System-Level Simulation for the Dependability Improvement of UHF RFID Systems

Vincent Beroulle, Oum-El-Keir Aktouf, David Hély
Univ. Grenoble Alpes, LCIS
F-26000, Valence, France
e-mail: firstname.lastname@lcis.grenoble-inp.fr

***Abstract*— The SafeRFID project targets the improvement of Ultra High Frequency Radio Frequency Identification (UHF RFID) system dependability using system level simulation and emulation. RFID systems are based on low cost components (tags) more and more often used in critical applications and running in harsh environments (railway, aeronautic, food production, product manufacturing). Defects can have different origins (1) hardware failures, (2) medium perturbations (electromagnetic interferences), or (3) software bugs. The main goals of this project are (1) to develop hardware and software validation environments to validate and evaluate methods for detecting and diagnosing defects within RFID systems, (2) to develop new middleware services to improve the performances of RFID systems in presence of defects and (3) to develop robust tag architectures. This paper sums up all these complementary solutions which have been validated thanks to system level simulation and emulation and which have been integrated in a global dependable UHF RFID system. The results of this work are (1) the design of a robust middleware and of (2) a hardware tag and (3) the evaluation of the dependability of such global RFID systems thanks to system level simulation and emulation.**

Keywords*— *RFID; system level simulation; dependability; middleware; tag architectures

I. INTRODUCTION

In critical domains, RFID system errors can have catastrophic consequences in terms of human safety whereas in high quality applications, they can have economic consequences for product quality, manufacturing costs, etc. Monitoring RFID systems, which are based on low cost and uncertain components, is thus a must in order to perform on-line detection of failures. These failures can result from hardware malfunctions (aging effects are particularly sensitive to harsh environments), medium disturbances (for example, electromagnetic bursts), or software bugs. For example, these failures can be due to a broken or a misplaced antenna, RF interferences, low signal strength, middleware dysfunctions, etc. Therefore, the main goal of the SafeRFID project is to propose a global strategy for the simulation of RFID system in order to develop and evaluate the on-line detection and diagnosis of defects in UHF RFID systems in order to enhance the RFID systems dependability.

The objectives of existing RFID middlewares are especially to manage various data sources in RFID systems and process large amount of raw data. Some of them also provide error fixing mechanisms such as WinRFID [5]. Other RFID middlewares focus on a reliable integration of RFID technology into existing applications (SunRFID [6], FlexRFID [7]). Fault-tolerance is taken into account in the RFID middleware [8] by detecting abnormal behavior of the system. However in these middleware no low level information (physical information) coming from each reader measurements are mixed with the high level information gathered by the numerous readers in the system.

The classical RFID system on-line monitoring methods are based on reader performances monitoring. In fact, to detect component or environment failures and defects, many performance parameters of the reader can be observed. The classical performance parameters observed are the Average Tag Traffic Volume (ATTV) and the Read Errors to Total Reads (RETR) [4]. ATTV allows determining unusual tag traffic which is a symptom of a faulty system. For instance, if between 8:00am and 11:00am a reader usually reads 100 tags/hour every day and if one day, during the same period, the same reader reads only 50 tags/hour, then it can be assumed that a failure or a disturbance has occurred. The second parameter RETR consists of counting erroneous reads over the total read attempts (correct and faulty) of a specific reader. High RETR means there is probably a problem. The evolution of this RETR can also be analyzed. These methods can also be used as final optimization approaches during RFID system deployment.

In order to validate RFID systems during design phases, several RFID simulators have been proposed in the literature [2][3][11], but none of them focuses on the RFID systems dependability evaluation. These simulators allow simulating the communication protocol between the tags and readers or the interactions between the readers and middleware. Thus, designers generally use these simulators to perform a functional verification of their systems. For instance, Rifidi [1] only fits with RFID system deployment issues; fault simulation with Rifidi would be unrealistic. RFIDSim [3] is a complete RFID simulator; nevertheless its main goal is to evaluate RFID protocols and tag hardware characteristics are not modelled.

This paper gathers the results of the SafeRFID project. This project integrates in the same RFID system complementary and multi-level solutions for improving the system dependability. These solutions target the improvement (1) of the tags hardware architecture, (2) of the readers fault detection capability and (3) of the middleware for multi-readers RFID systems fault diagnosis. In this context, our three main results are: (1) two new validation environments, a simulator and a FPGA-based emulation platform allowing hardware and software RFID systems co-design and fault simulation; (2) new on-line test and diagnostic services for RFID middleware, and (3) a new tag robust architecture.

 ISBN: 978-1-61208-514-2

The next sections of this article are organized as described in the following. In Section II, two new RFID validation environments are described. The first one is a system level simulator which is capable of performing fault injection. The second one is an emulation platform (based on FPGA), which is also capable of both performing hardware fault injections and monitoring its internal signals. Section III presents two test and diagnosis methods, which have been implemented and validated thanks to these simulators or emulators. This section also describes the robust tag architecture developed within the SafeRFID project. Section V includes the conclusions of the article.

II. VALIDATION ENVIRONMENTS

This section describes the two validation environments which have been developed for the purposes of the SafeRFID project. These two environments allow (1) the validation of software and hardware RFID components and (2) RFID system robustness thanks to fault injection. The first validation environment is a complete RFID System Level Simulator. The second one is a RFID emulation platform allowing modelling and evaluating tag IC digital architecture into actual RFID Systems. These two validation environments are compliant with the RFID UHF EPC Class 1 Gen 2 standard.

A. SERFID Simulator: a virtual validation environment

"Simulation and Evaluation of RFID Systems" (SERFID) is a UHF RFID systems simulator. It permits to evaluate RFID systems robustness thanks to fault simulation. It models the whole RFID system including the numerous hardware tags and readers and their electromagnetic environment. An Ethernet interface is plugged to the simulator so that SERFID can be controlled by a distributed middleware, as real readers usually are. Thus, SERFID allows validating and optimizing middleware implementation. Fig. 1 illustrates a SERFID high level view containing several readers and tags.

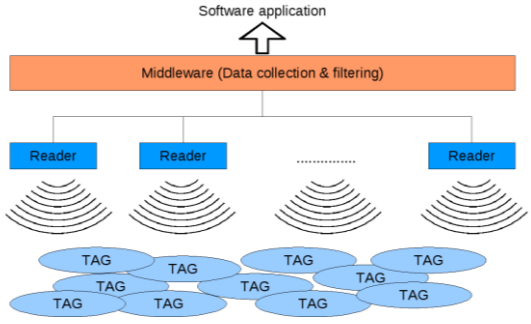

Figure 1. SERFID high level view model with several readers and tags

SERFID has been developed using the C++ SystemC library, which is adapted to both hardware and software components modeling. SERFID models the communication links between each tag and reader using high level functional models (Timed Transaction Level Model). The communication links between tags and readers have been divided into 2 parts. This distinction allows the injection of global defects affecting all the tags and readers and the injection of local defects affecting only one tag/reader couple. For example, the fault injection allows parametric variations on the Bit-Error-Rate (BER) of the global or local communication links. More details on this simulator are given in [9].

B. RFIM: an emulation platform

In order to evaluate tag digital baseband architectures, simulation is limited, since this requires low level (at least register transfer) time accurate simulation. Emulation is then an appropriate tool in order to evaluate tag digital baseband architectures taking into account the whole RFID system. 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 with this standard, (2) simulation time reduction and (3) in-circuit emulation. In-circuit emulation provides also the opportunity to inject errors within the tag to evaluate its effects within the tag and the system. This emulator aims at emulating all type of errors which can occur within the digital baseband in order to provide a tool for robustness evaluation and countermeasure validation. This emulator also allows monitoring the internal tag behavior which helps to understand fault propagation within the design. Moreover, the proposed monitoring system included into the emulator provides a convenient and powerful tool to analyze system behaviors. The emulator embeds a fault injection mechanism to validate the dependability of the IC. Errors are explicitly induced by the deliberate introduction (injection) of faults into the system. An emulation platform, the so called RFIM (RFID Fault injection and Monitoring) with fault injection capability has then been described in [10]. This FPGA based emulator is made of an UHF RFID tag with on chip faults injection mechanism.

As shown in Fig. 2, the RFIM platform is divided into eight modules: monitoring interface, fault injector, activation of injection, event detector, golden and instrumented faulty tags, register comparator and embedded microprocessor. The embedded microprocessor controls all the platform modules and then permits to perform on-line tag monitoring and to play on-line fault attacks. The processor allows the on-line capture of data in the two tag basebands for analyzing the RFID communication. The interface monitoring is a mechanism that transports the internal register values from the tag basebands to the microprocessor. This monitoring interface block uses a First-In-First-Out (FIFO) memory in order to compensate the latency of the microprocessor for outputting register values. Faults are only injected in the faulty tag. The golden tag, which is always fault free served as a reference. The register comparator compares all the internal registers of the golden and the faulty tags. This comparison helps the embedded processor to detect and to localize faults and errors in the faulty tags.

Our prototype has been validated into real RFID environment. It allows both observing and controlling the internal tag parameters and data. Thanks to these capabilities, the emulator can help designers to evaluate different digital IC architectures.

This evaluation concerns, on one hand, the validation of the tag robustness against environmental aggressions and, on the other hand, the validation of the tag security against human

 ISBN: 978-1-61208-514-2

attacks. These validations can be performed into real RFID system, using commercial readers and other commercial tags.

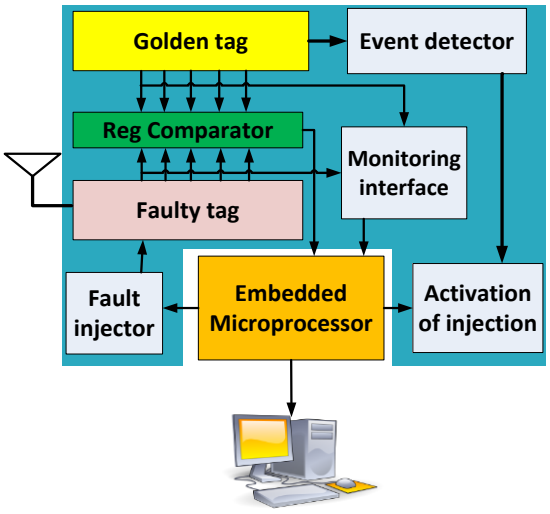

Figure 2. RFIM platform for faults injection and monitoring

This allows quick and accurate validation taking into account all the complex physical effects involved into RFID systems. The spying capabilities of the emulator gives us an opportunity to study some types of attacks on RFID system, to detect malicious hardware, which disturbs the security of this technology and to design and to validate solutions for robust and secure architectures.

III. TEST AND DIAGNOSIS METHODS AND TAG ROBUSTNESS ENHANCEMENT

This section describes the three main approaches which have been proposed by the SafeRFID project in order to improve UHF RFID system dependability. Each approach is embedded on a specific part of the RFID system: the reader, the middleware and the tag digital architecture.

A. *Profile test method*

The Profile test method is inspired by classical monitoring techniques (ATTV, RETR), which are based on reader performances monitoring. This method, as the classical monitoring methods are, is nonintrusive. In this method, we propose to measure and compare individual tags performance indicators rather than a single global average parameter. To do this, we define a new performance metric - called read rate profile – individually involving all the tags of the population rather than an average value computed for the same population.

The initialization of our monitoring method requires computing the statistical parameters of the fault free inventory read rate profiles. Let us first explain what these inventory read rate profiles are. Each tags inventory leads to a specific inventory read rate profile, which is the ordered read rate curve of the entire tag population. The '-'curve in Fig. 3 represents the inventory profile of a fault free inventory occurrence. Then, from all these initial inventory profiles, an average read rate profile is computed. This average profile is represented by the bold curve in Fig. 3. The second step for the initialization of our approach consists in computing a threshold for the failure detection. This threshold, called limit profile, is represented by the '+'curve in Fig. 3. An inventory profile with one or more tag read rates under this limit implies that the RFID system is considered faulty. The '•'curve in Fig. 3 illustrates a faulty inventory profile with several points under the limit. The limit profile is computed using the average profile and the standard deviation of each ordered tags. Details on this test approach are given in [11] [12] [13].

B. *SafeRFID-MW: a middleware for On-Line Testing and Diagnostic*

The proposed Profile testing method, as well as most existing test methods (RETR, ATTV, etc.), operates mainly at the reader level. These local results are not capitalized for global processing of errors at the whole system level. Consequently, in case of distributed RFID systems based on several readers, there are no means to determine the whole system state. In our work, this issue has been solved by developing a special RFID middleware that integrates not only testing operations at the level of each reader, but also diagnosis processes at the middleware level. Our middleware called SafeRFID-MW implements a diagnosis algorithm called RFID_Diag_Algo. This algorithm uses the basic idea of probabilistic diagnosis developed in the work of Fussel and Rangarajan [14] on multiprocessor systems. Nevertheless, the fault model, as well as the diagnosis operations has been largely adapted to the RFID constraints. RFID_Diag_Algo algorithm performs three steps: i) reader partitioning in groups according to some criteria issued by the application (i.e., which readers, read the same groups of tags), ii) read rate result comparison in a way that ensures a consensus on faulty components, whether readers or tags, iii) evaluation of the diagnosis accuracy by applying a new probabilistic model suitable to such systems. Details of this algorithm are presented in [15][16].

Although Low Level Reader Protocol (LLRP) is a complete communication protocol that allows notifying communication errors between the middleware and the readers, the LLRP protocol cannot detect failures due to reader misconfigurations or some runtime conditions. It can neither determine error causes. Therefore, it is not suitable as it for use in applications where demands for dependability are critical, especially as the tag-reader interface is very sensitive to external perturbations and may present a random behavior. In the SafeRFID project, the LLRP protocol has been extended to take into account errors [17].

 ISBN: 978-1-61208-514-2

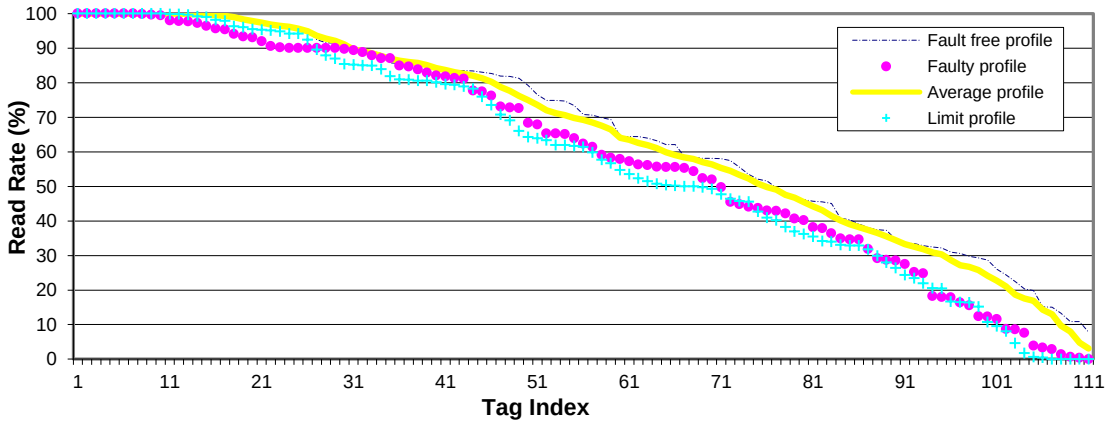

Figure 3. Average, limit, fault free and faulty inventory profiles

A prototype of the SafeRFID-MW has been developed using the Java language. Different implementations of the probabilistic diagnosis have been analyzed, and we have shown which one is better according to the running environment and the objectives of the end user [17].

C. Tag Robustness Enhancement

Thanks to RFIM, the most sensitive parts of the tag digital baseband architecture have been identified through fault injection campaigns. The fault injection campaigns consist in measuring for a given period the number of times the tag is detected by a reader while faults are injected in a part under analysis. This experiment has also been done when several tags are in front of the reader in order to evaluate the faulty tag effects on other tags. The experiments have been carried out on all registers of the digital baseband in order to identify the most sensitive ones. Experimental results [19] show that only a few registers dramatically decrease the system performance (i.e., the tag read rate). Fig. 4 hereafter gives the influence of the fault injection on the number of times the tag has been successfully identified. Light gray gives the value in case no faults are injected; dark gray gives the resulting number in case faults have been injected within the parameters given in horizontal axis.

At a first glance, we can see that all parameters are not equally sensitive. While some faulty parameters reduce the number of times the tag has been identified from 4500 to less than 500, other ones have a very limited influence on the tag response. This can be explained by the role played by the parameter during an inventory round, and the refreshment rate of the value during the same round.

We have proposed in a first approach to use hardware redundancy to decrease the fault effects. A Triple Modular Redundancy (TMR) has been applied on the most sensitive registers identified thanks to the fault injection campaigns. Since the tag digital baseband architecture is powered wirelessly and has a limited resource, the TMR was chosen to protect the most sensitive registers only. Moreover such registers are very small which makes the cost acceptable. As shown in Fig. 5, the TMR [4] technique consists on the triplication of the target component to protect.

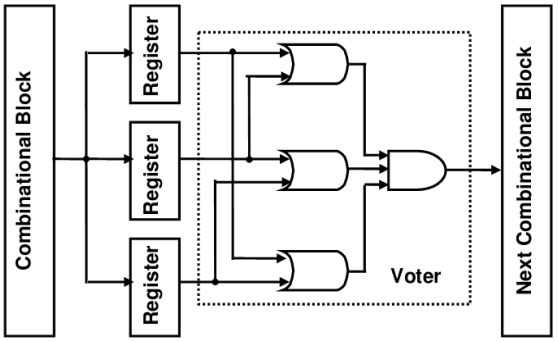

Figure 5. Triple Modular Redundancy Protection

The three resulting outputs from triplication are connected to a voter block that compares the three received data and elects that of majority. If one of the three components fails or suffers a direct SEU. TMR technique implies an area increase of the redundant part of more than 200% due to the component triplication. It also needs a voter that is implemented just with some OR and AND gates for each bit of the triplicated component. We have experimentally noted that the use of this TMR, improves the read rate in the presence of faults into sensitive registers. The proposed protection only adds 30 flip-flops to the whole circuit. TMR although expensive is in this case an acceptable method since thanks to the fault injection campaigns the most sensitive elements have been identified in a real RFID context, limiting the TMR use to only a few bits.

We have also proposed and validated a complementary approach allowing fault detection and diagnosis. This approach consists in adding hardware checkers into the tag circuit. Some of these checkers are provided by the synthesizable assertions available in the Open Verification Library library (OVL) and others are designed to monitor tag finite state machine transitions. The faults detected by the checkers are counted and saved within the tag memory.

 ISBN: 978-1-61208-514-2

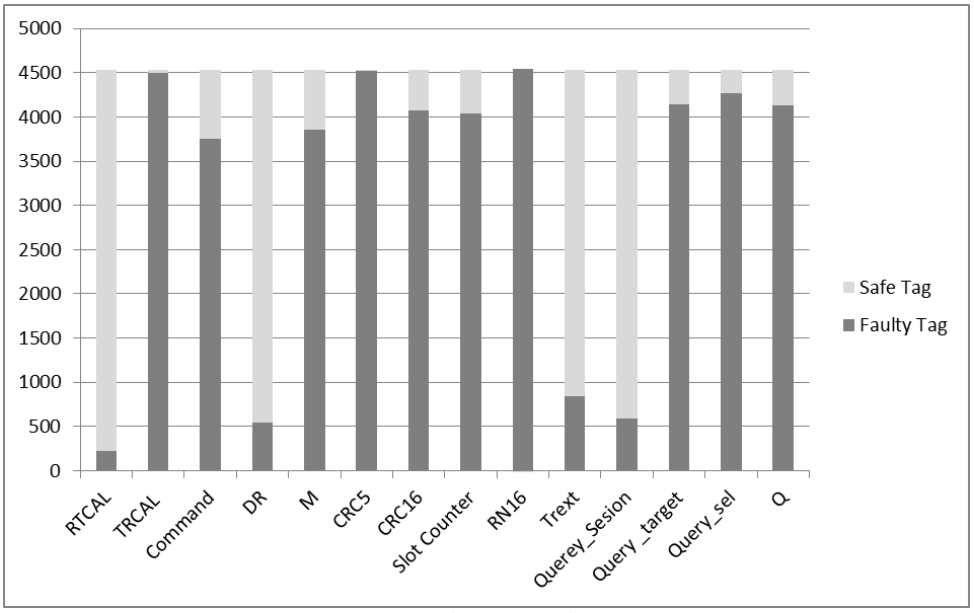

Figure 4. Successful Tag Identifications

Then, a user can read this information through the RFID reader and thereafter acquire diagnosis information. This approach has been implemented and evaluated on RFIM. Details on these robust architectures are given in [19] [11].

IV. CONCLUSION AND FUTURE WORK

The SafeRFID project addresses the dependability issues in RFID systems. The proposed framework considers both hardware and software components as well as analog and digital aspects of RFID systems. Three main layers have been identified: the hardware layer with tags and readers, the communication layer represented by the LLRP protocol and the software layer including the RFID middleware. The main results of this work are: (1) the development of a fault simulator (SERFID) and of an FPGA based emulator (RFIM) that allows fault injection and test method evaluations, (2) the design and implementation of a robust LLRP-compliant RFID middleware prototype that provides fault detection and diagnosis new services, and (3) the development of a tag robust architecture with self-diagnosis capability.

ACKNOWLEDGMENT

This work has been supported by the French National Research Agency project “SafeRFID” [ANR 2010 JCJC 0305 01]

REFERENCES

[1] C. E. Palazzi, A. Ceriali, and M. Dal Monte, “RFID Emulation in Rifidi Environment”, in Proc. of the International Symposium on Ubiquitous Computing (UCS'09), Beijing, China, Aug 2009.

[2] C. Angerer, R. Langwieser, “ Flexible evaluation of RFID system parameters using rapid prototyping”, RFID, 2009 IEEE International Conference on Digital Object Identifier: 10.1109/RFID.2009.4911188 Publication Year: 2009 , Page(s): 42 – 47

[3] C. Floerkemeier, S. Sarma, “RFIDSim—A Physical and Logical Layer "Simulation Engine for Passive RFID “ Automation Science and Engineering, IEEE Transactions on Volume: 6 , Issue: 1 Digital Object Identifier: 10.1109/TASE.2008.2007929 Publication Year: 2009 , Page(s): 33 – 43

[4] F. Thornton, “How to Cheat at Deploying and Securing RFID”, Syngress Publishing ©2007, ISBN 1597492302 9781597492300

[5] R. Shorey et al., Mobile, Wireless and Sensor Networks : Technology, Applications and Future Directions, Chapter “WinRFID – A middleware for the enablement of Radio Frequency Identification (RFID) based Applications” B. S. Prabhu et al., John Wiley and Sons Inc., 2006.

[6] Sun Microsystems, Inc., "Sun Java™ System RFID Software 3.0 Administration Guide," February 2006.

[7] A. Sengupta, S. Z. Schiller, “FlexRFID: A design, development and deployment framework for RFID-based business applications”, Information Systems Frontiers, vol. 12, n° 5, pp. 551-562, November 2010

[8] N. Ahmed, “Reliable Framework for Unreliable RFID Devices” 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), Mannheim, 2010

[9] G. Fritz, V. Beroulle, O-E-K. Aktouf, and D. Hély, “SystemC Modeling of RFID Systems for Robustness Analysis”, 19th International Conference on Software, Telecommunications and Computer Networks IEEE SoftCOM 2011Split - Hvar - Dubrovnik, September 15 – 17, 2011, IEEE Catalog Number: CFP1187A-CDR; ISBN 978-953-290-027-9

[10] O. Abdelmalek, D. Hély, and V. Beroulle “Fault Tolerance Evaluation of RFID Tags”, in IEEE Latin America Test Workshop (LATW 2014), Fortaleza, Brésil, 13-16 March 2014

[11] G. Fritz, V. Beroulle, O. Aktouf, M. D. Nguyen, and D. Hély, “RFID System On-line Testing Based on the Evaluation of the Tags Read-Error-Rate”, Journal of Electronic Testing: Volume 27, Issue 3 (2011), Page 267-276, (DOI: 10.1007/s10836-010-5191-6).

 ISBN: 978-1-61208-514-2

[12] G. Fritz, B. Maaloul, V. Beroulle, O-E-K. Aktouf, and D. Hély, "Read rate profile monitoring for defect detection in RFID Systems", IEEE International Conference on RFID-Technologies and Applications (RFID-TA 2011), , pp. 89-94, Sitges, Barcelona, Spain, on September 15-16, 2011, IEEE catalog number: CFP11RFT-CDR ; ISBN: 978-1-4577-0026-2

[13] G. Fritz, V. Beroulle, O-E-K. Aktouf, and D. Hély, "Evaluation of a new RFID system performance monitoring approach", Design, Automation & Test in Europe, (DATE 2012), interactive presentation, Dresden, Gremany, 12-16 march 2012

[14] D. Fussell, S. Rangarajan, "Probabilistic diagnosis of multiprocessor systems with arbitrary connectivity", IEEE 19th International Symposium on Fault-Tolerant Computing, FTCS-19. Digest of Papers., Chicago, IL, pp. 560-565, 1989.

[15] R. Kheddam, O. Aktouf, and I. Parissis, "Saferfid-mw: Safe and Fault-Tolerant rfid Middleware", R. Kheddam, O. Aktouf, I. Parissis, Journal of Communications Software and Systems (jcomms), Special issue on rfid Technologies and Internet of Things, Vol. 9, n° 1, mars 2013, pp. 57-73.

[16] R. Kheddam, O. Aktouf and I. Parissis, "On-line monitoring and diagnosis of rfid readers and tags", 20th ieee International Conference on Software, Telecommunications and Computer Networks (softcom 2012), Split, Croatia, 11-13 september 2012, pp. 1-9.

[17] R. Kheddam, O. Aktouf and I. Parissis, "An extended llrp model for rfid system test and diagnosis", 8th Workshop on Advances in Model Based Testing (a-most 2012) dans le cadre de 5th ieee International Conference on Software Testing, Verification and Validation. Montreal, Canada, 17-21 april 2012, pp. 529-538.

[18] R. Kheddam, O. Aktouf, I. Parissis and S. Boughazi, " Monitoring of rfid Failures Resulting from llrp Misconfigurations", 21st ieee International Conference on Software, Telecommunications and Computer Networks (softcom 2013), Split, Croatia, septembrer 2013, pp. 1-6.

[19] O. Abdelmalek, D. Hély, and V. Beroulle "Emulation of Faults Injection on UHF Transponders", in 17th IEEE Symposium on Design and Diagnosis of Electronic Circuit and System (DDECS 2014), Warsaw, Poland, 23-25 April 2014

[20] I. Mezzah et al., "Assertion based on-line fault detection applied on UHF RFID tag", 8th IEEE International Design & Test Symposium 2013, Maroc (2013)

 ISBN: 978-1-61208-514-2