TECHNIQUES
DE L'INGÉNIEUR

Réf. : **E1470 V2**

Systèmes et techniques RFID

Date de publication :
10 novembre 2015

Cet article est issu de : **Électronique - Photonique | Électronique**

par **Claude TETELIN**

Mots-clés
RFID | téléalimentation | radiofréquences | télécommunications

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 téléalimentation 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 | radiofrequency | telecommunication

Abstract Natural continuation of the barcode or the cornerstone of the Internet of Things, the RFID (Radio Frequency Identification) create 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

Systèmes et techniques RFID

par **Claude TETELIN**

Ingénieur ISEN, Docteur de l'Université de Lille, France
Directeur technique du Centre National RFID,
Président de la commission nationale AFNOR CN31

Note de l'éditeur

Cet article est la réédition actualisée de l'article E1470 intitulé « Systèmes et techniques RFID » paru en 2010, rédigé par Claude TETELIN

Insérer une clé pour démarrer un véhicule, 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 sont des gestes entrés dans le quotidien de bon nombre d'entre nous. Nous utilisons, sans en être toujours conscients, des technologies de capture automatique de données basées sur les ondes et rayonnements radiofréquence. Cette technologie est connue sous le nom de RFID pour Identification RadioFréquence. De même que chaque individu peut être identifié grâce à un passeport biométrique ou encore un badge d'accès personnel, les objets sont aujourd'hui de plus en plus

souvent porteurs d'étiquettes RFID contenant un identifiant unique et parfois quelques bytes ou kilobytes de données. La différence entre les objets et nous, c'est qu'ils ne présentent pas « volontairement » leur étiquette ou badge RFID lorsqu'on leur demande. Les conditions de lecture de ces étiquettes sont donc différentes et demandent généralement des distances de détection plus importantes. 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 téléalimentation, de télécommunications et d'encodage. 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 (pile ou batterie) est simplement inconcevable. Le tag serait trop volumineux, 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 la fournir. L'antenne de notre étiquette va non seulement servir pour communiquer avec l'interrogateur mais va également servir à capter l'énergie radiofréquence issue de ce dernier. On parle alors de téléalimentation ou alimentation à distance.

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 téléalimentation, 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 téléalimentation 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 (impédance, surface équivalente radar). Ceci va avoir pour effet de modifier les caractéristiques (amplitude et/ou phase) du signal réfléchi par le tag vers l'interrogateur. Cette technique, appelée **rétromodulation** est la base de communication 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'embarquer, dans ces tags passifs, une source d'énergie propre. Celle-ci sert alors à alimenter des « périphériques » au tag RFID comme des capteurs ou sert à améliorer les performances

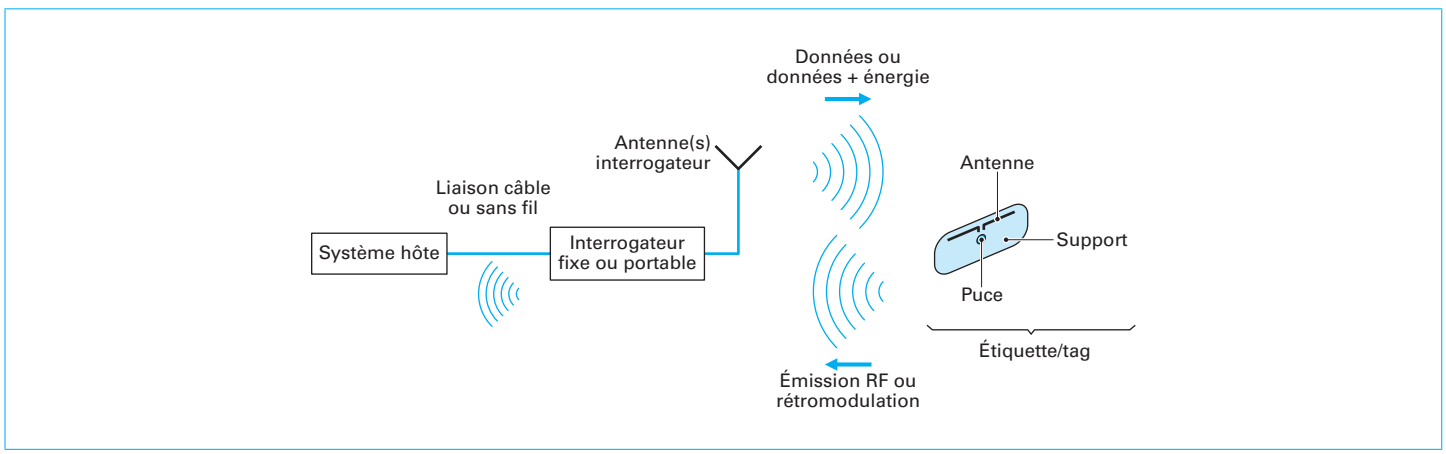


Figure 1 – Les éléments principaux d'un système RFID

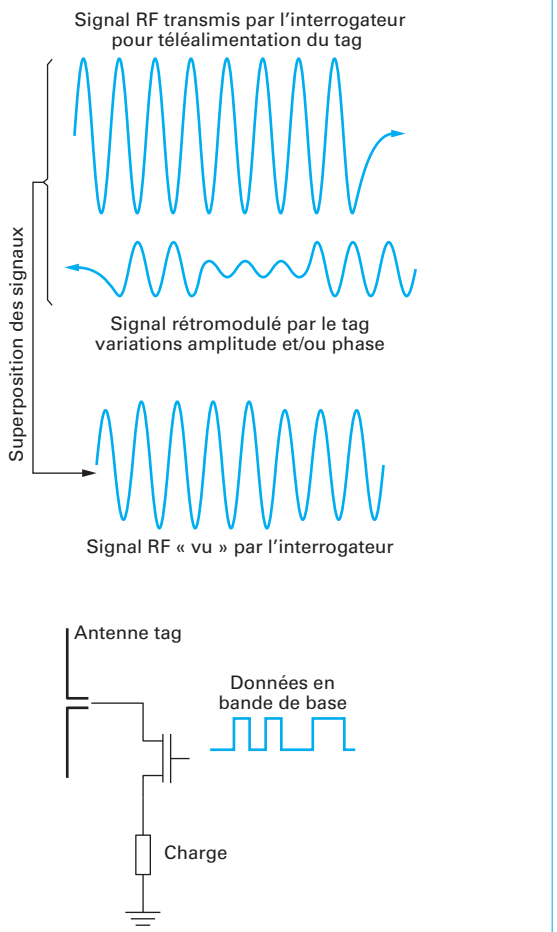


Figure 2 – Principe de la rétromodulation pour les tags passifs

globales du tag. La méthode de communication du tag vers le lecteur restant basée sur la rétromodulation, on est toujours dans le cas de tags passifs, ils sont simplement assistés d'une source d'énergie propre. On parle alors de **RFID BAP (*Battery Assisted Passive*)**.

La RFID n'est pas la seule technologie permettant la saisie automatique de données (avec geste volontaire ou non) et/ou l'identification. Les codes à barres (1D ou 2D), la reconnaissance optique de caractères sont largement répandus et ont l'avantage d'être (pour leur forme la plus simple) relativement bon marché. Cependant, la RFID a, par rapport à ces techniques, certains avantages que nous allons détailler ci-dessous.

Basée sur le rayonnement ou la propagation d'ondes électromagnétiques, la technologie RFID **ne requiert pas de visibilité optique** pour la lecture des étiquettes. Bien sûr, le métal et certains matériaux peuvent fortement perturber cette lecture.

Un deuxième avantage est que la lecture se fait **sans contact**. Suivant les fréquences et/ou les tailles d'étiquettes, la distance à laquelle une étiquette peut être lue varie de quelques millimètres à quelques mètres en technologie passive sans batterie. En technologie active (avec un émetteur RF à bord du tag RFID), cette distance peut dépasser la centaine de mètres sans difficultés.

Un autre avantage à mettre à l'actif de la technologie RFID est sa capacité **à 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 ceux les plus importants) réside dans le fait que cette technologie est **basée sur une puce électronique**. Son contenu est par définition le numéro (unique) d'identification de l'objet auquel le tag sera attaché. Suivant l'application, ce numéro unique d'identification peut être plus ou moins long. La technologie EPC (*Electronic Product Code*) prévoit un numéro d'identification sur 96 bits. Cela laisse imaginer jusque 2^{96} ou 8^{32} identifiants différents ou encore près de 8.10^{28} possibilités. Pour 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. On pourrait donc, avec 96 bits, identifier individuellement chaque grain de riz produit sur la terre pendant huit mille milliards d'années. Au-delà de cet identifiant, la puce peut posséder une zone mémoire programmable ou réinscriptible permettant à l'utilisateur d'accéder à de l'information directement en lisant le contenu de cette mémoire. Il peut également compléter ou modifier cette information lors des étapes de la vie de l'objet. Cette information peut bien sûr être cryptée et la zone mémoire peut être partagée par plusieurs utilisateurs avec une gestion des droits d'accès.

Avec toutes ces caractéristiques, nous voyons bien que la question qui vient rapidement à l'esprit lorsque l'on parle d'un système RFID : « à quelle distance puis-je lire une étiquette RFID ? » est bien sûr importante mais ne peut être que la première d'une longue série au cours de laquelle l'utilisateur potentiel devra décomposer son processus et parfois remettre en cause ses principes pour tirer parti du meilleur de cette technologie.

2. Familles de systèmes RFID et caractéristiques

L'identification par radiofréquences ou RFID est basée sur le fait que des informations contenues dans une puce électronique peuvent être transmises sans contact via un lien RF 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 classifier 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. On parle également de fonctionnement 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 active) ou qu'elle ne fait que rétromoduler un signal RF issu de l'interrogateur (on parle alors de RFID passive). 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 que la puce embarquée sur l'étiquette est en lecture seule ou

que l'on peut écrire (une fois ou plusieurs fois) de nouvelles informations 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 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 correctement la puce électronique. Les systèmes actifs doivent donc prévoir l'embarquement d'une source d'énergie propre à l'étiquette. Ajouté au fait que la puce possède son propre circuit d'émission, cela peut augmenter fortement le coût de l'étiquette RFID. La norme ISO/IEC 18000-7 prévoit le fonctionnement de systèmes actifs à 433 MHz. Avec de tels systèmes, 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 quant à lui sur la rétromodulation de l'onde provenant de l'interrogateur. Cette onde (ou ce champ) est alors partiellement réfléchie par l'étiquette. Quels que soient les fréquences ou les modes de couplage, le moyen utilisé pour réaliser cette rétromodulation, consiste à commuter une charge (impédance) placée en parallèle entre la puce électronique et l'antenne de l'étiquette.

Nota : il est clair que ce système de commutation de charge fait partie intégrante de la puce RFID.

Le signal réfléchi par l'étiquette vient alors se superposer au signal provenant de l'interrogateur. Dans le cas, très majoritairement rencontré, des étiquettes passives ne possédant pas de source d'énergie embarquée, le rapport entre la puissance du signal émis par l'interrogateur (pour alimenter la puce) et la puissance du signal rétromodulé par l'étiquette peut atteindre 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 meilleure charge 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, séparant ces notions de la présence ou non de source d'énergie embarquée par l'étiquette.

Dans la majorité des cas, la distance de communication entre une étiquette passive et son interrogateur est limitée par la distance de téléalimentation (sauf dans les cas, de plus en plus rares, où l'interrogateur n'a pas la sensibilité nécessaire). Une manière d'augmenter cette distance est d'ajouter à l'étiquette une source d'énergie propre. Cette source d'énergie va permettre d'alimenter le circuit de la puce électronique sans pour autant devoir capter l'énergie issue du signal RF transmis par l'interrogateur. Cette

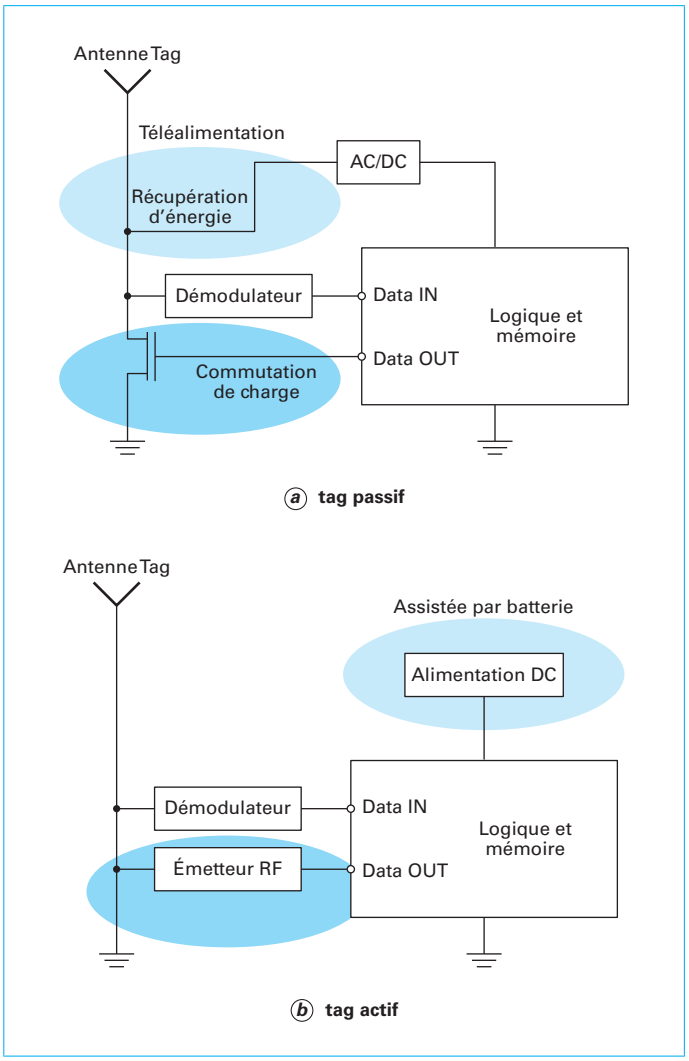


Figure 3 – Schémas de principe des étiquettes (*a*) passive et (*b*) active

source d'énergie peut également servir à alimenter d'autres systèmes électroniques associés à l'étiquette RFID comme des capteurs. L'étiquette RFID peut alors récupérer de l'information issue de ces capteurs, la stocker dans une zone mémoire particulière de la puce électronique sans pour autant être dans le champ rayonné par un interrogateur. Ces systèmes, appelés BAP (*Battery Assisted Passive*), se comportent comme des systèmes passifs sans source d'énergie une fois cette source épuisée.

2.2 Champ proche ou champ lointain

Les systèmes RFID passifs peuvent fonctionner à différentes fréquences. Dans un premier temps, l'interrogateur doit émettre un signal permettant la téléalimentation de la ou des étiquettes présentes à proximité. Pour rayonner et de la même manière recevoir un signal radio, il faut se poser la question de l'antenne la mieux 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 dans leur entourage proche alors que les secondes créeront plutôt un champ électrique. Au fur et à mesure que l'on s'éloigne de la

structure rayonnante, le champ électromagnétique 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 est formé dépend de la fréquence du signal et des dimensions de l'antenne.

La figure **4** 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. 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].

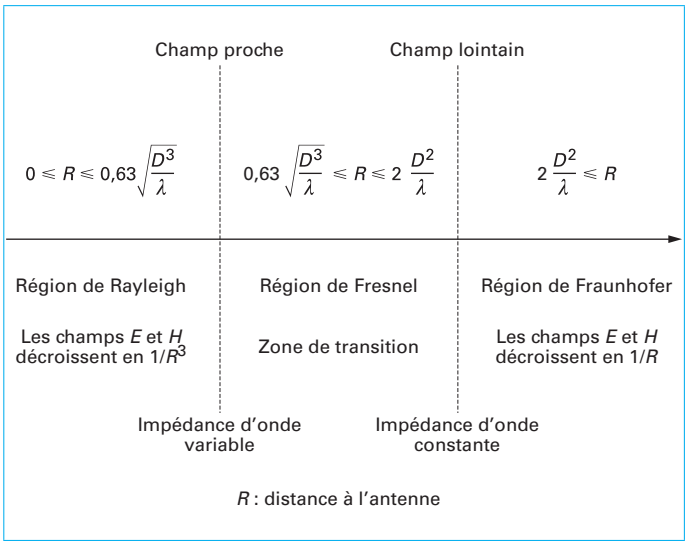


Figure 4 – Définition des zones de champs proche et lointain

Prenons l'exemple de système RFID fonctionnant **à 13,56 MHz**. Dans l'air (ou dans le vide), la longueur d'onde associée à cette fréquence est de plus de 22 m. Vu les champs maximaux que l'on est autorisé à rayonner, les distances auxquelles on pourra lire une étiquette ne dépasseront jamais 1 à 2 m. Cela signifie que les systèmes RFID fonctionnant à cette fréquence seront toujours dans la zone de champ proche. On peut alors se poser la question du type d'antenne. Allons-nous rayonner principalement un champ électrique (antenne dipôle) ou un champ magnétique (antenne boucle). Pour rayonner correctement un champ électrique, une antenne doit avoir des dimensions proches de la longueur d'onde. Avec des étiquettes de l'ordre de 22 m, aucune application RFID n'aurait pu voir le jour à 13,56 MHz. Le choix est donc par défaut celui des **antennes boucle** créant un champ magnétique.

Si on travaille à présent **à 900 MHz**, la longueur d'onde est d'environ 33 cm dans l'air libre. Les puissances que l'on peut rayonner dans cette gamme de fréquence permettent d'envisager des distances de communication comprises classiquement entre 5 et 10 m. Nous sommes cette fois dans la zone où le champ électromagnétique est formé. On peut véritablement parler de propagation d'onde entre l'interrogateur et l'étiquette. Se pose encore une fois le choix entre des antennes boucle ou des antennes de type dipôle. Cette fois, la taille du dipôle optimal est de l'ordre de $\lambda/2$ c'est-à-dire 15 cm. Cette taille est tout à fait compatible avec les contraintes des applications RFID. 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 choix des **antennes de type dipôle électrique** est tout à fait logique.

Pour être tout à fait complet, nous pouvons remarquer que la notion de champ proche peut parfaitement s'appliquer pour des systèmes RFID UHF. En effet, si l'étiquette se rapproche de l'antenne de l'interrogateur, le champ n'est pas encore formé et nous sommes dans un régime de champ proche. Dans ce cas, on peut très bien utiliser une antenne boucle pour récupérer le champ magnétique comme dans les applications RFID HF.

Les bandes de fréquence dans lesquelles peuvent fonctionner les systèmes RFID font partie des bandes non soumises à licence. Ces bandes, réservées aux applications industrielles, scientifiques et médicales (bandes ISM), si elles ne sont pas soumises à licence, ne sont utilisables qu'en respectant scrupuleusement des gabarits d'émission (largeur de bande autorisée, puissance ou champ maximal à ne pas dépasser, taux d'occupation à respecter). Les utilisateurs de ces bandes veilleront à respecter les règlements et régulations propres à chaque région du globe où sera déployée l'application RFID. Ceci sans compter les règlements liés à la sécurité sanitaire et à l'exposition humaine aux rayonnements non ionisants (la RFID n'utilise pas encore de rayons X ou gamma !). La figure **5** synthétise les fréquences couramment utilisées pour les applications RFID.

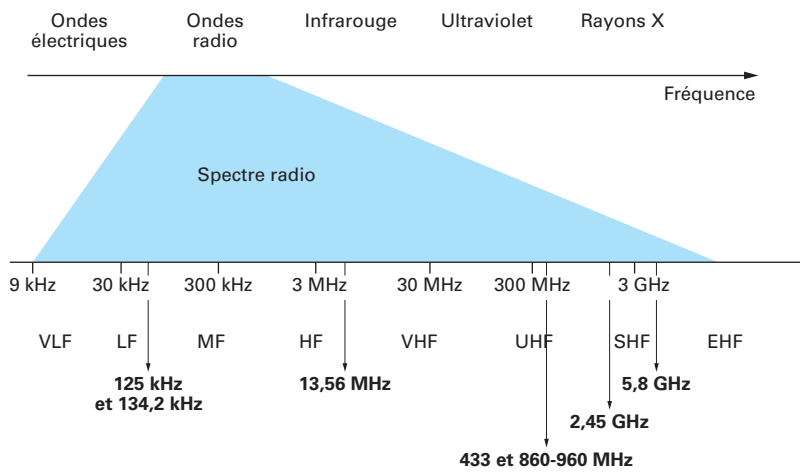


Figure 5 – Fréquences couramment utilisées en RFID

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 embarquée sur l'étiquette. 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. 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 certains cas, le numéro unique gravé par le fondeur de la puce n'est pas suffisant pour l'application finale. On peut donc trouver des puces possédant une zone mémoire vierge sur laquelle on puisse écrire un numéro particulier propre à l'utilisateur final du système RFID (comme le code EPC (*Electronic Product Code*) par exemple). Une fois ce numéro écrit, il ne peut plus être modifié. On parle alors de **puce à mémoire WORM** (*Write Once, Read Multiple*).

D'autres types d'application 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'opération de maintenance en zone isolée ou sur le théâtre d'opérations militaires). Les puces sont alors de **type MTP** (*Multi Time Programmable*) et possèdent de la mémoire généralement de type 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 une classique 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 sont *batteryless* (sans source d'énergie embarquée), 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, la communication entre l'interrogateur et l'étiquette n'a pas, à proprement parler, débuté. Une fois la puce de l'étiquette 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.

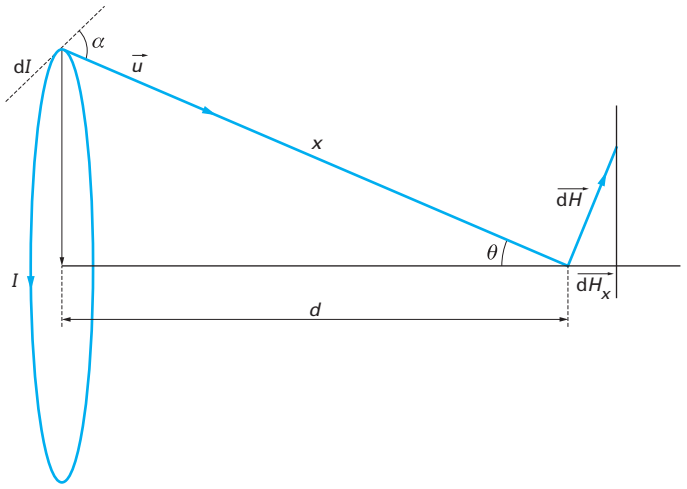
Parmi les avantages du protocole TTF, on peut noter la rapidité avec laquelle il est possible d'identifier une étiquette quand celle-ci est seule dans le champ rayonné par l'interrogateur. On peut également noter que lorsque l'interrogateur ne communique pas avec des étiquettes, il ne fait que rayonner 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 (*trigger*) 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.

3. Téléalimentation des étiquettes RFID

Comme nous l'avons vu dans les paragraphes précédents, la plupart des étiquettes RFID n'embarquent pas de source d'énergie. La première mission de l'interrogateur est donc de téléalimenter la puce électronique présente sur l'étiquette. Suivant les fréquences utilisées et les distances de téléalimentation 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 fonctionnant à 13,56 MHz ou à des fréquences inférieures, la taille des antennes électriques qu'il faudrait déployer est incompatible avec les contraintes des applications. Les antennes boucle créant principalement un champ magnétique en zone de Rayleigh sont donc préférées. Par contre, pour les applications RFID en UHF ou SHF, le système fonctionnera plutôt en champ lointain et la taille des antennes électriques devient compatible avec les contraintes géométriques des applications.

3.1 Téléalimentation 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 $A.m^{-1}$) créé par le courant



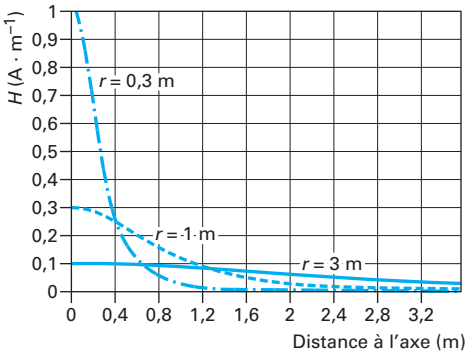


Figure 6 – Spire parcourue par un courant et champ magnétique résultant

d'intensité I parcourant une spire de rayon r sur un point de l'axe de la spire situé à une distance d. Le résultat est donné dans l'équation suivante :

$$H_x = \frac{Ir^2}{2\,(r^2+d^2)^{3/2}} \qquad \textbf{(1)}$$

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 $I/2r$, 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 téléalimentation 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 téléalimenté 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 l'induction magnétique. Il suffit de remarquer que le flux de l'induction magnétique à travers la spire peut s'écrire :

$$\Phi = \oiint_s \vec{B}.\vec{ds} \approx B_{(d=0)}\, Ns$$

avec N nombre de tours de l'antenne spire,

s 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 H) :

$$L = \frac{N^2 \mu \pi r}{2} \qquad \textbf{(2)}$$

L'induction magnétique B (en T ou V.s.m^{-2}) peut à présent s'écrire en fonction de l'inductance, de la tension U appliquée à ses bornes et de la fréquence f :

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

Dans l'équation (3), il faut bien noter que L est une fonction des dimensions de l'antenne (voir l'équation (2)). 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) étiquette interrogateur connue et fixée, la taille de l'antenne peut être facilement optimisée pour maximiser le champ magnétique créé.

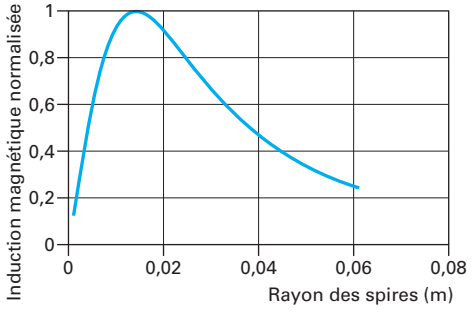


Figure 7 – Induction magnétique à distance fixée en fonction de la taille d'antenne

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 (4)) disant que toute variation de flux de champ magnétique à travers un circuit fermé crée une différence de potentiel à ses bornes :

$$e = \oint_{\Gamma} -\frac{\partial \vec{A}}{\partial t} = -\frac{\partial}{\partial t} \iint_{\Sigma} \overrightarrow{\text{rot}}\, \vec{A} \cdot \overrightarrow{ds} = -\frac{\partial}{\partial t} \iint_{s} \vec{B} \cdot \overrightarrow{ds} = -\frac{\partial \Phi}{\partial t} \qquad \textbf{(4)}$$

avec $\vec{A}$ (Wb.m^{-1}) potentiel vecteur,

e (V) différence de potentiel induite.

L'antenne de l'étiquette RFID est donc naturellement une boucle. La figue **8** schématise le couplage entre les antennes de l'interrogateur et de l'étiquette. Dans les applications RFID, seule une partie du flux magnétique créée par l'interrogateur est « captée » par l'étiquette.

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 :

$$k = \frac{\Phi_{usefull}}{\Phi_{complete}} = \frac{M}{\sqrt{L_1 L_2}} \qquad \textbf{(5)}$$

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 %.

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.

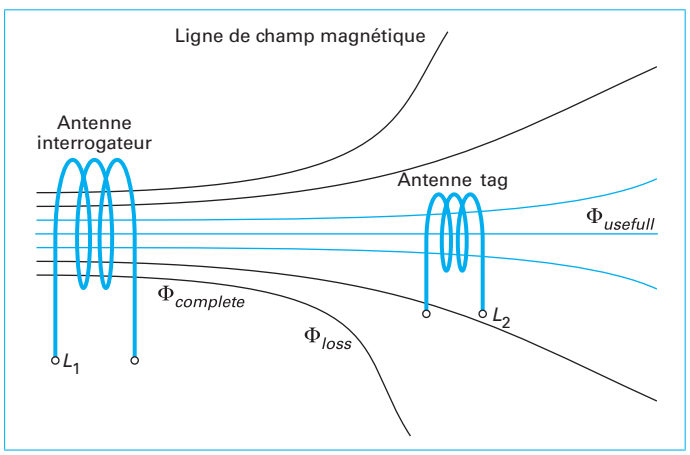


Figure 8 – Couplage magnétique entre antennes interrogateur et étiquette

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 la relation :

$$C_i = \frac{1}{L_i \omega^2} \quad \text{avec} \quad i = 1 \text{ ou } 2 \qquad \textbf{(6)}$$

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.

$$Z_1 = j\omega L_1 - \frac{\omega^2 M^2}{Z_2 - j\omega L_2} \quad \text{avec} \quad Z_2 = R_2 + R_{ic} \,//\, \frac{1}{jC_2\omega} \qquad \textbf{(7)}$$

avec Z_1 et Z_2 en Ω.

En combinant les équations (7) et (5), on obtient une expression de l'impédance faisant intervenir le coefficient de couplage. Au final, l'impédance « vue » par le générateur peut s'écrire :

$$Z_{\text{générateur}} = R_1 + \frac{1}{jC_1\omega} + j\omega L_1 - \frac{\omega^2 k^2 L_1 L_2}{Z_2 - j\omega L_2} \qquad \textbf{(8)}$$

À la pulsation de résonance, et uniquement à cette pulsation, les termes $1/jC_1\omega$ et $j\omega L_1$ se compensent et disparaissent de l'équation (8).

Partant du schéma de la figure **9**, il est également possible de calculer la fonction de transfert entre la tension appliquée aux bornes de l'antenne de l'interrogateur et la tension présente aux bornes du circuit électronique de la puce. La figure **10** montre les résultats de simulation pour trois valeurs de coefficient de couplage différents pour un système HF à 13,56 MHz.

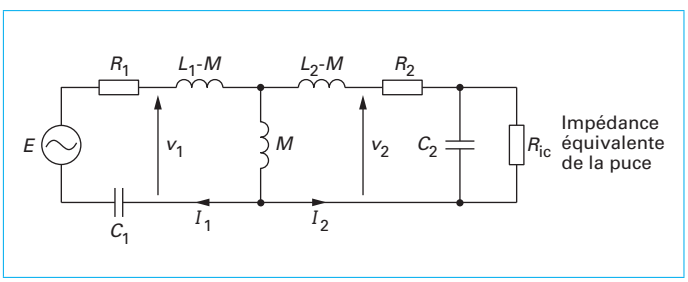


Figure 9 – Schéma électrique équivalent en RFID HF

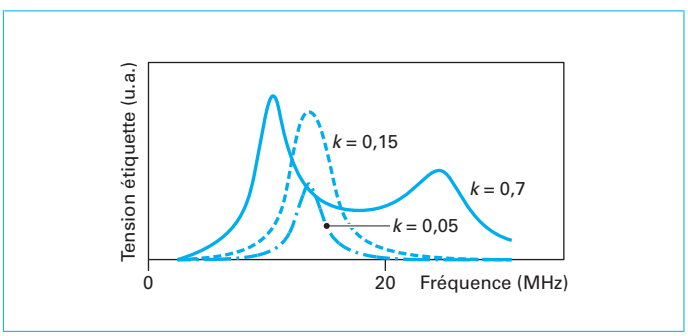


Figure 10 – Variation de tension simulée aux bornes du tag en fonction de la fréquence pour différents coefficients de couplage

Lorsque le coefficient de couplage est nul, aucun transfert d'énergie n'est possible entre l'interrogateur et le tag et la tension à ses bornes est nulle. Lorsque *k* commence à augmenter, 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 téléalimentation 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].

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} n'est qu'une première approximation. Une capacité d'entrée est généralement présente en parallèle de cette résistance. Dans certaines notes d'application fournies par les fabricants de circuits intégrés, des designs d'antennes sont proposés. Ces antennes, avec leurs géométries et les matériaux qui les composent ont l'avantage de présenter une inductance en parfaite résonance avec la capacité interne des puces électroniques. Cela permet d'éviter aux fabricants d'étiquettes ou cartes sans contact d'avoir à intégrer un composant supplémentaire. Néanmoins, 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 Téléalimentation en UHF, équation de Friis

Lorsque la fréquence d'une onde électromagnétique augmente, sa longueur d'onde diminue. Dans les systèmes RFID UHF et SHF, il est courant de considérer que les tags reçoivent de l'interrogateur des champs électromagnétiques formés (zone de Fraunhofer, *cf.* figure **4**). Les antennes utilisées sont généralement des antennes basées sur le dipôle ou le patch. À ces fréquences, les antennes sont caractérisées par leur gain, leur polarisation et leur directivité [2] [E3284]. 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 d'une antenne peut donc s'écrire sous la forme :

$$Gain = \frac{\text{densité de puissance rayonnée par l'antenne dans la direction considérée à une distance } d}{\text{densité de puissance rayonnée par une antenne isotrope à la même distance } d} \quad \textbf{(9)}$$

Le gain G 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 suivante :

$$\Sigma = G\frac{\lambda^2}{4\pi} \quad \textbf{(10)}$$

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

$$P_{ant\text{-}tag} = P_{int} G_{ant\text{-}int} \frac{1}{4\pi d^2} \Sigma_{ant\text{-}tag} = P_{int} G_{ant\text{-}tag} G_{ant\text{-}int} \left(\frac{\lambda}{4\pi d}\right)^2 \quad \textbf{(11)}$$

Dans cette équation, $G_{ant–int}$ représente le gain de l'antenne de l'interrogateur et $G_{ant–tag}$ 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. L'équation (11) tient donc compte des positions des antennes l'une par rapport à l'autre (élévation et azimut). Pour calculer la distance maximale de téléalimentation d'une étiquette, il faut donc considérer les gains maximaux des antennes. Il est important de noter plusieurs choses concernant l'équation (11). La première est que $P_{ant–tag}$ 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 (équation (19)). La seconde est que l'atténuation $(4\pi d/\lambda)^2$ est celle correspondant à une propagation d'onde électromagnétique en espace libre (ellipsoïde de Fresnel dégagée de tout obstacle). Enfin, l'équation (11) ne tient pas compte des polarisations respectives des antennes. Le tableau **1** résume les atténuations supplémentaires 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 : $R_{ant–tag} = R_{puce}$ 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 re-rayonnée par l'antenne du tag.

Connaissant la puissance minimale nécessaire à l'alimentation de la puce (entre – 20 et – 10 dBm typiquement 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 téléalimentation. Ainsi, en tenant compte des régulations en

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

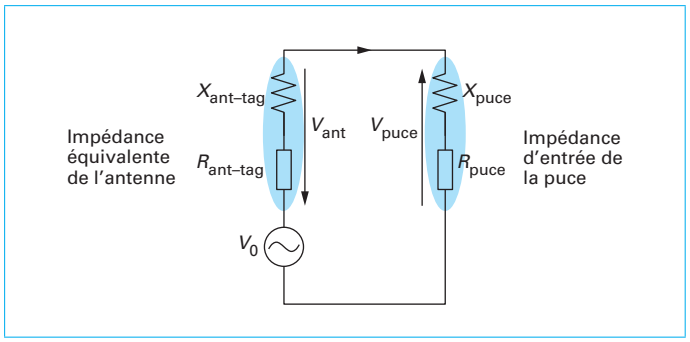


Figure 11 – Schéma électrique équivalent de l'antenne UHF et de la puce

vigueur dans les principales zones géographiques, des distances maximales de téléalimentation de l'ordre de 10 m peuvent être calculées. Le monde réel étant plus complexe, les imperfections font que les distances maximales mesurées sont plutôt de l'ordre de 6 à 7 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, des étiquettes sans source d'énergie embarquée. Pour les systèmes passifs, le rapport de puissance entre l'onde émise par l'interrogateur et celle réfléchie par le tag peut atteindre typiquement des valeurs de 40 à 60 dB. Il est clair que la gestion de l'énergie est tout à fait cruciale.

En ce qui concerne l'interrogateur, 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. Il va sans dire que faire un tel compromis est inenvisageable 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.

L'utilisation de composants résistifs n'intervient pas dans la réalisation de l'adaptation d'impédance à proprement parler mais peut servir à contrôler (généralement diminuer) le coefficient de qualité du système « générateur + antenne ». 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 téléalimentation du tag). Un gain de 3 dB en puissance est attendu entre un système simplement résonant et un système adapté.

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 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 téléalimentation) mais également pour connaître la proportion de puissance rerayonnée vers l'interrogateur (signal utile dans la communication tag vers interrogateur). Pour cela, nous devons définir le coefficient de réflexion en tension issu de la désadaptation entre deux impédances (ici $Z_{ant\text{-}tag}$ et Z_{puce}) :

$$\Gamma = \frac{Z_{puce} - Z_{ant\text{-}tag}}{Z_{puce} + Z_{ant\text{-}tag}} \text{ (sans unité)} \qquad \textbf{(12)}$$

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 :

$$T = 1 - |\Gamma|^2 \qquad \textbf{(13)}$$

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

$$T = \frac{4 R_{ant\text{-}tag} R_{puce}}{|Z_{ant\text{-}tag} + Z_{puce}|^2} \qquad \textbf{(14)}$$

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].

$$K = |1 - \Gamma|^2 = \frac{4 R_{ant\text{-}tag}^2}{|Z_{ant\text{-}tag} + Z_{puce}|^2} \qquad \textbf{(15)}$$

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

	Z_{puce}	*T*	*K*
Court-circuit	0	0	$\frac{4\,R^2_{ant\text{-}tag}}{R^2_{ant\text{-}tag}+X^2_{ant\text{-}tag}}$
Réactive	$-jX_{ant\text{-}tag}$	0	4
Circuit ouvert	infinie	0	0
Adaptation	$Z^*_{ant\text{-}tag}$	1	1

À partir des équations (14) et (15), 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.

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

4. Communication et codage des informations

Une fois les circuits des étiquettes RFID alimentés (par téléalimentation de l'interrogateur ou non), 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 *uplink*) ou d'un tag vers l'interrogateur (liaison *downlink*).

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 ne sont pas d'actualité. La modulation, quant à elle, 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 téléalimentés), 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 régulations 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. La question qui partage encore la communauté de la RFID est de savoir quel indice de modulation appliquer. Le schéma de la figure **12** montre les représentations temporelle et fréquentielle 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 (16). Pour comparaison, la profondeur de modulation est donnée par l'équation (17).

$$mi = \frac{A_{max} - A_{min}}{A_{max} + A_{min}} \quad \textbf{(16)}$$

$$md = \frac{A_{max} - A_{min}}{A_{max}} \quad \textbf{(17)}$$

Un signal modulé à 10 % présente de faibles variations d'amplitude propices à la téléalimentation 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. Au-delà des aspects concernant la robustesse de la modulation utilisée et de l'indice de modulation choisi, il est important d'intégrer les contraintes liées à la réglementation. La figure **13** représente le gabarit spectral que doivent respecter les signaux radiofréquences pour des communications centrées sur 13,56 MHz.

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 une telle pénurie. Il faudra donc associer cette modulation à des codes limitant au maximum le nombre de coupures (consécutives).

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 Class1 Generation 2) impose une profondeur comprise entre 82 et 100 %.

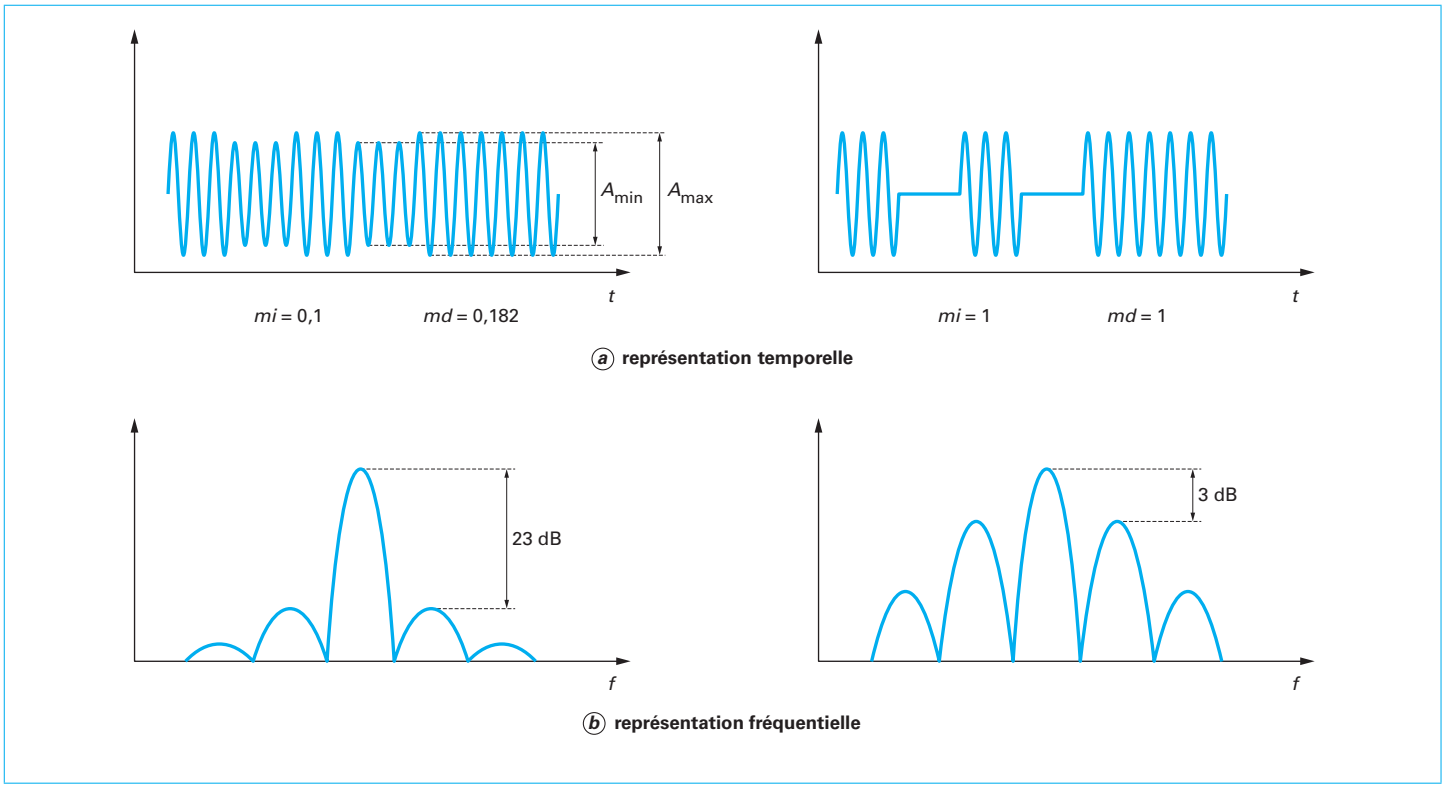


Figure 12 – Représentations temporelle et spectrale de signaux modulés en amplitude

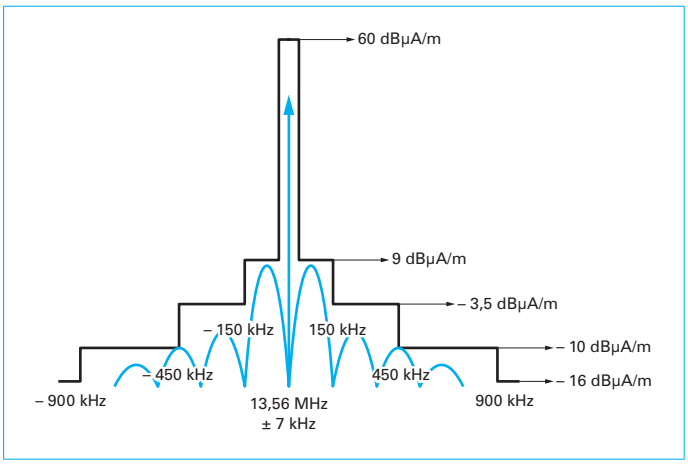


Figure 13 – Comparaison des spectres de signaux modulés en amplitude par rapport aux gabarits des régulations à 13,56 MHz (ETSI EN 300 330-1 v1.6.2)

Une autre manière de transporter l'information sur une porteuse radioélectrique est de modifier sa phase au rythme des données à transmettre. On sait que toute 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 n'étant pas spécialement larges, 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 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 téléalimentation vis-à-vis du codage employé. Bien qu'il ne s'agisse pas dans ce cas d'un problème lié à la téléalimentation, 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, 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 passive, le tag présentera un coefficient de qualité plus ou moins important sans que sa fréquence de résonance 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 :

$$Q_{int} = \frac{Q_{int\text{-}ant}}{1 + Q_{int\text{-}ant} Q_{tag} k^2} \quad \textbf{(18)}$$

avec $Q_{int–ant}$ centré coefficient de qualité de l'antenne de l'interrogateur,

k coefficient de couplage,

Q_{tag} coefficient de qualité du tag :

$$Q_{tag} = \frac{Q_{puce} Q_{tag\text{-}ant}}{Q_{puce} + Q_{tag\text{-}ant}}$$

Ce coefficient de qualité dépend du coefficient de qualité de la puce Q_{puce} et de celui de l'antenne du tag $Q_{tag\ –\ ant}$. 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 (11) peut être complétée 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 :

$$\frac{P_{ant\text{-}int}}{P_{int}} = G_{ant\text{-}int} \frac{1}{4\pi d^2} \sigma \frac{1}{4\pi d^2} \Sigma_{ant\text{-}int} = \frac{G^2_{ant\text{-}int} \lambda^2 \sigma}{(4\pi)^3 d^4} \quad \textbf{(19)}$$

Cette équation donne le rapport entre la puissance incidente appliquée par le générateur à l'antenne de l'interrogateur (P_{int}) et la puissance réfléchie au niveau de l'antenne de l'interrogateur ($P_{ant\text{-}int}$). Ce rapport fait apparaître la surface équivalente radar du tag RFID, σ (en m^2), encore appelée *Radar Cross Section* ou RCS. Cette surface peut être reliée au gain de l'antenne du tag et au coefficient de rerayonnement K, donné par l'équation (15) :

$$\sigma = \frac{K}{4\pi} \lambda^2 G^2_{ant\text{-}tag} \ PLF \quad \textbf{(20)}$$

Dans cette équation, *PLF* représente les pertes éventuelles dues à la polarisation (*cf.* tableau **1**).

Comme pour les systèmes RFID inductifs, la commutation d'une charge en parallèle de la puce électrique 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 court-circuit et le circuit ouvert. Dans les deux cas, ces charges compromettent fortement la téléalimentation de la puce ce qui les rend inutilisables d'un point de vue pratique. 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 téléalimentation. 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 pour-cent dans le meilleur des cas). Bien sûr, dans certains cas (UHF notamment), il est possible de séparer l'onde incidente servant à la téléalimentation de la puce électronique du tag, de l'onde réfléchie par ce tag. Il en résulte un meilleur rapport signal à bruit et une plus grande facilité de démodulation. Enfin, pour certains interrogateurs, la démodulation peut se faire en utilisant la technique IQ (*In Phase and Quadrature*) tirant partie des variations d'amplitude et de phase engendrées par la commutation de charges.

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). En RFID, nous avons insisté sur le fait que, pour les systèmes passifs, les communications *uplink* et *downlink* ne sont pas équivalentes. D'autre part, la technologie disponible au niveau de l'interrogateur est sans commune mesure avec les ressources disponibles au niveau des 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 trouver le codage ad hoc pour la liaison montante et le codage ad hoc pour la liaison descendante.

4.2.1 Codes dans la communication « uplink »

Pour les systèmes RFID téléalimentés, le code choisi devra permettre une gestion efficace de l'énergie. Ceci sera à rapprocher de la modulation qui lui sera associée. 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 une électronique trop évoluée). Une troisième caractéristique des codes utilisés dans la communication de l'interrogateur vers le tag concerne le respect des régulations des émetteurs radiofréquence. 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 dans les liaisons montantes.

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 rétromodulées 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 sur la figure **14** dans le cas d'un codage Manchester avec une sous-porteuse quatre fois plus élevée que la fréquence des données.

Tableau 3 – Principaux codes en liaison montante RFID

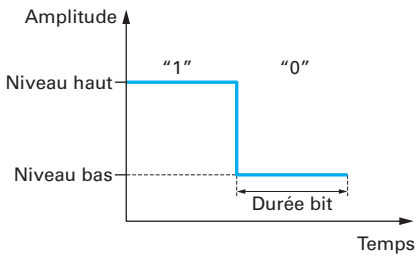
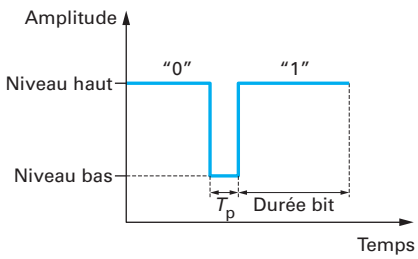
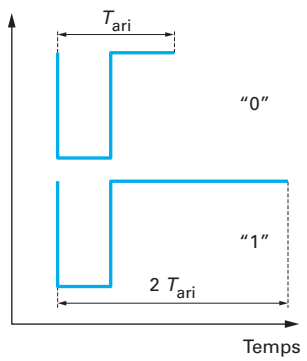
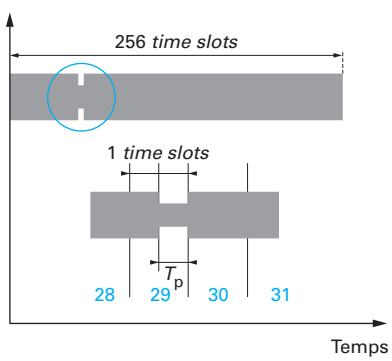
Nom	Représentation	Avantages/Inconvénients
NRZ (Non-Retour à Zéro) Durant toute la durée d'un bit, le signal reste dans un même état (haut ou bas)		– Peu de transitions – Faible efficacité énergétique + Simplicité
RZI *coded pulse* (Retour à Zéro Inversé) Un « 0 » logique est caractérisé par une impulsion de durée T_p, le « 1 » logique est représenté par un niveau haut		– 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	 T_{ari} : *reference time interval for a data -0 in interrogator-to-tag signalling*, d'après ISO 18000-63	+ 2 transitions à chaque bit + Création simple de symboles supplémentaires (SOF, EOF) – Le décodage nécessite une horloge – Débit variable suivant données transférées
PPM (*Pulse Position Modulation*) 1 parmi 256 La position de l'impulsion code 8 bits		+ Efficacité énergétique optimisée – Le décodage nécessite une horloge précise – Faibles débits

Tableau 3 – Principaux codes en liaison montante RFID (Suite)

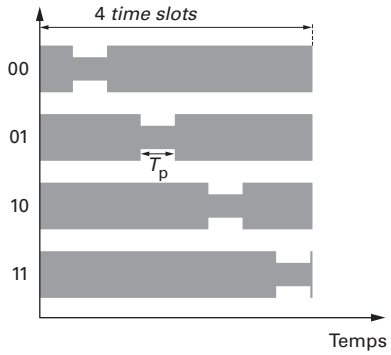
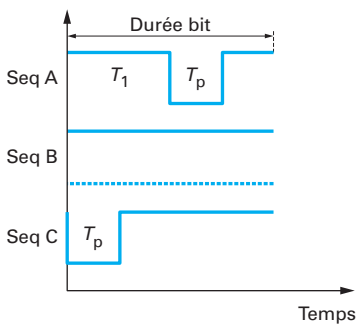
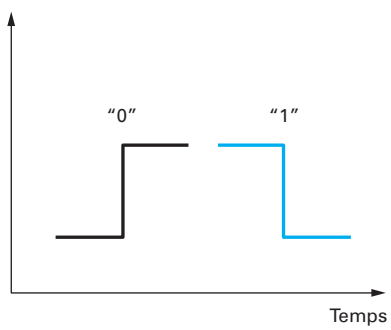
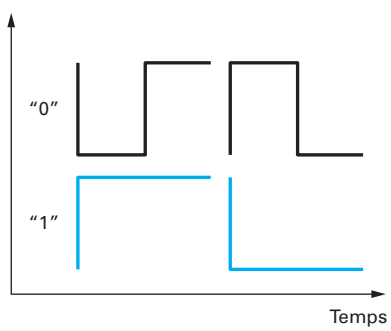
Nom	Représentation	Avantages/Inconvénients
PPM (*Pulse Position Modulation*) 1 parmi 4 La position de l'impulsion code 2 bits		+ Efficacité énergétique + Débits plus élevés qu'avec le code 1 parmi 256 – Le décodage nécessite une horloge

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 (*Bi-Phase Level*)		+ Détection des collisions au niveau bit + Transition systématique en milieu de bit
FM0 (*Bi-Phase Space*) « 0 » présente une transition au début et au milieu du bit « 1 » présente une transition au début du bit		+ Immunité aux bruits

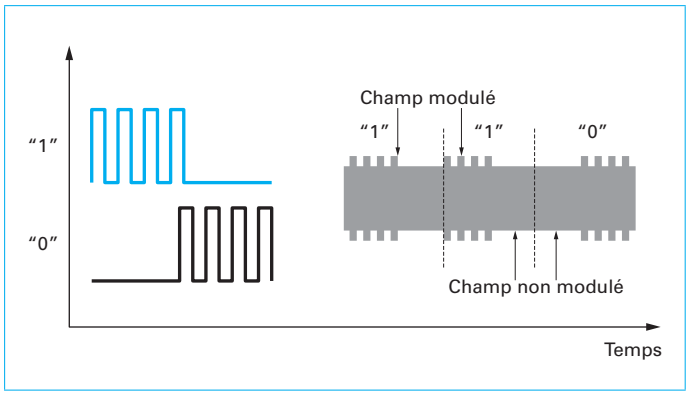


Figure 14 – Manchester codé sous-porteuse (représentation des bits et du signal rétromodulé)

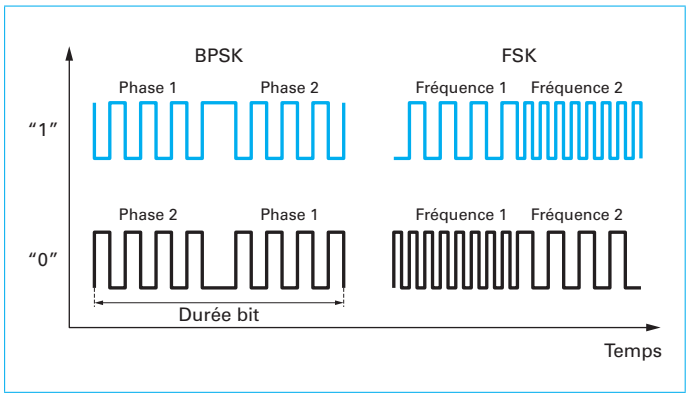


Figure 15 – Manchester codé sous-porteuse avec modulations BPSK et FSK

Le principal avantage de l'utilisation d'une sous-porteuse est de pouvoir translater 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 **15** 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 les références [R380] et [10].

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 stations de base. 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 d'éviter ce type de collision sont l'étalement de spectre (saut de fréquence), le principe de LBT (*Listen Before Talk*) ou l'ajustement dynamique de puissance.

Dans la suite de ce paragraphe, nous nous focalisons sur les collisions tags vers interrogateur qui sont les plus fréquentes dans les applications RFID. Pour les autres types de collision, le lecteur peut se référencer 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. Les algorithmes aléatoires sont généralement basés sur la transmission par l'interrogateur d'un nombre de *time slots* 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 **16** 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 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 **17** avec trois tags ayant des identifiants sur trois bits : tag 1 (001), tag 2 (011), tag 3 (110).

Uplink	1re itération Downlink	Uplink	2e itération Downlink	Uplink	3e itération Downlink	Uplink	...	Uplink
Req < 1111	Tag1 1010 Tag2 1011 Tag3 1110 Résultat 1C1C	Req < 1011	Tag1 1010 Tag2 1011 Tag3 NA Résultat 101C	Req < 1010	Tag1 1010 Tag2 NA Tag3 NA Résultat 1010	Select 1010		Unselect 1010

Uplink	1re itération Downlink	Uplink	2e itération Downlink	Uplink	...	Uplink	...
Req < 1111	Tag1 NA Tag2 1011 Tag3 1110 Résultat 1C1C	Req < 1011	Tag1 NA Tag2 1011 Tag3 NA Résultat 1011	Select 1011		Unselect 1011	

Figure 16 – Exemple de singulation déterministe

Uplink	1re itération Downlink	Uplink	2e itération Downlink	Uplink	3e itération Downlink	...	Uplink
Req	Tag1 (001) 0 Tag2 (011) 0 Tag3 (110) 1 Résultat C	Req 0	Tag1 (001) 0 Tag2 (011) 0 Tag3 (110) NA Résultat C	Req 0	Tag1 (001) 1 Tag2 (011) NA Tag3 (110) NA Résultat OK		Unselect Tag1

Uplink	1re itération Downlink	Uplink	2e itération Downlink	Uplink	3e itération Downlink	...	Uplink
Req	Tag1 (001) Na Tag2 (011) 0 Tag3 (110) 1 Résultat C	Req 0	Tag1 (001) NA Tag2 (011) 1 Tag3 (110) NA Résultat OK	Req 1	Tag1 (001) NA Tag2 (011) 1 Tag3 (110) NA Résultat OK		Unselect Tag2

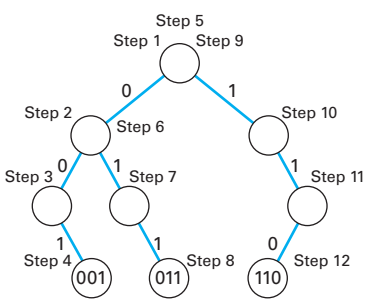


Figure 17 – Exemple de singulation déterministe bit à bit

D'autres variantes d'algorithmes déterministes peuvent être mises en place suivant la complexité de protocole que peut supporter le tag. 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

L'ensemble des 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 **18**.

Un des inconvénients majeurs de l'algorithme ALOHA présenté sur la figure **18** 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'espaces temporels (*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. Dans le cas où un seul tag aurait choisi un *time slot* particulier, son identifiant est décodé et une commande d'acquittement lui est transmise. Le processus recommence

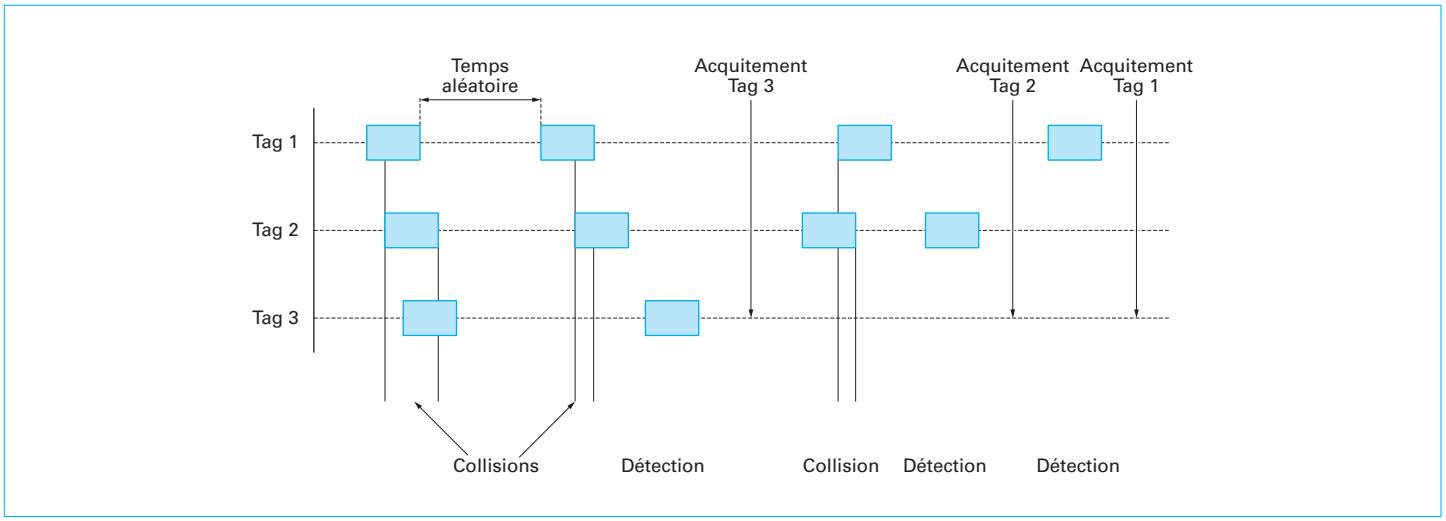


Figure 18 – Exemple de singulation aléatoire ALOHA

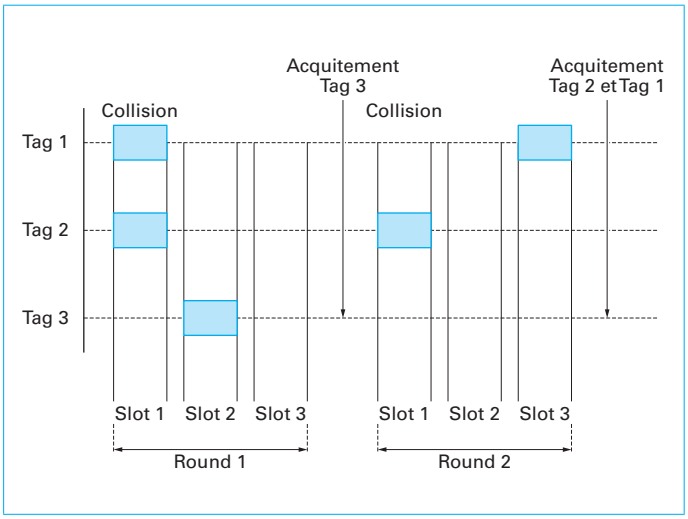


Figure 19 – Exemple de singulation aléatoire Frame Slotted ALOHA

jusqu'à ce qu'il n'y ait plus aucune collision. Cet algorithme est décrit sur la figure **19**.

Dans l'exemple de la figure **19**, l'interrogateur propose trois slots différents à trois tags présents dans le champ. Dans une première itération, les tags 1 et 2 répondent dans la 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 slots différents. 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 présent 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 slots proposés d'une itération à l'autre. Un exemple d'algorithme adaptatif est présenté sur la figure **20**.

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

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 comportera 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.

6. 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 paragraphe, 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 selon 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 tech-

Figure 20 – Exemple de singulation aléatoire Frame Slotted ALOHA adaptatif

nologies 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.

6.1 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 ». Au niveau du droit international, la recommandation 70-03 a été reprise par une directive de la Commission européenne : 1999/05/EC, plus connue sous le nom de directive R (Radio Telecommunication Terminal Equipment).

Des adaptations de la recommandation de l'UIT ont été faites dans les autres régions du globe. Aux États-Unis, par exemple, la Federal Communication 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 860-960 MHz. 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, l'Europe se prépare à proposer de nouvelles bandes (915-921 MHz) en plus de celles existantes (865-868 MHz). Des révisions de la Recommandation 70-03 ainsi que de la norme ETSI 302-208 ont été publiées. Les adoptions nationales sont en cours.

6.2 RFID et santé publique

Tout comme pour les régulations, il existe des recommandations internationales visant à établir des seuils d'exposition des individus (professionnel 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 directive 2013/35/EC devrait être appliquée et reprise dans le droit national de chaque État membre de l'Union européenne.

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. Ce document concerne les systèmes RFID UHF. Il est téléchargeable gratuitement sur le site du CNRFID.

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 de transport, inventaires, logistiques...) doit faire l'objet d'une évaluation d'impact sur la vie privée (EIVP ou *Privacy Impact Assessment* PIA en anglais). La nouvelle 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 »).

6.3 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 Organization for Standardization) 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 Comittee), 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 barres compris. Dans ce sous-comité 31, sept 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 associées des rapports techniques (TR *Technical Report*), 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 les normes ISO/IEC 15962 et 15963 définissant les règles d'encodage et la manière d'identifier de manière unique les tags RFID. Le WG4 propose également des guides d'implémentation (TR 24729) s'intéressant notamment au recyclage des tags.

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 barres 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 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 commercialise les standards mis au point par des laboratoires partenaires (Auto Id Labs). Le principal standard concernant l'interface air-UHF est connu sous le nom de EPC Class1 Gen2. Il a été quasi intégralement repris par l'ISO sous le nom de ISO/IEC 18000-63 (mode C).

7. 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 la RFID est basée sur des principes de radiofréquences. L'analyse de l'environnement et la customisation des solutions restent des éléments incontournables pour garantir le succès de l'application. De nombreuses normes internationales accompagnées de guides de bonnes pratiques permettent néanmoins de simplifier la mise en œuvre.

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. De nouvelles puces bi-fréquences (HF/UHF) sont aujourd'hui disponibles. Cela permet 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.

8. 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 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, on parle de couplage électromagnétique. Le champ électromagnétique et formé et les équations de Friis s'appliquent 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/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*) ou l'UII (*Unique Item Identifier*). 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 renvoie et module un signal porteur envoyé par un interrogateur. L'étiquette passive utilise généralement l'énergie émise par le lecteur pour se mettre en service.

RFID active ; *active RFID*

Dispositif RFID capable de produire un signal radio au moyen d'une source d'énergie interne (batterie, par exemple).

Singulation ; *singulation*

Processus permettant d'identifier un tag parmi une population de tags activés par un même lecteur.

Systèmes et techniques RFID

par **Claude TETELIN**
Ingénieur ISEN, Docteur de l'Université de Lille, France
Directeur technique du Centre National RFID,
Président de la commission nationale AFNOR CN31

Sources bibliographiques

[1] PARET (D.). – *RFID en ultra et super-hautes fréquences UHF-SHF : Théorie et mise en œuvre*, Dunod (2008).

[2] COMBES (P.-F.). – *Micro-ondes. Tome 2 : Circuits passifs, propagation, antennes*, Dunod (1997).

[3] PARET (D.). – *Identification radiofréquence et carte à puce sans contact. Description*, Dunod (2001).

[4] FINKENZELLER (K.). – *RFID Handbook : radio-frequency identification Fundamentals and applications,* Wiley (1999).

[5] BOWICK (Ch.). – *RF circuit design*, Newnes (1982).

[6] de DIEULEVEULT (F.). – *Électronique appliquée aux hautes fréquences*, Dunod (1999).

[7] VIZMULLER (P.). – *RF design guide, systems, circuits and equations*, Artech House (1995).

[8] VENTRE (D.). – *Communications analogiques*, Ellipses (1998).

[9] ZHANG (Y.), YANG (L.) et CHEN (J.). – *RFID and sensor networks*, CRC Press (2010).

[10] BELLANGER (M.). – *Traitement numérique du signal – Théorie et pratique*, Dunod (2006).

[11] GREEN (R.B.). – *The general theory of antenna scattering*, OSU report 1223-17 (1963).

[12] SCHNEIDER (R.K.). – *A re-look at antenna in-band RCSR via load mismatching*, IEEE Antennas and Propagation Society International Symposium, vol.2, pp 1398-1401 (1996).

[13] DOBKIN (D.). – *The RF in RFID : Passive UHF RFID in practice*, Newnes (2008).

À lire également dans nos bases

BEGAUD (X.). – *Antennes – Techniques* [E 3284] (2016).

MAGNE (F.). – *Télécommunications haut débit en ondes millimétriques* [E 6250] (1998).

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

BREMAUD (J.-C.) et et HAMON (G.). – *Émetteurs radioélectriques – Caractéristiques et conception* [TE 6207] (2000).

LEFEBVRE (J.-N.). – *Traçabilité des bagages dans le transport aérien – Déploiement de la technologie RFID* [TR 670] (2009).

Sites Internet

CNRFID : Centre national de référence RFID
http://www.centrenational-rfid.com

RAIN RFID : Association des fournisseurs de technologie RFID UHF
http://www.rainrfid.org/

FILRFID : Association des industriels intégrateurs, conseils et éditeurs de logiciels RFID
http://www.filrfid.org

EPC Global : Industry-driven standards for the Electronic Product Code (EPC) to support the use of Radio Frequency Identification (RFID)
http://www.epcglobalinc.org

RFID Journal
http://www.rfidjournal.com/

Direction générale des entreprises
http://www.telecom.gouv.fr

Événements

Congrès : International RFID Congress, France.
http://www.rfid-congress.com/en/

Salon : RFID journal Live, USA.
http://www.rfidjournalevents.com/live/

Congrès : RFID Kongress, Allemagne.
http://www.rfid-im-blick.de/de/201502052517/internationaler-rfid-kongress-2015.html

Salon : SITL, Semaine Internationale du Transport et de la Logistique, Paris.
http://www.sitl.eu/

Salon : Eurold ID World, International Exhibition and Conference for Identification.
http://www.datacollection.eu

Salon : Cartes, Paris.
http://fr.cartes.com/

Congrès : IEEE RFID Technology and Applications
http://2015.ieee-rfid-ta.org/

Normes et standards

Liste des principales normes de protocoles RFID

ISO/CEI 18000-2: Octobre 2009	Technologies de l'information – Identification par radiofréquence (RFID) pour la gestion d'objets — Partie 2 : paramètres de communications d'une interface d'air à moins de 135 kHz.
ISO/CEI 18000-3: Novembre 2010	Technologies de l'information – Identification par radiofréquence (RFID) pour la gestion d'objets – Partie 3 : paramètres de communications d'une interface d'air à 13,56 MHz.
ISO/CEI 18000-4: Février 2015	Technologies de l'information – Identification par radiofréquence (RFID) pour la gestion d'objets – Partie 4 : paramètres de communications d'une interface d'air à 2,45 GHz.
ISO/CEI 18000-7: Septembre 2014	Technologies de l'information – Identification par radiofréquence (RFID) pour la gestion d'objets – Partie 7 : paramètres de communications actives d'une interface d'air à 433 MHz.
ISO/CEI 18000-63: Janvier 2013	Technologies de l'information – Identification par radiofréquence (RFID) pour la gestion d'objets – partie 63 : Paramètres de communications d'une interface radio entre 860 MHz et 960 MHz, Type C.
ISO/CEI 15693-x	Cartes d'identification – Cartes à circuit intégré sans contact – Cartes de voisinage.
ISO/CEI 14443-x	Cartes d'identification – Cartes à circuit(s) intégré(s) sans contact – Cartes de proximité.
ISO/CEI 18092:Mars 2013	Technologies de l'information – Télécommunications et échange d'information entre systèmes – Communication de champ proche – Interface et protocole (NFCIP-1).
ISO/CEI 21481: Juillet 2012	Technologies de l'information – Télécommunications et échange d'information entre systèmes – Interface et protocole -2 en communication de champ proche (NFCIP-2).

Annuaire

Constructeurs – Fournisseurs – Distributeurs (liste non exhaustive)

3M http://solutions.3mfrance.fr
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
Embisphère : http://www.embisphere.com/
EM Microelectronic Marin : http://www.emmicroelectronic.com
Feig : http://www.feig.de/home.html
Fréquentiel : 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 : 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)

Organismes de normalisation

ISO International Organization for Standardization
http://www.iso.org

CEN Comité européen de normalisation
http://www.cen.eu

Afnor Association française de normalisation
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 électrotechnique
http://www.cenelec.eu

IEC International Electrotechnical Commission
http://www.iec.ch

Autres organismes

CNRFID : Centre national de référence RFID
http://www.centrenational-rfid.com

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)

CNRFID : Centre National de Référence RFID
http://www.centrenational-rfid.com

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

Comités techniques

ISO/IEC/JTC1/SC31 sous-comité 31 : *Automatic identification and data capture*
http://www.iso.org

Afnor CN31 Comité miroir CN31 : *RFID, codes à barres et autres techniques d'identification automatique des objets*
http://www.afnor.org

ICNIRP International Commission on Non Ionizing Radiation Protection
http://www.icnirp.de

CEN/TC225 comité technique chargé des technologies d'identification et de saisie automatique de données
http://www.cen.eu

Laboratoires

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.soliatis-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/

Écoles

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

TECHNIQUES DE L'INGÉNIEUR

GAGNEZ DU TEMPS ET SÉCURISEZ VOS PROJETS EN UTILISANT UNE SOURCE ACTUALISÉE ET FIABLE

Techniques de l'Ingénieur propose la plus importante collection documentaire technique et scientifique en français !

Grâce à vos droits d'accès, retrouvez l'ensemble des **articles et fiches pratiques de votre offre, leurs compléments et mises à jour,** et bénéficiez des **services inclus.**

RÉDIGÉE ET VALIDÉE PAR DES EXPERTS	MISE À JOUR PERMANENTE	100 % COMPATIBLE SUR TOUS SUPPORTS NUMÉRIQUES	SERVICES INCLUS DANS CHAQUE OFFRE

- **+ de 350 000 utilisateurs**
- **+ de 10 000 articles de référence**
- **+ de 80 offres**
- **15 domaines d'expertise**

- **Automatique - Robotique**
- **Biomédical - Pharma**
- **Construction et travaux publics**
- **Électronique - Photonique**
- **Énergies**
- **Environnement - Sécurité**
- **Génie industriel**
- **Ingénierie des transports**
- **Innovation**
- **Matériaux**
- **Mécanique**
- **Mesures - Analyses**
- **Procédés chimie - Bio - Agro**
- **Sciences fondamentales**
- **Technologies de l'information**

Pour des offres toujours plus adaptées à votre métier, découvrez les offres dédiées à votre secteur d'activité

Depuis plus de 70 ans, Techniques de l'Ingénieur est la source d'informations de référence des bureaux d'études, de la R&D et de l'innovation.

www.techniques-ingenieur.fr

CONTACT : Tél. : + 33 (0)1 53 35 20 20 - Fax : +33 (0)1 53 26 79 18 - E-mail : infos.clients@teching.com

TECHNIQUES DE L'INGÉNIEUR

LES AVANTAGES ET SERVICES compris dans les offres Techniques de l'Ingénieur

ACCÈS

Accès illimité aux articles en HTML
Enrichis et mis à jour pendant toute la durée de la souscription

Téléchargement des articles au format PDF
Pour un usage en toute liberté

Consultation sur tous les supports numériques
Des contenus optimisés pour ordinateurs, tablettes et mobiles

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

Impression à la demande
Commandez les éditions papier de vos ressources documentaires

Alertes actualisations
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.

ILS NOUS FONT CONFIANCE

AgroParisTech · AIRBUS · cea · CESI Enseignement Supérieur et Formation Professionnelle · cnes Centre National d'Études Spatiales · CSTB le futur en construction · ENGIE · GE · L'ORÉAL · Leroy-Somer · École Polytechnique Université Paris-Saclay · SAFRAN Aerospace Defence Security · Sagemcom · SAINT-GOBAIN · Schneider Electric · THALES · TOTAL · Valeo · VEOLIA · Wallonie · SPW Service public de Wallonie

www.techniques-ingenieur.fr

CONTACT : Tél. : + 33 (0)1 53 35 20 20 - Fax : +33 (0)1 53 26 79 18 - E-mail : infos.clients@teching.com