SystemC Modeling of RFID Systems for Robustness Analysis

Gilles Fritz, Vincent Beroulle, Oum-El-Kheir Aktouf, David Hély
Grenoble Institute of Technology, LCIS
Valence, FRANCE
Firstname.Lastname@grenoble-inp.fr

ABSTRACT

Abstract: **RFID systems are complex heterogeneous systems, consisting of analog and digital hardware components (readers and tags) and software components (middlewares and ERP applications). In addition to these complexity and heterogeneity, RFID systems rely on low cost tags and are often used in harsh environments. As a consequence, they do not always ensure robust communications (i.e. tag detection). Thus, for critical applications, the robustness evaluation and optimization of RFID systems are a must. This article proposes a SystemC model of an HF RFID system for the Simulation and Evaluation of RFID systems (SERFID). SERFID allows performing realistic bit error injections in the RF channel. An industrial critical application of an HF RFID system is described to show how SERFID can help in evaluating and optimizing the dependability of a critical application.**

1. INTRODUCTION

In critical domains, RFID system errors can have catastrophic consequences in terms of human safety whereas in high quality applications, they can have economical consequences in terms of product quality, manufacturing costs, etc.

This study[1] focuses on HF passive tags which represent the main part of the RFID market. Typical HF RFID applications are for instance containers tracking, ID cards, financial cards, e-passports, etc. This article proposes a SystemC model of an HF RFID system. The goal of this model is to conjointly simulate hardware and software components to evaluate the RFID system global robustness thanks to software fault injection and simulation. In fact, robustness analysis requires the capability to inject realistic faults into the model. Thus, the air channels have been described with enough details to be used for fault simulation.

The outline of the paper is the following. The next section provides a short overview of the existing RFID simulators. In section 3, we briefly describe the tag-reader air channel modeling with SystemC. In section 4, an industrial HF RFID system case study is described and we show how our SystemC model allows to evaluate and to optimize the dependability of this critical application.

[1] This work is supported by the ANR (French Research Agency, www.agence-nationale-recherche.fr) within the framework of the SAFERFID project.

2. STATE-OF-THE-ART OF RFID SIMULATORS

Several RFID simulators have already been developed. These simulators allow simulating (1) the communication protocol between the tags and the readers (called "air protocol"), (2) the interactions between the readers and the middleware. Designers generally use these simulators to perform a functional verification of their systems. In [PAL09], the authors present a case study using the RFID emulation environment *Rifidi*. This tool only emulates the reader/client interface of an RFID reader. So, neither the tag internal functioning, nor the communication between tags and readers are simulated by Rifidi. Indeed, the information about the tags in the reader field is directly applied on the reader model. Hence, Rifidi only fits with RFID deployment issues: fault simulation with Rifidi would be unrealistic. In [ANG09], the authors propose an RFID simulation and prototyping system. Although the system can handle reader-tag requests, it mainly focuses on the tag design and their RF front end. The digital part is described using the SystemC Library [SYSC] and 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 dynamic interactions between digital and analog parts. Moreover, this solution is very time consuming and unrealistic for complex RFID Systems simulations. In [FLO09], Floerkemeir et al. present the RFID simulator RFIDSim. RFIDSim is a complete RFID simulator; nevertheless its main goal is to evaluate RFID protocols. This is why it has been developed using a high-level language – Java – so some aspects of tag digital architecture, such as internal concurrent signals, cannot be easily modeled. In addition, it is entirely designed to simulate UHF RFID systems using EPC Class1 Gen2 protocol only.

3. SERFID: SIMULATION AND EVALUATION OF RFID SYSTEMS

The proposed simulator, SERFID (Simulation and Evaluation of RFID Systems) can model numerous readers and moving HF tags controlled by one distributed middleware. Figure 1 illustrates a SERFID model containing several readers and tags.

SERFID has been developed using the SystemC library which is adapted to both hardware and software components modeling. This model also includes the RF communication links between each tag and the readers. In the following, the communication model between tags and reader is described.

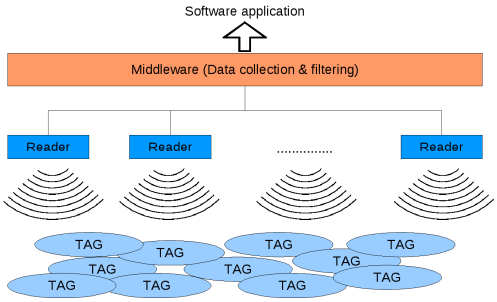

Figure 1 - SERFID high level view model with several readers and tags

3.1 Tag - reader communication

All digital functions in Figure 1 have been modeled using the Transaction Level Modeling with Distributed Time (TLM-DT) [CAI03]. In fact, this level allows a trade-off between simulation accuracy and speed. The messages which model the communications between a tag and a reader are asynchronously sent (i.e. without the need of clock synchronization): components wake up when a message is coming in and fall asleep after dealing with this message. Timing is locally managed in each component (Distributed Time) by including within component descriptions the amount of time it needs to deal with a specific message.

Specific SystemC ports and types have been developed to allow communication between tags and readers. A new data type, simply named "Data", has been introduced. This type allows modeling an RFID communication standard frame [ISO 15693] consisting of Flags, Command code, Parameters, CRC, etc. Table 1 shows the different fields of a "Data", i.e. of an ISO15693 frame.

Table 1 – Fields of an ISO15693 frame

Flags (configuration of tag)	8bits
Command code (action to be performed by tag)	8bits
Parameters (configuration of the action)	variable
Data (data associated to the action, if needed)	variable
CRC	16bits

The anti-collision protocol used in ISO-15693 is a sort of Dynamic Framed Slotted Aloha [ISO15693]. This protocol organizes communication of several tags with a reader to avoid collision. It splits time in n slots and each tag chooses a slot according to its unique identifier to communicate with the reader.

In addition to simulating the communication protocol, SERFID implements also timing defined in ISO-15693. This means that minimum waiting time between slots, frames, data and also bit-rate of transmissions are used to simulate the system. So, it is possible to evaluate time of inventories. In section 4, we will show the advantages of this accurate timing evaluation.

3.2 Tag and reader analog parameters

The main analog characteristics used are: the minimal tag supply power, the signal attenuation between the tag and the reader (in HF, the coupling factor), the signal quality (extrinsic and intrinsic noises), the reader and tag coils equivalent inductances, etc. The minimal tag supply power is the minimal power needed by the tag to operate correctly. If a tag does not receive enough power, then it cannot switch on or, if it is on, it will switch off. Power received by a tag is the power sent by a reader after propagation, so power received by the tag is attenuated in comparison to power sent by the reader. The attenuation is proportional to the cubed reader-tag distance, which is the standard attenuation for near field communication.

As the SystemC library is adapted to model discrete event systems only, we model the analog component interactions considering only discrete data transactions. A data transaction consists in a packet transmission between readers and tags. Analog signals are thus described by modeling the analog signal characteristics or parameters instead of using the analog signal itself. The description of this analog signal, called "Information", consists of different fields or parameters: (1) modulation type – ASK, PSK … – (2) Bit-rate (3) bit encoding – PIE, Miller, Manchester … – (4) Binary Data – the "Data" defined previously – (5) start of frame format (6) end of frame format and (7) the quality of the signal. Thanks to this description, analog signals are not continuously calculated. The signal changes only when one of these seven parameters changes.

3.3 Collisions and bit error rate

In addition, in order to deal with the modeling of the RF communication (in particular, the collisions and remote powering), new resolved signals have been created: a signal carrying "Information" able to be simultaneously driven by several components (tags or readers) and a signal "Power" carrying power with the same ability.

The first signal allows modeling collisions. In fact, two or more tags can simultaneously send signals of type "Information" to a reader. If these "Information" signals are different, resolved signal can notify the conflict by emitting a collision "Information". The second signal allows modeling the tag remote powering by two or more readers. If a tag is in the field of two or more readers, it receives power from all these readers. The "Power" resolved signal sums the different powers sent by all the readers and delivers to the tag the results of this sum.

Finally, in order to model global and local environment effects, the RF links between tags and readers have been divided into 2 parts: (1) a local RF link, which is specific to a couple of tag-reader and (2) a global RF link, which is a common RF environment for all the tags and the readers. This distinction allows the injection of global defects affecting all the tags and the readers or the injection of local defects affecting only one tag or one reader. On one hand, the local RF link parameters allow a particular communication between a tag and a reader to be tuned independently of the other communications. These local parameters are: the distance between a tag and a reader, the quality of the RF link, the Bit Error Rate (BER), and the attenuation of the RF signal. A specific component has been defined to allow timed fault injection. This component, called "Channel", is connected to the reader and the channel according to previously described signals. When there is no fault, it just transmits Information and power from one side to the other. On the other hand, the global RF link parameter allows introducing parameters like the quality of the global RF environment, transient electromagnetic interferences, etc… Figure 2 illustrates the interactions between tags and readers.

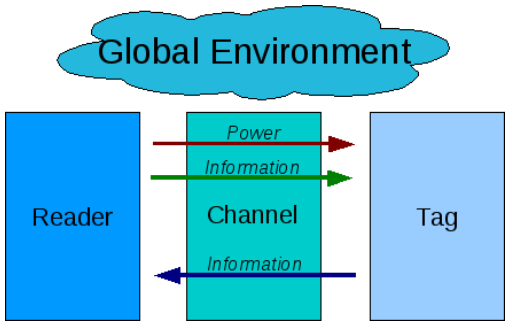

Figure 2 – Signals between a tag and a reader

Figure 3 shows the analog connections between tags and readers (through the resolved signals "Information" and "Power"). This figure shows many tags, many readers and their interconnections. It also shows the global environment previously presented (global RF link parameters). In Fig. 3, there is a specific coupling (or interconnection) for each pair of tag-reader. So, 6 couplings are needed when there are 2 readers and 3 tags: one for reader#1 – tag#1, one for reader#1 – tag#2, one for reader#1 – tag#3, another for reader#2 – tag#1, another one for reader#2 – tag#2 and finally one for reader#2 – tag#3.

Moreover, in order to connect a reader to a tag (or a tag to a reader), two "Information" resolved signals have to be used: one for the communication from the reader to the tag and another one for the communication from the tag to the reader. So, when a reader wants to send an "Information", it writes it into its reader-to-tag "Information" resolved signal. This signal transmits this "Information" to all the coupling components linked with this reader (see Fig. 3). Then, each coupling component transmits this "Information" to a tag (through a reader-to-tag "Information" resolved signal). The same operations are done to send "Information" from tags to readers. If two tags send different "Information" to a reader at the same time, the tag-to-reader resolved "Information" signal of the reader resolves this conflict by generating a collision "Information" to the reader.

For tag remote powering, we only use one resolved power signal for each tag: this signal is directed from the reader to the tag. So, as it is shown in Figure 3, the RF power sent by a reader is transmitted to each tag going through a specific coupling component. This coupling component attenuates the power value according to the local and the global parameters (retrieved from the global environment).

3.4 Evaluation of RFID systems parameters with SERFID

Many RFID parameters can be evaluated with SERFID. SERFID can be used (1) to choose one configuration among several RFID system configurations (position and number of tags and readers), (2) to observe internal hardware signals within the tag and the reader in presence of fault (i.e. to perform fault simulation).

Perhaps the most important parameter which can be analyzed is the inventory time. In fact, as previously described, SERFID totally implements the standard HF RFID protocol ISO-15693. So, SERFID allows analyzing the inventory time according to different scenarios: for example, in ideal environments (*i.e.* without error) or in faulty environments.

Finally, another parameter which can be evaluated with SERFID is the ratio Read Errors to Total Reads (RETR). RETR consists of counting erroneous reads over the total (correct and faulty) reads for a specific reader. In practice, this parameter is often used to monitor RFID systems [THO07]. The RETR is then continuously checked during system functioning and if the RETR is above a fixed threshold the system is considered fault free. In our work [FRI10], we propose to use SERFID to analyze the quality of a new monitoring approach based on the tag RETR monitoring (rather than the reader RETR monitoring).

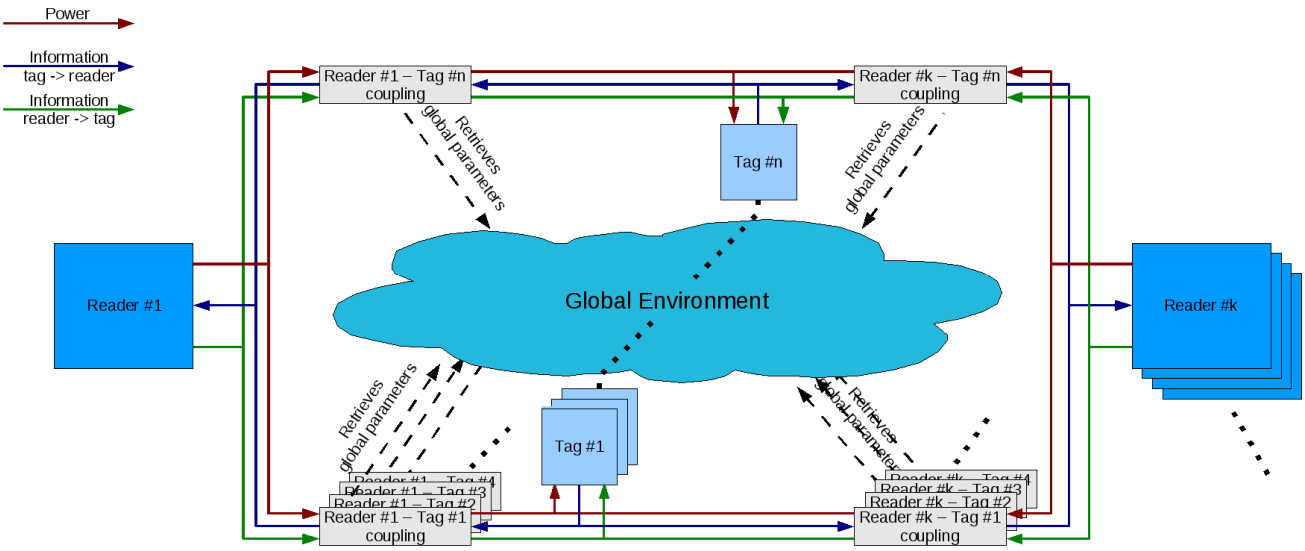

Figure.3 – Tags and readers analog connections

4. HF RFID APPLICATION TEST CASE

4.1 Collisions and bit error rate

In the context of *smart grid electricity,* HF RFID has been proposed to be used into electrical distribution switchboards in order to enhance the detection of electrical defects [ROU06]. The real time defect detection is a critical constraint for this application. In electrical distribution switchboards, tags are coupled with sensors to measure the current and the voltage of each line of the electrical distribution network. All the information gathered by all the tags is then sent to a server for example for monitoring home electrical power consumption. Numerous tags are placed into the limited volume of the electrical switchboard. Electrical interferences can disturb the HF RFID communication between the tags and the reader. Indeed, these interferences are mainly due to the electromagnetic emissions involved by the high pick transient current in the electrical lines. Electromagnetic Compatibility (EMC) standards (IEC 61000) describe the requirements in term of immunity of electrical and electronic equipment to repetitive electrical fast transients (called bursts). The RFID system deployed into the electrical distribution board must be compliant with these requirements. The burst duration is defined as 15 ms with bursts repeated every 300 ms (IEC 61000-4-4).

Our simulations will study how the HF RFID protocol ISO-15693 is able to deal with all these interferences to efficiently communicate with the tags into the electrical board. We will analyze how the choice of adapted protocol parameters can help to increase the system robustness. In our simulations we will assume that whatever the physical parameters are (communicating range, coil power, etc.), bursts defined by the EMC standards will always transiently inhibit the communication: i.e. all the tags will remain undetected during the bursts. However, the reader must be able to detect all the tags in a deterministic time to meet real time constraints of the application.

4.2 Results

We have performed two system simulations with two different protocol configurations and 20 embedded tags into the electrical distribution switchboard. The objectives of these simulations are to show how SERFID can help us to evaluate the impact of the bursts on the system depending on two protocol configurations.

In the first protocol configuration, the reader performs inventory using the standard anti-collision slotted Aloha protocol. In the second protocol configuration, illustrated in Figure 4, each frame of the slotted Aloha protocol consisting of 16 time slots is doubled. This implies that the same reader query is performed successively twice for each tag mask. Hence, the global inventory time for the second configuration will be longer than for the first one. In the following, simulation results will show how this second configuration will increase the robustness of the RFID system.

As the inventory time of 20 tags lasts more than 300 ms (which is the time period of the bursts) then all inventories are disturbed by (at least) one burst. For the two protocol configurations (the standard inventory and the doubled inventory), Table 2 shows how often some tags are detected during 100 successive inventories: it gives an approximation of the tags Read Rates. The second configuration with the doubled frames has a higher average Read Rate – 67% – than the first configuration one – 50% –. Moreover, the

lowest tag Read Rate of the standard protocol is 3% whereas the lowest tag Read Rate is 47% for the second configuration. The reason is that each burst, which exactly lasts 15 ms, inhibits few slots of the 16 time-slots and then tags are not detected. On the contrary, in the second configuration, as the slots are performed twice, the tags which are inhibited during the first frame answer during the second frame and then are detected.

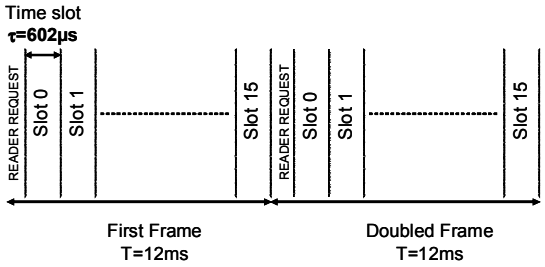

Fig. 4 – Slotted Aloha protocol with two identical successive frames

In addition, we observe that the Average Inventory Times of the second configuration (estimated with 100 simulated inventories) are highly increased comparing to the first configuration ones. These times are given in Table 2. By simulation, we observe that the maximal number of inventories between two detections of the same tag is 33 for the standard protocol but only 3 for the second configuration. Hence, the worst time to detect a tag with the standard protocol is about 24 s and only 11.6 s with the doubled frames protocol. Thank to SERFID, we then conclude that the doubled protocol configuration helps to reduce the detection times in case of interferences.

5. CONCLUSION

This article presents a new RFID simulator called SERFID based on SystemC modeling. This simulator is able to simulate a complete HF RFID system, from tags to the middleware. The SystemC model developed for HF RFID systems includes both hardware and software components, as well as both analog and digital signals. This article shows, for a realistic case study, how SERFID can help to evaluate and to optimize the robustness of HF RFID systems: different uses of ISO-15693 HF RFID protocol are explored in order to cope with bursts interferences.

In our future work, an adaptation of SERFID to UHF RFID systems using EPC Class1 Gen2 protocols will be done. In addition, complex RFID scenarios will be validated using SERFID to measure the impact of fault injections.

Table 2 – Read Rate and time estimation for standard and doubled inventory protocols

Tag	Standard inventory Read Rate	Doubled inventory Read Rate
Tag1	100,00%	92,00%
Tag4	44,00%	46,00%
Tag5	30,00%	59,00%
Tag8	3,00%	47,00%
Tag9	27,00%	59,00%
Tag11	97,00%	92,00%
Tag12	50,00%	62,00%
Tag17	80,00%	92,00%
Inventory Average time	727ms	3880ms

REFERENCES

[ANG09] Angerer, C.; Langwieser, R.; " 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

[CAI03] Lukai Cai and Daniel Gajski. 2003. Transaction level modeling: an overview. In Proceedings of the 1st IEEE/ACM/IFIP international conference on Hardware/software codesign and system synthesis (CODES+ISSS '03). ACM, New York, NY, USA, 19-24.

[FLO09] Floerkemeier, C.; Sarma, S.; "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

[FRI10] G. Fritz, V. Beroulle, O. Aktouf, M. D. Nguyen, D. Hély, "RFID System On-line Testing Based on the Evaluation of the Tags Read-Error-Rate", JOURNAL OF ELECTRONIC TESTING, (DOI: 10.1007/s10836-010-5191-6), pp 1-10, december 2010.

[ISO15693] ISO/IEC 15693-3:2009 Identification cards – Contactless integrated circuit cards – Vicinity cards – Part 3: Anticollision and transmission protocol

[PAL09]C. E. Palazzi, A. Ceriali, M. Dal Monte, "RFID Emulation in Rifidi Environment", in Proc. of the International Symposium on Ubiquitous Computing (UCS'09), Beijing, China, Aug 2009.

[ROU06] Roudet, F. Coutelou, O. Bruel, M. Vuong, T.-P. Tedjini, S. , "RFID tags physical positions detection for on/off sensors applications in electrical distribution switchboards", 2006 IEEE Antenna & Propagation Symposium/URSI Symposium, Albuquerque, New Mexico, USA, July 10, 2006

[THO07] Frank Thornton,"How to cheat at deploying and securing RFID", Syngress, ISBN-10: 9781597492300, December 28, 2007.

[SYSC] http://www.systemc.org/home/