DE LA RECHERCHE À L'INDUSTRIE

cea

INSPIRING INNOVATION | INNOVANTE PAR TRADITION

Ecole Nationale Supérieure des Mines SAINT-ETIENNE

Sept 25-27 2013

Chip-to-Cloud Security Forum

From physical stresses to timing constraints violation

ZUSSA Loïc,
DUTERTRE Jean-Max,
CLEDIERE Jessy,
TRIA Assia

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

Research subject

- **Characterization and analysis of common fault injection mechanism**

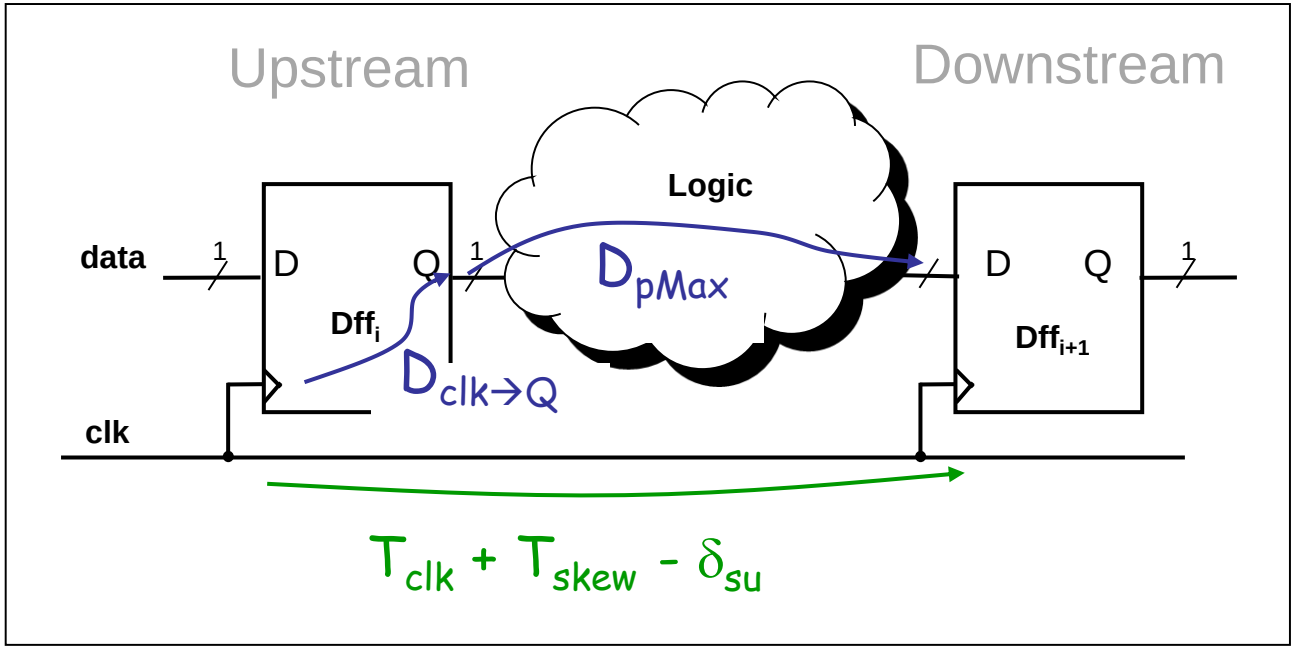
Today's subject

- **Power glitches as a fault injection mechanism**
  - **Analysis and practice**

Agenda

- **Timing constraints of synchronous digital IC**
- **Static stresses (global effect)**
- **Transient stresses**
- **Conclusion**

Timing constraints



data arrival time = $D_{clk \rightarrow Q} + D_{pMax}$

data required time = $T_{clk} + T_{skew} - \delta_{su}$

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

How to inject faults through timing constraints violation?

- Overclocking: (Frequency increase, i.e. period decrease)

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

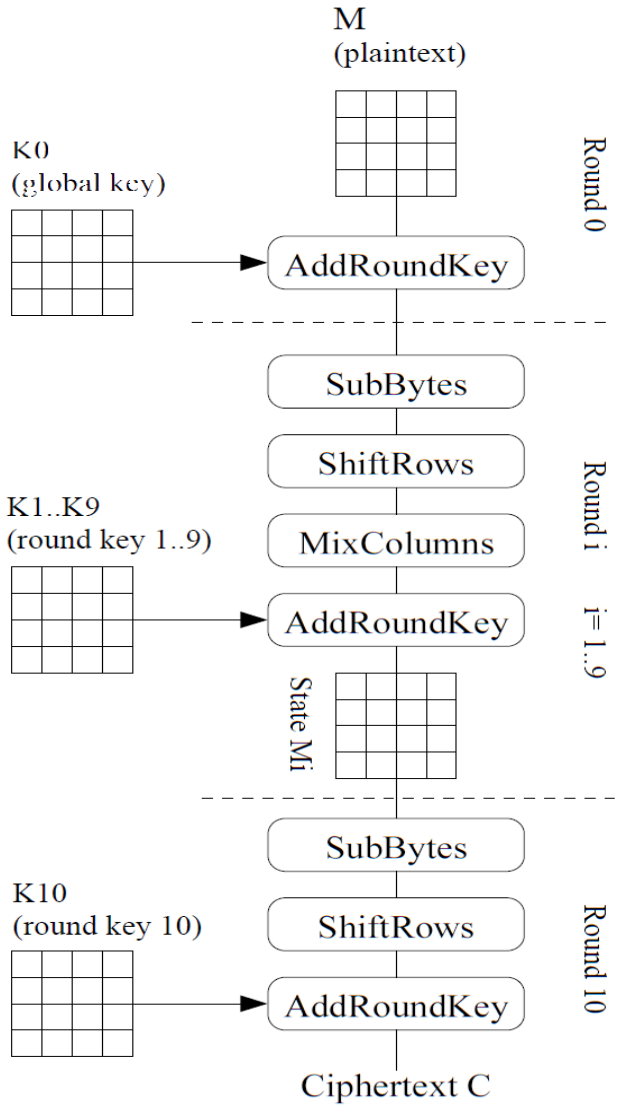
- Underpowering or overheating: (Propagation time increase)

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

Experimental setup

Target

- Platform: FPGA Spartan 3A
- Algorithm: AES 128 bit
  none-secure implementation
- Frequency: 100 MHz
- Power supply: 1.2V



Static perturbations

Common fault injection means

- Clock stress (overclocking)
- Power stress (underpowering)
- Overheating

A **common mechanism** !

⇒ Timing constraints violations.

Experimental proof

- 10,000 input dataset
- Critical path faulted

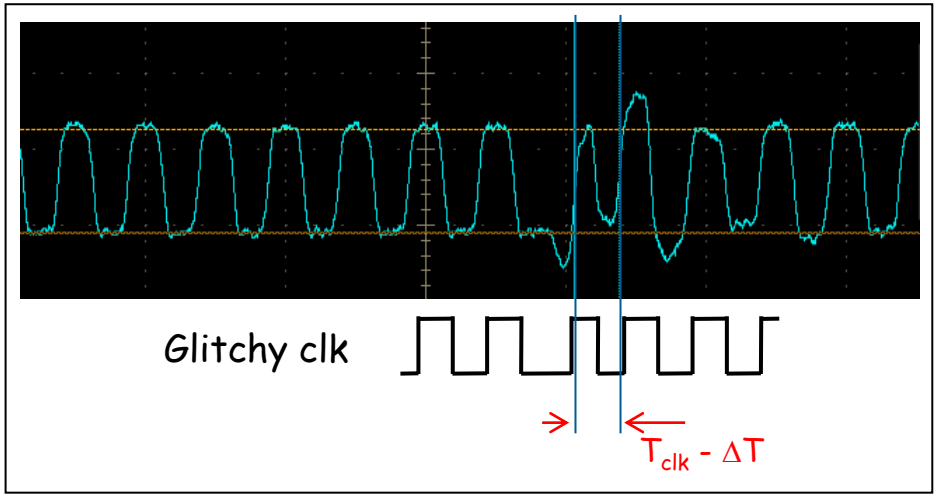
Transient perturbations

- Clock glitch
- Power supply glitch

Questions

- Injection mechanism? Timing violation?
- Achievable resolution?

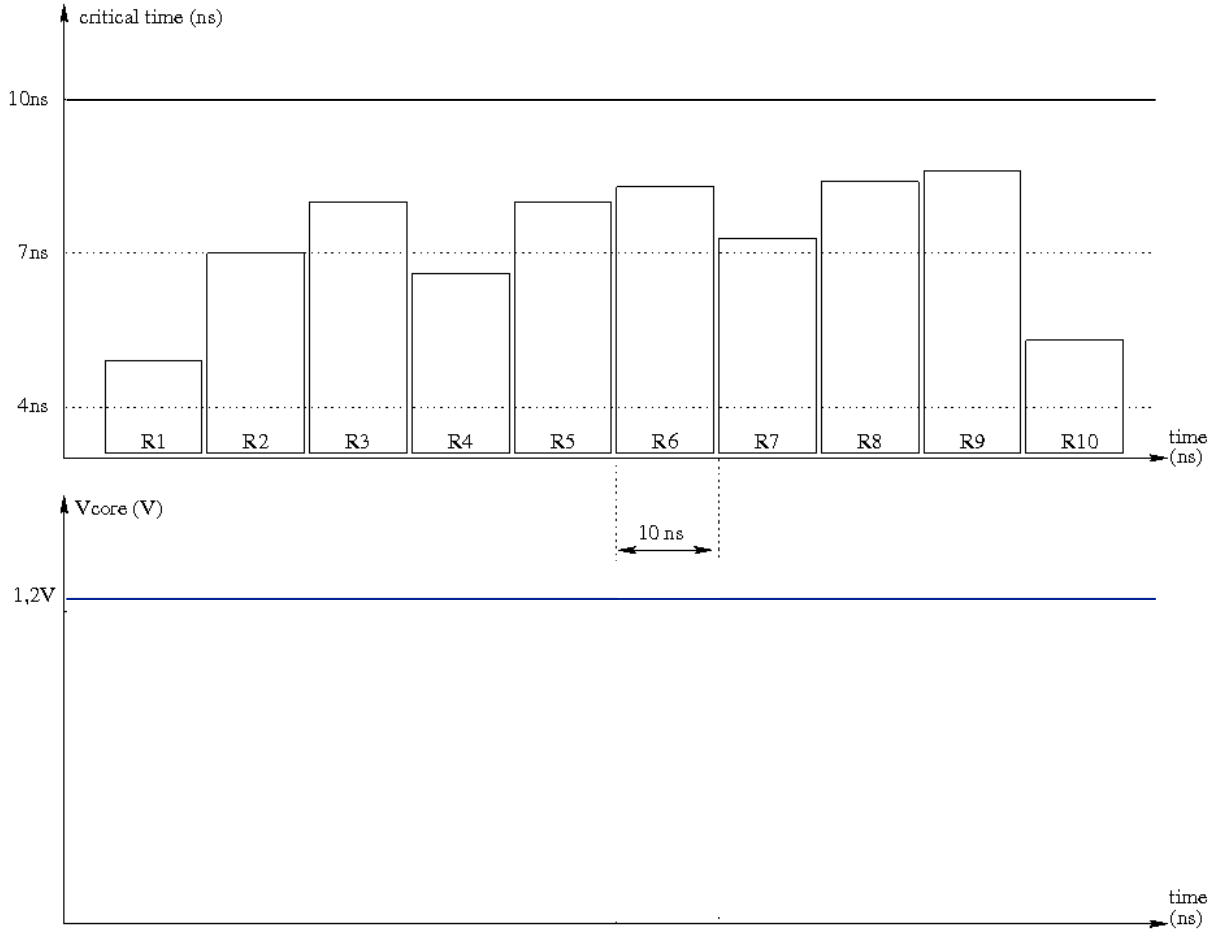
Clock glitch



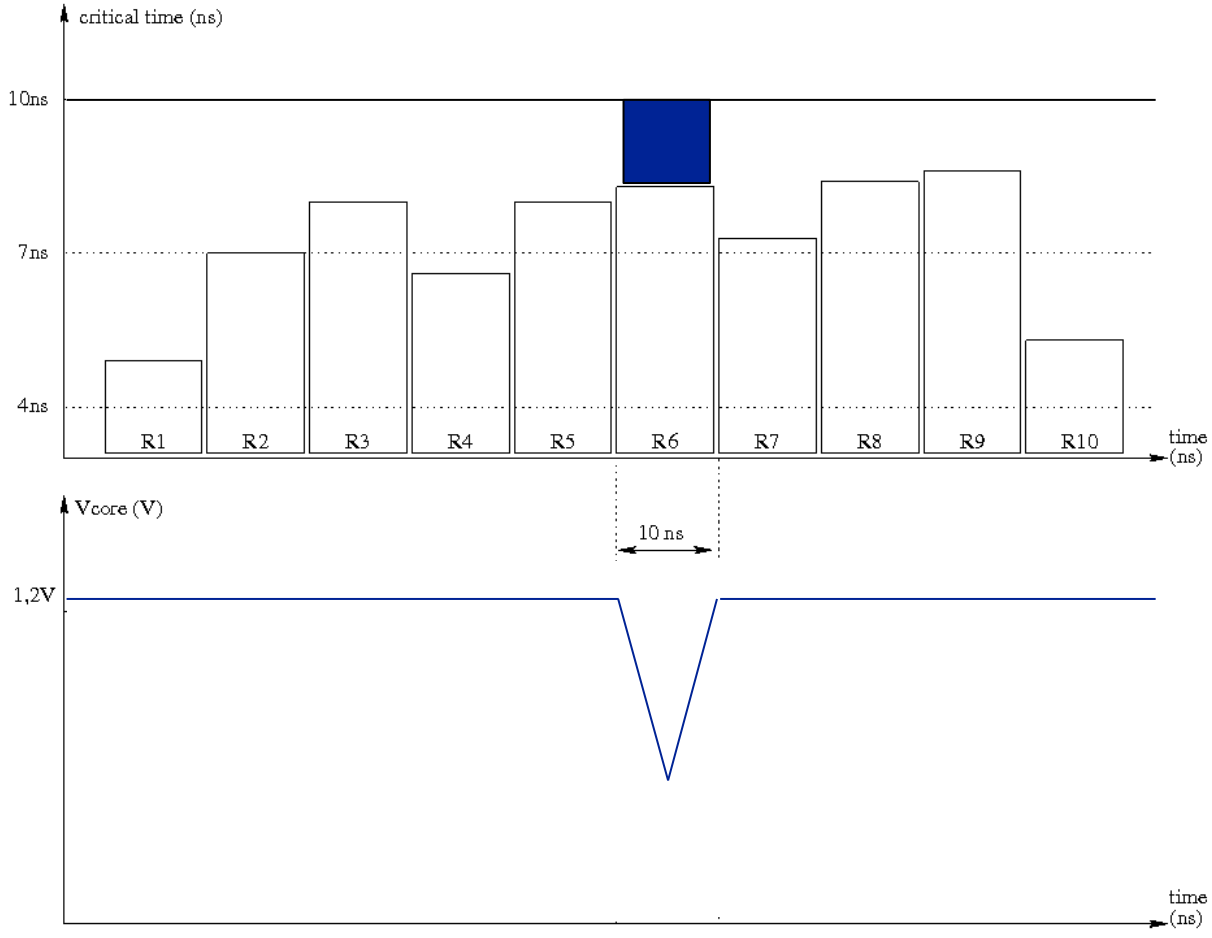
- 35ps resolution
- Global effect
- Timing constraints violation (obvious)
- A tool for critical time measurement
- Used to build a template/**reference library**

To be compared.

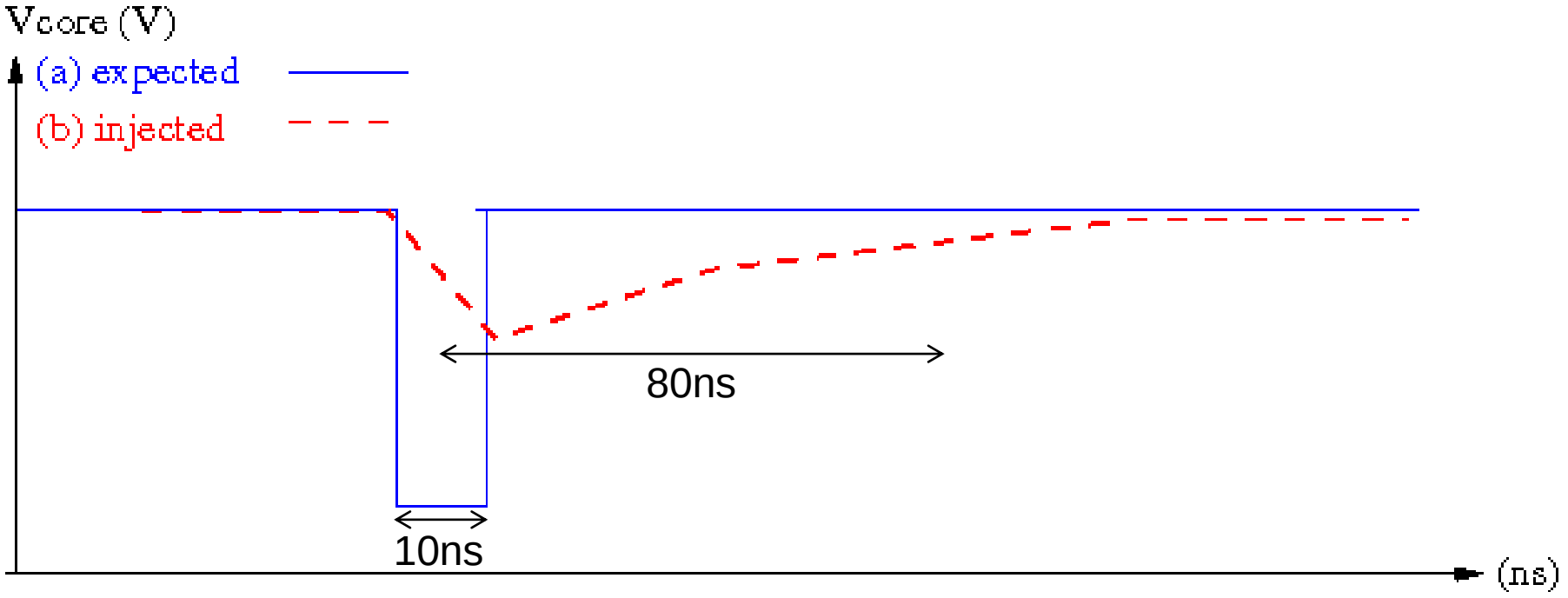
Power glitch: Ideal



Power glitch: Ideal

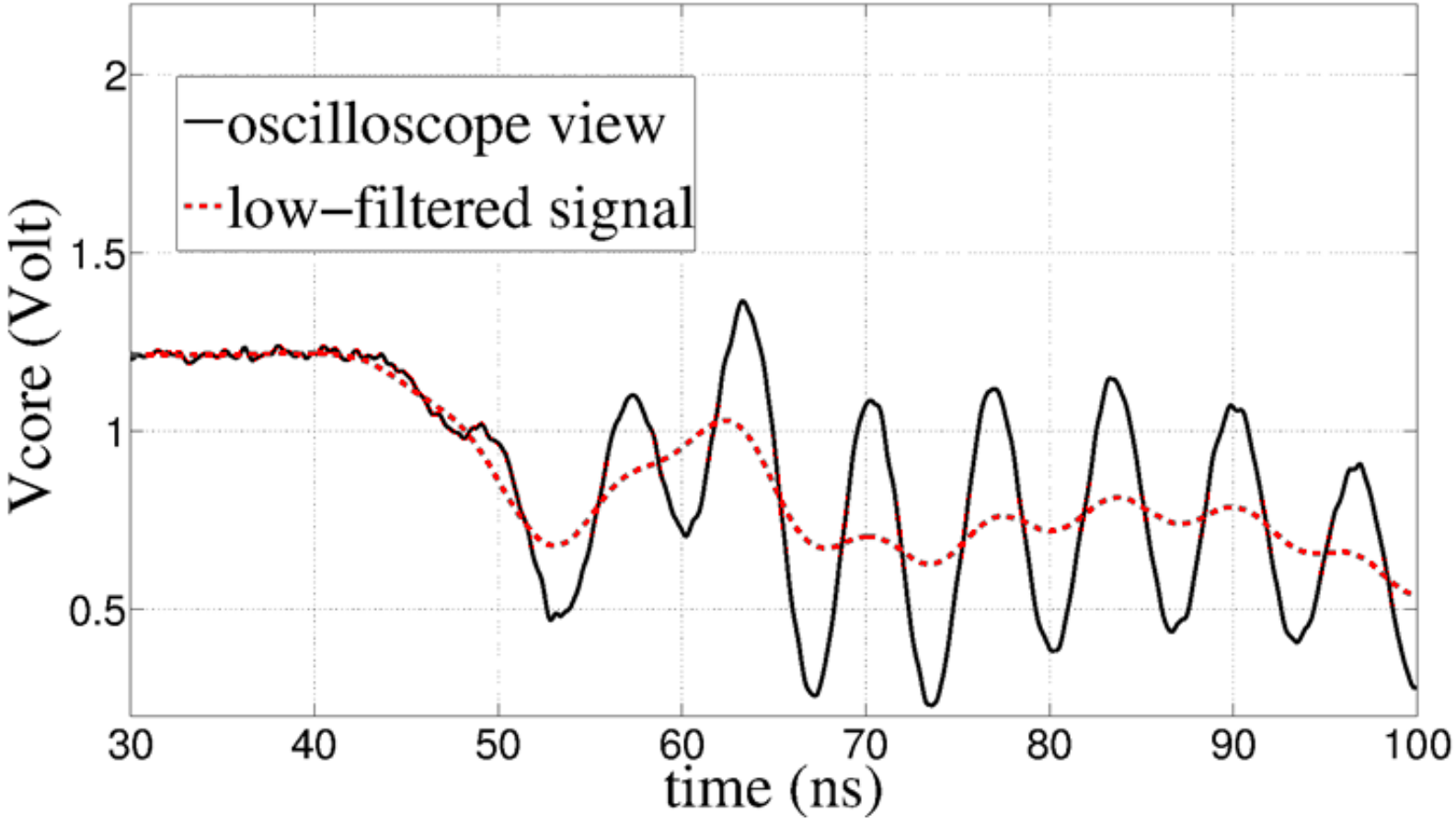


Power glitch: capacitances

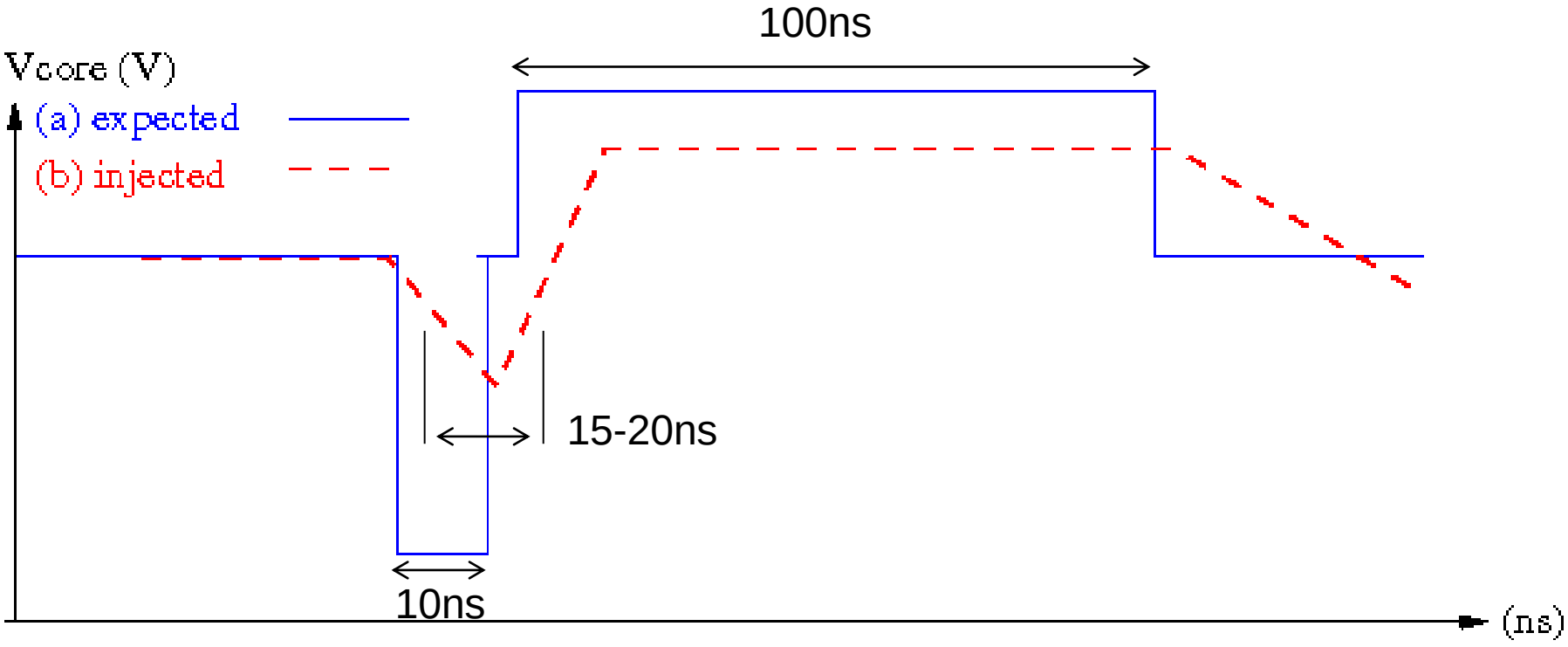


Transient perturbations

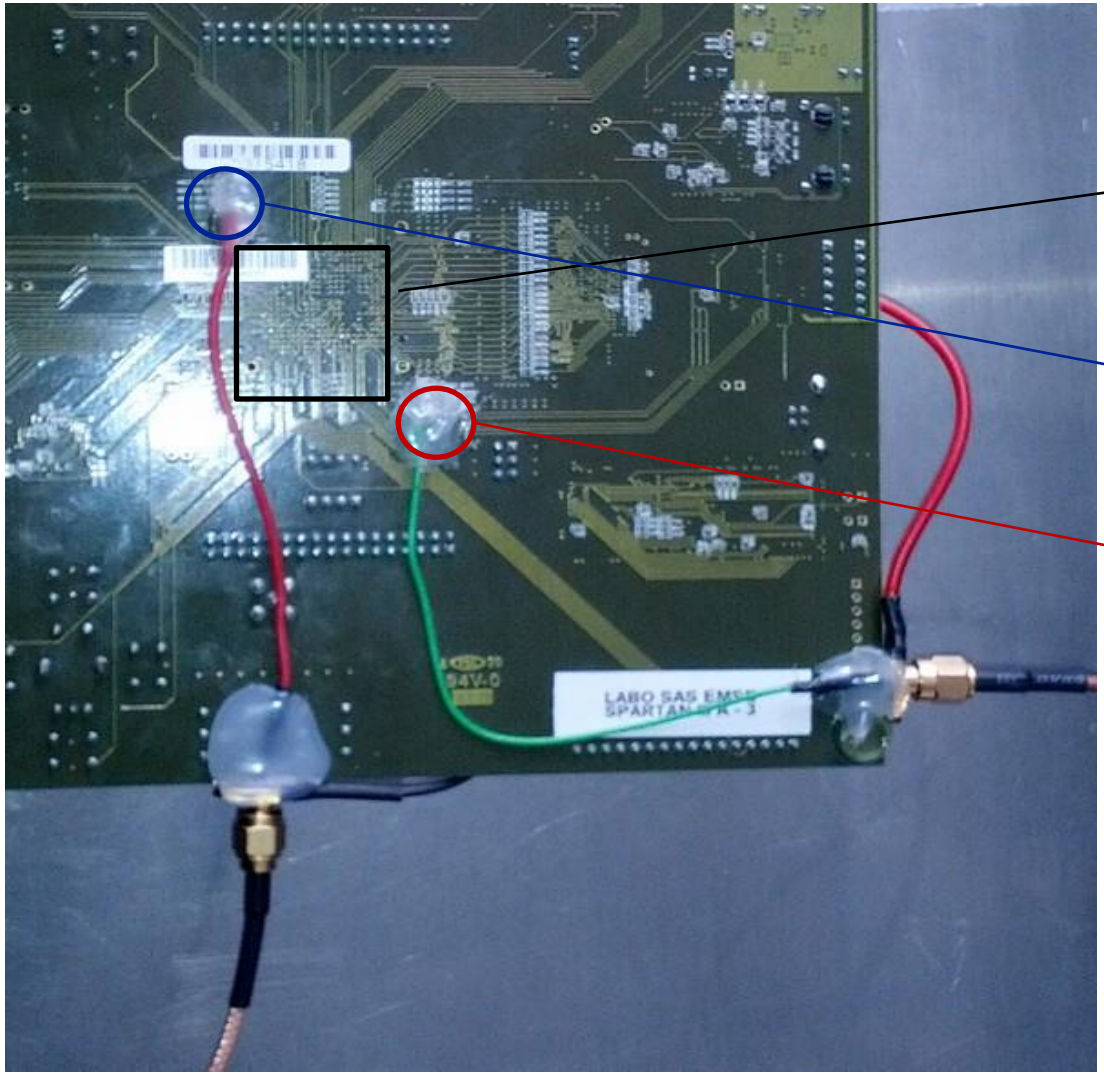
Power glitch: impedance adaptation



Power glitch: capacitances

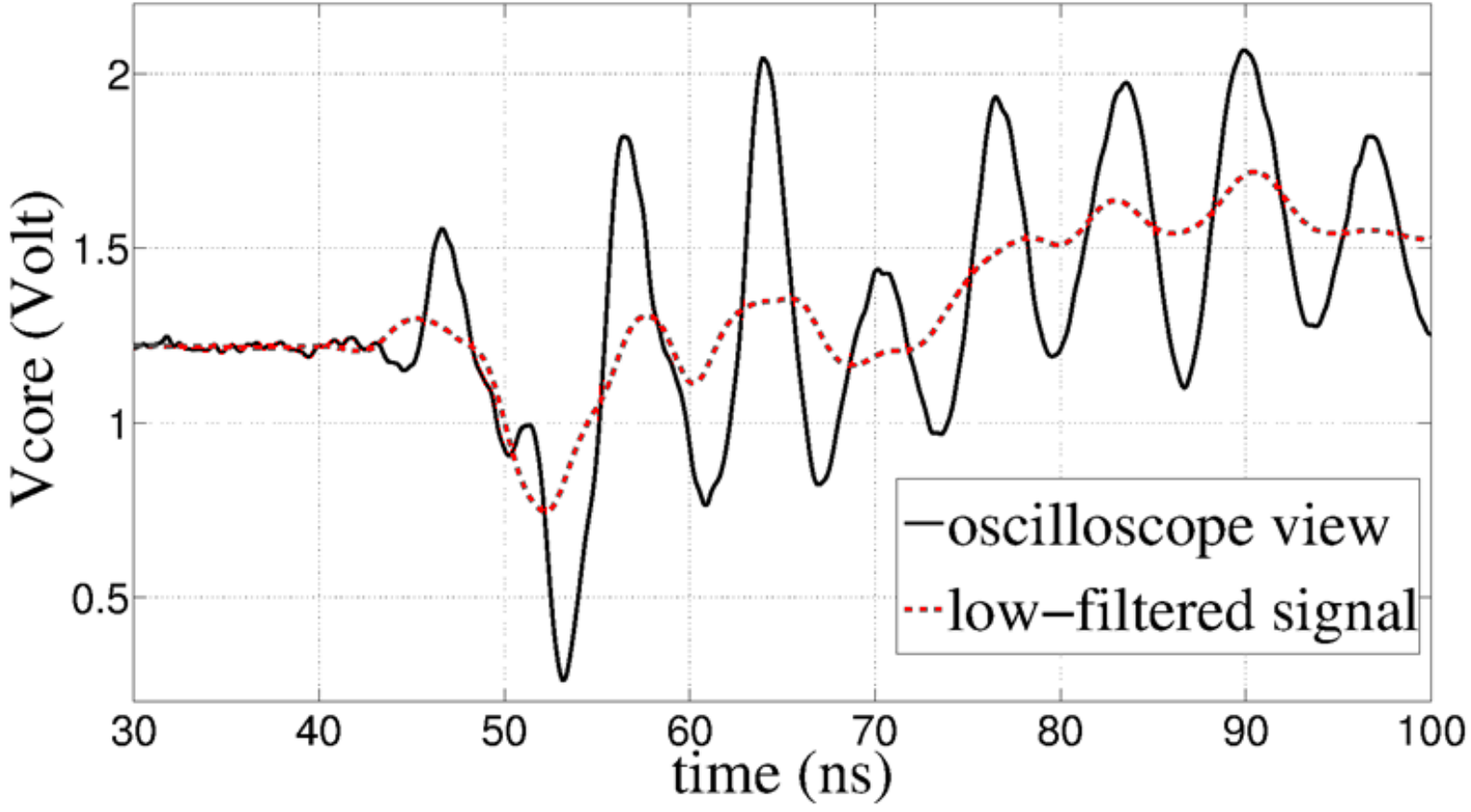


Transient perturbations



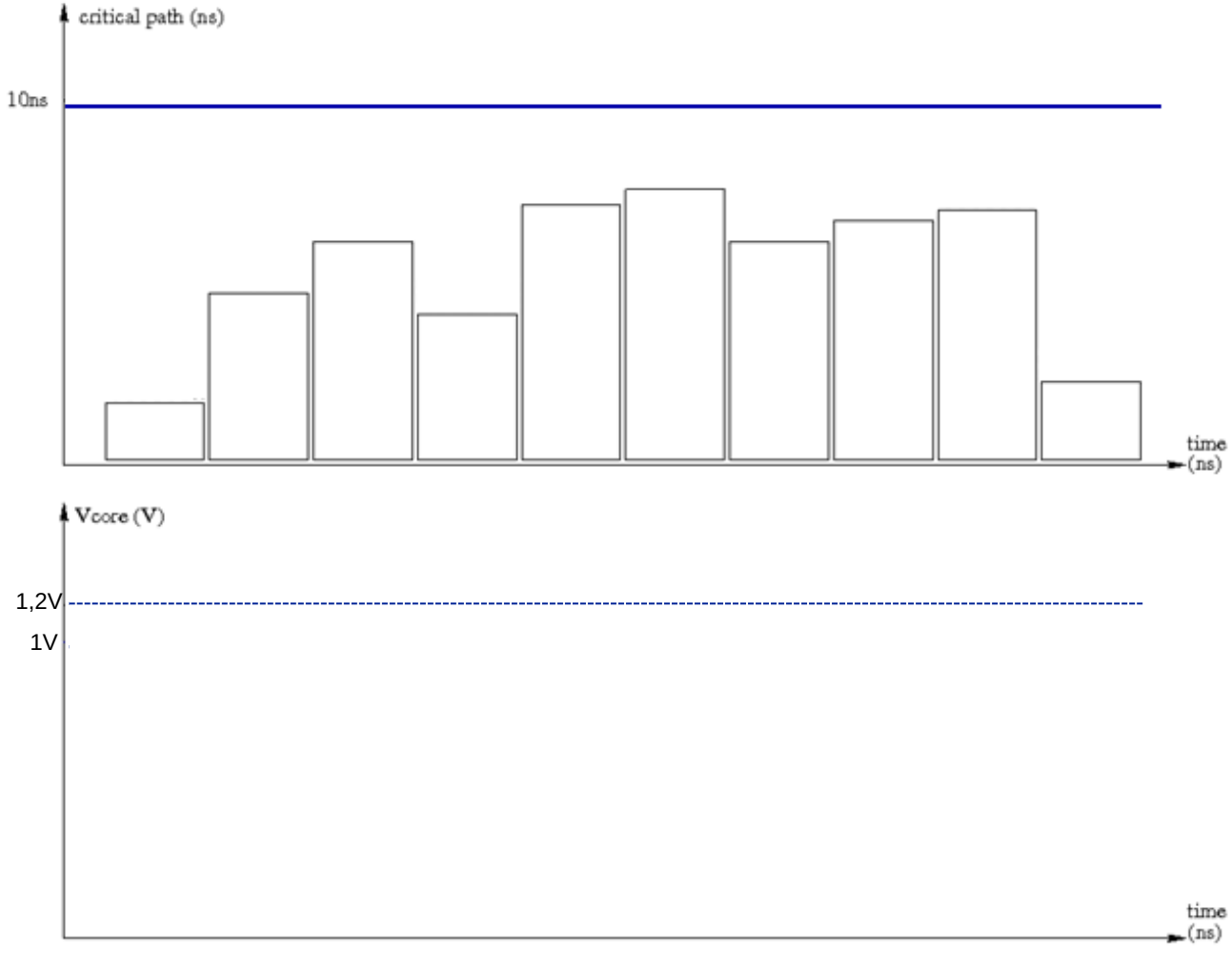
Transient perturbations

Power glitch: impedance adaptation



Transient perturbations

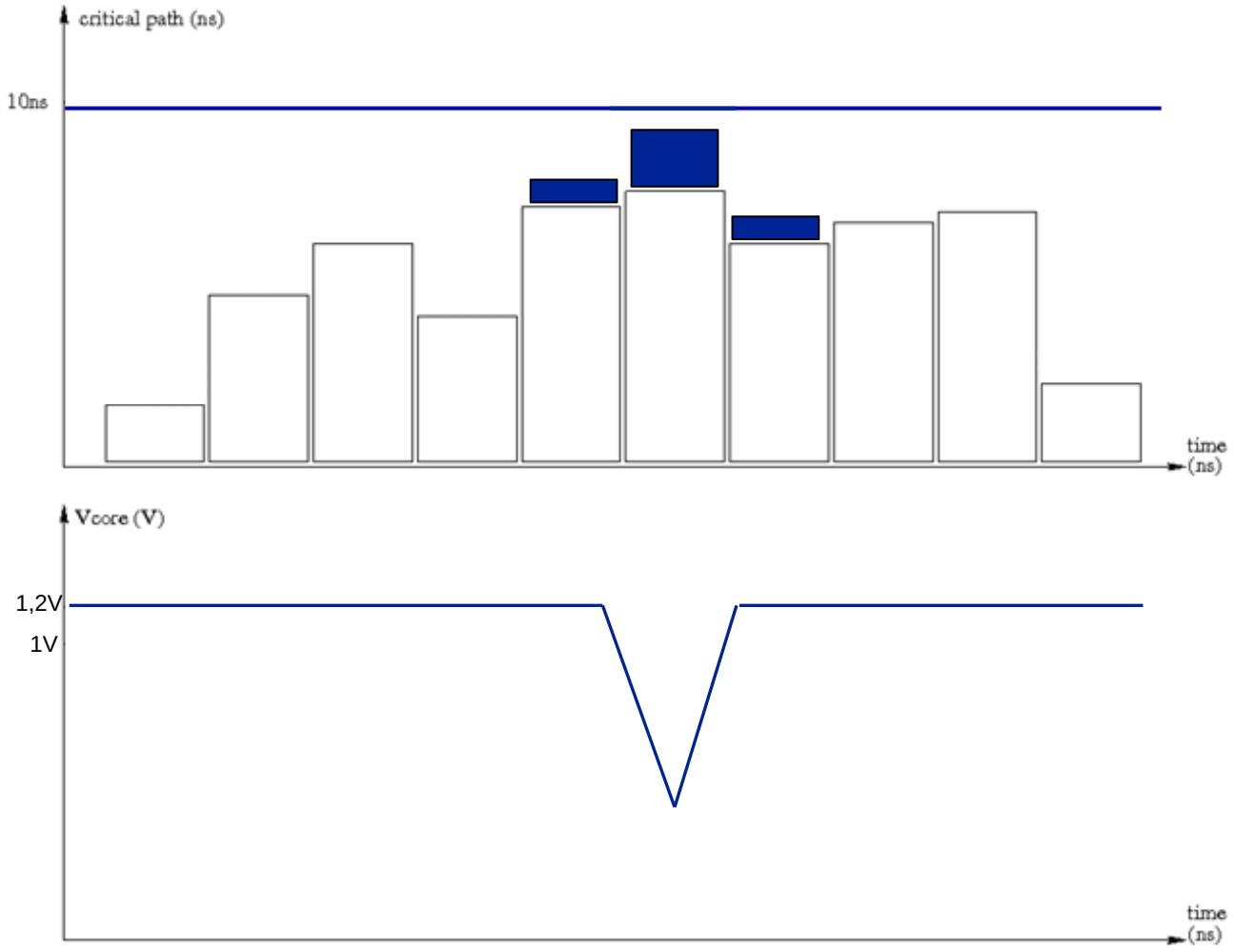
Power glitch



Transient perturbations

Power glitch

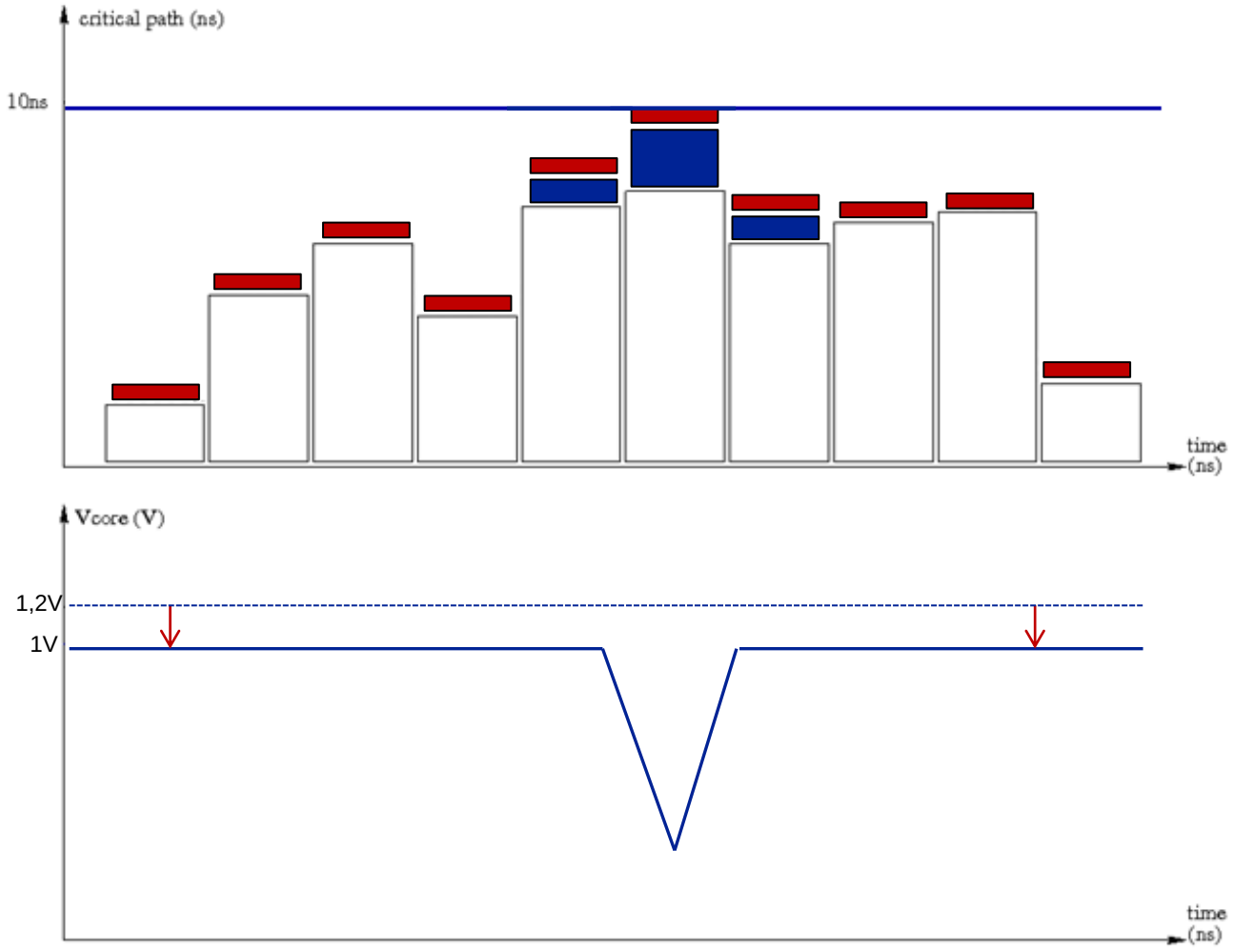
- Target a specific round but **also affect the neighboring rounds**



Transient perturbations

Power glitch

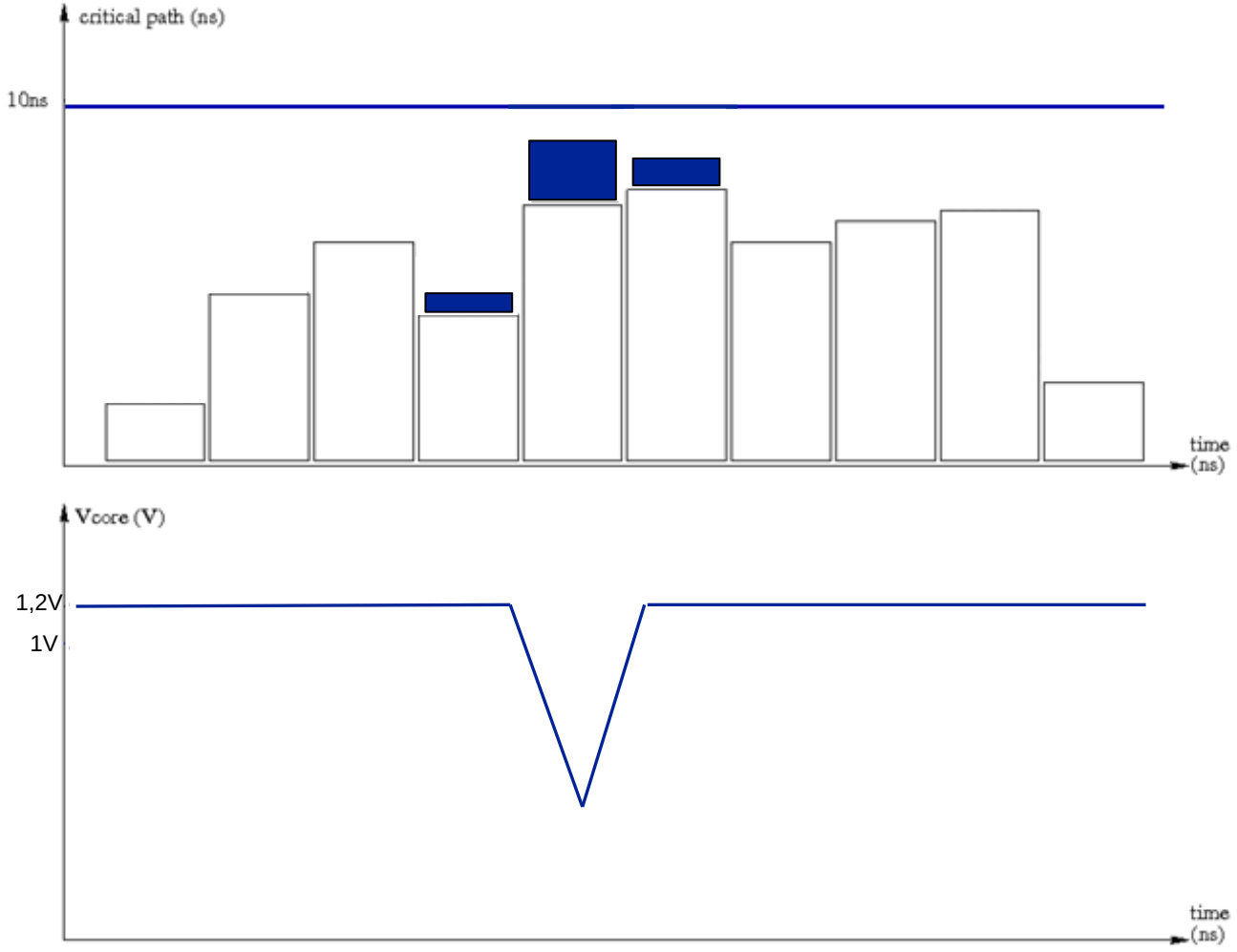
- Target a specific round but **also affect the neighboring rounds**
- Global offset must be added.



Transient perturbations

Power glitch

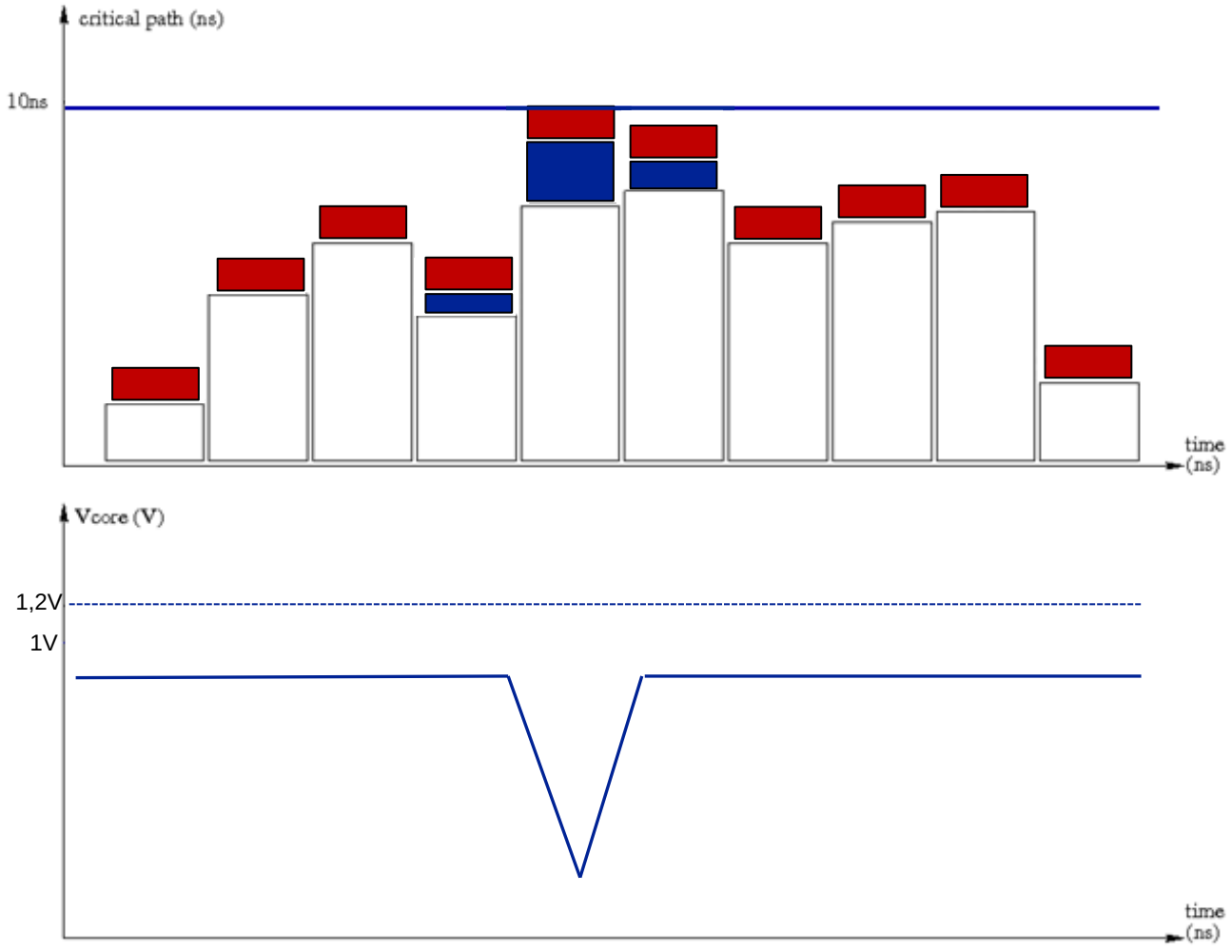
- When a specific round is targeted.
- Monobit fault during the targeted round 90% of the time.



Transient perturbations

Power glitch

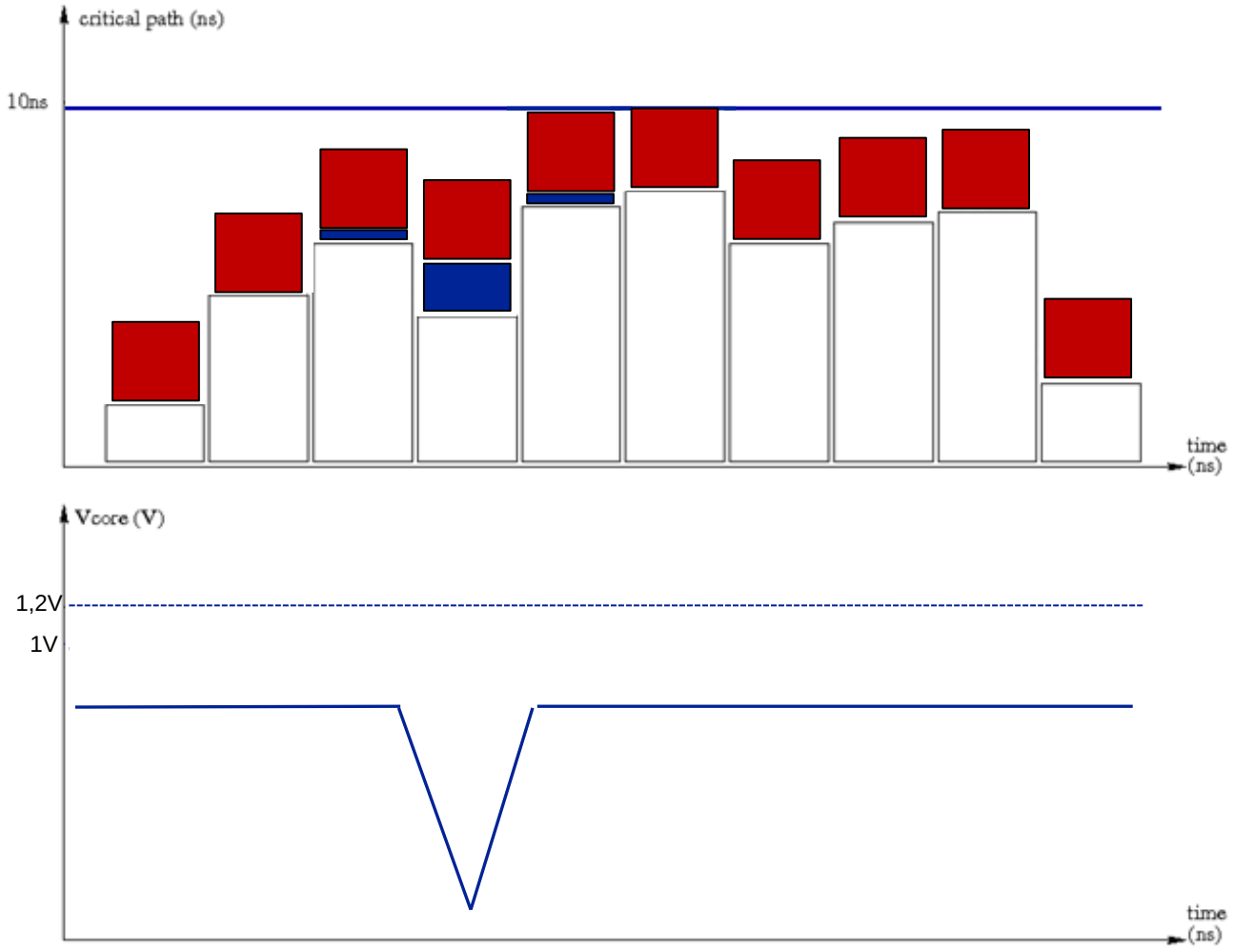
- When a specific round is targeted.
- Monobit fault during the targeted round 80% of the time.



Transient perturbations

Power glitch

BUT 20% of the time the fault appear during a neighboring round.



Power glitch

- Analysis of injected faults:
  - 70% identical to clock glitch injection
  - 20% neighboring rounds
  - 10% the second most critical path of the round
- Conclusion: Clock and power glitch induced faults are due to timing constraints violation
- >90% single-bit fault

Power glitch

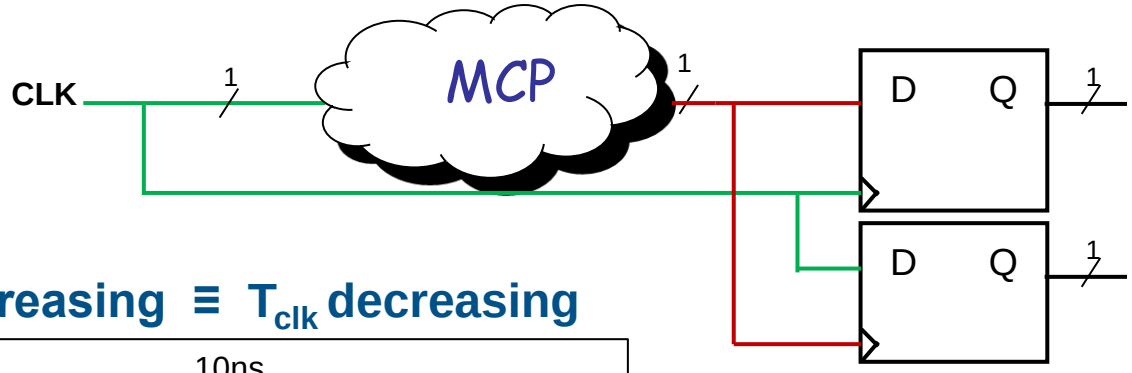
- Analysis of injected faults:
  - 70% identical to clock glitch injection
  - 20% neighboring rounds
  - 10% the second most critical path of the round
- Conclusion: Clock and power glitch induced faults are due to timing constraints violation
- >90% single-bit fault

A spatial effect component?

Linked to voltage transient propagation through the power supply grid

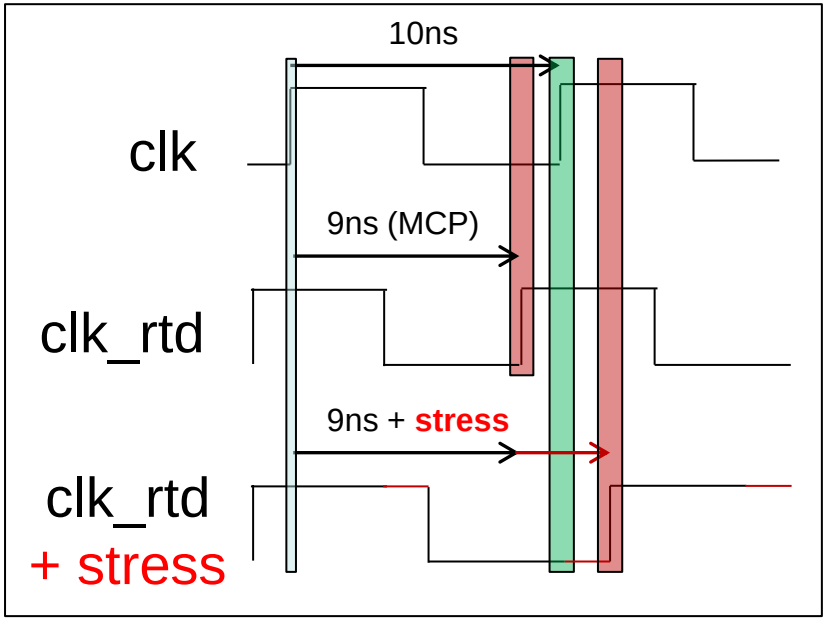
Questions

Most Critical Path (MCP)

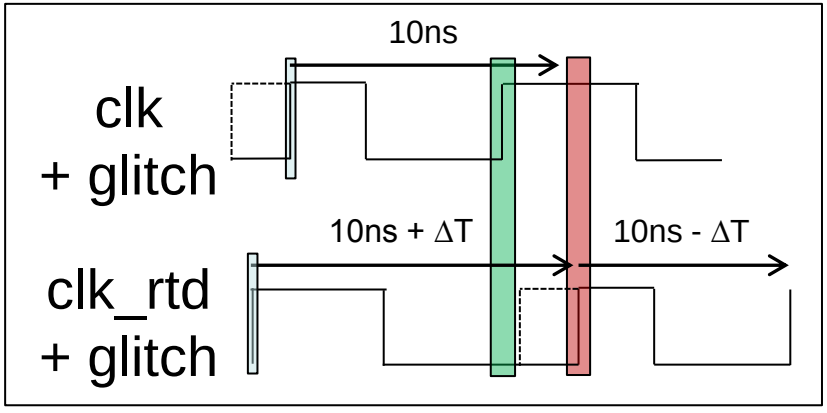


Nominal	Stressed
1	0
0	1

D_{pMax} increasing ≡ T_{clk} decreasing

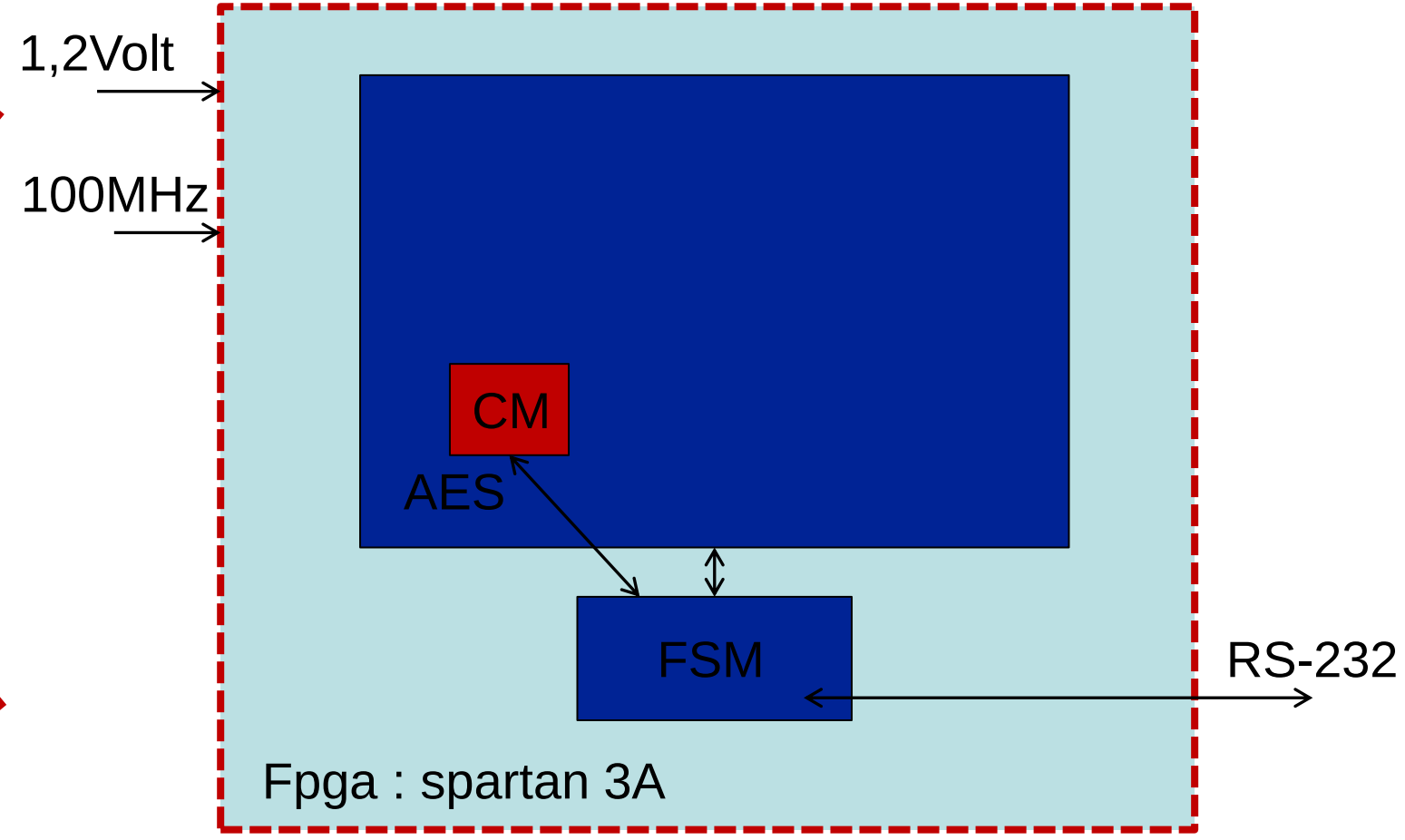


Clock glitch

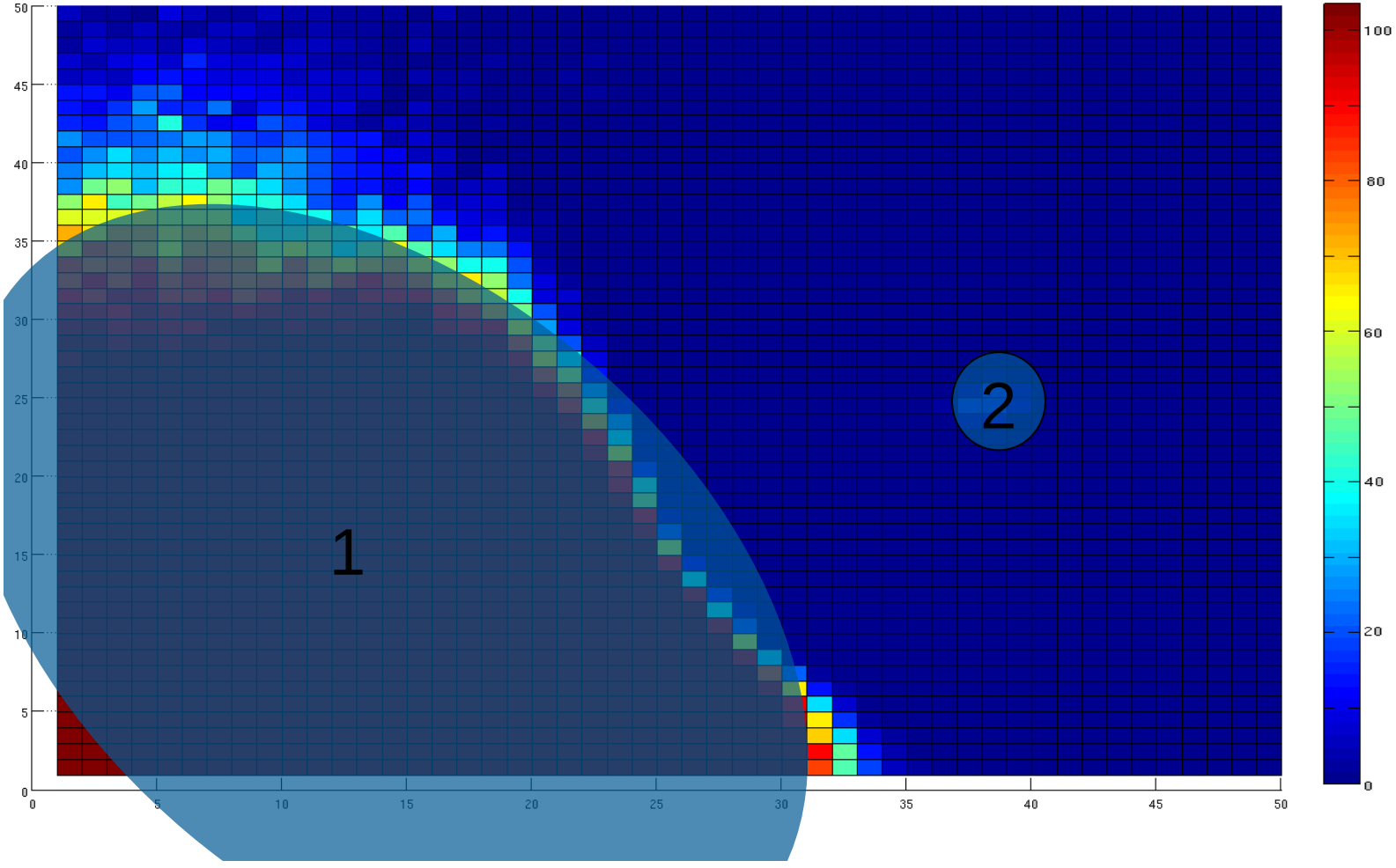


CM Spatial Limitation

FPGA + AES + Countermeasure



CM Spatial Limitation



1 : detection zone

2 : faulted zone
(bit 64 / round 2)