EPC Class 1 GEN 2 UHF RFID Tag Emulator for Robustness Evaluation and Improvement

Omar Abdelmalek, David Hély and Vincent Beroulle

Grenoble Institute of Technology
omar.abelmaleck@lcis.grenoble-inp.fr

Journées scientifiques 2013 du projet SEmba

Outline

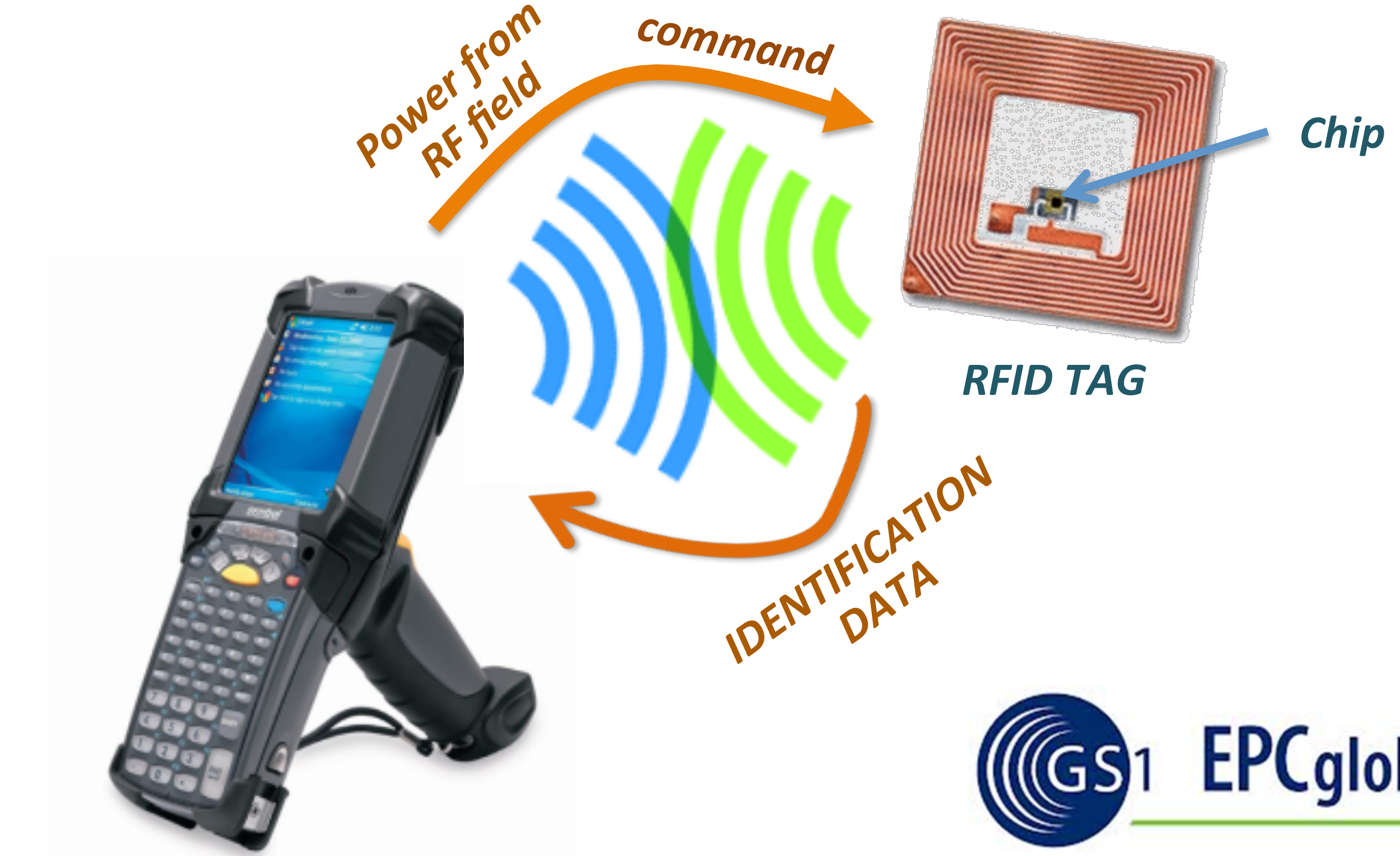
- RFID System and Application
- EPC GEN2 Security and robustness issues
- The RFID tag Verification Issues
- RFID IC Emulation system
- The Emulator
- Conclusion and Perspectives

Outline

- RFID System and Application
- EPC GEN2 Security and robustness issues
- The RFID tag Verification Issues
- RFID IC Emulation system
- The Emulator
- Conclusion and Perspectives

Introduction

Radio Frequency Identification



Power from RF field

command

Chip

RFID TAG

IDENTIFICATION DATA

RFID Reader (Interogator)

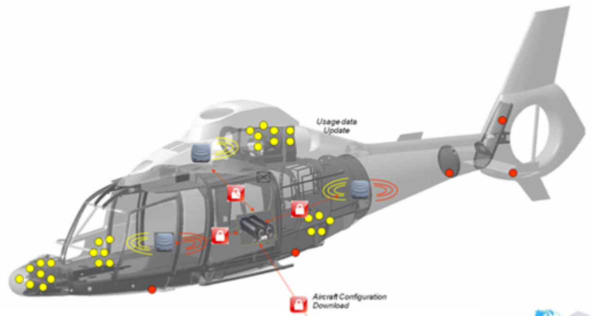
GS1 EPCglobal

Introduction

RFID is used for Safety Applications:

- □ Medicine
- □ Military
- □ Industry

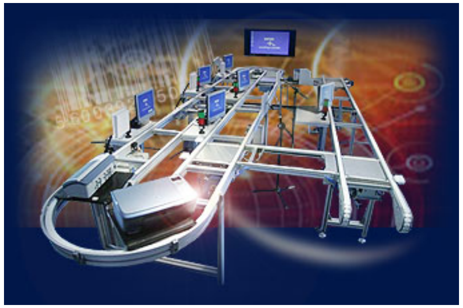
Catastrophic failures



RFID is used for Security Applications

- □ Counterfeiting
- □ Identification
- □ Access Control

Privacy risks



Introduction

Work objectives:

To develop a methodology to:

- ❑ **Design safe and secure RFID tags**
- ❑ **Evaluate RFID tags in complex RFID system**
- ❑ **Evaluate hardware countermeasures**
- ❑ **Evaluate RFID Security Threats**

Outline

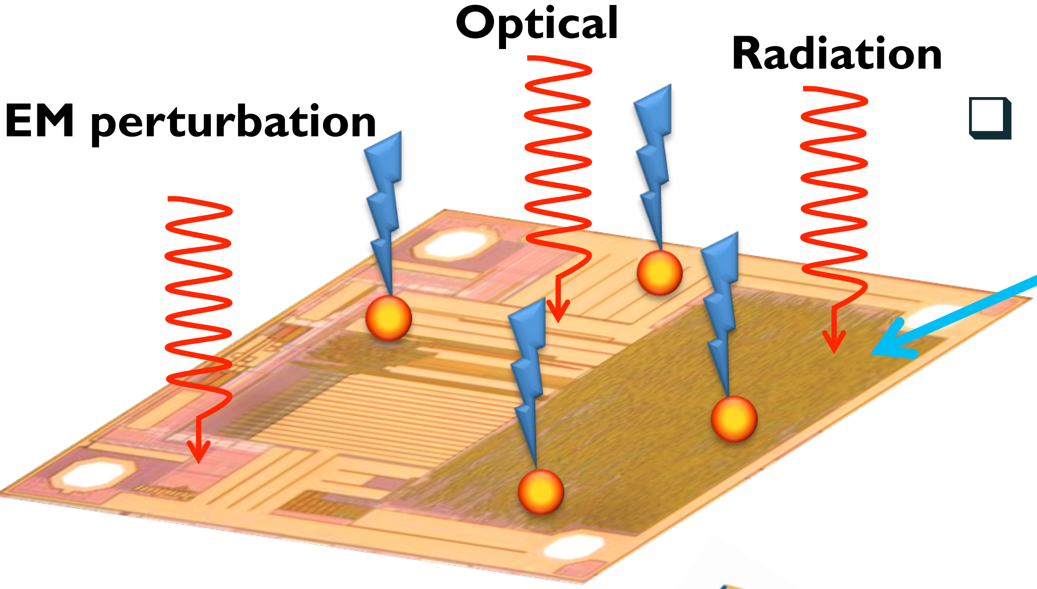
- RFID System and Application
- **EPC GEN2 Security and robustness issues**
- The RFID tag Verification Issues
- RFID IC Emulation system
- The Emulator
- Conclusion and Perspectives

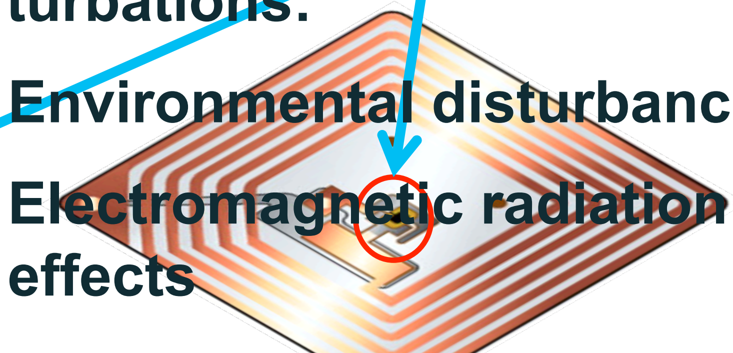
EPC GEN2 Security and robustness issues

Environmental and Intentional Perturbations

RFID system failure

RFID TAG chip

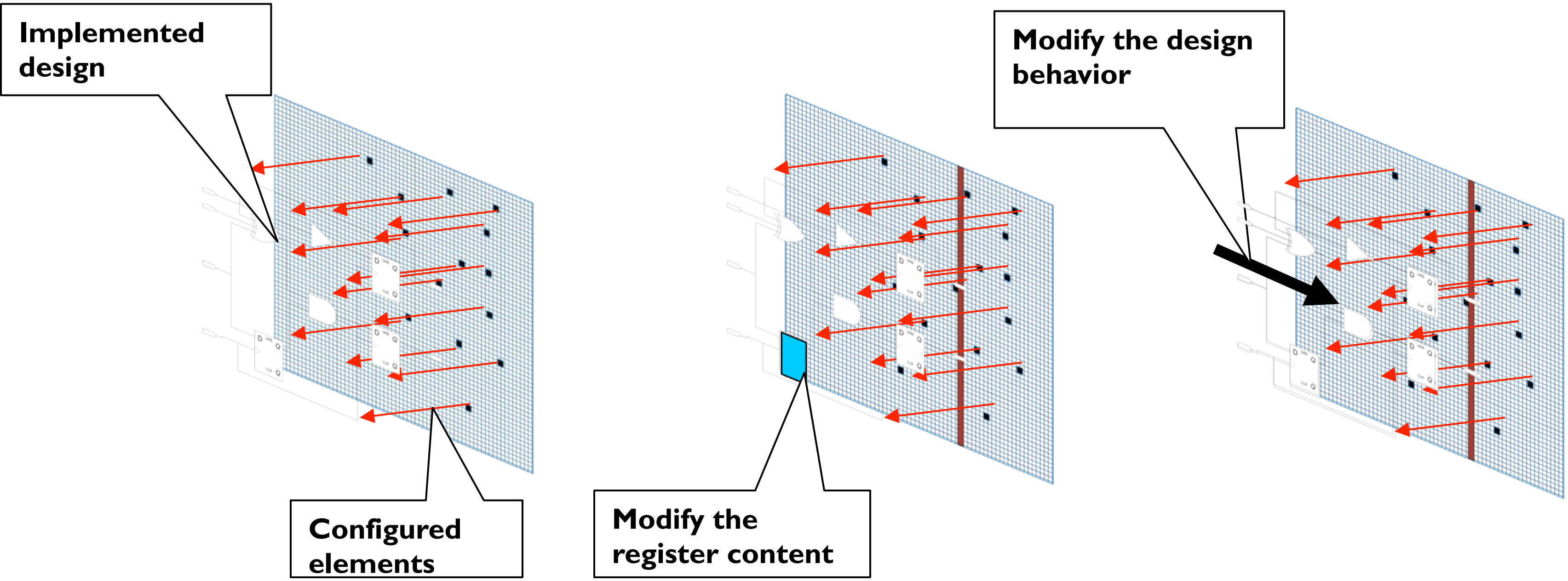




- ❑ Perturbations:
  - ❑ Environmental disturbance
  - ❑ Electromagnetic radiation effects
  - ❑ Optical radiation effects
  - ❑ IC Aging
- ❑ Effects
  - ❑ SEU/MEU
  - ❑ Protocol Errors

Harsh environment

EPC GEN2 Security and robustness issues

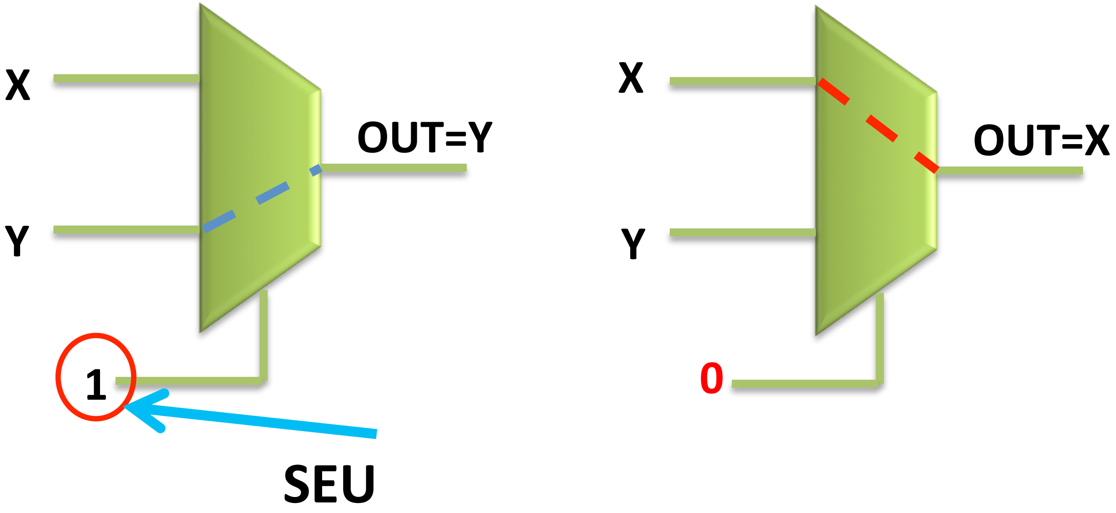


Implemented design

Configured elements

Modify the register content

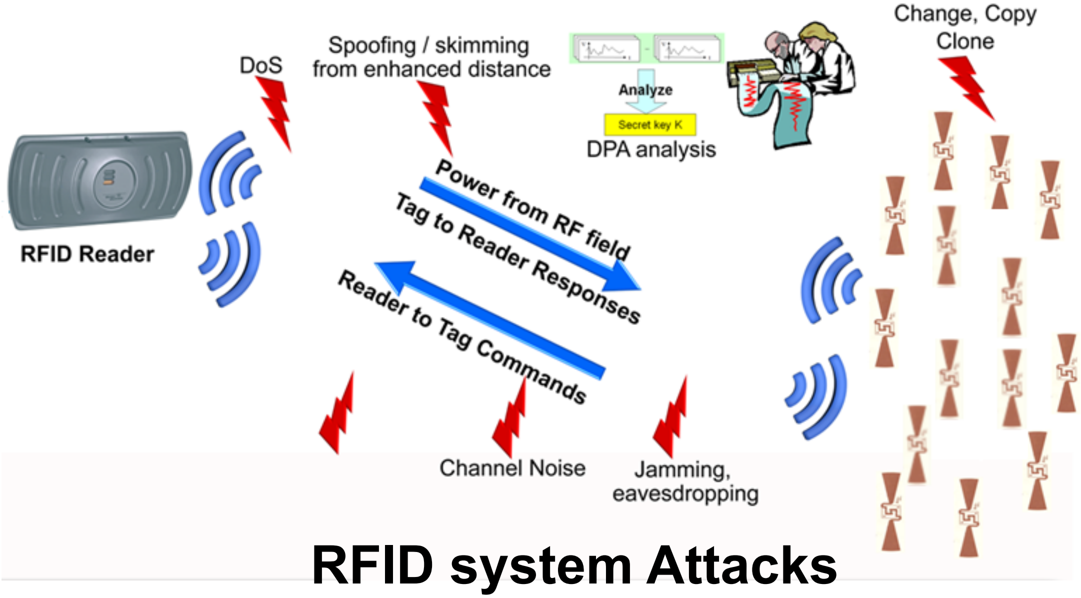
Modify the design behavior



Error effects in Implemented design

EPC GEN2 Security and robustness issues

Security and robustness issues



RFID system Attacks

- ❑ Attacks on the system :
  - ❑ Spoofing, skimming, Denial of Service, Eavesdroping
- ❑ Attacks on the tag:
  - ❑ DPA, Fault Attack, cloning, Memory contents change

Outline

- RFID System and Application
- EPC GEN2 Security and robustness issues
- **The RFID tag Verification Issues**
- RFID IC Emulation system
- The Emulator
- Conclusion and Perspectives

The RFID tag Verification Issues

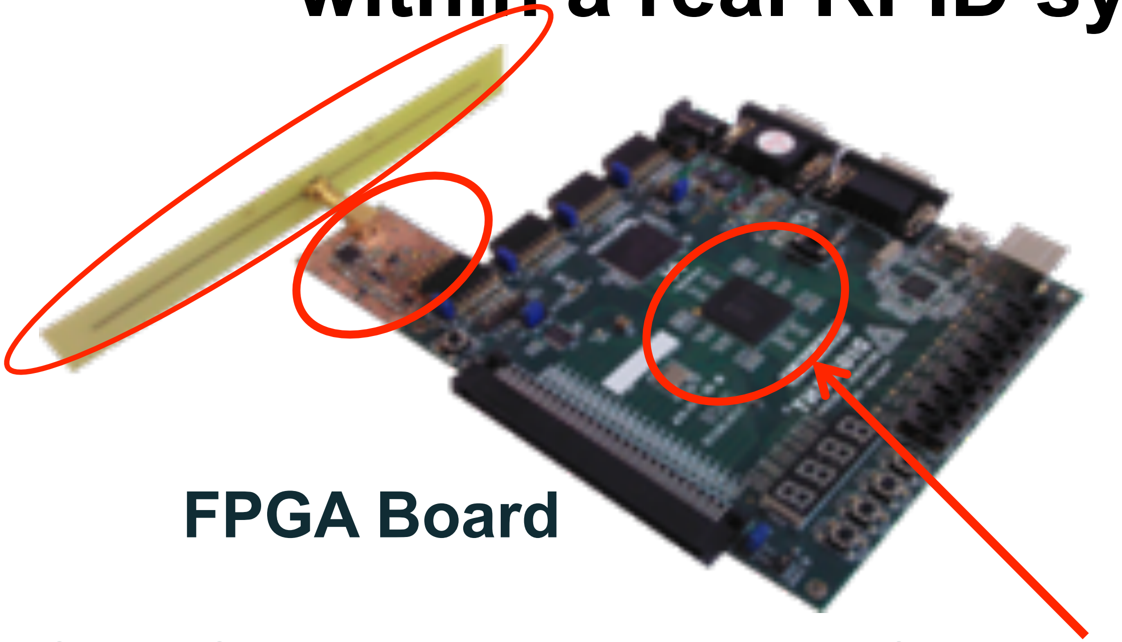
- ❑ **Validation of the tag architecture**
  - ➢ In standalone
  - ➢ Within the whole RFID System
- ❑ **Validation must take into account RFID system specificities:**
  - ➢ Complex and harsh environment
  - ➢ Heterogeneous system considering:
    - ▪ The tag under evaluation
    - ▪ The other elements of the system

Impossible using simulation(many affects)

RFID IC Emulation System

What is the solution ?

RFID prototype to emulate the RFID IC within a real RFID system



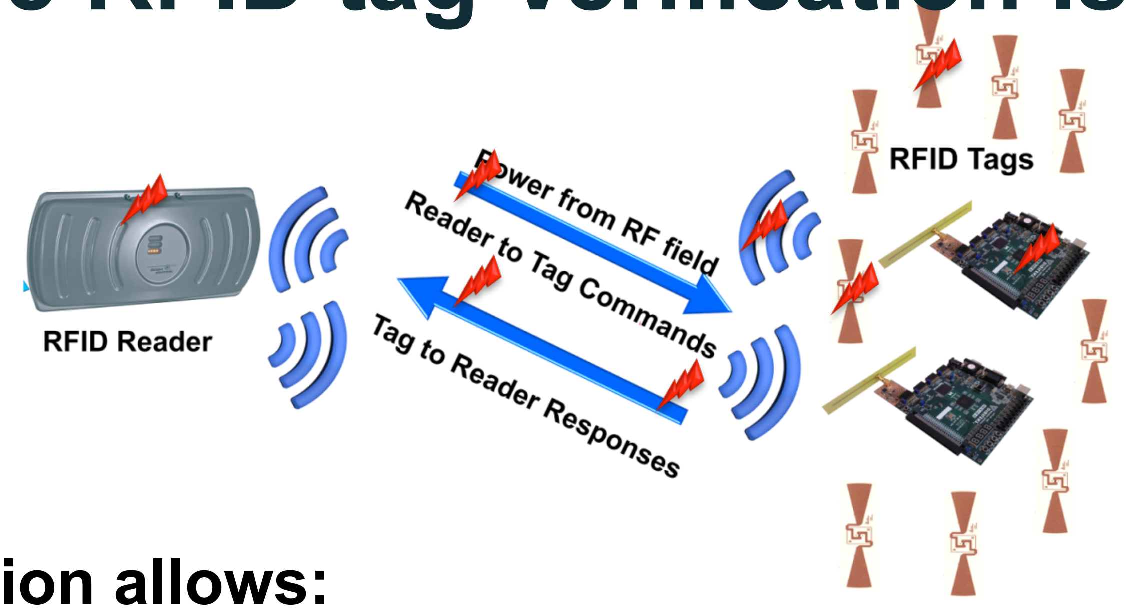
FPGA Board

- □ Antenna
- □ Analog front end
- □ Digital baseband

Perform functional validation of Digital part of RFID IC

Grenoble INP

The RFID tag Verification Issues



- ❑ **Emulation allows:**
  - ❑ **To validate the compliance of the tag against the standard**
  - ❑ **To validate the effect of the faults on the tag**
    - ❑ Considering environmental and intentional errors
  - ❑ **To validate the effect of the faulty tag on the rest of the system**
    - ❑ The application, the other tags (performance degradation, visibility of other tags…)

Outline

- RFID System and Application
- EPC GEN2 Security and robustness issues
- The RFID tag Verification Issues
- **RFID IC Emulation system**
- The Emulator
- Conclusion and Perspectives

RFID IC Emulation System

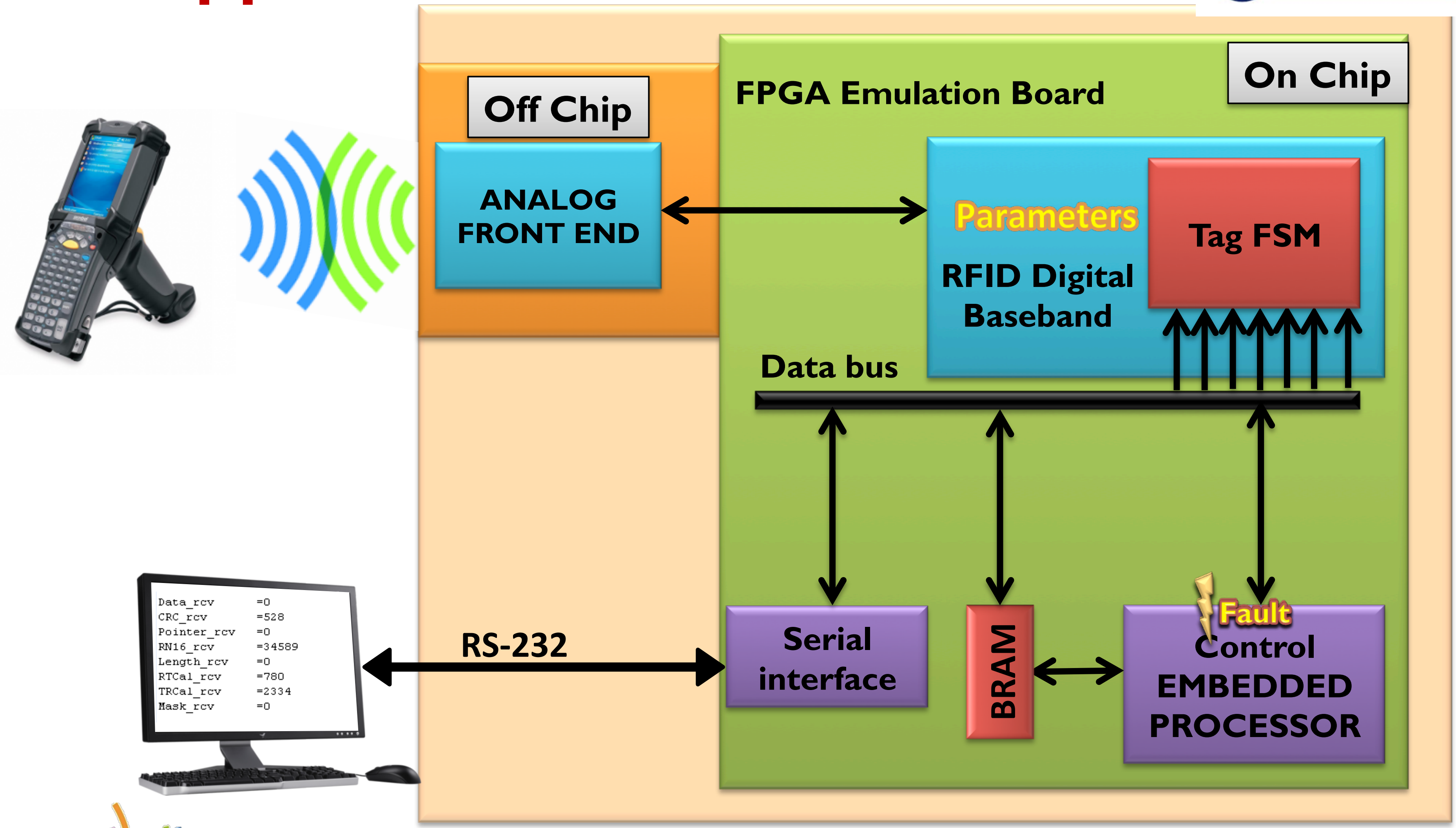
Interests of the emulator:

❑ **On chip monitoring and control of internal tag nodes in order to:**

- ❑ Analyze the data exchange between the reader-tag
- ❑ Emulate fault effects by fault injection(fault model, bit flipping)
- ❑ Identify weakest parts of the architecture

RFID IC Emulation System

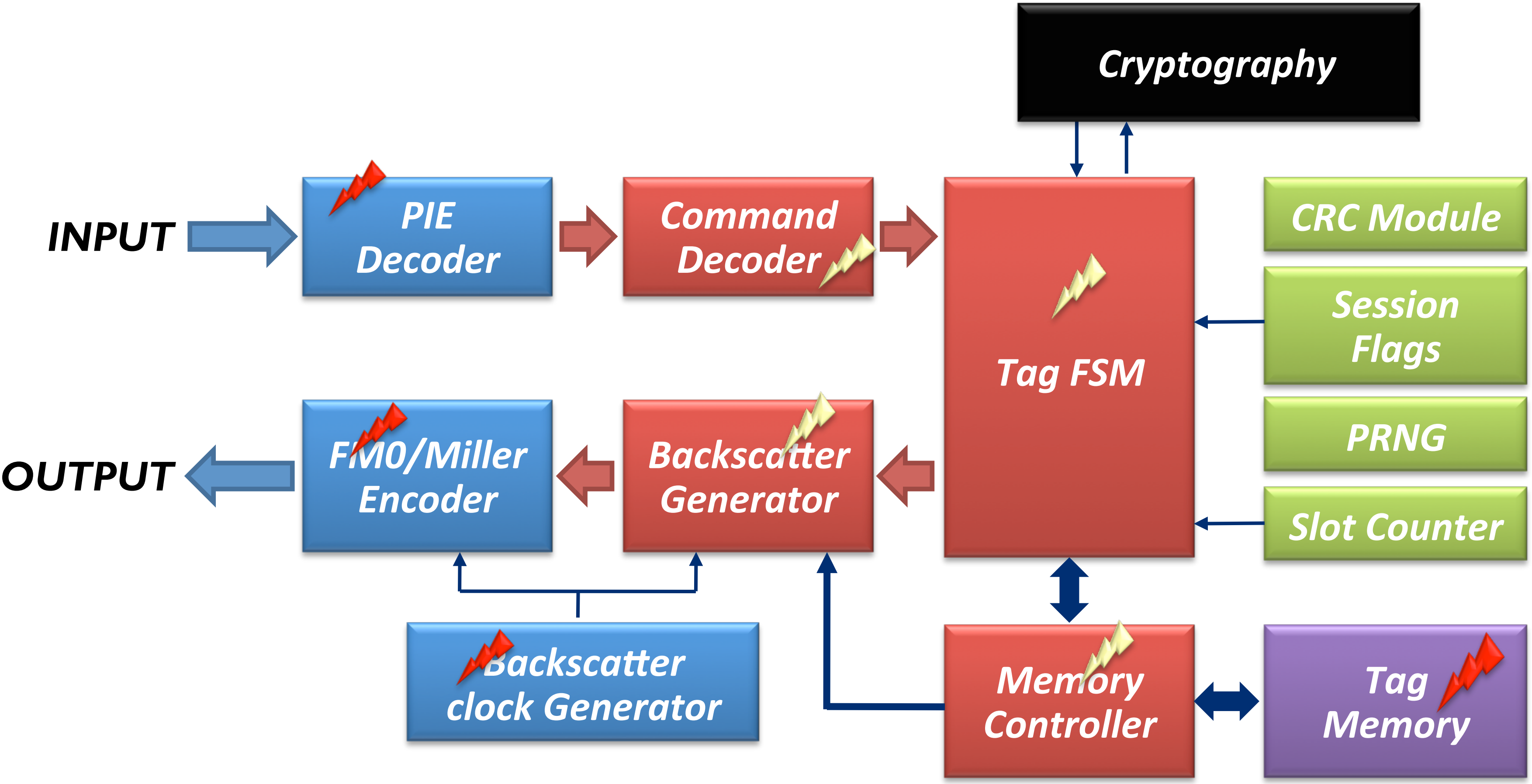
Our approach:



```
Data_rcv        =0
CRC_rcv         =528
Pointer_rcv     =0
RN16_rcv        =34589
Length_rcv      =0
RTCal_rcv       =780
TRCal_rcv       =2334
Mask_rcv        =0
```

Emulation Using embedded processor

RFID IC Emulation System



GS1 EPCglobal

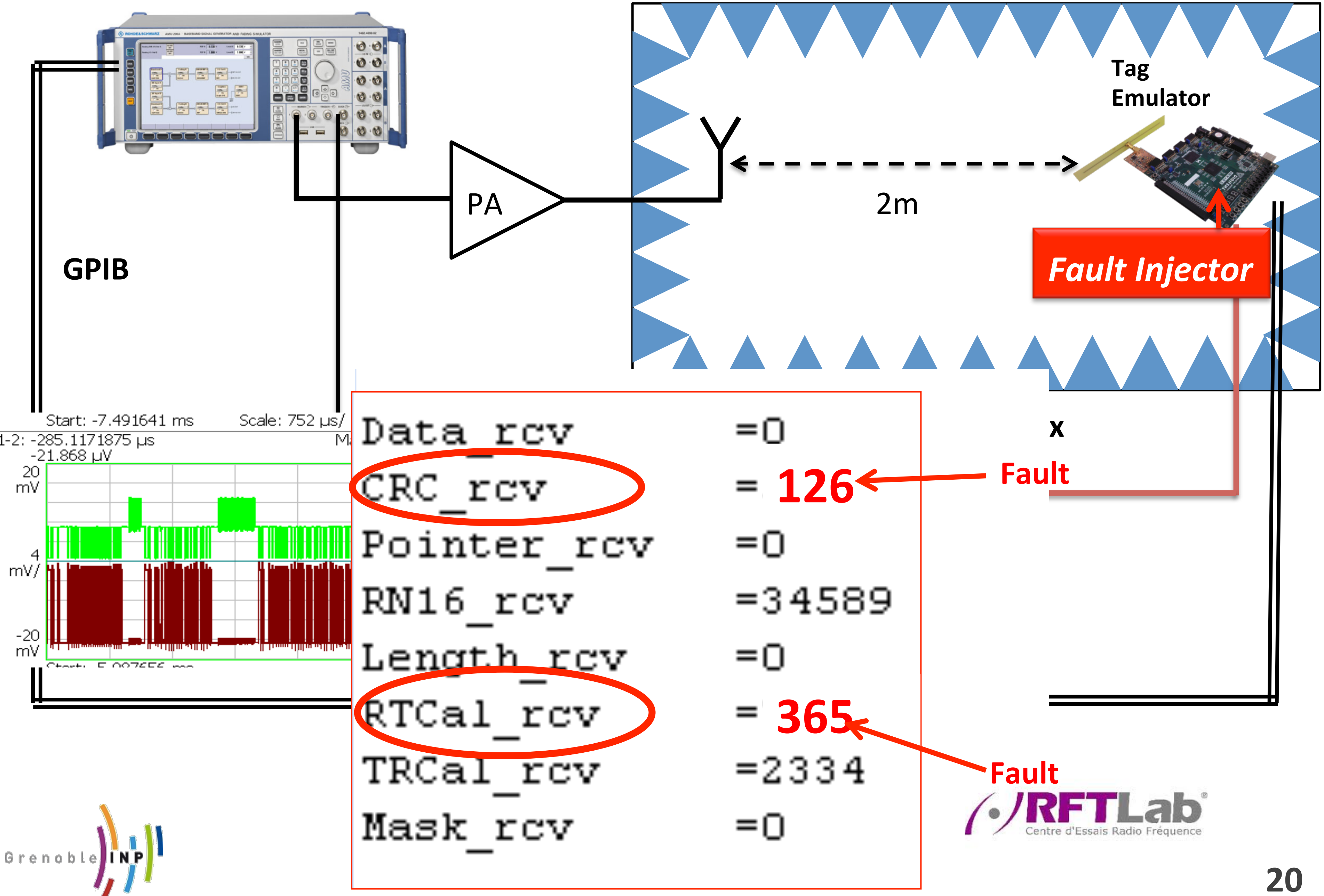
Grenoble INP

RFID Tag Baseband block diagram

Outline

- RFID System and Application
- EPC GEN2 Security and robustness issues
- The RFID tag Verification Issues
- RFID IC Emulation system
- **The Emulator**
- Conclusion and Perspectives

Emulator Validation

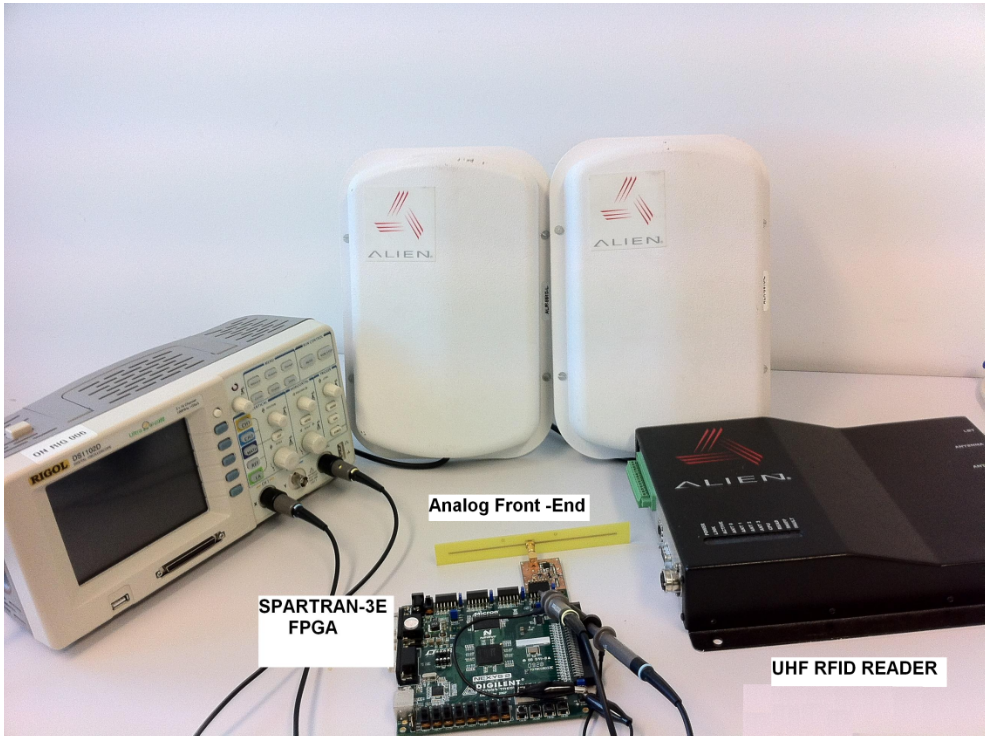


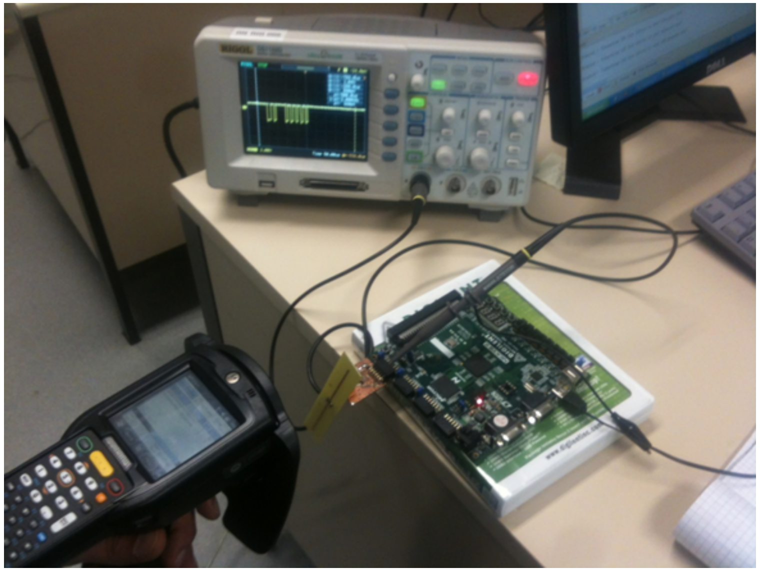
```
Data_rcv        =0
CRC_rcv         = 126
Pointer_rcv     =0
RN16_rcv        =34589
Length_rcv      =0
RTCal_rcv       = 365
TRCal_rcv       =2334
Mask_rcv        =0
```

Grenoble INP

RFTLab
Centre d'Essais Radio Fréquence

UHF RFID TAG emulator





Validation of RFID TAG emulator In anechoic chamber

Outline

- RFID System and Application
- EPC GEN2 Security and robustness issues
- The RFID tag Verification Issues
- RFID IC Emulation system
- The Emulator
- **Conclusion and Perspectives**

Conclusions

- ❑ A validation platform dedicated to RFID IC has been developped
- ❑ The platform can be used to validate security and safety properties at the chip level and the system level
- ❑ This platform allows to take into account the heterogenity of RFID system (simulation of such system is limited)
- ❑ The platform is now completed and validated against the standard.

Perspectives

- ❑ **Identify the weakest and most sensitive elements of a tag.**

- ❑ **Perform faults injection campaigns for a dedicated application in order to evaluate countermeasure at the chip level and the system level**

- ❑ **Define and validate new robust architecture**

- ❑ **Evaluate new security threats**

  - ❑ Work in progress to insert and evaluate hardware trojans within RFID tag.

Thank You

Journées scientifiques 2013 du projet SEmba

SEmba 2013

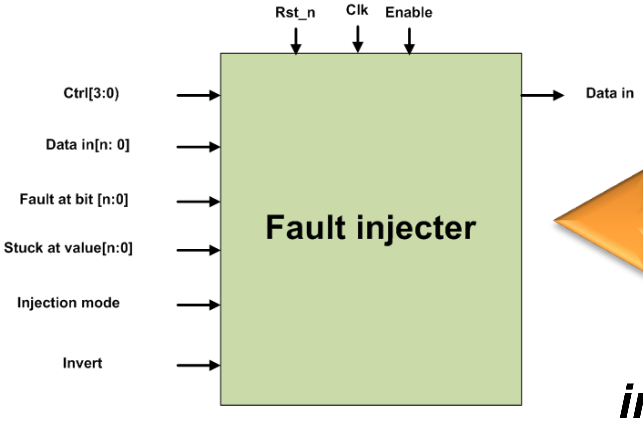
CITI

LCIS
LABORATOIRE
DE CONCEPTION ET D'INTEGRATION
DES SYSTEMES

arc
COMMUNAUTÉS
DE RECHERCHE
ACADÉMIQUE
RhôneAlpes

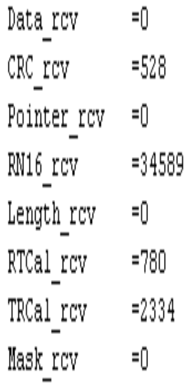
T.I.C. ET USAGES
INFORMATIQUES
INNOVANTS

INNOVATIONS,
MOBILITÉS, TERRITOIRES
ET DYNAMIQUES URBAINES



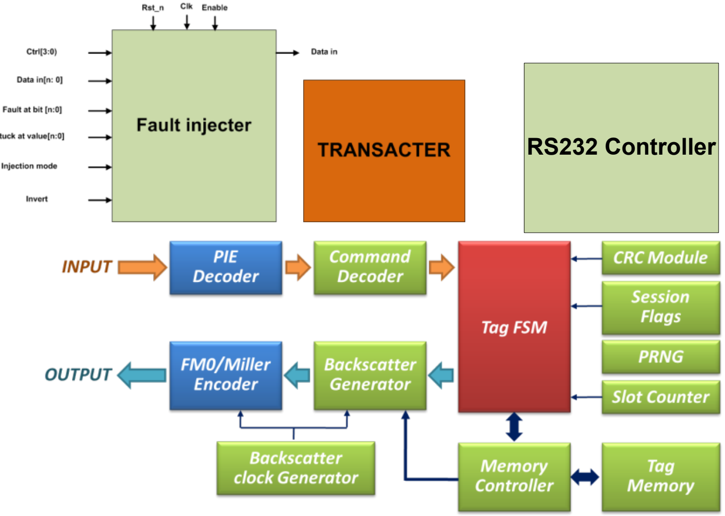
MicroBlaze

Terminal



```
Data_rcv     =0
CRC_rcv      =528
Pointer_rcv  =0
RN16_rcv     =34589
Length_rcv   =0
RTCal_rcv    =780
TRCal_rcv    =2334
Mask_rcv     =0
```

Configuration of fault injector using microblaze

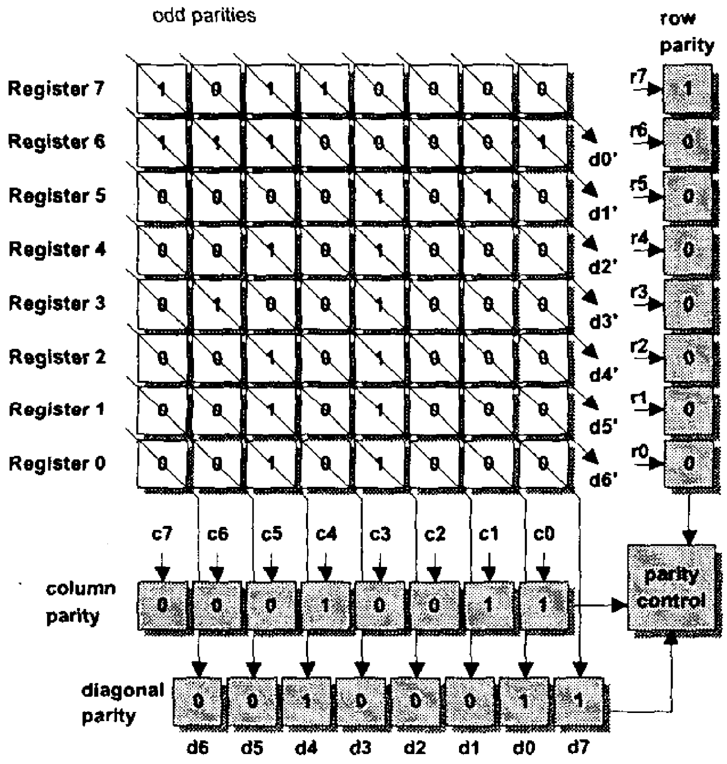


Internal register Information

command file to transacter

command	Reg value

Cross parity check



	c7	c6	c5	c4	c3	c2	c1	c0	row parity
Register 7	1	0	1	1	0	0	0	0	1
Register 6	1	1	1	0	0	0	0	1	0
Register 5	0	0	0	0	1	0	1	0	0
Register 4	0	0	1	0	1	0	0	0	0
Register 3	0	1	0	0	1	0	0	0	0
Register 2	0	0	1	0	1	0	0	0	0
Register 1	0	0	1	0	1	0	0	0	0
Register 0	0	0	1	0	1	0	0	0	0
column parity	0	0	0	1	0	0	1	1	

d6	d5	d4	d3	d2	d1	d0	d7
0	0	1	0	0	0	1	1

FIG. 2: CROSS-PARITY ORGANIZATION FOR REGISTER-FILES