Reliability analysis of digital sensors against perturbations of FPGAs

Sylvain Guilley[1,2], **Richard Newell**[3] and **Thibault Porteboeuf**[2]

[1] TELECOM-ParisTech
[2] Secure-IC S.A.S.
[3] Microsemi Corp.

1. Introduction

2. Detecting fault attacks

3. Digital sensor®

4. Technological dispersion

5. Design and tolerances

Two constraints to be met simultaneously...

Security / Reliability

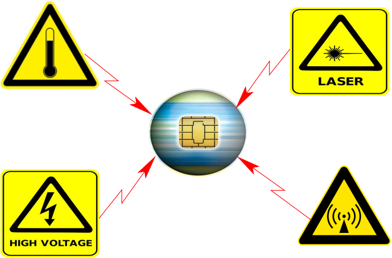
- **Security**: detecting as many faults as possible
- **Reliability**: detecting only necessary faults

Fault attacks

Many means:

- Clock
- Voltage
- Temperature

Dedicated sensors?



State-of-the-art industrial solutions

Dedicated sensors

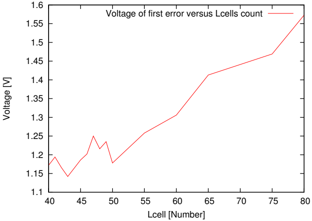
- Frequency monitors
- Voltage monitors
- Temperature monitors

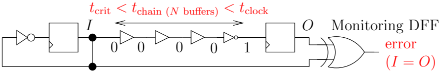
Problem

- Analog, hence costly to tune
- Many alarms arrive in parallel: management is complex

Digital sensor®

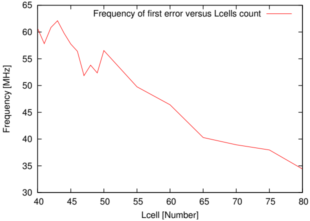
Sensor performance:

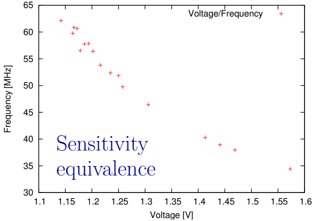



$t_{\text{crit}} < t_{\text{chain }(N\text{ buffers})} < t_{\text{clock}}$

Digital, hence portable & low-cost:

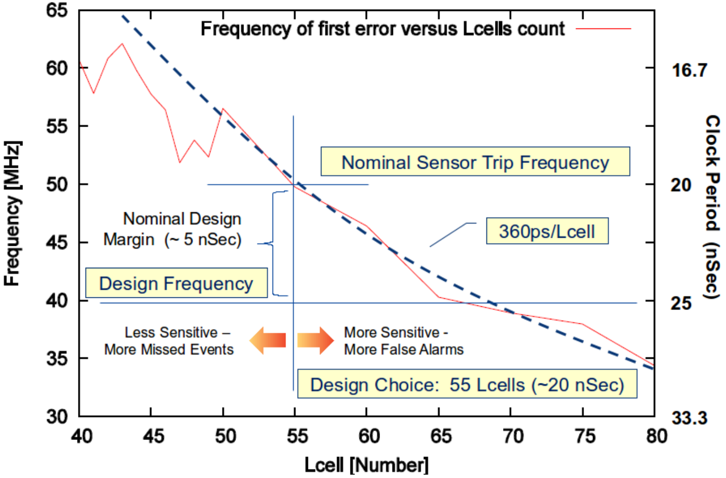
- can be spread over the circuit
- difficult to spot by an attacker
- responds to any kind of stress (clock / power glitches, heating, overclocking, laser spots)
- suitable for both ASIC or FPGA implementations



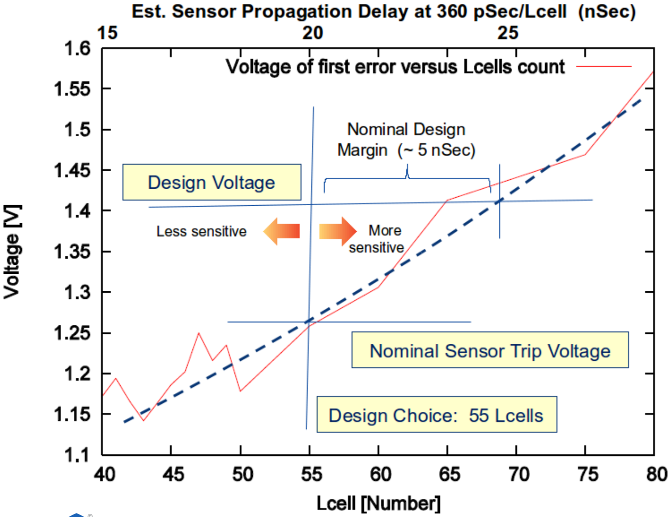


Sensitivity equivalence

Design Example: Frequency Sensitivity

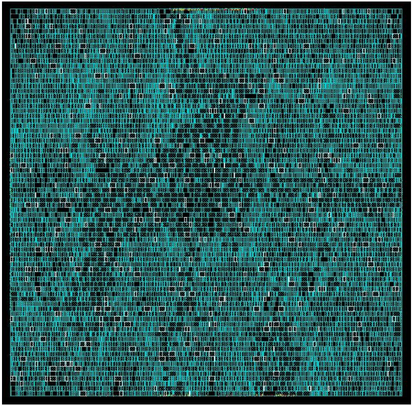


Design Example: Voltage Sensitivity



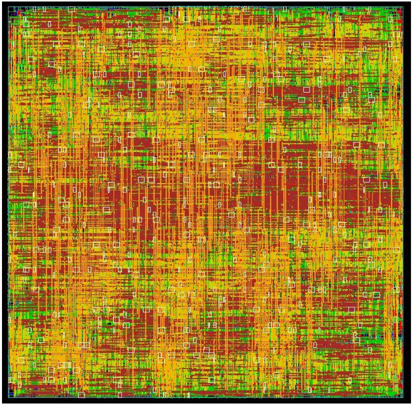
Main technical characteristics

- Simple API
- Stable
- Small
- Descreet, more difficult to recognize
- Melted with the rest of the SoC, more difficult to bypass
- Low power
- Clock gating possible
- Even more obscured in FPGA implementations



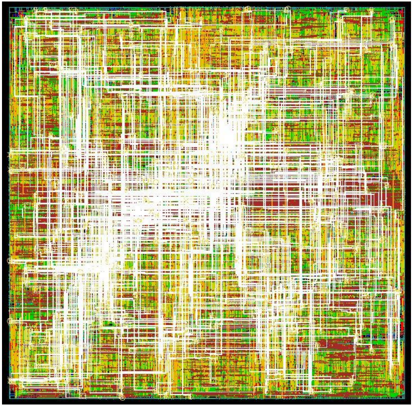
Main technical characteristics

- Simple API
- Stable
- Small
- Descreet, more difficult to recognize
- Melted with the rest of the SoC, more difficult to bypass
- Low power
- Clock gating possible
- Even more obscured in FPGA implementations

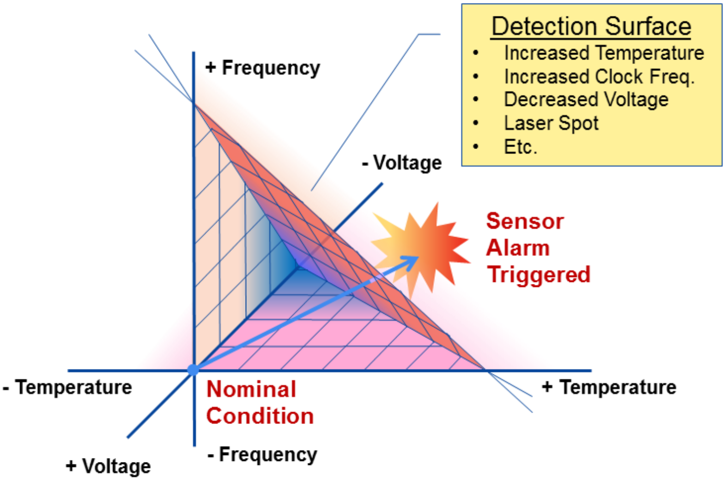


Main technical characteristics

- Simple API
- Stable
- Small
- Descreet, more difficult to recognize
- Melted with the rest of the SoC, more difficult to bypass
- Low power
- Clock gating possible
- Even more obscured in FPGA implementations



Advantage

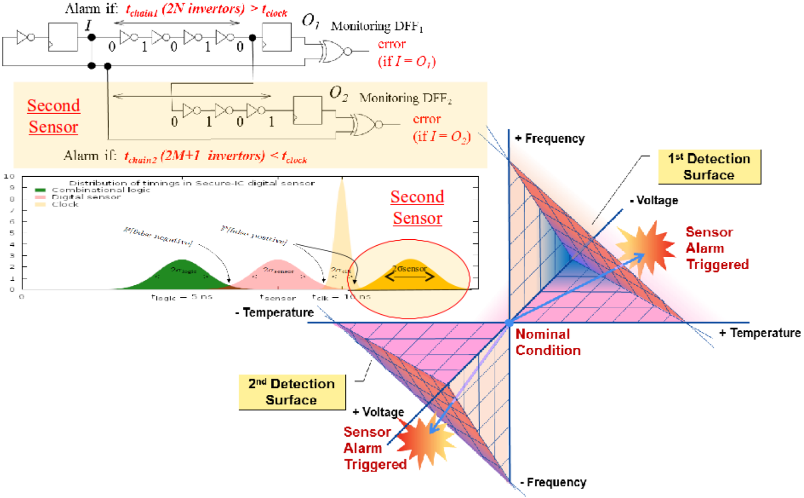


Detection Surface

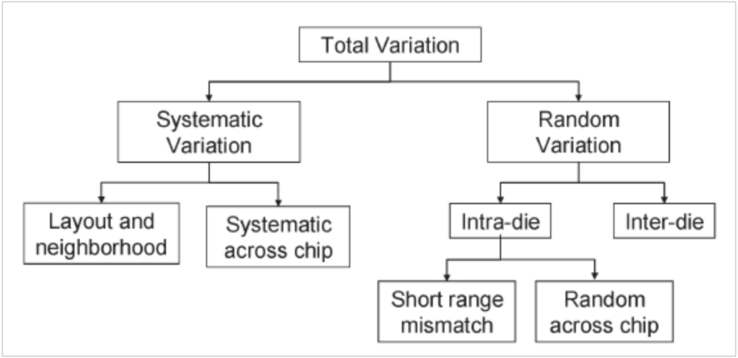
- Increased Temperature
- Increased Clock Freq.
- Decreased Voltage
- Laser Spot
- Etc.

See also: [SBG+09, BSGD09, SBGD11].

Add 2nd Sensor – Test Opposite Conditions



Sorts of variations



Total Variation

Systematic Variation

Random Variation

Layout and neighborhood

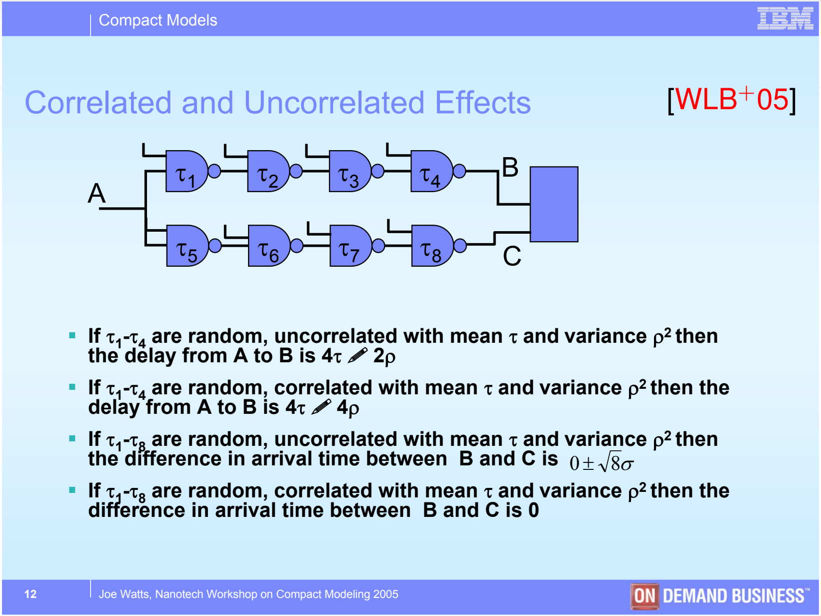
Systematic across chip

Intra-die

Inter-die

Short range mismatch

Random across chip



Compact Models

Correlated and Uncorrelated Effects

[WLB$^+$05]

A
τ_1
τ_2
τ_3
τ_4
B
τ_5
τ_6
τ_7
τ_8
C

- **If τ_1-τ_4 are random, uncorrelated with mean τ and variance ρ^2 then the delay from A to B is 4τ ✎ 2ρ**
- **If τ_1-τ_4 are random, correlated with mean τ and variance ρ^2 then the delay from A to B is 4τ ✎ 4ρ**
- **If τ_1-τ_8 are random, uncorrelated with mean τ and variance ρ^2 then the difference in arrival time between B and C is** $0 \pm \sqrt{8}\sigma$
- **If τ_1-τ_8 are random, correlated with mean τ and variance ρ^2 then the difference in arrival time between B and C is 0**

12 Joe Watts, Nanotech Workshop on Compact Modeling 2005

ON DEMAND BUSINESS™

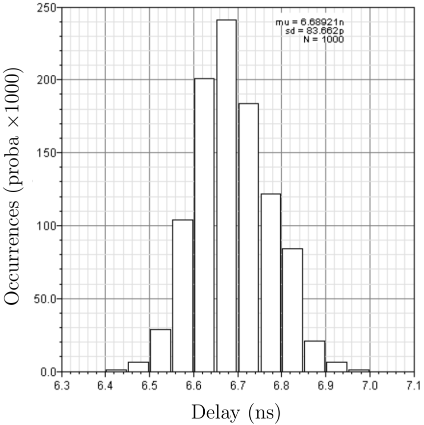
Best / worst cases

Worst case

- Correlated in the digital sensor
- Non-correlated between the digital sensor & critical path

In the sequel, we model only uncorrelated noise (*in transistors*).

In 65 nm technology



- Monte-Carlo simulation, under Cadence
- 37 identical buffers, $\times 4$ drive
- 1000 runs

Orders of magnitude

1× buffer

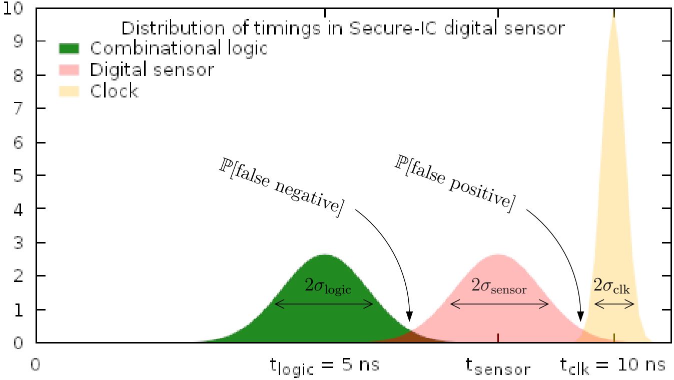
- 90 ps delay
- 6.0 ps variation

10× buffer

- 90 ps delay
- 2.3 ps variation

Typical chain: 40 gates, $\approx$ 4 ns delay, but only 14 ps standard deviation!

Indeed, uncorrelated variances add, thus the standard deviation only grow with the square root of the number of delay elements.



Probability density functions in the digital sensor setup.

Computations

Definitions

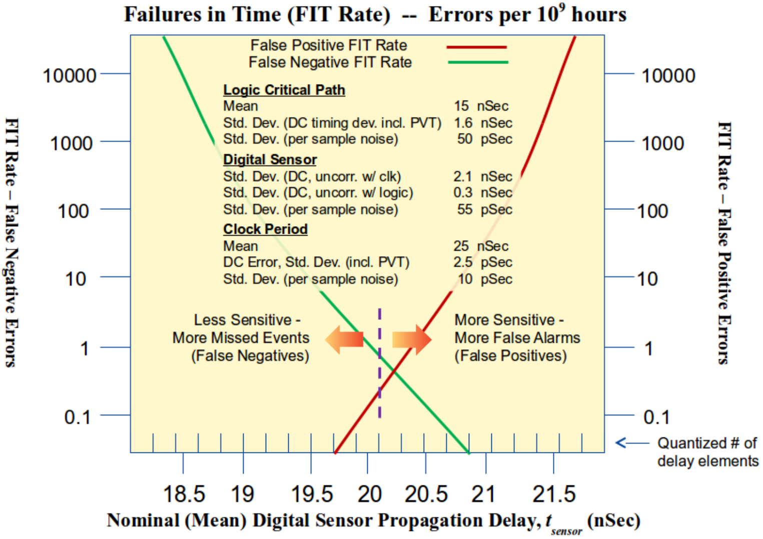
- **False positives**: a fault is reported but there was none.
- **False negatives**: a fault has not been detected.

Equations (*example for the probability of false positives*)

$$\begin{aligned}\mathbb{P}_{\mathrm{FP}} &= \mathbb{P}(T_{\mathrm{sensor}} > T_{\mathrm{clock}}) = \mathbb{E}(\mathbb{1}_{T_{\mathrm{sensor}} > T_{\mathrm{clock}}}) \\ &= \iint \phi_{t_{\mathrm{sensor}},\sigma^2_{\mathrm{sensor}}}(t) \cdot \phi_{t_{\mathrm{clock}},\sigma^2_{\mathrm{clock}}}(t') \cdot \mathbb{1}_{t>t'} \, \mathrm{d}t \, \mathrm{d}t' \\ &= \int_{-\infty}^{+\infty} \int_{-\infty}^{t} \phi_{t_{\mathrm{sensor}},\sigma^2_{\mathrm{sensor}}}(t) \cdot \phi_{t_{\mathrm{clock}},\sigma^2_{\mathrm{clock}}}(t') \, \mathrm{d}t \, \mathrm{d}t' \quad ,\end{aligned}$$

where $\phi_{\mu,\sigma^2}(t) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp -\frac{(t-\mu)^2}{2\sigma^2}$ is the probability density function of the a normal law $\mathcal{N}(\mu, \sigma^2)$.

Illustrative “Receiver Operating Characteristic” (ROC)



Logic Critical Path

Mean	15 nSec
Std. Dev. (DC timing dev. incl. PVT)	1.6 nSec
Std. Dev. (per sample noise)	50 pSec

Digital Sensor

Std. Dev. (DC, uncorr. w/ clk)	2.1 nSec
Std. Dev. (DC, uncorr. w/ logic)	0.3 nSec
Std. Dev. (per sample noise)	55 pSec

Clock Period

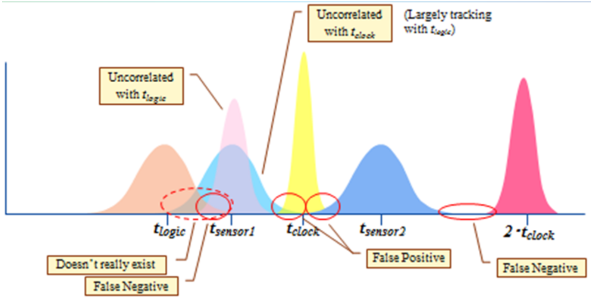
Mean	25 nSec
DC Error, Std. Dev. (incl. PVT)	2.5 pSec
Std. Dev. (per sample noise)	10 pSec

Less Sensitive -
More Missed Events
(False Negatives)

More Sensitive -
More False Alarms
(False Positives)

Advanced considerations: Improvements

- **Exposure probability**: tampering happens only maybe between zero and some few hours over the life of the part ($<$ 100 ppm)
- In case of environmental modifications, **user logic and sensor track one another**, hence they can never cross each other. But this is ideal: do delays remain proportionate under these circumstances?



Bibliographical References

[BSGD09] Shivam Bhasin, Nidhal Selmane, Sylvain Guilley, and Jean-Luc Danger.
Security Evaluation of Different AES Implementations Against Practical Setup Time Violation Attacks in FPGAs.
In *HOST (Hardware Oriented Security and Trust)*, pages 15–21. IEEE Computer Society, July 27th 2009.
DOI: 10.1109/HST.2009.5225057; In conjunction with DAC-2009, Moscone Center, San Francisco, CA, USA.

[SBG+09] Nidhal Selmane, Shivam Bhasin, Sylvain Guilley, Tarik Graba, and Jean-Luc Danger.
WDDL is Protected Against Setup Time Violation Attacks.
In *FDTC*, pages 73–83. IEEE Computer Society, September 6th 2009.
In conjunction with CHES'09, Lausanne, Switzerland. DOI: 10.1109/FDTC.2009.40; Online version: `http://hal.archives-ouvertes.fr/hal-00410135/en/`.

[SBGD11] Nidhal Selmane, Shivam Bhasin, Sylvain Guilley, and Jean-Luc Danger.
Security evaluation of application-specific integrated circuits and field programmable gate arrays against setup time violation attacks.
IET Information Security, 5(4):181–190, December 2011.
DOI: 10.1049/iet-ifs.2010.0238.

[WLB+05] Josef Watts, Ning Lu, Calvin Bittner, Steven Grundon, and Jeffrey Oppold.
Modeling FET Variation within a chip as a Function of Circuit Design and Layout Choices.
In *WCM (Workshop on Compact Modeling)*, May 8-12 2005.
Anaheim Marriott & Convention Center, Anaheim, CA, USA;
`http://www.nsti.org/Nanotech2005/WCM2005/` (in Association with Eighth International Conference on Modeling and Simulation of Microsystems MSM 2005).

Reliability analysis of digital sensors against perturbations of FPGAs

Sylvain Guilley[1,2], **Richard Newell**[3] and
Thibault Porteboeuf[2]

[1] TELECOM-ParisTech
[2] Secure-IC S.A.S.
[3] Microsemi Corp.