Sûreté de fonctionnement des systèmes RFID – Evaluation et simulation des dysfonctionnements

Gilles FRITZ
Grenoble INP – ESISAR
LCIS – EA 3747
50 rue Barthélémy de Laffemas
26000 VALENCE

Vincent BEROULLE
Oum-El-Kheir AKTOUF
Minh-Duc NGUYEN

Email : gilles.fritz@esisar.grenoble-inp.fr

Résumé

Le développement d'infrastructures complexes pour l'exploitation de la technologie d'identification par radiofréquence RFID soulève le problème de la sûreté de fonctionnement de tels systèmes. En effet, lors de l'implantation de systèmes RFID, les problèmes de fiabilité du matériel et du logiciel, ainsi que les perturbations liées à l'environnement, sont souvent négligés. L'étude proposée dans ce document vise à analyser les dysfonctionnements possibles des éléments de ce système. Un modèle de système RFID est proposé afin d'étudier l'impact de ces dysfonctionnements sur le système complet. Pour pouvoir simuler les parties matérielles et logicielles, ce modèle a été développé avec SystemC.

1. Introduction

Les systèmes RFID sont utilisés dans un nombre croissant d'applications telles que la finance, le contrôle d'accès, l'inventaire et le suivi d'objet. En effet, cette technologie permet l'identification automatique et sans contact d'objets ou de personnes. Plus généralement, elle permet l'échange d'informations à distance par radiofréquence ; cette information est généralement sauvegardée dans un petit médium à faible coût. L'intérêt principal de cette technologie est de pouvoir accéder à cette information sans contact ni vision direct pour de nombreux objets simultanément.

Un système RFID est composé par :

- des tags ou étiquettes : cet objet stocke l'information. Chaque objet à identifier doit être lié à un tag, d'où la nécessité pour ce tag d'être petit et peu cher.
- des lecteurs : cet appareil permet de lire (ou écrire) les informations sauvegardées dans le tag.

Dans cette étude, nous considèrerons un tag passif[1] fonctionnant en Haute-Fréquence (HF – 13,59MHz), c'est-à-dire qu'il n'embarque pas de source d'énergie pour fonctionner. Il transforme une partie du signal RF transmis par le lecteur en énergie, afin de fonctionner et de communiquer avec le lecteur. De plus, on prendra le cas d'un tag simple, qui n'intègre que les fonctions de base : lecture et écriture des données à distance, verrouillage et déverrouillage des données et désactivation définitive du tag.

Dans certains cas, comme la logistique ou la distribution, ces appareils sont le plus souvent connectés à des infrastructures complexes : ils sont connectés à travers un réseau local, eux-mêmes souvent interconnectés grâce à des réseaux plus grands. Ce genre d'installation génère une très grande quantité de données ; on utilise alors des intergiciels ou middlewares pour gérer ces appareils et ces données afin de les rendre utilisables par les applications métiers. Ils récupèrent les données présentes sur les tags, les mettent en forme, puis les redirigent vers les applications de gestion. Ils permettent aussi de gérer la communication entre l'application finale et les lecteurs en servant d'intermédiaire lors de la configuration et la gestion des lecteurs. En effet, ils masquent l'interface des lecteurs, souvent propriétaire et donc fortement hétérogène. Il existe de nos jours plusieurs middlewares, certains libres comme *Fosstrak* [2], *WinRFID* [3] ou *Aspire* [4] et d'autres commerciaux tels que *You-R Open* [5] ou *OAT System* [6].

La figure 1 montre le système RFID dans son ensemble. On y retrouve les tags et les lecteurs qui communiquent, les lecteurs connectés à un réseau local et le middleware qui gère les lecteurs et les flux de données pour transmettre l'information utile aux applications métiers.

Au vu de la complexité de tels systèmes, il devient nécessaire de s'intéresser aux défaillances pouvant subvenir dans les systèmes RFID. A partir de cette étude, nous pourrons alors proposer des stratégies améliorant la sûreté de fonctionnement du système : méthodes de test et de diagnostic pour détecter les défaillances afin de les corriger.

Cet article va présenter dans un premier temps une analyse de la sûreté de fonctionnement, et en particulier les défaillances possibles, d'un système RFID. Dans un second temps, il présentera le modèle que nous proposons

[1] Une classification des différents tags existants est donnée dans [1]

afin d'étudier les défaillances du système puis l'implantation de ce modèle en SystemC.

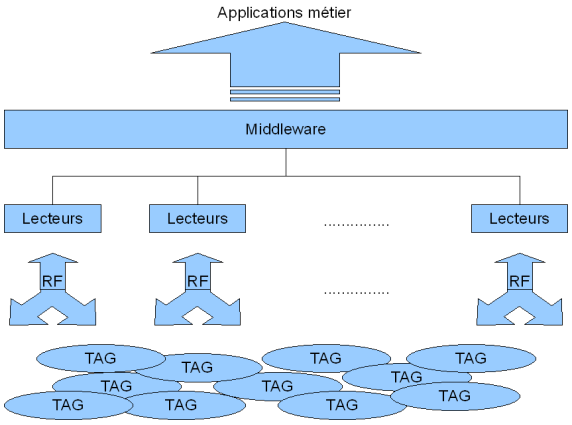

Figure 1. Système RFID

2. Sûreté de fonctionnement des systèmes RFID

Jean-Claude Laprie définit la sûreté de fonctionnement comme étant la « *propriété qui permet aux utilisateurs d'un système de placer une confiance justifiée dans le service qu'il leur délivre* » [7]. Cette propriété est définie par les attributs suivants :

- la fiabilité : probabilité qu'un système fonctionne sur l'intervalle de temps [0,*t*]
- la disponibilité : probabilité qu'un système fonctionne à un instant donné *t*
- la maintenabilité : aptitude d'une entité à être maintenue ou remise en état de fonctionnement
- la sécurité-innocuité : aptitude d'un système à protéger son environnement et ses utilisateurs contre les conséquences catastrophiques
- la sécurité-confidentialité : aptitude d'un système à garantir l'intégrité des données et à en protéger l'accès et les modifications

Dans le cas des systèmes RFID, le dernier attribut de la sûreté de fonctionnement est largement étudié. En effet, les tags (1) stockent des informations qui peuvent être sensibles ; (2) sont attachés à des objets destinés à être déplacé ; (3) peuvent communiquer sans contact ni vision direct. Il y a cependant très peu d'études sur la fiabilité et la disponibilité de ce genre de système et peu d'analyses des modes de défaillance, la plupart se concentrant sur les tags [8]. Nous proposons donc dans un premier temps d'analyser les effets sur le système complet des défaillances des éléments du système. Notre but est d'avoir une meilleure compréhension sur les comportements erronés que peuvent avoir ces défaillances.

Une *Analyse des Modes de Défaillance et de leurs Effets* (AMDE) est une procédure classique lors de l'analyse des modes de défaillance possible d'un système. Cette analyse tente de déterminer tous les effets sur le système ainsi que leurs causes.

Le tableau 1 montre l'AMDE de la couche physique du système. La même analyse a été conduite sur tous les composants – logiciels et matériels – du système RFID. Chaque mode de défaillance implique l'étude : (1) de l'effet sur le système, (2) des causes possibles. Ici, nous avons identifié 3 modes de défaillance pour la couche physique : non réception des signaux par le tag ou le lecteur, non émission des signaux par le tag ou le lecteur et l'émission continue. Pour le premier mode, l'effet sur le système est la perte d'informations. Le lecteur ne voit donc pas la présence d'un tag. Enfin, l'AMDE montre comment les modes de défaillance sont liées au défaut des composants. Par exemple, une agression externe sur l'antenne, engendrant donc une déformation de celle-ci, peut conduire à la non réception du signal.

Composant	Modes de défaillance	Causes possible	Effets sur le système
Couche physique (Antenne, modulateur, démodulateur)	Non réception des signaux par le tag ou le lecteur	Sensibilité de détection défaillante	Perte d'informations
		Perturbation EM	
		Agression externe sur l'antenne du tag ou du lecteur	
	Non émission des signaux par le tag ou le lecteur	Défaillance interne du tag	
		Défaillance interne du lecteur	
	Emission continue	Défaillance interne du tag	Canal surchargé
		Défaillance interne du lecteur	
		Répétition continue de tentatives d'émission (défaillance logiciel)	

Table 1. AMDE de la couche physique (Antenne, modulateur et démodulateur)

Cette analyse théorique des modes de défaillance du système, de leurs effets sur le système complet et de leurs causes est une tâche compliquée. Afin d'automatiser cette analyse, et aussi pour évaluer, concevoir et valider nos solutions de test, nous avons développé un simulateur de système RFID. Ce simulateur est présenté dans la section suivante.

3. Simulateur de Système RFID

Il existe déjà plusieurs simulateurs de système RFID. Ces simulateurs permettent de simuler le protocole de communication entre plusieurs tags et lecteurs, ou les interactions entre lecteurs et middlewares. Ils sont utilisés en général pour effectuer une vérification formelle d'une partie du système. En voici quelques uns : *RIFIDI* [9], *Fosstrak* provenant du middleware du même nom, *RFIDSim* [10]. En plus de ces simulateurs, le document [11] présente un simulateur dédié au prototypage commun de tag et lecteur. Il permet la simulation des parties analogique et numérique. La partie numérique est décrite à l'aide de la librairie *SystemC* [12]. La partie analogique, c'est-à-dire la modulation, la démodulation et la propagation du signal, est simulée avec *Matlab*. Malheureusement, la simulation du système complet est faite en deux étapes : en premier la partie numérique, puis ensuite la partie analogique. Il n'est donc pas possible de simuler ces deux parties en même temps (co-simulation).

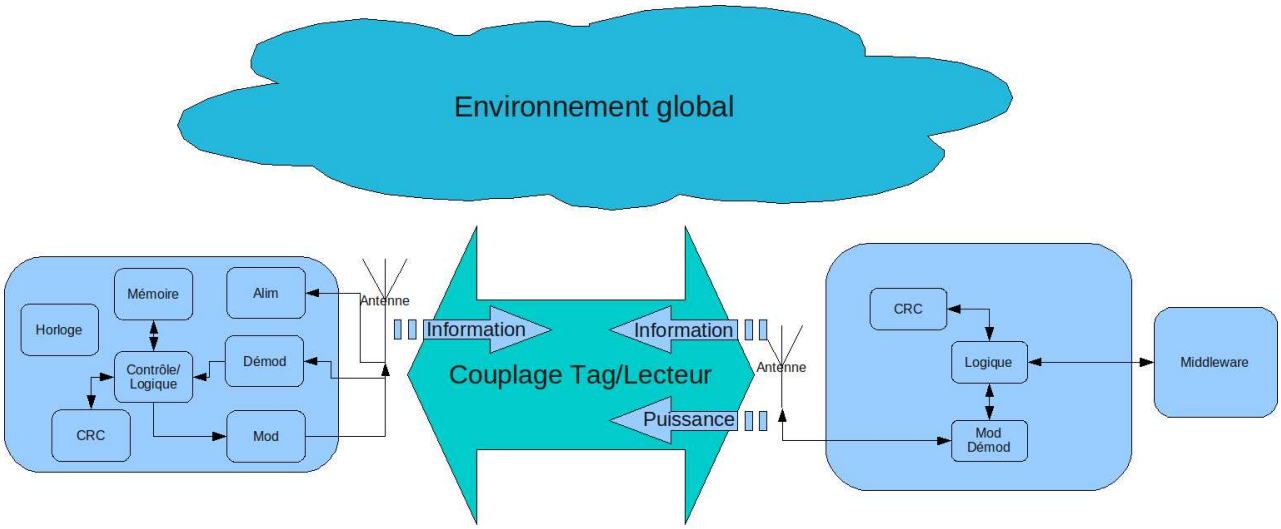

Figure 2. Architecture du simulateur

De plus, une simulation complète prend beaucoup de temps.

Les simulateurs existants ne permettent pas de simuler un système RFID complet. En effet, un système RFID est composé de partie analogique, numérique, logiciel et matériel. Il communique en plus avec un middleware. Les simulateurs que nous avons vus précédemment ont été développés afin de faciliter le déploiement de la RFID, en particulier pour la conception et la configuration de middlewares.

Pour ces raisons, nous avons développé un modèle d'un système RFID incluant le tag, le canal de transmission, le lecteur et le middleware. Celui-ci nous permettra d'évaluer la tolérance aux fautes du système, puis de proposer et d'évaluer des méthodes de tests et de diagnostics. Il nous permettra aussi de faire du co-design matériel-middleware.

Notre cas d'étude est un système RFID HF (13,56MHz). Nous utiliserons la norme ISO-15693 afin de fixer le protocole de communication entre le tag et le lecteur, ainsi que les fonctionnalités de base de chacun.

Afin de respecter la nécessité de simuler conjointement le logiciel et le matériel, nous avons choisi d'utiliser *SystemC* pour développer notre modèle. Ensuite, nous avons décidé de représenté les signaux analogiques par des signaux numériques qui stockent les différents paramètres du signal analogique.

Chaque composant du tag et du lecteur a été modélisé : mémoire, CPU, logique combinatoire, bloc CRC, etc. Ces composants sont des unités numériques classiques et ne présentent pas de difficultés particulières. Ils ne seront donc pas présentés ici.

Afin de simuler le lien entre les tags et les lecteurs, c'est-à-dire le signal analogique entre le tag et le lecteur, le modulateur, le démodulateur et la télé-alimentation du tag, plusieurs possibilités ont été considérées : (1) simuler le comportement de chaque composant analogique et la propagation du signal RF, ce qui est possible grâce à l'extension *SystemC-AMS*. Cette solution simule avec beaucoup de précision le comportement du lien RF mais le temps de simulation est élevé. De plus, les composants numériques ne sont pas simulés avec autant de précision ; (2) représenter les signaux analogiques à l'aide de signaux numériques. Les signaux numériques n'ont qu'à stocker les paramètres les plus significatifs. Cela permet de simuler le système plus rapidement. Nous avons donc retenu cette option.

Pour représenter ce lien correctement, le signal entre le tag et le lecteur est séparé en deux parties :

- Le contenu : c'est le message échangé. La norme ISO-15693 permet de définir le contenu : il est composé par (1) des *flags*, (2) une *commande*, (3) des *paramètres*, (4) des *données* et (5) un *code CRC*. Toutes ces informations permettent au lecteur et au tag d'échanger des informations correctement.
- Le contenant : c'est le signal analogique transportant le message. La norme que nous utilisons définit les principales caractéristiques de ce signal tel que l'*encodage des bits* et la *modulation*. Nous rajoutons un paramètre à ceux définis par la norme : la *qualité* du signal. Ce paramètre permet, entre autre, de prendre en compte le bruit du signal.

L'architecture du simulateur est présentée sur la figure 2. On y voit un tag et un lecteur représentés avec leurs composants respectifs. Nous y voyons aussi l'interface avec le middleware. Enfin, nous pouvons voir le lien entre le lecteur et le tag (nommé couplage). Ce lien permet de faire transiter l'information (contenu + contenant) entre le tag et le lecteur, ainsi que la puissance que fournit le lecteur au tag.

L'intérêt de ce simulateur réside dans : (1) la simulation des composants internes de chaque élément du système, permettant ainsi d'observer les signaux internes des composants ; (2) la simulation de la partie analogique du système, permettant d'observer les signaux analogiques que s'échangent les tags et les lecteurs ; (3) et enfin d'avoir la possibilité de connecter ce simulateur à un middleware afin d'observer le système dans son ensemble.

4. Conclusion

La RFID pose un certain nombre de défis pour la recherche. Ceux-ci incluent la sûreté de fonctionnement des systèmes RFID, et, en particulier, la fiabilité et la

disponibilité du système RFID complet : logiciel et matériel, du tag jusqu'à l'application métier, en passant par le lecteur et le middleware. Nous avons regardé les fautes possibles d'un système RFID. Elles sont multiples et variables : elles peuvent être inhérentes à l'utilisation de composants électroniques (fautes dans la mémoire, dans la logique de contrôle), mais aussi à l'environnement dans lequel évolue le système (perturbation électromagnétique, etc.) et à la gestion des données (lecture, tri, sauvegarde, etc.). Pour aider à cette analyse, ainsi qu'à l'analyse des effets des modes de défaillance sur le système complet, nous avons développé un simulateur. Il permet la simulation des composants de chaque élément, et aussi de lien RF entre le tag et le lecteur, ainsi que le protocole de communication utilisé.

Par la suite, les effets des dysfonctionnements locaux sur le système complet devront être étudiés. Grâce à cela, nous pourrons proposer des stratégies de sûreté de fonctionnement : test, diagnostic et reconfiguration.

Une première piste de recherche est d'utiliser le taux d'erreurs de lecture des tags (TEL) et son maximum (TEL_{max}). En effet, de part leur nature, les systèmes RFID ont un TEL non nul. Par exemple, si le TEL_{max} est de 3/10, alors un tag sera considéré comme présent lorsqu'il est lu 7 fois sur 10. Une fois que le TEL_{max} est connu, il est possible de détecter des défauts et de les localiser grâce à un mécanisme de tests itératifs. Ainsi, et grâce au middleware qui permet de gérer tous les lecteurs et les tags, il est possible d'effectuer des statistiques sur le TEL de chaque tag et de chaque lecteur. En recoupant ces différentes mesures, il devient possible de détecter la défaillance et d'identifier son origine.

Une autre piste de recherche est d'adapter les techniques de test[2] intégré afin d'effectuer des tests en ligne. Par exemple, [13, 14]. Le document [15] propose aussi des tests en ligne de mémoires pour détecter les fautes classiques, mais uniquement pour les mémoires classiques et non pas pour les mémoires embarquées ayant de forte contraintes d'alimentation.

Références

[1] S. Preradovic, N. Karmakar and I. Balbin, *"RFID Transponders"*, Microwave Magazine, IEEE, (Octobre 2008) pp 90-103.

[2] http://www.fosstrak.org

[3] 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)

[4] http://wiki.aspire.ow2.org

[5] http://www.rf-it-solutions.com

[6] http://www.oatsystems.com

[7] J. Laprie, *"Le Guide de la Sûreté de Fonctionnement, 2e édition"*, CEPADUES (1996)

[8]B. Sood, D. Das, M. Azarian, M. Pecht, B. Bolton and T. Lin, *"Failure Site Isolation on Passive RFID Tags"*, 15th IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (2008) pp 337-341.

[9] http://www.rifidi.org

[10] C. Floerkemeier and S. Sarma, *"RFIDSim – a physical and logical layer simulation engine for passive RFID"*, IEEE Transactions on Automation Science and Engineering (Janvier 2009) pp 33-43.

[11] 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 (2007) pp 51-54.

[12] http://www.systemc.org

[13] J.M. Portal, H. Aziza and D. Nee, *"EEPROM memory: threshold voltage built in self diagnosis"*, Proceedings of the International Test Conference (2003) pp 23-28.

[14] C.W. Wang, C.F. Wu, J.F. Li, C.W. Wu, T. Teng, K. Chiu and H.P. Lin, *"A Built-In Self-Test and Self-Diagnosis scheme for embedded SRAM"*, Proceedings of the Ninth Asian Test Symposium (2000) pp 45-50.

[15] K. Thaller and A. Steininger, *"A transparent online memory test for simultaneous detection of functional faults and soft errors in memories"*, IEEE Transactions on Reliability (2003) pp 413-422.

[2] Techniques de BIST (Build-In-Self-Test) et de BISD (Build-In-Self-Diagnosis)