Université ABBES LAGHROUR Khenchela
Faculté des Sciences et de la Technologie
Département de Génie Industriel
جامـــعة عبـــاس لـــــغرور خـنـشـلة
كليـــة العلـــوم والتكنـــولـــوجيـا
قسم الهندسة الصنـاعية

N° Série :.....

Mémoire de fin d'étude

Présenté pour l'obtention du diplôme de Master

Filière : Télécommunications

Spécialité : Systèmes des Télécommunications

THEME

Etude et simulation d'une étiquette d'identification d'article par radiofréquence RFID comportant une antenne intégrée

Réalisé par :

BERRAH SAMIR

TAYANE OUAHID

Devant Le Jury :

Présidente: ***Dr. MAAMRI Fouzia***

Examinateur : ***Dr. BEDRA Sami***

Rapporteur : ***Dr. HASSAD Mourad***

Promotion 2020/2021

Remerciements

Nous remercions tout d'abord, Allah qui nous a donné la force et le courage afin de parvenir à élaborer ce modeste travail.

Nous tenons à remercier notre encadreur : M^{r}. HASSAD MOURAD maitre de conférences classe B à l'université ABESS LAGHROUR KHENCHELA pour nous avoir offert un cadre de travail agréable et un encadrement de qualité.

Nos mots de reconnaissance vont à M^{r} HASSAD MOURAD maitre de conférences classe B à l'université ABBES LAGHROUR, M^{me} MAAMRI FOUZIA ET M^{r} BEDRA SAMI pour avoir accepté de présider cet honorable jury.

Nous adressons de même nos remerciements à Mr maitre de conférences classe B à l'université ABBES LAGHROUR KHENCHELA, pour l'intérêt qu'il a bien voulu porter à ce travail en acceptant de faire partie du jury.

Nous adressons aussi nos remerciements à M pour son aide dans notre travail.

Enfin, nous remercions tous nos enseignants du département de télécommunication de l'université ABBES LAGHROUR KHENCHELA, sans oublier de citer tous les enseignants qui ont contribué à notre formation depuis l'école primaire jusqu'aux études universitaire.

Dédicaces

On a l'immense honneur de dédier ce mémoire :

À nos très chers parents qui étaient présents de nos côtés durant toute notre vie.

À nos frères et nos sœurs.

À mes très chers amies et collègues.

À tous mes connaissances.

À tous mes enseignants qui ont fait leurs possibles pour nous donner le maximum d'informations concernant notre étude.

À tous la promotion RT 2021.

Résumé :

La technologie RFID (Radio Frequency Identification) fait partie des technologies d'identification automatique. Les opérations de lecture et de détection et les mesures des capteurs sont inévitablement soumises aux erreurs. Nous étudions la tolérance aux fautes dans les systèmes RFID comme un moyen pour assurer la sûreté de fonctionnement. La tolérance aux fautes est l'ensemble des moyens pour que le logiciel fonctionne en dépit des différentes fautes (fautes physiques, fautes de conception, erreurs de l'utilisateur, fautes intentionnelles …). L'approche que nous développons consiste à concevoir un système de décision RFID distribué qui détecte et localise les défaillances en en comparant les résultats des inventaires des différents lecteurs, d'une part et d'autre part, comparer les résultats des différents capteurs homogènes en utilisant des techniques statistiques sur les résultats obtenus et permettre à l'application de détecter l'élément défectueux, corriger les fautes et continuer son exécution en présence de ces entraves. Pour tester et évaluer nos méthodes, nous avons conçu un mini- middleware SOARFID basé sur la SOA (Service Oriented Architecture) et nous avons intégré les modules d'analyse des données dans le module de filtrage et de collection.

Mots-Clés — Sûreté de fonctionnement, RFID, Tolérance aux fautes, Middleware, Services web, SOA.

Abstract

The operations of reading and detection of the readers and measurements of the sensors in a RFID system are inevitably subject to error. We study the Fault Tolerance (FT) in RFID systems as a mean to ensure the dependability. The approach that we develop consists to conceive a fault-tolerant distributed RFID system of decision that detects and locates faults by comparing the results of the inventories of different readers, first and second, compare the results of various homogeneous sensors by using statistical techniques on results and allow the application to detect the defective item, correct errors and continue its execution in the presence of these faults.

Keywords — Dependability, RFID, Fault-Tolérance , Middleware, web Services, SOA.

ملخص:

تعد تقنية RFID (تحديد الترددات الراديوية) إحدى تقنيات التعرف التلقائي. عمليات القراءة والاستشعار وقياسات المستشعرات عرضة للأخطاء حتمًا. نحن ندرس التسامح مع الخطأ في أنظمة RFIDكطريقة لضمان الموثوقية. تحمل الأخطاء هي مجموعة من الوسائل التي يمكن للبرنامج أن يعمل بها على الرغم من العيوب المختلفة (العيوب المادية، وأخطاء التصميم، وأخطاء المستخدم، والأخطاء المتعمدة، وما إلى ذلك). يتكون النهج الذي نطوره من تصميم نظام قرار RFID موزع يكتشف ويحدد حالات الفشل من خلال مقارنة نتائج قوائم جرد القراء المختلفين، من ناحية، ومن ناحية أخرى، مقارنة نتائج المستشعرات المتجانسة المختلفة في استخدام التقنيات الإحصائية على النتائج التي تم الحصول عليها والسماح للتطبيق باكتشاف العنصر المعيب وتصحيح العيوب ومتابعة تنفيذه في ظل وجود هذه العوائق. لاختبار أساليبنا وتقييمها، قمنا بتصميم البرمجيات الوسيطة الصغيرة SOARFID استنادًا إلى (SOA البنية الموجهة للخدمة) وقمنا بدمج وحدات تحليل البيانات في وحدة الترشيح والتجميع.

الكلمات الرئيسية ـ الموثوقية، RFID، تحمل الأخطاء، البرامج الوسيطة، خدمات الويب، .SOA

Sommaire

Sommaire

Chapitre I: Généralité Sur La Technologie RFID

Chapitre II: Etude théorique et simulation de la technologie RFID

Chapitre III: Conception et réalisation du système

Liste des figures

Liste des tableaux

Introduction générale

Introduction générale :

Les premières applications à grande échelle de la technologie RFID (Radio Frequency Identification) ont vu le jour durant les années 90 pour l'identification des animaux, principalement les bovins et ovins, dans les systèmes de contrôle d'accès dans les immeubles ou les autobus, la logistique, ou encore pour la protection contre le vol [1]. Les études de marché annoncent une utilisation accrue de cette technologie dans les années à venir et ce dans divers domaines de la vie courante.

Le principe de base du fonctionnement de la RFID est simple. Il s'agit d'échanger des informations numériques à moyenne distance par radiofréquence ; ces informations devront être contenues sur un support de très petite taille et de très faible coût [2]. Cette technologie offre la possibilité de faire de la lecture multiple (lecture de plusieurs objets simultanément) et la vision directe n'est pas nécessaire.

Au minimum, l'infrastructure RFID comporte des étiquettes, des lecteurs, un middleware et des applications fonctionnant par exemple, sur des serveurs d'entreprise.

Un système RFID simple est composé de deux parties :

- Un élément communément appelé transpondeur, étiquette communicante ou tag qui se compose d'une antenne et d'une puce électronique contenant des informations.

- Un appareil de lecture communément appelé interrogateur, base station ou lecteur qui permet de lire et d'écrire les informations numériques dans la puce du transpondeur.

Les éléments d'un système RFID - antennes, tags, lecteurs - sont rarement utilisés seuls. En fait, seule leur utilisation dans le cadre de systèmes de production ou de distribution complexes est susceptible d'apporter une grande plus-value. Ainsi, les différents systèmes RFID utilisés dans les systèmes de production sont généralement constitués de réseaux locaux (regroupement de plusieurs lecteurs) et globaux (regroupement de plusieurs réseaux locaux) ainsi que d'applications utilisant les données collectées. Dans ce contexte, les middlewares (ou inter logiciels) permettent de transférer les données capturées d'un lecteur vers une base de données [3]. Ces middlewares constituent le lien entre le monde matériel et le monde logiciel. L'inter logiciel RFID, est indispensable pour trois raisons principales :

1. La nécessité de filtrer les lectures doubles et l'information redondante afin d'éviter la transmission de l'information non nécessaire pour les applications, et en même temps optimiser les ressources du réseau.

2. La nécessité d'une interface pour prendre en compte des lecteurs, des étiquettes et des dispositifs dans un environnement à plusieurs fournisseurs hétérogènes.

3. La nécessité de passer et d'acheminer des flux de données RFID à différentes applications et bases de données.

Alors le middleware RFID joue un rôle crucial en assurant plusieurs tâches. Il constitue le cerveau de la chaîne logicielle qui confère de l'intelligence aux données récupérées sur les produits étiquetés d'une puce radiofréquence [3].

Parmi les propriétés attendues des services offerts par les systèmes RFID : la sûreté de fonctionnement. La sûreté de fonctionnement est " la propriété qui permet de placer une confiance justifiée dans les services que délivrent ces systèmes" [4]. Malheureusement, les opérations de lectures et de détection et les mesures de capteurs sont inévitablement soumises aux erreurs. Une faute peut être définie comme une valeur arbitraire d'une opération de détection ou d'inventaire par un lecteur ou d'une mesure incohérente par un capteur, qui ne peut pas être compensée systématiquement. L'une des techniques de sûreté de fonctionnent que traite ce travail est la tolérance aux fautes. La tolérance aux fautes peut être définie comme la : "méthode qui permet à un système de remplir ses fonctions en dépit des fautes pouvant affecter ses composants, sa conception ou ses interactions avec des hommes ou d'autres systèmes"

La plupart des travaux sur la tolérance aux fautes ont été conçus et évalués dans les réseaux des capteurs. Nous nous intéressons dans ce travail à deux travaux faits. Le premier est le travail présenté dans [6] qui présente une technique basée sur la validation pour la détection en ligne des fautes des capteurs. Le deuxième travail est celui présenté dans [7] dans lequel les auteurs traitent la tolérance aux fautes distribuée dans les réseaux de capteurs. Peu de travaux ont étudié la tolérance aux fautes dans les systèmes RFID, la plupart des solutions dans ces systèmes traitent le manque de fiabilité inhérent dans les technologies de RFID. Les auteurs dans [8] ont étudié le comportement incertain des dispositifs de RFID et ils ont conçu et ont mis en application un inter logiciel RFID appelé RF2ID (infrastructure fiable pour

l'identification par radiofréquence) pour organiser et soutenir des requêtes sur des flux de données d'une façon efficace.

L'approche que nous développons consiste à concevoir un système de décision RFID tolérant aux fautes et distribué qui détecte et localise les défaillances en comparant les résultats des inventaires des différents lecteurs, d'une part et d'autre part, en comparant les résultats des différents capteurs homogènes en utilisant des techniques statistiques non paramétriques sur les résultats obtenus. Ce qui permet à l'application de détecter l'élément défectueux, corriger les fautes et continuer son exécution en présence de ces entraves.

I. OBJECTIF PRINCIPAL

L'objectif de notre travail est d'assurer la sûreté de fonctionnement d'un système RFID en développant des modules d'analyse de données statistiques fonctionnant au niveau du middleware et précisément dans le module de filtrage et de collection.

Pour réaliser la tolérance aux fautes de manière extensible et distribuée, nous proposons un schéma de détection dans lequel nous utilisons la technique de redondance logicielle avec utilisation d'un middleware qui analyse les données provenant des stations. Nous utilisons aussi la redondance matérielle passive. Si les valeurs obtenues pour un lecteur ou pour un capteur n'appartiennent pas à un intervalle de confiance calculé par la méthode percentile, ce lecteur ou ce capteur est considéré défectueux. Le middleware peut inventorier les étiquettes, prendre une décision binaire concernant l'événement étudié (événement ou non-événement) et détecter en ligne les lecteurs et les capteurs défectueux.

Le résultat global est alors le développement d'un inter logiciel RFID plus complexe qui tolère les fautes qui peuvent survenir aux différents niveaux d'un système RFID, et qui prend des décisions finales fiables malgré la présence de fautes.

Puisque notre système peut recouvrir plusieurs sites géographiques pour prendre des décisions sur plusieurs événements, notre middleware ainsi que notre application doivent être distribués. Nous utiliserons pour cela l'architecture SOA (Service Oriented Architecture) [11].

II. ORGANISATION DU MÉMOIRE

Le chapitre I décrit les concepts nécessaires pour familiariser le lecteur aux contextes de la RFID et lui permettre de suivre sans difficulté le reste du mémoire. Ce chapitre présente la terminologie utilisée dans le mémoire. Ce chapitre commence par définir la technologie RFID

qui fait partie des technologies d'identification automatique, que l'on appelle aussi AIDC (Automatique l 'identification and Data Capture).

Ensuite, il décrit les différents éléments de l'infrastructure RFID : les étiquettes, les capteurs, les lecteurs et les middlewares RFID. Il réalise à la fin une synthèse sur les middlewares les plus connus.

Le chapitre II présente, en particulier, la notion de sûreté de fonctionnement et les méthodes statistiques utilisées. La première section de ce chapitre présente brièvement les concepts de base de la sûreté de fonctionnement. Elle donne quelques techniques de sûreté de fonctionnement et de tolérance aux fautes. Sa deuxième section discute la tolérance aux fautes à deux niveaux d'abstraction (le matériel et l'inter logiciel). Les travaux sur la tolérance aux fautes au niveau des systèmes RFID, les travaux faits et évalués sur la tolérance aux fautes dans les réseaux de capteurs et dont nous nous sommes inspirés sont décrits dans ce chapitre.

Le chapitre III présente notre contribution : Tolérance aux fautes distribuée à base de redondance matérielle, les composants matériels principaux et la méthodologie proposée pour palier au problème de la tolérance aux fautes dans les systèmes RFID. Ce chapitre alors propose un schéma de détection pour réaliser la tolérance aux fautes de manière extensible et distribuée dans lequel la technique de redondance logicielle est utilisée avec l'utilisation d'un middleware qui analyse les données provenant des lecteurs et des capteurs RFID. Un exemple d'illustration et de validation est ensuite fourni.

Une Conclusion clôture ce travail et souligne les principales perspectives et l'aspect recherche liée à la sûreté de fonctionnement dans les systèmes RFID.

La problématique

L'étiquette d'identification d'article par radiofréquence RFID comportant une antenne intégrée.

Une étiquette d'identification par radiofréquence utilise une antenne formée en association avec, et donc intégrée à, un article, un emballage, un conteneur d'emballage, une étiquette et / ou un badge d'identification. Dans un mode de réalisation préféré, un ensemble de puce de circuit d'étiquette d'identification par radiofréquence est fixé à l'article et est couplé électriquement à l'antenne formée sur l'article. L'impression d'un motif conducteur sur l'article en utilisant une encre conductrice forme une antenne préférée.

Chapitre I :

Généralité Sur La Technologie RFID

I.1 Introduction

Les entreprises ; soucieuses d'apporter à leurs clients un niveau de service toujours plus élevé et souhaitant assurer la transmission des informations ; font aujourd'hui face à un défi majeur : suivre en temps réel les produits qu'elles produisent ou distribuent.

Les contraintes réglementaires ou de rentabilité incitent les entreprises à améliorer leurs méthodes de gestion. La logistique n'échappe pas à cette tendance et cette fonction, longtemps oubliée par les dirigeants est au centre des préoccupations actuelles.

La RFID, « Radio Frequency Identification » est aujourd'hui l'un des axes d'amélioration de la gestion de la logistique amont. La connaissance et la compréhension de cette technologie sont encore faiblement diffusées. Certaines entreprises apparaissent enthousiastes vis à vis de cette innovation, d'autres sont plus méfiantes. Pourtant, les champs d'applications sont nombreux et l'ensemble de la chaîne logistique devrait pouvoir bénéficier des apports de cette technologie.

Créée lors de la seconde guerre mondiale la RFID a connu une longue période pendant laquelle elle est restée en sommeil. Les années **2000** marquent l'entrée de cette technologie dans la réalité de l'entreprise.

Quelles sont les champs d'applications de la RFID au niveau de la logistiquement ?

Après avoir fait un état des lieux de la technologie, nous listerons les avantages de ce système et les applications possibles dans le domaine de la supplychain avec notamment l'étude de projets mis en place par des entreprises. Enfin nous définirons les modalités d'implantation ainsi que les perspectives d'avenir pour la RFID.

I.2 Principes de fonctionnement

I.2.1 Historique

La RFID n'est pas une technologie nouvelle, elle était déjà utilisée lors de la seconde guerre mondiale avec les transpondeurs servant à identifier les avions. Ainsi, la Royal **Air** Force et l'armée américaine l'utilisaient déjà afin de différencier ses avions de ceux des ennemis« Friend or Foe » (ami ou ennemi). Jusque dans le milieu des années 90, cette technologie n'a pas été répandue. Mais les évolutions technologiques se sont faites rapidement et au cœur du Medialab, basé au Massachusetts Institute of Technology (MIT), des chercheurs ont inventé une carte de visite déplacée machinalement au-dessus d'un certain

tapis de souris et les informations apparaissent dans le carnet d'adresses électronique. L'objet a eu tant de succès que ses trois inventeurs ont fondé fin **1998**, Presto Technologies, une startup qui se chargera de mettre le tapis sur le marché. Comme les détecteurs antivol dans les magasins, le tapis Presto envoyait des ondes électromagnétiques vers les « tags », qu'une bobine en forme de spirale captait et transformait en signal électrique chargé de dialoguer avec la puce avant de récupérer ses informations.

L'équipe Things That Think (les choses qui pensent) du MIT a largement développé les étiquettes RFID. Aujourd'hui, cette technologie est souvent appelée étiquette intelligente et on la retrouve actuellement dans de nombreuses situations. Ainsi nous sommes identifiés par nos déplacements par des badges d'accès aux entreprises ou par le passNavigo de la RATP à Paris. Elle est aussi présente dans la lingerie industrielle, les bibliothèques, le verrouillage des voitures ou le télépéage autoroutier. De même, la chaîne alimentaire en France est l'une des plus surveillée du monde et tout ce que nous mangeons est tracé depuis les champs jusqu'au supermarché. C'est le développement de la technologie grâce à l'utilisation de fréquences et de normes adaptées qui permet aujourd'hui une optimisation des lectures de quelques dizaines de centimètres à quelques mètres.

I.2.2 Description technique

La RFID est une technologie de pointe visant à assurer l'identification détaillée d'objets de tous types. La RFID permet de procéder à une saisie de données rapide et automatique grâce aux ondes radio. Dans sa version la plus simple, cette étiquette intelligente associe une mémoire, contenue dans un microprocesseur, à une antenne miniature permettant de transmettre les données par fréquences radio et à un mécanisme de production d'énergie. Ce dernier permet d'abaisser son coût et d'augmenter sa durée de vie en se passant de batterie. En effet, c'est l'appareil de lecture à distance qui va réveiller la puce en lui transmettant un champ électromagnétique. Celui-ci est aussitôt converti en énergie, suffisante pour que l'étiquette puisse adresser en retour au lecteur un signal radio qui contient toutes les informations souhaitées.

La distance à laquelle peut être effectué le contrôle dépend de la longueur d'onde radio utilisée : elle varie entre 10 centimètres et une dizaine de mètres selon les quatre fréquences autorisées par lesnormes internationales. Les étiquettes RFID sont dotées d'une mémoire dans certains modèles. Le tag est toujours activable. A chaque fois qu'un signal est émis par l'antenne d'un lecteur, le tag réagit en communiquant les données qu'il contient. La

technologie RFID peut aussi autoriser un véritable dialogue entre le lecteur et la puce, dont le contenu pourra alors être reprogrammé à volonté. Le contenu du tag est ainsi décrypté, voir modifié, par le lecteur, à chaque passage près de celui-ci, automatiquement. Les informations contenues dans le tag peuvent donc être transférées via Internet aux intéressés qui se chargent du traitement des données.

Actuellement quatre gammes de fréquences radio sont principalement utilisées en RFID. Leur différence tient surtout dans la distance et la vitesse de lecture. La basse fréquence (125 kHz) permet une lecture seule de 20 à 50 cm. La haute fréquence de 13,56 MHz associe soit une grande vitesse à petite distance soit une vitesse moyenne jusqu'à 70 cm de distance. Nous trouvons aussi l'ultra haute fréquence de 800 à 950 MHz avec des lectures de 2 à 5 mètres et l'hyper fréquence de 2,4 à 5,8 GHz pour de plus grandes distances encore.

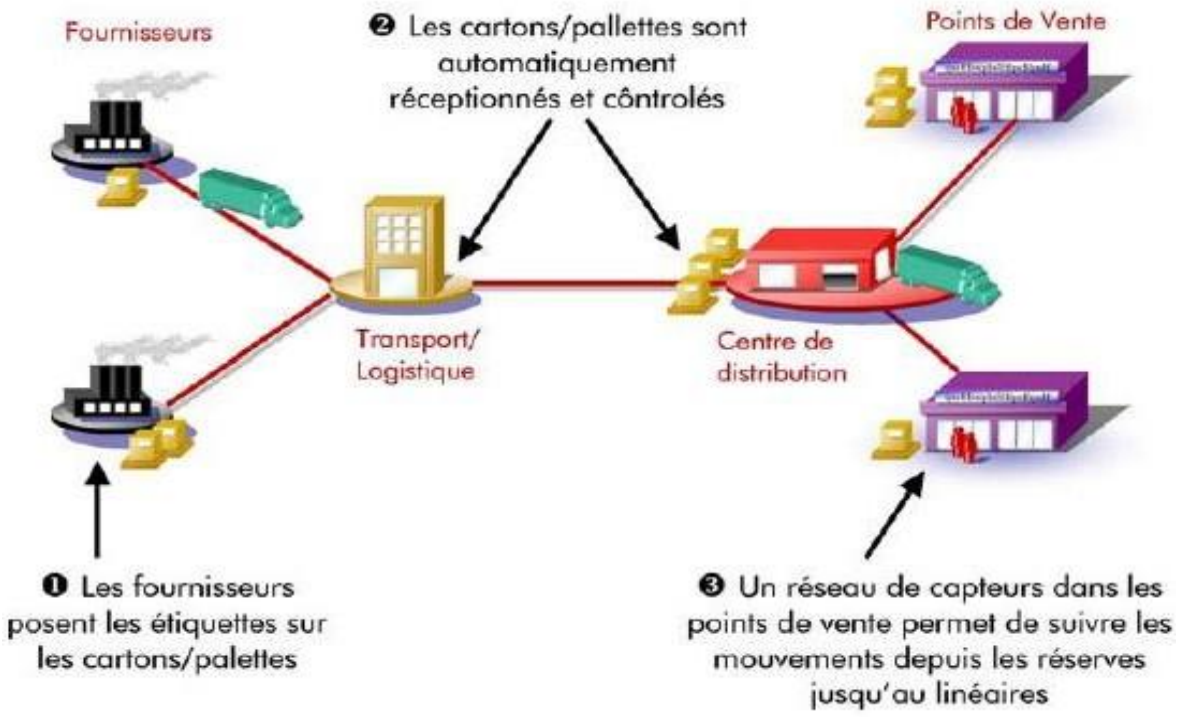


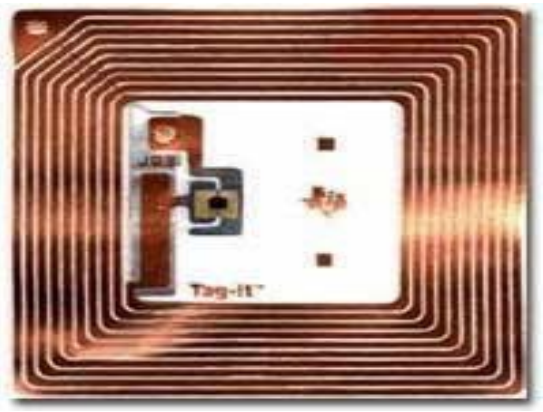
Figure I.1: Principe général de l'utilisation de la RFID

I.2.3 Les différents modèles de puce

Les puces RFID sont composées de **2** éléments principaux : la puce électronique qui contient les données et l'antenne qui transmet les informations au lecteur. Il existe aujourd'hui plusieurs types de puces RFID. Ces différents modèles permettent aux utilisateurs de s'adapter en fonction de l'environnement dans lequel ils utilisent cette technologie. De nombreuses puces existent, ellespeuvent être aussi grosses qu'un grain de riz ou aussi lourdes qu'une brique. Leur autonomie et leur performance varient fortement selon les modèles.

On peut différencier **3** types de puces :

- Active
- Passive
- Semi active



a) Les puces passives

Les puces passives ont pour caractéristique principale de ne pas avoir de système d'alimentation (une batterie par exemple). Ces puces utilisent donc l'énergie du lecteur pour transmettre les données. Ces tags ont donc une durée de vie longue et peuvent être lues à une distance comprise entre quelques centimètres jusqu'à **9** mètres.

Ces puces possèdent également une antenne qui permet de conduire l'énergie du lecteur vers la puce. La taille de cette antenne dépend de l'utilisation que l'on veut faire de l'étiquette RFID. Selon les conditions d'utilisation et la distance de lecture voulue, l'antenne sera plus ou moins longue.

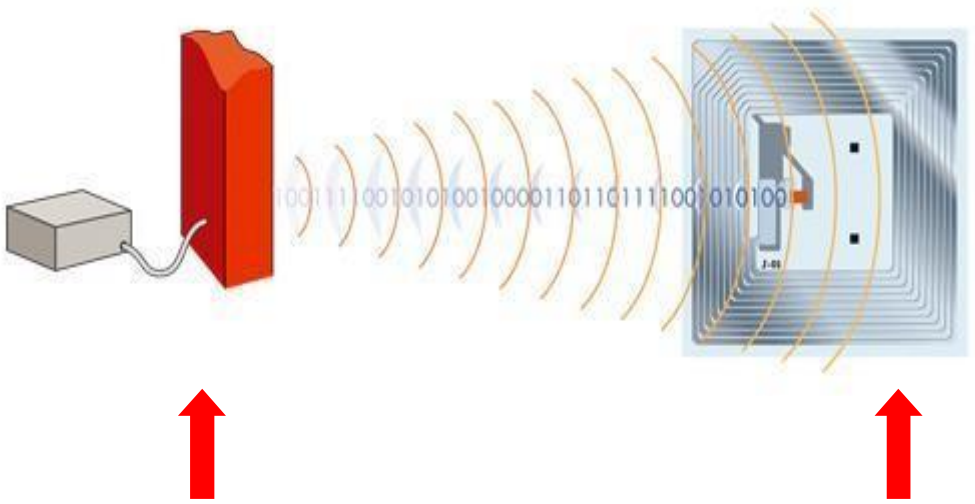


Figure I.2: Lecteur Puce RFID

b) Les puces actives

La puces active, à l'inverse de celle passive possède sa propre source d'énergie. Cette source d'énergie peut être solaire ou sous forme de batterie. L 'avantage de ces étiquettes est qu'elles transmettent leur information en continu et elles ne nécessitent pas la présence d'un

lecteur pour fonctionner. Un mode « veille » existe sur ce type d'étiquette afin d'économiser la source d'énergie. Elles ont de plus comme avantage de pouvoir être lues à une distance plus grande.

Désavantage de la technologie, la multiplication des ondes dans un environnement peut créer des interférences. En effet, si la puce communique en continu, le nombre de message dans un entrepôt peut être trop important.

c) **Les puces semi actives**

Ces étiquettes sont bien sûr à mi-chemin entre les deux technologies vues ci-dessus. L'étiquette possède une source d'énergie propre mais nécessite un lecteur pour émettre les données qu'elle contient. L'avantage de cette technologie par rapport à une étiquette passive est qu'elle sera lu beaucoup plus vite et surtout à une distance plus longue. Le tag semi-actif n'ayant pas besoin de l'énergie du lecteur pour être activé, elle pourra être utilisé dans des conditions particulières comme la lecture à grande vitesse et sera beaucoup plus efficace lors de l'utilisation de matériaux opaques ou absorbants

I.3 Les différentes utilisations des puces RFID

Il existe **3** types d'utilisation de ces puces.

- Lecture seule
- Ecriture unique et lecture multiple
- Lecture/Ecriture

I.3.1 La lecture seule

La « lecture seule » est la technologie la plus simple. Elle consiste en une étiquette contenant des données qui peuvent être lues par un lecteur mais sans possibilité de les modifier. L'étiquette est bloquée dès sa fabrication. Ce sera donc l'entreprise qui la fabrique qui entrera les données dans la puce et qui bloquera cette dernière. Ce type d'étiquette s'adresse donc plutôt à de grands volumes et à une utilisation de masse comme dans la grande distribution.

I.3.2 Les puces WORM

Les puces WORM (Write Once, Read Many) permettent à l'utilisateur d'entrer les données dans la puce au moment de son utilisation. L'écriture se fait donc en une seule fois et

regroupe l'ensemble des informations. Pourtant il existe également des étiquettes WORM auxquelles on peut ajouter certaines informations sans pouvoir modifier celles déjà existantes. Cela offre une plus grande flexibilité dans l'utilisation de ce type de technologie.

I.3.3 Les puces Lecture/Ecriture

Enfin, les étiquettes les plus complexes permettent la lecture et l'écriture. Les opérations peuvent être répétées entre **10 000** et **100 000** fois selon le modèle utilisé. On peut même penser qu'il sera possible dans quelques années d'avoir des étiquettes utilisables des millions de fois. Cette possibilité est donc un avantage précieux pour les entreprises désireuses d'utiliser la technologie RFID. Seul problème actuel pour l'utilisation des étiquettes « Lecture /Ecriture », leur coût qui reste encore assez élevé.

On peut donc voir que la technologie des puces d'identification par radiofréquence est étendue et permet de s'adapter à des situations différentes. De plus, la recherche dans le domaine de la RFID est en constante évolution et apportera donc dans les années à venir des améliorations continues notamment dans le domaine de la fiabilité, de la miniaturisation et de l'autonomie.

I.4 Les outils nécessaires à l'utilisation de la RFID

I.4.1 Les imprimantes d'étiquettes

La RFID prend sa source chez les fondeurs de silicium tels que AMI, Atmel, EM Micro électronic Marin, Fuji Tsu, Hitachi, Impinj, Infineum, Philips, Sames, Sony, STMicroelectronics, Texas Instruments. Ces industriels produisent les tranches de silicium à partir desquelles on construit les puces électroniques pour fabriquer des tags. Ensuite interviennent les producteurs d'étiquettes ou autres supports dans lesquels s'intègrent les puces. Les acteurs de ce secteur sont innombrables : ASK, Assa Abloy, IER, Intermec, Omron, Rafsec, Siemens, Tagsys, Texas Instruments et autres AllienTechnology, Zebra, Balogh et Matrics Inc.

Aujourd'hui, l'utilisation de la technologie RFID se fait au travers l'utilisation d'étiquettes . Ce sont et ce seront dans un avenir proche les puces les plus utilisées. Les étiquettes RFID sont imprimées et les données peuvent être encodées soit en même temps que l'impression de l'étiquette soit après l'édition de cette dernière. Un lecteur prévu pour encoder permet de mettre les données dans la puce. Cependant, il existe des imprimantes d'étiquettes qui offre une solution globale d'impression de l'étiquette et d'encodage

Figure I.3: l'étiquette et d'encodage

Associé au système informatique de l'entreprise contenant les données à mettre dans la puce, ce type de machine est donc une solution idéale pour l'édition d'étiquettes. On évite ainsi les risques d'erreurs puisque les puces sont encodées lors de la création de l'étiquette. L'encodage des puces après l'édition de ces dernières peut donner lieu à une confusion entre les différentes étiquettes.

Figure I.4: DATAMAX RFID Printer Encoder.

La combinaison des technologies RFID et Code à Barre sera à court et moyen terme obligatoire pour les entreprises désireuses d'introduire la RFID dans la gestion de leur supplychain. Les spécialistes de l'impression d'étiquettes l'ont bien compris et proposent donc des imprimantes en mesure d'imprimer des étiquettes intelligentes, intégrant puce et antenne mais aussi un code à barres, textes et graphiques si nécessaire

I.4.2 Les lecteurs de puces

Le lecteur est un élément essentiel pour l'utilisation de la RFID. Il envoie un signal à la puce RFID et dans le cas de puce passive, il fournit également l'énergie nécessaire pour, que la puce envoie les informations qu'elle contient. Les lecteurs peuvent prendre des formes diverses. N'ayant pas besoin d'être en contact direct avec la puce, les lecteurs sont le plus souvent fixes. Sous forme de portiques à l'entrée ou à la sortie des entrepôts ou de bornes fixes, ces lecteurs ont des capacités diverses et variées.

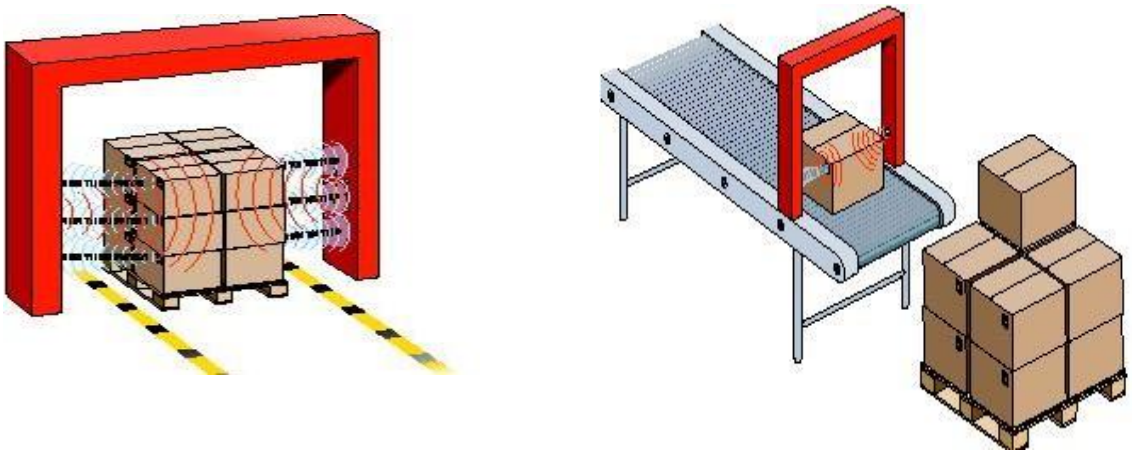


Figure I.5: Lecteurs RFID sous forme de portique

Il existe aujourd'hui de nombreuses entreprises offrant des produits adaptés à chaque projet. L'offre contient des lecteurs mobiles, sous la même forme que les « flachers » portatifs de codes à barres. Certains matériels combinent les **2** technologies, code à barres et RFID. Enfin, on peut même noter l'existence de lecteur que l'on peut adapter sur des PDA ou PALM et communicant directement avec le réseau de l'entreprise.

Permettant la lecture des puces RFID et des Codes à barres Produit PSC Inc[1]

I.5 Les avantages de la RFID par rapport au code-barres

I.5.1 la lecture des données

a) **La lecture à distanc**e

L'avantage principal de la technologie RFID par rapport au code à barres se situe au niveau de la lecture. Tout d'abord, la lecture des puces RFID ne nécessite pas un flashage systématique de toutes les étiquettes. Pour la réception de marchandises, des contrôleurs scannent chaque palette, carton ou produit un par un pour effectuer l'entrée en stock. Il en va de même pour les inventaires ou chaque produit doit être scanné pour entrer dans la base de données. Cela pose bien sûr des problèmes logistiques surtout dans le cas de traitement de

grands volumes. En plus l'intervention humaine peut donner lieu à des erreurs et donc à une mauvaise analyse des données. La puce RFID peut être lue à distance et donc bien plus rapidement. Les distances de lecture varient selon les fréquences utilisées, de quelques centimètres à plusieurs dizaines de mètres.

b) **La lecture de masse**

Tous les experts sont unanimes, le potentiel de la RFID va bien au-delà d'une simple automatisation des applications de lecture actuelles. Elle permet d'inventer de nouveaux modes d'identification. De par sa capacité à identifier simultanément et à distance des objets, qu'ils soient visibles ou "cachés", elle multiplie les schémas de lecture possibles. En matière de lecture RFID, il convient de distinguer deux grandes catégories d'application : les applications de lecture unitaire : le lecteur identifie un objet à la fois. La RFID permet, en premier lieu, une simplification du processusde lecture tel qu'il existe aujourd'hui avec le code à barres. Un lecteur RFID peut identifier un objet sans intervention humaine, ni automatisme supplémentaire; · les applications de lecture simultanée : le lecteur identifie plusieurs objets à la fois. La RFID offre ainsi des perspectives nouvelles. Elle permet d'identifier les composants d'un regroupement d'objets et plus seulement le regroupement lui-même. On parle dans ce cas de lecture en masse. Qu'il s'agisse d'identifier des unités consommateursdans un carton ou des cartons sur une palette, la lecture en masse représente un saut qualitatif sans précédent.

Actuellement, le marquage code à barres ne permet pas, pour des raisons de performance et de productivité, de multiplier les points de lecture, en dehors des opérations de constitution des palettes. En effet, chaque contrôle d'une unité d'expédition nécessiterait son démantèlement puis sa reconstitution à l'identique. La lecture en masse permettrait, a contrario, de multiplier les points de contrôle de façon presque transparente pour les organisations.

Les derniers tests effectués par GS1 France sur la lecture de masse démontre que pour les produits dit neutres, c'est à dire qui n'émettent pas d'interférences, le taux de lecture d'une palette est de **100** %.

Enfin les puces RFID sont mieux protéger. La variété de packagings utilisables pour protéger les puces RFID apporte une réponse concrète à cette préoccupation. Située dans l'étiquette ou un autre support, elle résiste mieux aux détériorations dues à la manipulations des unités logistiques. Pour les codes à barres, la qualité est très importante. Si le taux de lecture des codes à barres est élevé, en cas de destruction partielle du code à barres, les

données peuvent ne plus être lues par le lecteur. De plus, les étiquettes RFID ne sont pas forcément placées en évidence que les unités logistiques puisque le contact direct avec le lecteur n'est pas obligatoire.

I.5.2 Les données contenues dans la puce RFID

c) Une capacité de stockage supérieure

La technologie du code à barres a fait ses preuves depuis maintenant plus de 30 ans mais elle connaît également des limites au niveau des informations qu'elle contient. C'est pourquoi la RFID apparaît comme un alternative offrant des possibilités largement supérieures. Avec une capacité de stockage qui varie de 1 Ko jusqu'à plusieurs dizaines voir centaines de Ko, les possibilités d'écriture d'informations sont infinies. On peut ainsi noter tout au long du cycle de vie de la puce de nombreuses informations concernant le ou les produits. Des matières premières utilisées jusqu'à la date d'enlèvement en entrepôt, toutes ces informations peuvent être stockées dans la puce RFID. Pour cela, l'utilisation de puce réutilisable et permettant l'ajout de données au fur et à mesure est nécessaire. Il est égalementpossible de coupler les puces RFID contenant le code EPC unique à une base de donnée centrale. Avec ce système, il est suffisant d'utiliser des puces à écriture unique. Les données sont alors ajoutées au fur et à mesure dans la base de données.

La RFID propose donc une technologie qui s'adapte en fonction des besoins de l'entreprise, le large spectre des options la démarque du code à barre qui est bien plus limitée. Pour le transport par exemple, une palette devra recevoir un nouveau code- barres si l'un des éléments est enlevé ou si certains sont ajoutés. Cela nécessite donc une manipulation supplémentaire en cas de changement.

d) Des puces réutilisables

Les puces RFID sont également réutilisables selon les modèles. En fonction les besoins de l'entreprise, l'utilisation de ce type de puces réinscriptibles s'avère être une solution parfaitement adaptée. La gestion des supports de manutentions en est l'un des meilleurs exemple. Pour des raisons d'efficacité, il est important que la technologie utilisée pour identifier les supports reste opérationnelle durant l'intégralité de la vie du support. De plus le coût unitaire de chaque puce ne représente plus une limite d'utilisation puisque ce type de puce peut être utilisée jusqu'à **100000** fois.

e) Une meilleure utilisation des données

C'est sûrement l'avantage principal de la puce RFID, le traitement des données en direct offre des possibilités très importantes pour les entreprises. En effet, là où le scannage est obligatoire pour le code-barres, la RFID permet de connaître la situation en temps réel, que ce soit pour le transport, le stockage ou tout autre aspect de lachaîne logistique. Le mécanisme de suivi de la traçabilité ; c'est à dire la capacité à suivre le mouvement de produits individuels ou de conteneurs tout au long du processus de leur distribution et de leur livraison, à présenter des états sur ces mouvements et à répondre à toute requête correspondante ; est primordial pour les entreprises. Ce suivi permet notamment la compréhension des erreurs et offre les outils nécessaires pour améliorer la chaîne dans son ensemble. Le suivi en temps réel est par conséquent un gain de temps pour l'entreprise et donc une meilleure réactivité face aux problèmes.

La possibilité d'intégrer un système de tracking par GPS ou tout autre outil de mesure dans ces puces est également une grande avancée en terme de suivi et de traçabilité des produits. Les entreprises pourront ainsi suivre leurs produits en temps réel et être plus réactives si des problèmes survenaient. La transmission de l'information étant plus rapide, la capacité de réaction l'est également.

f) Une technologie difficilement reproductible

La contrefaçon est encore l'un des domaines ou la RFID possède un avantage sur le code à barres. La reproduction des codes à barres est relativement facile puisqu'ils utilisent une technologie très simple. L'expertise nécessaire pour la fabrication de puce RFID demanderait alors un investissement et des compétences difficiles à réunir. De plus les numéros EPC par exemple sont particulièrement difficile à reproduire

g)Les limites de la RFID par rapport au code-barres

Nous avons pu constater que le RFID avait un certain nombres d'avantages par rapport au code à barres. Cependant, cette technologie est aujourd'hui en pleine expansion et comme toutes les nouvelles technologies, présente des défauts dejeunesse mais aussi certaines limites techniques. Enfin, la RFID manque également de repères et de standard quant à son utilisation.

I .5.3 Les limites techniques

Le code à barres bénéficie d'une longue histoire et par conséquent d'une expérience importante des entreprises pour son utilisation. Ce n'est pas le cas de la RFID qui est encore en phase de découverte. La technologie s'améliore de jour en jour et les chercheurs trouvent de nouvelles solutions pour améliorer ce produit.

L'une des premières limites techniques est celle associée aux interférences. La RFID fonctionne par ondes et certaines matières endommagent le message transmis par la puce au lecteur. Voici les différents cas de figures ou la RFID ne fonctionne pas correctement.

a) La lecture avec des produits à forte teneur en eau

L'eau présente comme caractéristique d'absorber les signaux émis par les puces RFID. Le taux de lecture est alors fortement diminué. La présence d'humidité dans un container ou sur une palette pourrait également perturber la lecture du contenu des puces. Cette point négatif pose des limites pour l'utilisation du marquage par radiofréquence sur certains produits. Les produits surgelés sont également concernés, les puces résistent mal à l'humidité et au froid généré par ce type de produits.

b) Les produits avec un emballage métallique

La présence de métal à proximité des puces RFID dérègle le fonctionnement de leur antenne. Cette antenne qui permet à la puce de transmettre les données mais aussi de s'activer par l'énergie envoyée par le lecteur (pour les puces passives). Là aussi, le taux de lecture est fortement réduit.

De plus, comme pour les produits à forte teneuren eau, le métal provoque des interférences qui réduisent également le taux de lecture pour des palettes complètes par exemple.

c) Une lecture de masse imparfaite

On constate dans certains cas que la lecture de masse n'offre pas une fiabilité maximum. Si les conditions sont optimums, donc sans aucun liquide et sans présence de métal, on considère qu'il est possible de lire plus d'une centaine de puces RFID en même temps. Par contre, la présence d'éléments perturbateurs oblige à diminuer le nombre de puce lues

d) **L'utilisation des fréquences**

L'utilisation, des fréquences, voilà une contrainte qui apparaît souvent lorsque les nouvelles technologies utilisent les ondes. On avait déjà observé ce problème pour l'utilisation de masse des téléphones portables dans les années 90. L'armée avait bloqué certaines fréquences en France. Le problème se reproduit pour la RFID puisque l'armée tarde encore à autoriser l'utilisation des fréquences nécessaires. Ce retard entraîne une difficulté de déploiement de la technologie en France. Cependant, on a appris que l'armée venait de libérer au début de l'année la fréquence **865-868** MHz utile pour la technologie développée par GS1 avec sa puce Gen**2.** Une bonne nouvelle pour le l'introduction de la RFID en France. Mais ce problème risque de se reproduire dans le futur ou d'autres fréquences seront utilisées. Les industriels pourraient retarder leurs projets à cause de cette contrainte.

e) **La RFID piratable ?**

Une équipe de chercheur néerlandais a réussi à créer le premier virus pour les puces RFID. La puce transmettant les données qu'elle contient, les chercheurs ont tenté de prouver qu'elle pouvait au moment de sa lecture infecter l'ensemble d'un système informatique. Les chercheurs ont réussi à introduire ce virus dans une base dedonnées Oracle qu'ils avaient utilisé pour faire un test.

Alors faut-il s'inquiéter de cette découverte ? La RFID sera t-elle menacée par ces virus?

«Cette opération a été réalisée dans des conditions techniques et avec des équipements spécifiques. Il me semble peu probable qu'un virus comparable apparaisse dans les mois à venir en dehors des laboratoires spécialisés [6]» constate François Paget chercheur chez l'éditeur antivirus McAfee France. Ce premier test aura au moins le mérite d'interpeller les acteurs du marché

I.5.4 Le prix des puces

L'utilisation d'une nouvelle technologie représente toujours un défi mobilisateur dans l'entreprises. Cette innovation dans l'entreprise permet de renouveler les procès,on a pu voir que la RFID offrait certaines opportunités dans ce domaine, mais la question du coût est essentielle.

Aujourd'hui, le principal frein au développement de la RFID est son prix. Technologie encore récente et peu utilisée au vue des prévisions pour le futur, les puces conservent un prix

élevé. Roland Dashs, président de l'Aslog (Associations de logisticiens français) le confirme, « A terme, ce sera un apport indéniable mais, investir dans un nouvel outil ne se justifie que s'il crée de la valeur ajoutée. Pour la RFID, il ne faut pas sous-estimer le coût des nouvelles organisations nécessaires au nouvel outil[7] » Le prix des puces est très variable étant donné la multitude de produit disponible sur le marché. Les puces réinscriptibles ou modifiables n'ont bien sûr pas le même prix que celles à utilisation unique. On observe donc des prix variant de **15** centimes d'euros voir moins pour les puces les plus basiques à quelques euros pièce pour les plus sophistiquées. Evidemment, le prix peut paraître peu élevé à l'unité mais si l'on rapporte ce prix à des volumes importants, l'investissement devient conséquent. A cela, il convient d'ajouter l'ensemble des investissements nécessaires à l'utilisation des puces (imprimantes, lecteurs …) et au traitement des données qu'elles contiennent. On obtient alors un investissement que peu d'entreprises sont en mesure d'assurer actuellement comparé à l'utilisation du code à barre qui à l'unité ne coûte pratiquement rien et dont les outils d'utilisation et de gestion sont aux aussi relativement abordables.

Pourtant, on observe depuis quelques années, une baisse continue des prix des puces et des équipements. Au fur et à mesure que les entreprises investissent dans cette technologie, les solutions s'améliorent et l'utilisation de la RFID à grande échelle entraînera obligatoirement une fortebaisse des prix.

La RFID possède un avantage technologique décisif par rapport au code à barres. Nous verrons dans la prochaine partie que les applications pour la logistique amont sont nombreuses et que les entreprises utilisent déjà cette technologie. Pourtant, la RFID est encore une innovation naissante et l'ensemble du secteur ne la maîtrise pas parfaitement. Les opportunités sont tout de même très attrayantes. Le code à barres quant à lui est utilisé dans le monde entier, l'ensemble des entreprises de la planète connaissent cet outil et le maîtrise. Plus de **20** ans ont été nécessaires pour l'adapter au besoins des entreprises à grande échelle et il ne risque pas de disparaître de sitôt

Vers une utilisation des 2 technologies

Souvent présentée comme la remplaçante du code barre à court terme l'étiquette RFID possède effectivement des avantages qui offrent aux entreprises des alternatives en terme de gestion de la chaîne logistique amont. Pourtant, le code barre devrait survivre encore de nombreuses années.

Mais pendant ce temps, la solution d'une combinaison des **2** techniques dans les entreprises se profile de plus en plus. Ces entreprises souhaitent en effet conserver encore pour un temps leur système de code à barres très fiables même si moins performant. Beaucoup de professionnels conseillent de ne pas remplacer entièrement les codes à barres par de la RFID du jour au lendemain. Cette combinaison des **2** technologies s'avère tout à fait réalisable, compte tenu du fait qu'il existe désormais des installations matérielles permettant de lire les deux indifféremment.

Par exemple au Sernam, le déploiement de la RFID n'est pas complet. Les étiquettes sont jetables (car en circuit ouvert) et donc trop chères pour les implanter sur toute la chaîne. Quant une impossibilité technique avec la RFID se présente, l'usage du code- barres est alors entièrement possible et compatible. Les opérateurs de ces sociétés peuvent désormais avoir des équipements polyvalents et, suivant les postes de travail, lire une puce ou un code à barre. Ceci signifie qu'il est possible de combiner les deux technologies et donc de développer des solutions adaptées à chaque étape du déploiement de la RFID.

En plus d'être complémentaires, les technologies ne sont pas forcément utilisées pour les mêmes besoins. En effet « il ne faut pas systématiquement comparer RFID et Cette exigence de traçabilité ne concerne pas seulement le secteur alimentaire ou pharmaceutique. L'ensemble des entreprises est conscient maintenant de la nécessité de suivre les produits et de déterminer leurs parcours tout au long de la chaîne logistique. La RFID propose des solutions innovantes dans ce domaine, les possibilités des puces sont totalement compatibles avec cette exigence de traçabilité.

Conclusion

Nous avons introduit dans ce chapitre la technologie RFID en étant l'une des technologies d'identification automatique. Elle a la particularité de fonctionner à distance. Nous avons essayé de présenter les différents éléments de l'infrastructure RFID et principalement l'inter logiciel ou le middleware RFID qui joue un rôle important dans notre contribution puisque nous avons développé nos méthodes d'analyse de données au niveau de l'inter-logiciel et précisément dans le module de filtrage et de collection. Le chapitre suivant présente les principaux concepts de la sûreté de fonctionnement et de tolérance aux fautes dans les systèmes RFID.

Références bibliographiques

"Rfid So urcebook"

de Sandip Lahiri

Edition IBM Press (août 2005)

"RFID Ha ndbook : Fundamentals and Applications in Contactless Smart Cardsand Identification" ,

de Klaus Finkenzeller, (Mai 2003)Edition John Wiley & Sons

RFID Labeling: Smart Labeling Concepts and Applications for the Consumer Packaged Goods Supply Chain

de Robert A. Kleist, David A. Sakai, Theodore A. Chapman

Edition Banta Book Group (septembre 2005)

Livre blanc "Vers la tra nsparence de la chaîne logistique; une nouvelle ère detraçabilité grâce à la RFID",

de Clive Macmillan-Davies, Geoff Squires& Alison Greene (Juin 2004)

Chapitre II:

Etude théorique et simulation de la technologie RFID

II.1 INTRODUCTION

Dans ce chapitre, nous introduisons les concepts de base de la fiabilité. Nous introduisons d'abord le concept de fiabilité dans les systèmes informatiques. Elle peut être définie comme la caractéristique qui permet d'accorder une confiance justifiée aux services fournis par ces systèmes [4]. Ensuite, nous décrivons les différents concepts de base et les principales méthodes de fiabilité et de tolérance aux pannes. Enfin, nous montrons les différents niveaux auxquels la tolérance aux pannes peut être appliquée.

Nous consacrons une section à la définition des concepts statistiques utilisés dans notre approche proposée pour effectuer l'analyse des données du système RFID afin d'assurer la tolérance aux pannes. Ce chapitre est organisé comme suit : La première section présente les concepts de base de la fiabilité. La deuxième section traite de la tolérance aux pannes à deux niveaux d'abstraction (matériel et logiciel interne). La dernière section présente le travail de tolérance aux pannes des réseaux de capteurs dont nous nous sommes inspirés.

.En revanche Dans notre projet on peut illustrer les figures suivantes en possession le programme compilé sur matlab :

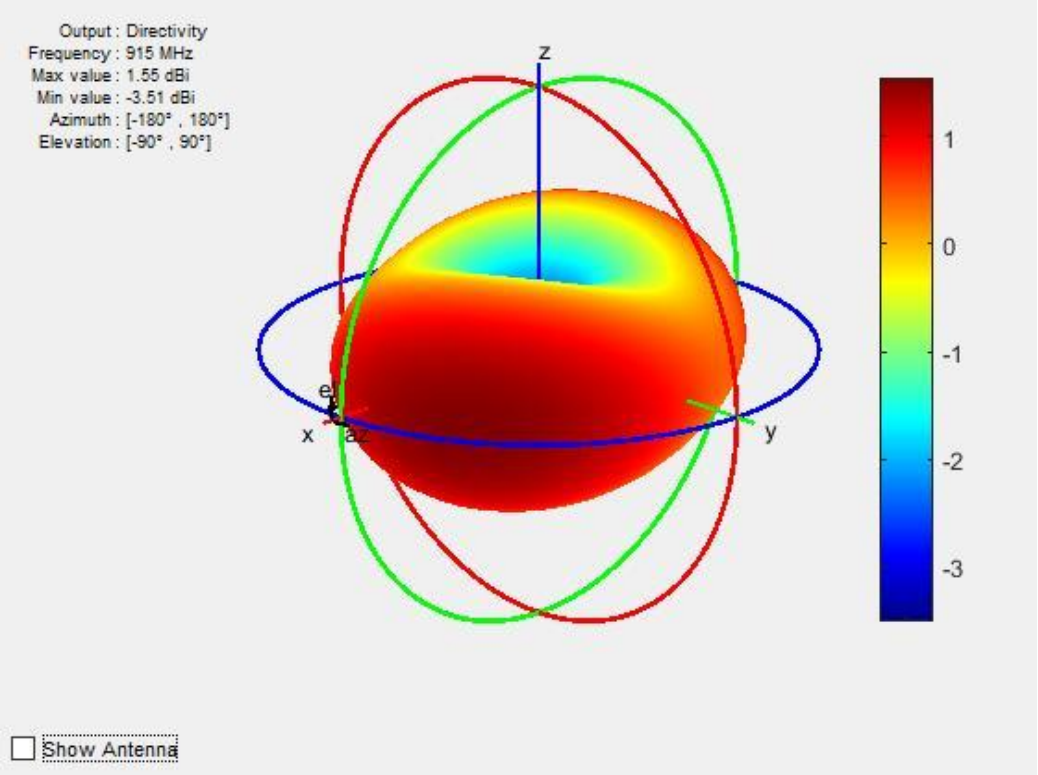
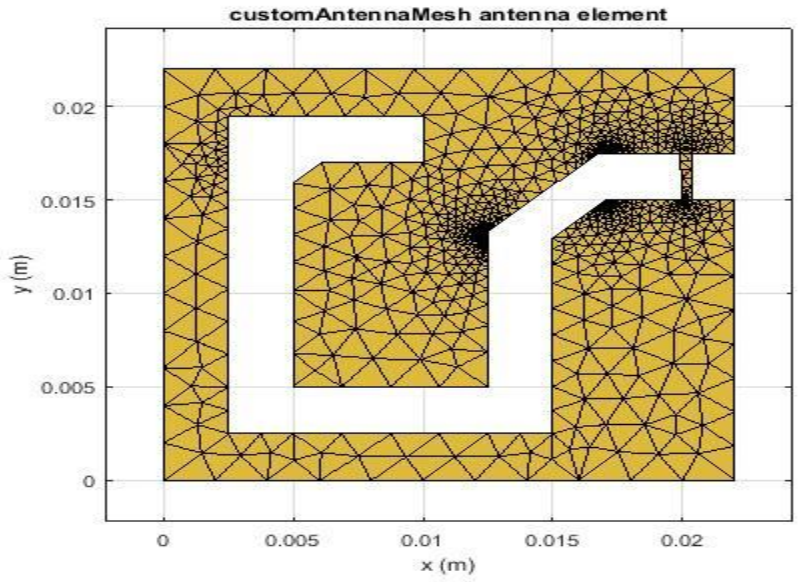


Figure II.6: Diagramme de rayonnement d'une antenne rfid




```
load RFIDtag
ant = customAntennaMesh(p, t);
createFeed(ant, [0.0201 0.0168], [0.0201, 0.0161]);
show(ant);
view(2);
z = impedance(ant, 915e6)
z =

   7.3653e-01 + 2.9269e+02i
   pattern(ant, 915e6);
```

Figure II.7: La geometrie physique d'une antenne rfid

Interprétation:

Les résultats expérimentaux obtenus sont presque les mêmes aux résultats de simulation.

II.2 CONCEPTS DE BASE DE LA SÛRETÉ DE FONCTIONNEMENT

II.2.1 La sûreté de fonctionnement des systèmes informatiques

C'est " la propriété qui permet de placer une confiance justifiée dans les services que délivrent ces systèmes." [4].

Les concepts de base de la sûreté de fonctionnement sont :

- Les entraves
- Les attributs
- Les moyens

La FIG.II.9 résume ces concepts et nous expliquons par la suite le sens de ces concepts.

A. Les entraves

Nous avons trois types d'entraves : les fautes, les erreurs et les défaillances.

1. Les fautes

Une faute peut être définie comme une cause pouvant provoquer une erreur.

Les fautes de programmation, la malveillance et les catastrophes naturelles sont des exemples de fautes. Quand une faute est activée, la partie du code affectée est exécutée. Une erreur est alors créée.

Les fautes peuvent être classées selon:

- La cause comme les fautes physiques et les fautes dues à l'homme.
- La nature comme les fautes accidentelles et les fautes intentionnelles.
- La phase de création ou d'occurrence par rapport à la vie du système comme les fautes de développement et les fautes opérationnelles.
- La situation des fautes par rapport aux frontières du système comme les fautes internes et les fautes externes.
- La persistance comme les fautes permanentes et les fautes temporaires.

2. Les erreurs

Une erreur est un état (ou partie de l'état) du système susceptible de provoquer une défaillance.

Un exemple d'erreur est lorsqu'une connexion est coupée entre deux points qui devraient être reliés entre eux.

3. Les défaillances

Une défaillance du système apparaît lorsque le service rendu par le système ne correspond pas à la réalisation de la fonction du système .C'est une transition d'un service correct vers un service incorrect.

Les défaillances sont classées selon le domaine de défaillance comme des défaillances en valeur et des défaillances temporelles.

Impact de la faute

On peut aller de la faute à la défaillance comme suit: quand une faute est activée ,elle provoque une erreur. En propageant ,l'erreur en gendre une défaillance(voir laFIG.II.2).

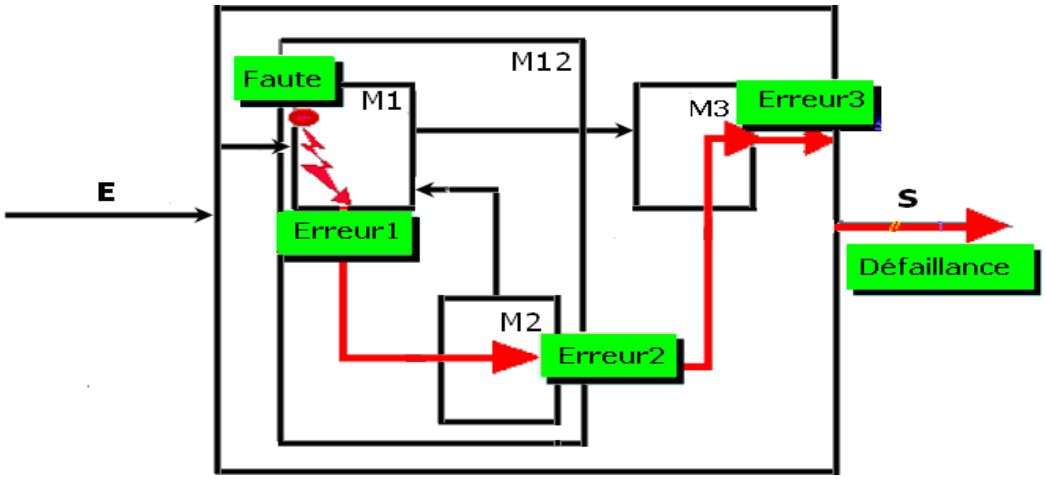


Figure II.8: De la faute à la défaillance

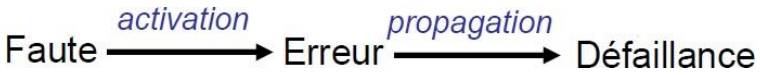


Figure II.9: le sens de ces concepts

La Fig .II.8 présente un système composé de trois modulesM_1,M_2etM_3.L'activation de la faute au niveau du module M_1 aprovoqué une erreur .En propageant ,l'erreur 1engendre une autre erreur au niveau du module M_2 puis une autre au niveau du modu le M_3 .Le service rendu par le système ne correspond pas à l'objectif attendu : nous avons une défaillance.

Nous avons montré les différents états des entraves .Nous expliquerons par la suite les différents attributsde la sûreté de fonctionnement.

B. Les attributs [4]

Les différents attributs de la sûreté de fonctionnement sont :

1. **Disponibilité :**La capacité du système à être prêt à fournir le service. C'est une fonction du temps définie comme la probabilité que le système fonctionne correctement et soit disponible à l'instant

2. **Fiabilité:** Elle est définie par rapport à la continuité du service. C'est une fonction du temps définie comme la probabilité conditionnelle que le système ait fonctionné correctement sur une période de temps [t0, t] étant donné qu'il a fonctionné correctement au temps t0.

3. **Sécurité-innocuité :** Elle est définie par rapport à la séparation des conséquences catastrophiques pour l'environnement du système. Il s'agit de la fonction temporelle définie comme la probabilité à l'instant t que le système fonctionne correctement ou s'arrête de fonctionner afin de ne pas nuire à la sécurité des personnes et des autres systèmes associés.

4. **Sécurité-confidentialité :** elle est définie par rapport à la préservation de la confidentialité et de l'intégrité des informations.

5. **Maintenabilité :** elle mesure la facilité de réparation d'un système défaillant. C'est la probabilité que le système défaillance etre vienne à un état de fonctionnement correct après un délai.

6. **Performabilité :** elle peut être définie comme étant la poursuite du fonctionnement correct d'un système en présence d'éléments défaillants avec des performances moindres. C'est une fonction du temps définie comme étant la probabilité que les performances du système soient supérieures ou égales au seuilL à l'instant.

7. **Testabilité:** mesure de la facilité d'exécution de certains test sur le système.

C. Les moyens de la Sûreté de Fonctionnement (SF)[27]

Les moyens de la sûreté de fonctionnement sont classés en quatre familles:

1. **Prévention des fautes**

C’est la méthode qui permet d’empêcher l'introduction de fautes de conception ou de fabrication et d’éviter l'apparition des fautes dans la phase opérationnelle(phase de programmation structurée ,phase de modularisation,...).

2. **Tolérance aux fautes**

C’est l’ensemble des moyens permettant au système de fonctionner en dépit des :

- Fautes physiques,

- fautes de conception,
- erreurs de l'utilisateur,
- fautes intentionnelles.
- **Élimination des fautes**

Elle peut être réalisée en réduisant le nombre ou la sévérité des :

- Fautes fonctionnelles,
- fautes matérielles.

En utilisant des méthodes de test et de vérification.

- **Prévision des fautes**

C'est la méthode qui permet d'estimer la présence, la création et les conséquences des fautes.

La figure II.10 résume tous les concepts de la sureté de fonctionnement.

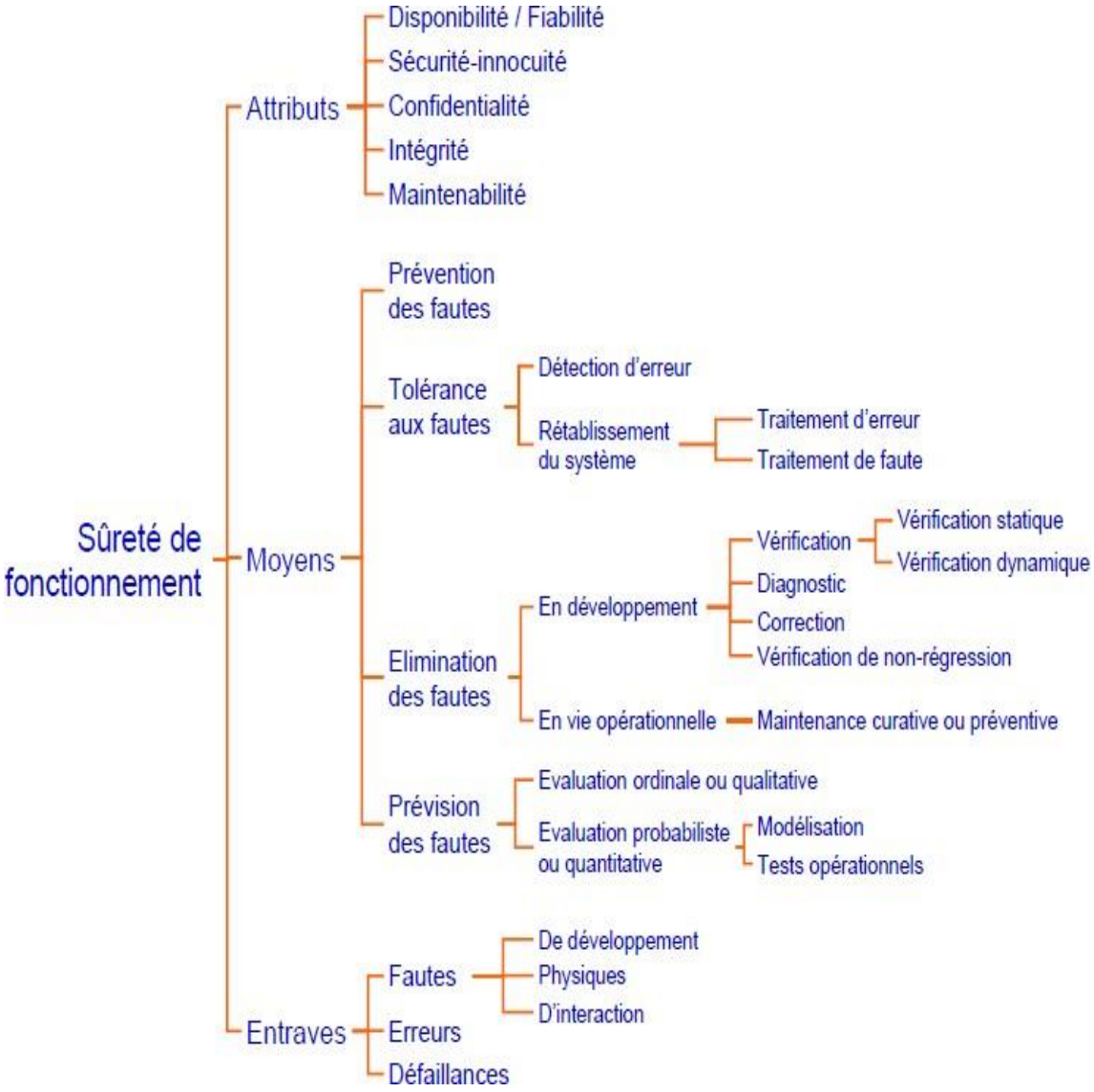


Figure II.10: Concepts de base de la sûreté de fonctionnement des systèmes informatiques [28]

4. Tolérance aux fautes

La tolérance aux pannes peut être définie comme « la méthode qui permet à un système d'exécuter ses fonctions malgré des défauts pouvant affecter ses composants, sa conception ou son interaction avec l'homme ou d'autres systèmes » [5].

Quelles que soient les précautions prises, la survenance de défauts est inévitable (erreur humaine, intention malveillante, obsolescence des équipements, catastrophe naturelle, etc.). Les mesures prises ne peuvent que réduire la probabilité de sa survenue [26].

L'approche la plus courante pour traiter les erreurs consiste à détecter la présence d'un état incorrect (erreur), puis à remplacer l'état incorrect par l'état correct (dans la spécification).

La sous-section suivante présente les différents types de méthodes de détection d'erreurs.

5. La détection des erreurs[5]

Il y a différents types de moyens de contrôle utilisés pour détecter l'erreur. Parmi ces types, nous citons :

1. Codes détecteurs d'erreurs.
2. Redondance.
3. Contrôle devrai semblance.
4. Contrôle de données structurées.
5. Le diagnostic enligne:

La sous-section suivante présente l'une des techniques de contrôle utilisées pour détecter l'erreur :la redondance.

6. Redondance: [29]

Dans cette section, nous nous concentrerons sur une technique galvaudée qui assure la fiabilité opérationnelle : la redondance. Son principe est d'ajouter des ressources, des informations ou du temps au-delà de ce qui est nécessaire au fonctionnement du système. Le but ici est de permettre la détection et la tolérance d'erreur. Il existe quatre formes de répétition:

- matérielle
- logicielle
- temporelle
- d'information

Dans notre approche (dans le chapitre suivant), nous avons utilisé la redondance matérielle et dans nos futurs travaux, nous avons l'intention d'utiliser l'itération logicielle. Ensuite, nous introduisons ces deux formes de répétition.

a. Redondance Matérielle

C'est la forme la plus répandue de redondance raison de la diminution de coût du matériel et de la minimisation de la taille des composants. Il existe trois types de techniques:

- Les techniques passives
- Les techniques actives ou dynamiques
- Les techniques hybrides.

1. Redondance matérielle passive

L'objectif de la redondance matérielle passive est de masquer les fautes et éviter leur propagation en erreurs .Son mécanisme de basee le vote majoritaire .Un exemple est la redondance modulaire triple (Triple ModularRedundancyou TMR)[30](voirlaFig.II.11).

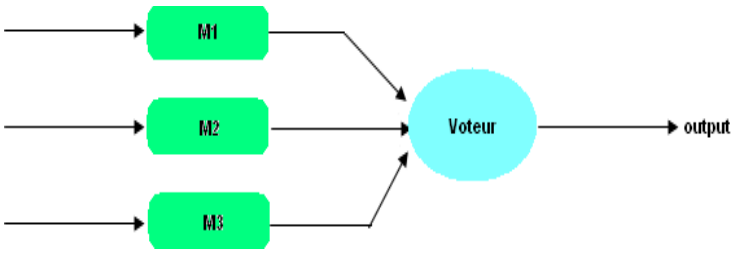


Figure II.11: TMR (triple modular redundancy).

La Fig .II.11présente leTMR.M_1,M_2etM_3sont trois modules qui génèrent des données homogènes .Le voteur permet de produire la donnée finale.

II.2.2 Généralisation de TMR

On généralise le cas de la FIG.II.4àNmodaires:RedondanceN-modulaire(N-modularredundancyou NMR). N modules identiques sont utilisés avec Nimpair.

Les systèmes utilisant la redondance matérielle passive se caractérisent par les points suivants:

a. Niveau d'insertion du vote

On donne dans la Fig.II.5un exemple où Le vote peut être inséré à différents niveaux: Système de controle industriel.

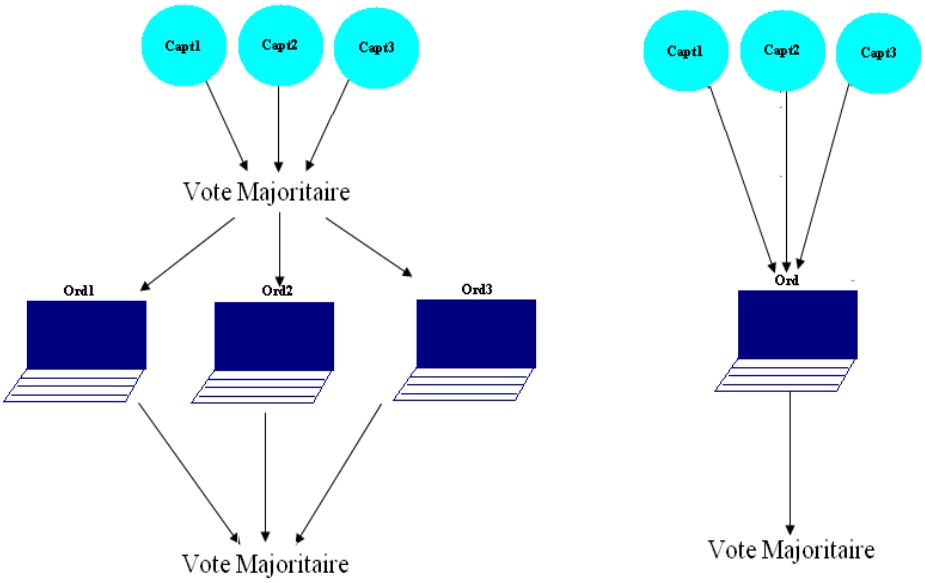


Figure II.12: Système de contrôle industriel

b. Choix de conception

Le voteur peut être un voteur matériel ou un voteur logiciel. Les critères pour choisir le type du voteur sont:

- la disponibilité d'un processus,
- la vitesse d'exécution du vote,
- la limitation de puissance, de poids,
- le nombre de voteurs à réaliser.

c. Discordance des valeurs obtenues

C'est quand les valeurs fournies par les différents modules sont différentes alors quel 'environnement est correct .Dans ce cas, on considère souvent la valeur médiane.

Nous avons présenté l'une des formes de la redondance matérielle : la redondance matérielle passive .La sous-section suivante présente une autre forme: la redondance matérielle active.

2. Redondance matérielle active[29]

Il existe plusieurs types de redondance matérielle active :la duplication et la comparaison ,l'utilisation des modules «spares» et l'approche «pair-and-a-spare».

- Duplication et comparaison

Elle consiste à :

1. Dupliquer le même matériel
2. Exécuter la même application sur chaque instance du matériel
3. Comparer les résultats obtenus

Les limitations de ce type de redondance sont :

- Le cas d'entrées fausses.
- L'inexactitude de la comparaison.
- La défaillance du comparateur.

- Utilisation des modules «spares»

On parle dans cette technique du remplacements tandbyou de la disponibilités tandby.Le principe est qu'un seul module est opérationnel ,les autres sont des spares (modules disponibles);si on détecte des fautes dans le module principal ,on procède à son remplacement.

On peut avoir :

- Un remplacement à chaud(modules de remplacement sont opérationnels).
- Un remplacement à froid(modules de remplacement non opérationnels).

- L'approche « pair-and-a-spare »

Dans cette approche deux modules fonctionnent en parallèle et leurs résultats sont comparés .Si un module est défaillant, on le remplace par un spare. On peut remplacer la paire entièreen cas de défaillance.

3. Redondance matérielle hybride [29]

Dans cette technique, on combine la redondance active et la redondance passive .La faute est masquée pour éviter la propagation en erreur. Si une erreur a lieu, elle est détectée et localisée pour permettre une reconfiguration du système.

Nous avons présenté dans la sous-section a le premier type de redondance :la redondance matérielle .Nous présentonsdanslasous-sectionbuneautreforme:laredondancelogicielle.

b. La redondance logicielle

La redondance logicielle consiste à écrire plusieurs versions du programme.Elle est réalisée parles techniques suivantes:

1. N-self-checkingprogramming

Elle consiste à écrire Nversions d'un même programme (voir la FIGII.6)..Chaque version possède son propre jeu de test .Une logique des élection choisit les résultats d'une version ayant passé avec succès l'ensemble de ses tests.

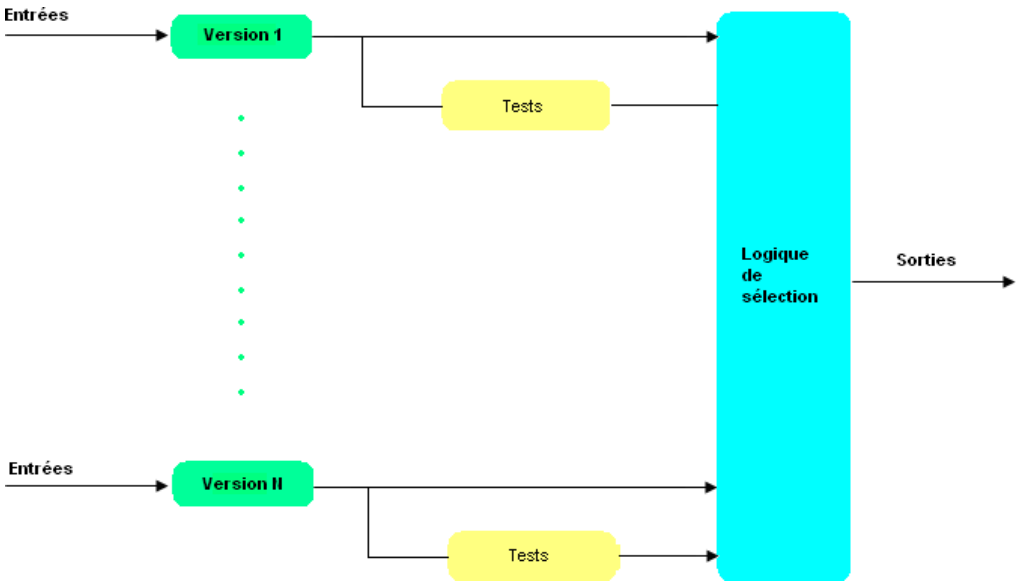


Figure 13: N-self-checking programming

2. N-Version programming

Elle consiste à concevoir et coder le logiciel Nfois e

t puis effectuer un vote majoritair e sur les N résultats obtenus.

Néanmoins, cette approche présente des inconvénients :

- Les concepteurs et programmeurs peuvent faire les mêmes erreurs.

- S'il y a des erreurs dans les spécifications, elles se propagent sur toutes les versions.

3. Blocs de recouvrement

4. Ce type est caractérisé par:

- N versions du programme

- Même ensemble de tests

- Une version est primaire, les autres sont secondaires.

Le principe est que si les tests indiquent une erreur dans la version primaire, nous prenons une version secondaire, …etc.

Nous avons tenter de présenter les principaux concepts de la sûreté de fonctionnement:la tolérance aux fautes et la redondance .La section suivante discute la tolérance aux fautes dans les systèmes RFID.

II.2.3 TOLÉRANCE AUX FAUTESDESSYSTÈMESRFID

La tolérance aux pannes est l'un des problèmes critiques dans le monde RFID, en raison de la nature incertaine des communications par radiofréquence (RF).

Les étiquettes RFID sont attachées aux articles, peuvent être trouvées à tout moment via des lecteurs RFID et un système de base de données en réseau, et peuvent être surveillées tout au long de leur cycle de vie. Les étiquettes RFID sont des puces en silicium avec leurs identifiants, des fonctions de radiofréquence, ainsi qu'une logique et une mémoire supplémentaires. La plupart des étiquettes RFID sont dotées de la capacité de communiquer par radiofréquence avec des lecteurs externes. L'infrastructure RFID peut s'étendre sur plusieurs sites, ce qui nécessite des outils de configuration et de surveillance à distance. De plus, pour avoir une infrastructure robuste, une redondance doit être établie à chaque couche, avec des capacités de sauvegarde..

Tolérance aux fautes aux différents niveaux

La tolérance aux fautes peut être **i**ntégrée à différents niveaux de l’infrastructure :le matériel ,l’inter logiciel et l’application*5](voirlaFIG.II.14).

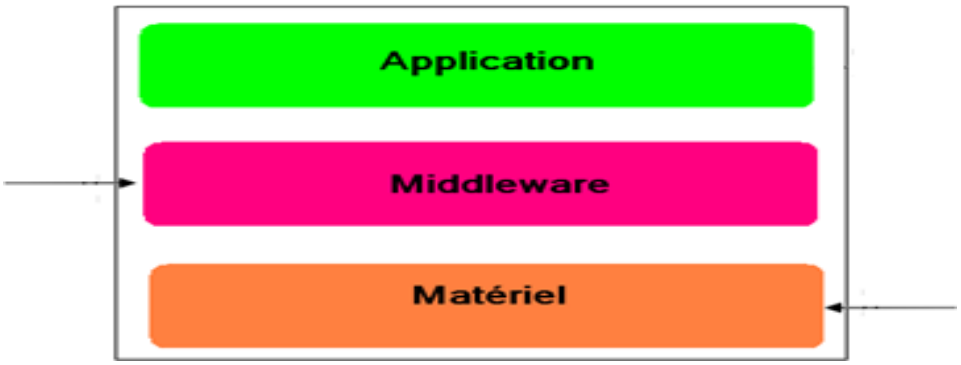


Figure II.14: Les couches d'intégration de la tolérance aux fautes dans un système RFID

Nous allons discuter la tolérance aux fautes à deux niveaux d'abstraction (le matériel et l'inter logiciel)

a. Matériel

Au niveau du matériel, se trouvent les puces et les lecteurs RFID.

Les lecteurs RFID ont une vitesse de traitement décente et une grande mémoire. Grâce à la puissante combinaison d'un processeur puissant et d'une mémoire de 1 Go en option, le lecteur RFID est capable de fournir un traitement plus rapide.

Lorsque le système hôte ou l'alimentation tombe en panne, une grande capacité de mémoire et des capacités de communication hors ligne garantissent la conservation des données, même dans les environnements avec une plus grande taille d'étiquette. En fait, lorsque le disque dur en option est installé, les lecteurs RFID peuvent stocker des milliards d'étiquettes EPC.

En raison de la diversité de l'environnement d'application, les lecteurs RFID sont multi protocoles et prennent en charge une large gamme de protocoles RFID, intègrent des modules de communication sans fil et utilisent un traitement tolérant aux pannes pour améliorer la fiabilité de la détection.

Les deux types d'étiquettes (étiquettes passives et étiquettes actives) sont très fiables du fait de leur structure relativement simple et régulière.

La capacité mémoire varie de 32 à 128 bits (non réglable) pour les étiquettes passives et peut aller jusqu'à 10 kilobits pour les étiquettes actives (elle peut être écrite plusieurs fois, effacée, modifiée et lue, le nombre d'itérations pour ces opérations peut dépasser 500 000 ou 1 million pour ce type de label) [12].

Bien que la principale préoccupation des utilisateurs RFID soit la performance opérationnelle du matériel et des logiciels, les batteries jouent un rôle très important dans le système. Sans alimentation par batterie, l'étiquette ne peut pas envoyer les informations nécessaires au lecteur du système. Le choix de la technologie de batterie a certainement un impact sur les performances globales du système à long terme. Cet effet est lié à des facteurs tels que la durée et la fiabilité des performances de la marque dans toutes les conditions.

b. Niveau intermédiaire

Le principe de la tolérance aux pannes à ce niveau est d'intégrer les mécanismes de tolérance aux pannes dans les programmes internes [5]. Puisqu'il est difficile de fournir de manière rentable une tolérance aux pannes au niveau du lecteur de nommage, nous nous attendons à ce que de nombreuses approches tolérantes aux pannes pour cette tâche au niveau logiciel émergent. Alors que la plupart des applications sont actuellement très simples, afin de gérer des applications plus complexes, il existe un besoin de développer des logiciels internes plus complexes [6].

Nous présentons ici quelques travaux qui abordent la tolérance aux pannes dans les systèmes RFID.

Travaux sur la tolérance aux fautes dans les systèmes RFID

La plupart des travaux sur la tolérance aux fautes ont été faits et évalués dans les réseaux des capteurs .Peu de travaux ont étudié la tolérance aux fautes dans les systèmes RFID ,la grande partie des solutions dans ces systèmes traitent le manque de fiabilité inhérent dans les technologies de RFID.

a. RFID: Une infrastructure d'inter logiciel fiable pour le déploiement de la RFID[8]

Les auteurs dans[8]ont étudié des solutions de logiciel système pour réaliser un déploiement fortement fiable qui atténue le manque de fiabilité inhérent dans les technologies RFID.

Ils ont développé:

1. Une abstraction virtuelle de lecteur pour améliorer la nature potentiellement sujet aux erreurs des données produites par les lecteurs.
2. Une abstraction originale de chemin pour capturer le flux d'information logique parmi les lecteurs virtuels.

Ils ont conçue tontmise n application un inter logiciel RFID :RFID (infrastructure fiable pour l'identification par radio fréquence)pour organiser et soutenir des requêtes sur des flux de données d'une façon efficace.

L'implémentation du prototype utilisant les lecteurs RFID et lecteurs simulés employant un modèle empirique de lecteurs RFID montre que RF^2ID peut fournir une fiabilité élevée et soutenir la détection basée sur le chemin d'objet.Le sauteur semploient la nature du flux de données pour améliorer la fiabilité .De plus, le flux de données peut aider dans l'organisation de données.

Les contributions principales de leur travail sont:

- Étude du comportement incertain des dispositifs RFID : Ils ont fait une étude étendue de ces dispositifs pour identifier la variété de paramètres qui affectent le fonctionnement du lecteur RFID.

- La conception d'un système qui a une architecture basée sur le chemin :RF^2ID utilise un chemin virtuel(V path)pour distinguer logiquement l'écoulement des flux de données .Utilisant V path,le système peut fournir une fiabilité plus élevée ,fournir des possibilités pour organiser les flux de données pour la gestion efficace des requêtes, et offrir un véhicule pour l'équilibrage de la charge parmi les lecteurs.

- Implémentation du système RF^2ID et son évaluation : Ils ont développé un prototype de l'architecture RF^2ID. L'implémentation incorpore les lecteurs physiques aussi bien que les lecteurs physiques simulés pour permettre des expériences commandées d'évolutivité .Les évaluations démontrent la fiabilité du système et les possibilités améliorées de détection d'articles d'une architecture basée sur la notion de chemin.

b. Travail de **AgustiSolanasetal.**[31]

Les auteurs dans [31]ont montré que les lecteurs peuvent localiser une étiquette en collaborant. Afin d'exécuter correctement ,les lecteurs doivent pouvoir communiquer entre eux .À cet effet ,ils proposent l'utilisation d'une topologie de réseau qui peut être représentée comme un graphe où les nœuds sont des lecteurs et les arcs sont des connexions entre les lecteurs.

c. Le travail de JulienDavid

Les contributions dans [32] étaient le développement d'un contrôleur de lecteurs RFID qui contrôle une centaine de lecteurs et en réalisant la coordination entre eux .L'auteur a étudié l'émulateur du middleware RIFIDI (nous l'utiliserons dans notre implémentation ,voir la section 3.4 du Chapitre IV) .Il a constaté que cet émulateur ne peut simuler plus que 6 lecteurs.

Nous avons présenté quelques travaux qui rapprochent de la tolérance aux fautes dans les systèmes RFID .La section suivante par le de la tolérance aux fautes dans les réseaux de capteurs et des travaux dont nous nous sommes inspirés.

II.3 LATOLÉRANCEAUXFAUTESDANSLESRÉSEAUXDECAPTEURS

II.3.1 définition:

Un réseau de capteurs sans fil est un réseau adhoc avec des petits nœuds sans fil communicants où chaque nœud est équipé de composants multiples .En particulier ,chaque nœud a un moteur de calcul ,dessous- systèmes de communication et de stockage ,une batterie en réserve ,des capteurs et dans certains cas des composants en actions[6].

Les micro-capteurs sont capables de récolter et de transmettre des données environnementales d'une manière autonome .La position de ces nœuds n'est pas obligatoirement prédéterminée .Ils peuvent être aléatoirement dispersés dans une zone géographique ,appelée «champ de captage» correspondant au terrain d'intérêt pour le phénomène capté .Les données captées par les nœuds sont acheminées grâce à un routage multi-saut à un nœud considéré comme un" point de collecte", appelé nœud-puits(ou sink).Ce dernier peut être connecté à l'utilisateur du réseau(via Internet ,un satellite ou un autre système).L'usager peut adresser des requêtes aux autres nœuds du réseau ,précisant le type de données requises et récolter les données environnementales captées par le biaisd un œud puits.

Le schéma de la figure II.8montre la grande ressemblance au niveau de l'infrastructure entre un système RFID complexe et un réseau de capteurs qui sont tous deux des systèmes embarqués.

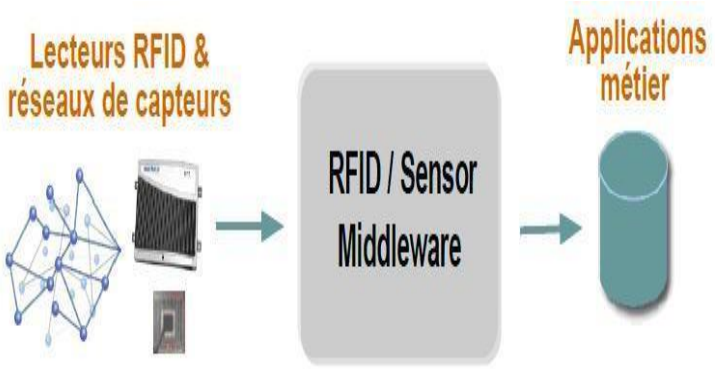


Figure II.15: Infrastructure RFID/Réseau de capteurs

Un système embarqué peut être défini comme un système électronique et informatique autonome, qui est dédié à une tâche bien précise.

Un système embarqué intègre des logiciels et des matériels conjointement et spécifiquement conçus pour assurer des fonctionnalités souvent critiques [33]. Ses ressources disponibles sont généralement limitées. Cette limitation est généralement d'ordre spatial (taille limitée)et énergétique(consommation restreinte). Le terme de système embarqué désigne aussi bien le matériel que le logiciel utilisé .Les systèmes embarqués exécutent des tâches prédéfinies et ont un cahier des charges contraignant à remplir ,qui peut aborder les aspects:

- **Coût :** le prix de revient doit être le plus faible possible surtout si le système est produit en grande série.
- **Espace compté**: ayant un espace mémoire limité de l'ordre de quelques maximum.
- Il convient de concevoir des systèmes embarqués qui répondent au besoin au plus juste pour éviter un sur coût.
- **Puissance de calcul .**Il convient d'avoir la puissance de calcul juste nécessaire pour répondre aux besoins et aux contraintes temporelles de la tâche prédéfinie .Ceci en vue d'éviter un sur coût de l'appareil et une consommation excédentaire d'énergie (courant électrique).
- **Consommation énergétique la plus faible possible:** due à l'utilisation de batterieset/ou ,de panneaux solaires voire de pile à combustible pour certains proto types.
- **Temporel ,**dont les temps d'exécution et l'échéance temporelle d'une tâche sont déterminés(les délais sont connus ou borné sa priori). Cette dernière contrainte fait que généralement de tels système sont des propriétés temps réel.

- **Sûreté de fonctionnement:** s'il arrive que certains de ces systèmes embarqués subissent une défaillance, ils mettent des vies humaines en danger ou mettent en péril des investissements importants. Ils sont alors dits «critiques» et ne doivent jamais faillir.

- **Sécurité:** ces systèmes peuvent se révéler être porteurs d'informations confidentielles pour leur (s) utilisateur(s), qu'il convient de conserver et de protéger. Notamment, en ce qui concerne l'acquisition et la transmission d'informations médicales. Par exemple, des systèmes personnels permettant l'acquisition ,par le patient lui –même ,et la transmission à distance d'information sa caractère confidentiel, comme des données médicales, ou relatives à la vie privée du ou des utilisateurs en général.

Vu la quasi absence des travaux de tolérance aux fautes au niveau des systèmes RFID et vu la grande ressemblance au niveau de l'infrastructure d'un réseau de capteur et un système RFID complexe, nous pouvons nous inspirer des travaux faits pour la tolérance aux fautes dans les réseaux de capteurs.

Nous présentons par la suite les deux travaux sur la tolérance aux fautes dans les réseaux de capteurs dont nous nous sommes principalement inspirés.

II.3.2 Travaux sur la tolérance aux fautes dans les réseaux de capteurs

A. Travail de Koushanfar : Tolérance aux fautes dans les réseaux de capteurs

LetravaildeFarinazKoushanfaretal.[6]présenteunetechniquebaséesurlavalidationpourladétectionen ligne des fautes de capteurs.

Les auteurs réalisent l'analyse statistique sur les données pour chaque capteur . Si les valeurs obtenues pour un capteur ne sont pas conformes dans un intervalle de confiance calculé par la méthode percentile, ce capteur est considéré défectueux.

La sous-section suivante présente les notions statistiques : percentile et intervalle de confiance.

B. Percentile et intervalle de confiance

Cette section présente les notions statistiques mentionnées dans [6]et que nous allons utilisé dans notre approche pour l'étude du comportement des lecteurs et des capteurs : le percentile et l'intervalle de confiance.

- Percentiles [34]

Les statistiques d'ordre fournissent une manière d'estimer des proportions de données qui devraient être en haute tau des sous d'une valeur donnée, appelées un percentile .Le p^{ième} percentile est une valeur ,Y(p), telle qu'au plus (100p)% des mesures sont inférieures à cette valeur et au plus 100 (1-p)% sont plus grandes. Le cinquantième percentiles' appelle la médiane.

Les percentiles coupent un ensemble de données ordonnées en centièmes. Par exemple, 70% des données devraient être au-dessous du soixante- dixième percentile.

C. Évaluation des percentiles

Les percentiles peuvent être estimés à partir des N mesures comme suit: pour le p ^{ième} percentile, mettons p(N+1)égale à k+d pour k un nombre entier, et d ,une fraction supérieure ou égale à 0 et inférieure à1.

$$Y(p)=Y_{[k]} + d\left(Y_{[k+1]}-Y_{[k]}\right)$$

1. Pour0<k<N,

2. Pour k = 0, Y (p) = Y $_{[1]}$

3. Pour k = N, Y (p) = Y $_{[N]}$

Un exemple

Nous donnons ici un exemple pour bien comprendre la méthode de calcul des percentiles.

Douze mesures d'une étude de mesures sont montrées ci-dessous .Les mesures sont en cm (voir Tableau II.1).

Tableau 1: Résultats de mesure

I	Mesures	Statistiques d'ordre	Rang
1	95.1772	95.0610	**9**
2	95.1567	95.0925	**6**
3	95.1937	95.1065	**10**
4	95.1959	95.1195	**11**
5	95.1442	95.1442	**5**
6	95.0610	95.1567	**1**
7	95.1591	95.1591	**7**
8	95.1195	95.1682	**4**
9	95.1065	95.1772	**3**
10	95.0925	95.1937	**2**
11	95.1990	95.1959	**12**
12	**95.1682**	**95.1990**	**8**

Pour trouver le 90% percentile, nous remplaçons dans la formule de la condition (1)(voir: Évaluation des percentiles).

p (N+1) = 0,9 (13) =11.7 ; k = 11, et d = 0,7 (avec N=12 et p=0,9).

De la condition (1),on estime que Y(0,90)=95,1981cm .Ce percentile ,bien que ce soit une évaluation d'un petit échantillon de mesures ,il donne une indication sur la population des mesures.

- **Intervalle de confiance** [35]

En statistique, et surtout en théorie des enquêtes, lorsqu'on cherche à estimer la valeur d'un paramètre, on parle d'intervalle de confiance lorsqu'on donne une période contenant, avec un certain degré de confiance, la valeur à estimer. Le degré de confiance de principe est exprimé sous forme de probabilité. Par exemple, un intervalle de confiance à 95 % (ou à un

seuil de risque de 5 % et un score de confiance à 95 %) a une probabilité de 0,95 de contenir la valeur du paramètre que l'on cherche à estimer. Ainsi, lors de la conduite d'une enquête (sélection aléatoire d'un sous-ensemble de la population), l'estimation d'un montant d'intérêt donné est aléatoire et correspond rarement exactement à la valeur de la quantité que l'on cherche à estimer. En introduisant l'estimation non pas comme une valeur mais comme un cadre, on détermine d'une certaine manière l'incertitude de la valeur estimée.

Plus l'intervalle de confiance est petit, plus l'incertitude de la valeur estimée est faible.

Les limites de l'intervalle de confiance sont les pourcentages qui croisent l'ensemble de données. Par exemple, pour un IC à 95 %, 95 % des données doivent être au-dessus de la limite inférieure et en dessous de la limite supérieure.

Pour interpréter correctement l'intervalle de confiance et la plage, nous sommes allés à la référence [36]

A. Etendue de l'intervalle de confiance (IC) [36]

L'étendue de l'intervalle de confiance est égale à la borne supérieure moins la borne inférieure. Il détermine la précision de l'estimation : plus la plage est petite, plus l'estimation est précise.

Plus la taille de l'échantillon est grande, plus la plage d'IC à 95 % est petite. Pour diviser par deux la gamme, vous devez inclure 4 fois plus de sujets. Pour diviser la plage par k, incluez k^2 fois plus de cibles.

Plus l'échantillon est hétérogène (c'est-à-dire plus la variance ou l'écart type est élevé), plus la plage est élevée. L'étendue du %CI est directement proportionnelle à l'écart type de la variable mesurée.

L'utilisation la plus simple des intervalles de confiance concerne la population à distribution normale (en cloche) pour laquelle on cherche à moyenner [37]. Si l'on connaît l'écart type $\sigma(X)$ (ou si l'on connaît une estimation assez fiable) de cette distribution, et si l'on mesure la moyenne sur un échantillon de taille n pris au hasard, alors:

- l'intervalle:

$$\left[\overline{x} - \frac{\sigma(X)}{\sqrt{n}}; \overline{x} + \frac{\sigma(X)}{\sqrt{n}}\right]$$

Est un intervalle de confiance de à environ 68%

$\overline{X}$

- l'intervalle:

$$\left[\overline{x} - 2\frac{\sigma(X)}{\sqrt{n}}; \overline{x} + 2\frac{\sigma(X)}{\sqrt{n}}\right]$$

Est un intervalle de confiance de à environ 95%.

$\overline{X}$

- l'intervalle:

$$\left[\overline{x} - 3\frac{\sigma(X)}{\sqrt{n}}; \overline{x} + 3\frac{\sigma(X)}{\sqrt{n}}\right]$$

Est un intervalle de confiance de à environ99,7%.

$\overline{X}$

Ces formules sont valables pour des échantillons supposés grands(n>100).Dans le cas d'échantillon plus petit,la consultation d'une table de distribution de la loi de Student est nécessaire.

Pour augmenter la confiance ,il faut élargir l'intervalle et pour obtenir un intervalle plus fin avec le même degré de confiance ,il faut augmenter la taille de l'échantillon[36].

B. La détection et la tolérance aux fautes distribuée dans les réseaux de capteurs

XuanwenLuo Ming Dong et Yinlun Huang [7], proposent la tolérance aux fautes distribuée.

L'idée de base de la détection distribuée est que chaque capteur indépendant prend une décision locale (généralement binaire) et ces décisions sont ensuite combinées dans le capteur de fusion pour produire la décision globale.

Les n capteurs (S1, S2, ..., Sn) observent une hypothèse inconnue (voir Fig. II.9).

Les observations des capteurs sont indépendantes et distribuées, donnant l'hypothèse inconnue.

Chaque capteur transmet sa décision via un canal d'accès multiple au capteur de fusion. Sur la base de la décision reçue du capteur, le capteur de fusion produit la conclusion finale concernant l'hypothèse inconnue.

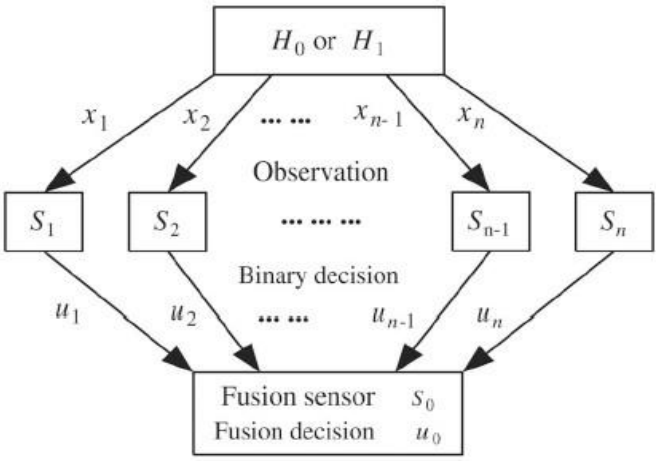


Figure II.16: detection distribué de l'evenement

Il est également possible que le réseau considéré contienne des nœuds de capteurs défectueux pour des raisons d'environnement et de fabrication. Normalement, l'événement, s'il se produit, doit être détecté comme « se produisant » par les capteurs de localisation. Le comportement erroné qu'ils considèrent se produit lorsque la décision de détection est décalée sur « non survenue » en raison d'une erreur de capteur, ou vice versa. La tolérance aux pannes est obtenue grâce à la redondance (nombre de capteurs homogènes) : Le capteur de fusion dépend de L'idée de base de la détection distribuée est que chaque capteur indépendant prend une décision locale (généralement binaire) et ces décisions sont ensuite combinées dans le capteur de fusion pour produire la décision globale.

Les n capteurs (S1, S2, ..., Sn) observent une hypothèse inconnue (voir Fig. II.16).

Les observations des capteurs sont indépendantes et distribuées, donnant l'hypothèse inconnue.

Chaque capteur transmet sa décision via un canal d'accès multiple au capteur de fusion. Sur la base de la résolution reçue du capteur, le capteur de fusion produit le résultat final par rapport à l'hypothèse inconnue.

Il est également possible que le réseau étudié contienne des nœuds capteurs défectueux pour des raisons environnementales et de fabrication. Habituellement, si cela se produit, l'événement doit être détecté comme « s'étant produit » par les capteurs de localisation. Le comportement défectueux qu'ils considèrent se produit lorsque la décision de détection est déplacée vers « ne s'est pas produit » en raison d'un défaut du capteur, ou vice versa. La tolérance aux erreurs est obtenue grâce à la redondance (nombre de capteurs homogènes) : le capteur de fusion dépend du résultat de plusieurs capteurs pour donner sa décision finale sur l'événement.FIG II.16. Détection distribuée de l'événement

II.3.3 Synthèse sur les deux travaux

Le travail présenté dans [6] donne une technique basée sur la validation pour la détection en ligne des défauts des capteurs. Une analyse statistique est effectuée sur les données de chaque capteur pour détecter les capteurs défectueux. L'intervalle de confiance utilisé dans ce travail (dans notre approche) nous permet de détecter les lecteurs et capteurs défaillants après analyse et saisie des résultats des inventaires.

Les travaux présentés dans [7] suggèrent une tolérance aux pannes distribuée. L'idée de base de la détection distribuée est que chaque capteur indépendant prend une décision locale (généralement binaire) et ces décisions sont ensuite combinées dans le capteur de fusion pour produire la décision globale. Les observations des capteurs sont indépendantes et distribuées symétriquement, donnant l'hypothèse inconnue. Dans notre approche que nous décrivons au chapitre trois, chaque lecteur attribue un score d'inventaire indépendamment des autres lecteurs. Ainsi, chaque capteur donne son observation indépendamment des autres capteurs. Tous ces résultats sont combinés avec le middleware qui les analyse et donne une note finale pour chaque type de capteur, un résultat final d'inventaire et une décision finale sur l'événement..

CONCLUSION

Ce chapitre présente les principaux concepts de fiabilité.

Les sections 1 et 2 présentent les concepts de base de la fiabilité et présentent quelques techniques de fiabilité et de tolérance aux pannes.

La troisième section traite de la tolérance aux pannes dans les systèmes RFID à deux niveaux d'abstraction (interfaces matérielles et logicielles). Les travaux sur la tolérance aux pannes au niveau des systèmes RFID étant quasi inexistants et la similitude d'infrastructure entre un système RFID complexe et un réseau de capteurs étant évidente, nous nous sommes inspirés et avons évalué les travaux qui ont été réalisés pour eux. Réseaux de capteurs, la quatrième section présente ce travail.

Le chapitre suivant donne notre contribution.

Références bibliographiques

[1] Klaus Finkenzeller. *RFID Handbook : Fundamentals and Applications in Contactless Smart Cards and Identification*. Deuxième Édition, John Wiley & Sons, Ltd., England. ISBN 0-470-84402-7.2003.

[2] Pattabhiraman Krishna et David Husak. *RFID INFRASTRUCTURE*. IEEE Communications Magazine.Volume: 45, Issue: 9, Pages: 4-10. Septembre 2007.

[3] Yves Saint-Oyant et Jonathan Brisart. *La norme RFID*. Thèse de Master IAGL. Université desciences et technologies. Lille1. 2010.

[4] Laprie, J. C, et al. *Guide de la sûreté de fonctionnement.* 2ème édition, Cépaduès Éditions. ISBN2-85428-382-1. 1996.

[5]

a. Thi-Quynh Bui, Oum-El-Kheir Aktouf, Michel Dang, Levent Gürgen et Claudia Roncancio. *Diagnosis Service for Software Component and Its Application to a Heterogeneous Sensor Data Management System.* depend, pp.143-149. Second International Conference on Dependability. 2009.

b. Thi Quynh BUI. *SERVICE DE DIAGNOSTIC EN LIGNE POUR LES APPLICATIONS A BASE DE COMPOSANTS LOGICIELS*. THESE pour obtenir le grade de DOCTEUR DE GRENOBLE INP - Préparée au Laboratoire de Conception et d'Intégration des Systèmes (LCIS) dans le cadre de l'Ecole Doctorale "Mathématiques, Sciences et Technologies de l'Information, Informatiques (MSTII)" . 14 Octobre 2009.

[6] F. Koushanfar , M. Potkonjak et A. Sangiovanni-Vincentelli. *Fault-Tolerance in Sensor Networks*. Book chapter, in: « Handbook of Sensor Networks », I. Mahgoub and M. Ilyas (eds.), CRC press, Section VIII, no. 36. 2004.

[7] Xuanwen Luo, Ming Dong et Yinlun Huang. *On Distributed Fault-Tolerant Detection in Wireless Sensor Networks.* IEEE Transactions on Computers, vol. 55, no. 1, pp. 58-70. Jan. 2006.

[8] Nova Ahmed, Rajnish Kumar, Robert Steven French et Umakishore Ramachandran. *RF^{2}ID: A Reliable Middleware Framework for RFID Deployment.* In the Proceedings of the 21st International Parallel and Distributed Processing Symposium. IPDPS 2007. California.

[9] Imad Belkacem, Oum-El-Kheir Aktouf et Safia Nait Bahloul. *Vers la tolérance aux fautes dans les systèmes RFID.* In Proceedings of the Second International Conference on Systems and Information Processing, ICSIP'11. page 65. Guelma, Algeria. May 15-17, 2011.

[10] Imad Belkacem, Oum-El-Kheir Aktouf et Safia Nait Bahloul. *Analyse des données d'un système RFID en vue de sa sûreté de fonctionnement.* In Proceedings of the 1st International Conference on Information Systems and Technologies, ICIST'11. Tébessa, Algeria. 2011.

[11] I. Belkacem, I. Kara Mostapha. Simulation à base de services web. Mémoire de fin d'études pour l'obtention du diplôme d'ingénieur d'état en informatique. Département d'Informatique, Faculté des sciences, Université de Mostaganem. 2008.

[12] JEANNE-BEYLOT Bernard. ABC de l'identification par étiquettes radiofréquence. Décembre 2003.

[13] Antti Ruhanen , Marko Hanhikorpi , Fabrizio Bertuccelli , Annamaria Colonna , Westy Malik , Damith Ranasinghe , Tomas Sánchez López , Na Yan et Matti Tavilampi . Sensor-enabled RFID tag handbook . Building Radio frequency IDentification for the Global Environment Project. 2008.

[14] H. Norton. Transducer fundamentals. In Handbook of Transducers. Englewood Cliffs, NJ: Prentice Hall, ch. 2. 1989.

[15] Xavier BARRAS. RFID, Normes et Standards. Conférence. Salon de Traçabilité. CNIT. 2006.

[16] John Footen et Joey Faust. The Service-Oriented Media Enterprise: SOA, BPM, and Web Services in Professional Media Systems, Focal Press. Chapitre 4 definition of a middleware. ISBN : 9780240809779. 2008.

[17] AIRIAU Roland (France Télécom R&D), BALTER Roland (ScalAgent / ObjectWeb), DONSEZ Didier (Univ. Joseph Fourier, Grenoble), GENON-CATALOT Denis (Université Pierre Mendés France, Valence), LEGENDRE Jean-François (AFNOR), LETELLIER François (INRIA / ObjectWeb), MENGA David (EDF), ROJEY Laurent (Minéfi / DGE) , SARRAILLON Joël Pôle (Traçabilité), TATOUT Frédéric (Minéfi / DGE) et THONNET Michèle (Ministère de la Santé). Étiquettes électroniques (RFID) -

Infrastructures logicielles et middleware. Rapport d'une étude RFID de la .Direction Générale des Entreprises (Minéfi).2006.

[18] Michel Rousseau. Ce qu'attendent les applications d'un middleware RFID. Solutions et applications RFID. 2006.

[19] B.S. Prabhu, Xiaoyong Su, Charlie Qiu, Harish Ramamurthy, Peter Chu et Rajit Gadh. WinRFID – Middleware for Distributed RFID Infrastructure. Wireless Internet for the Mobile Enterprise Consortium. University of California, Los Angeles. 2005.

[20] AspireRFID. Site officiel de AspireRFID. http://wiki.aspire.ow2.org.

[21] AspireRFID Architecture.

http://wiki.aspire.ow2.org/xwiki/bin/view/Main.Documentation/AspireRfidArchitecture.

[22] Fosstrak: Open Source RFID Software Platform .Site officiel de Fosstrak. http://www.fosstrak.org/.

[23] John Soldatos et Didier Donsez. The AspireRfid Project: Is Open Source RFID Middleware still an option? RFID World. 2009.

[24] Nikos Kefalakis, Nektarios Leontiadis, John Soldatos, and Didier Donsez. Middleware Building Blocks for Architecting RFID Systems. 1st Mobilight Conference. May 2009.

WinRFID. Site de WINMEC : http://winmec.ucla.edu/rfid/winrfid/.

Chapitre III:

Conception et réalisation du système

III.1. INTRODUCTION

Parmi les caractéristiques attendues des services offerts par les systèmes RFID : la fiabilité. Malheureusement, la lecture, la détection et les mesures des capteurs sont inévitablement sujettes à des erreurs. Une erreur peut être définie comme une valeur arbitraire d'un processus de détection ou d'inventaire par un lecteur ou une mesure incohérente par un capteur, qui ne peut être systématiquement compensée. Nous considérons les défauts liés à des mesures incorrectes. Une technique de sécurité

La fonction dont traitent ces notes est la tolérance aux pannes. Elle peut être définie comme : « La méthode qui permet à un système d'exécuter ses fonctions malgré des défauts pouvant affecter ses composants, sa conception ou son interaction avec les humains ou d'autres systèmes » [5]. Quelles que soient les précautions prises, la survenance de défauts est inévitable (erreur humaine, intention malveillante, obsolescence des équipements, catastrophe naturelle, etc.). Cependant, il est nécessaire de s'assurer que le service est fourni malgré l'apparition de dysfonctionnements [26]. Comme il est coûteux de construire une tolérance aux pannes au niveau de l'étiquette du lecteur, nous nous attendons à ce que de nombreuses approches tolérantes aux pannes pour cette tâche émergent au niveau du logiciel interne. Le développement d'applications complexes conduit à la nécessité de développer des logiciels internes plus complexes. Inter-logiciel est le modèle logiciel utilisé par l'industrie pour incorporer diverses technologies dans l'infrastructure de traitement existante avec une interruption minimale. Le logiciel interne fournit des services de haut niveau liés aux besoins de communication des applications. Nous expliquons ici le concept du logiciel RFID et montrons le rôle essentiel qu'il joue.

La plupart des travaux liés à la tolérance aux pannes et à son évaluation ont été réalisés dans des réseaux de capteurs. Nous nous intéressons à ce travail dans deux ouvrages. Le premier est le travail de FarinazKoushanfar, MiodragPotkonjak et Alberto Sangiovanni-Vincentelli [6] qui introduit une technique basée sur la validation pour la détection en ligne des défauts des capteurs. Le deuxième travail est [7] dans lequel les auteurs abordent la tolérance aux pannes distribuée dans les réseaux de capteurs. Peu de travaux ont étudié la tolérance aux pannes dans les systèmes RFID, et la plupart des solutions de ces systèmes traitent du manque de fiabilité inhérent des technologies RFID et ne traitent pas spécifiquement de la tolérance aux pannes. Dans [8], les auteurs ont étudié le comportement incertain des dispositifs RFID et ont conçu et mis en œuvre un middleware RFID appelé

RF2ID (Reliable Radio Frequency Identification Infrastructure) pour réguler et gérer les demandes de flux de données. données de manière efficace.

L'approche que nous souhaitons développer est basée sur deux idées **:**

1. ConcevoirunsystèmededécisionRFIDdistribuéens'inspirantdutravaildeXuanwenLuoet al.[7].
2. Comparer les résultats des inventaires des différents lecteurs, d'une part. Ensuite ,comparer les résultats des différents capteurs homogènes en utilisant des techniques statistiques non paramétriques sur les résultats obtenus pour identifier les mesures qui ne sont pas corrigeables. Nous nous inspirons du travail de F.K oushanfaretal.[6].

Nous traitons dans la section suivant e notre contribution et le schéma proposé pour palier au problème de la tolérance aux fautes dans les systèmes RFID:" Analyse des données d'un système RFID en vue de sa sûreté de fonctionnement"

III.2CONTRIBUTION:"ANALYSEDESDONNÉESD'UNSYSTÈMERFID ENVUEDESA SÛRETÉ DEFONCTIONNEMENT"

Schéma adopté

L'objectif de notre approche est de concevoir un système de décision RFID tolérant aux pannes vis-à-vis d'un événement.

Pour cela, nous considérons des articles auxquels sont attachées des étiquettes RFID, et certaines de ces étiquettes sont équipées de capteurs de température, d'humidité, etc. (voir Figure III.18).

Nous avons N lecteurs qui découvrent et confinent un ensemble d'étiquettes contenant M capteurs pour surveiller une hypothèse inconnue. Chaque lecteur transmet ses résultats (inventaire des étiquettes, résultats des différents capteurs) au middleware. Nous comparons les valeurs pour chaque détection faite par les lecteurs et pour chaque mesure de capteur. Enfin, nous effectuons une analyse statistique sur les données pour chaque lecteur et chaque capteur. Si les valeurs obtenues pour le lecteur ou capteur n'entrent pas dans l'intervalle de confiance calculé par la méthode des pourcentages, alors ce lecteur ou capteur est considéré comme défectueux. Les lecteurs et les capteurs de proximité sont susceptibles d'avoir des résultats similaires. Les étiquettes électroniques sont affichées dans une zone spécifique et

certaines de ces étiquettes sont équipées de capteurs (capteurs M) pour surveiller un événement.

Chaque lecteur RFID inventorie et détecte un ensemble d'étiquettes indépendamment des autres lecteurs, et certaines étiquettes sont équipées de capteurs. Les résultats sont agrégés par le middleware pour permettre une prise de décision globale pour le phénomène étudié (décision à prendre au niveau du middleware pour l'exemple illustratif de la section 5 pour les produits alimentaires : événement (produits alimentaires modifiés) ou non-événement (pas de changement) produits alimentaires).

Nous avons réparti la charge sur plusieurs stations : chaque station sera responsable d'un groupe de lecteurs pour améliorer la nature des données produites par les lecteurs. Avec de grandes quantités de données et réparties sur plusieurs emplacements géographiques pour les systèmes RFID, le système global doit être capable d'atteindre des complexités qui permettent à son évolutivité de répondre efficacement aux demandes des utilisateurs. Ces problèmes sont amplifiés dans les systèmes RFID où les données sont générées par des appareils susceptibles de tomber en panne, tels que les lecteurs et capteurs RFID. Lect1, Lect2, ..., LectN et les capteurs adjacents produisent généralement des résultats et des mesures similaires.

Ainsi, les principaux composants de notre architecture sont les terminaux, les lecteurs, les tags et les capteurs RFID. La station est responsable d'un groupe de lecteurs. Une station est un composant statique identifié par son adresse IP.

Chaque lecteur est identifié par son adresse IP (la station à laquelle il appartient) et son numéro de port.

Les lecteurs sont des dispositifs actifs capables de détecter des tags en envoyant un signal d'une certaine fréquence. Nous supposons que le disque a certaines capacités de traitement et de stockage (par exemple, le disque doit pouvoir mettre en cache un certain nombre d'ID, etc.). La couverture des lecteurs est un paramètre système qui doit être pris en compte lors du processus de publication.

Les tags pris en compte dans notre système sont des dispositifs actifs pouvant répondre aux demandes des lecteurs. Nous utilisons des étiquettes actives (ex : tag RFID actif - capteur de température ITEMS_ET° : ce sont des étiquettes longue portée avec capteur de température intégré, l'étiquette donne les codes d'identification et de température) (voir Figure III.17).

Figure III.17: Tag RFID Active- capteur température ITEMS_ET°

Chaque tag possède un identifiant unique et le renvoie lorsque le lecteur le lui demande. De plus, nous supposons que les étiquettes peuvent changer de position à tout moment.

Il est possible que le réseau considéré contienne des lecteurs ou capteurs défectueux et cela est dû : à l'environnement qui est parfois sévère et aussi aux raisons de fabrication. Alors que la sécurité de fonctionnement des systèmes RFID dépend non seulement de la sécurité de fonctionnement des lecteurs et des capteurs, mais également d'autres facteurs (interférences RF, environnement de déploiement, placement des lecteurs et des étiquettes, configuration des lecteurs) [8].

Pour atteindre la tolérance aux pannes de manière évolutive et distribuée, nous proposons un schéma de détection (Fig. 2.II) dans lequel nous utilisons une technique d'itération logicielle avec un middleware qui analyse les données reçues des stations. Nous utilisons également la redondance dans les appareils

Passif. Le middleware reçoit des données de différents terminaux, chaque terminal S étant responsable d'un ensemble de lecteurs RFID physiques. Chaque station S est responsable de la gestion des données, de la gestion des itinéraires et de la gestion des commandes. Les stations utilisent des variables locales et des structures de données pour prendre des décisions locales individuelles qui affectent le comportement du système dans son ensemble.

À partir des résultats qui viennent des lecteurs, le middleware peut :

1. inventorier les étiquettes;
2. détecte renligne les lecteurs et les capteurs défectueux en faisant une analyse statistique sur les résultas des lecteurs et des capteurs.

3. Prendre une décision binaire concernant l'événement étudié (événement ou non événement ,par exemple si la température dépasse 40° ,le produit alimentaire est considéré altéré);

Nous voulons que la décision finale prise par notre système soit fiable même s'il y a des défaillances dans certains composants de notre système. Notre objectif est d'atteindre une tolérance aux pannes distribuée car la décision finale d'inventaire n'est pas prise par un seul lecteur. Ainsi, la décision finale pour chaque type d'observation n'est pas prise à partir des résultats d'un seul capteur. Les lecteurs et capteurs qui donnent des résultats qui ne correspondent pas à ceux des autres lecteurs et capteurs sont considérés comme défectueux et leurs résultats sont éliminés dans l'analyse : nous avons corrigé des dysfonctionnements qui pourraient affecter les résultats finaux du middleware.

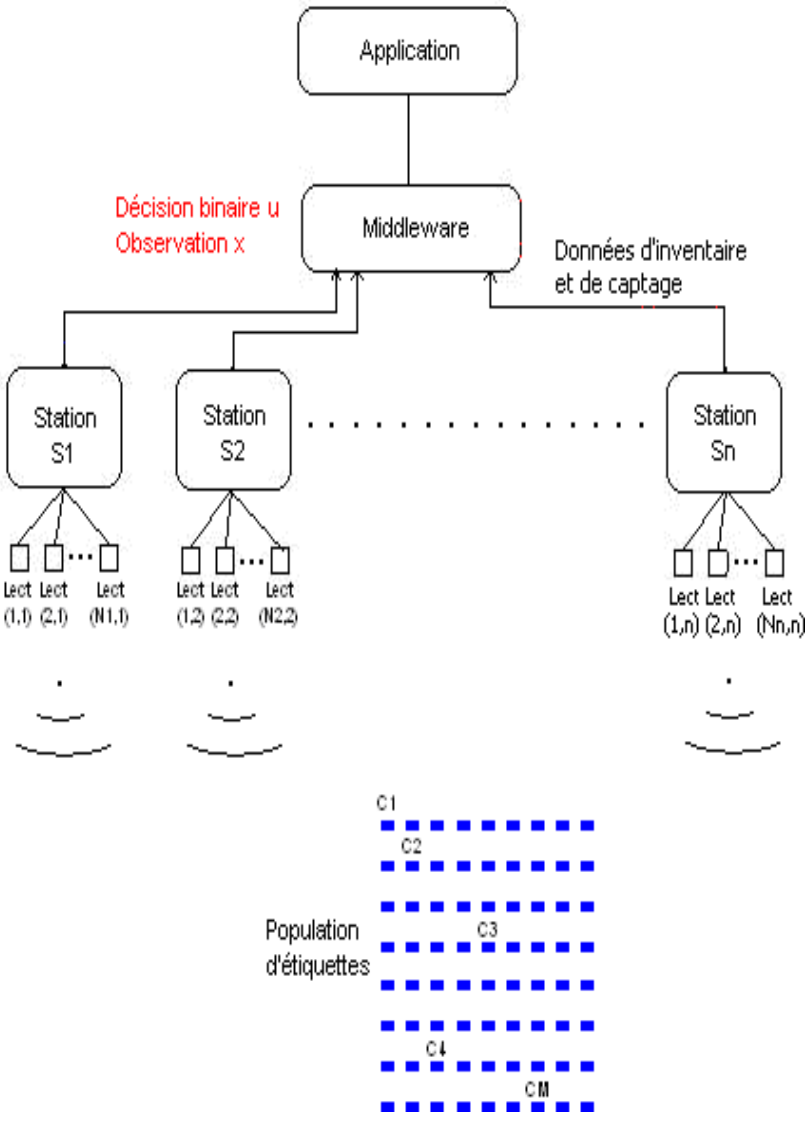


Figure III.18: Redondance matérielle passive (duplication du matériel :lecteurs ,capteurs et station se t un voteur logiciel au niveau du middleware).

III.3 Notre méthodologie

Nous décrivons dans cette section notre méthodologie pour détecter les lecteurs et les capteurs défectueux pour avoir une décision globale(événement ou non événement)plus fiable.

a. L'activation des lecteurs se fait pendant des intervalles de temps séparés pour éviter les interférences lecteur –lecteur qui peuvent influencer l'exactitude de notre étude.

b. Le middleware récupère les résultats des différents lecteurs :l'inventaire des lecteurs et les données des différents capteurs(de chaleur et d'humidité par exemple).

c. Le middleware analyse statistiquement les résultats des inventaires réalisés par les lecteurs en sélectionnant un pourcentage approprié (95 % par exemple). Le choix du pourcentage est crucial dans notre étude. Si le résultat du compteur n'entre pas dans l'IC (ici à 95 %) alors ce compteur est considéré comme défectueux ; Ensuite, les résultats que prend ce lecteur ne sont pas pris en compte dans l'analyse statistique des capteurs. Nous incluons ce lecteur dans la liste des lecteurs défectueux (LD).

d. **L'analyse statistique** est faite ensuite sur les données collectées parles capteurs .Nous souhaitons détecter les capteurs endommagés. Nous voulons détecter les capteurs endommagés. Nous étudions chaque type de capteur en ignorant les résultats renvoyés par les lecteurs appartenant aux difficiles à apprendre. Nous concevons une matrice de données. Nous choisissons l'intervalle de confiance à 95%. Nous obtenons les indices des capteurs qui ont donné des résultats en dehors de l'intervalle de confiance. Ces capteurs sont suspectés d'être défectueux. Cependant, la question se pose : quand considère-t-on que le capteur est défectueux ? Nous devons donc définir le seuil de fausses valeurs dans chaque analyse par lequel nous déterminons que ce capteur est faux

e. Après avoir supprimé les valeurs prises par les capteurs défaillants, le middleware prend une note finale pour chaque type de capteur xi (une moyenne recalculée peut être utile) à partir de laquelle une décision binaire globale u (événement ou non-événement) est prise..

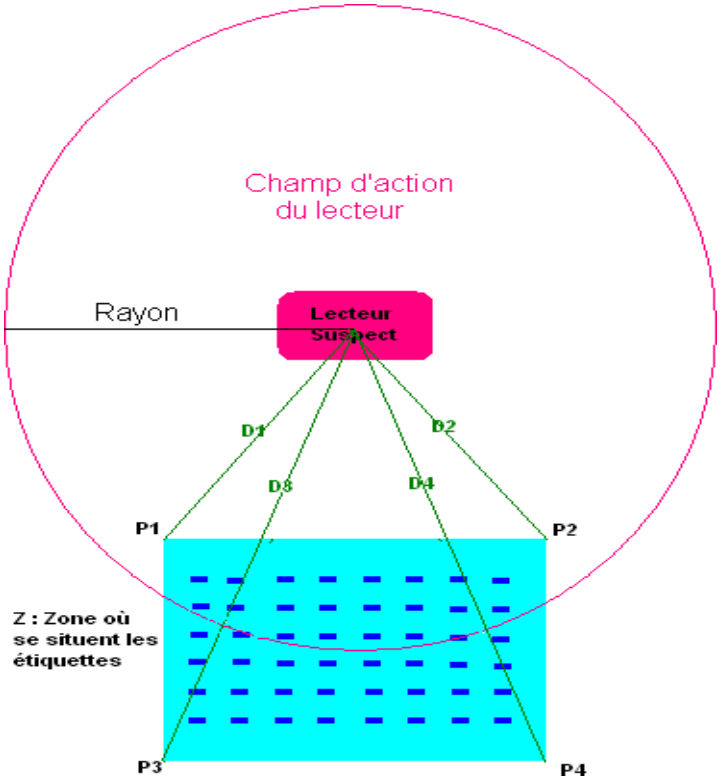


Figure III.19: Validité de la décision concernant le lecteur suspect

Nous supposons connues les coordonnées des quatre points d'extrémité P_1 ,P_2,P_3 ,P_4 de la zone où les étiquettes se déplacent.

Le GPS nous retourne les informations relatives à l'emplacement du lecteur.

Nous calcule les distances D_1 ,D_2,D_3 ,D_4 et nous les comparons avec le rayon du champ d'action R du lecteur.

Si $D_1<R$ et $D_2<R$ et $D_3<R$ et $D_4<R$.

Cela signifie que le champ d'action couvre 100% la zone Z, alors le lecteur suspect devient défectueux.

EXEMPLEILLUSTRATIF

La figure III.4 illustre notre exemple. Nous avons les données suivantes :

Nous avons 24 étiquettes, les étiquettes sont numérotées dans la figure E_1,…, E_{24} . Certaines de ces étiquettes sont équipées de capteurs .C_1,C_2, C_3 sont des capteurs de chaleur ;C'_1 ,C'_2 ,C'_3 sont des capteurs d'humidité.

Pour les capteurs de température :le capteur C_1 est attaché à l'étiquette E_1 ,le capteur C_2 est attaché à l'étiquette E_{10} et le capteur C_3 est attaché à l'étiquette E_{20}.

Pour les capteurs d'humidité :le capteur C'_1 est attaché à l'étiquette E_4, le capteur C'_2 est attaché à l'étiquette E_{14} et le capteur C'_3 est attaché à l'étiquette E_{24}.

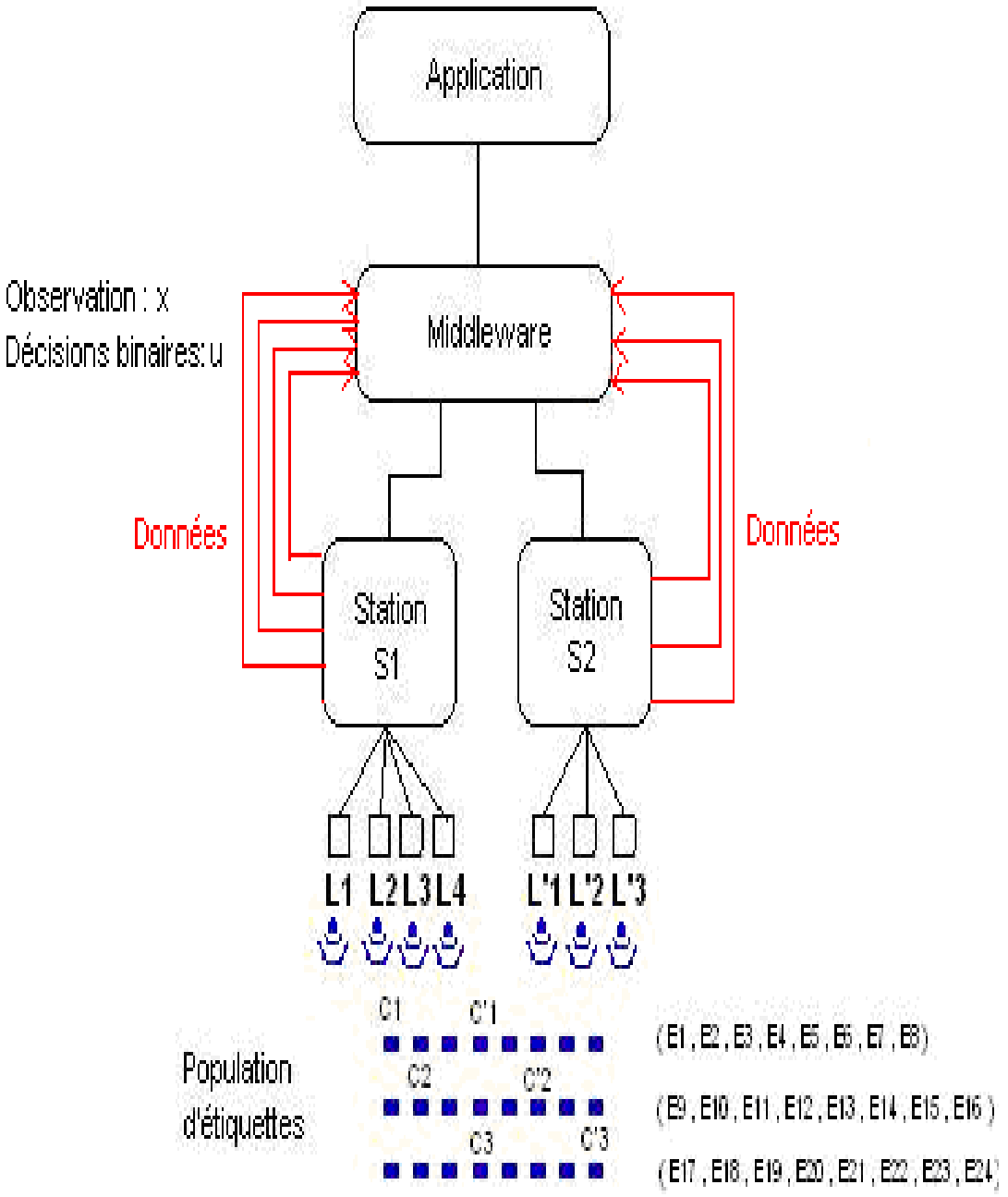


Figure 20: exemple illustratif

Ces étiquettes sont lues par 7 lecteurs qui sont attachés à deux stations :L_1,L_2 ,L_3 ,L_4 sont attachés à la station S_1; L' $_1$, L'$_2$,L'$_3$ à la station S_2.

En résumé, nous avons :

Le nombre d'étiquettes E=24.

Le nombre de lecteursN=7;N_1=4,N_2=3. Le nombre de capteursM=6;M_1=M_2=3.

La liste des lecteurs attachés à la station S_1:L_1={L_1,L2,L3,L4}. La liste des lecteurs attachés à la station S_2:L_2={L'$_1$,L'2,L'3}. La liste des capteurs de température :CT={C_1,C2,C3}.

La liste des capteurs d'humidité: CH = {C'$_1$, C'2, C'3}.

Les étiquettes sont attachées à des produits alimentaires .Nous faisons les inventaires des différents lecteurs et la collection des données des différents capteurs d'une façon périodique (chaque quart d'heure). L'activation des lecteurs est séparée par une période t pour éviter les interférences lecteur -à- lecteur et lecteur-à-étiquette[2].

Au niveau du middleware ,nous avons la décision globale :le middleware décide après inventaires et après récupération des résultats des capteurs quels sont les lecteurs et les capteurs défectueux .Si aucun lecteur ou capteurn' est défectueux ,le middleware prend:

- Une observation finale concernant chaque type de capteur X.
- La décision globale binaire concernant le produit alimentaire :événement ou non événement.

Si Température >40° ou Humidité >80% alors le produit alimentaire est altéré(événement)si non le produit alimentaire est non altéré (non événement).

II.4 Résultats des inventaires et des observations des capteurs :

Une étiquette est considérée lue si le lecteur par vient à lires on identifiant .Les résultats des inventaires des différents lecteurs sont:

Pour la station S_1: le lecteur L_1 a détecté 22 étiquettes, le lecteur L_2 a détecté 23 étiquettes, le lecteur L_3 a détecté 24 étiquettes, le lecteur L_4 a détecté 24 étiquettes.

Pour la stationS_2: le lecteur L'_1 a détecté 10 étiquettes, le lecteur L'_2 a détecté 23 étiquettes le lecteur L'_3 a détecté 22 étiquettes.

En lisant l'étiquette, le lecteur détecte si cette étiquette est dotée d'un capteur .Si c'est le cas, il détecte son type et récupère son observation .Les observations des différents capteurs sont données dans le Tableau III.2. Le symbole / Signifie que l'étiquette qui inclut ce capteur n'a pas été détectée par le lecteur associé.

Tableau III.2: Résultats de captage

	L_1	L_2	L_3	L_4	L'_1	L'_2	L'_3
C_1	37°	38°	37°	37°	/	37°	38°
C_2	36°	37°	37°	37°	/	38°	/
C_3	37°	36°	36°	38°	37°	38°	37°
C'_1	70 %	71 %	70 %	70 %	72 %	69 %	68 %
C'_2	50 %	23 %	69 %	89 %	46 %	25 %	24 %
C'_3	/	/	70 %	70 %	/	72 %	69 %

1ère Analyse des données

Analyse des résultats des inventaires

Nous appliquons la formule suivante pour calculer la moyenne arithmétique :

$$\bar{x} = \frac{x_1 + x_2 + ... + x_n}{n} = \frac{1}{n}\sum_{i=1}^{n} x_i$$

…… (1)

Avec n=7, X_1=22 étiquettes, X_2= 23 , X_3=24 ,X_4=24, X_5=10,X_6=23 ,X_7=22, alors :

$\overline{X}$ (la moyenne)= 21.24 .

Pour calculer l'écart-type σ , nous appliquons la formule suivante :

$$\sigma = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_i - \overline{x})^2}$$

avec n=7, x =21.24 , alors : σ (écart-type)= 4.62

L'écarttypeestimportantcequisignifiequelesvaleursd'inventairesnesontpascentréesautour de la moyenne [38],ce qui signifie qu'il est fortprobablequ'unlecteurn'observepasbeaucoupd'étiquettes.

Si nous calculons l'intervalle de confiance de $\overline{X}$ (la moyenne)àenviron95%, **l**'intervalle de confiance à 95%est:

$$\overline{x} \pm$$

(□: écart type, x : moyenne, n : taille de l'échantillon).

Avec n=7,x=21.24(la moyenne) et σ(écart-type)=4.62. L'intervalle de confiance I C95%=[17.66,24.62]

Le résultat du lecteur L'_1 n'appartient pas à l'intervalle de confiance alors le lecteur L'_1 est défectueux**.** Nous ajoutons L'_1 dans la liste des lecteurs défectueux :LD={L'_1}.

Analyse des résultats des capteurs d'humidité

Nous concevons la matrice des valeurs en éliminant les valeurs prises par le lecteur L'_1(voirleTableauIII.3).

Tableau III.3: Matrice d'humidité

	L_1	L_2	L_3	L_4	L'_2	L'_3
C'_1	70 %	71 %	70 %	70 %	69 %	68 %
C'_2	50 %	23 %	69 %	89 %	25 %	24 %
C'_3	/	/	70 %	70 %	72 %	69 %

Nous utilisons la formule (1) pour calculer la moyenne x :

n=16,X_1=70%,X_2=71%,X_3=70%,X_4=70%,X_5=69%,X_6=68%,X_7=50%,X_8=23%,X_9=69%,X_{10}=89%,X_{11}=25%,
X_{12}=24%,X_{13}=70%,X_{14}=70%,X_{15}=72%etX_{16}=69%.Alors:x(lamoyenne)=61.19%.

Nous appliquons la formule (2) pour calculer l'écart-type ɵ :

n=16,X_1=70%,X_2=71%,X_3=70%,X_4=70%,X_5=69%,X_6=68%,X_7=50%,X_8=23%,X_9=69%,X_{10}=89%,X_{11}=25%,
X_{12}=24%,X_{13}=70%,X_{14}=70%,X_{15}=72%,X_{16}=69%etx(lamoyenne)=61.19%.Alors:ɵ(écart-type)=19.16.

Nous appliquons la formule (3) pour calculer l'intervalle de confiance à 95% :

Nous avons n=16, x (la moyenne) = 61.19% et ɵ (écart-type)=19.16 alors : IC95%= [51.61%, 70.77%]

Nous parcourons la matrice des valeurs et nous testons chaque valeur. Si cette valeur n'appartient pas à l'intervalle de confiance , nous récupérons l'indice de ligne(indice du capteur).

Les valeurs 50% , 23% , 89% , 25% , 24%, 72% n'appartiennent pas à IC95%.

III 2.2 Discussion : Comment considérer qu'un capteur est défectueux ?

Les valeurs prises par chaque capteur peuvent varier : elles sont prises à des moments différents. Nous pensons qu'un capteur ne peut être considéré comme défectueux que s'il donne une valeur qui n'entre pas dans l'intervalle de confiance. Nous suggérons donc d'utiliser un rapport R pour chaque capteur qui produit des résultats en dehors de l'intervalle de confiance pour décider si ce capteur est mauvais ou non. Pour chaque capteur dont nous extrayons l'indice, nous calculons le rapport:

$$R = \frac{\text{Le nombre des valeurs qui n'appartiennent pas à IC95\%}}{\text{Le nombre total des valeurs prises par ce capteur}}$$

Et nous définissons un seuil à partir du quel nous décidons que le capteur est défectueux ,par exemple80% PourC'_2:R=6/7=0.86% alors le capteur C'_2 est défectueux.

Nous insérons ce capteur dans la liste des capteurs d'humidité défectueux :CHD={C'_2}
Analyse des résultats des capteurs de température

Nous refaisons la même analyse pour les capteurs de température.

Nous utilisons la formule (1) pour calculer la moyenne x :

n=18,X_1=37°,X_2=38°,X_3=37°,X_4=37°,X_5=37°,X_6=38°,X_7=36°,X_8=37°,X_9=37°,X_{10}=37°, X_{11}=38°,X_{12}=37°,
X_{13}=36°,X_{14}=36°,X_{15}=38°,X_{16}=37°,X_{17}=38°etX_{18}=37°.Alors:x(lamoyenne)=37.12°

Nous appliquons la formule (2) pour calculer l'écart-type ɵ :

n=18,X_1=37°,X_2=38°,X_3=37°,X_4=37°,X_5=37°,X_6=38°,X_7=36°,X_8=37°,X_9=37°,X_{10}=37°, X_{11}=38°,X_{12}=37°,
X_{13}=36°,X_{14}=36°,X_{15}=38°,X_{16}=37°,X_{17}=38°,X_{18}=37°etx(lamoyenne)=37.12°.Alors:ɵ(écart-type)=0.67

Nous appliquons la formule (3) pour calculer l'intervalle de confiance à 95% :

Nous avons n=18, x (la moyenne) = 37.12° et ɵ (écart-type)=0.67 alors : IC95%=[36.79,37.45].

L'étendue=Borne Supérieure – Borne inférieure de l'IC95% =37.45-36.79=0.66 n'est pas importante.

L'écart type n'est pas important ce qui signifie que les valeurs d'inventaires sont centrées autour de la moyenne, cela veut dire que tous les capteurs de température donnent des résultats proches et raisonnables.

2ème Analyse:Réétude avec la non prise en compte des résultats provenant des lecteurs et capteurs défectueux

Le but ici est la production de décisions finales fiables .Nous construisons une nouvelle matrice de données, cette matrice n 'inclut pas les résultats des lecteurs et des capteurs défectueux.

Tableau III.4: Nouvelle matrice de données

	L_1	L_2	L_3	L_4	L'_2	L'_3
C_1	37°	38°	37°	37°	37°	38°
C_2	36°	37°	37°	37°	38°	/
C_3	37°	36°	36°	38°	38°	37°
C'_1	70 %	71 %	70 %	70 %	69 %	68 %
C'_3	/	/	70 %	70 %	72 %	69 %

Inventaires des lecteurs :Nombre d'étiquettes = 23 étiquettes (la moyenne des inventaires est prise en excluant le résultat du lecteur$\overline{L'1}$).

Les capteurs de chaleurs : L'observation finale de température : x_T=**37.12°**

Les capteurs d'humidité : L'observation finale d'humidité (après élimination les résultats du capteur C'_2) :

x_H = **69.90°.**

La décision finale concernant l'événement :u=0Produit non altéré (Non événement)car température<40° et Humidité <80%.

Pour obtenir une meilleure correction d'erreur, notre schéma de décision doit prendre en compte l'erreur de détection du lecteur et l'erreur du capteur en choisissant un meilleur pourcentage et un meilleur intervalle de confiance (si l'intervalle de confiance à 95% génère beaucoup de valeurs erronées, nous pouvons utiliser par exemple l'intervalle à 99,7 %) et en optimisant le seuil R pour déterminer que le lecteur est défectueux.

CONCLUSION

Dans ce chapitre, nous présentons notre contribution à la résolution du problème de tolérance aux pannes des systèmes RFID : « Analyse des données d'un système RFID en vue de son intégrité opérationnelle ».

Pour atteindre la tolérance aux pannes de manière évolutive et distribuée, nous avons proposé un schéma de décision dans lequel nous avons utilisé une technique d'itération logicielle avec un middleware qui analyse les données provenant des stations. Notre objectif était d'atteindre une tolérance aux pannes distribuée puisque la décision finale n'est pas prise par un seul lecteur ou par un seul capteur par type. Les lecteurs et capteurs qui donnent des résultats qui ne correspondent pas à ceux des autres lecteurs et capteurs sont considérés comme défectueux et leurs résultats sont rejetés dans l'analyse, ce qui permet de corriger les erreurs qui pourraient affecter nos résultats.

Références bibliographiques

[25] Klaus Finkenzeller. *RFID Handbook : Fundamentals and Applications in Contactless Smart Cards and Identification*. Deuxième Édition, John Wiley & Sons, Ltd., England. ISBN 0-470-84402-7.2003.

[26] Pattabhiraman Krishna et David Husak. *RFID INFRASTRUCTURE*. IEEE Communications Magazine.Volume: 45, Issue: 9, Pages: 4-10. Septembre 2007.

[27] Yves Saint-Oyant et Jonathan Brisart. *La norme RFID*. Thèse de Master IAGL. Université desciences et technologies. Lille1. 2010.

[28] Laprie, J. C, et al. *Guide de la sûreté de fonctionnement.* 2ème édition, Cépaduès Éditions. ISBN2-85428-382-1. 1996.

[29]

a. Thi-Quynh Bui, Oum-El-Kheir Aktouf, Michel Dang, Levent Gürgen et Claudia Roncancio. *Diagnosis Service for Software Component and Its Application to a Heterogeneous Sensor Data Management System.* depend, pp.143-149. Second International Conference on Dependability. 2009.

b. Thi Quynh BUI. *SERVICE DE DIAGNOSTIC EN LIGNE POUR LES APPLICATIONS A BASE DE COMPOSANTS LOGICIELS*. THESE pour obtenir le grade de DOCTEUR DE GRENOBLE INP - Préparée au Laboratoire de Conception et d'Intégration des Systèmes (LCIS) dans le cadre de l'Ecole Doctorale "Mathématiques, Sciences et Technologies de l'Information, Informatiques (MSTII)" . 14 Octobre 2009.

[30] F. Koushanfar , M. Potkonjak et A. Sangiovanni-Vincentelli. *Fault-Tolerance in Sensor Networks*. Book chapter, in: « Handbook of Sensor Networks », I. Mahgoub and M. Ilyas (eds.), CRC press, Section VIII, no. 36. 2004.

[31] Xuanwen Luo, Ming Dong et Yinlun Huang. *On Distributed Fault-Tolerant Detection in Wireless Sensor Networks.* IEEE Transactions on Computers, vol. 55, no. 1, pp. 58-70. Jan. 2006.

[32] Nova Ahmed, Rajnish Kumar, Robert Steven French et Umakishore Ramachandran. *RF^{2}ID: A Reliable Middleware Framework for RFID Deployment.* In the Proceedings of the 21st International Parallel and Distributed Processing Symposium. IPDPS 2007.

California.

[33] Imad Belkacem, Oum-El-Kheir Aktouf et Safia Nait Bahloul. *Vers la tolérance aux fautes dans les systèmes RFID.* In Proceedings of the Second International Conference on Systems and Information Processing, ICSIP'11. page 65. Guelma, Algeria. May 15-17, 2011.

[34] Imad Belkacem, Oum-El-Kheir Aktouf et Safia Nait Bahloul. *Analyse des données d'un système RFID en vue de sa sûreté de fonctionnement.* In Proceedings of the 1st International Conference on Information Systems and Technologies, ICIST'11. Tébessa, Algeria. 2011.

[35] I. Belkacem, I. Kara Mostapha. *Simulation à base de services web*. Mémoire de fin d'études pour l'obtention du diplôme d'ingénieur d'état en informatique. Département d'Informatique, Faculté des sciences, Université de Mostaganem. 2008.

[36] JEANNE-BEYLOT Bernard. *ABC de l'identification par étiquettes radiofréquence*. Décembre 2003.

[37] Antti Ruhanen , Marko Hanhikorpi , Fabrizio Bertuccelli , Annamaria Colonna , Westy Malik , Damith Ranasinghe , Tomas Sánchez López , Na Yan et Matti Tavilampi . *Sensor-enabled RFID tag handbook* . Building Radio frequency IDentification for the Global Environment Project. 2008.

[38] H. Norton. *Transducer fundamentals*. In Handbook of Transducers. Englewood Cliffs, NJ: PrenticeHall, ch. 2. 1989.

[39] Xavier BARRAS. *RFID, Normes et Standards*. Conférence. Salon de Traçabilité. CNIT. 2006.

[40] John Footen et Joey Faust. *The Service-Oriented Media Enterprise: SOA, BPM, and Web Services in Professional Media Systems*, Focal Press. Chapitre 4 *definition of a middleware*. ISBN : 9780240809779. 2008.

[41] AIRIAU Roland (France Télécom R&D), BALTER Roland (ScalAgent / ObjectWeb), DONSEZ Didier (Univ. Joseph Fourier, Grenoble), GENON-CATALOT Denis (Université Pierre Mendés France, Valence), LEGENDRE Jean-François (AFNOR), LETELLIER François (INRIA / ObjectWeb), MENGA David (EDF), ROJEY Laurent (Minéfi / DGE) , SARRAILLON Joël Pôle (Traçabilité), TATOUT Frédéric (Minéfi /

DGE) et THONNET Michèle (Ministère de la Santé). *Étiquettes électroniques (RFID) - Infrastructures logicielles et middleware*. Rapport d'une étude RFID de la .Direction Générale des Entreprises (Minéfi).2006.

[42] Michel Rousseau. *Ce qu'attendent les applications d'un middleware RFID*. Solutions etapplications RFID. 2006.

[43] B.S. Prabhu, Xiaoyong Su, Charlie Qiu, Harish Ramamurthy, Peter Chu et Rajit Gadh. *WinRFID – Middleware for Distributed RFID Infrastructure*. Wireless Internet for the Mobile Enterprise Consortium. University of California, Los Angeles. 2005.

[44] *AspireRFID*. Site officiel de AspireRFID. http://wiki.aspire.ow2.org.

[45] *AspireRFID Architecture*. http://wiki.aspire.ow2.org/xwiki/bin/view/Main.Documentation/AspireRfidArchitecture.

[46] *Fosstrak: Open Source RFID Software Platform* .Site officiel de Fosstrak. http://www.fosstrak.org/.

[47] John Soldatos et Didier Donsez. *The AspireRfid Project: Is Open Source RFID Middleware still anoption?* RFID World. 2009.

[48] Nikos Kefalakis, Nektarios Leontiadis, John Soldatos, and Didier Donsez. Middleware Building Blocks for Architecting RFID Systems. 1st Mobilight Conference. May 2009.

WinRFID. Site de WINMEC : http://winmec.ucla.edu/rfid/winrfid/.

Conclusion générale

Conclusion générale

Dans ce travail nous avons étudié et simulés les antennes RFID en utilisant le logiciel CST studio suite. Les différentes étapes de conception et de simulation de ces antennes ont été présentées en détail. Nous avons suivi ces étapes afin de faire notre nouvelle structure et nouveaux paramètres et pour arriver au simulation avec une optimisation dans le but d'obtenir des bons résultats dont une adaptation entre l'antenne et la puce dans le cas où on a un tag avec puce, Nous avons aussi présenté les résultats de simulation de tous les antennes conçues. Dans le but de montrer l'effet des différents paramètres géométriques et physique tel que la permittivité sur les caractéristiques de l'antenne une étude paramétrique a été effectué afin de savoir quel est le paramètre le plus influant sur le rendement de notre antenne, après nous avons fait une optimisation pour arriver à la meilleure structure avec les conditions données. nous avons lancé la simulation avec une modélisation d'une puce commercialisée pour afficher les résultats dont le coefficient de réflexion à une fréquence bien précise, la bande passante, diagramme de rayonnement et la portée (distance de lecture).

Actuellement, le code à barres est progressivement remplacé par des tags RFID (Radio Fréquence Identification) dites aussi « étiquettes communicantes ayant la possibilité de stocker de l'information de manière dynamique et de communiquer sans fil avec leur l'environnement ambiant. Cette technologie trouve ses applications dans différents domaines tels que la traçabilité, suivi médical de l'état d'une passion, le pilotage de la production, Etc.…

La technologie RFID est devenue de plus en plus utilisée dans les divers domaines de la vie. La sûreté de fonctionnement de ces systèmes est donc indispensable pour permettre la livraison de services corrects aux utilisateurs du système.

Bibliographies

Bibliographie

[1] Klaus Finkenzeller. RFID Handbook : Fundamentals and Applications in Contactless Smart Cards and Identification. Deuxième Édition, John Wiley& Sons, Ltd., England. ISBN 0-470-84402-7. 2003.

[2] Pattabhiraman Krishna et David Husak. RFID INFRASTRUCTURE. IEEE Communications Magazine. Volume: 45, Issue: 9, Pages: 4-10. Septembre 2007.

[3] Yves Saint-Oyant et Jonathan Brisart. La norme RFID. Thèse de Master IAGL. Université de sciences et technologies. Lille1. 2010.

[4] Laprie, J. C, et al. Guide de la sûreté de fonctionnement. 2ème édition, Cépaduès Éditions. ISBN 2-85428-382-1. 1996.

[5] a. Thi-Quynh Bui, Oum-El-KheirAktouf, Michel Dang, LeventGürgen et Claudia Roncancio. Diagnosis Service for Software Component and Its Application to a Heterogeneous Sensor Data Management System.depend, pp.143-149. Second International Conference on Dependability. 2009.

b. Thi Quynh BUI. SERVICE DE DIAGNOSTIC EN LIGNE POUR LES APPLICATIONS A BASE DE COMPOSANTS LOGICIELS. THESE pour obtenir le grade de DOCTEUR DE GRENOBLE INP - Préparée au Laboratoire de Conception et d'Intégration des Systèmes (LCIS) dans le cadre de l'Ecole Doctorale "Mathématiques, Sciences et Technologies de l'Information, Informatiques (MSTII)" .14 Octobre 2009.

[6] F. Koushanfar , M. Potkonjak et A. Sangiovanni-Vincentelli. Fault-Tolerance in Sensor Networks.Book chapter, in: « Handbook of Sensor Networks », I. Mahgoub and M. Ilyas (eds.), CRC press, Section VIII, no. 36. 2004.

[7] XuanwenLuo, Ming Dong etYinlun Huang. On Distributed Fault-Tolerant Detection in Wireless Sensor Networks. IEEE Transactions on Computers, vol. 55, no. 1, pp. 58-70. Jan. 2006.

[8] Nova Ahmed, Rajnish Kumar, Robert Steven French etUmakishoreRamachandran. RF2ID: A Reliable Middleware Framework for RFID Deployment. In the Proceedings of the 21st International Parallel and Distributed Processing Symposium.IPDPS 2007. California.

[9] Imad Belkacem, Oum-El-KheirAktouf et Safia Nait Bahloul. Vers la tolérance aux

fautes dans les systèmes RFID. In Proceedings of the Second International Conference on Systems and Information Processing, ICSIP'11.page 65. Guelma, Algeria. May 15-17, 2011.

[10] Imad Belkacem, Oum-El-KheirAktouf et Safia Nait Bahloul. Analyse des données d'un système RFID en vue de sa sûreté de fonctionnement. In Proceedings of the 1st International Conference on Information Systems and Technologies, ICIST'11.Tébessa, Algeria. 2011.

[11] I. Belkacem, I. Kara Mostapha. Simulation à base de services web. Mémoire de fin d'études pour l'obtention du diplôme d'ingénieur d'état en informatique. Département d'Informatique, Faculté des sciences, Université de Mostaganem. 2008.

[12] JEANNE-BEYLOT Bernard. ABC de l'identification par étiquettes radiofréquence. Décembre 2003.

[13] AnttiRuhanen , Marko Hanhikorpi , Fabrizio Bertuccelli , Annamaria Colonna , Westy Malik , DamithRanasinghe , Tomas SánchezLópez , Na Yan et MattiTavilampi . Sensor-enabled RFID tag handbook .Building Radio frequency IDentification for the Global Environment Project. 2008.

[14] H. Norton. Transducer fundamentals.In Handbook of Transducers. Englewood Cliffs, NJ: Prentice Hall, ch. 2. 1989.

[15] Xavier BARRAS. RFID, Normes et Standards. Conférence. Salon de Traçabilité. CNIT. 2006.

[16] John Footenet Joey Faust. The Service-Oriented Media Enterprise: SOA, BPM, and Web Services in Professional Media Systems, Focal Press. Chapitre 4 definition of a middleware. ISBN : 9780240809779. 2008.

[17] AIRIAU Roland (France Télécom R&D), BALTER Roland (ScalAgent / ObjectWeb), DONSEZ Didier (Univ. Joseph Fourier, Grenoble), GENON-CATALOT Denis (Université Pierre Mendés France, Valence), LEGENDRE Jean-François (AFNOR), LETELLIER François (INRIA / ObjectWeb), MENGA David (EDF), ROJEY Laurent (Minéfi / DGE) , SARRAILLON Joël Pôle (Traçabilité), TATOUT Frédéric (Minéfi / DGE) et THONNET Michèle (Ministère de la Santé). Étiquettes électroniques (RFID) - Infrastructures logicielles et middleware. Rapport d'une étude RFID de la .Direction Générale des Entreprises (Minéfi).2006.

[18] Michel Rousseau. Ce qu'attendent les applications d'un middleware RFID. Solutions et applications RFID. 2006.

[19] B.S. Prabhu, Xiaoyong Su, Charlie Qiu, HarishRamamurthy, Peter Chu et RajitGadh. WinRFID – Middleware for Distributed RFID Infrastructure. Wireless Internet for the Mobile Enterprise Consortium.University of California, Los Angeles. 2005.

[20] AspireRFID. Site officiel de AspireRFID. http://wiki.aspire.ow2.org.

[21] AspireRFID Architecture. http://wiki.aspire.ow2.org/xwiki/bin/view/Main.Documentation/AspireRfidArchitecture.

[22] Fosstrak: Open Source RFID Software Platform .Site officiel de Fosstrak. http://www.fosstrak.org/.

[23] John Soldatos et Didier Donsez. The AspireRfid Project: Is Open Source RFID Middleware still an option? RFID World. 2009.

[24] Nikos Kefalakis, NektariosLeontiadis, John Soldatos, and Didier Donsez.Middleware Building Blocks for Architecting RFID Systems.1st Mobilight Conference. May 2009.

[25] WinRFID. Site de WINMEC : http://winmec.ucla.edu/rfid/winrfid/.

[26] Jean Arlat, Yves Crouzet, Yves Deswarte, Jean-Charles Fabre, Jean-Claude Laprie et David Powell. Tolérance aux fautes. Dans « Encyclopédie de l'informatique et des systèmes d'information », (J. Akoka and I. Comyn-Wattiau, Eds.), Partie 1 : La dimension technologique des systèmes d'information - Section 2 : L'architecture et les systèmes (M. Banâtre, Ed.), pp. 240-270. ISBN : 27117-4846-4,Vuibert. Paris, France. 2006.

[27] Mehdi JALLOULI. Méthodologie de conception d'architectures de processeur sûres de fonctionnement pour les applications mécatroniques. THESE DE DOCTORAT présentée pour obtenir le grade de docteur.Université Paul Verlaine – Metz. Discipline: Electronique, Spécialité: Microélectronique. Juin 2009.

[28] J-C. Laprie. Sûreté de fonctionnement des systèmes : concepts de base et terminologie. Revue de l'Électricité et de l'Électronique, No. 11, pp. 95-105. Déc 2004.

[29] Oum El KheirAktouf. Sûreté de fonctionnement des systèmes informatiques. Présentation de cours. Université d'Oran. 2009.

[30] Lala, P. K. Self-Checking and Fault-Tolerant Digital Design. Morgan Kaufmann Publishers. USA.

2001.

[31] AgustiSolanas, Josep Domingo-Ferrer, Antoni Martínez-Ballesté et VanesaDaza. A Distributed Architecture for Scalable Private RFID Tag Identification.In Proceedings of Computer Networks, Vol. 51, no. 0, pp. 2268-2279.ISSN: 1389-1286. Aug 2007.

[32] Julien David. Design d'un contrôleur de lecteurs RFID. Mémoire du projet de fin d'étude. Universitéd'Ottawa. Juillet 2008.

[33] R. Zurawski. Embedded Systems Handbook. Editions CRC Press. 2005.

[34] Hyndman RH et Fan Y. Sample quantiles in statistical packages. The American Statistician 50 (4): 361-365. 1996.

[35] Zar, J.H. Biostatistical Analysis. Prentice Hall International, New Jersey. pp 43–45. 1984.

[36] G. COSTANTINI. Estimation ponctuelle- Estimation par intervalle de confiance. Cours de statisiques.

www.sante.univ-nantes.fr/med/IntervalleDeConfiance.ppt.

[37] Rees. D.G. Essential Statistics.4th Edition, Chapman and Hall/CRC.ISBN 1-58488-007-4. 2001. [38]Walker, Helen. Studies in the History of the Statistical Method. Baltimore, MD: Williams & Wilkins

Co. pp. 24–25. 1931.

[39]M. HadiValipour, BavarAmirZafari, Kh. NikiMaleki, NeginDaneshpour. A Brief Survey of Software Architecture Concepts and Service Oriented Architecture .In Proceedings of 2nd IEEE International Conference on Computer Science and Information Technology, ICCSIT'09, pp 34-38. China. Aug 2009.

[40] Arsanjani A., Liang-Jie Zhang, Ellis M., Allam A. et Channabasavaiah K. S3: A Service-Oriented Reference Architecture .IT Professional Volume 9, Issue 3, Pages:10–17. May-June 2007.

[41] Z. Chergui et K. Djelloul. Approche de simulation DEVS à base de services web. Mémoire de fin d'études pour l'obtention du diplôme d'ingénieur d'état en informatique. Département d'Informatique, Faculté des sciences, Université d'Oran. 2007.

[42] Christoph Schroth et Till Janner. Web 2.0 and SOA: Converging Concepts Enabling the Internet of Services. IT Professional 9(3): 36-41 .2007.

[43] JDeveloper. Site officiel de Oracle JDeveloper. http://www.oracle.com/technetwork/developer-tools/jdev/overview/index.html.

[44]M. Guedda, A. Yazid. Une approche J2EE pour piloter une simulation sur le web. Mémoire de fin d'études pour l'obtention du diplôme d'ingénieur d'état en informatique, Département d'Informatique, Faculté des sciences, Université d'Oran< ; 2002.

[45] Rifidi. Site officiel de Rifidi. http://wiki.rifidi.org/index.php.

[46] Emulator User's Guide. http://wiki.rifidi.org/index.php/Emulator_User%27s_Guide. [47]Le protocole Telnet. Site officiel du protocole. http://www.telnet.org/

[48] Alien 9800. http://wiki.rifidi.org/index.php/Alien_9800.

[49] Honarkhah, M etCaers, J. Stochastic Simulation of Patterns Using Distance-Based Pattern Modeling, Mathematical Geosciences, 42: 487 – 517. 2010.

[50] D.E Zegour. Structures de Données et de Fichiers : Programmation Pascal et C. Edition Chihab. 1996.

[51] Johnson, N.L., Kotz, S. etBalakrishnan, N. Continuous Univariate Distributions, Volume 2, 2nd Edition. Wiley.ISBN 0-471-58494-0. 1995.

" Analysis and comparison of the potential of RFID-technology in European and

U.S. retail supply chains" , Stefan Hofmayr, Vienna University of Economics and Business Administration, 2005.

[52]" RFID: Cha nging the face of Supply Chain Management" , Manish Nikam&SagarSatpute, WELINGKAR Institute of Management development & research, 2005.

[53] " Integ rating the supply chain with RFID : a technica l and business analysis" , ZaheeruddinAsif&MunirMandviwalla, Fox School of Business and Management Temple University, 2005

[54] " Radio Frequency IDentification: Evaluation of the Technology Supporting, the Development of an Assets Tracking Application", Bachelor Thesis, Dominique Guinard, September 2005,