RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ IBN-KHALDOUN DE TIARET

FACULTÉ DES SCIENCES APPLIQUEES

DÉPARTEMENT DE GENIE ELECTRIQUE

MEMOIRE DE FIN D'ETUDES

Pour l'obtention du diplôme de Master

Domaine : Sciences et Technologie

Département : Génie Electrique

Spécialité : Electronique des Systèmes Embarqués

THÈME

Techniques de réduction de la consommation de l'énergie des systèmes embarqués à faible puissance. Application aux étiquettes RFID et cartes à puce.

Préparé par :
BELHADJ Ouissam
BOUFARROUDJ Bentaleb

Devant le Jury :

Nom et prénoms	Grade	Qualité
M.MAASKRI	MAA	Président
M.BELARBI	MCA	Examinateur
B.SAHLI	MCA	Encadreur

Dédicaces

Ce travail modeste est dédié :

À nos parents Qu'ils trouvent en nous la source de leur fierté à qui nous devons tout ; et plus particulièrement, à tous nos proches des familles **BELHADJ** *et* **BOUFARROUDJ**, *à tous nos chers amis et nos camarades de l'Université Ibn Khaldoun de Tiaret ;*

Et à tous ceux qui nous ont enseigné au long de notre vie scolaire.

Remerciement

Tout d'abord, nous remercions le tout puissant ALLAH, notre créateur de nous avoir donné la force, la volonté et le courage afin d'accomplir ce travail modeste.

Nous adressons le grand remerciement à notre encadreur Mr. SAHLI BELGACEM, pour ses conseils et sa disponibilité du début à la fin de ce travail, ainsi qu'à l'ensemble des professeurs qui ont contribué à notre formation.

Enfin, nous adressons nos plus sincères remerciements à nos familles qui nous ont soutenues moralement de loin ou de près, toutes les personnes qui ont participé à ces recherches et à l'élaboration de ce mémoire. Ainsi, nos proches et nos amis, qui nous ont accompagnés, aidé, soutenu et encouragé tout au long de la réalisation de ce mémoire.

Sommaire

CHAPITRE II:

CHAPITRE III :

Liste des abréviations

RFID: Radio-Frequency Identification.

RFIC: Radio-Frequency Integrated Circuit.

DSP: Digital Signal Processor.

CPU: Central Processing Unit.

CMOS: Complementary Metal Oxyde Semi-conductor.

TTL: Transistor Transistor Logique.

CU: Control Unit.

EU: Execution Unit.

ALU: Arithmetic Logic Unit.

GPP: General Purpose Processors.

DMA: Direct Memory Access.

E/S: Entre/Sortie.

RF: Radio-Frequency.

CRFID: Computational Radio-Frequency Identification.

RAM: Random Access Memory.

VCC: Collector supply voltage.

VDD: Drain supply.

VSS: source supply.

NFC: Near Field Communication.

CCP: Compte Cheque Postal.

POR: Power-On Reset.

R-T: Receiver- Transmission.

EEPROM: Electrically Erasable Programmable Read-Only Memory.

SC: Storage Capacitor.

UHF: Ultra High Frequency.

LF: Low Frequency.

HF: High Frequency.

SHF: Super High Frequency.

ICC: Integrated Circuit Card.

ROM: Read Only Memory.

IP: Internet Protocol.

UART: Universal Asynchronous Receiver-Transmitter.

IEEE: Institute of Electrical and Electronic Engineers.

LRWPAN: Low Rate Wireless Personal Area Network.

ISO: International Organization for Standardization.

MMU: Memory Management Unit.

ADC: Analog to Digital Converter.

TI: Texas Instruments.

VLSI: Very Large Scale Integration.

DVFS: Dynamic Voltage Frequency Scaling.

MCU: Micro Controller Unit.

ULP: Ultra-Low Power.

AM: Active Mode.

LPM: Low Power Modes.

ACLK: Auxiliary Clock.

SMCLK: Secondary Clock.

MCLK: Principal Clock.

DSSS: spread spectrum with direct sequence.

FFD: Dispositive A Full Function.

DCO: Digitally controlled oscillator.

RISC: Reduce Instruction Set Computer.

A/N: Analogic Numeric.

DTC: Data Transfer Controller.

SPI: Serial Peripheral Interface.

RTC: Real Time Clock.

GPIO: General Purpose Input/output.

BOR: Brown out Reset.

SVS: Supply Voltage Supervisor.

FRAM: Ferroelectric RAM Random Access Memory.

AES: Advanced Encryption Standard.

MIPS: Millions Instruction per Second.

RFD: Reduced Function Device.

CSMA-CA: Carrier Sense Multiple Access with Collision Avoidance.

ISM: industrial scientific medical.

SOC: Systems on a Chip.

DPA: Differential Power Analysis.

FIFO: First In First Out.

NIST: National Institute of Standards and Technology.

NRZ: Non-Return-To-Zero.

DM: Différentiel Manchester.

MDM: Manchester /Différentiel Manchester.

CISC: Complex Instruction Set Computer.

VHDL: VHSIC Hardware Description Language.

VHSIC: Very High Speed Integrated Circuits.

MAC: Medium access control.

RTF: Reader Talks First.

TTF: Tag Talks First.

Liste des figures

Liste des Tableaux

Introduction Générale :

Au cours des dernières années, on a assisté à une prolifération de dispositifs intégrés de faible puissance [85,86,87,88] avec des plages de puissance de quelques milliwatts (alimentation par batterie) à des microwatts (sans piles) [89]. Les capacités et la taille des systèmes intégrés continuent de s'améliorer considérablement ; Cependant, l'amélioration de la densité de la batterie et de la récupération d'énergie n'a pas réussi à imiter la loi de Moore. La densité d'énergie de la batterie est la tendance la plus lente de l'informatique mobile et ne s'adapte pas de manière exponentielle [90]. Ainsi, l'énergie reste un formidable goulot d'étranglement pour les systèmes embarqués à faible consommation. Par exemple, les circuits d'une lentille intelligente peuvent être suffisamment miniaturisés pour être implantés à l'intérieur d'un œil [91] ; cependant, les piles correspondantes ne sont pas assez petites pour une telle implantation.

Chaque année, rien qu'aux États-Unis, plus de 3 milliards de piles sont achetées [92], dont une fraction est utilisée pour l'alimentation de systèmes embarqués allant des détecteurs de fumée aux compteurs grand public, en passant par les transpondeurs d'autoroutes à péage (utilisant des étiquettes RFID actives) et les stimulateurs cardiaques. D'un point de vue écologique, l'humanité souhaite un avenir dans lequel moins de batteries chimiques sont achetées et qui atterrissent sur la terre, même si les dispositifs à piles continuent de devenir plus puissants sur le plan informatique. De plus, des dispositifs sans batterie sont développés et utilisés dans des endroits qui n'étaient pas possibles auparavant.

La réalisation de cette vision nécessitera des avancées sur de nombreux fronts : améliorations des technologies de batterie en termes d'énergie par densité, schémas de récupération d'énergie plus productifs, langages de programmation plus éco énergétiques et nouvelles méthodes permettant de réduire la consommation d'énergie des appareils existants. Plus fondamentalement, nous aimerions redéfinir et réexaminer les objectifs et les exigences de conception pour les systèmes basse consommation qui ne sont pas aussi bien équipés que leurs descendants plus puissants, les ordinateurs de bureau.

Les RFID sont utilisées pour remplacer les codes à barres sur les marchandises et pour suivre les stocks [93]. Les grains "Smart Dust" [87] sont de minuscules nœuds autonomes contenant des capteurs, des émetteurs-récepteurs et une source d'alimentation. Ils ont une puissance de calcul limitée. Tous ces périphériques communiquent sans fil et leur source d'énergie est

extrêmement limitée. Les piles pour ces périphériques sont minuscules et ne peuvent fournir 10 W en un jour seulement [87]. En outre, certaines de ces technologies captent l'énergie de sources environnementales, telles que la lumière, la chaleur, le bruit ou les vibrations. Les appareils qui exploitent l'énergie de sources environnementales sont communément appelés les récupérateurs de puissance et les nœuds autonomes utilisant des récupérateurs sont appelés auto-alimentés. Une implémentation d'une unité de traitement du signal alimentée par un dispositif de filtrage de grande capacité pouvant générer jusqu'à 400 µW est décrite dans [94]. Les nouveaux récupérateurs sont basés sur des systèmes microélectromécaniques (MEMS). Ils peuvent être intégrés sur la puce et donc réduire le coût et la taille. Le capteur présenté dans [95] produit environ 8 W d'énergie en se basant uniquement sur la température ambiante. Les réseaux de capteurs distribués sont une application majeure de cette technologie. Les aspects de sécurité de ces réseaux ont été examinés par NAI Labs dans [96]. Cependant, cette étude s'est concentrée uniquement sur les implémentations logicielles sur les processeurs actuels dont la consommation d'énergie dépasse de loin la quantité pouvant être fournie par un circuit de nettoyage.

Dans notre travail, nous nous concentrons exclusivement sur la réduction de la consommation de l'énergie fournie par la batterie des systèmes embarqués à faible puissance. Par conséquent, nous ciblons particulièrement les systèmes RFID à étiquettes actives (munies de batteries).

Chapitre I

- Les systèmes embarqués à faible puissance alimentés par batteries.

I Introduction :

Avec le développement rapide de la technologie, les systèmes embarqués sont devenus intégrés dans de nombreux domaines, tels que l'aviation, les transports intelligents, les réseaux intelligents, la maison intelligente, les soins médicaux, la surveillance de la santé des grands bâtiments, cependant, la haute performance des processeurs permettra également une consommation d'énergie élevée. La gestion de l'énergie est donc importante pour la performance des systèmes embarqués, notamment les systèmes embarqués alimenté par batteries.

Les systèmes embarqués doivent généralement être de faible puissance et hautement fiables, donc il faut le stimuler en exécutant des applications aussi longtemps que possible avec une consommation d'énergie minimale. Dans un système fonctionnant par batterie, ce besoin est amplifié. De plus, une faible puissance signifie des couts d'exploitation réduite et des batteries da taille réduite pour rendre les applications plus attrayantes.

I.1 Généralité sur les systèmes embarqués :

Avant de définir les systèmes embarqués il faut définir d'abord un système autonome.

I.1.1 Système autonome :

Système qui fonctionne sans intervention humaine et ne possédant pas des entrées-sorties standards [2] tels qu'un clavier ou un écran d'ordinateur [1], c'est-à-dire un système qui est capable de réaliser des tâches sans aucune assistance extérieure [3].

I.1.2 Système embarqué :

Les systèmes embarqués sont des systèmes informatiques, électroniques et autonomes pour le traitement de l'information, c'est à dire l'unité de traitement possédant une certaine autonomie, cette autonomie est la propriété la plus couramment associée à la notion de système embarqué. Ces systèmes contiennent une ou plusieurs unités de traitement ou processeurs de signal numérique (DSP).

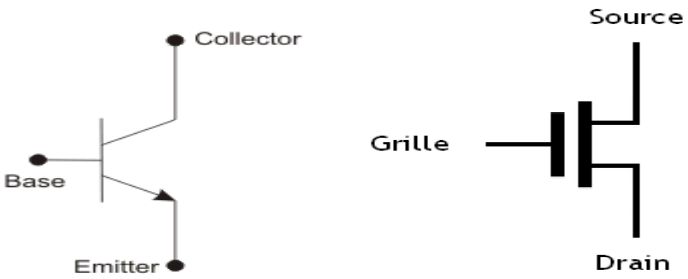
Les exemples incluent les systèmes embarqués dans les voitures, les trains, les avions et les équipements de télécommunication ou de fabrication.

Ils sont conçus comme une combinaison de plate-forme matérielle et de couches logicielles permettant d'exécuter une tâche dédiée souvent avec des contraintes en temps réel, et la fiabilité ainsi que les exigences d'efficacité [14, 15, 16, 17].

I.1.3 Les processeurs :

Le CPU est l'abréviation de l'unité centrale. Parfois appelé simplement le processeur central, mais plus communément appelé processeur [5].

Ces processeurs sont fabriqués avec des composants électroniques qu'on appelle des transistors TTL (Transistor Transistor Logic) ou CMOS (Complementary Metal Oxyde Semi-conductor) [13].



TTL CMOS

Figure 1: Transistor CMOS et TTL [13].

Le processeur est le cœur d'un système Embarqué. C'est l'unité de base qui prend les entrées et produit une sortie après le traitement des données [6].

Un processeur a deux unités essentielles comme le montre la **Figure 2** :

Unité de contrôle de flux de programme **(CU),**

Unité d'exécution (**UE**) inclut l'unité arithmétique et logique (**ALU**).

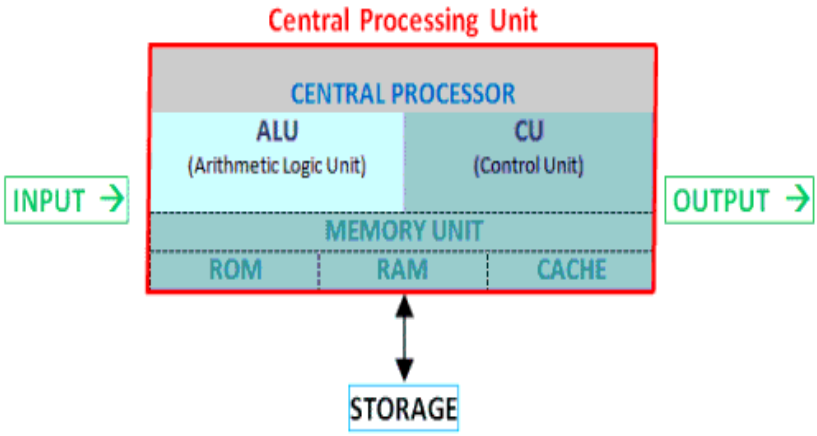


Figure 2: Les composants de CPU [5].

I.1.3.1 Les types de processeurs :

I.1.3.1.1 Processeur à usage général (GPP) :

Les processeurs à usage général (GPP) sont conçus pour les ordinateurs à usage général tels que les PC ou les stations de travail. La vitesse de calcul d'un GPP est la principale préoccupation et son coût est généralement beaucoup plus élevé que celui des DSP et des microcontrôleurs et Processeur Embarqué. Toutes les techniques pouvant augmentées la vitesse du processeur ont été appliquées aux GPP. Par exemple, les GPP incluent généralement le cache sur puce et les DMA sur puce. Les opérations mathématiques couramment utilisées sont également prises en charge par le matériel sur puce. Les GPP ne sont pas conçus pour les applications rapides en temps réel. La structure scalaire est courante dans les GPP mais rarement observée dans les DSP et les microcontrôleurs [4].

I.1.3.1.2 Les processeurs embarqués et les µc :

Un processeur embarqué est un type de microprocesseur conçu dans un système pour contrôler les fonctions électriques et mécaniques. Les processeurs embarqués ont généralement une conception simple, une puissance de calcul et des capacités d'E / S limitées, ainsi que des besoins en énergie minimaux. Au niveau de base, les processeurs intégrés sont une puce de processeur placée dans un système qu'elle permet de contrôler.

Les processeurs embarqués sont souvent confondus avec les microcontrôleurs. S'ils remplissent des fonctions similaires, ils s'intègrent à leur système de différentes manières. Les fonctions qu'elles remplissent peuvent également être différentes.

Les microcontrôleurs (µc) sont le résultat des avancées technologiques permettant de réduire la taille des contrôleurs. Finalement, tous les composants d'un contrôleur, y compris les périphériques d'E / S et la mémoire, ont évolué en une seule puce, nous donnant le «micro» microcontrôleur. Ces puces sont de petits périphériques autonomes dotés de toutes les fonctionnalités nécessaires pour contrôler le système dans lequel elles sont intégrées.

Cette autonomie de contrôle constitue la principale différence entre les microcontrôleurs et les processeurs embarqués. Les processeurs embarqués ont besoin d'autres composants externes, tels qu'une mémoire embarqué et des interfaces de périphériques, pour remplir leurs fonctions. Les deux périphériques sont souvent désignés sous le nom de périphérique unique, car les processeurs embarqués sont souvent des composants d'un microcontrôleur [4].

I.2 Les systèmes embarqués à faible puissance :

Cette partie est basée sur les appareils à faible consommation d'énergie disposant de ressources énergétiques limitées, qu'il s'agisse d'une batterie ou de l'énergie récupérée stockée dans des condensateurs. Alors on va décrire brièvement les systèmes embarqués alimentés par batterie et les systèmes alimentés par intermittence c'est à dire des périphériques sans batterie qui perdent régulièrement de la puissance (par exemple, les systèmes RFID passifs).

I.2.1 Les systèmes embarqués alimenté par batterie :

La nécessité d'améliorer la durée de vie de la batterie a largement motivé la recherche et le développement de techniques de conception à faible consommation d'énergie pour les circuits et systèmes embarqués. Les techniques de conception à faible consommation d'énergie permettent de réduire l'énergie tirée de la batterie et, par conséquent, d'améliorer sa durée de vie. Cependant, pour maximiser la durée de vie d'une batterie, il faut comprendre à la fois la source d'énergie et le système qui la consomme [19].

Les systèmes embarqués à faible puissance nécessitent une autonomie énergétique. Ceci est réalisé par des batteries servant de source d'énergie dédiée. L'exigence de portabilité impose de sévères restrictions en termes de taille et de poids, ce qui limite la quantité d'énergie disponible en permanence pour maintenir le bon fonctionnement du système. Pour ces raisons, l'utilisation efficace de l'énergie est devenue l'un des principaux défis du concepteur de systèmes embarqués alimentés par batterie [18]. Avec le nombre croissant de systèmes électroniques alimentés par batterie, la vie de la batterie devient une considération clé de la conception. Pour maximiser la durée de vie des batteries, les concepteurs de systèmes doivent

comprendre les capacités et les limites des batteries qui exploitent ces systèmes et les intégrer au processus de conception.

Des recherches récentes ont démontré que la quantité d'énergie pouvant être fournie par une batterie donnée varie de manière significative en fonction de la manière dont l'énergie est extraite. Ainsi, les chercheurs tentent de développer de nouvelles méthodes de conception du système basées sur les batteries, offrant des améliorations de la durée de vie de la batterie allant au-delà de ce qui peut être obtenu avec des techniques de conception énergétique standard [18].

Exemple sur des applications faible puissance alimentées par batterie :

Nous retrouvons ces systèmes dans de nombreux dispositifs électroniques tels que les détecteurs de fumée, les cartes RFID alimentées par batterie (Active) et d'autres dispositifs de détection utilisant des processeurs intégrés.

I.2.2 Des systèmes alimentés par intermittence :

Contrairement aux dispositifs alimentés par batterie qui supposent que leur ressource énergétique sera disponible sur des commandes de plusieurs mois, un système sans batterie qui vit de l'énergie récoltée (est le processus par lequel de l'énergie est tirée de sources externes) s'attend à des interruptions d'énergie toutes les quelques secondes. Nous définissons les périphériques alimentés par intermittence comme des systèmes qui ne reposent pas sur une source d'alimentation constante et qui doivent redémarrer très régulièrement.

Des exemples de dispositifs ciblés et expérimentés dans cette partie sont les étiquettes RFID passif et les cartes à puce, qui reposent toutes les deux sur une alimentation par radiofréquence (RF) [20].

I.2.2.1 RFID computationnels :

Les dispositifs RFID computationnels sans pile (CRFID) offrent des possibilités intéressantes pour des applications informatiques omniprésentes. Ils nécessitent un minimum de maintenance, sont peu coûteux à fabriquer et ont un facteur de forme réduit. Cependant, les CRFID manquent d'autonomie en raison de la nécessité d'une puissance constante grâce à des lecteurs RFID [21].

Les composants d’un CRFID sont les suivants : un microcontrôleur à faible consommation (processeur embarqué); RAM embarquée; mémoire flash (sur ou hors du microcontrôleur);

des circuits de récupération d'énergie accordés à une certaine fréquence ; une antenne; un transistor entre l'antenne et le microcontrôleur pour moduler l'impédance de l'antenne; un condensateur pour le stockage de l'énergie récoltée; un ou plusieurs convertisseurs analogique-numérique; et des capteurs optionnels pour des phénomènes physiques tels que l'accélération, la chaleur ou la lumière. Le premier exemple d'utilisation d'un CRFID est la plateforme d'identification et de détection sans fil [20].

I.2.2.2 Carte à contact :

Nous prenons les cartes à puce comme exemple, selon le mode d'alimentation, elles sont considérées comme étant à contact ou sans contact. Les cartes à puce à contact, plus courantes que les cartes sans contact, utilisent six broches pour communiquer avec un lecteur de carte. Une des broches est le VCC qui devrait être en contact avec le lecteur.

Bien que certaines cartes à puce soient alimentées par batterie non rechargeable, lorsque la batterie se décharge c'est la fin de vie du produit, nous parlons ici de celles qui ne dépendent que de l'énergie reçue du lecteur. Par exemple, les cartes de crédit. Le temps de lecture de la carte, qui est égal au temps de mise sous tension, doit être inférieur à 300 ms-500ms (délai acceptable par les clients pour utiliser une carte). Les courtes périodes de mise sous tension rendent les cartes à puce comme des appareils alimentés par intermittence [20].

I.3 Des applications basse consommation :

Pour comprendre pourquoi nous avons maintenant des mobiles et des services NFC (Near Field Communication : est une technologie de connexion sans fil à courte distance qui vous permet de payer vos achats, de valider vos titres de transport ou d'accéder à des contenus en lisant un tag NFC avec votre mobile.) (CCP) à notre disposition, il nous faut revenir sur un certain nombre de technologies qui les ont précédés comme les technologies radiofréquences ou la carte à puce et c'est l'objet de ce chapitre.

I.3.1 La Technologie RFID :

Insérer une clé pour démarrer un véhicule, badge pour accéder à un bâtiment ou une salle, utiliser les remontées mécaniques lors d'un séjour au ski, valider un titre de transport dans le bus ou le métro sont des gestes entrés dans le quotidien de bon nombre d'entre nous. Nous utilisons, sans en être toujours conscients, des technologies de capture automatique de données basées sur les ondes et rayonnements radiofréquence. Cette technologie est connue

sous le nom de RFID pour Identification Radiofréquence (**Figure 3**). De même que chaque individu peut être identifié grâce à un passeport biométrique ou encore un badge d'accès personnel, les objets sont aujourd'hui de plus en plus souvent porteurs d'étiquettes RFID contenant un identifiant unique et parfois quelques octet ou kilooctets de données. La différence entre les objets et nous, c'est qu'ils ne présentent pas « volontairement » leur étiquette ou badge RFID lorsqu'on leur demande. Les conditions de lecture de ces étiquettes sont donc différentes et demandent généralement des distances de détection plus importantes [21].

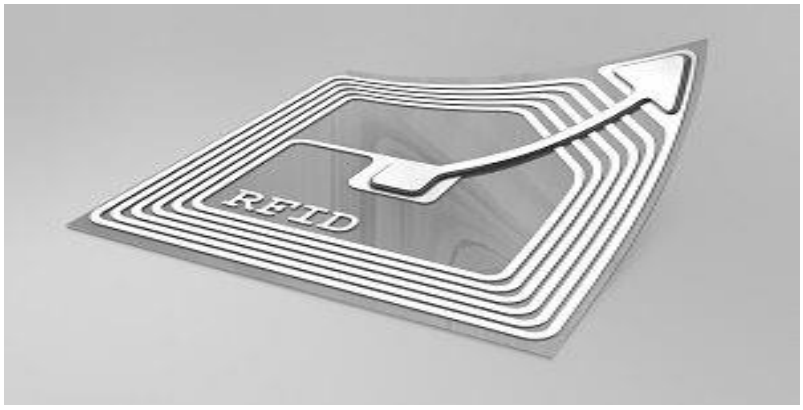


Figure 3: RFID tag.

I.3.1.1 L'identification par radiofréquence (RFID) :

L'identification par radiofréquence (RFID) est une technologie qui utilise la radio comme une ressource énergivore et permet de lire des informations et de les récupérer à distance [23] à partir d'un dispositif commercial sans fil peu coûteux, appelé étiquette RFID, équipé d'une puce informatique et d'une antenne.

Un dispositif RFID peut simplement transmettre son numéro d'identification unique ; il peut également transmettre des données supplémentaires sur un objet spécifique (par exemple, la date d'emballage, le prix, l'usine d'origine, etc.) ou une personne (par exemple, le nom, l'état de santé, etc.) [25].

Il est plus fiable, efficace, sécurisé, économique et précis que d'autres identificateurs automatiques similaires, tels que les réseaux de capteurs, les systèmes d'imagerie, etc. Ces raisons sont la raison pour laquelle la technologie RFID est plus populaire, récemment [24].

I.3.1.2 Les différents composants d'un système RFID :

Un système complet utilisant la technologie RFID est composé des éléments suivants :

I.3.1.2.1 L'étiquette RFID :

La **Figure 4** présente la composition du tag RFID. La puce RF (RFIC) qui est la IDS-SL13A **(**est très intéressant pour les systèmes embarqués car il dispose de deux régulateurs intégrés : un pour la partie digitale et l'autre pour la partie analogique. Ces régulateurs peuvent être activés et désactivés séparément. Cette petite particularité permet de réaliser des économies d'énergie considérables sur un système embarqué car on peut grâce à cela déconnecter toute la partie analogique tout en gardant le microcontrôleur (MCU) activé**)** transmette sa puissance à l'antenne. Si la batterie est présente, elle alimente en même temps le MCU et le RFIC. Dans le cas contraire, le champ RF alimente d'abord le RFIC qui peut ensuite fournir une tension régulée au MCU.

L'interface pour programmer le microcontrôleur JTAG (Joint Test Action Group : est une interface matérielle commune qui fournit à votre ordinateur un moyen de communiquer directement avec les puces d'une carte.), Le MCU est un MSP430F2122. Il est chargé de piloter les capteurs. Les capteurs utilisés pour le projet étant capacitifs, il est nécessaire d'utiliser un composant qui convertie la valeur de la capacité dans un format compréhensible par le MCU. Le composant AD7150 réalise cette tâche. Il transforme la valeur de la capacité en une valeur digitale d'une résolution de 12 bits qui est ensuite transmise au MCU.

Si la batterie est présente, elle alimente en même temps le MCU et le RFIC. Dans le cas contraire, le champ RF alimente d'abord le RFIC qui peut ensuite fournir une tension régulée au MCU. Le MCU est alors capable d'alimenter le convertisseur quand bon lui semble depuis un de ses ports [71].

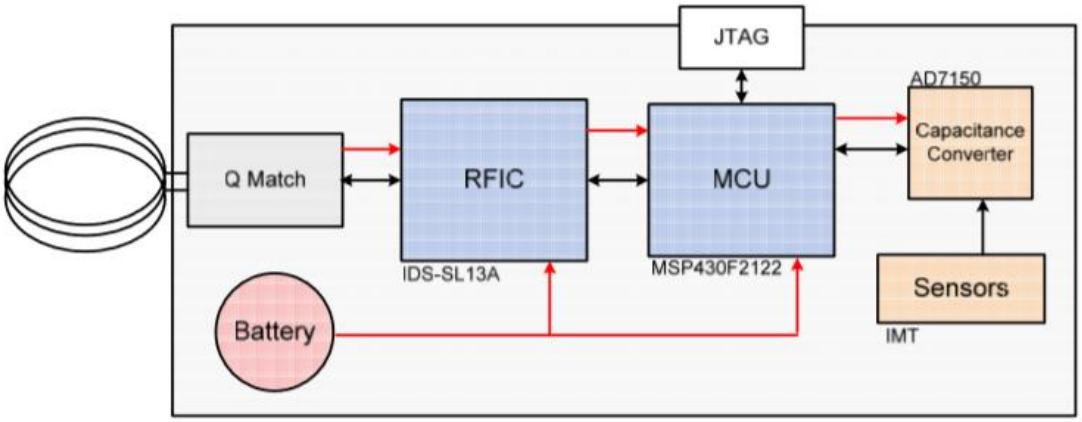


Figure 4: Architecture de l'étiquette RFID.

I.3.1.2.1.1 Les transpondeurs passifs, semi-passifs et actifs :

Nous avons déjà noté qu'il est souvent avantageux d'éliminer l'émetteur radio et batterie à partir d'une étiquette RFID pour économiser de l'argent et de l'espace. La présence ou l'absence de ces composants constitue la base d'un deuxième moyen de classer les systèmes RFID, par le pouvoir et les capacités des étiquettes (**Figure 5**). Les étiquettes passives ne disposent d'aucune source indépendante d'énergie électrique pour piloter les circuits dans le terminal. Les étiquettes semi-passives, également appelées étiquettes passives assistées par batterie, fournissent une batterie locale alimentant le circuit de l'étiquette, mais toujours utilisant des communications rétrodiffusées pour le lecteur de l'étiquette. Les tags actifs ont à la fois une source d'alimentation locale et une source conventionnelle. Émetteur et récepteur sont donc configurés comme des communications radio bidirectionnelles à dispositifs classiques [70,72].

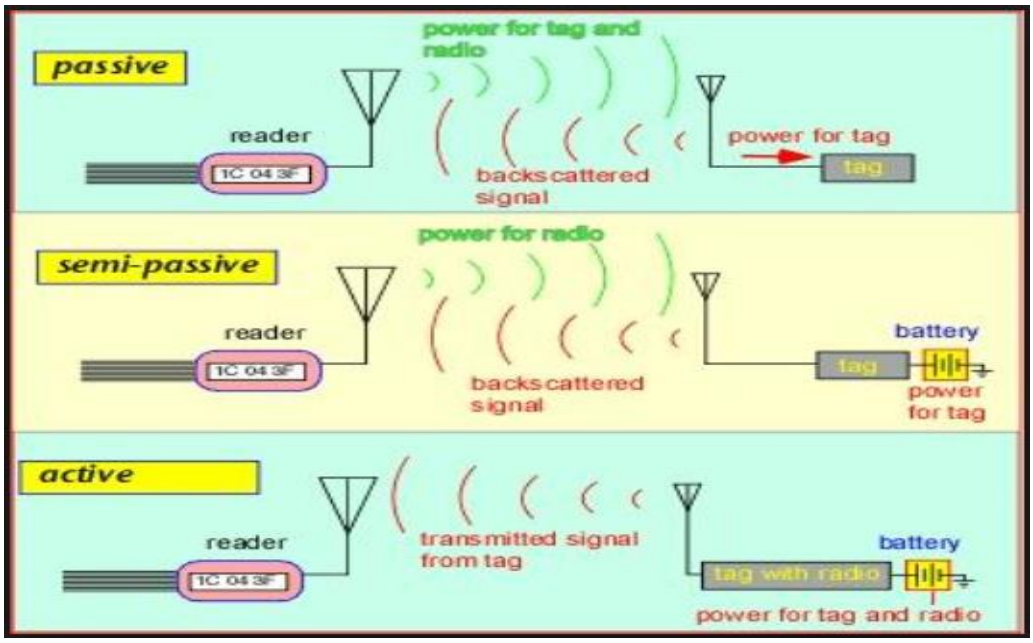


Figure 5: transpondeurs passives, semi-passives et actives [70].

I.3.1.2.1.2 Les transpondeurs actifs :

Un transpondeur actif a les caractéristiques suivantes :

- Possède sa propre source d'alimentation (batterie).
- Durée de vie limitée.
- Génère constamment des ondes électromagnétiques.
- Plus coûteux qu'une étiquette de type passif.
- lecture jusqu'à 150 m.

I.3.1.2.1.3 Les transpondeurs passifs :

Un transpondeur passif a les caractéristiques suivantes :

- Activé uniquement au passage d'un lecteur.
- Ne génère des ondes électromagnétiques qu'au moment de son activation.
- Sans batterie.
- Plus léger.
- lecture à quelques centimètres.

I.3.1.2.2 Lecteur RFID :

C’est un émetteur-récepteur, qui peut à la fois lire et écrire des données sur un transpondeur, et le sous-système de traitement de données qui utilise les données obtenues de l'émetteur-récepteur de manière utile.

Les lecteurs RFID sont constitués d’un module de fréquence radio, d’une unité de contrôle et d’un élément de couplage permettant d’interroger les étiquettes électroniques par communication radiofréquence. En outre, de nombreux émetteurs-récepteurs sont dotés d'une interface leur permettant de communiquer les données qu'ils ont reçues à un sous-système de traitement de données, par exemple une base de données s'exécutant sur un ordinateur personnel [27, 38].

I.3.1.2.3 Une antenne :

Qui est généralement intégrée au lecteur RFID et à l’étiquette RFID. Elle permet d’activer les tags afin de recevoir des données et d’en transmettre les informations **Figure 6** [26].

Figure 6: Antennes de Tags RFID [26].

I.3.1.3 Fonctionnement de la RFID :

Un système d'Identification par ondes Radiofréquences se compose de deux éléments principaux : un Tag et un Lecteur. Le Tag contient toutes les données relatives à l'objet qui l'identifie de façon unique. Les données, stockées dans une puce électronique, «chip», peuvent être lues grâce à une antenne qui reçoit et transmet des signaux radio vers et depuis le Lecteur ou interrogateur. Le Lecteur, fixe ou tenu à la main, est le dispositif qui est en charge de la lecture des Tags RFID situés dans son champ de lecture et capable de convertir les ondes radio du Tag en un signal numérique qui peut être transféré à un PC. La **Figure 7** décrit le fonctionnement général d’un système d’identification par radiofréquence [25].

Figure 7: Fonctionnement de la RFID [25].

I.3.1.4 La famille des radiofréquences :

La **Figure 8** présente les bandes de fréquences pour RFID**,** l'usage commercial du terme RFID est la plupart du temps associé avec une bande de fréquence spécifique, dit **Ultra High Frequency (UHF)** utilise le couplage radiatif en champ lointain. Il existe d'autre fréquence comme **: Low Frequency (LF) et High Frequency (HF)** utilise le couplage inductif en champ proche (Voir **Figure 9**) [28].

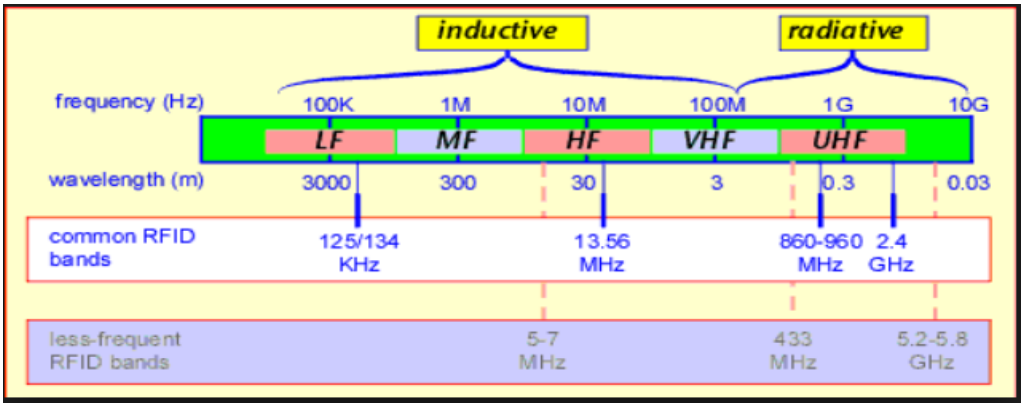


Figure 8: Bandes de fréquences pour RFID [70].

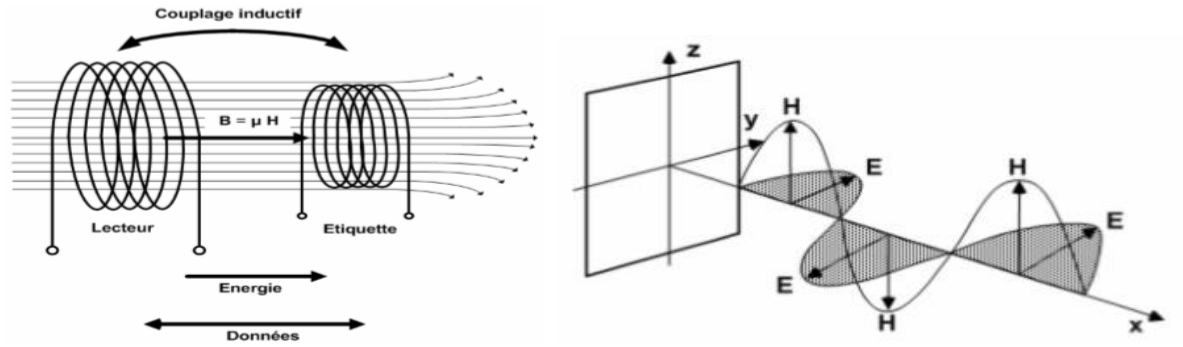


Figure 9: Couplage inductif et radiatif [25].

I.3.1.5 Le marché de la RFID :

Le marché de la RFID a atteint une valeur de 7,67 Milliards de dollars en 2012 avec une hausse de 17% par rapport à 2011 où il était à une valeur de 6,51 Milliards de dollars. Ce marché comprend les tags ou étiquettes, les lecteurs, les cartes et tout ce qui touche à la RFID. 3,98 Milliards de tags ont été vendus en 2012 contre 2,93 Milliards en 2011. Essentiellement des tags passifs pour les très hautes fréquences (100MHz – 1GHz) selon une étude menée par IDTechEx [22]. **Figure 10** met en avant l'évolution du marché prévue sur les 2 prochaines années. Un marché en perpétuelle évolution.

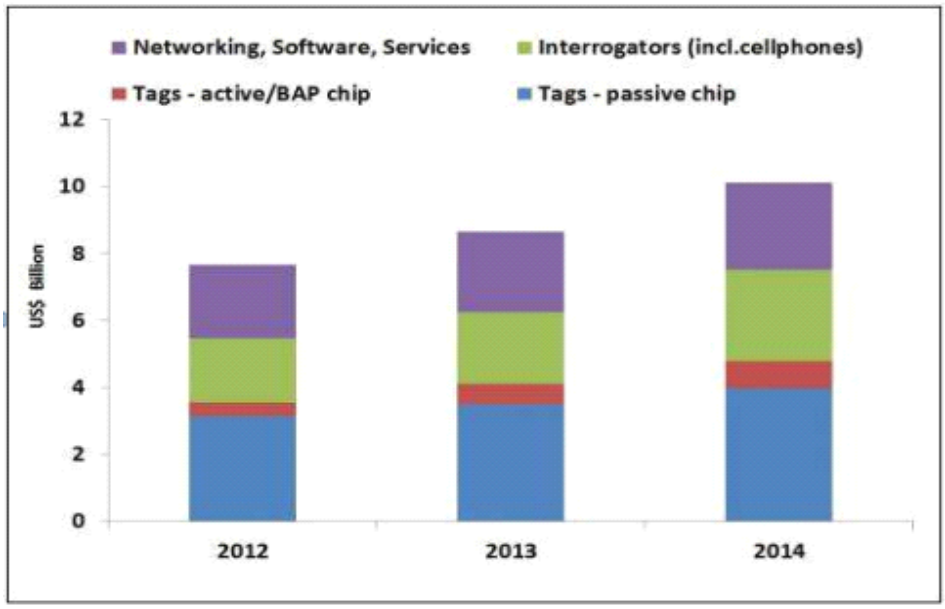


Figure 10: Projection du marché de la RFID en Milliards de dollars [22].

I.3.2 Technologie des cartes à puce :

La technologie des cartes à puce a beaucoup évolué depuis que l'idée d'utiliser des cartes en plastique pour transporter des puces microélectroniques a été brevetée en 1968 par **Dethloff** et **Gro¨trupp**. En juillet 2001, un numéro spécial de Computer Networks était consacré aux cartes à puce, dans le but de passer en revue les problèmes clés et les solutions qui avaient transformé les cartes à puce en ordinateurs à part entière (avec ou sans carte plastique autour de la micro puce). Depuis le tournant du siècle, un autre saut qualitatif a eu lieu et les cartes à puce sont devenues des appareils intelligents, en ce sens qu'elles ont conquis de nouveaux domaines d'application liés à l'informatique généralisée. Sur le haut de gamme, sont apparues des cartes à puce réseau intégrant des fonctionnalités réseau. Les cartes à puce se sont transformées en étiquettes d'identification par radiofréquence (RFID) [29].

Actuellement, les applications de cartes à puce sont utilisées pour encourager et protéger les activités économiques licites; assurer la survie des infrastructures critiques et protéger les individus et les sociétés contre ceux qui voudraient délibérément leur faire du mal. De nombreux facteurs contributifs déterminent le développement et le déploiement de systèmes de cartes à puce. Parmi celles-ci figurent la manière dont les cartes à puce ont été inventées et commercialisées ; orientations actuelles en recherche appliquée et développement ; l'élaboration et le soutien des normes internationales ; et l'impact des préoccupations humaines sur la sécurité et la confidentialité des données [32].

I.3.2.1 Carte à puce :

Une carte à puce (Smart Card), également appelée carte à circuit intégré (ICC) (**Figure 11**), est une carte en plastique intégrée dans une puce qui stocke et transfère des données entre utilisateurs. Ces données sont liées à une valeur ou à une information, ou aux deux. Ces données sont stockées et traitées dans une puce, qu'il s'agisse d'une mémoire ou d'un microprocesseur.

La carte à puce peut être cryptée afin de disposer de nombreuses fonctionnalités de sécurité qui peuvent protéger les données sensibles de cryptage et fournir un environnement de traitement sécurisé [30, 31].

Figure 11: Carte à puce.

I.3.2.2 L'architecture de base d'une carte à puce :

Le développement de circuits intégrés de cartes à puce suit l'évolution de plusieurs technologies de conception différentes. Ces technologies comprennent la technologie des semi-conducteurs, l'intégration de technologies mixtes et les techniques de conception de consommation d'énergie. Le circuit intégré résultant de la carte à puce est un système complexe basé sur un système sécurisé comprenant un cœur de processeur, des blocs IP dédiés, un logiciel intégré natif et des fonctions de gestion de la mémoire et de sécurité [35]. Le cœur d'une carte à puce est une CPU entourée de quatre blocs fonctionnels [34]: ROM, EEPROM, RAM et un port d'E / S (Uart) (voir **Figure 12)**. La carte comprend également des circuits spéciaux pour la sécurité (Crypto) et la gestion de la mémoire (MMU).

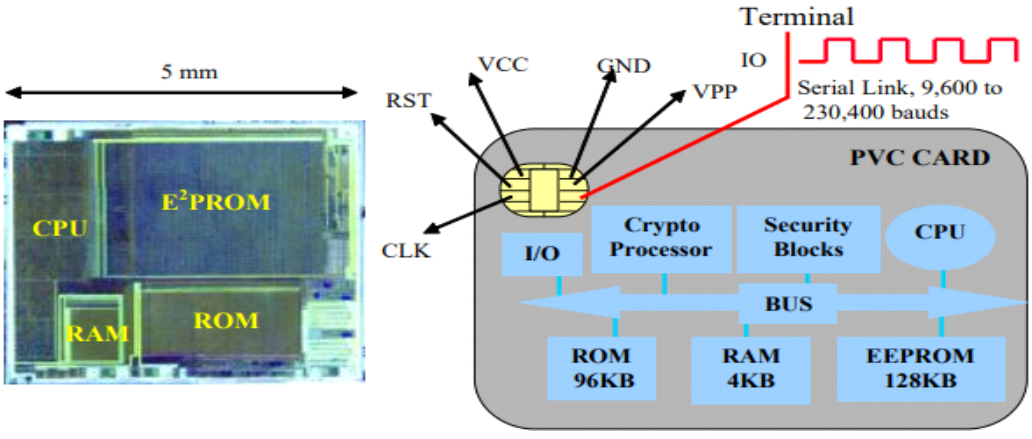


Figure 12: Architecture de base d'une carte à puce [7].

La plupart des conceptions de cartes à puce reposent sur une architecture de microprocesseur 8 bits à usage général.

La **ROM** contient le système d'exploitation de la puce (ou masque) qui a été inséré lors de la fabrication. La **ROM** est efficace en termes d'espace et de consommation électrique. Elle est

également utilisée pour stocker des données fixes, des routines standard et des tables de consultation. Le code et les données placés dans la mémoire morte lors de la fabrication de la carte ne peuvent en aucun cas être modifiés. Le contenu de la **ROM** est statique pendant toute la vie de la puce.

Les **RAM** une mémoire volatile, sont rapides, de petite taille et sont utilisées comme tampons temporaires lors de l'exécution du programme.

Les **EEPROM** une mémoire non volatile, stockent les programmes d'application écrits dans le langage d'assemblage du microprocesseur embarqué. Le système de fichiers utilisé dans **l'EEPROM** est une structure hiérarchique simple avec un seul fichier maître servant de racine du système de fichiers sur chaque carte à puce. Un fichier maître peut contenir plusieurs sous-fichiers. Les données stockées dans **l'EEPROM** peuvent être modifiées par le microprocesseur.

Le port **d'E/S** d'une carte à puce est principalement utilisé pour la communication et l'authentification. Les transferts de données ont lieu sous forme d'octets ou de blocs en mode semi-duplex asynchrone. Les cartes à puce stockent les codes d'accès, les mots de passe et les clés publiques et privées utilisés dans cryptage et authentification [33, 30, 36].

I.3.2.3 Les types de carte à puce :

Il existe deux grandes catégories de carte à puce, avec contact et sans contact, réparties en fonction de la manière dont elles communiquent avec les lecteurs.

I.3.2.3.1 Carte à puce avec contact :

Les cartes à puce à contact ont une zone de contact composée de plusieurs plages de contact plaquées or. Lorsqu'elle est insérée dans un lecteur, la puce établit un contact avec des connecteurs électriques capables de lire des informations à partir de la puce et de les écrire en retour. La **Figure 13** montre les contacts de la puce dans une carte à puce à contact typique. Le **Tableau 1** décrit la description des contacts de la **Figure 13**.

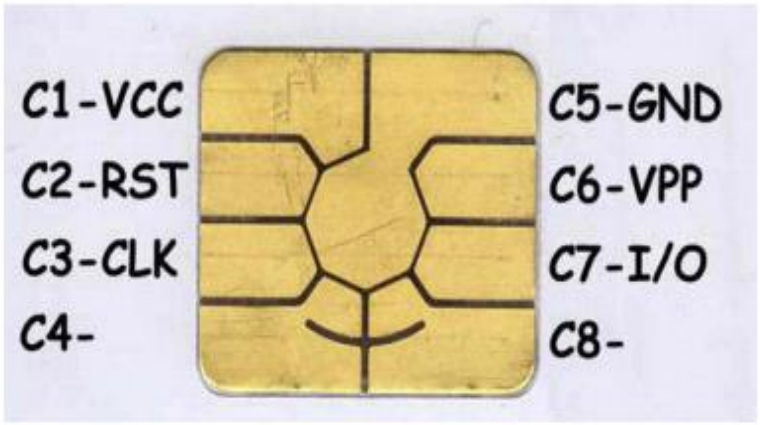


Figure 13: les contacts de la puce dans une carte à puce à contact typique [37].

Contact	Designation	Function
C1	VCC	Supply voltage
C2	RST	Reset input
C3	CLK	Clock input
C4	AUX1	Auxiliary contact 1
C5	GND	Ground
C6	VPP	Programming voltage (no longer used)
C7	I/O	Input/output
C8	AUX2	Auxiliary contact 2

Tableau 1: Description de chaque contact [37].

I.3.2.3.2 Carte à puce sans contact :

Une carte à puce sans contact comme le montre la (**Figure 14).** Comprend un microcontrôleur sécurisé intégré ou une intelligence équivalente, une mémoire interne et une petite antenne et communique avec un lecteur via l'interface RF. La technologie des cartes à puce sans contact est principalement utilisée dans les applications qui doivent permettre des transactions rapides et sécurisées, telles que les cartes de paiement pour le transport en commun, les cartes d'identité gouvernementales et d'entreprise, des documents tels que les passeports et visas électroniques et les cartes de paiement.

Les systèmes de cartes à puce sans contact sont très similaires aux systèmes de cartes à puce à contact. À l'instar des systèmes à carte à puce à contact, les informations sont stockées sur une puce. La différence est que la puce d'une carte à puce sans contact est incorporée dans le corps en plastique, tandis que la carte à puce à contact possède une puce exposée. Ainsi, la puce de

la carte à puce sans contact est mieux protégée que la carte à puce à contact. Dans la carte à puce sans contact, l'énergie fournie à la carte ainsi que l'échange de données entre la carte et le lecteur sont obtenus sans utiliser des contacts, les champs magnétiques ou électromagnétiques générés par le lecteur alimentent à la fois la carte et le serveur comme canal de communication.

Comme tous les appareils adoptent la technologie radio, la carte à puce sans contact contient une antenne également intégrée dans le corps en plastique de la carte (ou dans un porte-clés, une montre, une étiquette ou du papier). Lorsque la carte est insérée dans le champ électromagnétique du lecteur, l'antenne est alimentée par le champ électromagnétique, puis la puce de la carte est sous tension. Une fois la puce mise sous tension, un protocole de communication sans fil est lancé. Une fois la partie authentification du protocole terminée, le canal de transfert de données est établie entre la carte et le lecteur [37].

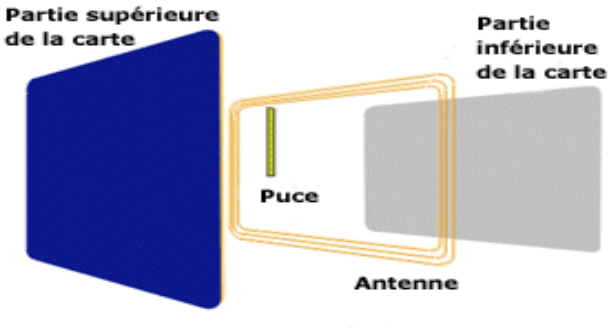


Figure 14: L'intérieur de carte à puce sans contact.

I.3.3 Système d'étiquette RFID active :

Ce qui nous intéresse dans cette recherche, c'est la réduction de la consommation d'énergie dans les systèmes embarqués faible puissance, c'est pour cette raison qu'on a choisi la technologie RFID, notamment les RFID alimentée par batterie **(active)** parmi les technologies que nous avons étudiées auparavant.

Une étiquette RFID est appelée étiquette active lorsqu'elle est alimentée par une batterie pouvant servir de source d'alimentation partielle ou complète pour les circuits et l'antenne de l'étiquette. La **Figure 15** illustre le concept de base d'une étiquette RFID active constituée de composants tels qu'émetteur-récepteur (transceiver), microcontrôleur pour le contrôle des

transactions de données, une batterie pour l'alimentation et une antenne comme support de conversion en onde électromagnétique [39].

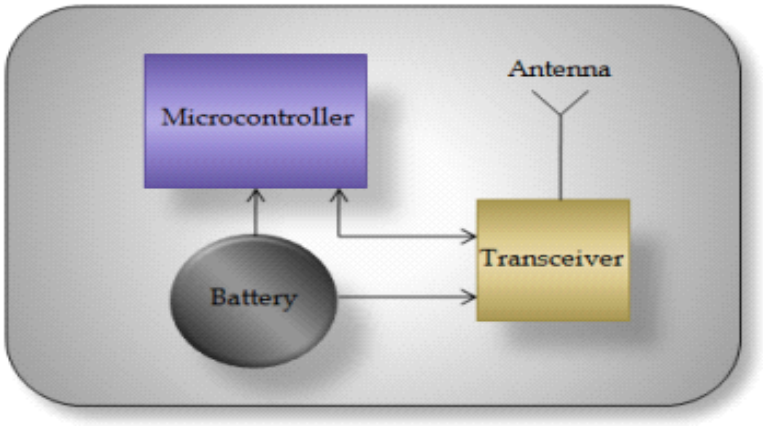


Figure 15: Concept de base d'une étiquette RFID active [39].

Après un test comparatif (test de benchmark) des caractéristiques de plusieurs microcontrôleurs, le Texas Instruments **MSP430** a été sélectionné, car il possède trois modes de consommation de puissance différents, une mémoire interne de 55 Ko et 5 Ko de RAM et la possibilité d'être alimenté par deux tensions différentes, tant en numérique qu'en analogique [40]. L'ADC doit être alimenté à 2,2 V ou plus. Pour cette raison, une batterie est utilisée pour alimenter la partie analogique. La partie numérique est alimentée en 1,8V afin de réduire la consommation électrique [41].

Chapitre II

➢ Les techniques de la réduction de la consommation d'énergie des systèmes embarqués à faible puissance.

II Introduction :

Lors du développement d'un système embarqué de faible puissance, l'attention des concepteurs est concentrée sur la minimisation de la puissance dissipée par les circuits et les interfaces qui effectuent les calculs, le stockage et le transfert / la communication de données. Des modèles de puissance précis et efficaces pour les circuits numériques à différents niveaux d'abstraction ont été développés pour faciliter l'exploration de l'espace de conception. Malheureusement, beaucoup moins d'attention a été consacrée aux modèles d'alimentation. Dans de nombreux cas, il est implicitement supposé que l'alimentation fournit une tension constante et fournit une quantité d'énergie fixe. Cette hypothèse n'est pas valable dans le cas des appareils à piles.

Même si la dissipation de puissance est une préoccupation majeure dans la conception des appareils électroniques portables, les spécifications de haut niveau ne sont pas données en termes de puissance moyenne maximale (ou d'énergie), mais plutôt en termes de durée de vie minimale de la batterie. De plus, l'exigence de portabilité impose des contraintes strictes sur le poids maximal de la batterie. Pour ces raisons, les applications portables réussies associent des techniques de conception à faible consommation avec une sélection rigoureuse des batteries et une conception de l'alimentation.

Pour cela, la consommation et la durée de vie de la batterie comptent parmi les préoccupations les plus critiques des systèmes embarqués légers. Améliorer les performances de la vie de la batterie a toutefois toujours constitué un défi scientifique majeur pour les chercheurs. Afin d'optimiser la consommation d'énergie de tels systèmes, les chercheurs doivent d'abord comprendre les principales sources de consommation d'énergie que nous étudierons dans ce chapitre.

II.1 Propriétés de conception basse consommation :

La plupart des concepteurs sont réellement préoccupés par la réduction de la consommation d'énergie. En effet, les batteries ont une alimentation en énergie finie. L'énergie est l'intégrale de la puissance dans le temps ; si la consommation d'énergie est une constante, l'énergie est simplement la puissance multipliée par le temps pendant lequel elle est consommée. Réduire la consommation d'énergie ne permet d'économiser de l'énergie que si le temps requis pour accomplir la tâche n'augmente pas trop.

Nous définissons l'efficacité énergétique **e** comme la dissipation d'énergie nécessaire pour remplir une certaine fonction, divisée par la dissipation d'énergie totale réellement utilisée [59].

$$e = \frac{\text{la dissipation d'énergie nécessaire pour une certaine fonction}}{\text{la dissipation d'énergie totale réellement utilisée}}$$

II.1.1 Flux de conception :

Le flux de conception d'un système comprend différents niveaux d'abstraction. Lorsqu'un système est conçu en mettant l'accent sur l'optimisation de la puissance comme objectif de performance, la conception doit intégrer l'optimisation à tous les niveaux du flux de conception. En général, il y a trois niveaux auxquels la réduction d'énergie peut être incorporée. Le niveau du système, le niveau de l'architecture et le niveau technologique. Par exemple, au niveau du système, les modules inactifs peuvent être désactivés pour économiser de l'énergie. Au niveau architectural, un matériel parallèle peut être utilisé pour réduire l'interconnexion globale et permettre une réduction de la tension d'alimentation sans dégrader le débit du système. Au niveau technologique, plusieurs optimisations peuvent être appliquées au niveau de la porte (gate).

II.1.2 Modèle CMOS :

II.1.2.1 Les principales sources de la consommation d'énergie :

De nos jours, la technologie TTL (transistor transistor logique) tend à être remplacée par la technologie CMOS (Complementary Metal Oxyde Semiconductor), la plupart des composants sont fabriqués à l'aide de cette technologie. À mesure que la technologie du circuit CMOS évolue, de nouvelles possibilités se présentent pour la production en série d'étiquettes actives à bas prix et à longue durée de vie [77]. La CMOS statique est l'un des styles de circuit les plus populaires pour les systèmes numériques VLSI intégration à très grande échelle (est une technologie de circuit intégré dont la densité d'intégration permet de supporter plus de 100 000 composants électroniques sur une même puce) [48]. Les sources de consommation d'énergie sur une puce CMOS peuvent être classées en dissipation d'énergie (Le taux d'énergie qui est pris à la source et converti en chaleur) [69] statique et dynamique comme montré dans la **Figure 15**. La consommation d'énergie statique est causée par la puissance de fuite (Pleakage). La consommation d'énergie dynamique est causée par la puissance de court-

circuit (Pshort-ciruit) et de commutation (Pswitching), elle est provoquée par l'effort réel du circuit à commuter.

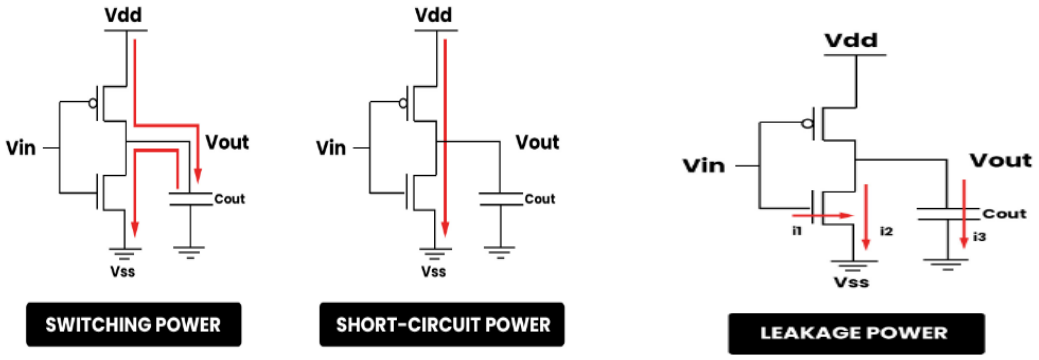


Figure 16: Concept de base d'une étiquette RFID active [39].

Les trois principales sources de dissipation de puissance dans les circuits CMOS numériques sont résumées dans l'équation suivante [42, 43, 44] :

$$Pmoy = Psw + Psc + Pleak$$

$$= \propto 0 \rightarrow 1\ CL \cdot VDD^2 \cdot fclk + Isc \cdot VDD + Ileakage \cdot VDD \qquad \text{(eq01)}$$

Le premier terme représente la puissance de commutation dynamique, Psw, est le composant de dissipation de puissance actif dominant dans les circuits CMOS et résulte de la charge ou de la décharge des charges capacitives effectives comme montré dans la **Figure 16**. Le deuxième terme est la puissance de court-circuit, Psc, due à l'existence d'un chemin de conduction entre l'alimentation et la terre pendant la brève période au cours de laquelle une porte est commutée, elle est généralement faible comparée à Psw. Enfin, le composant de puissance de fuite Pleak, qui peut résulter de l'injection de substrat et d'effets inférieurs au seuil comme montré dans la **Figure 17** (différentes causes de la puissance de fuite, telles que le courant de polarisation inverse I1, le courant de fuite inférieur au canal I2, fuite de réduction de la barrière induite par le drain I3, fuite de drain induite par la porte I4, perforation I5, effet de largeur réduite I6, courant de tunnel d'oxyde de porte I7 et courant d'injection de porteur chaud I8), est principalement déterminé par des considérations de technologie de fabrication. Ces composants de fuite augmentent, devenant un pourcentage plus important de la dissipation moyenne de puissance [44, 45, 46, 47, 48, 52].

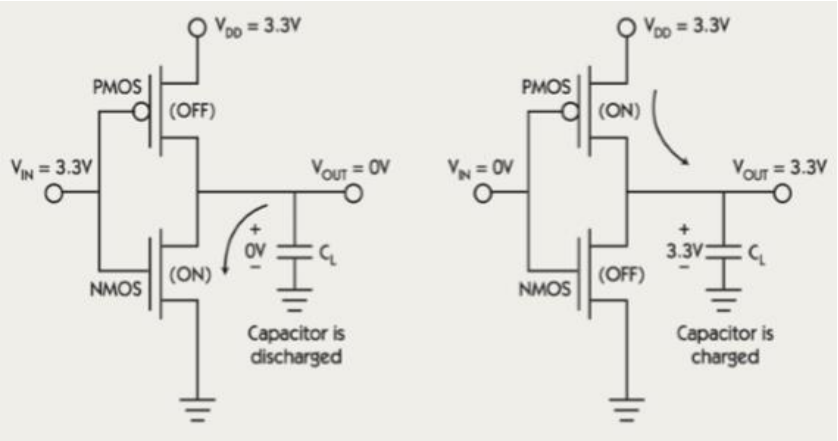


Figure 17 : Les Phénomènes dynamiques dans CMOS: pertes d'énergie dans les condensateurs [52].

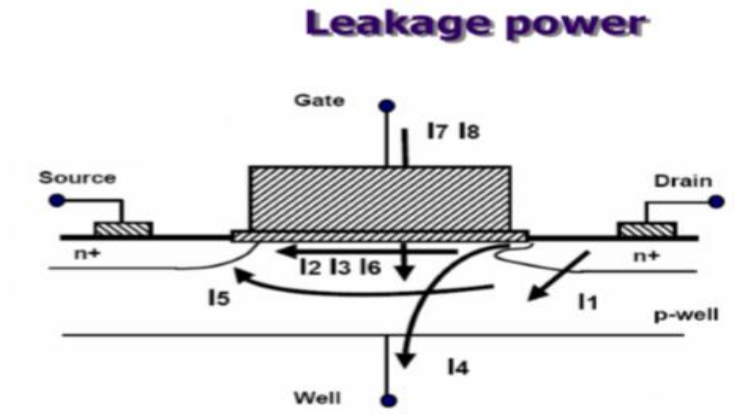


Figure 18 : Les causes de puissance de fuite [52].

La puissance de commutation dynamique est définie comme :

$$Pdynamique = \frac{1}{T}\int_0^T iDD(t)VDDdt = \frac{VDD}{T}\int_0^T iDD(t)dt = \frac{VDD}{T}[TfswCVDD = CVDD^2fsw$$

Avec $fsw = \propto \cdot f$ alors :

$$Pdynamique = \propto CVDD^2f$$

(eq02)

Où α est l'activité de commutation, CL la capacité de charge, VDD la tension d'alimentation et f la fréquence de fonctionnement. Étant donné que la composante de puissance active principale d'un circuit CMOS est proportionnelle au carré de la tension d'alimentation, la mise à l'échelle de VDD est un moyen très efficace de réduire la dissipation de puissance. La puissance de fuite, Pleak, est proportionnelle à la zone et à la température de l'appareil. Le composant de fuite inférieur au seuil dépend fortement de la tension de seuil du dispositif, Vt,

et devient un facteur important car la mise à l'échelle de la tension d'alimentation est utilisée pour réduire la puissance. Particulièrement pour les systèmes portables avec un rapport élevé entre le mode veille et le mode actif, la puissance de fuite peut être le facteur dominant dans la détermination de la durée de vie de la batterie. Actuellement, les technologies CMOS avancées offrant deux choix de Vt ou plus peuvent être efficaces pour réduire les courants de fuite Ileakage en mode veille [48, 49, 50].

II.1.3 Modèle de batterie :

De nombreux types de piles sont utilisés dans une large gamme d'applications [54]. Ils peuvent être divisés en batteries primaires (non rechargeables) pour les appareils avec pile, et batteries secondaires (rechargeables) pour les appareils sans pile [53].

Avec l'augmentation des fonctions de calcul et de communication souhaitées pour les systèmes mobiles sans fil, la densité énergétique des technologies de batteries existantes est loin de répondre aux besoins. Le **Tableau 2** montre les potentiels énergétiques de la technologie actuelle des batteries [59].

Battery	rechargeable	Wh/kg
Alkaline MnO2	no	130
Li/MnO2	no	210
Zinc Air	no	280
Lead acid	yes	30
Nickel-Cadmium NiCd	yes	40
Nickel-metal hybride NiMH	yes	60
Lithium-ion	yes	60
Methanol fuel cell	yes	6200

Tableau 2: Les potentiels énergétiques de la technologie actuelle des batteries [59].

Le développement, l'accroissement des performances des capacités de ces batteries reste modeste en comparaison avec celles des composants électroniques comme on peut le constater sur la **Figure 18** Cette figure représente l'évolution des performances des composants d'un ordinateur portable. En d'autres termes pour améliorer l'autonomie du nœud, il est nécessaire d'augmenter la taille des batteries, ce qui est contradictoire avec l'intégration voulue pour un microsystème autonome [55].

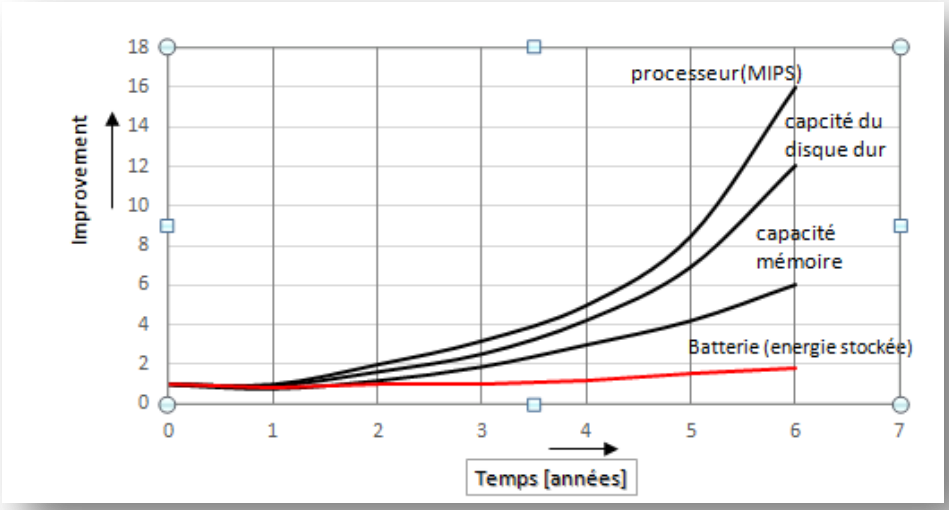


Figure 19: Evolution des différents composants d'un ordinateur portable [13].

Dans la **Figure 19**, nous comparons la densité d'énergie (Wh / kg) des trois compositions chimiques lithium-ion et nous les comparons à l'acide de plomb traditionnel, nickel-cadmium, nickel-hydrure métallique. On peut constater l'amélioration progressive du manganèse et du phosphate par rapport aux technologies plus anciennes. Le cobalt offre la densité d'énergie la plus élevée, mais il est moins stable thermiquement et ne peut pas délivrer de courants de charge élevés.

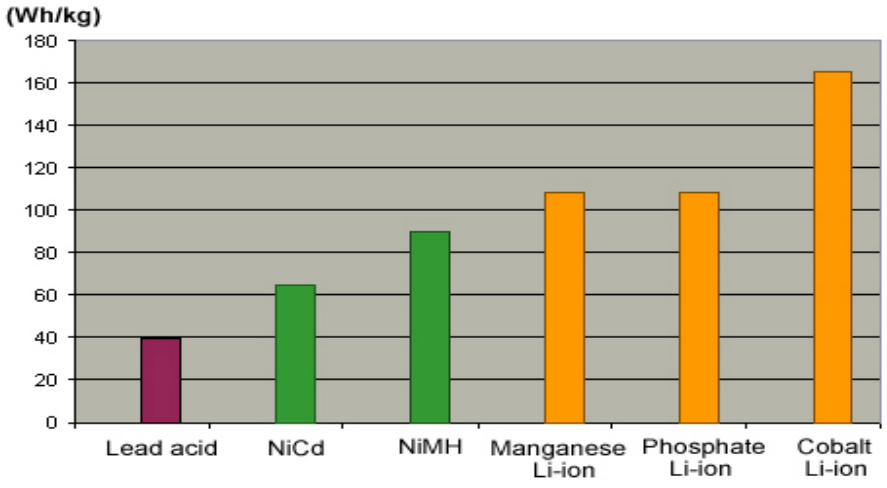


Figure 20: Densités énergétiques des compositions chimiques courantes des batteries.

II.1.3.1 Définition de la densité d'énergie et de la densité de puissance :

La densité d'énergie (Wh / kg) est une mesure de la quantité d'énergie qu'une batterie peut contenir. Plus la densité d'énergie est élevée, plus la durée d'exécution sera longue. Les ions lithium avec cathodes de cobalt offrent les densités d'énergie les plus élevées. Les applications typiques sont les téléphones cellulaires, les ordinateurs portables et les appareils photo numériques. La densité de puissance (W / kg) indique la quantité de puissance qu'une batterie peut fournir à la demande. L'accent est mis sur les pics de puissance, tels que le forage dans de l'acier lourd, plutôt que sur le temps d'exécution. Le lithium-ion à base de manganèse et de phosphate, ainsi que les produits chimiques à base de nickel, figurent parmi les plus performants. Les batteries à haute densité de puissance sont utilisées dans les outils électriques, les appareils médicaux et les systèmes de transport.

Une analogie entre les densités d'énergie et de puissance peut être faite avec une bouteille d'eau. La taille de la bouteille est la densité d'énergie, tandis que l'ouverture (le goulot) indique la densité de puissance. Une grande bouteille peut contenir beaucoup d'eau, alors qu'une grande ouverture peut la déverser rapidement. Le grand récipient à large ouverture est la meilleure combinaison.

II.1.3.2 Durée de vie de la batterie :

La durée de vie de la batterie est une spécification critique pour toute application alimentée par batterie. Les valeurs nominales de la batterie sont exprimées en unités mA -Hr, ce qui signifie que la batterie peut fournir un courant «X» mA pendant une heure. Si nous connaissons le courant moyen, nous pouvons calculer la durée de vie de la batterie [61]:

$$\text{Vie de batterie} = \frac{\text{l'évaluation de la batterie}}{\text{le courant moyen}} \qquad \text{(eq03)}$$

(eq03) donne la durée de vie de la batterie en heures si I moyen est donné en mA.

II.2 Minimisation d'énergie :

II.2.1 Minimisation au niveau technologique :

Les équations 1 et 2 suggèrent qu'il existe essentiellement quatre moyens de réduire la puissance:

1) réduire la charge capacitive C
2) réduire la tension d'alimentation V
3) réduire la fréquence de découpage f
4) réduire l'activité α

II.2.1.1 Minimiser la capacité :

La consommation d'énergie dans les circuits CMOS est proportionnelle à la capacité. Par conséquent, un chemin qui peut être suivi pour réduire la consommation d'énergie consiste à minimiser la capacité. Ceci peut non seulement être atteint au niveau technologique, mais une architecture exploitant la localité de référence et la régularité peut être très profitable. Les connexions aux composants externes ont généralement une capacité beaucoup plus grande que les connexions aux ressources sur puce. Par conséquent, afin d'économiser de l'énergie, utilisez peu de sorties externes et faites-les commuter le moins souvent possible. Par exemple, accéder à la mémoire externe consomme beaucoup d'énergie. Un moyen de réduire la capacité consiste donc à réduire les accès externes et à optimiser le système en utilisant des ressources sur puce telles que des caches et des registres.

La réduction de l'énergie peut donc être atteinte en optimisant la fréquence d'horloge de la conception même si les performances obtenues dépassent de loin les exigences.

Une autre façon de réduire la capacité consiste à réduire la surface de la puce. Cependant, notez qu'une seule réduction de la surface de puce pourrait conduire à une conception inefficace en énergie. Par exemple, une architecture efficace en énergie occupant une plus grande surface peut réduire la consommation énergétique globale.

II.2.1.2 Réduire la tension et la fréquence (DVFS) :

DVFS (Dynamic Voltage Frequency Scaling) est l'un des moyens les plus efficaces de réduire la consommation d'énergie d'un circuit au niveau technologique qui consiste à réduire la tension d'alimentation, car la consommation d'énergie diminue de façon quadratique avec la tension d'alimentation. Par exemple, réduire une tension d'alimentation de 5,0 à 3,3 volts (réduction de 44%) réduit la consommation d'énergie d'environ 56% (**Figure 21**).

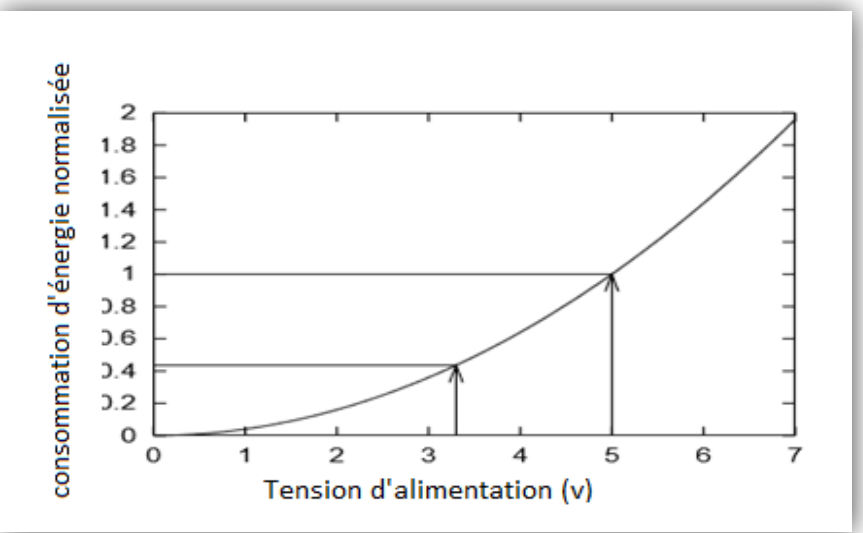


Figure 21: Réduction de la tension d'alimentation de 5,0 à 3,3 volts [58].

Weiser et al. [57] ont proposé un système dans lequel la fréquence d'horloge et la tension de fonctionnement varient de manière dynamique sous le contrôle du système d'exploitation, tout en permettant au processeur de respecter ses délais d'achèvement des tâches. Ils soulignent que pour fonctionner correctement à une tension inférieure, la fréquence d'horloge doit être simultanément réduite [42].

II.2.1.3 Éviter les activités inutiles :

La pondération d'activité α de l'équation 2 peut être minimisée en évitant les activités inutiles. Il existe plusieurs techniques pour y parvenir.

II.2.1.3.1 Contrôle de l'horloge :

Étant donné que la consommation d'énergie du CMOS est proportionnelle à la fréquence d'horloge, il est évident que couper l'horloge de manière dynamique pour activer les périphériques inutilisés est un moyen évident de réduire la consommation d'énergie. Le contrôle peut être effectué au niveau matériel ou peut être géré par le système d'exploitation ou l'application. Certains processeurs et périphériques matériels ont des modes veille ou inactif. Généralement, ils éteignent l'horloge pour toutes les sections sauf certaines afin de réduire la consommation d'énergie. Pendant le sommeil, l'appareil ne fonctionne pas. Un événement de réveil sort le périphérique du mode veille. Les appareils peuvent nécessiter différentes heures pour se réveiller à partir de différents modes de veille. Par exemple, de nombreux modes de «veille profonde» arrêtent les oscillateurs sur puce utilisés pour la

génération d'horloge. Un problème est que ces oscillateurs peuvent nécessiter des microsecondes ou parfois même des millisecondes pour se stabiliser après avoir été activés. Il est donc rentable d'entrer en mode de veille profonde lorsque l'appareil doit rester en veille pendant une période relativement longue [42].

II.2.1.3.2 Minimiser les transitions :

La consommation d'énergie est proportionnelle à la fréquence à laquelle les signaux changent d'état de 0 à 1 ou inversement et à la capacité sur la ligne de signal. Cela est vrai pour chaque chemin de signal dans un système, qu'il s'agisse d'un signal d'horloge, d'une broche de données ou d'une ligne d'adresse. Cela implique que la consommation d'énergie peut être réduite en minimisant soigneusement le nombre de transitions. Dans ce contexte, nous pouvons affirmer qu'un choix correct de la représentation des nombres peut avoir un impact important sur l'activité de commutation. Par exemple, les compteurs de programme dans les processeurs utilisent généralement un code binaire. En moyenne, deux bits sont modifiés pour chaque transition d'état. L'utilisation d'un code Gray **Tableau 3** (est un type de codage binaire permettant de ne modifier qu'un seul bit à la fois quand un nombre est augmenté d'une unité), qui entraînera généralement des modifications sur un seul bit, peut générer des économies d'énergie intéressantes.

Valeur décimale	Code en complément à deux	Code de Gray
0	0000	0000
1	0001	0001
2	0010	0011
3	0011	0010
4	0100	0110
5	0101	0111
6	0110	0101
7	0111	0100

Tableau 3: Code de Gray [60].

II.2.1.3.3 Conception asynchrone :

Une autre façon d'éviter des activités inutiles consiste à appliquer une méthodologie de conception asynchrone. Le CMOS est une bonne technologie à faible consommation d'énergie, car les portes ne dissipent de l'énergie que lorsqu'ils commutent. Cela devrait normalement correspondre au travail utile de la porte, mais malheureusement dans un circuit synchrone, ce n'est pas toujours le cas. De nombreuses portes commutent parce qu'elles sont connectées à l'horloge et non parce qu'elles ont de nouvelles entrées à traiter. La plus grande porte de tous est le pilote d'horloge qui doit distribuer un signal d'horloge uniformément à toutes les parties d'un circuit, et il doit commuter tout le temps pour fournir la référence de synchronisation même si seule une petite partie de la puce a quelque chose d'utile à faire. Un circuit synchrone gaspille donc de la puissance lorsque des blocs de logique particuliers ne sont pas utilisés, par exemple au profit d'une unité à virgule flottante lorsqu'une arithmétique entière est effectuée [59, 42].

II.2.2 Minimisation au niveau µ contrôleur MCU :

Le principal problème relatif à la consommation des systèmes embarqués est l'autonomie. Pour étendre l'autonomie de fonctionnement d'un système, deux méthodes existent : augmenter la quantité d'énergie embarquée ou diminuer la consommation du système. il faudra trouver un compromis entre les deux. Il existe plusieurs méthodes [60] pour obtenir un système à faible consommation.

II.2.2.1 Conception à faible consommation d'énergie utilisant le MSP430 :

II.2.2.1.1 µcontrôleur de Texas Instruments TI MSP430 :

Le MSP430 est le nom d´une famille de microcontrôleurs de la marque Texas Instruments. Il est spécialement conçu pour les applications embarquées à faible consommation d'énergie et alimentées par batterie (Appareils sans fil) comme notre cas ciblé : identification par radio fréquence [64]. Ces derniers embarquent leur propre source d'énergie pour alimenter leurs circuits de communication, leurs capteurs et leur microcontrôleur. Ainsi, le remplacement fréquent de la batterie n'est pas souhaitable. Alors cette partie présente des solutions d'alimentation simples mais efficaces qui réduisent encore la consommation d'énergie du MSP430 et allongent la durée de vie de la batterie [63].

II.2.2.1.1.1 Le schéma fonctionnel :

La famille de microcontrôleurs ULP (Ultra-Low Power) de Texas Instruments MSP430 est composée de plusieurs dispositifs présentant différents ensembles de périphériques destinés à diverses applications. L'architecture, associée à cinq modes basse consommation et un mode actif sélectionnables par logiciel, est optimisée pour prolonger la durée de vie de la batterie dans les applications portables.

Mode actif AM :

-Toutes les horloges sont actives.

Mode basse consommation 0 (LPM0) :

-La CPU est désactivée, ACLK (Horloge auxiliaire) et SMCLK (horloge secondaire) restent actifs.

-MCLK (horloge principale) est désactivé.

Mode basse consommation 1 (LPM1) :

-La CPU est désactivée ACLK et SMCLK restent actifs.

-MCLK est désactivé.

-Le générateur DCO est désactivé si le DCO n'est pas utilisé en mode actif.

Mode basse consommation 2 (LPM2) :

-La CPU est désactivée MCLK et SMCLK sont désactivés.

-Le générateur de courant continu de DCO reste activé.

-ACLK reste actif.

Mode basse consommation 3 (LPM3) :

- La CPU est désactivée MCLK et SMCLK sont désactivés.

- Le générateur DCO est désactivé ACLK reste actif.

Mode basse consommation 4 (LPM4) :

- La CPU est désactivée ACLK est désactivé MCLK et SMCLK sont désactivés.

-Le générateur de courant continu du DCO est désactivé.

-L'oscillateur Crystal est arrêté.

L'appareil dispose d'un processeur puissant (CPU) RISC (Reduce Instruction Set Computer) (est une structure interne d'un processeur) 16 bits, de registres 16 bits et de générateurs constants qui optimisent l'efficacité du code. L'oscillateur à commande numérique (DCO) permet de passer des modes basses consommation au mode actif en moins de 6µs. Les séries MSP430x11x2 et MSP430x12x2 sont des microcontrôleurs à signaux mixtes ultra-faible avec une minuterie intégrée de 16 bits, un convertisseur A / N de 10 bits avec un contrôleur de transfert de référence et de données (DTC) intégré et de 14 ou 22 broches d'E / S. De plus, les microcontrôleurs de la série MSP430x12x2 ont une capacité de communication intégrée utilisant les protocoles asynchrone (UART) et synchrone (SPI) (**Figure 22**) [64].

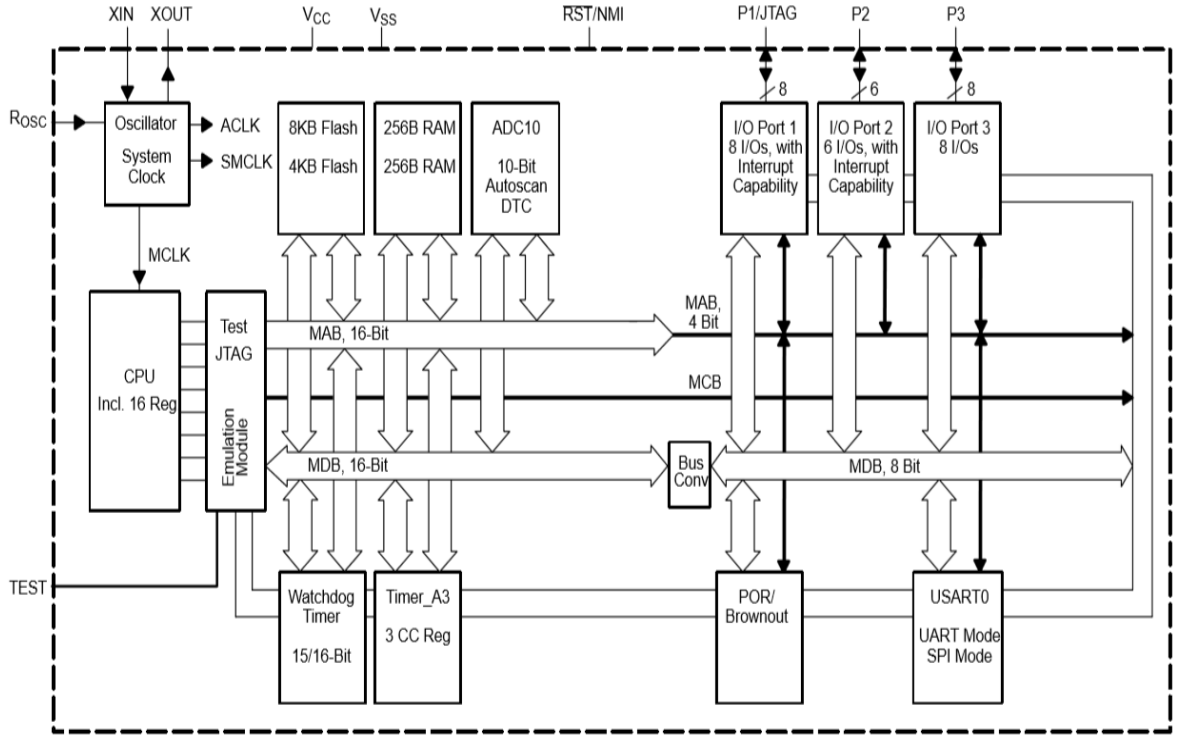


Figure 22: Schéma fonctionnel de MSP430FX12X2 [64].

II.2.2.2 Les techniques de réduction d'énergie au MCU :

Pour minimiser la consommation d'énergie du système à microcontrôleur, un développeur doit prendre en compte quatre catégories d'alimentation principales :

II.2.2.2.1 Energie en mode veille (Standby) :

Les applications de microcontrôleur classiques passent la majeure partie de leur vie en mode veille à faible consommation d'énergie, en attendant qu'un événement interne ou externe

réveille le processeur pour qu'il traite les données, prenne des décisions et communique avec les autres composants du système. Dans de nombreuses applications alimentées par batterie, l'alimentation de veille consomme la plus grande quantité d'énergie AM (Active mode) **Figure 23** montre la consommation de courant en mode fonctionnement (mode active) et en mode veille.

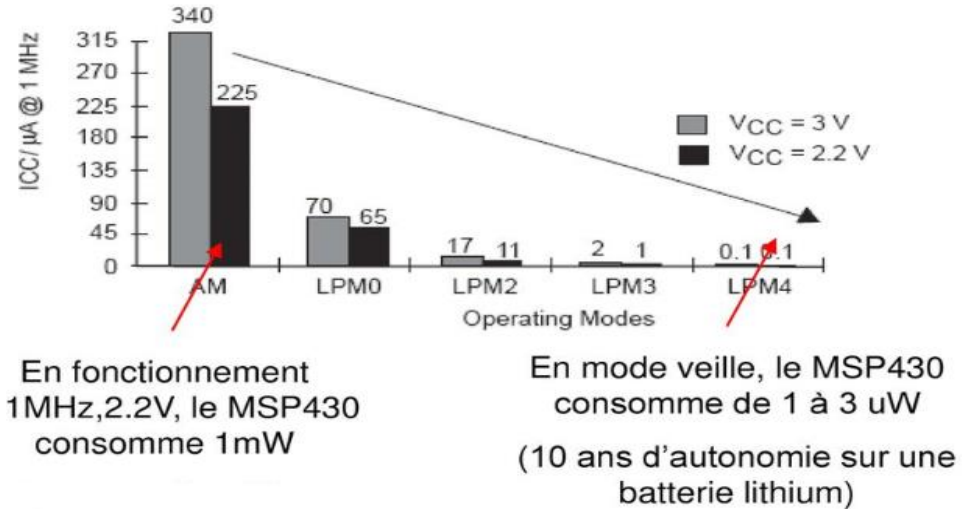


Figure 23: Consommation de courant typique [68].

Il est courant que les développeurs lancent leur analyse de la puissance du processeur en prenant en compte la puissance de traitement active. Bien que cela puisse sembler contre-intuitif, la puissance consommée par le microcontrôleur lorsqu'il ne fonctionne pas est souvent plus importante que la puissance de traitement active. Pour l'application de télédétection, le système sort du mode veille toutes les trois secondes. Le système est donc en mode veille plus de 99% du temps.

II.2.2.2.1.1 Réveil automatique sur les intervalles de temps :

Les microcontrôleurs modernes offrent souvent des horloges en temps réel (RTC) pouvant fonctionner en mode veille à faible consommation d'énergie, ce qui permet au microcontrôleur de se réveiller automatiquement à des intervalles de temps spécifiés. Par exemple l'application de télédétection utilise cette capacité pour se réveiller une fois toutes les trois secondes afin de mesurer des données analogiques. Il est important de comprendre le courant requis pour faire fonctionner le RTC en mode veille, car cela peut représenter une part importante du courant en veille.

II.2.2.2.1.2 Rétention de la RAM en veille :

Maintenir le contenu de la RAM en veille permet aux microcontrôleurs de se réveiller rapidement sans exécuter de code de démarrage qui consomme une énergie précieuse. Cela économise de l'énergie et du temps pour une latence plus faible du système. Le courant requis pour activer les modes de rétention de la RAM peut être important et doit être examiné avec considération.

II.2.2.2.1.3 Capacités d'interruption :

Les microcontrôleurs peuvent souvent laisser certains périphériques actifs en mode veille, ce qui permet au microcontrôleur de se réveiller rapidement avec certains événements tels qu'une commande UART (émetteur-récepteur asynchrone universel utilisé pour faire la liaison entre l'ordinateur et le port série) ou une interruption GPIO (Entrée-sortie à usage général). L'exemple de télédétection surveille en permanence deux à trois lignes GPIO afin de réveiller le processeur pour une activité instantanée.

II.2.2.2.1.4 Surveillance de la puissance :

Brown Out Reset (BOR) (est automatiquement mis le processeur en réinitialisation si le courant entrant dans la puce n'est pas suffisant pour fonctionner de manière fiable.) et Supply Voltage Supervisor (SVS) (utilisé pour surveiller la tension d'alimentation des systèmes à microcontrôleurs intégrés et autres dans des conditions de tension insuffisante) sont des circuits importants permettant de surveiller l'intégrité de la source d'alimentation du microcontrôleur. Les défaillances et les interruptions de la source d'alimentation du microcontrôleur peuvent avoir une incidence sur la fiabilité du fonctionnement. Il est essentiel d'inclure ces courants dans les estimations de courant en veille. Cela ne peut ajouter que quelques nano ampères et jusqu'à 500 microampères aux numéros en veille.

II.2.2.2.1.5 Température :

Les systèmes à faible puissance négligent souvent la température, mais les processus modernes à semi-conducteurs génèrent souvent des courants de fuite beaucoup plus élevés à des températures plus élevées - dans certains cas 10 à 15 fois plus de courant en veille entre 25 ° C et 85 ° C.

II.2.2.2.2 Puissance des périphériques :

Les microcontrôleurs, tels que les périphériques MSP430FR59xx de TI, ont été conçus pour optimiser la consommation en veille en utilisant des fonctionnalités avancées de couplage de la puissance et de l'horloge, des conceptions de circuits analogiques à très faible consommation et des avancées en matière de technologie silicium, telles que la mémoire FerroElectricRAM FRAM (est une technologie de mémoire non volatile particulièrement flexible qui peut être utilisée pour la mémoire de programme ou de données). Dans le cas de l'application de détection à distance, le microcontrôleur MSP430FR59xx peut activer le mode veille RTC avec rétention de mémoire vive, capacité d'interruption SVS / BOR et GPIO pour aussi peu que 500 nano ampères. Pour de nombreuses applications alimentées par batterie faible consommation, l'alimentation en veille peut être le principal impact sur la durée de vie de la batterie. Il est donc essentiel que les développeurs prennent en compte l'impact des fonctionnalités requises par l'application sur le courant en veille. Cela peut faire une différence en termes d'années de vie de la batterie ou d'économiser sur le coût du système en utilisant une batterie de capacité inférieure moins chère. Dans l'exemple de la télédétection, le courant de veille moyen peut être estimé comme suit (eq04):

$$\text{Imoyenne Veille} = \text{IVeille} \cdot \left(\frac{\text{TVeille}}{\text{Ttotal}}\right) = \left(\frac{2.997s}{3s}\right) \cdot 0.5\mu\text{A} = 0.4995\mu\text{A} \qquad \text{(eq04)}$$

II.2.2.2.3 Puissance d'enregistrement des données :

La plupart des applications de microcontrôleur enregistrent les données pour analyse ou transmission ultérieure. Ces données sont enregistrées dans une mémoire non volatile (mémoire qui conserve ses données en l'absence d'alimentation électrique.) du microcontrôleur. Selon la fréquence et la quantité de données à enregistrer, la journalisation des données peut avoir un impact important sur la durée de vie de la batterie. De nombreuses applications de microcontrôleurs doivent enregistrer les mesures et les données pour une utilisation ultérieure dans l'application. Par exemple, les données les plus récentes pourraient être comparées aux données antérieures enregistrées pour rechercher des tendances plus larges. L'enregistrement des données sur le capteur lui-même peut également fournir aux utilisateurs des informations critiques dès le moment de la défaillance, comme dans le cas de disjoncteurs intelligents ou de boîtes noires pour véhicules. L'enregistrement de données peut être extrêmement difficile lorsque vous utilisez une petite batterie peu coûteuse. Le courant nécessaire pour effacer et programmer le flash peut varier de 4 à 12 mA. Cela ne peut pas être

directement recherché par des piles bouton ayant un courant maximal de 3 à 4 mA. En outre, de telles opérations prennent plus de deux douzaines de millisecondes pour mettre en place et effacer la mémoire avant la programmation, puis à peu près au même moment pour écrire le secteur de Flash requis. De plus, si une mémoire externe est utilisée pour le stockage, l'utilisation de l'interface de communication série pour transférer des données entraîne des frais supplémentaires. Cela ajoute une consommation de courant périphérique et active au système. Cela est important car cela signifie que vous devez utiliser une batterie plus grosse et plus chère, ou une mémoire externe de faible puissance doit être ajoutée à la conception. Ce sont des options coûteuses et parfois difficiles à mettre en œuvre en raison de contraintes de taille. Un autre point clé est que la consignation de données à des vitesses plus lentes en FRAM réduit considérablement la consommation actuelle. La journalisation des données à un taux relativement rapide de 13 kilo-octets par seconde peut atteindre 9 µA. C'est environ 500 fois moins que le même taux avec Flash.

$$Imoy\ data = T\ data \cdot \left(\frac{Idata}{Ttotal}\right) = 0.0012s \cdot \frac{9\mu A}{3s} = 0.0036\mu A \qquad \text{(eq05)}$$

Assumptions: 16 bytes at 13kBps is 0.00128s at 9µA

(Benchmark Measure ou mesure de référence)

II.2.2.2.4 Puissance active :

Comprendre l'alimentation lorsque le processeur est en cours de traitement est essentiel pour maximiser la durée de vie de la batterie.

$$Energie\ total = Energie\ active + Energie\ en\ mode\ vielle$$
$$T \cdot I \cdot V = Tactive \cdot Iactive \cdot V + Tvielle \cdot Iveille \cdot V \qquad \text{(eq06)}$$

Pour les applications alimentées par batterie, 3V est la tension nominale typique de la batterie. C'est également la tension à laquelle de nombreux numéros de consommation d'énergie sont spécifiés dans les fiches techniques.

La puissance active du CPU est souvent considérée comme le plus gros consommateur d'énergie dans les applications alimentées par batterie. Cela dit, il est important que le logiciel et le matériel du microcontrôleur soient optimisés afin de minimiser la puissance active afin de tirer parti des périphériques intelligents et d'utiliser des modes d'alimentation en veille moins énergivores.

II.2.2.2.4.1 Exécution du logiciel à partir du RAM :

Les développeurs doivent examiner avec soin si le logiciel est exécuté à partir de mémoires non volatiles ou de RAM pour estimer la consommation actuelle. L'exécution à partir de la RAM peut offrir des spécifications de courant actif inférieures. Cependant, de nombreuses applications ne sont pas assez petites pour être exécutées à partir de la RAM uniquement et nécessitent que les programmes soient exécutés à partir de la mémoire non volatile.

II.2.2.2.4.2 Accélération :

Les microcontrôleurs faibles consommation utilisent généralement des accélérateurs qui réduisent le nombre de cycles et l'énergie requise pour des tâches spécifiques. Par exemple, le cryptage AES256 (processus qui transforme des données en une forme qui peut uniquement être lue par le destinataire prévu.) peut nécessiter jusqu'à 7 000 cycles de processeur sans accélération. Avec les accélérateurs matériels, le même chiffrement peut prendre environ 500 cycles de traitement. Dans ce cas, l'accélération matérielle peut réduire le temps de traitement actif de plus de 10 fois [67].

II.2.2.2.4.3 Optimisation de code :

Le code du microcontrôleur peut être optimisé pour une durée d'exécution plus courte en utilisant une structure de code intelligente et des optimisations du compilateur. Bien que la consommation due à l'exécution d'un programme soit difficile à estimer, il existe une relation entre le nombre d'instructions exécutées et la consommation. D'une manière générale, plus le nombre d'instructions est élevé, plus la consommation est importante, les techniques d'optimisation logicielles peuvent donc aider à diminuer cette consommation [67, 9].

II.2.3 Minimisation d'énergie au RFID système :

II.2.3.1 Système matériel de l'étiquette RFID active :

II.2.3.1.1 Microcontrôleur du système étiquette actif :

Le cadre du système RFID actif est illustré à la **Figure 24**. Il est composé d'un module RF, d'un microcontrôleur MSP430 et d'une alimentation. Ce système utilise le MCUMSP430 à faible consommation d'énergie de TI, qui est un système sur puce en tant que contrôleur. La tension est comprise entre 1,8V et 3,6V. 3V est choisi par ce système. Le courant de rétention de la RAM est de 0,1 µA; un courant en mode horloge temps réel est O.8µA; Le courant de

l'état actif est de 250µA/MIPS. L'architecture MSP430 ultra basse consommation prolonge la vie de la batterie [65].

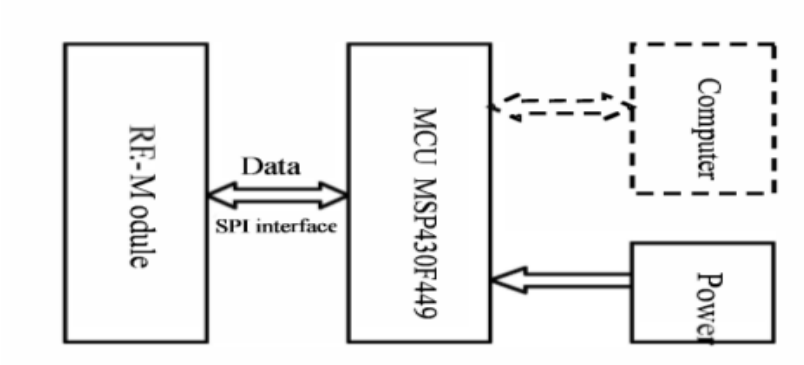


Figure 24: Système RFID active utilisant le MSP430 [65].

II.2.3.1.2 Module RF d'étiquette active :

La **Figure 25** montre la géométrie de l'antenne boucle rectangulaire, a_1 est la longueur de l'antenne, a_2 est la largeur de l'antenne, b_1 est l'épaisseur du conducteur de boucle, et b_2 est la largeur du conducteur de boucle.

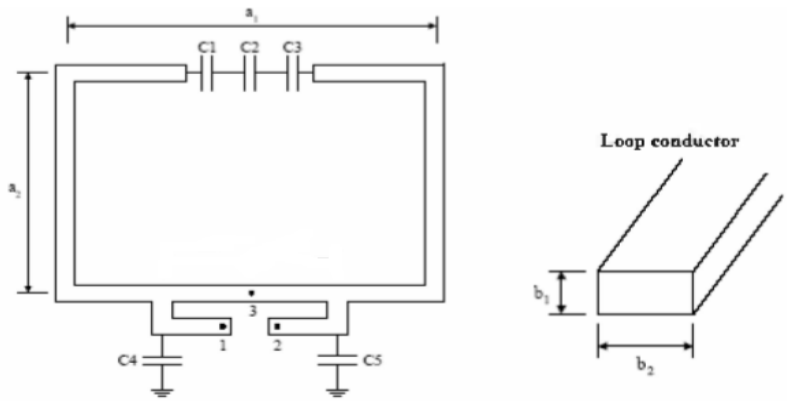


Figure 25: Géométrie de l'antenne boucle rectangulaire [65].

Le module de transmission RF de l'antenne boucle rectangulaire est basé sur le nRF905 (est un émetteur-récepteur radio mono puce pour la bande ISM 433/868/915 MHz) du semi-conducteur nordique (société spécialisée dans les systèmes sans fil ultra-basse consommation sur puce (SoC)) est utilisé pour la transmission sans fil dans la couche physique. La plage d'alimentation est de 1,9V à 03,6V. La consommation de courant est très faible. En émission, le courant n'est que de 9 mA. Le mode ShockBurst ™ de nRF905 permet d'utiliser le débit de données élevé offert par le nRF905 sans le recours à un microcontrôleur coûteux et à grande

vitesse pour le traitement des données et la récupération de l'horloge. Le mode ShockBurst ™ nRF905 réduit la consommation de courant moyenne dans les applications [65].

II.2.3.1.3 Communication entre RF-Module et MCUMSP430 :

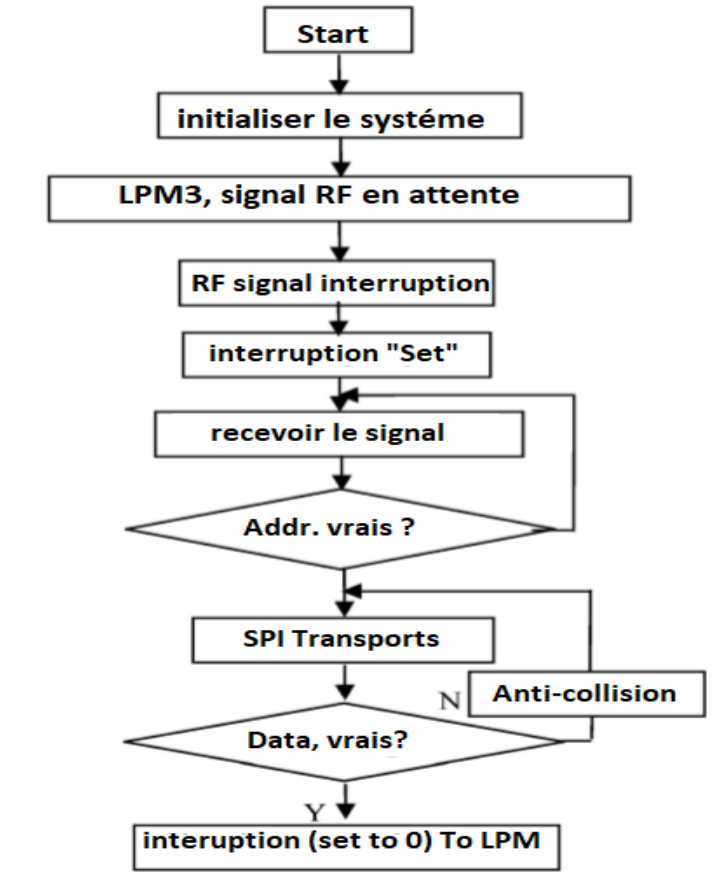


Figure 26: Logiciel d'identification dans le cadre du système RFID actif [65].

La Figure 26 montre le module RF en communication avec le MCUMSP430. RF-Module est connecté aux broches d'interruption. S'il n'y a pas de signaux d'interruption, le MSP430 et le module RF sont à l'état de faible puissance.

Avant l'enregistrement sur le système d'authentification, le module de transmission RF est en mode veille prolongée. Après l'enregistrement, un aimant est utilisé pour entrer le signal de déclenchement afin d'initier le module de transmission RF. De plus, le MSP430 est configuré pour fonctionner en mode d'économie d'énergie LPM3 (0,9 μA) et l'interruption d'horloge interne de la puce de contrôle principale est utilisée pour transmettre des trames de données uniquement à un moment prédéterminé afin d'obtenir le meilleur effet d'économie d'énergie[66].

II.2.3.2 Les techniques de réduction d'énergie des systèmes RFID actifs :

II.2.3.2.1 Les problèmes :

La technologie RFID active pose plusieurs problèmes :

Le premier problème est les pertes de dissipation d'énergie et la nécessité des fonctions de sécurité basse consommation.

Le deuxième problème est l'efficacité énergétique des protocoles RFID actifs.

II.2.3.2.1.1 La dissipation d'énergie des systèmes RFID actifs :

Un émetteur-récepteur (Tranceiver) et un contrôleur sont deux composants dominants d'une étiquette RFID active traditionnelle. Deux sources importantes de dissipation d'énergie peuvent être observées lors du fonctionnement d'étiquettes RFID actives, en termes de consommation d'énergie de l'émetteur-récepteur et du µcontrôleur. L'une des sources importantes de consommation d'énergie est la nécessité de mettre l'émetteur-récepteur sous tension en permanence afin de recevoir tout signal entrant. Comme l'interrogateur RFID domine la communication, chaque communication sera initiée par le lecteur. L'énergie consommée par un récepteur (Er) est proportionnelle au temps (Tr) de mise sous tension du récepteur, si la consommation d'énergie du récepteur (Pr) est constante, indiquée dans (eq07). La solution pour réduire l'énergie consommée dans le récepteur (Er) consiste à compresser Tr.

$$E_r = E_r^s + E_r^a = P_r^s \cdot T_r^s + P_r^a \cdot T_r^a$$

$$K = T_r^s + T_r^a \qquad \text{(eq07)}$$

$$E = E_c^s + E_c^a = P_c^s \cdot T_c^s + P_c^a \cdot T_c^a = P_c^s \cdot T_c^s + P_c^a \cdot (T_{sc} \cdot N_c)$$

$$K = T_c^s + T_c^a \qquad \text{(eq08)}$$

a : mode active et s : standby mode (mode veille)

L'autre partie importante de la dissipation d'énergie provient du µcontrôleur. Un microcontrôleur a besoin de 2,2 à 8 mA pour rester en mode actif et seulement de 1 à 15 µA

pour rester en mode veille. Cependant, dans les systèmes RFID, le microcontrôleur d'une étiquette active est réveillé par les commandes entrantes destinées à d'autres étiquettes.

(Eq8) montre l'énergie consommée par le µcontrôleur pour une étiquette RFID active. L'énergie générée a été abandonnée à la suite de l'estimation de (E_c^s) et (E_c^a). La consommation actuelle du contrôleur est en mode veille, ce qui peut être atteint par la consommation électrique (P_c^s) fois la durée (T_c^s). Et $E_c^a = P_c^a \times T_c^a$ présente l'énergie consommée par un contrôleur lorsqu'il est activé, où P_c^a illustre la consommation d'énergie lorsqu'un µcontrôleur est en mode d'activation et T_c^a indique la durée de traitement des commandes par un contrôleur. La variable de temps, T_c^a, est déterminée par le nombre de commandes traitées (Nc) et le temps de traitement d'une commande unique (T_c^s).

II.2.3.2.1.2 Sécurité et énergie :

Les étiquettes RFID traditionnelles fournissent des fonctionnalités de sécurité en activant leur µcontrôleur avec une consommation d'énergie croissante. Cette situation crée un équilibre entre la sécurité et l'énergie. Cependant, les systèmes RFID requièrent la sécurité, car ils doivent être mis en œuvre de manière à offrir un degré de protection élevé sans augmenter de manière significative la complexité du système. La complexité peut augmenter la consommation d'énergie et les coûts de mise en œuvre.

Model	PIC18F6720	MSP430F16x	ATmega128L
Frequency (MHz)	20	8	8
Word size (bit)	8	16	8
Power (awake; *mA*)	2.2	2	8
Power (Sleep; *µA*)	1	1.1	15

Tableau 4: Exigences d'alimentation des microcontrôleurs.

Tableau 4 Listes des microcontrôleurs utilisés pour la création de prototypes de RFID actifs dans les produits commerciaux sans fil [73, 74, 75]. Une étiquette active doit fournir une puissance adéquate, de 2 mA à 8 mA, pour fournir à un microcontrôleur suffisamment d'énergie pour exécuter des fonctions de sécurité.

II.2.3.2.1.3 Efficacités énergétique des protocoles RFID actifs :

La consommation d'énergie est un paramètre critique dans un système RFID actif. Une étiquette se trouve dans l'un des deux états suivants : à la portée d'un lecteur ou à l'extérieur d'un lecteur. Une étiquette doit pouvoir fonctionner de manière économe en énergie dans ces deux états. Le protocole doit prendre en charge les modifications du cycle de réveil, c'est-à-dire la fréquence à laquelle une étiquette sort de l'état de veille et peut être découverte par un lecteur. Plus loin, le cycle de réveil est appelé "cycle". Le choix de la durée du cycle est un compromis entre maintenir la consommation d'énergie au minimum et disposer d'une latence acceptable dans la découverte par le lecteur. Les exigences relatives à la topologie du réseau diffèrent également entre les systèmes RFID et les réseaux de capteurs. La technologie RFID active est une application très orientée connexion et la topologie peut être considérée comme une topologie en étoile très dynamique. Un réseau de capteurs, d'autre part, stocke les informations et les stocke pour les transmettre ultérieurement à un lecteur RFID. En outre, la plage de lecture et la directivité sont améliorées par rapport à la RFID passive, en raison de la puissance de sortie plus élevée de l'étiquette émettrice et également du fait qu'un récepteur plus sensible peut être construit dans l'étiquette. L'inconvénient est que l'utilisation de circuits actifs limite la durée de vie de l'étiquette active par rapport à celle du passif. La liaison RF sans fil est la partie qui consomme le plus d'énergie. Par conséquent, pour prolonger la durée de vie de la batterie d'une étiquette active, un protocole économe en énergie pour Active RFID doit être utilisé.

II.2.3.2.2 Des solutions :

II.2.3.2.2.1 Etiquette RFID active-passive :

Une architecture innovante pour les étiquettes RFID actives appelée étiquette RFID active-passive, illustrée dans la **Figure 27**, qui intègre les avantages des étiquettes RFID passives et actives. Il est conçu pour une solution RFID basse consommation, longue portée et sécurisée [81]. Dans cette partie, il est proposé cinq contributions qui étudient comment réduire la consommation d'énergie des étiquettes RFID actives passives, comment augmenter le niveau de sécurité des données pour les communications RFID avec une limitation de puissance minimale et comment calculer la consommation d'énergie des transactions de données RFID. Plus précisément, cinq contributions sont (1) la conception de circuits Smart Buffer, (2) la conception multicouches comprenant le codage Manchester / Manchester différentielle, (3) le

développement d'une norme de cryptage avancé (AES) avec résistance de l'analyse de puissance différentielle (DPA) [83].

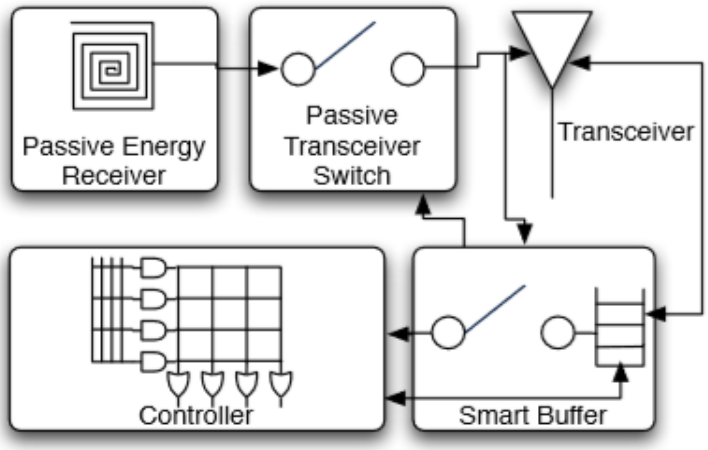


Figure 27: Architecture de L'étiquette active passive RFID [83].

II.2.3.2.2.1.1 Technique de commutateur intelligent (Smart Buffer) :

Le commutateur intelligent est un préprocesseur basé sur le matériel, illustré à la **Figure 27**, conçu non seulement pour le prétraitement de paquets RFID à faible dissipation de puissance avant le contrôleur RFID, mais également pour la gestion de l'alimentation du contrôleur d'étiquettes RFID actives passives. L'architecture principale du commutateur intelligent est illustrée à la **Figure 28**. Une partie importante de la dissipation de puissance d'une étiquette RFID provient du contrôleur RFID, qui calcule une réponse des commandes RFID entrantes pendant l'état actif. Une étiquette RFID typique écoute toujours tout paquet RFID entrant. Indépendamment du fait que le paquet soit destiné à cette étiquette RFID particulière, son contrôleur détermine si l'étiquette répond ou abandonne le paquet RFID en fonction de la destination du paquet RFID. Si la destination du paquet RFID peut être détectée et déterminée alors que le contrôleur reste dans un état de faible puissance ou de veille, des économies d'énergie significatives peuvent être réalisées. Le circuit à puces RFID actif offre une capacité de (1) déterminer la destination de chaque paquet RFID entrant sans place le contrôleur, (2) déterminant si le paquet doit être abandonné ou transmis au contrôleur et (3) en maintenant le contrôleur en mode veille lorsque le paquet est reçu et mis en mémoire tampon. Après avoir détecté le paquet RFID, il extrait des informations, telles que l'identificateur de destination et la commande RFID acheminée par le paquet RFID, et réveille le contrôleur du mode veille si les informations appropriées sont appariées [82].

II.2.3.2.2.1.1.1 Architecture Smart Buffer :

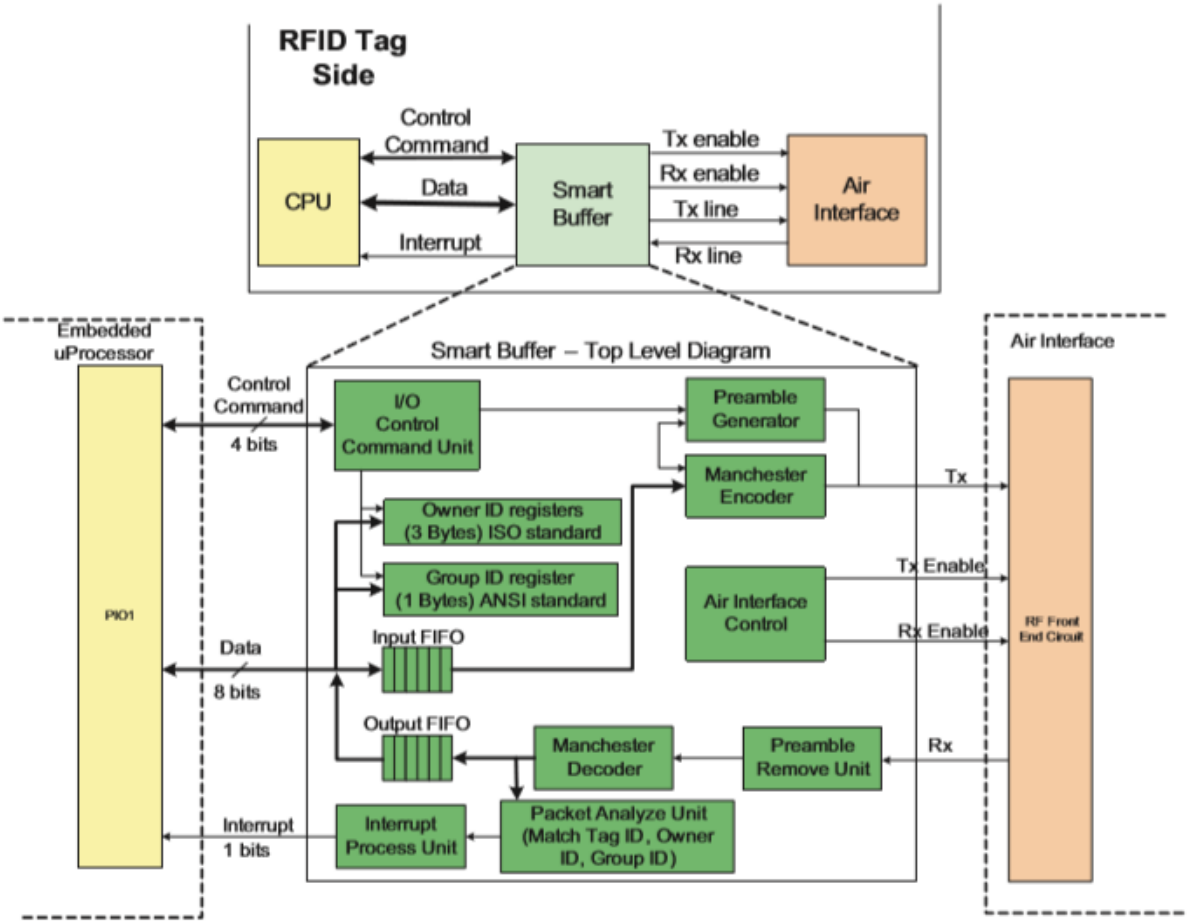


Figure 28: Bloc diagramme de niveau supérieur pour l'architecture Smart Buffer [82].

La **Figure 28** illustre le diagramme de niveau supérieur du commutateur intelligent. Le commutateur intelligent dispose de quatre broches d'E / S sur le circuit frontal RF. Les blocs décrits à la figure 9 sont énumérés dans les sections suivantes :

Unité de suppression de préambule: détecte le signal de préambule entrant et différencie les signaux destinés aux étiquettes et aux lecteurs.

Manchester Décoder: Convertit le code de Manchester en valeurs binaires.

Préambule Générateur: Génère le code Manchester pour la réponse de tag. **Unité d'analyse de paquets**: détecte les drapeaux d'identification pour déterminer s'il faut réactiver le processeur.

Unité de traitement d'interruption: génère une interruption pour le processeur.

Unité de commande de contrôle du processeur: communique les données à destination et en provenance du processeur.

Unité d'interface aérienne: communique les données depuis et vers l'interface aérienne.

Lorsqu'une commande entrante arrive sur le circuit frontal RF, l'unité de suppression de préambule détecte un signal de préambule entrant valide. Une fois que la commande entière est mise en mémoire tampon / stockée dans le commutateur intelligent, le décodeur Manchester convertit les données codées par Manchester immédiatement après un préambule valide. Sur la base des informations d'en-tête contenues dans le paquet RFID, la détermination de l'unité d'analyse de paquet est définie par les caractéristiques du paquet requis afin de déterminer si le contrôleur doit être généré pour la génération de réponse. C'est la procédure clé. Si l'en-tête du paquet transportant des informations erronées, identifiant de tag ou utilisateur non pertinent, Smart Buffer abandonne le paquet. L'unité de traitement d'interruption n'accepte le contrôleur que lorsqu'un paquet RFID complet est stocké dans la FIFO (First in first out) de sortie et que le résultat de l'analyse transmis par l'unité d'analyse de paquet est positif. L'unité de contrôle de commande extrait les commandes de contrôle de l'automate, telles que lire et écrire des données dans FIFO, mettre à jour l'ID de tag, etc. Le générateur de préambule génère un signal de préambule suivi de l'impulsion de synchronisation finale. Lorsque l'impulsion de synchronisation finale est transmise, le générateur de préambule en informe le serveur principal pour obtenir un enregistrement de sortie en série. L'unité d'interface air dispose de signaux de commande de sortie qui sont activés lorsque le Smart Buffer doit écouter les signaux entrants en provenance de l'air ou lorsqu'il est prêt à transmettre une réponse aux lecteurs [76].

II.2.3.2.2.1.1.2 Algorithme pour la technique de commutateur intelligent :

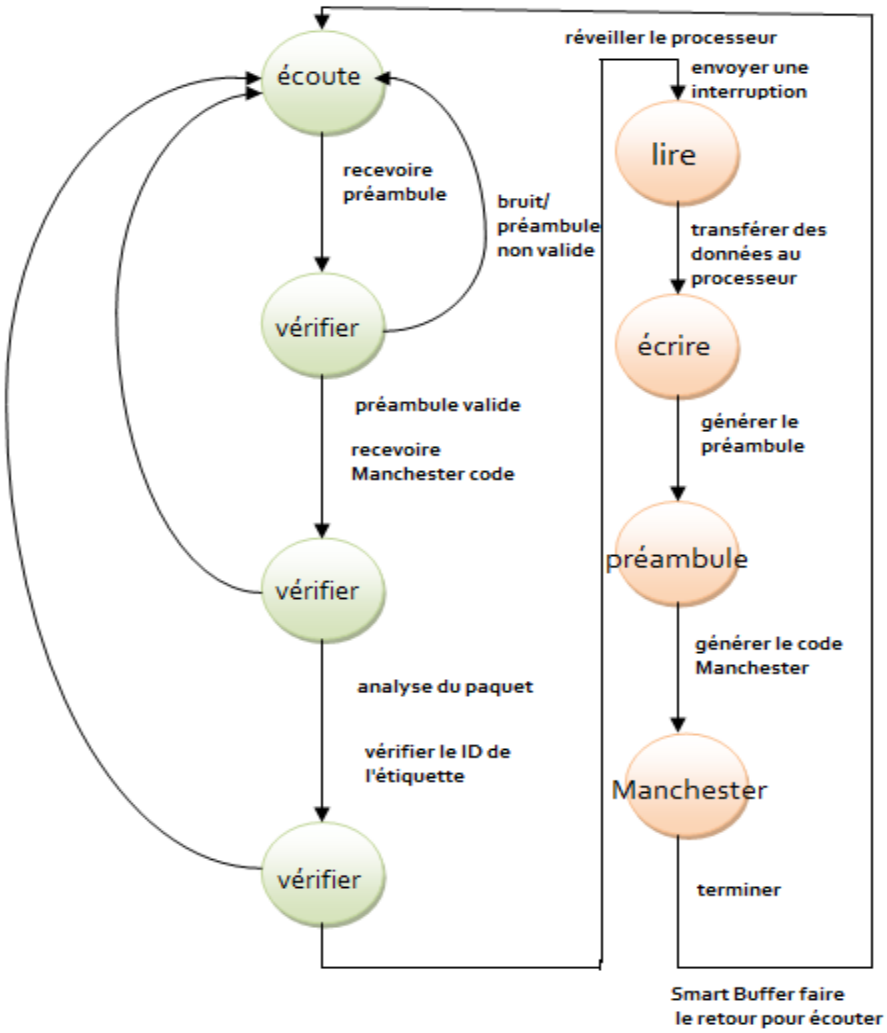


Figure 29: Le flux conceptuel du Smart Buffer [82].

Le flux conceptuel de la **Figure 29** illustre le mécanisme du coprocesseur émetteur-récepteur RF, c'est-à-dire le commutateur intelligent. Dans les quatre premiers états surlignés en vert, le Smart Buffer vérifie le préambule (Le préambule est une suite de 0 et de 1 alternés. Il permet à l'horloge du récepteur de se synchroniser sur celle de l'émetteur) [10] du message et met en mémoire tampon le paquet entrant. Le commutateur intelligent vérifie ensuite si le paquet était prévu pour un départ. Le processeur n'est pas utilisé pour effectuer la vérification, cela se fait dans le matériel pendant que le processeur reste inactif ou en veille. De ce fait, seul le Smart Buffer consomme de l'énergie. Si le paquet entrant n'est pas valide, le commutateur intelligent l'ignorera et reviendra à l'état de veille. Si le paquet entrant est identifié comme étant le paquet prévu pour l'étiquette, en mettant en correspondance l'ID de tag, le commutateur intelligent réveillera le processeur pour qu'il traite le paquet. Le processeur lit

les données du Smart Buffer et répond en conséquence. Une fois que le processeur a écrit les données de réponse dans le commutateur intelligent, celui-ci génère un flux de données constitué d'un signal de préambule et des données de réponse codées par Manchester. C'est à ce stade que le processeur revient au mode basse consommation. A la fin de l'envoi de la réponse au paquet, le commutateur intelligent revient à écouter le préambule suivant.

II.2.3.2.2.1.2 Les techniques multicouches de la sécurité à faible consommation d'énergie:

Les protocoles de sécurité multicouches proposés dans cette partie sécurisent l'accès aux étiquettes (passive active) et la communication RF entre les étiquettes et un lecteur. l'encodage Manchester / Manchester différentiel et l'encryptage / décryptage AES(Advanced Encryption Standard algorithme de chiffrement symétrique de l'Institut national des normes et de la technologie (NIST)) représentent respectivement les protocoles de sécurité de la couche physique, de la couche liaison de données et de la couche application [84]. Le commutateur de rafale est un récepteur passif utilisé pour le commutateur d'émetteur-récepteur passif des étiquettes (passive active) de la **Figure 27**, qui permet à l'émetteur-récepteur actif sur l'étiquette d'entrer en mode veille lorsqu'il est inactif. Le récepteur passif réveille l'émetteur-récepteur lorsqu'il reçoit un signal RF. Toutefois, le commutateur de rafales peut être activé par tout signal RF tel que du bruit, une communication provenant d'autres systèmes sans fil ou même d'un lecteur malveillant. Ainsi, le commutateur de rafale seul n'est pas suffisant. Le codage du commutateur en rafale est créé pour résoudre ce problème. Le décodeur de commutation en rafales de faible puissance a la capacité de traiter n rafales, où n est le nombre de rafales et est équivalent au nombre de registres du décodeur. Si et seulement si les rafales de séquence entrantes reçues correspondent à la valeur attendue dans le décodeur, le décodeur de commutateur en rafale de faible puissance est capable de réveiller le reste de l'étiquette RFID [82, 83].

II.2.3.2.2.1.2.1 Manchester / Manchester différentiel encodage:

Sécurise la communication RF entre les étiquettes et un lecteur qui mélange des techniques de codage de données basées sur une clé secrète. Il améliore la flexibilité et la sécurité du codage. Manchester et le codage Manchester différentiel ne peuvent pas être distingués par inspection, mais ont des formes différentes pour coder la même valeur. En mélangeant les codages ensemble, les bits réels peuvent être obscurcis par une attaque de surveillance. La technique de codage Manchester utilise des données et les combine avec une horloge de

synchronisation. Une transition se produit au milieu d'une "fenêtre de bits" du signal codé. Une transition négative (de haut en bas) représente une non-return-to-zero NRZ ’0’ et une transition positive (de bas en haute) représente une NRZ ’1’. Le codage Manchester différentiel (DM) se concentre sur les transitions au bord de chaque fenêtre de bits. Si une transition existe entre les fenêtres, cela représente un NRZ ’0’. Si aucune transition n’est présente, cela représente un NRZ ’1’. Pour extraire des informations codées dans un vecteur de bits NRZ, le décodeur détecte et échantillonne simultanément au début et au milieu de la fenêtre. Pour appliquer cette technologie de décodage aux étiquettes RFID, il est souhaitable de minimiser la taille du décodeur pour économiser de la surface (coût) et de la puissance (batterie). Par conséquent, au lieu d'utiliser un décodeur Manchester et un décodeur DM séparément, l'architecture utilise un décodeur MDM (Manchester / Manchester Différentiel), qui partage la plupart des parties logiques de deux décodeurs. Il augmente la taille de 42% et la consommation d'énergie de 38% par rapport au décodeur Manchester [82, 83 ,84].

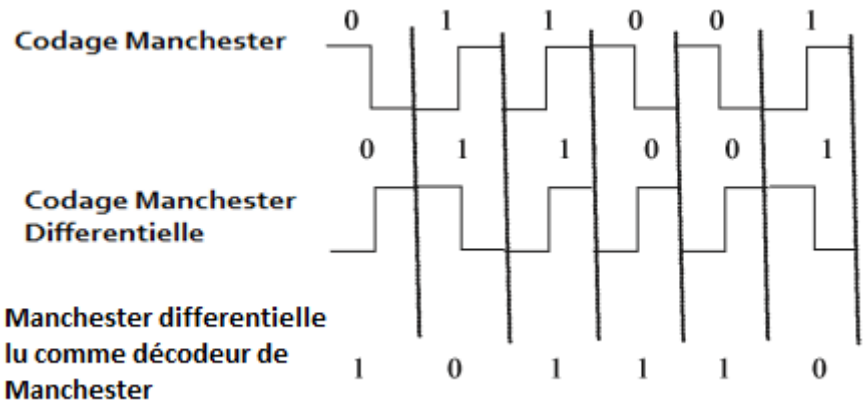


Figure 30: fournit un exemple de codage Manchester et Manchester différentielle [82].

Figure 30 un exemple de codage Manchester et de Manchester différentielle. Pour convertir le code Manchester ou Manchester différentielle en vecteurs de bits, le signal est échantillonné afin de détecter la transition au milieu ou au début de la fenêtre, respectivement. Pour extraire les valeurs d’un signal combinant le code de Manchester dans le même signal, il est nécessaire, par exemple, de passer au mode de transition, à la fois au début et à la fin de la fenêtre, simultanément. Cela nécessite de doubler le taux d'échantillonnage sur l'un ou l'autre codage seul. De plus, il sera nécessaire de créer une logique pour détecter l'existence ou l'absence d'une transition au début de la fenêtre et la direction de la transition au milieu de la fenêtre pour déterminer la valeur. Cependant, la clé peut être utilisée comme signal d'activation pour ces blocs, de sorte que le bloc inactif ne consomme pas d'énergie [82].

II.2.3.2.2.1.2.2 Transmission de données cryptées avec AES :

L'algorithme AES (Advanced Encryption Standard) est conçu non seulement pour établir un profil d'étiquette RFID à faible puissance, mais également pour augmenter la résistance aux attaques DPA (Differential Power Analysis qui utilise l'analyse statistique pour aider à découvrir la clé secrète) [82]. Il peut être utilisé pour le contrôleur RFID des étiquettes (passive active). Basé sur le compilateur SuperCISC, un outil d'automatisation de la conception capable de convertir du C en VHDL, la partie logique (code VHDL) du cryptage et du décryptage AES a été générée automatiquement. Après analyse place-et-route et puissance, la dissipation de puissance et la taille (surface) de l'AES se situent dans les limites acceptables pour les étiquettes RFID. Afin de vérifier sa résistance aux attaques de DPA, un flux d'automatisation a été développé pour générer des données de stimulus et examiner le profil de puissance de l'AES automatiquement. Le résultat des expériences montre que notre conception AES est capable de résister à une attaque par DPA [82, 83].

II.2.3.2.2.1.2.2.1 Architecture AES :

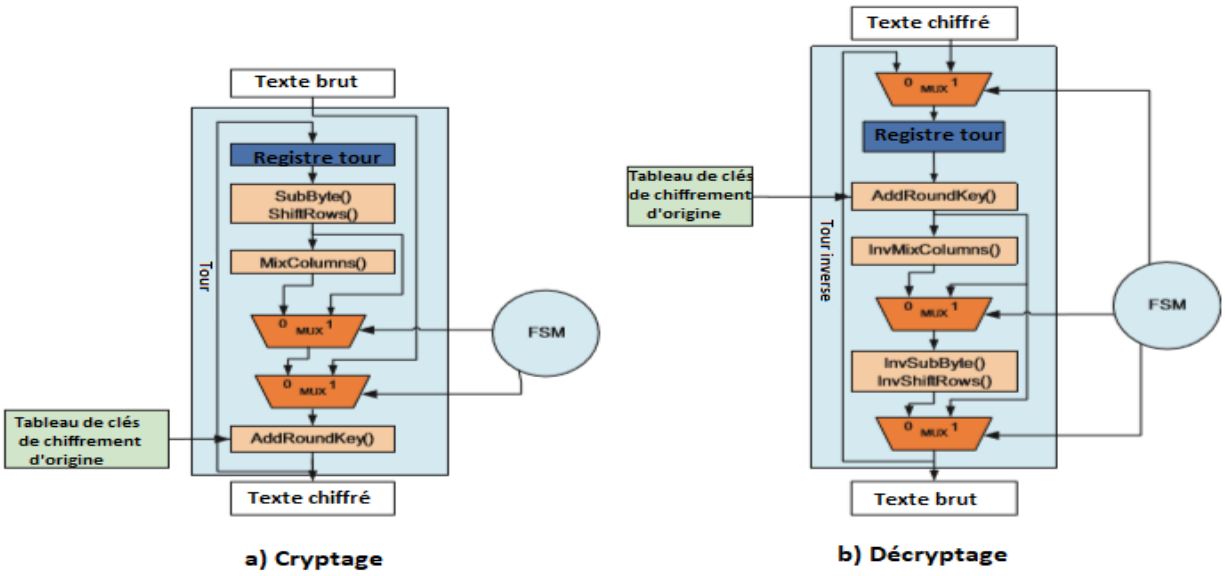


Figure 31: Architecture AES [82].

La **Figure 31** présente une vue d'ensemble de l'approche de mise en œuvre du AES. Un total de cinq blocs pour la mise en œuvre de l'AES a été synthétisé à l'aide de SuperCISC. Pour le cryptage, AES nécessite 12 cycles de calcul avec quatre fonctions successives: SubByte (), ShiftRows (), MixColumns () et AddRoundKey () avec AddRoundKey () en cours d'exécution

avant ces cycles et toutes les fonctions à l'exception de MixColumns () en cours d'exécution une fois après les tours. Ainsi pour le chiffrement, trois blocs ont été synthétisés:

AddRoundKey (), qui est principalement la combinaison de SubByte () et ShiftRows (), qui simplifie la recherche dans les tables et le routage, et MixColumns (). En utilisant une machine à états finis simple, le bloc de chiffrement résultant est présenté à la **Figure 31** (a). Le déchiffrement nécessite des fonctions complémentaires InvMixColumns () et la combinaison de InvSubByte () et d'InvShiftRows () et de blockAddecodes () block from encryption. Le déchiffrement est mis en œuvre de la même manière que le chiffrement, comme illustré à la **Figure 31** (b) [82].

II.2.3.2.2.2 Protocoles et normes RFID active existants :

Quatre protocoles pour la RFID active concernent l'efficacité énergétique:

Le protocole de Free2move qui est basé sur le spectre étalé à sauts de fréquence et sur l'accès multiple par répartition dans le temps (ci-après appeler le "protocole actuel"). Il utilise deux modes différents qui peuvent être choisis pour s'adapter à l'application.

Un protocole amélioré basé sur le protocole actuel Free2move (ci-après appeler le "protocole amélioré"), mais avec des améliorations qui utilisent davantage le canal radio.

802.15.4 (Zigbee MAClayer), utilisé comme protocole à créneaux basé sur les conflits.

Un "protocole de référence" fictif, un protocole optimisé avec les mêmes contraintes dans le canal radio que les protocoles Free2move mais en supposant qu'aucune énergie n'est nécessaire pour détecter un lecteur RFID.

II.2.3.2.2.2.1 Le protocole actuel :

Le protocole Free2move existant fonctionne soit en mode système synchronisé soit en mode système non synchronisé. En mode synchronisé (également appelé RTF, mode "Reader Talks First"), le lecteur envoie des signaux de l'étiquette (émet une **onde radio** à faible portée) [12] sur lesquels les étiquettes réagissent, alors qu'en mode non synchronisé (également appelé TTF, mode "Tag Talks First"), les étiquettes réagissent indépendamment le lecteur. Une étiquette fonctionne généralement de manière périodique, réveillant et transmettant des informations au lecteur, puis entrant à nouveau en mode veille. En mode RTF, le lecteur envoie en permanence des signaux de balise pour créer un schéma à créneaux. La taille de

trame est toujours la même mais, elle peut être modifiée pour obtenir un débit plus élevé. Entre les balises, le lecteur écoute les réponses des étiquettes et il peut écouter deux canaux de fréquence en même temps et recevoir des informations de deux étiquettes synchronisées avec le signal du lecteur. En répondant, l'étiquette choisit au hasard l'une des deux fréquences. Le lecteur bascule et transmet également sur deux canaux différents. En mode TTF, une étiquette se réveille de manière aléatoire et fournit des informations au lecteur sur une fréquence possible sur quatre, sans être synchrones avec le lecteur. Ces quatre fréquences sont divisées en deux groupes et sur chaque groupe, les informations provenant de deux étiquettes émettant simultanément peuvent être reçues simultanément. En raison de l'absence de synchronisation entre les étiquettes, la première étiquette reconnue (sur l'une de ces fréquences de groupe) est lue par le lecteur, tandis que la seconde (sur ce canal) est exclue d'une lecture. C'est une technique du «premier arrivé, premier servi. Les étiquettes TTF et RTF doivent être reconfigurées en termes de fonctionnalité (décalage entre RTF et TTF, en tant que nœud capteur ou nœud ID pur) en étant dirigées vers une file d'attente FIFO planifiée; ceci est fait par le lecteur sur un canal de configuration spécial. Les deux approches différentes de Free2move, RTF et TTF, sont incluses dans un protocole. En utilisant des configurations utilisateur, le protocole peut être ajusté pour s'adapter à un large éventail d'applications logistiques et automatisées, telles que les transports en vol, où une étiquette serait de préférence en RTF et n'écoutait que de l'énergie, n'émettant pas d'énergie RF susceptible de perturber l'avion. En quittant l'avion, l'étiquette entre en TTF car plusieurs lecteurs non perturbateurs sont utilisés. Cette reconfiguration fonctionne à la volée, ce qui signifie que son utilisateur peut adapter l'étiquette à l'application [77,79 ,80].

II.2.3.2.2.2.2 Le protocole amélioré :

Ce protocole permet d'ajouter des fonctionnalités dans le protocole actuel pour améliorer encore ses performances. La modification la plus importante consistait à inclure un paramètre de "sommeil profond" dans le message d'accusé de réception du lecteur. Ce paramètre indique à l'étiquette d'entrer dans un mode de veille profonde pendant une durée variable spécifiée par le responsable. La deuxième amélioration est une utilisation améliorée du canal radio en RTF en utilisant tous les créneaux disponibles pour les signaux de balise et non toutes les secondes sur des canaux différents comme dans le protocole actuel. Ces améliorations réduisent considérablement la consommation d'énergie; par exemple, pendant que le lecteur est disponible et lorsque l'étiquette est réglée pour dormir profondément pendant dix secondes après avoir livré avec succès sa charge utile au lecteur, la consommation d'énergie est réduite

avec 9000. Lorsqu'il n'y a pas de lecteur disponible à proximité, la consommation d'énergie est réduite avec 3 400 (en utilisant un cycle d'une seconde) en raison du temps réduit nécessaire à l'écoute d'un signal. La **Figure 32** montre comment une étiquette s'exécute dans les deux modes améliorés différents pour délivrer un paquet à un lecteur. Il montre le comportement de l'étiquette lorsqu'un lecteur est disponible et quand aucun lecteur n'est disponible. Il montre également le protocole de travail de référence. Le plus efficace (en ce qui concerne l'efficacité énergétique) est bien sûr l'exécution du protocole de référence, car l'état de sommeil et l'état de sommeil profond sont des états dans lesquels presque aucune énergie n'est consommée [77,79 ,80].

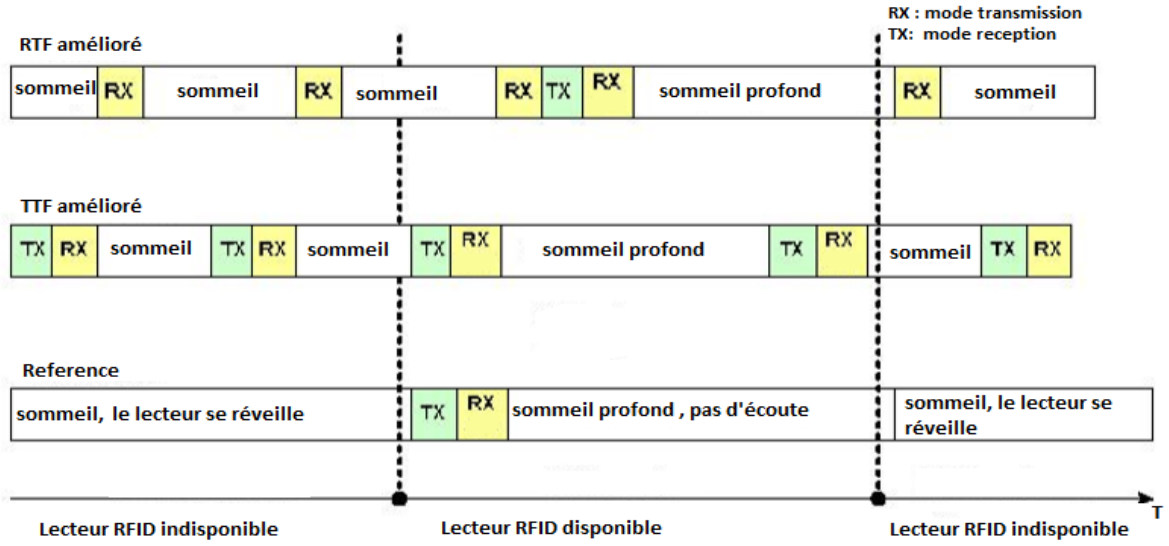


Figure 32: Etiquette exécutant différents modes dans le protocole amélioré lorsqu'aucun lecteur n'est disponible et lorsqu'il en existe un.

II.2.3.2.2.2.3 IEEE 802.15.4 :

Une technologie radio existante supposée être nominée pour Active RFID est la norme IEEE 802.15.4 (est un protocole de communication défini par Institut des ingénieurs électriciens et électronicien. Il est destiné aux réseaux sans fil de la famille des LR WPAN (Low Rate Wireless Personal Area Network) du fait de leur faible consommation, de leur faible portée et du faible débit des dispositifs utilisant ce protocole.) [78]. Il fait partie de la suite IEEE 802.15.x, destinée aux réseaux sans fil personnels. La spécification IEEE 802.15.4 prend en charge l'interconnexion radioélectrique à courte portée, à faible débit et à faible puissance de dispositifs électroniques. La couche physique est basée sur le spectre étalé à séquence directe (DSSS) et est disponible en deux versions; la première version fonctionne dans la bande de

fréquences qui peuvent être utilisées dans un espace réduit pour des applications industrielles, scientifiques, médicales ISM 868/915 MHz et la seconde dans la bande ISM 2,45 GHz. Les versions 868 MHz (Europe) et 915 MHz (États-Unis) prennent en charge un débit brut de 20/40 kbit / s et la version 2,45 GHz (dans le monde entier) prend en charge un débit brut de 250 kbit / s par liaison radio. Deux topologies de réseau différentes sont prises en charge: une topologie d'égal à égal (est un groupe de nœuds. Dans ce réseau, chaque système agit en tant que nœud et partage des ressources sans passer par un ordinateur serveur distinct) [11] et une topologie en étoile. La topologie en étoile convient aux applications RFID actives et est composée de deux types de dispositifs: le dispositif à fonctionnement complet (FFD) et le dispositif à fonctionnement réduit (RFD). Une topologie en étoile doit contenir au moins un FFD, appelé coordinateur. Dans les applications RFID actives, le lecteur est un dispositif FFD (coordinateur) et les étiquettes RFID sont des RFD. L'accès au canal basé sur la contention et sans contention est pris en charge par IEEE 802.15.4. Pour les applications RFID actives, le mécanisme d'accès au canal par contention est préférable, car le nombre et l'identité des étiquettes dans la plage du lecteur (coordinateur) évoluent dans le temps, c'est-à-dire que l'attribution de ressources est inutile si la cible est destinée à fournir l'ID de périphérique (ou une autre petite quantité de données au lecteur) une seule fois. Le mécanisme d'accès au canal basé sur la contention est basé sur une méthode d'accès à un support de détection de porteuse distribuée avec / sans ou avec attribution avec un algorithme de déconnexion de prévention de collision CSMA-CA (La couche liaison de données ou méthode d'accès). Si le CSMA-CA à créneaux est utilisé, le coordinateur envoie une balise, par exemple tous les 16 créneaux, pour synchroniser toutes les unités. Quand une étiquette se réveille, elle commence par écouter la balise, puis, lorsqu'elle trouve la balise, elle attend une heure de retour aléatoire. Une fois que l'heure de désactivation aléatoire est passée, l'étiquette qui acquiert le canal effectue la détection de la porteuse et, si le canal est libre, la transmission est lancée [77,79 ,80].

II.3 Conclusion :

La réduction de la consommation d'énergie est un problème important dans les systèmes modernes, par conséquent, toute méthode permettant de réduire cette consommation doit être étudiée, évaluée et appliquée aux dispositifs en développement. Les techniques présentées dans ce chapitre promettent un moyen intéressant de résoudre ce problème.

Chapitre III

- Comparaison et résultats des différentes techniques.

III Introduction :

Ce chapitre exprimé les résultats qui nous avons trouvé à partir les différentes techniques qui nous avons étudiés auparavant 1) la conception de circuit de Smart Buffer, conception multicouches comprenant le codage de Manchester/ Manchester différentielle, le développement d'une norme de cryptage avancés (AES) pour résoudre le problème des pertes de dissipation d'énergie et sécurité 2) les protocoles concernant l'efficacité énergétique ; protocole actuelle (FreetoMove), protocole amélioré , protocole IEEE 802.15.4 (Zigbee MAClayer)

Alors on a comparé et discuté les résultats des différentes techniques a fin de savoir l'importance de ces nouvelles techniques sur notre système RFID active pour réduire la consommation d'énergie donc la duré de vie de batterie plus que possible.

III.1 Consommation du tag :

Le tag peut se trouver dans trois états différents. Ils sont décrits avec leur consommation sur la **Figure 33.**

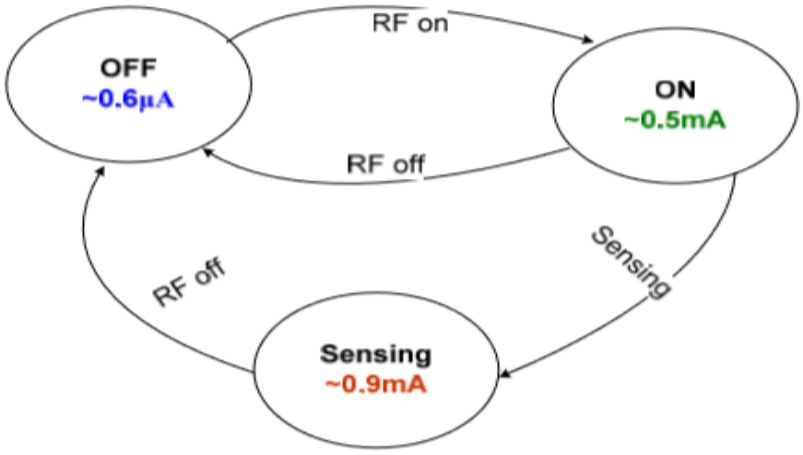


Figure 33:Diagramme des états de consommation effective du tag.

Dans l'état OFF le microcontrôleur est dans la mode LMP4. Lorsque le champ RF se présente le microcontrôleur se réveille (état ON) et consomme 500µA. Lorsque le lecteur demande une lecture des capteurs, la consommation s'élève à 900µA. Cette augmentation est sans doute due à l'écriture sur la mémoire. En effet, les capteurs, une fois la lecture terminée, sont éteints par le microcontrôleur. La consommation reste quant même à 900µA tant que le champ RF n'est pas enlevé [71].

La capacité de la pile bouton utilisé sur le tag est de 170mAh. Le tag peut rester dans l'état OFF environ 32 années (11800 jours). Si le tag est interrogé chaque 10 minute par un lecteur, le nombre de mesure peut se calculer comme suit :

$$\frac{170mA\ .3600}{3s\ .0{,}5mA+3s\ .0{,}9mA+600s\ .0{,}6\mu A} \sim 134000 \qquad \text{(eq09)}$$

III.2 Comparaison et résultats de la consommation d'énergie :

III.2.1 Comparaison entre les µcontrôleurs et le smart buffer :

Pour pouvoir utiliser le Smart Buffer, une étiquette RFID active à très faible consommation doit consommer une puissance supplémentaire de 8 µW, ce qui est proche de la consommation d'un microcontrôleur restant en mode veille (1 à 15 µ A), comme indiqué dans le tableau 6.

Le tableau 6 répertorie la consommation d'énergie des microcontrôleurs et du Smart Buffer. Une étiquette active consomme l'énergie supplémentaire (c'est-à-dire 0,008 mW) pour éviter de réveiller fréquemment le microcontrôleur. Selon le tableau 6, le microcontrôleur consomme de 2 à 8 mA à chaque réveil.

modèle	PIC18F6720	MSP430F16x	ATmega128L	*Smart Buffer*
Frequence (MHz)	20	8	8	10
Taille de mot (Bit)	8	16	8	8
P (active:mA)	2.2*mA*	2*mA*	8*mA*	0.008*mW*
p (veille: µA)	1μA	1.1μA	15μA	8μW

Tableau 5: Comparaison entre les µcontrôleurs et le smart buffer.

III.2.2 Comparaison et résultats de la technique Manchester / Manchester différentiel encodage :

La conception a été étendue comme le montre la **Figure 34** pour inclure le décodage Manchester différentiel simultané et la sélection basée sur une clé. Les résultats de ces deux

conceptions sont résumés dans le **tableau 7**. Les frais généraux liés à l'ajout du décodage différentiel de Manchester augmentent la puissance consommée de 38%.

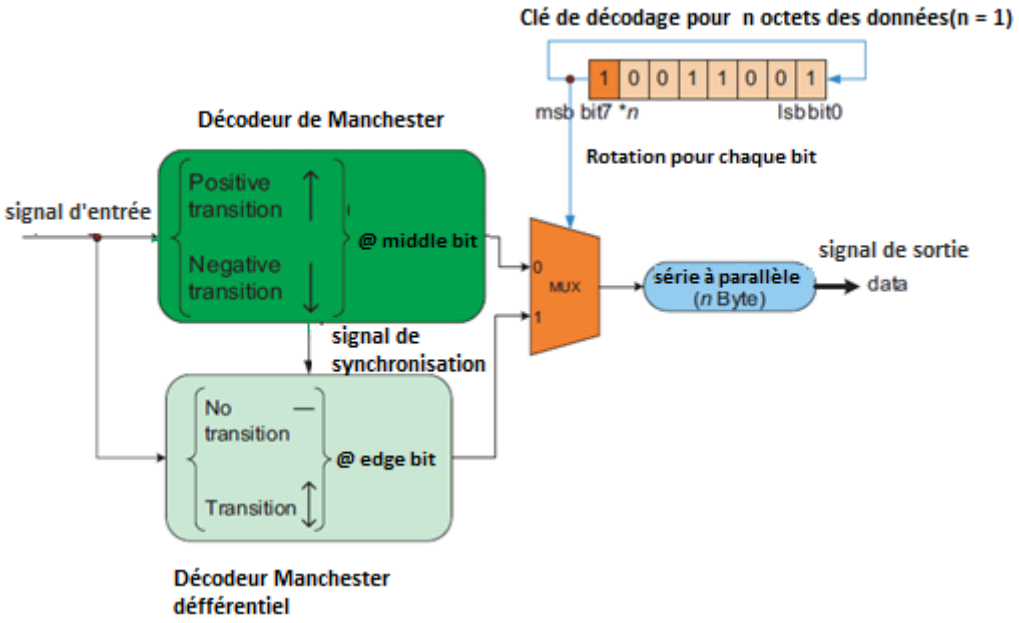


Figure 34: Bloc codeur et décodeur permettant de combiner les codages Manchester et Manchester Différentiel à l'aide d'une clé.

Décodeur	Energy (µW)
Décodeur de Manchester	2.886
Décodeur Manchester et manchester différentielle	3.996

Tableau 6: Surcharge pour ajouter le décodage Manchester différentiel à l'aide d'une clé à un décodeur Manchester.

III.2.3 Comparaison et résultat de la technique transmission de données cryptées avec AES:

Les composants de chiffrement et de déchiffrement AES ont été implémentés à l'aide du compilateur Synopsys Design. La consommation d'énergie a été analysée et les résultats sont rapportés dans le tableau 8. Les résultats montrent que, même s'il existe une grande variation de consommation d'énergie en fonction de la vitesse, la consommation d'énergie pour

l'ensemble du fonctionnement de l'AES est relativement similaire, variant entre 4,18 et 5,17 nJ pour le cryptage et 6,16 et 7,76 nJ pour décryptage. Si la solution d'énergie minimale était choisie, ce serait la vitesse de 500 kHz permettant un débit de 5 Mb / s, ce qui correspond à la vitesse d'horloge du décodeur Manchester. Toutefois, pour des vitesses de ligne de 27,7 kHz telles que définies par la norme ISO 18000 part 7 (est une norme internationale qui décrit une série de technologies RFID, chacune associée à une plage de fréquence unique, contient différents volets (nommé Part) part 7 défini paramètres pour les communications par interface air à 433 MHz) pour les étiquettes actives, l'horloge à 10 kHz générant un débit de 106 Kb / s est plus que suffisante [82].

AES Mode	vitesse de l'horloge	Puissance	Énergie	Taux
Encryption:				
	10 MHz	4.62 mW	5.08 nJ	1 Gb/s
	500 kHz	0.19 mW	4.18 nJ	5 Mb/s
	100 kHz	0.047 mW	5.17 nJ	1 Mb/s
	10 kHz	4.056 μW	4.46 nJ	106 Kb/s
Decryption:				
	10 MHz	7.05 mW	7.76 nJ	1 Gb/s
	500 kHz	0.28 mW	6.16 nJ	5 Mb/s
	100 kHz	0.069 mW	7.59 nJ	1 Mb/s
	10 kHz	7.031 μW	7.73 nJ	106 Kb/s

Tableau 7: Puissance, énergie, débit et surface du bloc matériel AES.

III.2.4 Comparaison et résultats des performances du protocole :

Cette section présente les résultats en termes d'efficacité énergétique et de consommation d'énergie dans un système RFID actif. Deux aspects seront examinés, à savoir le coût énergétique de la livraison de la charge utile et la durée de vie de la batterie d'une étiquette. L'efficacité énergétique est décrite en termes d'énergie en Joules par bit de charge utile transmise avec succès (J / bit), ainsi qu'en termes de durée de vie de la batterie lors de la vidange d'une cellule de batterie d'étiquette. Elle est mesurée en nombre de jours. Le protocole de référence est utilisé pour comparer ce qui est possible avec les mêmes circuits radio et la même bande passante que celle décrite précédemment. Le calcul de la

consommation d'énergie doit prendre en compte s'il existe un lecteur disponible ou non, ainsi que le nombre de tags accessibles par le lecteur.

Lorsqu'une étiquette exécute différents protocoles dans différents modes, certaines d'entre elles consomment toujours une énergie constante, comme les RTF et TTF actuels, même si le nombre des étiquettes augmente à proximité. Lorsqu'une étiquette tente de fournir un paquet de données utiles à un lecteur, le paramètre de délai, décrit précédemment, doit être inclus. La **Figure 35** montre la croissance de la consommation d'énergie lorsque le nombre d'étiquettes à la portée du lecteur augmente. Le RTF amélioré (courbe du bas) montre de grandes améliorations, mais pour le TTF amélioré (courbe en pointillé), les améliorations sont modérées. Le protocole basé sur 802.15.4 (troisième courbe en partant du bas) montre également de bons résultats par rapport aux différents modes du protocole actuel.

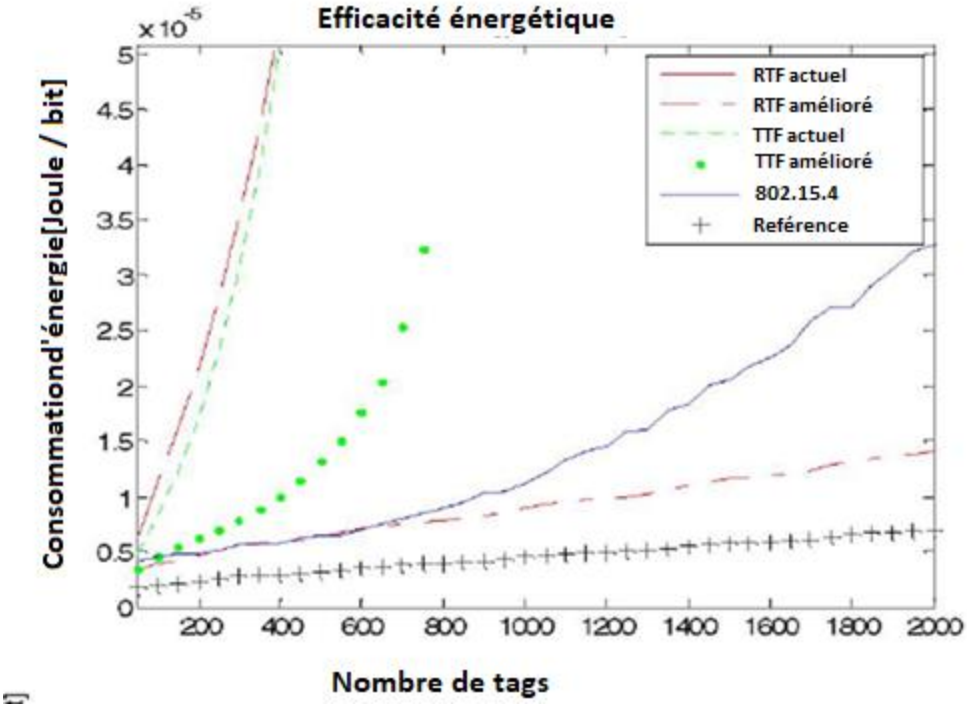


Figure 35: Consommation d'énergie durant l'exécution des différents protocoles.

La Figure 36 montre la consommation totale d'énergie lorsqu'un lecteur est disponible. Le 802.15.4 (courbe supérieure) indique une consommation totale d'énergie plus élevée. Les variantes améliorées de RTF et TTF (deuxième et troisième courbes inférieures) présentent une consommation totale d'énergie inférieure, car l'étiquette utilise le mode de veille prolongée après un paquet de charge utile remis avec succès. La RTF actuelle (seconde courbe supérieure) indique une consommation d'énergie constante, mais le tag n'a aucune connaissance de ce qu'il en est si un paquet de charge utile a atteint le lecteur ou non. Il en va

de même pour le TTF actuel (ligne droite inférieure). Lorsqu'il n'y a pas de lecteur disponible, la consommation totale d'énergie est constante pour tous les protocoles. La durée de vie d'une étiquette peut facilement être calculée et décrite en jours, comme indiqué dans le **tableau 9**.

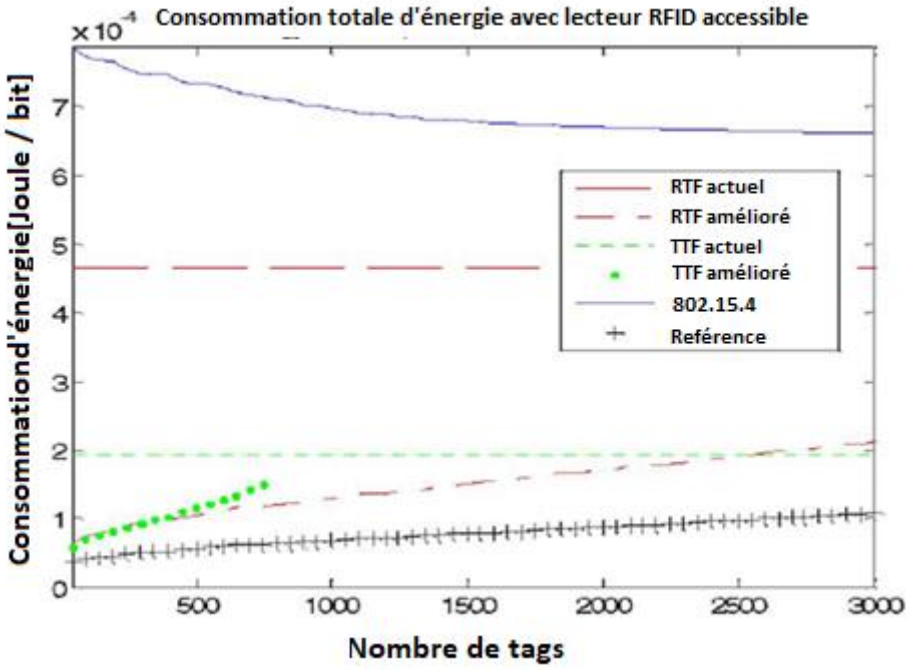


Figure 36: Consommation totale d'énergie lors de l'exécution de différents protocoles et présence d'un lecteur.

Protocole	Consommation d'énergie totale /cycle[mJoule]	Durée de vie avec 3V/180mAh CR2032 litium Cell [Days]
RTF actuel	0,467	48
RTF amélioré	0,307	73
TTF actuel	0,192	117
TTF amélioré	0,192	117
802.15.4	1,247	18
Reférance	0,011	2045

Tableau 8: Consommation d'énergie totale en l'absence de lecteur disponible et durée de vie lors de l'exécution de protocoles différents.

Les résultats lors de la vidange d'une cellule de batterie au lithium (CR2032, 3V / 18OmAh) avec une étiquette exécutant les différents protocoles dans le cas où un lecteur est présent sont illustrés à la **Figure 37**. Les deux modes améliorés donnent de bons résultats, avec une durée de vie maximale de 300 jours lorsque 50 étiquettes sont à proximité du lecteur. Dans la même

situation, l'utilisation de la courbe 802.15.4 (courbe inférieure) donne moins de 40 jours de durée de vie. Bien sur le protocole de référence donne les meilleurs résultats car il n'est pas nécessaire de dépenser de l'énergie pour écouter le signal d'une étiquette émis par un lecteur [79].

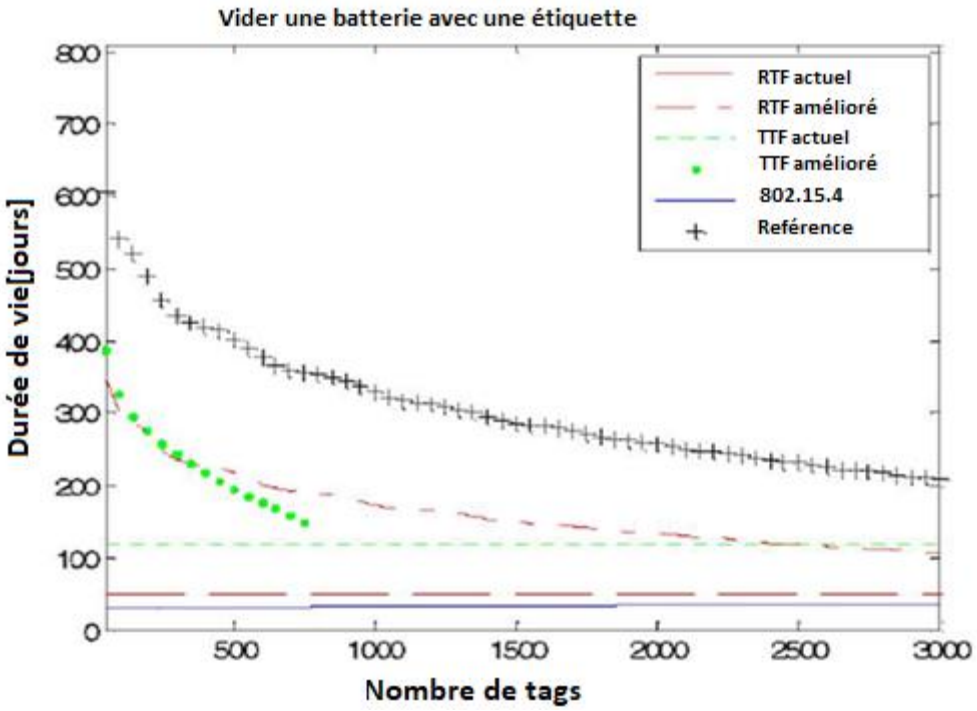


Figure 37: Durée de vie lors de l'exécution de différents protocoles et avec un lecteur disponible**.**

III.3 Conclusion :

Après les nouvelles technologies que nous avons étudiées précédemment, nous avons conclu que la consommation d'énergie avait considérablement diminué dans les systèmes utilisant la radio comme source d'énergie, en particulier dans les systèmes fonctionnant par piles tels que la technologie RFID active.

Après avoir testé la technique Smart Buffer, nous avons constaté que l'étiquette devrait consommer 8 µW par rapport au microcontrôleur en mode veille, cela montre que cette technique a considérablement réduit la consommation d'énergie. Concernant la technique de décodeur Manchester/Manchester Différentielle (MDM), nous avons constaté que l'ajout de décodeur Manchester Différentielle augmentait la consommation d'énergie de 38%, cela signifie que la combinaison des deux décodeurs mieux que les utilisent séparément. Dans la technique AES nous avons remarqué la rapidité de traitement de données

(chiffrement/déchiffrement) alors consommation d'énergie faible, donc si l'énergie minimale est sélectionnée, ce serait la vitesse de 500 kHz permettant un débit de 5 Mb / s.

Qu'un protocole pour la RFID active devrait utiliser le principe du protocole amélioré avec ses modes RTF et TTF afin de réduire la consommation d'énergie. Deuxièmement, ce protocole devrait également inclure la méthode de détection de la porteuse utilisée dans la norme 802.15.4 pour obtenir un débit supérieur et un délai de transmission plus rapide des paquets. Diminuer la consommation d'énergie dans le cas où aucun lecteur RFID n'est disponible constitue un défi de recherche intéressant. Idéalement, une étiquette ne devrait jamais avoir à se réveiller et à rechercher le lecteur, mais devrait rester en mode sommeil profond pour réduire la consommation d'énergie.

Conclusion Générale

La technologie RFID active pose plusieurs problèmes liés à la dissipation d'énergie, à une sécurité insuffisante, aux capacités de vérification du système et aux coûts de conception. Ils sont énumérés comme suit:

1. Dissipation de puissance inutile: dans une étiquette RFID active traditionnelle, de nombreux facteurs sont dissipés, tels qu'un émetteur et un contrôleur d'étiquette actifs en permanence. Si la dissipation de puissance peut être réduite, la durée de vie de la pile de l'étiquette peut être étendue ou contenir des fonctionnalités supplémentaires, telles que le cryptage des données. Il est important de développer une nouvelle technique pour aider les étiquettes RFID actives à réduire la consommation d'énergie.
2. Le besoin de fonctionnalités de sécurité à faible consommation d'énergie: Les étiquettes RFID actives traditionnelles fournissent des fonctionnalités de sécurité via leur contrôleur basé sur un processeur, ce qui augmente la surcharge de consommation d'énergie. Cette situation crée un équilibre entre la sécurité et l'énergie. Cependant, les systèmes RFID nécessitent la mise en œuvre de fonctions de sécurité utilisant des techniques offrant un degré élevé de protection sans augmenter de manière significative la complexité du système, cette complexité pouvant augmenter la consommation d'énergie et les coûts de mise en œuvre. Il est donc important de développer de nouvelles techniques de sécurité qui exploitent les propriétés fondamentales de la communication RFID, telles que les protocoles de couche physique, les extensions de communication à faible consommation, les modes de veille, les variations d'implémentation physique, etc.
3. Augmentation des coûts et des délais de conception: la technologie RFID relève les défis du coût croissant de la conception et de la mise en œuvre de divers systèmes RFID. Afin de répondre aux exigences des différentes situations RFID et de prendre en charge de nombreuses applications RFID, il existe plusieurs normes. Dans la plupart des applications, le matériel / logiciel d'étiquette RFID et de lecteur doit être spécifiquement conçu pour chaque application. Cela maintient le temps de conception global et le coût du système élevé. Il est essentiel de développer un outil d'automatisation de la conception afin de réduire les coûts et le temps de conception.

Références bibliographiques

Références bibliographiques

[1] Https://www.technologuepro.com/cours-systemes-embarques/cours-systemes-embarques-introduction.htm

[2] Http://systemesembarques.e-monsite.com/medias/files/introduction-aux-systemes-embarques-isetgv4.pdf

[3] Http://www.cresitt.com/wp-content/uploads/2015/05/Les-modules-autonomes-28-sept-2011.pdf

[4] Https://www.microcontrollertips.com/the-basics-what-is-an-embedded-processor/

[5] Https://www.webopedia.com/TERM/C/CPU.html

[6] Https://www.tutorialspoint.com/embedded_systems/es_processors.htm

[7] Https://perso.telecom-paristech.fr/urien/intro_carte_2012.pdf

[8] Https://gogul09.github.io/hardware/low-power-vlsi-design-basics-1

[9] Https://eu.mouser.com/applications/low-power-ewc-optimizing/

[10] Https://inetdoc.net/articles/ethernet/ethernet.trame.format.html

[11] Https://www.orosk.com/peer-peer-topology/

[12] Https://www.ubidreams.fr/beacons/

[13] Sais et Bocoum, « Réduction de la consommation énergétique du processeur lors de l'exécution d'un système informatique en temps réel » Université Ibn Khaldoun de Tiaret, 2018.

[14] Frédéric Parain - Michel Banâtre - Gilbert Cabillic - Teresa Higuera - Valérie Issarny-Jean_Philippe Lesot, «Techniques de réduction de la consommation dans les systèmes embarqués temps-réel », Institut National de Recherche en Informatique et en Automatique, Mai 2000.

[15] Shariq Hussain , «Energy Optimization for Low Power Embedded Systems», Department of Software Engineering, Rawalpindi Campus, Foundation University Islamabad, Pakistan, Vol.5, No.8, 2015.

[16]B. HAJJI, «Conception de Systèmes Embarqués », ENSA, Université Mohammed Premier, Oujda, Maroc, 107/05/2012.

[17]Peter Marwedel, « Embedded Systems Foundations of Cuber-Physical Systems», Departement of computer science, Donamed Bren school of information and computer sciences, University of California, Irvine.

[18] Sachin Gupta, « Optimizing Low Power Embedded Designs», Applications Engineer Sr, and Madhan Kumar, Applications Engineer, Cypress Semiconductor Corp, November 2010.

[19] K. Lahiri, A. Raghunathan et D. Panigrahi, « Battery-driven system design: a new frontier in low power design », Design Automation Conference, 2002. Proceedings of ASP-DAC 2002. 7th Asia and South Pacific and the 15th International Conference on VLSI Design. Proceedings.IEEE, 11 janvier 2002.

[20] Mastooreh Salajegheh, «Software Techniques to Reduce the Energy Consumption of Low-Power Devices at the Limits of Digital Abstractions», University of Massachusetts Amherst, 2013.

[21] Shane S. Clark, Jeremy Gummeson, Kevin Fu, Deepak Ganesan, «Towards Autonomously-Powered CRFIDs », University of Massachusetts Amherst, Dept. of Computer Science, 03 January 2014.

[22] Fatine LAHMANI, «Conception et optimisation d'un circuit autonome et communicant au format carte bancaire. Application à une serrure de vélo à assistance électrique», Thèse pour obtenir le grade de docteur de l'Université de Cergy-Pontoise, Ecole doctorale Sciences et Ingénierie, 2014.

[23] Dawood Moeinfar, Hossein Shamsi, Fatemeh Nafar, «Design and Implementation of a Low-Power Active RFID for Container Tracking at 2.4 GHz Frequency», Electrical Faculty, K. N. Toosi University of Technology, Tehran, Iran, January 10, 2012.

[24] Document 2.1.4 – 4, «Guidelines regarding the processing of personal data by means of smart cards and rfid tags», Final Version – February 2012.

[25] Mondher Dhaouadi, « Conception et optimisation des antennes RFID UHF en vue d'améliorer la fiabilité des systèmes RFID », Thèse de Doctorat, Ecole Supérieure des Communications de Tunis, Université de Carthage, 19/12/2014.

[26] Yahiaoui, Sfaïhi, «Technologie RFID : Étude et application», Mémoire de master académique, Université A/Mira de Béjaïa, Faculté des Technologie Département d'Électronique, Promotion 2014/2015.

[27] Sanjay E. Sarma, Stephen A. Weis, and Daniel W. Engels, «RFID Systems and Security and Privacy Implications», Auto-ID Center Massachusetts Institute of Technology Cambridge, MA 02139, 2003.

[28] M.Jourdaine, « Les technologies sans contact».
https://www.boutique.afnor.org/resources/cf195160-5165-47bc-872c-9962baacd403.pdf

[29] Josep Domingo, Ferrer, Joachim Posegga, Francesc Sebé, Vicenç Torra, « Advences in Smart Cards», Universuty Hamburg, department of informatics, Germany, 30 January 2007.

[30] Borst, J., Preneel, B., & Rijmen, V, «Cryptography on smart cards», Departement Electrical Engineering, 2001.

[31] Document 7100030, «Smart Card and Security Basics », 2009.

[32] Katherine M. Shelfer, Chris Corum, J. Drew Procaccino, Joseph Didier, «Smart Cards», Drexel University, Philadelphia , PA , U S A, 2004.

[33] Afzel Noore, «Highly Robust Biometric Smart Card Design», Department of Computer Science and Electrical Engineering West Virginia University, Morgantown, WV 26506-61 01, July 26, 2000.

[34]:R. Wolfgang, John Wiley and Sons, « Design models for using and programming smart cards», 2007.

[35]:R. Wolfgang and E. Wolfgang, John Wiley and Sons, «Smart Card Handbook», 3rd Edition, 2004.

[36] George Selimis, Apostolos Fournaris, George Kostopoulos, and Odysseas Koufopavlou, «Software and Hardware Issues in Smart Card Technology », IEEE Communications Surveys & Tutorials, Vol. 11, No. 3, Third Quarter 2009.

[37] Xuefei Leng , «Smart card applications and security, University of London, 12 July 2009.

[38] document, «La technologie Radio Frequency IDentification (RFID)», Août 2017.

[39] Evizal, Tharek Abdul Rahman, Sharul Kamal Abdul Rahim, «Active RFID Technology for Asset Tracking and Management System », Universiti Teknologi Malaysia, 81310, Johor, Malaysia , Wireless Communication Centre, Faculty of Electrical Engineering, January 29, 2013.

[40] MSP430x15x, MSP430x16x, MSP430x161x mixed signal microcontroller datasheet.

[41] Raed Abdulla and Sathish Kumar Selvaperumal, «Active RFID System with Wireless Sensor Network for Power », School of Engineering, Asia Pacific University of Technology & Innovation, 57000 Kuala Lumpur, Malaysia, 2018.

[42] Paul J.M. Havinga, Gerard J.M. Smit, «Design techniques for low power systems», University of Twente, department of Computer Science.

[43] : Anantha P. Chandrakasan, Robert W. Brodersen, «Low Power Digital Cmos Design », Massachusetts Institute of Technology, University of California/Berkeley, 1995.

[44] Chandrakasan, A. P., & Brodersen, R. W. «Minimizing power consumption in digital CMOS circuits». Proceedings of the IEEE, 83(4), 1995.

[45] K. Yano et al., «A 3.8-11s CMOS 16 x 16 multiplier using complementary pass transistor logic» IEEE J. Solid-State Circuits, vol. 25. pp. 388-395, Apr. 1990.

[46] H. J. M. Veendrick, « Short-circuit dissipation of static CMOS circuitry and its impact on the design of buffer circuits» IEEE J. SolidState Circuits, vol. SC-19, pp. 468-473, Aug. 1984.

[47] Chandrakasan, A. P., Sheng, S., & Brodersen, R. W. «Low-power CMOS digital design». IEEE Journal of Solid-State Circuits,1992.

[48] Kosonocky, S. V., Bhavnagarwala, A. J., Chin, K., Gristede, G. D., Haen, A.-M., Hwang, W., … Zyuban, V. «Low-power circuits and technology for wireless digital systems», IBM Journal of Research and Development, 2003.

[49] W. Chen, W. Hwang, P. Kudva, G. D. Gristede, S. Kosonocky, and R. V. Joshi, «Mixed Multi-Threshold Differential Cascode Voltage Switch (MT-DCVS) Circuit Styles and Strategies for Low Power VLSI Design» Proceedings of the International Symposium on Low Power Electronics and Design, August 2001.

[50] Kao, J. T., & Chandrakasan, A. P, «Dual-threshold voltage techniques for low-power digital circuits», IEEE Journal of Solid-State Circuits, 2000.

[51] Chennai, «Low Power VlSI Design », a Design and Verification Company, Vinchip Systems.

[52] R. Sivakumar, D. Jothi, «Recent Trends in Low Power VLSI Design », Department of ECE, RMK Engineering College, India, November 5, 2014.

[53] Pedram, M., & Qing Wu, «Battery-powered digital CMOS design». IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2002.

[54] M. Pedram, «Power minimization in IC design: Principles and applications», ACM Trans. Design Automat. Electron. Syst., vol. 1, no. 1, pp. 3–56, Jan, 1996.

[55] Ammar Y, «Conception de systèmes de gestion d'énergie pour microsystèmes autonomes». Thèse de l'Université Joseph Fournier de Grenoble, Février 2006.

[56] Rabaey J. et al, «Low Power Design of Memory Intensive Functions Case Study: Vector Quantization», IEEE VLSI Signal Processing Conference, 1994.

[57] Weiser, M, et al.« Scheduling for reduced CPU energy», proceedings of the first USENIX Symposium on operating systems design and implementation, pp. 13-23, November 1994.

[58] Tiebing Zhang. « RTOS Performance and energy consumption analysis based on an embedded system tested ».Thesis submitted to the faculty of the graduate school of the University of Maryland at college park in partial fulfillment of the requirements for the degree of Master of science. 2001.

[59] « Design techniques for energy efficient and low-power systems». Journal of Systems Architecture, and were presented at the IEEE International Conference on Personal Wireless Communications. 2000.

[56] Parain F, Banâtre M, Cabilic G, Higuera T, Issarny V, Lesot JP. « Techniques de réduction de la consommation dans les systèmes embarqués temps-rée» l. Rapport de recherche INRIA. Mai 2000.

[61] Sachin Gupta, Madhan Kumar. «Optimizing Low Power Embedded Designs». Applications Engineer, Cypress Semiconductor Corp. November 2010.

[62] B. Gyselinckx, C. Van Hoof et J. Ryckaert, « Human++: autonomous wireless sensors for body area networks », Custom Integrated Circuits Conference, 2005. Proceedings of the IEEE 2005, IEEE, 21 septembre 2005.

[63] Michael Day. «Power Management Using power solutions to extend battery life in MSP430 applications» . Applications Manager, Portable Power Product, Texas Instruments Incorporated.

[64] Msp430: Ultra-Low-Power Microcontroller Texas Instruments.

[65] Geng, S. -q., Hou, L. -g., Wang, J. -h., Zuo Lei, Zhang Wang, & Wu, W. -c. « Design of RFID active tag system based on MSP430 ». IET 2nd International Conference on Wireless, Mobile and Multimedia Networks (ICWMMN 2008).

[66] Hsi-Wen Wang, Ren-Guey Lee, Chun-Chieh Hsiao+ And Guan-Yu Hsieh. «Active RFID System with Cryptography and Authentication Mechanisms».HSIEH Department of Electronic Engineering National Taipei University of Technology Taipei, 106 Taiwan +Department of Electrical Engineering National Taiwan University Taipei, 106 Taiwan +Department of Computer Information and Network Engineering Lunghwa University of Science and Technology Taoyuan, 333 Taiwan.

[67] Jacob Borgeson, Stefan Schauer,Horst Diewald. «Benchmarking MCU power consumption for ultra-low-power applications ». Texas Instruments /WHITE PAPER.

[68] Patrice Bouffard. «Un exemple de processeur embarqué Le MSP430». université de RENNE .

[69] International Standards Organization, «ISO/IEC FDIS 18000-7:2004(E) ».Standard Specification, 2004.

[70]: Daniel M.Dobkin. «The RF in RFID: Passive UHF RFID in Practice». Communications Engineering Series. 2007.

[71] «Système RFID pour la lecture de capteurs ISO 15693, 13.56MHz». nov.-08

[72] Valais-Wallis. « Système RFID pour la lecture de capteurs ; ISO 15693, 13.56MHz». HES-SO , institue de microtechnique IMT , université de Neuchâtel.

[73] R. Roman, C. Alcaraz, and J. Lopez. «A survey of cryptographic primitives and implementations for hardware-constrained sensor network nodes». Mob. Netw. Appl., Vol. 12, No. 4, pp. 231–244, 2007.

[74] H. Cho and Y. Baek, «Design and Implementation of an Active RFID System Platform». SAINT-W '06: Proceedings of the International Symposium on Applications on Internet Workshops, (Washington, DC, USA), pp. 80–83, IEEE Computer Society, 2006.

[75] H.-J.Chae,D.J.Yeager,J.R.Smith,andK.Fu. «Maximalistcryptographyandcomputation on the WISP UHF RFID tag». In Proceedings of the Conference on RFID Security, July 2007.

[76] A. K. Jones, R. Hoare, S. Dontharaju, S. Tung, R. Sprang, J. Fazekas, J. T. Cain, and M. H. Mickle. «An Automated, FPGA-based Reconfigurable, Low-power RFID Tag». Journal of Microprocessors and Microsystems, Vol. 31, pp. 116–134, March 2007.

[77] Björn Nilsson. «Energy Efficient Protocols For Active Rfid ». Thesis For The Degree Of Doctor Of Philosophy, Department Of Computer Science And Engineering , Chalmers University Of Technology , School Of Information Science, Computer And Electrical Engineering, Halmstad University , Halmstad. Sweden 2010.

[78] IEEE Computer Society LAN MAN Standards Committee. IEEE Std 802.15.4-2003 Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs). The Institute of Electrical and Electronics Engineers, NewYork, U.S. May 2003.

[79] Björn Nilsson. «Towards Energy Efficient Protocols for Active RFID ».Department of Computer Science and Engineering, Chalmers University Of Technology, School of Information Science, Computer and Electrical Engineering, Halmstad. Sweden 2007.

[80] Nilsson B, Bengtsson L, Svensson B. Protocols for active RFID - the energy consumption aspect. In: International Symposium on Industrial Embedded Systems, 2007. SIES '07. Piscataway, N.J.: IEEE; 2007. p. 41-48.

[81] A. K. Jones, S. Dontharaju, S. Tung, P. Hawrylak, L. Mats, R. Hoare, J. T. Cain, and M. H. Mickle. Passive active radio frequency tags (part). International Journal of Radio Frequency Identification Technology and Applications, 2006.

[82] Shen-ChihTung B.S. «An Architectural Approach For Reducing Power And Increasing Security Of Rfid Tags». National Taiwan Ocean University, Taiwan, 1997 M.S. Telecommunication, University of Pittsburgh, 2000,Submitted to the Graduate Faculty of the Swanson School of Engineering in partial fulfillment of the requirements for the degree of Doctor of Philosophy University of Pittsburgh 2008.

[83] Shenchih Tung, Advisor: Alex K. Jones. «An Architectural Approach for Reducing Power and Increasing Security of RFID Tags». Department of Electrical and Computer Engineering, University of Pittsburgh Estimated Graduation Date: Fall 2007.

[84] A. K. Jones, S. Tung, S. Dontharaju, J. T. Cain, and M. H. Mickle. «A secure transaction methodology for the passive activce rfid tag (part) ». Submitted to IEEE Transactions on Automation Science and Engineering (TOASE), in review since January 2007.

[85] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., and Cayirci, E. Wireless «sensor networks: a survey». Computer Networks 38, 4 (2002), 393–422.

[86] Buettner, Michael, Greenstein, Ben, Sample, Alanson, Smith, Joshua R., and Wetherall, David. «Revisiting smart dust with RFID sensor networks». In Proc. 7th ACM Workshop on Hot Topics in Networks (HotNets-VII) (Oct. 2008).

[87] Kahn, J. M., Katz, R. H., and Pister, K. S. J. «Next century challenges: mobile networking for "Smart Dust" ». In Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom) (1999), pp. 271–278.

[88] Mainwaring, Alan, Culler, David, Polastre, Joseph, Szewczyk, Robert, and Anderson, John. «Wireless sensor networks for habitat monitoring». In Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications (2002), pp. 88–97.

[89] Kaps, Jens-Peter. «Cryptography for Ultra-Low Power Devices». PhD thesis, Worcester Polytechnic Institute, 2006.

[90] Paradiso, Joseph A., and Starner, Thad. «Energy scavenging for mobile and wireless electronics». IEEE Pervasive Computing 4, 1 (Jan. 2005), 18–27.

[91] Ho, H., Saeedi, E., Kim, S.S., Shen, T.T., and Parviz, B.A. « Contact lens with integrated inorganic semiconductor devices». In Micro Electro Mechanical Systems. IEEE 21st International Conference on (Jan. 2008), pp. 403–406.

[92] Agency, United States Environmental Protection. «Common wastes and materials, batteries». http://www.epa.gov/wastes/conserve/materials/battery.htm.

[93] Sanjay Sarma, David L. Brock, and Kevin Ashton. The networked physical world - proposals for engineering the next generation of computing, commerce & automatic identi¯cation». White paper, MIT: Auto-ID Center, Oct 2000.

[94] Rajeevan Amirtharajah and Anantha P. Chandrakasan. «Self-powered signal processing using vibration-based power generation». IEEE Journal of Solid-State Circuits, 33(5):687{695, May 1998.

[95] Scott Meininger, Jose Oscar Mur-Miranda, Rajeevan Amirtharajah, Anantha P. Chandrakasan, and Je®rey H. Lang. «Vibration-to-electric energy conversion». IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 9(1):64{76, Feb 2001.

[96] David W. Carman, Peter S. Kruus, and Brian J. Matt. «Constraints and approaches for distributed sensor network security» . Technical report, NAI Labs, Secutity Research Division, Glenwood, MD, Sep 2000.

Résumé

En somme ce résumé nous englobe en général des techniques modernes utilisées pour réduire la consommation en énergie des systèmes embarqués à faible puissance, application sur l'étiquette RFID et les cartes a puce.

Après notre étude nous avons constaté que les RFID active sont des étiquettes fonctionnant par batterie contrairement aux les étiquettes passifs et les cartes a puce, fonctionnant par une énergie stocké dans les condensateurs qui vient par le lecteur. Le problème c'est que les systèmes à faible puissance nécessitent une autonomie énergétique. Ceci est réalisé par des batteries servant de source d'énergie dédiée. Pour ces raisons, l'utilisation efficace de l'énergie est devenue l'un des principaux défis du concepteur de systèmes embarqués alimentés par batterie. Alors Tout les techniques qui nous avons étudié dans ce mémoire concerne les systèmes qui fonctionnent par batterie comme la RFID active.

Concernant les techniques : 1) les techniques au niveau technologique (on a choisies la technologie CMOS par ce qu'elle est très utilisé dans les systèmes ultra faible consommation par rapport au TTL et elle a des avantages plus que TTL), 2) les techniques au niveau MCU MSP430 (Quatre modes d'alimentation), 3) les techniques au niveau système (l'étiquette RFID active) :

- Technique Smart Buffer (le commutateur intelligent).
- une technique multicouche à faible consommation d'énergie
- Les protocoles pour la RFID active concernent l'efficacité énergétique.

ملخص

باختصار ، يشمل هذا الملخص بشكل عام التقنيات الحديثة المستخدمة لتقليل استهلاك الطاقة للأنظمة المدمجة منخفضة الطاقة، والتطبيق على علامة RFID و البطاقات الذكية.

بعد دراستنا ، وجدنا أن RFID النشطة هي علامات تعمل بالبطاريات على عكس العلامات السلبية والبطاقات الذكية ، والتي تعمل بالطاقة المخزنة في المكثفات التي تأتي من خلال القارئ. المشكلة هي أن أنظمة الطاقة المنخفضة تتطلب استقلالية الطاقة. يتحقق ذلك من خلال البطاريات التي تعمل كمصدر مخصص للطاقة. لهذه الأسباب ، أصبح الاستخدام الفعال للطاقة أحد التحديات الرئيسية لمصمم الأنظمة المدمجة التي تعمل بالبطاريات. لذا فإن كل التقنيات التي درسناها في هذه المذكرة تتعلق بالنظم التي تعمل بالبطارية مثل RFID نشطة.

فيما يتعلق بالتقنيات: 1) التقنيات على المستوى التكنولوجي (اخترنا تكنولوجيا CMOS لأنها تستخدم على نطاق واسع في أنظمة الطاقة المنخفضة للغاية مقارنةً ب TTL ولها مزايا مقارنة مع TTL) ، 2) التقنيات على مستوى(MCUMSP430أربعة أوضاع طاقة) ، 3) تقنيات على مستوى النظام (علامة RFID النشطة) :

- تقنية SMART BUFFER.
- تقنية متعددة الطبقات مع انخفاض استهلاك الطاقة.
- بروتوكولات RFID النشطة تتعلق بكفاءة الطاقة.