Département Microélectronique

MIC

EM fault Modelling : the sampling fault Model explained

M. Dumont, M. Lisart, P. Maurine

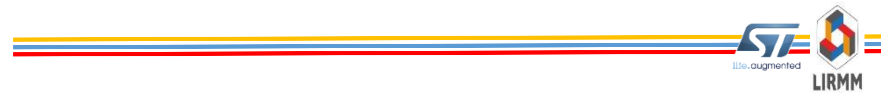
23 Mai 2019

Agenda

life.augmented LIRMM

- State of the Art & the Sampling fault model
- Lessons from EM Induction theory
- Modeling
  - Impact of an EMFI on the power and ground grids
  - Impact of an EMFI on IC operation
- Lessons to design robust ICs
- Lessons to design efficient EMFI platforms
- Conclusion

State of the Art



State of the Art

life.augmented

LIRMM

Year	Finding	Reference
2002	EM injection disrupts the behavior of embedded memories	'Eddy current for Magnetic Analysis with Active Sensor' (Esmart 2002)
2007	EM injection disrupts the course of a RSA algorithm	'Optical and EM Fault-Attacks on CRT-based RSA: Concrete Results' (Austrochip 2007)
2009	Harmonic EM Injection modifies the ***propagation delays*** of logical paths	'Assessment of the Immunity of Unshielded Multicore Integrated Circuits to Near Field Injection' (EMC-Zurich 2009)
2011	Harmonic EM Injection modifies **the oscillating Frequency** of an internal clock generator	'Local and Direct EM Injection of Power Into CMOS Integrated Circuits' (FDTC 2011)
2012	Harmonic EM Injection modifies the behavior of RO based TRNG **(phase locking)**	'Contactless Electromagnetic Active Attack on Ring Oscillator Based True Random Number Generator' (COSADE 2012)
2012	EM pulse Injection produces ***timing faults*** during the course of hardware cryptographic modules	'Injection of transient faults using electromagnetic pulses - Practical results on a cryptographic system' (ePrint 2012)
2012	EM pulse Injection produces ***timing faults*** during the course of hardware and software …	'Electromagnetic Transient Faults Injection on a Hardware and a Software Implementations of AES' (FDTC2012)
2014	Evaluation of a countermeasure based on the ***timing slack monitoring***	'Efficiency of a Glitch Detector against Electromagnetic Fault Injection' (DATE 2014)
2014	EM injection does not induce only ***timing faults***	'Evidence of a Larger EM-Induced Fault Model' (Cardis 2014)
2016	EM injection induces ***Sampling Faults***	'A fully-digital EM pulse detector' (DATE 2016)
2016	A low cost digital EMFI detector based on the ***Sampling Fault Model***	'Electromagnetic fault injection: the curse of flip-flops' (J. Cryptographic Engineering 2017)

Sampling Fault Model

Electromagnetic fault injection: the curse of flip-flops. (J. Cryptographic Engineering 2017)

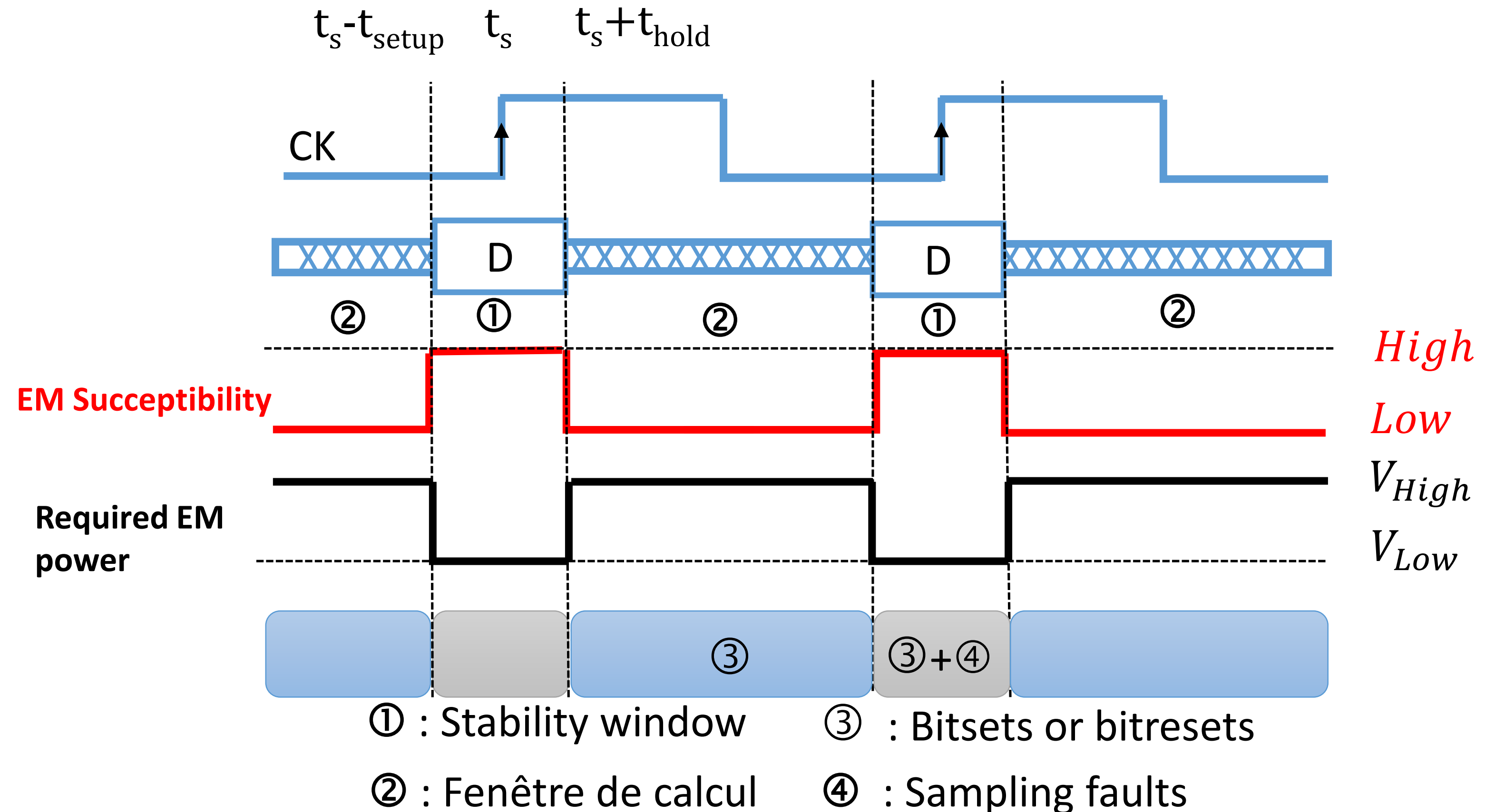
i) Deduced from expirementations

ii) EMFI disrupts signals at the input of DFFs :

- data D,
- Clock CK,
- Reset R ,
- Set,
- Vdd and Gnd

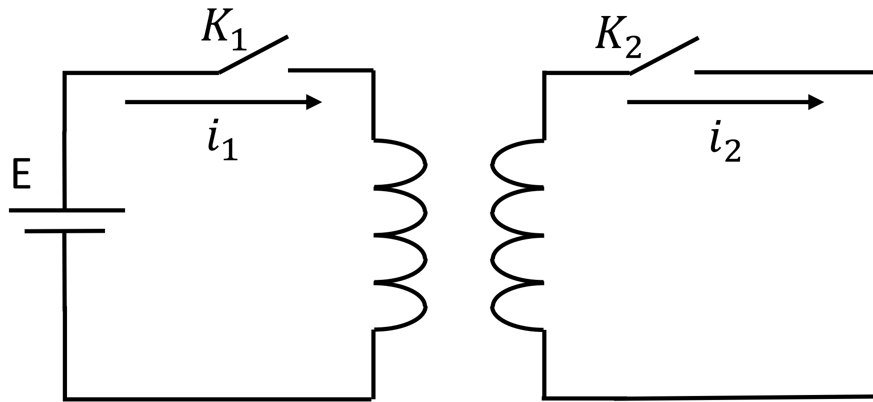
iii) Fauts occur within the sampling window of duration ~($t_{setup+}t_{hold}$) arround rising clock edges)

iv) EM susceptibility is maximum during sampling windows



EM Induction

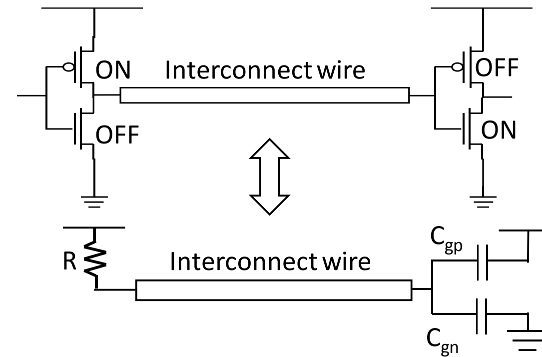
EM Induction : basics and implications related to EMFI



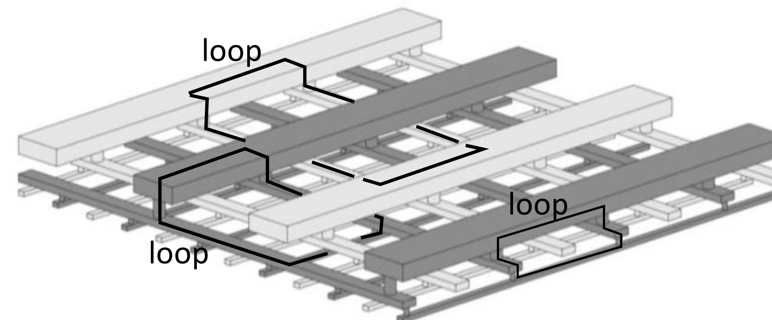
K_2 *open*	K_1 *open*	$i_1=0$	$i_2=0$	
	K_1 *closed*	$i_1>0$	$i_2=0$	
K_2 *closed*	K_1 *open*	$i_1=0$	$i_2=0$	
	K_1 *closed*	$i_1>0$	$\frac{di_1}{dt}>0$	$i_2<0$
			$\frac{di_1}{dt}=0$	$i_2=0$

EM induction induces a emf on closed loops !

Interconnect wires

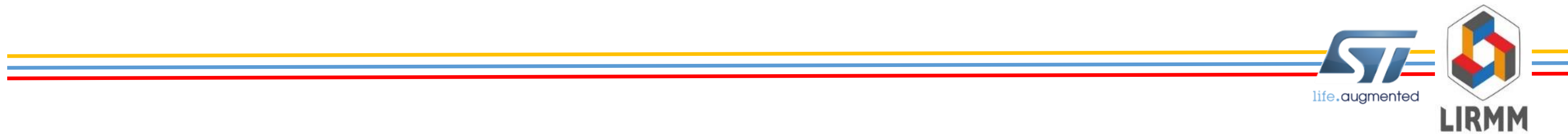


Supply and ground networks



EMFI induces parasitic currents only in the power and ground networks

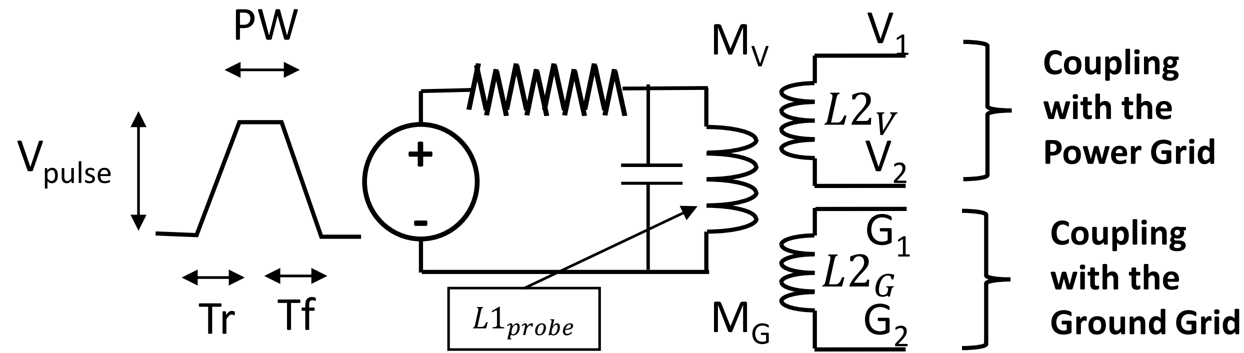
Impact of EMFI on the power and ground grids



Modeling @ Phyiscal level

EM Induction on the power & ground grids

life.augmented LIRMM



$$M_V = k_V \sqrt{L1_{probe} \times L2_V}$$

$$M_G = k_G \sqrt{L1_{probe} \times L2_G}$$

Asymetric EM coupling

V_1 V_2

VDC, Rpad, L, Vdd, R, Vddi, Vddj, Vdd, L, Rpad, VDC

C_{decap}, C_{GV}, C_{GV}, C_{decap}

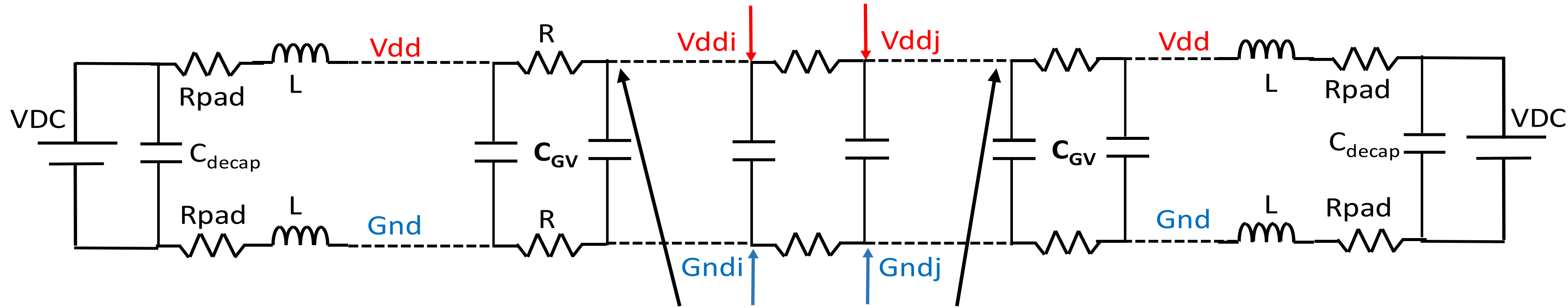
Rpad, L, Gnd, R, Gndi, Gndj, Gnd, L, Rpad

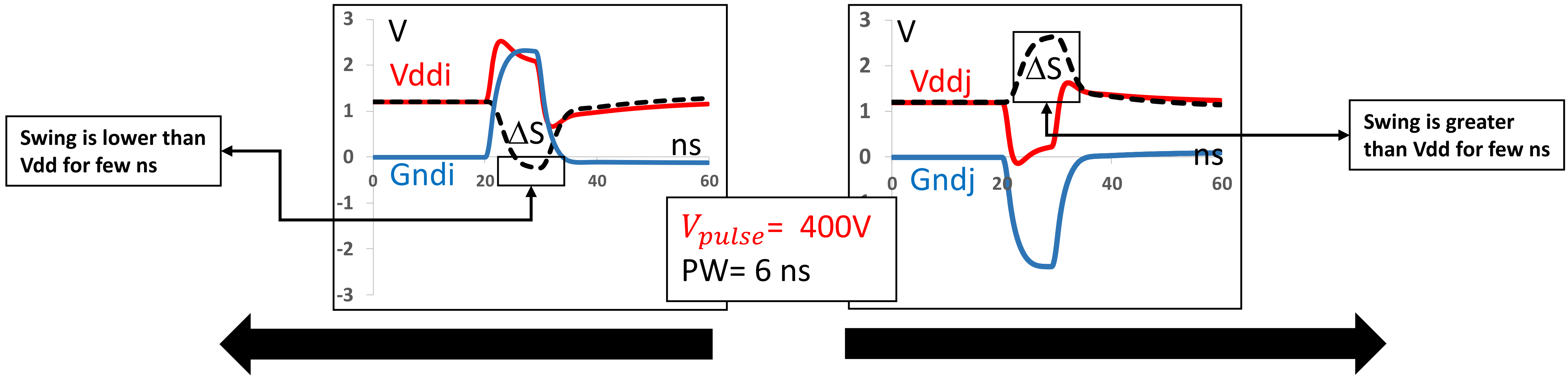
G_1 G_2

Supply & Pad | Power & Ground Grids | Supply & Pad

EM Induction on the power & ground grids : Swing

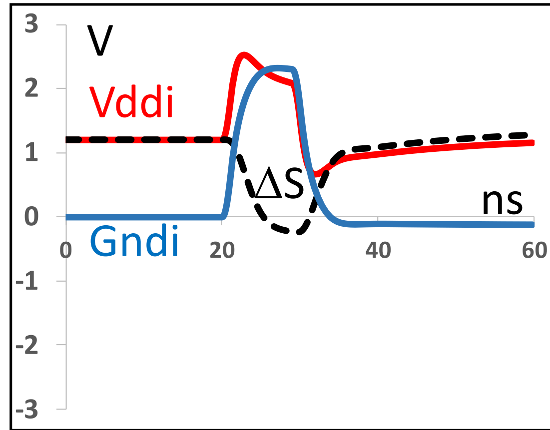
- $L1_{probe} = 1nH$
- $L2_V = 300pH$,
- $L2_G = 400pH$
- $k_V = 0{,}3$
- $k_G = 0{,}9$
- $R \;\; = 1\,\Omega$
- $C_{GV} = 1$ nF

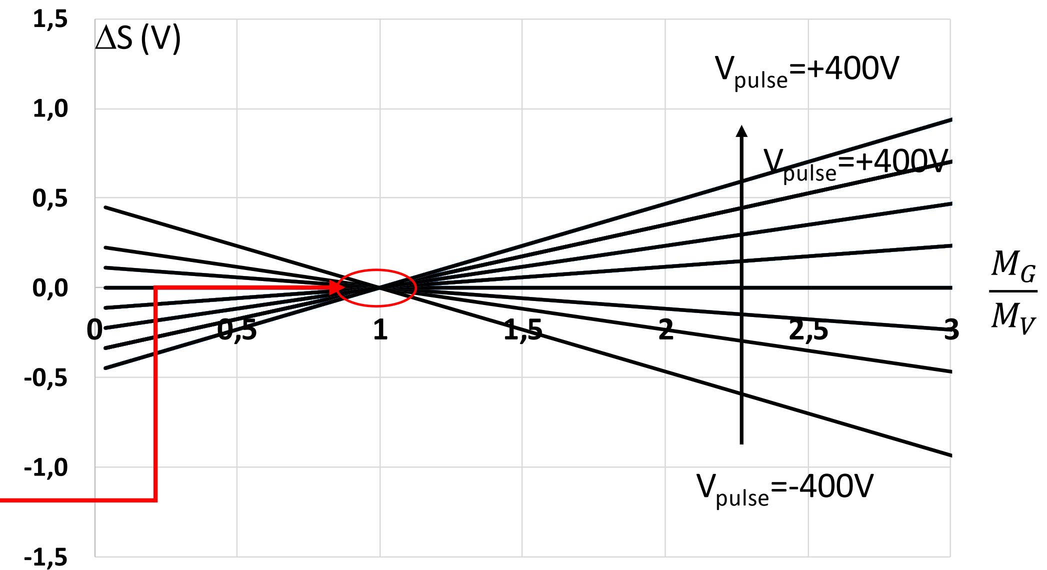




Propagation and attenuation of the swing drop / bounce toward or from the supply pads

EM Induction on the power & ground grids



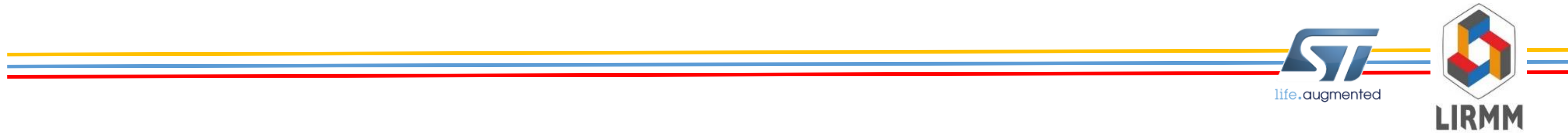


If $k_V = k_G$ EMFI has not effect on IC operation

But there is no reason to have symetric EM couplings and plenty to have asymetric ones:

- probe position
- probe geometry
- asymetric geometries of power and ground networks
- ...

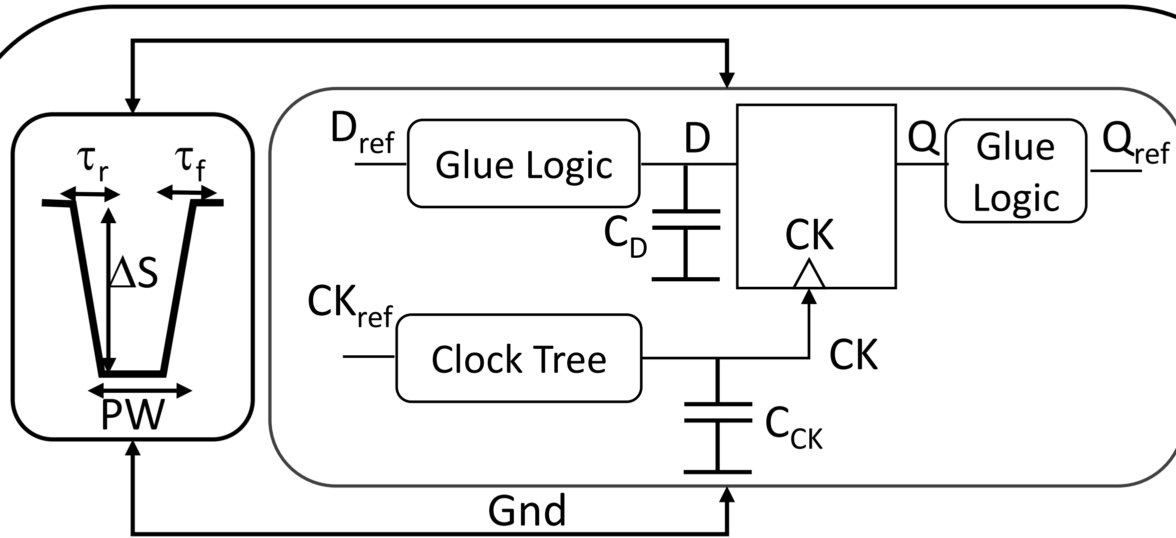
Impact of EMFI on IC operation



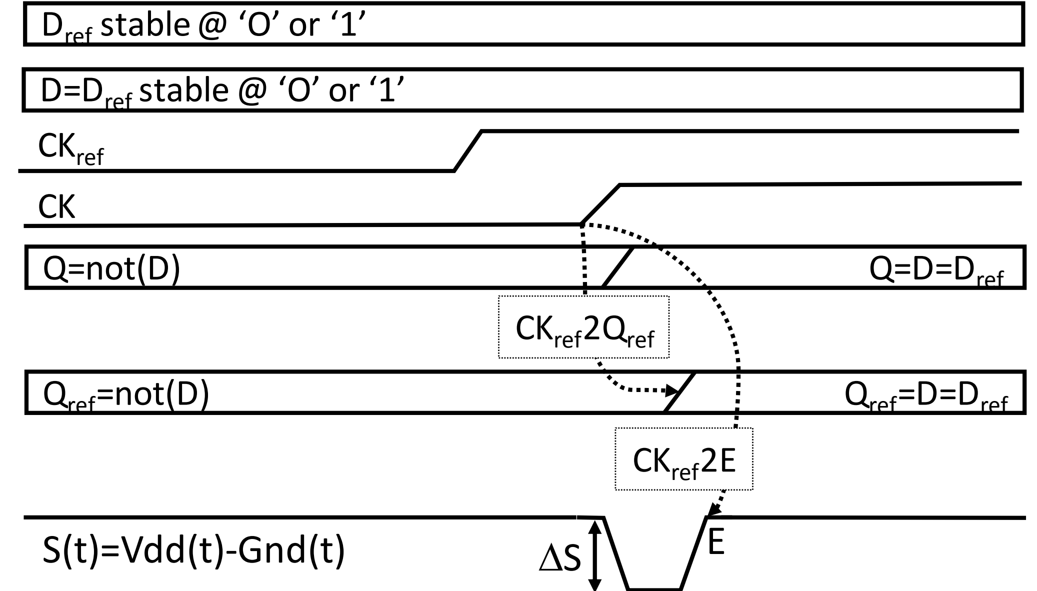
Modeling @ Logical level

Impact of EMFI on IC operation: simulation testbench

life.augmented LIRMM



- all elements experience the same perturbation
- D_{ref} stable (no timing fault possible)
- observation of 1 rising clock edge



$$F = \frac{CK2Q|nom}{CK2Q[inj}$$

- F>1 Speed up
- F=1 Normal operation
- 0<F<1 Slowing down : potential timing fault @ the next clock edge (depends on T_{CK})
- F=0 Sampling fault

Impact of EMFI on IC operation: Amplitude Variation

F

ΔS=0V

ΔS=1.2V

ΔS=1.5V

ΔS=1.6V

Δ S=1.8V

ΔS=2.2V

Sampling fault windows

Independent of clock frequency

1.0

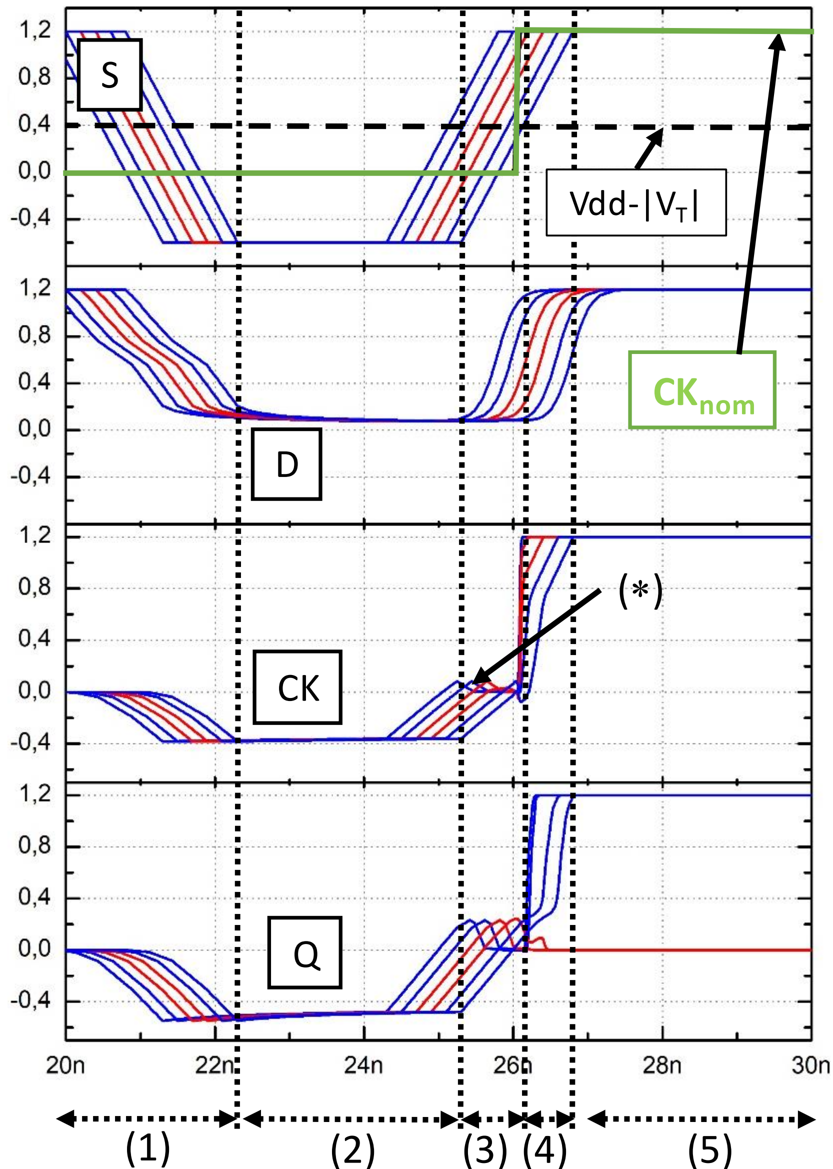
0.5

0.1

-1 0 1 2 3

$CK_{nom}2E$ (ns)

How EM faults occur ?



(1) First edge of V_{pulse} reverses the supply voltage

(2) 'IC is frozen' (part of it)

(3) Second edge of V_{pulse}
- Supply voltage recovery starts
- IC remains 'frozen' , $S<Vdd-|V_T|$
- Even the clock edge is 'frozen' and thus delayed

(4) Second edge of V_{pulse}
- IC wakes up , $S>Vdd-|V_T|$ and according to CK_{ref}2E a sampling fault occurs or not

(5) IC works again in nominal conditions

Importance of having 2 opposite EM pulses

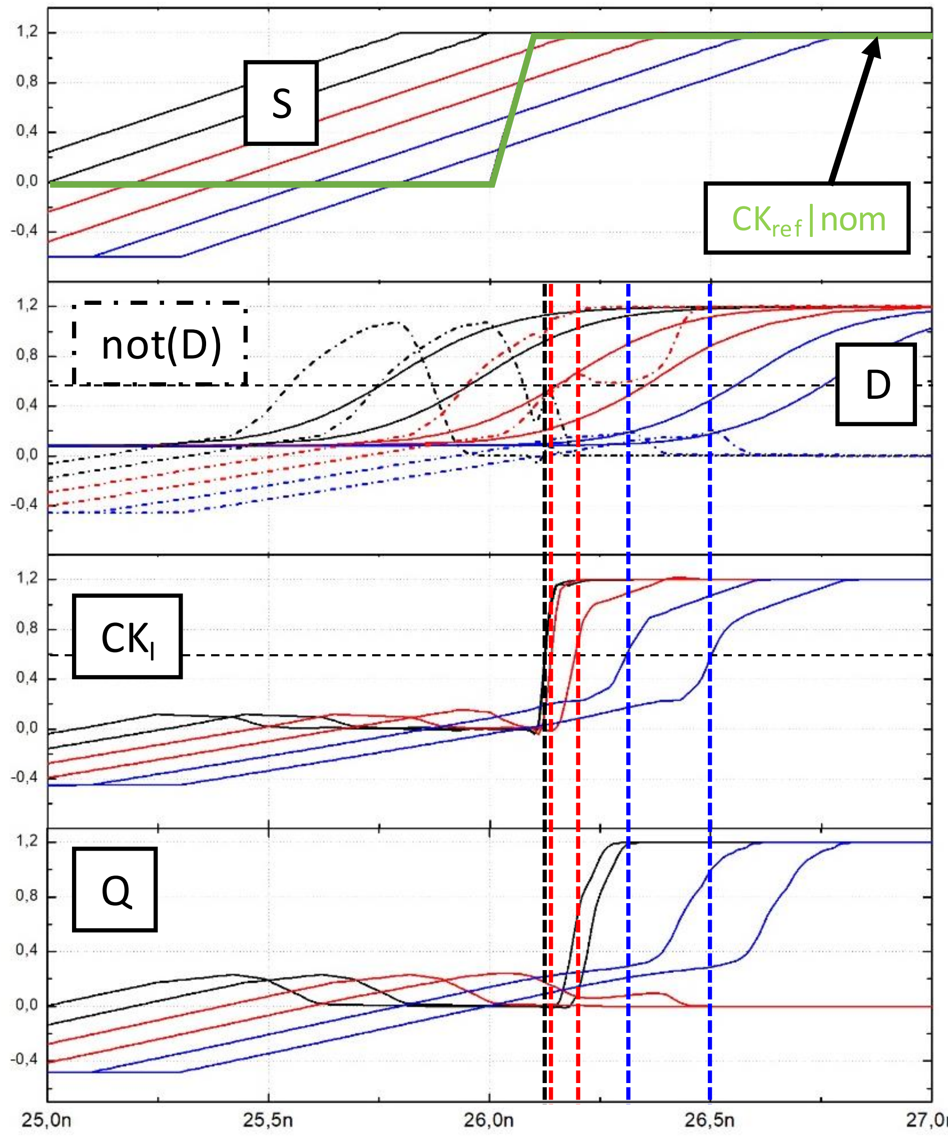
- 1st EM pulse reverses the supply voltage
- 2nd EM pulse controls the wake up phase

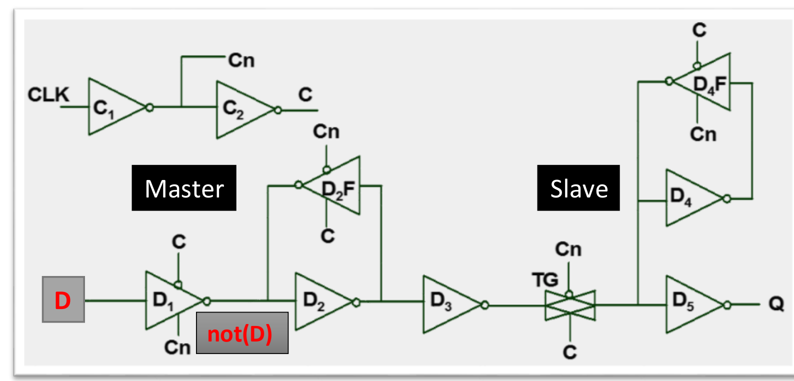
Importance of fine timing tuning EMFIs

- required time resolution ~100ps

life.augmented LIRMM

How EM faults occur ?





With respect to the normal arrival time of the rising clock edge

(1) Too early EMFIs
IC recovery was sufficiently long to not have a fault

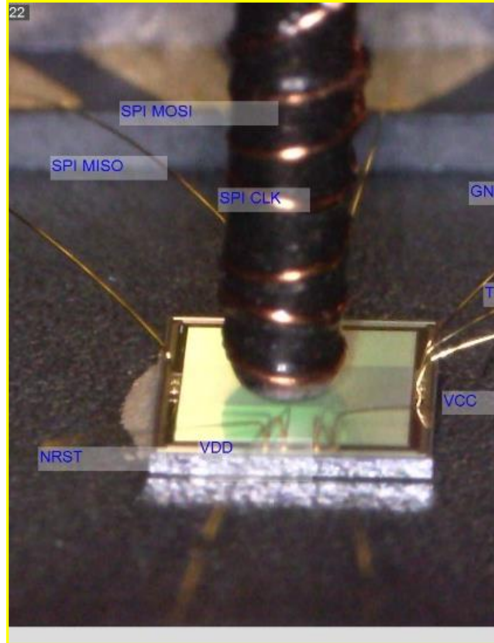
(2) Successfull EMFIs
D<0.5 Vdd
Not(D) >0.5Vdd (normal operation Not(D) = 0)

=> the DFF samples a wrong value

(3) Too late EMFIs
IC has not enough recovered
D<0.5 Vdd
Not(D) <<0.5 Vdd

=> the DFF abnormaly samples the right value

Experimental evidences



Testchip 40nm

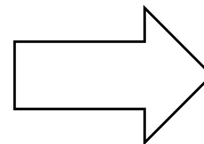
Hardware AES

Controllable clock

How demonstrate the soundness of the modelling ??

EMFI pollutes measurements at several meters from the DUT …

Look for indirect experimental evidences



Look for indirect evidences

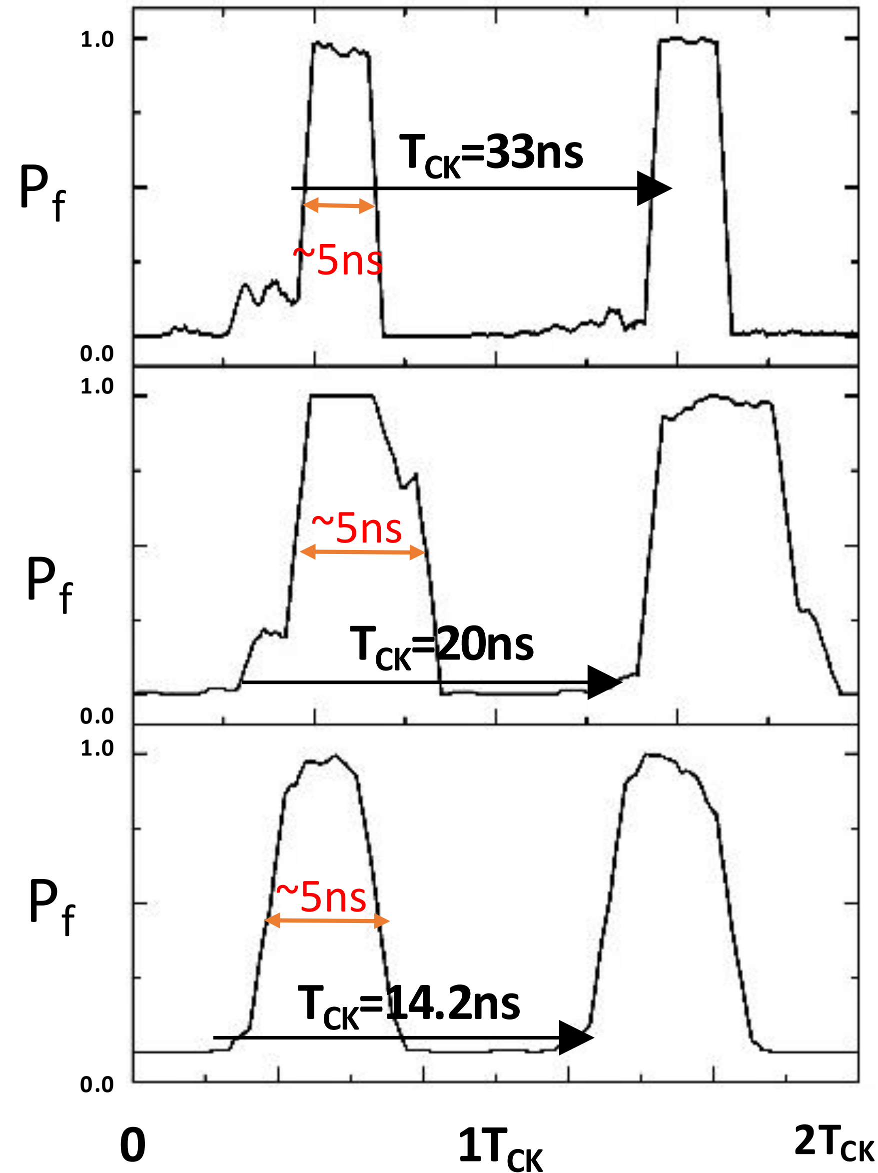
- Vary EMFI settings in simulation and experimentations

- Compare simulated and experimental trends

Experimental evidences

Simulations predict periodical sampling fault windows of constant width with period equal to T_{CK}

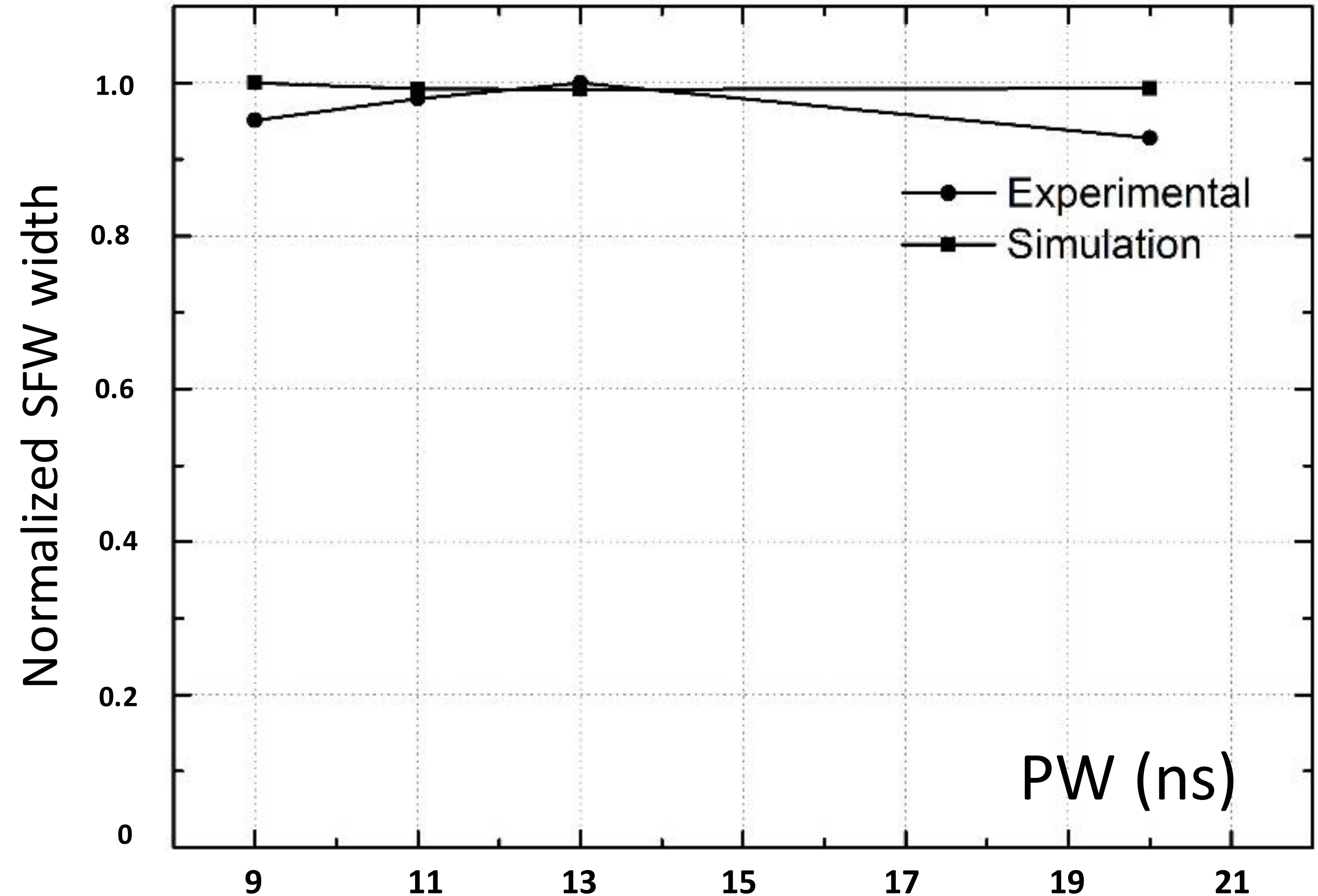
Experiments confirms this prediction despite the jitter (1.5ns) of the voltage pulse generator (SFW ~5 to 6ns)



Experimental evidences

Model predicts sampling fault width is independent of PW, the width of the pulse applied to the probe

Experiments confirms this prediction …



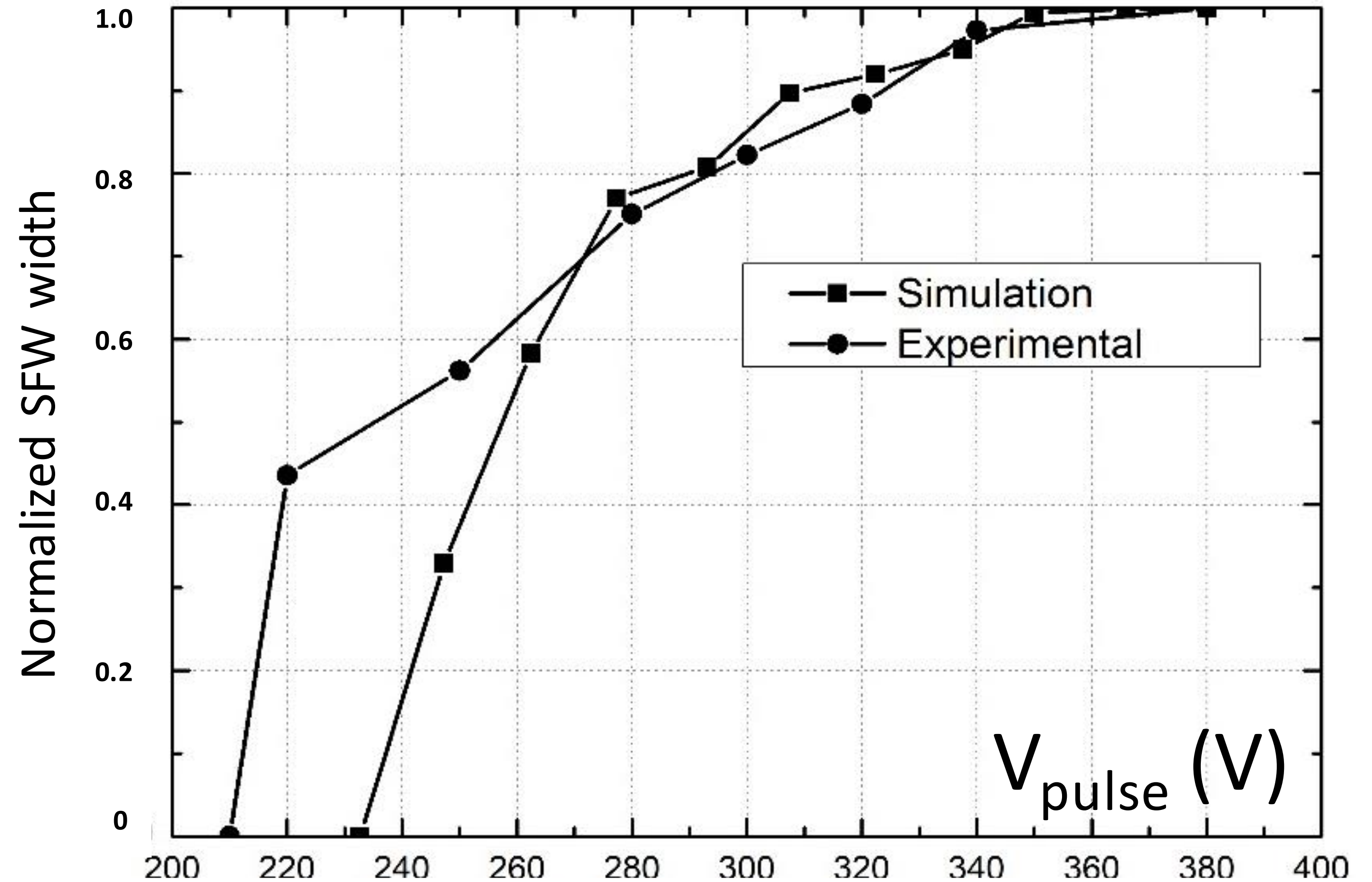
Experimental evidences

Simulations predict :

- a threshold on V_{pulse} to induce fault

- an increase of the width sampling fault windows with V_{pulse}

Experiments confirms this prediction …



Conclusions

life.augmented LIRMM

- **explanation on how EM faults occur (@least on µC)**
  - **EMFI locally freezes and wakes up the supply voltage**
  - **Induction of sampling faults**
  - **Sampling faults occur during the supply voltage recovery**

- **Guidelines for the design of more robust ICs**

- **Perspectives :**
  - **enhanced EMFI platforms to target SoC**
  - **modeling EM faults in SoC context with current EMFI platforms**