Read-Error-Rate evaluation for RFID system on-line testing

G. Fritz, V. Beroulle, M.D Nguyen, O. Aktouf, I. Parissis
Grenoble Institute of Technology
LCIS, 50 rue B. de Laffemas BP54 26902 VALENCE Cedex 9 FRANCE
firstname.name@ lcis.grenoble-inp.fr

Abstract

RFID systems are complex hybrid systems, consisting of analog and digital hardware and software components. RFID technologies are often used into critical domains or into harsh environments. But RFID system is only based on low cost equipments which then do not allow achieving robust communications. All these points make the on-line testing of RFID systems a very complex task. Thus, this article proposes the on-line characterization of a statistical system parameter, the Read-Error-Rate, to perform the on-line detection of faulty RFID components.

As an introduction to the on-line testing of RFID systems, a FMEA first describes the effects on these systems of potential defects impacting the communication part. Second, a SystemC model of the RFID system is discussed as a way to evaluate the proposed test solutions. Finally, the way the maximal Read-Error-Rate can be determined using system-level simulation is explained.

INDEX TERMS

RFID, on-line testing, FMEA, RFID system model, middleware, anti-collision protocol

1 INTRODUCTION

Today, simple radio-frequency communicating labels, tomorrow smart network interacting systems: the RFID applications are going to generate numerous great industrial opportunities. The RFID global market should quickly grow from $5.56 Billions in 2009 to about $26 Billions in 2016 [RAG09]. Indeed, product traceability is a key point for companies who wish to increase their productivity and their product quality. Furthermore, RFID is impacting a lot of different domains: warehouse inventories, product authentication, struggle against theft…

The numerous international standards (ISO 15693, ISO 18000, IDCode, EPC Class 0, 1…) which drive the RFID deployment only focus on RFID system functional or architectural characteristics: power level of readers, RFID communication protocols, allowed RF frequency intervals, maximal response times, middleware and reader services... In these numerous standards as in the industrial fields, reliability issues are always presented as key points for RFID deployment.

In fact, RFID systems can be used, for example, to perform inventories or sensor data collection, into critical domains such as avionics, transportation, health care… In these critical applications, a RFID system error can have catastrophic consequences in terms of human safety. In addition, even if the applications in which RFID systems are involved are not critical, for example access control or warehouse inventories, errors can have economical consequences in term of product quality, manufacturing costs…

One of the most important characteristics in the context of RFID communication is resumed in [DER07]: "*Although the accuracy of current RFID observations is improving, RFID data can be still considered as generally inaccurate. The observed read rate accuracy in real RFID deployments remains still on average in the 60-70 % range, which is one of the major factors limiting widespread adoption of RFID technology* ». Thus, our project aims at improving the RFID systems dependability. Our main goal is to propose methods to detect and diagnose defects in RFID (in-situ) systems. Defects can come from hardware failures (aging effects are particularly sensitive to harsh environments), medium disturbances (for example, electromagnetic bursts), and software bugs.

In this work, on line testing and diagnosis of RFID systems are investigated as a first step towards a global dependability approach of these systems.

More precisely, this paper sets the foundations of a new statistical test method to detect hardware internal defects into both tags and readers, or due to the environment. In particular, we focus on the analog functions or characteristics of the signal transmission. We define a communication feature, the Read-Error-Rate, and we show that this feature is clearly a key factor for the overall system quality.

The outline of the paper is the following. The next section provides a short overview of the RFID domain with a focus on the existing test solutions. In section 3, we present a *Failure Mode and Effects Analysis* (FMEA) centered on the analog parts of the RFID system. In section 4, we propose a model of the RFID system that should be used to evaluate future test strategies. Then, in

978-1-4244-7793-7/10/$26.00 ©2010 IEEE

section 5, this model is used to evaluate the average fault free Read-Error-Rate.

2 State-of-the-Art on RFID systems

In RFID systems, data are exchanged over small (<10cm) or medium (<3m) ranges using wireless Radio-Frequency communication. The two basic components of a RFID system are:

- the tag (or transponder), which is a very small and generally inexpensive smart label, made of one chip and one antenna;
- the reader (or base-station, or interrogator) which is able to read or write digital information into the tags, and which is connected to a local or global network.

Tags can be Passive, Active or Semi-passive. Passive tags do not have batteries, and simply "reflect" the communication when prompted. On the contrary, active tags have batteries and can initiate the communication. Semi-passive tags have a battery but also "reflect" the communication; they cannot, however, initiate the communication. Our study focuses on passive tags which represent the main part of the RFID market.

The advantages of a passive tag are (1) the tag functions without a battery, so that it can have a very long lifeline, twenty years or more, (2) the tag is inexpensive, (3) the tag is much smaller. The disadvantages of a passive RFID tag are (1) the tag can be read only at very short distances, which limits the use of the device for only specific applications, (2) it may not be possible to include sensors within the tag, (3) only very basic functions are available.

As far as we know, no global strategy to improve RFID dependability has been proposed. In addition, in the literature, the RFID systems dependability has not been directly studied. Only few works concern the manufacturing test of chips for tags, or the Failure Mode Analysis of tags. At the opposite, a lot of French (e.g. CEA-LETI) and international laboratories (Auto-ID Labs, or the center for Advanced RFID research) study the security issues in the RFID systems from the data confidentiality and integrity point of view only.

At the circuit level, existing RFID test solutions mainly concern manufacturing test of the tag's chips [NAT07] [MUR04]; these tests are off-line tests using Design-for-Test (DfT) techniques to reduce chips' test cost and application time.

At the system level, the proliferation of readers involves more complexity. RFID middleware is a new class of software which facilitates data and information communication between readers and enterprise software applications [RIF] [REV] [RSM]. Middleware also includes monitoring the status of RFID readers and accessing the RFID reader configurations remotely. In SUN RFID [SUN] or in *RF2ID* [AHM07] event and data management are used to ensure reliability within the RFID system by capturing, filtering and analyzing generated events. As the data transmission between tags and readers is not robust, there are numerous errors and this leads to a high level of Read-Error-Rate. The identification process is then made effective using several iterative transmissions.

Finally, the middleware hides the physical defects to the application. However, this may not be sufficient as it is often necessary to precisely locate the source of a failure in order to reconfigure the system and ensure system reliability and fault-tolerance. In the next section, we analyze the failure mode impacts to evaluate how the previous filtering strategy increases the RFID system robustness.

3 RFID system Failure Mode and Effects Analysis

Only a few failure mode analyses exist in the field of RFID; most of them only concern the tags [SOO08]. We first propose to analyze what is the effect on the whole RFID system of the analog part defects. This analysis would help characterizing the faulty behaviors that these defects can cause.

A *Failure Modes and Effects Analysis* (FMEA) is a classical procedure for the analysis of potential failure modes within a system. This analysis aims at determining all the effects that defects have on the system and their causes. Thus, an FMEA makes it possible to classify the possible faulty behaviors of a RFID system.

For instance, in Table 1, a FMEA focusing on the analog subsystems of an RFID system is presented. The analog subsystems are the physical transmission layer (antenna, modulation and demodulation functions) and the tag power supply. Note that, the same analysis, which has been made for the digital and software subsystems. Due to space limitation, this analysis is not presented here.

FMEA requires defining the subsystems failure modes. In fact, their functionalities must be fault free to assure the correct behavior of the overall RFID system. For each failure mode both following aspects must be studied: (1) the effects that a subsystem failure has on the system, (2) the possible causes of the subsystem failure. For example, for the physical layer, 3 failure modes have been identified: (1) non reception or (2) non transmission by the tag or the reader, and (3) continuous transmission. For the latter mode, the effect on the system is the overload of the transmission channel. This means that no other transmission is possible between tags and readers.

Tab 1 – FMEA centered on the analog subsystems of an RFID system.

Subsystem	Failure modes	Possible causes	Effects on the RFID System
Physical layer (antenna / modulator / demodulator)	Non reception of signals by tag or reader	Tag or reader sensibility detection defect	Loss of information
		EM disturbance	
		External aggression on the tag or reader antennas	
	Non transmission of signals by tag or reader	Reader internal failure	
		Tag internal failure	
	Continuous transmission	Reader internal failure	Channel overload
		Tag internal failure	
		Continuous repetition of attempts issue (software failure)	
Tag power supply	Non conversion of enough electrical power	Insufficient power provided by the antenna	Tag does not turn on
	Conversion of enough electrical power when it should not be	The reader emits too much energy	Tag turns on and communicates with reader

This kind of failure mode has already been identified, by RSA Security as a possible attack where a *blocker tag* continuously jams the readers. Finally, the FMEA also shows how the failure modes are related to component specific defects. For example, internal hardware defects into the tag or into the reader or software bugs can cause such a continuous transmissions.

The middleware filtering strategy, based on successive tag readings, allows hardening the RFID system only when wrong readings are minority. In particular, this strategy is inefficient for permanent reading failure such as overloaded channel.

Theoretically analyzing all the possible ways the defects impact the behaviors of the analog subsystems and then their effects on the overall system are complex tasks. So, to automate the FMEA, to evaluate our test approaches and to design test solutions, we have developed a RFID system simulator called SERFID (Simulator and Evaluator of RFID System). This simulator is presented in the next section.

4 RFID Simulator

4. 1 Existing RFID simulators

Several RFID simulators have already been developed. These simulators allow simulating the communication protocols between the tags and the readers, or the interactions between the readers and the middleware. Designers generally use these simulators to perform a functional verification of their systems. Some of these simulators are *RIFIDI* [RIF], *Fosstrak* (related to the Fosstrak middleware) [FOS], *RFIDSim* [RSM]. In addition, [ANG07] presents a simulator which allows prototyping both tag and reader digital and analog architectures. The digital part is described using the *SystemC Library* [SYS]. The analog parts, i.e. modulation, demodulation and signal propagation, are modeled with *Matlab*. But the complete system co-simulation is performed in two separate steps: the digital part is first simulated and then the analog part is considered. So, it is not a real co-simulation environment with a dynamic interaction between digital and analog parts. Moreover, this solution is very time consuming.

The existing RFID simulators do not allow simulating entire RFID systems consisting of analog, RF or digital hardware together with middleware or software applications. These simulators have been used to improve the deployment of RFID systems. In particular, they allow co-designing the reader and the middleware. However, they do not model the internal architectures of tags or readers, do not consider the RF link between tags and readers (noise or attenuation), do not take into account the modulation/demodulation aspects… For example, they can neither be used to explore new tag's architectures, nor to evaluate the fault tolerance of the RFID systems.

On the contrary, a low level model of a UHF RFID communication and RF link has already been proposed [KHO06]. But this very accurate model, which considers transient effects, would be too time consuming to be used in a complete hardware/software system level RFID system model. Hence, we have developed a complete system level model of a whole HF RFID system including tag, medium, reader and middleware in order to: (1) co-design hardware and middleware, (2) evaluate the system fault tolerance, (3) propose and evaluate new test and diagnosis methods. This model allows us to perform simulation or fault simulation in order to evaluate our test strategy efficiency. Moreover, this model will also help us to develop new middleware services or DfT solutions embedded into tags or readers.

The RFID system model we have developed uses (1) HF frequency (13.56MHz), and (2) ISO-15693 RFID communication standard. Of course, it will be possible to develop other models for RFID communication standards using UHF frequencies (860-930MHz or 2,45GHz).

4. 2 SERFID simulator

SERFID can include numerous readers and several moving tags controlled by one distributed middleware. Numerous parameters are needed to evaluate the tag response times. For instance, the tag response times increase with the number of tags (due to the anti-collision algorithm) and with the electromagnetic disturbance level. Other parameters are: the power transmission, the power setup time of tags, the data transmission throughput, the exchanged data volume…

SERFID has been developed using the SystemC library which is adapted to both hardware and software components modeling. A description of the hardware parts (analog and digital functions) is given in Fig. 1. This model also considers the communication link between one tag (on the bottom-left) and one reader (on the bottom-right). Of course a complete RFID application would involve more interactions between tags and readers.

The basic functions of passive tags and of standard readers can be classified into analog and digital functionalities. Digital functions consist of memory, control logic (baseband data processing and anti-collision protocols), Cyclic Redudancy Check (CRC) controller …

To model the analog functions, we distinguish three parts: (1) the “antenna and RF link” modeling, (2) the power supply and (3) the modulation/demodulation functions. These functions have been modeled using a common behavioral modeling approach adapted to system level simulation. As the SystemC library is adapted to model discrete event systems only, we model the analog component interactions considering only the data transactions. A data transaction consists here in a packet transmission between readers and tags. The same modeling strategy has already been used to model analog part using digital HDL descriptions. However, HDL are not well adapted to develop *Transaction Level Models* (TLM) and to co-design both hardware and software components. In the future, SystemC-AMS will be used to model the analog signal of the RFID system.

The main analog characteristics used into this SystemC model are: the minimal tag supply power, the signal attenuation between tag and reader (in HF, the *coupling factor*), the signal quality (extrinsic and intrinsic noises), the reader and tag coils equivalent inductances...

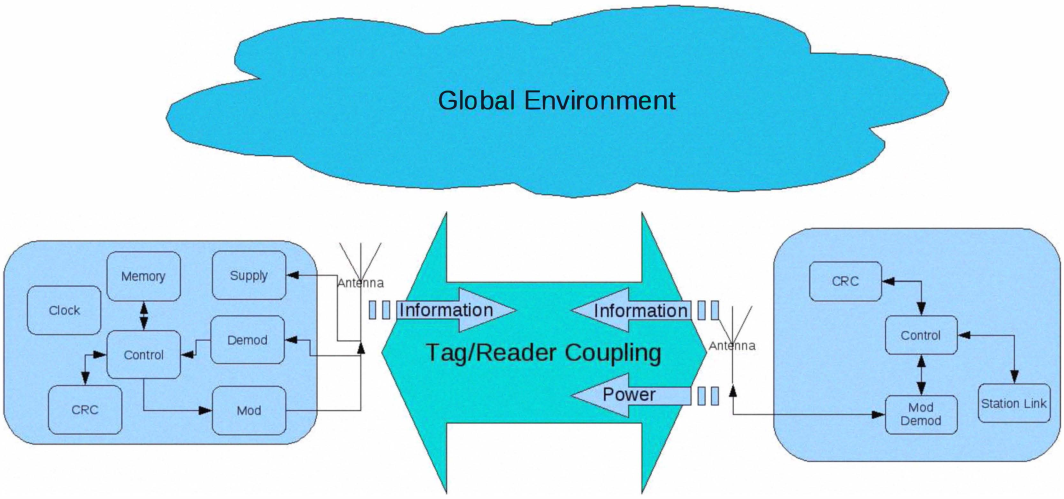

Fig. 1 – RFID System hardware modeling

An example of one analog equation used in this model, describing the power attenuation between the reader and the tag, is given in the following [HAN03]:

$$V_{tag} = k.\sqrt{L_{tag}}\sqrt{P}\sqrt{\frac{Q_{reader}}{Q_{tag}}}.\frac{1}{\omega}$$

Where V_{tag} is the tension collected into the tag, k the coupling factor between tag and reader coils, L_{tag} the inductance of the tag coil, P the power emitted by the reader, Q_{reader} and Q_{ag} respectively the reader and tag quality factors, and ω the pulsation. The values of these parameters are defined into the specification of each RFID product. This equation is related to the arrow labeled *Power* in Fig. 1.

As shown in the following, SERFID allows us to evaluate the average Read-Error-Rate for different RFID systems.

5 Read-Error-Rate evaluation

5.1 RFID system on-line testing approach

The statistical test approach we propose to use is based on the evaluation of the Read-Error-Rate (RER_{max}). The Read-Error-Rate is defined as the ratio between the number of failed reads over the total number of read cycles. According to [EPC], "*a read cycle* corresponds to one protocol run which attempts to read the tag IDs of all tags within the reader's field".

For example, if this RER_{max} is fixed to 3/10, the identification of a new tag coming into the reader field is considered valid only when it is read 7 times over the last 10 read cycles. Once the RER_{max} is known, it is possible to detect defects. Indeed, the reading of a tag less than 7 times over the last 10 read cycles is considered as a failure. Morevoer, once a failure is detected it is then possible to locate it using iterative tests. In fact, in a complete RFID system, the tags, readers, antennas and global environments are abundant. As previously explained, the middleware allows hiding the RFID physical layer to the software application filtering successive identical read cycles results. These successive results can also be used to diagnose the origin of a system error.

For example, assuming a pallet embedding one hundred tagged items, if only 1 tag over 100 is not identified then the problem may come from the unidentified tag or from its global environment. But if during the next identification process the same tag can be read then the problem was due to its environment. In this on-line test approach, we assume that transient defects are only due to transient electromagnetic disturbances. If, at the contrary, the tag always remains not identified whatever the readers, the antennas or the environment are, then we conclude that the tag is faulty.

5.2 Read-Error-Rate estimation

Within this test and diagnosis approaches, the knowledge of an accurate RER_{max} is crucial to detect transmission errors. In fact, an accurate value should allow to detect more defects. However the RER_{max} is difficult to foresee as it depends on a lot of parameters.

The RER characterization consists in counting the number of read errors during the tag identification process. Fig. 2 shows how the RER varies depending on the Bit-Error-Rate (BER) and for different numbers of tags: 1, 10 or 100. The BER depends on Signal to Noise Ratio (SNR), therefore depends on electromagnetic noise into the channel and distance between tags and reader. A relation between BER and SNR can be calculated [BAR05] and therefore BER can be determined for a specific environment. The RER_{max} is then defined by the BER_{max} related to the communication channel quality.

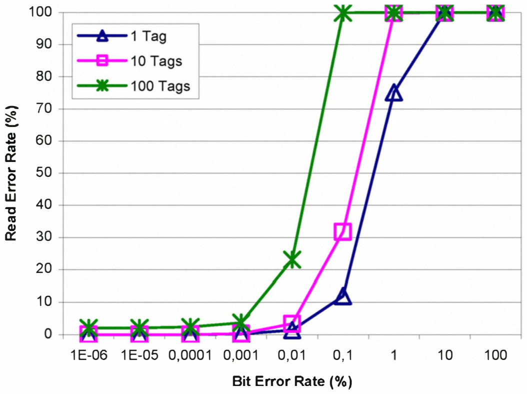

Fig. 2 – Read-Error-Rate variations according to Bit-Error-Rate for 1, 10 and 100 tags

5.3 Identification time estimation

The tag identification times vary according to the tags number and the BER. Indeed, a RFID system consisting of 100 tags will produce more collisions than a system consisting of 10 tags only. Then, the anti-collision protocol is disturbed by the bit error occurrences. Fig. 3 gives an evaluation of the average time to perform two successive identifications for each tag according to BER (curves). This tag identification process is here chosen according to the EPCGlobal specifications [EPC]: a tag is considered *observed* when it is read in two successive read cycles. Fig. 3 also gives an evaluation of the number of read cycles required to check successively twice a tag according to BER (histograms). For example, with a BER equal to 0.1% and 10 tags into the system, 3 read cycles have to be done to check successively twice a tag, and those 3 reads take about 2 sec. We observe that it's not possible to read successively twice a tag for BER greater than 1% for 1 and 10 tags or BER greater than 0.01% for 100 tags.

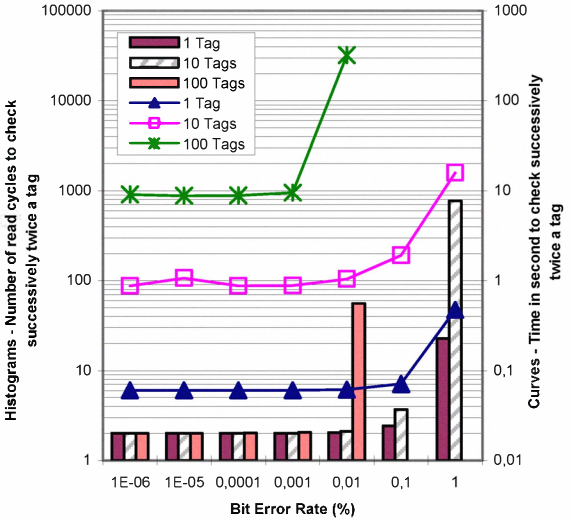

Fig. 3 – Average time and number of read cycles required to check successively twice a tag according to Bit Error Rate

6 Conclusion

This article identifies a RFID system characteristic, the Read-Error-Rate, which could make possible the on-line detection of error-prone RFID components. A model is used to evaluate the maximal allowed Read-Error-Rate depending on the system specifications. *Our near term perspective is to develop a system level test strategy controlled by the RFID middleware. This strategy, totally integrated as a new middleware function, will use the Read-Error-Rate on-line characterization.*

In this article, we assume that the digital and software components of the RFID system are fault-free. As it has already been proposed for wireless in-situ testing, the digital parts included into tags and readers could be validated using manufacturing test data. Of course, this will imply that special on-line test mode and architecture can be used to apply these data.

Acknowledgements

We would like to thank the Grenoble INP – ESISAR RFTLab which helps us to realize this work and the Grenoble Institute of Technology for supporting this project.

Reference

[ANG07] C. Angerer, B. Knerr, M. Holzer, A. Adalan, and M. Rupp. Flexible simulation and prototyping for rfid designs. First International EURASIP Workshop on RFID Technology, pages 51-54, 2007.

[AHM07] N. Ahmed, R. Kumar, R. S. French, and U. Ramachandaran, “RF2ID: A Reliable Middleware Framework for RFID Deployment,” in proc. IEEE International Parallel and Distributed Processing Symposium (IPDPS), 2007.

[ASP] www.fp7-aspire.eu

[BAR05] S. Barbu “Design and Development of a methodology system for 13.56MHz “contactless” systems’RF part”, Thesis, 2005

[DER07] R. Derakhshan, M. E. Orlowska and X. Li, “RFID Data Management: Challenges and Opportunities”, 2007 IEEE International Conference on RFID, USA, 2007

[EPS] EPCGlobal, “Reader Protocol Standard v1.1”, 2006

[FOS] www.fosstrak.org

[HAN03] RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, Second Edition, by Klaus Finkenzeller ISBN:0470844027, John Wiley & Sons © 2003

[KHO06] R. Khouri, V. Beroulle, T.P. Vuong, S. Tedjini,« UHF RFID tag-antenna matching optimization using VHDL-AMS behavioral modeling », Analog Integrated Circuits and Signal Processing, Springer Netherlands, Volume 50, Number 2 / February, 2007, ISSN : 0925-1030, pp. 81-162, Friday, December 22, 2006

[OAT] www.oatsystems.com

[PRA06] B. S. Prabhu and al., “WinRFID – A Middleware for the enablement of Radio Frequency Identification (RFID) based Applications”, in Mobile, Wireless and Sensor Networks: Technology, Applications and Future, John Wiley & Sons, Inc, Mars 2006.

[RAG09] Raghu Das, Peter Harrop, “RFID Forecasts, Players and Opportunities 2009-2019”, IdTechEx report, 2009

[REV] www.revasystems.com

[RIF] www.rifidi.org

[RSM]. trac.assembla.com/RFIDSim

[SUN] java.sun.com/developer/technicalArticles/ Ecommerce/rfid/sjsrfid/RFID.html/

[SYS] www.systemc.org

[YRO] www.rf-it-solutions.com