KU LEUVEN

COSIC

Design Considerations for EM Pulse Fault Injection

Arthur Beckers, Masahiro Kinugawa, Yuichi Hayashi, Daisuke Fujimoto, Josep Balasch, Benedikt Gierlichs, and Ingrid Verbauwhede

CARDIS 2019

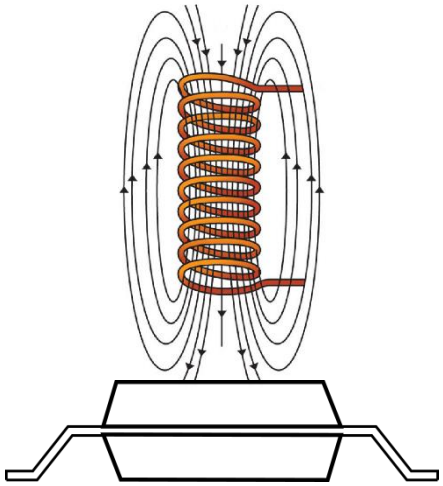
What is EM-fault injection

Injection of electromagnetic field into a target IC

Properties:

+ Locality → relatively good spatial resolution (100um - mm)
+ In theory no decapsulation needed → non invasive
+ Relatively good timing resolution
+ Can be done cheaply (100 euro)

- Completely black box behaviour of the device



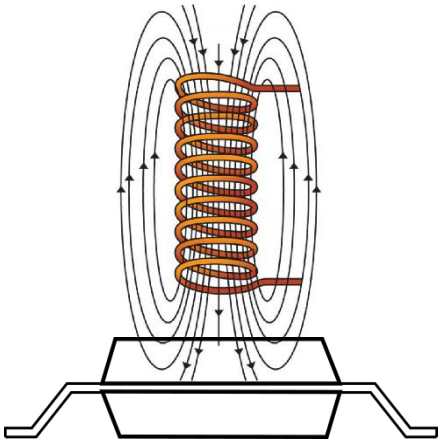
Injected fields:

- E-field
- H-field
- Combination of both

H-field EM pulse injection

H-field probe characteristics:

- Solenoid shape
- Air or ferrite core
- 0.1- 10mm diameter
- 1 - 20 windings

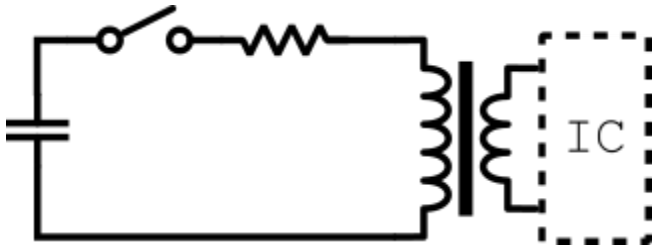


H-field EM pulse characteristics:

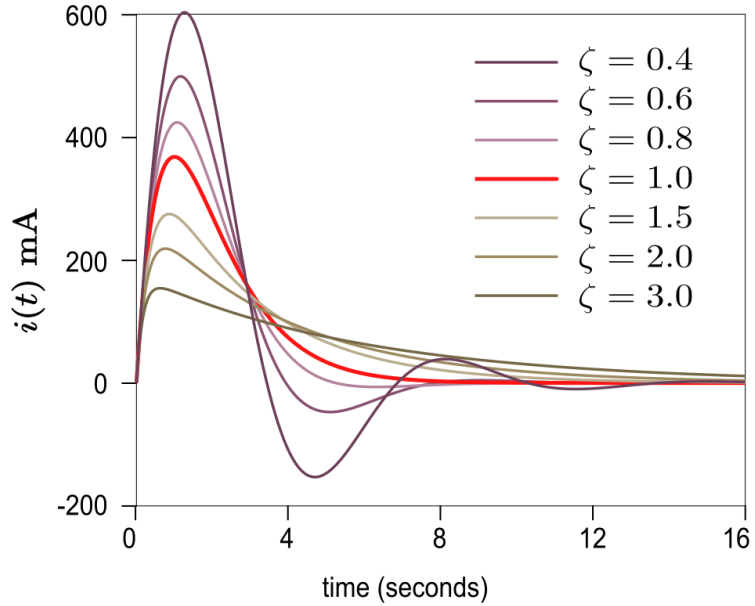
- ns rise times
- Currents in ampere range

Magnetic flux density : $B = \frac{k\mu_0 N}{2l} I \left[\frac{l}{\sqrt{l^2+r^2}}\right]$

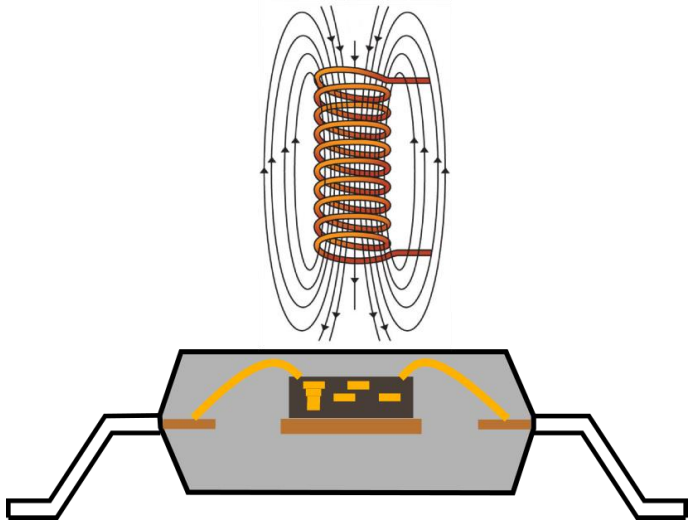
EM-pulse injection modelling



RLC response ($\zeta = \frac{R}{2}\sqrt{\frac{C}{L}}$)



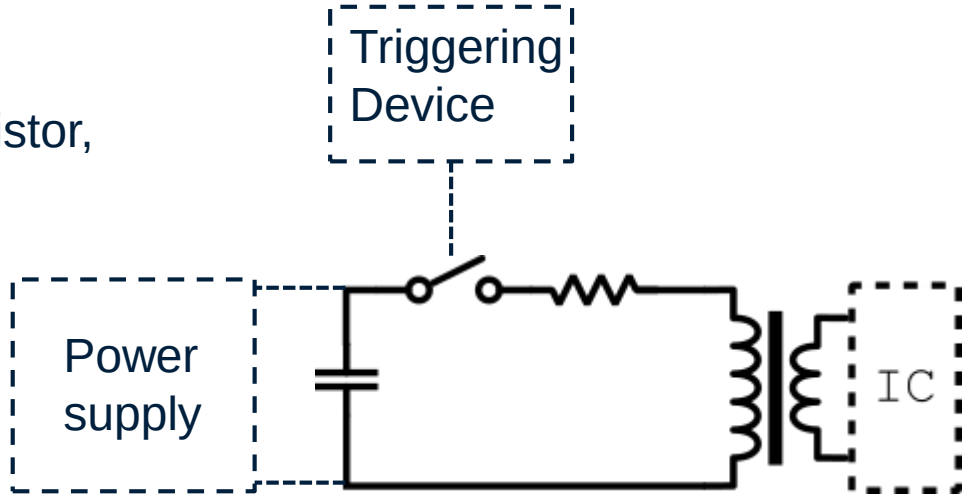
IC coupling



KU LEUVEN

EM fault injection setup

- Switching element:
  - Fast rise time
  - Small parasitics
  - Consistent timing/ controllable
  - E.g Mosfet, IGBT, bipolar transistor, …
- Triggering device:
  - High timing resolution
  - Small amount jitter
- Power supply
  - 100-500V DC
- Injection probe :
  - Characteristics are target dependent



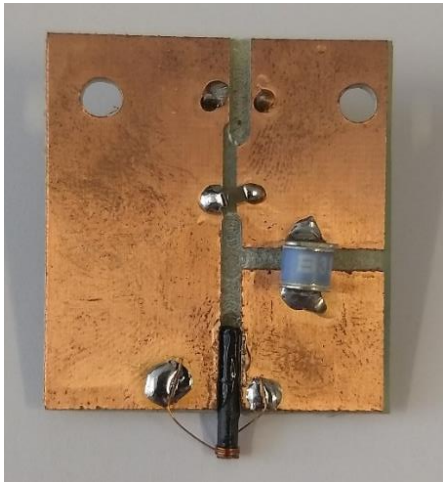
KU LEUVEN

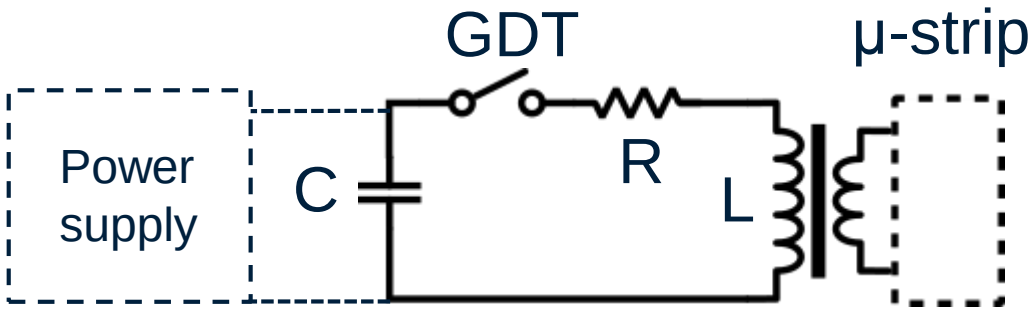
Characterization strategy

- Goal: illustrate how different passive components impact pulse response

- Test circuit:
  - Gas discharge tube switch (GDT) → 370V breakdown voltage
  - 47pF capacitor
  - 2mm ferrite core
  - 2 windings

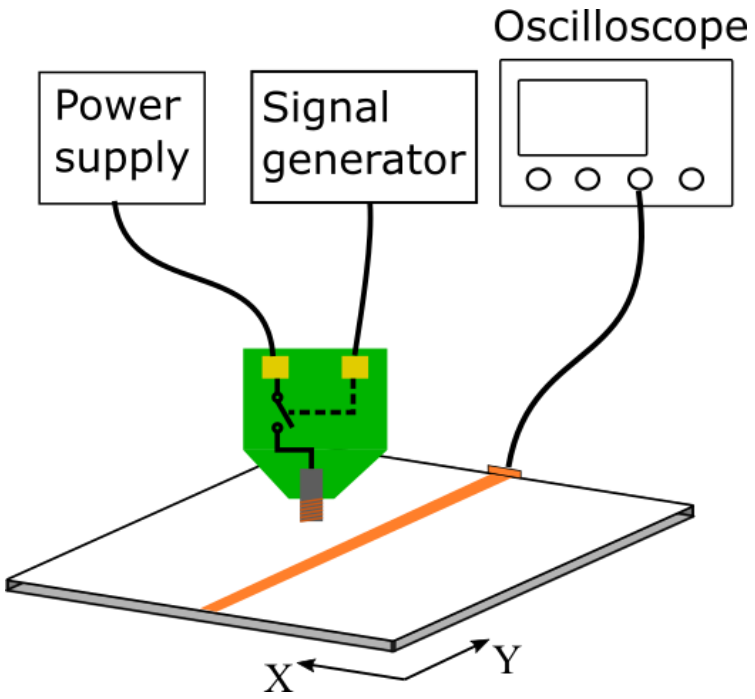
- Test method:
  - 50Ω microstripline



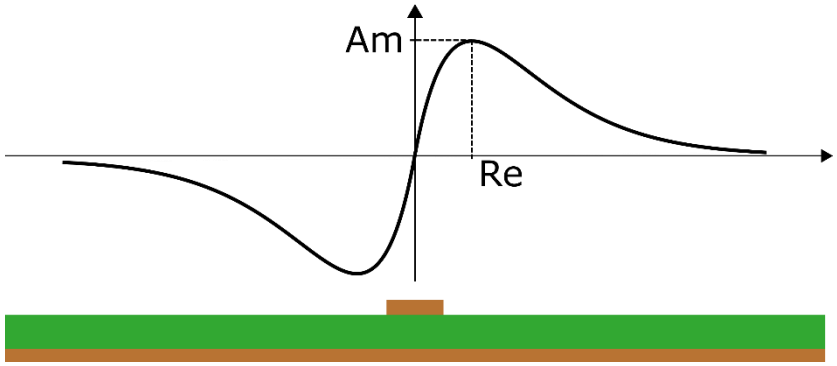


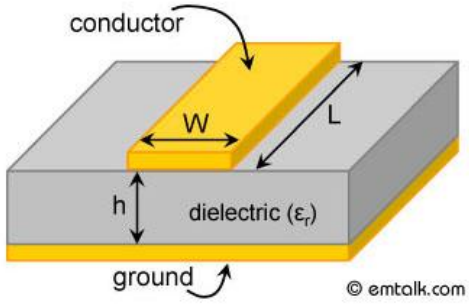
KU LEUVEN

Microstripline measurement method



50Ω microstripline response

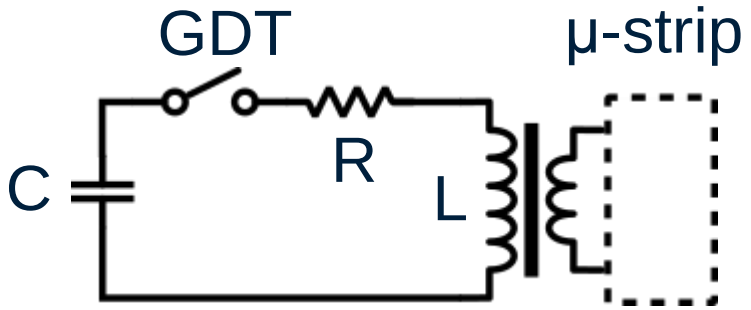


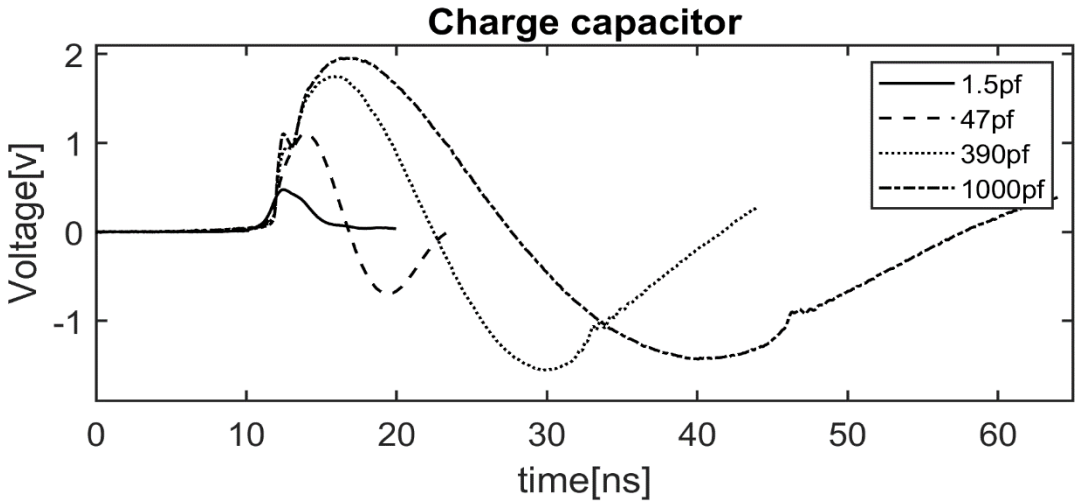


KU LEUVEN

Probe characterization

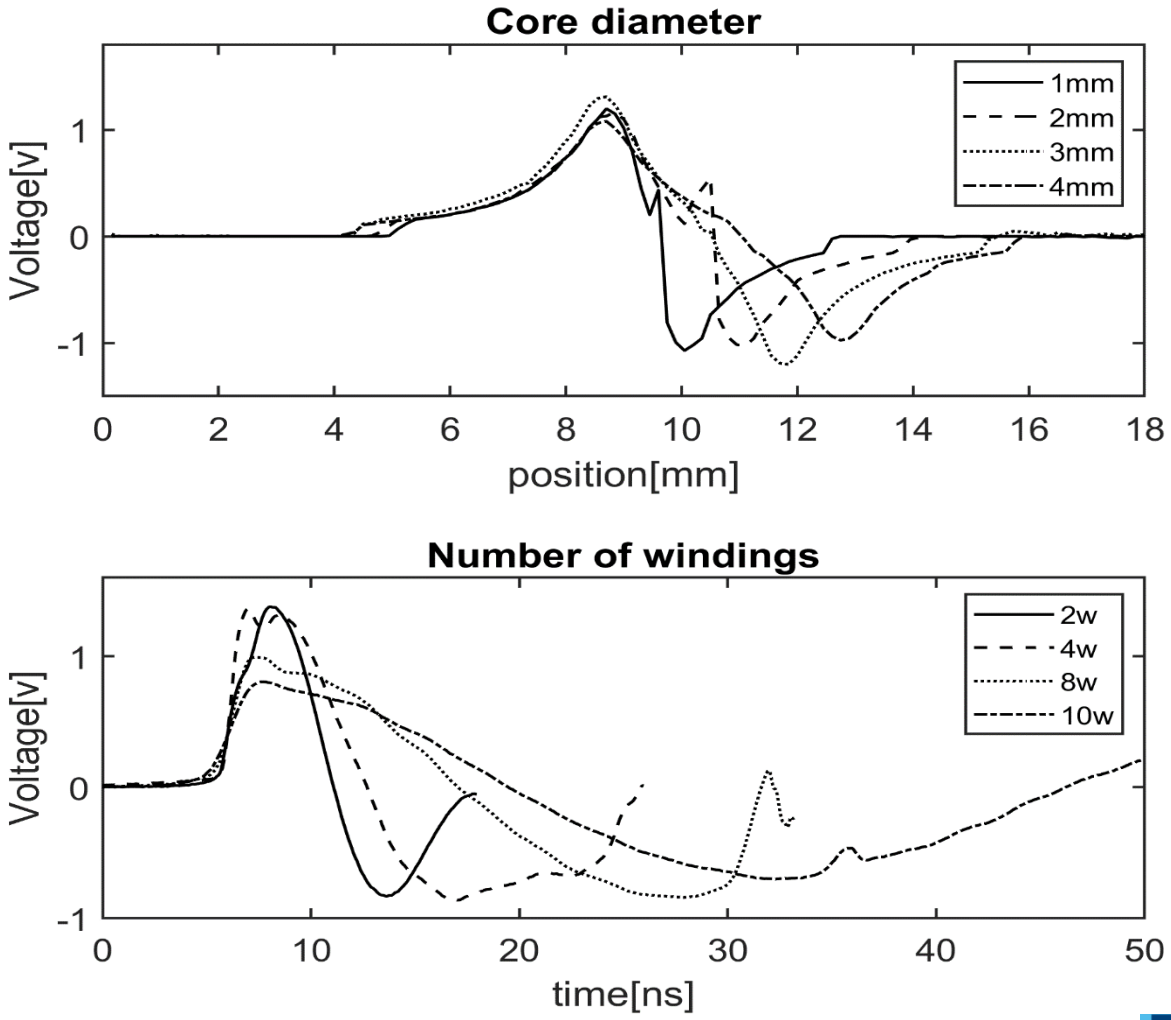
- Parameters injection circuit:
  - Capacitance
  - Ferrite core diameter
  - Number of windings
  - Ferrite type
  - Winding geometry



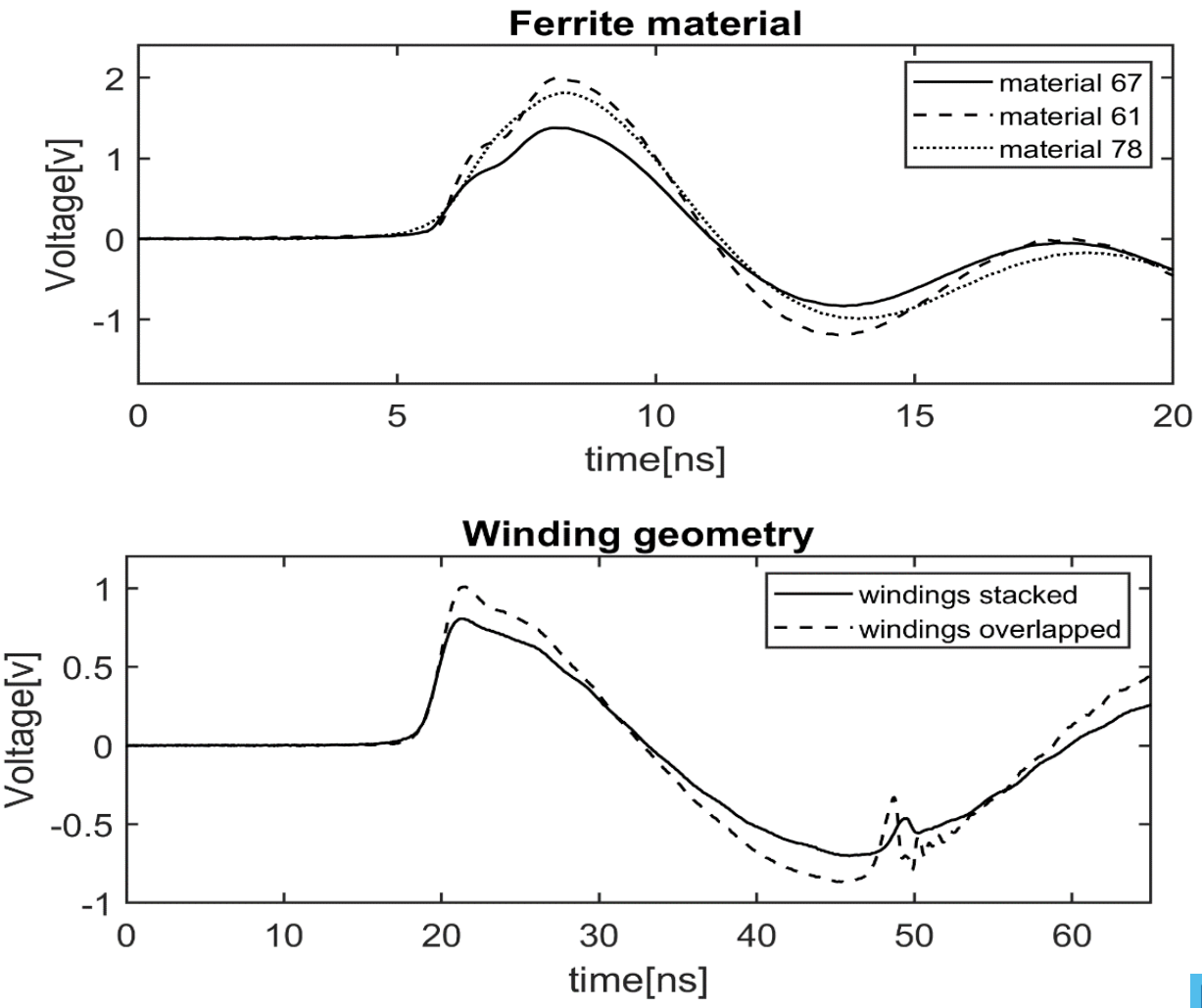


KU LEUVEN

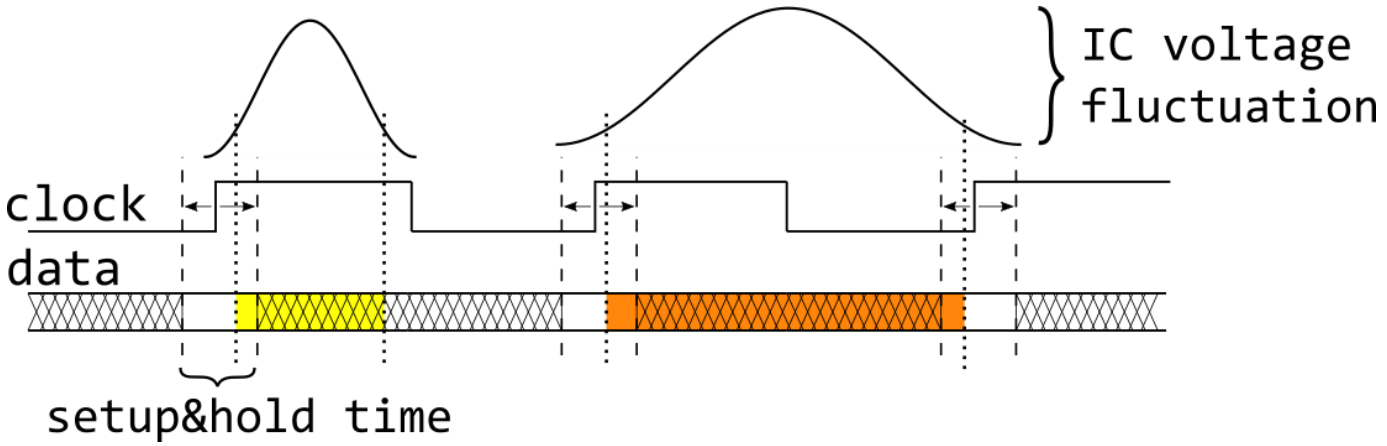
Probe characterization



Probe characterization



EM-pulse faulting mechanism



[1] Ordas et al., Evidence of a larger em-induced fault model. CARDIS 2015

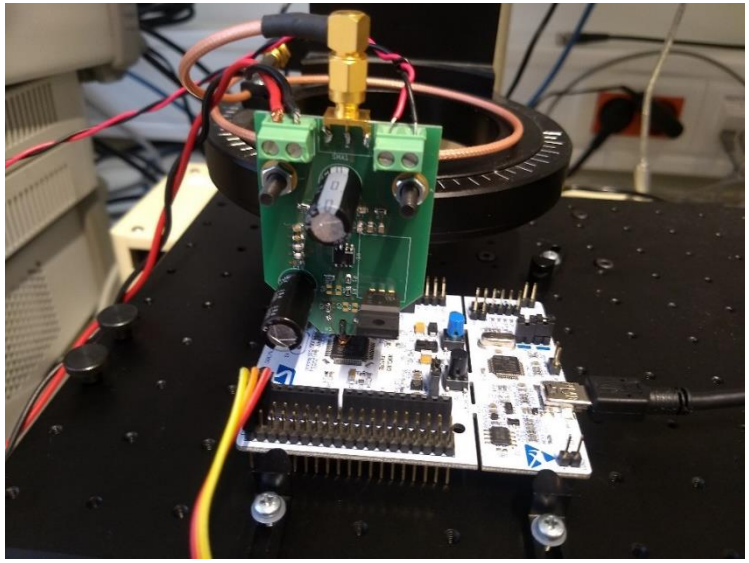
KU LEUVEN

Experimental validation

Goal:
demonstrate the impact of the pulse shape on the fault pattern

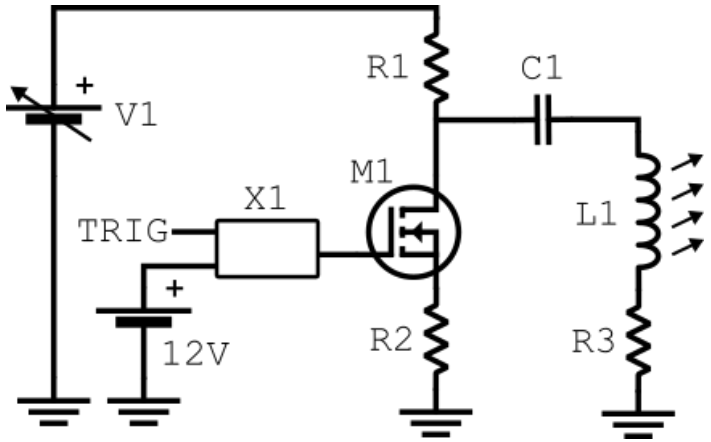
Target device:
- STM32F411
- Clock frequency: 100MHz
- Not decapsulated

Target code:
- STM {r0-r9} (store multiple)
- Data: 0x55555555



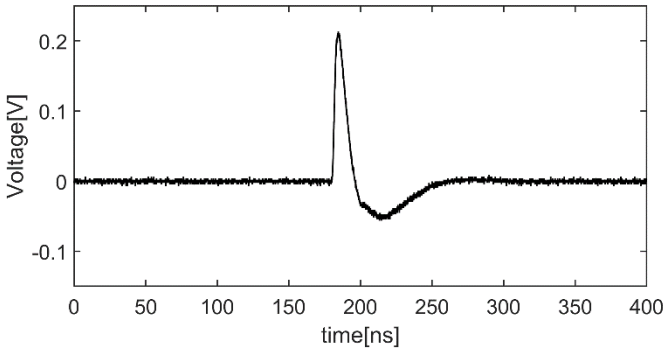
EM-fault injector

- Switching element:
  - MOSFET, n-channel
- Injection probe :
  - 0,75mm
  - 4 windings
- Triggering device:
  - Signal generator + Mosfet driver
- Power supply:
  - 100V - 600 V
- Passive components:
  - C1: 1000 pF
  - R2: 0.22 Ω
  - R3: 10 Ω

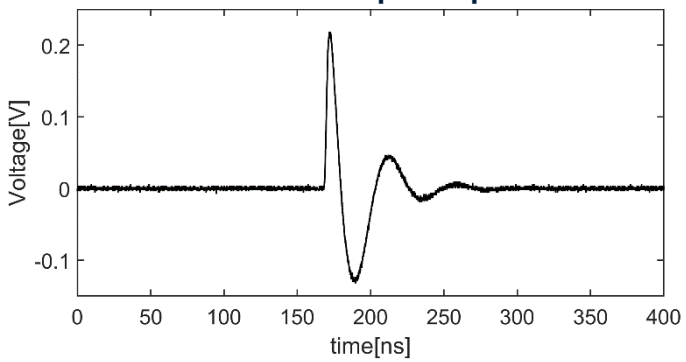


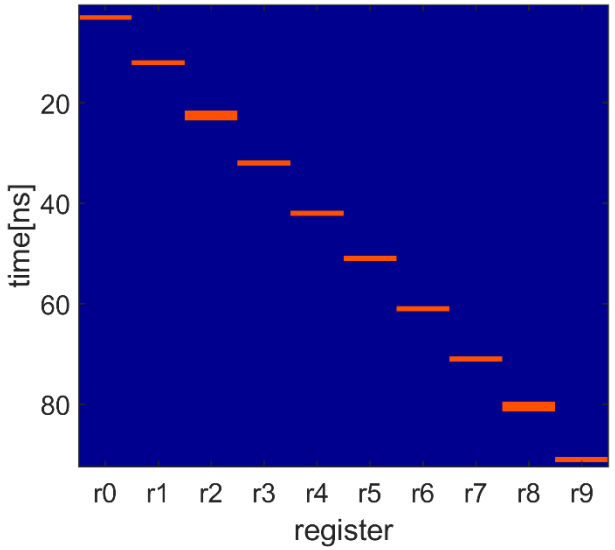
Experimental results

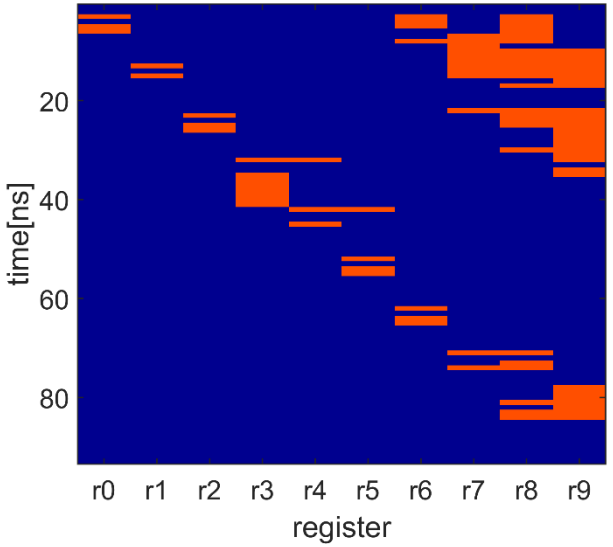
Critically damped probe



Under damped probe







KU LEUVEN

Conclusion

- Illustrated the impact of the different components on the pulse shape
- Built an EM-pulse fault injection circuit based on the previous findings
- Demonstrated the effect different pulse shapes can have on a fault injection campaign