An EM Fault Injection Susceptibility Criterion and its application to the localisation of hotstpots

M. MADAU, M. AGOYAN, P. MAURINE

Laboratoire d'Informatique de Robotique et de Microélectronique de Montpellier (LIRMM), STMicroelectronics

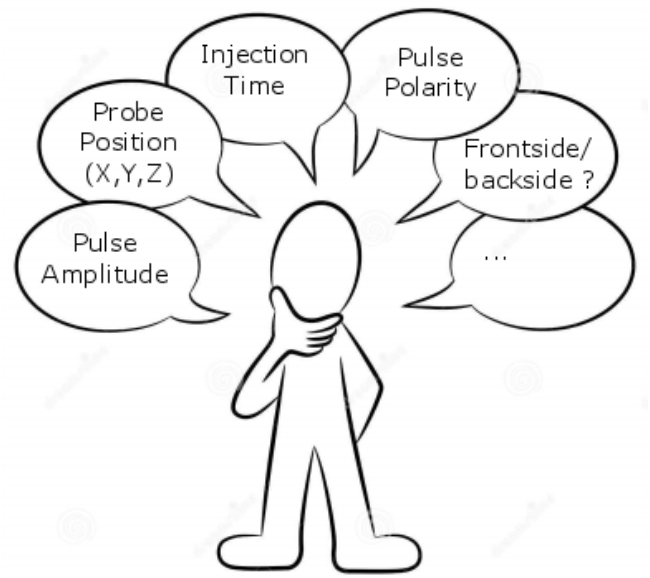
2017

Linking injection/observation channel

"Attack"	Channel	information from observation channel.
Power Glitch	V_{dd} network	temporal information.
Body Bias Injection	bulk	none.
EMFI	EM	temporal and spatial information
Laser	photon	spatial information. Light observation is expensive.

Why binding EM analysis to injection ?

EMFI combinatory complexity:



Time efficiency[a]:

Analysis map → one day for three executables.

Injection map (fixed parameters) → three days for one executable.

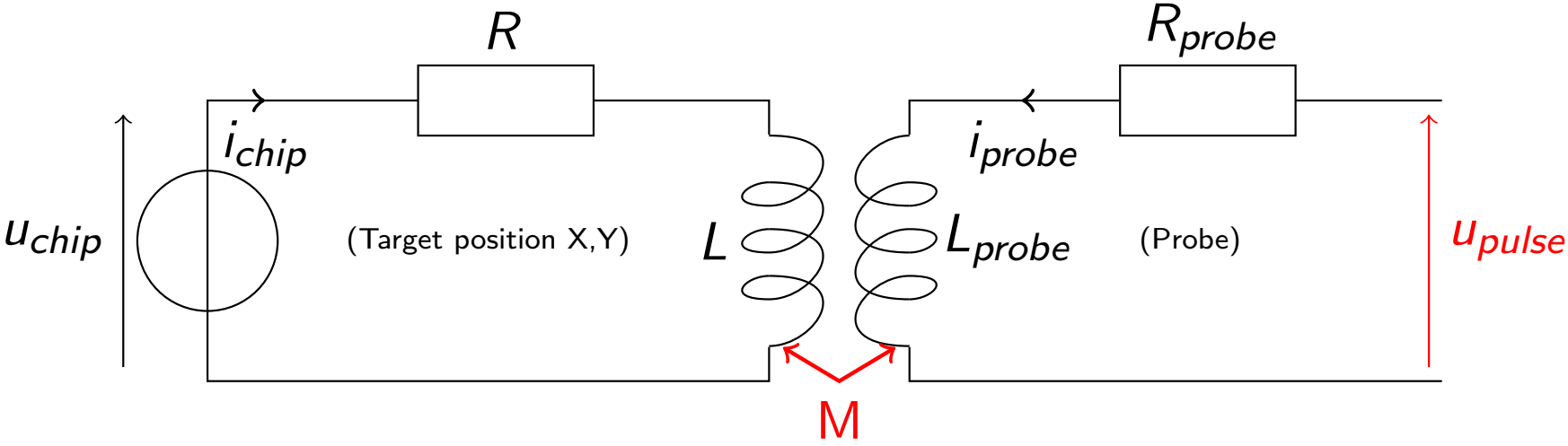
[a] timing are relative to our setup

Aim:

Ease and fasten EMFI security characterisation → (X,Y) position.

Table of Contents

EM coupling



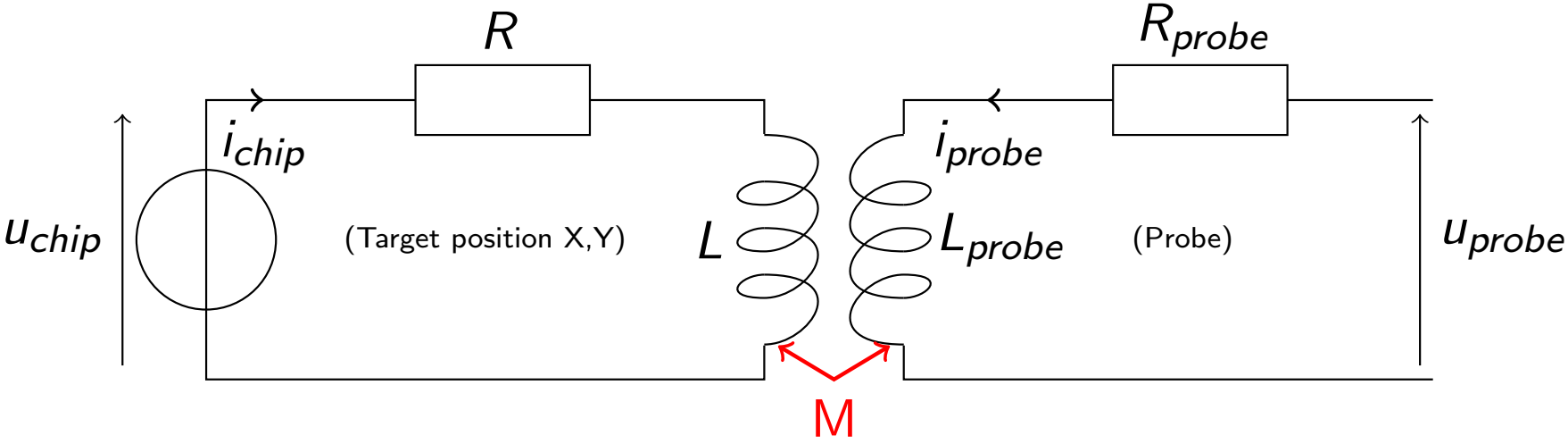
Coupling: *(injection case)*

$$u_{chip} = Ri_{chip} + L\frac{\mathrm{d}i_{chip}}{\mathrm{d}t} + M\frac{\mathrm{d}i_{probe}}{\mathrm{d}t}$$

LIRMM

life.augmented

EM coupling



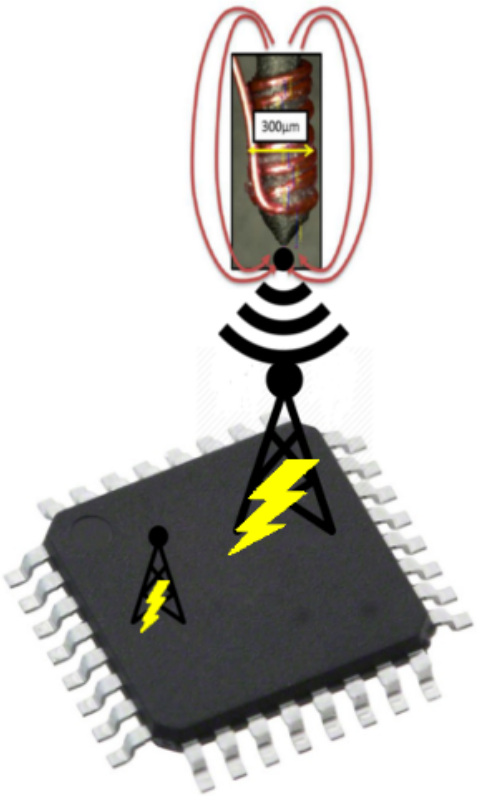
Coupling: *(analysis case)*

$$u_{probe} = Ri_{probe} + L_{probe}\frac{\mathrm{d}i_{probe}}{\mathrm{d}t} + M\frac{\mathrm{d}i_{chip}}{\mathrm{d}t}$$

LIRMM

life.augmented

Antenna reciprocity



Antenna reciprocity:

The efficiency of a receiving antenna is as important as its transmitting efficiency.

Conclusion 1:
Finding high emission antenna

$\rightarrow$ best coupling positions on circuits.

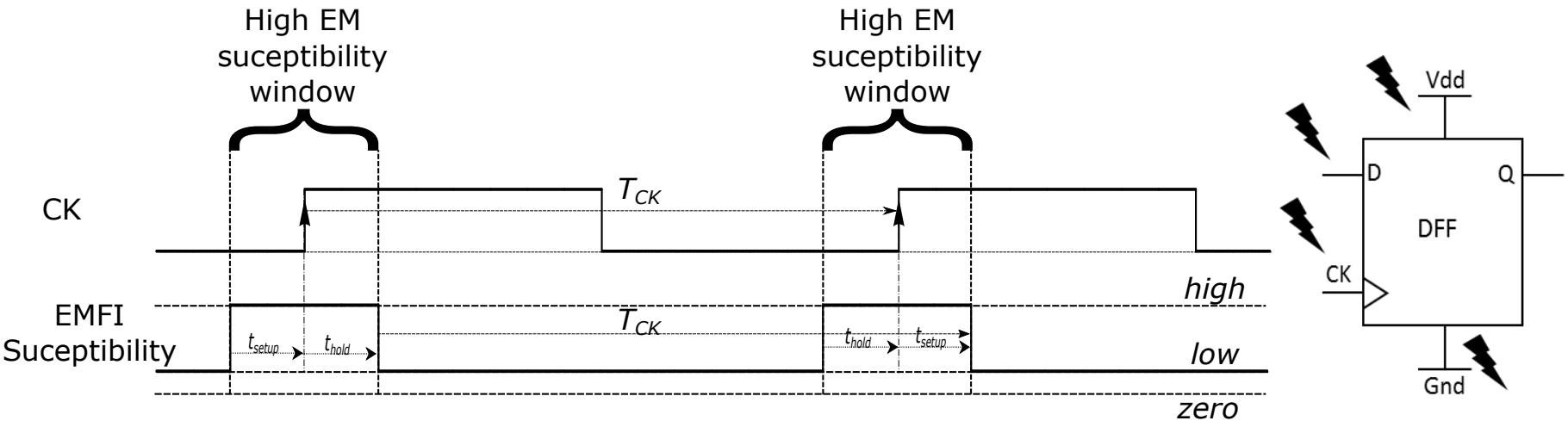
Conclusion 2:
High emission antenna $\neq$ best entry point

$\rightarrow$ not necessarily linked to data.

LIRMM

life.augmented

Sampling fault model[1]



System target:

↪DFF are more likely to be faulted by EM injection.

↪Target event occurring at f_{CK}

[1] *EM injection: fault model and locality* S. Ordas, L.Guillaume-Sage, P. Maurinne FDTC 2015.

EMFI Criterion definition

Area to target are positions:

- *(guideline 1)* emitting the strongest signal (in terms of power) associated to the clock signal or clock tree.

  $\rightarrow$ tool: Power Spectral Density $PSD(f_{CK})$

- *(guideline 2)* emitting signal tightly bind to both targeted algorithm and clock frequency (f_{CK}).

  $\rightarrow$ tool: **inc***oherence*(f_{CK})

Guideline 2 tools:

$$inc_{s_1,s_2}(f) = 1 - \frac{psd_{s_1,s_2}(f)^2}{psd_{s_1,s_1}(f) \cdot psd_{s_2,s_2}(f)}$$

Notation:

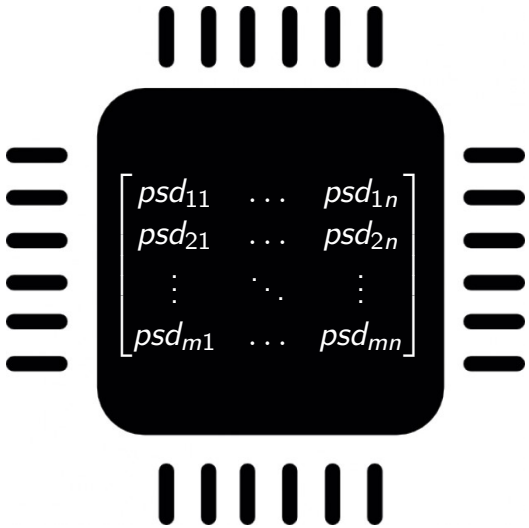
s_1 = EM emission for input 1.

s_2 = EM emission for input 2.

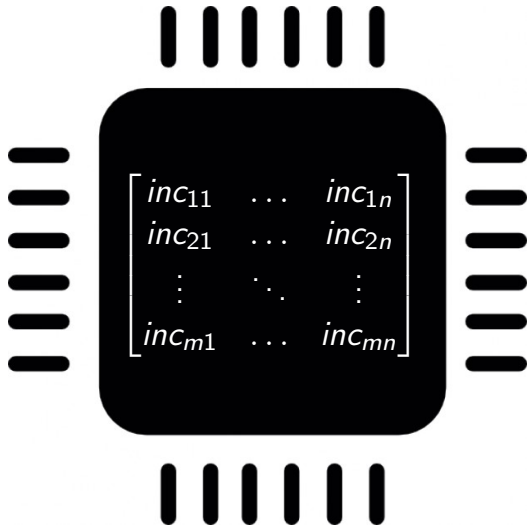
Aim

$\hookrightarrow$ Look for differences in spectrum occurring at f_{CK} *ie* DFF used by algorithm.

How to combine and weight those two measures ?

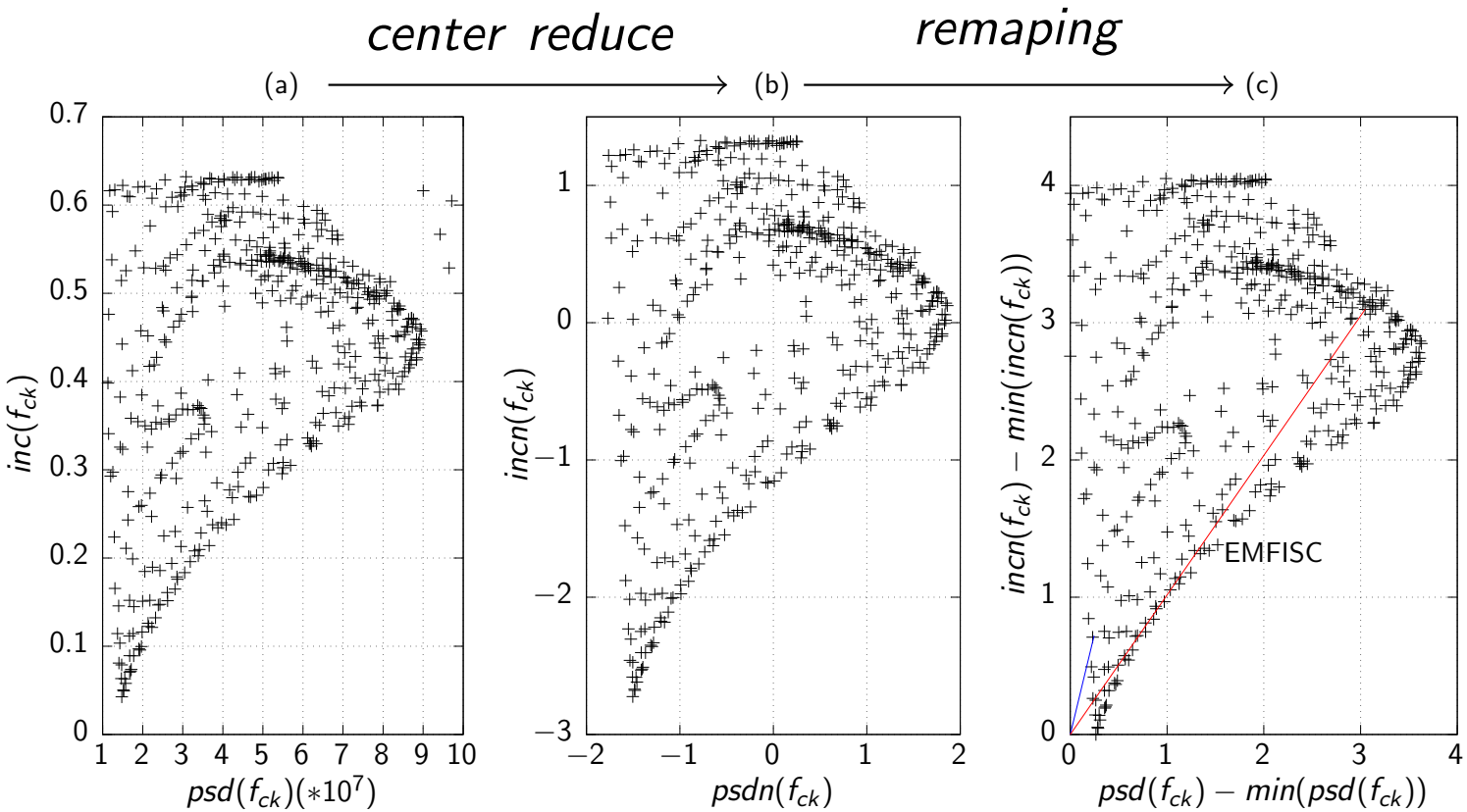


$0 \leq psd \leq ?$



$0 \leq inc \leq 1$

Raw data: PSD, Incoherence view



$$inc_{s_1,s_2}(f) = 1 - \frac{psd_{s_1,s_2}(f)^2}{psd_{s_1,s_1}(f) \cdot psd_{s_2,s_2}(f)}$$

EMFISC Procedure

Algorithm 1 EMFISC

Input: f_{CK}, matrix of s_1 and s_2,
α (% chip to keep),
a (weight *psd* compared to *incoherence*)
Output: $emfisc_{x,y}$

1: **for** X,Y positions **do**
2: compute $psd_{s_1}(f)$
3: compute $inc_{s_1,s_2}(f)$
4: **end for**
5: $psdn_{x,y}$ and $incn_{x,y}$ = center reduce $psd_{x,y}$ and $inc_{x,y}$ population
6: remap $psdn_{x,y}$ and $incn_{x,y}$ population
7: compute $emfisc_{x,y} = \sqrt{(1-a) * psdn_{x,y}^2 + a * incn_{x,y}^2}$
8: quantile($emfisc_{x,y}$,α)

Table of Contents

Experimental protocol

Target algorithm:

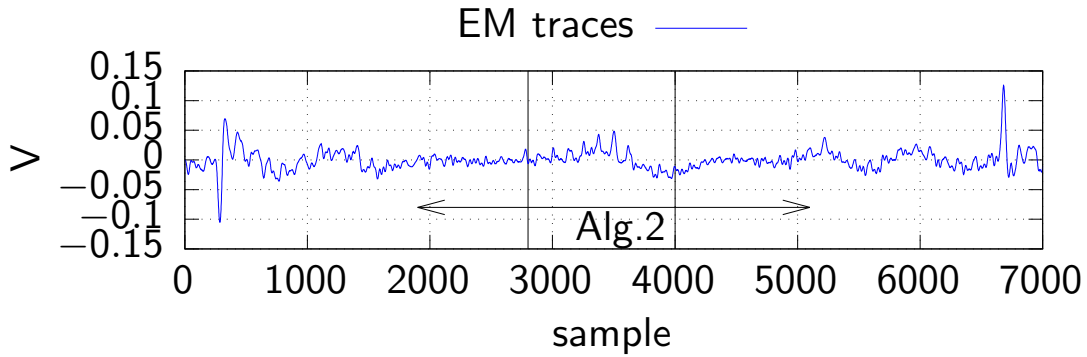
Algorithm 2 Pattern (AddrSRAM32, AddrSRAM96)

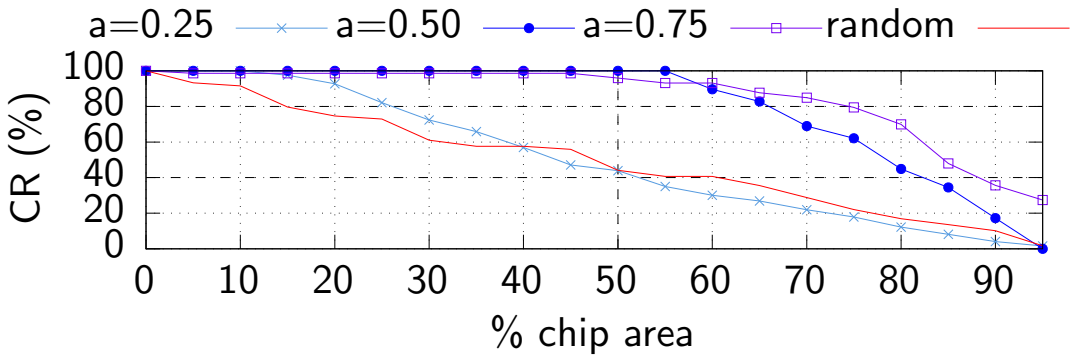
```
1: PUSH { lr }
2: ADD R0,R0,#0; 11 times
3: LDR R2,[R0]; read SRAM32
4: STR R2,[R1]; write SRAM96
5: LDR R3,[R1]; read back
6: ADD R0,R0,#0; 11 times
7: POP { pc }
```

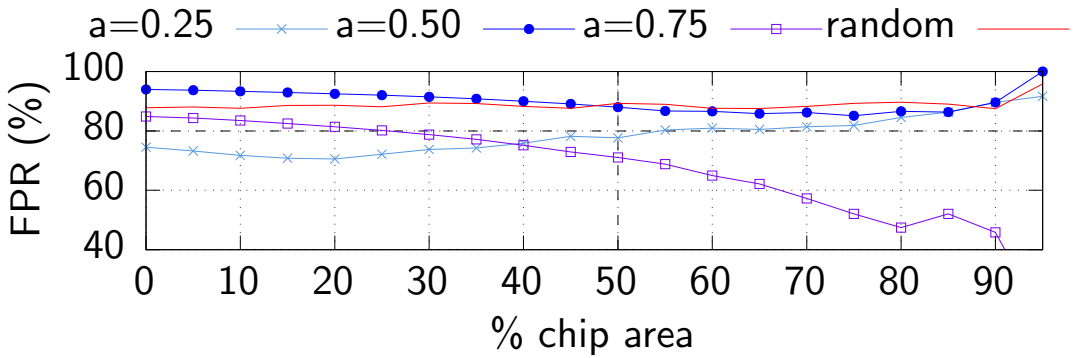
LIRMM

life.augmented

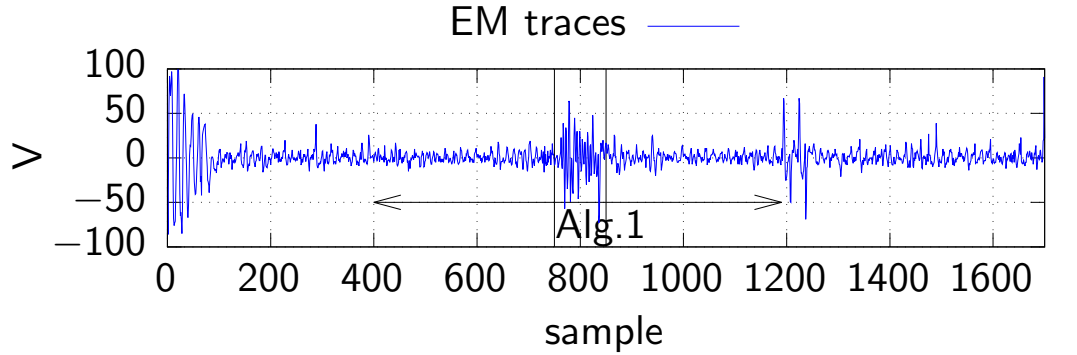
EMFISC figures of merit (target 1 130V)

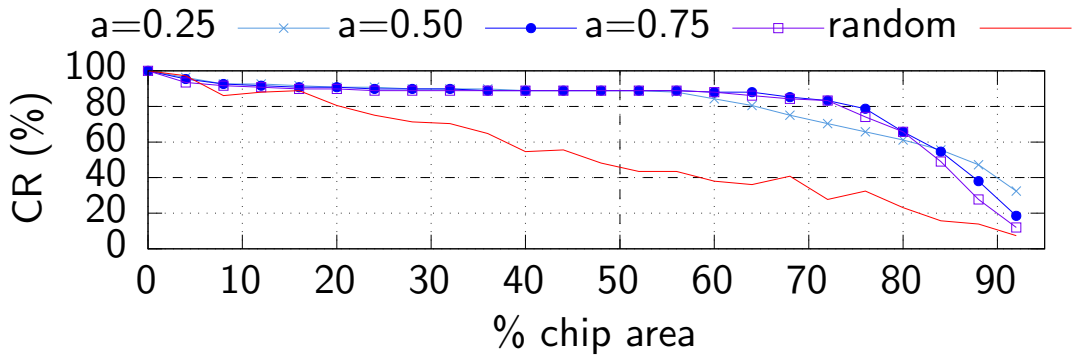


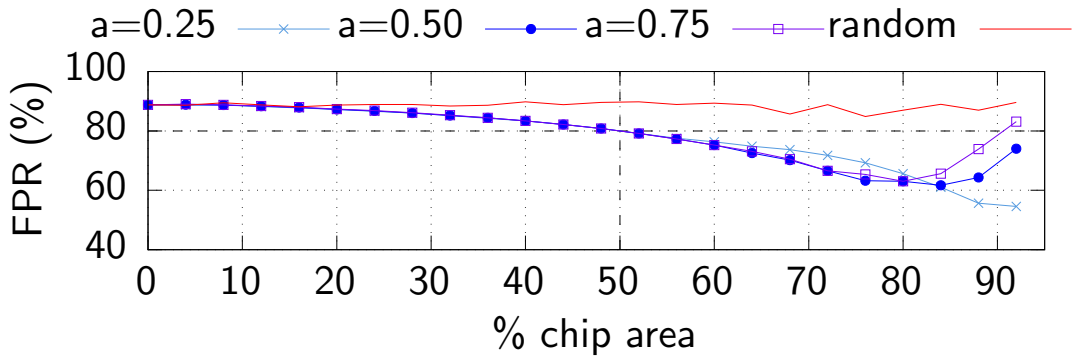




EMFISC figures of merit (target 2 198V)



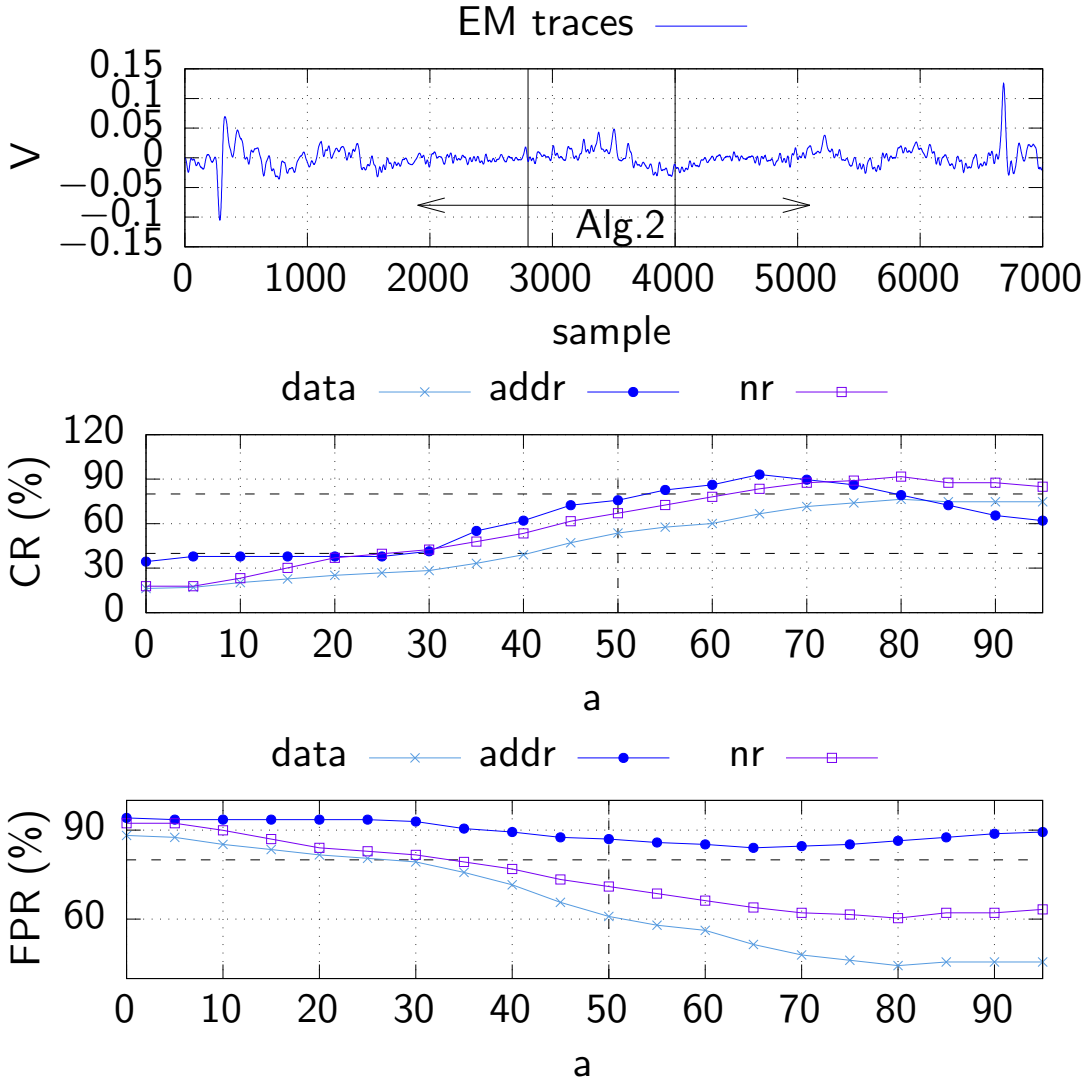




LIRMM

life.augmented

Quantile fixed at 60% target 1



LIRMM

life.augmented

Results:

- There is a link between EM emissions and EMFI.
- This link can be use to ease EMFI characterisation.

Refining the criterion:

- Other combination of PSD and Incoherence curves.
- Finding a way to weight PSD and Incoherence.
- Adding a criterion more target specific, such as a better measurement of M parameter.

Thanks
Any questions ?