DE LA RECHERCHE À L'INDUSTRIE

cea

INSPIRING INNOVATION | INNOVANTE PAR TRADITION

Ecole Nationale Supérieure des Mines SAINT-ETIENNE

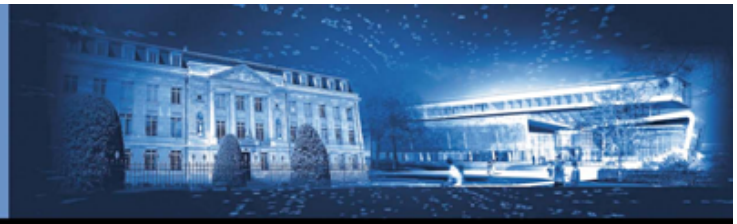
Cosade 2013

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

Introduction

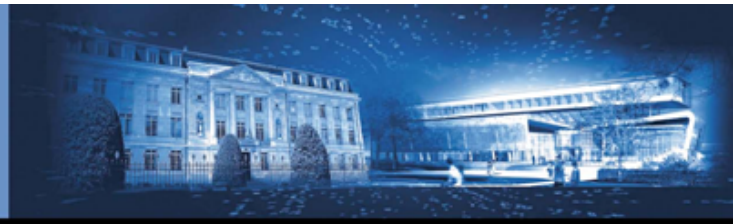


Research subject

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

Today's subject

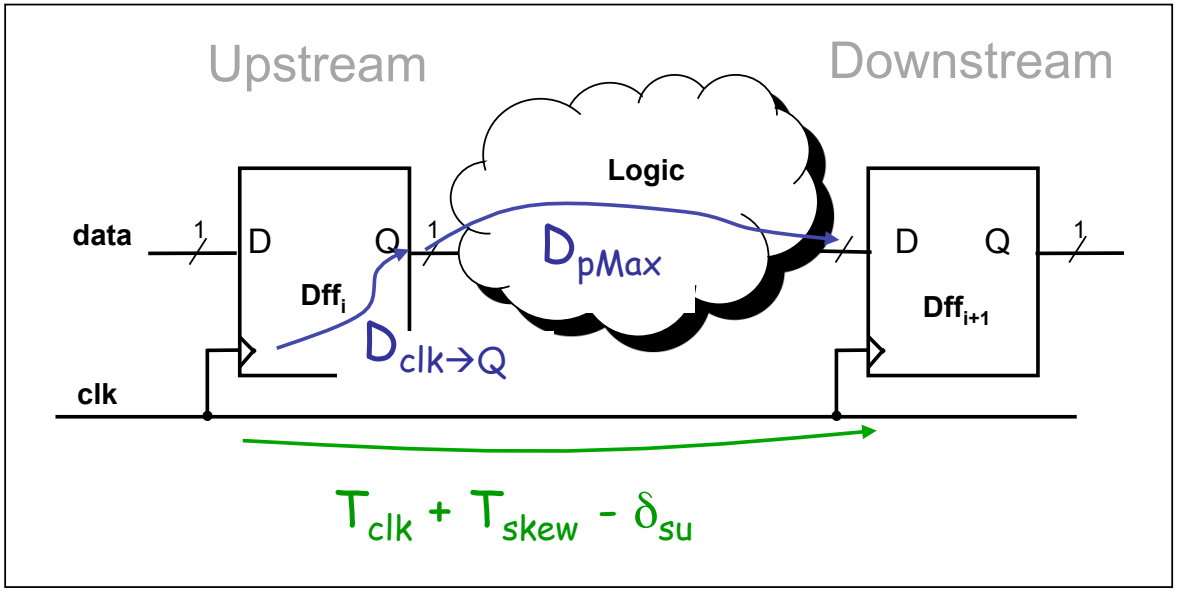
- **Power glitches fault injection mechanism**
  - **Analysis and practice**



Agenda

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

Timing constraints

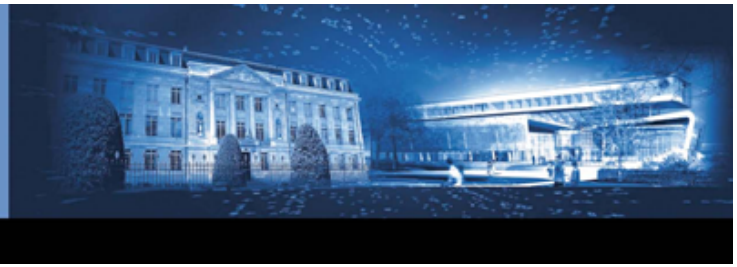


data arrival time = $D_{clk \rightarrow Q} + D_{pMax}$

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

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

Timing constraints violation



How to inject faults through timing constraints violation?

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

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

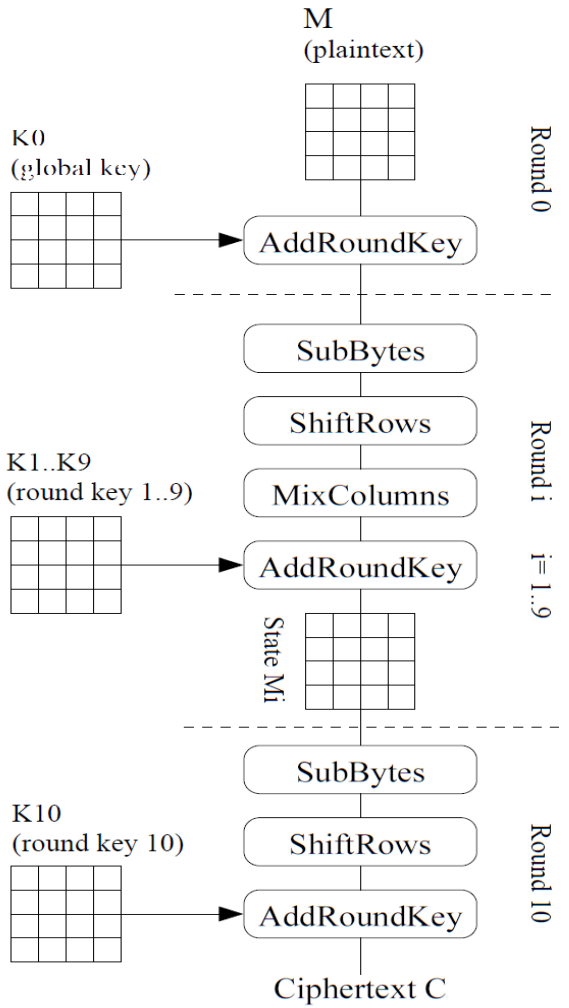
- Underpowering or overheating: (Propagation time increase)

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

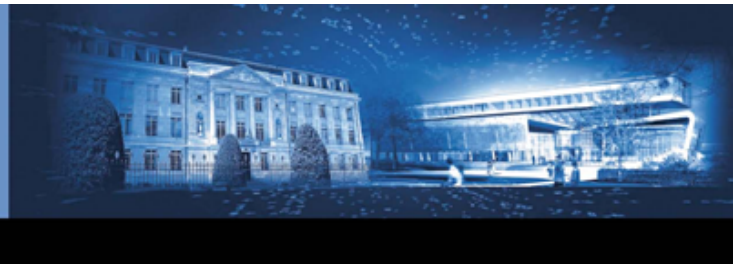
Experimental setup

Target

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



Previous research work



Common fault injection means

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

A **common mechanism** !

⇒ Timing constraints violations.

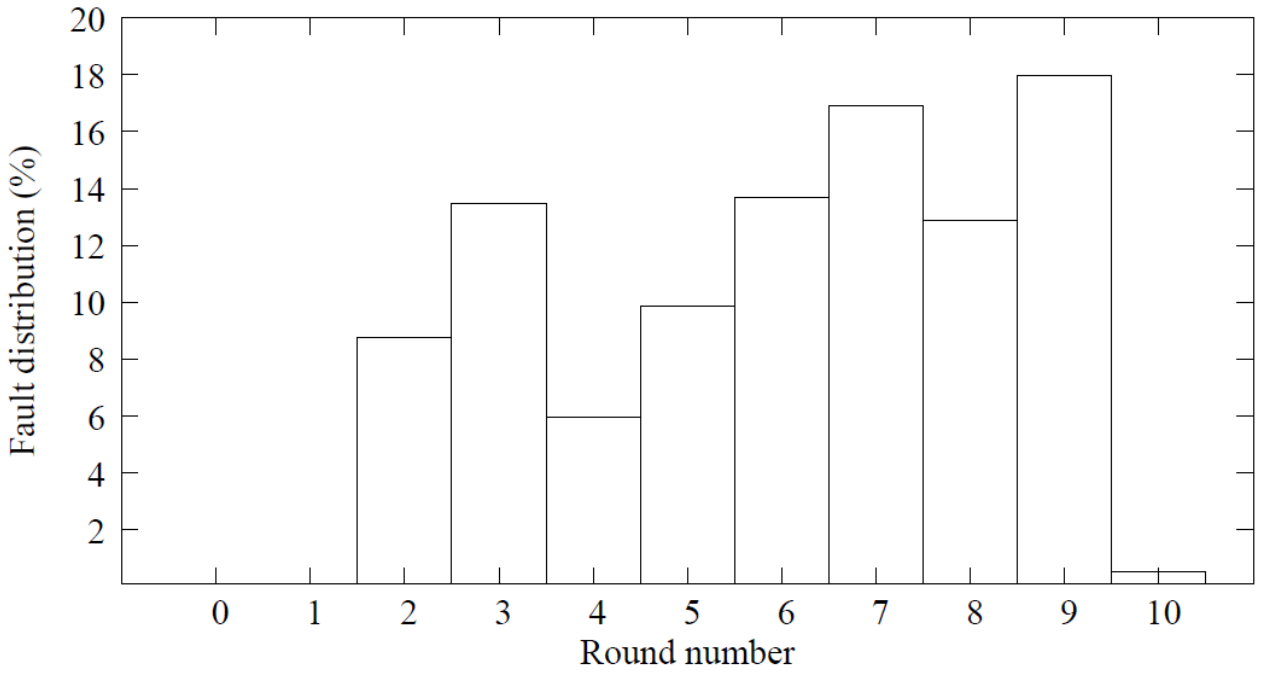
Experimental proof

- 10,000 input dataset
- Critical path faulted

Static perturbations

Issues

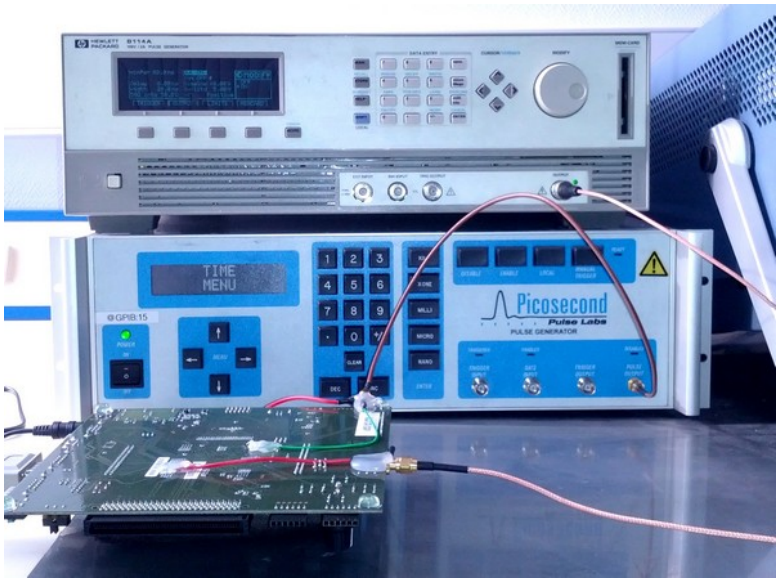
- Low timing resolution



Transient perturbations

Transient perturbations

- Clock glitch
- Power supply glitch

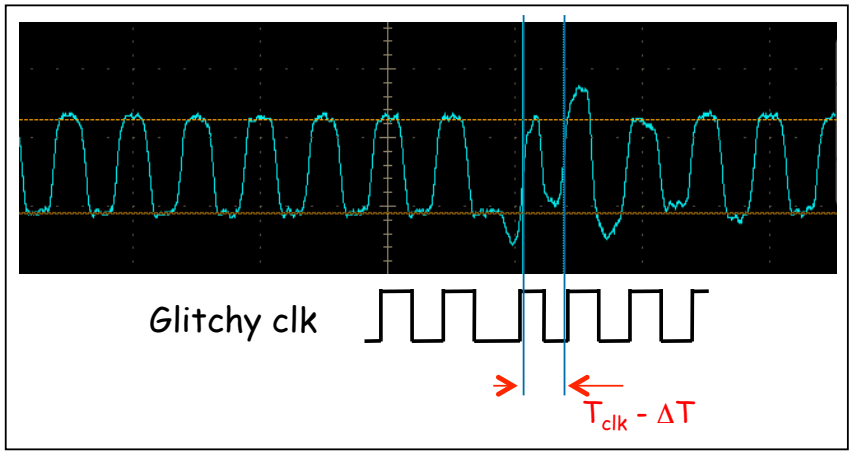


Questions

- Injection mechanism? Timing violation?
- Achievable resolution?

Transient perturbations

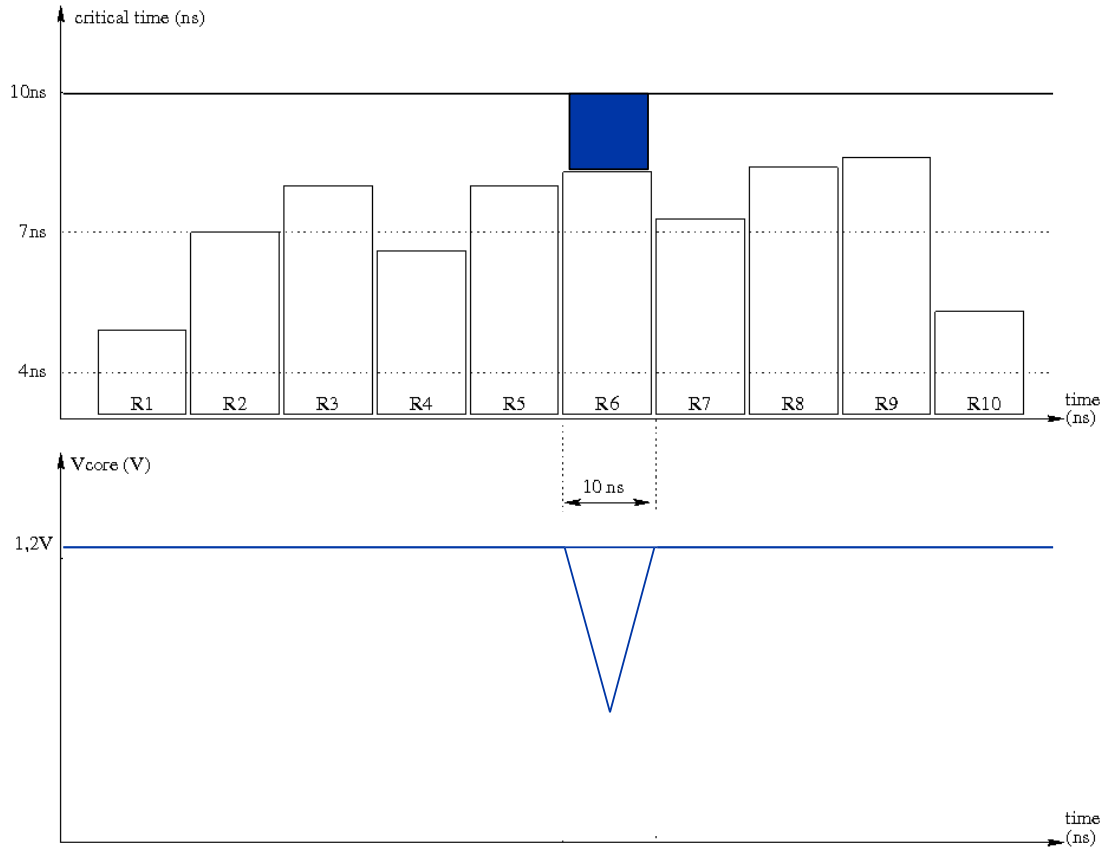
Clock glitch



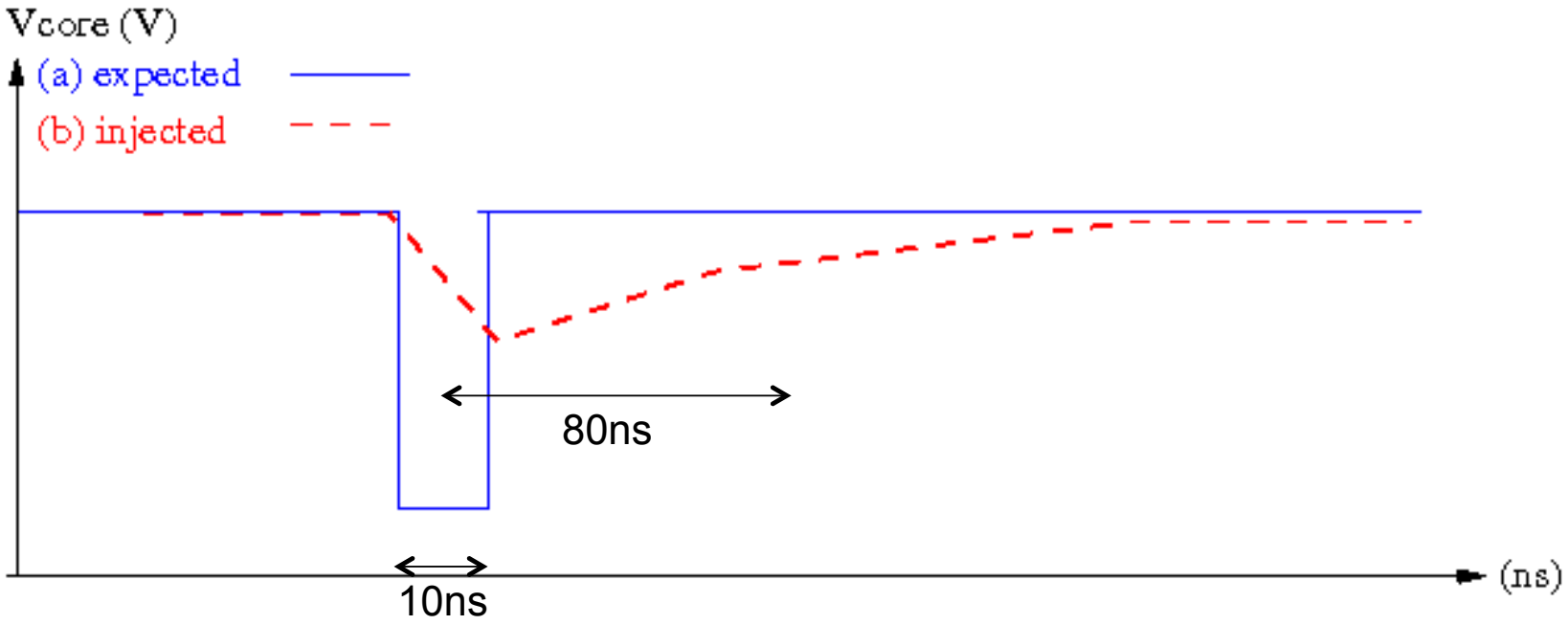
- 35ps resolution
- Global effect
- Timing constraints violation (obvious)
- A tool for critical time measurement
- Used to build a template/**reference library**

To be compared,

Power glitch: Ideal

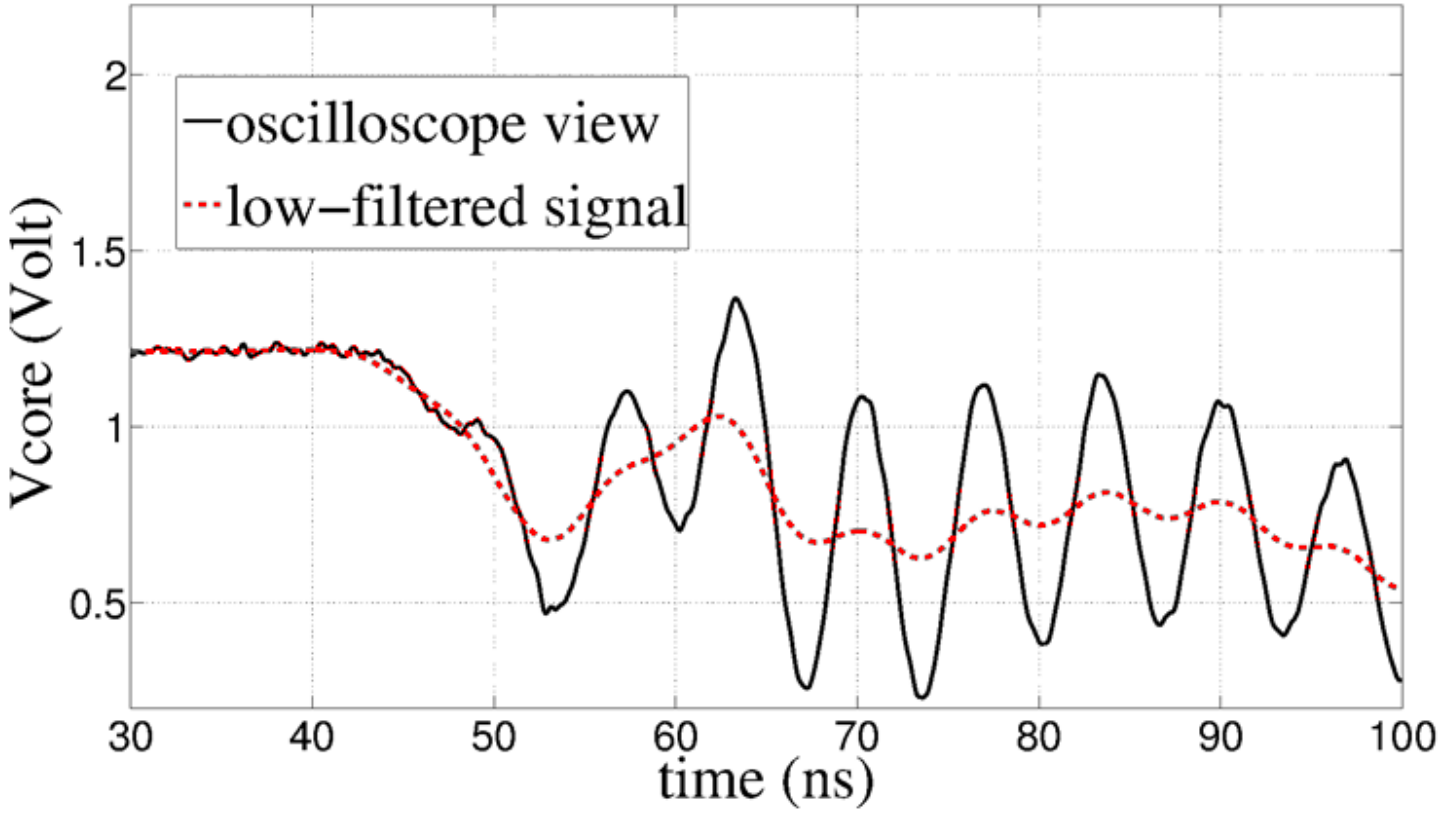


Power glitch: Input capacitance

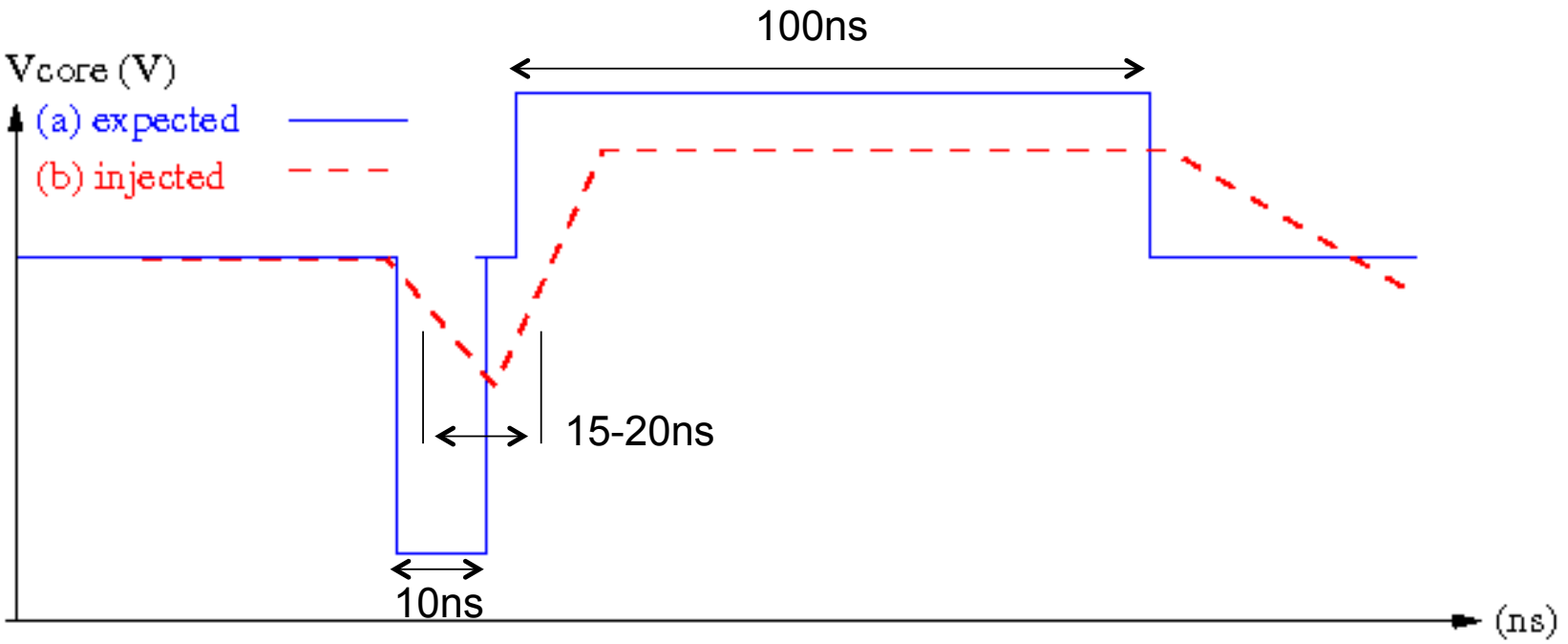


Transient perturbations

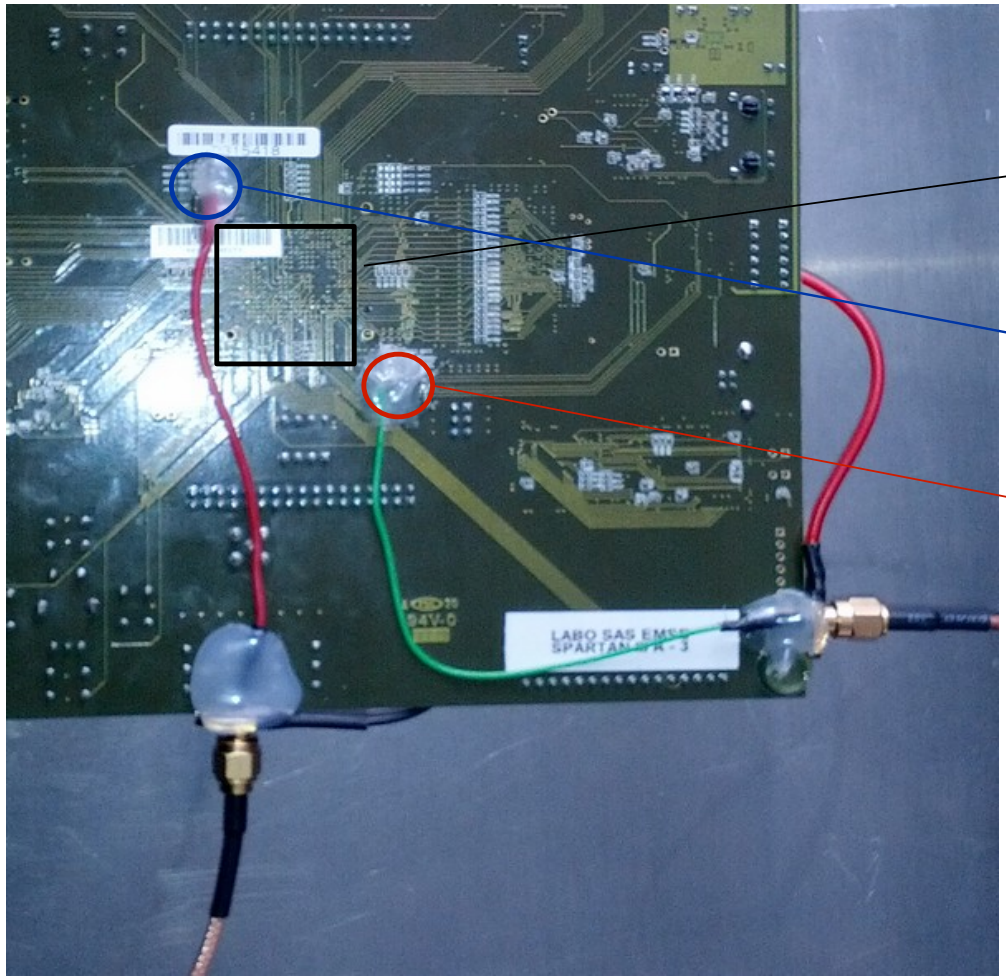
Power glitch: impedance adaptation



Power glitch: Input capacitance

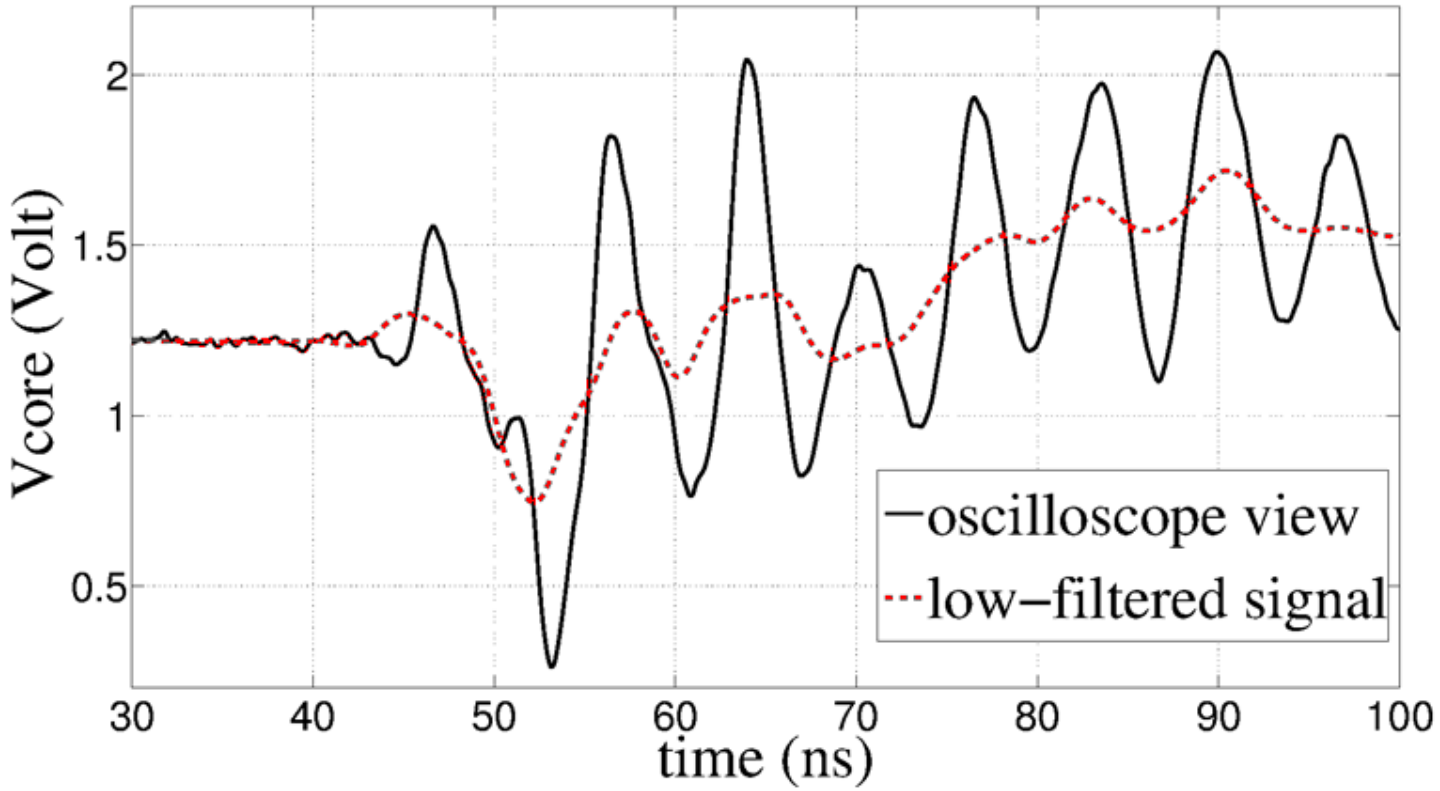


Transient perturbations



Transient perturbations

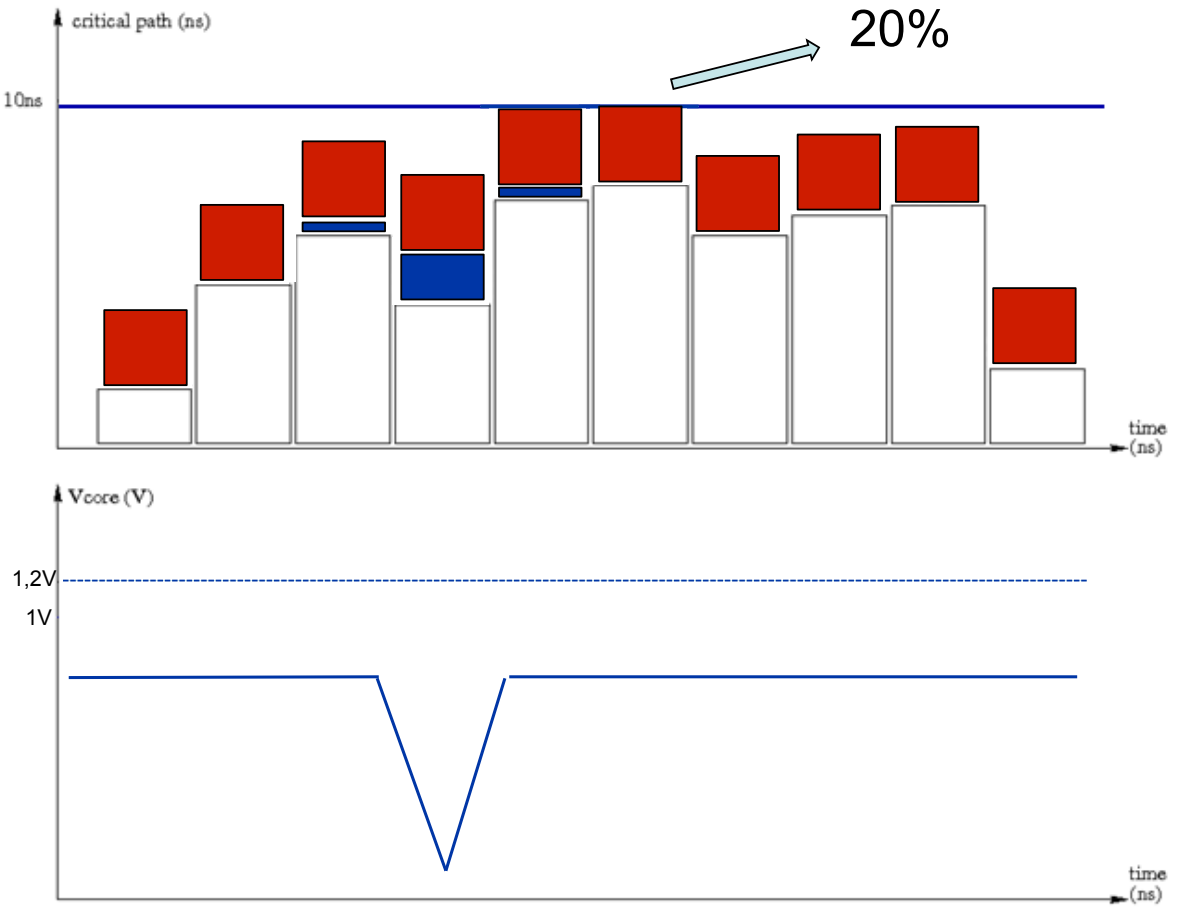
Power glitch: impedance adaptation



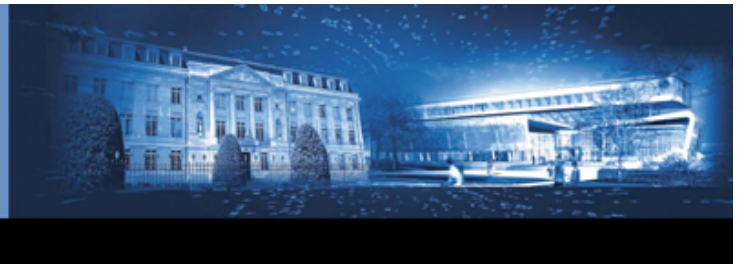
Transient perturbations

Power glitch

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



Conclusion



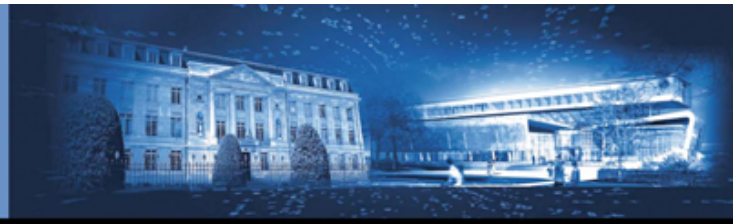
Power glitch

- 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

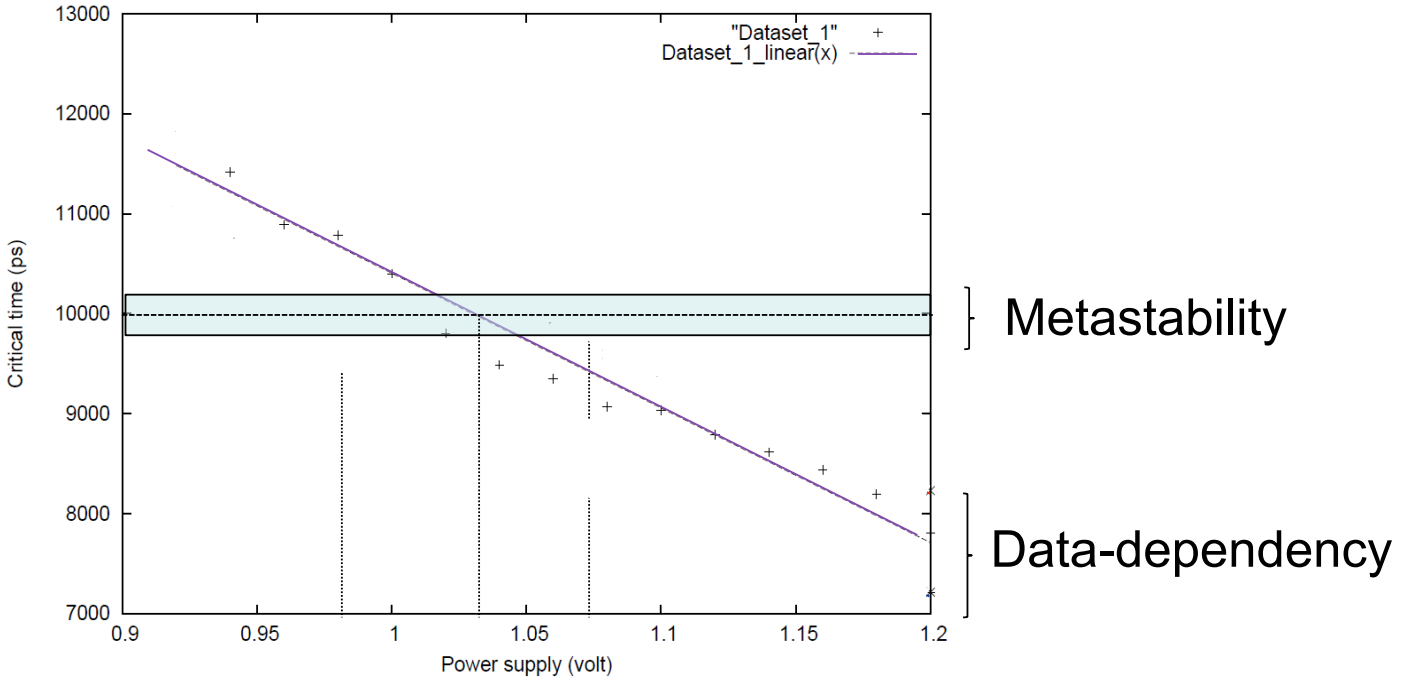
Questions



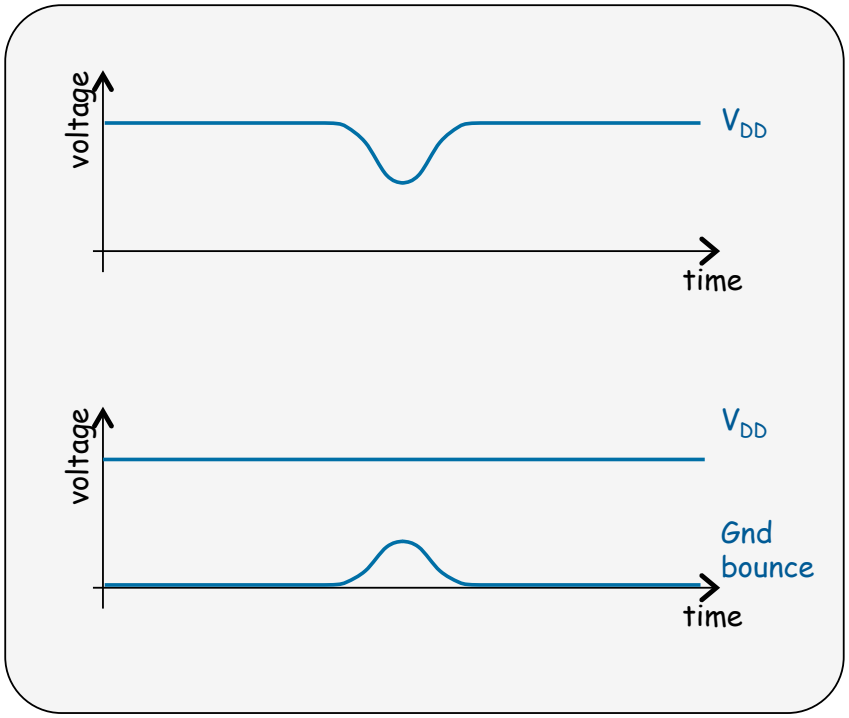
Static perturbations

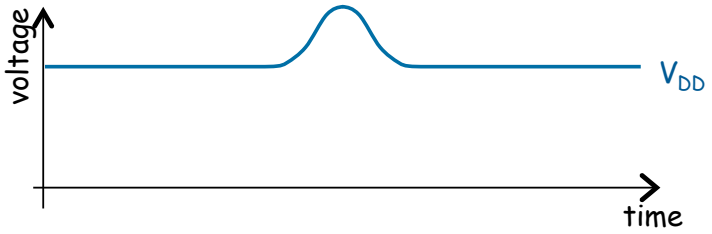
Underpowering

- Voltage decrement => critical path increase



Power glitch

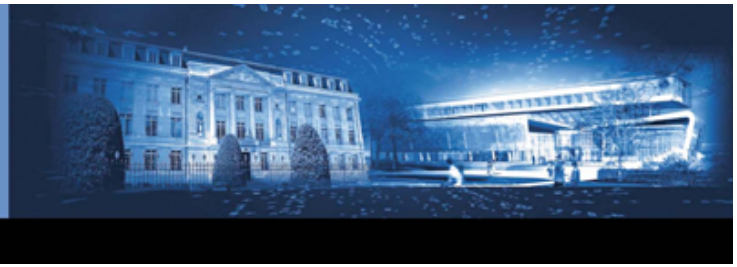




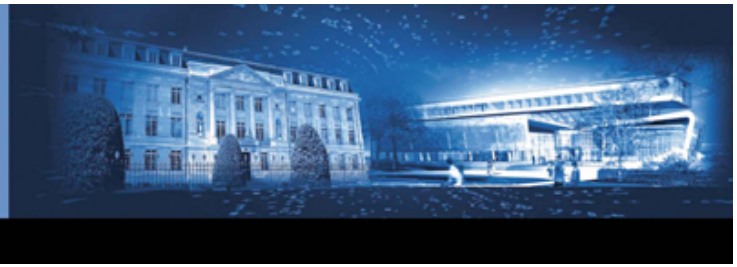
- Injection mechanism?

=> Timing violation

Conclusion

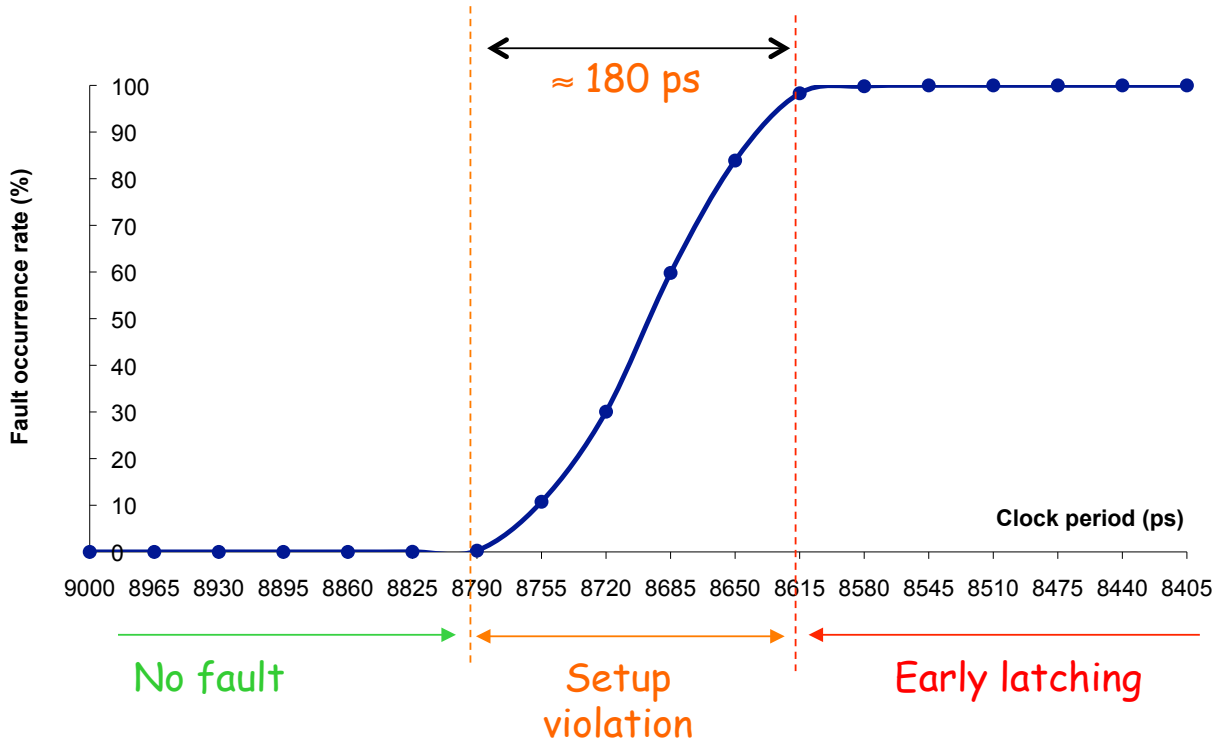


- **Overclocking, underpowering, overheating** generate exactly the sames faults => **same mechanism**,
- **Static stresses** give **accurate results** BUT **random temporal localization**,
- **Transient stresses** give a **better temporal localization** BUT inducing **spactial effect**,
- Indepth investigation are going to explain these spatial effects.



Overclocking

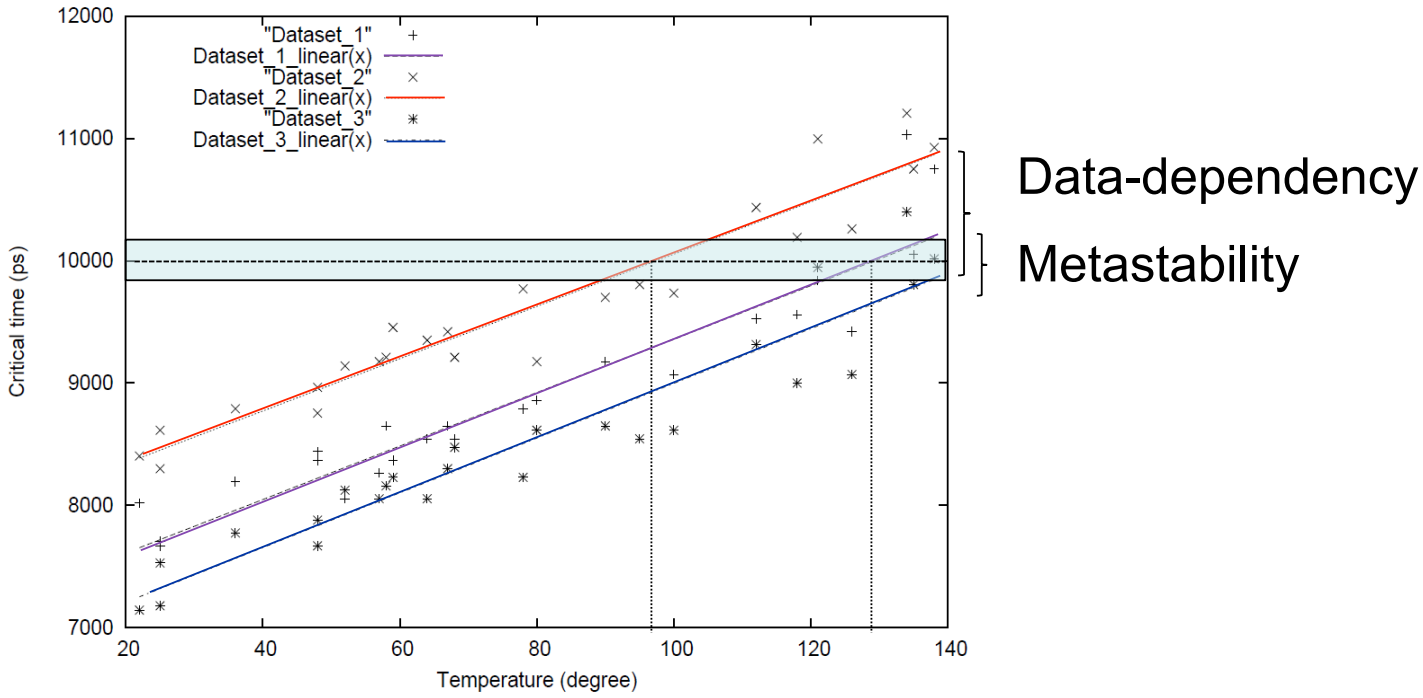
- Fault occurrence rate vs applied stress



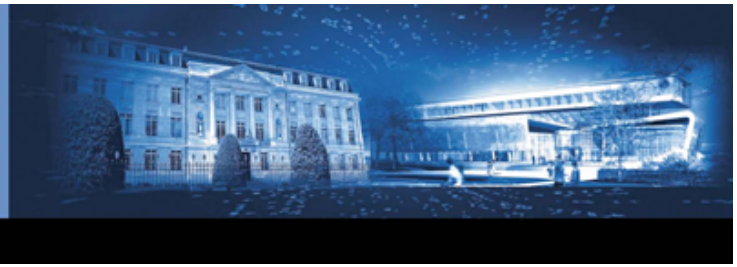
Static perturbations

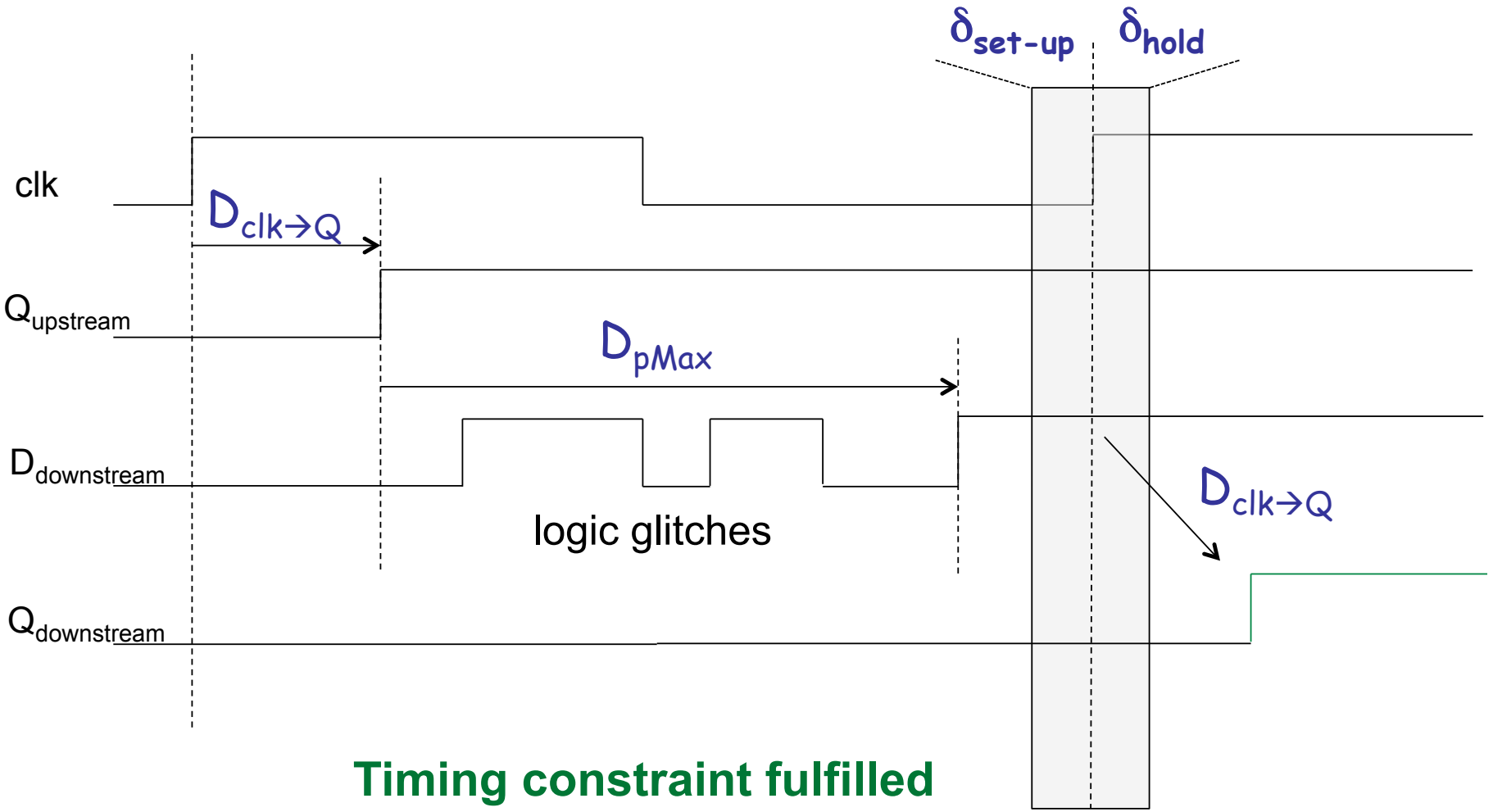
Overheating

- Temperature increase => critical path increase



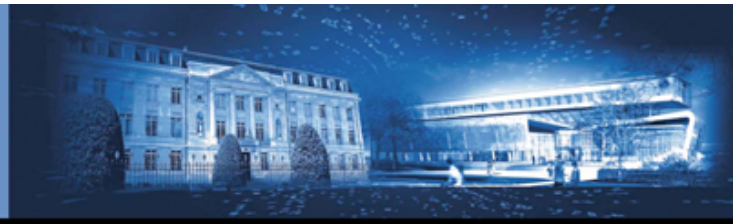
Overclocking

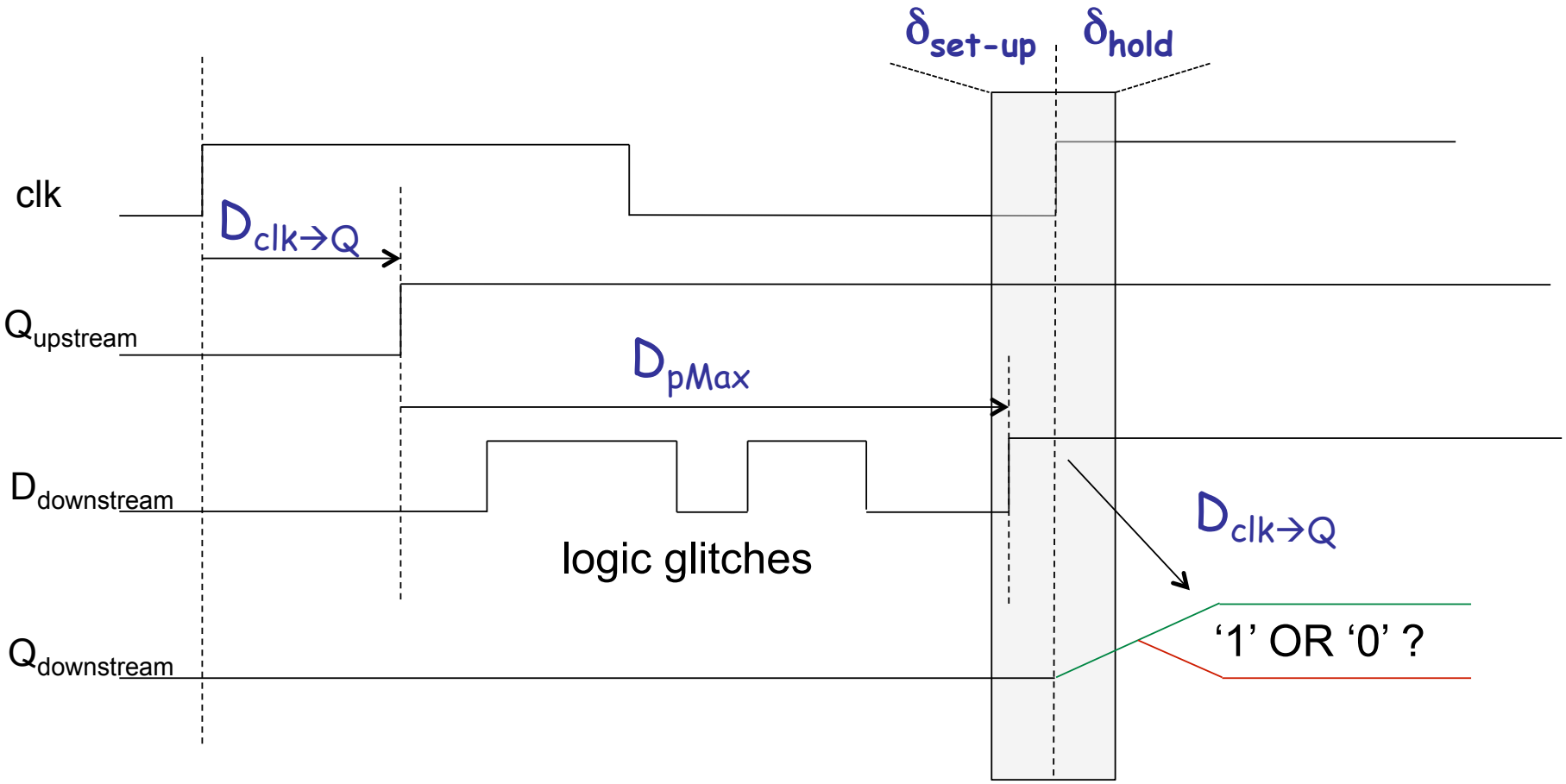




Timing constraint fulfilled

Overclocking

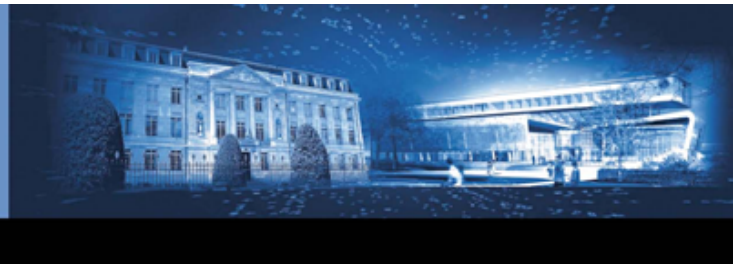


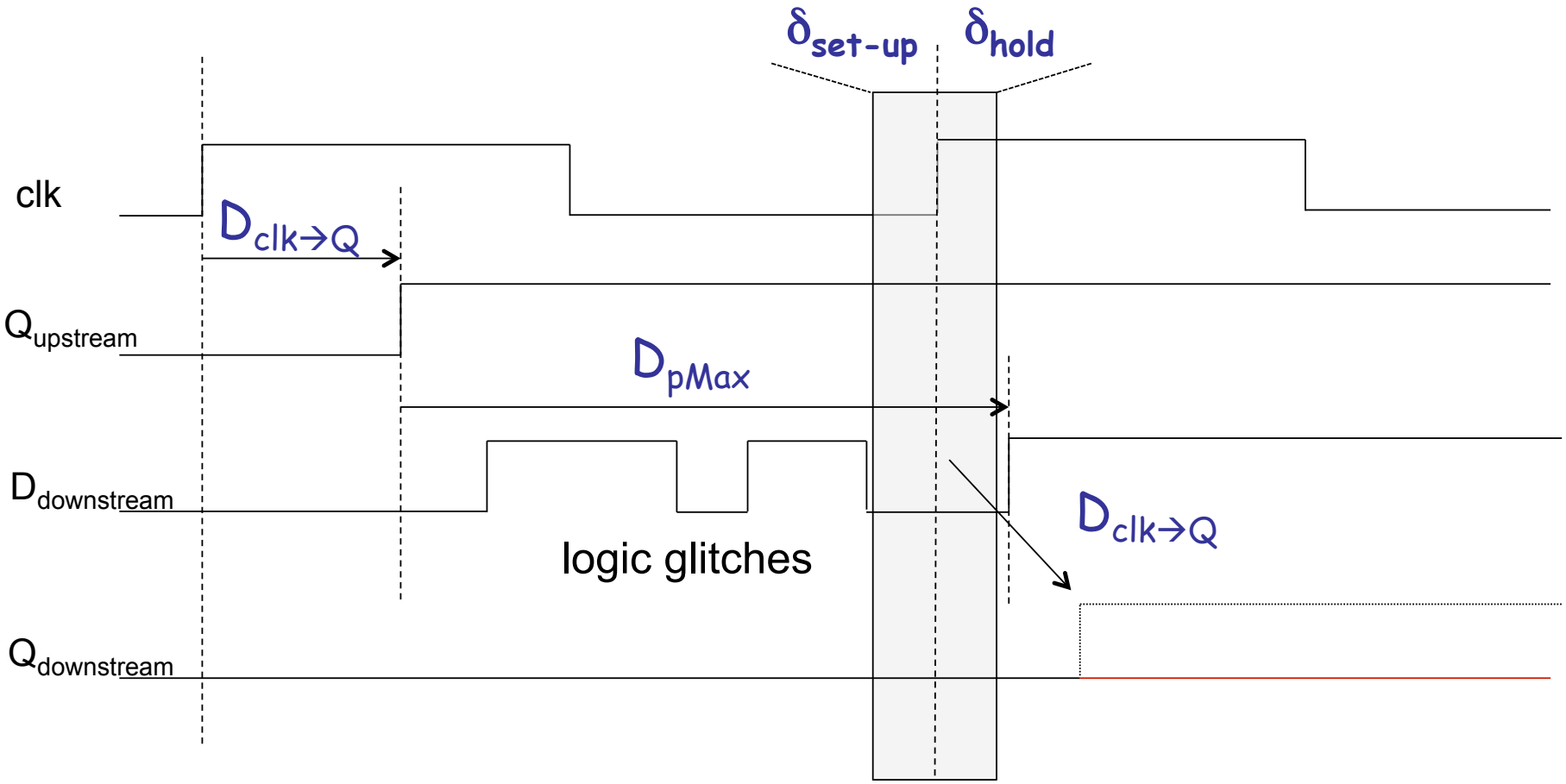


Setup time violation (i.e. timing constraint violation) :

⇒ metastability (non-deterministic)

Overclocking

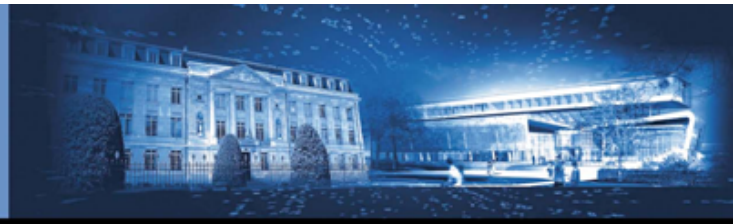


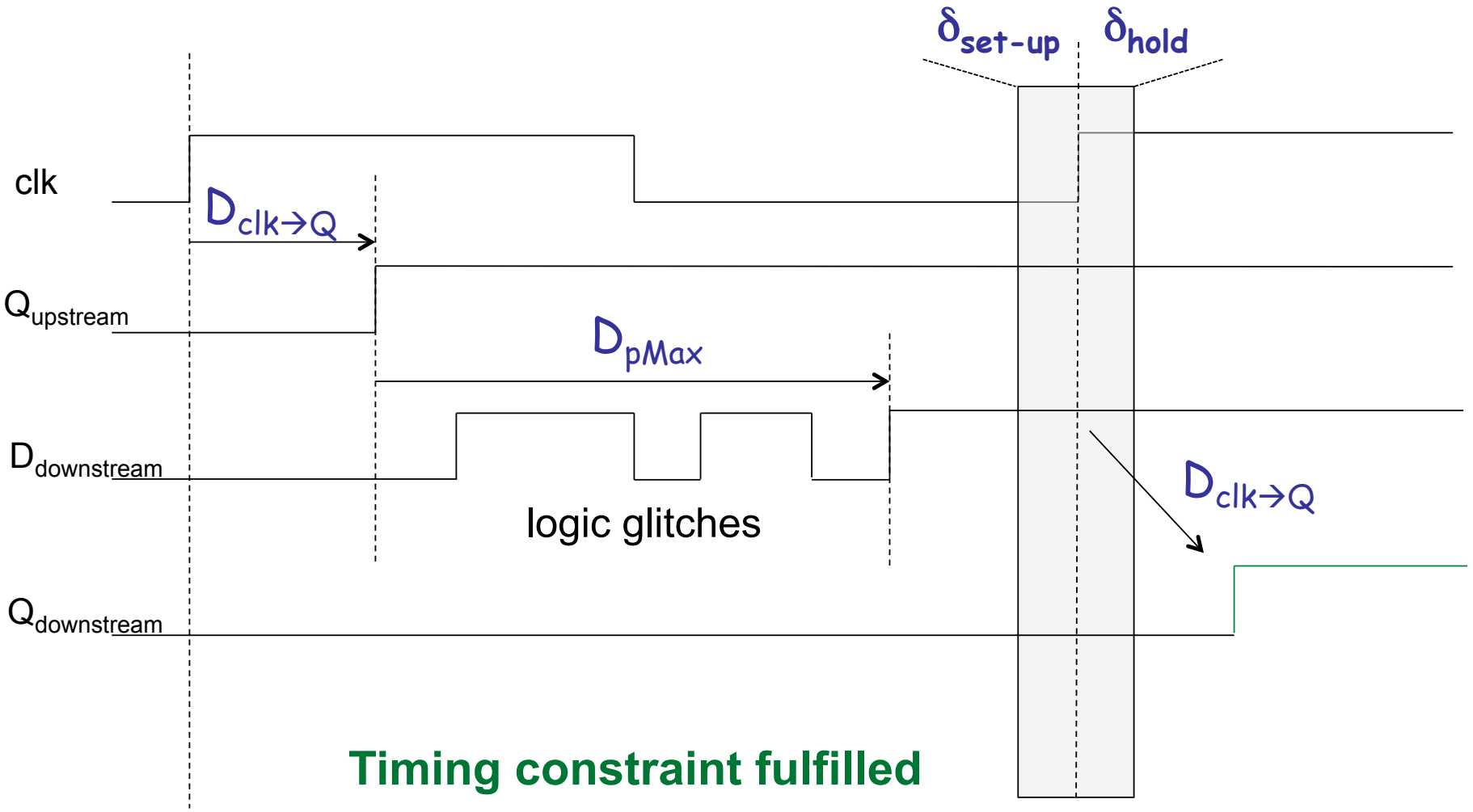


Timing constraint violation :

Early latching (deterministic)

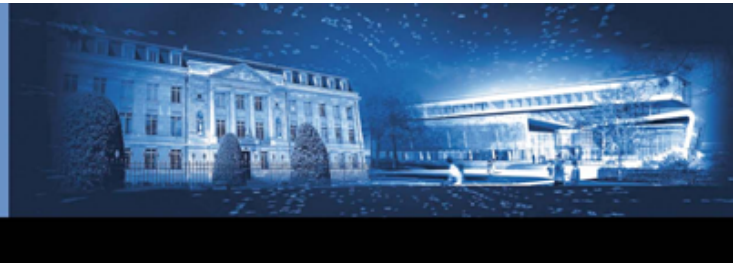
Underpowering/Overheating

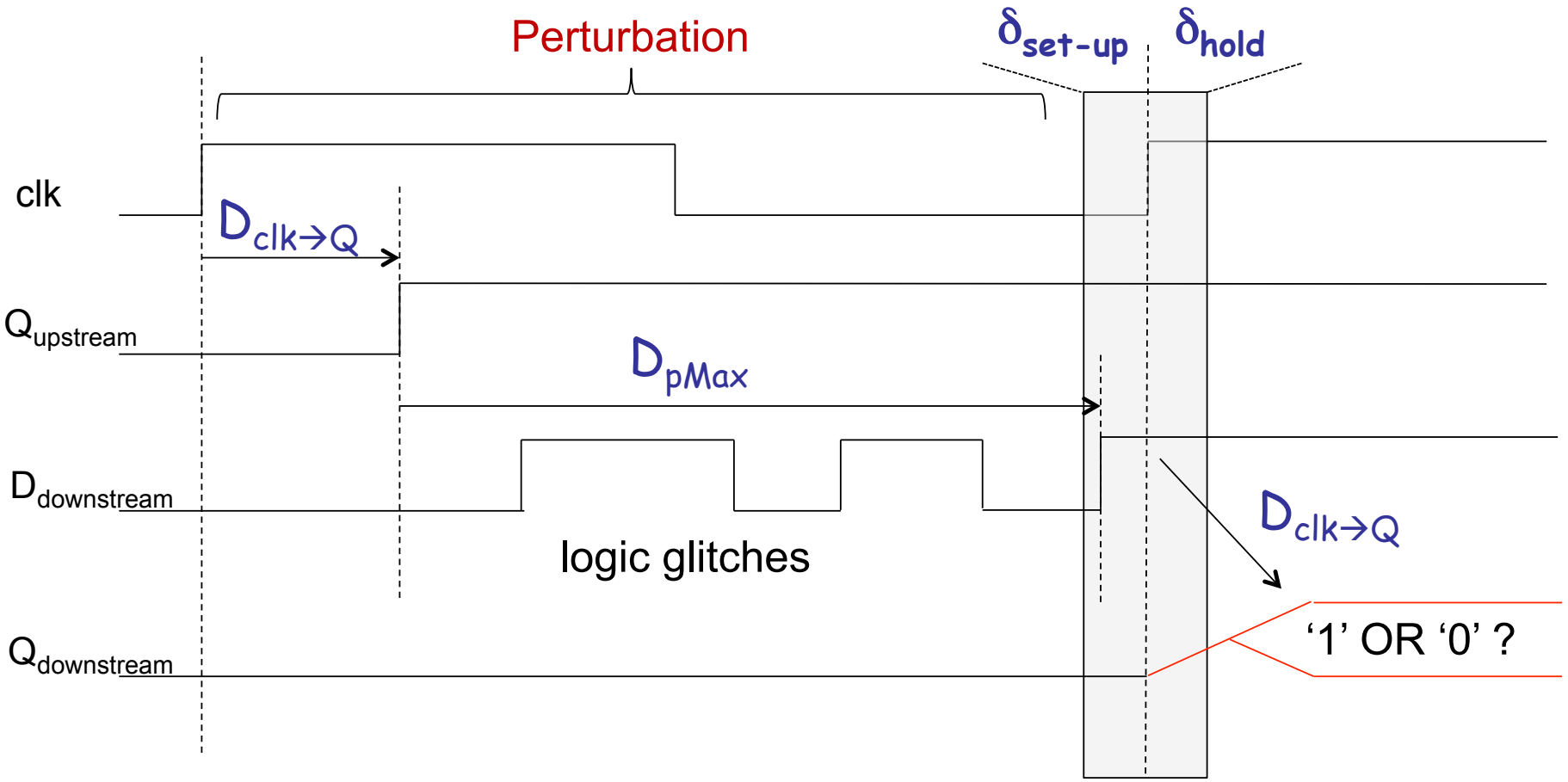




Timing constraint fulfilled

Underpowering/Overheating

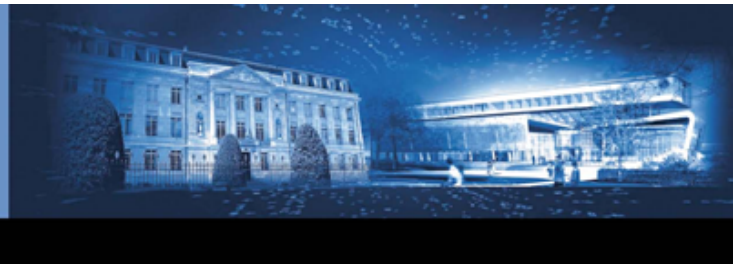


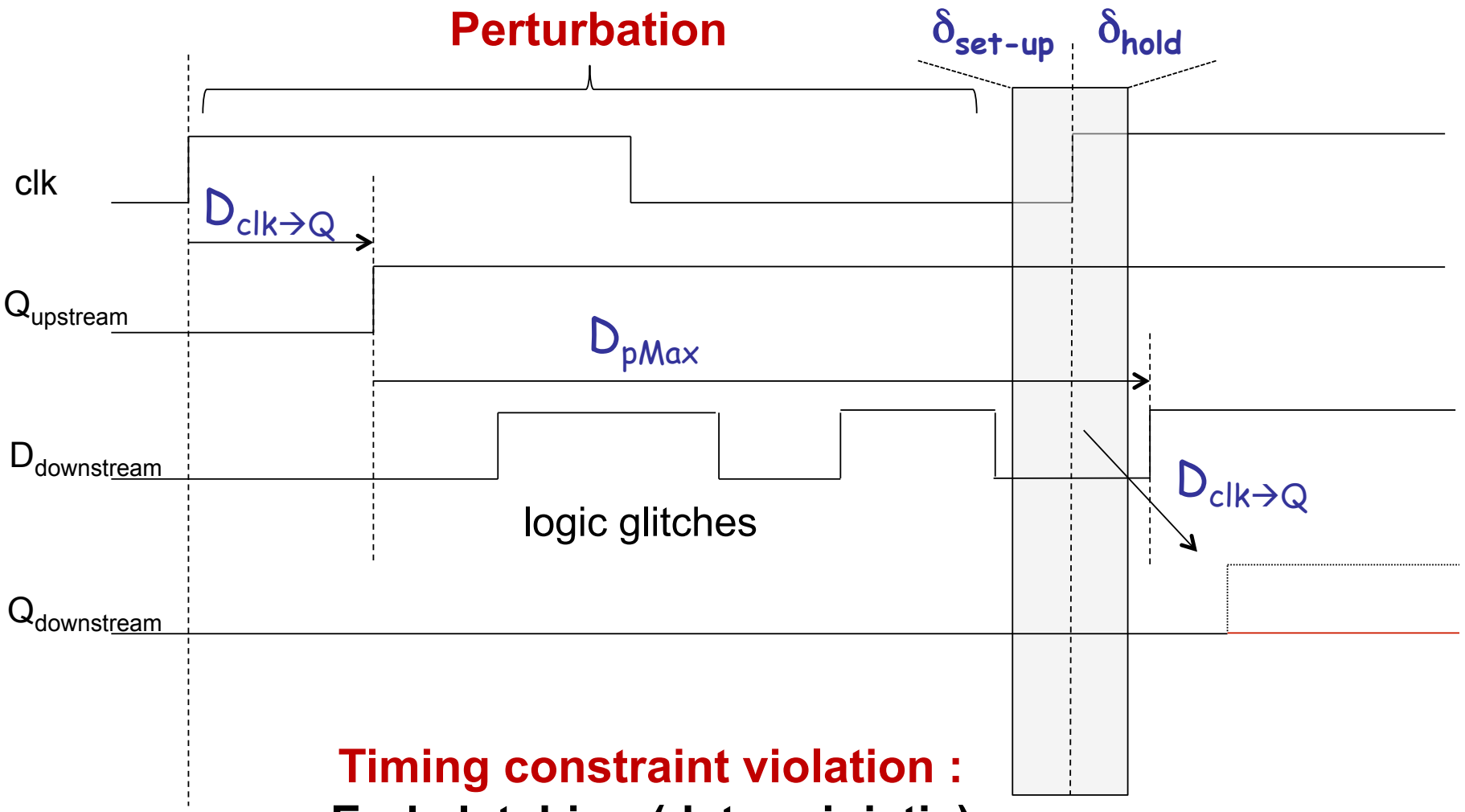


Setup time violation (i.e. timing constraint violation) :

⇒ metastability (non-deterministic)

Underpowering/Overheating



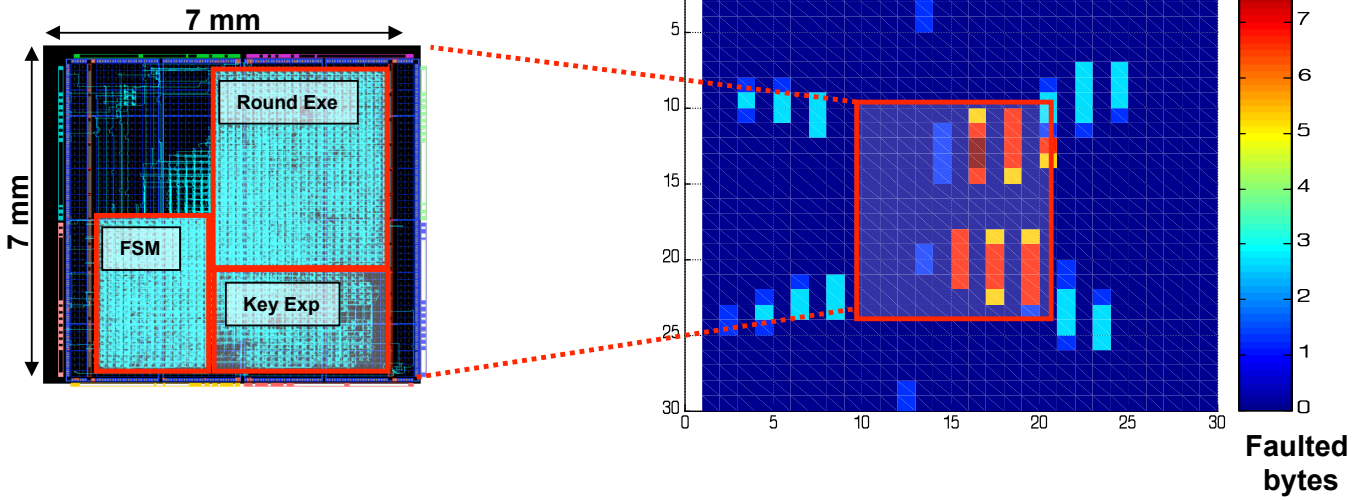


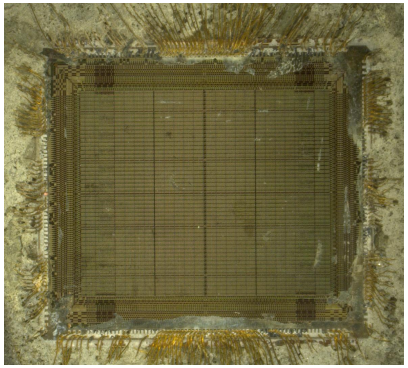
Timing constraint violation :

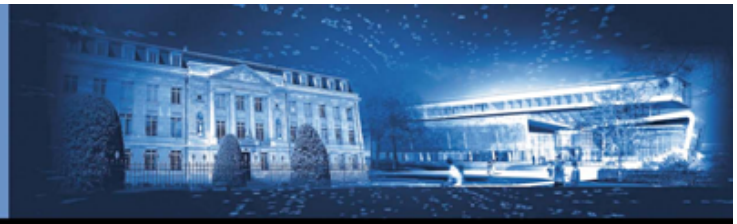
Early latching (deterministic)

Further work

EM pulse



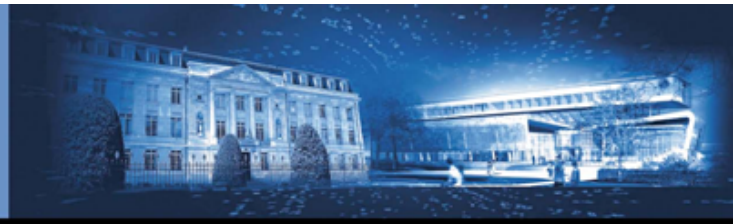




Context

- Many of our daily used electronic devices embed cryptographic features,
- Often targeted by malicious attackers,
- Indepth understanding of attack means is needed to protect properly these devices.

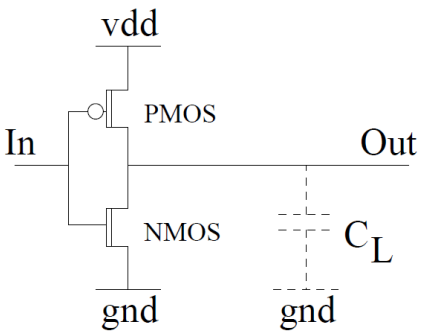
References

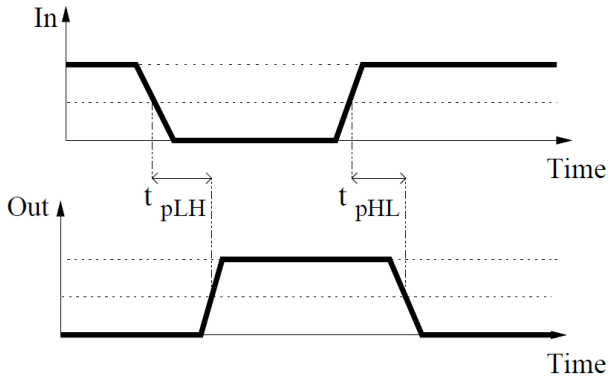


- Josep Balasch, Benedikt Gierlichs, and Ingrid Verbauwhede. An indepth and black-box characterization of the effects of clock glitches on 8-bit mcus. 2011.
- H. BarEl, H. Choukri, D. Naccache, M. Tunstall, and C. Whelan. The sorcerer's apprentice guide to fault attacks. 2006.
- Alessandro Barenghi, Guido Bertoni, Luca Breveglieri, Mauro Pellicioli, and Gerardo Pelosi. Low voltage fault attacks to aes. 2010.
- E. Biham and A. Shamir. Differential fault analysis of secret key cryptosystems. 1997.
- D. Boneh, R.A. DeMillo, and R.J. Lipton. On the importance of checking cryptographic protocols for faults. 1997.
- Eric Brier, Christophe Clavier, and Francis Olivier. Correlation power analysis with a leakage model. 2004.
- D. Ha, K. Woo, S. Meninger, T. Xanthopoulos, E. Crain, and D. Ham. Time-domain cmos temperature sensors with dual delay-locked loops for microprocessor thermal monitoring. 2011.
- J.U. Horstmann, H.W. Eichel, and R.L. Coates. Metastability behavior of cmos asic flip-flops in theory and test. 1989.
- Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. 1999.
- Oliver K¨ommerling and Markus G. Kuhn. Design principles for tamperresistant smartcard processors. 1999.
- Yang Li, Kazuo Ohta, and Kazuo Sakiyama. New fault-based sidechannel attack using fault sensitivity. 2012.
- N. Selmane, S. Bhasin, S. Guilley, and J.L. Danger. Security evaluation of asics and field programmable gate arrays against setup time violation attacks. 2011.
- Sung-Ming Yen and Marc Joye. Checking before output may not be enough against fault-based cryptanalysis. 2000.

Timing constraints violation

Inverter :





$$t_{pLH} = \frac{C_L \left[\frac{2|V_{th,p}|}{V_{DD} - |V_{th,p}|} + \ln\left(3 - 4\frac{|V_{th,p}|}{V_{DD}}\right) \right]}{\mu_p C_{ox} \frac{W_p}{L_p} (V_{DD} - |V_{th,p}|)}$$

- Power Supply.

V_{DD} ↘ => t_{pLH} ↗

- Mobility :

temperature dependent.

T° ↗ => t_{pLH} ↗

(generally)