Saut d'instructions consécutives induit par impulsion EM sur microcontrôleur 8 bits

Journée thématique injection de faute, Jussieu

[1]A. Menu, [2]J-L. Danger, [1]J-M. Dutertre,
[1]E. Kharbouche, [1]O. Potin, [1]J-B. Rigaud

29 Mai 2018

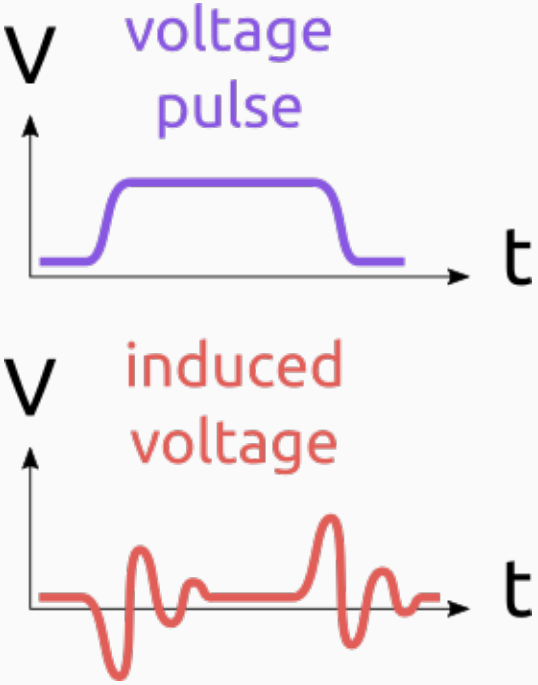
[1]Ecole des Mines de Saint-Etienne, {prenom}.{nom}@emse.fr
[2]Telecom Paristech, {prenom}.{nom}@telecom-paristech.fr

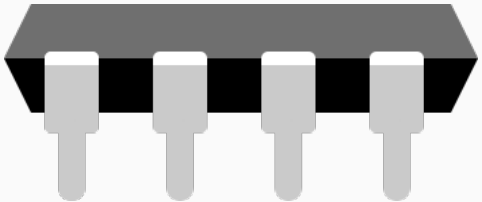
Sommaire

Contexte

Injection de faute EM

Principe physique : la loi de Lenz-Faraday





Injection de faute EM

Avantages de la méthode

- **non-invasive** [Schmidt'07]
- **locale** [Poucheret'11, Chusseau'14]
- **précise et reproductible** [Dehbaoui'12]

Injection de faute EM

Avantages de la méthode

- **non-invasive** [Schmidt'07]
- **locale** [Poucheret'11, Chusseau'14]
- **précise et reproductible** [Dehbaoui'12]

Compromis précision / investissement financier et humain

Injection de faute EM

Quels modèles de faute observés ?

- Interraction entre flot de données et flot de contrôle [Dehbaoui'12, Moro'13]
- Comment caractériser une faute ?

	flot de contrôle				flot de données	
	Rejeu	Saut d'instr.	Corruption Opcode	Corruption PC	Faute mono-octet	Faute mono-bit
Schmidt'07		?	?	?		
Dehbaoui'12		✓	?	?	✓	
Moro'13		✓	✓	✓	✓	
Rivière'15	✓					

Revue non-exhaustive des modèles de faute observés en injection de faute par impulsion EM

Injection de faute EM

Direction adoptée : privilégier le **saut d'instruction**

- construction de modèles de faute variés
- facilité de mise en oeuvre

Injection de faute EM

Saut d'instruction **unique** par injection de faute sur cible 8 bits et 32 bits

Un modèle de faute réaliste

- glitch de tension [Schmidt'08]
- sous-alimentation [Barenghi'09]
- glitch d'horloge [Balasch'11]
- injection laser [Breier'15]

Injection de faute EM

Saut d'instruction **unique** par injection de faute sur cible 8 bits et 32 bits

Un modèle de faute réaliste

- glitch de tension [Schmidt'08]
- sous-alimentation [Barenghi'09]
- glitch d'horloge [Balasch'11]
- injection laser [Breier'15]

Pris en compte dans l'analyse de vulnérabilités et le design de contre-mesures

- simulateur de faute embarqué (EFS) [Berthier'14]
- remplacement par instruction idempotente et duplication [Moro'14, Barry'16]

Injection de faute EM

Saut de **plusieurs** instructions consécutives ?

Injection de faute EM

Saut de **plusieurs** instructions consécutives ?

- rejeu d'instruction [Rivière'15]
- glitch d'horloge sur architecture pipelinée [Yuce'16]

Injection de faute EM

Saut de **plusieurs** instructions consécutives ?

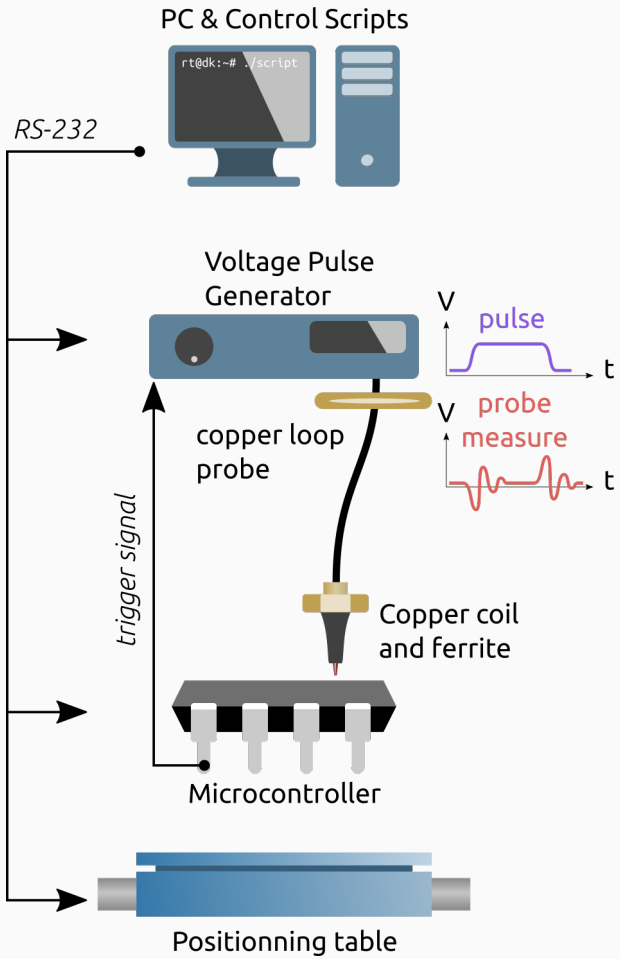
- rejeu d'instruction [Rivière'15]
- glitch d'horloge sur architecture pipelinée [Yuce'16]

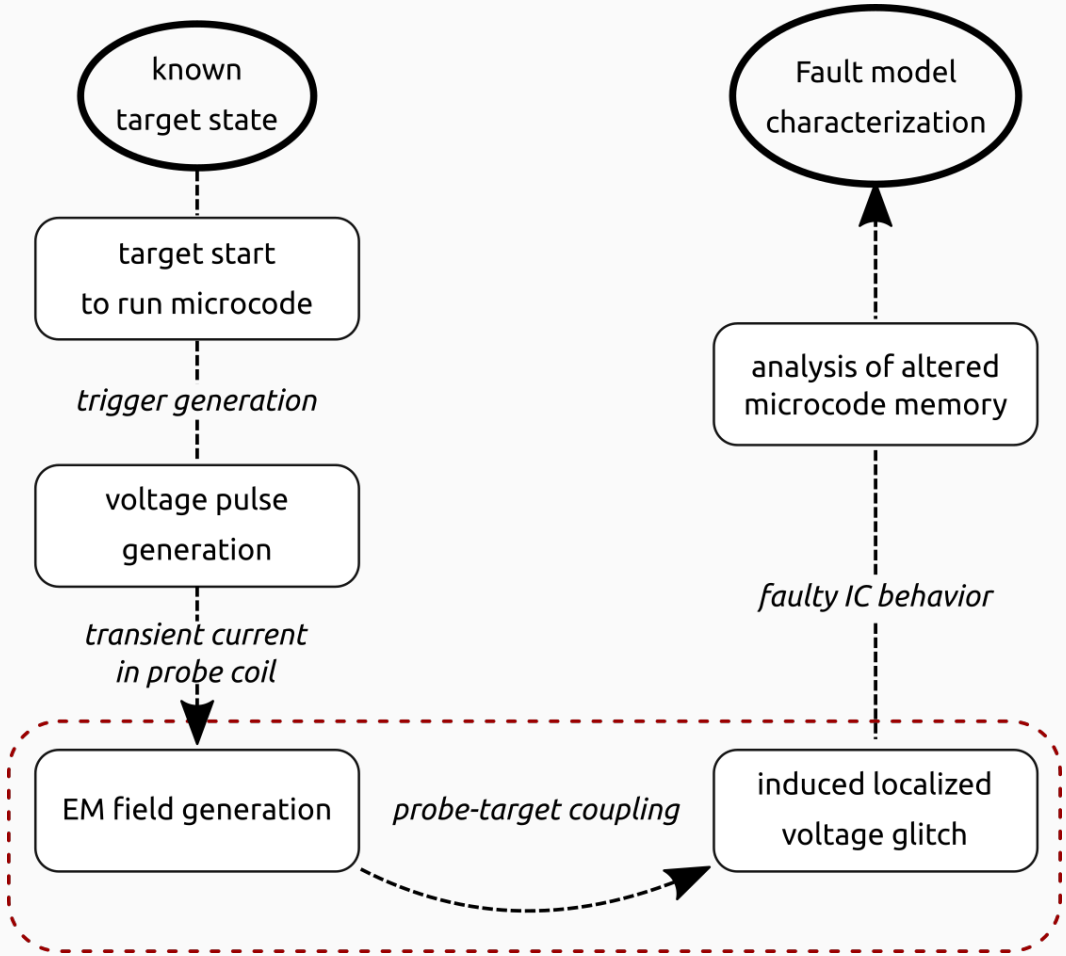
Contribution:
Sauter plusieurs instructions consécutives, un modèle de faute réaliste en injection EM ?

Analyse des paramètres d'injection

Analyse des paramètres d'injection

Dispositif expérimental et méthodologie

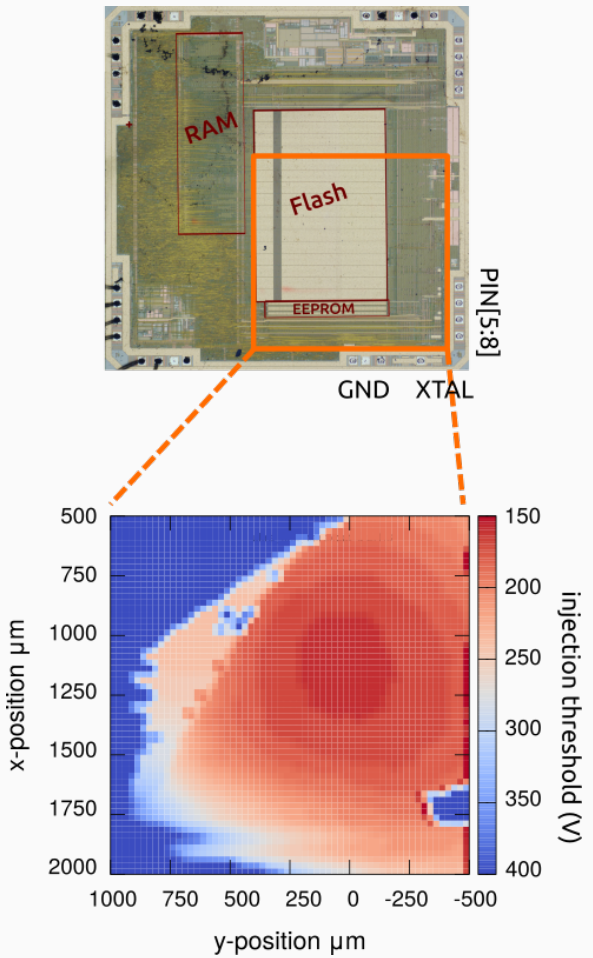




Analyse des paramètres d'injection

Paramètres expérimentaux

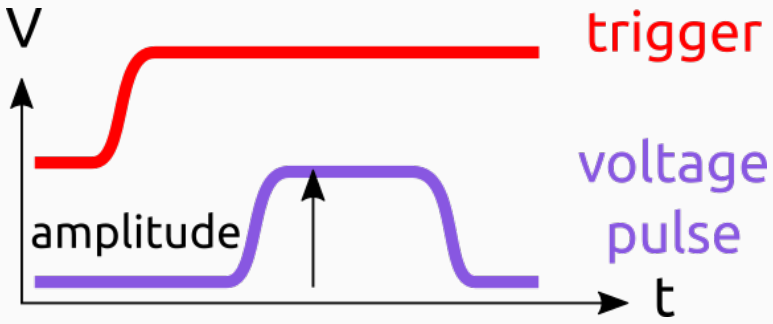
- Position de la sonde (x, y, z)
- Amplitude de l'impulsion
- Délai ou timing d'injection
- Largeur de l'impulsion



Analyse des paramètres d'injection

Paramètres expérimentaux

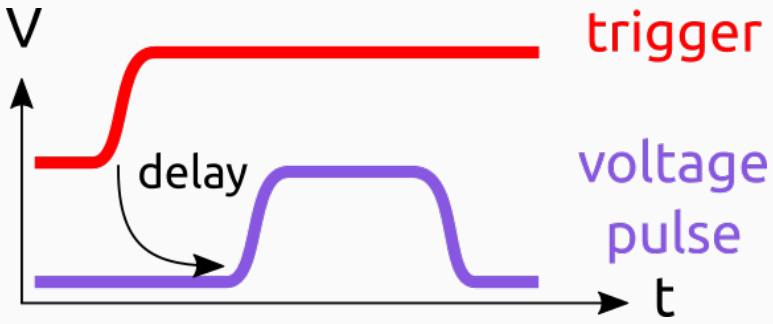
- Position de la sonde (x, y, z)
- Amplitude de l'impulsion
- Délai ou timing d'injection
- Largeur de l'impulsion



Analyse des paramètres d'injection

Paramètres expérimentaux

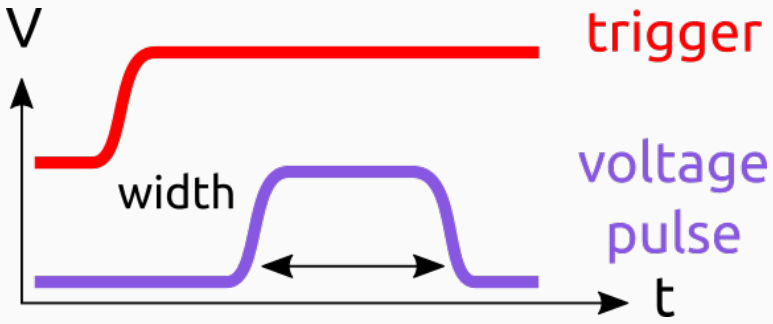
- Position de la sonde (x, y, z)
- Amplitude de l'impulsion
- Délai ou timing d'injection
- Largeur de l'impulsion



Analyse des paramètres d'injection

Paramètres expérimentaux

- Position de la sonde (x, y, z)
- Amplitude de l'impulsion
- Délai ou timing d'injection
- Largeur de l'impulsion



Analyse des paramètres d'injection

Paramètres expérimentaux

- Position de la sonde (x, y, z)
- Amplitude de l'impulsion
- délai entre le front montant du trigger et l'impulsion de tension
- largeur de l'impulsion

⚠ **Principal challenge : explosion combinatoire !** ⚠

Analyse des paramètres d'injection

Caractérisation d'un saut d'instruction

- Récupération des valeurs d'initialisation ?
- Réduction du temps d'éxecution ?
  ($T_{LOAD} = 2T_{NOP}$)

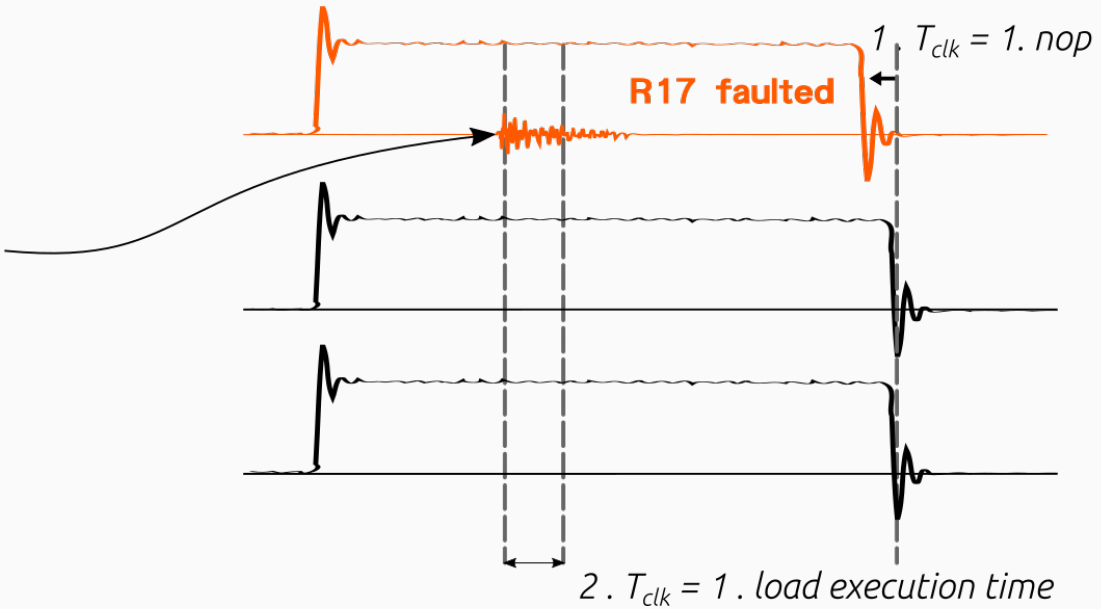
```
#start
ld r16, 0x55
...
ld r25, 0x55

#rise trigger
ld r16, 0x39
ld r17, 0x38
...
ld r25, 0x30
#clear trigger

#readback
mov %[reg16], r16
...
mov %[reg25], r25
#end
```

Analyse des paramètres d'injection

Mécanisme de faute spécifique à l'EM

```
#start
#init with 0x55

#rise trigger
ld r16, 0x39
ld r17, 0x38
ld r18, 0x37
...
#clear trigger

#readback
#39 38 37 36 35
#34 33 32 31 30
#end
```

```
#start
#init with 0x55

#rise trigger
ld r16, 0x39
nop
ld r18, 0x37
...
#clear trigger

#readback
#39 55 37 36 35
#34 33 32 31 30
#end
```

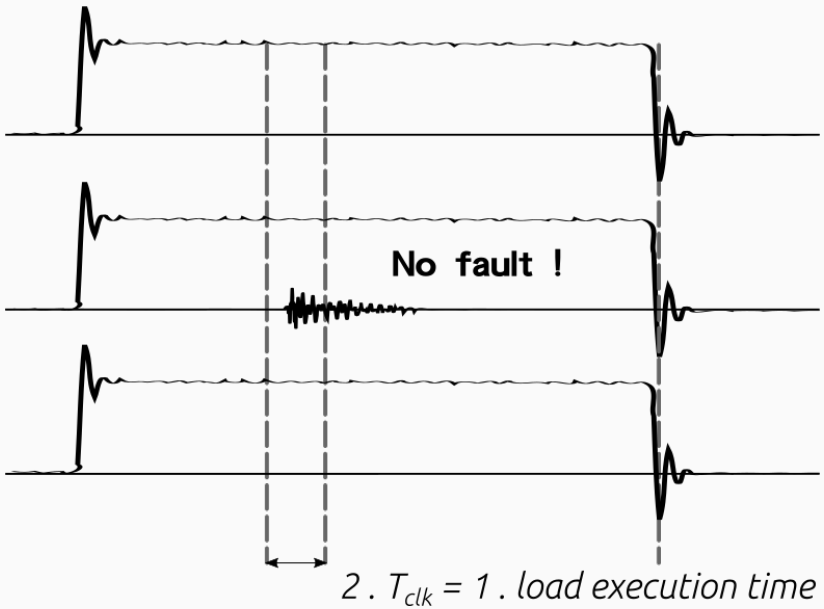


Analyse des paramètres d'injection

Mécanisme de faute spécifique à l'EM

```
#start
#init with 0x55

#rise trigger
ld r16, 0x39
ld r17, 0x38
ld r18, 0x37
...
#clear trigger

#readback
#39 38 37 36 35
#34 33 32 31 30
#end
```

```
#start
#init with 0x55

#rise trigger
ld r16, 0x39
ld r17, 0x38
ld r18, 0x37
...
#clear trigger

#readback
#39 38 37 36 35
#34 33 32 31 30
#end
```

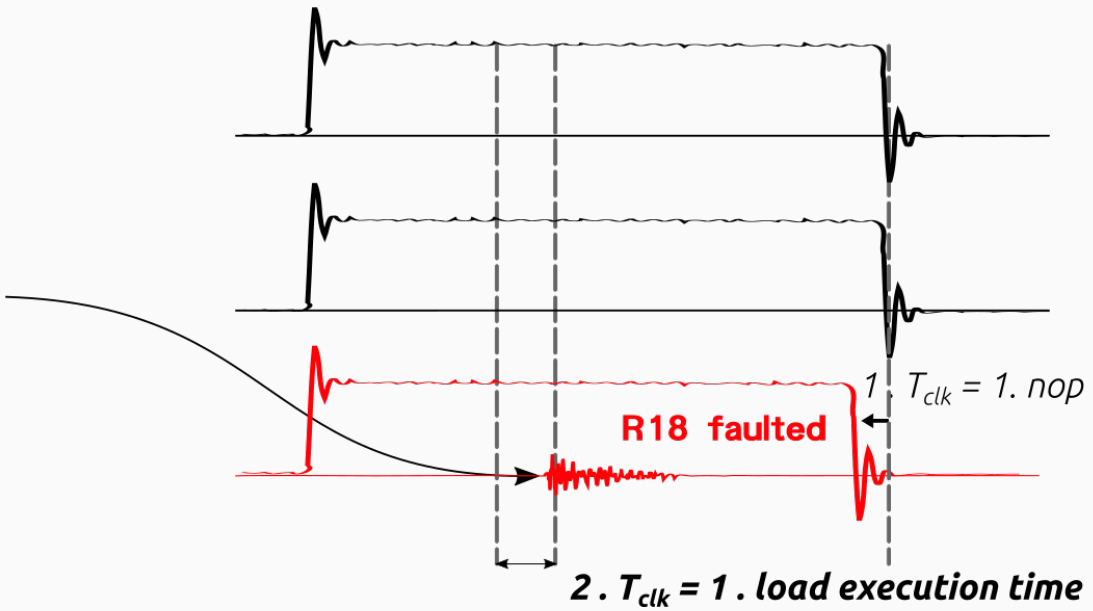


Analyse des paramètres d'injection

Mécanisme de faute spécifique à l'EM

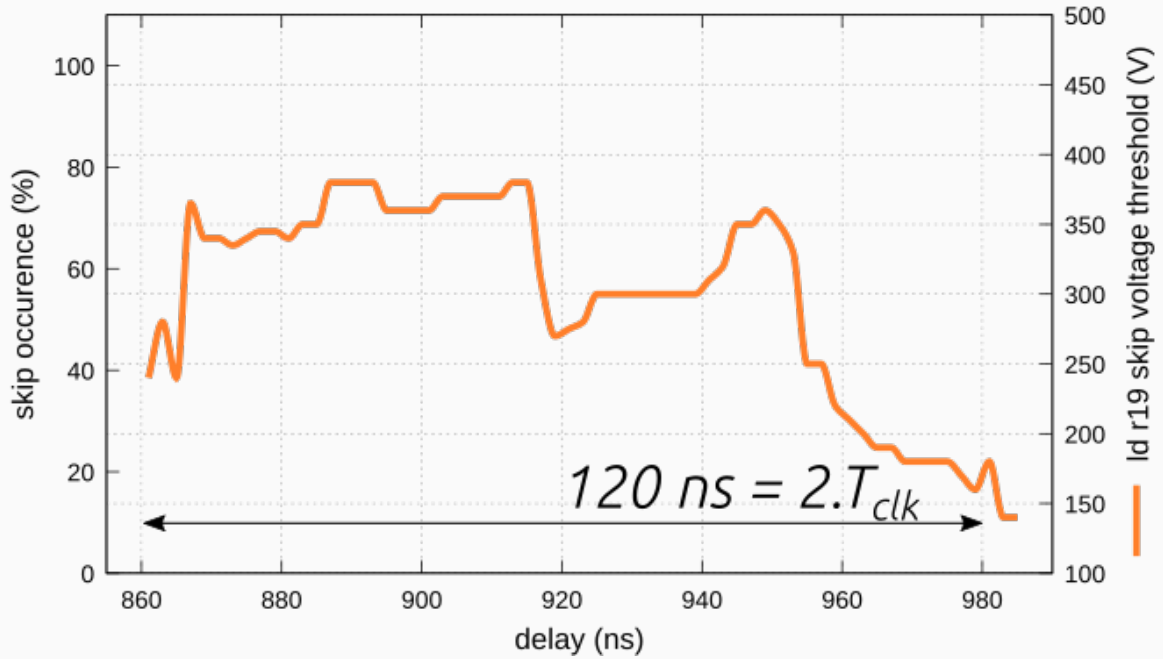
```
#start
#init with 0x55

#rise trigger
ld r16, 0x39
ld r17, 0x38
ld r18, 0x37
...
#clear trigger

#readback
#39 38 37 36 35
#34 33 32 31 30
#end
```

```
#start
#init with 0x55

#rise trigger
ld r16, 0x39
ld r17, 0X38
nop
...
#clear trigger

#readback
#39 38 55 36 35
#34 33 32 31 30
#end
```



Analyse des paramètres d'injection

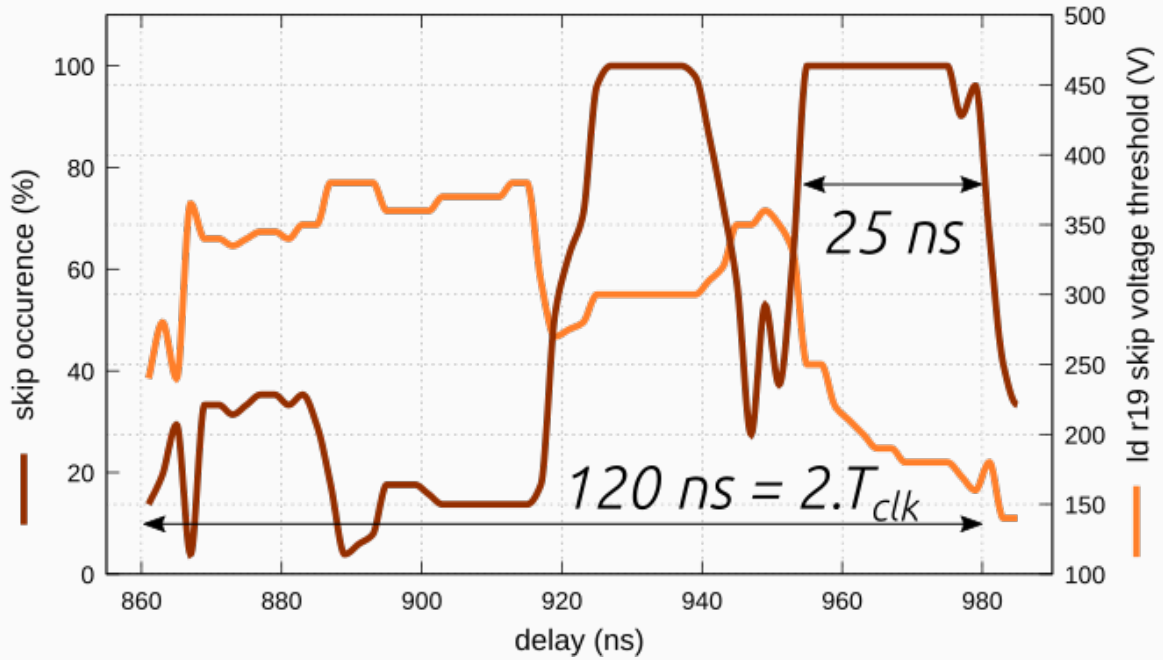
Le **Seuil d'injection** est défini comme l'amplitude minimale permettant l'injection d'un saut d'instruction.



Quelle reproductibilité ?

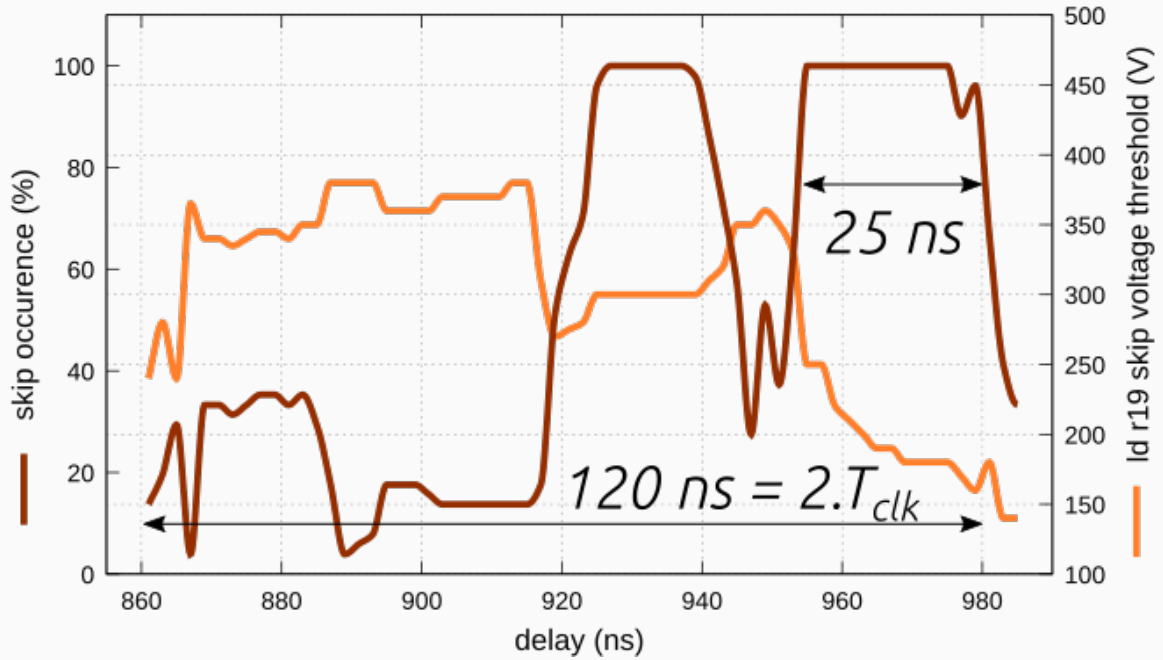
Analyse des paramètres d'injection

- 50 répétitions de la cartographie temporelle
- Apparition de fenêtre de susceptibilité [Ordas'15]



Analyse des paramètres d'injection

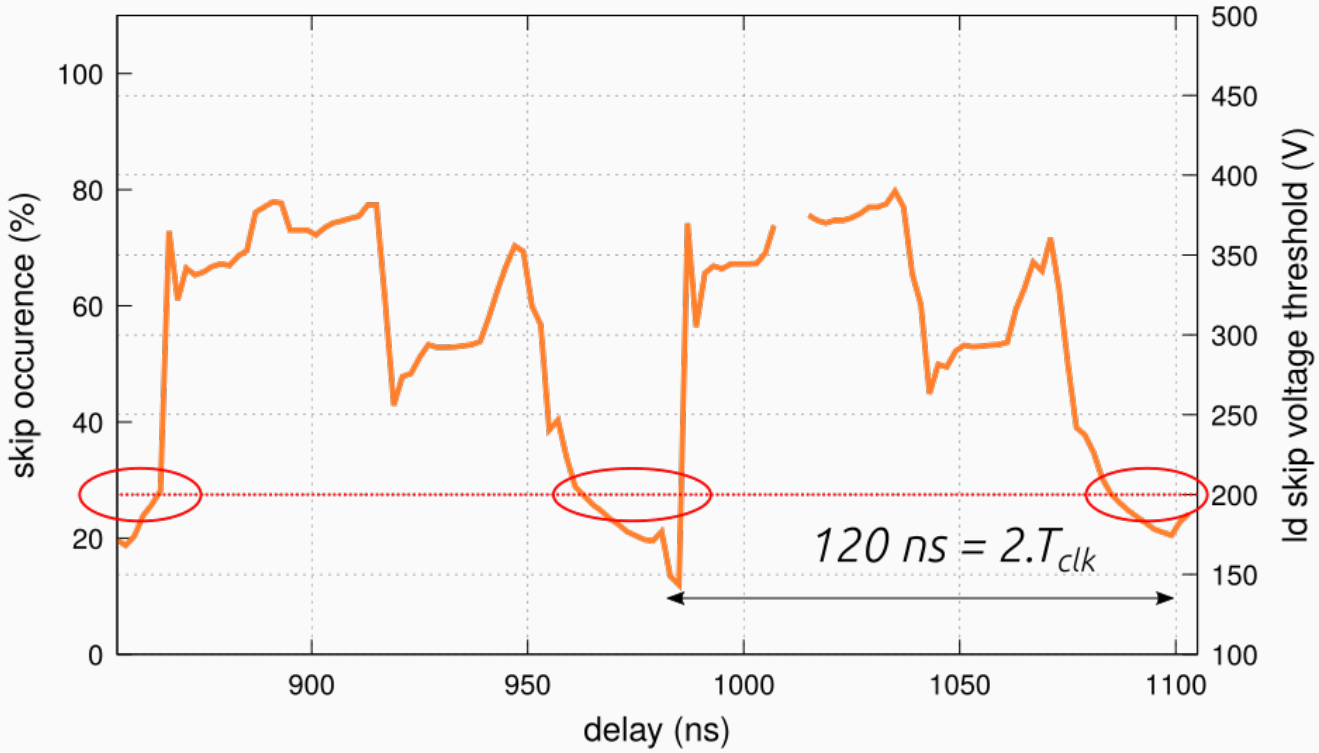
- 50 répétitions de la cartographie temporelle
- Apparition de fenêtre de susceptibilité [Ordas'15]



Une bonne résolution temporelle est cruciale !

Analyse des paramètres d'injection

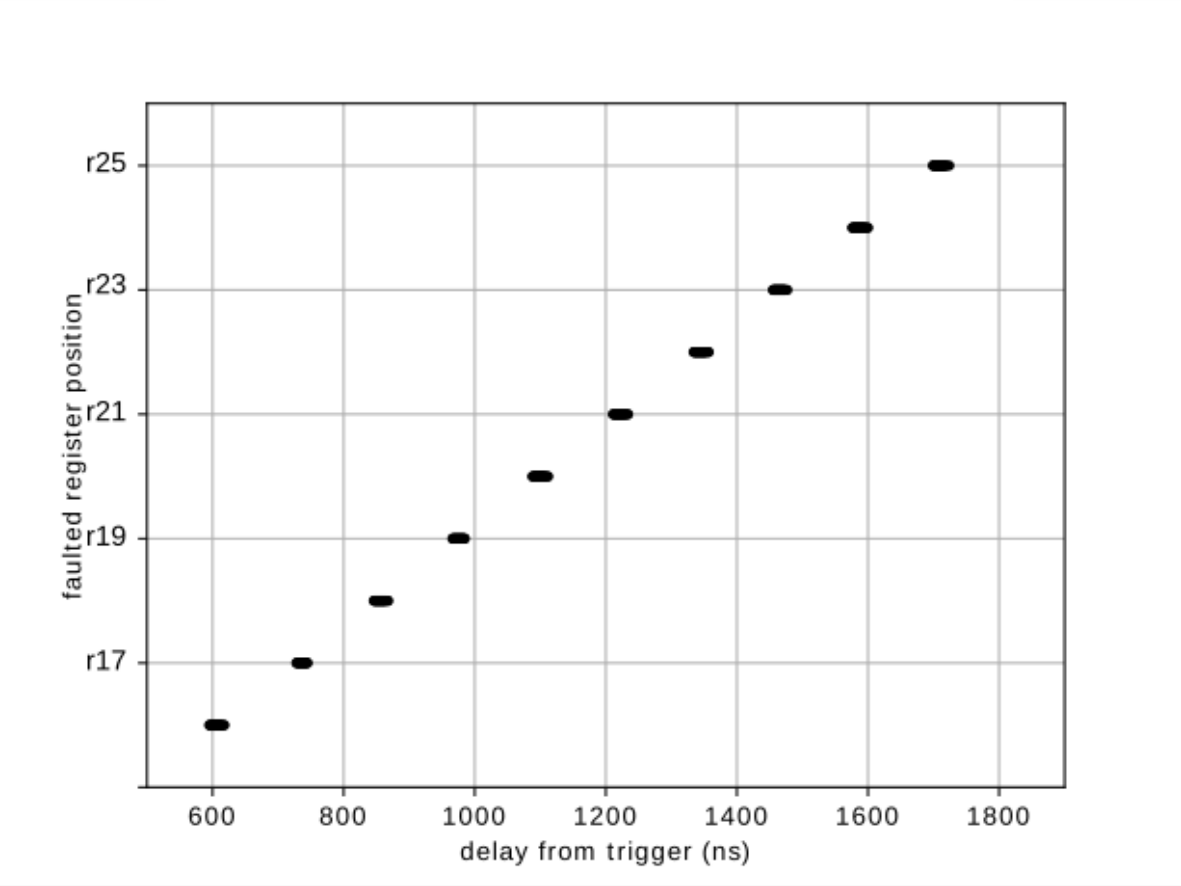
Périodicité de la sensibilité temporelle d'injection



Possibilité de sélectionner les instructions fautées ?

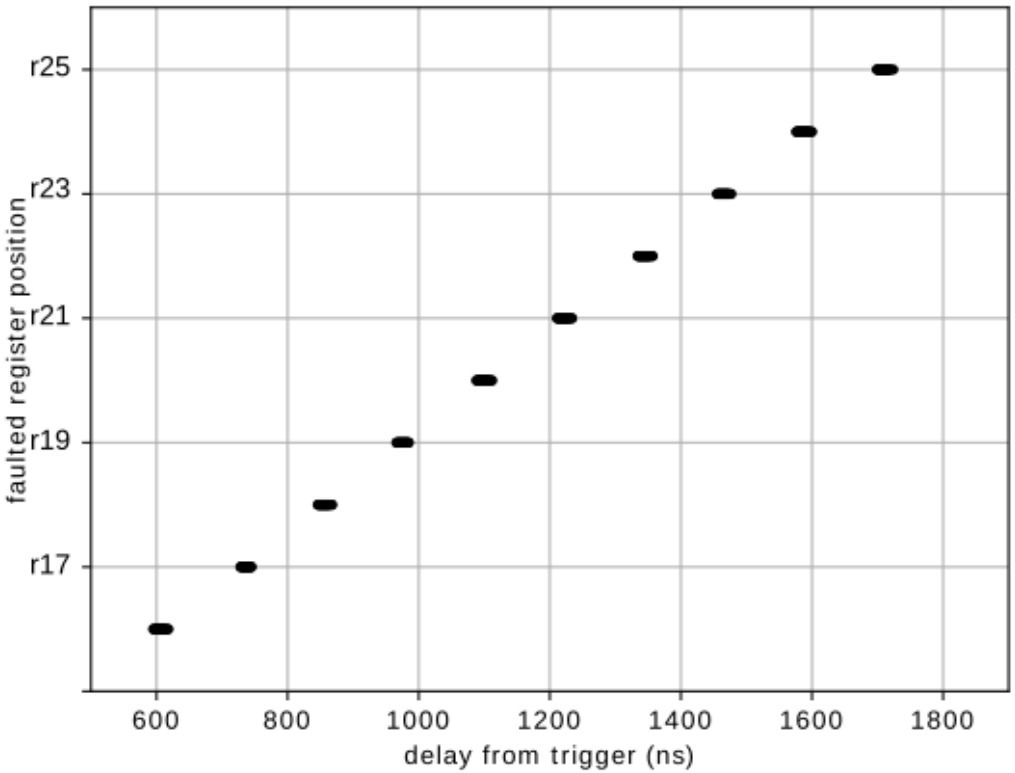
Analyse des paramètres d'injection

Sélectivité des instructions fautées



Analyse des paramètres d'injection

Sélectivité des instructions fautées



Comparable aux résultats obtenus au laser [Breier'15]

Analyse des paramètres d'injection

En résumé

- Méthodologie d'analyse des paramètres d'injection
- Saut d'instruction unique sur microcontrôleur 8 bits
- Sélection de l'instruction fautée (Amplitude et Timing d'injection)
- Saut reproductible dans les fenêtres de susceptibilité

Analyse des paramètres d'injection

En résumé

- Méthodologie d'analyse des paramètres d'injection
- Saut d'instruction unique sur microcontrôleur 8 bits
- Sélection de l'instruction fautée (Amplitude et Timing d'injection)
- Saut reproductible dans les fenêtres de susceptibilité

Influence de la largeur de l'impulsion ?

Saut d'instructions consécutives

Saut d'instructions consécutives

Observations :

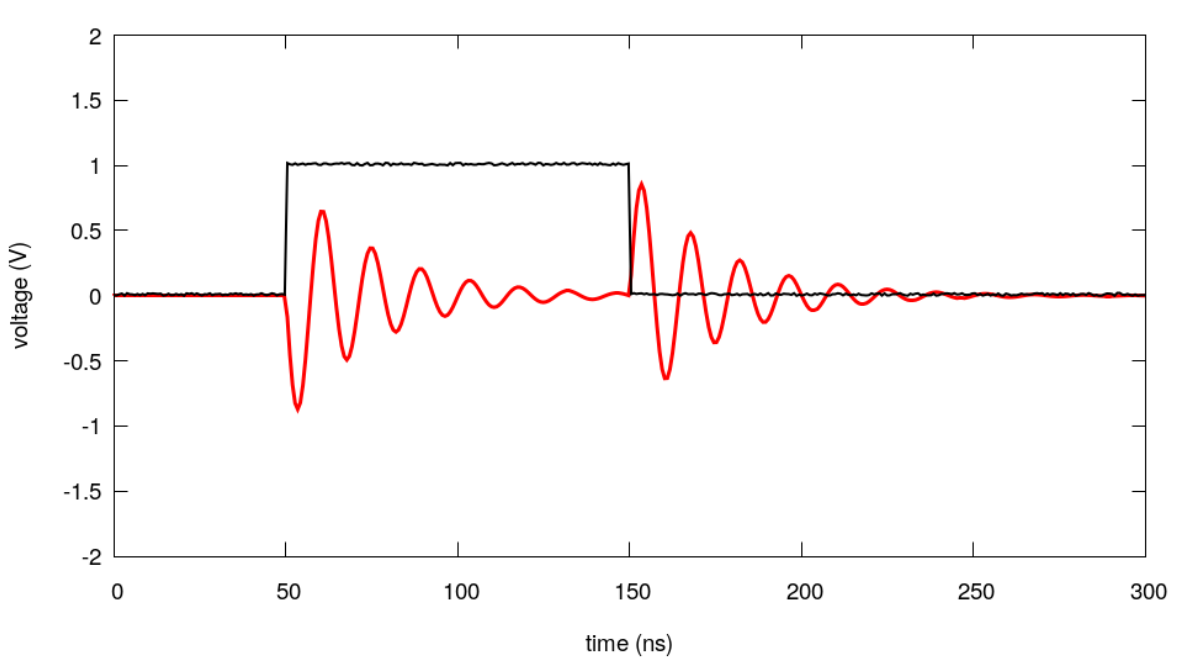
- impulsions larges = réduction du stress induit [Moro'13]
- impulsion **très faible** = réduction du stress induit
- valeurs d'impulsion faible = **amplification** du stress induit

Cadre explicatif ?

Saut d'instructions consécutives

Hypothèse : paquets d'ondes amortis sur le réseau d'alimentation

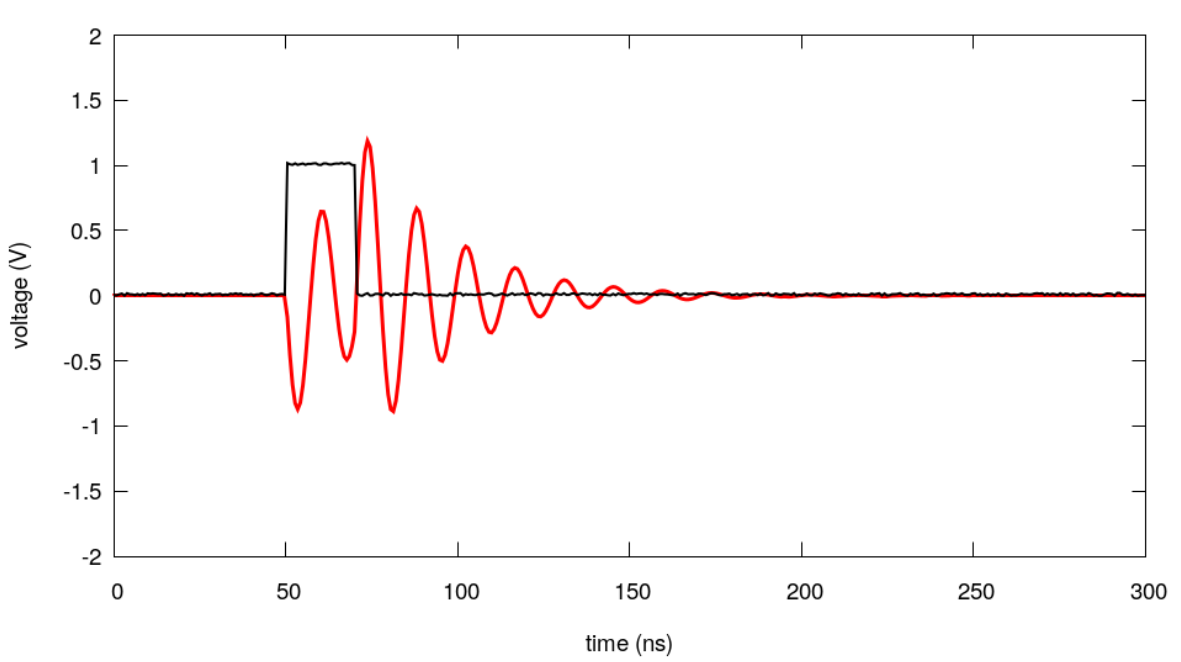
- Couplage sonde / réseau d'alimentation [Poucheret'11]
- Réponse du réseau d'alimentation à un glitch de tension [Zussa'14]



Saut d'instructions consécutives

Hypothèse : paquets d'ondes amortis sur le réseau d'alimentation

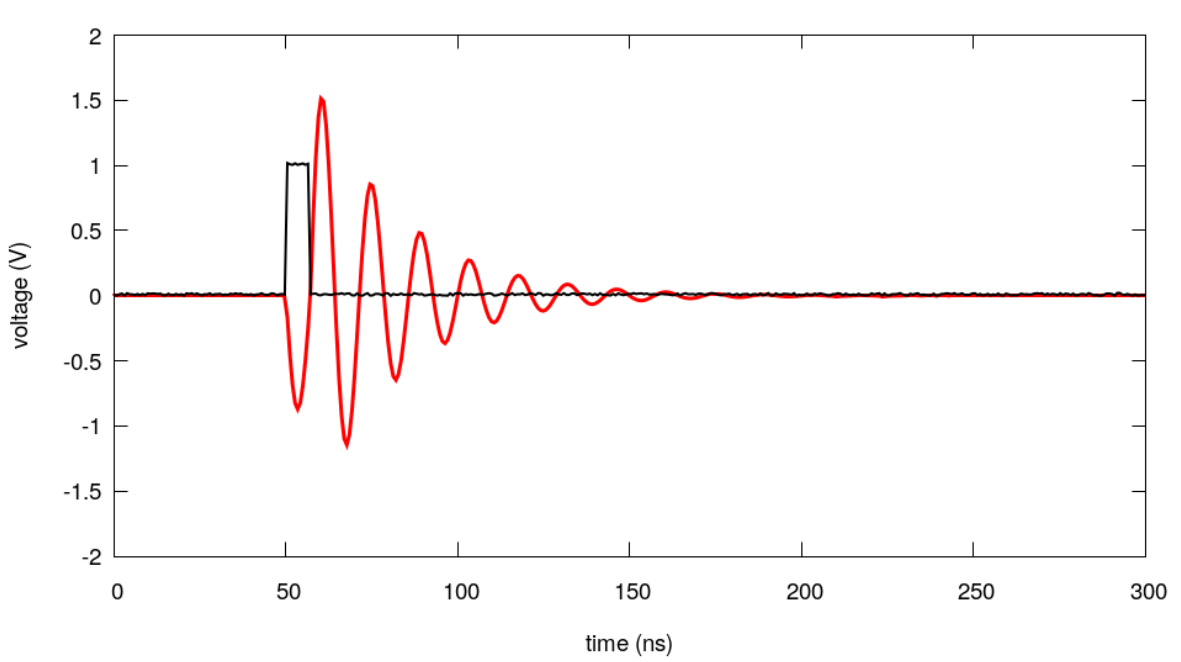
- Couplage sonde / réseau d'alimentation [Poucheret'11]
- Réponse du réseau d'alimentation à un glitch de tension [Zussa'14]



Saut d'instructions consécutives

Hypothèse : paquets d'ondes amortis sur le réseau d'alimentation

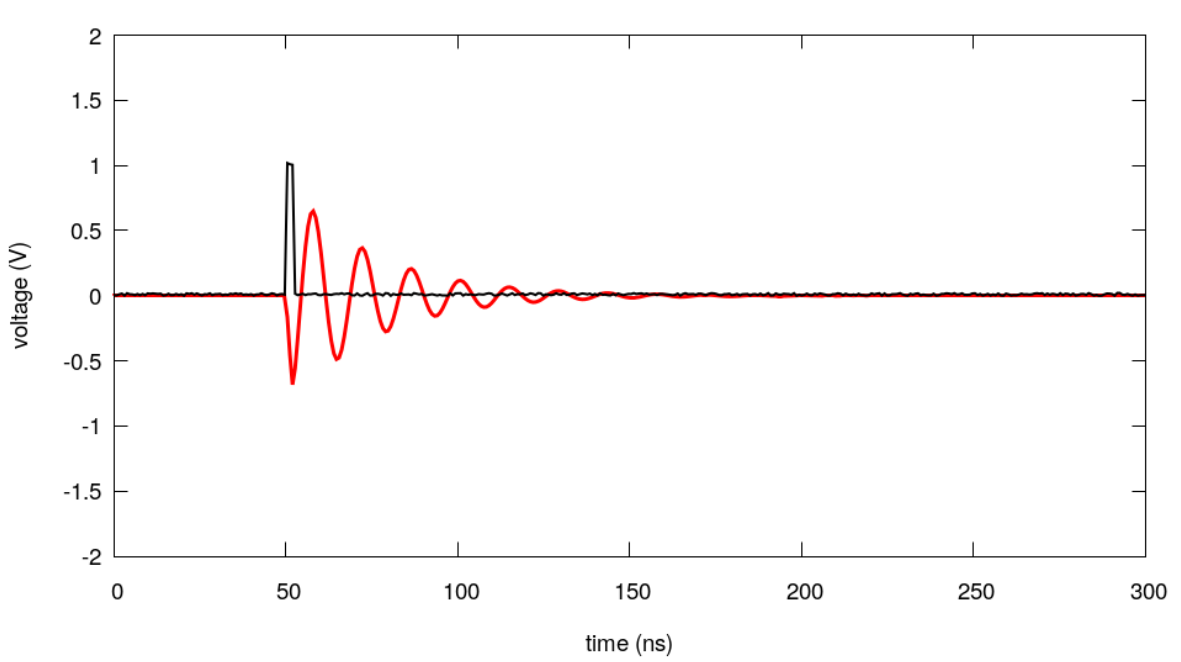
- Couplage sonde / réseau d'alimentation [Poucheret'11]
- Réponse du réseau d'alimentation à un glitch de tension [Zussa'14]



Saut d'instructions consécutives

Hypothèse : paquets d'ondes amortis sur le réseau d'alimentation

- Couplage sonde / réseau d'alimentation [Poucheret'11]
- Réponse du réseau d'alimentation à un glitch de tension [Zussa'14]



Saut d'instructions consécutives

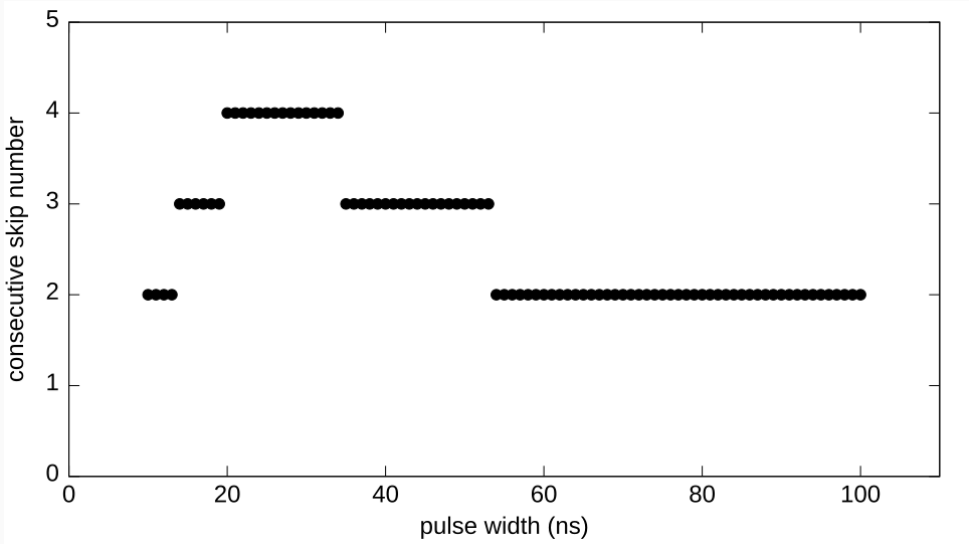
Méthodologie :

1. Se placer spatialement dans une zone sensible
2. Se placer temporellement dans une fenêtre de susceptibilité
3. Diminuer la largeur d'impulsion à tension constante
4. Relever le nombre d'instructions non-exécutées
5. Réaliser un reset de la cible
6. Réitérer à partir du point 3

Saut d'instructions consécutives

Hypothèse : paquet d'onde amorti sur le réseau d'alimentation

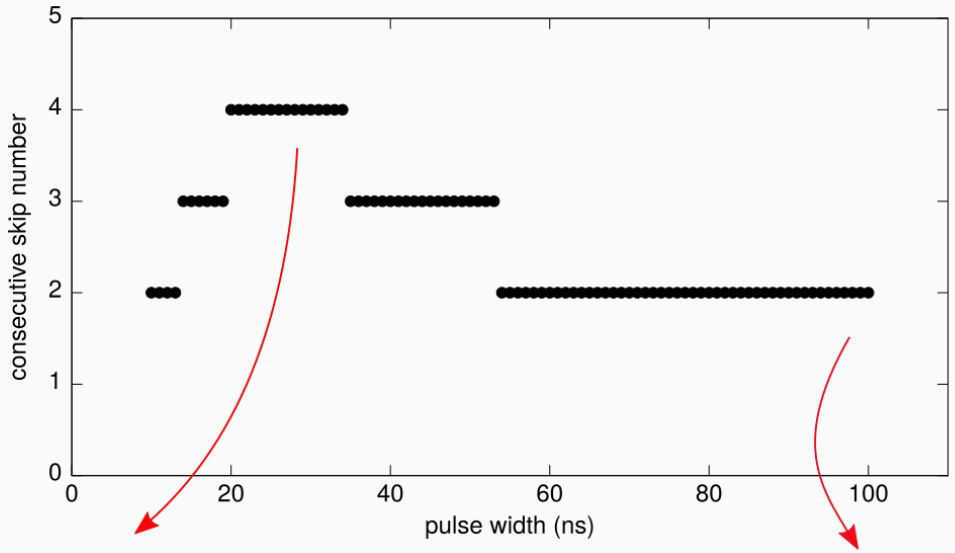
- Interférences destructives $w < 20$ *ns*
- Interférences constructives $w \approx 25$ *ns*
- Pas d'interférences $w > 50$ *ns*

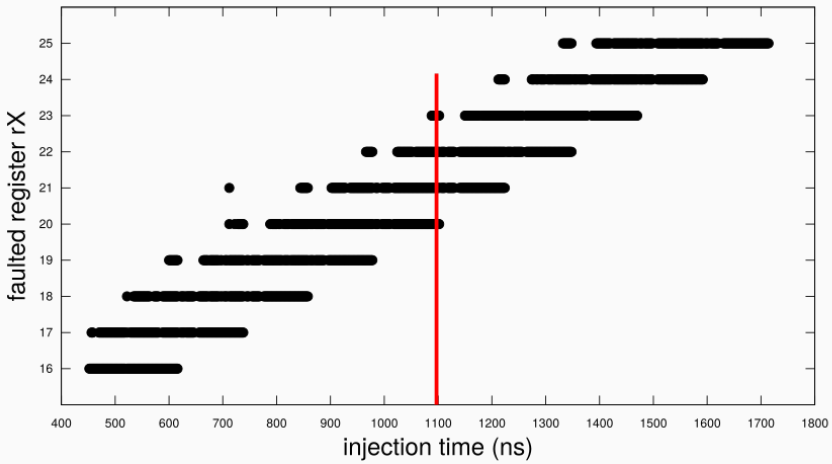


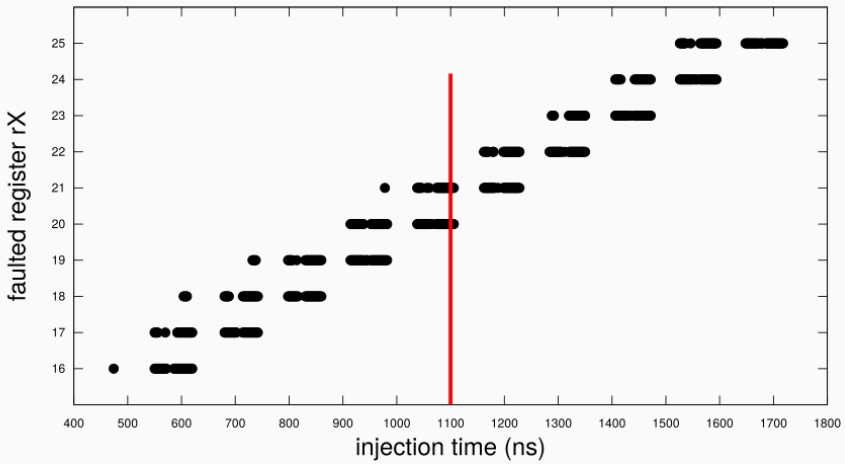
Dépendance entre l'instant d'injection et le nombre de saut ?

Saut d'instructions consécutives

Sélection temporelle du bloc d'instruction non-exécuté







Conclusion

Conclusion

- Méthodologie d'analyse des paramètres d'injection

Conclusion

- Méthodologie d'analyse des paramètres d'injection
- Sélection temporelle des instructions fautées

Conclusion

- Méthodologie d'analyse des paramètres d'injection
- Sélection temporelle des instructions fautées
- Sélection indépendante du nombre d'instruction consécutives fautées

Conclusion

- Méthodologie d'analyse des paramètres d'injection
- Sélection temporelle des instructions fautées
- Sélection indépendante du nombre d'instruction consécutives fautées
- Sauts multiples reproductibles

Conclusion

- Méthodologie d'analyse des paramètres d'injection
- Sélection temporelle des instructions fautées
- Sélection indépendante du nombre d'instruction consécutives fautées
- Sauts multiples reproductibles
- Nécessité de réglage fin timing injection / largeur d'impulsion

Perspective

- Résultats valable sur une architecture 32 bit ?
- Syncronisation externe ?
- Attaque Secure boot ? [Timmers'16]

Merci pour votre attention !

alexandre.menu@emse.fr

References

[1] J. Balasch, B. Gierlichs, and I. Verbauwhede. An in-depth and black-box characterization of the effects of clock glitches on 8-bit mcus. In *2011 Workshop on Fault Diagnosis and Tolerance in Cryptography*, pages 105–114, Sept 2011.

[2] A. Barenghi, G. Bertoni, E. Parrinello, and G. Pelosi. Low voltage fault attacks on the rsa cryptosystem. In *2009 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pages 23–31, Sept 2009.

Références ii

[3] T. Barry, D. Couroussé, and B. Robisson. Compilation of a countermeasure against instruction-skip fault attacks. In *Proceedings of the Third Workshop on Cryptography and Security in Computing Systems*, CS2 '16, pages 1–6, New York, NY, USA, 2016. ACM.

[4] J. Breier, D. Jap, and C.-N. Chen. Laser profiling for the back-side fault attacks: With a practical laser skip instruction attack on aes. In *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security*, CPSS '15, pages 99–103, New York, NY, USA, 2015. ACM.

Références iii

[5] L. Chusseau, R. Omarouayache, J. Raoult, S. Jarrix, P. Maurine, K. Tobich, A. Bover, B. Vrignon, J. Shepherd, T. H. Le, M. Berthier, L. Rivière, B. Robisson, and A. L. Ribotta. Electromagnetic analysis, deciphering and reverse engineering of integrated circuits (e-mata hari). In *2014 22nd International Conference on Very Large Scale Integration (VLSI-SoC)*, pages 1–6, Oct 2014.

[6] A. Dehbaoui, J. M. Dutertre, B. Robisson, and A. Tria. Electromagnetic transient faults injection on a hardware and a software implementations of aes. In *2012 Workshop on Fault Diagnosis and Tolerance in Cryptography*, pages 7–15, Sept 2012.

[7] J. marc Schmidt and M. Hutter. Optical and em fault-attacks on crt-based rsa: Concrete results, 2007.

Références iv

[8] N. Moro, A. Dehbaoui, K. Heydemann, B. Robisson, and E. Encrenaz. Electromagnetic fault injection: Towards a fault model on a 32-bit microcontroller. In *2013 Workshop on Fault Diagnosis and Tolerance in Cryptography*, pages 77–88, Aug 2013.

[9] N. Moro, K. Heydemann, A. Dehbaoui, B. Robisson, and E. Encrenaz. Experimental evaluation of two software countermeasures against fault attacks. In *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, pages 112–117, May 2014.

[10] S. Ordas, L. Guillaume-Sage, and P. Maurine. Em injection: Fault model and locality. In *2015 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pages 3–13, Sept 2015.

Références v

[11] F. Poucheret, L. Chusseau, B. Robisson, and P. Maurine. Local electromagnetic coupling with cmos integrated circuits. In *2011 8th Workshop on Electromagnetic Compatibility of Integrated Circuits*, pages 137–141, Nov 2011.

[12] L. Rivière, Z. Najm, P. Rauzy, J.-L. Danger, J. Bringer, and L. Sauvage. High Precision Fault Injections on the Instruction Cache of ARMv7-M Architectures. In *HOST 2015: IEEE International Symposium on Hardware-Oriented Security and Trust*, Washington, United States, May 2015.

[13] J. M. Schmidt and C. Herbst. A practical fault attack on square and multiply. In *2008 5th Workshop on Fault Diagnosis and Tolerance in Cryptography*, pages 53–58, Aug 2008.

Références vi

[14] B. Yuce, N. F. Ghalaty, H. Santapuri, C. Deshpande, C. Patrick, and P. Schaumont. Software fault resistance is futile: Effective single-glitch attacks. In *2016 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pages 47–58, Aug 2016.

[15] L. Zussa, J. M. Dutertre, J. Clediere, and B. Robisson. Analysis of the fault injection mechanism related to negative and positive power supply glitches using an on-chip voltmeter. In *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, pages 130–135, May 2014.