REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE MOHAMED BOUDIAF - M'SILA

FACULTE DE TECHNOLOGIE

DEPARTEMENT D'ELECTRONIQUE

N° : ……..

DOMAINE : SCIENCES ET TECHNOLOGIE

FILIERE : ELECTRONIQUE

OPTION : SYSTÈM EMBARQUÉS

Mémoire présenté pour l'obtention
Du diplôme de Master Académique

Par: ZIKEM Lahcene

BENELBAR Hicham

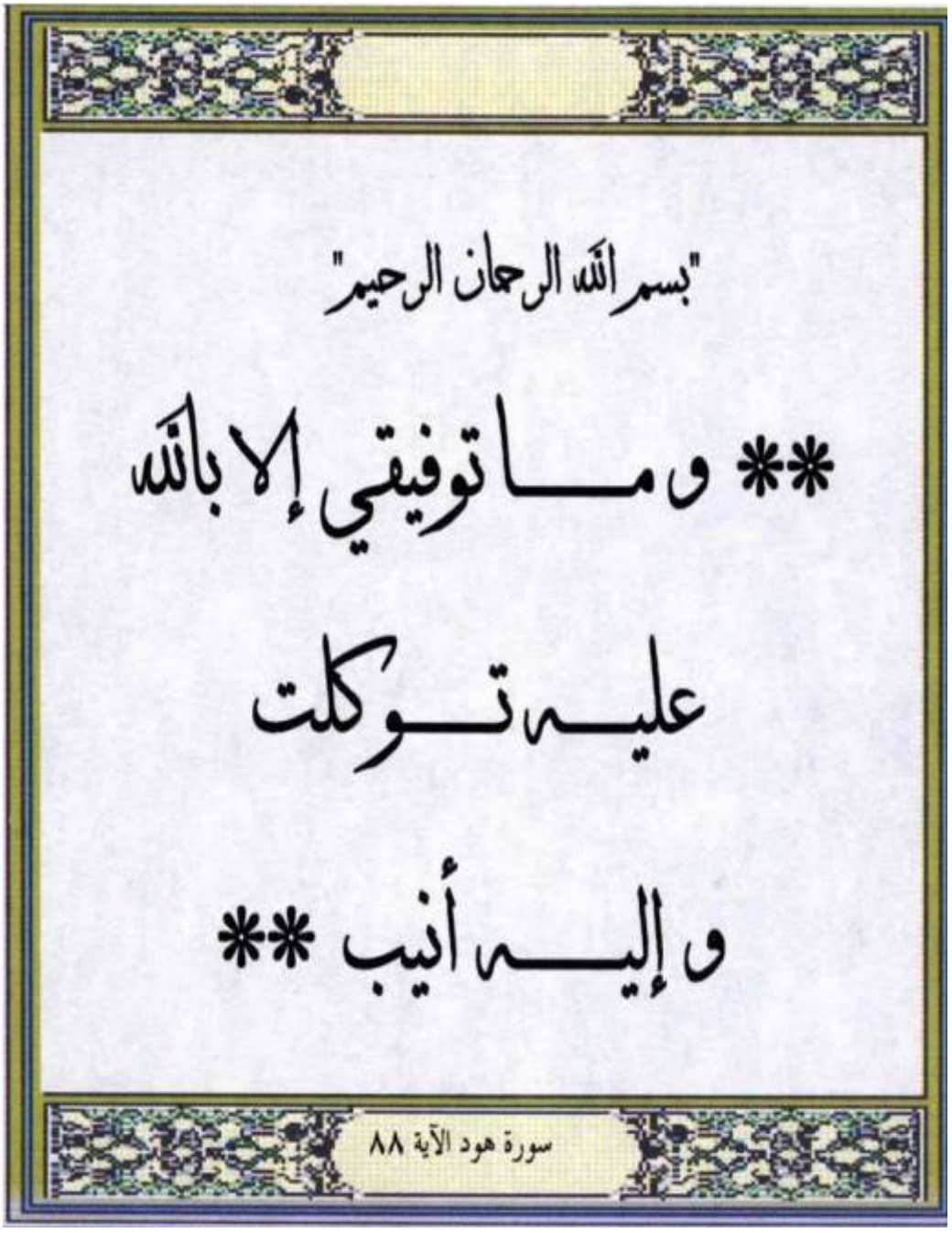
Intitulé

Réalisation d'un dispositif d'identification basé sur la technologie RFID

Soutenu devant le jury composé de :

Dr. MEZAACHE hatem	Université M'sila	Président
Dr. BENAHCENE Madani	Université M'sila	Encadreur
Dr. GAREH Messaoud	Université M'sila	Examinateur

Année Universitaire : 2018 /2019



۞ *Et ma réussite ne dépend que d'**Allah**، Et lui je place ma confiance، et c'est vers lui que je reviens repentant* ۞

REMERCIEMENTS

A Dieu, le tout puissant, nous rendons grâce pour nous avoir donné santé, patience, volonté et surtout raison.

En premier lieu, je tiens à remercier mon encadreur Mr. BENAHCENE Madani qui m'a aidé et conseillé durant ce travail.

Mes remerciements vont également aux membres de jury pour m'avoir honoré par leur évaluation de ce travail.

Je remercie également tous les enseignants du département de l'électronique de l'université de M'SILA pour leur aide et encouragement.

Enfin, je remercie tous ceux qui m'ont soutenu, encouragé et donné l'envie de mener à terme ce travail.

Dédicace

Toutes les lettres ne sauraient trouver les mots qu'il faut…

Tous les mots ne sauraient exprimer la gratitude,

L'amour, le respect, la reconnaissance… Aussi,

c'est tout simplement que Nous dédions cette travail

…

À NOS CHERS PARENTS

Aucune dédicace ne saurait exprimer nos respects, notre amour éternel et nos considérations pour les sacrifices que vous avez consenti pour nous, nous vous remercions pour tout le soutien et l'amour que vous nous portez depuis notre enfance et nous espérons que votre bénédiction nous accompagnons toujours vous instruction et notre bienêtre. Que ce modeste travail soit l'exaucement de vos vœux tant formulés, le fruit de vos innombrables sacrifices, bien que nous ne vous en acquitterai jamais assez. Puisse Dieu, le Très Haut, vous accorder santé, bonheur et longue vie et faire en sorte que jamais nous ne vous décevrons.

À NOS AMIS DE TOUJOURS

- *Mes très chers frères et mes chères sœurs*
- *Mes cousins et cousins*
- *Tous ceux que j'aime*
- *Toutes mes amies.*

Liste des figures

Chapitre I

ChapitreII

Sommaire

Chapitre II

Chapiter III

Introduction Générale

La notion de RFID (identification par fréquences radio) est apparue la première fois lors de la 2éme Guerre Mondiale ; elle est directement liée au développement de la radio et du radar. Pour identifier si les avions qui arrivaient dans l'espace aérien britannique étaient amis ou ennemis, les alliés mettaient en place dans leurs avions des transpondeurs (sorte d'imposantes balises) afin de répondre aux interrogations de leurs radars. Ce système, dit IFF pour "Identify : Friend or Foe", est la première utilisation de la RFID. De nos jours, le contrôle du traffic aérien reste basé sur ce principe.Alors on peut décrire la radio-identification (ou RFID de « Radio Frequency Identification ») comme étant une façon de reconnaitre à distance un objet, d'en suivre le cheminement et d'en connaître les caractéristiques. Elle permet aussi d'identifier une personne sans avoir à sortir sa carte d'identité grâce à une étiquette émettant des ondes radio, attachée ou incorporée à la personne ou à l'objet.

La technologie RFID permet la lecture des identifiants même sans ligne de vue directe et peut traverser de fines couches de matériaux (peinture, neige, boites etc.).

Le développement du module RFID passif faible coût fait l'objet de nos travaux. Nous nous intéressons tout particulièrement à exploiter cette technologie dans le cadre d'un système complet d'identification en veillant sur la sécurité et l'intégration des donnée.

Ce mémoire décrit l'ensemble de nos travaux. Il est constitué de la présente introduction, de trois chapitres et d'une conclusion.

Dans le premier chapitre, nous donnons une présentation des systèmes et techniques d'identification qui existent tels que les codes à barre, les systèmes optiques tout en les comparant avec les systèmes RFID. Nous détaillons ensuite les différents domaines d'application de la technologie RFID. Dans le deuxième chapitre, on présente l'architecture et le fonctionnement des différents systèmes RFID existants.

Troisième chapitre est dédié à la présentation des différents montages réalisées pour construire progressivement un système de contrôle d'accès RFID et d'alerte par module GSM et protégé par mot de passe

Finalement, la conclusion résumera l'ensemble des travaux de cette mémoire et présentera les perspectives envisagées.

Chapitre I

Généralités sur les technologies d'identification automatique des objets

I .1 Introduction

L'identification est l'action d'identifier un objet, ou à le discriminer parmi d'autres objets identiques, à lui conférer en définitive une identité unique lui permettant d'être reconnu automatiquement et sans confusion possible par un système de traitement de données.

Une identification peut se faire avec plusieurs types de technologies et de différentes manières. Ces technologies présentent aussi bien des avantages que des inconvénients.

Ainsi le présent chapitre est consacré à ces dernières qui sont : le code à barres, la reconnaissance optique des caractères, la carte à puces et la RFID.

I.2Les code à barres

Le code à barres est néà la fin de la deuxième guerre mondiale dans une chaîne de magasin alimentaire. L'entreprise avait besoin d'une solution de saisie automatique des données relatives aux produits passant aux caisses de ses magasins. Il représente la codification graphique d'une information. C'est donc une solution technique d'acquisition automatique d'une information entre le papier et l'informatique ou plus exactement une interconnexion des systèmes d'information et leur mise à jour en temps réel. C'est la plus utilisée. Elle permet de limiter les temps de saisie nécessaires au suivi d'un produit dans un processus de fabrication ou d'un document devant circuler au sein d'un service, d'une entreprise ou d'un couple fournisseur et client.

Très fréquents dans notre quotidien, les codes à barres dominent les systèmes d'identification automatique depuis plus de 40 ans. Le code à barre est un code binaire représenté par une séquence de barres vides et de barres pleines, larges ou étroites, disposées parallèlement. La séquence peut être interprétée numériquement ou alpha numériquement. Elle est lue par balayage optique au laser, c'est-à-dire d'après la différence de réflexion du rayon laser par les barres noires et les espaces blancs [1].

Il existe une dizaine de types de codes à barres différents que nous présentons dans la suite.

I.2.1 Les codes à barres unidimensionnels ou linéaires [1]

• Le code EAN-13

Figure I.1 : Code à barres EAN-13

Le code à barres « European Article Numbering » (EAN) a été développé à partirdu code américain « Universal Product Code » (UPC) pour les besoins spécifiquesdu commerce européen. Il existe deux variantes, l'une à 8 chiffres et l'autre à13 chiffres, la seconde étant la plus utilisée.

• Le code 39

Figure I.2 : Code à barres 39

Le code à barres 39 est fréquemment utilisé dans le domaine de la vente des produits pharmaceutiques.

Chaque caractère est composé de 9 éléments : 5 barres et 4 espaces.Chaque barre ou espace est « large » ou « étroit » et 3 parmi les 9 éléments sont toujours « larges ». C'est d'ailleurs ce qui est à l'origine de son nom : Code 39.

I.2.2 Les codes à barres linéaires empilés [1]

• Le code PDF 147

Figure 1.3 : Code PDF 147

De longueur variable et comportant jusqu'à 1850 caractères alphanumériques ou 2710 caractères numériques, il permet d'imprimer beaucoup d'information sur très peu de surface : 180 caractères alphanumériques par cm^2. La grande capacité du code PDF 147 est mise à profit lorsque des informations détaillées doivent impérativement être attachées à l'objet identifié, comme c'est le cas dans le transport des matières dangereuses par exemple.

• Le code 16K

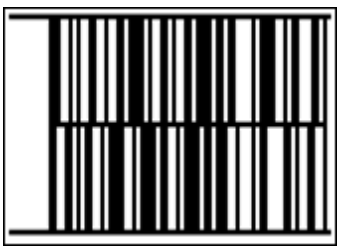


Figure I.4 : Code 16K

De longueur variable et permettant de codifier les 128 premiers caractères«American Standard Code for Information Interchange» (ASCII), il a une densité maximum de 32 caractères alphanumériques, ou de 65 caractères numériques, par cm^2. Il comprend 2 à 16 lignes de 5 caractères ASCII. Le code 16 K est utilisé dans de nombreux domaines (défense, santé, industries électroniques et chimiques,. . .), à l'exception du commerce de détail.

I.3 Les codes à barres à deux dimensions [1]

• Le code One

Figure I.5 : Code One

De longueur variable, et comportant jusqu'à 2218 caractères alphanumériquesou 3550 caractères numériques, il permet d'imprimer beaucoup d'informationssur très peu de surface soit : 500 caractères alphanumériques sur 1,6 cm^2.

• Le code Datamatrix à 2 dimensions :

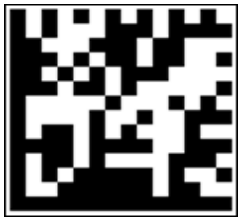


Figure I.6 : Code Datamatrix

De longueur variable, et comportant jusqu'à 2335 caractères alphanumériques ou 3116 caractères numériques, il permet d'imprimer beaucoup d'informations sur très peu de surface. Il incorpore un système de correction d'erreur de lecture.

Aussi ancien que les autres technologies d'identification, le code barre conserve des avantages importants notamment son coût quasiment nul et sa large diffusion.

En revanche, il présente plusieurs inconvénients tels que : sa fragilité, il doit être lu de manière optique et peut être remplacé par quelqu'un de mal intentionné. De plus, il ne peut pas être modifié à distance, contient peu d'informations et n'a bien sûr aucune capacité de traitement de données [1].

I.3.1 La reconnaissance optique des caractères[1].

La reconnaissance optique des caractères (Optical Character Recognition, OCR)fut la technologie la plus utilisée des années 1960 Plusieurs polices de caractères furent développées

pour cette technologie qui est basée sur la conception de caractères lisibles à la fois par l'homme et par la machine.

De nos jours, On utilise les systèmes OCR dans le domaine administratif et les services bancaires, notamment pour l'encaissement de moyens de paiement, tels que les chèques ou les bulletins de versement. Cependant, les systèmes OCR n'ont pas connu un grand succès, c'est notamment dû à la complexité des lecteurs et à leur prix élevé en comparaison avec d'autres systèmes d'identification.

I.4 LES SMART CARDS [1]

Une smart card («carte intelligente» ou «carte à puce»), est un système électronique de stockage de données, éventuellement avec une capacité de traitement (carte à microprocesseur) qui, par commodité, est incorporé dans une carte en plastique de la taille d'une carte de crédit. Les premières smart cards sont apparues en 1984, sous la forme de cartes téléphoniques prépayées. Pour fonctionner, les smart cardsdoivent être placées dans un lecteur, qui entre en contact avec la surface de contact de la smart card. Le lecteur fournit à la smart card l'énergie et la pulsation d'horloge.

Les transferts de données entre le lecteur et la carte se font par une interface série bidirectionnelle (port E/S) .

Un des principaux avantages des smart cards est que les données qui y sont stockées peuvent être protégées contre les accès (lecture et/ou écriture) non désirés.

Les smart cards simplifient et sécurisent de nombreux services, à commencer par les transactions financières. En 1992, 200 millions de smart cards avaient déjà été produites dans le monde. En 1995, ce chiffre était de 600 millions, dont 500 millions de cartes mémoire et inconvénients, basés sur la nécessité du contact et des manipulations : elles sont vulnérables à la corrosion et la poussière. Les lecteurs qui sont utilisés fréquemment (cabines téléphoniques, automates à billets,...) tombent en panne et sont chers à entretenir. De plus, les lecteurs accessibles au public ne peuvent pas être protégés contre le vandalisme.

On distingue deux types de smart card dont la différence est basée sur leur fonctionnement interne : la carte mémoire et la carte à microprocesseurs [2].

I.4.1Les cartes mémoires [2]

Les cartes mémoires fonctionnent sur le principe d'une machine à états ; on accède à la mémoire généralement une EEPROM selon une logique séquentielle. Elles peuvent contenir des algorithmes de sécurité simples. Les fonctionnalités des cartes mémoires sont

généralement optimisées pour une application spécifique. Les applications sont assez rigides, mais les cartes sont bon marché ; on les utilise dans des applications à large échelle, là où le coût est un facteur essentiel.

I.4.2 Les cartes à microprocesseur [2]

Les cartes à microprocesseur comme leur nom l'indique, contiennent un microprocesseur, connecté à une mémoire segmentée (segments ROM, RAM et EEPROM).

La ROM (Read Only Memory) : Elle comprend un système d'exploitation pour le microprocesseur. Le contenu de la ROM est inséré lors de la fabrication de la puce; il est identique sur toutes les puces issues du même lot et ne peut pas être modifié.

L'EEPROM (ElectricallyErasable Programmable Read Only Memory) : Elle contient les données et le programme relatif à l'application. La lecture et l'écriture de cette zone mémoire sont contrôlées par le système d'exploitation et se fait après la fabrication.

La RAM (Random Access Memory) : C'est la mémoire temporaire de travail du microprocesseur. Les données stockées dans la RAM sont perdues quand l'alimentation électrique est interrompue. Les cartes à microprocesseur sont très pratiques, puisque l'on peut facilement intégrer plusieurs applications différentes dans une même carte (multi-applications). Les cartes à microprocesseur sont surtout utilisées dans les applications qui demandent un certain niveau de sécurité, comme les cartes pour téléphones GSM ou les cartes de type « porte-monnaie électronique ». La possibilité de programmer les cartes à microprocesseur favorise l'adoption rapide de nouvelles applications.

I.5 La RFID

La RFID est une technologie d'identification par radiofréquence. Acronyme anglophone signifiant « Radio FrequencyIdentification », elle est parfois traduite par IDRF ou IDFR (respectivement « Identification par RadioFréquences et Identification par Fréquences Radio). Elle fait partie des technologies d'identification automatique au même titre que la OCR et le code à barres et permet d'identifier un objet ou une personne, d'en suivre le cheminement et d'en connaître les caractéristiques à distance grâce à une étiquette émettant des ondes radio, attachée ou incorporée à l'objet ou à la personne.

La commission européenne dans sa recommandation du 12 mai 2009 définit la RFID comme étant « l'utilisation d'ondes électromagnétiques rayonnantes ou d'un couplagede champ réactif dans une portion de spectres radiofréquences pour communiquer vers ou à partir d'une étiquette selon différents schémas de modulation et d'encodage afin de lire, de façon

univoque, l'identité d'une étiquette radiofréquence ou d'autres données stockées sur celle-ci» [4].

Les systèmes RFID sont très proches des smart cards. Comme sur les smart cards, les données sont stockées sur une puce électronique (Tag). Cette puce peut être de type « machine à états » ou contenir un microprocesseur, elle peut avoir différents types de mémoire. Par contre, à la différence des smart cards, il n'y a pas de contact physique entre la puce et le lecteur ; l'alimentation électrique de la puce se fait par télé-alimentation. Les données sont transmises par couplage magnétique ainsi que par réflexion des ondes radio. C'est bien de là que vient le nom de cette technologie :Radio Frequencyd'Identification[1].

I.6 Les avantages de la RFID par rapport au code-barres

I.6.1 La lecture des données

a) La lecture à distance

L'avantage principal de la technologie RFID par rapport au code à barres se situe au niveau de la lecture. Tout d'abord, la lecture des puces RFID ne nécessite pas un flashage systématique de toutes les étiquettes. Pour la réception de marchandises, des contrôleurs scannent chaque palette, carton ou produit un par un pour effectuer l'entrée en stock. Il en va de même pour les inventaires ou chaque produit doit être scanné pour entrer dans la base de données. Cela pose bien sûr des problèmes logistiques surtout dans le cas de traitement de grands volumes. En plus l'intervention humaine peut donner lieu à des erreurs et donc à une mauvaise analyse des données. La puce RFID peut être lue à distance et donc bien plus rapidement. Les distances de lecture varient selon les fréquences utilisées, de quelques centimètres à plusieurs dizaines de mètres.

b) La lecture de masse

Tous les experts sont unanimes, le potentiel de la RFID va bien au-delà d'une simple automatisation des applications de lecture actuelles. Elle permet d'inventer de nouveaux modes d'identification. De par sa capacité à identifier simultanément et à distance des objets, qu'ils soient visibles ou "cachés", elle multiplie les schémas de lecture possibles. En matière de lecture RFID, il convient de distinguer deux grandes catégories d'application : les applications de lecture unitaire : le lecteur identifie un objet à la fois. La RFID permet, en premier lieu, une simplification du processus de lecture tel qu'il existe aujourd'hui avec le code à barres. Un lecteur RFID peut identifier un objet sans intervention humaine, ni automatisme supplémentaire; · les applications de lecture simultanée : le lecteur identifie plusieurs objets à la fois. La RFID offre ainsi des perspectives nouvelles. Elle permet

d'identifier les composants d'un regroupement d'objets et plus seulement le regroupement lui-même. On parle dans ce cas de lecture en masse. Qu'il s'agisse d'identifier des unités consommateurs dans un carton ou des cartons sur une palette, la lecture en masse représente un saut qualitatif sans précédent. [4]

Actuellement, le marquage code à barres ne permet pas, pour des raisons de performance et de productivité, de multiplier les points de lecture, en dehors des opérations de constitution des palettes. En effet, chaque contrôle d'une unité d'expédition nécessiterait son démantèlement puis sa reconstitution à l'identique. La lecture en masse permettrait, a contrario, de multiplier les points de contrôle de façon presque transparente pour les organisations[4].

Les derniers tests effectués par GS1 France sur la lecture de masse[1]démontre quepour les produits dit neutres, c'est à dire qui n'émettent pas d'interférences, le tauxde lecture d'une palette est de 100 %.

I.6.2 Les données contenues dans la puce RFID

a) Une capacité de stockage supérieure

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

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

b) Des puces réutilisables

Les puces RFID sont également réutilisables selon les modèles. En fonction lesbesoins de l'entreprise, l'utilisation de ce type de puces réinscriptibles s'avère êtreune solution parfaitement adaptée. La gestion des supports de manutentions en estl'un des meilleurs exemples. Pour des raisons d'efficacité, il est important que latechnologie utilisée pour identifier les supports reste opérationnelle durantl'intégralité de la vie du support. De plus le coût unitaire de chaque puce nereprésente plus une limite d'utilisation puisque ce type de puce peut être utiliséejusqu'à 100 000 fois [4].

c) Une meilleure utilisation des données

C'est sûrement l'avantage principal de la puce RFID, le traitement des données endirect offre des possibilités très importantes pour les entreprises. En effet, là où lescannage est obligatoire pour le code-barres, la RFID permet de connaître la situationen temps réel, que ce soit pour le transport, le stockage ou tout autre aspect de lachaîne logistique. Le mécanisme de suivi de la traçabilité [4] ; c'est à dire la capacité àsuivre le mouvement de produits individuels ou de conteneurs tout au long duprocessus de leur distribution et de leur livraison, à présenter des états sur cesmouvements et à répondre à toute requête correspondante ; est primordial pour lesentreprises. Ce suivi permet notamment la compréhension des erreurs et offre lesoutils nécessaires pour améliorer la chaîne dans son ensemble. Le suivi en temps réelest par conséquent un gain de temps pour l'entreprise et donc une meilleure réactivitéface aux problèmes.

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

d) Une technologie difficilement reproductible

La contrefaçon est encore l'un des domaines ou la RFID possède un avantage sur lecode à barres. La reproduction des codes à barres est relativement facile puisqu'ilsutilisent une technologie très simple. L'expertise nécessaire pour la fabrication depuce RFID demanderait alors un investissement et des compétences difficiles àréunir. De plus les numéros EPC par exemple sont particulièrement difficiles àreproduire.

I.7*Les limites de la RFID par rapport au code-barres*

Nous avons pu constater que le RFID avait un certain nombre d'avantages parrapport au code à barres. Cependant, cette technologie est aujourd'hui en pleineexpansion et comme

toutes les nouvelles technologies, présente des défauts mais aussi certaines limites techniques. Enfin, la RFID manque égalementde repères et de standard quant à son utilisation.

I.7.1 Les limites techniques

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

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

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

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

b) Les produits avec un emballage métallique

La présence de métal à proximité des puces RFID dérègle le fonctionnement de leurantenne. Cette antenne qui permet à la puce de transmettre les données mais aussi des'activer par l'énergie envoyée par le lecteur (pour les puces passives). Là aussi, letaux de lecture est fortement réduit. De plus, comme pour les produits à forte teneuren eau, le métal provoque des interférences qui réduisent également le taux de lecturepour des palettes complètes par exemple

c) Une lecture de masse imparfaite

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

d) L'utilisation des fréquences

L'utilisation, des fréquences, voilà une contrainte qui apparaît souvent lorsque lesnouvelles technologies utilisent les ondes. On avait déjà observé ce problème

pourl'utilisation de masse des téléphones portables dans les années 90. L'armée avaitbloqué certaines fréquences en France. Le problème se reproduit pour la RFIDpuisque l'armée tarde encore à autoriser l'utilisation des fréquences nécessaires. Ceretard entraîne une difficulté de déploiement de la technologie en France.

e) La RFID piratable

Une équipe de chercheur néerlandais a réussi à créer le premier virus pour les pucesRFID. La puce transmettant les données qu'elle contient, les chercheurs ont tenté deprouver qu'elle pouvait au moment de sa lecture infecter l'ensemble d'un systèmeinformatique. Les chercheurs ont réussi à introduire ce virus dans une base dedonnées Oracle qu'ils avaient utilisé pour faire un test. Alors faut-il s'inquiéter decette découverte ? La RFID sera-t-elle menacée par ces virus ?

I.7.2 Le prix des puces

L'utilisation d'une nouvelle technologie représente toujours un défi mobilisateur dans l'entreprisse. Cette innovation dans l'entreprise permet de renouveler lesprocess, on a pu voir que la RFID offrait certaines opportunités dans ce domaine, mais la question du coût est essentielle. Aujourd'hui, le principal frein au développement de la RFID est son prix.Technologie encore récente et peu utilisée au vue des prévisions pour le futur, lespuces conservent un prix élevé réinscriptibles ou modifiables n'ont bien sûr pasle même prix que celles à utilisation unique. A cela, il convient d'ajouter l'ensemble des investissements nécessairesà l'utilisation des puces (imprimantes, lecteurs …) et au traitement des donnéesqu'elles contiennent. On obtient alors un investissement que peu d'entreprises sonten mesure d'assurer actuellement comparé à l'utilisation du code à barre qui à l'unité ne coûte pratiquement rien et dont les outils d'utilisation et de gestion sont eux aussirelativement abordablesPourtant, on observe depuis quelques années, une baisse continue des prix des puceset des équipements. Au fur et à mesure que les entreprises investissent dans cettetechnologie, les solutions s'améliorent et l'utilisation de la RFID à grande échelleentraînera obligatoirement une forte baisse des prix. On observe déjà certainesentreprises capables de fournir l'ensemble puce, antenne et étiquette à moins de 10centimes d'euros si les volumes sont supérieurs à 1 million d'unités. Selon certainesétudes, le marché de la RFID devrait progresser et on prévoit plus de 30 milliardsd'objets équipés de puces en 2020 et surement des centaines de milliards d'ici 15 ou20 ans. On imagine donc que ces volumes importants auront une incidence sur lesprixsource .

I.8 vers une utilisation des 2 technologies

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

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

Quand une impossibilité technique avec la RFID se présente, l'usage du code-barres est alors entièrement possible et compatible. Les opérateurs de ces sociétéspeuvent désormais avoir des équipements polyvalents et, suivant les postes de travail,lire une puce ou un code à barre. Ceci signifie qu'il est possible de combiner les deuxtechnologies et donc de développer des solutions adaptées à chaque étape dudéploiement de la RFID.

En plus d'être complémentaires, les technologies ne sont pas forcément utilisées pourles mêmes besoins. En effet « il ne faut pas systématiquement comparer RFID etcode à barres, les 2 technologies ont des applications différentes [5]». Chaqueentreprise doit donc déterminer si la RFID s'intègre dans sa stratégie logistique et sielle apporte une véritable plus-value. Le passage à la RFID obligera les entreprises àconserver les codes à barres pendant une période de transition. Il n'est pas sûr quetous les acteurs de la chaîne logistique se convertissent à la RFID rapidement. Ons'achemine donc vers une utilisation commune de la RFID et du code à barrespendant les années à venir. De la même façon que le texte n'a pas disparu desétiquettes code à barres, les étiquettes RFID conserveront une zone dédiée à cettetechnologie. D'ailleurs la plupart des fabricants de matériels RFID l'ont bien compriset propose des outils permettant d'utiliser les 2 technologies indifféremment. Leslecteurs portatifs RFID ont également sur certains modèles la capacité de flasher descodes à barres.

I.9La traçabilité et le tracking

Crises sanitaires, retraits de produit, rappels, voilà des situations où le suivi desmarchandises a toute son importance. La traçabilité des produits connaît undéveloppement important et les industriels autant que les distributeurs sont désireuxde connaître l'endroit où sont les produits, leurs provenances …

Cette exigence de traçabilité ne concerne pas seulement le secteur alimentaire Ou pharmaceutique. L'ensemble des entreprises est conscient maintenant de la nécessité de suivre les produits et de déterminer leurs parcours tout au long de la chaîne logistique. La RFID propose des solutions innovantes dans ce domaine, les possibilités des puces sont totalement compatibles avec cette exigence de traçabilité.

a) La puce lecture écriture : Une solution globale de traçabilité

Les solutions de traçabilité pour les entreprises dépendent du type de puces qu'ellesutiliseront. Les puces passives du type WORM (Write One Read Many) fonctionneront de la même façon qu'un code à barres avec tous les avantages que propose la RFID : Vitesse de lecture, lecture de masse … Dans ce cas, le fonctionnement du système de traçabilité sera classique avec une compilation des données tout au long de la chaîne logistique dans une base de données centrale qui permettra de suivre les produits tout au long de la chaîne.L'avantage de la RFID est la lecture automatique qui évite les erreurs et les oublis. Une fois le système au point, la traçabilité est automatique. Autre spécificité de la RFID, la puce n'est pas facilement reproductible et limite donc les risques de contrefaçon .Là où la RFID peut apporter un vrai plus, c'est dans le cas de l'utilisation d'une puce permettant la lecture et l'écriture. Ce système offre la possibilité de se passer d'une base de données centrale. L'unité logistique où le produit recevra au fur et à mesure différentes informations leconcernant. On inscrira ainsi dans la puce, la date de production, mais aussi les matières premières utilisées et l'adresse de livraison prévue. Puis au moment de l'expédition, le prestataire de transport entrera la date d'enlèvement puis celle de livraison à l'entrepôt du distributeur. Ensuite le distributeur entrera ses propres informations avant de mettre le produit à la vente. Lors de la mise en vente du produit, le distributeur peut compiler l'ensemble de ses informations dans sa base de données. La transmission d'information se fait par la puce et non plus par système EDI. Bien sûr, cette solution demande que tous les acteurs de la chaîne logistique possèdent les mêmes normes et les outils adéquats pour traiter l'information et l'inscrire dans la puce au fur et à mesure.

b) Le suivi des marchandises

Le suivi des marchandises est également une autre application de la RFID. La lectureà distance permet de multiplier les points de contrôle et donc de connaître l'emplacement exact d'une unité logistique à un moment donné. Pour cela, il faut disposer les lecteurs RFI à des endroits stratégiques comme les quais de réception et de livraison mais aussi au niveau de la préparation de commande. On connaît ainsi l'avancement des produits dans le processus de livraison en temps réel et le moment de leur départ.

Une autre solution est de mettre en place un système regroupant une puce RFID et unSystème GPS permettant le suivi de marchandises en temps réel. Le coût de telséquipements est très élevé. Ils sont d'ailleurs pour l'instant à l'étude mais l'arrivée depuces munies d'un composant GPS pour suivre cette puce en temps réel sera uneréalité d'ici quelques temps. On imagine bien les débouchés d'une telle technologie.

De nombreux secteurs d'activités seront intéressés par ce produit. On pensenotamment aux messageries express ou à certains produits de valeur ou urgents quipourraient être suivis en continu. Ce suivi des produits offre une meilleure visibilitépour la gestion des transports et de la logistique en général.

I.9.1.2La gestion de production

L'introduction de la RFID sur les chaînes de montage, voilà encore l'une des applications de la radio fréquence. Les puces permettent alors de suivre l'évolution de la production mais aussi de connaître le niveau de stocks des composants et des produits semi finis. Les éléments sont également automatiquement dirigés vers le bon atelier de montage. On obtient alors une visibilité totale de la chaîne de production. L'entreprise possède alors toutes les informations pour faire face en cas de problème. On estime que le gain en termes de coût est compris entre 2 et 8% [5].

I.9.1.3 Le transport

Le transport est l'un des centres de coût important pour une entreprise productrice oudistributrice de produits. L'optimisation du transport peut passer par la technologie RFID qui propose des améliorations intéressantes dans ce domaine. Tout professionnel a été confronté un jour à une erreur de chargement ou de destination. Ces problèmes récurrents dans le transport peuvent être réduits grâce la RFID.

a) Des temps de contrôle réduits

La RFID ouvre des perspectives immenses pour le secteur du transport. Dans un futur proche il sera possible d'équiper un camion de nombreux équipements utiles pour le suivi des marchandises. Tout d'abord, un système GPS communicant avec les puces RFID contenues dans les camions pour ainsi suivre le trajet et les délais de livraisons des marchandises.

Il pourra également être équipé d'instruments de mesure pour certains types de produits.

Des appareils de mesure de la température ou du taux d'humidité placé dans le camion enregistreront l'ensemble des données et pourront même les communiquer aux puces RFIDplacées sur les unités logistiques. En plus des données concernant le produit lui-même, on obtiendra aussi les données sur les conditions de transport et ainsi vérifier toutes anomalies possibles. Toutes ces innovations ne sont totalement applicables du fait de leur coût et du manque de maîtrise de la technologie RFID mais on peut penser qu'elles seront disponibles dans le futur.

I.9.1.4 La gestion de stock

L'utilisation de la RFID apporte de nombreux gains tout au long de la chaîne logistique. La gestion d'entrepôt en bénéficie évidemment et c'est peut-être dans ce domaine que les progrès en terme d'efficacité sont les plus importants. De la réception à l'expédition en passant par l'entreposage, la RFID apporte une véritable valeur ajoutée pour ce type d'activité.

a) La réception

La réception, endroit stratégique dans un entrepôt profite pleinement de l'introduction de la

RFID. C'est en terme de temps et d'efficacité que la RFID apporte un vrai plus dans la gestion des réceptions de marchandises. Là où le code-barres oblige un ou plusieurs employés scanner le code de chaque carton ou de la palette entière, la RFID offre la lecture instantanée et simultanée de l'ensemble des marchandises contenues sur la palette ou l'unité logistique. Les marchandises sont alors contrôlées avec un ensemble de données important. Couplé au système informatique de l'entrepôt, il n'est plus nécessaire de contrôler (bill of lading ou packinglist). Le temps de contrôle d'un camion entier passe ainsi de 23 minutes à 3 minutes avec des portiques RFID permettant la lecture en grand nombre [14]. Comme nous avons pu le voir également précédemment, la possibilité de rechercher rapidement un colis ou une palette offre un gain de rapidité pour les colis urgents.

Ces améliorations s'accompagneront également d'une réduction du nombre d'employés nécessaires à la réception des marchandises.

b) La gestion du cross-docking

Pour les opérations de cross-docking et de distribution de gros volumes, la RFID représente une solution d'optimisation. L'utilisation d'étiquettes sur les palettes permet une meilleure efficacité pour sélectionner les palettes et les mettre sur leur emplacement avant leurréexpédition. Si les cartons sont également tagués avec de la RFID, on peut également repérer les cartons de produits pour reformer des palettes et ainsi les réexpédier au plus vite. Cela limite également les risques d'erreur et le temps de scannage de toutes les étiquettes.

c) L'entreposage et picking

Les bénéfices que l'on peut retirer de la RFID pour l'entreposage sont plus difficiles pour le moment à identifier. Cependant on pourrait imaginer l'installation de puce RFID sur les différents racks de stockage qui donneraient en temps réel des indications aux manutentionnaires. Si l'employé fait une erreur de placement de la palette il en sera informé de suite avec un système d'alerte. L'utilisation des étiquettes RFID pour le stockage temporaire est un axe d'amélioration de la gestion des stocks. La RFID offre plus de flexibilité au niveau de la zone de stockage temporaire ainsi que pour l'emplacement des palettes qui la composent. Tous ces bénéfices seront également utiles lors du picking des marchandises.

On observera là également des gains de productivité même si ces derniers seront moins importants que pour la réception et l'expédition

d) Les inventaires

En multipliant les points de contrôles, les entreprises possèdent avec la RFID la capacité de connaître en temps réel l'état des stocks. Là où le code à barres obligeait à effectuer des inventaires de manière annuelle ou semestrielle, la RFID multiplie le nombre de lectures possibles. Des lecteurs sont alors placés sur les racks pour contrôler le nombre de cartons ou palettes présents et donnent donc une vision globale et en temps réel de l'ensemble des produits. Il est également envisageable d'effectuer ces inventaires avec un lecteur mobile. Les employés balayeraient alors l'ensemble des palettes. Un système d'alerte déterminerait les unités logistiques mal placées. Cependant, il faut être réaliste, la technologie permet d'équiper un entrepont dans sa totalité en lecteur RFID mais l'investissement serait bien trop élevé par

rapport aux gains espérés. Un entrepôt donnant en temps réel le nombre de cartons présents est encore impossible mais c'est l'une des pistes d'utilisation de la RFID pour le futur.

e) L'expédition

La possibilité de vérifier en temps réel le chargement d'un camion est un gain énorme en termes d'efficacité et de temps pour l'expédition des marchandises. Le contrôle des marchandises à l'expédition et à la réception se fera plus rapidement. Les informations sur le connaissement seront également vérifiées plus vite.

Les gains dans le domaine de l'entreposage sont donc importants. Comme le prouve le tableau ci-dessous, on peut espérer des gains particulièrement élevés dans les domaines de la réception, l'expédition et le contrôle des marchandises. Ces gains dépendront de l'avancée de la technologie, du coût ainsi que du niveau d'investissements.

Pour conclure, les possibilités de la RFID sont immenses et elles représentent une véritable révolution dans le domaine du suivi des marchandises. Elle reste pourtantune technologie jeune et en devenir certaines contraintes technologiques doivent êtreétudiées et optimisées. Enfin elle ne remet pas en cause l'utilisation du code à barresqui survivra encore de nombreuses années.Dans le chapitre prochain nous allons les types de systèmes RFID leurs compositions et leurs principes de fonctionnement.

Chapitre II

Présentation de RFID

II.1Introduction :

Insérer une clé pour démarrer un véhicule, badger pour accéder à un bâtiment ou une salle, valider un titre de transport dans le bus ou le métro sont des gestes entrés dans le quotidien de bon nombre d'entre nous. On utilise, sans en être toujours conscient, des technologies de capture automatique.

En effet la Radio-Identification ou la RFID est l'annonce d'une mutation radicale dans l'organisation du commerce, du transport, de la sécurité et de la surveillance.

L'objectif de ce chapitre est de présenter la technologie RFID. La première section aborde les différentes architectures des systèmes RFID. La seconde section détaille leprincipe de leur fonctionnement. La troisième section développe les techniques de communication entre lecteurs et transpondeurs d'un système RFID. Enfin la dernière section présente quelques applications et une conclusion.

II.2Composants des systèmes RFID :

II.2.1Tags :

Les tags RFID, également appelés transpondeurs, peuvent être classés en plusieurs catégories selon toute une série de caractéristiques. Ainsi, on fait généralement une distinction entre les puces actives et passives. La capacité de mémoire et les fonctions de lecture- écriture sont d'autres critères de distinction.

Pour représenter simplement l'architecture interne d'un transpondeur, il est intéressant de se référer au croquis suivant :

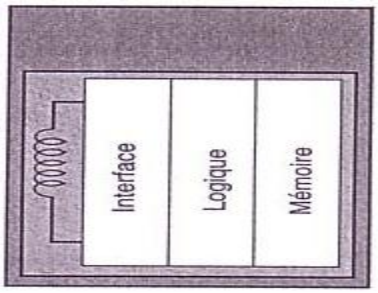


Figure II.1 : tag RFID

Ce schéma présente globalement les modules fonctionnels qui composent un transpondeur. Comme on peut le constater, un tag est tout d'abord équipé d'une interface radiofréquence dont le rôle est d'assurer la réception des signaux RF et de réagir à ces signaux pour se faire

comprendre du lecteur et lui fournir une réponse RF. Il est ensuite constitué d'une partie logique responsable du traitement des signaux. Ce module est utile s'il est nécessaire d'intégrer des mécanismes d'authentification et de sécurisation de l'accès aux données. Le transpondeur intègre enfin une mémoire qui stocke les informations, sécurisées ou non, en son sein.

Chacun de ces modules interagit de la façon qui suit avec les autres :

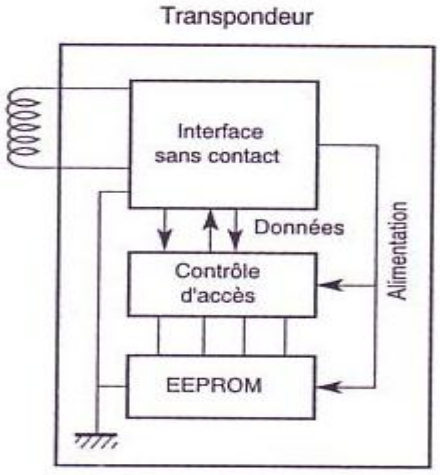


Figure II.2 : tag RFID

Sur le schéma ci-dessus, on peut remarquer que la partie logique ("contrôle d'accès") ainsi que la mémoire ("EEPROM") sont alimentées par la partie RF. Cela est valable dans le cas de télé alimentation.

Il est à noter que les transpondeurs se différencient également par le type de mémoire utilisé. Comme le schéma l'indique, le type de mémoire le plus couramment utilisé est l'EEPROM, ou E2PROM, (Electrically Erasable Programmable Read Only Memory) qui a la particularité d'être effaçable et programmable. Une mémoire EEPROM permet jusqu'à 500.000 réécriture possible. Le type de mémoire utilisé définit les modes de lecture et écriture possibles. Certains tags permettent de la lecture uniquement, ou bien une écriture unique (cas de tags initialement "vierges"). Encore une fois, le type de mémoire utilisé dépend de l'utilisation des transpondeurs. Dans le cas de simples vérifications d'accès, seule la lecture aura du sens pour les tags utilisés.

On letrouve souvent intégré dans un boîtier en plastique, ou à l'intérieur d’une étiquette d'un emballage dit « intelligent ». Le transpondeur comprend une antenne associée à une puce électronique qui peut répondre aux requêtes émises depuis un émetteur-récepteur [15].

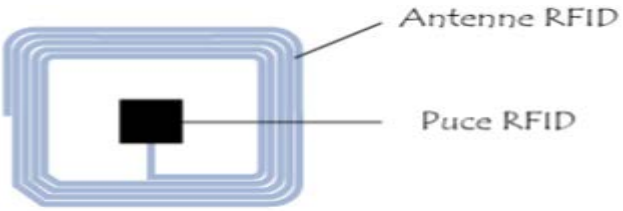


Figure II.3 :tag RFID

Il existe plusieurs types de fonctionnement et de communication possibles pour les étiquettes : ▪ Les étiquettes « lecture seule », c'est-à-dire non modifiables ce mode permet seulement de lire le contenu du tag.

▪ Les étiquettes « écriture une fois, lecture multiple »

▪ Les étiquettes en « écriture plusieurs fois et lecture plusieurs fois » ce mode de fonctionnement permet la réutilisation, le tag est réinscriptible.

II. 2.2Les types de tag

- Tag actif

La radio identification active est une forme de technologie d'identification caractérisée par l'usage de tags actifs également appelés étiquettes actives c'est-à-dire qu'ils sont alimentés par une source d'énergie embarquée : batterie, pile... etc. Une source d'énergie qui a la capacité de diffuser un signal vers le lecteur RFID à travers une antenne. Les tags sont de petits objets qui peuvent être collés sur des produits ou insérés dans ces mêmes produits, ils sont composés :

- D'une source d'énergie
- D'une puce électronique.
- D'une antenne

Son alimentation provient d'une source interne qui se dessine sous forme d'une batterie, d'une pile, etc. Ceci peut effectivement augmenter la portée du signal et ainsi communiquer avec un type de lecteur de faible puissance et à des distances de 20 à 100 mètres environ [16]. De ce fait, on parle d'indentification active lorsque l'étiquette elle-même est active L'avantage principal de ce type de tag réside dans le fait que le tag n'est pas forcement obligé d'être à proximité du lecteur.

Figure II.4 : tag RFID actif [16]

- Tag passif

Contrairement aux tags actifs, les tags passifs ne disposent pas d'une source d'énergie. Ils puisent leur énergie à travers le signal électromagnétique du lecteur qui permet d'activer le tag et lui permet ainsi d'émettre les informations. Les tags passifs utilisent différentes bandes de fréquences radio selon :

- Leur capacité à transmettre les données à des distances plus ou moins grandes.
- La structure des différents obstacles que les ondes électromagnétique doivent traverser (air, eau, métal...).

Comparé au tag actif, le tag passif est moins coûteux et peut être de plus petite dimension. Quand le tag reçoit un signal électromagnétique, il emmagasine l'énergie dans un condensateur embarqué (on-boardcapacitor) [16] et ce processus est appelé couplage inductif. Quand le condensateur est suffisamment chargé, il alimente le circuit du tag qui transmet à son tour un signal modulé au récepteur (lecteur) qui comprend des informations contenues dans le tag. La communication entre les deux dispositifs utilise deux méthodes pour moduler le signal transmettre.

Deux autres méthodes de classification des tags RFID furent : la lecture seule (RO) et la lecture/écriture (RW). Le type RO est caractérisé par une mémoire qui ne peut qu'être lue. On peut les assimiler à des codes bars de par sa mémoire statique. Ainsi cette dernière ne pouvant pas être altérée, ce type est fréquemment programmé avec une quantité de données limitées et statiques pour ystocker un numéro de série ou d'identification par exemple [17]. Le

type RW aussi appelé "Smart", plus maniable que les tags RO peuvent stocker une large quantité de données avec une mémoire adressable qu'on peut modifier facilement, les données peuvent être modifiées ou bien effacées autant de fois qu'on le souhaite. Ainsi certains Tags sont

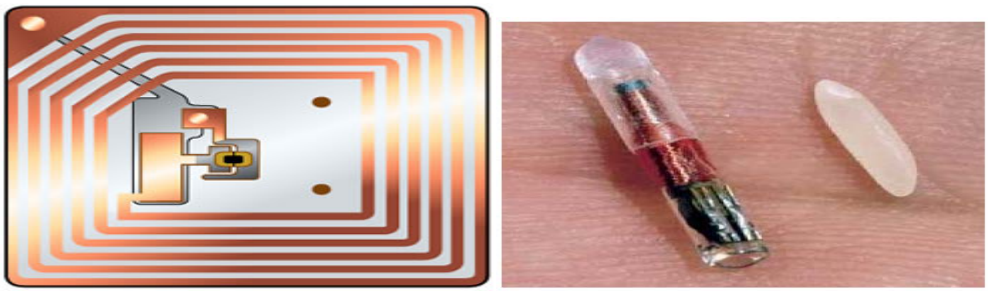


Figure II .5 :Tag RFID passif comparé à un grain de riz[17]

munis des deux types de mémoire Read Only et RW en même temps. Par exemple, le tag RFID d'une palette a un numéro de série contenu dans la section RO de la mémoire pour toute la durée d'utilisation de cette dernière et la section RW peut être utilisée pour indiquer le contenu à n'importe quel moment et quand la marchandise est renouvelée ou bien changée ; cette section de la mémoire est réécrite afin de suivre le changement du contenu

II.2.3Lecteurs

Les lecteurs, souvent appelés « interrogateurs », sont des équipements actifs, portables ou fixes, constitués d'un circuit qui émet une énergie sous forme de champ magnétique ou d'onde radio. Dans un scénario type, le lecteur envoie un signal à la puce et attend sa réponse. La puce détecte le signal et envoie une réponse qui contient un numéro de série ainsi qu'éventuellement d'autres informations au lecteur. Cette communication se fait grâce à chaque antenne RFID intégrée dans chacun d'entre eux. Dans les systèmes plus sophistiqués, le signal radio du lecteur peut contenir des commandes destinées à la puce, des instructions pour effectuer des opérations de lecture/d'écriture dans la mémoire de la puce, voire des mots de passe. La taille du lecteur, dépend de nombreux paramètres. Il peut varier de la taille d'une pièce de monnaie à celle d'un ordinateur de poche.

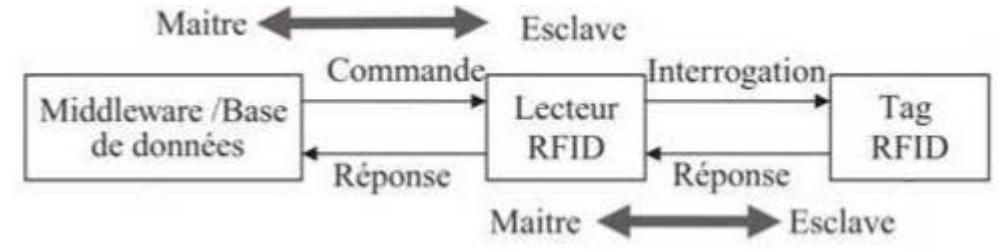
Un lecteur peut être doté de fonctionnalités GPS et de dispositifs de connexion à des systèmes et des réseaux d'information.

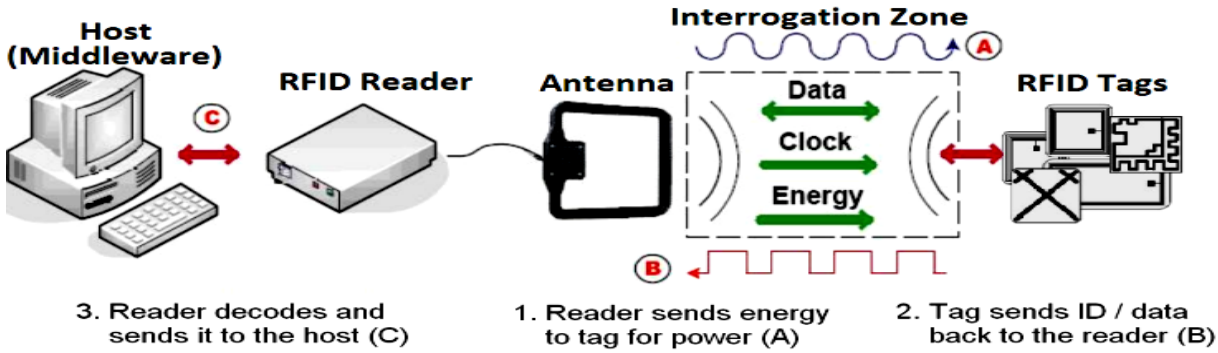
II. 2.4 Architecture d'un Lecteur RFID HF

Les lecteurs RFID d'aujourd'hui sont composés de systèmes d'antenne intelligents, d'unités numériques dédiées au traitement du signal et de systèmes embarqués aux côtés de middleware et de composants réseaux. Ces composants permettent une intégration facile des détecteurs RFID dans les réseaux de données conformes aux protocoles de transfert de donnéesnormalisées.[19].

Les lecteurs RFID sont des dispositifs qui effectuent l'interrogatoire d'étiquettes RFID. Dans un système RFID, le lecteur détecte le tag en utilisant des techniques de traitement du signal, de démodulation pour extraire des données à partir du signal du tag. Une étiquette passive RFID ne peut pas générer un signal sans que le lecteur n'envoie d'abord un signal d'interrogation au tag. Par conséquent, le lecteur et les étiquettes sont dans une relation maître-esclave dans laquelle le lecteur agit comme un maître tandis que les étiquettes fonctionnent comme des esclaves. Néanmoins, les lecteurs RFID eux-mêmes sont également dans une position esclave avec le logiciel qui gère l'application appelée middleware et qui traite les données de la RFID[19].

Voici un schéma bloc qui illustre la relation maitre-esclave (Master-Slave) entre les composants du système RFID :





FigureII.6 : Illustration de la relation maitre-esclave (Master-Slave) [5]

II. 2.5Station de base

Voici quelques équipements de stations de base :

Le premier modèle de station de base est un appareil couramment utilisé dans les applications d'identification par badge d'accès. Ces modèles sont installés près des portes et permettent d'y accéder si le tag de la carte d'accès possède les autorisations nécessaires.

Le second est un modèle portable plus évolué. Le lecteur est encapsulé dans un terminal portable permettant d'effectuer des mesures et des calculs dans le domaine d'application dans lequel il est utilisé. On rencontre ce genre de dispositif dans le milieu industriel pour effectuer du contrôle de flux et de gestion de stock, par exemple.

II. 2.6Constitution d'une station de base

Pour représenter simplement l'architecture interne d'une station de base, il est intéressant de se référer au croquis suivant :

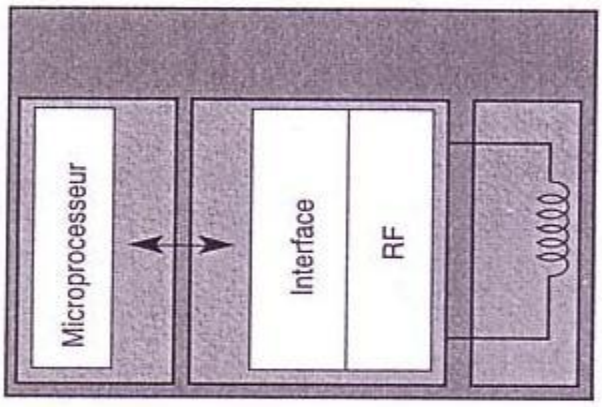


Figure II .7 : Tag RFID passif

Ce schéma présente globalement les modules fonctionnels qui composent une station de base. Un lecteur est tout d'abord équipé d'une interface, qui n'apparaît pas ici, avec le système hôte. Comme on peut le constater, il est ensuite constitué d'un microprocesseur qui permet de réaliser les calculs et effectuer les opérations nécessaires. Ce microprocesseur est interfacé avec la partie analogique (partie RF) qui assure la réception et l'émission des signaux radiofréquence. Le lecteur intègre également tous les circuits de gestion du protocole de communication et de la communication (comprenant les mécanismes d'anticollision, d'authentification et de cryptographie s'ils existent).

Etudions d'un peu plus près la constitution de la partie RF de la station de base :

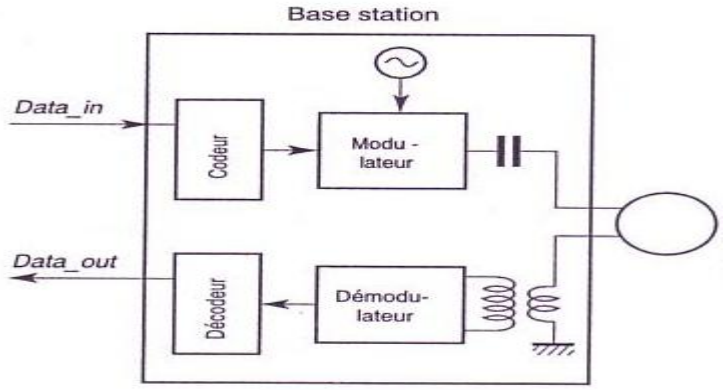


Figure II .8 : Tag RFID passif

Nous constatons que ce module est constitué d'outils de codage et décodage pour convertir les données binaires en signaux RF, et vice versa, et d'outils de modulation et démodulation pour transmettre le message grâce à une porteuse RF.

II.3Principe de fonctionnement de la RFID

Il a été découvert que lorsqu'on appliquait un courant électrique à une bobine de cuivre, alors un champ magnétique était induit. Par réciproque, lorsqu'une bobine de cuivre est parcourue par un champ magnétique, alors un courant électrique est induit à ses bornes. C'est ce que l'on appelle l'induction électromagnétique. Tout le mécanisme de communication en RFID repose sur ce principe.

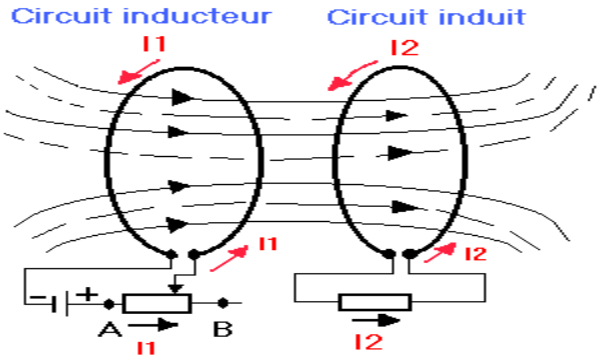


Figure II .9: Tag RFID passif

La première ellipse (gauche) du schéma ci-dessus représente la bobine de cuivre du circuit inducteur. Comme le montre le croquis, un courant électrique est, en effet, généré dans un circuit et parcourt la bobine : un champ magnétique est donc induit. Les lignes de champ magnétique sont représentées par des flèches sur le schéma (le sens du champ magnétique est lié au sens de propagation du courant dans la bobine - ici, les lignes de champs sont propagées vers la droite, parallèlement à l'axe de la bobine).

La seconde ellipse (droite) représente la bobine de cuivre du circuit induit. Cette bobine se trouve dans l'axe des lignes de champ magnétique et est donc parcourue par ce champ : un courant est donc induit à ses bornes et alimente son circuit. Il est à noter que la bobine du circuit induit est parcourue par le champ magnétique dans le même sens que la bobinedu circuit inducteur. Les courants parcourant les deux circuits sont donc propagés dans le même sens également.

Comme on peut le remarquer, dans les parties précédentes, les antennes utilisées pour les transpondeurs et les stations de base sont des bobines de cuivre. Les circuits de la station de base, dont l'antenne, sont alimentés par son environnement (hôte). De ce fait, un champ magnétique est induit et propagé par l'antenne du lecteur. Lorsqu'un transpondeur entre dans le champ magnétique d'un lecteur, son antenne de cuivre est parcourue par ce champ. Ses circuits sont alors alimentés par le courant électrique induit. Les deux appareils sont donc en mesure de communiquer.

Un système RFID se compose d'étiquettes et de lecteurs. L'étiquette contient l'identité à transmettre, tandis que le lecteur émet des signaux radio afin de lire ou d'inscrire des données sur l'étiquette. Lorsqu'une étiquette RFID détecte le signal entrant d'un lecteur (c'est-à-dire lorsqu'elle passe à distance de lecture de celui-ci), elle répond par un signal

sortant qui contient l'identité. Le lecteur reçoit alors cette identité et la transmet pour traitement à l'ordinateur auquel il est relié.

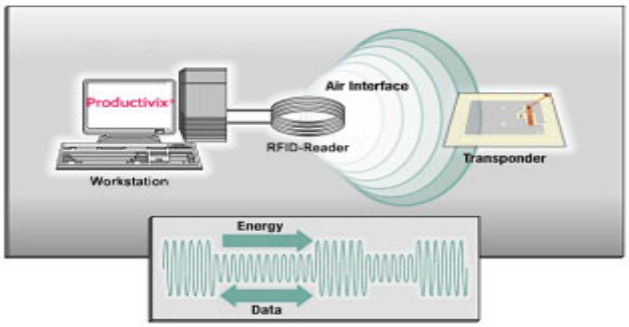


Figure II.10: Fonctionnement du RFID

Les données captées par le lecteur sont transmises et traitées par un système informatique comportant un logiciel, tel qu'un système de contrôle d'inventaire, un système de contrôle d'accès ou d'un système de contrôle de production.

II.4Principe de communication de la RFID

Voici, pour rappel, une représentation basique de la communication entre un transpondeur et une station de base :

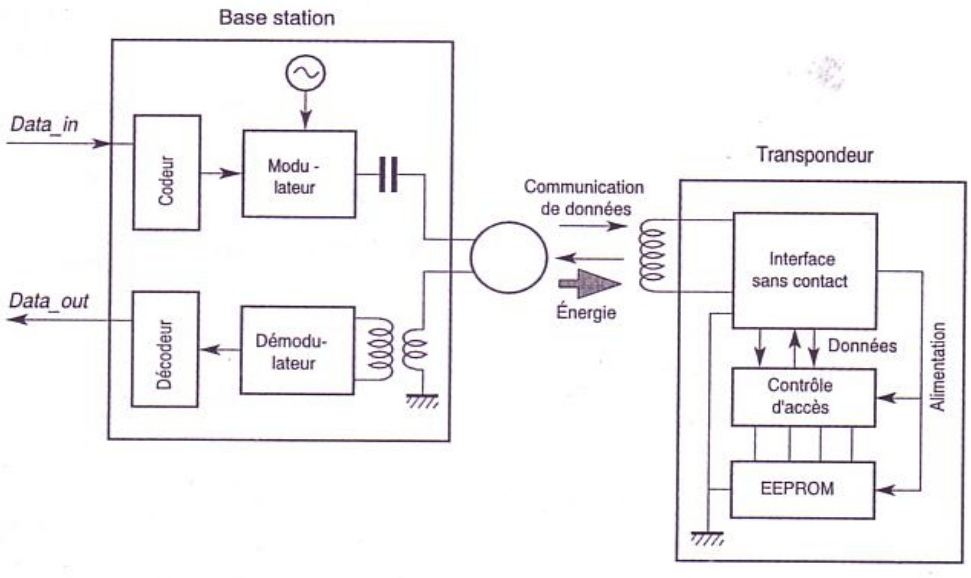


Figure II .11: Tag RFID passif

Comme nous l'avons déjà vu, la station de base est composée des outils de codage et décodage des signaux qui vont lui permettre de convertir les données binaires en signaux RF,

et vice versa. Elle intègre également les composants de modulation et démodulation qui vont permettre de transmettre les messages RF obtenus en modulant un autre signal radiofréquence : la porteuse. Nous allons donc décrire les principes de fonctionnement de l'ensemble de ces composants.

Nous avons également énoncé que le transpondeur possède, lui aussi, des outils de modulation/démodulation, inclus dans son interface sans contact, qui lui permettent de réagir aux signaux reçus et de se faire comprendre du lecteur. Nous allons également expliquer ces principes.

Nature de la communication

Le schéma ci-dessus présente deux éléments dans la composition de la communication : tout d'abord, les données qui sont effectivement échangées entre les deux équipements, mais aussi de l'énergie transmise du lecteur vers le transpondeur. Cette énergie est la source d'alimentation utilisée dans le cas de téléalimentation.

Les communications RFID, comme dans la plupart des communications sans fil, sont half-duplex. Cela signifie que chacun des interlocuteurs (ici la station de base et le ou les transpondeurs) communiquent à tour de rôle. Il existe cependant deux modes de communication liés à la présence des deux types d'information transmis :

- simultané : les données et l'énergie sont transmises simultanément au transpondeur,
- non simultané : les données et l'énergie sont fournies alternativement au transpondeur.

Comme dans toute conversation, l'un des deux interlocuteurs doit nécessairement initialiser la communication. Pour cela, il existe deux modes :

TTF (Tag Talks First) : dans ce mode, le tag annonce sa présence à son arrivée dans le champ d'un lecteur. Ce mode peut poser des conflits lorsque plusieurs tags annoncent leur présence simultanément.

RTF (Reader Talks First) : dans ce mode, le lecteur interroge constamment son environnement afin de détecter la présence de nouveaux arrivants. Une requête est propagée régulièrement et, lorsqu'un transpondeur entre dans le champ et est capable de répondre, il renvoie une réponse annonçant sa présence.

Bien évidemment, l'utilisation simultanée des deux modes impliquent des conflits importants. Pour ces raisons, il faut veiller à appliquer un mode unique dans des secteurs fermés employant la technologie RFID. Certains pays d'Extrême-Orient ont même complètement banni l'utilisation du mode TTF.

Toute communication RFID est basée sur des protocoles simples ou complexes. Les protocoles permettent, par exemple, d'inclure des mécanismes de gestion de collisions, de sécurisation, d'authentification, etc., en plus du simple mécanisme d'échange des données.

Normes OSI

Devant l'ampleur et l'essor de la technologie, il est devenu nécessaire de standardiser et normaliser la RFID. Des normes ont donc été rédigées dans ce but. ISO/IEC (ISO et International Electrotechnical Commission) ont donc établi la norme 18000 : RFID Air Interface Standards, dont la norme 18000-1 factorise tous les éléments communs à la technologie. Les normes 18000-2 à 18000-7 décrivent les standards pour chaque fréquence ou gamme de fréquence utilisée en RFID. Pour chacune de ces normes, il existe des spécifications propres aux algorithmes et méthodes de fonctionnement de la communication des fréquences concernées.

Le modèle OSI défini en RFID présente les couches suivantes :

Couche	Transpondeur	Station de base
7 : Application	Application	Application
2 : Liaison de données	Protocole de communication	Protocole de communication
1 : Physique	Antenne, partie analogique	Antenne, partie analogique
Medium	Air	Air

Le medium correspond au milieu de propagation de la communication, ici l'air.

Codage des signaux

Intérêts

Le codage des signaux est la première étape dans la préparation à la communication en RFID. Par symétrie, la phase de décodage des signaux est la dernière étape. Les algorithmes de codage et décodage des signaux sont, bien évidemment, symétriques.

L'intérêt du codage des signaux est de pouvoir convertir les données binaires en signaux radiofréquence et de faciliter le transfert de ces données d'un interlocuteur vers l'autre. Pour pouvoir transférer ces données, nous verrons, dans la partie suivante, qu'il est nécessaire de moduler les signaux. Le type de modulation varie en fonction du sens de communication et, pour ces raisons, le type de codage varie selon le sens de la communication également. Dans tous les cas, l'objectif reste de pouvoir simplifier ce transfert et faciliter la récupération des informations au niveau du destinataire.

Nous allons, cependant, étudier le codage des données en signaux de part et d'autre, selon le sens de la communication :

- liaison montante : de la station de base vers le transpondeur,
- liaison descendante : du transpondeur vers la station de base.

Liaison montante

Dans le cas d'une liaison montante, la station de base utilise des modulations classiques pour transférer les données au transpondeur. L'objectif est de pouvoir maintenir le signal de fréquence porteuse le plus longtemps possible.

On utilise volontiers des codages tels que NRZ (No Return to Zero) ou le Delay Mode (plus couramment appelé code de Miller) :

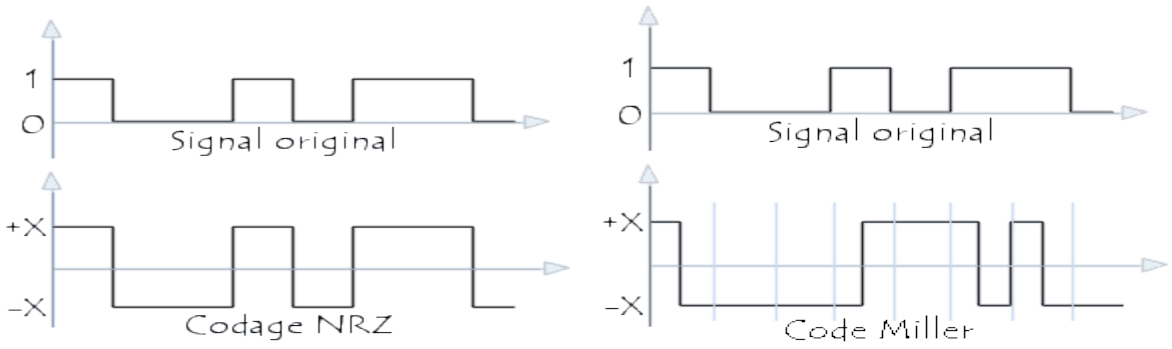


Figure II .12: Tag RFID passif

Le codage NRZ (ici bipolaire) définit des valeurs -X Volts pour la valeur binaire '0' et +X Volts pour la valeur binaire '1'. Il s'agit d'un code simple qui ne possède que deux états (0 et 1) et est donc facile à mettre en œuvre. La forme du signal fréquentiel obtenu est proche de celle du signal binaire de données.

Le code de Miller est différent dans le sens où il fait intervenir la notion des "transitions milieu de bit". En effet, nous faisons correspondre aux valeurs binaires des transitions montantes ou descendantes de signal qui sont effectuées en "milieu" de bit. Dans le cadre du Delay Mode, la valeur binaire '0' est représentée par "pas de transition" et la valeur binaire '1' par "une transition milieu de bit". En fonction de la valeur initiale, la transition peut être soit montante, soit descendante, de façon à inverser la polarité du signal.

Liaison descendante

Dans le cas d'une liaison descendante, l'approche est un peu différente. Dans de nombreux cas, plusieurs transpondeurs peuvent être susceptibles de dialoguer avec le lecteur. De plus, la distance d'un transpondeur à une station de base peut impliquer que la puissance des signaux RF de communication soit atténuée. L'objectif est donc de pouvoir identifier clairement les données de chaque transpondeur et de les différencier du bruit fréquentiel. On préfèrera donc utiliser un codage qui implique de nombreuses transitions, facilitant ainsi le repérage du signal.

Pour cette raison, les codages Manchester et Manchester différentiel sont tout désignés :

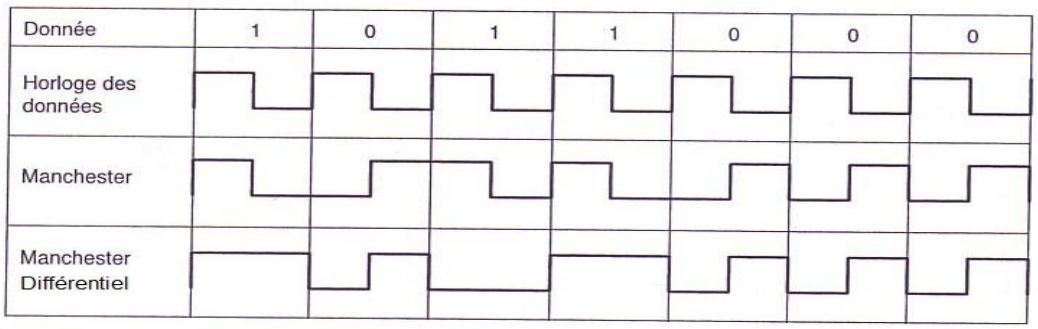


Figure II .13 : Tag RFID passif

Le codage Manchester n'utilise que la notion de "transitions milieu de bit" :

la valeur binaire '0' est représentée par une transition milieu de bit montante,

la valeur binaire '1' est représentée par une transition milieu de bit descendante.

Le codage Manchester différentiel, quant à lui, utilise la notion de "transitions milieu de bit", mais aussi celle de "transitions fin de bit". Une transition fin de bit est une transition qui survient à la "fin" du bit. En se référant au schéma, le codage est Manchester est décrit comme suit :

la valeur binaire '0' est représentée par une transition milieu de bit montante,

la valeur binaire '1' est représentée par une transition fin de bit.

Intéressons-nous maintenant plus particulièrement au code Manchester. Nous constatons qu'il existe plus de deux états possibles : transition milieu de bit descendante, transition milieu de bit montante, '0' sur la durée d'un bit, '1' sur la durée d'un bit. Seuls les deux premiers états énumérés ici correspondent à des valeurs, comme nous l'avons décrit. Cela signifie que si la station de base reçoit un message avec des états non définis, elle sera en mesure de conclure que des erreurs se sont produites. Cette particularité est essentielle dans la gestion de collisions.

Modulations

La modulation des signaux est la seconde étape dans la préparation à la communication en RFID. Par symétrie, la phase de modulation implique une phase de démodulation des signaux à la réception de signaux RF de réponse. Les méthodes de modulation et démodulation des signaux sont, bien évidemment, symétriques.

L'intérêt de la modulation est de pouvoir transmettre le signal fréquentiel de données. Pour cela, nos outils de codage des signaux ont permis de convertir les données binaires à transmettre en signaux fréquentiels que nous appellerons des messages. Pour que la station de base puisse transmettre un message à un transpondeur, elle doit d'abord le moduler avec une porteuse. La porteuse est un signal de haute fréquence que nous allons moduler selon des techniques différentes, mais qui conduiront au final à la transmission du message.

En RFID, les dispositifs qui communiquent ne sont pas technologiquement conçus de la même façon. Pour cette raison, des types de modulation différents sont utilisés selon le sens de la communication :

- liaison montante : de la station de base vers le transpondeur,
- liaison descendante : du transpondeur vers la station de base.

C'est pour cette raison que différents types de codage sont utilisés selon le sens de la communication.

Liaison montante

Les modulations les plus couramment utilisées sont :

ASK (Amplitude Shift Keying) : modulation d'amplitude. Dans ce type de modulation, la porteuse est modulée en amplitude, c'est-à-dire que des variations d'amplitude de ce signal permettent de traduire le message à transmettre,

FSK (Fréquency Shift Keying) : modulation de fréquence. Dans ce type de modulation, la porteuse est modulée en fréquence, c'est-à-dire que des variations de fréquence de ce signal permettent de traduire le message à transmettre.

Dans le cas d'une liaison montante, la station de base utilise ces types de modulations pour transmettre les messages aux transpondeurs :

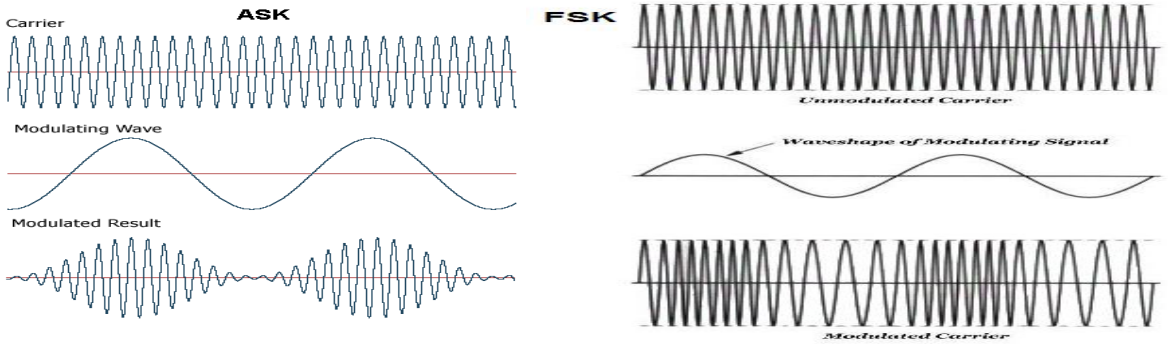


Figure II .14 : Tag RFID passif

"carrier" est la porteuse,"modulatingwave", ou "modulating signal", est le signal modulant, c'est-à-dire le message à transmettre,"modulatedresult", ou "modulated carrier", correspond à la porteuse modulée par le message.

Liaison descendante

Contrairement à ce qu'on pourrait initialement penser, le transpondeur ne peut pas se comporter comme un émetteur de signaux RF. En effet, il ne dispose pas, dans son interface RF, des mécanismes permettant d'émettre un signal radio-fréquence vers la station de base. Les transpondeurs utilisent ce qu'on appelle la réflexion d'ondes pour se faire comprendre des lecteurs. Pour cela, les tags utilisent une modulation différente que l'on nomme modulation de charge (Load Modulation) qui consiste à faire varier la charge résistive du circuit. Effectivement, en faisant varier la charge, le tag fait varier l'intensité du courant dans son circuit et donc l'intensité qui circule dans l'antenne. La consommation d'énergie qu'il représente dans le champ magnétique s'en trouve alors également modifiée et, par couplage magnétique, cela influe sur l'intensité du courant dans l'antenne de la station de base. De proche en proche, les signaux RF reçus de la station de base, qui sont réfléchis par le

transpondeur, permettent donc de transporter des réponses en faisant varier l'intensité du circuit du lecteur.

Il s'agit ici d'un procédé assez complexe mais qui repose à la base sur de la modulation. Cette modulation de charge résistive à l'origine de la transmission de la réponse s'appuie sur une modulation courante appelée OOK (On Off Keying) et correspond à de la modulation d'amplitude "tout ou rien". La modulation OOK agit un peu comme un interrupteur : la valeur binaire '0' correspond à 0V (on ne laisse passer aucun signal), la valeur binaire '1' permet de laisser passer le signal tel quel.

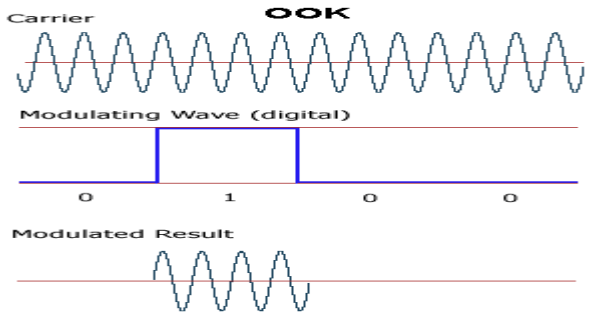


Figure II .15 : Tag RFID passif

A l'aide d'une modulation de type OOK, comme présentée précédemment, on crée une modulation de charge qui fait varier la charge résistive du circuit et donc la tension aux bornes du circuit RF du transpondeur :

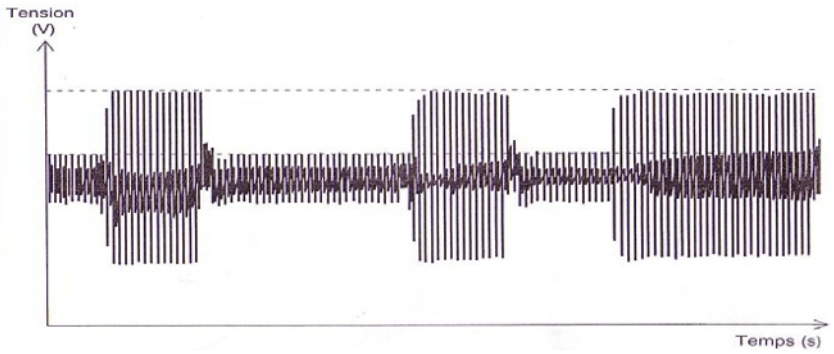


Figure II .16 modulation de type OOK

Gestion de collisions - Introduction

Lorsqu'une station de base communique avec plusieurs transpondeurs présents dans son champ magnétique, les messages émis par chacun des tags sont susceptibles de se heurter. La superposition de signaux fréquentiels revient à sommer ces signaux en amplitude. Vous

comprendrez logiquement que le mélange des signaux provoquent des conflits et rend la distinction de chaque message difficile pour la station de base. C'est ce que l'on appelle des collisions.

Pour pallier ce problème, de nombreux dispositifs intègrent des outils qui permettent de gérer les collisions. En effet, comme nous l'avons mentionné précédemment, les stations de base possèdent des circuits de gestion de la communication. Elles peuvent notamment intégrer des algorithmes anticollisions.

Causes des collisions

Plusieurs phénomènes ou cas de figure sont à l'origine des collisions fréquentielles en RFID parmi lesquelles les plus courantes sont :

le "tag stack" : en français, cela signifie la "pile de tags". Dans ce cas de figure, plusieurs tags sont empilés les uns sur les autres ou, tout du moins, suffisamment proches les uns des autres. Lorsque la station de base communique avec l'un des transpondeurs, elle est susceptible de fournir de l'énergie à tous les transpondeurs par téléalimentation et d'entrer en communication avec eux. Cela pose évidemment des problèmes d'interférences. Par exemple : les forfaits de ski sont équipés de la technologie RFID et l'on vous conseille généralement de placer ce pass isolément dans une poche, ceci afin d'éviter qu'il se dé-magnétise. Les trois cas classiques de tag stack sont : un porte-feuille contenant plusieurs cartes à puce sans contact, les piles de lettres recommandées équipées de tags et les piles de jetons de casino intégrant des tags (cela existe pour certains jeux).

les "weak collisions" : elles désignent les collisions de faibles signaux. Ce cas de figure survient notamment lorsque plusieurs transpondeurs sont placés de façon éloignée dans un champ magnétique assez vaste. Les signaux fréquentiels réfléchis vers la station sont atténués par la distance et la collision des messages est donc plus difficile à identifier. De plus, si les signaux sont trop faibles, ils sont plus difficiles à distinguer du bruit fréquentiel.

l'absorption magnétique : ce phénomène se caractérise par la situation "un transpondeur peut en cacher un autre". Supposons qu'un transpondeur relativement proche de la station de base soit placé entre cette station et un tag beaucoup plus éloigné. Alors, les signaux du transpondeur le plus éloigné, faibles devant ceux du transpondeur le plus proche, seront "absorbés" par ceux du tag placé sur son chemin. Cette absorption est susceptible de générer des collisions.

Exemples de collisions Voici deux exemples de collisions :

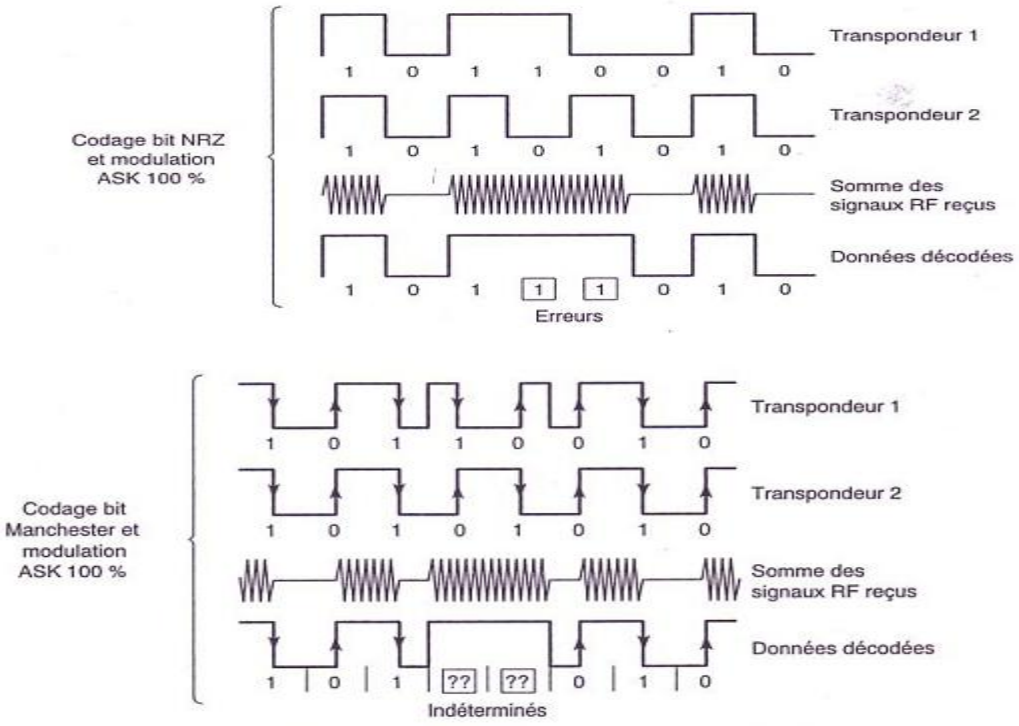


Figure II .17 : Exemples de collisions

Dans le cas du premier exemple, le codage des données en signal fréquentiel utilisé est le codage NRZ et la modulation utilisée pour transmettre le message est une modulation d'amplitude (ASK). Les transpondeurs 1 et 2 diffusent leurs messages respectifs à la station de base. Les signaux fréquentiels sont alors superposés et la station de base reçoit et décode ce message. Par collision, les données reçues ne correspondent ni à celles provenant du transpondeur 1, ni à celles provenant du transpondeur 2. On conclut donc à des erreurs.

Dans le cas du second exemple, le codage des données en signal fréquentiel utilisé est le code Manchester et la modulation utilisée pour transmettre le message est une modulation d'amplitude (ASK). Les transpondeurs 1 et 2 diffusent leurs messages respectifs à la station de base. Les signaux fréquentiels sont alors superposés et la station de base reçoit et décode ce message. Par collision, les données reçues ne correspondent à aucun des deux messages initiaux. De plus, au niveau de la collision, la superposition des informations ne constitue pas des transitions milieu de bit. Le format des données obtenues au niveau de la collision ne correspond donc pas à un message codé en Manchester. On conclut donc à des états indéterminés.

Ce dernier exemple soulève donc un point important. En effet, dans les deux cas de collision, les données récupérées ne correspondent à aucun des deux messages que la station de base attendait. Néanmoins, dans le premier cas, les états obtenus par collision sont des états cohérents ('0' ou '1'). Dans le second cas, la collision génère des états qui ne sont pas définis dans le code Manchester (pas de transition milieu de bit). C'est là un point intéressant que nous avions déjà évoqué dans l'étude des codages utilisés. Nous constatons que le code Manchester possède cet avantage de pouvoir distinguer plus facilement les collisions, grâce à la présence d'états indéterminés. C'est une des raisons pour lesquelles, le code couramment utilisé dans les liaisons descendantes est le code Manchester. Cela est d'autant plus important que, de par cette particularité, il est possible d'effectuer des corrections bit à bit en code Manchester. Il existe pour cela des algorithmes qui sont utilisés par les algorithmes anticollisions.

Méthodes de gestion des collisions

Pour pallier les problèmes de collisions, il existe différents types d'algorithmes. Ces algorithmes s’appuient sur des techniques de gestion de collisions variées :

fréquentielle : la plage fréquentielle utilisée par le dispositif RFID est divisée en plusieurs canaux fréquentiels. Chaque canal de bande passante est alors alloué à un transpondeur spécifique et sera utilisé par la station de base pour communiquer avec ce tag uniquement,

spatiale : la station de base analyse l'espace de son champ magnétique par petites parcelles. Cela diminue considérablement la probabilité de détecter plusieurs transpondeurs simultanément car l'espace "scanné" est très réduit. Cette technique permet donc d'identifier chaque transpondeur isolément, en réduisant les possibilités de collisions.

temporelle : de la même manière que pour la gestion fréquentielle, cette technique permet de mettre en place une gestion temporelle des communications. Des slots de temps d'une certaine durée sont établis et utilisés périodiquement. Chaque slot est alors dédié à la communication avec un transpondeur particulier.

Les méthodes utilisées pour gérer les collisions en RFID reposent sur deux types d'algorithmes :

les algorithmes déterministes : dont le but est d'identifier chaque transpondeur par son UID (Unique IDentifier) de façon certaine et le plus rapidement possible. Cette méthode peut

s'avérer longue mais est complètement déterminée. Les temps pour sélectionner les transpondeurs sont calculables et nous sommes certains, au final, d'identifier tous les transpondeurs de proche en proche. Ceci afin de pouvoir établir des dialogues individuels et donc limiter les risques de collisions.

Les algorithmes probabilistes : qui sont plus efficaces que leurs prédécesseurs lorsque le codage bit et les effets de masquage provoquent des collisions niveau bit plus difficiles à détecter. Ils sont utiles contre les pollutions radiofréquence. Cependant, tout n'est pas déterminable et calculable avec ces méthodes probabilistes. Les algorithmes fonctionnent de proche en proche.

Nous nous proposons donc d'analyser un type d'algorithme déterministe et un type d'algorithme probabiliste.

Algorithmes déterministes

Préliminaires

La première phase dans le déroulement de l'exemple d'algorithme déterministe que je vais présenter consiste à détecter si des transpondeurs sont présents dans le champ magnétique de la station de base. Pour cela, le lecteur constitue une requête générale d'1octet qui permettra aux transpondeurs aptes à répondre de le faire. La requête est propagée dans le champ et tous les transpondeurs pouvant l'interpréter constituent une réponse adéquate. Cette réponse est un acquittement générique de 2octets qui a le même format quel que soit le transpondeur. Chaque transpondeur identifié renvoie donc cet acquittement, signifiant ainsi sa présence.

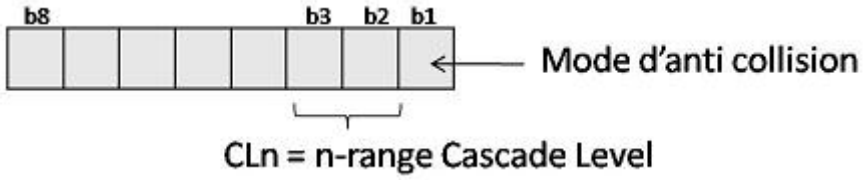
NB : les acquittements étant tous identiques, la superposition des réponses ne pose aucun soucis. Le but de cette manoeuvre pour la station de base est simplement d'identifier qu'au moins un tag est présent dans son champ.

La station de base ayant détecté des transpondeurs, elle constitue alors une "trame de commande anticollision", dont le format est le suivant :

SEL	NVB	Données UID CLn
8 bits	8 bits	0 à 40 bits

- Octet SEL

Le premier octet de cette trame (premier 8bits) est l'octet de sélection SEL. Il représente la commande de sélection pour interroger les UID de chaque transpondeur. L'octet SEL est composé de la manière suivante :



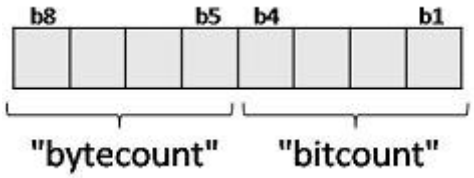
Le CLn signifie "Niveau de Cascade de rang n". Le Cascade Level est utile pour spécifier la taille des UID des transpondeurs. En effet, il existe des UID de tailles différentes :

- CL1 : UID sur 32 bits = 4 octets,
- CL2 : UID sur 56 bits = 7 octets,
- CL3 : UID sur 80 bits = 10 octets.

Les 2ème et 3ème bits de poids faible (b2 et b3) permettent de spécifier le Cascade Level correspondant au format des UID. Cette valeur est modifiée durant l'algorithme. Le bit de poids le plus faible (b1), quant à lui, spécifie le mode d'anticollision utilisé : si la valeur est '0', la gestion anticollision est orientée octet par octet, si la valeur est '1', la gestion anticollision est orientée bit par bit. Le plus généralement, la gestion anticollision est orientée bit par bit.

- Octet NVB

Le second octet, NVB (Number of Valid Bits), correspond au nombre de bits valides. Il définit combien d'octets sont utiles dans la transmission et combien de bits de l'UID des transpondeurs doivent être considérés comme valides et pris en compte pour la suite de l'algorithme. L'octet NVB est composé de la façon suivante :



Les quatre bits de poids fort (b5 à b8) consituent le "bytecount", c'est-à-dire le nombre d'octets transmis par la station de base. Le bytecount est au moins égal à 2 : octet SEL + octet NVB au minimum. Il varie ensuite en fonction du nombre d'octets de données qui complètent la trame.

Les quatres bits de poids faible (b1 à b4) représentent le "bitcount", c'est-à-dire le nombre de bits de données additionnels.

Nous nous intéresserons surtout au bytecount.

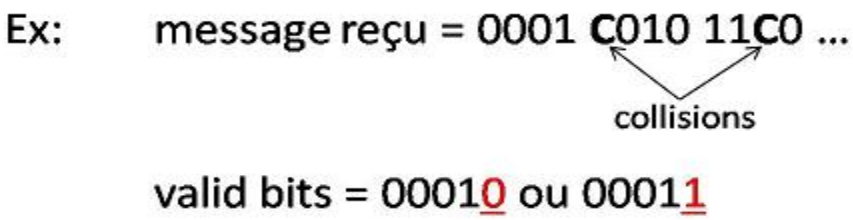
- Données

Enfin, la trame peut être complétée avec 40 octets de données. Cela sera utile durant la procédure de l'algorithme que nous allons détailler.

Procédure de l'algorithme

La station de base a initialement assigné le CLn à la commande de sélection SEL. Puis, elle a transmis la première trame, constituée uniquement des octets SEL et NVB, afin d'identifier tous les transpondeurs par leurs UID. Les transpondeurs répondent donc à la trame en fournissant leurs UID respectifs. A ce niveau de l'algorithme, s'il y a des réponses simultanées et synchrones des transpondeurs, on est capable d'utiliser la correction bit à bit du code Manchester, mentionnée précédemment, pour résoudre les collisions bit à bit simples.

Voici un exemple simple de message reçu suite aux réponses de la part des transpondeurs :



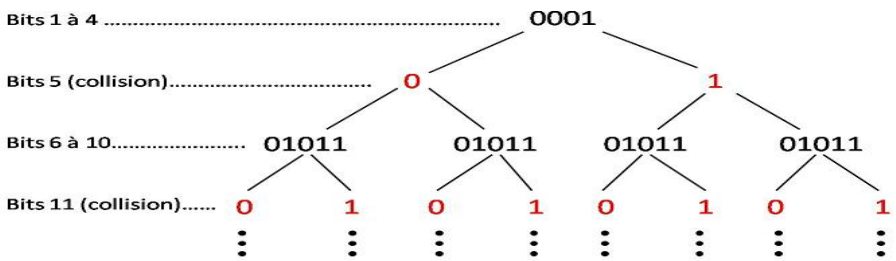
Dans le message reçu, nous constatons qu'une première collision a eu lieu au niveau du 5ème bit. Nous allons donc commencer par traiter cette collision. Seuls les 4 premiers bits sont valides. Pour résoudre le problème, nous choisissons indépendamment de compléter ces 4 bits valides par un '0' ou par un '1'. En vérité, il est nécessaire d'étudier les deux cas pour poursuivre l'algorithme.

Considérons, dans un premier temps, que nous complétons les bits valides par un '0'. Nous obtenons alors la suite de bits valides : 00010. Le nombre de bits valides est donc placés à 5 dans la commande NVB. La station de base constitue alors une nouvelle trame composée de l'octet SEL et du nouvel octet NVB, puis elle complète cette trame en fournissant en données la suite des 5 bits valides.

Seuls les transpondeurs dont les UID commencent par la suite de bits valides, ici 00010, sont alors invités à re-communiquer leurs UID personnels. La collision au 5ème bit a donc été éliminée. Si une autre collision survient plus loin dans le message, alors la même méthode est appliquée, jusqu'à ce que chaque UID complet soit déterminé.

Nous avions, au préalable, choisi délibérément de compléter les bits valides avec un '0'. Nous effectuons donc, maintenant, la même opération en complétant la suite de bits valides avec un '1'. La suite de bits valides est alors : 00011. Puis chacune des étapes énoncées précédemment est accomplie.

Comme vous l'aurez compris, nous balayons donc, de proche en proche, toutes les solutions possibles d'UID, en éliminant une à une les collisions générées par la superposition des messages des transpondeurs. De cette manière, les UID de tous les transpondeurs sont déterminés comme par un parcours d'arbre :



Une fois que chaque transpondeur a été identifié par son UID unique, la station de base est en mesure de communiquer avec ce tag en utilisant son identifiant unique. De cette manière, les problèmes de collisions sont résolus.

Intérêts

Les algorithmes déterministes sont efficaces car :

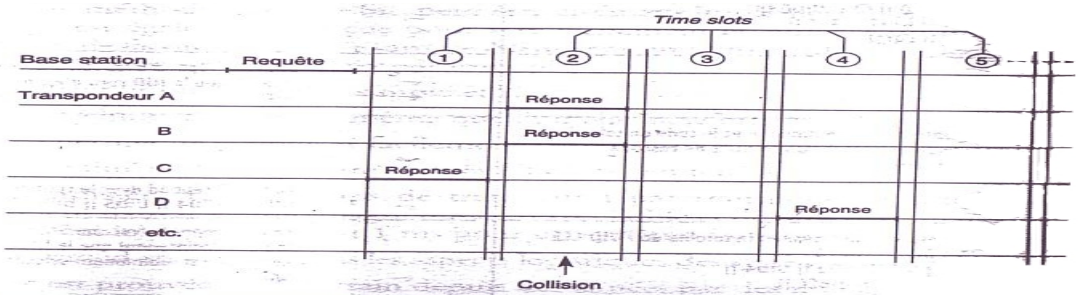
- Le temps maximum de calcul est défini et invariable,
- La vitesse est optimisée : détection d'erreurs pendant la phase d'anticollision,
- La méthode bit à bit est facilement implémentable en logique câblée et peut être étendue à la méthode octet par octet,
- Il s'agit de méthodes prouvées sur le terrain depuis des années. La méthode ci-présentée a été retenue pour la normalisation des cartes à puces sans contact de proximité.

Algorithmes probabilistes

Il existe de nombreux algorithmes probabilistes. On présentera ici la méthode temporelle mentionnée dans l'introduction à la gestion de collisions, appelée "méthode des time slots" ou "méthode des créneaux de temps".

Cette méthode consiste à partager le temps périodiquement. La période choisie doit définir des slots (créneaux temporels) pendant lesquels la station de base pourra dialoguer avec les transpondeurs. Chaque transpondeur se voit donc attribuer un canal temporel spécifique durant lequel il sera autorisé à communiquer avec la station de base.

Voici une représentation du partage temporel de la méthode des time slots :



Procédure de l'algorithme

La première étape consiste, pour la station de base, à définir et annoncer la "hashValue" à tous les transpondeurs. La hashValue est la valeur qui correspond au nombre de créneaux de temps alloués pour le dialogue.

Chaque transpondeur est alors invité à choisir arbitrairement un slot pendant lequel il pourra dialoguer avec le lecteur. Le transpondeur peut soit déterminer une valeur aléatoire dans l'intervalle [1; hashValue] pour choisir un créneau, soit déterminer son créneau en effectuant un calcul à l'aide de la hashValue et son UID (ou une partie de l'UID). Cette dernière méthode peut garantir un meilleur résultat du fait de l'unicité de l'UID. Lorsque chaque transpondeur a déterminé son time slot, il y transmet sa réponse à la station de base.

Pour chaque time slot alloué, deux cas de figure sont envisageables pour la station de base :

- Si le message reçu est bien interprété, alors il n'y a pas eu de collision. Cela signifie qu'un seul transpondeur a désigné ce créneau de temps. Dans ce cas, le lecteur fournit une commande de "Quit" au transpondeur pour lui indiquer que ce créneau lui est désormais dédié et que leurs échanges s'effectueront dans ce time slot périodique.

- Si le message reçu est incohérent, alors une collision est survenue. Cela signifie qu'au moins deux transpondeurs ont choisi ce créneau de temps. La station de base relance alors la procédure initiale pour les transpondeurs partageant le même créneau de temps.

Lorsque chaque transpondeur s'est vu attribuer un créneau de temps individuel, la station de base peut donc établir des communications uniques avec chaque tag de son champ.

Approche problématique

S'il y a plus de transpondeurs que de créneaux de temps alloués par la station de base, alors trop peu de créneaux sont définis, et certains time slots provoqueront constamment des collisions. A l'inverse, nous pouvons imaginer que si trop de créneaux sont alloués, alors un gain de temps plus ou moins important sera perdu, puisqu'il existera des slots durant lesquels aucune communication ne sera échangée.

C'est en cela que ce type d'algorithme est probabiliste. La station de base doit estimer le nombre de transpondeurs susceptibles d'être présents dans le champ magnétique et cela est problématique. En fait, la valeur de la hashValue doit, ici, dépendre du type d'application de la RFID. De nombreuses simulations ont été effectuées et démontrent que la solution optimale consiste à cibler le double du nombre de transpondeurs espérés.

Avantages

Les algorithmes probabilistes sont efficaces car :

- Des communications individuelles sont établies avec chaque transpondeur,
- Le nombre d'échanges est minimalisé, par conséquent les perturbations radioélectriques sont réduites,
- Les risques de collision sont éliminés.

Cependant, les algorithmes déterministes restent plus rapides que les algorithmes probabilistes.

II.5 Quelques exemples d'application par fréquences

<135 kHz : Tri des déchets,Identification animale (134,2 kHz),Système d'alarme, surveillance des arbres de Paris,...

13,56 MHz : Cartes à puce sans contact, cartes de transport,…Réservation de billets d'avion, manutention des bagages,Forfait de station de ski,…

443 et 900MHz : Traçage de palettes, de conteneurs,Télécommandes d'ouverture centralisée…

2,45 et 5,8 GHz :Télépéage ,Délivrance automatique du carburant dans les stations-service.

II.6 Conclusion :

La RFID (Radio Frequency IDentification) est une technologie qui permet de communiquer par ondes radio-fréquences. Il existe, de nos jours, plusieurs gammes de fréquences autorisées, selon les régions mondiales, pour établir des communications RFID. Il s'agit d'une technologie largement déployée à notre époque et qui ne cesse de croître dans de multiples domaines. Le principal objectif de la RFID est d'assurer l'identification, la traçabilité, la sécurisation dans des activités variées.

CHAPITRE III

Réalisation d’un système de contrôle d’accès RFID et d’alerte

CHAPITRE 3

Dans ce chapitre nous allons présenter les résultats des montages et tests effectuées pour le contrôle d'accès. Pour cela, nous allons utiliser l'identification RFID avec la carte UNO en 7 étapes et ce en introduisant progressivement des composants à chaque étape afin d'aboutir à la fin à une application générale de contrôle d'accès avec alerte GPS :

Etape 1 : Principes de base de la RFID et interface de module RFID
Etape 2 : Serrure de porte basée sur RFID et clavier
Etape 3 : Système de verrouillage de porte et d'alerte basé sur RFID, clavier et module GSM
Etape 4 :Système de contrôle d'accès basé sur RFID
Etape 5 :Système de contrôle d'accès et d'alerte basé sur la RFID et module GSM
Etape 6 :Système de contrôle d'accès basé sur RFID et clavier
Etape 7 :Système de contrôle d'accès et d'alerte basé sur le clavier et RFID et module GSM

III.1. Principes de base de la RFID et interface de module RFID avec Arduino

Dans cette étape,nousallons réaliser un montage qui permet de lire l'identificateur UID des tagsmodule RFID MFRC522. Ensuite, nous allons réaliserun autre montage qui constitue un verrou de porte sécurisé RFID.

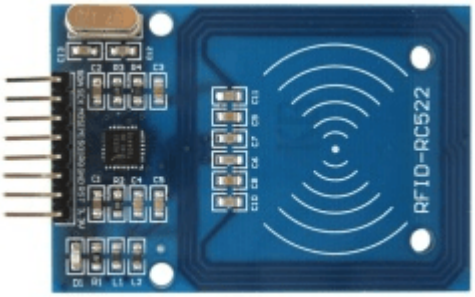
RFID signifie identification par radiofréquence et utilise essentiellement les ondes radio pour lire les informations sur l'étiquette. Les étiquettes RFID contiennent l'émetteur et le récepteur intégrés attachés à un objet. La RFID est rapide et ne nécessite aucun contact entre le lecteur et l'étiquette et peut être lue à distance. Le système RFID MFRC522 que nous allons utiliser comprend deux parties: Tag et Reader. L'Étiquette (tag) qui est passive contient une puce pour stocker des informations sur un objet physique et une antenne pour recevoir et transmettre un signal. Elle peut généralement stocker 1 Ko de données, mais cela suffit pour stocker le nom, le numéro de carte de crédit, le numéro d'identification unique, la date de naissance et d'autres informations.

Une étiquette passive n'a pas de pile et utilise l'énergie transmise par le lecteur.

Une étiquette active contient une batterie intégrée qui lui permet d’envoyer un signal plus puissant et la portée augmente à 100 pieds. Les autres fonctionnalités sont les mêmes que les balises passives.

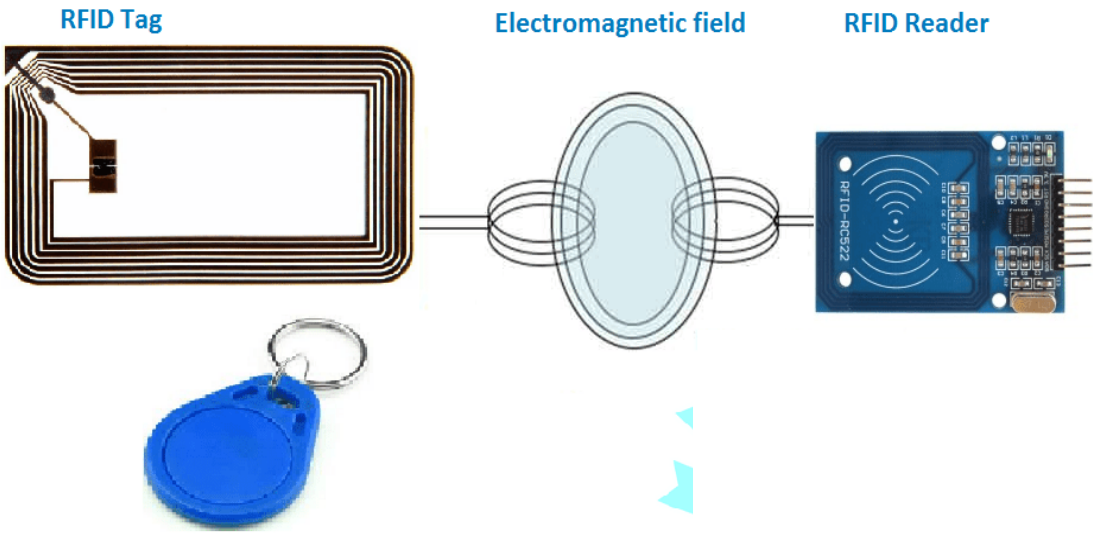
Lecteur RFID

Le lecteur RFID remplit deux fonctions: transmettre et recevoir d’un émetteur-récepteur. Le lecteur RFID contient une antenne, un module radiofréquence et une unité de contrôle.



Comment fonctionne la RFID

Le lecteur RFID génère un champ électromagnétique à haute fréquence et lorsque l'étiquette s'en approche, une tension est induite dans la bobine d'antenne de l'étiquette en raison de l'induction. Cette tension induite agit en tant que puissance pour le tag. L'étiquette en retour convertit le signal en puissance et répond au lecteur.

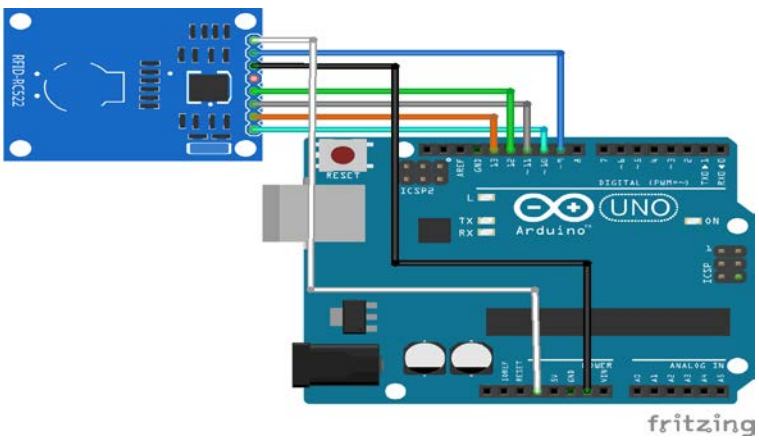


Interfaçage du module RFID avec la carte ArduinoUno

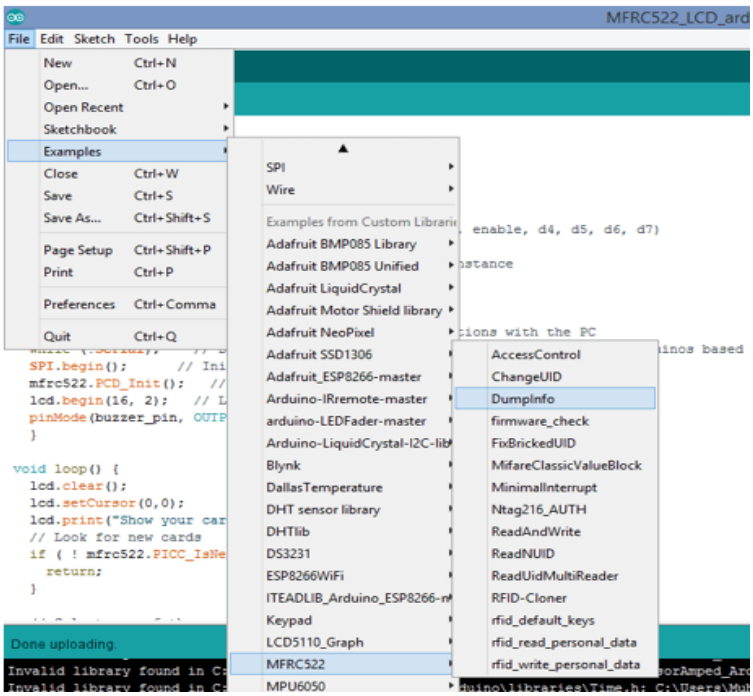
Le lecteur RFID que nous allons utiliser est un module de lecture MFRC522 qui communique avec l'Arduino via le protocole SPI. Il fonctionne à la fréquence 13,56 MHz. Les tags sont basés sur le protocole MIFARE et disposent de 1 Ko de mémoire. Ils ont également une puce qui peut effectuer des opérations arithmétiques. Pour l'interfaçage RFID avec la carte Arduino, nous avons besoin des pièces suivantes :

- ArduinoUno
- Module RFID du MFRC522
- Écran LCD I2C,trois LED (vert, rouge, bleu)
- servomoteur Sg90, 3 résistances de 220 ohms
- Avertisseur sonore

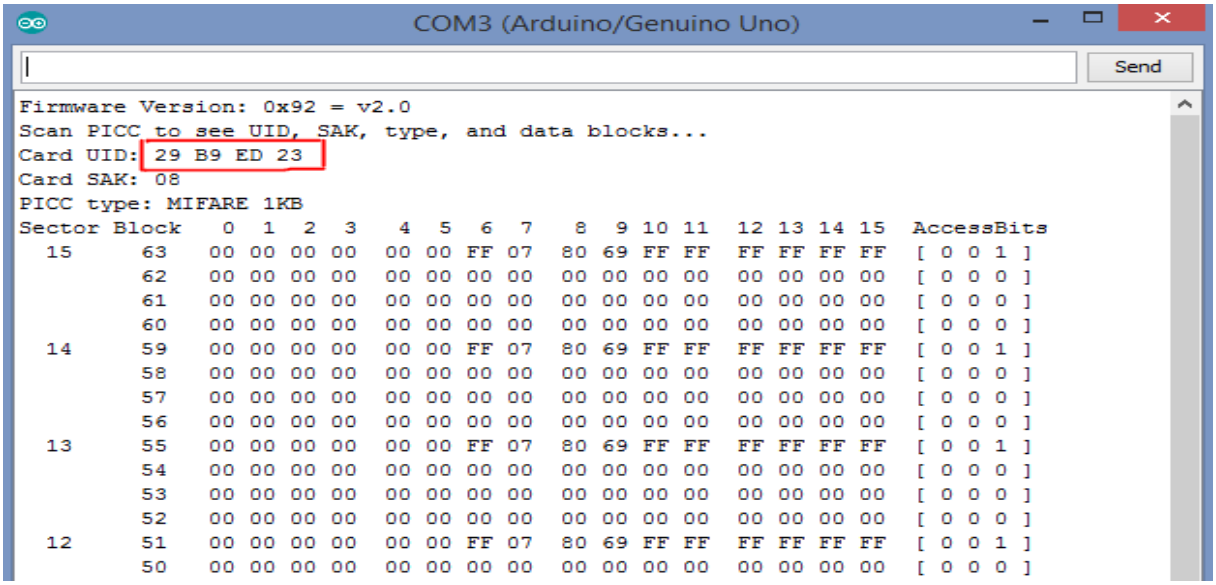
Nous réalisons le câblage du schéma suivant :



Après cela, en ouvrant dans le menu fichier → exemples → MFRC522→Dumpinfo» à partir d'exemples de l'IDE Arduino comme indiqué dans la figure ci-dessous.



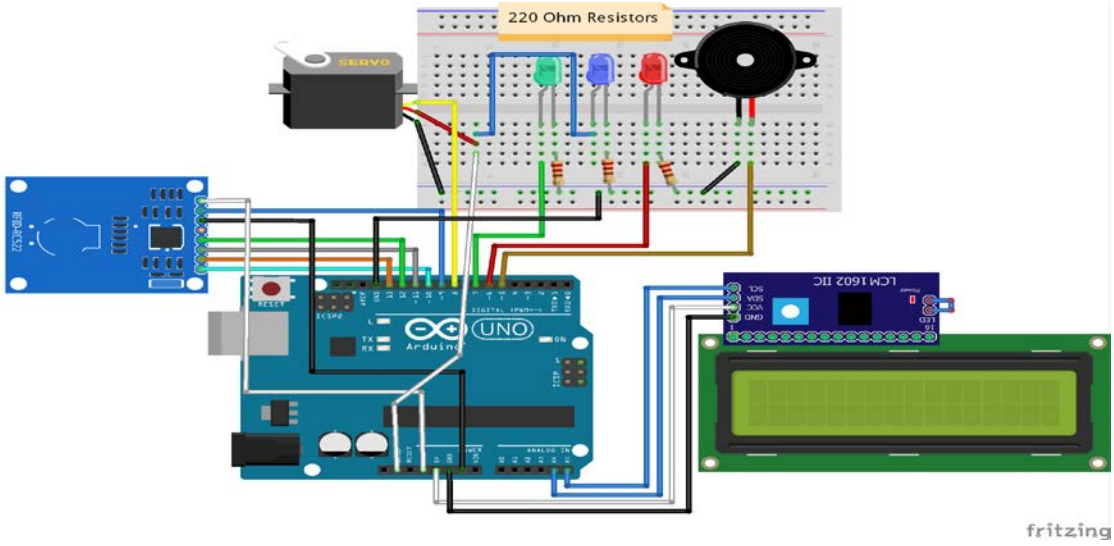
En ouvrant le moniteur série de l'IDE et en amenant la carte RFID devant le lecteur, elle nous montrera les informations de l'étiquette RFID. On enregistre le numéro UID, qu'on va utiliser dans le deuxième montage.



Dans l'image ci-dessus, vous pouvez voir le numéro UID de la balise, ainsi que les 1 Ko de mémoire répartis en 16 secteurs. Chaque secteur a 4 blocs et chaque bloc peut stocker 4 octets.

Nous allons créer un verrou de porte sécurisé par RFID qui ouvrira la porte au balayage de la bonne étiquette et interdira l'accès au balayage de la mauvaise étiquette. En reprenant le montage précédent, on lui ajoutant l'écran LCD I2C , un avertisseur et servomoteur..

Le schéma de circuit complet est comme suit :



la mise sous tension la led bleue et le lcd s'allume. Le servomoteur se met en position fermée. Si on balaie le lecteur par un tag autorisé la led verte s'allume le servomoteur tourne un quart de tour pour ouvrir la serrure, temporise un instant, puis se ferme et la led verte s'éteint.Si on balaie le lecteur par un tag non autorisé la led rouge s'allume et l'avertisseur klaxonne.

III.2 Serrure de porte basée sur RFID et clavier

Dans cette étape nous allons réaliser un verrou de porte basé sur RFID et clavier. Pour ouvrir la porte, l'utilisateur devra d'abord présenter la bonne étiquette autorisée, puis saisir le mot de passe correct. En scannant la mauvaise étiquette ou en entrant le mauvais mot de passe, le système refusera l'accès.

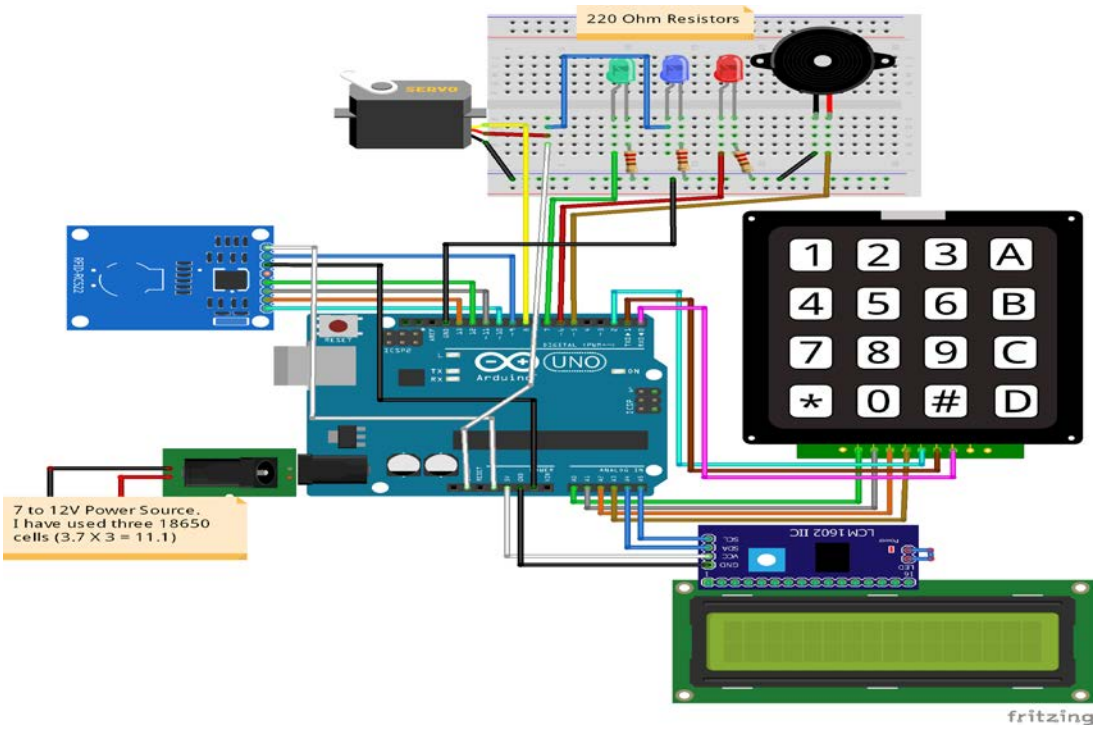
Composants requis pour la serrure de porte basée sur RFID et clavier :

- ArduinoUno
- LCD I2C
- Lecteur RFID MFRC522
- Moteur servo SG90 Clavier 4X4 ou Clavier 4X3, 3 X LED (rouge, vert, bleu) 3 résistances de 220 ohms

- Avertisseur sonore
- Alimentation 6 à 12, 2A

Nous allons ensuite connecter le clavier à la carte Arduino. Le clavier 4X3 a 8 connexions, mais nous n'avons pas besoin de la dernière colonne du clavier. Nous avons seulement besoin de chiffres pour le mot de passe. Nous n'utilisons donc pas la dernière broche du clavier, qui correspond à la quatrième colonne.

Le schéma est donc le suivant :



-

III.3 Système de verrouillage de porte et d'alerte basé sur RFID et clavier

Dans l'étape précédente nous avons réalisé le montage du système de verrouillage de porte basé sur un clavier dans lequel on devra d'abord présenter la bonne étiquette, puis saisir le mot de passe correct pour ouvrir le verrou de porte. Nous allons maintenant ajouter le module Sim900 dans ce système pour en faire un système de verrouillage de porte et d'alerte basé sur le RFID et le clavier.

Fonctionnement : En scannant la mauvaise étiquette ou en entrant le mauvais mot de passe, il nous enverra une alerte.

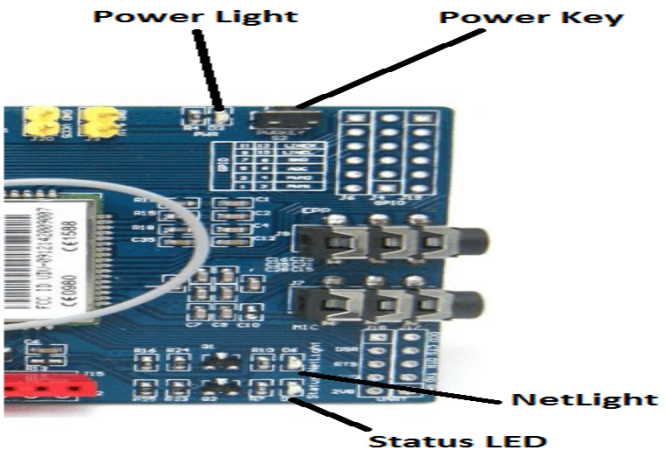
En scannant la bonne étiquette et en entrant le bon mot de passe, il nous enverra un message de confirmation de l'ouverture de la porte.

Vous pouvez arrêter le système en envoyant un message «fermer» à la carte Arduino. Ce dernier ne reviendra en mode normal que lorsque vous enverrez le message «ouvert» à la carte Arduino. Pendant le temps d’arrêt, il n’analysera aucun tag et ne recherchera que les messages. Nous pouvons également ouvrir la porte en envoyant un message à Arduino.

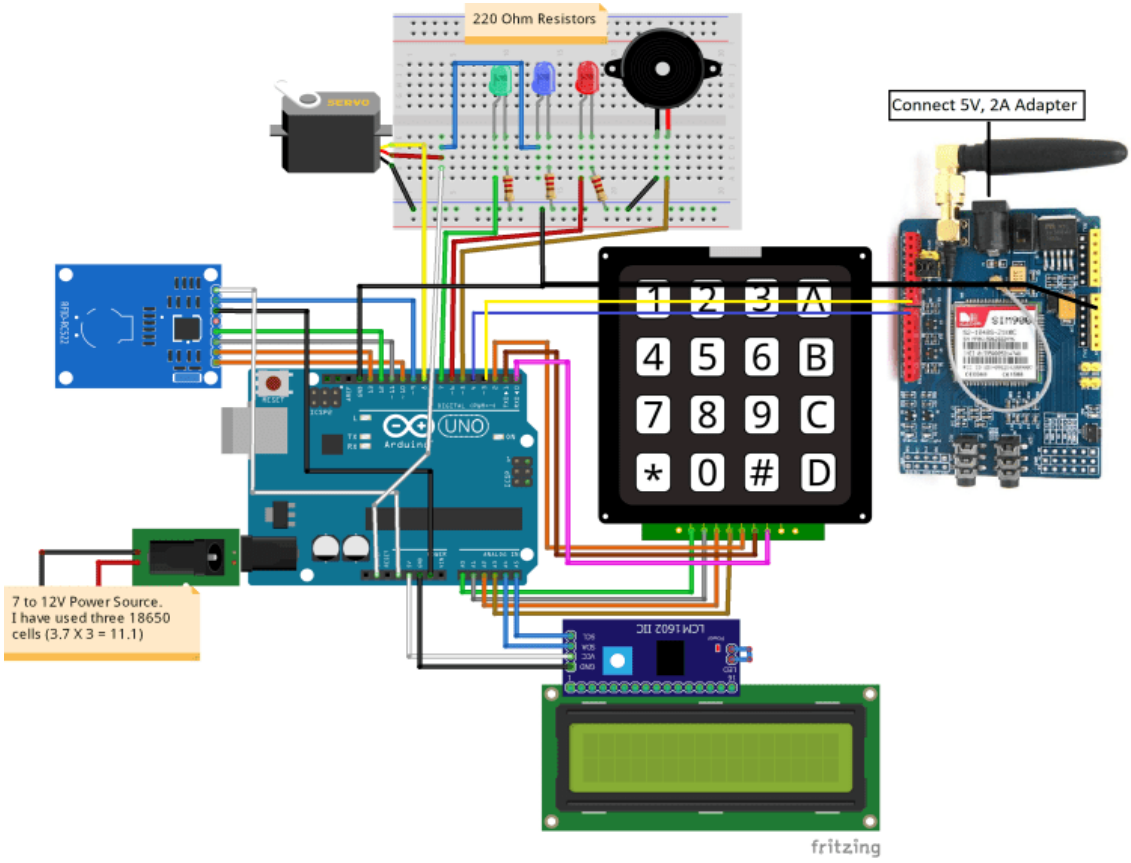
Composants requis

- ArduinoUno
- LCD I2C
- Lecteur RFID MFRC522
- Module GSM SIM900
- Adaptateur secteur 5V, 2A
- Moteur servo SG90
- Clavier 4X4 ou Clavier 4X3
- 3 X LED (rouge, vert, bleu)
- 3 résistances de 220 ohms
- Avertisseur sonore
- Alimentation 6 à 12V

Pour alimenter le module SIM900, l'alimentation recommandée est de 5V, 2A. Une fois le module SIM900 est mis sous tension, le voyant d'alimentation s'allume et, une fois qu’on ait appuyé sur la touche d'alimentation, le voyant d'état doit s'allumer et le voyant Netlight devrait commencer à clignoter. À ce stade, on appelle avec le téléphone portable la puce sim que nous avons placé dans le module SIM900. Si l'appel passe, notre sim fonctionne correctement avec le module SIM900.



Le schéma de circuit complet pour le système de verrouillage de porte et d'alerte basé sur RFID et clavier utilisant Arduino est le suivant:



III.4 Système de contrôle d'accès basé sur RFID utilisant Arduino

Dans l'étape précédente, nous avonsréalisé un système de verrouillage de porte et d'alerte utilisant l'Arduino basé sur le RFID et le clavier, dans lequel l'utilisateur devait présenter la bonne étiquette et saisir le bon mot de passe pour ouvrir le verrou de porte. Le système nous a également envoyé le message de confirmation. Dans cet article, nousallons réaliser un système de contrôle d'accès basé sur l'identification par radiofréquence utilisant Arduino. Le système n'autorise l'accès que sur l'analyse de la bonne étiquette et sur celle de la mauvaise, le système refuse l'accès et la sonnerie émet un bip. Il y aura une balise principale qui sera utilisée pour ajouter / supprimer d'autres balises. Les tags enregistrés resteront même après la mise hors tension du module. Le seul moyen de réinitialiser le système consiste à utiliser le bouton de nettoyage qui effacera toutes les données de la mémoire EEPROM. L'EEPROM a environ 100 000 cycles d'écriture limités.

Fonctionnement du système de contrôle d'accès basé sur RFID utilisant Arduino

Lors du démarrage du projet pour la première fois, il nous sera demandé de définir un tag maitre et le tag que nous souhaitons présenter sera notre tag maitre. La balise principale agira en tant que programmeur et on pourra l'utiliser pour ajouter ou supprimer d'autres balises.

Après avoir défini la balise principale, on devra ajouter d'autres balises qui seront autorisées à ouvrir la porte. Pour ce faire, on scanne l’étiquette principale et le système passera en mode programme.

En mode programme, l'analyse des balises ajoutera / supprimera celles-ci du système. On scanne les tags que nous souhaitons utiliser pour ouvrir la porte et le système stockera les UID de ces tags dans la mémoire EEPROM. On scanne à nouveau la balise pour la supprimer de la mémoire EEPROM. Pour quitter le mode programme, on scanne l’étiquette principale.

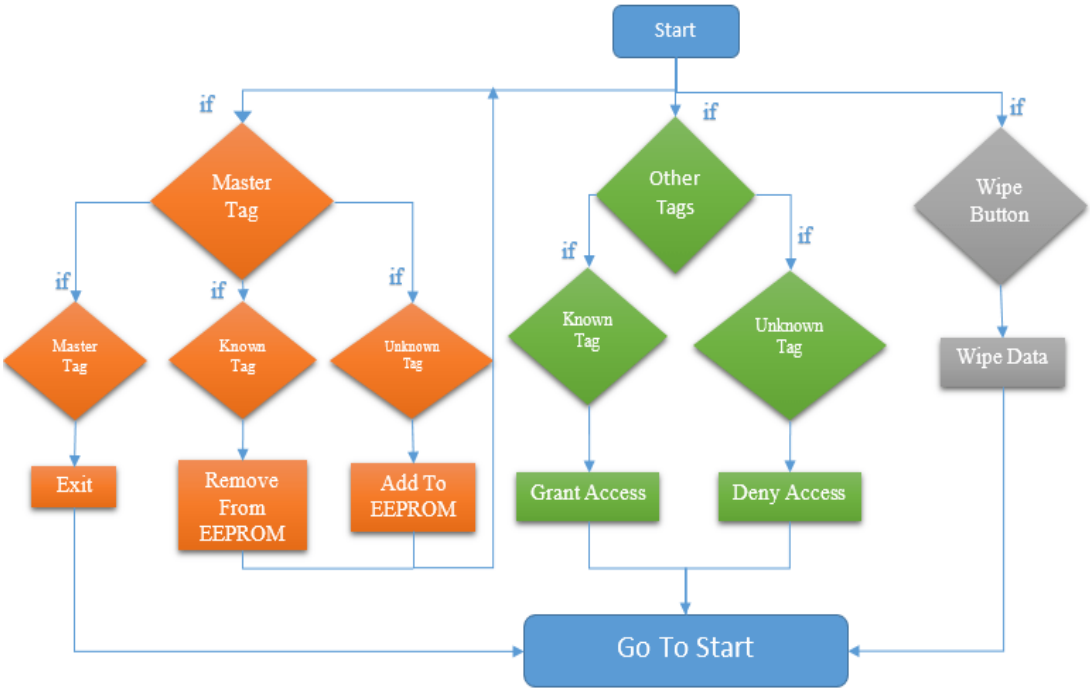
On analyse maintenant les étiquettes que nous avons ajoutées dans le système pour ouvrir la porte. Lorsqu’on scanne la mauvaise étiquette, la porte restera fermée.

Pour réinitialiser le système, on appuie sur le bouton de réinitialisation d’Arduino, puis on appuie longuement sur le bouton d’effacement pendant 10 secondes. Cela supprimera toutes les données de la mémoire EEPROM, y compris la balise principale.

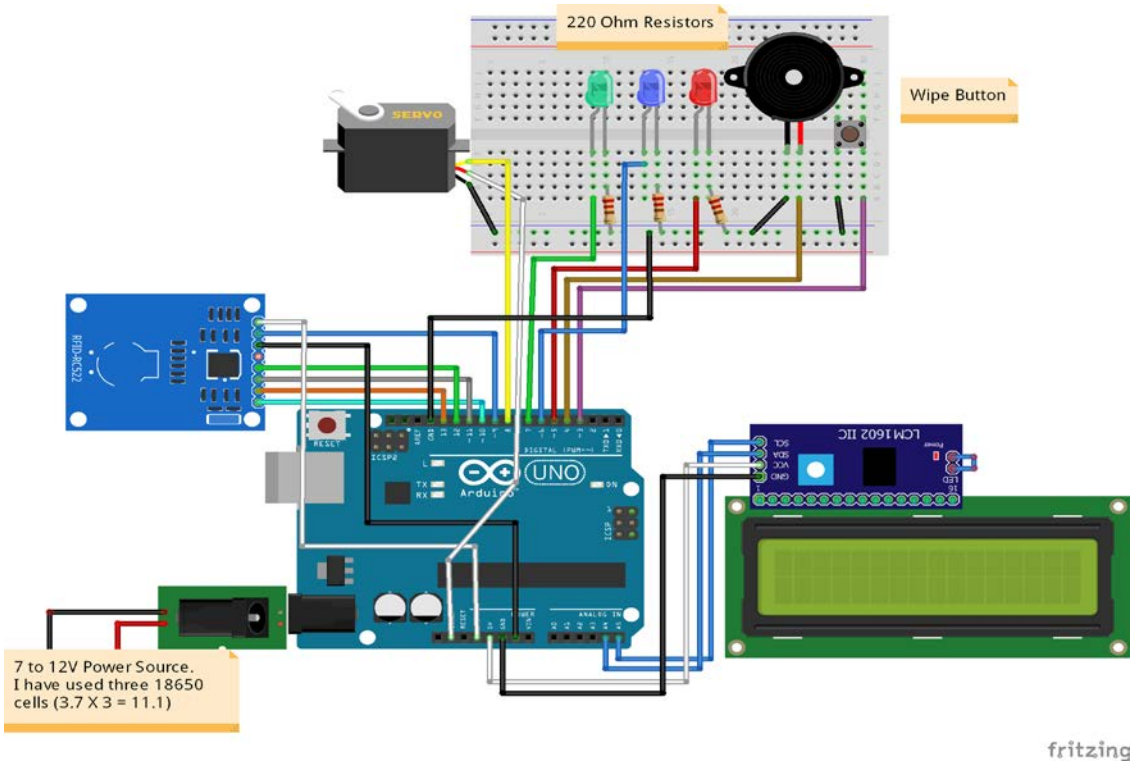
Composants requis

- ArduinoUno
- LCD I2C
- Lecteur RFID MFRC522
- Moteur servo SG90
- 3 X LED (rouge, vert, bleu)
- 3 résistances de 220 ohms
- Avertisseur sonore
- Bouton poussoir
- Alimentation 6 à 12V (adaptateur AC/DC 12V 2A)

On résume le fonctionnement par l'organigramme suivant :



Le schéma complet du système de contrôle d'accès basé sur RFID utilisant Arduino est le suivant:



III.5 Système de contrôle d'accès et d'alerte basé sur RFID utilisant Arduino

Dans l’étape précédente le système n'autorisait l'accès qu'en analysant si l'étiquette est autorisée et refuse l'accès à l'étiquette non autorisée. Une balise (étiquette) principale a été utilisée pour ajouter / supprimer d'autres balises.

Fonctionnement du système de contrôle d'accès et d'alerte basé sur la RFID

Lors du démarrage du projet pour la première fois, il nous demandera de définir une balise principale et quelle que soit la balise que nous scannerons sera notre balise principale. L'étiquette principale agira en tant que programmeur et on pourra l'utiliser pour ajouter ou supprimer d'autres balises.

Après avoir défini l'étiquette principale, on devra ajouter d'autres balises qu’on peut utiliser pour ouvrir la porte. Pour ce faire, on scanne l'étiquette principale et il prendra le système en mode programme.

Dans le mode programme, le balayage des balises les ajoutera/supprimera du système. On balaye les balises qu’on souhaite utiliser pour ouvrir la porte et le système stockera l'UID de ces balises dans l'EEPROM. On scanne à nouveau l'étiquette pour la supprimer de l'EEPROM. Pour sortir du mode programme, on scanne l'étiquette principale.

Maintenant, on scanne les balises que nous avons ajoutées dans le système pour ouvrir la porte, il nous enverra un message de confirmation. Lors du balayage de la mauvaise étiquette, la porte restera fermée et elle nous enverra un message d'alerte.

Nous serons également en mesure d'arrêter le système en envoyant le message «ferme» à Arduino. Pendant ce temps, le système ne sera actionné que soit par des balises principauxou des messages.

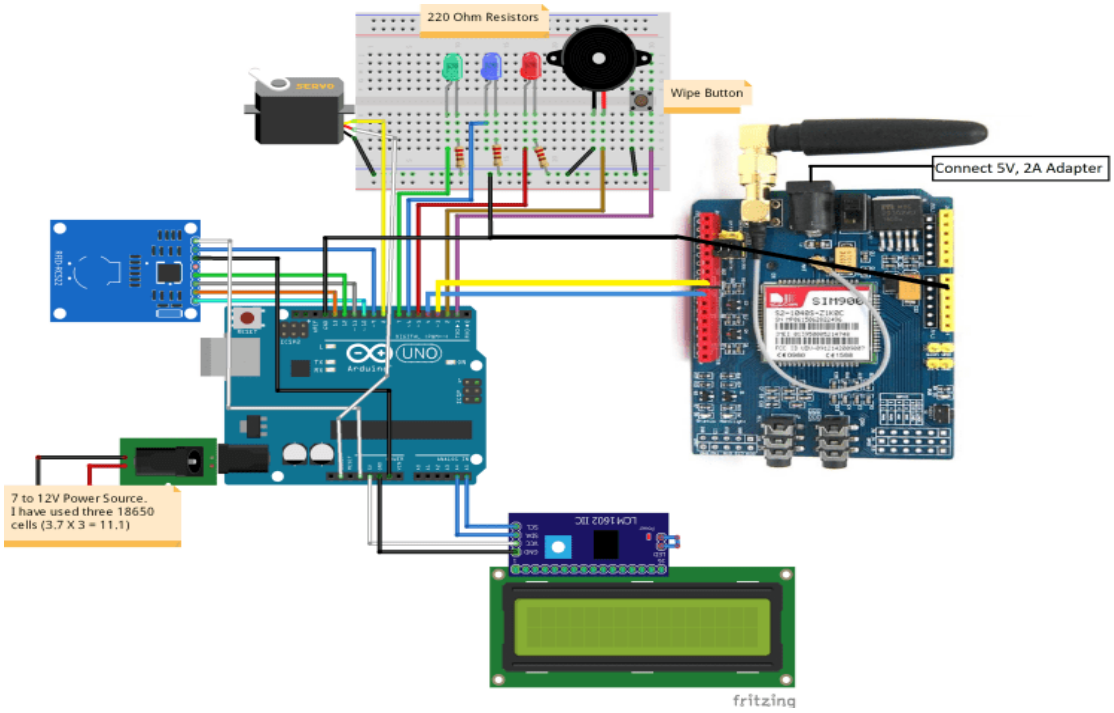
Pour réinitialicesler le système, appuyez sur le bouton de réinitialisation d'Arduino, puis appuyez sur le bouton d'essuie-glace pendant 10 secondes. Cela supprimera toutes les données de l'EEPROM, y compris l'étiquette principale.

Composants requis

- ArduinoUno
- i2C LCD

- Lecteur RFID MFRC522
- Tags
- Module GSM SIM900
- Adaptateur d'alimentation 2A
- Moteur Servo SG90
- 3 X LED (rouge, vert, bleu)
- 3 X 220 ohm résistances
- Buzzer
- Bouton poussoir
- Source d'alimentation de 6 à 12V

Le diagramme de circuit complet pour le système de contrôle et d'alerte d'accès basé sur RFID utilisant Arduino est le suivant :



III.6 Système de contrôle d'accès basé sur la RFID et le Clavier

Dans l'étapeprécédent, nous avons réalisé un système de contrôle d'accès RFID et d'alerte en utilisant Arduino dans lequel le système nous envoie des messages lorsque l'accès a été accordé ou refusé. Nous avons également été en mesure d'ouvrir la serrure de la porte et d'arrêter le système en envoyant le message à Arduino. Il y avait une balise principale qui a été utilisée pour ajouter /supprimer d'autres balises.

Dans ce qui suit, nous allons construire un système de contrôle d'accès RFID et clavier dans lequel l'utilisateur devra d'abord scanner la bonne balise, puis il devra entrer le mot de passe pour cette balise pour ouvrir le verrou de la porte. Il y aura une balise principale qui sera utilisée pour ajouter/supprimer d'autres balises et chaque balise aura son propre mot de passe.

Les balises et le mot de passe resteront enregistrés même après avoir arrêté l'alimentation du module. La seule façon de réinitialiser le système est d'utiliser le bouton d'effacement qui effacera toutes les données de l'EEPROM

Fonctionnement du système de contrôle d'accès RFID et Keypad à l'aide d'Arduino

Lors du démarrage du projet pour la première fois, il vous demandera de définir une balise principale et mot de passe pour elle. L'étiquette principale agira en tant que programmeur et vous pouvez l'utiliser pour ajouter ou supprimer d'autres balises.

Après avoir défini l'étiquette principale, vous devrez ajouter d'autres balises que vous pouvez utiliser pour ouvrir la porte. Pour ce faire, scannez l'étiquette principale et entrez le mot de passe pour elle et il prendra le système en mode programme.

Dans le mode programme, le balayage des balises les ajoutera/supprimera du système. Scannez les balises que vous souhaitez utiliser pour ouvrir la porte et entrez le mot de passe de cette balise. Le système stockera l'UID et le mot de passe de ces balises dans l'EEPROM. Scannez à nouveau l'étiquette et entrez son mot de passe pour la supprimer de l'EEPROM. Pour sortir du mode programme, scannez l'étiquette principale.

Maintenant, scannez les balises que vous avez ajoutées dans le système et entrez leurs mots de passe pour ouvrir la porte et lors de la numérisation de la mauvaise balise ou en entrant le mauvais mot de passe, la porte restera fermée.

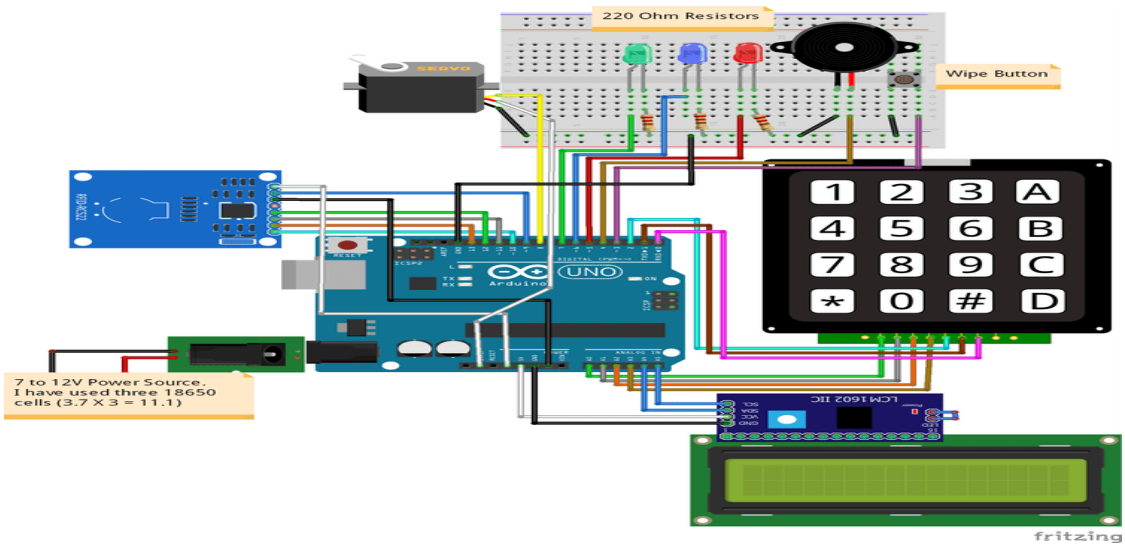
Pour réinitialiser le système, appuyez sur le bouton de réinitialisation d'Arduino, puis appuyez sur le bouton d'essuie-glace pendant 10 secondes. Cela supprimera toutes les données de l'EEPROM, y compris l'étiquette principale.

Composants requis

- ArduinoMega 2560
- L'i2C LCD
- Lecteur RFID MFRC522
- Moteur Servo SG90

- Clavier 4X4 ou Clavier 4X3
- 3 X LED (rouge, vert, bleu)
- Buzzer
- Bouton poussoir
- Source d'alimentation de 6 à 12V (j'ai utilisé 3 cellules X 18650)

Le diagramme complet du circuit est le suivant :



III.7 Système de contrôle d’accès et d'alerte basé sur la RFID et le clavier

Dans l’étape précédente, nous avons réalisé un montage contrôle d'accès basé sur RFID et clavier basé dans lequel l'utilisateur doit d'abord scanner la bonne étiquette, puis il doit entrer le mot de passe pour cette balise pour ouvrir le verrou de la porte. Il y avait une balise principale qui a été utilisée pour ajouter / supprimer d'autres balises et chaque balise avait son propre mot de passe.

Dans cette étape, nous allons ajouter le module Sim900 GSM pour réaliserun système de contrôle d’accès et d'alerte basé sur la RFID et le Clavier. Le système nousenverra des messages lorsque l'accès sera accordé ou refusé. Nous serons également en mesure d'ouvrir le verrou de la porte ou d'arrêter le système en envoyant le message à Arduino. Le système reviendra en mode normal en scannant l'étiquette principale ou en envoyant le message « ouvrir » à Arduino.

Fonctionnement du système de contrôle d'accèset d'alerte basé sur RFIDet clavier

Lors du démarrage du système pour la première fois, il vous demandera de définir une balise principale et mot de passe pour elle. L'étiquette principale agira en tant que programmeur et vous pouvez l'utiliser pour ajouter ou supprimer d'autres balises.

Après avoir défini l'étiquette principale, vous devrez ajouter d'autres balises que vous pouvez utiliser pour ouvrir la porte. Pour ce faire, scannez l'étiquette principale et entrez le mot de passe pour elle et il rendra le système en mode programme.

Dans le mode programme, le balayage des balises les ajoutera/supprimera du système. Scannez les balises que vous souhaitez utiliser pour ouvrir la porte et entrez le mot de passe de cette balise. Le système stockera l'UID et le mot de passe de ces balises dans l'EEPROM. Scannez à nouveau l'étiquette pour la supprimer de l'EEPROM. Pour sortir du mode programme, scannez encore une fois l'étiquette principale.

Maintenant, scannez les balises que vous avez ajoutées dans le système et entrez leurs mots de passe pour ouvrir la porte. Pendant l'ouverture du verrou de porte, il nous enverra le message de confirmation. Lors du balayage de la mauvaise balise ou en entrant le mauvais mot de passe, la porte restera fermée et elle nous enverra un message d'alerte.

Nous serons également en mesure d'arrêter le système en envoyant le message «fermer» à Arduino. Pendant ce temps, le système ne s’activera que par des balises principaux ou des messages.

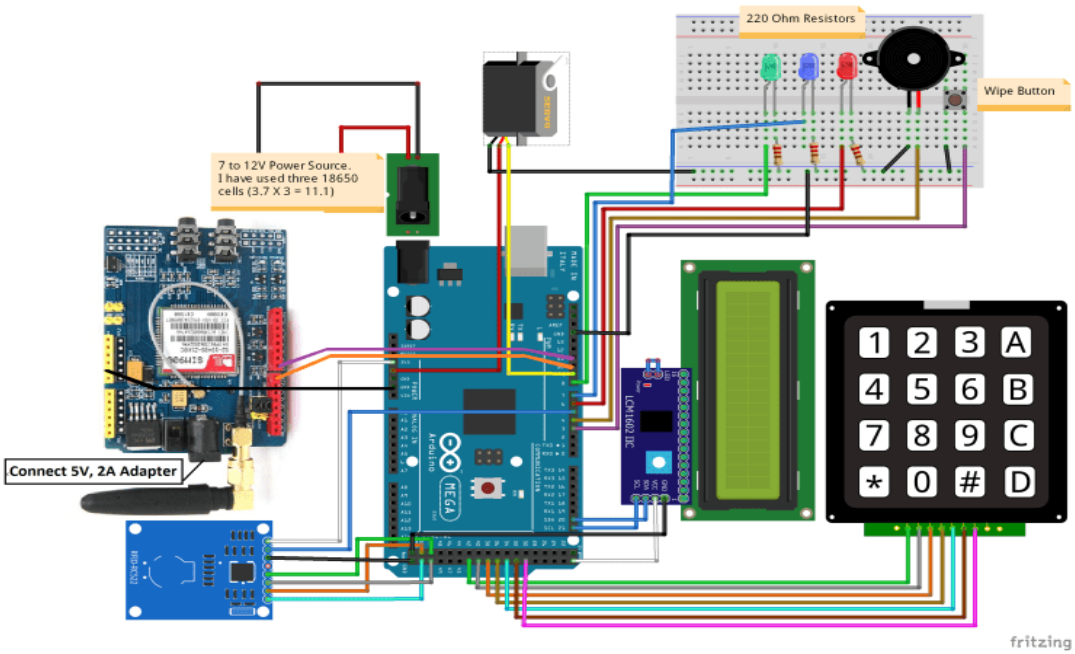
Pour réinitialiser le système, appuyez sur le bouton de réinitialisation d'Arduino, puis appuyez sur le bouton poussoir pendant 10 secondes. Cela supprimera toutes les données de l'EEPROM, y compris l'étiquette principale.

Composants requis

- Arduino Mega 2560
- L'i2C LCD
- Lecteur RFID MFRC522
- Tags
- Moteur Servo SG90
- Module GSM SIM900
- Adaptateur d'alimentation 2A

- Clavier 4X4 ou Clavier 4X3
- 3 X LED (rouge, vert, bleu)
- 3 X 220 ohm résistances
- Buzzer
- Bouton poussoir
- Source d'alimentation de 6 à 12V
-

Le diagramme complet du circuit est le suivant :



III.8 Conclusion :

Les montages réalisés et les tests effectués montrent que pour sécuriser l'accès à des endroits sensibles, nous devons renforcer l'accès par RFID avec un mot de passe pour chaque tag autorisé qui est introduit par clavier. Nous devons associer au système un module d'alerte par GSM qui avisera les intrus et qui permettra aussi de commander l'ouverture et la fermeture du système ainsi que l'accès à distance.

Conclusion général

Conclusion général

L’identification par radio fréquence RFID fait référence aux technologies qui utilisent les ondes radio pour identifier automatiquement des articles individuels ou groupés. La RFID promet de devenir la technologie de pointe dans l’identification automatique. De plus la RFID permet d’améliorer les services, réduire les couts et réaliser des traitements professionnels comme la gestion des stocks, l’expédition, l’identification, et un suivi réellement efficace.

La technologie de définition radio est une technologie moderne qui a plusieurs utilisations dans les systèmes embarqué afin qu'elle puisse être abordée dans le domaine de la sécurité et de la protection. Au début du projet, l'objectif était de fournir un support basé sur la carte Arduino et la carte RC255 ainsi que le modèle GSM pour la conception du système de contrôle d'accès

L'utilisation des cartes d'interface Arduino a grandement facilité la mise en œuvre du système et nous a permis d'obtenir un résultat assez concluant. Dans le dernier chapitre, nous avons mis au point un scénario pour soutenir l'utilité de notre idée en utilisant le contrôle d'accès. Nous avons montré la simplicité de ce système, mais surtout, la valeur de ce système, qui met l'accent sur l'identification, la sécurité et la responsabilité de la sécurité

BIBLIOGRAPHIE

BIBLIOGRAPHIE

[1] Nicolas SERIOT. Les systèmes d'identification radio (RFID) : fonctionnement, applications et dangers. Technical report, Yverdon-les-Bains, 13-janvier-2005.

[2] Monvèa Maurice SESSOU Conception d'un système de contrôle automatique des cartes de visite technique des véhicules au Bénin. Mémoire d'ingénieurs soutenu 15-décembre-2019

[3] CITC-EuraRFID. La gestion d'un projet RFID : Conseils et témoignages, 2012.

[4] Barthe Frédéric RFID : Quelles perspectives pour la chaîne logistique amont ? Université Paris I Master 2 Logistique juin 2006

[5] Rafik KHEDDAM. Approches logicielles de sûreté de fonctionnement pour les systèmes RFID. Thèse soutenue publiquement le 09 avril 2014

[6] S. Lahiri, RFID Sourcebook. Pearson P T R, 2011.

[7] « Different Types of RFID Systems | Impinj ». [En ligne]. Disponible sur : https://www.impinj.com/about-rfid/types-of-rfid-systems/.

[8] T. Igoe, Getting started with RFID, First edition. Sebastopol, CA: O'Reilly Media, Inc, 2012.

[9] K. Finkenzeller, Fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication, 3rd ed. Chichester, West Sussex ; Hoboken, NJ: Wiley, 2010.

[10] D. M. Dobkin, The RF in RFID: UHF RFID in practice, Second edition. Amsterdam : Elsevier/Newnes, 2013.

[11] « Le contrôle des stocks et la traça bilité,... » [En ligne]. Disponible sur: https://www.lsa-conso.fr/le-controle-des-stocks-et-la-traca-bilite-premiers-enjeux-de-la-rfid,125690.

[12] « Smart Cities utilisent RFID et Wireless IoT - RFID & Wireless IoT tomorrow ». [En ligne]. Disponible sur: https://www.rfid-wiot-tomorrow.com/fr/smart-cities-utilisent-rfid-et-wireless-iot-160.

[13] « 13 applications RFID : Art ». [En ligne]. Disponible sur: http://www.journaldunet.com/solutions/0703/070322-rfid/11.shtml

[14] « Arduino - Software ». [En ligne]. Disponible sur: https://www.arduino.cc/en/Main/Software?

[15] « Arduino - Products ». [En ligne]. Disponible sur: https://www.arduino.cc/en/Main/Products.

Résumé

De nos jours l'exploitation de la technologie RFID commence à se généraliser sur des axes d'applications très variés : passeports biométriques, cartes de crédits, cabines de péage, badges sécurisés, systèmes de stock sécurisés et identification. Notre pays commence à préparer une large utilisation de cette technologie avec la mise en place de la législation nécessaire.

Le présent projet consiste à réaliser un prototype complet d'identification pour le contrôle d'accès avec un système d'alerte par module GSM en veillant à la sécurité et l'intégration des données. Nous dotons notre prototype par un programme de gestion de la base de données des badges (tags) autorisés à l'accès.

Abstract

Nowadays, the exploitation of RFID technology is beginning to spread over a wide range of applications: biometric passports, credit cards, toll booths, secure badges, secure stock systems and identification. Our country is starting to prepare a wide use of this technology with the implementation of the necessary legislation.

The present project consists in carrying out a complete identification prototype for access control with a GSM module alert system while ensuring the security and integration of data. We provide our prototype with a database management program badges (tags) allowed access.

ملخص

في الوقت الحاضر ، بدأ استغلال تقنية RFID في الانتشار على مجموعة واسعة من التطبيقات: جوازات السفر البيو مترية ، وبطاقات الائتمان ، ومقصورات الخسائر ، والشارات الآمنة، ونظم الأوراق المالية الآمنة وتحديد الهوية. بدأ بلدنا في إعداد استخدام واسع لهذه التكنولوجيا من خلال تنفيذ التشريعات اللازمة.

يتكون المشروع الحالي من تنفيذ نموذج تعريف كامل للتحكم في الوصول باستخدام وحدة نظام تنبيه GSM مع ضمان أمن البيانات وتكاملها. نحن نقدم النموذج الأولي لدينا مع شارات برنامج إدارة قواعد البيانات يسمح بالدخول.