RFID / NFC

Table des matières

Le NFC est un standard de communication RF (radio fréquence) sans-contact à courte distance permettant une communication entre deux dispositifs électroniques. La communication du NFC est basée sur la technologie RFID (Identification par Radio Fréquence) qui est largement utilisée depuis plus de 30 ans.

1. Introduction

Grâce aux technologies NFC et RFID, la démocratisation des objets communicants est en marche et le M2M (communication Machine to Machine) à la portée de tous.

La Near Field Communication est une des technologies de communication sans contact permettant l'échange d'informations à très courte distance (quelques centimètres maximum) entre un terminal mobile (après validation de l'utilisateur) et un récepteur.

Elle est un des fers de lance des prochains modèles de téléphones mobiles pour remplacer à terme les paiements par carte bancaire.

Déjà testée dans de grands centres urbains pour les paiements de titres de transport, à la caisse des magasins par exemple, cette technologie équiperait 1 million de smartphones sur le marché français à la fin 2011.

Les prochains BlackBerry et iPhone5 devraient bénéficier prochainement des avantages de cette puce, les mobiles avec l'OS Androïd en version 2.3.3 également.

Mais la NFC s'ouvre aussi à d'autres objets, comme la clé de voiture BMW qui permettrait à son propriétaire d'effectuer ses achats de carburants, de nourriture en drive-in, etc.

1.1. RFID, l'atout logistique

La Radio Frequency IDentification est aussi une technologie sans contact par radiofréquences. Elle permet une détection automatique avec des distances de lecture supérieures (de 10 à 200 m selon le type de puces) à celles de la NFC.

Elle permet également la détection de produits marqués en grande quantité, jusqu'à 200 par seconde et sans orientation directe vers le détecteur.

Les tags RFID insérés sur ou dans les objets et leur lecteur ont d'ores et déjà discrètement mais efficacement intégré notre quotidien et trouvé de très nombreuses applications et telles que :

- Le contrôle d'authentification et d'accès sur des lieux sécurisés ou payants (bureau, parking, passeport biométrique, télépéage autoroutier)
- La traçabilité des produits, le suivi de production, de colis, de chargements complets en camion, de containers
- La gestion intégrale d'une chaîne d'approvisionnement, les inventaires
- La billetterie pour les spectacles ou les abonnements de transport commun etc.

Fiable, rapide, peu coûteuse, la RFID offre des avantages indéniables pour de nombreux secteurs économiques.

1.2. La RFID et le vivant

La RFID s'applique aussi au monde du vivant. Plantes, bétails, animaux de compagnie peuvent être tracés grâce à l'intégration de puce dans les fibres ou en sous-cutané.

Les humains n'y échappent pas non plus, à des fins de paiement (expérimenté par une boîte de nuit espagnole pour faciliter l'entrée et les consommations des VIP), suivi médical, localisation automatique de personnes susceptibles d'être kidnappées (au Mexique)…

Pour 2010, IBM évaluait à environ 30 milliards le nombre d'étiquettes RFID produites dans le monde et à 1 milliard de transistors pour les êtres humains.

1.3. Développement durable

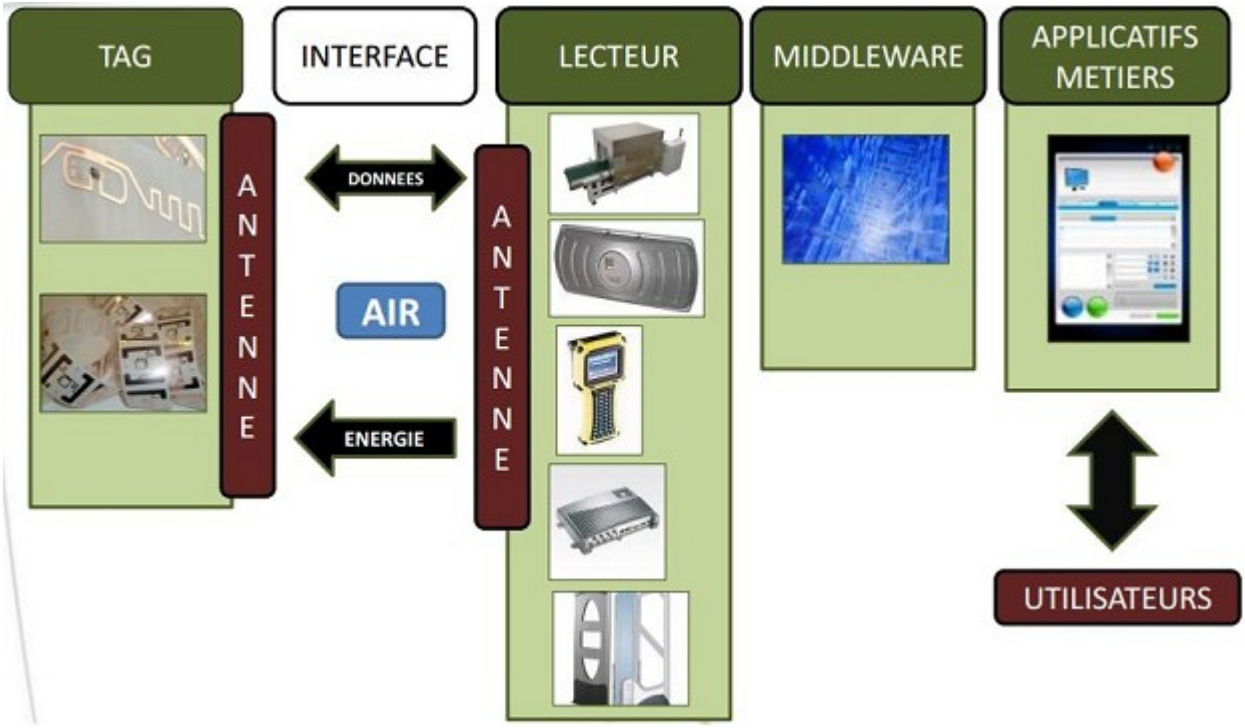
En ces temps de réduction des coûts et d'émission de CO_2, la technologie green RFID est un véritable atout pour les industriels.

Loin d'être un phénomène de mode, les applications de la RFID sécurisent les flux, réduisent les erreurs de traitement et les gaspillages, font gagner du temps, permettent d'économiser des moyens (manutention et transport) et réduisent ainsi l'énergie utilisée.

2. RFID

2.1. Définition

On peut donner la définition suivante à la RFID - Radio Frequency IDentification : d'après le Technologie d'identification automatique qui utilise le rayonnement radiofréquence pour identifier les objets porteurs d'étiquettes lorsqu'ils passent à proximité d'un interrogateur.



2.2. Les constituants

La RFID ne peut pas se résumer à une seule technologie.

En effet, il existe plusieurs fréquences radio utilisées par la RFID, plusieurs types d'étiquette ayant différents types de mode de communication et d'alimentation.

Pour transmettre des informations à l'interrogateur (encore appelé station de base ou plus généralement lecteur), un tag RFID est généralement muni 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.

2.3. Les informations

Les informations contenues dans la puce électronique d'un tag RFID dépendent de l'application.

Il peut s'agir d'un identifiant unique (UII, Unique Item Identifier ou code EPC, Electronic Product Code, etc.).

Une fois écrit dans le circuit électronique, cet identifiant ne peut plus être modifié mais uniquement lu (WORM Write Once Read Multiple).

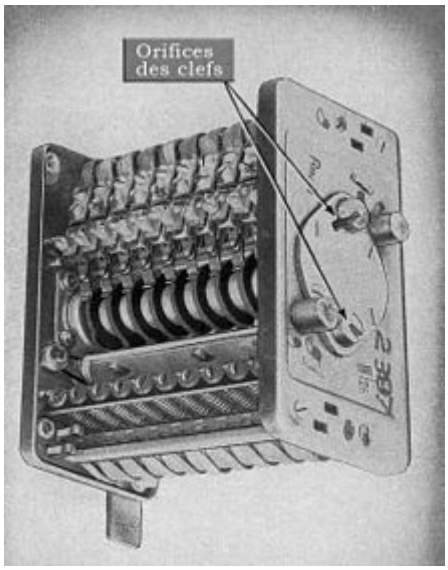
Certaines puce électroniques disposent d'une autre zone mémoire dans laquelle l'utilisateur peut écrire, modifier, effacer ses propres données.

La taille de ces mémoires varie de quelques bits à quelques dizaines de kilobits.

2.4. Histoire de la RFID

1940 Le principe de la RFID est utilisé pour la première fois lors de la Seconde Guerre Mondiale pour identifier/ authentifier des appareils en vol (IFF : Identifie Friendly Foe). Il s'agissait de compléter la signature RADAR des avions en lisant un identifiant fixe permettant l'authentification des avions alliés.

La photo ci–contre présente le tout premier IFF au monde, le FuG-25a « Erstling » (début), mis au point en Allemagne en 1940.



Il reçoit les fréquences radar de 125 MHz (Radar Freya) et 550–580 MHz (Radar Würzburg).

Pour démarrer la procédure d'identification l'opérateur au sol commute la fréquence d'impulsions de son radar de 3 750 Hz à 5 000 Hz.

Le récepteur radio embarqué de l'avion décode ce changement et lance l'émission de son propre code.

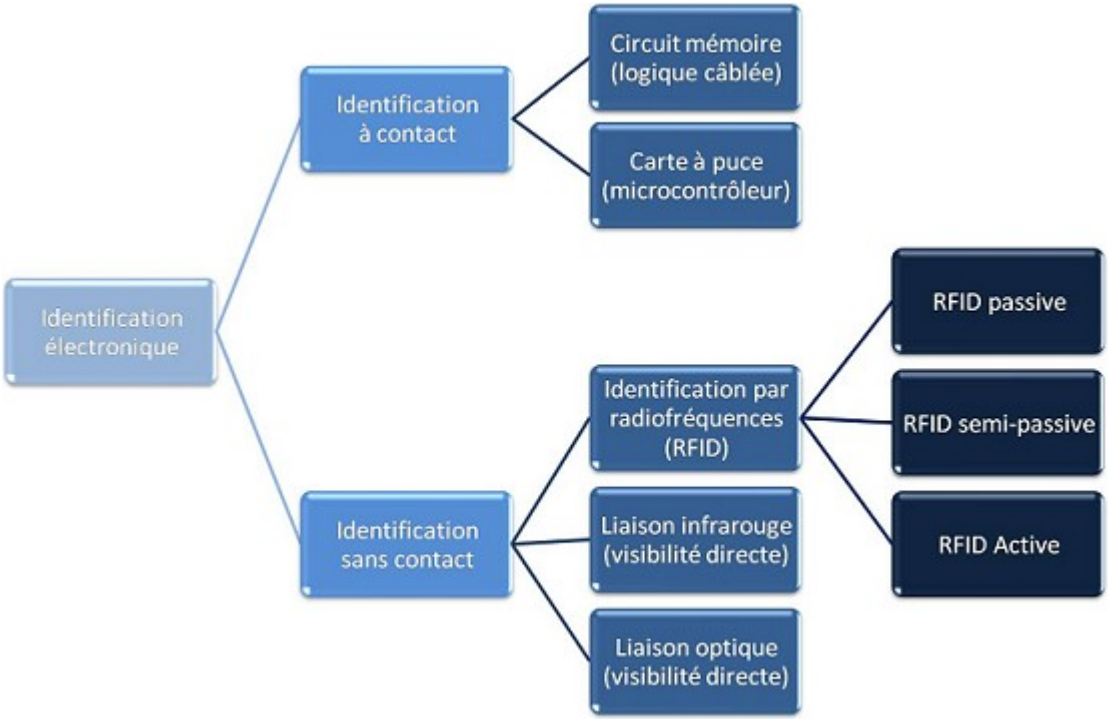
Avant le décollage, deux clefs mécaniques de 10 bits chacune sont insérées dans le lecteur visible sur la photographie. L'émetteur IFF transmet sur la fréquence de 168 MHz avec une puissance de 400 W

	PEP1. Malheureusement pour les Allemands, les Britanniques ont fabriqué leur propre système IFF qu'ils ont appelé « Perfectos » et qui est capable, lorsqu'il est installé sur un Mosquito de la Royal Air Force, de déclencher le FuG–25 ce qui, du coup, trahit la position des chasseurs de nuit. Pour éviter cela le FuG–25 devait être coupé le plus souvent possible.
1970	Durant les années 1960-1970, les systèmes RFID restent une technologie confidentielle, à usage militaire pour le contrôle d'accès aux sites sensibles, notamment dans le nucléaire.
1980	Les avancées technologiques permettent l'apparition du tag passif. Le tag RFID rétromodule l'onde rayonnée par l'interrogateur pour transmettre des informations. Cette technologie permet de s'affranchir de source d'énergie embarquée sur l'étiquette réduisant de ce fait son coût et sa maintenance.
1990	Début de la normalisation pour une interopérabilité des équipements RFID.
1999	Fondation par le MIT (Massachusetts Institute of Technology) de l' Auto-ID center : centre de recherches spécialisé en identification automatique (entre autre RFID).
2004	L'auto-ID du MIT devient "EPCglobal", une organisation chargée de promouvoir la norme EPC (Electronic Product Code), extension du code barre à la RFID.
A partir de 2005	Les technologies RFID sont aujourd'hui largement répandues dans quasiment tous les secteurs industriels (aéronautique, automobile, logistique, transport, santé, vie quotidienne, etc.). L'ISO (International Standard Organisation) a largement contribué à la mise en place de normes tant techniques qu'applicatives permettant d'avoir un haut degré d'interopérabilité voire d'interchangeabilité.
2009	Création du Centre National de Référence RFID.

2.5. De l'identification à la RFID

L'identification électronique se divise en deux branches :

- L'identification « à contact »
- L'identification « sans contact »



2.5.1. Identification à contact

Il s'agit de dispositifs comportant un circuit électronique dont l'alimentation et la communication sont assurées par des contacts électriques. Les deux principaux exemples d'identification à contact sont :

- Les circuits « mémoire » : ils comportent des fonctions mémoire embarqués sur des modules de formes et de tailles variées.
- Les cartes à puces : Les exemples de cartes à puces les plus connus sont les cartes bancaires, la carte vitale ou encore la carte SIM (Subscriber Identity Module).

2.5.2. Identification sans contact

On peut décomposer les identifications sans contacts en trois sous-branches principales :

- La vision optique : ce type de liaison nécessite une vision directe entre l'identifiant et le lecteur (laser, camera CCD...). La technologie la plus répandue est le code à barre linéaire et les codes 2D (PDF417, QR Code, etc.). La technologie OCR (Optical Character Recognition) est également largement utilisée (scan MRZ (Machine Readable Zone) sur les passeports ou Carte National d'Identité).
- La liaison infrarouge : Ce type de liaison assure un grand débit d'information, une grande directivité qu'une bonne distance de fonctionnement. Ces systèmes nécessitent également une visibilité directe.
- Les liaisons Radiofréquences : Ce type de liaison permet la communication entre l'identifiant et un interrogateur, sans nécessité de visibilité directe. De plus, il est également possible de gérer la présence simultanée de plusieurs identifiants dans le champ d'action du lecteur (anti-collisions).

3. Classification des tags RFID

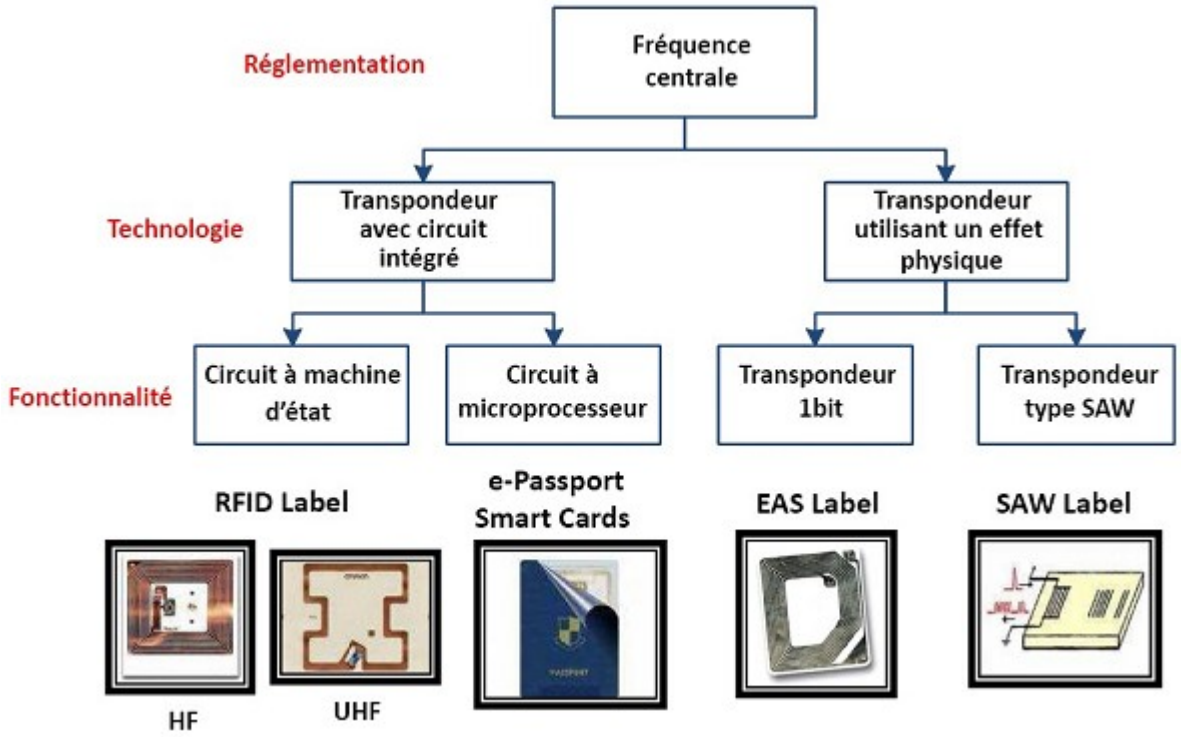
3.1. Le tag RFID, avec ou sans puce électronique

Une première classification possible des tags ou étiquettes RFID est basée sur la présence ou non d'une puce électronique.

Le tag RFID SAW (Surface Acoustic Wave) n'est pas équipé de circuits intégrés. Il ne représente aujourd'hui qu'une très faible part du marché (quelques %). Il s'agit d'un transpondeur à lecture seule et ne comportant pas d'alimentation embarquée. On le nomme également code à barres RF.

Le tag RFID 1 bit est un système passif à diodes capacitives, dit « transpondeur 1 bit». Ce bit permet d'indiquer la présence ou non du tag dans le champ d'action de l'interrogateur. Il est largement utilisé comme système antivol.

Le tag RFID à circuits intégrés est le système le plus utilisé sur le marché actuel. Il se compose d'une antenne et d'un circuit intégré plus ou moins complexe (simple machine d'état ou véritable microcontrôleur).



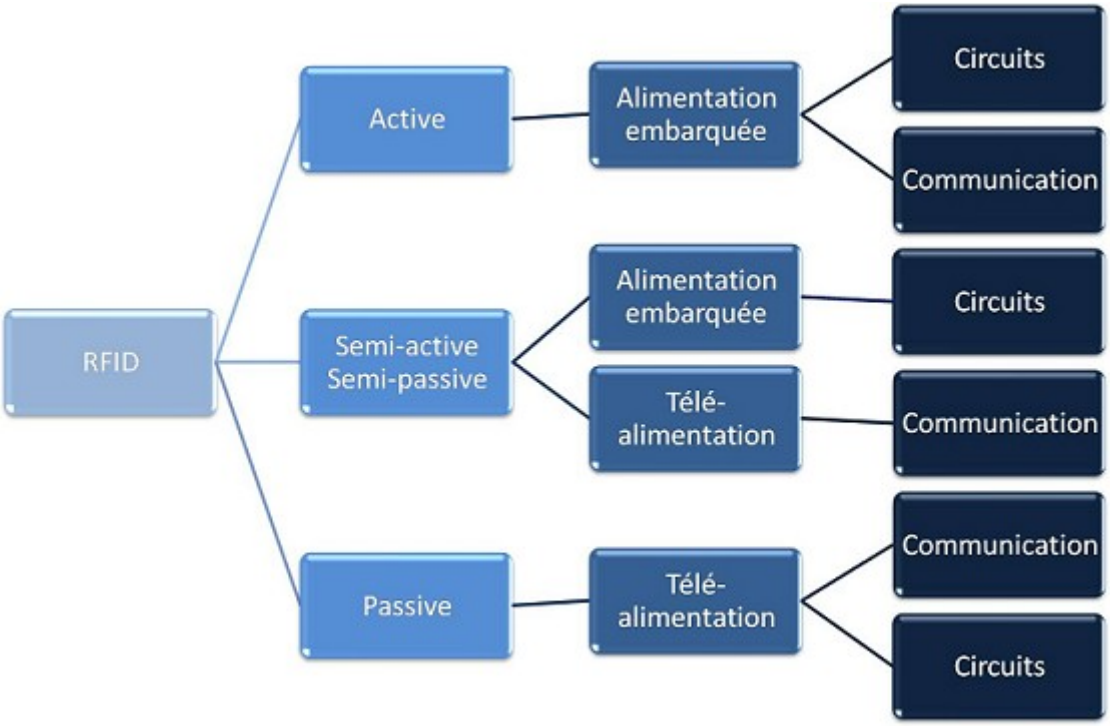
3.2. Le tag RFID, avec ou sans émetteur RF (actif ou passif)

Le tag RFID passif : c'est un tag qui rétromodule l'onde issue de l'interrogateur pour transmettre des informations. Il n'intègre pas d'émetteurs RF. Le tag passif utilise généralement l'onde (magnétique ou électromagnétique) issue de l'interrogateur pour alimenter le circuit électronique embarqué.

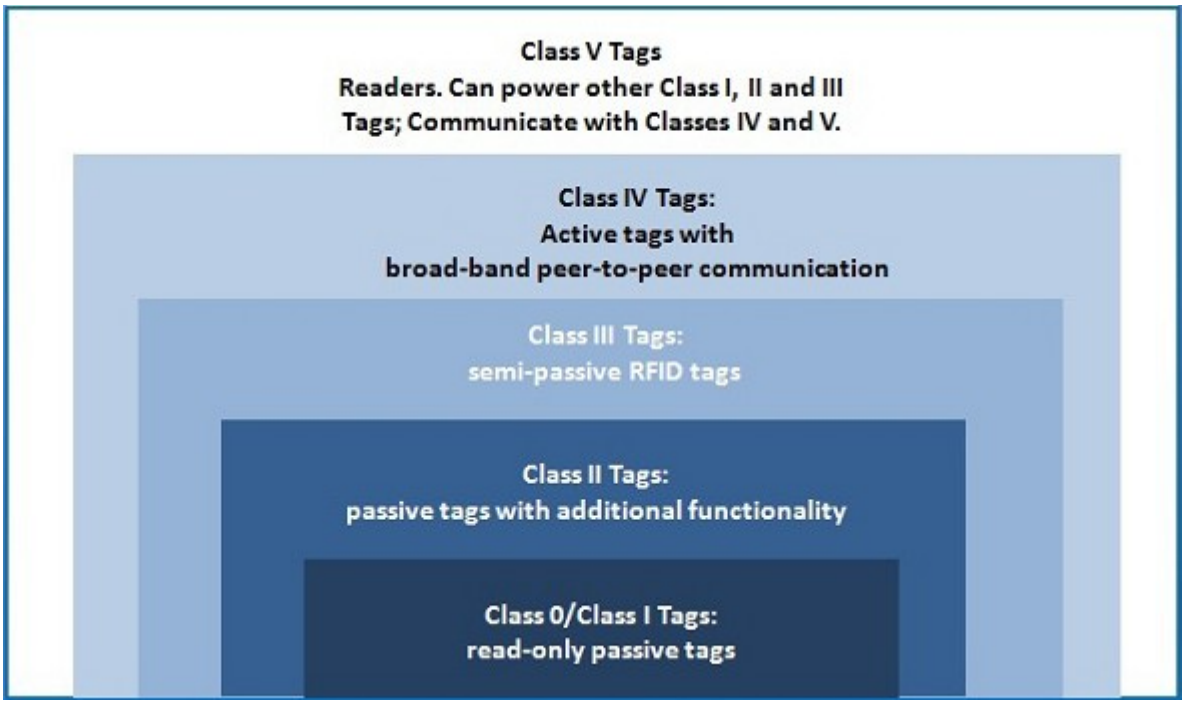
Le tag RFID passif assisté par batterie (BAP Battery Assisted Passive) : il comporte une alimentation embarquée (piles, batteries...). Cette dernière n'est pas utilisée pour alimenter un émetteur puisque le principe de communication reste la rétromodulation (comme pour le tag passif), mais pour alimenter le circuit électronique du tag ou tout autre circuits ou capteur connecté au circuit de base. Cette alimentation permet, en théorie, d'améliorer les performances. Ce tag est

largement utilisé pour des applications nécessitant une capture d'information (température, choc, lumière, etc.) indépendante de la présence d'un interrogateur.

Le tag RFID actif : c'est un tag qui embarque un émetteur RF. La communication avec l'interrogateur est donc de type pair à pair. Ce tag embarque généralement une source d'énergie.



3.3. Simple identifiant / fonction plus complexe



- Classe 0 et classe 1 : tags passifs à lecture seule (on ne peut que lire l'identifiant unique du

tag)

- Classe 2 : tags passifs à fonctions additionnelles (écriture mémoire)
- Classe 3 : tags passifs assistés par batterie
- Classe 4 : tags actifs. Communication large-bande du type « peer-to-peer »
- Classe 5 : interrogateurs. Alimentent les tags de classe 0, 1, 2 et 3. Communiquent avec les tags de classe 4.

3.4. 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 dans la mémoire 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 (TID Tag IDentifier). 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 (UII Unique Item Identifier ou Code EPC Electronic Product Code par exemple). Une fois ce numéro écrit, il ne peut plus être modifié. On parle alors de puce WORM (Write Once, Read Multiple).

D'autres types d'applications vont nécessiter la présence d'une zone mémoire accessible par l'utilisateur et réinscriptible. Cette zone, ne dépassant pas les quelques dizaines de kilo octets dans la majeure partie des cas, peut servir lorsque l'accès à une base de données centrale n'est pas garantie (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.

3.5. Protocole TTF ou ITF

Qui parle le premier : le tag ou l'interrogateur ?

Cette question, a priori anodine, prend tout son sens lorsque plusieurs étiquettes se trouvent simultanément dans le champ de l'interrogateur où 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).

A 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) ou 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'anti-collision). 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 palier ce problème, il est possible de demander aux étudiants de ne donner leur nom qu'après avoir écouté et s'être assuré 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.

A 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.

3.6. Caractéristiques du tag RFID passif

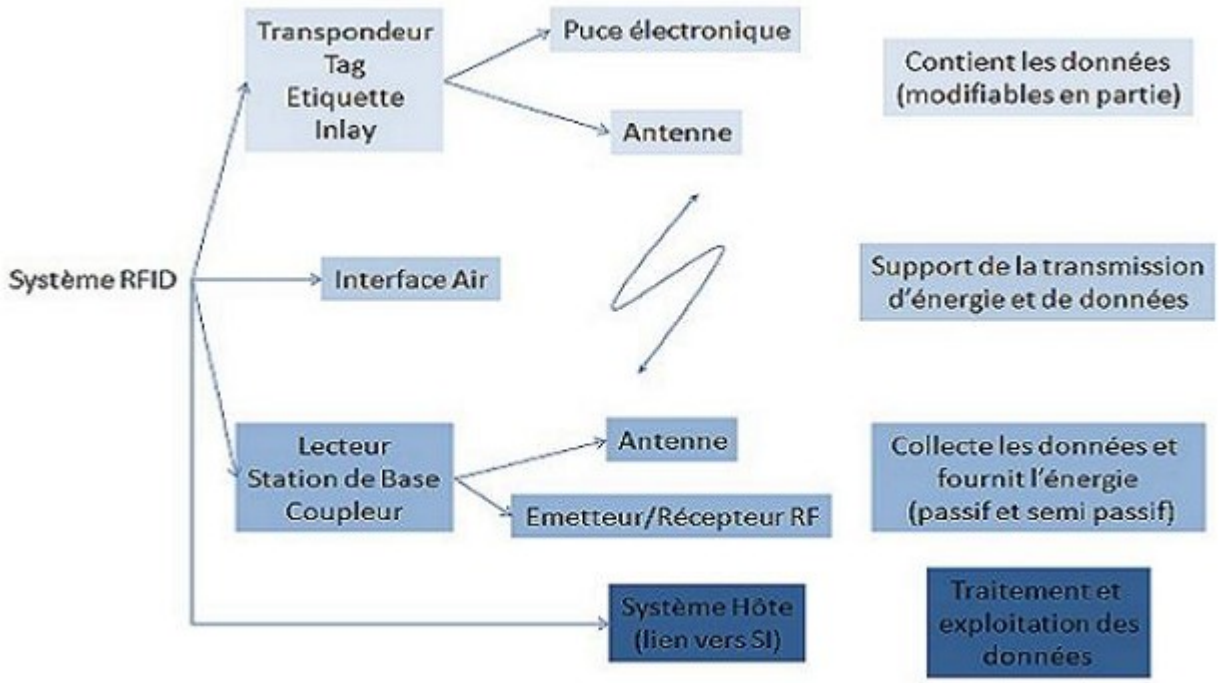
Les tags passifs sont de très loin les plus utilisés sur le marché actuel. Leur prix unitaire varie entre quelques centimes d'euros et une dizaine d'euros selon leur fréquence, leur forme, leur taille et surtout leur packaging...

Voici les caractéristiques générales des transpondeurs passifs actuels :

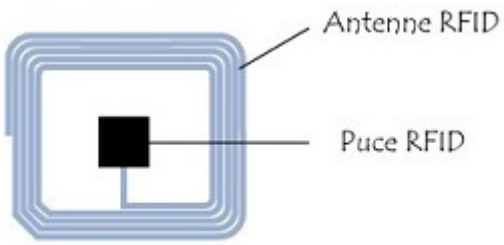
Fréquence	125 et 134,2 kHz LF	13,56 MHz HF	868 à 915 MHz UHF	2,45 et 5,8 GHz SHF
Portée typique max	0,5 m	1 m	3 à 6 m	1 m
Caractéristiques générales	-Relativement cher même par gros volumes - L'antenne nécessite un nombre de tours important - Faible dégradation des performances en milieu métallique ou liquide	-Moins cher que les tags LF - Bien adapté aux applications qui ne demande pas de lire beaucoup de tags à grande distance -Fréquence unique dans le monde	-En gros volume, les tags UHF sont moins chers que les tags HF et LF - Adapté à la lecture en volume à longue distance - Performances dégradées par rapport à la HF en milieu métallique ou aqueux	-Performances similaires à l'UHF - Très forte sensibilité aux métaux et liquides - Liaison lecteur/tag plus directive que pour les fréquences plus basses
Principales Normes	ISO 14223/1 ISO 18000-2	ISO 14443 ISO 15693 ISO 18000-3	ISO 18000-6	ISO 18000-4

4. Fonctionnement d'un système RFID

4.1. Les composants d'un système RFID



Système RFID : Un système RFID (Radio Fréquence Identification) se compose de transpondeurs (aussi nommés étiquettes, marqueurs, tags, identifiants...) et d'un ou plusieurs interrogateurs (aussi nommés coupleurs, base station...).



Interrogateurs RFID : Ce sont des dispositifs actifs, émetteurs de radiofréquences qui vont activer les tags qui passent devant eux en leur fournissant l'énergie dont ils ont besoin pour fonctionner. Outre de l'énergie pour l'étiquette, l'interrogateur envoie des commandes particulières auxquelles répond le tag. L'une des réponses les plus simples possibles est le renvoi d'une identification numérique. La fréquence utilisée par les interrogateurs est variable selon le type d'application visé et les performances recherchées. Ces dernières sont détaillées dans la partie « Gammes de fréquences »

Tag RFID : C'est un dispositif récepteur, que l'on place sur les éléments à tracer (objet, animal...). Ils sont munis d'une puce contenant les informations et d'une antenne pour permettre les échanges d'informations.

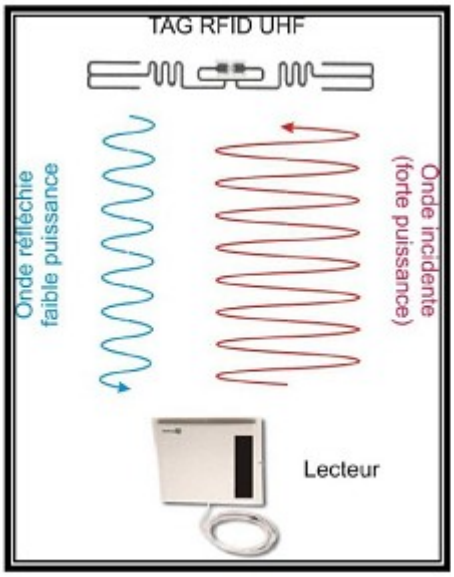
Middleware : un système dont la fonction est d'assurer la gestion des données, des interrogateurs et de transférer les informations ad hoc aux applications de plus haut niveau.

Interface : L'interface est le support de transmission de l'énergie et des données. Dans le cadre des systèmes RFID, il s'agit de l'air.

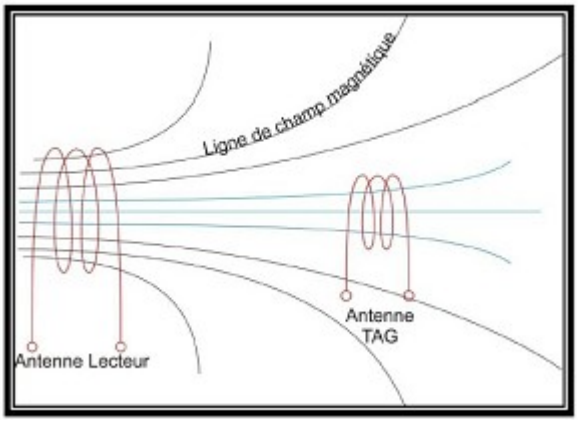
4.2. Le couplage tag RFID / lecteur RFID

La liaison entre tag et interrogateur se réalise par :

- Couplage magnétique dans le cas d'un champ proche (quelques cm à 1,5 m). L'interrogateur utilise alors des LF (Basses Fréquences) ou des HF (Hautes Fréquences). Les antennes sont alors constituées de boucles inductives.
- Couplage électrique dans le cas d'un champ lointain (jusqu'à 6m). L'interrogateur utilise alors des UHF (Ultra Hautes Fréquences) ou des SHF (Super Hautes Fréquences). Les antennes de base sont alors des dipôles ou des patchs.



couplage électrique
UHF et SHF
champ lointain



couplage magnétique
HF et LF
champ proche

5. Les gammes de fréquences RFID

5.1. La RFID dans le spectre radio

L'utilisation de ressources radio est soumise à autorisation et suit des règlements nationaux ou internationaux :

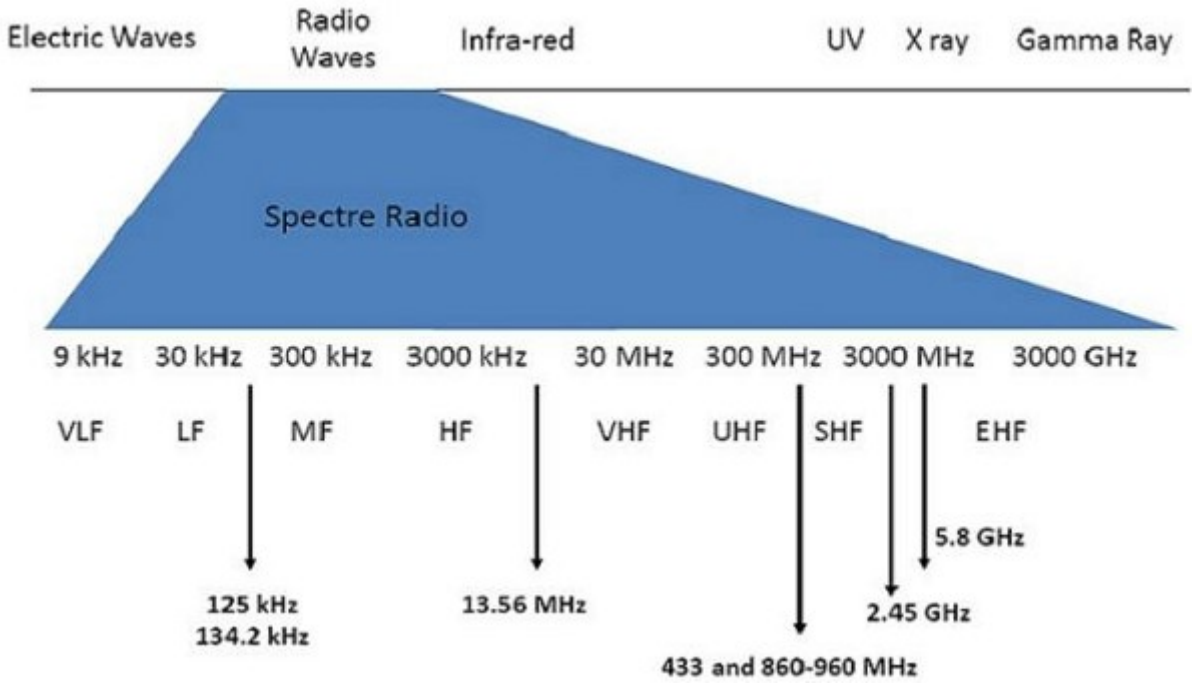
LF : 125 kHz - 134,2 kHz : basses fréquences,

HF : 13,56 MHz : hautes fréquences,

UHF : 860 MHz - 960 MHz : ultra hautes fréquences,

SHF : 2,45 GHz : super hautes fréquences.

Voici un aperçu des fréquences de la RFID dans le spectre radio :



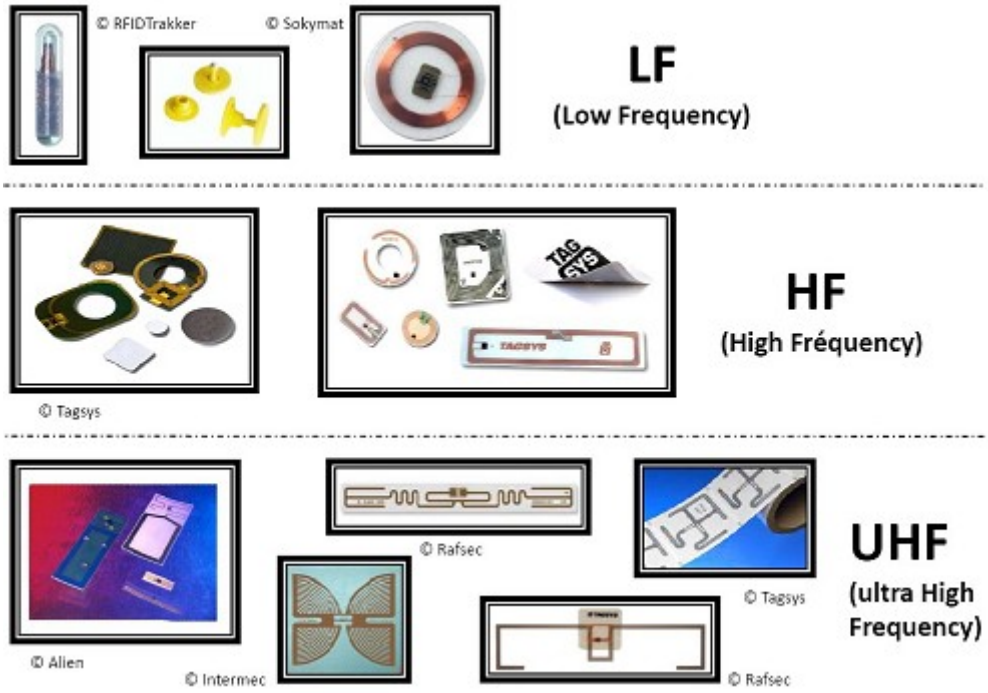
5.2. Les tags RFID UHF, HF, LF

Voici les trois fréquences de tags RFID :

- Les tags RFID UHF à 900 MHz possèdent des antennes imprimées ou gravées. En technologie passive, ils peuvent être lus à plusieurs mètres. Ils sont plus sensibles à l'environnement (métal, eau) du fait de la fréquence utilisée mais des design particuliers d'antenne et de packaging permettent de les utiliser sur des supports métalliques. Les fréquences UHF réservées à la RFID n'étant pas harmonisées dans toutes les régions du monde (entre 860 et 960 MHz), les tags doivent généralement présenter des bandes passantes importantes qui réduisent leurs performances.
- Les tags RFID HF 13.56 MHz sont utilisés dans des applications de logistique et de traçabilité. Les antennes boucle peuvent être imprimées ou gravées ce qui rend les tags particulièrement fins. Ils sont largement répandus dans les applications de transport et d'identité (passeport, pass Navigo, cartes sans contact). Cette technologie est à la base des applications NFC (Near Field Communication) que l'on trouve dans de plus en plus de

smartphones.

- Les tags RFID LF 125 kHz sont adaptés aux applications de logistique et traçabilité. Les caractéristiques physiques de ces tags, d'un poids et une taille réduits, font d'eux des candidats idéals pour être intégrés dans tout type de matériaux, textiles, métaux, plastiques, etc.



6. TP ARDUINO - PN532 RFID/NFC SHIELD 13.56MHz

6.1. Description

Shield AdaFruit pour Arduino :

- applications RFID 13.56MHz ou NFC (Near Field Communication - Communication proche sans contact).

  Ce shield AdaFruit utilise le contrôleur PN532 (le composant NFC le plus populaire sur le marché) qui se trouve inclus dans presque tous les téléphones et appareils récents supportant NFC.

  Ce shield peut presque tout faire, comme lire et écrire des cartes ou des tags, communiquer avec des téléphones (par exemple, pour exécuter des paiements) mais aussi agir comme un tag NFC.

- NFC (Near Field Communications - Communication proche sans contact) permet à deux appareils de communiquer ensembles lorsqu'ils sont très proches l'un de l'autre. Une sorte de communication Bluetooth très très courte distance qui ne nécessite pas d'authentification. NFC est une extension de RFID, il est donc possible de réaliser toutes les applications RFID à partir de NFC. Avec NFC, vous pouvez réaliser des applications plus avancées telles que la communication bi-directionnelle avec un téléphone portable.

Parce qu'il est capable de lire et d'écrire des TAGs, vous pouvez toujours utiliser ce shield pour des

projets orientés RFID.

Il est également capable de traiter des tout autres types de tag NFC/RFID du Type 1 au 4 (et bien entendu tous les autres tags de type NXP MiFare Google)

Le shield Adafruit a été conçu pour fonctionner sur une distance de 10 cm, la distance maximale en utilisant une technologie 13.56MHz.

Vous pouvez facilement attacher le shield derrière une plaque en plastique (un boîtier) et continuer à lire les cartes derrière cette barrière non métallique.

6.2. Branchement avec Arduino

Ce shield est conçu pour supporter les protoles de communication I2C ou SPI.

Par défaut le shield est configuré en I2C, et utilise donc moins de broches: analogique 4 et 5 sont utilisées pour la communication I2C (et bien entendu, vous pouvez toujours connecter d'autres périphériques I2C sur le bus).

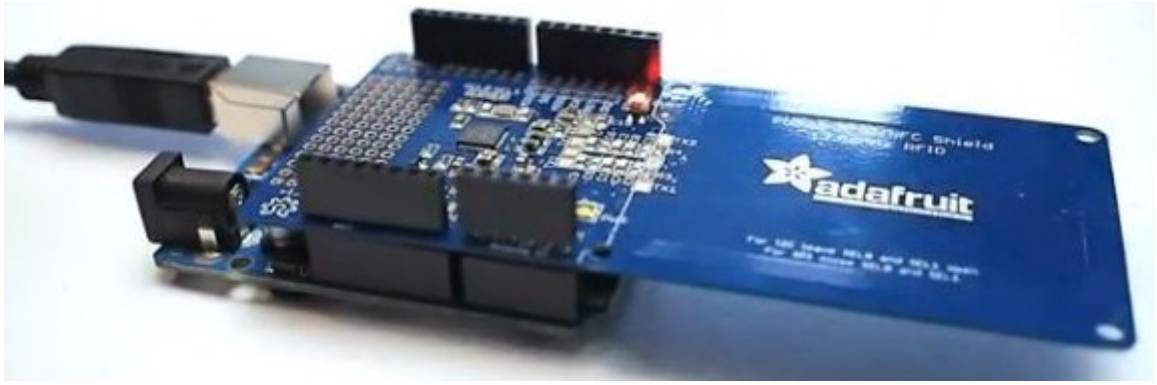
La broche/pin digitale 2 est utilisée pour les notifications via "interruption". Cela signifie que votre programme ne doit pas constamment interroger la carte RFID pour demander si un Tag est présent.

La pin digitale 2 sera mise à la masse (pulled down) quand une carte, téléphone, etc passe dans le champs de communication. Vous pouvez changer la broche utilisée pour cette notification si vous désirez garder la Pin 2 pour une autre chose.

Il est également facile de changer le protocole de communication de I2C en SPI où vous pouvez utiliser 4 pins digitales en soudant les deux pastilles Jumper sur le dessus du PCB.

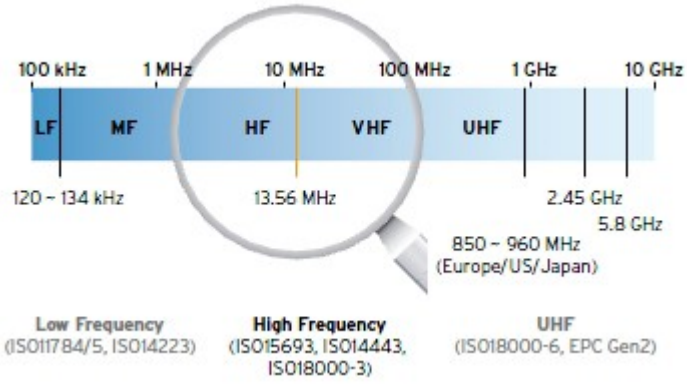
Compatible avec tous les Arduino "classique" - NG, Diecimilla, Duemilanove, UNO - ainsi qu'avec les MEGA R3 et suivants.

Pour utiliser l'interface I2C sur un Mega R2 (ou précédent), deux fils doivent être soudés puisque les pins I2C sont placées différemment sur les versions Mega antérieures.

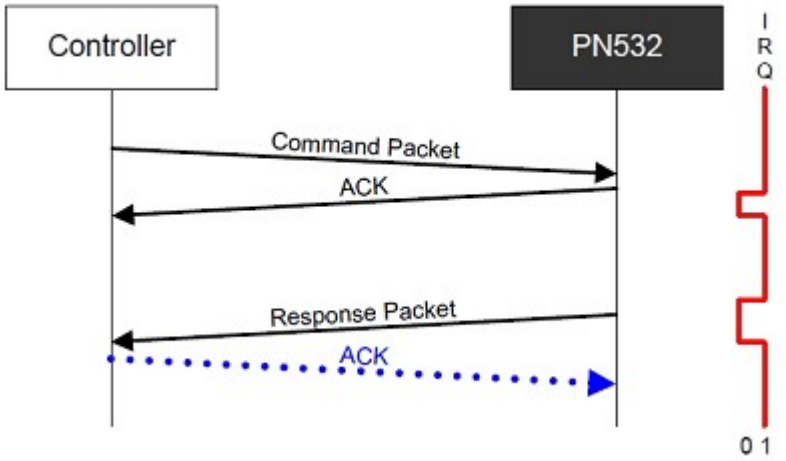


6.3. Fonctionnement du Shield PN532

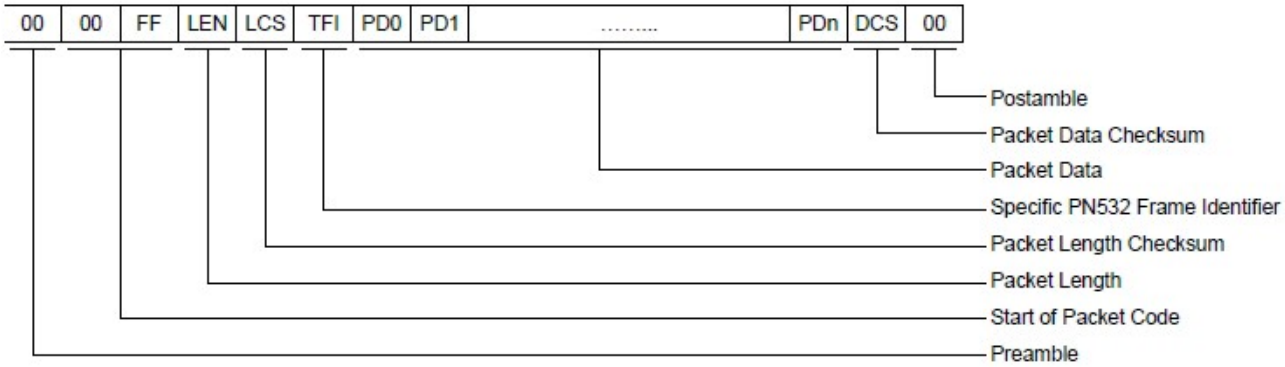
Gamme de fréquences :



Protocole :



Trame :



PREAMBLE	1 byte
START CODE	2 bytes (00h and FFh)
LEN	1 byte indicating the number of bytes in the data field (TFI and PDO to PDn)
LCSI	1 Packet Length Checksum LCS byte that satisfies the relation: Lower byte of [LEN + LCS] = 00h
TFI	1 byte the PN532 Frame Identifier. the value of this byte depends on the way of the message

- D4h in case of a frame from the system controller to the the PN532
- D5h in case of a frame from the the PN532 to the system controller

DATA	LEN-1 bytes of Packet Data Information The first byte PDO is the Command Code
DCS	1 Data Checksum DCS byte that satisfies the relation: Lower byte of [TFI + PDO + PD1 + ... + PDn + DCS] = 00h
POSTAMBLE	1 byte

6.4. Programme 1 : lecteur de carte RFID simple

```
/*
 * Lecteur de carte RFID
 */

#include <Wire.h>
#include <Adafruit_NFCShield_I2C.h>
#include <SoftwareSerial.h>

const int IRQ = 2;       // DEFINITION DE L'INTERRUPTION
const int RESET = 3;     // NON CONNECTE PAR DEFAUT SUR LE SHIELD NFC

Adafruit_NFCShield_I2C nfc(IRQ, RESET);

void setup()
{
    Serial.begin(115200);
    Serial.println("Hello!");

    nfc.begin();
    uint32_t versiondata = nfc.getFirmwareVersion();
    if ( ! versiondata ) {
        Serial.print("Didn't find PN53x board");
        while (1); // halt
        }

    // Got ok data, print it out!
    Serial.print("Found chip PN5");
    Serial.println((versiondata>>24) & 0xFF, HEX);

    Serial.print("Firmware ver. ");
    Serial.print((versiondata>>16) & 0xFF, DEC);
    Serial.print('.');
    Serial.println((versiondata>>8) & 0xFF, DEC);

    // Set the max number of retry attempts to read from a card
    // This prevents us from waiting forever for a card, which is
    // the default behaviour of the PN532.
    nfc.setPassiveActivationRetries(0xFF);

    // configure board to read RFID tags
    nfc.SAMConfig();

    Serial.println("Waiting for an ISO14443A card");
```

```
}

void loop()
{
    // Buffer to store the returned UID
    uint8_t uid[] = { 0, 0, 0, 0, 0, 0, 0 };
    // Length of the UID (4 or 7 bytes depending on ISO14443A card type)
    uint8_t uidLength;

   // Wait for an ISO14443A type cards (Mifare, etc.). When one is found
   // 'uid' will be populated with the UID, and uidLength will indicate
   // if the uid is 4 bytes (Mifare Classic) or 7 bytes (Mifare Ultralight)
   if ( nfc.readPassiveTargetID(PN532_MIFARE_ISO14443A, &uid[0], &uidLength) ) {
        Serial.println("Found a card!");

        Serial.print("UID Length: ");
        Serial.print(uidLength, DEC);
        Serial.println(" bytes");

        Serial.print("UID Value: ");
        for (uint8_t i=0; i < uidLength; i++) {
            Serial.print(" 0x");
            Serial.print(uid[i], HEX);
            }
        Serial.println("");

        // Wait 1 second before continuing
        delay(1000);
      }
    else
      // PN532 probably timed out waiting for a card
        Serial.println("Timed out waiting for a card");
}
```

Configuration Xbee

1. Connecter un Shield Xbee configuré en USB sur une carte Arduino connectée au PC, transférer un programme exemple type Blink.
2. Connecter un deuxième Shield Xbee sur la platine Arduino qui est déjà associée au Shield RFID.

   Attention, câbler des fils de connexions :

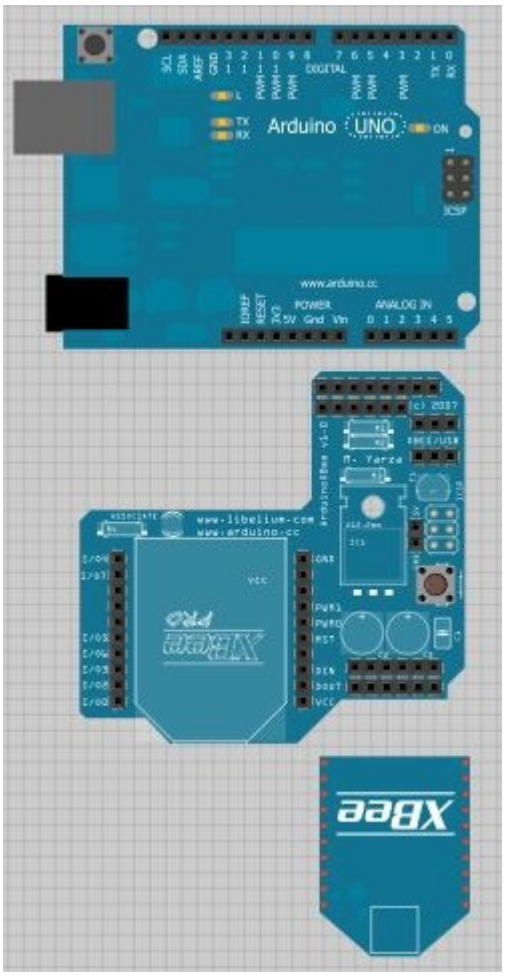
   sur le 5V

   sur le GND

   de A4 RFID à A4 XBEE

   de A5 RFID à A5 XBEE

   et de D2 RFID à D2 XBEE
3. Configurer le Xbee en mode USB.
4. Télécharger le programme n°2 (vitesse de la liaison série en 9600 baud) dans l'Arduino.
5. Reconfigurer le Xbee en mode Xbee.



6.5. Programme 2 : communication XBEE

Même programme que le n°1 mais vitesse de 9600 baud pour le xbee

```
/*
 * communication XBee
 */

#include <Wire.h>
#include <Adafruit_NFCShield_I2C.h>
#include <SoftwareSerial.h>

const int IRQ = 2;
const int RESET = 3; // Not connected by default on the NFC Shield

Adafruit_NFCShield_I2C nfc(IRQ, RESET);

void setup()
{
    Serial.begin(9600);
    Serial.println("Hello!");

    nfc.begin();
    uint32_t versiondata = nfc.getFirmwareVersion();
    if ( ! versiondata ) {
```

```
        Serial.print("Didn't find PN53x board");
        while (1); // halt
        }

    // Got ok data, print it out!
    Serial.print("Found chip PN5");
    Serial.println((versiondata>>24) & 0xFF, HEX);

    Serial.print("Firmware ver. ");
    Serial.print((versiondata>>16) & 0xFF, DEC);
    Serial.print('.');
    Serial.println((versiondata>>8) & 0xFF, DEC);

    // Set the max number of retry attempts to read from a card
    // This prevents us from waiting forever for a card, which is
    // the default behaviour of the PN532.
    nfc.setPassiveActivationRetries(0xFF);

    // configure board to read RFID tags
    nfc.SAMConfig();

    Serial.println("Waiting for an ISO14443A card");
}

void loop()
{
    // Buffer to store the returned UID
    uint8_t uid[] = { 0, 0, 0, 0, 0, 0, 0 };
    // Length of the UID (4 or 7 bytes depending on ISO14443A card type)
    uint8_t uidLength;

    // Wait for an ISO14443A type cards (Mifare, etc.). When one is found
    // 'uid' will be populated with the UID, and uidLength will indicate
    // if the uid is 4 bytes (Mifare Classic) or 7 bytes (Mifare Ultralight)
    if ( nfc.readPassiveTargetID(PN532_MIFARE_ISO14443A, &uid[0], &uidLength) ) {
        Serial.println("Found a card!");

        Serial.print("UID Length: ");
        Serial.print(uidLength, DEC);
        Serial.println(" bytes");

        Serial.print("UID Value: ");
        for (uint8_t i=0; i < uidLength; i++) {
            Serial.print(" 0x");
            Serial.print(uid[i], HEX);
            }
        Serial.println("");

        // Wait 1 second before continuing
        delay(1000);
        }
    else
      // PN532 probably timed out waiting for a card
        Serial.println("Timed out waiting for a card");
}
```