Fault Tolerance Evaluation of RFID Tags

Omar Abdelmalek, David Hély and Vincent Beroulle
omar.abelmaleck@lcis.grenoble-inp.fr

Laboratory of Systems Design and Integration
Grenoble Institute of Technology

14th IEEE Latin-American Test Workshop (LATW 2014)
March 12, 2014
Outline

1. **UHF RFID Systems**

2. **In System UHF RFID IC Emulation with fault injection capabilities**

3. **Experimental Results**

4. **Robustness Enhancement**

5. **Conclusions**
Introduction

- Radio Frequency Identification system

RFID Reader (Interrogator)
Introduction

- Radio Frequency Identification system

RFID SYSTEM Environment

RFID Reader (Interrogator)

RFID TAG

Antenna

Chip

POWER FROM RF FIELD

COMMANDS

IDENTIFICATION DATA
EPC Class-1 GEN2 Protocol

RFID Reader (Interrogator)

POWER FROM RF FIELD

COMMANDS

IDENTIFICATION DATA

Chip

RFID TAG

EPC inventory
EPC Class-1 GEN2 Protocol

(1) Reader Issues a Query

(2) Generate RN16
   Slot = RN16, Execute slot_counter
   If slot = 0: Tag response RN16
   If slot <> 0: No reply

(3) Reder Acknowledges Tag by issuing ACK with the same RN16

(4) If valid RN16: Tag response PC, EPC, CRC16
   If invalid: No reply

EPC inventory
RFID Systems and Critical Applications

• **RFID is used for Safety Applications:**
  - Medicine
  - Military
  - Industry

• **RFID is used for Security Applications**
  - Counterfeiting
  - Identification
  - Access Control
RFID Systems and Critical Applications

• **RFID is used for Safety Applications:**
  - Medicine
  - Military
  - Industry

  \[\text{Catastrophic failures}\]

• **RFID is used for Security Applications**
  - Counterfeiting
  - Identification
  - Access Control

  \[\text{Privacy risks}\]
Motivations

- **UHF RFID IC digital baseband in system emulation with faults injection in order to:**
  - Identify the most sensitive parts of the IC regarding fault effects on:
    - The tag read rate
    - The system performance (i.e. other tag read rates)

- Propose and validate low cost enhancement in order to improve the system performances in a faulty environment
Outline

1. UHF RFID Systems
2. In System UHF RFID IC Emulation with fault injection capabilities
3. Experimental Results
4. Robustness Enhancement
5. Conclusions
RFID Systems are heterogeneous systems, emulation allows to evaluate the tag under design taking into account:

- The protocol implemented within the **READER software**
- The interactions with the **environment**
- The interactions with other...
UHF RFID Emulation: Fault Injection

- The Emulator is instrumented to perform **RT level faults injection**.
- **SEU** Faults are injected into the **14 registers** that store standard parameters.
UHF RFID Emulation: Fault Injection

- The Emulator is instrumented to perform **RT level faults injection**.
- **SEU** Faults are injected into the **14 registers** that store standard parameters.
UHF RFID Emulation: Fault Injection

- The Emulator is instrumented to perform **RT level faults injection**.
- **SEU** Faults are injected into the **14 registers** that store standard parameters.

---

Diagram:
- **Command Decoder**
- **Right Command id register**
- **Single Event Upset**
- **Fault Injector**
- **Tag FSM**
- **Faulty Command id register**

Fault injection configuration
• The Emulator is instrumented to perform **RT level faults injection**.

• **SEU** Faults are injected into the **14 registers** that store standard parameters

---

**Diagram Description**

- **Command Decoder**
- **Tag FSM**
- **Faulty Command id register**
- **Fault injection configuration**
- **Single Event Upset**

**Diagram Elements**

- **Command Decoder** connected to **Fault Injector**.
- **Fault Injector** connected to **Tag FSM**.
- **Single Event Upset** indicated on the **Fault Injector**.
UHF RFID Emulation: Fault Injection

• The Emulator is instrumented to perform RT level faults injection.

• SEU Faults are injected into the 14 registers that store standard parameters

1. RTCAL
2. TRCAL
3. Command
4. DR
5. M
6. CRC5
7. CRC16
8. Slot Counter
9. RN16
10. Trext
11. Query Session
12. Query target
13. Query sel
14. Q
Outline

1. UHF RFID Systems
2. In System UHF RFID IC Emulation with fault injection capabilities
3. Experimental Results
4. Robustness Enhancement
5. Conclusions
Experimental Results

- Faults Injection Campaigns Process

- Experimental Operations:
  1. Measure the fault free tag read rate
  2. Select a tag register as a fault injection target
  3. Measure the faulty tag read rate
  4. Analyze the sensitivity of the register regarding the tag read rate
Experimental Results

- Single Tag Evaluation:

  - UHF RFID Reader
  - UHF RFID Tag Emulation
Experimental Results

- Single Tag Evaluation:
Single Tag Evaluation:

![Bar chart showing experimental results for different tags with and without fault.](image)
Experimental Results:

- Single Tag Evaluation:
  
  - All parameters are not equally sensitive.
  
  - Significant drop in the number of tag reading when the fault injected in:
    
    - RTCAL Register
    - DR register
    - Query session
    - Trext

  - Faults within registers used to compute response frame are the most sensitive
Experimental Results:

- **Single Tag Evaluation:**
Experimental Results:

- **Single Tag Evaluation:**

```
Faulty Backscatter clock
= \frac{DR}{TRCAL}
```

Backscatter clock frequency divider $= \frac{DR}{TRCAL}$
Experimental Results:

- **Multi Tag Evaluation**

  ![Diagram of Multi Tag Evaluation](image)

  - UHF RFID Reader
  - Tag 1
  - Tag 2
  - UHF RFID Tag Emulator
  - Tag 3
  - Tag 4
Experimental Results:

- **Multi Tag Evaluation**

Fault effects on each tags
Experimental Results:

- **Multi Tag Evaluation**

  Fault effects on each tag.

  ![Bar chart showing fault effects on RFID tag evaluation.](chart.png)
Experimental Results:

- **Multi Tag Evaluation**

  - Results corresponding to the faulty tag are similar to the ones obtained in case the tag is alone.
  - Read rate increases for the other tags
Experimental Results:

Multi Tag Evaluation

- Results corresponding to the faulty tag are similar to the ones obtained in case the tag is alone.
- Read rate increases for the other tags

<table>
<thead>
<tr>
<th>Reader</th>
<th>Query</th>
<th>AKN</th>
<th>Rep</th>
<th>Rep</th>
<th>Rep</th>
<th>Rep</th>
<th>Rep</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Slot</td>
<td></td>
<td>Slot</td>
<td></td>
<td>Slot</td>
<td></td>
<td>Slot</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Emulator</th>
<th>RN16</th>
<th>EPC</th>
<th>RN16</th>
<th>RN16</th>
<th>RN16</th>
<th>RN16</th>
<th>RN16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tag 1</td>
<td>RN16</td>
<td></td>
<td>RN16</td>
<td></td>
<td>RN16</td>
<td></td>
<td>RN16</td>
</tr>
<tr>
<td>Tag 2</td>
<td>RN16</td>
<td></td>
<td>RN16</td>
<td></td>
<td>RN16</td>
<td></td>
<td>RN16</td>
</tr>
<tr>
<td>Tag 3</td>
<td></td>
<td></td>
<td>RN16</td>
<td></td>
<td></td>
<td></td>
<td>RN16</td>
</tr>
<tr>
<td>Tag 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RN16</td>
</tr>
</tbody>
</table>
Outline

1. UHF RFID Systems
2. In System UHF RFID IC Emulation with fault injection capabilities
3. Experimental Results
4. Robustness Enhancement
5. Conclusions
Robustness Enhancement

• The most **sensitive registers** have been **identified**
  
  • RTcal => 6 bits
  
  • DR register => 1 bit
  
  • TRext register => 1 bit
  
  • Query session register => 2 bits

• There is only 10 bit to protect

• Simple Hardware **redundancy** is chosen to mitigate the fault effects:
  
  • **3 %** change in the design area

• TMR

• Requires 20 additional flip flops
Robustness Enhancement

TMR Experimental Evaluation

Tag Read Rate with TMR with SEU injection
Outline

1. UHF RFID Systems
2. In System UHF RFID IC Emulation with fault injection capabilities
3. Experimental Results
4. Robustness Enhancement
5. Conclusions
Conclusions

- In system fault injection campaigns have been carried out to analyze chip level fault effect on the system performance taking into account the whole RFID system.

- Experimental results identify the most sensitive part of the design to propose a simple and low cost countermeasure.

- **Future work:**
  
  More experimental results are being processed in order to consider:
  
  1. Other fault models
  2. Other readers (with different protocols)
  3. Larger systems (increasing the number of tags)
  4. Cryptographic protocol
Thank you