Design and emulation of new robust architectures
for UHF RFID Tags

Omar Abdelmalek, David Hely, and Vincent Beroulle
Grenoble Institute of Technology
Valence, France
Email: firstname.lastname@lcis.grenoble-inp.fr

Abstract—RFID ICs such as EPC gen2 tag are low cost tags which can be used for critical or secure applications. Increasing their robustness is not trivial due to the wide range of error sinks (EM perturbation, attacks...). Moreover increasing the robustness must have a minimum impact on the die area but also must fit with a standardized protocol. In this work we propose a design methodology in order to develop hardened EPC architecture with a dedicated verification environment taking into account all RFID system parameter.

Keywords- Fault Injection, RFID Security, RFID attacks, FPGA prototype, Secure IC, Robust IC, EPC.

I. INTRODUCTION

RFID tags are more and more used for critical applications within harsh environments (aeronautics, railways) or for secure applications such as identification, countermeasure against counterfeiting. However, such low cost systems, initially designed for non critical applications with a high volume, are not robust by themselves. For critical applications, a malfunction of RFID chip may have serious consequences or induce a severe security breach for hackers. Dysfunctions can have many origins: for instance, hardware issues can be due to aging effects or can also be due to hackers attack such as optical or electromagnetic fault injection [1]. It is thus a common practice for critical applications to increase the robustness of RFID system thanks to hardware redundancy. Such a method has some drawbacks: it increases the global system cost and adds more and more complexity to the protocol and the associated middleware. Robust tags would then allow limiting the use of redundancy.

The main purpose of this work is to increase UHF tags robustness by proposing a dedicated validation methodology and platform for RFID IC and then new digital architectures of RFID chips which would be resilient against both hardware attacks and natural defects. The work specifically focuses on EPC RFID tags. We will first present the EPC standard, then in a second part of this paper we will present the verification issues due to RFID system, and then we will present the proposed architecture.

II. GEN2 SECURITY AND DEPENDABILITY ISSUES

RFID is a wireless technology that allows for automated remote identification of objects, the major components of an RFID system are tags or transponders that are affixed to objects of interest and readers or interrogators that communicate remotely with the tags to enable identification as depicted in Fig 1.

When a reader antenna transmits radio signals, those signals are picked up by the tags, which answers with a responding radio signal, that signal is then read by the reader’s receiver. Depending on the tag’s computational power, the tag may perform some Logical operation. In this work, we focus on the standardized EPC global Class 1 GEN2 (C1-GEN2) protocol [2], which is the standard for long range identification.

RFID systems are sensitive to perturbations which can deteriorate the global system efficiency by increasing for example the required time needed to perform an inventory of all the tags present in the field of the reader or by making this inventory false. Defects can result from hardware failures of the tag (aging effects are particularly sensitive to harsh environments), but also medium disturbances (for example, electromagnetic bursts). Moreover since RFID systems are used for authentication or traceability such system may be the subject of attack like any other information system managing sensitive data. In [3] RFID attacks are classified in detailed. We distinguish three levels of RFID attacks, based on which part of the system they target: Hardware layer, the Communication layer, and the Back-end layer. The most common is hardware attacks which affect the RFID chip like unauthorized access or modification to the data stored on the tag or sent via the air interface. The attacker can also make a duplicate of the tag, with has the same functionality.

Another threat is the malicious modification of the memory content of the RFID tag, with a view to changing attributes reported by the tag or using the tag as a carrier of malware.

In RFID system we can introduce countermeasures at different levels that increase the confidentiality and integrity of tag data. Measures to prevent the disclosure or modification of tag contents include encryption and access controls. EPC tags
are then modified so that they embed cryptographic capabilities as described in [4]. Also the IC tag can be modified in order to be robust against perturbation with redundancy for instance. An other method is to add specific on line test feature which can be called by the reader in order to test the integrity of the tag. There are others methods to protect against the RFID system failure using on-line test method to secure EPC Protocol [5]. This methods are developed at the system level in order to detect faulty behavior. The heterogeneity of the countermeasures make the validation a challenging step since it may involves hardware, protocol or system software.

III. RFID IC VERIFICATION

RFID IC robustness verification is not a trivial task. Mitigation techniques to increase digital IC robustness can be based on hardware redundancy [6] or also can be done at higher level such as protocol, application... This induces several issues in order to verify the quality of the robustness techniques which are implemented. When validating a robustness solution for RFID it is necessary to measure both its impact on the IC and the system. Indeed specific feature may have incidence on the time needed for a global inventory with several tags. Also, specific features may be added to the tag to increase the robustness but may also need a modification of the reader firmware.

Once robustness strategies have designed it is also necessary to validate the effect against errors. Errors can be induced within the tag or can be due to the environment. It is thus necessary to perform a dedicated fault injection campaign. This fault injection should be able to model SEU within the digital part and the memory of the tag, but also errors within the EPC C1-GEN2 protocol and finally to model electromagnetic errors within the RF field.

Some RFID simulators have been developed to simulate RFID systems and can be used to perform fault injection by altering the communication BER (bit error ratio) [6]. Some emulators have been developed to simulate SEU within a digital description of an IC [7]. In this work we propose an RFID prototyping platform which could be used to emulate an RFID tag within a real system. The prototype should be able to emulate any EPC C1-GEN2 tag and should be instrumented so that: (1) it is possible to inject any errors within the tag, (2) it is possible to spy any part of the tags in order to identify the weakest part of the design.

IV. THE PROTOTYPING PLATFORM

A global view of the verification environment is shown in Fig. 2. This environment consists of a Xilinx Spartan 3a FPGA development board associated to an Analog Front-End (Fig. 3), and a commercial reader. Unlike a standard RFID tag, power and clock will be supplied by the FPGA board.

FPGA emulation provides three major advantages over simulation: (1) proof of compliance with the standard protocol, as we will use an RFID reader known to be compliant, (2) simulation time reduction and (3) in-circuit emulation.

Interfacing tag components with the XILINX Microblaze processor will allow us to read the content of several registers or to inject faults into these registers during operations.

![FPGA RFID platform](image1.png)

![Analog Front-end](image2.png)

V. CONCLUSION

In this work, we propose a design methodology in order to develop hardened C1-GEN2 tag architecture. Our prototype will be validated into real RFID environment. Then, we will perform faults injection campaigns to evaluate and to improve the robustness of the architecture.

REFERENCES