PROJET RFID

Projet de fin d'étude (option RSM)

Par

BACHOTI Youssef

BELHAJ SENDAGUE Bassim

RODRIGUES OLIVEIRA Joao Gabriel

Professeurs responsables : M. AFIFI Hossam, M. AUBRY Patrice

Le 25 janvier 2011

SOMMAIRE

REMERCIEMENTS

Tout d'abord nous tenons à remercier tout le staff de RSM pour leur collaboration avec nous pendant le projet spécialement Monsieur AFIFI Hossam et M. AUBRY Patrice.

Apres, nous remercions aussi tous les professeurs et chercheurs qui ont pu nous aider pendant la réalisation du projet, ainsi que tous les étudiants et doctorants.

Nous remercions aussi tous les gens du département réseau de l'école pour leur aide quand on avait besoin de matériel et logistique.

Un grand Merci

1. **INTRODUCTION :**

Le but de ce stage est de mettre en œuvre l'analyseur de spectre Agilent afin de détecter les numéros de badges TSP utilisés en RFID.

Le projet consiste donc à se familiariser à un appareil de mesures haut de gamme RF :

- mettre en place une procédure de reconnaissance de trames RFID's ;
- trouver la valeur transmise en RF.

Il faut donc pouvoir afficher les informations et données qui se transmettent entre le lecteur de badge et son badge.

Apprendre à utiliser les différents logiciels contenus dans l'analyseur du signal.

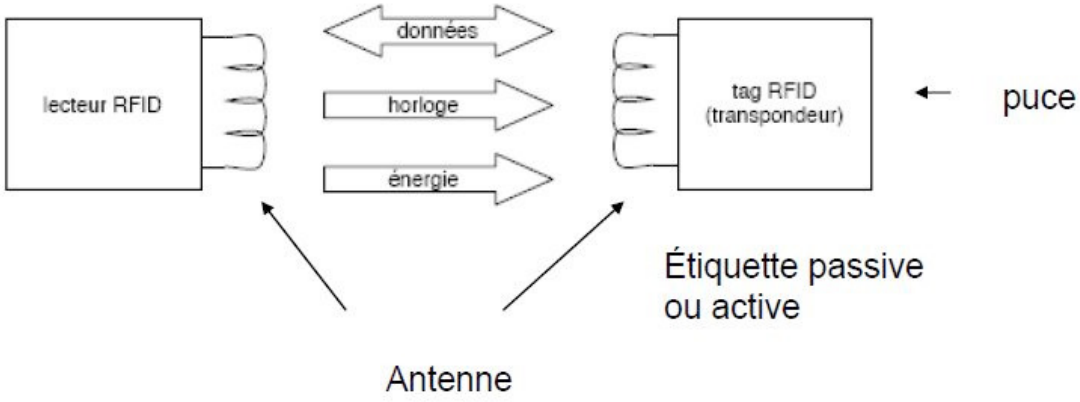
Puis effectuer des captures du *burst* des informations.

Après il faut enregistrer les données et essayer de les représenter pour pouvoir en tirer des informations utiles.

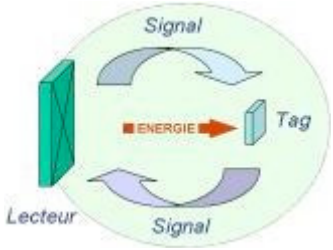
Et enfin trouver la valeur transmise c'est-à-dire le numéro transmis sous un codage prédéfini dans cette communication.

2. PRINCIPE FONDAMENTAL DE LA RFID

RFID fait partie des technologies d'identification automatique, au même titre que la reconnaissance optique de caractères ou de codes barre. Cette technologie permet d'identifier un objet ou une personne, d'en suivre le cheminement et d'en connaître les caractéristiques à distance grâce à une étiquette émettant des ondes radio, attachée ou incorporée à l'objet ou à la personne. La technologie RFID permet la lecture des étiquettes même sans ligne de vue directe et peut traverser de fines couches de matériaux (peinture, neige, etc.).



Source : Nicolas Seriot, IL–2005b, Yverdon-les-Bains



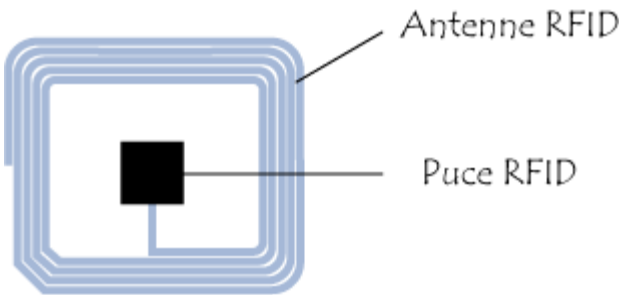
2.1. Composants et fonctionnement du système

Une solution complète de RFID comprend les étiquettes, les lecteurs et encodeurs et l'intergiciel (middleware). Ce dernier permet d'intégrer le flux des données dans le système d'information de l'entreprise.

2.1.1. Le tag (étiquette)

Une des méthodes d'identification les plus utilisées est d'abriter un numéro de série ou une suite de données dans une puce (chip) et de relier cette dernière à une petite antenne. Ce couple (puce silicium + antenne) est alors encapsulé dans un support (RFID Tag ou RFID

Label). Ces "tag" peuvent alors être incorporés dans des objets ou être collés sur des produits. Le tout est alors imprimé sur un support pliable, souvent adhésif. Le format des données inscrites sur les étiquettes est standardisé à l'initiative d'EPC Global (Electronic Product Code).



2.1.2. Le lecteur

Le lecteur/enregistreur est constitué d'un circuit qui émet une énergie électromagnétique à travers une antenne, et d'une électronique qui reçoit et décode les informations envoyées par le transpondeur et les envoie au dispositif de collecte des données. Non contents de lire les étiquettes RFID, il est à même d'écrire leur contenu. Le lecteur RFID est l'élément responsable de la lecture des étiquettes radiofréquence et de la transmission des informations qu'elles contiennent (code EPC ou autre, informations d'état, clé cryptographique…) vers le niveau suivant du système (middleware). Cette communication entre le lecteur et l'étiquette s'effectue en quatre temps :

1) Le lecteur transmet par radio l'énergie nécessaire à l'activation du tag ;

2) Il lance alors une requête interrogeant les étiquettes à proximité ;

3) Il écoute les réponses et élimine les doublons ou les collisions entre réponses ;

4) Enfin, il transmet les résultats obtenus aux applications concernées.

La communication entre le lecteur et l'étiquette s'effectue via les antennes qui équipent l'un et l'autre, ces éléments étant responsables du rayonnement radiofréquence. Les antennes dont dispose le lecteur sont plus ou moins standardisées, mais offrent les mêmes différences que les haut-parleurs d'une chaîne stéréo d'un modèle à l'autre. Pour continuer ce paradigme, la logique de la chaîne stéréo s'applique tout aussi bien ici puisque la lecture ne sera bonne que si l'antenne est de bonne facture. D'où l'importance de ce composant dans le choix de la solution. De même, si le lecteur s'avère de qualité insuffisante, le traitement des données en souffrira. Il y a donc là un équilibre à trouver entre ces deux composants. La puissance du lecteur est donc à combiner avec l'antenne adéquate, ceci permettant de déterminer la portée optimale de la lecture. Généralement, on distingue quatre modalités :

- Lecture de proximité : entre 10 et 25 cm ;
- Lecture de voisinage : jusqu'à 1 mètre ;

- Lecture à moyenne distance : de 1 à 9 mètres ;

- Lecture longue portée : jusqu'à plusieurs centaines de mètres.

Par ailleurs, le terme de lecteur RFID est en fait une impropriété, puisque ce dernier est également capable d'écrire des informations sur l'étiquette. Car, si bon nombre d'étiquettes sont en lecture seule (le code qu'elles contiennent ayant été « imprimé » en même temps que l'étiquette elle-même, d'autres contiennent, au-delà du code de base, une zone mémoire pouvant contenir des données variables.

Le premier concerne les basses fréquences (de 9 à 150 KHz; la fréquence la plus utilisée étant celle de 125 KHz) ainsi que les hautes fréquences (plus particulièrement la bande des 13,56 MHz), le second concernant les très hautes fréquences (de 300 à 1200 MHz). Signalons encore que certains fabricants se dédient à une bande particulière, tandis que d'autres « ratissent large ». Quoi qu'il en soit, pour des raisons de cohérence, nous laisserons de côté la bande basse fréquence, surtout utilisée pour le marquage du bétail et nous nous préoccuperons uniquement des bandes HF et UHF. Indépendamment de la fréquence, certaines caractéristiques sont communes à tous les types de contrôleurs. C'est tout d'abord la présence (ou non) d'une antenne interne, cette dernière étant surtout adoptée par les modèles de faible envergure lesquels ont une puissance et une portée plus limitée. En ce qui concerne les liaisons exploitant des antennes externes, les solutions sont extrêmement variées, les constructeurs ayant donné libre cours non pas à leur imagination mais aux développements résultant de leurs recherches. Généralement, on emploie les antennes circulaires lorsque l'orientation de lecture varie ainsi que dans les milieux soumis à de nombreuses réflexions du signal RF. Les antennes linéaires, quant à elles, sont utilisées lorsque les tags présentent toujours la même orientation. Il est également possible de relier les antennes à un multiplexeur, ce qui permet d'augmenter le nombre d'entre elles connectées à un contrôleur. Toutefois, certaines antennes peuvent perturber leurs voisines ou être perturbées par celles-ci. C'est pourquoi des fonctionnalités sont intégrées dans les contrôleurs pour pallier ce problème de collision. On dispose ainsi notamment d'un variateur de puissance qui corrige et ajuste la puissance des antennes et dans le cadre de la HF, d'un ASIC de couplage inductif donnant un peu plus d'intelligence au contrôleur. C'est d'ailleurs au niveau de cette intelligence que se fait toute la différence entre produits. Certains disposent en effet de fonctions middleware intégrées qui leur permettent d'expédier directement des données assimilables par l'ERP de l'entreprise. D'autres sont seulement programmables en langage machine, tandis que d'autres encore disposent d'un système d'exploitation dédié. Au niveau le plus bas, on peut opérer la classification suivante à propos de la lecture de l'étiquette :

- lecture seule : le lecteur prélève le code du tag émettant le signal le plus fort

- lecture multiple : le lecteur explore le champ de lecture pour prélever les codes de toutes les étiquettes en émission RF

En ce qui concerne en revanche le fonctionnement du lecteur:

- Autonome: le lecteur active le signal RF après avoir reçu une entrée ou une commande du logiciel ;
- Interactif : le lecteur lit lorsqu'il reçoit une requête d'une autre application à un autre niveau.

2.2. Les différents types de tags et leurs spécificités techniques

2.2.1. Tags actifs – tags passifs

Pour exploiter les informations contenues dans ces étiquettes, il faut impérativement disposer du lecteur approprié. Celui-ci émet des ondes radios en direction de la capsule ce qui permet de l'alimenter en énergie (alimentation par induction électromagnétique), en d'autres termes de l'activer (la puce renvoie alors des données), pour en extraire les informations qu'elle renferme. Ces puces ne sont pas capables d'effectuer des traitements dynamiques mais seulement de renvoyer des données statiques.

2.2.2. Tags passifs (sans batterie)

Ne disposant d'aucune alimentation externe, ils dépendent de l'effet électromagnétique de réception d'un signal émis par le lecteur. C'est ce courant qui leur permet d'alimenter leurs microcircuits. Ils sont peu coûteux à produire et sont généralement réservés à des productions en volume. Ce sont eux que l'on trouve plus particulièrement dans la logistique et le transport. Ils utilisent différentes bandes de fréquences radio selon leur capacité à transmettre à distance plus ou moins importante et au travers de substances différentes (air, eau, métal). La distance de lecture est inférieure à un mètre. Les basses et hautes fréquences sont normalisées au niveau mondial. Ces puces sont collées sur les produits pour un suivi allant jusqu'aux inventaires. Elles sont jetables ou réutilisables suivant les cas. Les puces avec une antenne de type "papillon" ont une portée courante de 1 à 6 mètres (images 3, 5, 6 et 7). Ces puces UHF (Ultra Haute Fréquence) sont utilisées pour la traçabilité des palettes dans les entrepôts. Par contre, la tolérance aux obstacles est moyenne. Pour les très hautes fréquences (UHF), l'Europe, l'Asie et les Etats-Unis se distinguent par des fréquences et des réglementations différentes

2.2.3. Tags semi-passifs

Ces tags sont similaires aux cartes d'identification passive. Ils emploient des technologies proches, mais avec quelques différences importantes. Ils disposent en effet eux aussi d'une petite batterie qui fonctionne en permanence, ce qui libère l'antenne pour d'autres tâches, dont 9 notamment la réception de signaux de retour. Ces tags sont plus robustes et plus rapides en lecture et en transmission que les tags passifs, mais ils sont aussi plus chers.

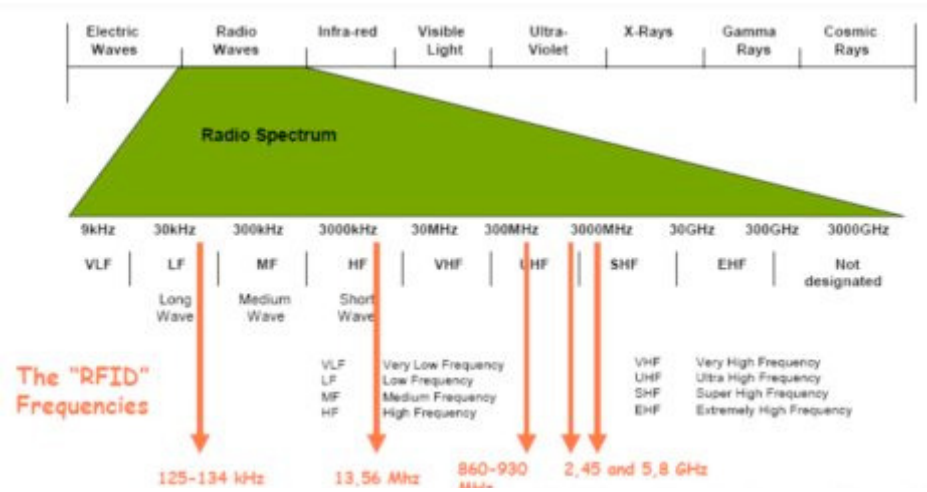
2.2.4. Tags actifs

Les étiquettes actives sont les plus chères car elles sont plus complexes à produire et assurent, outre des fonctions de transmission, des fonctions soit de captage soit de traitement de l'information captée, soit les deux. De ce fait, elles ont besoin d'une alimentation embarquée et sont donc caractérisées par la durée de vie de celle-ci. Si le prix est un facteur discriminatif, il faut savoir que ces étiquettes s 'avèrent particulièrement bien adaptées à certaines fonctions, dont notamment la création de systèmes d'authentification, de sécurisation, d'antivol, etc. Bref, elles sont idéales pour tout ce qui concerne le déclenchement d'une alerte ou d'une alarme. Elles peuvent émettent à plusieurs centaines de mètres. Le dernier cri est le tag «insensible à l'orientation du produit».

2.3. <u>Les fréquences d'utilisation</u>

Les systèmes RFID génèrent et réfléchissent des ondes électromagnétiques. Les systèmes RFID doivent notamment veiller à ne pas perturber le fonctionnement des autres systèmes radio. On ne peut, en principe, utiliser que les plages de fréquences spécifiquement réservées aux applications industrielles, scientifiques ou médicales. Ces plages de fréquences sont appelées ISM (Industriel – Scientifique – Médical). Les principales plages de fréquences utilisées par les systèmes RFID sont les basses fréquences (125 et 134.5 kHz) et les fréquences ISM : 6.78 MHz, 13.56 MHz, 27.125 MHz, 40.68 MHz, 433.92 MHz, 869.0 MHz, 915.0 MHz (pas en Europe), 2.45 GHz, 5.8 GHz et 24.125 GHz. La plage de fréquences la plus utilisée est de loin 13.56 MHz (haute fréquence).

LA GAMME DES FREQUENCES



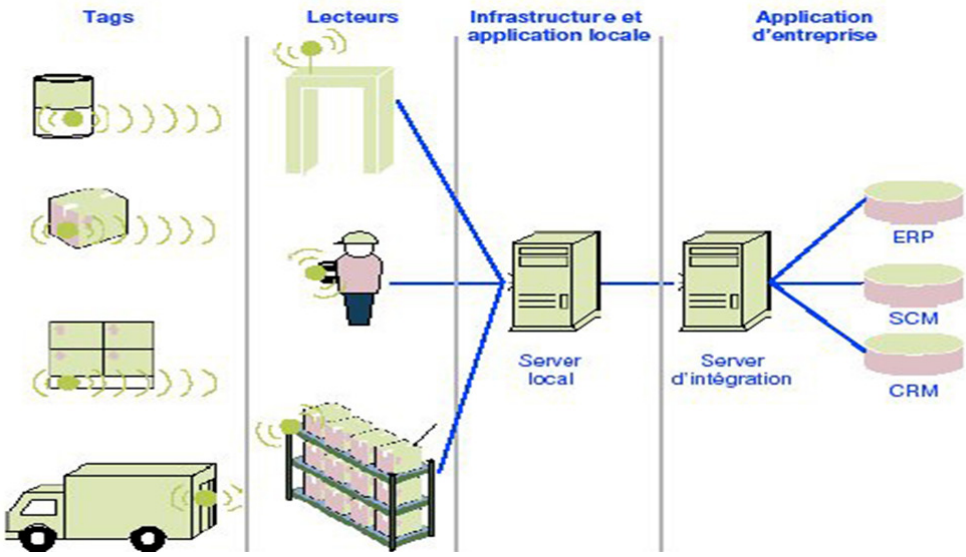
2.4. Application

Les applications RFID s'appuient sur différents standards dépendant des fonctionnalités exigées par les processus métier et par certaines contraintes locales. La RFID permet de répondre à un grand nombre de besoins. Elle se développe bien en intra entreprise et dans la logistique. Les principales difficultés auxquelles le standard RFID doit faire face sont en voie d'être surmontées : coût de l'étiquette (plus de 0,10€ pour les moins chères), gestion de l'anticollision en cas de lecture de nombreuses étiquettes en simultané, lecture au travers des fluides, adoption ou convergence trop lente de certains standards, remise en cause de processus anciens, problèmes de sécurité et d'éthique.

2.4.1. L'application aux entreprises

Les applications des étiquettes RFID sont déjà très nombreuses, il s'agit simplement ici de donner quelques exemples des possibilités offertes par cette technologie.

La gestion de la chaîne d'approvisionnement en matière logistique, quatre niveaux d'applications peuvent être distingués:



2.4.1.1. Expédition

L'étiquette peut faciliter le picking des produits, la constitution des palettes, leurs tris par destination, le contrôle du chargement. L'étiquette peut contenir, outre l'identification du produit, ou du contenu d'une palette, celle du numéro de lot de fabrication, l'identification du destinataire, le numéro de commande, des particularités de manutention, etc. Ces informations collectées au moment du chargement peuvent être stockées dans l'étiquette RFID du conteneur ou du moyen de transport afin de faciliter les contrôles en cours de transit, douane.

2.4.1.2. Réception

Les données pourront automatiquement être collectées pour effectuer les contrôles et mettre à jour les stocks et effectuer les rapprochements avec documents commerciaux ou les messages EDI.

2.4.1.3. En transit

L'étiquette permet de tracer les produits à chaque point de chargement et de déchargement ou simplement de passage. Ainsi l'expéditeur peut être à tout moment informé du déroulement du transport.

2.4.1.4. Local

Les étiquettes permettent les inventaires de produit, mais aussi la gestion des supports de manutention et des équipements (bouteilles de gaz...). La collecte des déchets Aussi bien en Europe qu'au Japon et aux Etats Unis les sociétés de collecte de déchets ménagers ou industriels, se préoccupent d'améliorer la répartition de la charge du ramassage et du traitement des ordures. Le principe est d'équiper chaque poubelle ou container d'une étiquette RFID, et les camions de collecte de lecteurs et de système de pesage, afin qu'à chaque opération puisse être automatiquement identifié le « producteur » et mesurer le poids des matières collectées. Le péage automatique de nombreuses sociétés de gestion d'autoroute à péage ont déjà mis en place des systèmes d'abonnement basé sur des étiquettes RFID, hyperfréquence, placées dans les véhicules. Les abonnés bénéficient ainsi de voie particulière de passage aux barrières de péage. Le paiement s'effectue sans arrêt du véhicule, par simple lecture de son identification.

Le contrôle d'accès Les étiquettes RFID sont déjà utilisées pour le contrôle d'accès des immeubles ou des parkings. Certaines stations-services américaines expérimentent, la délivrance automatique de carburant au propriétaire de véhicule muni d'une étiquette RFID à 2,45 GHz qui leur permet d'être identifié leur du stationnement devant les pompes. Des applications de plus en nombreuses de traçabilité des animaux se développent, que ce soit les étiquettes auriculaires sur les animaux d'élevage ou les étiquettes sous cutanées pour les chevaux ou les animaux domestiques. Dans tous les cas, il s'agit d'assurer une traçabilité des animaux dans un but de contrôle sanitaire ou de la qualité des cheptels. La gestion de la traçabilité des bouteilles de gaz pour des raisons de sécurité est très strictement réglementée. Des entreprises, comme l'Air Liquide, utilisent des étiquettes RFID pour tracer la vie des bouteilles de gaz. Il s'agit essentiellement d'en assurer la gestion des stocks et de

la distribution, et les opérations de maintenance obligatoires. Dans cette application, il faut noter que la composition métallique des bouteilles a été surmontée en isolant les étiquettes de la bouteille. Pour le nettoyage des vêtements de travail, des entreprises mettent en place des systèmes d'identification des uniformes basé sur une étiquette RFID d'un diamètre de 20 mm et d'une épaisseur de 2,5 mm, la fréquence 13,56 MHz en lecture / écriture à 20 cm. Ces étiquettes sont fixées au vêtement, elles résistent aux opérations de lavage. Elles permettent un suivi des opérations de lavage et une identification aisée du porteur de l'uniforme. Quelques applications originales et parfois controversées: le suivi des écoliers au Japon grâce à des étiquettes placées sur les cartables ou vêtements ; l'implantation d'étiquettes directement sous la peau de militaires au Mexique ; etc.

2.5. Avantages et inconvénients

2.5.1. Avantages

La capacité de mise à jour du contenu par les intervenants A la différence du code à barres pour lequel les données sont figées une fois imprimée ou marquée, le contenu des données stockées dans une étiquette radio fréquence va pouvoir être modifié, augmenté ou diminué par les intervenants autorisés (étiquettes en lecture et écriture multiple).

2.5.1.1. Une plus grande capacité de contenu

Dans une étiquette radiofréquence une capacité de 1000 caractères est aisément stockable sur 1mm2, et peut atteindre sans difficulté particulière 10000 caractères. Dans une étiquette logistique apposée sur une palette, les différentes unités contenues et leurs quantités respectives pourront être enregistrées et lues.

2.5.1.2. La vitesse de marquage

Le code à barres dans un contexte logistique nécessite le plus souvent l'impression d'un support papier. La manipulation et la pose des étiquettes restent des opérations manuelles ou mécaniques. Les étiquettes radio fréquence peuvent être inclues dans le support de manutention ou dans les conditionnements dès l'origine. Les données concernant les objets contenues ou transportées sont écrites en une fraction de seconde au moment de la constitution de l'unité logistique ou de transport, sans manipulation supplémentaire.

2.5.1.3. Une sécurité d'accès au contenu

Comme tout support numérique, l'étiquette radio fréquence peut être protégée par mot de passe en écriture ou en lecture. Les données peuvent être chiffrées. Dans une même étiquette, une partie de l'information peut être en accès libre, et l'autre protégée. Cette faculté fait de l'étiquette RF, un outil adaptée à la lutte contre le vol et la contrefaçon.

2.5.1.4. Une plus grande durée de vie

Dans les applications où un même objet peut être utilisé plusieurs fois, comme l'identification des supports de manutention, ou la consignation du contenant, une étiquette radio fréquence peut être réutilisée 1 000 000 de fois.

2.5.1.5. Une plus grande souplesse de positionnement

Avec l'étiquette radio fréquence, il est possible de s'abstraire des contraintes liées à la lecture optique, elle n'a pas besoin d'être vue. Il lui suffit d'entrer dans le champ du lecteur pour que sa présence soit détectée.

2.5.1.6. Une moindre sensibilité aux conditions environnementales

Les étiquettes RFID n'ont pas besoin d'être positionnées à l'extérieur de l'objet à identifier. Elles peuvent donc être mieux protégées des agressions liées aux stockages, aux manutentions ou au transport. De plus leur principe de fonctionnement ne les rend pas sensibles aux souillures, ou taches diverses qui nuisent à l'utilisation du code à barres.

2.5.2. Inconvénients

2.5.2.1. Le coût Les prix restent nettement supérieurs à ceux des étiquettes code à barres pour des unités consommateurs.

Utiliser les étiquettes radio fréquence en lieu et place du code à barres sur les produits de grande consommation, n'est donc pas aujourd'hui économiquement réaliste. Cela le devient pour lutter contre le vol ou la contrefaçon sur les produits à forte valeur ajoutée, ou pour tracer les produits dans le cadre du service après-vente, comme l'électroménager ou la hi-fi. Par contre au-delà du conditionnement unitaire, le coût de l'étiquette radio fréquence peut devenir marginal par rapport à la valeur des produits contenus. C'est pourquoi dans le domaine des produits de grande consommation, les premières applications de ces étiquettes peuvent voir le jour sur les cartons, sur les palettes et sur les unités de transport. Par ailleurs, si la comparaison se fait au niveau du système d'identification et de traçage, il faut prendre en compte les coûts lecteurs, favorables à la RFID, ainsi que le gain de temps venant de la non obligation de manipuler les objets pour présenter le code à barres devant le lecteur.

2.5.2.2. La perturbation par l'environnement physique

La lecture des étiquettes radio fréquences est perturbée par la présence, par exemple, de métaux dans leur environnement immédiat. Des solutions doivent être étudiées au cas par cas pour minimiser ces perturbations, comme cela a été fait par exemple pour l'identification des bouteilles de gaz.

2.5.2.3. Les perturbations induites par les étiquettes entre elles

Dans de nombreuses applications, plusieurs étiquettes radio fréquences peuvent se présenter en même temps dans le champ du lecteur volontairement ou involontairement. Ceci peut être voulu en magasin, au moment du passage à la caisse ou entre les portiques antivol.

2.5.2.4. La sensibilité aux ondes électromagnétiques parasites

Les systèmes de lecture RFID sont dans certaines circonstances sensibles aux ondes électromagnétiques parasites émises par des équipements informatiques (des écrans d'ordinateurs) ou des systèmes d'éclairages plus généralement par les équipements électriques. Leur emploi doit donc être testé en tenant compte de l'environnement.

2.5.2.5. Les interrogations sur l'impact de la radio fréquence sur la santé

Cette question fait débat depuis quelques années, en particulier concernant les portiques antivol et les téléphones portables. Les étiquettes passives ne présentent aucun risque quel que soit leur nombre puisqu'elles ne sont actives que lorsqu'elles se trouvent dans le champ d'un lecteur. Les études portent donc essentiellement sur les lecteurs et visent à définir les critères de régulation de leur puissance d'émission afin d'éviter qu'ils ne créent des perturbations sur les équipements de santé tels que les pacemakers, mais aussi sur l'organisme humain.

3. LE CONTENU DU PROJET

Afin de intercepter les données échangés entre les badges TSP et les lecteurs de cartes RFID de la marque HID, on a utilisé en résumé trois composants :

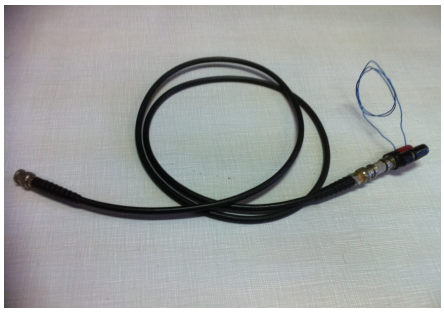
1. Un câble coaxial ;
2. Le *N9010A EXA Signal Analyzer* ;
3. Les systèmes de control d'accès HID.

Ensuite, nous décrivons chacun des trois éléments mentionnés ci-dessus.

3.1. Le câble coaxial

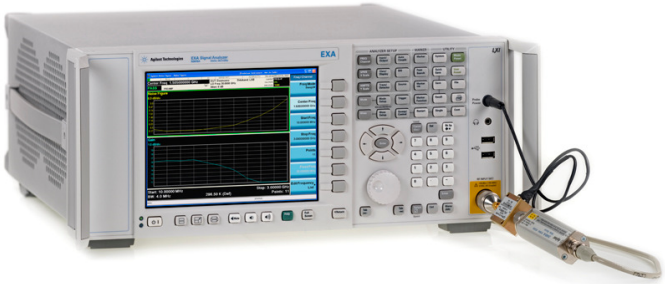
Un câble coaxial avec deux différentes configurations aux extrémités a été utilisé pour simuler une petite antenne capable d'intercepter la communication entre le badge et le lecteur.

Une extrémité du câble était attachée à l'analyseur de spectre en utilisant des adaptateurs. L'autre extrémité avec un petit fil enroulé, simulant une bobine, était placée entre le lecteur et le badge pour saisir la variation du champ magnétique dans la région d'échange d'informations RFID.



3.2. Le N9010A EXA Signal Analyzer

Après avoir connecté le câble à l'analyseur de spectre, nous avons commencé à analyser les données interceptés.



Sur le N9010A EXA Signal Analyzer est possible de trouver trois logiciels différents d'analyse des signaux installés:

1. *Spectrum Analyzer* ;
2. *VXA Vector Signal Analyzer* ;
3. *89600 Vector Signal Analyzer*.

Ensuite, nous décrivons chacun des trois logiciels mentionnés et leurs caractéristiques.

3.2.1. Spectrum Analyzer

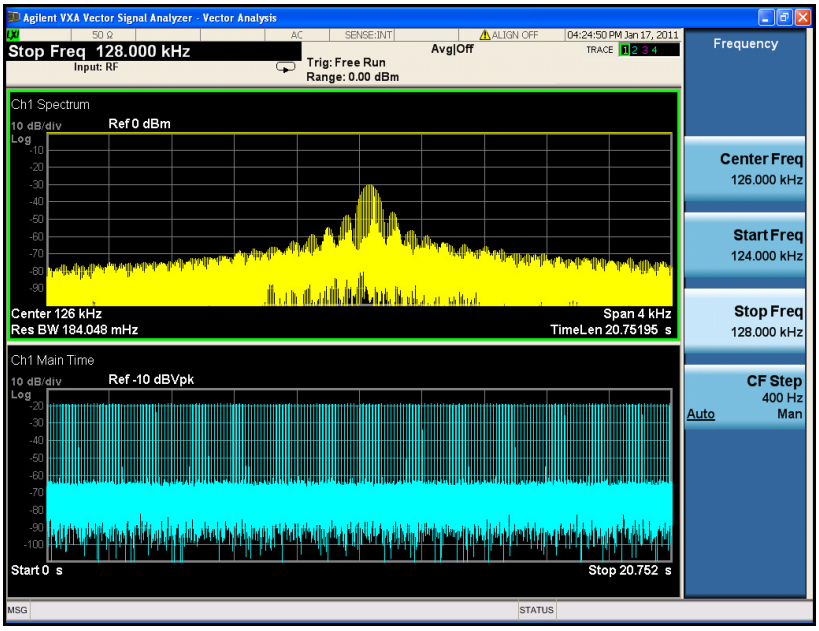
Logiciel plus basique installé sur l'analyseur utilisé dans ce projet pour trouver la fréquence de travail du système de contrôle d'accès HID.

Pour trouver cette fréquence, au début, on a utilisé une fenêtre de 0 Hz jusqu'à 1 GHz, parce que nous savions déjà que ce système fonctionne à basse fréquence. Ensuite, nous avons remarqué une petite impulsion dans la région proche à 125 KHz, on a ajusté la fenêtre spectrale à un intervalle entre 120 KHz et 130 KHz.

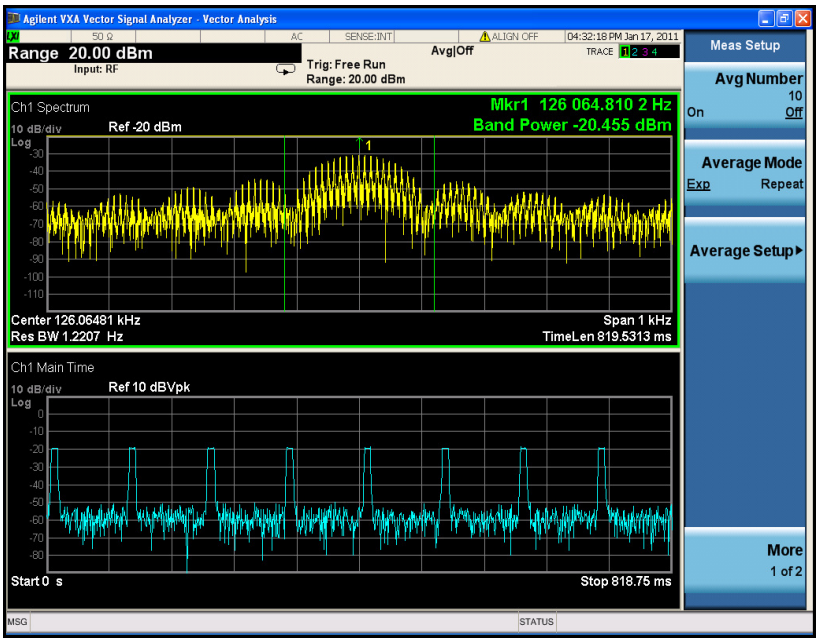
Après savoir l'intervalle de fréquence, on a utilisé la fonction de *Trigger Level* fixée à -15 dBm pour capturer l'image et remarquer et qui permettent de remarquer parfaitement la fréquence de travaille à 126 KHz..

3.2.2. VXA Vector Signal Analyzer

Après avoir trouvé la fréquence on a utilisé le *VXA Vector Signal Analyzer* pour voir ce qui se passe dans le domaine du temps et aussi mieux regarder la bande de fréquence utilisée.



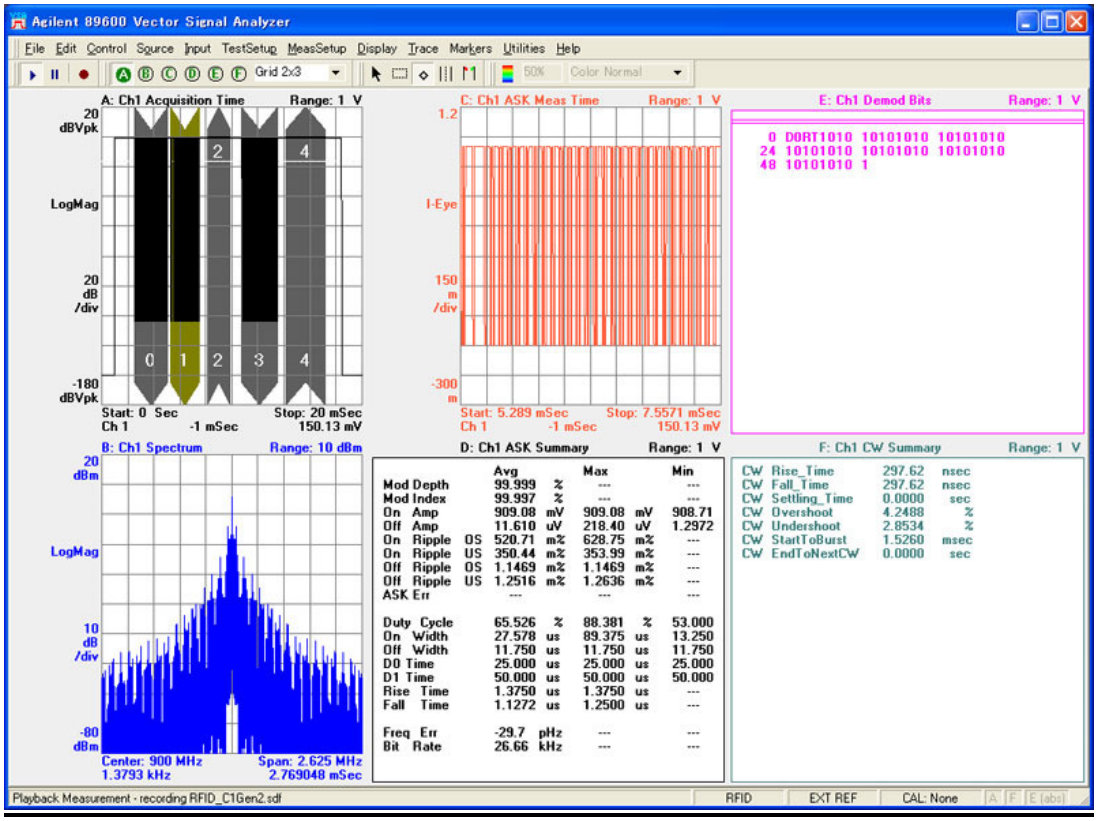
Une fois que la fréquence a été centralisé à 126 KHz, c'été possible d'observer un signal de duration ≈ 10 ms et période ≈ 100 ms dans le domaine temporel.



3.2.3. 89600 Vector Signal Analyzer

Le *89600 Vector Signal Analyzer* est le logiciel installé plus complet. Ce logiciel est capable de gérer jusqu'à six fenêtres différentes au même temps avec plusieurs informations différentes d'un même signal.

Ci-dessous est un exemple de cas idéal où la modulation du signal est connue, ASK, et nous avons une analyse simultanée de six fenêtres avec des informations différentes:



A : Le *burst* capturé ;

B : Le spectre de fréquence ;

C : Le signal dans le domaine temporel ;

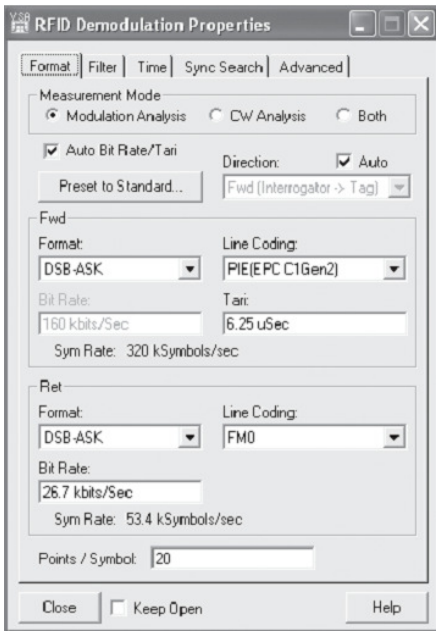
D : valeurs minimales, maximales et moyennes de certaines caractéristiques du signal;

E : Des bits après la démodulation ;

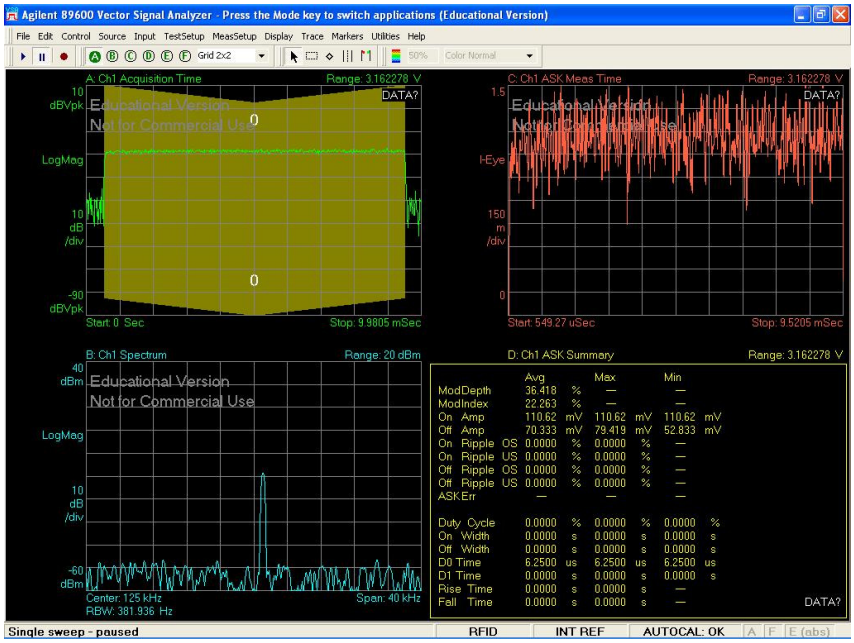
F : D'autres valeurs temporelles du signal.

Ce logiciel nous permet de faire trois différents types de démodulations : analogiques, numériques et RFID.

Après avoir sélectionné le type de démodulation RFID, vous pouvez définir tous les paramètres nécessaires indiquant comment le signal RFID d'activation et réponse du badge ont été modulées.



Comme le grand problème de ce projet était l'information sur le type de modulation appliquée aux signaux de communication du système de contrôle d'accès HID, il n'été pas possible de configurer correctement le démodulateur, et donc c'été impossible de capturer les données contenues dans le badge TSP.



L'image ci-dessus montre seulement des informations de temps et de fréquence qui ont déjà obtenu précédemment avec les autres deux logiciels. Elle ne montre pas des informations sur les données démodulées, car nous n'avons pas pu configurer correctement le démodulateur.

3.3. Le système de control d’accès HID

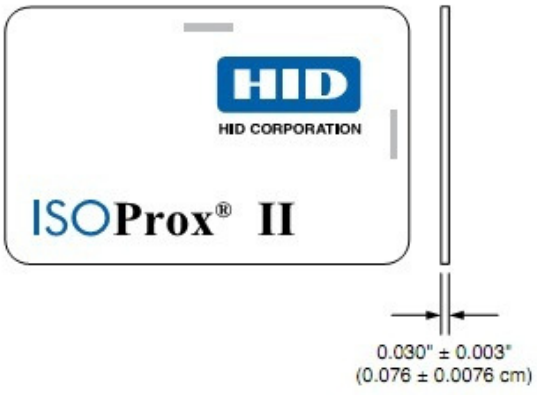
Tout système de contrôle d'accès se compose de quatre éléments de base. Selon la taille et le but du système, il peut avoir autres dispositifs, mais les quatre principaux sont:

1. Les cartes d’accès
2. Les lecteurs (peut-être équipé de claviers)
3. Panneaux de contrôle d'accès (contrôleurs)
4. Une interface opérateur ou "Host" PC

Afin de déterminer leurs fonctionnes et leur place dans le système de contrôle d'accès, on y va regarder individuellement les quatre éléments.

3.3.1. Les cartes d’accès

Toutes les cartes d'accès contient simplement un ensemble de nombres binaires (zéros et de uns) qui sont utilisés pour identifier le détenteur.



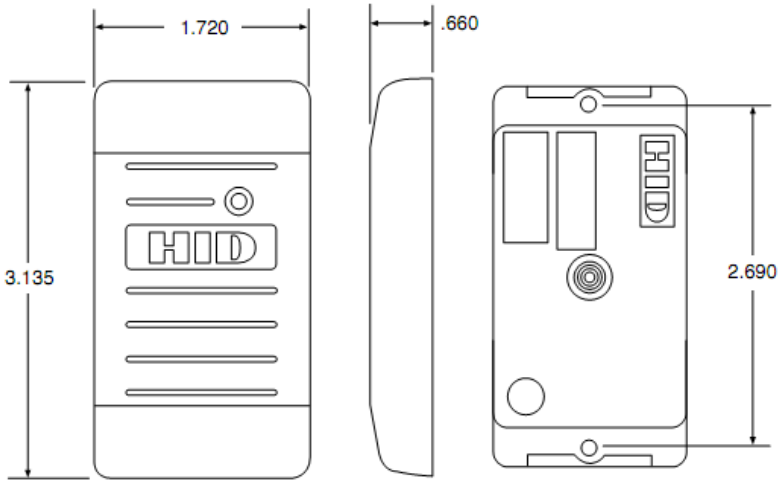
La plupart des cartes faites par HID combinent deux ou plusieurs technologies différentes en une seule carte. Les badges TSP sont tags passifs et combinent la technologie RFID avec un système de détection de proximité, de façon à économiser de l'énergie, parce que le lecteur va envoyer des commandes de lecture seulement si la carte est détectée comme près.

Le sens des données stockées sur la carte et comment sont transmises au lecteur varient selon la technologie utilisée. Mais de toute façon, les données de la carte sont numéros binaires avec une taille et configuration fixes. Ces données sont composées d'un "format" qui sera reçu par le contrôleur.

La carte n'est pas conscient de la composition de ses données, ni de tous les privilèges d'accès du titulaire de la carte. Cette information existe seulement au niveau du contrôleur et, éventuellement, du host.

3.3.2. Les lecteurs

Les lecteurs HID sont compatibles avec différents types de cartes, mais chaque lecteur peut seulement se communiquer avec leur type de carte correspondant, parce que les technologies sont uniques.



Les lecteurs plus utilisés dans les systèmes d'accès de la TSP sont les modèles ProxPoint Plus, et sont caractérisés par avoir des options de configuration variées. Ce modèle est capable de convertir les données binaires du badge au protocole *Wiegand* et après les envoyer sans modifications au contrôleur.

Comme les cartes d'accès, les lecteurs n'ont pas conscient de la composition des données, ni de tous les privilèges d'accès du titulaire de la carte.

3.3.3. The Access Control Panel (Controller)

Quand le contrôleur reçoit les données du lecteur, son logiciel les analyse et décide ou non d'accorder l'accès. Ceci est fait en plusieurs étapes.

- ✓ *Est-ce que la longueur des données correspond à ce que le contrôleur attend ?*

Certains contrôleurs ont été conçus de façon à n'accepter qu'une certaine longueur de données (34 bits par exemple). Si la taille des données de la carte est trop longue ou trop petit, le contrôleur peut complètement les ignorer. D'autres contrôleurs peuvent avoir un signal spécifique de type 'accès refusé' pour une taille de données qui ne correspondrait pas.

- ✓ *Est-ce que la structure des données a du sens pour le contrôleur ?*

Si la longueur est acceptable, le contrôleur décompose la trame. Ceci inclut :

- Code d'Installation
- Code du site
- Numéro de la carte

✓ *Est-ce que le code d'équipement correspond ?*

Le contrôleur analyse les données et détermine si le code d'installation correspond avec celui programmé dans le contrôleur. Certains contrôleurs peuvent supportés plusieurs Code d'Installation, voire sous plusieurs. Si le Code d'Installation ne correspond pas, l'accès sera refuse et un fichier de registre sera généré

✓ *Est-ce que le Code du Site correspond ?*

Si le format contient un Code de Site ou un autre identifiant secondaire, il sera analysé comme le Code d'Installation.

✓ *Est-ce que le Numéro de Carte est contenu dans la chaine appropriée ?*

Si oui, le processus de décision continue. Sinon, l'accès sera refusé et un fichier de registre sera généré.

✓ *Est-ce que le Numéro de Carte est mémorisé ?*

Si oui, le processus continue. Sinon, l'accès est refusé, un message 'carte inconnue' est enregistré dans le fichier registre.

✓ *Est-ce que la carte est encore valable ?*

Si oui, l'accès est autorisé, et le relais de verrouillage activé. Sinon, un message du motif du refus sera affiché.

Le contrôleur est le seul dispositif dans le système où le contenu de la carte peut être décodé et donc prendre des décisions. Seul le contrôleur (éventuellement l'hôte), sait si le contenu est falsifié ou si les données reçues ont du sens. Différentes marques de contrôleurs 'réagissent 'différemment à des formats de données incorrectes. Certains ont un message d'erreur pour tout type d''accès refusé', d'autres ont simplement un message 'accès refusé ' pour tout. Enfin, d'autres ignoreront complètement une carte avec un format de données incorrectes.

3.3.4. User Interface (Host software)

Chaque système de contrôle d'accès est relié à un terminal (PC ou autre) pour :

- Ajouter ou supprimer un titulaire de carte
- Changer les privilèges d'accès
- Créer ou modifier un planning en fonction de vacances par exemple
- Configurer le système pour des points d'alarme, des portes…
- Contrôler les événements systèmes en temps réel
- Générer un rapport de tous les événements

Dans certains cas exceptionnels, dans le cas de systèmes très grands et complexes, l'hôte est autorisé à décider. Mais dans la majeure partie des cas, c'est le contrôleur qui décide.

3.4. L'interface *Wiegand*

Dans le format *Wiegand*, les ID CARD sont programmés avec un format spécifique des bits. Le lecteur capture les données après de vérifier les codes utilisateurs et généralement il envoie le même format de bit au contrôleur.

Le format WIEGAND de 26 bits se compose de deux bits de parité et 24 bits de données. Le premier bit transmis P1 représente la parité paire calculé sur les 12 premiers bits de code. Le dernier bit transmis P2 représente la parité impaire calculé sur les 12 derniers.

Code Format

									1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2
1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6
P1	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	P2

Parity Format

									1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2
1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6
P1	E	E	E	E	E	E	E	E	E	E	E	E													
													O	O	O	O	O	O	O	O	O	O	O	O	P2

- P1: First, or even parity bit
- C: Code bits
- P2: Second, or odd parity bit
- E: Bits for calculation of even parity
- O: Bits for calculation of odd parity

Data format within the 24 code bits which includes the portioning of the bit, the designation of the *Most Significant Bit (MSB)* or the *Least Significant Bit (LSB)* shall be subject to definition by the panel and reader manufacturers and may remain proprietary.

Dans l'exemple suivant, on montre la sortie du lecteur qui est envoyé au contrôleur. Dans ce cas-là, l'ID card est '816' en décimal :

sentinel parity parity

customer code 10 zeros bit even facility code card number odd

[0 0 0 0 0 0 1] [0 0 0 0 0 0 0 0 0 0] [1] [0] [0 1 1 0 0 1 0 1] [0 0 0 0 0 0 1 1 0 0 1 1 0 0 0 0] [1]

| 0 | 2 | 0 | 0 | 4 | C | A | 0 | 6 | 6 | 1

Wiegand Output |0 | C | A | 0 | 6 | 6 | 1

Hex code numbers [6 | 5][0 | 3 | 3 | 0]

Decimal conversion [101][0816]

4. LA STANDARDISATION

L'absence de standardisation réelle dans le domaine des RFID est un obstacle à son développement. On a mentionné plus haut les problèmes inextricables que pose l'harmonisation de l'allocation des fréquences au niveau international. Mais un système RFID ne résume pas au choix d'une onde porteuse. Il faut évidemment, pour que les équipements soient interopérables entre eux, convenir d'une codification des objets, des données à échanger, des protocoles, des interfaces techniques etc.

La tâche est considérable et rappelle, en plus complexe, les efforts menés dans les années 1980/90 pour standardiser les bus de terrain. Certains doutent que, dans un domaine rapidement évolutif sur le plan technologique, où la confidentialité sur les stratégies et les progrès de chacun reste essentielle, la standardisation soit possible ni même souhaitable au stade actuel. Il ne faut donc pas s'étonner de ne trouver aujourd'hui que des éléments de standardisation.

L'analyse des différents chantiers en cours mériterait un article à lui seul. On se contentera ici de donner quelques indications.

Certaines normes particulières existent depuis plusieurs années ou sont en projet. C'est le cas des normes applicables aux cartes à puce de proximité (ISO 10536, 14443, 14693, 10373), des normes applicables à l'identification du bétail (ISO 11784,11785 et 14223), à la logistique (projets de normes ISO 17363 à 17367) et à l'identification des containers (ISO 10374).

Sur le plan général, l'ISO et l'IEC ont mis en place un comité technique commun, l'ISO/IEC/JTC1, qui s'est lui-même scindé en deux sous-comités, selon qu'il s'agit de la traçabilité des personnes ou des objets. Des groupes de travail spécialisés ont été constitués et des rapports techniques sont disponibles.

Afin de progresser dans la voie de l'interopérabilité, l'ISO et l'IEC ont publié les normes ISO/IEC 18000 définissant les règles à respecter par les étiquettes destinées aux objets dans les principales gammes de fréquence.

5. LE MARCHE DE LA RFID A L'HORIZON 2015 :

Après plus de 20 ans de balbutiement, la RFID, technique d'identification par radiofréquence, a enfin décollé au niveau mondial, mais aussi en France. Cette percée s'explique en grande partie par le déverrouillage du très prometteur segment de l'ultra haute fréquence (UHF) fin 2004. Le chiffre d'affaires mondial de la vente de composants et la prestation de services liés à la RFID, a ainsi bondi de près 40% par an depuis 2005.

Malgré un léger retard au démarrage, le marché français s'inscrit lui aussi dans cette tendance, même s'il n'a pas été épargné par la crise en 2009. Le développement de la RFID en France peut en effet s'appuyer sur de solides fondamentaux structurels. Les experts ont ainsi décrypté les grands moteurs qui porteront le marché dans les années à venir, notamment:

- les avancées technologiques et l'émulation de la recherche fondamentale et appliquée en amont qui conduisent les industriels des composants RFID à une réactivité maximale en matière d'innovation.

- la recherche permanente de qualité et de compétitivité de la part des entreprises, résultante d'une concurrence toujours plus âpre et des flux plus complexes. Dans ce contexte, la RFID constitue un levier indéniable de création de valeur tout au long de la chaîne logistique.

- des préoccupations sécuritaires grandissantes, reflets de la volonté des pouvoirs publics et des industriels de lutter contre la falsification, la contrefaçon, le vol mais aussi de garantir la sécurité des citoyens face au terrorisme et aux crises alimentaires et sanitaires, etc. Dans ces cas précis, l'identification par radiofréquence représente une solution idéale en matière de traçabilité.

- des enjeux marketing majeurs face à un consommateur de plus en plus volatil et désireux de toujours plus d'informations dans des délais plus courts. Dès lors, la RFID peut s'imposer comme un outil marketing puissant de conquête et de fidélisation du client.

Combinées au degré actuel d'utilisation et de structuration des applications par les entreprises, ces tendances de fond permettront de doubler la taille du marché mondial de la RFID à l'horizon 2015 et ainsi la porter à plus de 13 milliards de dollars. En France, la croissance du marché sera également extrêmement vigoureuse : les experts estiment ainsi que le chiffre d'affaires de la RFID dans l'Hexagone progressera de 10% au par an au cours des cinq prochaines années.

Toutefois, le développement à très grande échelle de la RFID devrait encore prendre du temps en France, comme dans le reste du monde. En effet, plusieurs éléments sont susceptibles de ralentir l'expansion du marché à moyen terme, notamment des verrous technologiques latents et des freins éthiques et psychologiques, compte tenu de la perception de cette technologie par la population et les entrepreneurs. Mais le principal écueil reste les entraves économiques, liées au coût global de déploiement de cette technologie et à l'épineuse

question du retour sur investissement. De plus, et malgré les efforts de l'ensemble des acteurs pour structurer le secteur, l'offre RFID apparaît toujours très fragmentée. Or, son caractère diffus décourage nombre d'utilisateurs potentiels, dont les attentes ont par ailleurs mûri pour se cristalliser sur des applicatifs packages, configurables et faciles à déployer.

Enfin, comme le montre l'analyse concurrentielle des experts en la matière, rares sont les opérateurs qui maîtrisent en interne l'intégralité de la chaîne de valeur, principal facteur clé de succès dans ce marché.

Au final, l'évangélisation du marché et l'adoption plus massive de la technologie RFID dépendent de la capacité des offreurs à proposer une promesse de valeur claire et facilement identifiable par leurs clients. Conscients de cet enjeu, les leaders se mettent en ordre de bataille, adoptant des stratégies plus offensives.

On constate donc que, la crise économique a quelque peu freiné le déploiement des RFID mais que la France, est prête aujourd'hui pour accueillir cette technologie et de l'utiliser dans le bon sens.

6. LES DIFFICULTES RENCONTREES LORS DE LA REALISATION DU PROJET

6.1. Matériels

Du a des problèmes de matériel, on a fait fasse a plusieurs problème qui on plusieurs fois stopper le développement du sujet traité :

Premièrement, plusieurs des instruments utilisés étaient pas compatible entre eux, et a chaque fois on vérifiait l'un d'entre eux pour qu'à la fin on découvre après beaucoup d'heures passées là-dessus que les deux instruments ne marchent pas ensemble, et donc pour avoir des résultats dans ce que nous faisions nous avons du improviser, chercher des alternatives pour réussir ce que nous faisions.

Nous avons eu le droit tout d'abord à un problème relié à la puissance d'émission des antennes que nous devions utiliser.

Vu que les fréquences de lecture du badge est fortement faible {125 KHz} après beaucoup d'essaies, on a opté pour un gadget créé par un groupe de l'année dernière qui travaillait sur un projet un peu similaire ou confronté au même problème ils ont créé une antenne manuel ou plutôt un circuit fermé d 'une boucle d'un côté pour et d'une entrée pour être lu sur l'analyseur du signal.

On a ensuite rencontré des problèmes sur le lecteur de badge qui ne pouvaient marcher à 125 KHz fréquence sur laquelle marche le badge. Pour pouvoir réussir notre prise de la fréquence, on a travaillé dans les couloirs du bâtiment B avec notre matériel dans un petit chariot. Ce fut gratifiant de voir que pour une fois, nous pouvions voir ce qui se passe grâce aux graphes sur l'analyseur du signal.

Aussi, nous avons eu un mal fou avec l'appareil qui, n'avait plus de guide d'utilisateur, et qui, était très difficile à utiliser surtout pour enregistrer les informations convenable, et pour montrer les données qui nous intéresse, on a fini par trouvé quelques moyens pour trouver les résultats qu'on voulait…

Après, pour chacun des composants, on a dû chercher la fréquence d'émission, de réception, et surtout la modulation utilisée qui dépendaient de beaucoup trop des standards utilisés.

6.2. Logiciel

Ne connaissant pas la nature du signal, il n'est pas possible de le voir hors de l'équipement, néanmoins, on a pu voir ce qui se passer sur l'équipement et on a pu enregistrer quelques données sur Excel.

La configuration de l'analyseur n'ayant pas été faite convenablement, la fiabilité des résultats est à remettre en question, vu que l'appareil été auto configuré pour étudier des fréquences relativement plus élevé que la fréquence que l'on doit étudier.

Et donc, les principales difficultés qu'on a eu sont des difficultés de l'ordre de la disposition et la compatibilité des matériels entre eux, et de, à chaque fois situer la source du problème et remettre en question le bon fonctionnement de tout.

Les données transmises par le badge vers le lecteur de badge et l'inverse se fait très rapidement et fut difficile à enregistrer surtout sachant qu'on ne savait pas exactement ce que l'analyseur de spectre était en train d'enregistrer.

L'appareil *EXA 9010A* est difficile à manipuler sans un guide d'utilisateur ciblé sur les bases du projet.

On a dut changer plusieurs fois un des instruments, appareils, pour des raisons souvent liées à l'incompatibilité des uns avec les autres.

7. CONCLUSION

L'identification par radio fréquence est un terrain qui devrait encore être développé dans les années à venir, et plusieurs ingénieurs et chercheurs travaillent déjà sur des standards pour mieux l'encadrer et parvenir à unifier les modulations et techniques pour traiter les informations qui circulent s'appuyant sur ce système.

En général, nous avons réussi à atteindre la majorité des objectifs du projet, nous avons vraiment réussi à nous familiariser avec l'appareil, nous avons vu et commenter ce qui se passait lors du passage du badge devant le lecteur.

Nous avons aussi réussi à sauvegarder les captures de données qu'on a réalisées et nous avons compris le fonctionnement du RFID.

Nous n'avons pas réussi à trouver un résultat concret vu les conditions requises mais manquantes pour y parvenir :

- La modulation inconnue et après renseignement souvent propriétaire.
- Les guides utilisateurs absent ou peu utiles.

Mais nous avons exposé un cas idéal ou tout marche et ou on connait la modélisation et on l'a commenté et expliquer pour combler ce manque.

Enfin, nous avons appris beaucoup de choses de ce projet même s'il n'a pas abouti à tous les résultats qu'on voulait atteindre et que le début fut un peu lent vu les besoins matériels requis, et donc pour pouvoir pirater les abonnements *Navigo*, il va falloir attendre les résultats des gens qui poursuivront ce projet les années à venir.