



**TECHNIQUES
DE L'INGÉNIEUR**

Réf. : **E1470 V3**

Systemes et techniques RFID

Date de publication :
10 septembre 2020

Date de dernière validation :
24 août 2021

Cet article est issu de : **Technologies de l'information | Réseaux Télécommunications**

par **Claude TETELIN**

Mots-clés

RFID | téléalimentation |
anticollision | Electronic
Product Code (EPC) |
identification automatique

Résumé Prolongement naturel du code à barres ou pierre angulaire de l'Internet des Objets, la RFID (Identification Radio Fréquence) crée une révolution industrielle tant le nombre de ses applications est immense. Quelles technologies se cachent derrière ce mot ? Cet article tente de présenter les fondements de la RFID en insistant sur les caractéristiques principales. De la télé-alimentation des étiquettes aux algorithmes d'anticollision, le vocabulaire et les équations de base sont introduits pour permettre de mieux comprendre les limites physiques de ces systèmes. La lecture de cet article doit permettre de choisir les bons paramètres (fréquence, modulation, codage, protocole, taille d'antenne, taille mémoire, etc.) pour répondre aux besoins et contraintes de l'application envisagée.

Keywords

RFID | telesupply | anticollision
| Electronic Product Code (EPC)
| automatic identification

Abstract Natural continuation of the barcode or the cornerstone of the Internet of Things, the RFID (Radio Frequency Identification) creates an industrial revolution so much the number of its applications is immense. What kind of technologies hide behind this word? This article tries to present the basics of RFID by pointing out the main characteristics. From tele-supply of labels to the algorithms for singulation, the vocabulary and the basic equations are introduced to allow a better understanding of the physical limits of these systems. The reading of this article has to allow to choose the good parameters (frequency, modulation, coding, protocol, antenna size, memory size, etc.) to meet the needs and constraints of the envisaged application.

Pour toute question :

Service Relation clientèle
Techniques de l'Ingénieur
Immeuble Pleyad 1
39, boulevard Ornano
93288 Saint-Denis Cedex

Par mail :
infos.clients@teching.com

Par téléphone :
00 33 (0)1 53 35 20 20

Document téléchargé le : **01/03/2023**

Pour le compte : **7200082406 - bibliotheque nationale de france // 154.59.125.51**

© Techniques de l'Ingénieur | tous droits réservés

Systemes et techniques RFID

par **Claude TETELIN**

Ingénieur ISEN, Docteur de l'Université de Lille, France
Directeur, Automatic Identification and Data Capture,
GS1 Global Office, Bruxelles, Belgique

1. Principes généraux de la RFID.....	E 1 470v3 – 2
2. Familles de systèmes RFID et caractéristiques	— 4
2.1 RFID active ou passive	— 4
2.2 Champ proche ou champ lointain	— 4
2.3 Lecture seule ou lecture/écriture	— 6
2.4 Protocole ITF ou TTF	— 6
3. Télé-alimentation des étiquettes RFID	— 7
3.1 Télé-alimentation en HF, couplage magnétique	— 7
3.2 Télé-alimentation en UHF, équation de Friis.....	— 9
3.3 Adaptations d'impédance interrogateur et étiquette	— 10
3.4 Évaluation de la puissance captée par l'antenne de l'interrogateur en UHF.....	— 11
3.5 Architectures des interrogateurs en UHF	— 13
4. Communication et codage des informations	— 14
4.1 Modulations en RFID.....	— 14
4.2 Codes utilisés en RFID	— 16
4.2.1 Codes dans la communication <i>uplink</i>	— 17
4.2.2 Codes dans la communication <i>downlink</i>	— 17
5. Protocoles d'anticollision	— 18
5.1 Algorithmes déterministes.....	— 20
5.2 Algorithmes aléatoires	— 20
5.3 Cas particulier du protocole Gen2v2 (ISO/IEC 18000-63).....	— 22
6. Encodage des tags RFID UHF passifs.....	— 24
6.1 Organisation de la mémoire d'un tag UHF passif Gen2v2 (ISO/IEC 18000-63).....	— 24
6.2 Les identifiants ULL et EPC en RFID UHF passive	— 26
6.2.1 Identifiants ISO	— 26
6.2.2 Identifiants GS1	— 27
7. Normes et réglementations	— 28
7.1 Régulations	— 28
7.2 RFID, santé publique et vie privée	— 28
7.3 Normes techniques	— 29
8. Conclusion.....	— 29
9. Glossaire	— 29
10. Sigles, notations et symboles	— 30
Pour en savoir plus.....	Doc. E 1 470v3

Démarrer son véhicule au moyen d'une clé électronique, badger pour accéder à un bâtiment ou une salle, utiliser les remontées mécaniques lors d'un séjour au ski, valider un titre de transport dans le bus ou le métro, payer ses achats avec une carte bancaire sans contact ou encore passer aux caisses automatiques de certains magasins sont des gestes entrés dans le quotidien de bon nombre d'entre nous. Nous utilisons, souvent sans en être conscients, des

technologies de capture automatique de données basées sur les ondes et rayonnements radiofréquences. Ces technologies sont connues sous le nom de **RFID** pour Identification Radio Fréquence. On les retrouve dans nos gestes du quotidien mais il faut bien comprendre qu'elles sont principalement utilisées dans les secteurs industriels, de la grande distribution aux forages pétroliers, en passant par les industries manufacturières aéronautiques, automobiles et le secteur de la santé. Chaque objet individuel, carton, palette, outil, portant une étiquette ou un tag RFID, va pouvoir être identifié de manière unique. Le nombre d'étiquettes ou de tags vendus à cet effet dépasse en 2020 les 20 milliards par an et est en constante augmentation. La différence entre les applications impliquant des individus et celles qui servent à la traçabilité des objets et autres colis, réside principalement dans la distance à laquelle on souhaite pouvoir détecter et lire ces étiquettes RFID. Lire une carte bancaire pour un paiement sans contact à quelques centimètres du lecteur est bien suffisant. Pour des processus industriels de logistique, il faudra pouvoir lire les tags à plusieurs mètres. L'objectif de cet article est de présenter les techniques qui sont mises en œuvre dans les systèmes d'identification par radiofréquence. Il s'agit principalement de télé-alimentation, de télécommunications, d'encodage et d'identification. Les personnes qui recherchent une solution à leur besoin d'automatisation de la traçabilité (identification, inventaire, authentification, etc.) trouveront dans cet article les bases permettant de choisir la technologie RFID la plus adaptée. Les notions telles que le retour sur investissement ou l'intégration de la RFID à un système informatique ne sont pas abordées et demandent généralement une étude au cas par cas.

1. Principes généraux de la RFID

Pour transmettre des informations à un interrogateur (encore appelé « station de base » ou plus généralement « lecteur »), une étiquette RFID est munie d'une puce électronique associée à une antenne. Cet ensemble, appelé *inlay*, est ensuite packagé pour résister aux conditions dans lesquelles il est amené à vivre. L'ensemble ainsi formé est appelé *tag*, *label* ou encore **transpondeur**. La figure 1 représente les éléments d'un système RFID : étiquette, interrogateur et système hôte.

Si l'interrogateur possède sa propre source d'énergie électrique (batterie ou branchement sur le secteur), qu'en est-il de l'étiquette ? Pour qu'une puce électronique puisse fonctionner, chacun sait qu'il faut l'alimenter. Dans bon nombre d'applications, le simple fait de devoir ajouter à notre tag une source d'énergie interne (pile ou batterie) est simplement inconcevable. Le tag serait trop volumineux, trop lourd, coûterait trop cher et une maintenance deviendrait nécessaire pour recharger la batterie ou changer la pile. Les étiquettes RFID doivent donc tirer leur énergie d'une autre source et c'est naturellement l'interrogateur qui va pouvoir la fournir. L'antenne de notre étiquette va non seulement servir pour communiquer avec l'interrogateur mais va devoir également capter l'énergie RF (Radio Fréquence) issue de ce dernier. On parle alors de **télé-alimentation** ou **alimentation à distance**.

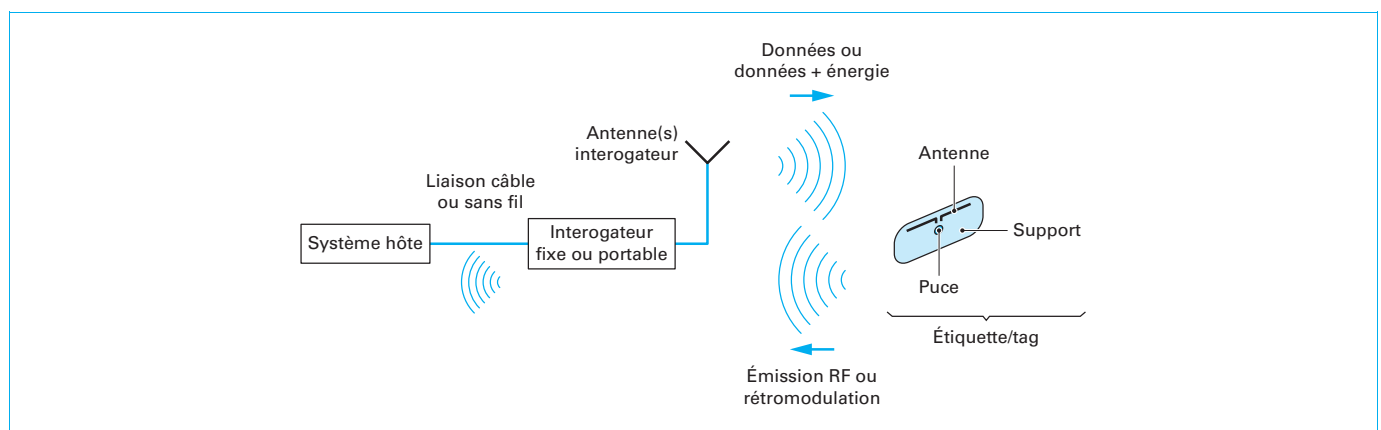


Figure 1 – Les éléments principaux d'un système RFID

Ayant cette source d'énergie à disposition, la puce de l'étiquette pourra alors décoder les commandes venant de l'interrogateur et répondre à ses commandes (ou transmettre des informations sans attendre que l'interrogateur lui demande). La manière de répondre aux commandes d'un interrogateur est, comme la télé-alimentation, une caractéristique des systèmes RFID. Nous pouvons (naturellement) imaginer que la puce de notre étiquette possède un émetteur radiofréquence capable de générer son propre signal. On parle alors de **RFID active**. Un tel émetteur complexifie le circuit électronique de la puce ce qui la rend plus chère. D'autre part, l'énergie récupérée par télé-alimentation ne sera certainement pas suffisante pour alimenter correctement un tel émetteur.

Pour éviter cette complexité tout en pouvant communiquer avec l'interrogateur, l'étiquette RFID va donc devoir modifier ses caractéristiques propres (notamment l'impédance de la puce électronique). Cette modification de l'impédance interne va avoir pour effet de modifier les caractéristiques (amplitude et/ou phase) du signal réfléchi par le tag vers l'interrogateur. Cette technique est appelée **rétromodulation** ou encore **rétrodiffusion** ou **backscattering** en anglais. Elle est à la base des communications des étiquettes RFID passives (sans émetteur RF propre). La figure 2 schématise cette technique de communication. Développée pour des applications radar dans les années 1930, elle a été appliquée pour des communications par Harry Stockman dès 1949.

Bien sûr, si l'application le permet ou le requiert, il est toujours possible d'ajouter, dans ces tags passifs, une source d'énergie propre. Cette source d'énergie peut principalement servir à deux

choses : soit à alimenter la puce RFID, soit à alimenter des modules externes connectés à la puce RFID comme des capteurs. Dans le premier cas, on va améliorer les performances globales du tag puisque celui-ci n'aura plus à être alimenté par le lecteur. La méthode de communication du tag vers le lecteur restant basée sur la rétrodiffusion, on est toujours dans le cas de tags passifs, ils sont simplement assistés d'une source d'énergie propre. On parlera alors de **RFID BAP** (*Battery Assisted Passive*). Pour information, on trouve encore dans certains articles le terme de RFID semi-passive. Ceci n'a pas vraiment de sens physique puisque le tag communique soit avec son propre émetteur RF (**RFID active**) ou par rétrodiffusion (**RFID passive**).

La RFID n'est pas la seule technologie permettant la saisie automatique de données et l'identification d'objets. Les codes à barres (1D ou 2D), la reconnaissance optique de caractères sont très largement répandus et ont l'avantage d'être (pour leur forme la plus simple) relativement bon marché. La RFID a d'autres avantages par rapport à ces techniques. Basée sur les champs magnétiques, électriques ou électromagnétiques, la technologie RFID ne requiert pas de visibilité optique pour la lecture des étiquettes. Un deuxième avantage est que la lecture se fait sans contact électrique direct entre le lecteur et les tags. Suivant les caractéristiques des technologies RFID (fréquences radio utilisées, et design et tailles des antennes par exemple), la distance à laquelle une étiquette peut être lue varie de quelques millimètres à quelques mètres en technologie passive sans batterie. En technologie active, cette distance peut dépasser plusieurs centaines de mètres sans difficulté.

Un autre avantage de la technologie RFID est sa capacité à pouvoir lire plusieurs étiquettes « simultanément ». Nous mettons ce dernier terme entre guillemets car nous verrons plus tard dans cet article, que la lecture de plusieurs étiquettes présentes face à un même interrogateur se fait par étapes et de manière séquentielle. Néanmoins, pour certains protocoles de communication, l'interrogateur peut identifier plusieurs centaines d'étiquettes différentes en quelques secondes. L'effet macroscopique est celui d'avoir identifié ces étiquettes de manière quasi instantanée.

Un dernier avantage de la RFID (parmi les plus importants) réside dans le fait que cette technologie est basée sur une puce électronique. C'est dans la mémoire de cette puce que seront encodés notamment les identifiants uniques permettant aux objets auxquels les tags seront attachés d'être identifiés de manière unique. Suivant l'application, la longueur et la structure de ces identifiants peuvent varier. Un des schémas les plus répandus, connu sous le nom d'EPC (*Electronic Product Code*) est proposé par l'organisme de standardisation GS1. Ce schéma regroupe plusieurs types d'identifiants dont notamment le SGTIN (*Serialized Global Trade Item Number*). Généralement codé sur 96 bits, cet identifiant est le véritable prolongement électronique des codes à barres EAN (*European Article Number*) et UPC (*Universal Product Code*) que l'on retrouve sur tous les articles du commerce. La longueur de 96 bits, même si elle peut paraître faible, permet de concevoir 2^{96} identifiants différents soit près de 8.10^{28} possibilités. Par comparaison, on pourrait identifier individuellement chaque grain de sable de toutes les plages du monde avec 51 bits et tous les atomes du corps humain avec 93 bits. Avec 96 bits, on pourrait identifier individuellement chaque grain de riz produit sur la terre pendant huit mille milliards d'années. Au-delà de cet identifiant, la puce électronique peut posséder d'autres zones de mémoire programmables ou réinscriptibles permettant à l'utilisateur de stocker puis d'accéder à des informations complémentaires en lisant le contenu de ces zones de mémoire. Il peut également compléter ou modifier cette information lors des étapes de la vie de l'objet. Cette information peut éventuellement être cryptée et les zones de mémoire peuvent être partagées par plusieurs utilisateurs avec une gestion des droits d'accès. Dans ce chapitre, nous avons introduit les principes généraux de la RFID. Ils font apparaître de nombreuses caractéristiques qui, suivant les choix réalisés, vont aboutir à des systèmes assez différents. Chacun de ces systèmes va répondre à des besoins et des cas d'usage différents. Certaines applications mettront l'accent sur la simplicité des étiquettes (pas de source

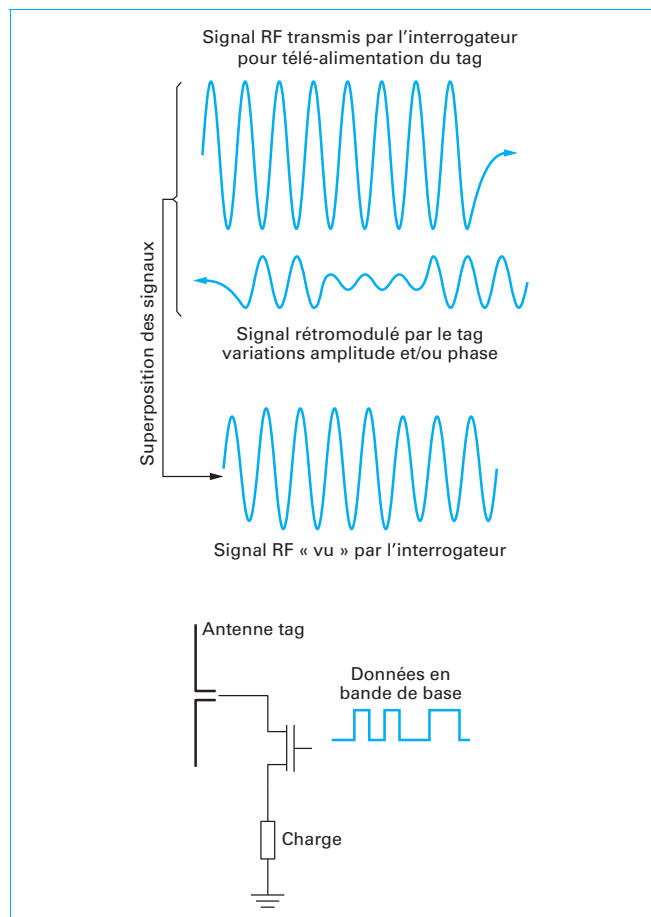


Figure 2 – Principe de la rétrodiffusion pour les tags passifs

d'énergie embarquée, des zones de mémoire réduites pour les identifiants uniques) alors que d'autres souhaiteront avant tout mettre en avant la sécurité des informations contenues dans les tags.

L'acronyme RFID regroupe de nombreuses technologies différentes (actif, passif, fréquences radio, zones de mémoire). Si elles ont en commun de permettre une identification des personnes ou des objets de manière rapide, fiable et automatique, elles présentent des caractéristiques différentes permettant de répondre à des cas d'usage variés. Le paiement sans contact, les inventaires en magasin ou les systèmes de localisation sur des chantiers industriels n'ont pas les mêmes contraintes et les mêmes besoins en termes de performance (distance de lecture, nombre de tags lus par seconde, sécurité des informations).

2. Familles de systèmes RFID et caractéristiques

La RFID est basée sur le fait que des informations contenues dans une puce électronique peuvent être transmises sans contact via un lien RF (Radio Fréquence) à un interrogateur fixe ou mobile. Pour ce faire, la puce électronique est reliée à une antenne, l'ensemble constituant ce que l'on appelle *inlay*. Cet *inlay* est finalement packagé pour répondre aux diverses contraintes de l'application finale.

Tous les tags ou étiquettes RFID ne fonctionnent pas de la même manière. Nous pouvons classer de plusieurs façons les systèmes RFID suivant des critères différents. Le premier critère qui vient à l'esprit est la fréquence à laquelle le système fonctionne. De 125 kHz à 2,4 GHz, voire 5,7 GHz en passant par 13,56 MHz et 900 MHz, on trouve de nombreuses applications répondant à des besoins et contraintes différentes. Cette première classification peut se résumer au fait que le couplage entre l'interrogateur et les étiquettes est soit principalement magnétique, soit principalement électromagnétique. Le couplage est lié également au fait que le système fonctionne en champ proche ou en champ lointain.

Une deuxième classification possible peut se faire suivant que l'étiquette RFID possède un émetteur RF propre (on parle alors de **RFID actif**) ou qu'elle communique par la rétro-modulation d'un signal RF issu de l'interrogateur (on parle alors de **RFID passif**). Il faut bien noter ici que les termes actif et passif n'ont rien à voir avec le fait que l'étiquette embarque ou non une source d'énergie.

Une troisième classification des systèmes RFID peut se faire suivant le type de données encodées dans la puce électronique. Dans certains cas, la puce électronique ne contient qu'un identifiant non modifiable, dans d'autres cas, on peut écrire (une fois ou plusieurs fois) des informations supplémentaires via des commandes transmises par l'interrogateur.

Enfin, une quatrième classification peut se faire suivant le protocole de communication entre l'étiquette et l'interrogateur. Dans une première famille, l'étiquette, une fois présente dans le champ de l'interrogateur, attend une commande de la station de base pour transmettre des informations. On parle de **protocole ITF** (*Interrogator Talk First*). Dans d'autres cas, l'étiquette transmet des informations dès son activation dans le champ de l'interrogateur. On parle alors de **protocole TTF** (*Tag Talk First*). Bien sûr, on trouvera des variantes de ces protocoles dans diverses normes ISO ou propriétaires.

2.1 RFID active ou passive

Dans les systèmes RFID actifs, l'étiquette possède une puce électronique ayant un émetteur RF. La communication entre l'interrogateur et l'étiquette peut donc se faire comme dans n'importe quel

système de communication pair à pair, en utilisant des protocoles full duplex par exemple. Généralement, l'énergie rayonnée par l'interrogateur et captée par l'étiquette n'est pas suffisante pour alimenter l'émetteur RF de la puce RFID active. Aujourd'hui, pour fonctionner, ces systèmes actifs doivent avoir une source d'énergie embarquée.

Nota : avec les avancées technologiques des systèmes de récupération d'énergie et la baisse de la consommation des émetteurs RF, il est possible que certains systèmes RFID actifs puissent fonctionner sans réelle batterie embarquée dans les tags.

Les tags RFID actifs sont généralement plus chers que les tags passifs puisque la puce électronique possède son propre circuit d'émission radio. La norme ISO/IEC 18000-7 prévoit le fonctionnement de systèmes actifs à 433 MHz. Suivant cette norme, la portée de communication entre un interrogateur et une étiquette peut atteindre sans difficulté la centaine de mètres. Le mode 3 de la norme ISO/IEC 18000-4 propose également un protocole basé sur l'utilisation de tags actifs dans la bande de fréquence 2,405 – 2,483 GHz. Ce protocole est d'ailleurs lui-même basé sur la couche physique (NPL : *Network Physical Layer*) de la norme IEEE 802.15.4 également utilisée dans les protocoles ZigBee et 6LoWPAN.

Le principe de fonctionnement des systèmes RFID passifs repose sur la rétro-modulation de l'onde provenant de l'interrogateur. Une onde électromagnétique (ou le champ magnétique, suivant la fréquence utilisée) est alors partiellement réfléchi par l'étiquette. Quels que soient les fréquences ou les modes de couplage, le moyen utilisé pour réaliser cette rétro-modulation, consiste à faire varier l'impédance de la puce vue par son antenne. Pour cela, la puce va commuter une (ou plusieurs) charge (impédance résistive ou capacitive). Cette variation d'impédance induit une variation (en amplitude et/ou en phase) du signal réfléchi par le tag. Ce signal réfléchi vient alors se superposer au signal provenant de l'interrogateur. Le rapport entre la puissance du signal émis par l'interrogateur (pour alimenter la puce) et la puissance du signal rétro-modulé par l'étiquette est largement supérieur à 60 dB. L'interrogateur doit donc présenter une bonne sensibilité pour détecter et décoder l'information issue de l'étiquette. La difficulté de ces systèmes consiste donc à trouver la (les) meilleure(s) charge(s) permettant de créer de fortes variations de signal réfléchi sans pour autant pénaliser l'alimentation du circuit lui-même.

La figure 3 schématise les grandes différences entre tags actifs et passifs d'un point de vue de la communication et d'un point de vue de l'alimentation du tag.

2.2 Champ proche ou champ lointain

Les systèmes RFID passifs peuvent fonctionner à différentes fréquences, dans des bandes réservées aux applications industrielles, scientifiques et médicales (bandes ISM). Ces bandes, si elles ne sont pas soumises à licence, ne sont utilisables qu'en respectant scrupuleusement des règlements et normes propres à chaque région du globe. Ces règlements définissent des gabarits d'émission (largeur de bande autorisée, puissance ou champ maximal à ne pas dépasser) et des taux maximaux d'occupation (§ 7). La figure 4 synthétise les fréquences couramment utilisées pour les applications RFID.

À 125 et 134,2 kHz, on parle de RFID LF (*Low Frequency*), à 13,56 MHz de RFID HF (*High Frequency*), à 433 et dans la bande 860 à 960 MHz de RFID UHF (*Ultra High Frequency*), et enfin, à 2,45 et 5,8 GHz, on parle de RFID SHF (*Supra High Frequency*).

Pour un système RFID passif sans batterie, quelle que soit sa fréquence, l'interrogateur doit émettre un signal permettant la télé-alimentation de la ou des étiquettes présentes à proximité. Pour rayonner ou recevoir un signal radio, il faut se poser la question de l'antenne la plus adaptée. Le concepteur a le choix entre deux grandes familles d'antennes : les antennes fermées (boucles) ou ouvertes (dipôles). Les premières vont plutôt créer un champ magnétique *H* dans leur entourage proche alors que les secondes créeront plutôt un champ électrique *E*. Au fur et à mesure que l'on s'éloigne de la structure rayonnante, le champ électromagnétique

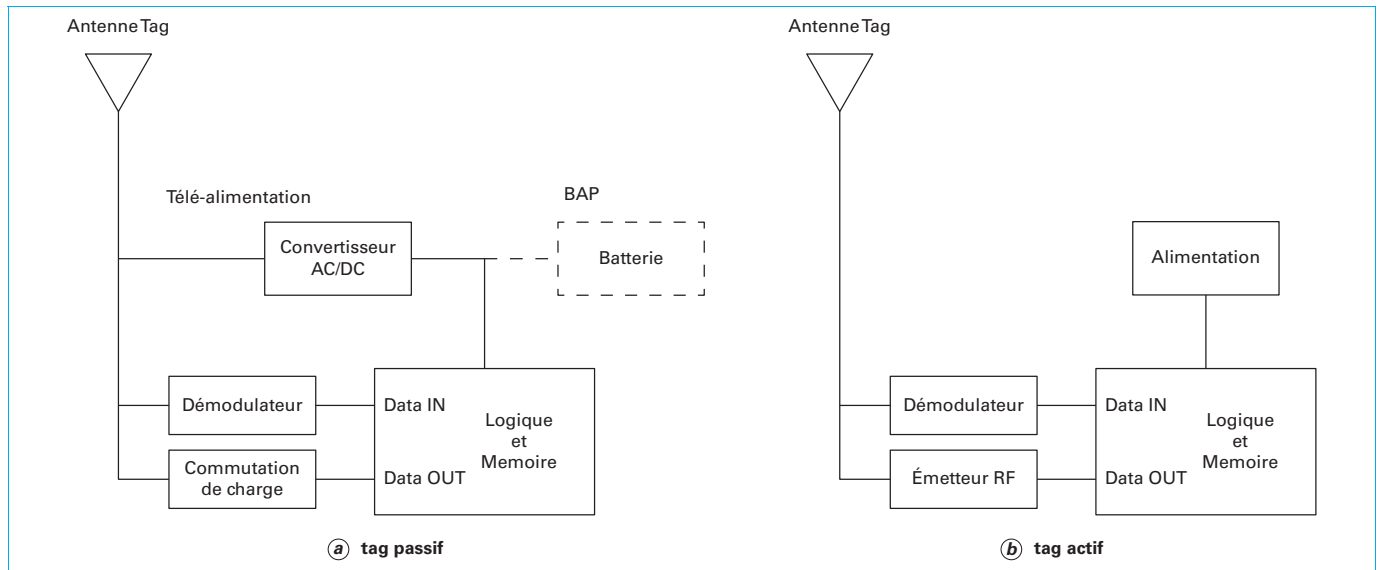


Figure 3 – Schémas de principe des étiquettes a) passives et b) actives

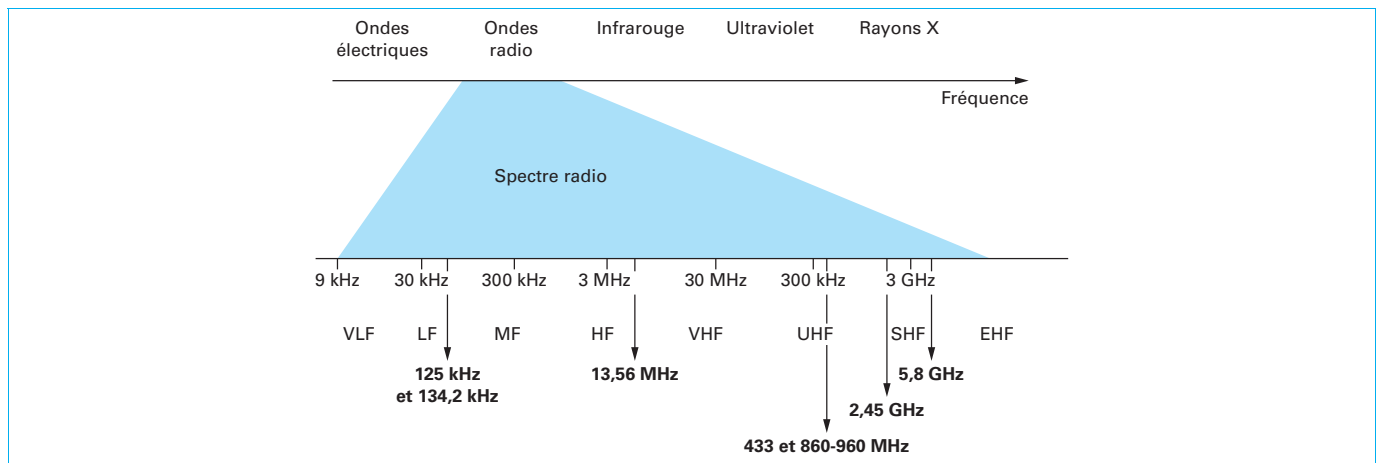


Figure 4 – Fréquences couramment utilisées en RFID

se forme et les célèbres équations de Maxwell permettent de relier champs magnétique et électrique. On parle alors de **champ formé** ou **champ lointain**. La distance à laquelle on peut considérer que le champ électromagnétique est formé dépend de la fréquence du signal et des dimensions de l'antenne.

La figure 5 résume les ordres de grandeur des extensions des zones de champ proche et de champ lointain. Les limites dépendent de D , la plus grande dimension de l'antenne rayonnant le champ électromagnétique et de λ la longueur d'onde du signal. La longueur d'onde est définie par le rapport entre la vitesse de propagation de l'onde électromagnétique c ($3 \cdot 10^8$ m/s dans le vide) et la fréquence du signal. Il n'est pas dans l'objectif de cet article de détailler plus en avant ces notions et le lecteur pourra se référer aux ouvrages [1] et [2].

Prenons l'exemple d'un système RFID HF (*High Frequency*) fonctionnant à 13,56 MHz pour une application de paiement sans contact. Dans l'air (ou dans le vide), la longueur d'onde associée à cette fréquence est de plus de 22 m. À cette fréquence, le champ magnétique maximum que l'on est autorisé à rayonner (§ 7) ne dépasse pas les 60 dBµA/m (ou 10^{-3} A/m) à 10 m. Cette valeur est

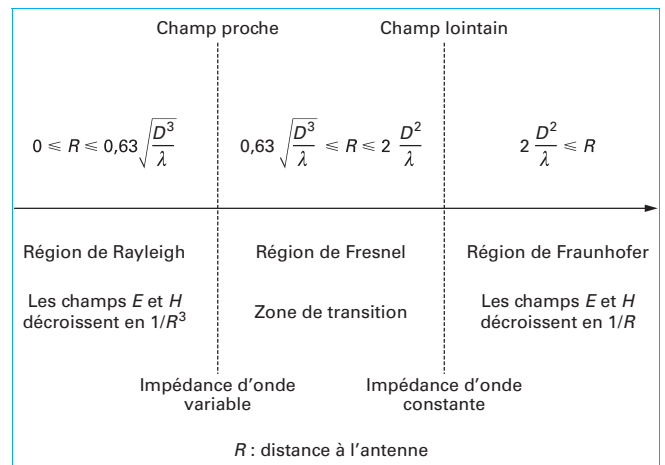


Figure 5 – Définition des zones de champs proche et lointain

très insuffisante pour alimenter une carte de paiement sans contact qui demande au minimum 1 à 2 A/m. Nous sommes donc sûrs que la communication se fera dans la zone de champ proche et jamais dans la zone de champ lointain. Dans cette zone, on peut soit créer principalement du champ magnétique avec une antenne fermée ou du champ électrique avec une antenne ouverte. Dans ce cas, l'antenne doit avoir une dimension proche de la demi-longueur d'onde, soit 11 m [E 3 284]. Il est difficile d'envisager des applications avec de telles tailles d'antenne. Le choix est donc par défaut celui des antennes boucle créant un champ magnétique car la taille de ces antennes n'est pas directement liée à la longueur d'onde du signal.

Si on considère à présent le cas d'un système RFID UHF (*Ultra High Frequency*) fonctionnant à des fréquences proches de 900 MHz, la longueur d'onde est d'environ 33 cm dans l'air libre. Dans cette gamme de fréquences, les régulations (§ 7) autorisent les lecteurs RFID à rayonner des puissances de l'ordre de 4 Watts PIRE (Puissance Isotrope Rayonnée Équivalente). Les tags RFID passifs fonctionnant à ces fréquences requièrent à peine plus de 10 μ Watt ce qui laisse envisager des distances de fonctionnement supérieures à 10 m. À ces distances et à ces fréquences, le système RFID fonctionne dans la zone où le champ électromagnétique est formé. Les équations de Maxwell, valables dans le cas du champ lointain, indiquent que pour une onde électromagnétique se propageant en espace libre, le rapport entre l'amplitude du champ électrique et celle du champ magnétique est constant. Ce rapport est égal à l'impédance du milieu de propagation et vaut, pour le vide, 377 Ω . La valeur de ce rapport montre que le champ électrique est plus propice au transfert d'énergie. Il est donc préférable d'utiliser des antennes ouvertes basées sur le dipôle électrique. Comme dans le cas précédent, la taille optimale de ce type d'antenne est de l'ordre de la demi-longueur d'onde, soit environ 15 cm à 900 MHz. Cette taille est tout à fait compatible avec des applications industrielles.

2.3 Lecture seule ou lecture/écriture

Quelle que soit la fréquence à laquelle le système RFID fonctionne, quel que soit le type d'étiquette passive ou active, on peut différencier les applications RFID suivant les possibilités de lecture et/ou d'écriture de la puce RFID. Le but de la RFID étant d'identifier de manière unique les objets portant des tags, la puce électronique doit au minimum contenir un identifiant numérique accessible par l'interrogateur. Ce numéro unique peut être celui gravé par le fondeur de la puce lors de la fabrication.

Nota : ce numéro unique est généralement appelé TID (*Tag Identifier*) pour les systèmes RFID UHF ou UID (*Unique Identifier*) pour les systèmes RFID HF. La sémantique et la syntaxe de ces identifiants sont définies dans les normes ISO/IEC 15693 et GS1 EPC Tag Data Standard.

Si cette puce ne possède pas d'autre zone mémoire, on parle de **puce en lecture seule**. Toute l'information liée au produit portant l'étiquette est donc déportée sur des systèmes d'informations indexés par l'identifiant unique.

Dans la majorité des cas, ce numéro unique gravé par le fondeur de la puce n'est pas adapté à l'application finale. On utilise alors des puces possédant une zone mémoire vierge sur laquelle on peut écrire un numéro particulier propre à l'utilisateur final du système RFID (comme le code EPC (*Electronic Product Code*)). Une fois ce numéro écrit ou encodé, il est nécessaire de pouvoir le protéger contre toute modification ultérieure. On peut parler alors de **puce à mémoire WORM** (*Write Once, Read Multiple*).

D'autres types d'applications vont nécessiter la présence d'une zone mémoire accessible par l'utilisateur et réinscriptible. Cette zone, ne dépassant pas les quelques dizaines de kilo-octets dans la majeure partie des cas, peut servir lorsque l'accès à une base de données centrale n'est pas garanti (lors d'opérations de maintenance en zone isolée ou sur le théâtre d'opérations militaires). On parle alors de **puces de type MTP** (*Multi Time Programmable*). Quel que soit le type de mémoire, la technologie la plus

généralement répandue pour les puces RFID est la technologie EEPROM (*Electrically-Erasable Programmable Read-Only Memory*).

Nota : pour être tout à fait précis, le concept de mémoire WORM n'est généralement pas implémenté de manière physique mais plutôt logique. En effet, la zone mémoire qui contient un identifiant unique (type EPC) est de technologie EEPROM à laquelle le fabricant a ajouté une fonctionnalité de blocage permanent en écriture (PERMALOCK). Une fois cette zone « permalockée », il est impossible à l'utilisateur de modifier (réécrire) cette zone mémoire.

2.4 Protocole ITF ou TTF

Qui parle le premier : l'étiquette ou l'interrogateur ? Cette question, a priori anodine, prend tout son sens lorsque plusieurs étiquettes se trouvent simultanément dans le champ de l'interrogateur ou lorsque les étiquettes ne sont pas statiques et qu'elles ne font que passer dans le champ rayonné par l'antenne de l'interrogateur. Dans le cas, rencontré très souvent en RFID, où les étiquettes n'ont pas de source d'énergie embarquée (*batteryless*), il est clair que la première chose à faire pour l'interrogateur est de transmettre de l'énergie à (aux) l'étiquette(s). Pour cela, l'interrogateur émet un signal à fréquence fixe (sans modulation). À ce moment-là, la communication entre l'interrogateur et l'étiquette n'a pas, à proprement parler, débuté. Une fois la puce de l'étiquette RFID alimentée, elle peut : soit transmettre immédiatement une information à l'interrogateur (protocole TTF pour *Tag Talk First*), soit répondre à une requête de l'interrogateur (protocole ITF pour *Interrogator Talk First*). Le choix d'un protocole ou de l'autre dépend fortement de la gestion de la ressource radio et de la gestion de la présence éventuelle de plusieurs étiquettes dans le champ rayonné par l'interrogateur (protocole d'anticollision).

Pour se faire une idée de l'implication sur la gestion des collisions du choix d'un protocole ou de l'autre, imaginons une salle de classe. L'enseignant joue le rôle de l'interrogateur, les élèves celui des étiquettes RFID. Pour les systèmes TTF, nous pouvons imaginer qu'en début de cours, chaque étudiant entrant dans l'amphithéâtre donne son nom. Bien sûr, mis à part quelques retardataires, les étudiants arrivent en cours à l'heure et chacun donnant son nom quasiment en même temps, nous pouvons douter que l'enseignant (l'interrogateur) puisse comprendre chaque nom individuellement et identifier chacun des étudiants (étiquettes). Pour essayer de pallier ce problème, il est possible de demander aux étudiants de ne donner leur nom qu'après avoir écouté et s'être assurés que personne d'autre n'a pris la parole. Cette variante du protocole TTF est appelée **TOTAL** pour *Tag Only Talk After Listening*. Pour des systèmes ITF, c'est l'enseignant (interrogateur) qui pose la première question et demande aux élèves de donner leur nom. Tous les étudiants présents dans l'amphithéâtre répondent alors à la requête de l'enseignant. Comme dans le cas précédent, il peut être difficile, voire impossible, à l'enseignant d'identifier chaque élève puisque ceux-ci répondront à la requête de façon simultanée.

À la vue de cet exemple, nous pouvons conclure que les deux protocoles sont incompatibles. De plus, la présence d'une étiquette TTF dans le champ d'un interrogateur ITF peut amener des perturbations brouillant la communication des étiquettes ITF.

Parmi les avantages du protocole TTF, on peut noter la rapidité avec laquelle il est possible d'identifier une étiquette quand celle-ci est seule dans le champ rayonné par l'interrogateur. On peut également noter que lorsque l'interrogateur ne communique pas avec des étiquettes, il ne fait que rayonner un signal RF sans modulation. Ce signal n'occupe donc qu'une faible partie du spectre électromagnétique. Cela permet de réduire le risque d'interférence avec d'autres émissions ou d'autres interrogateurs. En ce qui concerne le protocole ITF, le principal avantage est que la communication est initiée et dirigée par l'interrogateur. Toutes les réponses des tags peuvent donc être facilement superposées pour une détection de collision au niveau « bit » ou facilement séquencées pour singulariser les étiquettes.

Nota : Aujourd'hui, les applications RFID sont toutes basées sur le protocole ITF. Le protocole TTF a quasiment disparu.

Les différentes technologies RFID peuvent être classées suivant :

- la fréquence de fonctionnement (qui déterminera le type d'antenne à utiliser et le type de couplage existant entre lecteur et tag(s)) ;
- la méthode de communication des tags vers le lecteur (avec un émetteur RF pour la RFID active ou basée sur la rétro-modulation pour la RFID passive) ;
- le type d'information contenu dans la mémoire de la puce RFID (simple identifiant en lecture seule ou information partagée) ;
- le protocole de communication entre lecteur et tag(s).

Généralement, le simple fait de décrire l'application, les processus, les points bloquants existants et les améliorations attendues permet de répondre aux questions de base permettant alors de choisir la technologie la plus adaptée.

3. Télé-alimentation des étiquettes RFID

Pour répondre aux cas d'usage les plus courants, les étiquettes RFID pour la plupart n'embarquent pas de source d'énergie. La première mission de l'interrogateur est donc de télé-alimenter la puce électronique présente sur l'étiquette. Suivant les fréquences utilisées et les distances de télé-alimentation souhaitées, ce transfert d'énergie se fera soit via un champ magnétique, soit via une onde électromagnétique. Les antennes utilisées seront donc principalement des boucles dans le premier cas et des dipôles électriques dans le second. Dans les cas des systèmes RFID LF et HF, la taille des antennes électriques qu'il faudrait déployer est incompatible avec les contraintes des applications. Les antennes fermées créant principalement un champ magnétique en zone de Rayleigh sont donc préférées. En revanche, pour les applications RFID en UHF ou au-delà, le système fonctionnera plutôt en champ lointain et la taille des antennes électriques est généralement compatible avec les contraintes géométriques des applications. Les équations de télé-alimentation sont donc fondamentalement différentes.

3.1 Télé-alimentation en HF, couplage magnétique

Selon la loi de Biot et Savart, tout conducteur parcouru par un courant électrique crée, à distance, un champ magnétique. Pour maximiser le courant issu d'un générateur, il est préférable de le connecter à un circuit fermé (impédance nulle), une spire par exemple. En intégrant la loi de Biot et Savart, il est assez simple de calculer le champ magnétique \vec{H} (en $A \cdot m^{-1}$) créé par le courant d'intensité I parcourant une spire de rayon r sur un point de l'axe de la spire situé à une distance d . La figure 6 montre comment chaque élément de la spire crée un élément de champ $d\vec{H}$. Par symétrie, le champ total créé par la spire sera orienté suivant l'axe de cette spire. Le résultat de l'intégration vectorielle est donné dans l'équation (1) :

$$H_x = \frac{I r^2}{2(r^2 + d^2)^{3/2}} \quad (1)$$

Dans le cas où l'antenne est composée de N boucles jointives de même dimension, le champ magnétique résultant est N fois celui de l'équation (1).

La valeur maximale de ce champ est bien sûr obtenue pour une distance d nulle, c'est-à-dire au centre de la spire. Sa valeur vaut $NI/2r$, ce qui veut dire que plus la spire sera grande, plus le champ magnétique maximal sera faible. Lorsque l'on s'éloigne de la spire, c'est-à-dire lorsque d est grand devant r , nous pouvons remarquer que l'amplitude du champ magnétique diminue avec le cube de la distance. Ce qui pourrait paraître comme un désavantage pour la distance de télé-alimentation du tag peut devenir un avantage pour l'application RFID car nous pouvons considérer qu'avec une telle décroissance du champ magnétique, la zone dans laquelle le tag sera télé-alimenté sera bien définie dans l'espace. Ceci peut être un atout majeur pour les applications sécuritaires ou pour les applications dans lesquelles de nombreux interrogateurs peuvent se trouver proches les uns des autres. La figure 6 montre comment varie l'amplitude du champ magnétique en fonction de la distance au centre de la spire pour différents rayons de spire.

Pour mettre en place des modélisations électriques des systèmes RFID, il peut être intéressant de faire apparaître l'inductance de la spire dans l'équation du champ magnétique ou dans celle de

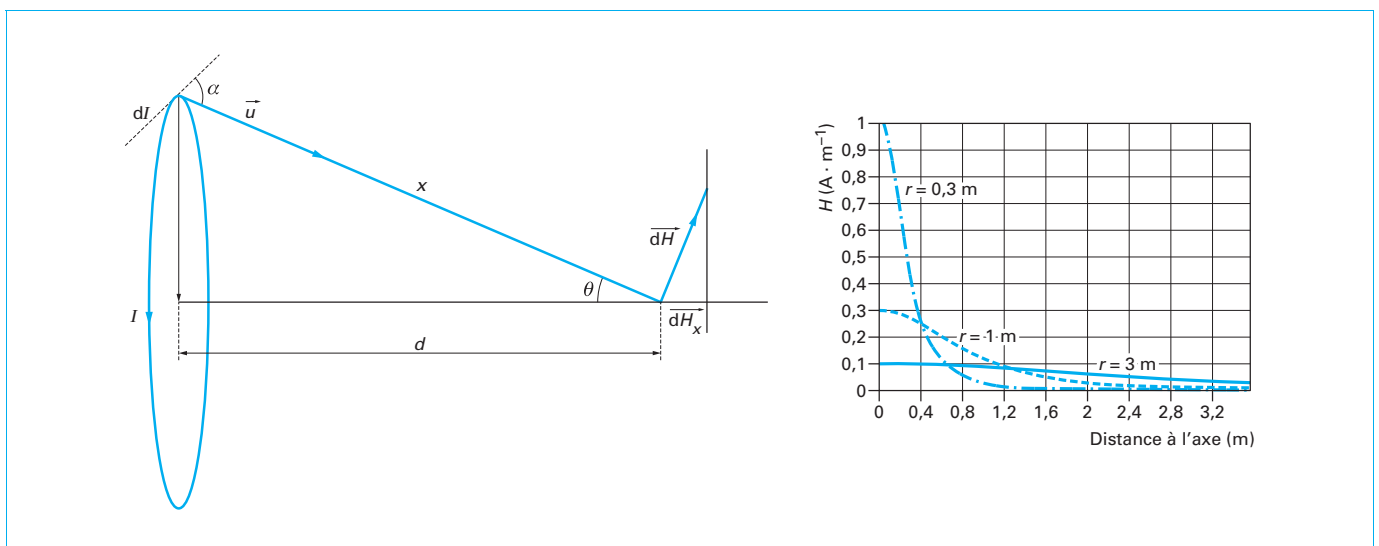


Figure 6 – Spire parcourue par un courant et champ magnétique résultant

l'induction magnétique. Il suffit de remarquer que le flux de l'induction magnétique à travers la spire peut s'écrire :

$$\Phi = \oint \vec{B} \cdot d\vec{s} = B_{d=0} Ns \quad (2)$$

où N est le nombre de tours de l'antenne spire et s la surface des spires.

L'approximation n'est valable que si l'induction magnétique est considérée constante sur toute la surface de la spire et que sa valeur est celle calculée au centre de la spire. D'autre part, ce flux peut s'écrire comme le produit de l'inductance des spires par le courant qui les parcourt, soit $\Phi = LI$. Nous pouvons donc en déduire la valeur de l'inductance (en Henry) :

$$\frac{N^2 \mu \pi r}{2} = L \quad (3)$$

L'induction magnétique B (en Tesla ou $V.s.m^{-2}$) est reliée au champ magnétique H par la relation $\vec{B} = \mu \vec{H}$ avec μ la perméabilité magnétique. En partant de l'équation (1), et en introduisant l'inductance de la spire (équation (3)), il est possible d'écrire l'induction magnétique en fonction de l'inductance, de la tension U appliquée à ses bornes et de la fréquence f :

$$B = \frac{U}{4\pi f} \left(\frac{r}{r^2 + d^2} \right)^{3/2} \sqrt{\frac{2\mu}{\pi L}} \quad (4)$$

Dans l'équation (4), il faut bien noter que L est une fonction des dimensions de l'antenne (voir l'équation (3)). Après avoir tracé l'évolution du champ magnétique H en fonction de la distance à l'axe de l'antenne, il peut être intéressant de tracer l'évolution de B en fonction de la taille de l'antenne pour une distance fixée. Cette évolution est représentée sur la figure 7.

Il est intéressant de noter que pour une distance (ou une plage de distances) de l'étiquette interrogateur connue et fixée, la taille de l'antenne peut être facilement optimisée pour maximiser le champ magnétique créé.

Une fois le champ magnétique créé par l'antenne boucle de l'interrogateur, l'étiquette RFID doit pouvoir en capter une partie et la transformer pour alimenter la puce électronique. Nous faisons alors appel à la loi de Faraday (équation (5)) disant que toute variation de flux de champ magnétique à travers un circuit fermé crée une différence de potentiel à ses bornes :

$$e = - \frac{\partial \Phi}{\partial t} \quad (5)$$

Dans cette équation, e (Volt) est la différence de potentiel induite. La figure 8 schématise le couplage entre les antennes de l'interrogateur et de l'étiquette. Dans les applications RFID, les deux antennes lecteur et tag ne sont pas de même taille et sont rarement exactement superposées. Les lignes de champ issues

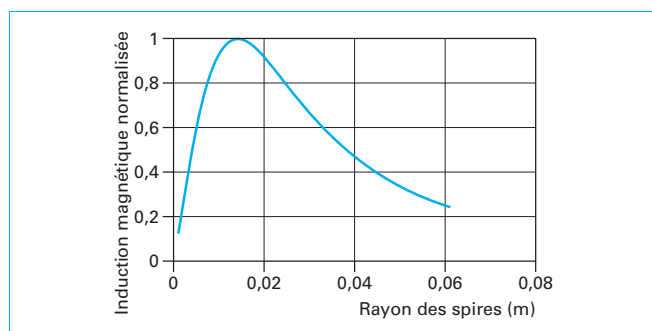


Figure 7 - Induction magnétique à distance fixée en fonction de la taille d'antenne

de l'antenne lecteur ne sont donc que partiellement captées par l'antenne du tag.

On définit alors le coefficient de couplage k (sans dimension) comme le rapport entre le flux magnétique capté par l'antenne de l'étiquette et le flux magnétique total créé par l'antenne de l'interrogateur :

$$k = \frac{\Phi_{Utile}}{\Phi_{Total}} = \frac{M}{\sqrt{L_1 L_2}} \quad (6)$$

Le lecteur pourra se référer à [3] et [4] pour trouver le détail des calculs montrant que le coefficient de couplage peut également s'écrire en fonction des inductances des antennes interrogateur et étiquette et de la mutuelle inductance M entre ces deux antennes. Dans les applications RFID HF, la valeur de k dépend de la géométrie des antennes (taille, spires concentriques ou jointives, spires circulaires ou rectangulaires), de la distance entre les antennes, de leurs positions respectives et de l'environnement magnétique (présence de métal, d'eau, etc.). Les valeurs typiques de k sont comprises entre 0 et 15 %.

Le schéma de la figure 8 peut être modélisé électriquement par un transformateur ayant des inductances au primaire et secondaire de L_1 et L_2 respectivement, et un couplage M .

Comme nous l'avons vu précédemment, les systèmes RFID sont prévus pour fonctionner à des fréquences bien précises. Il est évident que le transfert d'énergie entre l'interrogateur et les étiquettes doit être optimisé pour la fréquence de travail. Les inductances des antennes doivent être accordées à cette fréquence. Dans le cas de l'interrogateur, il s'agit de maximiser le courant circulant dans l'antenne puisque c'est ce courant qui est à l'origine du champ magnétique rayonné. La résonance doit donc se faire dans un modèle équivalent RLC série. D'un autre côté, le flux magnétique capté par l'antenne de l'étiquette génère un courant induit qui doit être transformé en tension pour alimenter la puce électronique. Une résonance tension est alors mise en œuvre grâce à un circuit RLC parallèle. La figure 9 montre le schéma électrique équivalent du système RFID HF résonant.

Dans le schéma de la figure 9, R_1 et R_2 sont les résistances équivalentes de perte des enroulements des antennes interrogateur et étiquette respectivement. Les capacités C_1 et C_2 (en F) sont calculées pour former avec les inductances L_1 et L_2 des circuits résonants suivant l'équation (7) :

$$C_i = \frac{1}{L_i \omega^2} \text{ avec } i = 1 \text{ ou } 2 \quad (7)$$

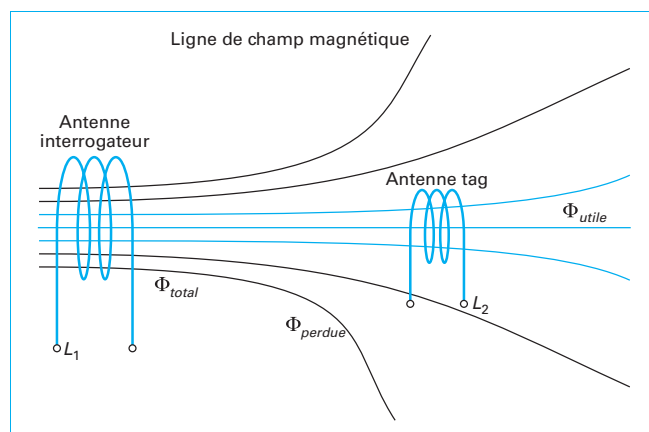


Figure 8 - Couplage magnétique entre antennes interrogateur et étiquette

À partir du schéma de la figure 9, il est possible de calculer l'impédance équivalente Z_1 , rapport de la tension V_1 et du courant I_1 , en fonction de Z_2 , rapport de la tension V_2 et du courant I_2 au niveau de l'étiquette :

$$Z_1 = j\omega L_1 - \frac{\omega^2 M^2}{Z_2 - j\omega L_2} \text{ avec } Z_2 = R_2 + R_{ic} // \frac{1}{jC_2\omega} \quad (8)$$

avec Z_1 et Z_2 en Ω .

En combinant les équations (8) et (6), on obtient une expression de l'impédance faisant intervenir le coefficient de couplage. Au final, l'impédance équivalente « vue » par le générateur peut s'écrire :

$$Z_{\text{générateur}} = R_1 + \frac{1}{jC_1\omega} + j\omega L_1 - \frac{\omega^2 k^2 L_1 L_2}{Z_2 - j\omega L_2} \quad (9)$$

À la pulsation de résonance, et uniquement à cette pulsation, les termes $\frac{1}{jC_1\omega}$ et $j\omega L_1$ se compensent et disparaissent de l'équation (9).

La figure 10 montre les variations de la tension V_2 (au niveau de l'antenne tag) en fonction de la valeur de k . Elle met en évidence trois modes de fonctionnement distincts, le sous-couplage, le couplage idéal et le sur-couplage.

Lorsque le coefficient de couplage est nul, aucun transfert d'énergie n'est possible entre l'interrogateur et le tag ; la tension aux bornes du tag est nulle. Lorsque k augmente, la tension aux bornes de la puce électronique du tag augmente également. À partir d'une certaine valeur de coefficient de couplage, il est possible d'observer l'apparition de deux fréquences de résonance distinctes de la fréquence de résonance de l'interrogateur et du tag. L'interrogateur rayonnant toujours un champ magnétique à sa fréquence de résonance, il est alors possible d'observer une chute de la tension induite aux bornes du tag. Ce phénomène de sur-couplage apparaît pour de fortes valeurs de k , c'est-à-dire lorsque l'interrogateur et le tag sont proches. Ce phénomène peut compromettre la télé-alimentation alors que le tag est au plus près de l'interrogateur. Les lecteurs désirant en savoir plus sur les circuits oscillants couplés peuvent se reporter à [5].

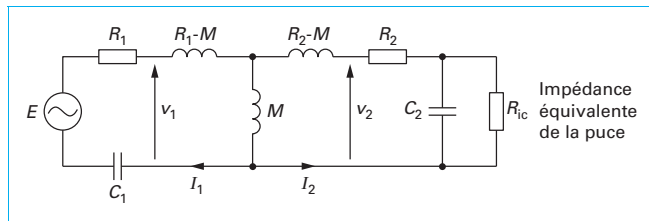


Figure 9 – Schéma électrique équivalent en RFID HF

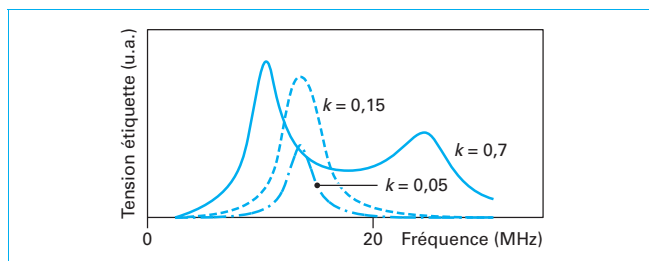


Figure 10 – Évolutions de la tension aux bornes du tag en fonction de la fréquence pour différents coefficients de couplage

Pour être complète, cette modélisation doit prendre en compte les variations d'impédance interne de la puce électronique. Une modélisation par une résistance fixe R_{ic} en parallèle avec une capacité C_2 n'est qu'une première approximation. L'impédance interne de la puce peut présenter des variations importantes suivant la distance qui sépare l'étiquette de l'interrogateur (variations de l'amplitude du champ magnétique et donc de la tension induite aux bornes de l'antenne du tag) ou suivant les fonctions qu'elle doit réaliser (écriture en mémoire, calculs cryptographiques, etc.). Pour optimiser le design de l'antenne de l'étiquette, il est donc important de connaître la plage de variation de l'impédance d'entrée de la puce que seul le fabricant de la puce peut donner ou qu'un laboratoire correctement équipé peut mesurer.

3.2 Télé-alimentation en UHF, équation de Friis

Lorsque la fréquence d'une onde électromagnétique augmente, sa longueur d'onde diminue. Dans les systèmes RFID UHF, il est courant de considérer que les tags reçoivent de l'interrogateur des champs électromagnétiques formés (zone de Fraunhofer, cf. § 2.2). Les antennes utilisées sont généralement des antennes basées sur le dipôle ou le patch. En champ formé, les antennes sont caractérisées par des paramètres tels que le gain, la surface équivalente, la directivité ou encore la polarisation. [2], [E 3 284]. Pour le gain, l'antenne de référence est l'antenne isotrope, c'est-à-dire une antenne rayonnant une onde électromagnétique de manière égale dans toutes les directions de l'espace. Le gain G d'une antenne peut donc s'écrire sous la forme :

$$\text{Gain} = \frac{\text{densité de puissance rayonnée par l'antenne dans la direction considérée à une distance } d}{\text{densité de puissance rayonnée par une antenne isotrope à la même distance } d} \quad (10)$$

Ce gain dépend de la fréquence à laquelle l'antenne fonctionne.

Le gain d'une antenne, grandeur utilisée lors du calcul de la densité de puissance rayonnée par cette antenne, peut être relié à la surface équivalente Σ (en m^2) de cette antenne, grandeur utilisée lors du calcul de la puissance captée par cette antenne. Cette relation est donnée par l'équation (11) :

$$\Sigma = G \frac{\lambda^2}{4\pi} \quad (11)$$

La puissance captée (en W) par l'antenne du tag est donc reliée à la puissance appliquée à l'antenne de l'interrogateur suivant l'équation (12) :

$$P_{\text{ant-tag}} = P_{\text{int}} G_{\text{int}} \frac{1}{4\pi d^2} \Sigma_{\text{tag}} = P_{\text{int}} G_{\text{int}} G_{\text{tag}} \left(\frac{\lambda}{4\pi d} \right)^2 \quad (12)$$

Dans cette équation, G_{int} représente le gain de l'antenne de l'interrogateur et G_{tag} celui de l'antenne du tag et d est la distance qui sépare l'interrogateur du tag. Il ne faut pas oublier que les gains dépendent de la direction dans laquelle une antenne émet (ou reçoit) une onde électromagnétique ainsi que de la fréquence à laquelle le système RFID fonctionne. L'équation (12) tient donc compte des positions des antennes l'une par rapport à l'autre (élévation et azimut). Pour calculer la distance maximale de télé-alimentation d'une étiquette, il faut donc considérer les gains maximaux des antennes. Il est important de noter plusieurs choses concernant l'équation (12). La première est que $P_{\text{ant-tag}}$ représente la puissance captée par l'antenne du tag. Ce n'est pas la puissance fournie à la puce électronique de l'étiquette. La relation liant ces deux puissances sera établie dans le paragraphe concernant l'adaptation de puissance (§ 3.3). La seconde est que l'atténuation $\left(\frac{4\pi d}{\lambda} \right)^2$

Tableau 1 – Atténuations supplémentaires dues à la polarisation de l’antenne de l’interrogateur et à l’alignement des antennes				
		Polarisation de l’antenne de l’interrogateur		
		Circulaire	Verticale	Horizontale
Orientation de l’antenne dipôle du tag	Verticale	3 dB	0 dB	Infinie
	Horizontale	3 dB	Infinie	0 dB
	Inclinée (45°)	3 dB	3 dB	3 dB
	Parallèle au rayon incident	Infinie	Infinie	Infinie

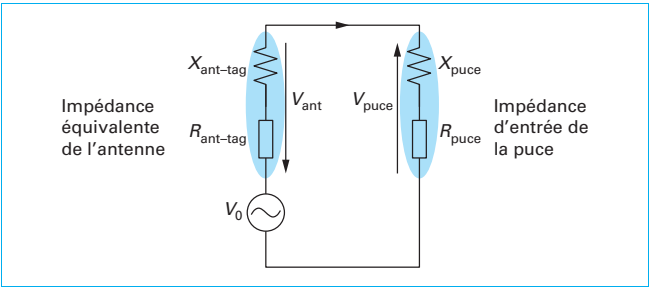


Figure 11 – Schéma électrique équivalent de l’antenne UHF et de la puce

est celle correspondant à une propagation d’onde électromagnétique en espace libre (ellipsoïde de Fresnel dégagée de tout obstacle). Enfin, l’équation (12) ne tient pas compte des polarisations respectives des antennes. Le tableau 1 résume l’atténuation supplémentaire à prendre en compte suivant les polarisations du couple d’antennes.

Pour connaître la puissance fournie à la puce de l’étiquette, il faut partir du schéma électrique équivalent de l’ensemble antenne et tag représenté sur la figure 11. Sur ce schéma, la tension V_0 (crête) représente la différence de potentiel créée aux bornes de l’antenne du tag quand aucune charge n’y est connectée. $R_{ant-tag}$ est la partie réelle de l’impédance de l’antenne du tag. Cette résistance est la somme de la résistance de rayonnement et de la résistance de pertes ohmiques. Dans le cas d’une adaptation parfaite entre l’impédance de l’antenne et celle de la puce, nous avons les relations suivantes :

$$R_{ant-tag} = R_{puce} \text{ et } X_{ant-tag} = -X_{puce}$$

Il vient assez facilement que la puissance totale reçue par l’antenne se divise en deux parties égales. Une première moitié de la puissance est transmise à la puce, l’autre moitié est en fait rayonnée par l’antenne du tag.

Connaissant la puissance minimale nécessaire à l’alimentation de la puce (typiquement entre – 25 et – 15 dBm suivant la technologie et la complexité de la puce), le degré d’adaptation entre l’antenne du tag et la puce, les gains des antennes de l’interrogateur et du tag, il est donc possible d’estimer la distance maximale de télé-alimentation. Ainsi, en tenant compte des régulations en vigueur dans les principales zones géographiques mondiales, des distances maximales théoriques de télé-alimentation supérieures à 15 m peuvent être calculées. Le monde réel étant plus complexe, les imperfections font que les distances de fonctionnement fiable sont plutôt de l’ordre de 8 à 10 m.

3.3 Adaptations d’impédance interrogateur et étiquette

Comme nous avons pu le voir dans les paragraphes précédents, les systèmes RFID utilisent, le plus souvent pour des raisons de coût et de simplicité d’utilisation, des étiquettes sans source d’énergie embarquée. Pour les systèmes passifs, le rapport de puissance entre l’onde émise par l’interrogateur et celle réfléchiée par le tag peut atteindre des valeurs bien supérieures à 60 dB.

En ce qui concerne l’interrogateur, comme pour tout émetteur RF, le problème est d’adapter l’impédance du générateur (HF ou UHF) à l’impédance de l’antenne qui lui est connectée. Ceci a pour but d’optimiser le transfert de puissance entre ces deux éléments. Une fois ce transfert optimisé, reste à savoir si la puissance transmise à l’antenne sera bien transformée en rayonnement magnétique ou électromagnétique ou simplement dissipée par effet Joule. Le transfert de puissance entre deux impédances est optimal si celles-ci sont complexes conjuguées. Pour obtenir un tel résultat, il faudrait pouvoir soit modifier l’impédance interne du générateur, soit modifier l’impédance équivalente de l’antenne de l’interrogateur. Généralement, les impédances internes des générateurs sont égales à 50 Ω. À moins de le concevoir soi-même, il est donc difficile de trouver le générateur qui satisfera la condition d’adaptation à une antenne donnée. Côté antenne, modifier son impédance équivalente (pour l’adapter à celle du générateur) revient à modifier sa géométrie, sa taille ou les matériaux qui la composent. Il faudrait donc trouver un compromis entre l’adaptation et les caractéristiques de rayonnement (HF ou UHF) de cette antenne. Ce compromis est difficile à atteindre pour les concepteurs de systèmes RFID. L’adaptation se fait donc par l’ajout, entre le générateur et l’antenne, de composants supplémentaires. Ces composants peuvent être localisés (inductances, capacités, voire résistances) ou répartis (*stub*, *slug*). Le choix dépend bien sûr de la fréquence du générateur et de la place disponible sur le circuit imprimé.

Dans le cas des antennes LF et HF, l’utilisation de composants résistifs n’intervient pas dans la réalisation de l’adaptation d’impédance à proprement parler mais peut servir à contrôler le coefficient de qualité du système « générateur + antenne ». Comme nous le verrons dans le chapitre suivant, ce coefficient de qualité joue un rôle important dans la valeur de la bande passante du système. L’utilisation de résistances est généralement préférée à la mise en œuvre de montages d’adaptation à quatre éléments réactifs pour des raisons de robustesse des performances finales aux tolérances des composants (dans le cadre d’une industrialisation). Pour une description approfondie des méthodes d’adaptation d’impédance en électronique radiofréquences, le lecteur pourra se reporter aux ouvrages [5] [6] [7].

Dans le cas des systèmes RFID fonctionnant à des fréquences LF ou HF, nous avons vu que les antennes (boucles inductives) doivent être connectées à des capacités pour former un circuit résonant optimisant le courant dans la boucle aux fréquences de travail. Cette résonance est intégrée au système d’adaptation de puissance.

Ceci a donc pour conséquence d'optimiser le transfert de puissance entre le générateur et l'antenne et d'optimiser le courant circulant dans la boucle (courant à l'origine du champ magnétique servant à la télé-alimentation du tag).

En ce qui concerne le tag, nous devons bien faire la distinction entre les systèmes HF (couplage magnétique) et UHF (couplage généralement électromagnétique). Pour les systèmes HF, l'antenne (boucle inductive) du tag, doit capter un maximum de flux magnétique pour assurer l'alimentation de la puce. Cette alimentation doit se faire avec un niveau de tension suffisant. Il faut donc transformer le courant induit dans l'antenne du tag en tension. C'est la raison pour laquelle on met en place une résonance LC de type parallèle. L'impédance d'entrée de la puce présentant généralement une partie réactive de type capacitif, l'ajout d'un composant supplémentaire en parallèle entre la boucle et la puce peut être évité si toutefois le design de la boucle est correctement ajusté (au prix d'un compromis sur les caractéristiques physico-géométriques de la boucle et donc sur les performances finales du système RFID).

En ce qui concerne les systèmes UHF, le problème se pose différemment puisque nous sommes (le plus souvent) en régime de champ formé. Nous sommes donc confrontés au même type de problème que pour les interrogateurs : il s'agit de transférer un maximum de puissance d'un générateur vers une charge. Cette fois, le générateur peut être modélisé comme un générateur de tension idéal (modèle de Thévenin) en série avec l'impédance équivalente de l'antenne du tag. La charge est l'impédance d'entrée de la puce électronique. Le schéma électrique équivalent est celui de la figure 11. Il peut être intéressant de s'attarder sur le bilan de puissance entre l'antenne et la puce non seulement pour connaître quelle proportion de la puissance captée par l'antenne arrivera aux bornes de la puce (important pour calculer la distance de télé-alimentation) mais également pour connaître la proportion de puissance re-rayonnée vers l'interrogateur (signal utile dans la communication tag vers interrogateur). Pour cela, nous devons définir le coefficient de réflexion en tension Γ issu de la désadaptation entre deux impédances (ici Z_{ant} et Z_{puce}) :

$$\Gamma = \frac{Z_{puce} - Z_{ant}}{Z_{puce} + Z_{ant}} \text{ (sans unité)} \quad (13)$$

À partir de ce coefficient de réflexion en tension, nous pouvons définir le coefficient de transmission T en puissance entre l'antenne et la puce :

$$T = 1 - |\Gamma|^2 \quad (14)$$

Ce coefficient de transmission peut se réécrire en fonction des paramètres circuit du tag :

$$T = \frac{4R_{ant}R_{puce}}{|Z_{ant} + Z_{puce}|^2} \quad (15)$$

En complément de ce coefficient de transmission, il est utile de définir le coefficient de re-rayonnement K (*backscattering coefficient*), exprimant la capacité d'une antenne à réfléchir une onde en fonction de ses caractéristiques et de l'impédance qui lui est connectée. Cette définition est issue des références [11] et [12]

$$K = |1 - \Gamma|^2 = \frac{4R_{ant}^2}{|Z_{ant} + Z_{puce}|^2} \quad (16)$$

À partir des équations (15) et (16), nous pouvons déduire que la puissance transmise à la puce est la puissance reçue par l'antenne multipliée par T et la puissance re-rayonnée par le tag est cette même puissance reçue multipliée, cette fois, par K . Le tableau 2 résume les principaux cas rencontrés en fonction des valeurs d'impédance.

Tableau 2 – Valeurs de K et T en fonction des impédances de puce et d'antenne

	Z_{puce}	T	K
Court-circuit	0	0	$\frac{4R_{ant}^2}{R_{ant}^2 + X_{ant}^2}$
Réactive	$-jX_{ant}$	0	4
Circuit ouvert	infinie	0	0
Adaptation	Z_{ant}^*	1	1

Les lecteurs pourront se référer à [1] et [13] pour une discussion plus approfondie des coefficients de transmission et de re-rayonnement.

3.4 Évaluation de la puissance captée par l'antenne de l'interrogateur en UHF

L'équation des bilans de puissance (équation (12)), encore connue sous le nom d'équation de Friis, peut être utilisée pour la liaison interrogateur vers le tag mais aussi pour la liaison retour, tag vers interrogateur. Le lecteur pourra se référer aux ouvrages [1] et [2] pour plus de détails. Il existe néanmoins une méthode graphique qui permet d'évaluer rapidement les puissances mises en jeu et de savoir quel est l'élément limitant dans une communication RFID. En effet, deux cas principaux peuvent se produire : la distance de communication est limitée par les performances du tag ou par les performances de l'interrogateur.

Le schéma de la figure 12 représente les puissances mises en jeu (en dBm) en fonction de la distance.

Nota : La puissance en dBm est donnée par dix fois le logarithme en base 10 de la puissance exprimée en mWatt. 1 mW correspond donc à 0 dBm et 30 dBm correspondent à 1 W.

L'interrogateur rayonne une puissance P_{Tx} équivalente au produit de la puissance conduite par le gain de l'antenne de l'interrogateur.

Nota : la puissance rayonnée par l'interrogateur est également appelée EIRP (*Equivalent Isotropic Radiated Power*). Cette puissance est bien sûr limitée par les réglementations locales. En Europe, cette puissance est limitée à 35,16 dBm (soit 3,28 W) alors qu'aux États-Unis, elle est limitée à 36 dBm (soit 4 W).

Cette puissance diminue avec le carré de la distance ce qui fait qu'elle perd 6 dB/octave. La sensibilité du tag correspond à la puissance minimum qu'il lui faut récupérer afin de pouvoir fonctionner. Avec les tags actuellement sur le marché, cette valeur est de l'ordre de -15 à -20 dBm. Par construction graphique, on déduit facilement la distance maximum jusqu'à laquelle le tag sera télé-alimenté. Comme nous l'avons vu précédemment, une fois alimenté, le tag sera capable de rétrodiffuser plus ou moins de puissance vers l'interrogateur. La différence entre la puissance reçue par le tag et la puissance réémise vers le lecteur est appelée **efficacité de rétrodiffusion**. Par définition, cette valeur est au minimum de 6 dB (cf. valeurs de K dans le tableau 2). Le signal rétrodiffusé par le tag parcourt à nouveau la distance qui le sépare du lecteur. Il est donc à nouveau atténué par la même valeur que lors du trajet aller. On en déduit donc graphiquement la valeur de P_{Rx} , puissance maximum que peut capter l'antenne de l'interrogateur. Cette puissance est à comparer avec la sensibilité du lecteur (typiquement comprise entre -75 et -95 dBm). Dans le cas de la figure 12, on s'aperçoit que la puissance P_{Rx} est supérieure à la sensibilité du lecteur. Il est donc fort probable que le lecteur soit capable de détecter le signal retour provenant du tag et que la communication puisse s'établir.

Nota : la sensibilité du lecteur n'est pas la seule valeur impactant la capacité d'un interrogateur à détecter et à communiquer avec un tag. Il faut également prendre en compte le rapport signal à bruit à l'entrée de l'interrogateur et la capacité du tag à rétromoduler des puissances différentes pour coder les informations qu'il doit envoyer au lecteur.

Dans le cas de la figure 12, on peut donc dire que la distance maximale de fonctionnement est limitée par les performances du tag. Dans l'exemple de la figure 13, ce sont les performances du lecteur qui limitent la distance maximale de fonctionnement. En effet, si l'on place le tag à sa distance maximale de télé-alimentation, on s'aperçoit aisément que la puissance du signal retour sera inférieure au seuil de sensibilité du lecteur et que, par conséquent, il sera incapable de détecter le signal du tag.

Les schémas des figures 12 et 13 peuvent être plus détaillés et faire intervenir les autres phénomènes d'atténuation afin d'évaluer

plus précisément les distances de fonctionnement. Il est également important de connaître comment le tag se comporte en fonction de la puissance qu'il reçoit. En effet, l'impédance équivalente de la puce RFID n'est pas constante et varie en fonction, entre autres, de la puissance appliquée à ses bornes. L'adaptation entre la puce RFID et son antenne n'est donc pas constante et dépend de la puissance rayonnée par le lecteur et/ou de la distance qui sépare le lecteur du tag. Par conséquent, l'efficacité de rétro-modulation n'est donc pas une grandeur constante et sa variation doit être prise en compte pour modéliser au mieux le système RFID.

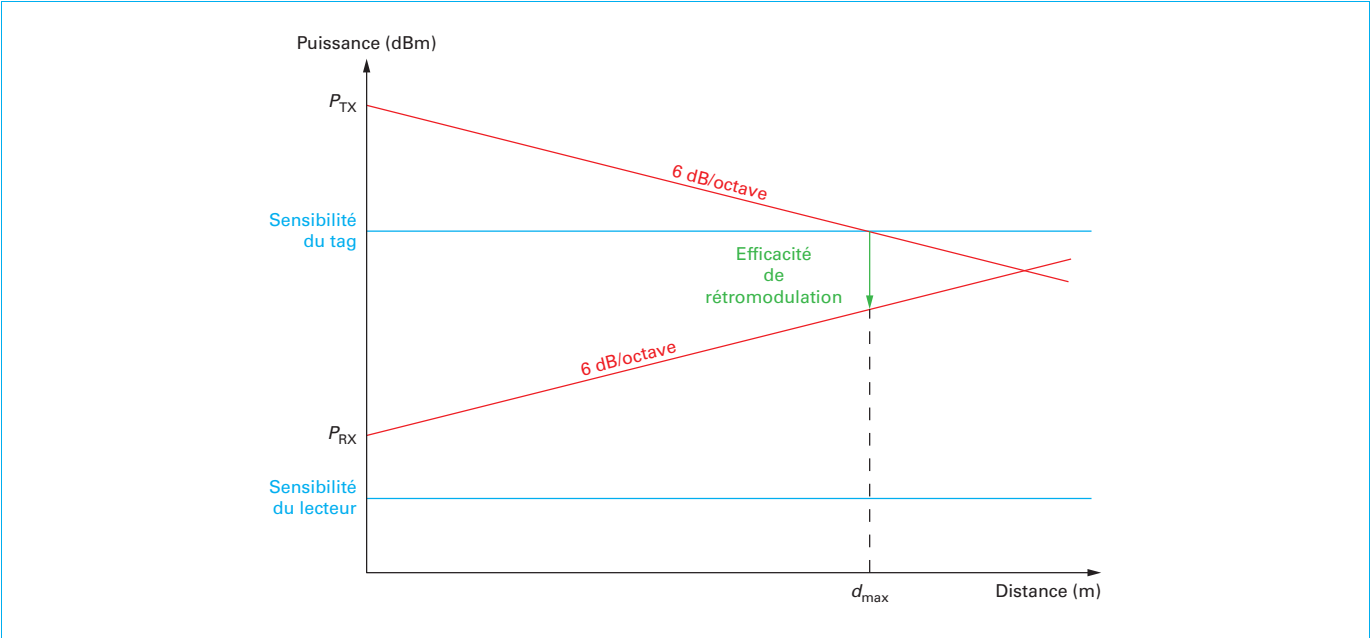


Figure 12 – Schéma des bilans de puissance en RFID UHF (limitation par le tag)

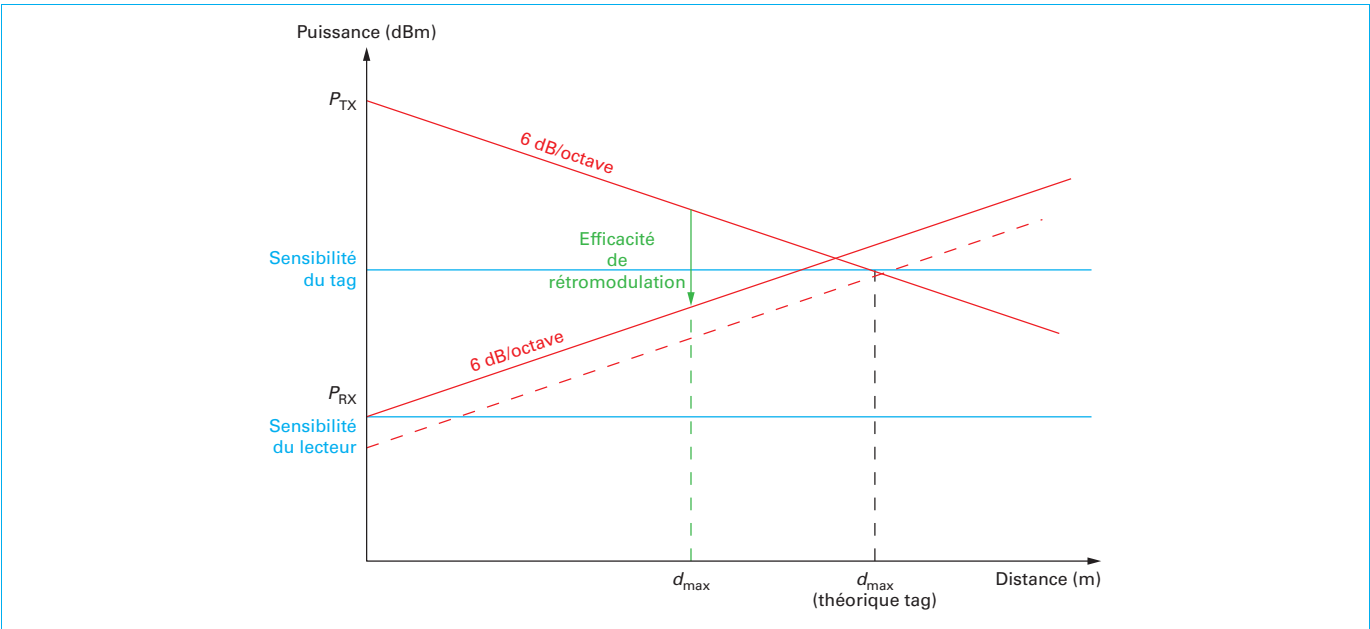


Figure 13 – Schéma des bilans de puissance en RFID UHF (limitation par le lecteur)

3.5 Architectures des interrogateurs en UHF

Comme pour tout système de communication radio, un lecteur RFID UHF est principalement composé d'un émetteur RF, d'un récepteur et d'un système antenne. Pour le côté émetteur RF, ses principales caractéristiques sont :

- sa stabilité. L'émetteur doit moduler un signal RF (porteuse) avec un signal en bande de base (commande à envoyer aux tags) et maintenir la porteuse à la fréquence souhaitée ;
- son efficacité énergétique. L'émetteur doit pouvoir fournir un signal RF sinusoïdal à la puissance souhaitée sans trop consommer d'énergie (surtout pour les lecteurs portables alimentés sur batterie) ;
- son faible rayonnement parasite. Toute distorsion du signal sinusoïdal transmis peut conduire à des émissions RF en dehors des bandes autorisées par les réglementations (§ 7). Il faut souvent trouver un compromis entre la puissance de signal RF, la consommation du lecteur et le faible rayonnement parasite.

Pour ce qui concerne le récepteur, les caractéristiques principales sont :

- sa sensibilité. Le récepteur doit être capable de détecter et décoder des signaux de très faible amplitude provenant des tags. La limite ultime de la sensibilité radio est le bruit thermique dont la densité spectrale est kTB . Dans cette équation, k est la constante de Boltzmann ($1,38064852 \cdot 10^{-23} \text{ m}^2 \cdot \text{kg} \cdot \text{s}^{-2} \cdot \text{K}^{-1}$), T est la température en Kelvin et B est la bande passante du récepteur. Dans une largeur de bande de 1 MHz, le bruit thermique à température ambiante est d'environ -114 dBm, soit environ $4 \cdot 10^{-15}$ Watt. Cette puissance est beaucoup plus faible que la puissance du signal reçu d'un tag UHF passif (entre -50 et -65 dBm typiquement). Dans de nombreux cas, la communication RFID est limitée par la télé-alimentation (bien que cela soit de moins en moins vrai avec la baisse de consommation des tags, cf. § 3.4). La sensibilité du récepteur est donc une caractéristique moins importante que dans de nombreux autres systèmes de communication radio. Dans le cas des tags BAP, la liaison tag vers lecteur devient le facteur limitant et une bonne sensibilité de réception est d'une importance primordiale ;

– sa dynamique de puissance d'entrée. Le même lecteur doit recevoir et interpréter les signaux de tags situés à 30 cm comme de ceux situés à plusieurs mètres. Les figures 12 et 13 montrent que ces puissances peuvent varier d'un facteur 10^4 , voire plus.

Les lecteurs RFID doivent fonctionner en mode duplex puisqu'ils doivent continuellement émettre un signal RF pour que les tags soient alimentés et qu'ils puissent communiquer en rétromodulant ce signal RF. Le problème est que la fréquence du signal reçu par le lecteur est la même que celle du signal émis. Les fuites entre l'étage d'émission et celui de réception peuvent constituer une limite importante à la capacité du lecteur à détecter et décoder les réponses des tags et ce, même si la puissance de ces signaux est supérieure à la sensibilité du lecteur. Pour pallier ce problème, deux architectures peuvent être utilisées.

La première méthode consiste à utiliser des antennes séparées pour transmettre le signal du lecteur et recevoir le signal du tag. Cette configuration est connue sous le nom de **bistatique**. Une telle configuration peut garantir qu'une très faible partie du signal émis sera captée par le récepteur. Encore faut-il que les antennes soient correctement positionnées et qu'aucun obstacle proche de l'antenne d'émission ne vienne réfléchir le signal vers l'antenne de réception. De plus, l'utilisation de deux antennes implique que l'on ait suffisamment de place. Elle est donc très difficile à mettre en œuvre pour des lecteurs portables. Une autre solution consiste à utiliser une seule antenne pour l'émission et la réception. On parle alors de **configuration monostatique**. Dans ce cas, le signal de forte puissance issu de l'émetteur doit être séparé de celui provenant des tags par la mise en place d'un circulateur. Ces deux configurations sont résumées dans la figure 14.

La télé-alimentation des tags RFID est basée sur des principes de transferts de puissance radio. Il faut bien différencier les systèmes RFID fonctionnant principalement en champ proche (systèmes LF et HF) de ceux fonctionnant plutôt en champ formé (systèmes UHF et SHF).

Pour les systèmes LF et HF, le couplage entre lecteur et tag(s) est magnétique et les antennes sont basées sur des boucles

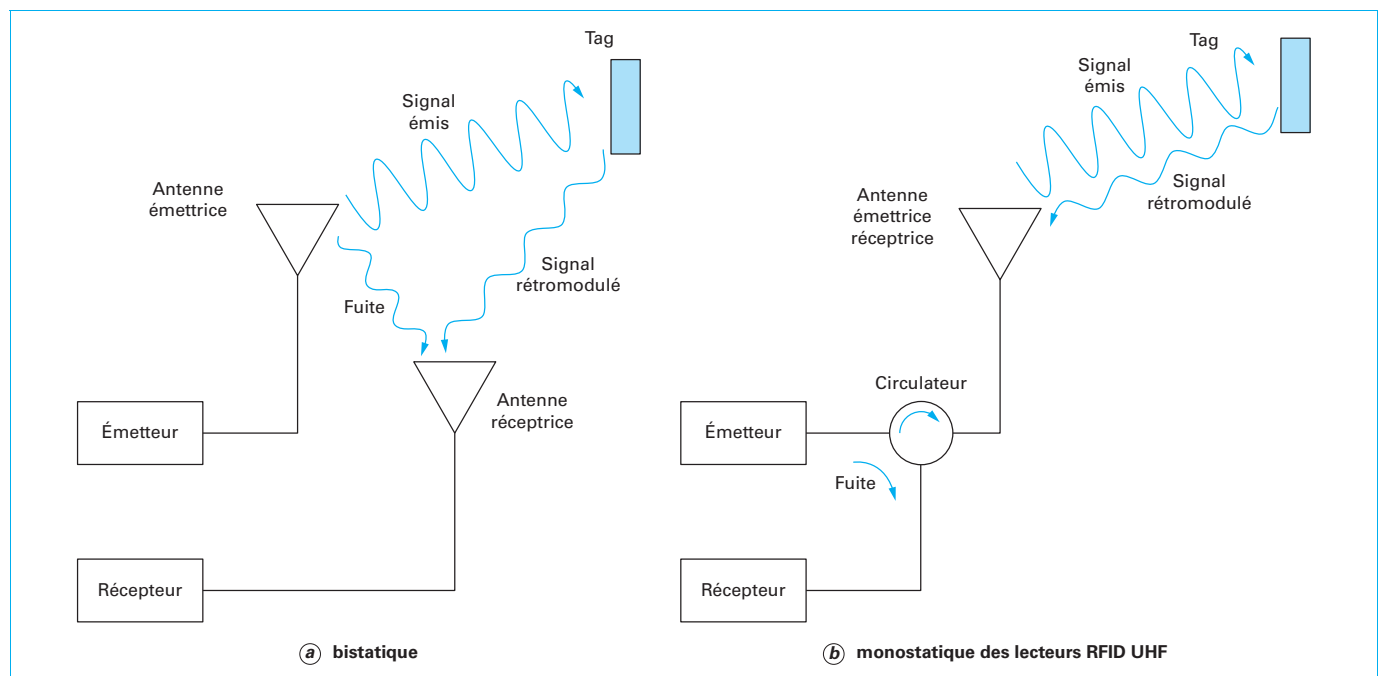


Figure 14 – Architecture a) bistatique et b) monostatique des lecteurs RFID UHF

inductives. Les équations permettant d'évaluer les transferts d'énergie sont basées sur celles des oscillateurs couplés.

Pour les systèmes UHF et SHF, le transfert d'énergie se fait à travers une onde électromagnétique. Les caractéristiques principales des antennes sont le gain, la directivité et l'efficacité de rayonnement. La formule de Friis permet d'avoir une bonne approximation des bilans d'énergie.

Comme pour tous les systèmes basés sur les radiofréquences, les systèmes RFID sont très sensibles aux phénomènes d'adaptation d'impédance. Il s'agit le plus souvent de trouver un compromis entre distance de télé-alimentation et capacité à détecter et décoder le signal retour.

4. Communication et codage des informations

Une fois les circuits des étiquettes RFID alimentés (par télé-alimentation de l'interrogateur ou en technologie « batterie assistée »), il s'agit de s'intéresser à la manière dont les informations vont être adaptées au canal de transmission pour être transmises de l'interrogateur vers le(s) tag(s) (liaison montante ou *uplink* en anglais) ou d'un tag vers l'interrogateur (liaison descendante ou *downlink* en anglais).

Il est utile de faire la distinction entre la modulation et le codage de l'information. Le codage correspond à la manière de représenter l'information à transmettre. Cette information est une suite de « 0 » et de « 1 » logiques. Du fait des faibles ressources de traitement dans les puces de tags RFID, les codes utilisés restent simples et n'emploient pas, jusqu'à présent, de mappings complexes. Les codes utilisés doivent donc représenter chaque bit logique de manière isolée. Les regroupements sous forme de symboles de 2, voire 3 bits (comme dans les modulations complexes I/Q) ne sont pas d'actualité. La modulation est la manière dont l'information sera portée par le signal radiofréquence (variation d'amplitude, de phase ou de fréquence, combinaison de ces paramètres). Contrairement à ce que l'on peut trouver dans les systèmes de télécommunication pair à pair, les systèmes RFID prévoient des différences de modulation et de codage suivant le sens (*uplink* ou *downlink*) dans lequel la transmission s'effectue. Ceci est principalement dû au fait que l'interrogateur doit continuer d'émettre un signal radiofréquence lorsque le tag communique (systèmes télé-alimentés), et que le tag ne peut que rétromoduler ce signal (systèmes passifs) pour transmettre de l'information. D'autre part, les niveaux de puissance mis en jeu sont si différents que les contraintes réglementaires ne sont pas ressenties de la même manière par les interrogateurs que par les tags.

4.1 Modulations en RFID

Comme pour tout système de télécommunication, les modulations employées en RFID sont basées sur les modulations d'amplitude et de phase. Le choix d'un type particulier de modulation va dépendre de plusieurs paramètres : la bande passante disponible pour la communication, le débit d'information souhaité, le rapport signal à bruit ou signal à interférence attendu dans le canal de transmission et, enfin, la complexité tolérée des systèmes d'émission et de réception. Au risque de nous répéter, les systèmes RFID (surtout les tags) ne disposent que de peu de ressources pour détecter et décoder les signaux. D'autre part, les réglementations auxquelles les systèmes RFID doivent se conformer ne laissent que peu d'espace spectral. Enfin, cet espace fait généralement partie des bandes de fréquence dites « ISM (Instrumentation Scientifique et Médicale) » non soumises à licence et qu'il faut donc partager avec d'autres systèmes de communication à courte portée (appelés SRD-NS pour *Short Range Devices Non Specific*). Les modulations

simples et robustes seront donc préférées à celles plus efficaces au niveau spectral mais au prix d'une complexité plus importante et parfois d'une plus grande sensibilité aux bruits ou interférences.

Dans la communication *uplink* (de l'interrogateur vers l'étiquette), la modulation d'amplitude est largement répandue car elle est simple à mettre en œuvre tant au niveau de l'émetteur qu'au niveau du récepteur et qu'elle est assez peu gourmande en termes de bande passante. La question qui se pose est de savoir comment choisir le meilleur indice de modulation. Le schéma de la figure 15 montre les représentations temporelles et fréquentielles de signaux modulés en amplitude avec 10 et 100 % d'indice de modulation. La mesure de l'indice de modulation d'un signal modulé en amplitude est donnée par l'équation (17). Pour comparaison, la profondeur de modulation est donnée par l'équation (18).

$$mi = \frac{A_{max} - A_{min}}{A_{max} + A_{min}} \quad (17)$$

$$md = \frac{A_{max} - A_{min}}{A_{max}} \quad (18)$$

Un signal modulé à 10 % présente de faibles variations d'amplitude propices à la télé-alimentation de la puce électronique du tag. Par contre, les lobes secondaires, porteurs de l'information, sont 23 dB sous le niveau du signal radiofréquence porteur. Cet écart peut être préjudiciable pour le bon décodage de l'information par le tag. Dans le cas d'un signal radiofréquence modulé en amplitude avec un indice de 100 % (modulation OOK *On-Off Keying*), il est clair que la porteuse est régulièrement coupée. Ceci implique que l'étiquette doit pouvoir « survivre » à ces coupures d'alimentation. Il faut donc prévoir un système de stockage d'énergie particulier. Avec ce type de modulation, le choix du code représentant les « 1 » et « 0 » logiques aura son importance. Imaginons un instant l'association d'une telle modulation avec un code NRZ pour lequel un « 0 » est représenté par un état bas. Une suite de « 0 » consécutifs aurait pour effet de couper un long moment la porteuse et donc l'alimentation du tag. Aucun système de stockage d'énergie ne pourrait prévoir telle pénurie. Il faudra donc associer cette modulation à des codes limitant au maximum le nombre de coupures (consécutives).

Au-delà des aspects concernant la robustesse de la modulation utilisée et la facilité de démodulation du signal par le tag, il est important d'intégrer, dans le choix de l'indice de modulation, les contraintes liées à la réglementation. La figure 16 représente la comparaison d'un signal issu d'un lecteur RFID HF avec le gabarit spectral que doivent respecter les signaux radiofréquences pour des communications centrées sur 13,56 MHz (Norme ETSI 300-330, § 7).

La norme ISO/IEC 18000-3 mode 1 (HF) laisse le choix à l'interrogateur de fixer l'indice de modulation (mi) à 10 ou 100 %. L'étiquette, si elle se veut conforme à cette norme, se doit de pouvoir décoder l'information quel que soit l'indice utilisé. En ce qui concerne les normes UHF, l'ISO/IEC 18000-61 (mode A) propose des profondeurs de modulation (md) variant de 18 à 100 %, l'ISO/IEC 18000-62 (mode B), comme précédemment en HF, impose un choix au départ : 10 ou 100 %. Enfin, l'ISO/IEC 18000-63 (mode C, équivalent à l'EPC Gen2v2) impose une profondeur comprise entre 82 et 100 %.

Une autre manière de transporter l'information sur une porteuse radioélectrique est de modifier sa phase au rythme des données à transmettre. Dans la grande majorité des cas, une modulation de phase (ou de fréquence) occupe, pour un même débit, plus d'espace spectral qu'une modulation d'amplitude. Les bandes de fréquence utilisables par la RFID étant assez étroites (quelques kHz à quelques centaines de kHz suivant les fréquences), il convient donc de réduire l'indice de modulation de phase à son strict minimum. La contrepartie à un encombrement spectral plus important est la meilleure robustesse aux bruits et interférences [8]. La norme ISO/IEC 18000-3 mode 2 (HF) met en œuvre une modulation de

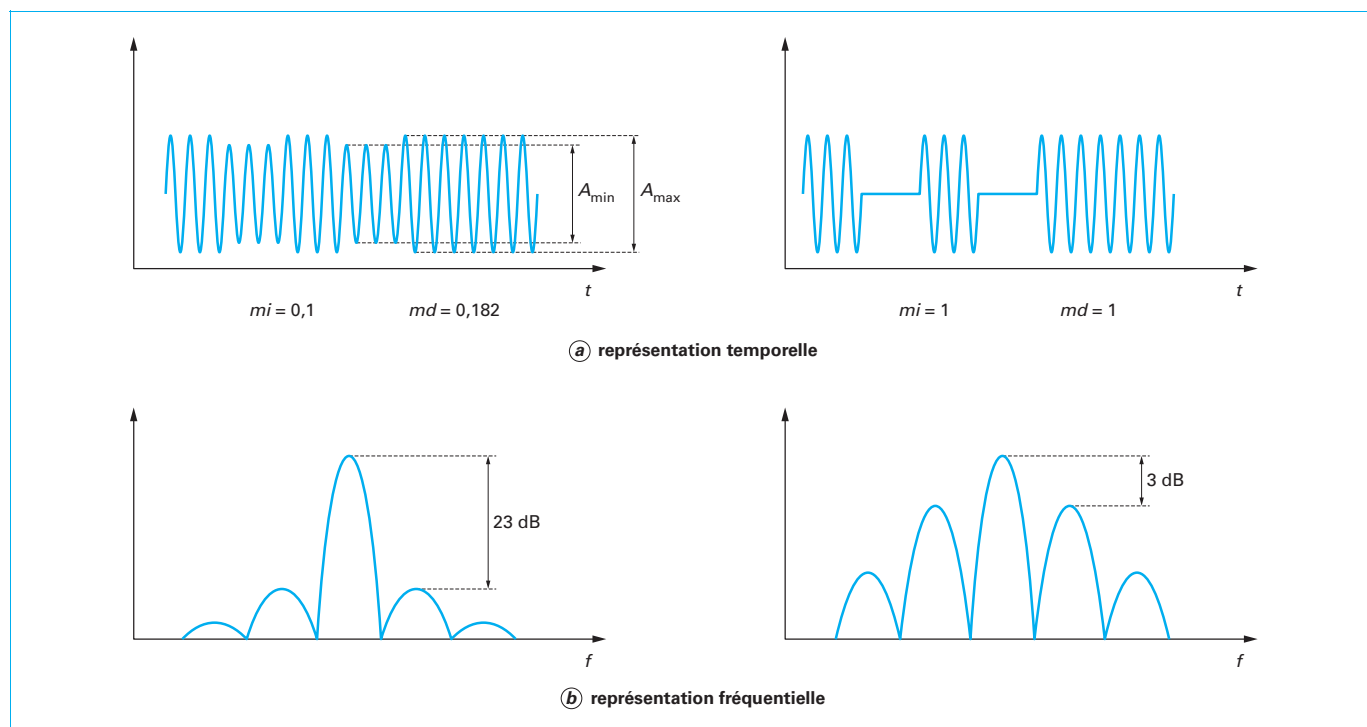


Figure 15 – Allures des représentations temporelle et spectrale de signaux modulés en amplitude

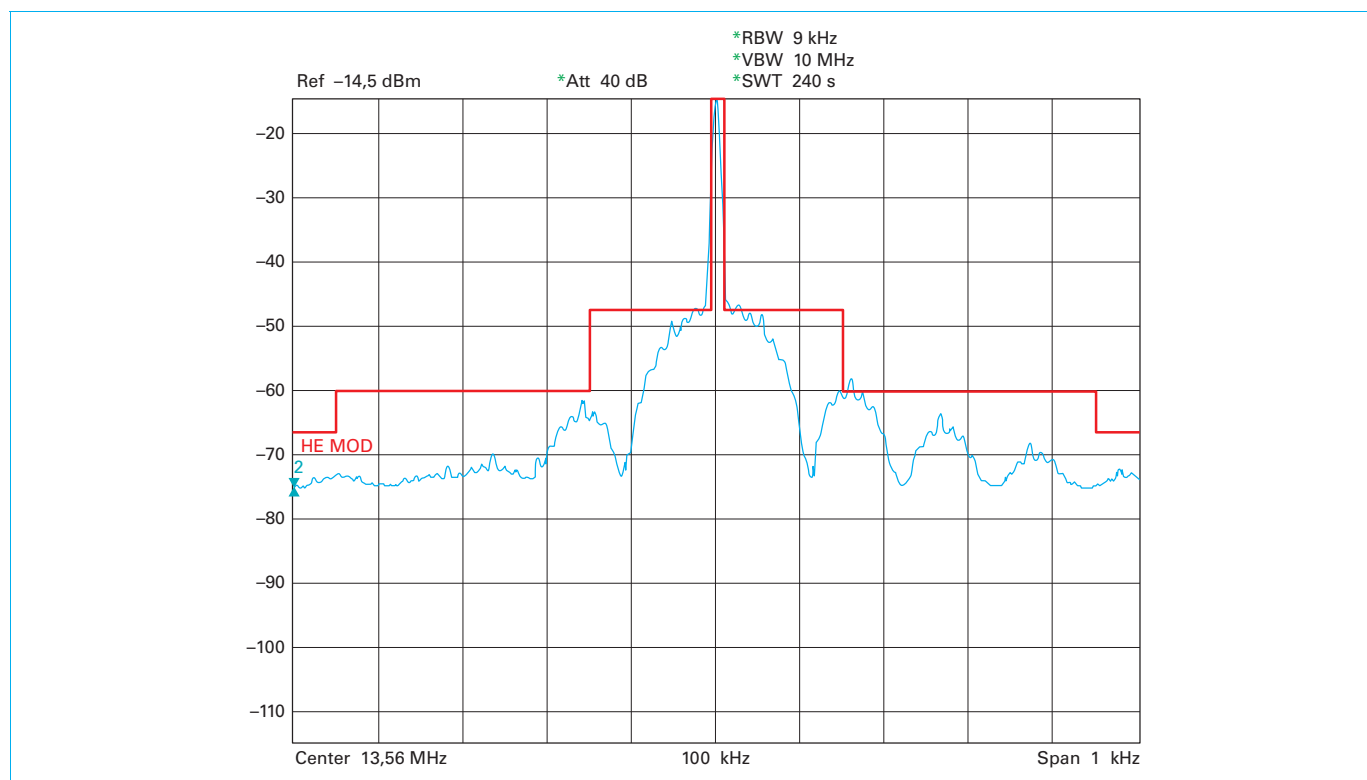


Figure 16 – Comparaison du spectre du signal émis par un lecteur RFID HF (courbe bleue) avec le gabarit de régulation ETSI 300-330 (courbe rouge)

phase appelée PJM (*Phase Jitter Modulation*). L'excursion en phase est réduite à plus ou moins 4 degrés maximum ce qui permet de réduire le spectre utilisé. Il s'agit en fait de la superposition d'un signal de référence et d'un signal en quadrature de très faible amplitude. Le principal avantage de cette modulation est qu'elle présente une enveloppe constante réglant ainsi le problème de la télé-alimentation vis-à-vis du codage employé. Bien qu'il ne s'agisse pas dans ce cas d'un problème lié à la télé-alimentation, la norme ISO/IEC 18000-7 (433 MHz) pour les systèmes RFID actifs (dont les tags embarquent généralement leur propre source d'énergie), impose l'utilisation d'une modulation de fréquence (FSK *Frequency Shift Keying*) présentant une excursion en fréquence de plus ou moins 50 kHz.

En ce qui concerne la communication *downlink*, le cas des étiquettes actives peut être soumis au même traitement que lors de la communication *uplink*. Les signaux générés par le(s) tag(s) doivent satisfaire aux mêmes exigences vis-à-vis des régulations locales (FCC, ETSI, etc.) en puissance comme en encombrement spectral. Pour les systèmes passifs LF ou HF, la variation d'impédance interne du circuit électronique du tag crée une variation de charge vue par l'interrogateur. La variation d'impédance interne du circuit électronique est réalisée par commutation de charge (passive ou réactive) placée entre les connexions destinées à l'antenne. Dans le cas des systèmes à couplage inductif, la modification de l'impédance interne du circuit électronique change le coefficient de qualité du tag. Si l'impédance commutée est résistive, le tag présentera un coefficient de qualité plus ou moins important sans que sa fréquence de résonance ne soit modifiée. Si l'impédance commutée est réactive, la modification de la fréquence de résonance qui en résultera impliquera une modification du coefficient de qualité. Grâce au schéma de la figure 9, il est possible de calculer le coefficient de qualité du système en fonction des divers coefficients de qualité de l'antenne du tag, de la puce électronique et de l'interrogateur. Cette relation est donnée par l'équation suivante :

$$Q_{int} = \frac{Q_{ant-int}}{1 + Q_{ant-int} Q_{tag} k^2} \quad (19)$$

Dans cette relation, $Q_{ant-int} = \frac{L_1 \omega}{R_1}$ est le coefficient de qualité de l'antenne de l'interrogateur, ω est la pulsation du signal RF ($\omega = 2\pi f$), k est le coefficient de couplage et $Q_{tag} = \frac{Q_{puce} Q_{ant-tag}}{Q_{puce} + Q_{ant-tag}}$ est le coefficient de qualité du tag. Ce coefficient de qualité dépend du coefficient de qualité de la puce $Q_{puce} = R_{ic} C_2 \omega$ et de celui de l'antenne du tag $Q_{ant-tag} = \frac{L_2 \omega}{R_2}$. Toute modification de Q_{puce} entraîne donc une modification de Q_{int} et donc de la tension vue aux bornes de l'antenne de l'interrogateur.

Dans le cas des systèmes à couplage électromagnétique (en UHF et SHF), l'équation (12) peut être utilisée pour évaluer la puissance réfléchie par le tag et captée par l'antenne de l'interrogateur. Il s'agit alors de l'équation typique des radars :

$$\frac{P_{ant-int}}{P_{int}} = G_{int} \frac{1}{4\pi d^2} \sigma \frac{1}{4\pi d^2} \Sigma_{int} = \frac{G_{int}^2 \lambda^2 \sigma}{(4\pi)^3 d^4}$$

Cette équation donne le rapport entre la puissance réfléchie par le tag captée au niveau de l'antenne de l'interrogateur ($P_{ant-int}$) et la puissance incidente appliquée par le générateur à l'antenne de l'interrogateur (P_{int}). Ce rapport fait apparaître la surface équivalente radar du tag RFID, σ (en m²), encore appelée en anglais *Radar Cross Section* ou RCS. Dans le cas des antennes de type dipôle, cette surface peut être reliée au gain de l'antenne du tag et au coefficient de re-rayonnement K , donné par l'équation (16) :

$$\sigma = \frac{K}{4\pi} \lambda^2 G_{tag}^2$$

Comme pour les systèmes RFID inductifs, la commutation d'une charge en parallèle de la puce électrique va modifier l'amplitude et la phase du signal rétrodiffusé par le tag, ce qui implique des variations de tension vues au niveau de l'interrogateur.

Quelles que soient les fréquences, les tags RFID doivent faire en sorte de commuter des charges particulières pour maximiser les variations de tension induites au niveau de l'interrogateur. Les charges optimales (d'un point de vue mathématique) sont bien sûr le circuit ouvert et l'impédance purement réactive de valeur opposée à la réactance de l'antenne. Dans les deux cas, ces charges compromettent la télé-alimentation de la puce puisque le coefficient de transmission est égal à 0 dans les deux cas. Tout l'art du concepteur de circuit intégré sera de choisir les charges permettant d'observer une variation maximale de signal au niveau de l'antenne de l'interrogateur sans pénaliser la télé-alimentation. Une étude complète sur le choix optimal des charges à commuter peut être trouvée dans les références [1] et [3]. Dans tous les cas, les variations consécutives à ces commutations de charge peuvent être assimilées, au niveau de l'interrogateur, à une modulation d'amplitude de très faible indice (de l'ordre de quelques pourcents dans le meilleur des cas).

Les modulations utilisées dans les systèmes RFID doivent être simples et robustes.

Pour les modulations des communications lecteur vers tag, il faut veiller à :

- respecter les gabarits d'émissions radiofréquences généralement à bande étroite ;
- simplifier la démodulation par les tags afin de ne pas augmenter leur coût.

Pour les modulations tag vers lecteur, les solutions sont basées sur la commutation de charge (résistive ou réactive). Il faut donc trouver un compromis entre puissance rétromodulée (pour une meilleure détection par le lecteur) et qualité de la télé-alimentation.

4.2 Codes utilisés en RFID

Dans un système de communication, le code est la manière de représenter les informations élémentaires. Il s'agit généralement d'états logiques (bits) comme le « 1 » ou le « 0 » ou de groupes de bits (symboles). Le codage peut faire intervenir des notions de niveau (haut/bas, on/off) d'une grandeur physique ou des notions de transition d'un état à un autre (bas vers haut, haut vers bas, 0° vers 180° ou 180° vers 0°, etc.). Ces niveaux ou ces transitions sont appliqués à l'amplitude ou la phase d'un signal porteur sinusoïdal suivant la modulation qui aura été choisie.

Le choix d'un codage particulier va dépendre des perturbations attendues lors de la transmission du signal entre émetteur et récepteur et de la technologie que l'on peut mettre en œuvre (contrainte de coût ou de surface silicium disponible). Il va également dépendre de l'encombrement spectral du signal et des techniques à mettre en œuvre pour coder et décoder les informations. En RFID, nous avons insisté sur le fait que, pour les systèmes passifs, les communications *uplink* et *downlink* ne sont pas équivalentes. Il est également important de noter que pour des raisons principalement de coûts et de consommation énergétique, les interrogateurs peuvent embarquer des technologies plus complexes et efficaces que les tags. Enfin, il est plus probable que plusieurs tags se trouvent face à un seul interrogateur que le contraire. Il faudra certainement prévoir des manières de coder l'information provenant des tags de manière à distinguer le fait que plusieurs tags communiquent en même temps. Nous devons donc choisir, parmi les solutions proposées dans les différents standards, les codages les plus pertinents pour la liaison montante et pour la liaison descendante.

4.2.1 Codes dans la communication *uplink*

Pour les systèmes RFID télé-alimentés, le code et sa modulation associée devront permettre une gestion efficace de l'énergie. Par exemple, dans le cas d'une modulation d'amplitude ayant un indice de 100 %, un code NRZ ayant un état logique « 0 » bas, impliquera une coupure de la porteuse durant 50 % du temps (dans le cas où la présence de « 1 » et « 0 » dans le message est équiprobable). Cette association code/modulation n'est donc pas la meilleure pour une communication *uplink*. Une deuxième caractéristique des codes est la présence régulière (ou non) de transitions dans une suite aléatoire de « 0 » et de « 1 ». Dans les communications montantes, le nombre de transitions doit être maximal afin de permettre au tag de se synchroniser facilement (sans devoir mettre en œuvre des circuits électroniques trop évolués). Une troisième caractéristique des codes utilisés dans la communication de l'interrogateur vers le tag concerne le respect des réglementations des émetteurs radiofréquences. Tout en gardant un rapport signal à bruit suffisant pour une communication de bonne qualité, le couple code/modulation devra se conformer aux gabarits énoncés dans les normes internationales.

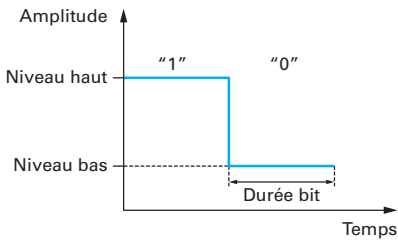
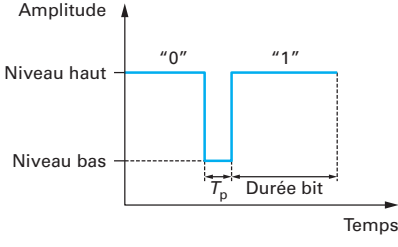
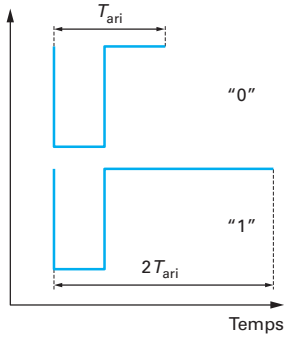
Le tableau 3 résume les principaux codes que l'on peut rencontrer dans les systèmes RFID.

4.2.2 Codes dans la communication *downlink*

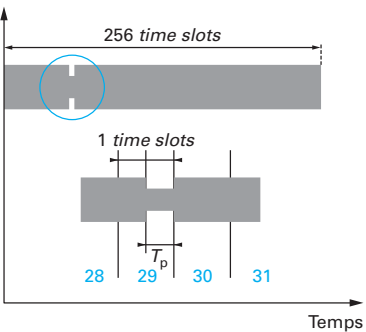
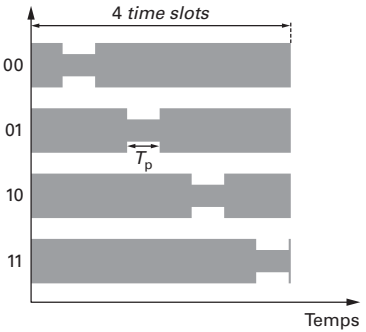
Dans le cas des systèmes passifs sans source d'énergie embarquée dans le tag RFID, les codes utilisés dans la liaison *downlink* devront être simples à mettre en œuvre et l'électronique permettant leur utilisation ne devra pas consommer trop d'énergie. Que l'on soit en HF ou en UHF, les puissances rétro-modulées sont si faibles que la conformité des signaux aux gabarits des normes de régulation n'est pas une contrainte majeure. Par contre, les codes utilisés devront présenter un nombre important de transitions afin d'atteindre un rapport signal à bruit suffisant pour leur détection par un interrogateur. Le tableau 4 résume les principaux codes utilisés en RFID dans les liaisons descendantes.

Dans les communications descendantes, les systèmes RFID peuvent également utiliser le principe de codage par sous-porteuse. Il s'agit en fait de la combinaison d'un code avec une modulation d'une fréquence multiple de la fréquence bit. Un exemple est donné

Tableau 3 – Principaux codes en liaison montante RFID

Nom	Représentation	Avantages/Inconvénients
NRZ (Non-Retour à Zéro) Durant toute la durée d'un bit, le signal reste dans un même état (haut ou bas)		<ul style="list-style-type: none"> – Peu de transitions – Faible efficacité énergétique + Simplicité
RZI coded pulse (Retour à Zéro Inversé) Un « 0 » logique est caractérisé par un niveau haut suivi par un niveau bas de durée T_p , le « 1 » logique est représenté par un niveau haut		<ul style="list-style-type: none"> – Peu de transitions – Meilleure efficacité énergétique que NRZ + Simplicité
PIE (Pulse Interval Encoding) Les « 0 » et « 1 » ont des durées différentes. Ils commencent par une impulsion		<ul style="list-style-type: none"> + 2 transitions à chaque bit + Possibilité de créer des symboles supplémentaires (<i>Start Of Frame</i> ou <i>End Of Frame</i>) – Le décodage nécessite une horloge – Le débit est variable suivant les données transférées

T_{ari} : reference time interval for a data -0 in interrogator-to-tag signalling, d'après ISO 18000-63

Tableau 3 – Principaux codes en liaison montante RFID (suite)		
Nom	Représentation	Avantages/Inconvénients
PPM (Pulse Position Modulation) 1 parmi 256 La position de l'impulsion code 8 bits		+ Efficacité énergétique optimisée – Décodage nécessite une horloge précise – Faibles débits
PPM (Pulse Position Modulation) 1 parmi 4 La position de l'impulsion code 2 bits		+ Efficacité énergétique + Débits plus élevés qu'avec le code 1 parmi 256 – Décodage nécessite une horloge

sur la figure 17 dans le cas d'un codage Manchester avec une sous-porteuse quatre fois plus élevée que la fréquence des données.

Le principal avantage de l'utilisation d'une sous-porteuse est de pouvoir translaté le spectre de l'information. Celui-ci peut donc être éloigné de la fréquence porteuse de la valeur de la fréquence sous-porteuse. Le résultat est une meilleure immunité aux bruits et un meilleur filtrage du signal par l'interrogateur. Ce type de codage s'accompagne également d'une plus grande facilité à détecter les collisions au niveau bit.

Les modulations telles que les modulations de phase (BPSK *Binary Phase Shift Keying*) ou de fréquence (FSK *Frequency Shift Keying*) peuvent alors être associées aux codes vus précédemment. Dans ce cas, ce n'est plus la présence (ou l'absence) de la sous-porteuse qui représente les niveaux des différents codes, mais la phase ou la fréquence de cette sous-porteuse. La figure 18 donne un exemple des modulations BPSK et FSK associées au codage Manchester.

Le calcul des spectres associés à l'ensemble des codes (avec ou sans sous-porteuse) est basé sur des concepts de traitement du signal que le lecteur pourra trouver dans [R 380] et [10].

Les codes utilisés dans les systèmes RFID servent à représenter les informations binaires échangées entre lecteurs et tags. Ces codes sont étroitement associés aux modulations utilisées et doivent répondre à des contraintes différentes suivant le sens de communication.

Pour les communications lecteur vers tags, il faut veiller à :

- respecter les gabarits d'émission radiofréquence ;
- trouver le meilleur compromis entre distance de communication et distance de télé-alimentation ;

– proposer des codes simples à décoder pour ne pas complexifier les puces des tags (ce qui entraînerait une augmentation du prix).

Pour les communications tag vers lecteur, il faut veiller à :

- augmenter le rapport signal sur bruit pour faciliter la détection par les lecteurs ;
- limiter le nombre de commutations de charge pour réduire la consommation du tag et augmenter la distance de télé-alimentation.

Un compromis doit être trouvé entre débit de communication, distance de télé-alimentation et taux de lecture (vitesse à laquelle les tags présents dans le champ du lecteur sont inventoriés).

5. Protocoles d'anticollision

En RFID, les collisions peuvent être classées en trois catégories :

- **collision tags vers interrogateur.** Ces collisions arrivent lorsque plusieurs tags se trouvent dans la zone éclairée par un interrogateur et tentent de répondre (simultanément) aux commandes de celui-ci ;
- **collision interrogateurs vers tag.** Dans ce cas, un tag RFID se trouve dans la zone d'interrogation de plusieurs lecteurs. Ce tag tente alors de répondre à plusieurs sollicitations qui peuvent être contradictoires. Le résultat le plus probable est que le tag devienne indétectable par les interrogateurs ;
- **collisions interrogateurs vers interrogateurs.** Il s'agit dans ce cas d'interférences « classiques » entre plusieurs émetteurs cherchant à utiliser la même ressource radio. Les méthodes permettant

Tableau 4 – Principaux codes en liaison descendante RFID

Nom	Représentation	Avantages/Inconvénients
Miller Modifié « 1 » représenté par Seq A « 0 » représenté par Seq B Tout « 0 » suivant un autre « 0 » représenté par Seq C		+ Bonne efficacité spectrale – Certaines collisions ne sont pas détectées au niveau bit
Manchester (<i>Bi-Phase Level</i>)		+ Détection des collisions au niveau bit + Transition systématique en milieu de bit
FM0 (<i>Bi-Phase Space</i>) « 0 » présente une transition au début et au milieu du bit « 1 » présente une transition au début du bit		+ Immunité aux bruits

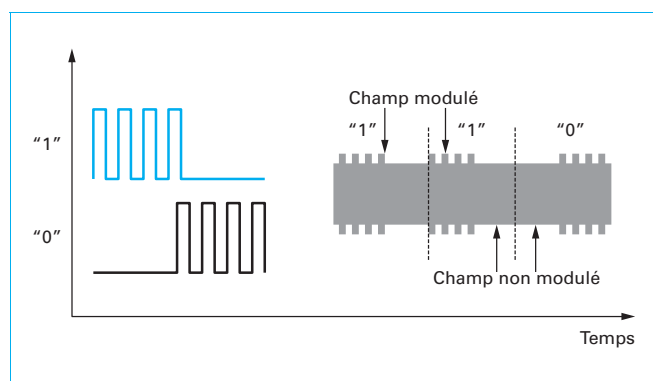


Figure 17 – Exemple de codage Manchester avec sous-porteuse (représentation des bits et du signal rétromodulé)

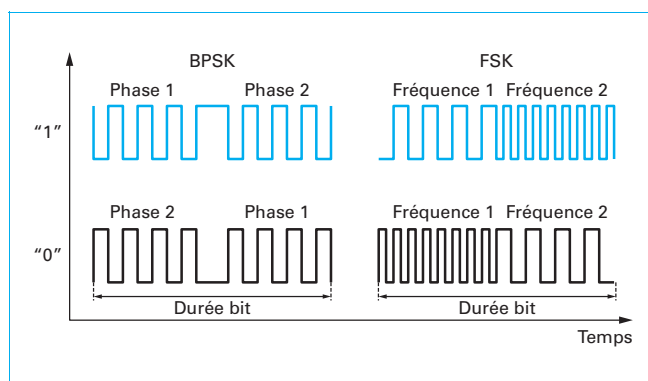


Figure 18 – Exemple de codage Manchester avec sous-porteuse avec modulation BPSK et FSK

d'éviter ce type de collision sont l'étalement de spectre (ici par saut de fréquence, FHSS ou *Frequency-Hopping Spread Spectrum* en anglais), le principe de LBT (*Listen Before Talk*) ou l'ajustement dynamique de puissance.

Dans la suite de ce paragraphe, nous nous focalisons sur les processus d'inventaire des tags (singulation) et sur la résolution des collisions tags vers interrogateur qui sont les plus fréquentes dans les applications RFID. Pour les autres types de collision, le lecteur peut se référer à [9].

Les collisions de plusieurs tags peuvent être catégorisées en deux familles d'algorithme. Les algorithmes déterministes (encore appelés algorithmes à arbres binaires de sélection) sont basés sur les numéros d'identification uniques des tags ou sur la génération d'un nombre aléatoire. Par jeu de questions/réponses entre l'interrogateur et les tags, l'interrogateur va parcourir un arbre binaire jusqu'à identification de chaque tag. D'autres algorithmes, dits « aléatoires » sont basés sur la transmission par l'interrogateur d'un nombre d'intervalles de temps (*time slots* en anglais) dans lesquels les tags choisissent de répondre de manière aléatoire.

5.1 Algorithmes déterministes

Les algorithmes déterministes sont basés sur le fait que l'interrogateur est capable de détecter une collision au niveau bit dans les réponses qu'il reçoit à une requête spécifique. Cela sous-entend que les tags répondent de façon synchrone à l'interrogateur en utilisant un codage permettant l'identification d'une collision (superposition d'un « 1 » et d'un « 0 » logique). Un exemple est souvent plus simple à comprendre qu'une longue démonstration. La figure 19 présente les étapes d'un algorithme déterministe dans le cas où trois tags sont présents dans le champ d'un interrogateur. Pour simplifier les explications, nous prenons le cas où l'identifiant d'un tag est codé sur simplement quatre bits.

Dans un premier temps, l'interrogateur demande à chaque tag présent dans le champ de répondre en envoyant son identifiant. Le résultat observé par l'interrogateur comporte des violations de code interprétées comme des collisions. L'interrogateur affine sa requête en fonction de la réponse reçue et de la position des collisions observées. Il élimine ainsi les tags qui ne répondent pas aux critères de la requête jusqu'au moment où plus aucune collision n'est observée. L'interrogateur peut alors passer en communication pair à pair avec le tag retenu. Une fois la communication terminée, l'interrogateur envoie une commande de mise en stand-by du tag (qui ne répondra plus à aucune autre requête de l'interrogateur) et reprend l'algorithme d'anticollision pour singulariser les tags restant dans le champ.

Une variante de l'algorithme déterministe consiste à parcourir l'arbre binaire bit à bit. Lorsque l'interrogateur commence l'algorithme, il demande aux tags présents dans le champ de répondre en donnant le premier bit de leur identifiant. S'il y a collision, l'interrogateur choisit de laisser le(s) tag(s) dont le premier bit est « 0 » répondre à une deuxième requête en donnant le deuxième bit de son (leur) identifiant. Le(s) autre(s) tag(s) (dont le premier bit de l'identifiant est « 1 ») reste(nt) muet(s). Le processus continue jusqu'au moment où il n'y a plus de collision. L'interrogateur remonte alors l'arbre binaire jusqu'à la dernière collision repérée et reprend l'algorithme d'anticollision. Cet algorithme est illustré sur la figure 20 avec trois tags ayant des identifiants sur trois bits : tag 1 (001), tag 2 (011), tag 3 (110).

D'autres variantes d'algorithmes déterministes peuvent être mises en place suivant la complexité de protocole que peut supporter le tag [9]. Plus le protocole sera complexe, plus le tag devra pouvoir être placé dans des états logiques différents. Il faudra donc pour cela qu'il dispose de machines d'état performantes ou de zones mémoires suffisantes et accessibles rapidement.

5.2 Algorithmes aléatoires

Tous les algorithmes d'anticollision RFID aléatoires sont basés sur l'algorithme ALOHA initialement mis au point dans les années 1970 pour gérer les connexions au réseau Internet. En RFID, l'algorithme ALOHA peut être utilisé dans un protocole ITF ou TTF. Dans les deux cas, soit après une requête de l'interrogateur (ITF), soit dès que le tag est alimenté, ce dernier choisit un temps aléatoire après lequel il transmet son identifiant. Si l'interrogateur comprend cet identifiant, il transmet au tag concerné une commande d'acquittement. Tant que les tags ne reçoivent pas cette commande, ils communiquent leur identifiant à des moments aléatoires. Cet algorithme est décrit sur la figure 21.

Un des inconvénients majeurs de l'algorithme ALOHA présenté sur la figure 23 est que les identifiants des tags, transmis à des moments aléatoires, peuvent se superposer sur de très courts instants. Cette superposition, si courte soit-elle, mène à une incompréhension des identifiants au niveau de l'interrogateur, donc à une collision. Pour pallier cet inconvénient, les systèmes RFID utilisent le plus souvent une synchronisation générée par l'interrogateur. On parle alors de « *Frame Slotted ALOHA* ». Dans cet algorithme, l'interrogateur transmet une requête aux tags présents dans le champ en indiquant un nombre d'intervalles de temps (*time slots*) dans lesquels les tags peuvent transmettre leur identifiant. Chaque tag recevant cette commande choisit un *time slot* au hasard et, en utilisant un compteur, transmet son identifiant au moment choisi. L'interrogateur vérifie dans chaque *time slot* s'il y a eu des collisions.

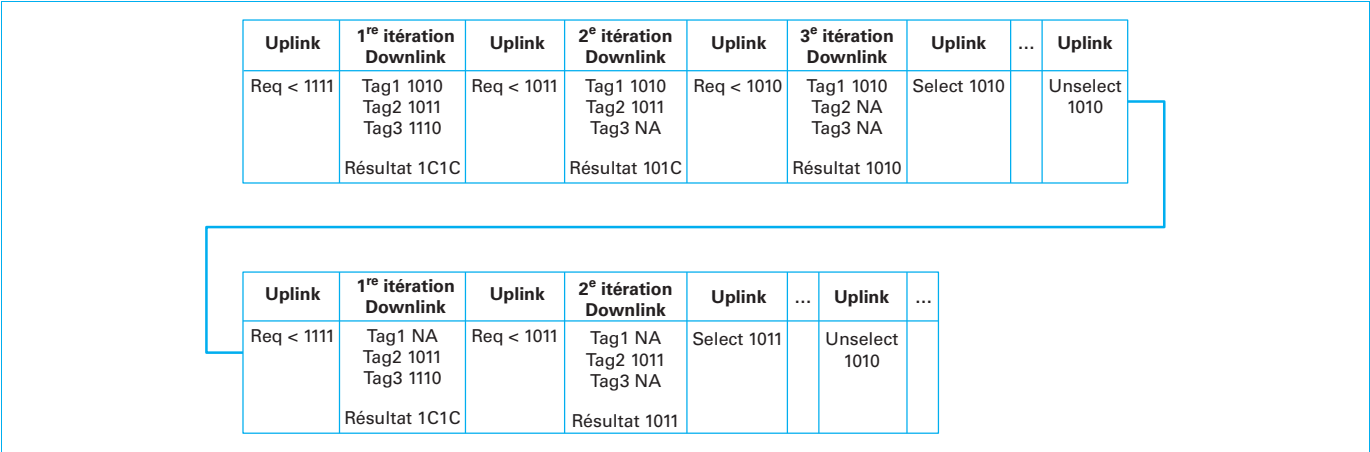


Figure 19 – Exemple de singulation déterministe

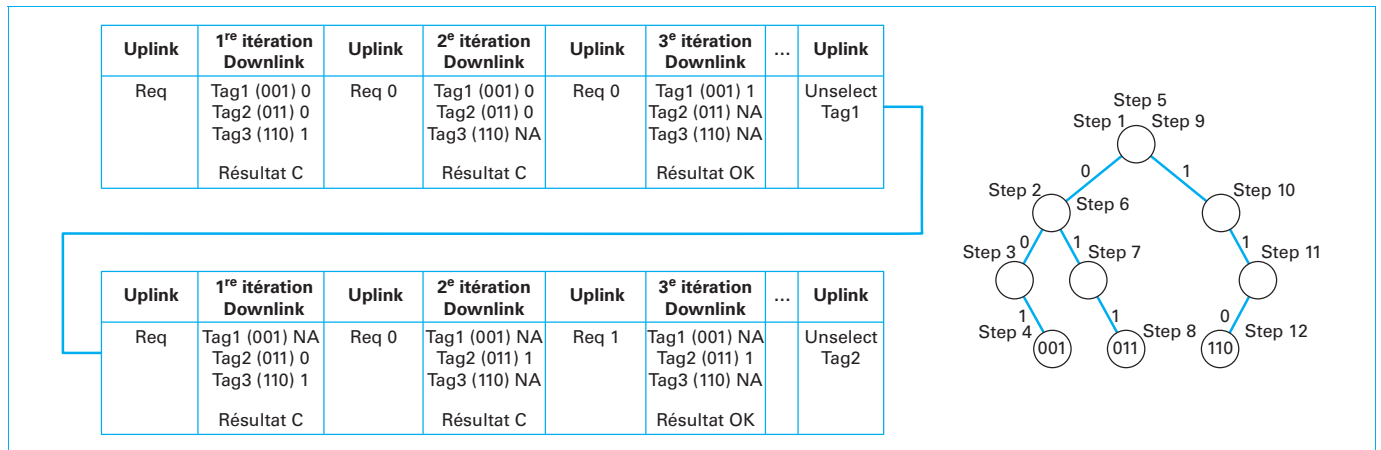


Figure 20 – Exemple de singulation déterministe bit à bit

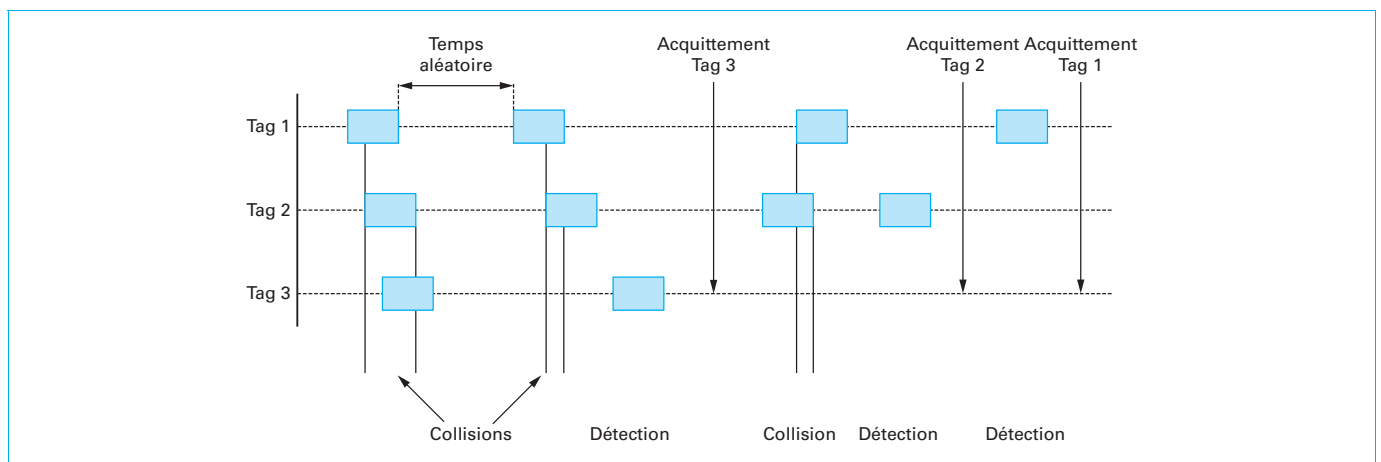


Figure 21 – Exemple de singulation aléatoire ALOHA

Dans le cas où un seul tag aurait choisi un *time slot* particulier, son identifiant est décodé et une commande d'acquiescement lui est transmise. Le processus recommence jusqu'à ce qu'il n'y ait plus aucune collision. Cet algorithme est décrit sur la figure 22.

Dans l'exemple de la figure 22, l'interrogateur propose trois intervalles de temps différents à trois tags présents dans le champ. Dans une première itération, les tags 1 et 2 répondent dans le premier *slot* amenant une collision. Le *slot* 2 est choisi par le tag 3. Il est identifié immédiatement. Le *slot* 3 reste vide. Lors d'une deuxième itération, seuls les tags 1 et 2 peuvent répondre. Ils ont à leur disposition trois *time slots* différents. Dans l'exemple, ils choisissent deux *slots* différents ce qui amène à leur identification. Bien sûr, il est possible d'imaginer qu'à chaque nouvelle itération, les tags non identifiés choisissent systématiquement le même *slot* pour répondre. Il n'y a pas de limite au nombre d'itérations et la singulation des tags peut alors devenir très longue, voire ne jamais aboutir. Le choix de nombre de *slots* proposé par l'interrogateur est alors un paramètre crucial. Il est à rapprocher du nombre de tags présents dans le champ et susceptibles de répondre à une requête d'identification. Ce nombre n'est pas forcément connu de l'interrogateur au moment de la première itération. Des algorithmes adaptatifs peuvent alors être mis en place. En fonction du nombre de collisions et du nombre de *slots* « vides », l'interrogateur adapte le nombre de *time slots* proposés d'une itération à l'autre. Un exemple d'algorithme adaptatif est présenté sur la figure 23.

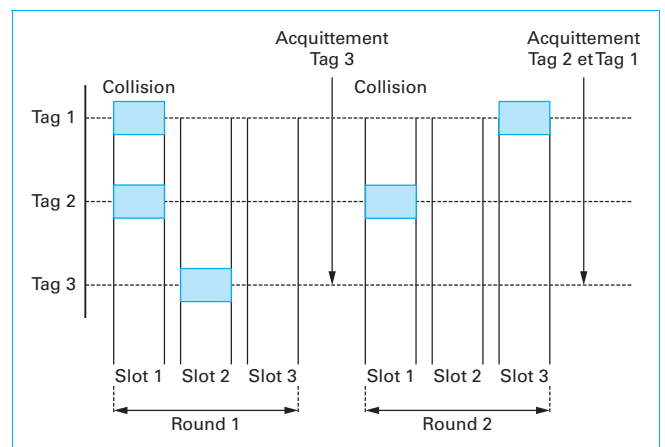


Figure 22 – Exemple de singulation aléatoire Frame Slotted ALOHA

L'adaptation du nombre de *slots* ouverts par l'interrogateur n'est pas quelque chose de normé et chaque fabricant de lecteurs utilisant cette technique propose sa propre variante en fonction des attentes et contraintes de l'utilisateur final.

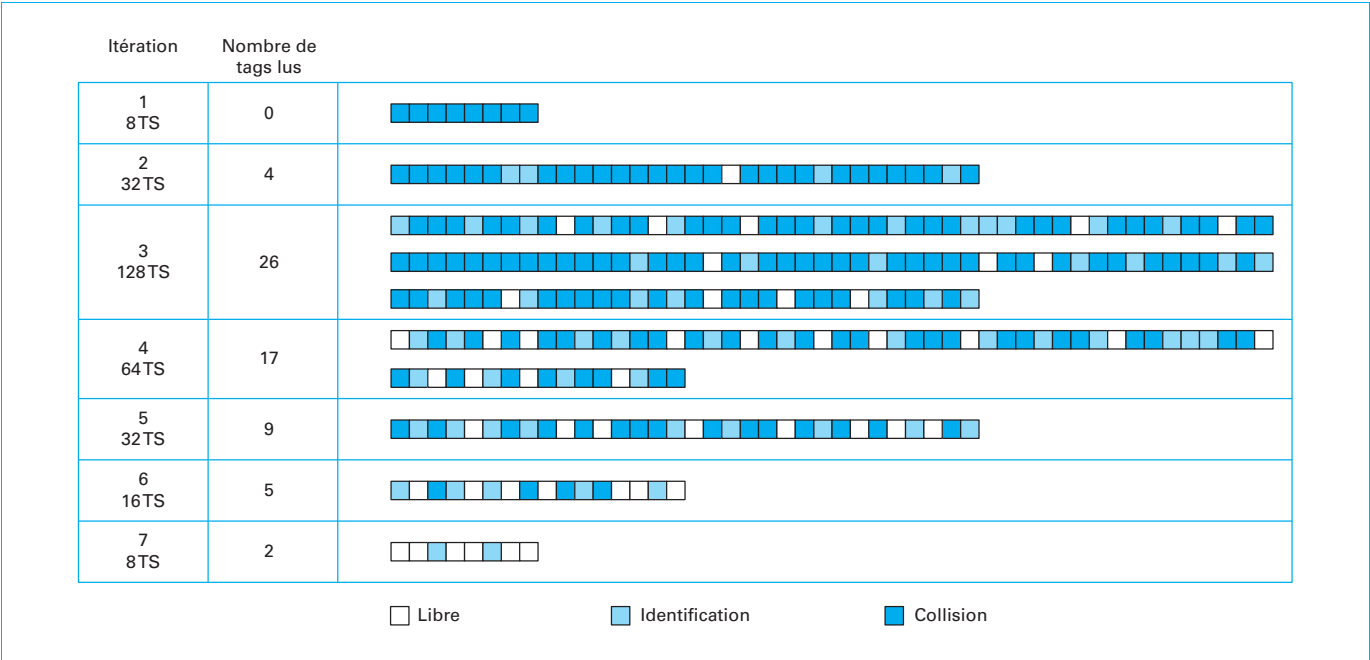


Figure 23 – Exemple de singulation aléatoire Frame Slotted ALOHA adaptatif

Enfin, qu’il soit déterministe ou aléatoire, l’algorithme de gestion des collisions doit encore prendre en compte les aspects dynamiques de la lecture d’identifiants. En effet, avant de choisir l’une ou l’autre des techniques, il faut savoir comment se comporter l’algorithme en présence de tags entrant dans le champ alors que la singulation a déjà débuté. La même question se pose lors de la sortie du champ d’un tag qui n’aurait pas pu être identifié lors d’itérations précédentes. Il est évident que les algorithmes aléatoires synchronisés se sortent mieux de ces situations que les algorithmes déterministes au prix d’un risque d’un nombre d’itérations important [9].

5.3 Cas particulier du protocole Gen2v2 (ISO/IEC 18000-63)

Parmi les différents protocoles RFID UHF standardisés, le plus utilisé, connu sous le nom de technologie RAIN et basé sur les standards ISO/IEC 18000-63 et GS1 EPC Gen2v2 (cf. § 7), a été défini pour permettre l’inventaire d’un grand nombre de tags en un minimum de temps. Pour cela, les débits de communication ont été optimisés mais la principale caractéristique de ce protocole réside dans sa manière de gérer les inventaires.

Dans les paragraphes précédents, nous avons vu que pour réaliser un inventaire des tags présents face à un lecteur, il faut que ces tags puissent, à un moment ou un autre, transmettre leur identifiant au lecteur. La question est donc de savoir comment sont construits ces identifiants et comment être sûr de leur unicité. La RFID étant, par définition, destinée à être utilisée dans de très nombreux secteurs (logistique, aéronautique, automobile, grande distribution, médical, etc.), il est inconcevable de penser que tous ces secteurs vont opter pour un même type (et surtout une même longueur) d’identifiants. Dans l’exemple de l’algorithme de singulation aléatoire présenté dans le paragraphe précédent, il faudrait donc que les *time slots* soient définis de manière à ce qu’ils puissent laisser le temps à tous les tags de renvoyer leurs identifiants. Il faudrait donc se baser sur les identifiants, les plus longs ce qui serait très pénalisant. Le protocole Gen2v2 contourne cette difficulté en imposant aux tags, non pas de renvoyer directement leurs identifiants, mais plutôt un nombre aléatoire de 16 bits appelé RN16. Ainsi,

quelle que soit la longueur de l’identifiant encodé dans les tags RFID, la longueur des *time slots* pourra être définie de manière unique pour tous les tags. Bien sûr, on peut se poser la question de la probabilité avec laquelle les tags présents dans le champ d’un lecteur pourraient « choisir » le même RN16. Cette probabilité est faible (une sur 65 536), mais pas nulle. Pour que ce soit un problème, encore faudrait-il que les deux tags ayant le même RN16 décident de répondre dans le même *time slot*. Un tel incident sera très vite détecté et résolu par le lecteur. En effet, le protocole prévoit que lorsqu’un tag est seul à répondre dans un *time slot* avec un RN16 donné (pas de collision détectée dans ce *time slot*), le lecteur envoie aussitôt une réponse à ce tag en lui demandant cette fois de renvoyer son identifiant complet. Une fois son identifiant décodé, le tag est dit « inventorié » et le lecteur peut alors passer au *time slot* suivant. Si deux tags avaient choisi de répondre dans le même *time slot* et avec, de surcroît, le même RN16, une collision aurait donc été détectée alors qu’ils renvoyaient leurs identifiants uniques.

Cette procédure est illustrée à la figure 24.

La figure 24a illustre le cas où un seul tag répond à la commande d’inventaire « Query » envoyée par le lecteur. Le RN16 est alors décodé par le lecteur qui renvoie au tag la commande « Ack » pour lui signifier la bonne réception de l’information (Acknowledgement). Le tag renvoie alors son véritable identifiant (Ull) ainsi que d’autres informations permettant au lecteur de mieux décoder cette information. La figure 24b résume les autres cas principaux que l’on peut rencontrer lors du processus d’inventaire. Le premier consiste à avoir plusieurs tags ayant choisi le même *time slot*. Plusieurs RN16 différents sont donc reçus par le lecteur qui détecte une collision. Il ne renvoie donc pas de commande « Ack » et les tags restent alors « silencieux ». À la place, le lecteur envoie une commande « QueryRep » signifiant à tous les tags que l’on passe au *time slot* suivant. Dans le cas de la figure 24b, aucun des tags participant au processus d’inventaire n’a « choisi » ce *time slot*. Le lecteur ne détecte donc aucun RN16 et passe rapidement au *time slot* suivant avec une nouvelle commande « QueryRep ». Le dernier cas illustré dans la figure 24b est celui où un tag unique renvoie son RN16 mais reste silencieux suite à la commande

« Ack ». Ceci peut venir du fait que le tag en question ne détecte pas la commande Ack ou qu'il est sorti du champ de vision du lecteur. Dans tous les cas, le lecteur passe alors au *time slot* suivant en envoyant une commande « QueryRep ». Lors d'un inventaire, d'autres cas peuvent se produire notamment si le tag supporte des commandes de capteur ou des commandes d'authentification cryptographiques. Nous invitons les lecteurs à se reporter au standard GS1/EPC Gen2v2 ou à la norme ISO/IEC 18000-63.

Nous avons vu précédemment que le nombre de *time slots* proposés aux tags lors de l'inventaire est un paramètre important et que sa valeur optimale est intimement liée au nombre de tags présents dans le champ du lecteur. Plus le nombre de tags est important, plus il faudra proposer un nombre important de *time slots*. Néanmoins, cela n'est pas la seule réponse au problème de surpopulation des tags. En effet, il faut bien comprendre que tous les tags ne répondent pas au lecteur avec la même « puissance ». Il y a donc parfois certains tags plus « faibles » ou « masqués » par d'autres qui seront détectés plus difficilement.

Pour répondre à ce type de problème, on peut alors utiliser le concept de session défini dans le protocole Gen2v2. Ces sessions vont correspondre à la manière dont les tags vont mémoriser le fait qu'ils aient été inventoriés ou non. Pour cela, il faut comprendre que les tags peuvent être inventoriés dans une session donnée indépendamment des autres sessions. Les tags possèdent 5 différents « flags » dont la valeur dépendra du fait qu'ils aient été inventoriés ou non dans une des 5 sessions disponibles.

Le tableau 5 présente les valeurs de persistance des flags en fonction de la session choisie. Par exemple, un tag inventorié durant une session S1 va conserver cette information durant un

temps compris entre 0,5 et 5 secondes qu'il soit alimenté ou non. Lorsque le lecteur relancera un inventaire dans cette même session, les tags déjà inventoriés ne participeront pas laissant ainsi plus de *time slots* disponibles aux autres tags. Ils participeront à nouveau aux inventaires lorsque leur temps de persistance sera écoulé.

Le choix d'une session particulière dépend de :

- la persistance du flag ;
- le nombre de tags présents dans le champ du lecteur ;
- la vitesse de lecture des tags (nombre de tags lus par seconde).

La session S0 est utilisée lorsque le nombre de tags est faible, c'est-à-dire quand on estime que tous les tags qui sont alimentés par le lecteur pourront être lus avant la durée maximale de temporisation réglementaire. Prenons l'exemple de 20 tags présents dans la zone de lecture avec un débit de 100 tags lus par seconde. Pour lire les 20 tags, il faut donc environ 200 ms. Ce temps est inférieur au temps d'arrêt maximum de 400 ms prévu par la réglementation américaine (Federal Communications Commission, Part. 15). Toutes les étiquettes peuvent être lues en une seule période de temps, ce qui est important car dès que le lecteur changera de fréquence, tous les tags inventoriés en session S0 seront réinitialisés. Ces tags pourront alors participer au prochain inventaire puisque leur flag S0 aura été réinitialisé. Par contre, s'il y a 50 tags présents devant le lecteur, dans les mêmes conditions que précédemment, le lecteur n'aura pas le temps de faire l'inventaire complet avant le saut de fréquence. Tous les tags seront réinitialisés lors de ce changement de fréquence. Il n'est donc pas conseillé d'utiliser cette session S0 dans ces conditions. Par contre, cela ne pose aucun problème dans le cas d'une réglementation européenne (ETSI 302-208) car elle autorise l'utilisation du canal pendant un temps maximum de 4 secondes.

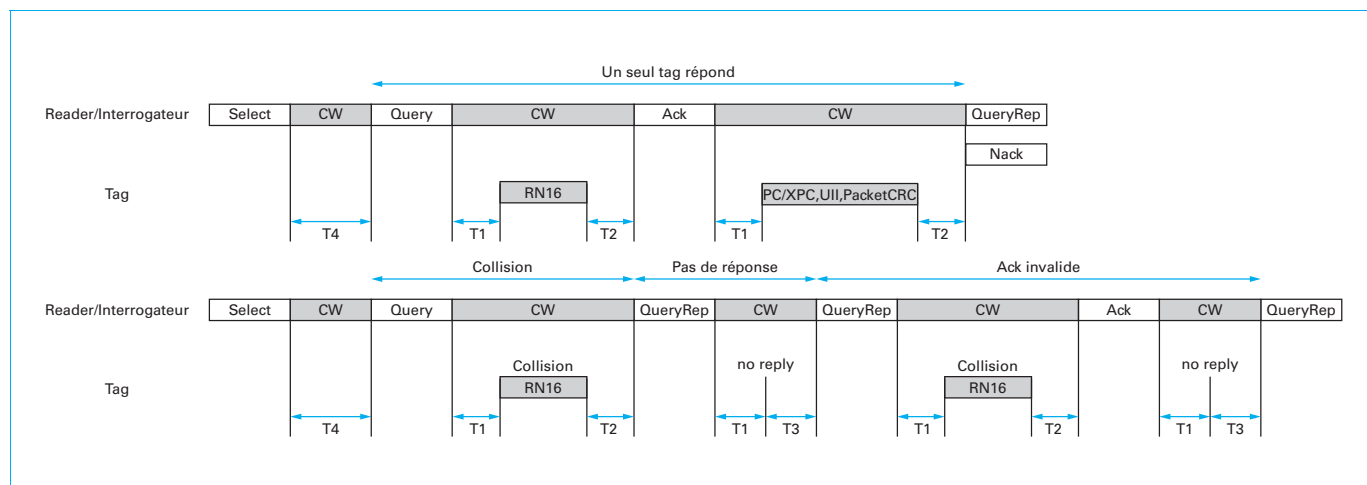


Figure 24 – Inventaire selon le protocole Gen2v2. a) Un seul tag répond dans un *time slot* donné et renvoie correctement son EPC. b) Autres cas possibles rencontrés dans le processus d'inventaire

Tableau 5 – Persistance des flags de session Gen2v2

Flag/Session	Temps de persistance	Tag passif alimenté	Tag passif non alimenté
S0	Aucune	La valeur du flag ne change jamais	La valeur du flag est immédiatement perdue
S1	Temps de persistance compris entre 0,5 et 5 secondes	La valeur du flag est maintenue durant le temps de persistance	La valeur du flag est maintenue durant le temps de persistance
S2, S3, SL	Temps de persistance supérieur à 2 secondes	La valeur du flag ne change jamais	La valeur du flag est maintenue durant le temps de persistance

La session S0 est donc particulièrement utile pour les petites populations de tags à déplacement rapide comme dans des applications de péages autoroutiers, de convoyeurs industriels ou d'identification de locomotives.

Si le nombre de tags est plus important, de sorte que tous les tags alimentés ne puissent pas être lus avant le temps d'arrêt maximum d'émission radiofréquence, il est alors conseillé d'utiliser l'une des sessions S1 à S3. Ces flags de session conservent leur état pendant de brèves périodes d'absence d'alimentation. La session S1 est unique en ce sens que ce flag reviendra toujours à l'état initial même avec le tag énergisé (avec un temps de persistance indiqué dans le tableau 5). Cela peut être utile lorsque le lecteur est capable d'inventorier de manière fiable tous les tags de la zone de lecture en moins de 500 millisecondes, soit le temps de persistance minimum de S1. Ainsi, le lecteur peut continuer d'inventorier de nouveaux tags arrivant dans son champ de lecture sans être « gêné » par les tags déjà inventoriés, sachant que tous les tags retourneront à l'état non inventorié au bout de 5 secondes. Là encore, cela dépend du nombre de tags divisé par le débit du lecteur. Si cette valeur est supérieure à 0,5 seconde, le lecteur devra certainement utiliser la session S2 ou S3 à persistance infinie pour des raisons de fiabilité. Comme ces deux sessions sont identiques en termes de persistance, on peut se poser la question de savoir laquelle utiliser. L'intérêt d'avoir deux sessions identiques vient des contraintes fortes des déploiements multilecteurs. Cela permet d'utiliser une approche « cellulaire » des sessions, en alternant, par exemple, la session S2 sur un lecteur, puis la session S3 sur le lecteur adjacent. L'idée étant de fournir autant de séparations que possible entre deux lecteurs utilisant la même session.

Enfin, le comportement temporel du flag SL est le même que celui des sessions S2 et S3. Il peut être utilisé pour sélectionner ou désélectionner des tags avant de commencer l'inventaire. Comme de plus en plus de tags RFID sont déployés, l'utilisation de la commande Select devient presque obligatoire.

Par **exemple**, pour le tri des bagages dans les aéroports, vous devez vous concentrer uniquement sur l'étiquette du bagage et ignorer les tags des vêtements à l'intérieur de la valise. Pour cette raison, une sélection des tags dédiés aux bagages peut être utile.

Les processus d'inventaire (singulation de tags) sont au cœur de tout système RFID. Il faut distinguer les systèmes plutôt prévus pour des communications pair à pair (paiement, titres de transport, documents sécurisés) de ceux conçus pour lire un maximum de tags en un minimum de temps.

Dans le cas d'inventaires de grand nombre de tags, les algorithmes dits « aléatoires » sont préférés et sont basés sur deux paramètres principaux : le nombre de *time slots* et les sessions. Avec le nombre croissant d'applications utilisant la RFID, le nombre de tags augmente et il faut de plus en plus mettre en œuvre des politiques de sélection de tags avant de démarrer le processus d'inventaire à proprement parler.

6. Encodage des tags RFID UHF passifs

Une fois les tags RFID alimentés et la communication avec les lecteurs établie, reste à se poser la question des informations échangées entre lecteurs et tags. Dans une application industrielle, c'est d'ailleurs la première question à se poser car, en fonction de la réponse, le choix de la technologie pourra se faire. Comme son nom l'indique, la RFID sert à identifier des objets porteurs de tags de manière rapide et fiable. Il faut donc savoir comment créer des identifiants uniques et comment les stocker et les protéger dans une puce électronique.

6.1 Organisation de la mémoire d'un tag UHF passif Gen2v2 (ISO/IEC 18000-63)

La structure de la mémoire d'une puce RFID UHF passive est définie dans les normes ISO/IEC 18000-63 et EPC Gen2v2. Ainsi, la mémoire physique de la puce est divisée en 4 banques de mémoires logiques (*Memory Banks*) qui sont accessibles à des adresses différentes et servent à des objectifs bien précis. La figure 25 présente l'organisation de ces 4 banques de mémoire.

Une fois n'est pas coutume, nous allons décrire le rôle de chacune de ces banques mémoire sans suivre l'ordre de leur numéro.

La RFID ayant été mise au point pour identifier des objets, la banque mémoire la plus « importante » est la banque 01 encore appelée banque Ull (*Unique Item Identifier*) ou banque EPC (*Electronic Product Code*). Elle contient notamment un identifiant unique construit à partir de règles et normes internationales permettant de s'assurer de l'unicité des identifiants au niveau mondial.

Nota : ces règles ou normes sont d'application volontaire (aucun texte de loi n'oblige à se conformer à ces normes). Il arrive donc parfois que certains acteurs les enfreignent (volontairement ou non). La conséquence est l'augmentation du nombre de tags « clones » ou « fantômes » qui perturbent les applications standardisées.

Cette banque mémoire contient également des informations supplémentaires codées dans ce qu'on appelle des mots de contrôle de protocole (PC et XPC). Ces informations indiquent par exemple quel est le standard d'encodage utilisé pour l'identifiant unique (GS1 vs. ISO) ou si le tag supporte ou non certaines commandes optionnelles du protocole. Ces informations sont malheureusement trop souvent ignorées par les utilisateurs. Elles permettent pourtant de réduire considérablement les erreurs de décodage et d'interprétation des informations. Il est important de noter que les informations contenues dans cette banque mémoire sont systématiquement communiquées par le tag lors du processus d'inventaire. La figure 23 montre que lorsqu'un tag est singulé, il renvoie automatiquement le contenu de cette banque mémoire. C'est généralement pour cela que l'on dit qu'il est plus rapide et plus simple de lire cette banque mémoire que les autres. En effet, les trois autres banques mémoire sont accessibles une fois l'inventaire terminé. Il faut alors que le lecteur envoie des commandes spécifiques pour accéder à ces banques mémoire. Leur accès est de facto plus long.

La banque mémoire 10 ou TID (*Tag Identifier*) contient un identifiant (*a priori*) unique. Cet identifiant est celui de la puce RFID. Il est encodé par le fabricant de la puce suivant des normes et standards internationaux (ISO/IEC 15963 et GS1 Tag DataStandard). Cet identifiant est globalement composé de 3 éléments :

- un identifiant de fabricant (MDID, *Mask Designer Identifier*) assigné par GS1 ; cet identifiant est unique pour chaque fabricant de puce RFID ;
- une référence de modèle de puce (TMN, *Tag Model Number*) assigné par chaque fabricant à un modèle de puce particulier ;
- un numéro de série unique, assigné par le fabricant à chaque puce individuelle.

Si l'on fait confiance aux fabricants de puces RFID, chaque puce a donc un TID unique. Dans certaines applications, on utilise ce TID et le fait qu'il soit, par définition, unique comme clé d'identification des objets. Cette idée peut paraître intéressante puisqu'elle évite à l'utilisateur de créer son propre identifiant (Ull ou EPC) mais elle requiert une base de données centrale qui doit faire le lien entre chaque TID et chaque objet associé. Lors d'un inventaire, chaque TID lu doit faire l'objet d'une interrogation de la base de données pour savoir à quel objet ce TID est associé. Il est à noter que ce TID est protégé en écriture par le fabricant de la puce RFID. Sa modification est donc impossible.

La banque mémoire 00 ou RESERVED sert à stocker deux mots de passe de 32 bits : l'Access password et le Kill password. Le premier sert à « protéger » les informations contenues dans les banques mémoire du tag. Si ce mot de passe est activé (si sa valeur est différente de 0), il permet, par exemple, de protéger en écriture

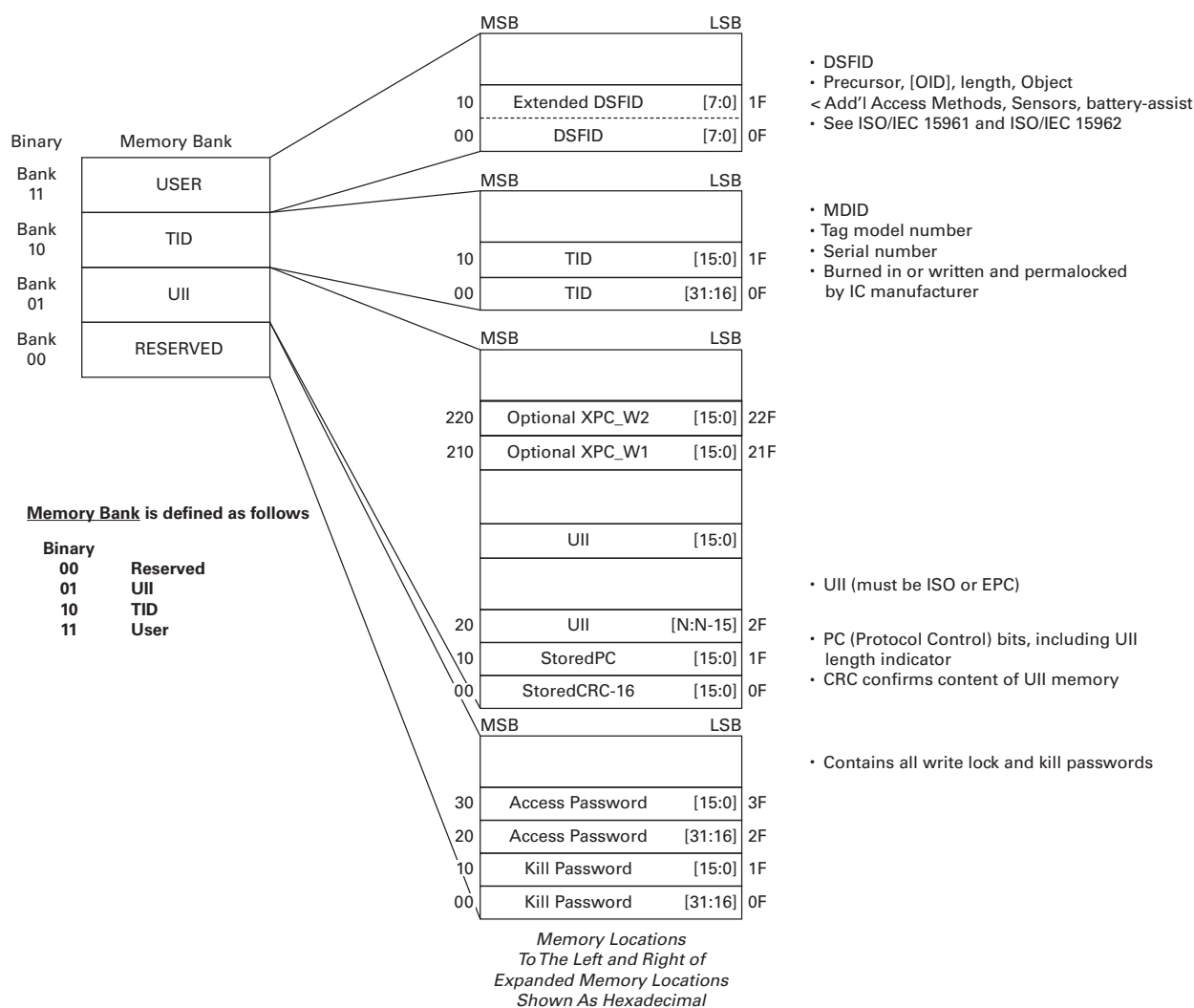


Figure 25 – Banques mémoire d'une puce RFID UHF ISO/IEC 18000-63 (EPC Gen2v2)

la banque mémoire 01 (UID ou EPC). Toute personne souhaitant modifier le contenu de cette banque mémoire devra connaître ce mot de passe.

Nota : protéger un identifiant d'objet (UID ou EPC) avec un simple mot de passe de 32 bits n'est pas très sécurisant. Dans les cas où il n'y a aucune raison de modifier l'UID ou l'EPC une fois le tag en service, on préfère généralement interdire de manière définitive toute modification. On utilise alors la commande « PermaLock » qui verrouille de manière permanente la banque mémoire visée, quelle que soit la valeur de l'Access password.

Nota : les mots de passe contenus dans la banque mémoire 00 (RESERVED) doivent également être protégés en lecture et en écriture. Dans le cas contraire, ces informations restent accessibles ce qui rend la protection par mot de passe totalement inutile.

Le mot de passe Kill sert à protéger l'utilisation de la commande Kill. Cette commande rend le tag définitivement silencieux, quelle que soit la commande envoyée par le lecteur. Cela revient donc à « tuer » le tag. On comprend facilement le danger que représente une telle commande. Elle a été mise en place afin de répondre aux questions de respect de la vie privée soulevées par certaines associations de consommateurs. L'idée est de désactiver (de manière

définitive) les tags RFID à la sortie des magasins. Pour cela, le mot de passe Kill doit être activé (différent de 0) et bien sûr protégé en lecture et en écriture. Ainsi, seuls ceux qui connaissent ce mot de passe pourront désactiver le tag. La mise en œuvre de cette fonction, si elle peut répondre à des questions de respect de la vie privée, empêche néanmoins l'utilisation du tag RFID une fois hors du circuit de vente. Toutes les applications de retour produit, de service après-vente et de recyclage ne peuvent donc plus bénéficier de la technologie. C'est pour cela qu'aujourd'hui, la fonction Kill n'est pas utilisée et qu'on lui préfère des commandes moins « définitives » telles que la commande Untraceable. Cette commande permet, en effet, de réduire les distances de communication et/ou de masquer certaines informations contenues dans le tag (comme un numéro de série par exemple). La fonction Kill doit donc être rendue impossible en verrouillant de manière définitive le mot de passe Kill à 0.

La dernière banque mémoire (11) est celle dite de l'utilisateur (USER). Sa présence est optionnelle et certains modèles de puce

RFID n'en proposent pas. La taille de cette banque mémoire est également laissée à la discrétion des fabricants qui répondent à des besoins et contraintes de leurs clients. Pour des applications « bas coût », on préfère ne pas implémenter cette banque mémoire alors que pour des applications du type « aéronautique », on peut trouver des puces RFID ayant des tailles de mémoire allant jusqu'à plusieurs dizaines de kilobits. On peut voir cette banque mémoire comme une espèce de tableau blanc à la disposition des utilisateurs qui souhaiteraient encoder des informations supplémentaires comme des dates de maintenance, des numéros de lots, des identifiants de personnes habilitées à exécuter certaines tâches, etc. Pour utiliser et surtout partager cet espace, il faut bien sûr se baser sur des règles d'encodage claires. Certaines sont génériques comme GS1 Tag Data Standard, d'autres sont spécifiques à un secteur industriel, comme l'ATA Spec 2000 dans l'aéronautique. Néanmoins, il est souvent préférable de stocker toute information « supplémentaire » dans une base de données. L'identifiant unique UII ou EPC sert alors de clé pour accéder aux informations pertinentes. Cela résout le problème de sécurité et d'espace de stockage. Pour ce faire, on peut se baser sur des normes telles que GS1 EPCIS (*EPC Information Service*) ou GS1 Digital link.

6.2 Les identifiants UII et EPC en RFID UHF passive

Comme nous l'avons vu précédemment, lors du processus d'inventaire, les tags RFID UHF passifs ISO/IEC 18000-63, une fois singulés, retournent le contenu de la banque mémoire MB01. Cette banque mémoire contient l'identifiant unique défini par l'utilisateur final de l'application ainsi que d'autres informations permettant, notamment, de décoder correctement cet identifiant.

La figure 26 représente de manière synthétique les différentes composantes de cette banque mémoire.

Le premier mot de 16 bits représente le CRC (*Cyclic Redundancy Check*), ou plus précisément le « StoredCRC » qui est calculé par le tag en fonction du contenu de la banque mémoire EPC. Cela permet de détecter d'éventuelles erreurs ou incohérences. Ce mot est différent de celui systématiquement renvoyé par le tag lors de l'envoi de message vers l'interrogateur, appelé PacketCRC. Bien sûr, toute tentative d'écriture par l'interrogateur aux adresses mémoire comprises entre 0x00 et 0x0F se solde par un échec car seul le tag peut calculer et modifier le StoredCRC en fonction de son contenu mémoire.

Les 5 bits suivants (0x10 à 0x14) représentent la longueur de l'identifiant UII ou EPC encodé à partir de l'adresse 0x20. Par exemple, si la valeur de ces 5 bits est 00110₂, cela signifie que l'UUI ou l'EPC est composé de 6 mots de 16 bits, soit une longueur totale de 96 bits.

La valeur du bit encodé à l'adresse 0x15 indique si la banque mémoire utilisateur contient des données ou non. Si c'est le cas, il peut être intéressant d'interroger spécifiquement cette banque mémoire.

La valeur du bit encodé à l'adresse 0x16 indique si le tag contient des informations additionnelles encodées dans le mot de protocole supplémentaire XPC. Ces informations concernent principalement les fonctionnalités optionnelles supportées ou non par le tag comme les fonctions Untraceable (pour la protection de la vie privée) ou des fonctions de cryptographie. Le contenu de ce mot de protocole supplémentaire est décrit dans la norme ISO/IEC 18000-63 et dans le standard EPC Gen2v2.

De manière à répondre aux besoins de la majorité des secteurs et industries utilisant la RFID, deux choix d'encodage sont disponibles : ISO ou GS1. Ce choix est défini par la valeur du bit 0x17 (*Toggle bit*) de la banque mémoire MB01. Lorsque la valeur de ce bit est « 0 », l'identifiant est encodé suivant GS1 EPC Tag Data Standard. Lorsque la valeur de ce bit est « 1 », l'identifiant est encodé suivant la norme ISO/IEC 15459 et les bits 0x18 à 0x1F représentent l'identifiant de famille d'application AFI (*Application Family Identifier*) défini par la norme ISO/IEC 15961.

Enfin, l'identifiant unique à proprement parler (UUI ou EPC) est encodé à partir de l'adresse mémoire 0x20.

6.2.1 Identifiants ISO

Les systèmes de numéros d'article ISO (identificateur d'article unique – UUI) sont généralement spécifiés par des organisations enregistrées, comme l'IATA (International Air Transport Association) ou JAIF (Joint Automotive Industry Forum), à qui l'autorité d'enregistrement ISO AIMglobal a attribué un AFI ISO/IEC 15961 (<https://www.aimglobal.org/registration-authority.html>).

La norme ISO/IEC 15961 spécifie également un ensemble d'AFI « réservés » pour les applications dites en boucles fermées :

- AFI 0 indique que le tag n'est pas configuré ;
- les AFI 1 à 3 peuvent être utilisés pour des identifiants propriétaires ;
- les AFI 4 à 15 sont attribués à des applications fermées spéciales.

Lorsque des identifiants ISO sont utilisés, le bit de basculement (*Toggle bit*) doit être mis à « 1 ». Généralement, un format de structure de données, DSFID (*Data Storage Format Identifier*) est défini pour l'identifiant ce qui permet de « comprendre » sa structure. Dans la majeure partie des cas, cet identifiant se compose d'au moins trois éléments :

- un code de l'organisme émetteur (IAC, *Issuing Agency Code*) ;
- un numéro d'identification de la société (CIN, *Company Identification Number*) ;
- un numéro de série (SN, *Serial Number*).

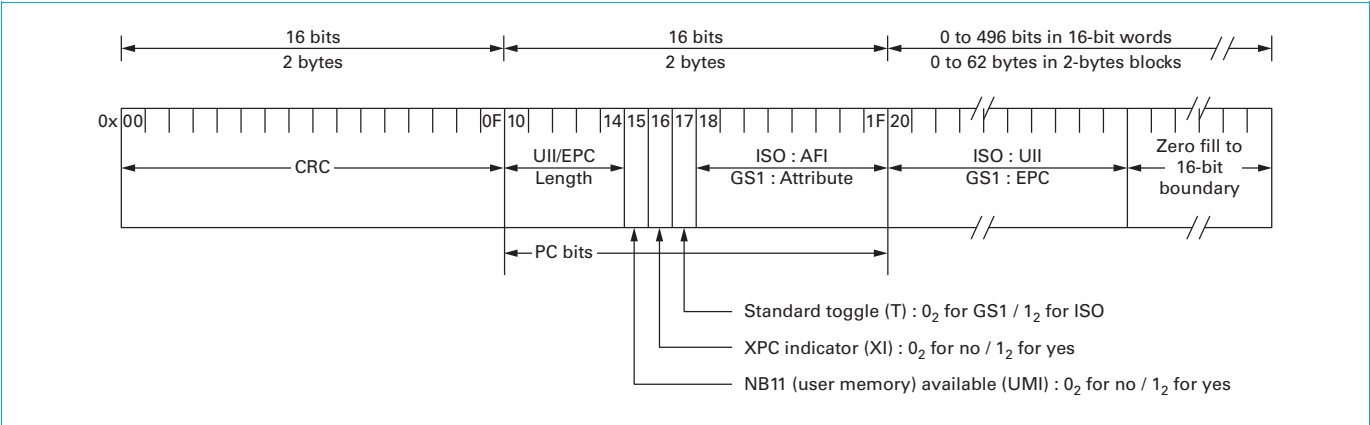


Figure 26 – Contenu de la banque mémoire MB01 d'une puce RFID UHF ISO/IEC 18000-63 (EPC Gen2v2).

L'autorité d'enregistrement, telle que définie par la norme ISO/IEC 15459, attribue un code unique (IAC) à chaque organisme enregistré. Cet organisme attribue, à son tour, des codes uniques à chacun de ses membres (CIN). Enfin, chaque entreprise identifiée par un CIN attribue le numéro de série (SN). Le numéro de série peut être composé de plusieurs parties, mais dans tous les cas, il doit être un identifiant unique dans le domaine des CIN.

La figure 27 présente un exemple d'encodage ISO pour la traçabilité des bagages aériens.

Dans cet exemple, les informations à encoder dans le tag RFID sont : un numéro d'identifiant de bagage et une date de vol. Grâce à ces deux informations, IATA garantit l'unicité des identifiants. La valeur du *Toggle bit* est « 1 » ce qui indique que l'identifiant est défini suivant une norme ISO. La valeur de l'AFI est donc à lire pour permettre le décodage de cet identifiant. L'AFI (0xC1) indique au lecteur du tag qu'il s'agit d'un tag de la « famille » des bagages aériens défini par l'IATA. Le DSFID (0x0C) indique alors que l'identifiant est composé de deux informations : le numéro de bagage et la date du vol. On peut donc aisément procéder au décodage de ces informations. Les autres valeurs encodées dans le mot de protocole (PC word) indiquent la longueur totale de l'identifiant (ici 6 mots de 16 bits), le fait qu'il n'y a pas d'information encodée dans la banque mémoire utilisateur (MB11) et qu'il n'y a pas de mot de protocole étendu (XPC word).

6.2.2 Identifiants GS1

Dans le cas de l'utilisation d'identifiants GS1, le document de référence est le GS1 Tag Data Standard. GS1 propose plusieurs types d'identifiants suivant les objets ou processus concernés. Un des plus emblématiques est le SGTIN (*Serialized Global Trade Item Number*) car il est le prolongement naturel des identifiants que l'on trouve sur tous les produits du commerce sous forme de code à barres : l'EAN (*European Article Number*) en Europe et l'UPC (*Universal Product Code*) aux États-Unis. Le système de numérotation GS1 repose principalement sur les identifiants de sociétés fournis et gérés par GS1, les GCP (GS1 Company Prefix). Chaque société enregistrée chez GS1 peut alors construire ses identifiants suivant les schémas proposés dans le standard.

Dans l'exemple du SGTIN, l'identifiant est composé de trois éléments : le GCP (assigné par GS1 à la société enregistrée), un numéro d'article (*Item number*, assigné par la société à chaque

type de produit différent) et un numéro de série (assigné par la société à chaque article individuel). Avant d'encoder ces informations dans la banque mémoire EPC (MB01) du tag RFID, on y ajoute trois autres types d'information :

- le Header. Cette information, codée sur 8 bits indique le type d'identifiant GS1 est utilisé ;
- un filtre qui informe sur le type d'article. Il peut s'agir d'un article destiné à la vente ou un objet destiné au stockage d'autres articles ;
- la partition. Cette information indique où se situe la séparation entre le GCP et la référence article (*Item number*).

Nota : suivant la taille de la société et le nombre d'articles différents qu'elle fabrique ou commercialise, la longueur du GCP est différente. Les sociétés les plus importantes ont des GCP courts permettant ainsi de créer de nombreuses références d'articles différentes.

La figure 28 montre un exemple d'encodage SGTIN sur 96 bits.

Dans cet exemple, la valeur du header est 0x30 ce qui indique au lecteur que la suite de l'identifiant est un SGTIN-96. La valeur du filtre indique qu'il s'agit d'un article destiné à la vente. La partition (101) indique que le GCP est composé de 7 digits, ce qui, par définition, laisse à la société 6 autres digits pour définir ses références d'article (soit la possibilité de « créer » 999 999 articles différents). Le numéro de série est, par définition, toujours encodé sur 38 bits ce qui permet d'avoir 2^{38} (274 877 906 944) articles uniques pour une même référence. Les autres informations, encodées dans le mot de protocole (PC word) ont une signification identique au cas précédent d'un identifiant ISO sauf que le *Toggle bit* doit être à « 0 » et que les 8 bits d'AFI ne sont pas utilisés.

D'autres formats d'identifiants sont disponibles suivant le type d'article ou d'information que l'on souhaite identifier. Par exemple, on peut encoder des informations de localisation dans un tag RFID en suivant le schéma GLN (*Global Location Number*) proposé par GS1. L'ensemble des identifiants proposés par GS1 est disponible à l'adresse : <https://www.gs1.org/standards/barcodes/application-identifiers>

Il est à noter que, par construction, seuls les identifiants sérialisés peuvent être utilisés en RFID.

L'encodage des informations dans un tag RFID est un élément crucial de l'application. Si celui-ci est mal réalisé, le décodage sera au mieux impossible, voire il induira le lecteur en erreur pensant identifier un type d'article alors qu'il est face à un autre.

MB01 (PC-Word)					MB01 (UII/EPC)		
Longueur UII (bits)	UMI (bit)	XI (bit)	Toggle (bit)	AFI (hexa)	UII (spécifié par IATA RP1740C)		
					DSFID (hexa)	N° d'identifiant de bagage (hexa)	Date du vol (hexa)
00110	0	0	T = 1 (ISO)	0xC1	0x0C	0x21050123456789	0x1202015E

Figure 27 – Exemple d'encodage ISO de la banque mémoire MB01 d'une puce RFID UHF ISO/IEC 18000-63 (EPC Gen2v2)

MB01 (PC-Word)					MB01 (UII/EPC)					
Longueur UII (bits)	UMI (bit)	XI (bit)	Toggle (bit)	AFI (hexa)	EPC (spécifié par GS1 Tag Data Standard)					
					Header (hexa)	Filtre (bits)	Partition (bits)	GCP (digit)	Item ref. (digit)	Serial number (digit)
00110	0	0	T = 0 (GS1)	NA	0x30	001	101	0614141	812345	6789

Figure 28 – Exemple d'encodage GS1 de la banque mémoire MB01 d'une puce RFID UHF ISO/IEC 18000-63 (EPC Gen2v2)

Pour les identifiants, il faut choisir, dès la conception de l'application, le schéma de numérotation ISO ou GS1. Il faut bien sûr veiller à ce que ce choix soit correctement encodé dans le tag (*Toggle bit*). Que ce soit GS1 ou ISO, les identifiants uniques sont globalement basés sur 3 composantes : un identifiant d'organisation (ou de société) assigné par une autorité d'enregistrement (GS1 ou autre), une référence d'article et un numéro de série.

Le nombre d'applications utilisant la RFID étant en forte croissance, tout schéma d'identification propriétaire est à déconseiller fortement. De plus, les stratégies consistant à filtrer les tags avant d'en faire l'inventaire sont aujourd'hui incontournables.

7. Normes et réglementations

Les normes, qui plus est internationales, ne doivent servir qu'à permettre le déploiement harmonieux des technologies dont elles décrivent le fonctionnement. Elles doivent servir de référence lorsque ces technologies sont utilisées en boucle ouverte et permettre l'interopérabilité des systèmes. Un interrogateur conforme à une norme doit pouvoir communiquer avec tout tag conforme à cette même norme et inversement. Nous verrons, un peu plus loin dans ce chapitre, que pour les applications industrielles, il faut parfois aller plus loin que l'interopérabilité, il faut atteindre l'interchangeabilité.

Avant d'aller plus en avant dans le sujet des normes, il est important de faire une distinction entre les objectifs qu'elles doivent atteindre. Une première catégorie de normes va servir à faire cohabiter divers systèmes partageant une même ressource. Pour la RFID, cette ressource commune à plusieurs systèmes est bien sûr le spectre électromagnétique. On parle alors de régulation. Une deuxième catégorie va servir à faire cohabiter les technologies avec les individus et la société. Il s'agit de normes de protection contre les éventuels effets des rayonnements électromagnétiques. Pour la RFID, les fréquences utilisées sont telles que l'on parle de rayonnements non ionisants. La RFID étant une technologie d'identification automatique, les problèmes liés à la sécurité des données (personnelles ou non) et le respect de la vie privée doivent également être adressés par les normes. Enfin, une troisième catégorie de normes va servir à décrire le fonctionnement des systèmes à proprement parler. On parle de normes techniques qui décrivent les méthodes de communication, d'accès aux ressources radio ainsi que la manière d'encoder les informations.

7.1 Régulations

Chaque pays est maître de l'utilisation sur son sol du spectre électromagnétique. Partant de ce principe, il semble utopique de croire qu'un système, utilisant une partie de ce spectre pour remplir sa fonction, puisse passer les frontières et retrouver partout où il est utilisé, la même ressource réservée pour son usage. L'Union Internationale des Télécommunications (UIT) a pour objectif d'établir des recommandations visant à harmoniser l'utilisation du spectre électromagnétique. Ces recommandations sont ensuite reprises dans chaque zone géographique du globe. En Europe, le CEPT (Commission Européenne des Postes et Télécommunications) et l'ERC (European Radiocommunications Committee) ont publié une recommandation (REC 70 03) visant à réguler l'utilisation des systèmes de communication de faible portée (SRD pour *Short Range Devices*). Cette recommandation est basée sur un certain nombre de normes rédigées sous l'égide de l'ETSI (European Telecommunications Standard Institute). Ces normes font partie de la famille EN 300-xxx « *Electromagnetic compatibility and radio spectrum matters ; Short range devices* ». Il est également à noter que la mise sur le marché d'équipements radioélectriques est soumise à des directives et lois nationales qui impliquent généralement de

réaliser un certain nombre de tests. Au niveau européen, il s'agit notamment de la directive RED (directive européenne 2014/53/UE1).

Des adaptations de la recommandation de l'UIT ont été faites dans les autres régions du globe. Aux États-Unis, par exemple, la Federal Communications Commission (FCC) sous l'égide de l'ANSI (American National Standard Institute) a établi son propre document (US Code of Federal Regulation). Le lecteur trouvera sur le site internet de l'UIT, l'ensemble des organisations régionales de télécommunications auxquelles il pourra se référer pour connaître les textes en vigueur dans chaque partie du globe.

Pour ce qui concerne plus particulièrement les systèmes RFID UHF, on assiste ces dernières années à une « harmonisation » des bandes autorisées. Classiquement, on parle de systèmes pouvant fonctionner dans la bande 860-960MHz. Les fréquences basses de cette bande sont plutôt utilisées en Europe, les fréquences moyennes en Amérique du Nord et les fréquences hautes en Asie. Aujourd'hui, de nombreux pays en Europe autorisent l'utilisation de 3 nouveaux canaux dans la bande 915-919,4MHz en plus de ceux existants dans la bande 865-868MHz. Des révisions de la Recommandation 70-03 ainsi que de la norme ETSI 302-208 ont été publiées. Dans d'autres pays, les adoptions nationales sont en cours.

7.2 RFID, santé publique et vie privée

Tout comme pour les régulations, il existe des recommandations internationales visant à établir des seuils d'exposition des individus (professionnels et grand public) aux champs électromagnétiques émis par tout équipement de télécommunication et installations radioélectriques. Pour les systèmes RFID, c'est l'ICNIRP (International Commission on Non Ionizing Radiation Protection) qui établit ces recommandations. La plus connue est le « *Guidelines for limiting exposure for time varying electric, magnetic and electromagnetic fields up to 300 GHz* ». D'autres organismes, comme l'IEEE (Institute of Electrical & Electronic Engineers), l'IEC (International Electrotechnical Commission) ou encore le CENELEC (Centre européen pour la normalisation en électrotechnique), ont publié des guides et méthodes d'évaluation. En ce qui concerne spécifiquement les systèmes RFID, la commission technique (TC 106) du CENELEC a rédigé la norme EN 62369 « *Evaluation of human exposure to electromagnetic fields from short range devices (SRDs) in various applications over the frequency range 0 GHz to 300 GHz. Fields produced by devices used for electronic article surveillance, radio frequency identification and similar systems* ». Ces normes et recommandations sont reprises dans le droit international.

En Europe, la Commission européenne a publié une recommandation en juillet 1999 (1999/519/EC). Cette recommandation a été transformée en directive (2004/40/EC). Initialement applicable en avril 2008, cette directive a finalement été abandonnée. Aujourd'hui, la nouvelle directive 2013/35/EC est appliquée et reprise dans le droit national de chaque état membre de l'Union européenne, notamment en France avec le décret d'application n° 2016-1074 du 3 août 2016.

De par les unités de mesure utilisées dans ces normes (*Specific Absorption Rate* et *Maximum Permissible Exposure*) et la diversité des méthodes de mesure, la vérification de conformité des installations RFID (et autres systèmes radioélectriques) n'est pas chose aisée. Néanmoins, les niveaux de champ préconisés par les normes de régulation sont tels que les niveaux de rayonnement sont bien en dessous des seuils définis par l'ICNIRP. Une méthode d'évaluation simple a été mise en place par un groupe d'experts sous la direction du Centre National de référence RFID (CNRFRID). Ce document concerne les systèmes RFID UHF. Il est téléchargeable gratuitement sur le site du CNRFRID.

Pour ce qui concerne la sécurité des données et le respect de la vie privée, la RFID a été au centre de plusieurs actions menées notamment par la Commission européenne. Avec la publication de la Recommandation du 12 mai 2009, les organismes de standardisation et notamment le CEN (Comité européen de normalisation)

ont travaillé à l'élaboration de normes permettant de garantir le respect de la vie privée. Comme prévu par la Recommandation, la mise en œuvre d'une application RFID (paiement sans contact, badges d'accès, billets transport, inventaires, logistiques, etc.) doit faire l'objet d'une évaluation d'impact sur la vie privée (EIVP ou *Privacy Impact Assessment* PIA en anglais). La norme européenne EN 16571 permet de réaliser cette étude d'impact grâce à un processus adapté aux risques spécifiques aux technologies RFID. D'autres textes normatifs complètent cette norme et permettent d'assurer la conformité des systèmes RFID vis-à-vis de la directive européenne (2002/58/EC : *Processing of personal data and protection of privacy*) mais aussi du nouveau règlement européen sur la protection des données (Règlement (UE) 2016/679).

7.3 Normes techniques

L'objet de ce paragraphe n'est pas de reprendre les normes techniques une à une et de décrire leur contenu. L'idée est de simplement donner au lecteur les moyens d'accéder rapidement à une norme technique particulière en fonction de l'application envisagée.

Comme nous l'avons dit au début de ce paragraphe, l'intérêt d'une norme est de servir de référence à des systèmes fabriqués et utilisés à travers le monde. C'est donc naturellement à l'ISO (International Standard Organisation) que les normes techniques de la RFID ont été (et continuent) d'être rédigées. L'ISO n'ayant pas de comité technique spécialement compétent dans les systèmes principalement basés sur l'électronique, c'est dans un groupe commun avec l'IEC (International Electrotechnical Commission) que nous allons trouver les comités d'experts chargés de la rédaction des normes techniques de la RFID. Dans ce groupe commun (JTC1 *Joint Technical Committee*), nous trouvons le sous-comité 31 (SC31 *Sub Committee*) spécialement dédié aux techniques d'identification et de capture automatique de données. Ce sous-comité ne s'intéresse pas uniquement à la RFID mais à toutes les techniques d'identification automatique, codes à barre compris. Dans ce sous-comité 31, plusieurs groupes de travail (WG *Working Group*) s'intéressent à des technologies ou des méthodes de capture particulières. La RFID est traitée dans le WG4. C'est de ce groupe que sont issues toutes les normes de la famille ISO/IEC/JTC1/SC31/18000-x. Le x (numéro de 1 à 7) sépare les systèmes RFID par fréquence. À ces normes, sont associés des rapports techniques (TR *Technical Report*), ainsi que les normes ISO/IEC 18046-x pour les tests de performance et ISO/IEC 18047-x pour les tests de conformité. Au-delà des normes décrivant les paramètres liés à la communication (interface air), il est important de noter que les normes ISO/IEC 15961, 15962 et 15963 définissent des règles d'encodage et la manière d'identifier de manière unique les tags RFID.

Directement liés à l'ISO, des comités techniques (TC *Technical Committee*) peuvent être considérés comme des utilisateurs de la RFID. Ces comités décrivent la manière d'utiliser la RFID pour des applications ou des métiers particuliers. Parmi ceux-ci on peut citer le TC23 pour l'identification animale ou le TC 122 pour les emballages (réutilisables ou non).

Dans tous les cas, les normes ou rapports techniques édités à travers l'ISO sont basés sur le principe du consensus. Dans les divers comités, la règle du « un pays – un vote » s'applique. Cela n'exclut pas le lobbying, parfois intense, de certains industriels lors de la phase de rédaction des documents mais cela garantit à chacun le fait de pouvoir s'exprimer. Au final, une norme doit être claire, indépendante de toute technologie particulière et doit permettre à chacun d'accéder aux diverses propriétés intellectuelles (RAND *Reasonable And Non Discriminatory*).

Enfin, comment terminer ce chapitre sans parler de l'EPCglobal. L'EPC (*Electronic Product Code*) est le prolongement du code à barre classique qui veut tirer parti de la puce d'une étiquette RFID pour identifier de façon unique tous les objets passant à un moment ou un autre par une « *supply chain* ». L'idée est de travailler avec un tag le moins cher possible (peu de ressources mémoire). Toute information supplémentaire concernant le produit est donc stockée sur une base de données accessible par Internet. L'identifiant unique

(EPC) sert alors de pointeur vers l'adresse internet où sont stockées les informations. EPCglobal, aujourd'hui géré par GS1 Global Office (<http://www.gs1.org>), propose un panel complet de standards mis au point par des industriels et laboratoires partenaires (Auto-Id Labs). Le principal standard concernant l'interface air UHF est connu sous le nom de EPC Gen2v2. Il a été quasi intégralement repris par l'ISO sous le nom de ISO/IEC 18000-63 (mode C).

8. Conclusion

Aujourd'hui, les techniques mises en œuvre dans les systèmes RFID sont globalement maîtrisées par les fournisseurs de solutions. Il n'en reste pas moins que, comme pour toute solution basée sur l'utilisation des radiofréquences, l'analyse de l'environnement et la customisation des solutions restent des éléments incontournables pour garantir le succès de l'application.

Avec les concepts d'Internet des objets et d'objets connectés, les fournisseurs font aujourd'hui face à de nouveaux défis. Les questions liées à la sécurité des données, le respect de la vie privée, l'interopérabilité avec d'autres systèmes de communication radio et l'utilisation de capteurs font que les applications faisant appel à la RFID se complexifient. Encore réservé, il y a quelque temps aux seules technologies des cartes à puces sans contact, on commence à trouver sur le marché des systèmes RFID UHF qui embarquent des modules cryptographiques permettant l'authentification des tags et lecteurs. De plus en plus de fournisseurs proposent des solutions permettant de protéger la vie privée en mettant « en veille » les tags RFID sans pour autant les désactiver de manière définitive (fonction Untraceable du standard EPC Gen2v2). De nouvelles puces bi-fréquences (HF/UHF) sont aujourd'hui disponibles permettant de tirer profit des deux technologies grâce à une seule étiquette (lecture en volume et lecture unitaire sécurisée). Les *smartphones* intègrent presque tous des lecteurs NFC. Ils intégreront certainement des lecteurs UHF dans un futur proche. Cela permet de pallier le problème du coût de la diffusion des moyens de lecture et permet de mettre en œuvre plus facilement des applications en boucle ouverte (applications dans lesquelles les acteurs partagent la valeur apportée par la RFID, depuis la fabrication du produit jusqu'à sa vente en passant par les circuits de distribution et stockage). Reste encore bien souvent à régler la question de l'encodage des tags RFID. Avec la multiplication des applications, les identifiants (TID, UID, EPC) devront avoir une unicité garantie et se pose donc le problème d'une (ou de plusieurs) autorités garantissant cette unicité. Cette question n'est pas propre à la RFID mais concerne tout l'Internet des objets et notamment de sa gouvernance.

Il n'en reste pas moins que de nombreux progrès technologiques dans les domaines de la récupération d'énergie, les composants « basse consommation », les SOC (*system on chip*), les matériaux intelligents, les tags sans puce (*chipless tags*) permettront à la RFID d'élargir son champ des possibles.

9. Glossaire

Anticollision ; Anticollision

Procédure permettant à un lecteur de réaliser l'inventaire des tags présents dans son champ d'action. Suivant le protocole utilisé, un lecteur peut identifier plusieurs centaines de tags en quelques secondes.

Communication en champ proche (NFC) ; Near Field Communication

Type de système RFID pour lequel la zone de fonctionnement des étiquettes (tags) se trouve dans la zone de champ proche créée par

le lecteur. Le couplage entre l'étiquette et le lecteur est alors généralement inductif. Les systèmes RFID LF (125 kHz) et HF (13,56 MHz) sont systématiquement en champ proche.

Couplage ; Coupling

Le couplage définit la liaison entre une étiquette et un lecteur. Les systèmes RFID LF et HF présentent généralement un couplage inductif. Dans ce cas, c'est le champ magnétique qui est utilisé pour transmettre l'énergie et les données. Pour les systèmes RFID UHF et SHF, il s'agit d'un couplage électromagnétique. Le champ électromagnétique est formé et l'équation des télécommunications (équation de Friis) s'applique comme dans le cas des télécommunications hertziennes « classiques ».

Identifiant unique ; Unique Identifier

Les systèmes RFID s'appuient sur un certain nombre d'identifiants permettant l'identification des objets et des personnes. Pour la puce RFID, on parle de TID (Tag Identifier) ou d'UID (Unique Identifier). Pour l'application, on utilise généralement un autre identifiant :

- le code EPC (Electronic Product Code) dans le système de numérotation proposé par GS1
- ou l'UII (Unique Item Identifier) dans un système de numérotation ouvert proposé par les standards ISO.

D'autres identifiants peuvent être mis en place tels que l'AFI (Application Family Identifier) qui, comme son nom l'indique, permet de classer les tags suivant leur application (carte de paiement, livre de bibliothèque, container maritime, etc.)

RFID passive ; passive RFID

Dispositif de RFID qui utilise des tags qui renvoient et modulent (rétromodulation) un signal porteur envoyé par un interrogateur pour communiquer avec ce dernier. Les tags passifs utilisent généralement l'énergie émise par le lecteur (télé-alimentation) pour se mettre en service.

RFID active ; active RFID

Dispositif RFID qui utilise des tags capables de produire leur propre signal radio au moyen d'un émetteur interne. Pour cela, les tags ont généralement besoin d'une source d'énergie interne (batterie, par exemple).

10. Sigles, notations et symboles

Symbole	Description	Unité
λ	Longueur d'onde	m
Γ	Coefficient de réflexion	S.U.
Σ	Surface effective d'antenne	m ²
AFI	Application Family Identifier	NA
B	Induction magnétique	Tesla
BAP	Battery Assisted Passive	NA
CIN	Company Identification Number	NA
CRC	Cyclic Redundancy Check	
DSFID	Data Storage Format Identifier	NA
E	Champ électrique	V/m

Symbole	Description	Unité
EAN	European Article Number	NA
EPC	Electronic Product Code	NA
EPCIS	Electronic Product Code Information Service	NA
ETSI	European Telecommunications Standard Institute	NA
FCC	Federal Communications Commission	NA
FM0	Bi-Phase Space	NA
G	Gain d'antenne	S.U.
GCP	GS1 Company Prefix	NA
H	Champ magnétique	A/m
HF	High Frequency	NA
ITF	Interrogator Talk First	NA
IAC	Issuing Agency Code	NA
IEC	International Electrotechnical Commission	NA
ISO	International Standard Organisation	NA
k	Coefficient de couplage	S.U.
K	Coefficient de re-rayonnement	S.U.
L	Inductance	Henry
LF	Low Frequency	NA
M	Mutuelle inductance	Henry
MB	Memory Bank	NA
md	Profondeur de modulation	S.U.
MDID	Mask Designer Identifier	NA
mi	Indice de modulation	S.U.
NRZ	Non Retour à Zéro	NA
PC	Protocol Control	NA
PIA	Privacy Impact Assessment	NA
PIE	Pulse Interval Encoding	NA
PPM	Pulse Position Modulation	NA
Q	Coefficient de qualité	S.U.
RFID	Radio Frequency Identification	NA
RN	Random Number	NA
RZI	Retour à Zéro Inversé	NA
SGTIN	Serialized Global Trade Item Number	NA

Symbole	Description	Unité
SN	<i>Serial Number</i>	NA
T	Coefficient de transmission	S.U.
TID	<i>Tag Identifier</i>	NA
TMN	<i>Tag Model Number</i>	NA
TOTAL	<i>Tag Only Talk After Listening</i>	NA
TTF	<i>Tag Talk First</i>	NA
UHF	<i>Ultra High Frequency</i>	NA
UII	<i>Unique Item Identifier</i>	NA
XPC	<i>Extended Protocol Control</i>	NA

Systemes et techniques RFID

par **Claude TETELIN**

Ingénieur ISEN, Docteur de l'Université de Lille, France
Directeur, Automatic Identification and Data Capture,
GS1 Global Office, Bruxelles, Belgique

Sources bibliographiques

- | | | |
|---|---|--|
| <p>[1] PARET (D.). – <i>RFID en ultra et super-hautes fréquences UHF-SHF</i>. Théorie et mise en œuvre. Dunod (2008).</p> <p>[2] COMBES (P.). – <i>Micro-Ondes 2, circuits passifs, propagation, antennes</i>. Dunod (1997).</p> <p>[3] PARET (D.). – <i>Identification radiofréquence et carte à puce sans contact, description</i>. Dunod (2001).</p> <p>[4] FINKENZELLER (K.). – <i>RFID Handbook, Radio-Frequency Identification Fundamentals and Applications</i>. Wiley (1999).</p> | <p>[5] BOWICK (Ch.). – <i>RF Circuit Design</i>. Newnes (1982).</p> <p>[6] DE DIEULEVEULT (F.). – <i>Électronique appliquée aux hautes fréquences</i>. Dunod (1999).</p> <p>[7] VIZMULLER (P.). – <i>RF Design Guide, systems, circuits and equations</i>. Artech House (1995).</p> <p>[8] VENTRE (D.). – <i>Communications analogiques</i>. Ellipses (1998).</p> <p>[9] ZHANG (Y.), YANG (L.) et CHEN (J.). – <i>RFID and Sensor Networks</i>. CRC Press (2010).</p> | <p>[10] BELLANGER (M.). – <i>Traitement numérique du signal – Théorie et pratique</i>. Dunod (2006).</p> <p>[11] GREEN (R.B.). – <i>The general theory of antenna scattering</i>. OSU report 1223-17 (1963).</p> <p>[12] SCHNEIDER (R.K.). – <i>A re-look at antenna in-band RCSR via load mismatching</i>. IEEE Antennas and Propagation Society International Symposium, vol. 2, p. 1398-1401 (1996).</p> <p>[13] DOBKIN (D.). – <i>The RF in RFID, Passive UHF RFID in practice</i>. Newnes (2008).</p> |
|---|---|--|

À lire également dans nos bases

BRÉMAUD (J.-C.) et HAMON (G.). – *Émetteurs radioélectriques – Caractéristiques et conception*. [TE 6 207] (2000).

GLAVIEUX (A.). – *Codage de l'information et modulation des signaux*. [R 380] (1991).

LEFÈBVRE (J.-N.). – *Traçabilité des bagages dans le transport aérien – Déploiement de la technologie RFID*. [TR 670] Technologies de l'information, Réseaux télécommunications (2009).

MAGNE (F.). – *Télécommunications haut débit en ondes millimétriques*. [E 6 250] (1998).

ROGER (J.). – *Antennes – Techniques*. [E 3 284] Électronique – Photonique (1999).

Normes et standards

ISO/IEC 18000-7	2014	Technologies de l'information – Identification par radiofréquence (RFID) pour la gestion d'objets – Partie 7 : Paramètres de communications actives d'une interface radio à 433 MHz.	ISO/IEC 18000-3 mode 1 (HF)	2010	Information technology – Radio frequency identification for item management – Part 3 : Parameters for air interface communications at 13,56 MHz.
ISO/IEC 18000-4	2015	Information technology – Radio frequency identification for item management – Part 4 : Parameters for air interface communications at 2,45 GHz.	ISO/IEC 18000-61	2012	Information technology – Radio frequency identification for item management – Part 61 : Parameters for air interface communications at 860 MHz to 960 MHz Type A.
IEEE 802.15.4	2015	IEEE Standard For Low-Rate Wireless Personal Area Networks (WPANs).	ISO/IEC 18000-62	2012	Information technology – Radio frequency identification for item management – Part 62 : Parameters for air interface communications at 860 MHz to 960 MHz Type B.
ISO/IEC 15693	2009	Cartes d'identification – Cartes à circuit(s) intégré(s) sans contact – Cartes de voisinage.	ISO/IEC 18000-63	2015	Information technology – Radio frequency identification for item management – Part 63 : Parameters for air interface communications at 860 MHz to 960 MHz Type C.
GS1 EPC Tag Data Standard.	2019	Tag Data Standard.			
ETSI 300-330	2017	Short Range Devices (SRD) ; Radio equipment in the frequency range 9 kHz to 25 MHz and inductive loop systems in the frequency range 9 kHz to 30 MHz ; Harmonised Standard			

GS1/EPC Gen2v2	2018	EPC UHF Gen2 Air Interface Protocol.	NF EN 62369	2009	Évaluation de l'exposition humaine aux champs électromagnétiques produits par les dispositifs radio à courte portée dans la plage de fréquence 0 GHz à 300 GHz.
ETSI 302-208	2016	Radio Frequency Identification Equipment operating in the band 865 MHz to 868 MHz with power levels up to 2 W and in the band 915 MHz to 921 MHz with power levels up to 4 W ; Harmonised Standard covering the essential requirements of article 3.2 of the Directive 2014/53/EU.	NF EN 16571	2014	Technologies de l'information – Processus d'évaluation d'impact sur la vie privée des applications RFID.
ISO/IEC 15459	2014	Information technology – Automatic identification and data capture techniques – Unique identification.	ISO/IEC 15962	2013	Information technology – Radio frequency identification (RFID) for item management – Data protocol : data encoding rules and logical memory functions.
ISO/IEC 15961	2019	Information technology – Data protocol for radio frequency identification (RFID) for item management.	ISO/IEC 15963	2020	Information technology – Radio frequency identification for item management.

Annuaire

Constructeurs – Fournisseurs – Distributeurs (liste non exhaustive)

3M : <http://www.3m.com>
 Alien technology : <http://www.alientechnology.com>
 ASK : <http://www.ask-rfid.com>
 Avery Dennison : <http://rbis.averydennison.com/en/home.html>
 Caen : <http://www.caen.it/rfid/index.php>
 CISC : <https://www.cisc.at/>
 Check Point : <http://www.checkpoint.com>
 Confidex : <http://www.confidex.com/>
 Deister Electronic : <http://www.deister.com>
 EM Microelectronic Marin : <http://www.emmicroelectronic.com>
 Feig : <http://www.feig.de/home.html>
 Fréquentiel : <http://www.frequentiel.com>
 HID : <http://www.hidglobal.com>
 IBM : <http://www.ibm.com>
 IER : <http://www.ier.fr>
 Impinj : <http://www.impinj.com>
 Intermec : <http://www.intermec.fr>
 Intellident : <http://www.intellident.co.uk>
 Ipico : <http://www.ipico.com>
 IRIS : <http://www.iris-rfid.com>
 Lyngsoe : <http://www.lyngsoesystems.com/frontpage/frontpage.asp>
 Maintag : <http://www.maintag.com>
 Murata : <http://www.murata.com>
 Nedap : <http://nedap.fr>
 Néopost ID : <http://www.neopost-id.com>
 NXP : <http://www.nxp.com>
 Odin : <http://www.odintechnologies.com>
 Omni Id : <http://www.omni-id.com>
 Orange Business : <http://www.orange-business.com/fr/entreprise/thematiques/m2m/solutions/rfid/tracabilite.jsp>
 Psion Teklogix : <http://www.psion.com>
 Sato : <http://www.satovicinity.com/fr/>
 Smart Packaging Solutions : <http://www.s-p-s.com>
 Smartrac : <https://www.smartrac-group.com/>
 ST Microelectronics : <http://www.st.com>

STID : <http://www.stid.com>
 Symbol : <http://www.symbol.com>
 Tageos : <http://www.tageos.com>
 Tagsys : <http://www.tagsysrfid.com>
 Texas Instruments : <http://www.ti.com>
 ThingMagic : <http://www.thingmagic.com>
 Zebra Technologies Corporation : <http://www.zebra.com>

Organismes – Fédérations – Associations (liste non exhaustive)

Connectwave : Centre National de Référence RFID
<http://www.connectwave.fr>
 RAIN :
<http://www.rainrfid.org/>
 FILRFID : Association des industriels intégrateurs, conseils et éditeurs de logiciels RFID
<http://www.filrfid.org>
 RFIDConnect : Social networking community for RFID business and technology leaders
<http://www.rfidconnect.com>
 EPC Global : Industry-driven standards for the Electronic Product Code (EPC) to support the use of Radio Frequency Identification (RFID)
<http://www.epcglobalinc.org>
 Délégation Générale de la Compétitivité, de l'Industrie et des Services
<http://www.telecom.gouv.fr/rfid>

Documentation – Formation – Séminaires (liste non exhaustive)

Connectwave : Centre National de Référence RFID
<http://www.connectwave.fr>

Laboratoires – Bureaux d'études – Écoles – Centres de recherche (liste non exhaustive)

ISO/IEC/JTC1/SC31 automatic identification and data capture
<http://www.iso.org>
 AFNOR comité miroir CN31
<http://www.afnor.org>
 ICNIRP International Commission on Non Ionizing Radiation Protection
<http://www.icnirp.de>
 ETSI European Telecommunication Standard Institute
<http://www.etsi.org>

CENELEC Comité Européen de Normalisation Electrotechnique

<http://www.cenelec.eu>

CEN/TC225 Comité Européen de Normalisation

<http://www.cen.eu>

CEA-Leti, Grenoble, laboratoire :

<http://www.leti.fr>

Emitech, Paris, Montpellier, laboratoire :

<http://www.emitech.fr>

FIME, Caen, Laboratoire :

<http://www.fime.com>

INRIA, Lille, Laboratoire :

<http://www.inria.fr/lille>

IM2NP, Marseille, laboratoire :

<http://www.im2np.fr>

Kéolabs, Salon de Provence, laboratoire :

<http://www.soliat-lab.com>

LCIS, Valence, laboratoire :

<http://lcis.grenoble-inp.fr>

LEAT, Sophia Antipolis, laboratoire :

<http://leat.unice.fr>

LNE, Trappes, laboratoire :

<http://www.lne.fr>

Mind Microtec, Archamps, laboratoire :

<http://www.mind-microtec.org>

RFTLab, Valence, laboratoire :

<http://www.rftlab.com>

XLim, Limoges, laboratoire :

<http://www.xlim.fr/>

ECE, Paris, école :

<http://www.ece.fr>

ENSEA, Cergy Pontoise, école :

<http://www.ensea.fr>

ENSI, Caen, école :

<http://www.ensicaen.fr>

ENSM-SE, Gardanne, école :

<http://www.emse.fr/spip/-CMP-.html>

ENST, Paris, école :

<http://www.telecom-paristech.fr>

ESE, Gif sur Yvette, Rennes, école :

<http://www.supelec.fr>

ESEO, Angers, école :

<http://www.eseo.fr>

ESIEE, Noisy le Grand, école :

<http://www.esiee-paris.fr>

ESIGETEL, Avon, école :

<http://www.esigetel.fr>

ESISAR, Valence, école :

<http://esisar.grenoble-inp.fr>

INT, Evry, école :

http://www.it-sudparis.eu/fr_accueil.html

ISEN, Toulon, école :

<http://www.isen.fr>

Université Paris Est, Marne la Vallée :

<http://www.univ-mlv.fr>

Gagnez du temps et sécurisez vos projets en utilisant une source actualisée et fiable



RÉDIGÉE ET VALIDÉE
PAR DES EXPERTS




MISE À JOUR
PERMANENTE



100 % COMPATIBLE
SUR TOUS SUPPORTS
NUMÉRIQUES



SERVICES INCLUS
DANS CHAQUE OFFRE

- + de 340 000 utilisateurs chaque mois
- + de 10 000 articles de référence et fiches pratiques
- Des Quiz interactifs pour valider la compréhension 

SERVICES ET OUTILS PRATIQUES



Questions aux experts*

Les meilleurs experts techniques et scientifiques vous répondent



Articles Découverte

La possibilité de consulter des articles en dehors de votre offre



Dictionnaire technique multilingue

45 000 termes en français, anglais, espagnol et allemand



Archives

Technologies anciennes et versions antérieures des articles



Info parution

Recevez par email toutes les nouveautés de vos ressources documentaires

*Questions aux experts est un service réservé aux entreprises, non proposé dans les offres écoles, universités ou pour tout autre organisme de formation.

Les offres Techniques de l'Ingénieur



INNOVATION

- Éco-conception et innovation responsable
- Nanosciences et nanotechnologies
- Innovations technologiques
- Management et ingénierie de l'innovation
- Smart city – Ville intelligente



MATÉRIAUX

- Bois et papiers
- Verres et céramiques
- Textiles
- Corrosion – Vieillessement
- Études et propriétés des métaux
- Mise en forme des métaux et fonderie
- Matériaux fonctionnels. Matériaux biosourcés
- Traitements des métaux
- Élaboration et recyclage des métaux
- Plastiques et composites



MÉCANIQUE

- Frottement, usure et lubrification
- Fonctions et composants mécaniques
- Travail des matériaux – Assemblage
- Machines hydrauliques, aérodynamiques et thermiques
- Fabrication additive – Impression 3D



ENVIRONNEMENT – SÉCURITÉ

- Sécurité et gestion des risques
- Environnement
- Génie écologique
- Technologies de l'eau
- Bruit et vibrations
- Métier : Responsable risque chimique
- Métier : Responsable environnement



ÉNERGIES

- Hydrogène
- Ressources énergétiques et stockage
- Froid industriel
- Physique énergétique
- Thermique industrielle
- Génie nucléaire
- Conversion de l'énergie électrique
- Réseaux électriques et applications



GÉNIE INDUSTRIEL

- Industrie du futur
- Management industriel
- Conception et production
- Logistique
- Métier : Responsable qualité
- Emballages
- Maintenance
- Traçabilité
- Métier : Responsable bureau d'étude / conception



ÉLECTRONIQUE – PHOTONIQUE

- Électronique
- Technologies radars et applications
- Optique – Photonique



TECHNOLOGIES DE L'INFORMATION

- Sécurité des systèmes d'information
- Réseaux Télécommunications
- Le traitement du signal et ses applications
- Technologies logicielles – Architectures des systèmes
- Sécurité des systèmes d'information



AUTOMATIQUE – ROBOTIQUE

- Automatique et ingénierie système
- Robotique



INGÉNIERIE DES TRANSPORTS

- Véhicule et mobilité du futur
- Systèmes aéronautiques et spatiaux
- Systèmes ferroviaires
- Transport fluvial et maritime



MESURES – ANALYSES

- Instrumentation et méthodes de mesure
- Mesures et tests électroniques
- Mesures mécaniques et dimensionnelles
- Qualité et sécurité au laboratoire
- Mesures physiques
- Techniques d'analyse
- Contrôle non destructif



PROCÉDÉS CHIMIE – BIO – AGRO

- Formulation
- Bioprocédés et bioproductions
- Chimie verte
- Opérations unitaires. Génie de la réaction chimique
- Agroalimentaire



SCIENCES FONDAMENTALES

- Mathématiques
- Physique Chimie
- Constantes physico-chimiques
- Caractérisation et propriétés de la matière



BIOMÉDICAL – PHARMA

- Technologies biomédicales
- Médicaments et produits pharmaceutiques



CONSTRUCTION ET TRAVAUX PUBLICS

- Droit et organisation générale de la construction
- La construction responsable
- Les superstructures du bâtiment
- Le second œuvre et l'équipement du bâtiment
- Vieillessement, pathologies et réhabilitation du bâtiment
- Travaux publics et infrastructures
- Mécanique des sols et géotechnique
- Préparer la construction
- L'enveloppe du bâtiment
- Le second œuvre et les lots techniques