Read rate profile monitoring for defect detection in RFID Systems

Gilles Fritz, Boutheina Maaloul, Vincent Beroulle, Oum-El-Kheir Aktouf, David Hély
Grenoble Institute of Technology, LCIS
50 rue B. de Laffemas, BP 54
26000 Valence, FRANCE
Firstname.Lastname@lcis.grenoble-inp.fr

Abstract— **RFID technologies are sometimes used into critical domains where the on-line detection of RFID system defects is a must. Moreover, as RFID systems are based on low cost tags which are often used into harsh environment, they do not always ensure robust functioning. This article proposes a new on-line monitoring approach allowing the detection of system defects to enhance system reliability and availability. This approach is based on the characterization of a statistical system parameter – the tag read rate profile – to perform the on-line detection of faulty RFID components. This monitoring approach is compared to classical monitoring approaches for a real case study and through several fault simulations. Results show that the proposed read rate profile monitoring is more efficient than the existing approaches. In addition, results show that this approach should be combined with an existing approach to maximize the fault detection.**

RFID; on-line testing; monitoring; dependability

I. Introduction

Monitoring RFID systems is a mandatory task in order to detect failures. As inventories within RFID systems are generally based on numerous successive attempts - called *acquire cycles* - to read all the tags, a system failure can have several meanings: (1) it can be a tag misread during an inventory or (2) it can be an increase of the number of read errors, which is the number of failed attempts to read a tag. In both cases, as RFID systems are nondeterministic communicating systems, a failure is detected when a particular metric exceeds a specific threshold. These failures can be due to the occurrence of one or several defects (or faults[1]) into the RFID System. These defects can appear on the readers, the tags or the network (connectivity between the readers and the software application). However, all defect occurrences do not necessarily involve system failure. Indeed, defects can reduce the tag performances for a specific environment or for a specific tags and protocol configurations only. For example, the ElectroMagnetic (EM) coupling effects between tags can involve tag misreads with a protocol but not with another one. Hence, the detection of defects is even more interesting than the detection of failures, as it may prevent failure occurrences. Therefore, the goal of our project[2] is to propose on-line methods to detect defects in HF or UHF RFID systems [2] [3]. These defects can result from hardware malfunctions (aging effects are particularly sensitive to harsh environments), medium disturbances (for example, electromagnetic bursts), or software bugs.

In this work, a new monitoring approach is proposed and compared to classical monitoring approaches. Our method is inspired by classical monitoring techniques. But, in our case, 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* - involving all the tags of the population rather than an average value computed for the same population. In this paper, we only focus on the detection of defects which can appear in UHF tags and in their EM environment. Our approach, as the classical monitoring approaches are, is nonintrusive because all the information we use are already available from normal RFID system operation.

The outline of the paper is the following. The next section provides a short overview of the classical RFID system monitoring approaches. In section 3, we present our case study. In section 4, we present the initialization phase of our monitoring approach. Finally, section 5 and 6 discuss the evaluation of the proposed approach by both hardware and software fault injections.

II. State-of-The-Art on RFID Systems Monitoring

There are two classical methods to monitor RFID systems in order to detect failures: the first method consists in remotely monitoring the reader status whereas the second one observes the reader performances.

Status monitoring consists in verifying whether a reader is on or not. Many catastrophic errors like disconnected readers from network or shutdown devices can be detected. This monitoring is easy to realize: a simple query using SNMP (Simple Network Management Protocol) can determine

[1] Classical terms, as defined in [1] are used: *failure* for system service deviation from the specified service and *fault* or *defect* for incorrect state of hardware or software that may lead to an *error*, which in turn may lead to a *failure*.

2 This work is part of SAFERFID project, funded by the French National Research Agency (www.agence-nationale-recherche.fr/)

whether the device is connected and if it properly works. However, this technique does not detect soft defects which only slightly decrease reader performances.

The second classical method is based on the performances monitoring of the readers. A lot of performance parameters can be observed to detect failures and defects. Two classical performances parameters are described below.

Average Tag Traffic Volume (ATTV) according to time, is the first parameter which can be measured [4]. ATTV is then compared to an ATTV reference profile determined during a learning phase. This comparison 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.

Read Errors to Total Reads (RETR) is the second parameter which also informs on the health of readers and of their environment [4]. RETR consists of counting erroneous reads over the total (correct and faulty) read attempts of a specific reader. High RETR means there is probably a problem: a faulty antenna, an improper placement of antennas, signal interferences in the range of RFID frequencies, low signal strength or software dysfunction. The evolution of this RETR can also be analyzed.

III. CASE STUDY

A. *Description*

Our UHF RFID system, set at 900MHz, allows the detection of EPC Class 1 Gen 2 tags stuck on boxes in a production chain. The boxes are arranged on a pallet; each pallet contains 111 boxes. The pallets are carried by a transporter from one point to another point of a production chain. To detect most of the boxes (or tags) the pallet goes through a rotating conveyor which is centered into the RFID reader field. The pallet rotates during 160 seconds before going to a next location. The pallet rotation speed is then 12 rounds per inventory or 4.5 revolutions per minute. Fig. 1 illustrates this RFID system which consists of: one pallet under a rotating conveyor, 111 tagged boxes and one controlling reader with two antennas.

Many points have been optimized to perform an inventory detecting almost all the tags in the pallet. These points are (1) the protocol parameters (detailed in the following), (2) the tag location and direction on the box surface, and (3) the antennas location and direction.

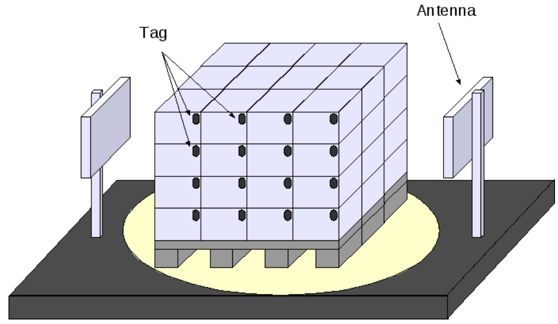

Figure 1. RFID system case study configuration

The reader is an ALIEN 8800 reader [5] controlled by a host computer via an Ethernet or serial connection. A Java program in the host computer commands the inventory execution. The same program also concurrently performs the result analysis for the on-line detection of the failures; this point will be described further.

The parameters of the reader protocol defined by EPC Class 1 Gen 2 [6] are CYCLE, ANTENNA, SELECT, COUNT, and Q. The definitions and the specific values we have chosen for these parameters are given in Table I below:

TABLE I. DEFINITIONS AND VALUES OF PROTOCOL PARAMETERS

EPC C1G2 protocol parameters	**Values**	**Definitions**
CYCLE	100	Number of acquire cycles
ANTENNA	2	Sequence of use of the reader antennas. For example, if ANTENNA is equal to 1,2,3 this means antenna #1 is used first, then antenna #2 and finally antenna #3
SELECT	1	Number of select command sequences. The select command awakes tags which then will answer to future read attempts.
COUNT	3	Number of read attempts
Q	5	Q parameter defines the number of used slots in the anti-collision protocol

The reader protocol is divided in several loops. Each loop is then linked to one of the previous parameters. Fig. 2 gives a simplified representation of the reader protocol algorithm. The *doAcquisition* function executes the *slotted Aloha* anti-collision protocol [6]. The COUNT value allows “weak tags” to be detected in presence of “strong tags”. Indeed, in the third reading session (*session 3*) each inventoried tag sleeps until it receives a new SELECT command. So, if there are strong tags, these tags respond first (hiding the weakest tag responses) and then go in SLEEP mode. During the next acquisition, the weak tags can be detected because strong tags are sleeping. This protocol is performed by the ALIEN reader controlled with the high level Java instructions executed by the host computer.

```
Foreach CYCLE
        Foreach ANTENNA
                SELECT
        Foreach COUNT
                Foreach ANTENNA
                        doAcquisition(Q)
```

Figure 2. EPC C1G2 protocol performed by the ALIEN 8800 reader

The tag location and direction on each box have also been studied and optimized. Each box contains 6 metallic syrup bottles. These bottles are very bad medium for EM propagation. We will see in section V that a small tag displacement or rotation involves lower tag detection. For the same reason, the boxes arrangement on the pallet has also been studied to give an accessible location for each tag on the boxes.

Finally, the ALIEN reader has been configured to use two circular antennas – one for emission and the other for reception. Once again, the locations and the directions of these two antennas have been chosen to optimize the tag detection.

B. *Case study inventory results*

Using the protocol parameters defined in Table I, we have obtained several read rate results for different pallets. These results are presented in Table II. For each detected tag, the reader returns a read rate; i.e. the number of times the tag has been read during the inventory over the total number of acquire cycles.

For seek of simplicity, not all obtained results are presented in Table II. But for illustration purposes, some of these read rates (highest, 61th, 62th, 63th, and lowest ones) are placed in Table II in descending order. These inventories, as they serve as references for our monitoring approach, have been performed without defect injection. Hence, to assure that there is no defect, all tags have been manually applied on boxes and have been individually controlled to assure the correctness of their location, performance, direction, etc. Then, for each inventory, the *Global Read Rate* (GRR) which is the average read rate of the tags of a pallet has been calculated. Table II gives for several inventories (1, 2, i, j) obtained GRRs, the average and the standard deviation of each GRR. In addition, we count the *number of detected tags* for each inventory and we determine the average and the standard deviation of this parameter. These values are also given in Table II.

TABLE II. STATISTICAL RESULTS FOR FAULT FREE INVENTORIES

	Inventory 1	**Inventory 2**	**…**	**Inventory i**	**Inventory j**	**…**	**Average**	**Standard Deviation**
Read rate 1 (high)	100	100	…	100	100	**…**	100.00	0.00
….	….	….	…	….	….	**…**	….	….
Read rate 61	63.2	62.4		62.3	63	**…**	61.12	3.44
Read rate 62	62.1	57.8	…	58.3	58.3	**…**	59.08	3.03
Read rate 63	58.4	57.3		56.4	57.1	**…**	57.94	2.89
…	…	…	…	…	…	**…**	…	…
Read rate k (low)	7.8	9.6	…	7.8	6.8	**…**	3.11	3.89
Global Read Rate	66.51	65.76	…	65.62	65.36	**…**	65.20	1.27
Number of detected tags	111	110	…	109	111	**…**	110.23	0.73

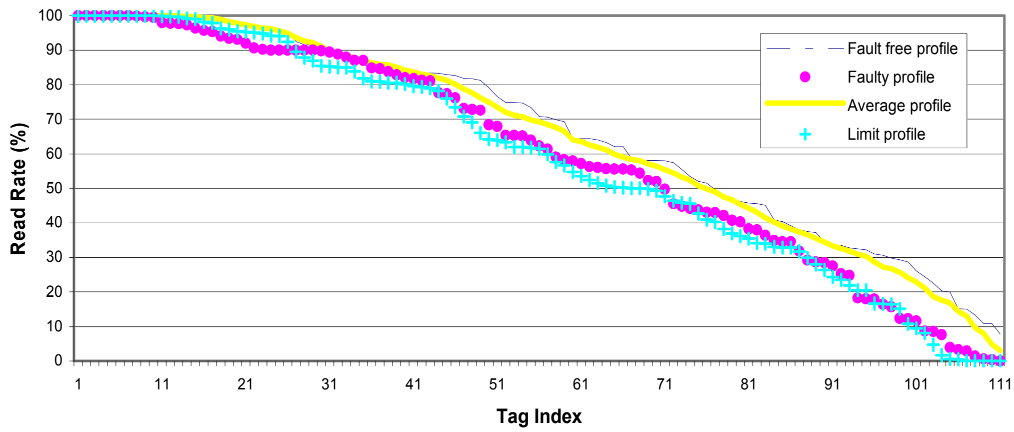

Figure 3. Average, limit, fault free and faulty inventory profiles

IV. New monitoring approach setup

A. Read rate profile definition

The initialization of our monitoring approach requires computing the statistical parameters of the fault free inventory profiles. Let us first explain what these inventory profiles are.

Each inventory in Table II leads to a specific inventory 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. As the tags are placed in descending order, the inventory profiles are always falling curves.

Then, from all these inventory profiles, an average profile is computed. This average profile is represented by the bold curve in Fig. 3. Of course, as successive inventories generate different tag ordering (or even different tag detection and non detection), the average profile does not allow analyzing individual tag behavior. Hence, our approach (as the classical RETR or ATTV approaches also do) does not allow determining the localization of the defects (i.e. the faulty tags).

B. Read rate limit profile definition

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 points (i.e. one ordered tag read rate) under this limit implies that the RFID system is considered faulty. Of course, we have verified that all the fault free inventory profiles are always above this limit. 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. We assume here that all the 111 tags statistical distributions are normal (Fig. 4). We then compute the limit L_i for each tag i using the classical formula given in (1) for a population of 99.7%.

$$L_i = \mu_i - 3\sigma_i \tag{1}$$

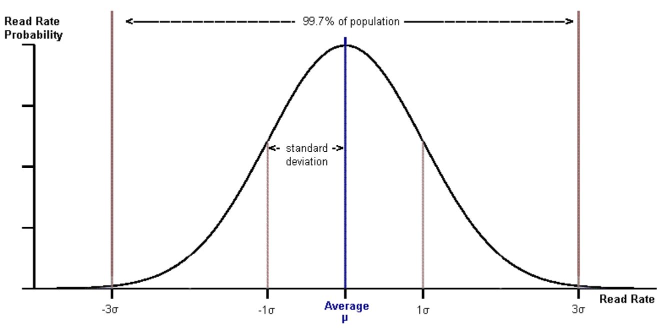

Figure 4. Normal distribution of a random variable X

V. Experimental validation

We want here to compare the efficiency of our approach with the classical monitoring approaches (RETR and ATTV). The quality of a monitoring approach is determined by its ability to detect faulty components or to its probability to generate false alerts. In order to validate our approach, we first manually generate several faulty RFID systems. Then, the host computer automatically compares each inventory profile with the limit profile. Failures are detected if an alert is emitted by the host computer.

To inject the faults into the RFID system, we use different methods: (1) we rotate by 90 degrees 5 random tags, (2) we change the location of 5 random tags, (3) we change the location of 15 random tags, (4) we change the location of 21 random tags, (5) we stop the pallet rotation during 15 s and (6) during 20 s.

Table III shows the statistical results computed after applying these hardware fault injections. These statistical parameters are: (1) the total number of detected tags during each faulty inventory, (2) the variation of the read rate (compared with the average read rate), (3) the number of tags with a read rate variation greater than +10% or (4) less than -10%. The same table also shows which monitoring methods detect the injected faults. We consider three monitoring methods: (1) the *Nb Tags method* which consists of counting the number of detected tags and to compare this number to a limit defined according to the measures from Table II, (2) the *GRR method* which consists in calculating the Global Read Rate of the inventory and to compare it to a limit defined with the measures from Table II, and (3) the *profile method* which is our proposed method. The first two methods are similar to the classical methods: Nb Tags and GRR methods are similar to ATTV and RETR discussed in section II.

These experimental results show that our new monitoring approach is efficient for detecting several fault injections which would not be detected with the classical approaches. In addition, our approach detects 4 fault injections while Nb Tags method detects 3 fault injections and GRR method detects no fault injections.

TABLE III – READ RATE EXPERIMENTAL RESULTS USING HARDWARE FAULT INJECTIONS

	Faulty system #1	Faulty system #2	Faulty system #3	Faulty system #4	Faulty system #5	Faulty system #6
Total number of detected tags	108	108	109	107	109	109
Read rate variation	-0.14	-0.64	2.7	2.48	1.58	3.2
Number of tags with a read rate variation > 10%	2	1	5	8	0	6
Number of tags with a read rate variation < -10%	0	0	0	0	0	0
Nb Tags method	Defect detect	Defect detect		Defect detect		
GRR method						
Profile method			Defect detect	Defect detect	Defect detect	Defect detect

VI. EVALUATION OF THE PROFILE METHOD BY SIMULATION

Manually generating a lot of faulty RFID systems is not easy. In fact, covering a large number of faulty configurations requires changing a lot of tags locations or directions. However, actually the boxes are difficult to assemble and disassemble on the pallets. Hence, we choose to use simulation to complete the previous validation. Indeed, as fault simulations can be done quickly, they allow us to apply our approach on a large number of faulty RFID systems. Software fault injections are directly performed on the obtained read rate results from fault free inventories: a fault injection consists in randomly changing the values of few tags read rates.

To inject faults into the fault free inventory results, we use different methods: (1) we subtract 40% to the read rates of 5 randomly chosen tags (2) we subtract 10% to the read rate of 20 random tags. The inventory results are randomly chosen among all the available fault free inventories. Even if these methods are simple they seem to be enough realistic to perform a second validation.

Table IV shows the number of fault detection achieved by the three monitoring approaches after applying 100 software fault injections. It shows that the profile monitoring method is the approach which detects most faults. In addition, Fig. 5 shows how these 3 approaches share the fault detection. It demonstrates that, even if most of the faults are detected by our approach, the Nb tags and profile methods must be used concurrently to detect the maximum number of faults.

TABLE IV – TEST METHODS EVALUATION USING SOFTWARE FAULT INJECTIONS

Methods	% faulty systems detected with faults injection 1	% faulty systems detected with faults injection 2
NbTags method	10	8
GRR method	7	7
Profile method	69	97

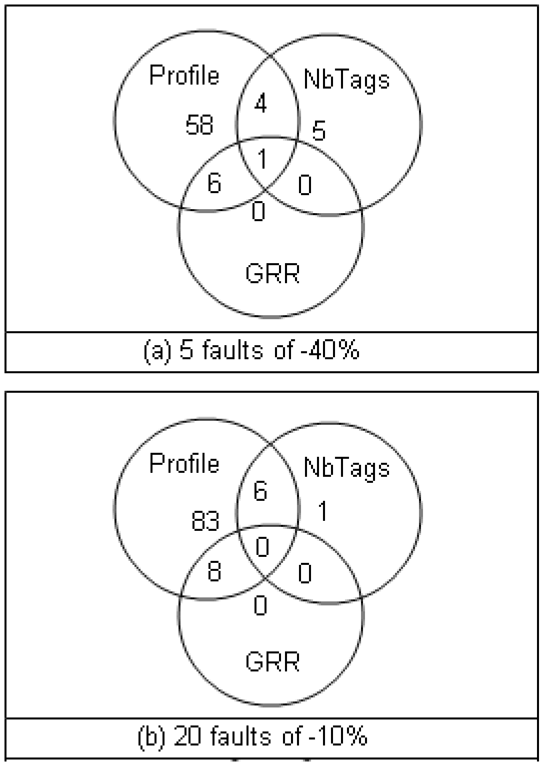

Fig 5 – Set diagrams showing the complementarities of the 3 monitoring methods for (a) 5 read rate fault injections of -40% and (b) 20 read rate fault injections of 10%

VII. CONCLUSION

This article proposes a new monitoring approach for the detection of defects in RFID systems. This approach is based on the tag read rate on-line evaluation and its comparison with a predefined profile. This profile is determined by observing the tags read rates of several fault free systems. This article compares this new approach with classical monitoring approaches for RFID systems. It brings out (1) the efficiency of proposed profile method and (2) the complementarities of this approach with one of the classical method. Future work will concern diagnostic and reconfiguration of the RFID systems to avoid system failures.

ACKNOWLEDGMENT

Authors of this paper would like to thank the RFTLab where all the experimentations presented here have been performed. The RFTLab is a French laboratory which performs test and characterization of various EM applications (CEM, RFID…)

REFERENCES

[1] J.-C. Laprie « Dependable Computing and Fault-Tolerance: Concepts and Terminology », 15th IEEE International Symposium on Fault-Tolerant Computing, Ann Arbor, MI, 1985, pp. 2-11.

[2] G. Fritz, V. Beroulle, M.D. Nguyen, O. Aktouf, I. Parissis, "Read-Error-Rate evaluation for RFID system on-line testing", Mixed-Signals, Sensors and Systems Test Workshop, 2010 IEEE 16th International, p1-6, 7-9 June 2010

[3] G. Fritz, V. Beroulle, O. Aktouf, M. 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, Décembre 2010

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

[5] http://www.alientechnology.com/docs/products/DS_ALR_8800.pdf

[6] EPC Radio-Frequency Identity Protocols – Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz – Version 1.2.0