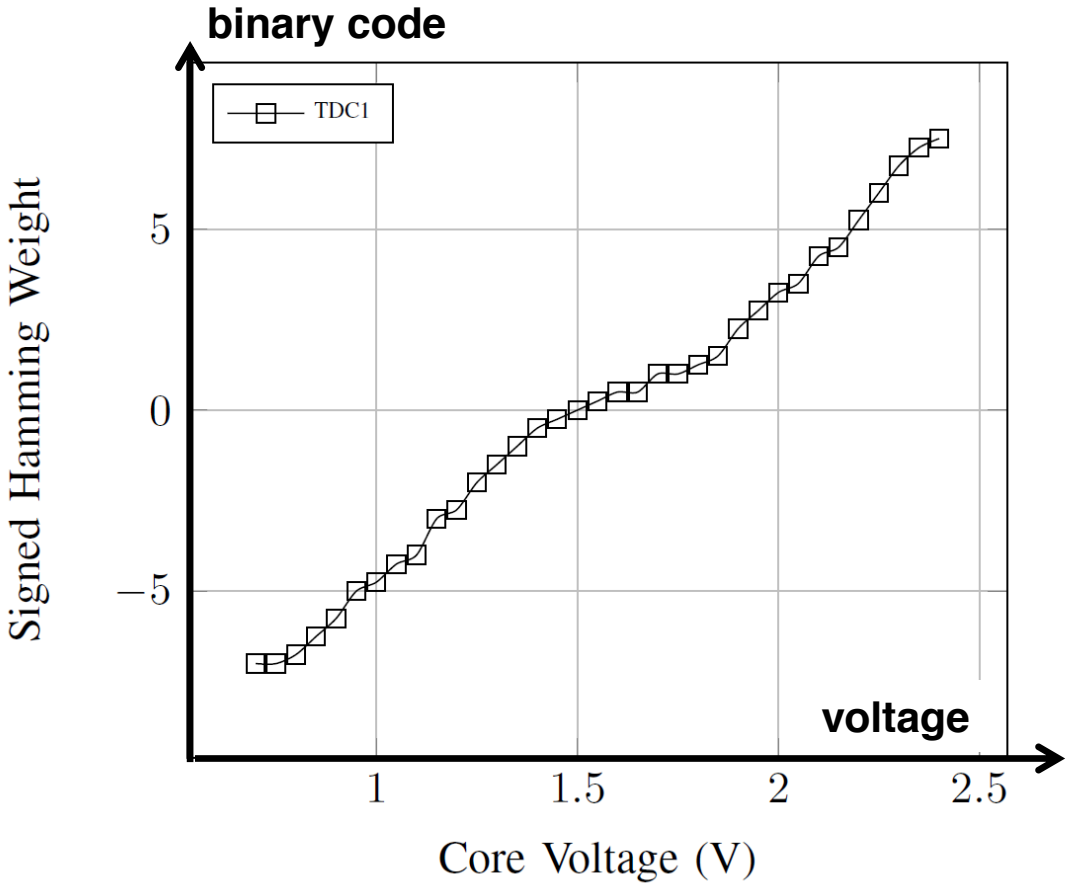
4 voltmeters implemented :

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

Only one “linear” zones

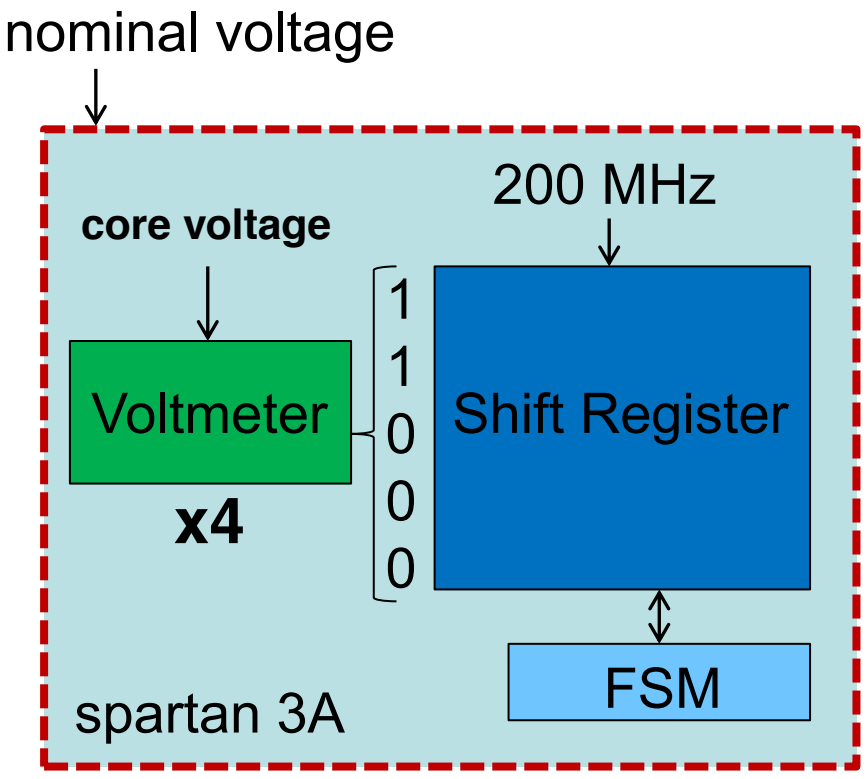
=> **resolution improving**

No “blind” zone



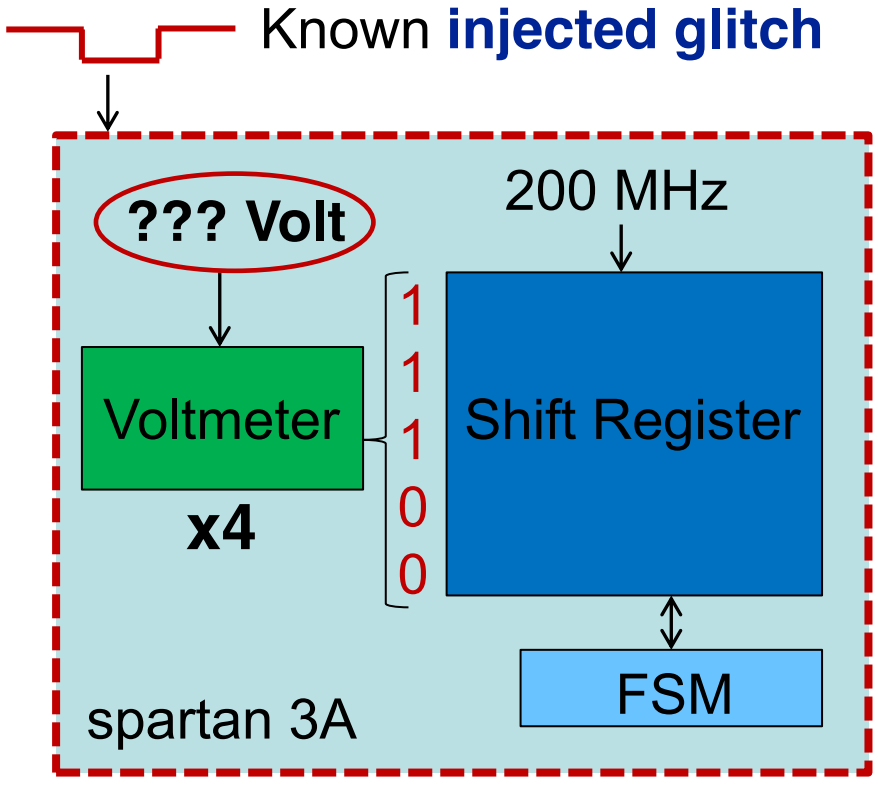
Experimental setup

Acquisition setup



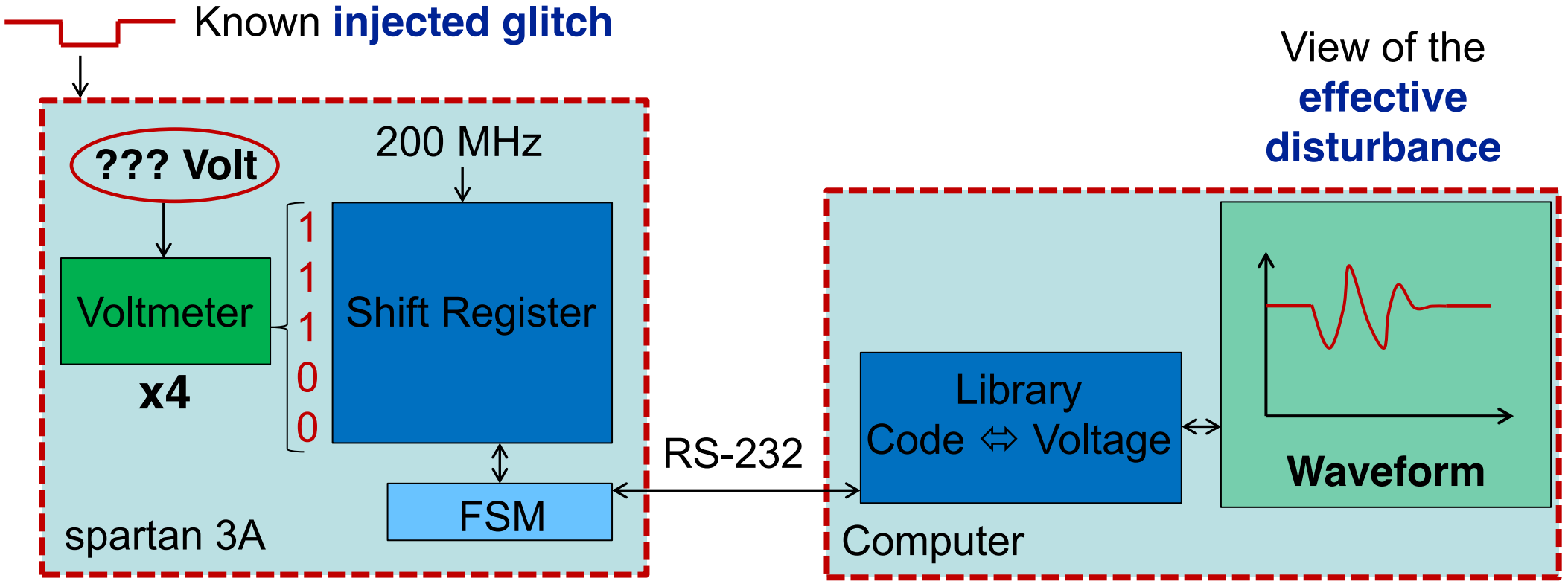
Experimental setup

Acquisition setup



Experimental setup

Acquisition setup

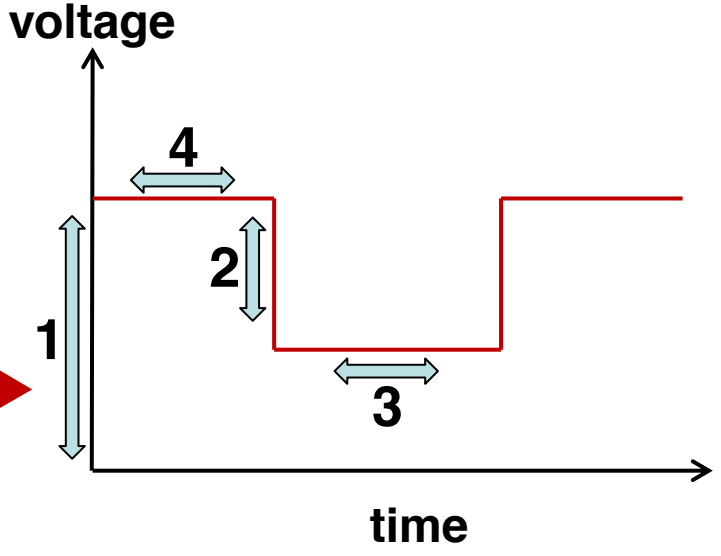


Experimental setup

Glitches injection setup

Pulse generator variables :

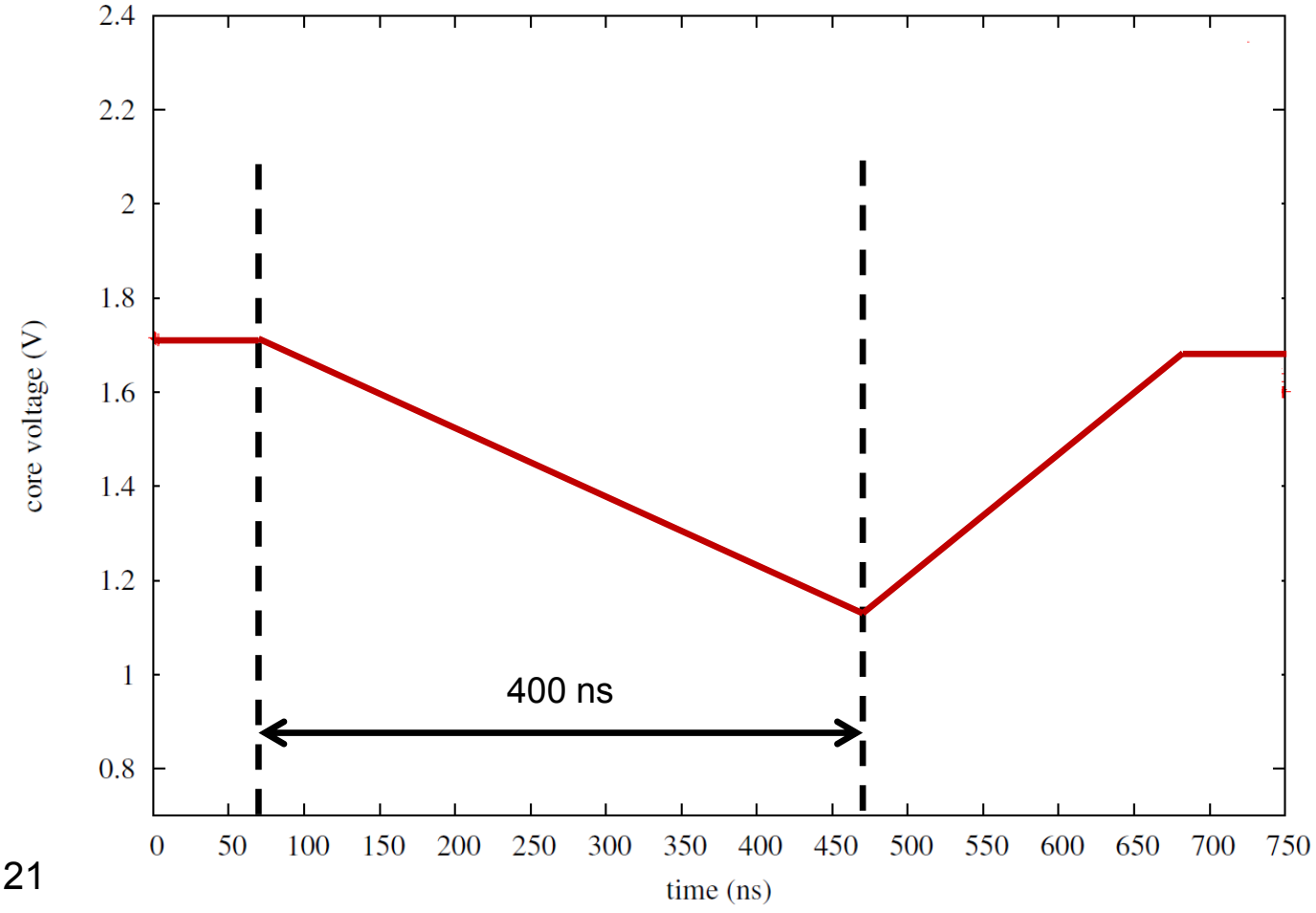
1. DC offset (Volts)
2. Amplitude (Volts)
3. Width (ns)
4. Delay (ns)



Experimental results

Negative voltage glitch : what I expected

amplitude : -14V **width** : 400ns



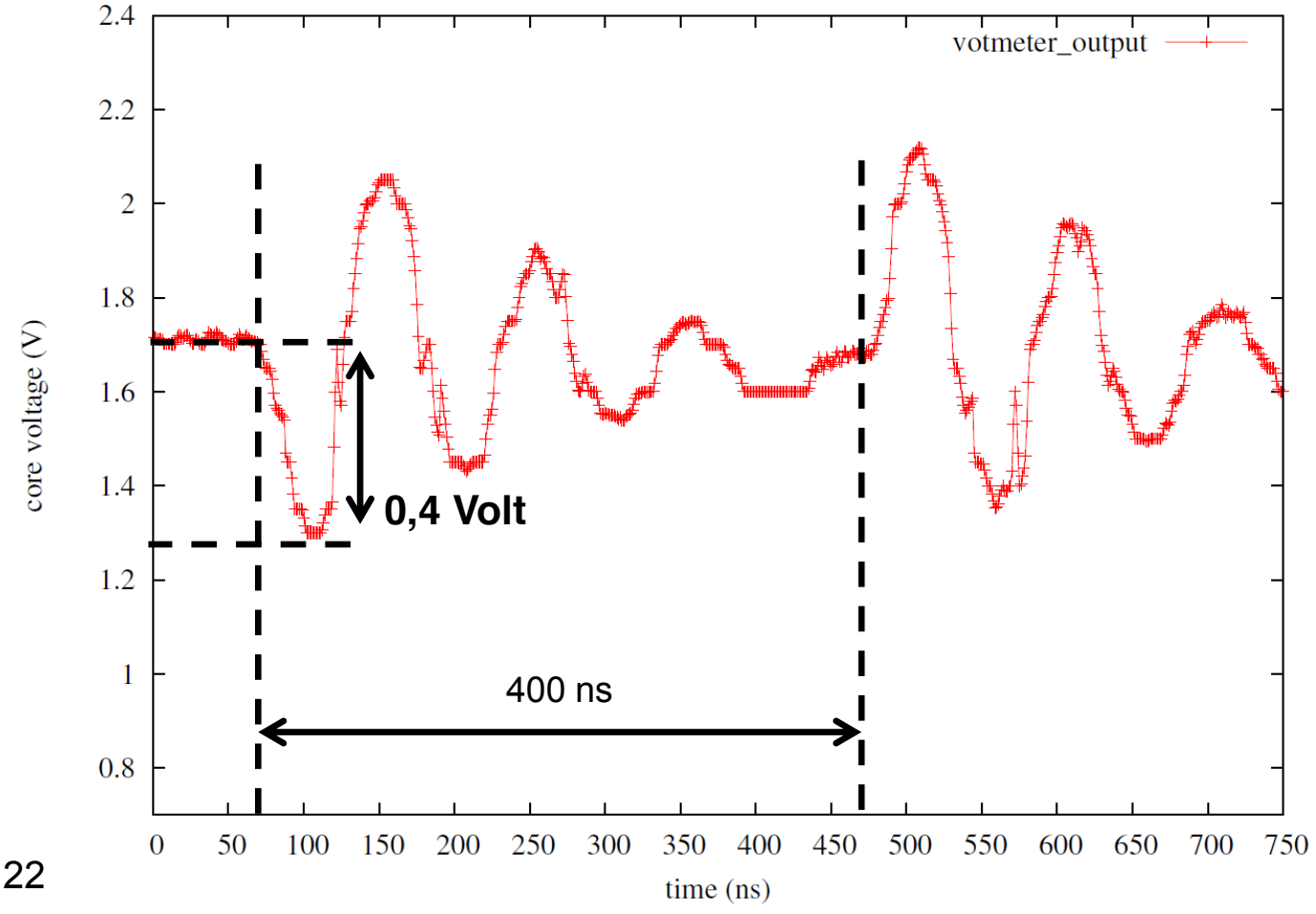
Expectation :

Filtered signal due to the **input capacitances**

Experimental results

Negative voltage glitch : what it is !

amplitude : -14V **width** : 400ns



Observation :

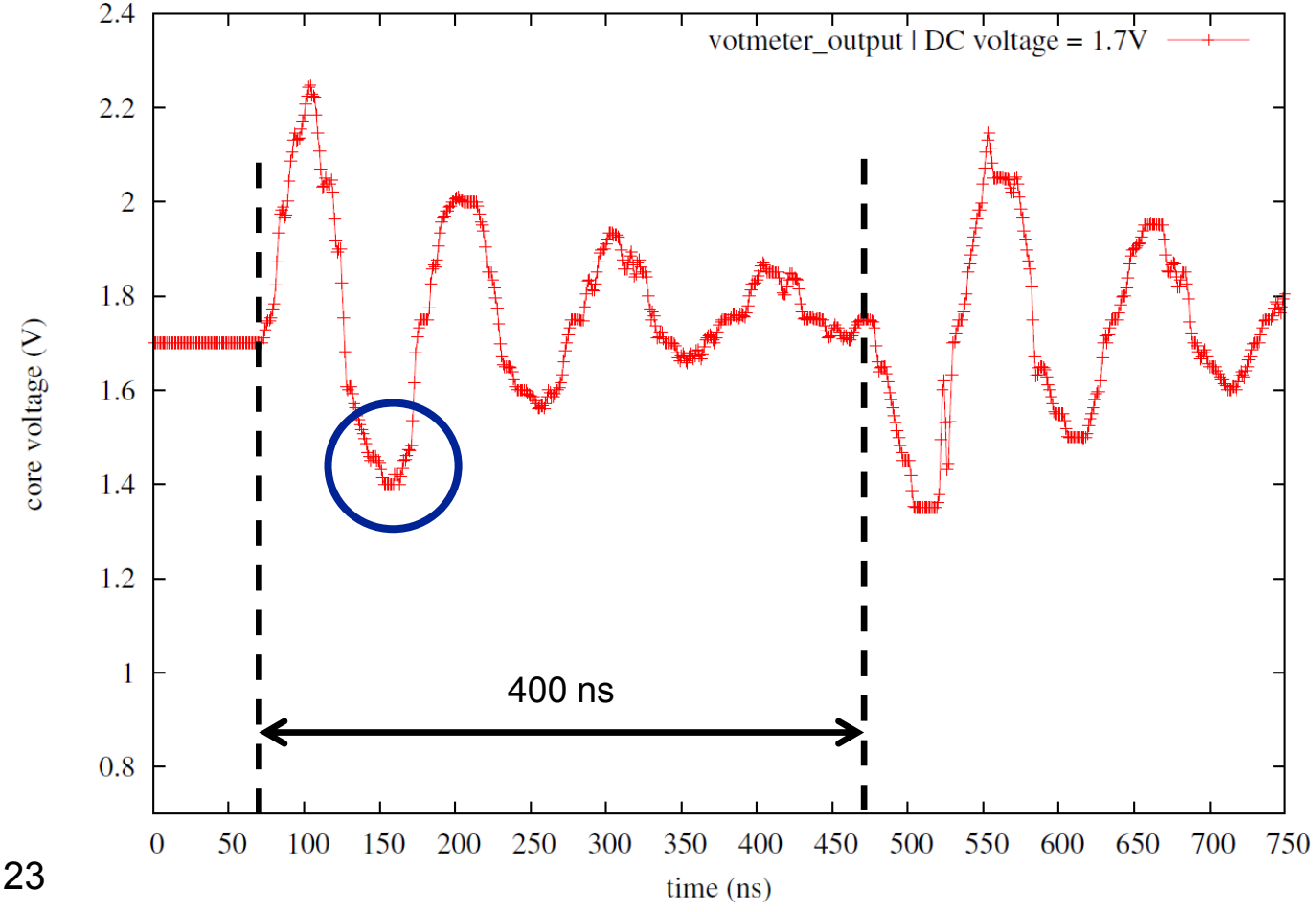
2 sets of **damping oscillations**

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

Experimental results

Positive voltage glitch

amplitude : **+**14V **width** : 400ns

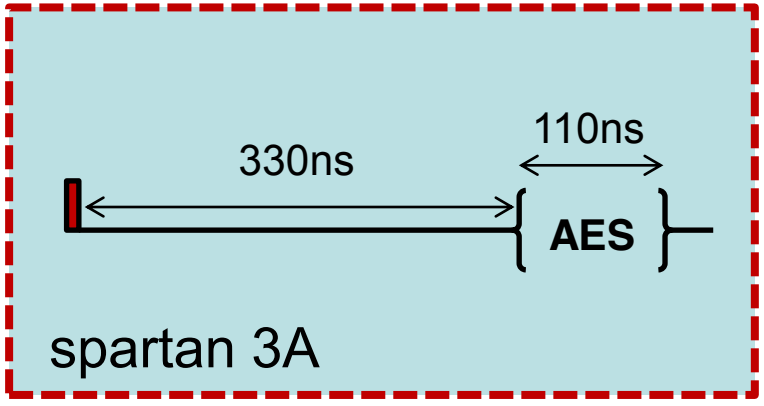


Observation :

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



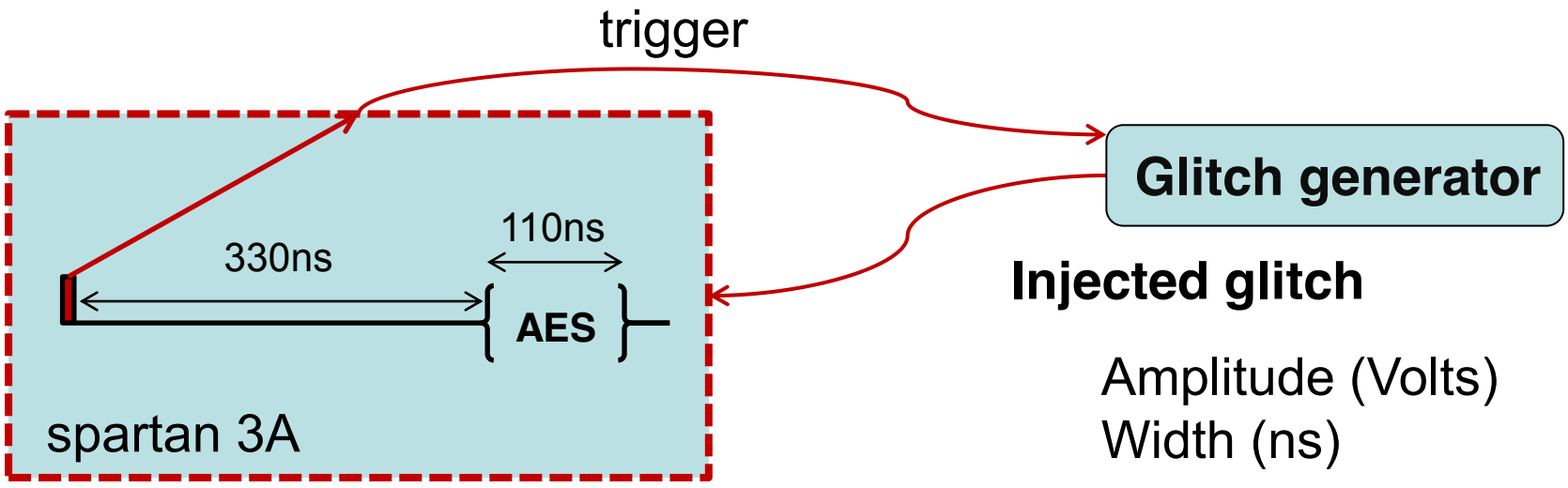
Target

AES 128bit - **100MHz**

Fault injection synchronization

Trig signal 330 ns before the AES calculation

Fault injection protocol



Injected glitch

Amplitude (Volts)
Width (ns)

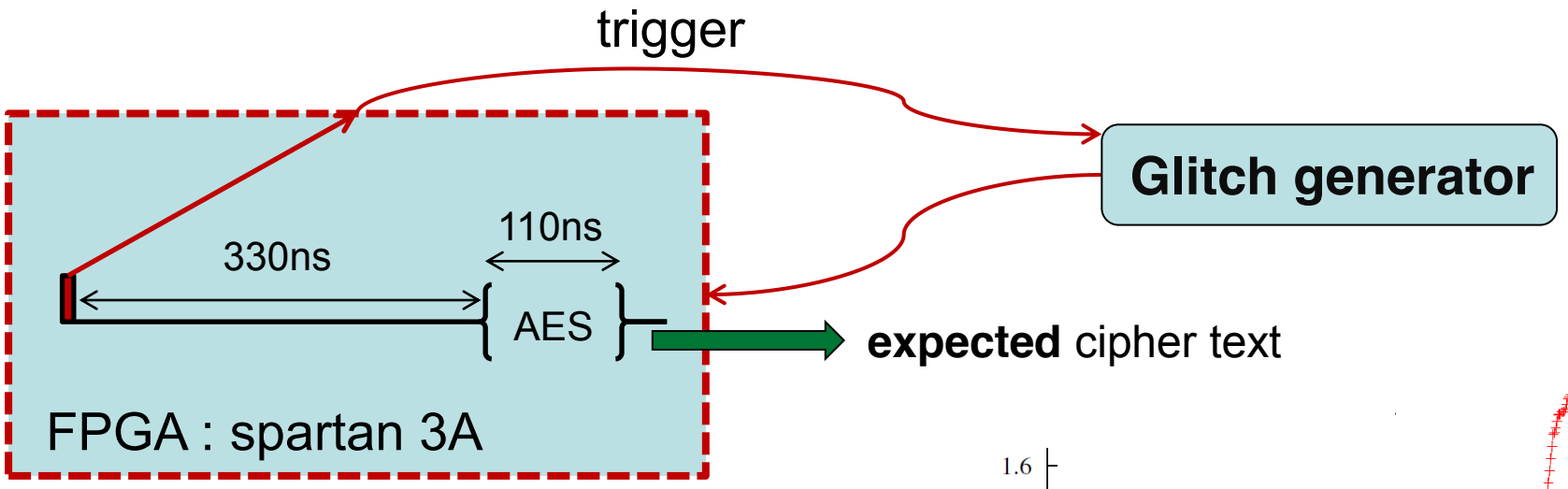
Variables

DC offset from **1,4** to **1,1 Volts**
Delay from **170** to **330 ns**

AES 128bit : 11 rounds - **100MHz**

Characterization

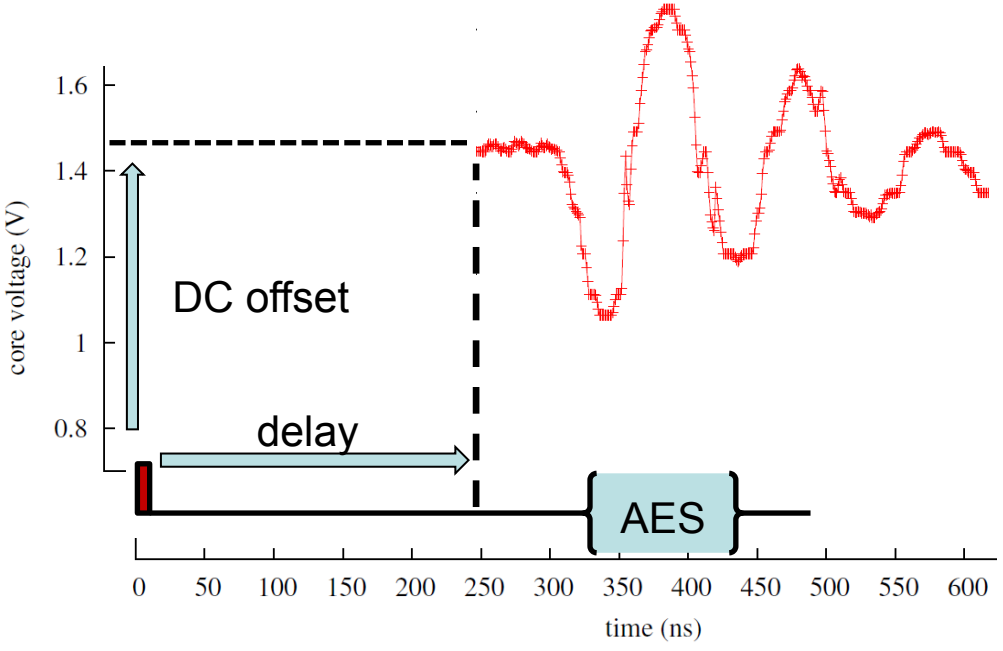
Fault injection protocol



AES 128bit : 11 rounds - **100MHz**

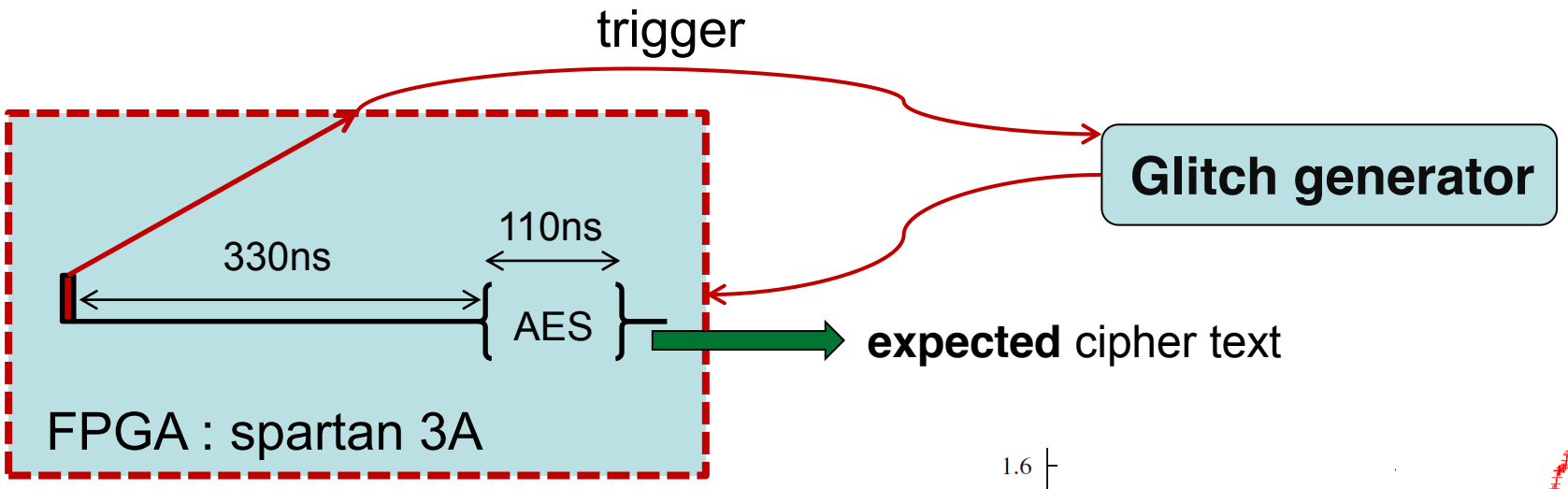
DC offset from **1,4** to **1,1 Volts**

Delay from **170** to **330 ns**



Characterization

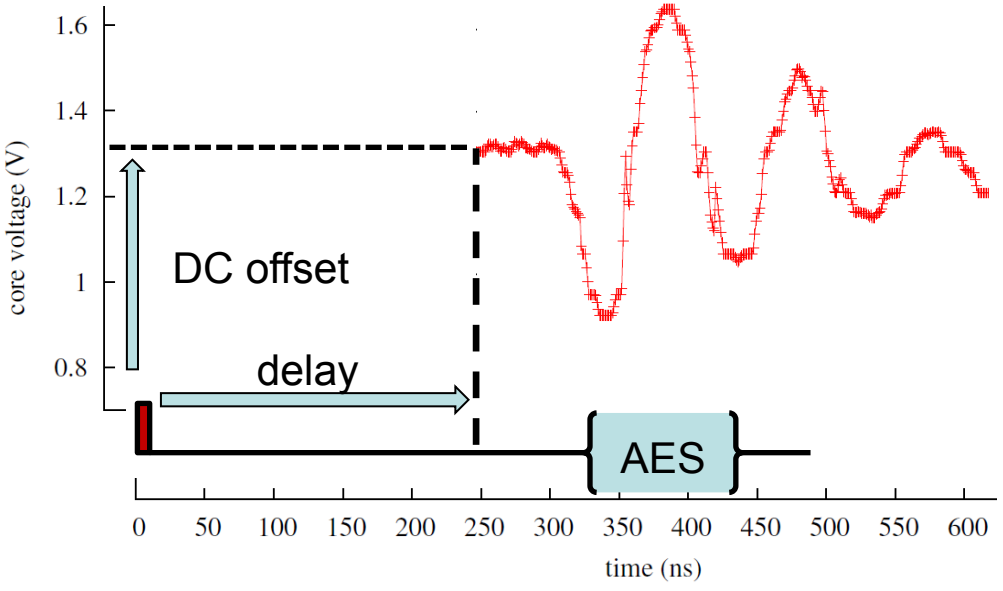
Fault injection protocol



AES 128bit : 11 rounds - **100MHz**

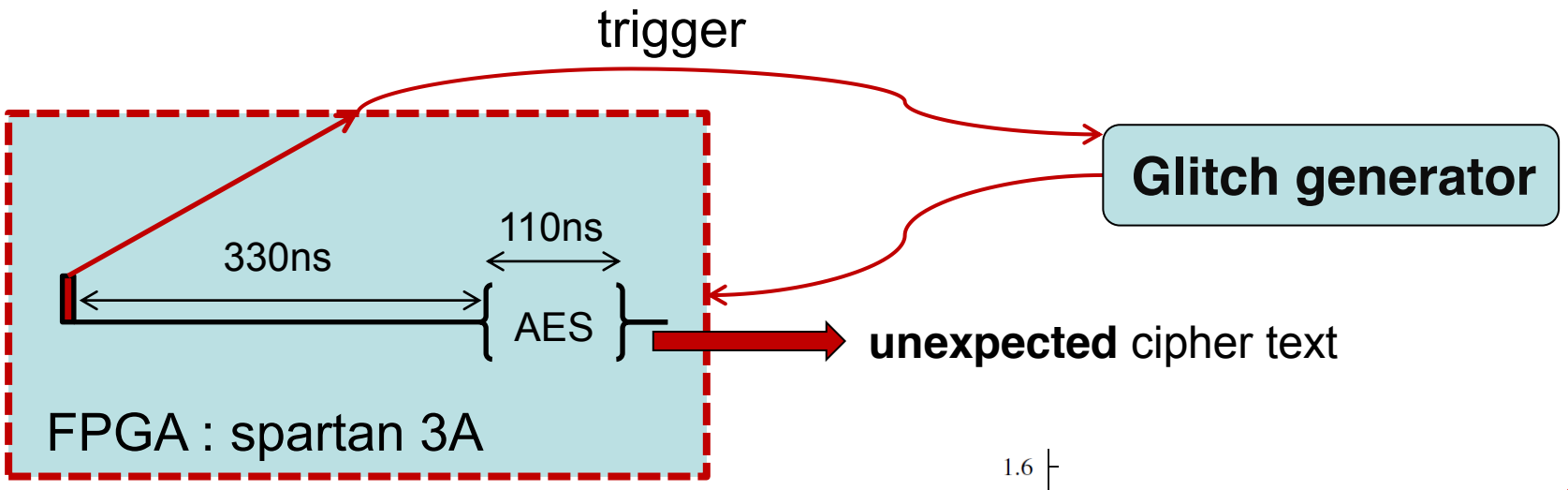
DC offset from **1,4** to **1,1 Volts**

Delay from **170** to **330 ns**



Characterization

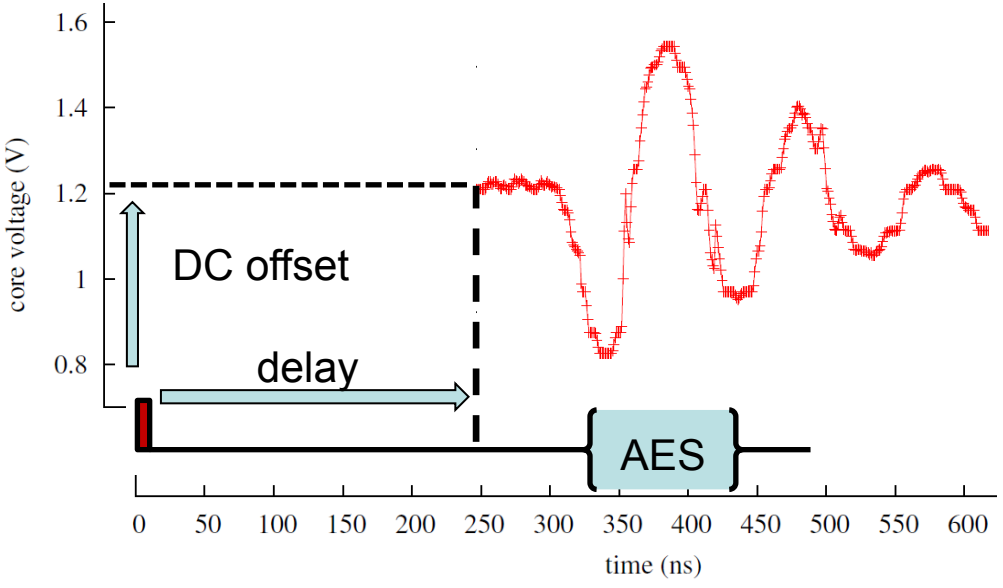
Fault injection protocol



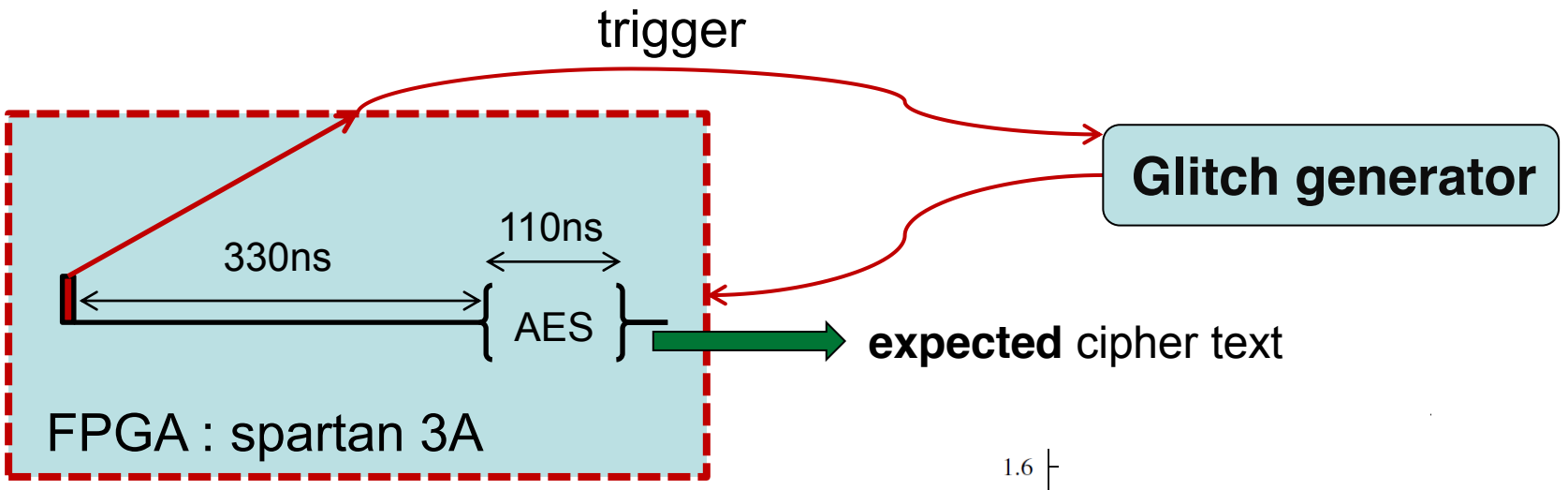
AES 128bit : 11 rounds - **100MHz**

DC offset from **1,4** to **1,1 Volts**

Delay from **170** to **330 ns**



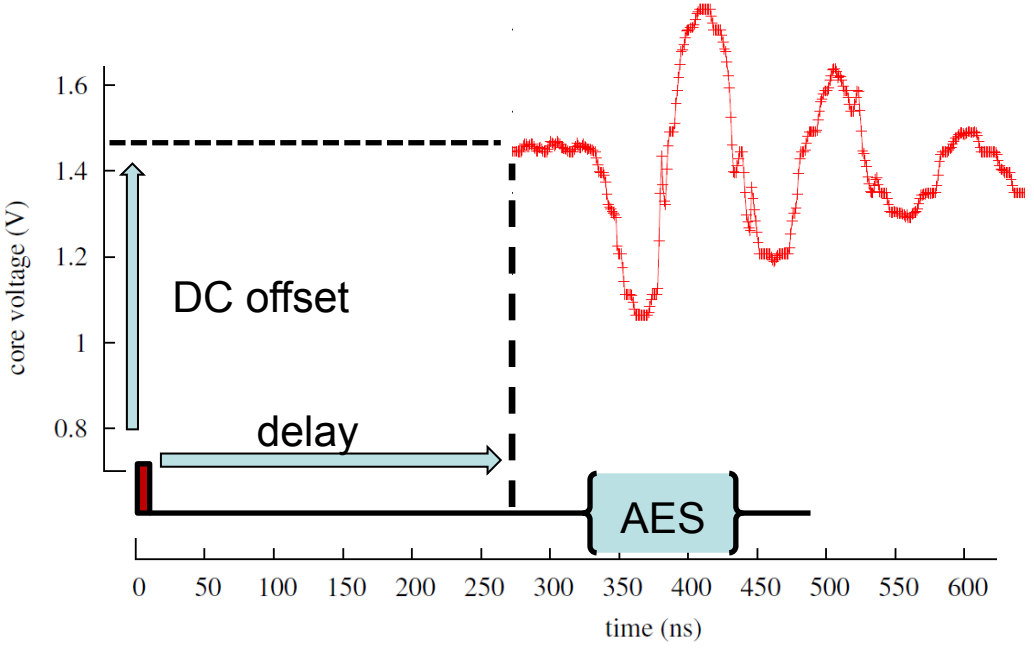
Fault injection protocol



AES 128bit : 11 rounds - **100MHz**

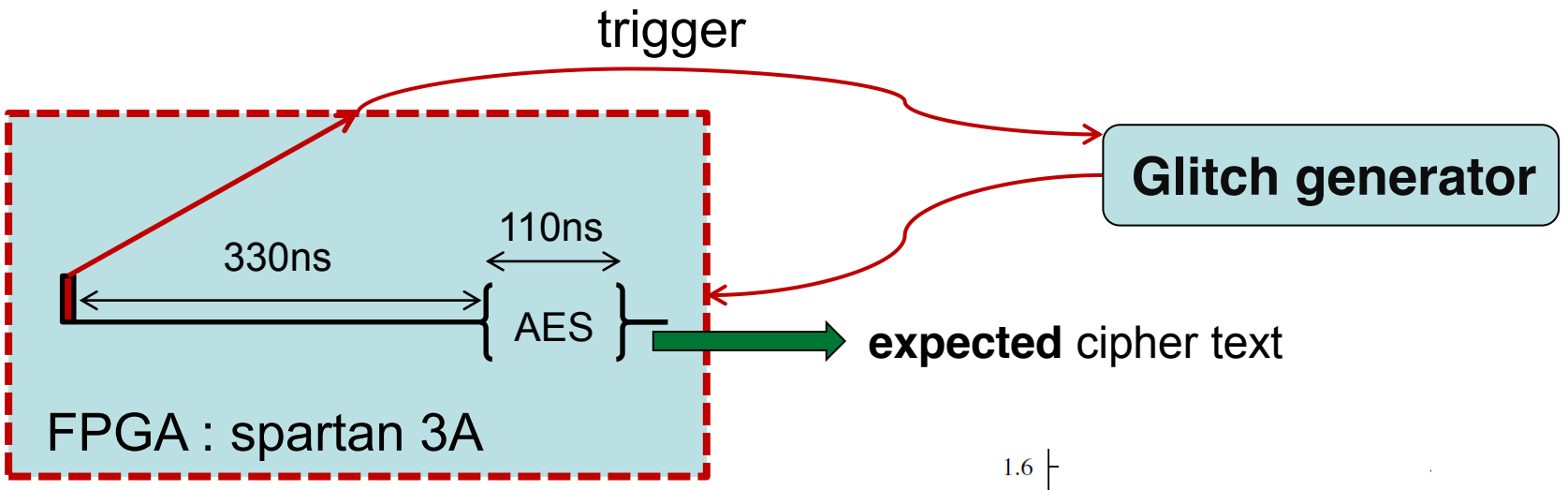
DC offset from **1,4** to **1,1 Volts**

Delay from **170** to **330 ns**



Characterization

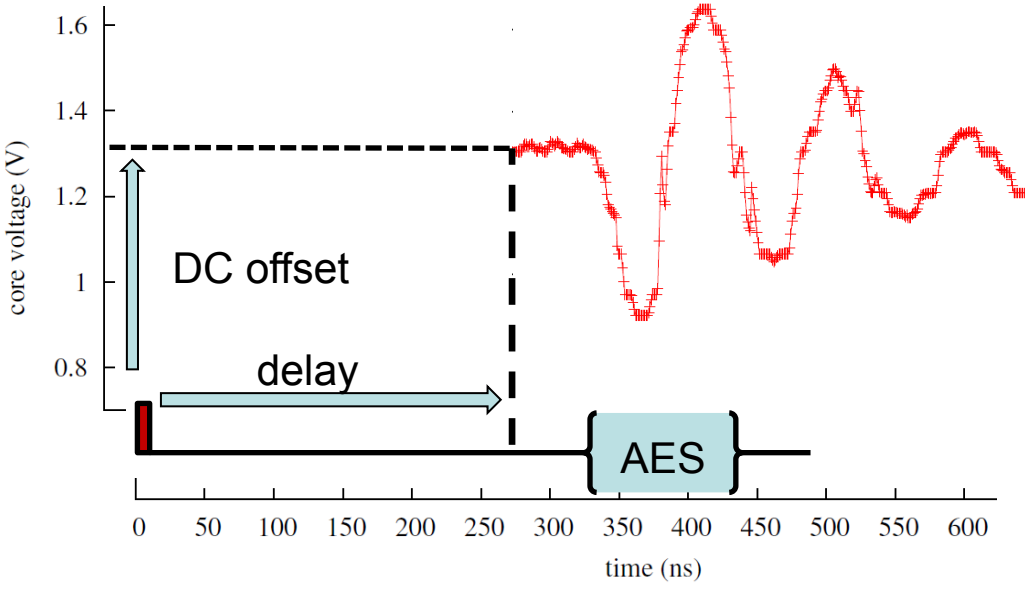
Fault injection protocol



AES 128bit : 11 rounds - **100MHz**

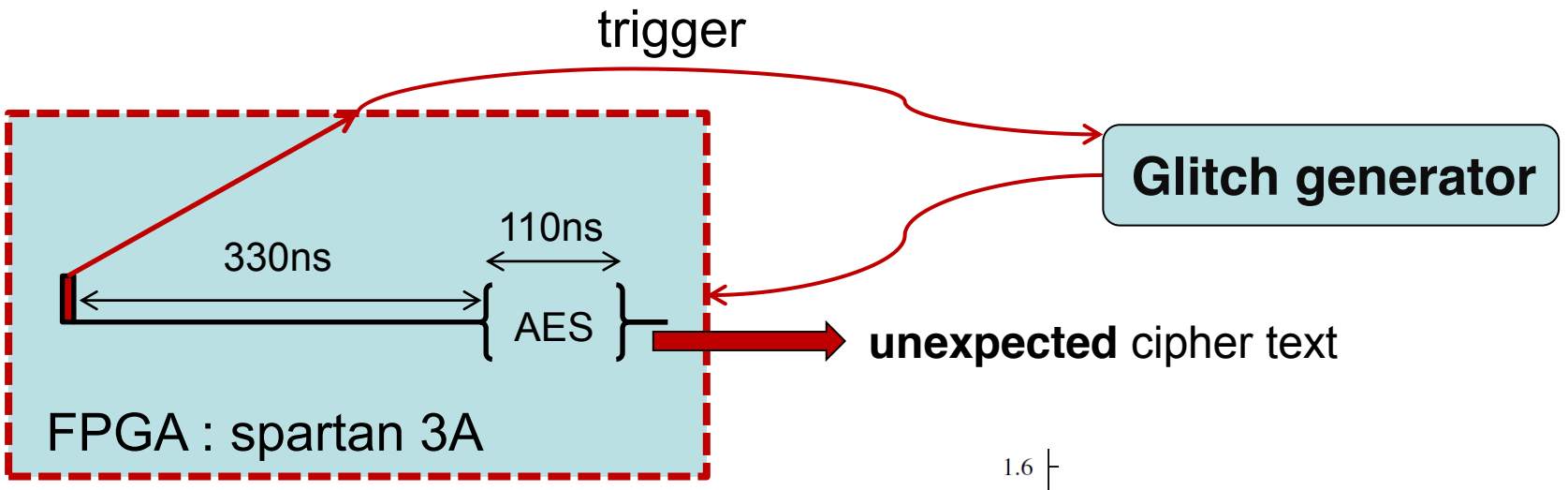
DC offset from **1,4** to **1,1 Volts**

Delay from **170** to **330 ns**



Characterization

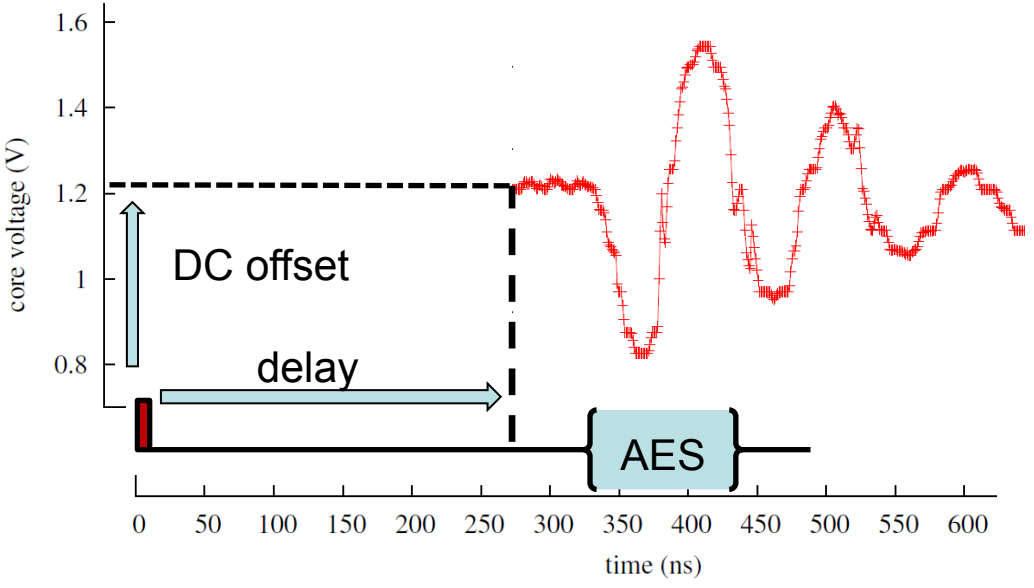
Fault injection protocol



AES 128bit : 11 rounds - **100MHz**

DC offset from **1,4** to **1,1 Volts**

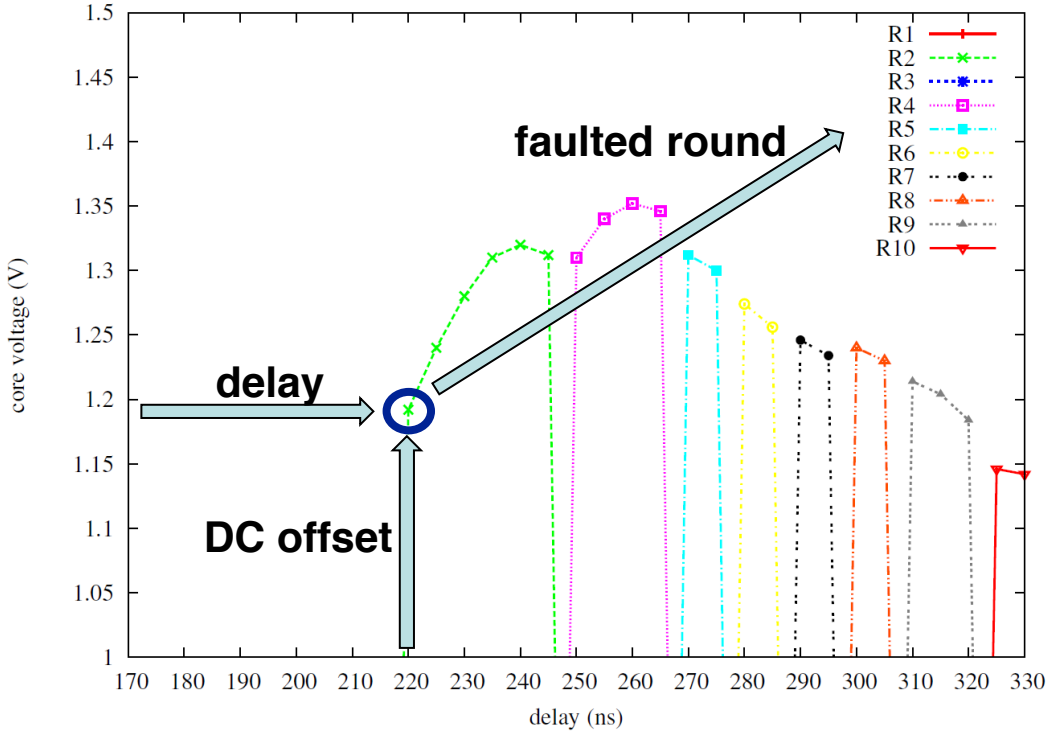
Delay from **170** to **330 ns**

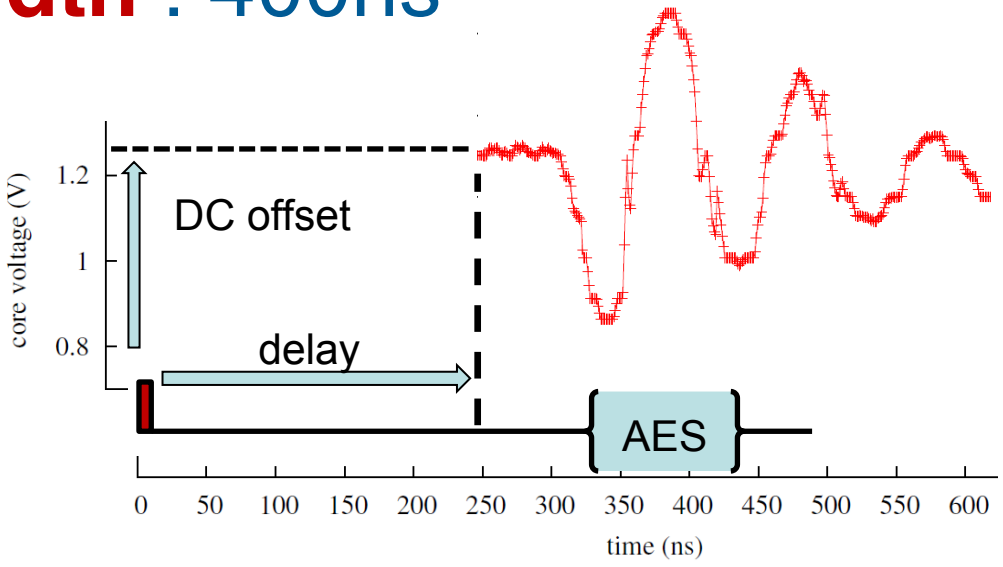


Experimental results

Negative voltage glitch characterization

amplitude : -14V **width** : 400ns

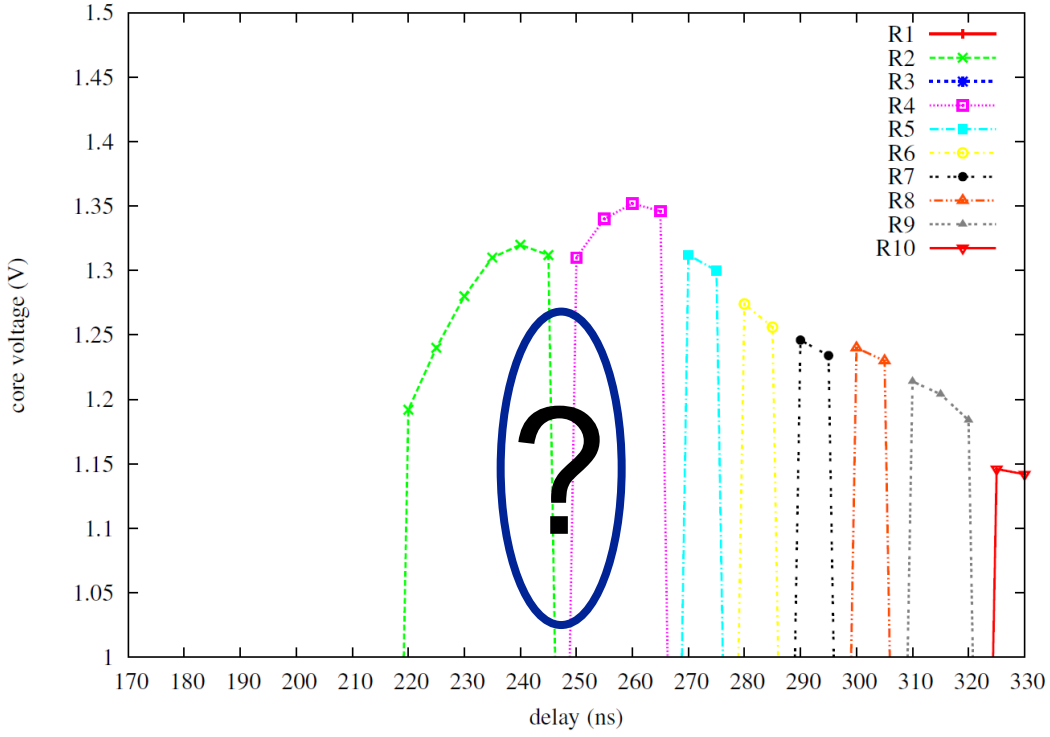


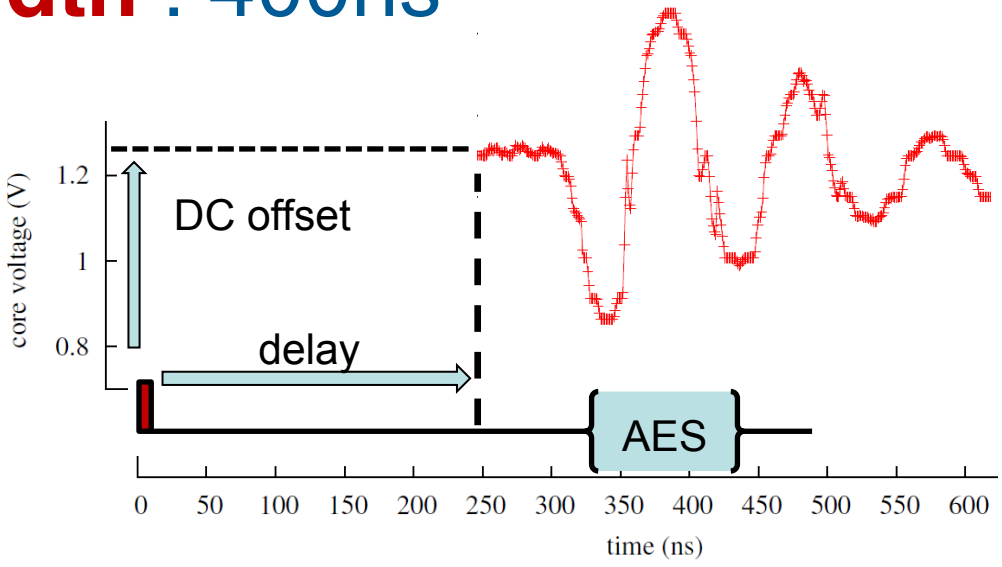


Experimental results

Negative voltage glitch characterization

amplitude : -14V **width** : 400ns





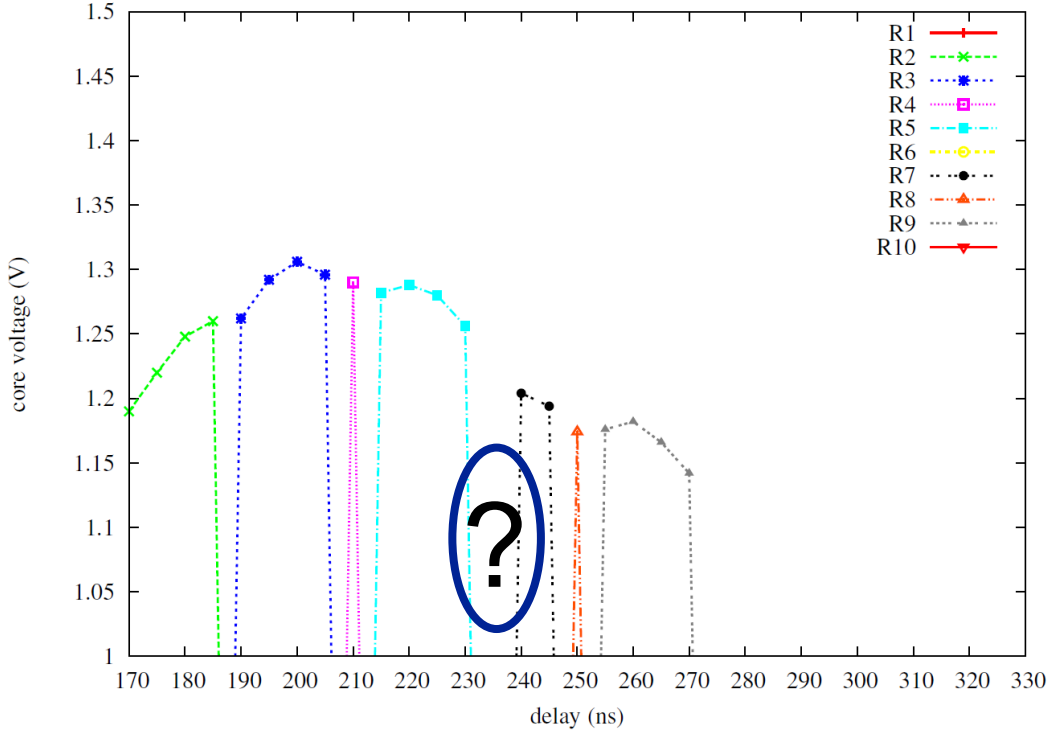
Observation :

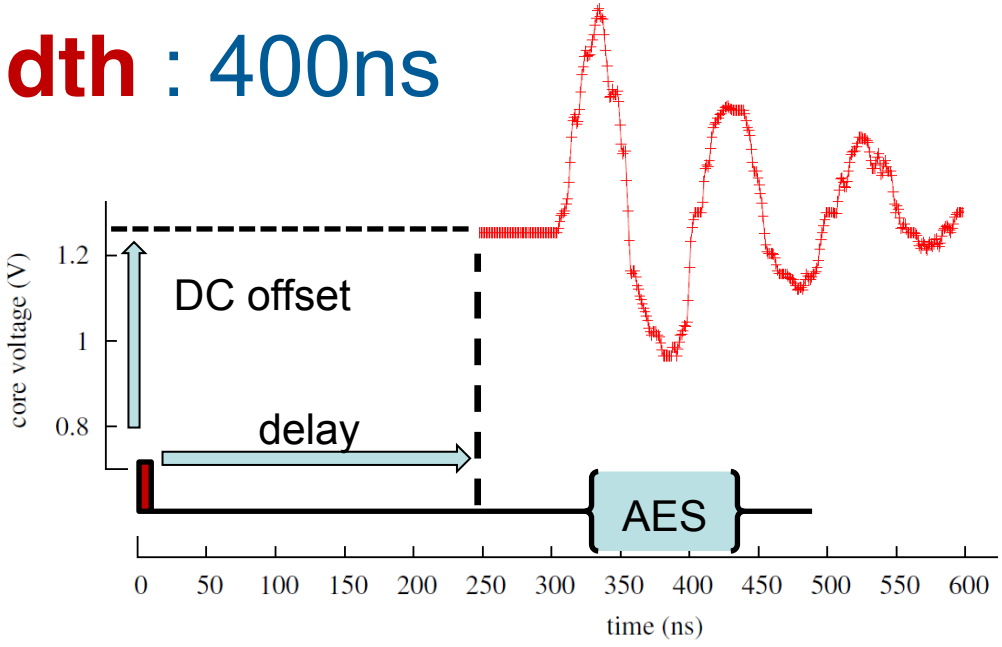
R3 wasn't faulted
The **negative disturbance is too large**
Faults were injected in R2 or R4 first

Experimental results

Positive voltage glitch characterization

amplitude : **+**14V **width** : 400ns



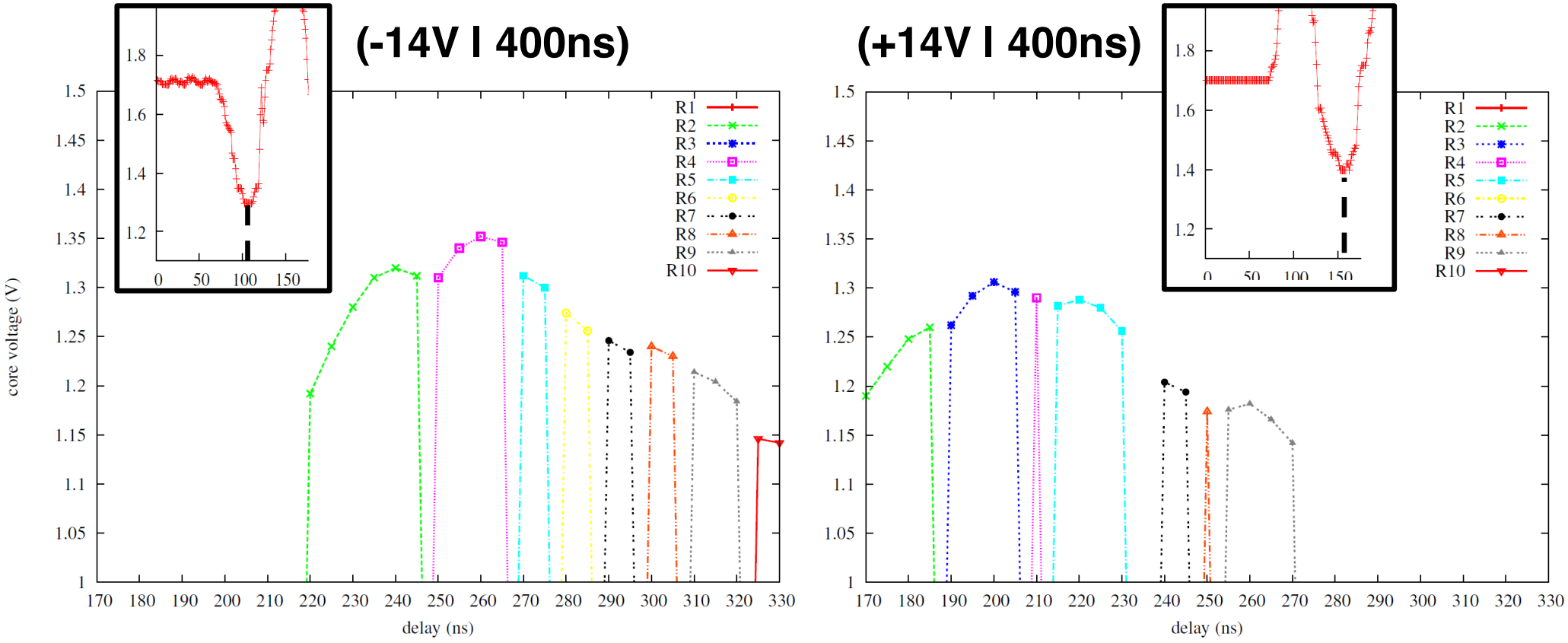


Observation :

R3 was faulted BUT R6 wasn't !

Experimental results

Injected faults comparison



⇒ Same injected faults

⇒ Different temporal accuracy

⇒ Same fault injection mechanism

Positive voltage glitches - Fault injection mechanism

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

For different plaintexts and keys of the AES, **positive and negative voltage glitches** induced **exactly the same faults**

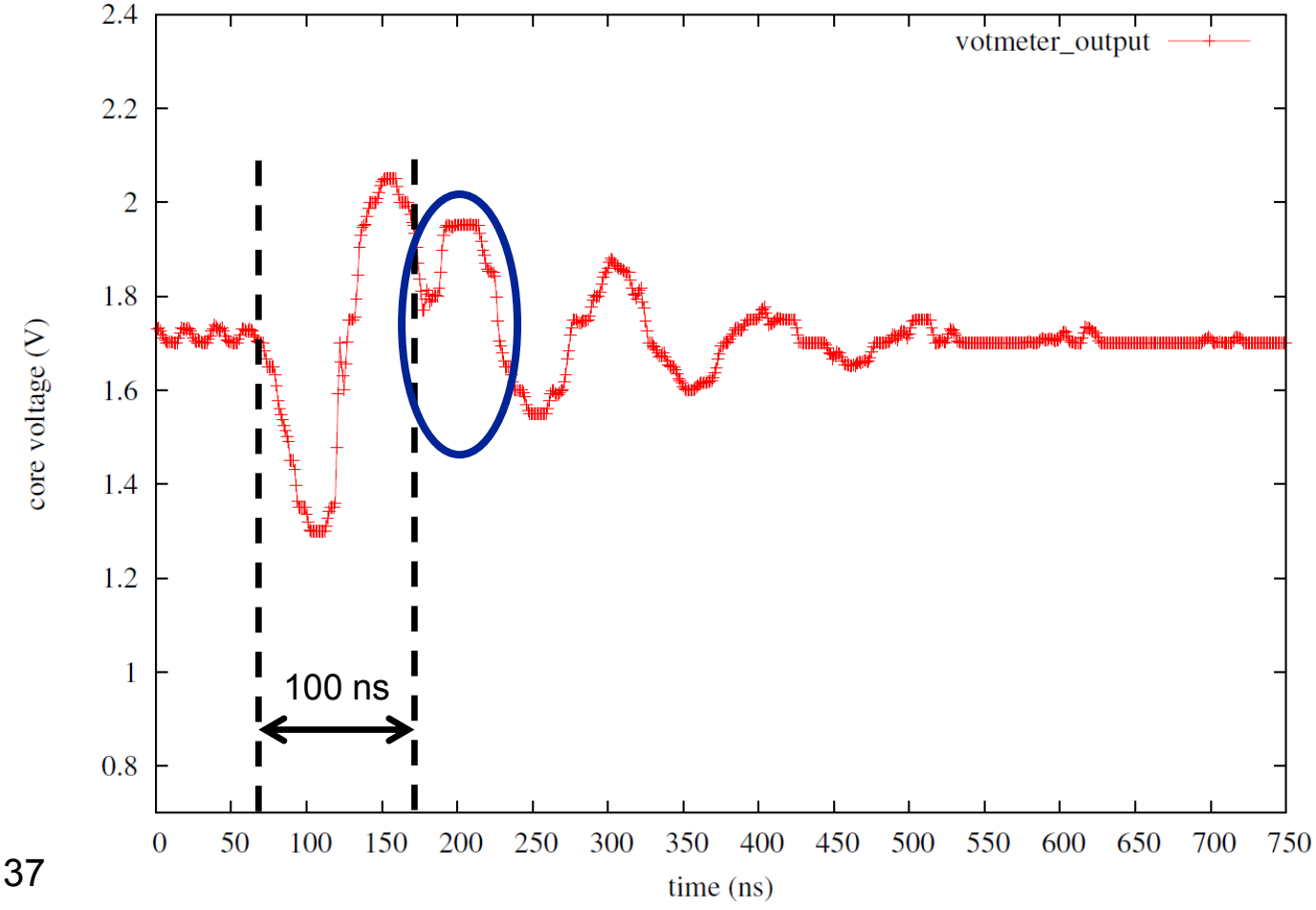
Negative and **positive** glitches share the same fault injection mechanism : **timing constraint violation**

Due to their different shape, positive and negative voltage glitches have **slightly different temporal accuracy**

Glitch shaping

Offsetting

amplitude : **-**14V **width** : 100ns



Observation :

Positive oscillations
due to the rising edge

COMPENSATE

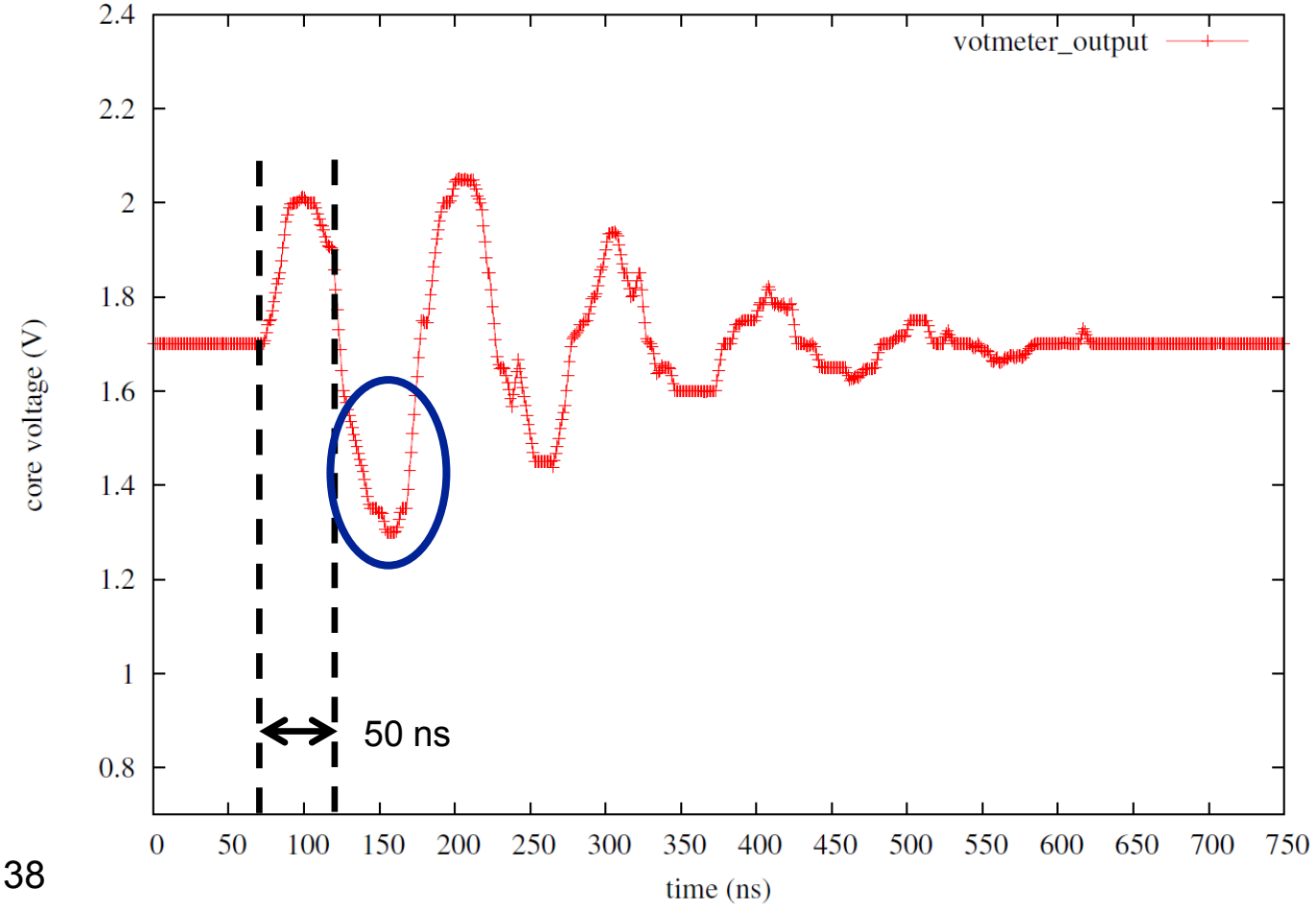
negative oscillations
due to the falling edge

➢ **Only one significant negative spike**

Glitch shaping

Addition

amplitude : +8V **width** : 50ns



Observation :

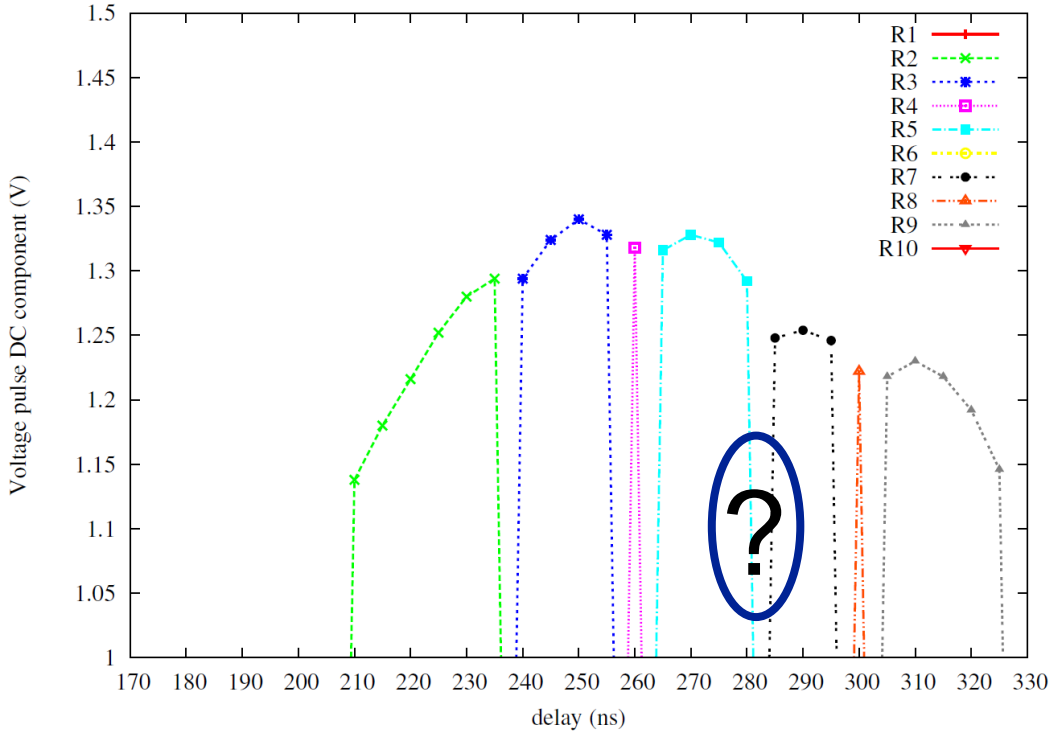
Negative oscillations due to the rising edge **and** due to the falling edge are

SYNCHRONIZED

➢ **More efficient glitch injection**

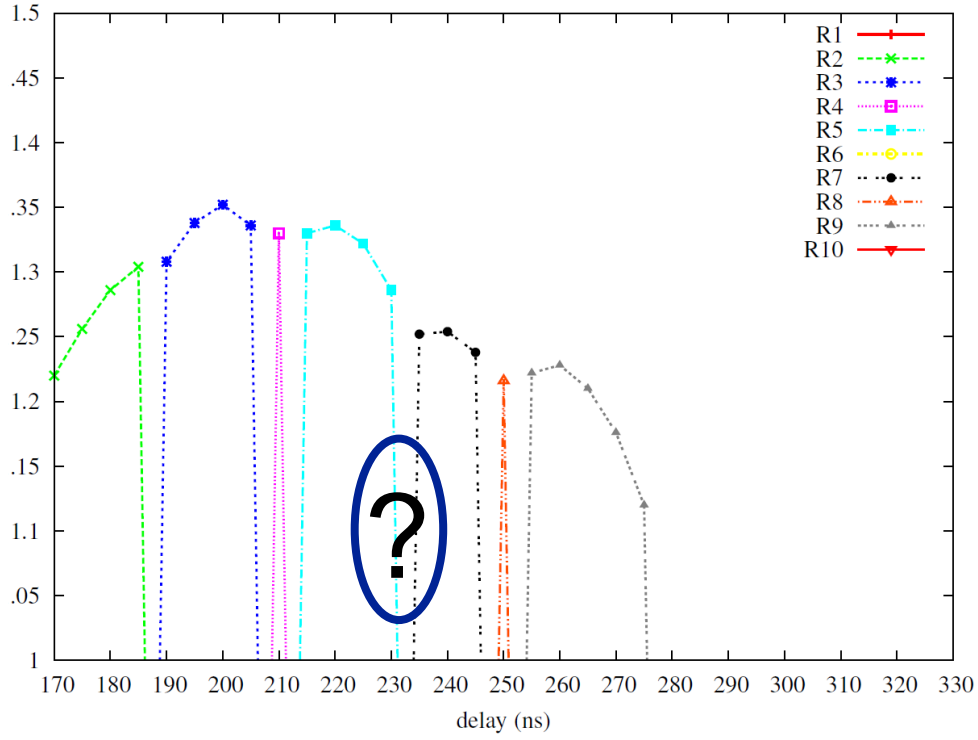
Injected faults comparison

(-14V I 100ns) : compensation



⇒ **Same injected faults**

(+8V I 50ns) : synchronization

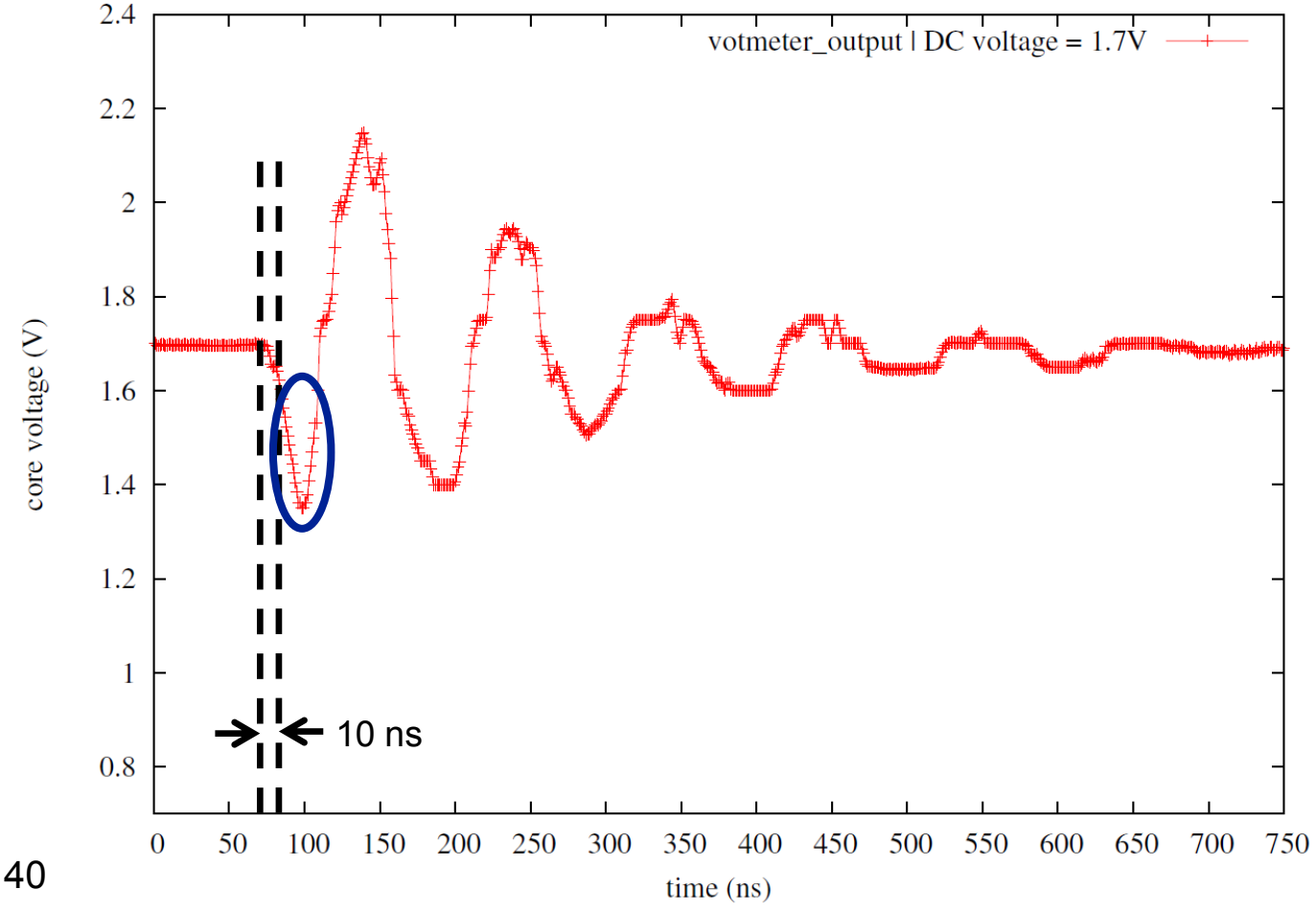


⇒ **Same temporal accuracy**

Glitch shaping

Sharping

amplitude : **-**22V **width** : 10ns



Observation :

Negative oscillation due to the falling edge is

SHORTEN

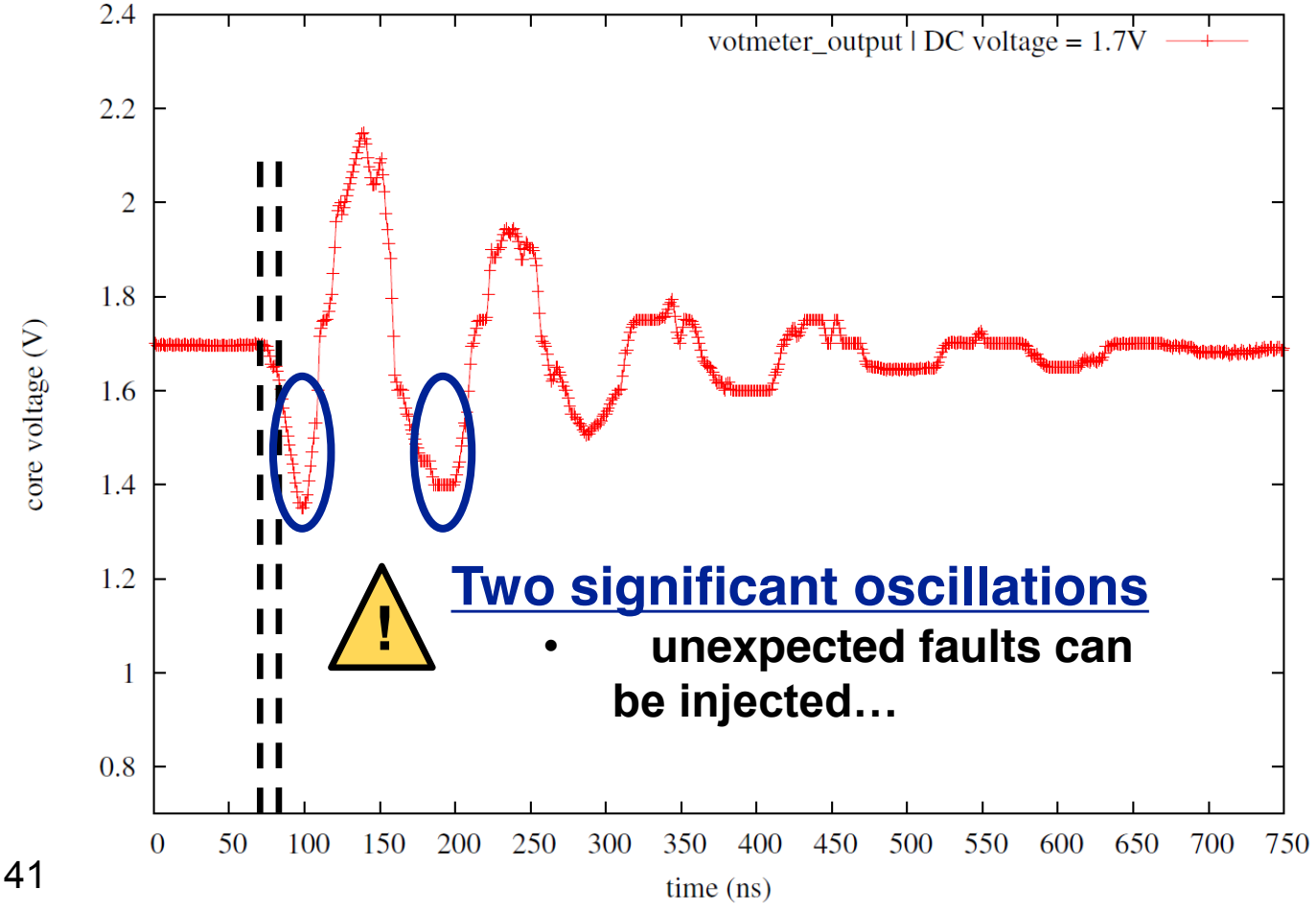
by the **positive oscillation** due to the rising edge

➢ **More accurate glitch injection**

Glitch shaping

Sharping

amplitude : **-**22V **width** : 10ns



Observation :

Negative oscillation due to the falling edge is

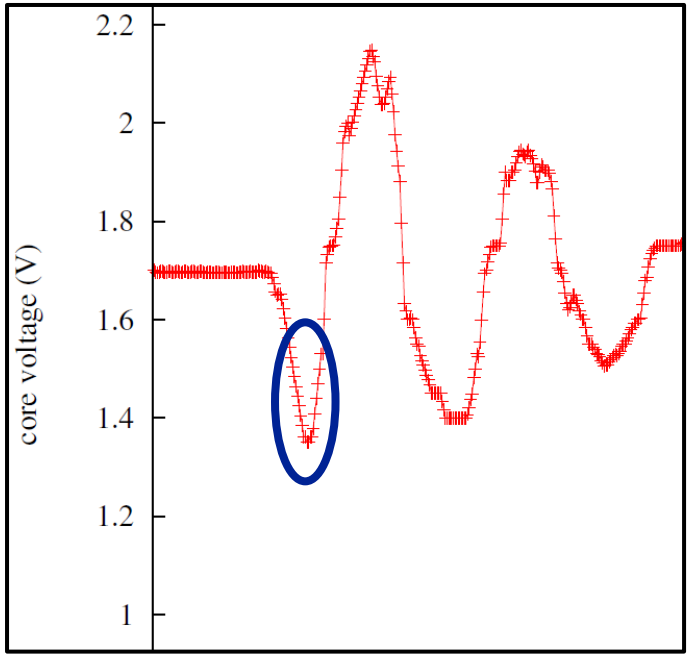
SHARPED

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

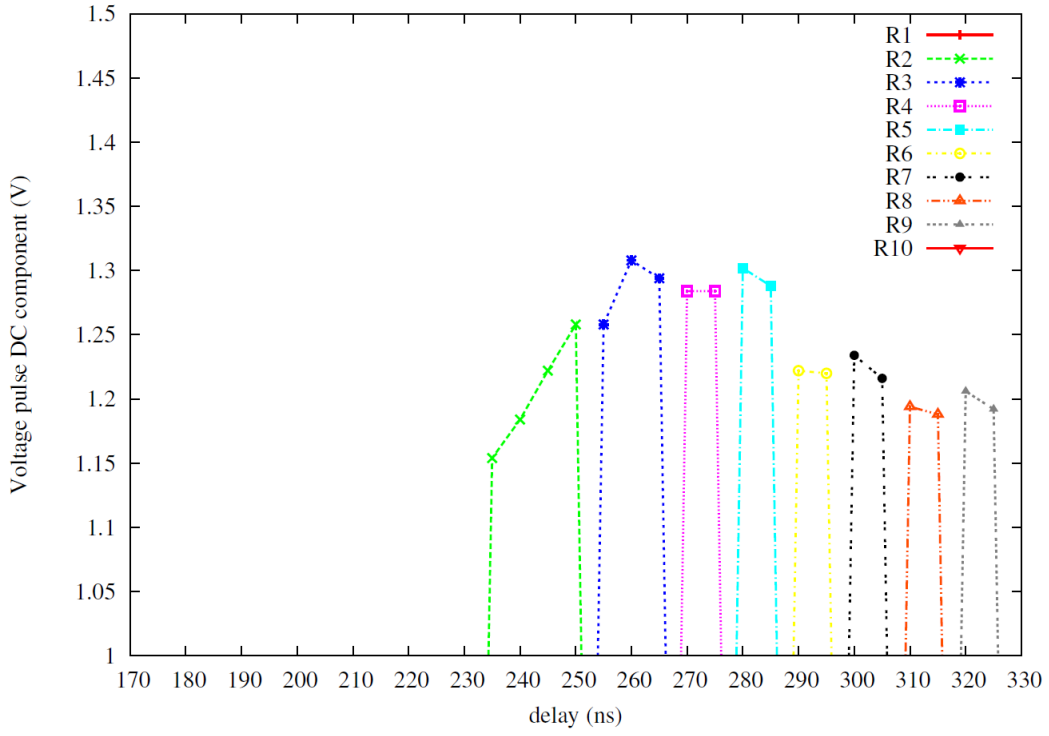
➢ **More accurate glitch injection**

Glitch shaping

Injected faults comparison



(-22V I 10ns) : sharping

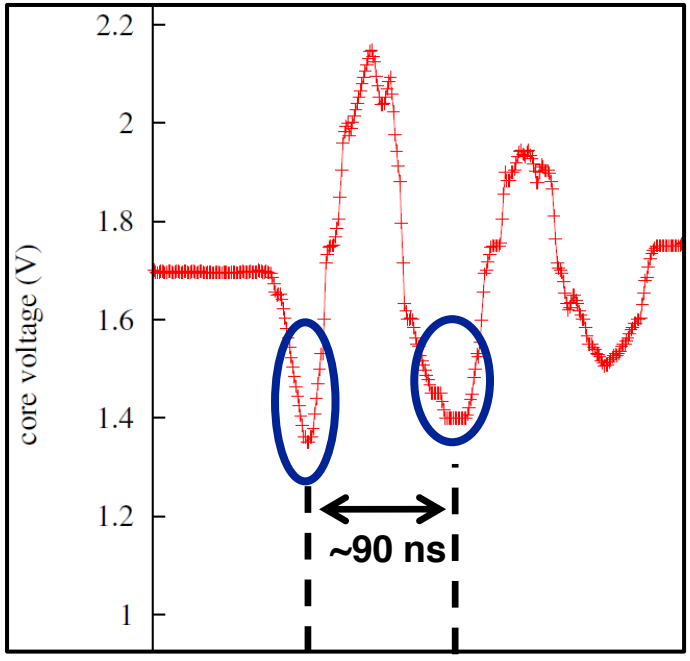


⇒ **Same injected faults**

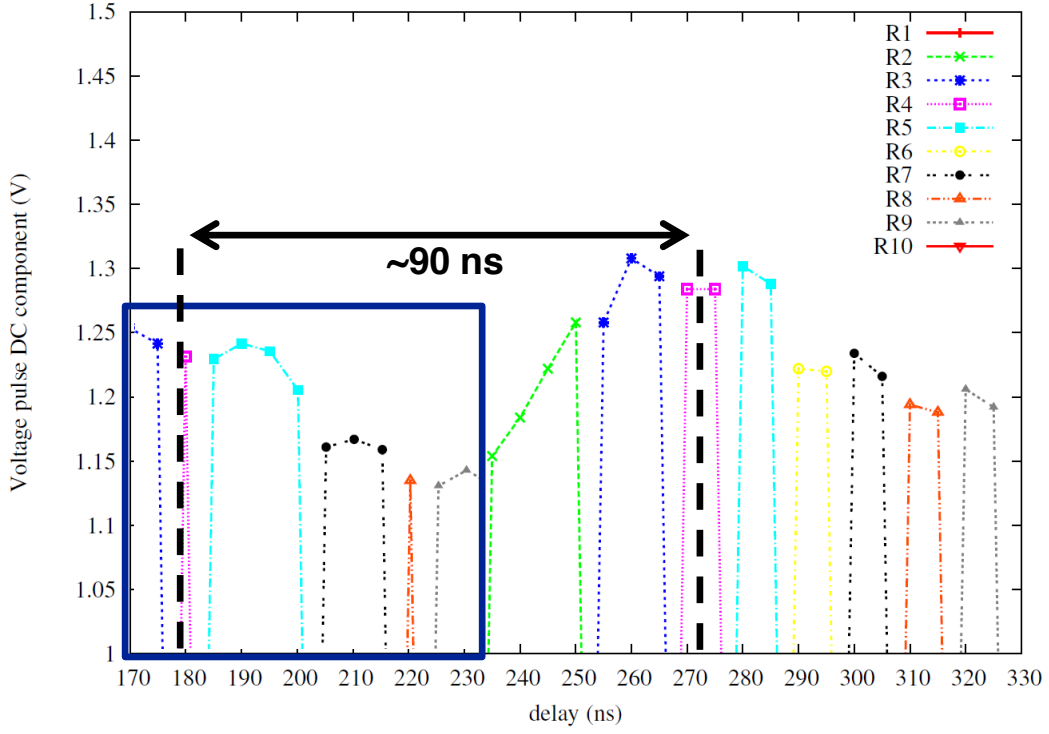
⇒ **Very good temporal accuracy**

Glitch shaping

Injected faults comparison



(-22V I 10ns) : sharping



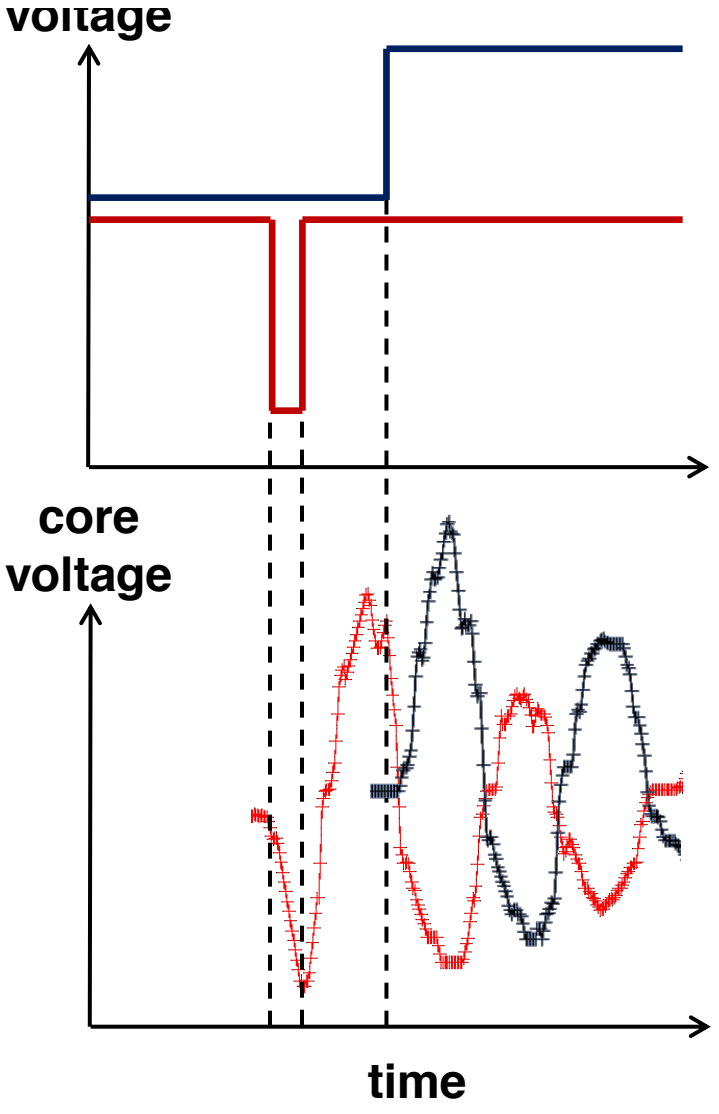
⇒ **Same injected faults**

⇒ **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

Presentation available on loic.zussa.fr/publications

ZUSSA Loïc

PhD Student

Secure integrated circuits and physical fault injections

zussa@emse.fr
+33 (0)4.42.61.67.12
880 route de Mimet 13541 Gardanne - FRANCE