République **A**lgérienne **D**émocratique et **P**opulaire
Ministère de l'**E**nseignement **S**upérieur et de la **R**echerche **S**cientifique

UNIVERSITE **M**OULOUD **M**AMMERI DE **T**IZI-**O**UZOU

FACULTE DU **G**ENIE **E**LECTRIQUE ET D'INFORMATIQUE
DEPARTEMENT D'INFORMATIQUE

Mémoire de Fin d'Etudes de MASTER ACADEMIQUE

Domaine : **Mathématiques et Informatique**

Filière : **Informatique**

Spécialité : **Réseaux, Mobilité et Systèmes Embarqués**

Présenté par

Tassadit CHAFA

Nacera OTMANI

Thème

Contrôle d'accès à base de la technologie RFID

Mémoire soutenu publiquement le 12/07/ 2016 devant le jury composé de :

Président : M^r^ **Mustapha LALAM**

Encadreur : M^me^ **Malika BELKADI**

Co-Encadreur : M^r^ **Smail DJIOUA**

Examinateur : M^r^ **Mohammed DAOUI**

Examinateur : M^me^ **Rachida AOUDJIT**

Sommaire

CHAPITRE III : Analyse et conception

Chapitre IV : Réalisation

Liste des figures

CHAPITRE 1

Généralités sur les systèmes Embarqués

I. Introduction :

Les technologies des systèmes embarqués; logiciel embarqué et microélectronique, ont la capacité de transformer tous les objets du monde physique du plus petit au plus grand, du plus simple au plus complexe en objets numériques, intelligents, autonomes et communicants. L'émergence du l'IOT *(Internet Of Things)*, jonction du monde du Web et de celui des systèmes embarqués, amplifie de façon considérable cette révolution. De fait, le déploiement généralisé des systèmes embarqués modifie profondément notre environnement, et porte de très nombreuses innovations de produits et d'usages et impacte l'ensemble des activités industrielles et de services.

Un système embarqué est défini comme un système électronique et informatique autonome, ne possédant pas d'entrées-sorties standards comme un clavier ou un écran d'ordinateur, spécialisé dans une tâche bien précise. Ses ressources sont généralement limitées d'après l'auteur de [SE3]. Un système embarqué utilise généralement un microprocesseur combiné avec d'autres matériels et logiciels pour résoudre un problème de calcul spécifique. Le système matériel et l'application sont intimement liés et ne sont discernables comme dans un environnement de travail classique de type PC [SE2].

Les systèmes embarqués fonctionnent généralement en temps réel: les opérations de calcul sont alors faites en réponse à un événement extérieur (interruption matérielle). Dans ce cas, ils doivent utiliser un système d'exploitation temps-réel (RTOS pour *Real Time Operating System*) [SE1].

II. Historique : [SE2]

1961

« Apollo Guidance Computer » est le premier système embarqué. Il est Composé d'environ un millier de circuits intégrés identiques.

1962

Un autre premier système embarqué est le « Autonetics D-17 guidance computer » qui servait de système de contrôle aux missiles nucléaires américains LGM-30 Minuteman, il était basé sur des transistors et contenait un disque dur comme mémoire principale.

1971

Intel produit le 4004, ce premier microprocesseur était le premier circuit intégré incorporant tous les éléments d'un ordinateur dans un seul boitier : unité de calcul, mémoire, contrôle des entrées/sorties, alors qu'il fallait plusieurs circuits intégrés différents, chacun dédié à une tache particulière. Premier circuit générique, personnalisable par logiciel.

1972

Lancement de l'Intel 8008, premier microprocesseur 8 bits (48 instructions, 800kHz).

1974
Lancement du 8080, premier microprocesseur largement diffusé, (8 bits, 64KB d'espace adressable, 2MHz - 3MHz).

1978
Création du Z80, processeur 8 bits.

1979
Création du MC68000, processeur 16/32 bits.

III. Caractéristiques d'un système embarqué : [SE1] [SE7]

Les points suivants permettent de caractériser un système embarqué :

➢ Fonctionnement en Temps Réel :

- Réactivité : des opérations de calcul doivent être faites en réponse à un événement extérieur (interruption matérielle).
- La validité d'un résultat dépend du moment où il est délivré, (deadlines).
- Rater une échéance peut causer une erreur de fonctionnement.
  - Temps réel dur : erreur sévère.
  - Temps réel mou : dégradation non dramatique des performances du système.
- La plus part des systèmes sont «multirates» : traitement d'informations à différents rythmes.

➢ Faible encombrement:

- Consommation électrique minimisée.
- Un système embarqué est souvent de petite taille si on le compare aux volumes importants atteints par les systèmes classiques multiusages.

➢ Ciblé et autonome :

- Le domaine d'action d'un système embarqué est limité aux fonctions pour lesquelles il a été créé.
- Une fois enfouis dans l'application, les systèmes embarqués ne sont (le plus souvent) plus accessibles.

➢ Faible consommation :

- Batterie de 8 heures et plus (PC portable : 2 heures).

➢ Faibles ressources :

- Les systèmes embarqués sont généralement limités par leurs ressources spatiales. Etant utilisés comme composants enfouis dans des systèmes plus complexes et étant conçus pour réaliser des tâches spécifiques, des mémoires de petite taille et des unités de calcul d'une faible puissance sont souvent suffisantes.

➢ Communication :

- Généralement les objets pour lesquels les systèmes embarqués sont conçus, sont des objets communicants, ainsi ces systèmes sont dotés de modules qui leur permettent de communiquer et de recevoir des informations sur de longues ou petites distances.

➢ Sécurité, fiabilité et sûreté :

- Le système doit toujours fonctionner correctement.
- Sûreté de fonctionnement du logiciel.
- Le logiciel nécessite une grande fiabilité car il est destiné à un fonctionnement complètement autonome et/ou critique.

➢ Faible coût:

- Beaucoup de systèmes embarqués sont fabriqués en grande série et doivent avoir des prix de revient extrêmement faibles.

➢ Environnement :

- L'environnement dans lequel opère le système embarqué n'est pas contrôlé. Cela suppose donc de prendre en compte ce paramètre lors de sa conception.
- Il faut prendre en compte les évolutions des caractéristiques électriques des composants en fonction de la température, des radiations,…etc.

Lors du développement et de la conception d'un système embarqué, ces caractéristiques sont considérées comme étant des contraintes, des facteurs à prendre en considération afin d'aboutir à un système optimal. Ces mesures concurrencent souvent l'une avec l'autre, en effet, une amélioration de l'une conduit souvent à une dégradation dans une autre. Par exemple, si nous réduisons la taille d'une implémentation, sa performance peut en souffrir.

IV. Classification des systèmes embarqués : [SE2]

Selon leurs rôles les systèmes embarqués peuvent être classés comme suit :

- ***Calcul général :*** Ce sont des applications similaires aux applications de bureau mais empaquetées dans un système embarqué. Exemple : jeu vidéo, set- top box.

- ***Contrôle de systèmes*** **:** Des applications dédiées au contrôle de systèmes en temps réel. Exemple : moteur d'automobile, traitement chimique, traitement nucléaire, système de navigation aérien.

- ***Traitement du signal*** **:** Calcul sur de grosses quantités de données. Exemple : GPS *(Global Positioning System)*, radar, sonar, compression vidéo.

- ***Télécommunication et réseaux :*** Transmission d'informations et commutation de paquets. Exemple : téléphone, dispositifs de l'internet.

V. Architecture matérielle d'un système embarqué :

Un système embarqué dispose d'une architecture semblable à celle des ordinateurs standards. En effet, on y retrouve les mêmes composants (processeur, mémoires, périphériques d'entrée/sortie) interconnectés à l'aide de bus.
D'autres composants viennent compléter l'architecture simplifiée des ordinateurs conventionnels. Ces composants répondent aux caractéristiques spécifiques et permettent la réalisation des tâches propres à ces systèmes. L'architecture typique d'un système embarqué peut être représentée par le schéma de la figure FigI.1.

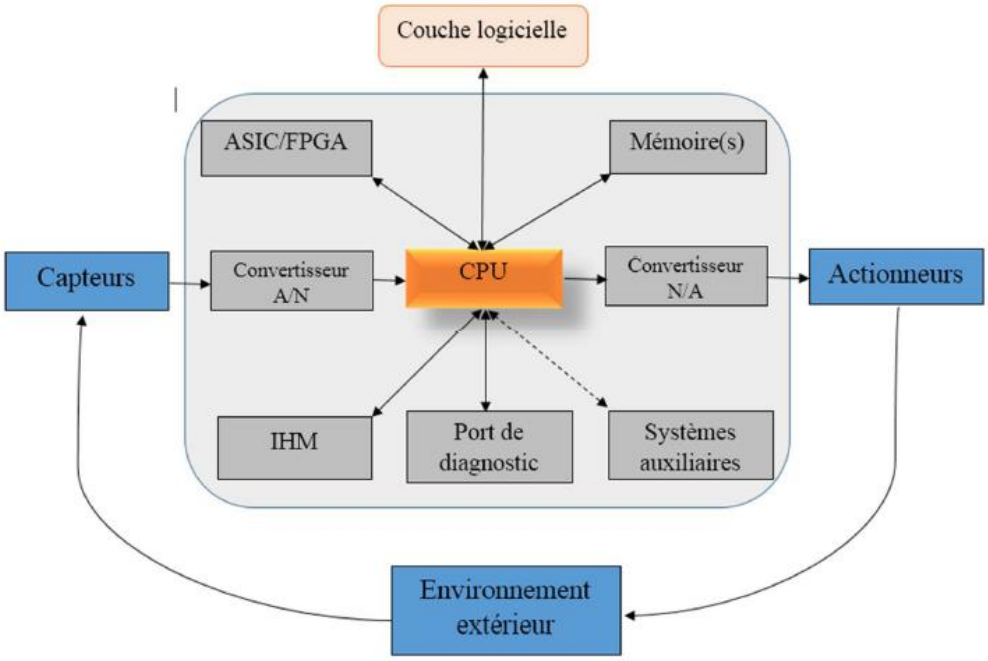


Fig.I.1 Architecture typique d'un système embarqué. [SE8]

On trouve en entrée des capteurs généralement analogiques couplés à des convertisseurs Analogiques/Numériques.
On trouve en sortie des actionneurs généralement analogiques couplés à des convertisseurs Numériques/Analogiques.
Au milieu, on trouve le calculateur mettant en œuvre un processeur embarqué et ses périphériques d'E/S.

On trouve aussi dans cette architecture:

- Un circuit FPGA[1] et/ou un ASIC[2] jouant le rôle de coprocesseur afin d'assurer des accélérations matérielles au processeur.

[1] FPGA : Field-Programmable Gate Array) : Circuit intégré composé de nombreuses cellules logiques élémentaires reprogrammables après fabrication.
[2] ASIC :(Application-Specific Integrated Circuit) : Circuit intégré configure pour réaliser une tâche spécifique.

- Ports de diagnostic utilisés pour la configuration du système et le débogage (USART[3], JTAG[4], etc.)
- Interfaces Homme-Machine (IHM) permettant à l'utilisateur d'interagir avec le système (écran LCD[5], etc.).
- Des systèmes auxiliaires qui peuvent compléter le système existant afin de réaliser plus de fonctionnalités.

Cette architecture peut varier selon les systèmes: on peut par exemple, ne pas trouver de systèmes auxiliaires dans de nombreux systèmes embarqués.
De même l'interface IHM n'est pas souvent existante, mais est souvent utile pour reconfigurer le système ou vérifier son comportement.

Le fonctionnement du système se résume ainsi:

- Il reçoit des informations de l'environnement extérieur qu'il convertit en signaux numériques
- L'unité de traitement composée de CPU[6], de la mémoire, du logiciel, de l'ASIC et éventuellement de systèmes externes, elle traite l'information
- Le traitement génère éventuellement une sortie qui est envoyée vers la sortie, les systèmes auxiliaire, les ports de monitoring ou l'IHM.

On présente dans ce qui suit les composants matériels essentiels d'un système embarqué:

V.1 Le processeur:[SE10]

Le processeur est le cerveau de l'ordinateur. Il permet de manipuler des informations numériques et d'exécuter les instructions stockées en mémoire.

Le premier microprocesseur (Intel 4004) a été inventé en 1971. Il s'agissait d'une unité de calcul de 4 bits, cadencé à 108 kHz. Depuis, la puissance des microprocesseurs augmente exponentiellement.

- Fonctionnement :

Le processeur est un circuit électronique cadencé au rythme d'une horloge interne, grâce à un cristal de quartz qui, soumit à un courant électrique, envoie des impulsions, appelées « top ». La fréquence d'horloge (appelée également cycle, correspondant au nombre d'impulsions par seconde, s'exprime en Hertz (Hz). Ainsi, un ordinateur à 200 MHz possède une horloge envoyant 200 000 000 de battements par seconde.

A chaque top d'horloge le processeur exécute une action, correspondant à une instruction ou une partie d'instruction. L'indicateur appelé CPI (*cycle per instruction*) permet de représenter le nombre moyen de cycles d'horloge nécessaire à l'exécution d'une instruction sur un microprocesseur. La puissance du processeur peut ainsi être caractérisée par le nombre d'instructions qu'il est capable de traiter par seconde. L'unité utilisée est le MIPS (*million instructions per second*) correspondant à la fréquence du processeur que divise le *CPI*.

[3] USART :(Universal Synchronous/Asynchronous Receiver Transmitter) : interface de communication série en mode synchrone ou asynchrone.
[4] JTAG : (Joint Test Action Group) : utilisé au lieu du terme générique Boundary Scan pour désigner le port de teste des cartes électroniques.
[5] LCD (Liquid Crystal Display) : écran à cristaux liquides.
[6] CPU: (Central Processing Unit).

V.2. Les mémoires [SE9]

La mémoire est un dispositif électronique qui sert à stocker des informations. C'est un composant essentiel, présent dans de nombreux appareils électroniques.
Il existe plusieurs types de mémoires qu'on peut classer selon différents critères :

V.2.1 Les mémoires volatiles (RAMs) :

Sont des mémoires qui ont besoin d'alimentation électrique continue pour conserver les données qui y sont enregistrées, elles sont à accès aléatoire en lecture et en écriture.
On retrouve deux types de mémoires volatiles :

- *Mémoires dynamiques (DRAM : Dynamic Random Access Memory)* : grande densité de sauvegarde, relativement lentes, elles contiennent le programme en exécution et ses données de travail.
- *Mémoires statiques (SRAM : Static Random Access Memory*): petite densité de sauvegarde, très rapides, coutent cher, utilisées surtout dans les mémoires cache et Scratchpad pour exécuter des portions de code les plus fréquentes ou les plus critiques.

V.2.2 Les mémoires non volatiles (ROMs) :

Appelées aussi mémoires mortes, L'utilité première de ce type de mémoire est de pouvoir conserver un logiciel ou un programme embarqué, qui ne s'efface jamais, même quand il n'y a plus de traitements numériques, ou même de coupure du courant.

Cette mémoire (contenant le programme ou les données numériques) reste en permanence intacte, même si l'ordinateur est éteint.
Nous pouvons distinguer plusieurs types de mémoires ROM *(Read Only Mémory),* depuis l'évolution de l'électronique et des besoins :

- La ROM : mémoire seulement lisible, mais non modifiable (impossible d'écrire dedans).
- La PROM *(Programmable Read Only Memory)* : idem que la ROM, sauf que le fabricant du composant de la mémoire, n'inscrit rien dedans, et laisse la possibilité d'écrire une seule fois un programme ou des données. Ce processus est appelé « burning».
- L'EPROM *(Erasable Programmable Read Only Memory)* : elle laisse la possibilité à un système de propagation U.V. de pouvoir la modifier. Généralement, un programme embarqué revient à son état initial sous une intensité suffisante de rayons d'U.V.

- L'EEPROM (*Electrically Erasable Programmable Read Only Memory)* : c'est la ROM la plus évoluée des quatre catégories, car elle a la possibilité d'être écrite et effacée de façon électrique. Pour cela, des impulsions électriques sont envoyés vers la mémoire EEPROM, provoquant l'écriture ou l'effacement. Elle est utilisée tout simplement par la carte mère de l'ordinateur, on l'appel alors la mémoire CMOS *(Complementary metal-oxide semiconductor),* et peut à tout moment être modifié

V.3 Les périphériques d'entrée/sortie :

Contrairement aux ordinateurs conventionnels, les périphériques des systèmes embarqués sont plus nombreux mais leur rôle est le même c.à.d. qu'ils permettent au processeur d'être en communication avec l'environnement extérieur à l'aide des interfaces d'entrées/sorties.
Les périphériques typiques des systèmes embarqués sont :

- Interfaces de communication série : USART, I2C[7], SPI[8], USB[9], etc.
- Les cartes multimédias (cartes SD, Compact Flash, etc.).
- Réseaux: Ethernet.
- Entrée/sortie discrète: General Purpose Input / Output (GPIO).
- Convertisseur Analogique-Numérique / Convertisseur Numérique-Analogique (CAN /CNA).

VI. Systèmes d'exploitation pour systèmes embarqués : [SE5]

Pour qu'un ordinateur soit capable de faire fonctionner un programme informatique (appelé parfois application ou logiciel), la machine doit être en mesure d'effectuer un certain nombre d'opérations préparatoires afin d'assurer les échanges entre le processeur, la mémoire, et les ressources physiques (périphériques).

Le système d'exploitation est chargé d'assurer la liaison entre les ressources matérielles, l'utilisateur et les applications. Ainsi lorsqu'un programme désire accéder à une ressource matérielle, il ne lui est pas nécessaire d'envoyer des informations spécifiques au périphérique, il lui suffit d'envoyer les informations au système d'exploitation, qui se charge de les transmettre au périphérique concerné via son pilote.

Il est difficile de recenser les nombreux systèmes d'exploitation embarqués existants d'autant que certains industriels ont parfois développé leurs propres systèmes afin de satisfaire des besoins ou des normes très particulières. Voici quelques exemples :

- **VxWorks :** le premier système d'exploitation temps réel, fournit une famille de produits qui offrent toute l'évolutivité, la sécurité et la virtualisation nécessaire pour relever les défis actuels de développement pour la construction intelligente. Il est le plus utilisé dans l'industrie.

- **TinyOS :** est un système d'exploitation open-source conçu pour des réseaux de capteurs sans fil. TinyOS est prévu pour fonctionner sur une multitude de plateformes.

[7] I2C ou IIC: Inter Integrated Circuit.
[8] SPI: Serial Peripheral Interface.
[9] USB : Universal Serial Bus.

- **Android :** est un système d'exploitation fondé sur un noyau Linux, Open Source pour tablettes tactiles, terminaux mobiles et TV connectées. Il a été conçu en 2007, par la société Android.

- **PalmOS :** gestion simplifiée de la mémoire, primitives de gestion de bases de données et de l'écran, bibliothèques mathématiques, applications minimalistes (philosophie du Palm), mono-application et mono-thread, ne nécessite pas beaucoup de puissance.

- **Windows CE :** tous les services d'un Windows, victime d'une réputation de fiabilité approximative, la portabilité des applications, pas de gestion du temps-réel, nécessite un processeur très puissant (ARM 400MHz).

- **Symbian OS :** orienté téléphonie, gestion des contacts, gestion de réseaux, divers (SMS, BlueTooth, GSM, TCP/IP), gestion multimédia, supporte Java (JavaPhone) et nécessite moins de ressources que Windows CE.

- **RTEMS et eCos :** exécutif configurable pour ne garder que ce qui est nécessaire services de synchronisation gestion du temps, gestion du réseau logiciel libre, ne nécessite pas beaucoup de puissance, Noyau RT, basé sur Linux.
  Largement utilisé (automobile, imprimante, lecteur MP3).

- **Forth :** système et langage de programmation, mono-application mais multi-threads en mode coopératif, permet le test interactif, ne nécessite pas beaucoup de ressources (PIC 16f876, 2k de programme, 80 octets de RAM).

VII. Langages de développement utilisés : [SE6]

Pour des raisons évidentes de contraintes matérielles, le langage assembleur a longtemps été le choix de prédilection des technologies de l'embarqué car il permettait à la fois d'optimiser la taille du code généré mais aussi ses performances et il permettait aux développeurs d'avoir un contrôle total sur le processeur et le matériel.

La gestion d'un projet complexe écrit en assembleur est cependant difficile et coûteuse, et le code assembleur manque de portabilité, cela a conduit à l'utilisation de l'assembleur principalement comme un complément aux langages de haut niveau, de plus, l'évolution des performances du matériel et des compilateurs permet aujourd'hui de se tourner vers des solutions plus confortables.

Aujourd'hui, le C est le langage de programmation le plus utilisé, en effet des compilateurs sont disponibles pour presque chaque processeur en usage. On trouve également un très grand corps de programmeurs expérimentés en C. En outre, le C a l'avantage d'être indépendant du processeur ce qui permet aux programmeurs de se concentrer sur les algorithmes et les applications, plutôt que sur les détails de l'architecture d'un processeur particulier. Le langage C est bien adapté au logiciel embarqué car il permet une programmation relativement proche du matériel (a une nature « de bas niveau »), il donne aux programmeurs en systèmes

embarqués un haut degré de contrôle direct sur le matériel sans sacrifier les avantages des langages de haut niveau.

Le langage C++ est aussi l'un des choix favori des développeurs, il représente la version orientée objet du C qui offre une meilleure abstraction des données.

D'autres langages orientés objet sont utilisés, et celui qui s'impose est le Java notamment Java Android qui est utilisé pour développer des applications destinées au système qui porte le même nom (Android), et qui est l'un des systèmes les plus connus pour la téléphonie mobile et les tablettes.

Dans le cas de l'utilisation de systèmes de type Unix, on pourra également employer d'autres langages de programmation ou langages de scripts plus appropriés dans certains cas. On citera en particulier le shell-script, langage de script d'Unix (ou Bourne shell) qui associé à d'autres commandes pourra se révéler très utile dans l'écriture de procédures systèmes.

D'autres langages de scripts célèbres dans le monde Unix comme Python, Perl ou Tcl/Tk sont aussi utilisés dans les environnements embarqués.

VIII. Domaines d'application des systèmes embarqués

Les domaines dans lesquels on trouve des systèmes embarqués sont de plus en plus nombreux :

- Installations industrielles (chimique, nucléaire, automobile, …)
- Astronautique : fusée, satellite artificiel, sonde spatiale, etc.
- Electroménager : télévision, four à micro-ondes
- Équipement médical
- Guichet automatique
- Domaine militaire : missile
- Multimédia : console de jeux vidéo, assistant personnel
- Télécommunication : Téléphonie, routeur, pare-feu, serveur de temps, Téléphone portable, etc.
- Transport : Automobile, Aéronautique (avionique), …etc.
- Domotique
- Périphériques informatiques : imprimantes, photocopieurs .

Dans ce qui suit, on présente deux exemples détaillés des domaines d'application des systèmes embarqués.

➢ Les transports intelligents

Les systèmes d'aide à la conduite sont un secteur en pleine mutation. La plupart des systèmes actuels présents en série dans les véhicules ont pour objectif de pallier aux défaillances du conducteur, mais l'évolution récente est d'ajouter l'intégration d'objectifs de confort ou d'efficacité énergétique. Les systèmes d'aide à la conduite agissent sur la sécurité soit en aidant le conducteur à éviter un accident ou une situation à risque, soit en cherchant à en minimiser les conséquences. Les principales catégories de fonction d'assistance sont les suivantes :

- Appel d'urgence: C'est un boitier capable de détecter un choc et donc de pouvoir prévenir plus rapidement les secours. Ces systèmes équipent parfois certains éléments de l'infrastructure.
- Assistance au freinage d'urgence : Il s'agit de systèmes de freinage électronique ou de systèmes de freinage antiblocage.
- Avertisseur d'obstacle et de collision : Un radar à l'avant du véhicule permet de mesurer la distance avec le véhicule le plus proche et donc de prévenir le conducteur en cas de risque.
- ESP *(Electronic stability program)* : Un équipement électronique permettant de stabiliser les trajectoires. Il existe aussi des systèmes de surveillance de trajectoire latérale LDW *(Lane Departure Warning).*
- Visibilité en conditions dégradées : L'objectif est d'améliorer la visibilité du conducteur à l'aide de caméras capables de voir dans la nuit ou dans le brouillard.
- Systèmes régulateurs de vitesse : Il s'agit des très communs régulateurs et limiteurs de vitesse, mais on trouve de plus en plus le régulateur de vitesse adaptatif. Une évolution récente non encore commercialisée est le limiteur adaptatif de la vitesse.

➢ Système de surveillance et de contrôle d'accès

La sécurité revêt une importance primordiale pour toutes les entreprises, que ce soit pour un système de surveillance, un système de contrôle d'accès ou encore un système de protection contre les incendies**.**

La surveillance peut être secrète ou évidente. Celle-ci a toujours été présente dans l'histoire humaine. Un système d'alarme contre intrusion peut informer les responsables d'un intrus, même si les habitants sont loin.

Un système d'alarme contre les incendies est un dispositif électronique permettant de détecter un départ de feu dans un bâtiment, et de gérer la sécurisation des personnes se trouvant dans celui-ci. Techniquement on appelle l'ensemble du dispositif un "Équipement d'Alarme".

Le contrôle d'accès devient de plus en plus populaire dans beaucoup d'entreprises, toutes catégories confondues. La capacité de limiter l'accès à des personnes pré-autorisées pour des salles d'entrainement, ou à circuler dans les différents départements de l'entreprise est certainement très attrayante.

IX. Conclusion :

Dans ce chapitre on a présenté des généralités sur les systèmes embarqués, en ce qui concerne l'architecteur matérielle, les systèmes et les langages utilisés, les contraintes qu'il faut prendre en considération lors de la conception de ces systèmes. Et parmi les champs d'application des systèmes embarqués on a cité le contrôle d'accès, ce dernier peut être assuré par plusieurs techniques et technologies, l'identification par radio fréquence est l'une de ces technologies qu'on va présenter dans le chapitre suivant.

Introduction Générale

Les nouvelles technologies de l'information et de la communication (les NTIC) ont un rôle fondamental dans notre société moderne. Elles participent à sa transformation par différents effets sur les plans économiques et sociaux. Le développement de ces technologies est initié par des découvertes scientifiques, lesquelles permettant de nouvelles applications technologiques, elles-mêmes participant au partage de la connaissance. Les technologies d'identification font partie de ces technologies de l'information. Elles trouvent leurs applications dans des domaines très divers tels que la logistique, la traçabilité, le transport la sécurité ou les loisirs. Jusqu'alors les technologies d'identifications étaient soit sans contact: marquage, code à barre, soit nécessitaient un contact : carte bancaire, carte d'appels téléphoniques…etc. Grâce au développement récent des systèmes sans fil et de la micro-électronique, d'autres nouvelles technologies d'identification sans contacts ont vu le jour : les technologies de radio-identification (ou RFID pour Radio-Frequency IDentification). Ces nouvelles technologies, par leur plus grande souplesse, rendent l'échange d'informations nettement plus rapide et efficace.

La technologie RFID est largement utilisée dans plusieurs domaines, l'identification d'objets ou de personnes, d'en suivre le cheminement et elle permet d'en connaitre les caractéristiques à distance grâce à une étiquette émettant des ondes radio attachée ou incorporée à l'objet ou à la personne (traçabilité), contrôler l'accès à une zone, puisque dans tous les endroits il y a un groupe de personnes qui partagent un espace commun, et personne ne souhaite voir son personnel mis en danger, et il n'existe pas de meilleures solutions que de sécurisé les accès (aux bâtiments, aux universités…etc.) avec un système de contrôle d'accès intelligent et fiable, qui permet d'isoler des zones précises et d'identifier tous les mouvements dans cette zone. Le système permet de gérer les ouvertures de portes automatiquement sans intervention humaine, garder un historique sur les entrées en temps réel pour chaque personne demandant l'accès grâce à un badge personnel (tag RFID) qui identifie chaque personne. La lecture de ces tags se fait par le lecteur RFID

C'est dans ce cadre que se situe notre projet de fin d'études intitulé «contrôle d'accès à base de la technologie RFID ». Notre travail consiste à concevoir un système embarqué afin d'assurer le contrôle d'accès à des zones particulières à base de la technologie RFID

Pour ce faire, nous avons divisé notre travail en quatre chapitres. Dans le premier chapitre on a présenté des généralités sur les systèmes embarqués, telles que l'architecteur matérielle, les systèmes et les langages utilisés, les contraintes qu'il faut prendre en considération lors de la conception de ces systèmes embarqués.
Le deuxième chapitre est constitué de deux parties, dans la première partie on a décrit la technologie RFID : son historique, son fonctionnement, ses composants, ses avantages et ses inconvénients dans la deuxième partie nous avons illustré quelques principes du contrôle d'accès.
Le troisième chapitre est consacré à l'analyse et conception de notre système.

La réalisation de notre application sera présentée, dans le quatrième chapitre, dans lequel nous présenterons l'environnement de développement et les divers composants implémentés dans l'architecture de notre système.
Nous finirons ce rapport par une conclusion générale.

CHAPITRE 2

Généralités sur les RFID
Et contrôle d'accès

Introduction

Le contrôle d'accès est une technique qui consiste à soumettre l'entrée d'un établissement ou, de locaux à l'intérieur d'une entreprise, à une autorisation d'accès à base de la technologie RFID (*Radio Fréquence IDentification*)

La RFID est une technologie alliant la flexibilité d'utilisation des ondes radiofréquences à faible coût. Basée sur la transmission d'ondes RF (*Radio Fréquence*).

Ce chapitre est structuré en deux partie, la deuxième partie décrit le contrôle d'accès, et dans la première nous présentons d'une manière sommaire la technologie RFID, son historique, son principe de fonctionnement, les éléments qu'ils la composent tels que lecteurs et étiquettes,…etc.

Partie 1 : Généralités sur les RFIDs

La radio-identification, plus souvent désignée par le sigle RFID ("Radio Frequency IDentification") est une méthode développée pour mémoriser et récupérer des données à distance en utilisant des marqueurs appelés radio-étiquettes ("Tag RFID ").

Cette technologie permet d'identifier un objet, d'en suivre le cheminement et d'en connaître les caractéristiques à distance grâce à une étiquette émettant des ondes radio, attachée ou incorporée à l'objet. La technologie RFID permet la lecture des étiquettes même sans ligne de vue directe et peut traverser de fines couches de matériaux (peinture, neige, etc.).[RF1]

I. Historique de la RFID: [RF2]

La technologie RFID a connu ses premiers pas dans les années 40, elle fut inventée au Royaume-Uni en 1939. Les RFID se sont ensuite développées comme suit :

1940

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

1970

Durant les années 1960-1970, les systèmes RFID restent une technologie confidentielle, à usage militaire pour le contrôle d'accès aux sites sensibles, notamment dans le nucléaire.

1980

Les avancées technologiques permettent l'apparition du tag passif. Le tag RFID rétromodule l'onde rayonnée par l'interrogateur (lecteur) pour transmettre des informations. Cette technologie permet de s'affranchir de source d'énergie embarquée sur l'étiquette réduisant de ce fait son coût et sa maintenance.

1990

Débute de la normalisation pour une interopérabilité des équipements RFID.

1999

Fondation par le MIT *(Massachusetts Institute of Technology)* de l'Auto-ID center : centre de recherches spécialisé en identification automatique (entre autre RFID).

2004

L'auto-ID du MIT devient "EPCglobal", une organisation chargée de promouvoir la norme EPC (Electronic Product Code), extension du code à barre à la RFID.

A partir de 2005

Les technologies RFID sont aujourd'hui largement répandues dans quasiment tous les secteurs industriels (aéronautique, automobile, logistique, transport, santé, vie quotidienne, etc.). L'ISO (*International Standard Organisation)* a largement contribué à la mise en place de normes tant techniques qu'applicatives permettant d'avoir un haut degré d'interopérabilité voire d'interchangeabilité.

2009

Une ambition : faciliter l'adoption de la RFID / NFC / Objets Connectés et développer ses usages et fédérer les initiatives au plan national

Créé en 2008 par le Ministère de l'Economie, de l'Industrie et du Numérique, le Centre National de Référence RFID a pour vocation de faciliter l'adoption et l'appropriation des technologies sans contact (RFID et NFC).

II. Le fonctionnement d'un système RFID et ses composants [RF3]

Un système RFID se compose principalement d'un ou de plusieurs lecteurs, d'une ou plusieurs étiquettes (tags) et d'un logiciel d'application (middleware). La figure suivante décrit le schéma général d'un système RFID

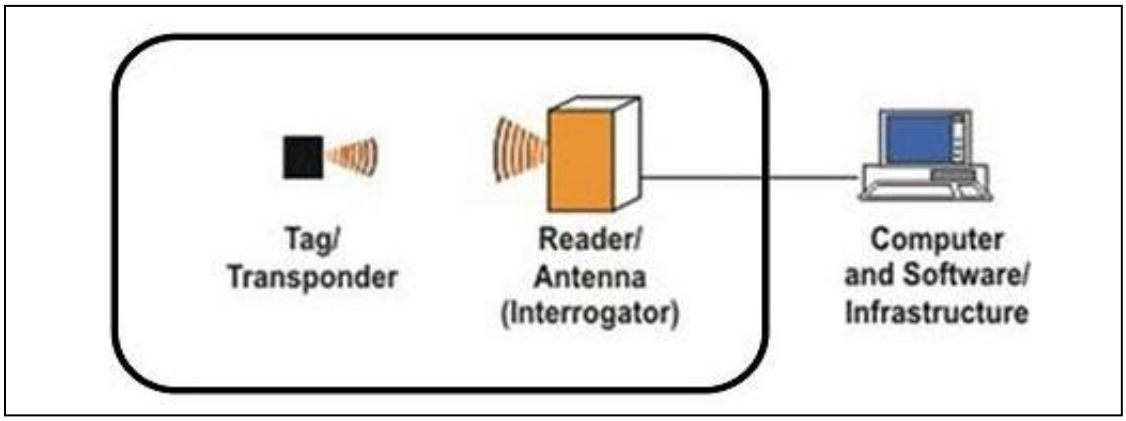


Fig II.1 : Les éléments d'un système RFID

II.1 Le fonctionnement

Le lecteur agit généralement en maître par rapport au tag; si le tag est dans la zone de lecture du lecteur, ce dernier l'active en lui envoyant une onde électromagnétique puis entame la communication et l'échange de données. Le lecteur est relié à un hôte d'application qui récupère l'information pour le logiciel d'application. Un lecteur RFID est donc chargé de l'interface avec le système global relatif à l'application et de la gestion de l'identification des tags qui se présentent à lui. Le tag est, quand à lui, constitué d'une antenne et d'une puce électronique miniature.

La liaison entre le lecteur et l'hôte de l'application peut être une liaison sans fil. Le lecteur interroge les étiquettes passives ou semi-actives en leurs envoyant la commande et l'énergie nécessaire pour interagir avec lui et dans le cas où le tag est actif c'est à dire possède sa propre batterie, il peut initier la communication.

II.2 Les composants

- L'étiquette :

L'étiquette (tag) appelée aussi transpondeur, pour transmitter–responder comprend une puce, dotée d'une mémoire et d'un microprocesseur, reliée à une antenne bobinée et lue par un lecteur captant et transmettant l'information.

Ces tags peuvent alors être incorporés dans des objets ou être collés sur des produits. Le format des données inscrites sur les étiquettes est standardisé à l'initiative d'EPC Global (*Electronic Product Code).*

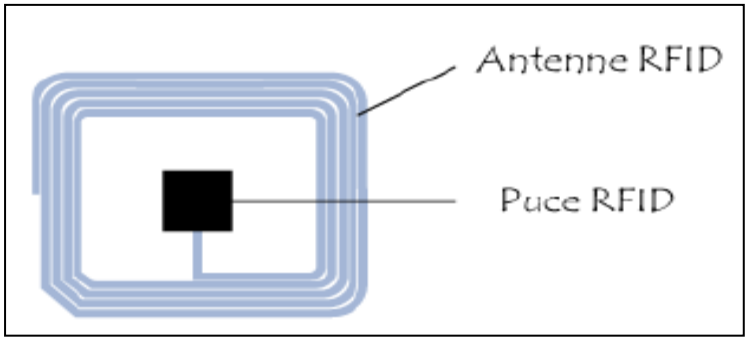


Fig II.2 : L'étiquette RFID

Il existe 3 types d'étiquettes (tag) : [RF4]

- Tag passif : ce sont les moins chers aujourd'hui. Ils ne possèdent pas leur propre alimentation en énergie et ne sont donc activés que par le signal de la base station qui leur sert d'alimentation en énergie. On dit que le transpondeur est télé- alimenté. Le tag ne peut pas émettre de signaux par lui même sans être préalablement interrogé par la base station.
- Tag semi-passif : possédant sa propre source d'alimentation en énergie, cela permet d'augmenter les distances de communication, mais fait également augmenter le coût et la taille du tag. En revanche, ces tags ne peuvent toujours pas émettre de signaux eux même.
- Tag actif : ces derniers possèdent un émetteur à haute fréquence ce qui leur permettent d'émettre sans être obligatoirement interrogés préalablement par la base station. Pour pouvoir émettre de lui même ce tag a besoin d'énergie, c'est pourquoi il embarque presque toujours un système d'alimentation. Il permet donc une plus grande distance de communication.

- Le lecteur **:**

Le lecteur RFID est un émetteur-récepteur radio spécialisé. Il doit générer des signaux à la fréquence porteuse et moduler ces signaux pour transmettre des informations aux tags. Il doit recevoir et identifier sélectivement des réponses à partir des tags. Pour cela, il est doté de circuits de démodulation et de fonctions de traitement lui permettant d'adresser et de communiquer sélectivement et individuellement avec tout tag dans son champ de lecture.
Ainsi le lecteur RFID est l'élément responsable de la lecture des tags radiofréquence et de la transmission des informations qu'elles contiennent (code EPC, information d'état, clé cryptographique…) vers le niveau suivant du système (middleware).

- Le middleware (ou intergiciel):

Un middleware, est un logiciel intermédiaire entre le réseau et le matériel d'une part, et les applications d'autre part. Cet intergiciel permet de collecter, de filtrer et d'agréger les données. Cela permet aussi une gestion plus facile des différents lecteurs.
Un intergiciel pour étiquettes électroniques est un logiciel tiers destiné à simplifier l'accès et l'exploitation des informations stockées dans des étiquettes RFID.
Le but d'un intergiciel entre le réseau et les applications est d'accomplir les taches techniques et les échanges de données. Dans les systèmes RFID, un intergiciel doit gérer les lecteurs, qui sont souvent hétérogènes, doit traiter les évènements issus des lecteurs RFID, et doit être connecté aux applications. Dans certains cas, il n'y a pas besoin d'intergiciel, comme dans le cas d'une petite et unique application telle que « compter le nombre d'identifiants lus », ou encore « lire les étiquettes dans le champs du lecteur »

III. Les composants d'une étiquette RFID [RF5]

Une étiquette RFID est composée d'une puce RFID et une antenne

III.1 Puce RFID :

La technologie des puces d'identification RFID est très étendue, elle permet de s'adapter à des multitudes de situations, l'identification, et d'embarquer d'autres informations sur le transpondeur (tag). Mais le besoin de chaque entreprise étant différent, il existe différents

modes de fonctionnement des transpondeurs que l'on peut regrouper sous deux différentes catégories :

- Les puces à usage unique (lecture seule) : la puce contient des données qui sont lues par le lecteur RFID sans possibilité de les modifier. C'est le mode de fonctionnement le plus simple du transpondeur et qui sert principalement pour les problèmes traitant seulement l'identification. Le transpondeur peut être lu uniquement par le lecteur, le transpondeur possède juste les informations qui ont été écrites par le fabriquant du tag. Ces informations peuvent être choisies par l'entreprise, mais une fois ces informations écrites, le transpondeur ne peut être que lu.
- Les puces réinscriptibles (lecture/écriture) : les données inscrites sur la puce peuvent être modifiées par le lecteur RFID selon les deux modes suivants :

Lecture/écriture unique : ce mode de fonctionnement est similaire à la lecture seule sauf que cette fois ci, le transpondeur livré par le fabriquant est vierge, il ne contient aucune information. C'est l'utilisateur du transpondeur qui va pouvoir écrire des informations dessus. Les informations ne peuvent être écrites qu'une seule fois, ensuite le transpondeur se comporte comme un transpondeur en lecture seule.

Lecture/écriture multiple : dans ce mode de fonctionnement, le transpondeur peut être livré vierge ou avec des informations. Mais les informations peuvent être effacées et réécrites par l'utilisateur du transpondeur presque autant de fois qu'il le souhaite. Ce type de transpondeur est très utile lorsque l'on vient écrire des informations à différents moments d'un processus ou bien lorsque l'on souhaite réutiliser les transpondeurs avec de nouvelles informations.

III.2 Antenne RFID :

L'antenne RFID est un élément primordial du système RFID qui est généralement intégré au lecteur RFID et à l'étiquette RFID, elle permet de transmettre les informations et d'activer les tags afin de recevoir des données dans le cas des étiquettes passives et semi-passives.
Le choix du type de l'antenne à intégrer au lecteur RFID diffère selon le type de lecture, le type d'étiquette, l'utilisation du système RFID…etc. Ainsi, deux types principaux d'antennes se distinguent :

- les antennes intégrées : elles sont intégrées au lecteur, leur utilisation est conseillée pour les lecteurs de basse fréquence à portée limitée.
- les antennes externes : elles ne font pas partie du lecteur, elles sont plus puissantes et s'avèrent donc utiles pour obtenir une plus grande portée.

IV. Les gammes de fréquences RFID [RF6]

Les systèmes RFID génèrent et réfléchissent des ondes électromagnétiques. Les systèmes RFID doivent notamment veiller à ne pas perturber le fonctionnement des autres systèmes radio. On ne peut, en principe, utiliser que les plages de fréquences spécifiquement réservées aux applications industrielles, scientifiques ou médicales. Ces plages de fréquences sont

appelées ISM (Industriel – Scientifique – Médical). Les principales plages de fréquences utilisées par les tags d'un système RFID sont :

- Les tags **RFID UHF à 900 MHz** possèdent des antennes imprimées ou gravées. En technologie passive, ils peuvent être lus à plusieurs mètres. Ils sont plus sensibles à l'environnement (métal, eau) du fait de la fréquence utilisée mais des designs particuliers d'antenne et de packaging permettent de les utiliser sur des supports métalliques. Les fréquences UHF réservées à la RFID n'étant pas harmonisées dans toutes les régions du monde (entre 860 et 960 MHz), les tags doivent généralement présenter des bandes passantes importantes qui réduisent leurs performances.

- Les tags **RFID HF 13.56 MHz** sont utilisés dans des applications de logistique et de traçabilité. Les antennes boucle peuvent être imprimées ou gravées ce qui rend les tags particulièrement fins. Ils sont largement répandus dans les applications de transport et d'identité (passeport, cartes sans contact…etc.). Cette technologie est à la base des applications NFC *(Near Field Communication*).

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

V. Les normes RFID [RF7]

Pour une interopérabilité, les équipements RFID (lecteurs et tags) doivent impérativement être normalisés quant à leur mode de fonctionnement soit, pour une fréquence d'utilisation donnée, que n'importe quel tag soit lu par n'importe quel lecteur. On parle alors de protocole de communication.
Le développement de standards est la responsabilité du comité technique de l'ISO.
L'ISO est l'union internationale des institutions nationales de standardisation, comme la DIN (Allemagne), l'ANSI (USA), l'AFNOR (France) ou la SNV (Suisse).
Les tags RFID fonctionnent selon des normes comme l'ISO 14443 (13.56 MHz) ou EPCglobal 96-bits (915 MHz).

VI. Les Avantages et les inconvénients [RF8]

Comme toute technologie, la RFID a des avantages comme elle a des inconvénients

VI.1 Les Avantages

Par rapport aux techniques d'identification classiques, les technologies RFID apportent une souplesse et des gains de productivité considérables. Elles permettent un gain de temps ainsi qu'une optimisation des opérations de lecture et améliorent la fiabilité et les capacités du système de traçabilité.

- Une sécurité d'accès au contenu

Comme tout support numérique, l'étiquette radio fréquence peut être protégée par mot de passe en écriture ou en lecture. Les données peuvent être chiffrées. Dans une même étiquette,

une partie de l'information peut être en accès libre, et l'autre protégée. Cette faculté fait de l'étiquette RF, un outil adaptée à la lutte contre le vol et la contrefaçon

- Lecture en masse d'étiquettes **:**

La technologie permet de lire un grand nombre d'étiquettes simultanément. Une palette complète de cartons ou produits peut ainsi être lue automatiquement au passage dans un système de lecture RFID.

- Evolutivité des informations :

La fonctionnalité de lecture/écriture permet de faire évoluer les informations stockées dans l'étiquette et ainsi de suivre le cycle de vie d'un objet ou d'un produit. Elle permet également une réutilisation des étiquettes.

- Une plus grande durée de vie

Dans les applications où un même objet peut être utilisé plusieurs fois, comme l'identification des supports de manutention, une étiquette radio fréquence peut être réutilisée 1 000 000 de fois.

- Une plus grande souplesse de positionnement

Avec l'étiquette radio fréquence, il est possible de s'abstraire des contraintes liées à la lecture optique, elle n'a pas besoin d'être vue. Il lui suffit d'entrer dans le champ du lecteur pour que sa présence soit détectée.

- Identification d'un produit de manière unique:

La technologie RFID permet de disposer d'un numéro unique d'identification dans chaque puce RFID afin d'identifier chaque objet d'une manière unique.

VI.2 Les inconvénients

- La perturbation par l'environnement physique

La lecture des étiquettes radio fréquence est perturbée par la présence, par exemple, de métaux dans leur environnement immédiat.

- Les perturbations induites par les étiquettes entre elles

Dans de nombreuses applications, plusieurs étiquettes radio fréquence peuvent se présenter en même temps dans le champ du lecteur volontairement ou involontairement. Ceci peut être voulu en magasin, au moment du passage à la caisse ou entre les portiques antivol.

- La sensibilité aux ondes électromagnétiques parasites

Les systèmes de lecture RFID sont dans certaines circonstances sensibles aux ondes électromagnétiques parasites émises par des équipements informatiques (des écrans d'ordinateurs) ou des systèmes d'éclairage plus généralement par les équipements électriques. Leur emploi doit donc être testé en tenant compte de l'environnement.

- Les interrogations sur l'impact de la radio fréquence sur la santé

Cette question fait débat depuis quelques années, en particulier concernant les portiques antivol et les téléphones portables. Les étiquettes passives ne présentent aucun risque quel que soit leur nombre puisqu'elles ne sont actives que lorsqu'elles se trouvent dans le champ d'un lecteur. Les études portent donc essentiellement sur les lecteurs et visent à définir les critères de régulation de leur puissance d'émission afin d'éviter qu'ils ne créent des perturbations sur les équipements de santé tels que les pacemakers (stimulateur cardiaque), mais aussi sur l'organisme humain.

- Sécurité et vie privée

L'utilisation d'ondes électromagnétiques pour transmettre des données entre deux dispositifs rend cette technologie intrusive et vulnérable aux attaques basées sur l'utilisation de la radiofréquence.

VII. Domaines d'application de RFID [RF9]

La technologie RFID est présente dans des domaines de plus en plus divers comme dans la sécurité, transport, logistique, fidélisation client, paiement, santé … etc.

- Les cartes de fidélité peuvent être renouvelées par le système RFID :

Le sans contact trouve également son application dans le secteur des cartes de fidélité. Equipés d'une carte de fidélité avec un tag RFID, les clients peuvent utiliser la borne pour connaître leur nombre de points ou se voir proposer des réductions. Le système est aussi lié au téléphone portable du client, qui peut recevoir des messages par SMS

- RFID est très utilisée dans les transports en commun :

Une des applications les plus connues et les plus démocratisées de la technologie RFID reste la carte de transport sans contact. L'usager du métro passe sa carte sur une base (généralement apposée à des tourniquets d'accès), qui l'authentifie, valide son titre de transport, et lui donne accès au réseau…

- La RFID et les documents d'identité

L'identification des individus passe aussi par l'authentification des papiers d'identité. La RFID est alors un moyen, d'une part, de s'assurer de la validité des documents, mais aussi de s'assurer que les informations contenues dans le passeport le sont également d'un point de vue numérique.

- La RFID pour améliorer l'hôpital

Dans le domaine de la santé, la localisation des patients et le suivi des processus de soins trouvent une synergie toute particulière grâce aux applications rendues possibles par la RFID.
Personnel comme patients sont ainsi équipés de tags qui permettent à la fois de les situer précisément dans l'établissement, et de vérifier que les parcours de soins sont correctement effectués.

- La RFID pour suivre les animaux domestiques

Accroché au collier d'un animal domestique, un boitier contenant un tag RFID permet de constituer des historiques des différentes activités, de son alimentation, ou encore de son état de santé. Il est également possible de suivre son animal à distance, via un portail Internet, pour connaître l'activité d'un animal pendant que le maître est absent.

- Contrôle d'accès des personnes

Dans les installations de fabrication, les laboratoires sécurisés, les entrées des sociétés et les bâtiments publics, les droits d'accès doivent être contrôlés. Ceci se fait grâce à la technologie RFID.

Partie 2 : contrôle d'accès

I. introduction

Le contrôle d'accès consiste à vérifier qu'une personne a bien les droits nécessaires pour accéder à un lieu, un bâtiment ou un local. Il permet d'organiser la circulation des personnes à l'intérieur d'un site et de gérer l'accessibilité des différentes zones de façon sélective. Ainsi, l'accès à des espaces sensibles peut être restreint à des utilisateurs identifiés, selon des plages horaires prédéfinies, avec un enregistrement de tous les déplacements.

II. Le fonctionnement d'un système de contrôle d'accès [CA1]

Quand une personne se présente devant une borne d'un système de contrôle d'accès, cette dernière transmet les informations d'identification présentées à un panneau de contrôle, qui les compare aux données dont il dispose et concernant les personnes autorisées. Le résultat de la comparaison détermine si la demande d'accès est accordée ou pas.

Un journal des transactions est alors mis à jour dans une base de données. Lorsque l'accès est refusé, la porte reste verrouillée. Sinon, le panneau de contrôle fonctionne un relais qui ouvre la porte.

Trois types d'éléments d'authentification de l'information peuvent être utilisés:

- mot de passe
- carte à puce
- empreintes digitales

Les mots de passe sont un moyen courant pour vérifier l'identité des utilisateurs.

III. Les composants de base d'un système de contrôle d'accès [CA2]

Les systèmes de contrôle d'accès varient considérablement dans le type et la complexité. Cependant, la plupart des systèmes de contrôle d'accès à la carte sont constitués d'au moins les composants de base suivants:

Cartes d'accès

La carte d'accès peut être considérée comme une «clé» électronique. La carte d'accès est utilisée par des personnes pour obtenir l'accès à travers les portes sécurisées par le système de contrôle d'accès. Chaque carte d'accès est codée de façon unique. La plupart des cartes d'accès ont à peu près la même taille qu'une carte de crédit standard, et peuvent facilement être transportées dans un porte-monnaie ou un sac à main.

Lecteurs de cartes

Les lecteurs de cartes sont les dispositifs utilisés pour électroniquement "lire" la carte d'accès. Les lecteurs de cartes peuvent être de type «insertion», qui nécessitent l'insertion de la carte dans le lecteur, ou type " proximité", qui ne nécessite que la carte soit à proximité du lecteur. Les lecteurs de cartes sont habituellement montés sur le côté extérieur (non sécurisé) de la porte qu'ils contrôlent.

Accès claviers de commande

Les claviers de contrôle d'accès sont des dispositifs qui peuvent être utilisés en plus ou à la place des lecteurs de cartes. Le clavier de contrôle d'accès a des touches numériques qui ressemblent aux touches d'un téléphone à clavier.

Le clavier de contrôle d'accès exige qu'une personne désirant avoir accès entre un code numérique correct. Lorsque les claviers de contrôle d'accès sont utilisés en plus des lecteurs de cartes, il faut que à la fois la carte soit valide et que le mot de code soit aussi correct pour que l'entrée soit autorisée.

Lorsque les claviers de contrôle d'accès sont utilisés à la place des lecteurs de cartes, seul un code correct est nécessaire pour avoir l'autorisation.

Serrure électrique Hardware

Matériel de verrouillage électrique est l'équipement qui est utilisé pour verrouiller et déverrouiller électriquement chaque porte qui est commandé par le système de contrôle d'accès.

Il existe une grande variété de types différents de matériel de serrure électrique. Ces types comprennent serrures électriques, gâches électriques, serrures électromagnétiques, des dispositifs de sortie électriques.

Dans presque tous les cas, le matériel de verrouillage électrique est conçu pour contrôler l'entrée dans un bâtiment ou dans un espace sécurisé. Pour se conformer aux codes du bâtiment et d'incendie, le matériel de serrure électrique offre la possibilité de quitter librement le bâtiment à tout moment.

Panneaux de champ de contrôle d'accès

Les panneaux de champ de contrôle d'accès (également appelés «contrôleurs intelligents») sont installés dans chaque bâtiment où le contrôle d'accès doit être fourni. Lecteurs de cartes, du matériel de serrure électrique, et d'autres dispositifs de contrôle d'accès sont tous reliés aux panneaux de champ de contrôle d'accès.

Les panneaux de champ de contrôle d'accès sont utilisés pour traiter l'activité de contrôle d'accès au niveau du bâtiment. Le nombre de panneaux de champ de contrôle d'accès à fournir à chaque bâtiment est en fonction du nombre de portes à contrôler. Les panneaux de champ de contrôle d'accès sont généralement installés dans les téléphones, les placards électriques…etc.

L'ordinateur serveur de contrôle d'accès

L'ordinateur serveur de contrôle d'accès est le «cerveau» du système de contrôle d'accès.
Il sert de la base de données centrale et le gestionnaire de fichiers pour le système de contrôle d'accès; et est responsable de l'enregistrement de l'activité du système et la diffusion d'informations vers et depuis les panneaux de champ de contrôle d'accès.
L'ordinateur serveur de contrôle d'accès est habituellement un ordinateur standard qui exécute un logiciel spécial de contrôle d'accès de l'application du système. Dans la plupart des cas, l'ordinateur est dédié pour une utilisation à plein temps avec le système de contrôle d'accès.

IV. Types de lecteurs

La borne comporte souvent un lecteur qui pourrait être un clavier un lecteur de cartes magnétiques ou à puce, ou un lecteur biométrique (à empreintes digitales, par exemple).
Selon leur fonctionnalité, ces lecteurs peuvent être classés:

• Lecteurs de base (non-intelligents): il suffit de lire le numéro de carte ou un code PIN et le transmettre à un panneau de contrôle. Les protocoles les plus utilisés pour transmettre des données au panneau de contrôle sont le RS-232, le RS-485. C'est le type le plus fréquemment utilisé des lecteurs de contrôle d'accès.

• lecteurs semi-intelligents: Ils possèdent toutes les entrées et sorties nécessaires pour contrôler le matériel de porte (serrure, contact de porte, bouton de sortie), mais ne peut pas prendre de décisions d'accès. Quand un utilisateur présente une carte ou saisit son code PIN, le lecteur envoie les informations au contrôleur principal et attend sa réponse. Si la connexion au contrôleur principal est interrompue, ces lecteurs cessent de travailler ou fonctionnent dans un mode dégradé. Habituellement, les lecteurs semi-intelligents sont connectés à un panneau de commande via un bus RS-485.

• lecteurs intelligents: Ils possèdent toutes les entrées et sorties nécessaires pour contrôler la porte ainsi que les outils de décision (base de données, organe de traitement et décision), nécessaires pour prendre des décisions d'accès de manière indépendante. Comme les lecteurs semi-intelligents, ils sont reliés à un panneau de commande via un bus RS-485. Le panneau de commande envoie des mises à jour de configuration et d'événements récupérés des lecteurs.

V. Domaines d'applications

Restreindre l'accès à certaines zones, contrôler, organiser et enregistrer les différents flux de personnes sont les objectifs principaux de nos systèmes de contrôle d'accès. L'utilisation de ces technologies de contrôle d'accès est indispensable pour certain type d'activité et lieu :

- Usines et grandes surfaces
- Locaux et bureaux
- Hôpitaux, cliniques
- Chantiers et entrepôts
- Entrées d'immeubles
- Aéroports
- Banques

Conclusion

Ce chapitre est constitué de deux parties, dans la première partie on a décrit la technologie RFID, son historique, son fonctionnement, ses composants, ses avantages et ses inconvénients. Dans la deuxième partie nous avons illustré quelques principes du contrôle d'accès.
Le chapitre suivant sera consacré à l'analyse et la conception de notre système

Chapitre 3

Analyse et conception

I. Introduction

Le processus de développement d'un système embarqué suit un cycle d'analyse, conception, implémentation, test et déploiement, comme est illustré dans la figure FigIII.1 [Con1]

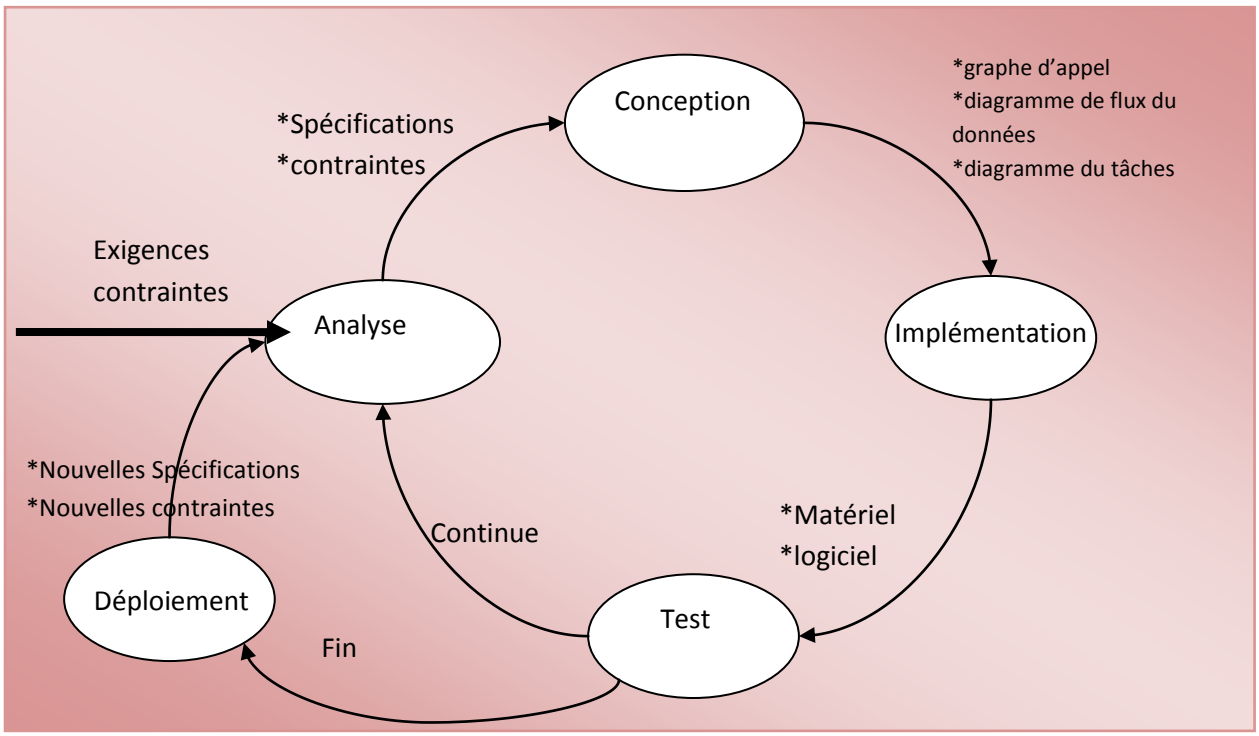


Fig III.1 Le cycle de vie de développement d'un système embarqué

Pour les systèmes complexes avec une longue durée de vie, il faut tourner plusieurs fois autour du cycle de vie. Pour les systèmes simples, un seul passage peut suffire.

Dans ce chapitre nous allons présenter la phase d'analyse et de conception, les autres phases seront présentées dans le chapitre suivant.

II. Analyse

Au cours de la phase d'analyse, nous recensons les exigences et les contraintes de notre système. Les exigences sont des paramètres spécifiques que le système doit satisfaire, et qui sont généralement écrites dans une liste de spécifications détaillées, telle que les spécifications sont des paramètres détaillés décrivant comment le système devrait fonctionner. Les contraintes sont des limitations, dans lesquels le système doit fonctionner.

II.1 Idée générale sur notre travail

Notre travail consiste à concevoir un système embarqué afin d'assurer le contrôle d'accès à des zones particulières et de garantir une meilleure traçabilité à base de la technologie RFID.

Notre système est composé de plusieurs portes, au niveau de chaque porte un lecteur de badge (tag RFID) est installé, ces lecteurs permettent de lire les identifiants des badges présentés par les demandeurs d'accès. Selon les droits d'accès du demandeur, la porte soit elle s'ouvre, soit elle reste fermée. Le fonctionnement de ce système est présenté dans la figure Fig III.2.

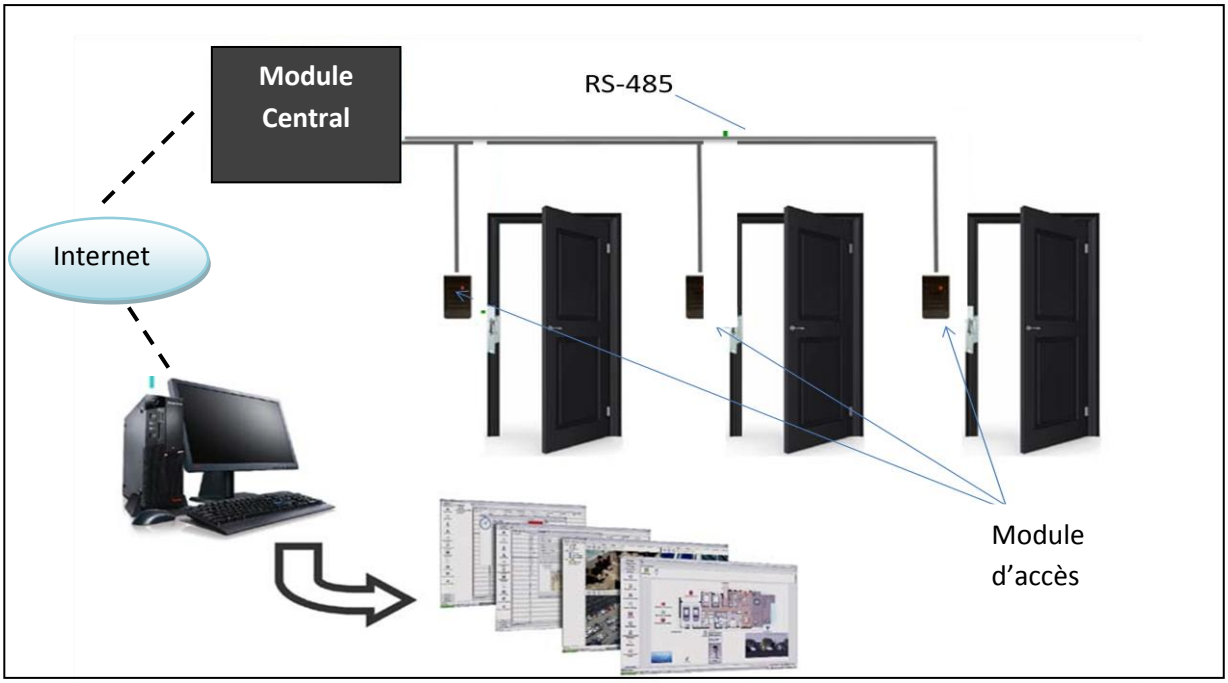


Fig III.2 Le fonctionnement de notre système contrôle d'accès

En cas de demande d'accès, l'utilisateur présente son badge, le lecteur de badge récupère son identifiant, puis via la liaison série RS485, les informations d'identifications sont transmises au module central. Ce dernier compare ces informations aux données dont il dispose. Le résultat de la comparaison détermine si la demande d'accès est accordée ou pas. Lorsque l'accès est refusé, la porte reste verrouillée. Sinon, la porte s'ouvre.

En plus du contrôle d'accès, l'administrateur du système peut procéder à la configuration du système par un logiciel de gestion. Il pourra par exemple ajouter un utilisateur qui a le droit d' y accéder en précisant les différentes zones où il a le droit de rentrer, consulter l'historique, modifier les autorisations d'accès.

II.2 Spécification des exigences fonctionnelles :

Lors de la demande d'accès à une zone, l'utilisateur doit présenter son badge, ayant a un identifiant unique.

Le système doit alors remplir les fonctionnalités suivantes :

- Attente d'un évènement (présentation d'un badge)
- Extraction du contenu (Identifiant)
- L'envoi de l'identifiant ainsi que l'adresse de la porte
- Vérification des droits d'accès
- Enregistrement des informations d'identification en cas d'autorisation
- Enregistrement des tentatives d'accès.
- L'envoi de la réponse (autoriser ou refuser)

On peut résumer le fonctionnement global du système dans le schéma de la figure III.3.

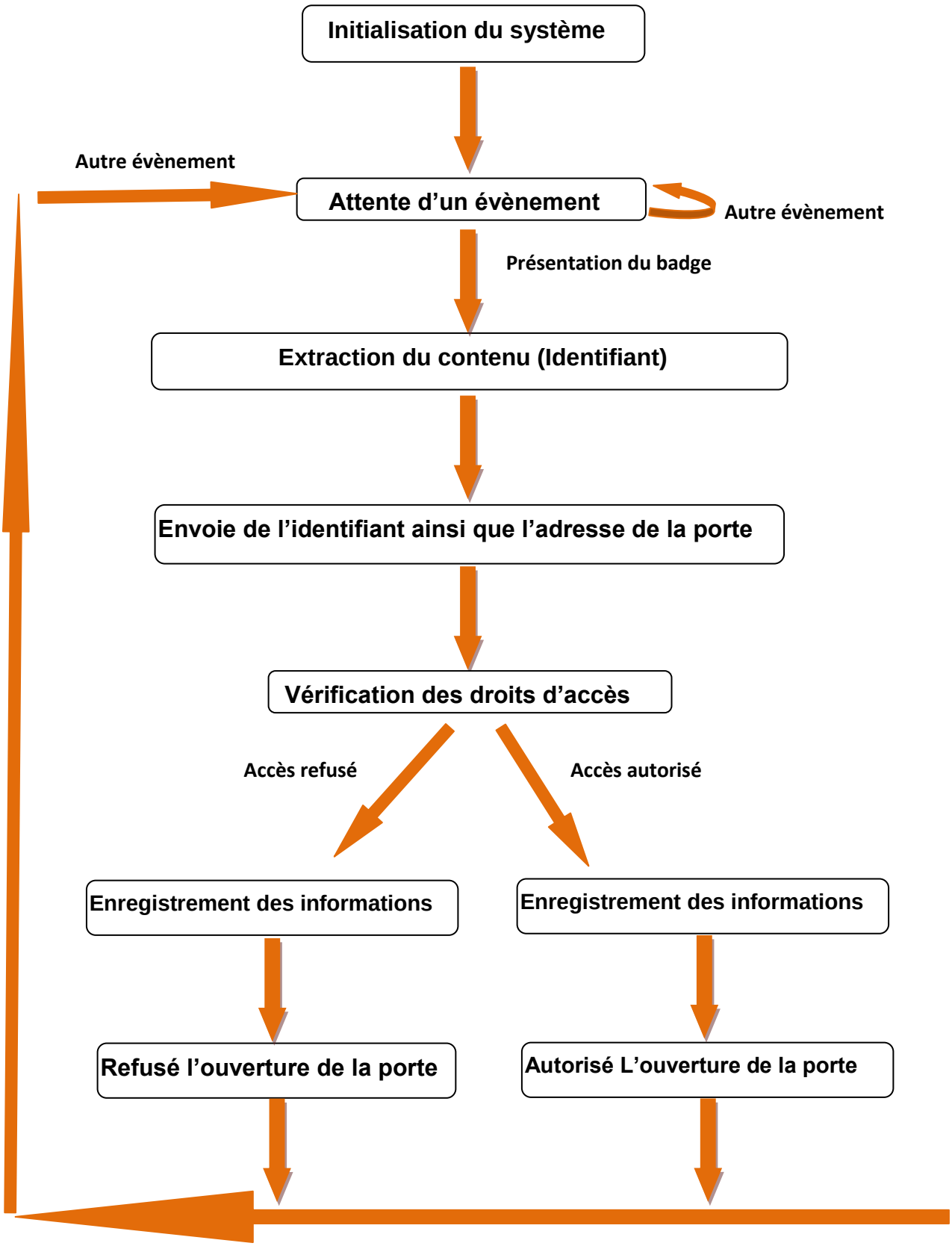


Fig.III.3 : Schéma de fonctionnement global du système

II.3 Spécification des besoins matériels

Afin de réaliser le système décrit précédemment, on doit utiliser un ensemble de composants matériels en interaction, chacun réalise une tâche précise.

Le système doit disposer d'un module central qui est chargé de commander et de recevoir les instructions des autres modules; c'est lui qui gère et qui maintient le fonctionnement du système.

Pour lire l'identifiant du badge et ensuite autorisé ou non l'accès à un endroit spécifique, le système doit disposer d'un module d'accès. Ce dernier est composé d'un lecteur de badge qui permet de récupérer l'identifiant du badge et d'un microcontrôleur qui commande une porte puis l'ouvrir si un accès est accordé.
Le module d'accès est connecté et commandé par le module central.

Pour la communication des deux modules(le module central et le module d'accès), le système doit assurer une communication à longue distance et cela est assuré par un module de communication RS485.

La façon dont les modules sont interconnectés est illustrée dans la figure Fig.III.4

Fig.III.4. Vue simplifiée de l'architecture matérielle du système.

III. Conception

III.1 Le modèle conceptuel matériel/ logiciel

Pendant la phase de conception, nous construisons un modèle conceptuel matériel / logiciel du système.

La figure Fig.III.5 présente les différents modules de notre système et la façon dont ils sont connectés

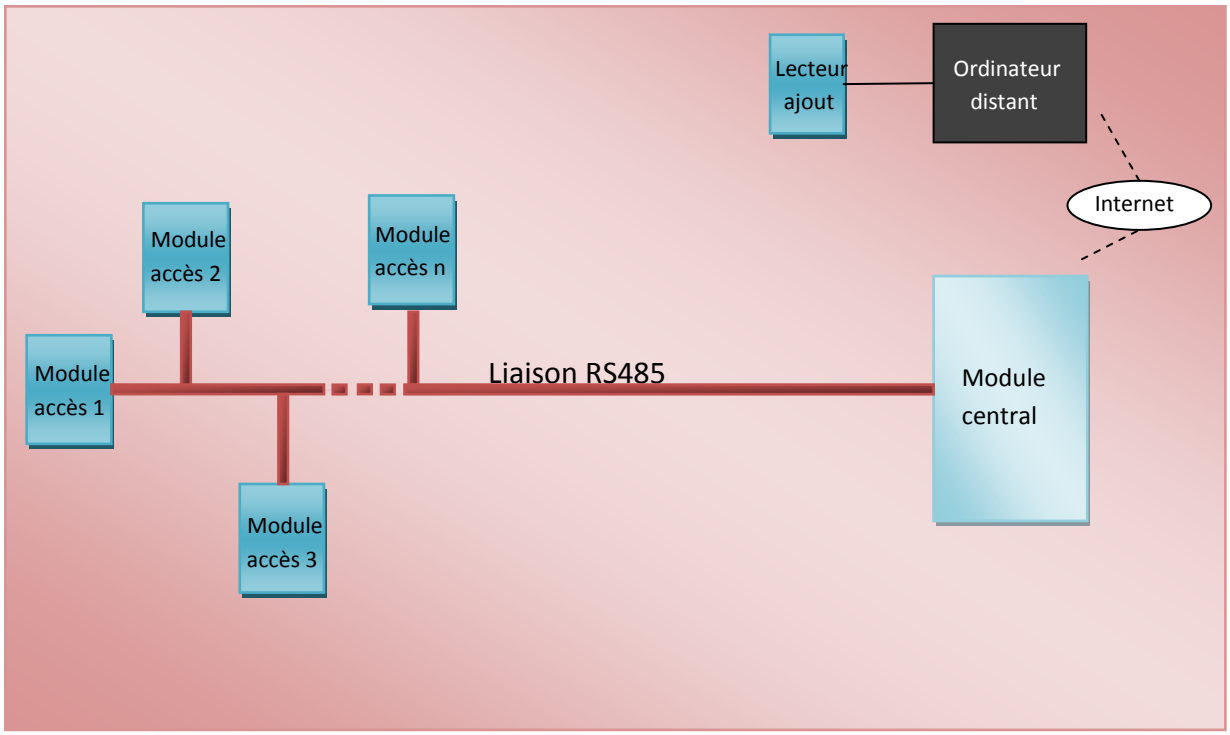


Fig.III.5: Diagramme synoptique du système de contrôle d'accès

Afin de comprendre le fonctionnement de ce système et de voir l'interaction entre les différents modules du système on a utilisé les diagrammes du modèle conceptuel matériel/logiciel (diagramme d'appel, flux de données et de tâche) [Con1].

- **Diagramme d'appel**

Le diagramme d'appel est un moyen graphique pour définir comment les modules logiciels / matériels sont interconnectés.

- **Diagramme de flux de données**

Un graphe de flux de données est un schéma fonctionnel du système montrant le flux d'informations. Les flèches indiquent la direction du flux (de la source à la destination). Les rectangles représentent les composants matériels et les ovales sont des modules logiciels, tout en cachant les détails de la façon dont il fonctionne.

- **Diagramme de tâches**

C'est la technique permettant de convertir un énoncé d'un problème en un algorithme logiciel. Nous commençons par une tâche puis on décompose la tâche en un ensemble de sous-tâches plus simples. Ensuite, les sous-tâches sont décomposées en simples sous-sous-tâches. On peut décomposer une tâche de trois manières différentes: la séquence, la condition, et l'itération, qui sont les trois éléments constitutifs de la programmation structurée.

On peut décomposer notre système en deux modules (module accès et module central), et ces modules seront reliés via un bus RS485.

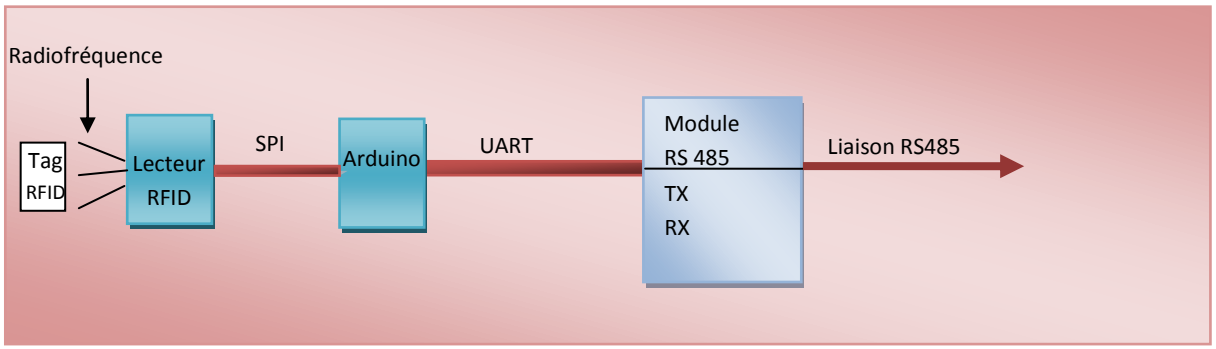
A. Module accès :

Ce module lit l'identifiant du badge présenté par un demandeur d'accès. Si ce dernier a le droit d'y accéder, le module d'accès commande électriquement l'ouverture de la porte concernée. Pour assurer son rôle, ce module doit comporter :

- Un lecteur RFID pour lire l'identifiant du badge.
- Une carte arduino pour communiquer l'identifiant lu ainsi que l'adresse de la porte qu'on veut ouvrir au module central et commander l'ouverture ou non de la porte.
- Le badge (tag RFID) : contient l'identifiant du demandeur d'accès.

Le lecteur et la carte arduino sont reliés via la liaison série SPI.

La figure FigIII.6 illustre les différents composants du module d'accès et la façon dont ils sont connectés.



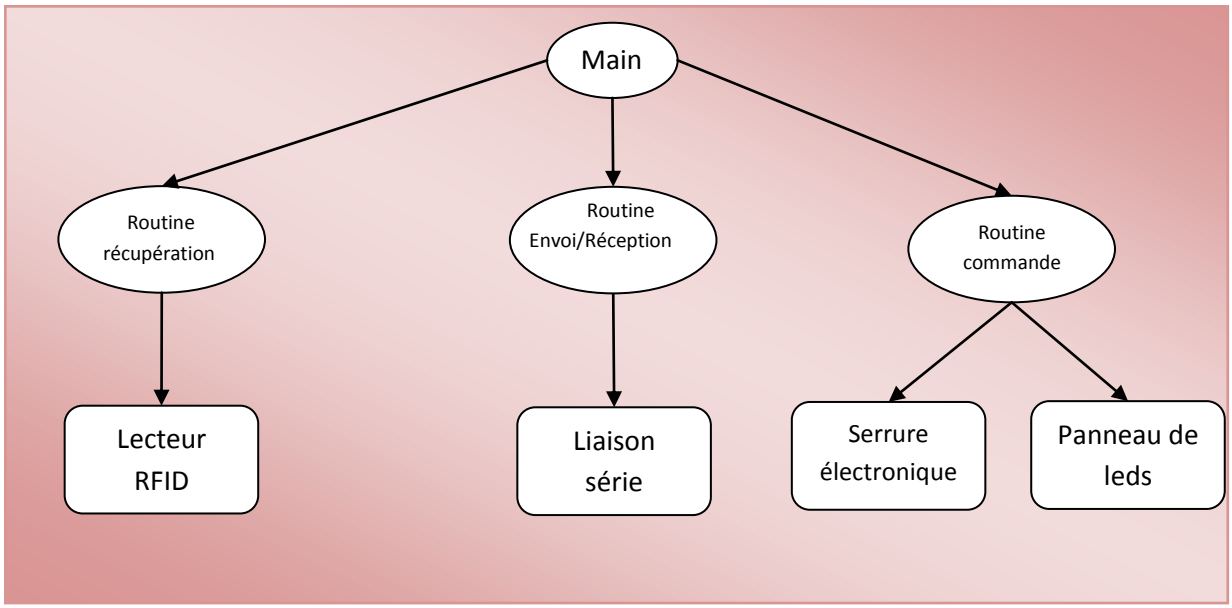
FigIII.6:Diagramme synoptique du module d'accès

- **Diagramme d'Appel du module d'accès :**

Ce module assure trois fonctions principales qui sont :

- La routine de récupération : permet de récupérer l'identifiant lu à partir d'un lecteur RFID.
- La routine d'envoi/réception : permet d'envoyer et de recevoir des données du module central via la liaison série rs485.
- La routine de commande : commande l'ouverture de porte et l'allumage d'une led du panneau des leds.

Le diagramme de la figure FigIII.7 montre comment les modules logiciels/matériels sont interconnectés



FigIII.7 Diagramme d'appel du module Accès

- **Diagramme de flux de données du module d'accès**

Afin d'assurer le contrôle d'accès, plusieurs informations traversent le système. La figure FigIII.8 montre le flux de données de notre système, le lecteur lit l'identifiant puis le communique à la carte arduino, qui lui ajoute l'adresse de la porte, puis via la liaison série, il communique ces informations au module central.
La carte arduino reçoit une réponse, et suivant cette réponse la porte s'ouvre et une led verte s'allume si l'accès est accordé sinon l'allumage une led rouge.

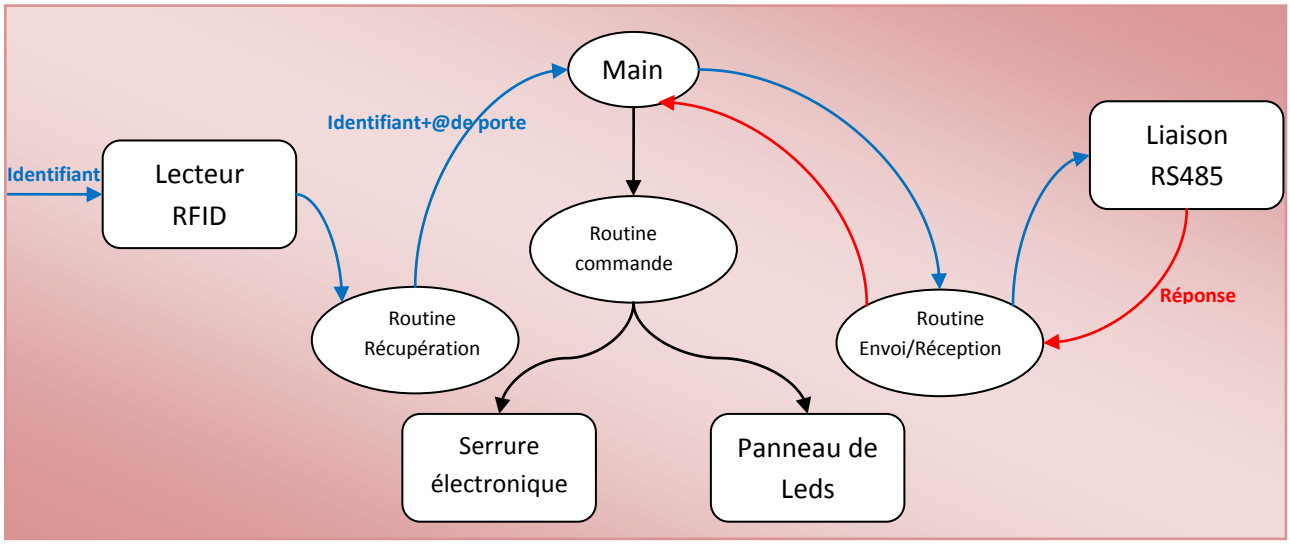


Fig III.8 diagramme de flux de données de module d'accès

- **Diagramme de tâches du module d'accès**

La manière dont notre algorithme est structuré est donnée par le diagramme de taches suivant

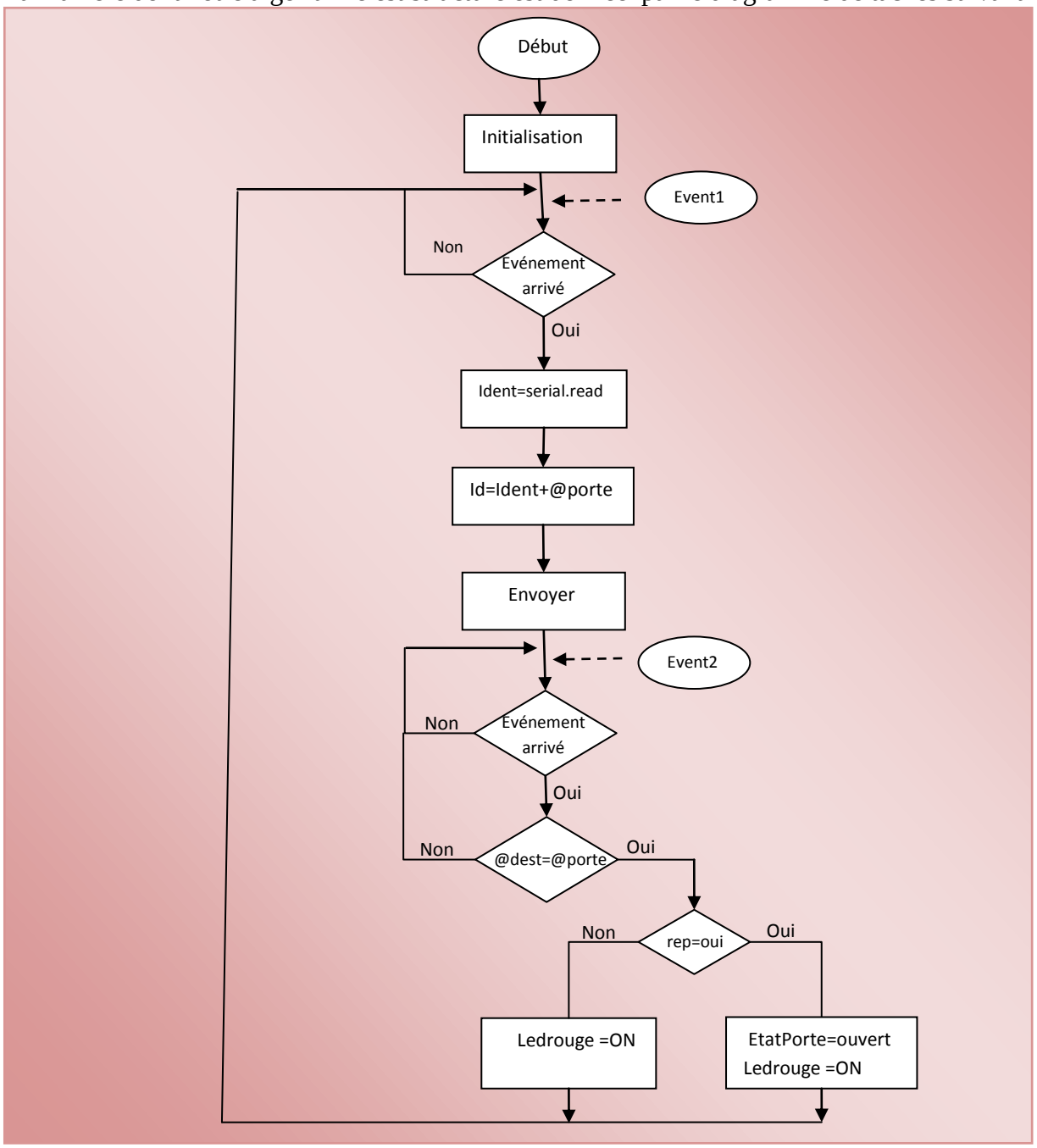
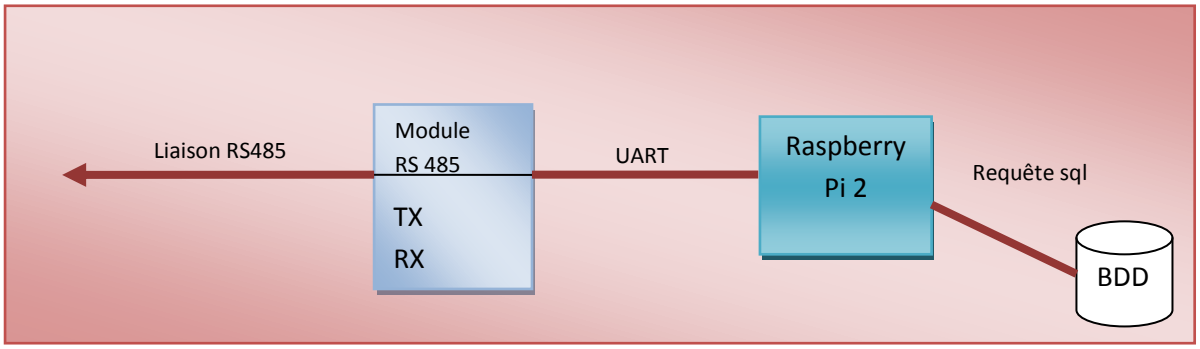


Fig III.9:Diagramme de tâches du module Accès

Event1 : la présentation du badge par un utilisateur.
Ident : Identifiant du badge
Event2 : La réponse après vérification des droits d'accès, elle contient l'adresse de destination (@dest), et une réponse à la demande d'accès (Rep).
@porte : Représente le numéro de la porte auquel l'utilisateur veut accéder
Ledrouge: Représente la broche reliée à une led qui s'allume si l'accès n'est pas accordé
Etatporte : représente la broche reliée à un relais électronique permettant l'ouverture d'une porte si l'accès est accordé

B. Module central :

Ce module est composé d'une carte Raspberry Pi qui est reliée aux autres modules par une liaison RS485, Ce module contient une base de données pour vérifier les droits d'accès, comme l'illustre la figure suivante :



FigIII.10 Le diagramme synoptique du module central

- **Graphe d'appel du module central**

Ce module assure deux fonctions principales qui sont :

- La routine d'envoi/réception : permet d'envoyer et de recevoir des données des autres modules via la liaison série.

- La routine de gestion : la vérification des droits d'accès et enregistrement dans la base de données.

Le diagramme suivant montre comment les modules logiciels/matériels sont interconnectés

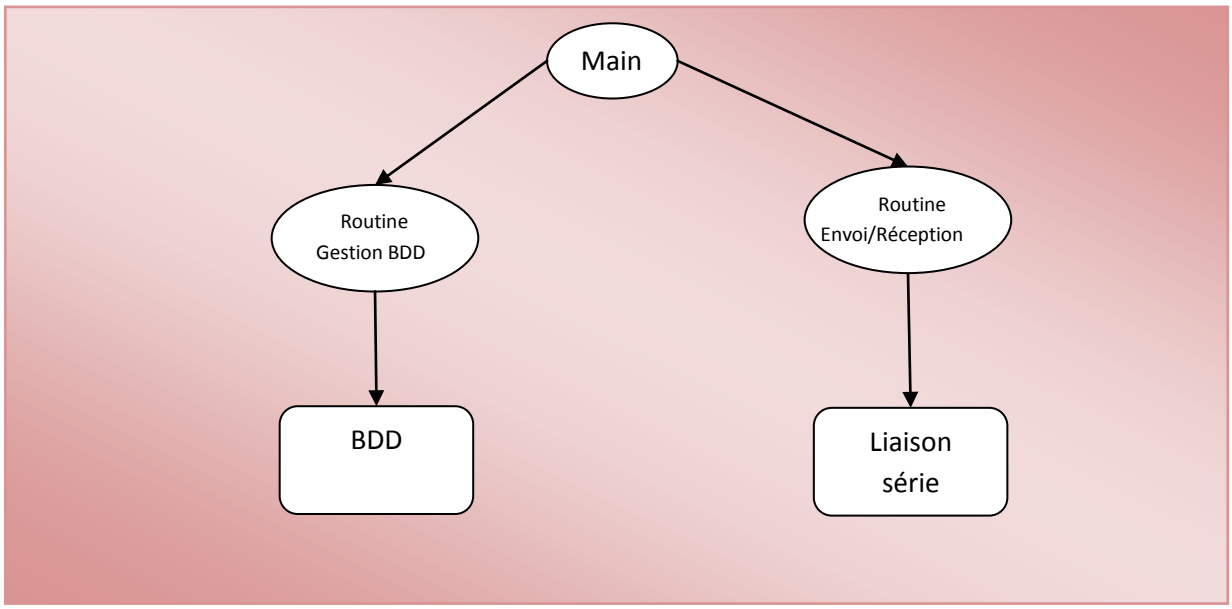


Fig III.11 Le diagramme d'appel du module central

- **Diagramme du flux de données du module central**

Afin d'assurer les fonctionnalités de ce module plusieurs informations sont communiquées ; ce module reçoit à partir du module d'accès l'identifiant du demandeur d'accès et l'adresse de la porte où il veut accéder. Ces informations seront comparées à celle de la base de données et une réponse est engendrée.

Pour enregistrer de nouveaux utilisateurs un identifiant sera récupéré par un lecteur RFID et cet identifiant sera communiqué à la routine d'enregistrement

Le flux d'information est présenté dans la figure FigIII.12.

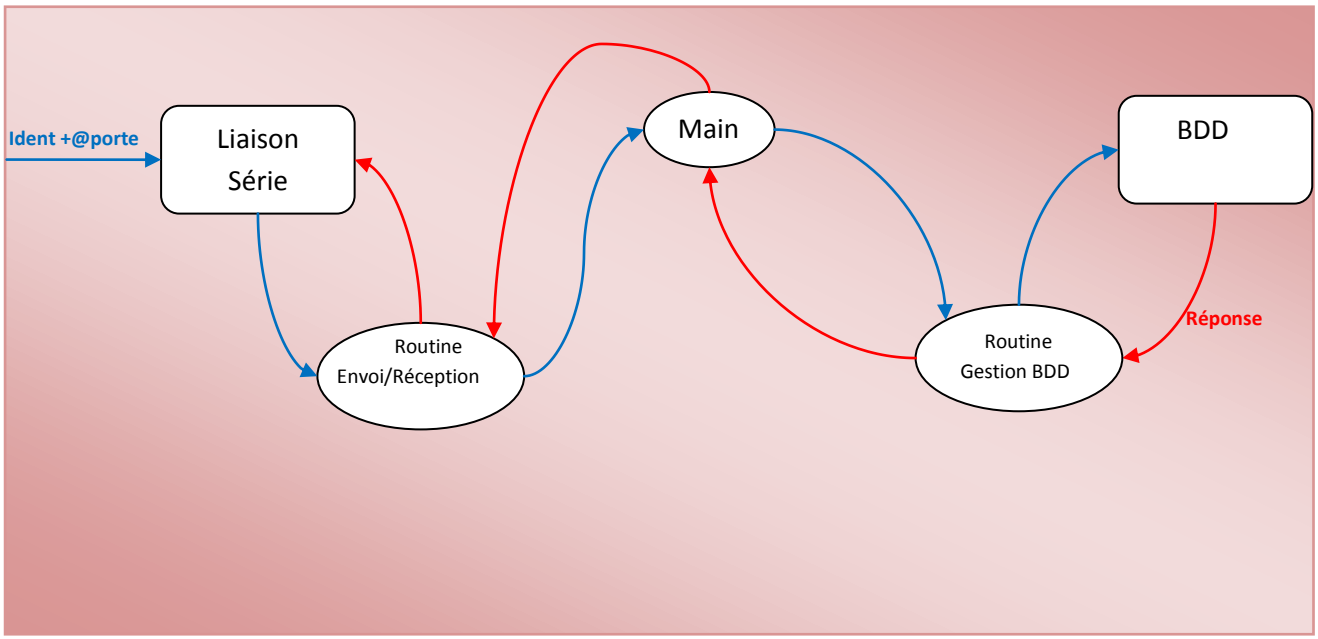


Fig III.12 Le diagramme du flux de données du module central

- **Le diagramme de tâches du module central**

La manière dont notre algorithme est structuré est donnée par le diagramme de tâches suivant :

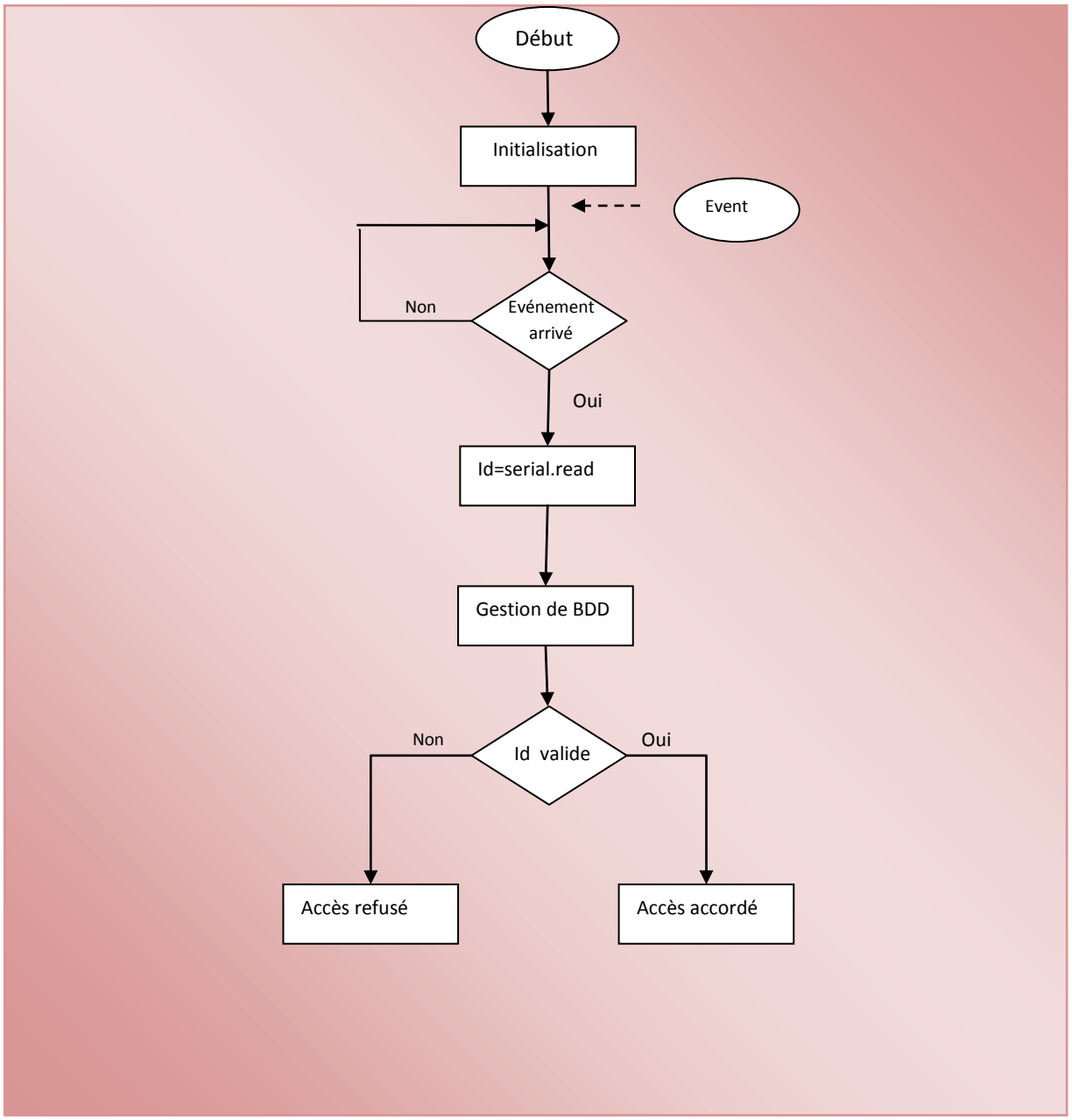


Fig III.13 Le diagramme de tâches du module central

Event : réception des données d'identification de la liaison série

Id : les données d'identification (identifiant du badge et l'adresse de la porte)

III.2. Composants matériels utilisés et leurs Descriptions

Pour réaliser notre système de contrôle d'accès, on utilise un ensemble de composants matériels tels que : La Raspberry Pi, l'Arduino, le NFC Shield, la MAX485.

III.2.1.La Raspberry Pi [rpi1]

La Raspberry Pi est une véritable carte mère de mini ordinateur de la taille d'une carte de crédit à très bas coût. Conçu dans le cadre de la « Fondation Raspberry », cet outil initialement destiné à l'initiation de la programmation informatique en Angleterre est suffisamment ouvert pour satisfaire de nombreuses exigences en termes d'embarqué. Fournie nue (la carte mère seule, sans clavier ni souris, sans écran, et même sans périphérique de stockage ou système d'exploitation).

Les différents modèles de Raspberry Pi

Initialement, la Raspberry Pi était distribuée sous deux modèles à savoir le modèle A et B. Mais par la suite, en raison du succès des appareils et des possibilités d'amélioration, deux nouveaux modèles ont été sorties : le modèle A+ et B+.

La Raspberry Pi 2 garde tout ce qui a fait le succès de son prédécesseur (qualité du matériel, performance) en y apportant des améliorations notoires, comme les 4 processeurs ARM v7 cadencés à 900Mhz et la mémoire vive double pouvant aller jusqu'à 1Go. La performance (environ six fois plus performante que le modèle B+) et la puissance sont les deux arguments majeurs pour le choix de la Raspberry Pi 2.

L'amélioration ne s'arrête pas. Pour répondre aux attentes des utilisateurs qui sont toujours en quête de plus de puissance, quelques mois après la sortie du Raspberry Pi 2, la fondation sort le modèle B du Raspberry Pi 2. Ce dernier se veut être beaucoup plus performant et puissant que son prédécesseur, d'où le choix de la Raspberry Pi 2 modèle B (Fig.III.14).

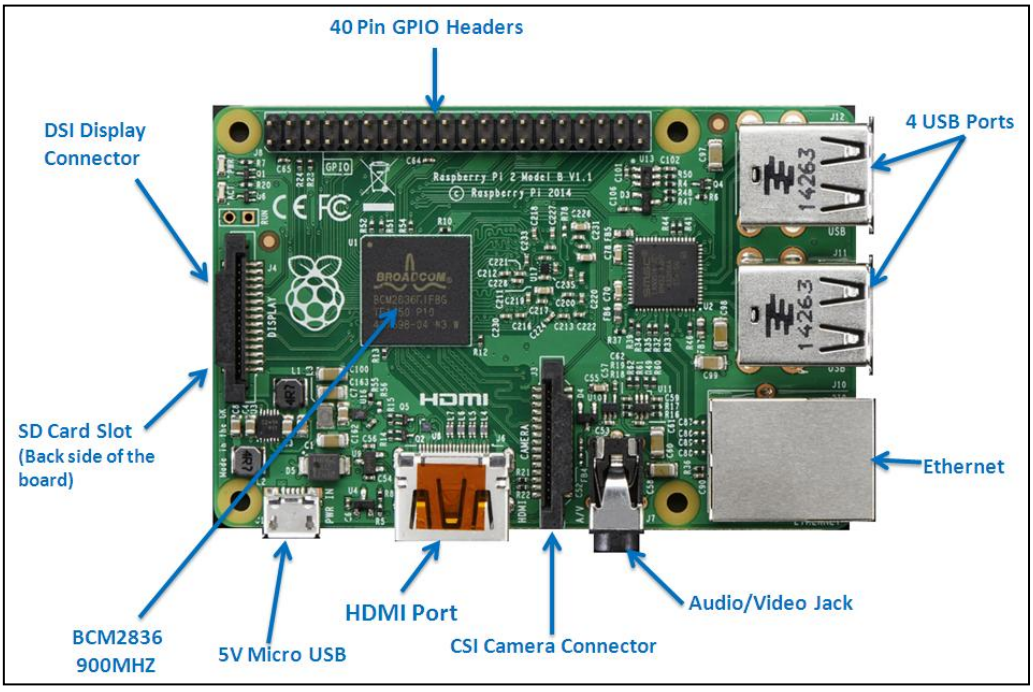


Fig III.14: Raspberry pi 2 model B

Caractéristiques et composants :

- Quatre cœurs ARMv7 à 900 MHz
- 1 Go de RAM

Comme le (Pi 1) Modèle B +, le pi 2modèle B a également:

- 4 ports USB
- 40 broches GPIO
- Port HDMI Full
- Port Ethernet
- Jack 3,5 mm audio combiné et vidéo composite
- Interface de l'appareil photo (CSI)
- Interface d'affichage (DSI)
- Micro SD slot pour carte
- Cœur graphique VideoCore IV 3D

Parmi les composants da la Raspberry Pi on va s'intéresser au GPIO et à la carte SD

- **Les GPIO :**

C'est l'abréviation de General Purpose Input/Output, ou plus simplement entrées/sorties à usage général. Ces entrées/ sorties permettent d'étendre les fonctionnalités du Raspberry Pi en lui donnant la possibilité d'agir sur des leds ou des afficheurs LCD par exemple, lire l'état d'un interrupteur, d'un capteur…etc.
Ce connecteur GPIO dispose de différents types de connexion :

- Des broches (Pins) utilisables en entrées ou en sorties numériques.
- Des broches pour une interface I2C (permettant de se connecter sur du matériel en utilisant uniquement 2 broches de contrôle.)
- Une interface SPI pour les périphériques SPI,
- Les broches Rx et Tx pour la communication avec les périphériques séries.
- Des broches pouvant être utilisés en PWM (*Pulse Width Modulation*) permettant le contrôle de puissance ou PPM (*Pulse Position Modulation*) permettant de contrôler des servo moteurs par exemple.

- **La carte SD**

La Raspberry Pi n'a pas de disque dur pour le stockage de masse, mais un lecteur de carte mémoire SD (Secure Digital) comme celles que l'on peut trouver équipant les appareils photo numériques. Avant de démarrer la Raspberry Pi, il faut préparer une carte SD et y installer la totalité du système d'exploitation. La Raspberry Pi est conçue pour faire fonctionner le système d'exploitation GNU Linux. La philosophie open source de Linux a permis de porter rapidement l'OS (Operating System) à l'architecture matérielle de la Raspberry Pi. Il existe à l'heure actuelle plusieurs variantes de Linux utilisables avec le circuit de la Raspberry Pi, appelées distributions Linux (Raspbian, Arch, Pidora, etc.). Par la suite, nous utiliserons une distribution Debian portée et optimisée pour Raspberry Pi nommée Raspbian.

III.2.2. La carte Arduino

Arduino est un circuit sur lequel il est possible de brancher toutes sortes d'appareils. Cette carte se programme sur l'ordinateur via un câbles USB (ou autre) et permet ensuite de diriger n'importe quel appareil, il suffit pour cela de modifier le code qu'exécute l'arduino. La particularité de ce système est qu'il est libre, c'est à dire que les plans des cartes sont disponibles gratuitement, il est possible de modifier et de réutiliser ces plans [ard1]

D'après [ard2], Arduino peut être défini aussi comme un véritable mini-ordinateur au succès planétaire, traitant les données provenant de composants et capteurs divers (capteur de température, luminosité, mouvement ou boutons-poussoirs, etc.) et communiquant des ordres pour allumer des lampes ou actionner des moteurs électriques, la carte électronique Arduino permet de créer et prototyper de véritables objets numériques interagissant avec le milieu extérieur.

L'environnement de programmation qui l'accompagne propose un IDE[1] et un langage basé sur les langages C / C++.

Il existe de nombreux modèles de cartes Arduino, la plus populaire étant la Uno.

- **Arduino Uno** [ard3]

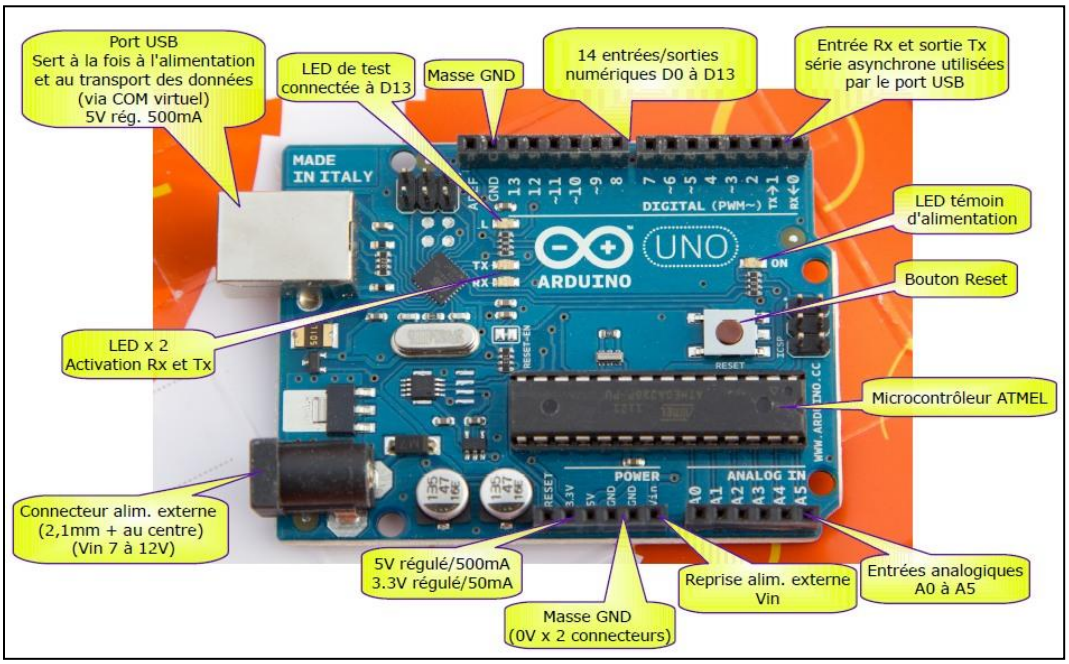


Fig III.15 La carte Arduino Uno [ard4]

[1] IDE : (Integrated Development Environment) : L'environnement de programmation Arduino

Caractéristiques de la carte Arduino Uno :

- Micro contrôleur : ATmega328
- Voltage opérationnel (au niveau logique) :5V
- Voltage d'entrée recommandé : de 7 à12 V
- Limite de voltage : de 6 à 20 V
- Entrées/sorties numériques : 14 dont 6 sorties PWM
- Entrées analogiques = 6
- Courant max par broches E/S = 40 mA
- Courant max sur sortie 3,3V = 50mA
- Mémoire Flash 32 KB dont 0.5 KB
- Mémoire SRAM 2 KB mémoire EEPROM 1 KB
- Fréquence horloge = 16 MHz
- Dimensions = 68.6mm x 53.3mm
- La carte s'interface au PC par l'intermédiaire de sa prise USB.
- La carte s'alimente par le jack d'alimentation (utilisation autonome) mais peut être alimentée par l'USB (en phase de développement par exemple).

III.2.3. Le module NFC Shield [nfc1]

Le NFC Shield est une carte d'interface compatible avec Arduino, basé sur le circuit PN532[2], il est utilisé pour reconnaitre des cartes ou des badges RFID.

Le NFC (Near Field Communication) est une technologie permettant d'établir une liaison sans contact à courte distante et est issue de la technologie RFID.

La carte Arduino et le NFC Shield communiquent via le bus SPI ce qui permet de laisser libre les autres ports de la carte Arduino pour d'autres applications. L'antenne déportée facilite l'intégration de module dans un boitier.

Le NFC Shield s'utilise avec des cartes ou badges possédant un code unique. Application : Contrôle d'accès, identification, suivi de produits, etc.

[2] PN532 : est un module émetteur-récepteur intégré pour la communication sans contact à 13,56 MHz

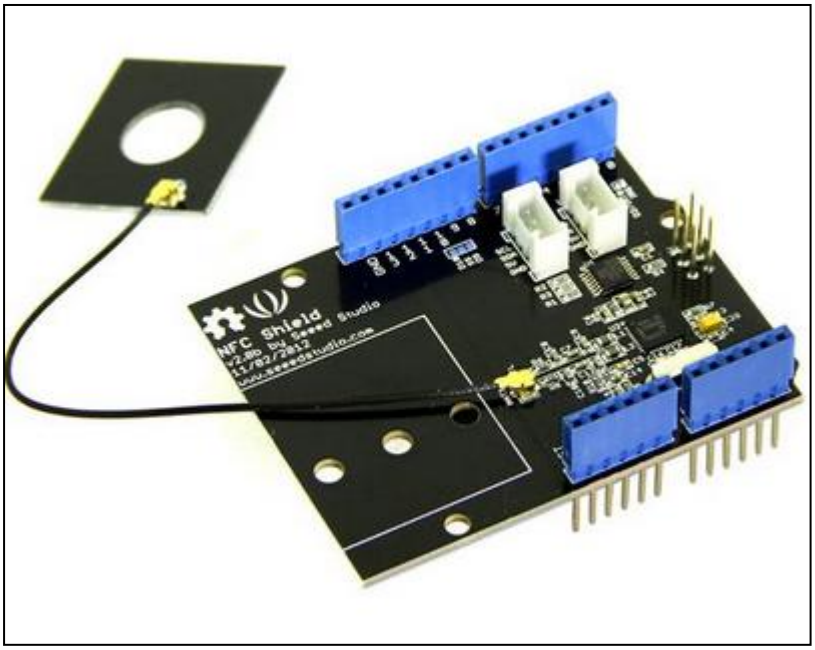


Fig III.16 Le module NFC Shield

Le NFC Shield est idéal pour des projets de domotique il permet d'identifier une personne avec son badge avant d'ouvrir la porte. Il peut être utilisé dans n'importe quel projet d'identification.

Caractéristiques :

- Alimentation: 5 Vcc (3,7 à 5,5 Vcc)
- Consommation: 150 mA maxi
- Fréquence: 13,56 MHz
- Antenne déportée
- Connecteur pour le raccordement d'autres Shields
- Portée de communication: 10 cm
- Interface SPI disponible
- Dimensions:
  - module: 70 x 56 x 20 mm
  - antenne: 28 x 30 mm

Arduino et NFC Shield

Comme il a été mentionné la récupération de l'identifiant se fait en reliant un lecteur RFID et une carte arduino et que ses composants sont reliés via la liaison SPI.

- **SPI (Serial Peripheral Interface)** [spi1]

SPI est une interface série créée par Motorola (Freescale) pour interconnecter les composants d'un système périphérique avec un minimum de fils. Le SPI a les caractéristiques suivantes:

- Master-Slave : Sur un bus SPI, il y a un maître qui initie toutes les communications et plusieurs slave qui ne transmettre que lorsque demandé par le maître.
- FULL-DUPLEX : La communication entre le maître et un esclave peut se faire simultanément dans les deux sens.

- Série : Les bits d'un mot sont transmis un à un…
- Synchrone : Une horloge indique le moment de transmettre un bit et le moment d'échantillonner un bit.

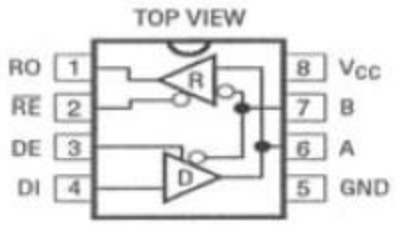
Le SPI n'est pas un protocole établi: il s'agit d'une couche de communication physique qui a été adoptée par de nombreux manufacturiers et qui s'est répandue universellement. Dans un bus SPI, il y a au moins quatre fils : SCLK, MOSI, MISO et SS :

- SCLK, Serial CLocK, est l'horloge du bus.
- MOSI, Master Out Slave In, est le fils qui véhicule les données du maître aux esclaves
- MISO, Master In Slave Out, est le fils qui véhicule les données des esclaves au maître.
- SS (actif LOW), Slave Select, est le chip qui permet d'activer ou désactiver l'esclave qui communiquera avec le maître. Lorsqu'il y a plusieurs esclaves, il y a plusieurs lignes de sélection.

III.2.4. Le circuit de connexion : Max485 [max1]

Dans notre réseau de communication RS485, nous avons utilisé la Max 485, qui est un émetteur/récepteur à bus/ligne différentiel de basse puissance 300 µA, conçu pour les applications du standard RS485 dans la transmission de données à multipoints, avec une portée étendue du mode commun (-7V jusqu'à 12V).

Le circuit de module MAX485 est présenté par le schéma de la figure suivante :



FigIII.17 : la MAX485

Il est connecté au microcontrôleur à travers le périphérique UART et il doit être présent des deux parts de la communication.

- **La communication Arduino et raspberry pi via RS485**

L'échange de données entre la raspberry Pi et l'arduino est assuré en reliant ces composants par un bus RS485.

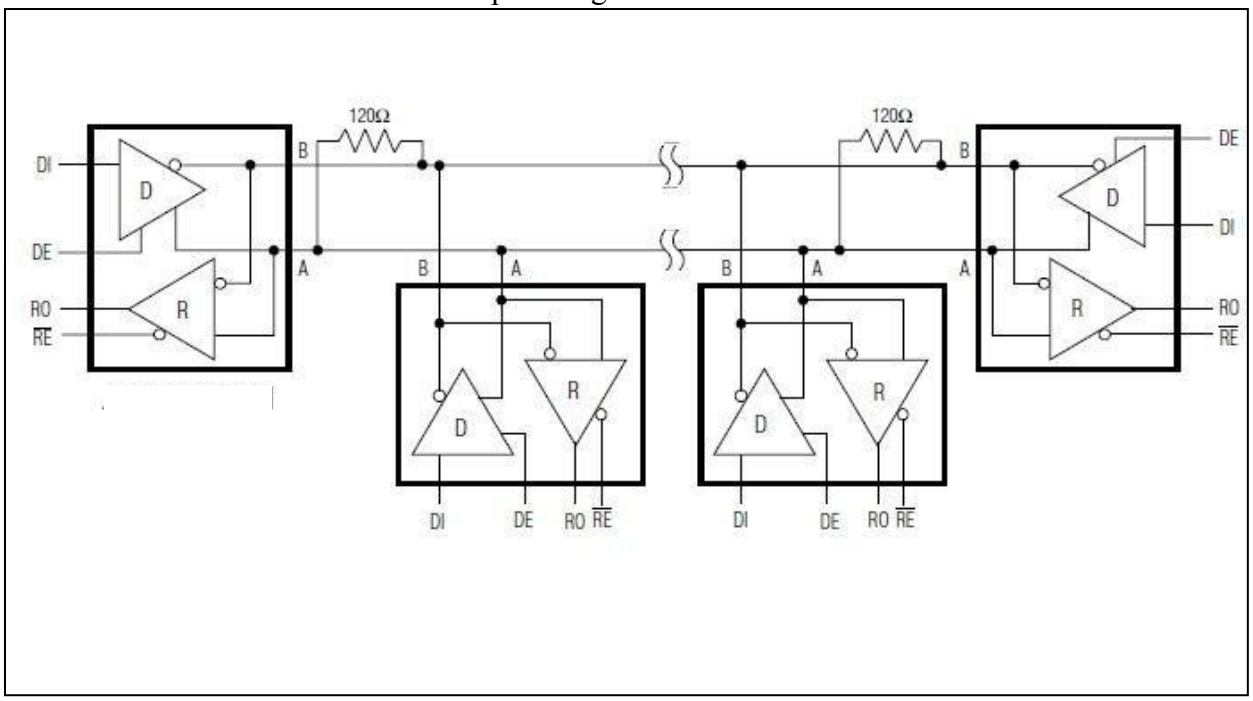
- **Bus RS485** [rs1]

Le bus RS485 est un bus normalisé par la norme EIA-485[3] utilisant une paire torsadée pour transmettre des données par des variations de tension en mode différentiel. Il permet une communication de type liaison série avec un maximum de 32 appareils, sur une distance allant

[3] EIA-RS485 : est une norme qui définit les caractéristiques électriques de la couche physique d'une interface numérique sérielle

jusqu'à 1200 mètres. RS485 utilise une paire de fils A et B sur lesquels les données sont transmises. L'état logiques 1 (off) et 0 (on), est donné par la polarité entre les bornes A et B (différentiel de tension). Si A est négatif par rapport à B, l'état binaire est 1.

Le schéma d'un bus RS485 est donné par la figure suivante :



FigIII.18 : le schéma d'un bus RS485

Le circuit Max485 est connecté aux modules (Arduino, Raspberry Pi) à travers le périphérique UART

- **UART** [uart]

UART, Universal Asynchronous Receiver/Transmitter est une interface classique de communication série en mode asynchrone. Pour l'émission l'UART permet de faire la conversion parallèle/série pour transmettre sur un même fil les données. En réception, l'UART reçoit une information série qu'il rend parallèle, il assure donc la conversion série/parallèle.

L'UART utilise des registres parallèle/série ou série/parallèle mais on ne peut pas l'assimiler à un simple registre à décalage. Il restera un circuit complexe programmable gérer par plusieurs signaux de commandes.
Parmi les blocs qui constituent l'UART, on trouve : l'émetteur et le récepteur. Ces deux derniers ont besoin d'une horloge qui détermine leur vitesse en Baud.

Structure de l'UART

Il contient habituellement les composants fondamentaux suivants :

- Un générateur d'horloge.
- Un canal d'émission (TRANSMITTER), TX
- Un canal de réception (RECEIVER), RX

Le schéma de câblage de notre système et ces composants est donnée par la figure suivante :

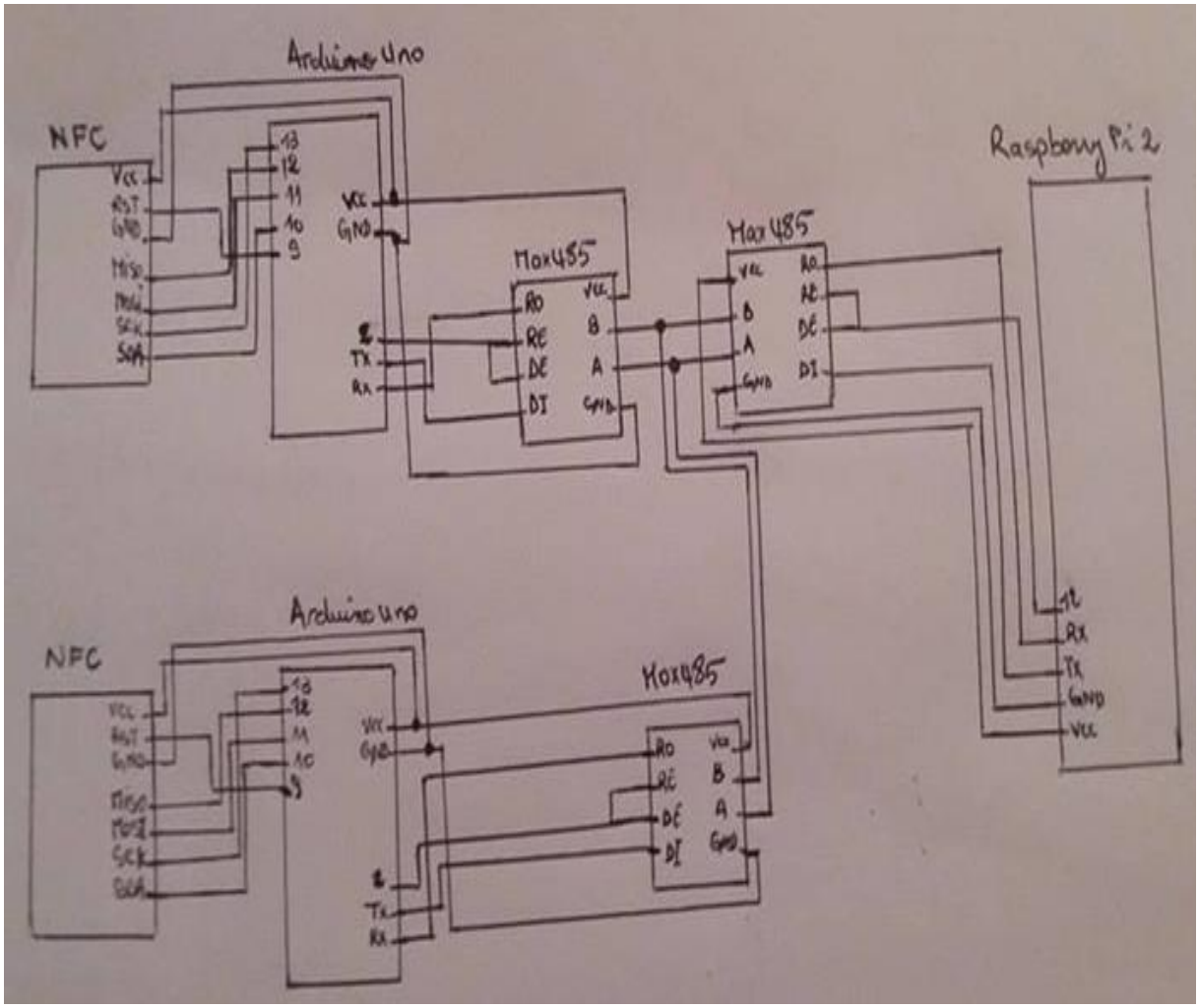


Fig.III.19 le Schéma de système contrôle d'accès

Comme nous l'avons souligné précédemment, notre système permet la mise à jour (ajout d'utilisateur, suppression, modification,…). Pour permettre cette mise à jour nous allons développer une application web permettant de faire des ajouts à distance, de consulter l'historique des accès,...etc.

IV. Analyse et conception de notre application web

Notre projet possède un seul type d'acteur qui est l'administrateur.

Administrateur : cet acteur a le droit de se servir de notre plateforme à distance ou localement.

IV.1 Spécification des scénarios

Acteur	Tâches	Scénarios
Administrateur	T0 : Se connecter à la plateforme	S0 : Saisir l'@ IP de raspberry Pi et l'URL de site dans le Navigateur
	T1 :S'authentifier	S1 : Accéder au formulaire d'authentification S2 : Saisir les coordonnées S3 : Valider l'authentification
	T2 : Manipuler les bases de données	S4 : consulter l'historique S5 : ajouter un utilisateur avec tous ses droits d'accès S6 : consulter /supprimer /modifier un utilisateur
	T3 : Se déconnecter	S7 : Cliquer sur le lien « Déconnexion »
	T4 : Modifier le mot de passe	S8 : Accéder au formulaire de modification de mot de passe S9 : Saisir les coordonnées S10 : Valider la modification

TabIII.1: Les scénarios des tâches de l'acteur de notre application.

IV.2 Spécification des cas d'utilisation :

- **Cas d'utilisation général de notre logiciel de gestion :**

A ce stade là, nous présentons le diagramme de cas d'utilisation général de notre logiciel indiqué dans la figure FigIII.20

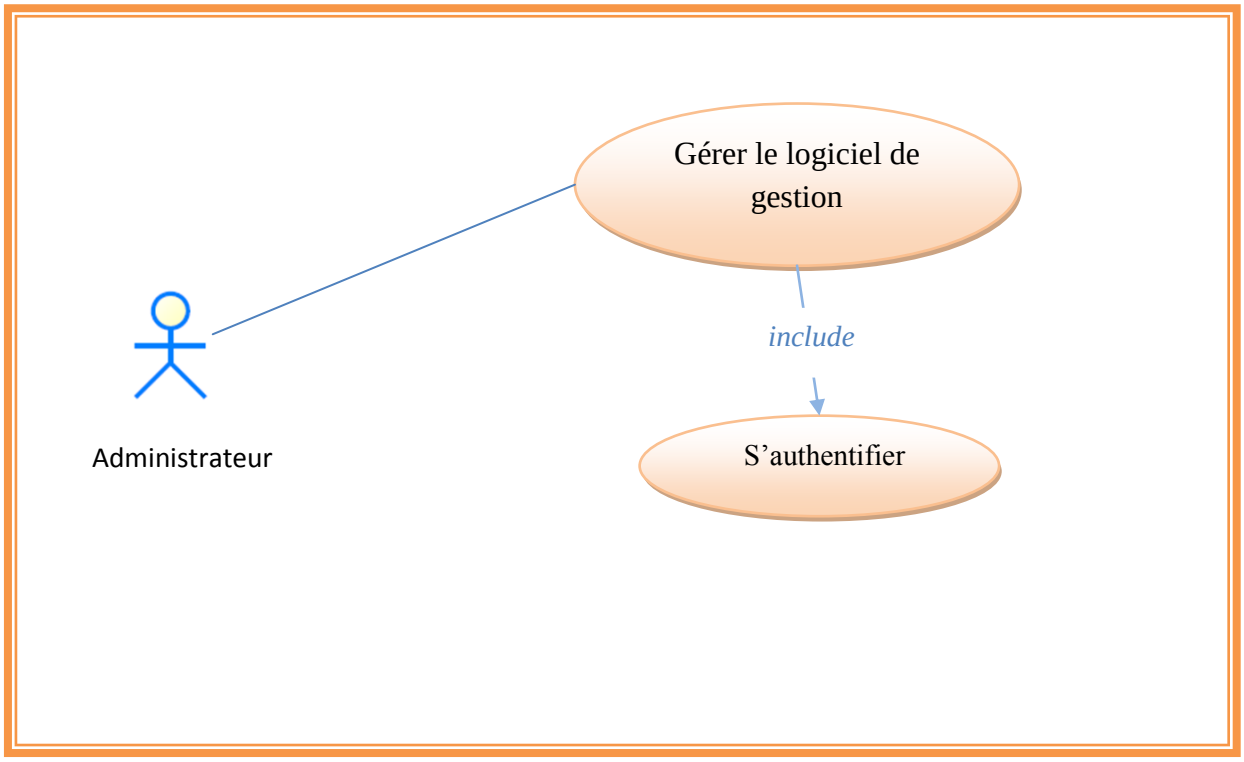


Fig.III.20 : Diagramme de cas d'utilisation général de notre logiciel de *gestion*

L'administrateur doit s'authentifier afin de pouvoir gérer le logiciel soit à distance soit localement.

- **Cas d'utilisation détaillé :**

Le fonctionnement de notre système contrôle d'accès peut être décrit par le cas d'utilisation de la figure Fig.III.21 :

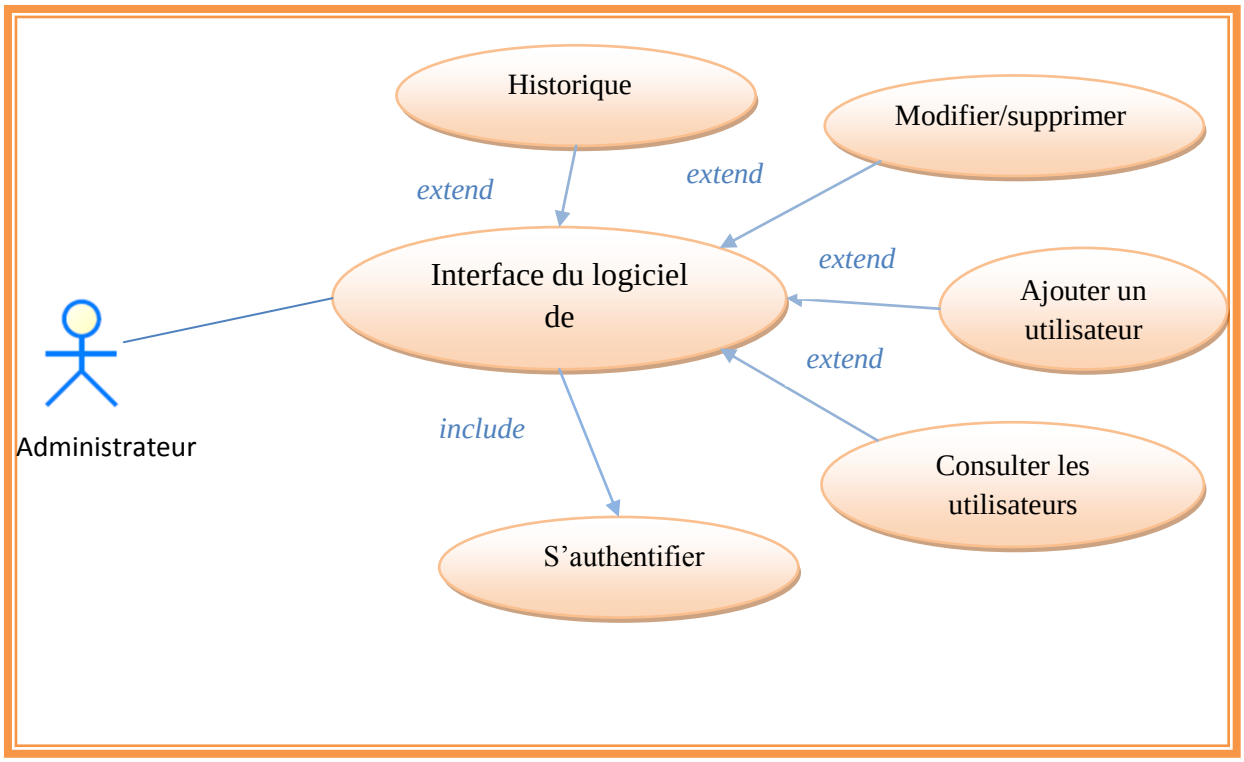


Fig.III.21 : Diagramme de cas d'utilisation détaillé de notre logiciel de gestion

IV.3 Les diagrammes de séquences

Les diagrammes de séquence permettent de décrire les interactions entre les objets pour chaque cas d'utilisation. Dans notre cas, ces diagrammes sont liés aux diagrammes de cas d'utilisation représentés auparavant.

- **Diagramme de séquence de «l'authentification de l'administrateur »**

Quand un administrateur se connecte au serveur, il peut accéder à l'interface de la plateforme via son téléphone portable ou son PC, puis saisit son login et son mot de passe, ces informations seront vérifiées, si tout est bon, l'interface de l'administrateur sera affichée. La figure suivante présente le diagramme de séquence « Authentification de l'administrateur ».

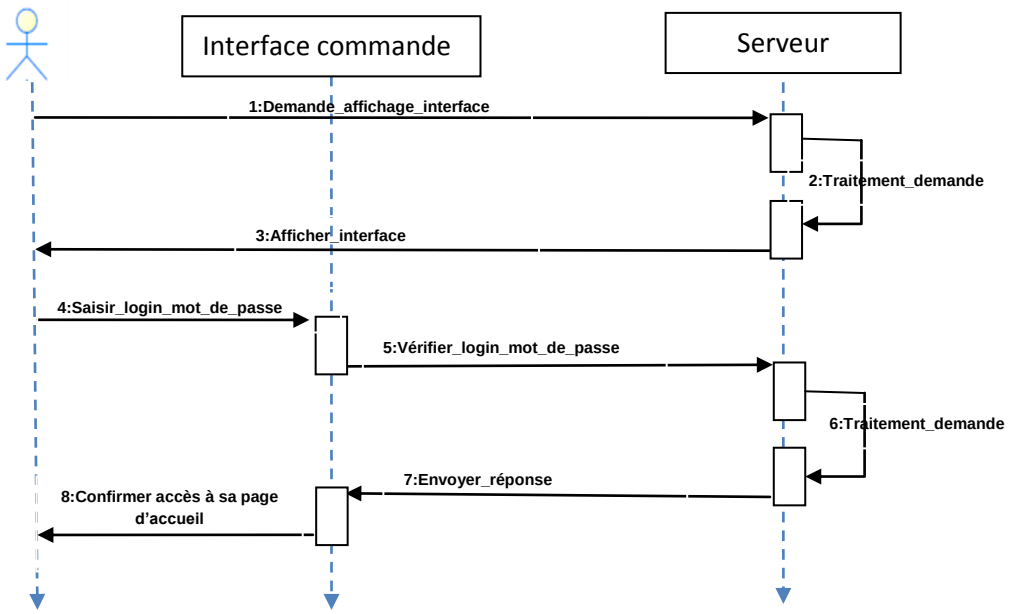


Fig.III.22: Diagramme de séquence «Authentification administrateur »

- **Diagramme de séquence de « historique »:**

Pour consulter l'historique, l'administrateur demande d'afficher la liste de tous ceux qui ont présentés leurs badges.

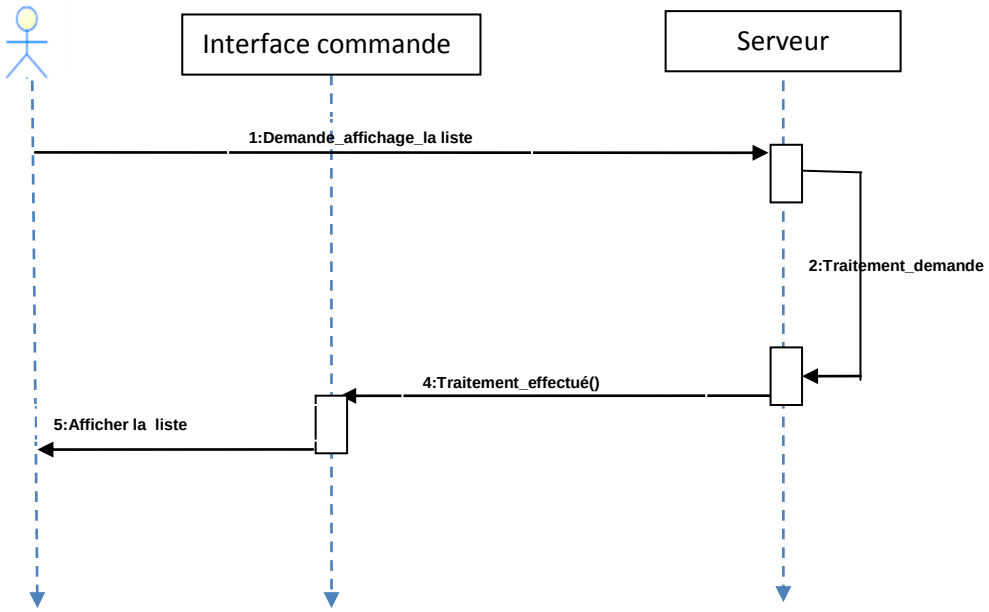


Fig.III.23 : Diagramme de séquence «Historique »

V. Conclusion

Dans ce chapitre, nous avons modélisé les deux parties de notre système. On a choisi les composants matériels nécessaires et nous avons déterminé les différents modules logiciels qui vont assurer le bon fonctionnement du système. Suite au travail accompli au niveau de cette partie, il reste les étapes d'implémentation et des tests qui vont faire l'objet du prochain chapitre.

Chapitre 4

Réalisation

I. Introduction

La réalisation est la phase la plus importante après celle de la conception. Le choix des outils de développement détermine énormément le coût en temps de programmation, ainsi que la flexibilité du produit à réaliser. Cette phase consiste à transformer le modèle conceptuel établi en des composants logiciels formant notre système. Dans un premier temps, nous allons procéder à la spécification de l'environnement matériel et logiciel utilisé dans notre projet.
Ensuite, nous nous intéresserons, à la description des différentes étapes de réalisation de notre système «Contrôle d'accès ».

II. Outils de développement utilisés :

Pour développer notre système, nous avons eu recours à divers éléments notamment les outils logiciels, les langages de programmation et les outils matériels qui nous ont permis la mise en œuvre de notre système.

II.1 Outils logiciels :

II.1.1 Le serveur web Apache2 :

Apache2 est un logiciel qui permet de mettre à disposition sur le réseau, d'un site web (pages html, php). Plus précisément apache2 est un serveur http. Les utilisateurs utilisent quant à eux un client http pour afficher à l'écran ce site, comme par exemple firefox, chrome, Microsoft Internet Explorer etc...

II.1.2 SQLite3 :

SQLite est un système de gestion de base de données embarqué qui a la particularité de fonctionner sans serveur. On peut l'utiliser avec beaucoup de langages : PHP, Python, Java, C/C++, Delphi, Ruby...
L'intérêt est qu'il est très léger et rapide à mettre en place, on peut s'en servir aussi bien pour stocker des données dans une vraie base de données sur une application pour Smartphone (iPhone ou Android), pour une application Windows, ou sur un serveur web.
Une base de données SQLite est bien plus performante et facile à utiliser que de stocker les données dans des fichiers XML ou binaires, d'ailleurs ces performances sont même comparables aux autres SGBD fonctionnant avec un serveur comme MySQL, Microsoft SQL Server ou PostgreSQL. **[12]**

II.2 Langages utilisés

II.2.1 HTML5 (**Hypertext Markup Language 5**) :

C'est la dernière révision majeure d'HTML (format de données conçu pour représenter les pages web). Il permet notamment d'implanter de l'hypertexte dans le contenu des pages et

repose sur un langage de balisage. HTML permet aussi de structurer sémantiquement et de mettre en forme le contenu des pages, d'inclure des ressources multimédias dont les images, les formulaires de saisie et des éléments programmables tels que des applets.

II.2.2 PHP5 :

C'est un langage de programmation compilé à la volée libre, principalement utilisé pour produire des pages Web dynamiques via un serveur HTTP, mais pouvant également fonctionner comme n'importe quel langage interprété de façon locale. ...

II.2.3 CSS3 :

Le terme CSS est l'acronyme anglais de Cascading Style Sheets qui peut se traduire par "feuilles de style en cascade". Le CSS est un langage informatique utilisé sur l'internet pour mettre en forme les fichiers HTML ou XML. Ainsi, les feuilles de style, aussi appelées les fichiers CSS, comprennent du code qui permet de gérer le design d'une page en HTML.

II.2.4 Python

Python est un langage de programmation objet, multi-paradigmes et multiplateformes. Il favorise la programmation impérative structurée, fonctionnelle et orientée objet. Il est doté d'un typage dynamique fort, d'une gestion automatique de la mémoire par ramasse-miettes et d'un système de gestion d'exceptions ; il est ainsi similaire à Perl, Ruby, Scheme, Small talk et Tcl.

Le langage Python est placé sous une licence libre et fonctionne sur la plupart des plates-formes. Il est conçu pour optimiser la productivité des programmeurs en offrant des outils de haut niveau et une syntaxe simple à utiliser.

Il est également apprécié par les pédagogues qui y trouvent un langage où la syntaxe, clairement séparée des mécanismes de bas niveau, permet une initiation aisée aux concepts de base de la programmation.

II.3 Outils matériel :

- **La raspberry pi 2 :** elle reçoit des informations et elle envoie ses commandes aux autres modules.
- **L'arduino :** envoyer des informations et recevoir des commandes de la Raspberry Pi et en fonction de ces commandes elle gère l'ouverture ou non de la porte.
- **NFC Shield :** C'est un lecteur qui sert à lire l'identifiant du badge
- **Badge RFID** (étiquette) : une carte qui contient un identifiant unique
- **Max485 :**c'est l'interface série du bus RS485.
- **Le lab d'essai :** Le lab d'essai nous a permis de réaliser et de tester l'interfaçage de nos modules au niveau matériel.
- **Leds à différentes couleurs :** définissent les différents états ou réponses du système par exemple une led rouge signifie un accès refusé.

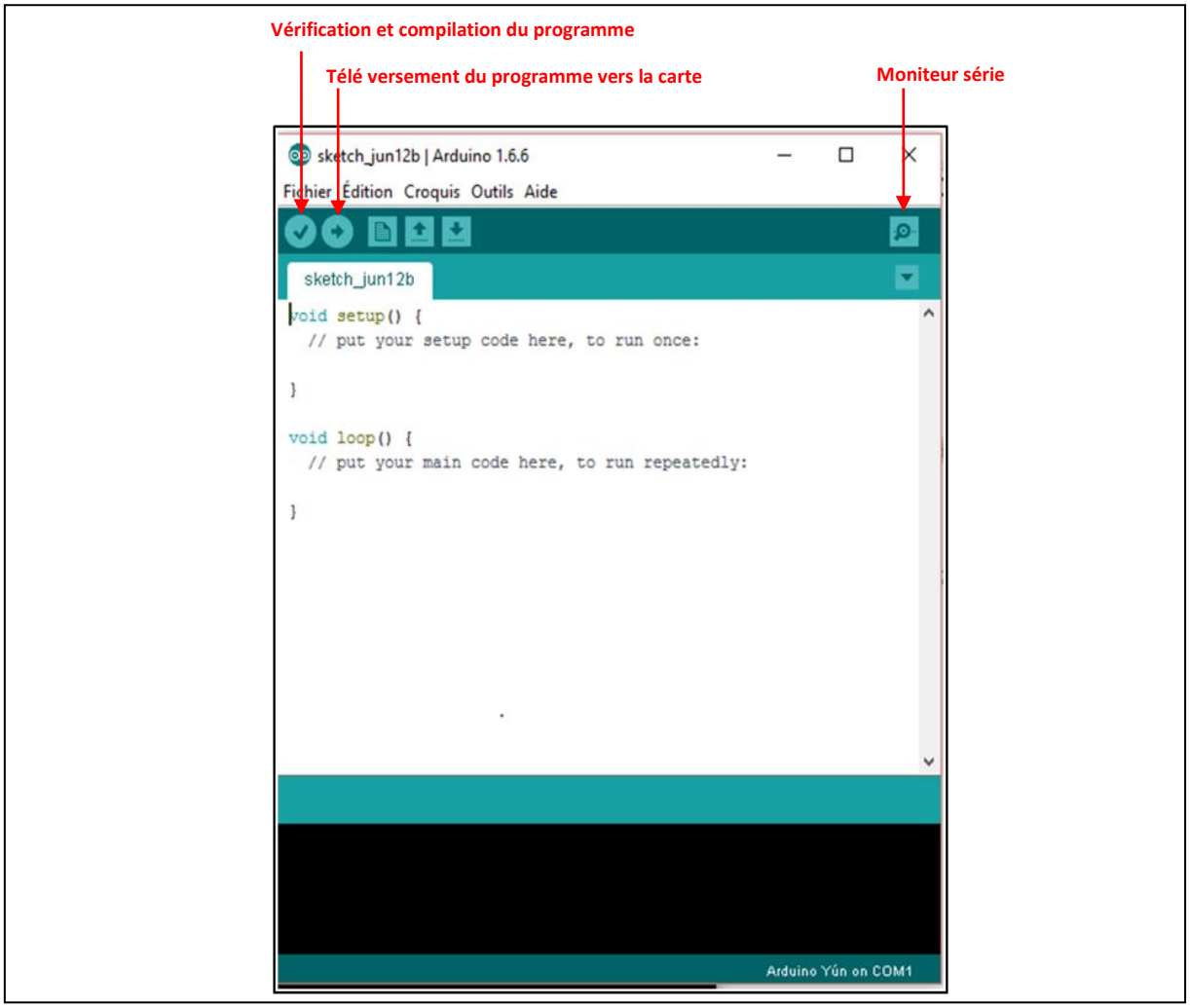
Dans ce qui suit on va s'intéresser à la description de l'environnement de développement d'arduino et à la configuration de la Raspberry Pi

II.4 L'environnement de développement Arduino

L'environnement de développement Arduino est une application Java multi-plateforme (fonctionnant sur plusieurs systèmes d'exploitation), servant d'éditeur de code et de compilateur, qui peut transférer le firmware (le programme) au travers de la liaison série asynchrone.

Le langage de programmation est une variante du C/C++, allégée et restreinte à l'utilisation de la carte, de ses entrées/sorties et de ses librairies associées.

À l'ouverture, l'interface visuelle de l'environnement ressemble à ceci:



FigIV.1 : L'interface de l'environnement de développement Arduino

Avant de démarrer l'environnement Arduino il faut brancher la carte à l'ordinateur, une fois l'environnement et lancer il faut sélectionner le bon port série dans le menu **Outil>Port** puis sélectionner le model de la carte **Outil>Type de carte.**

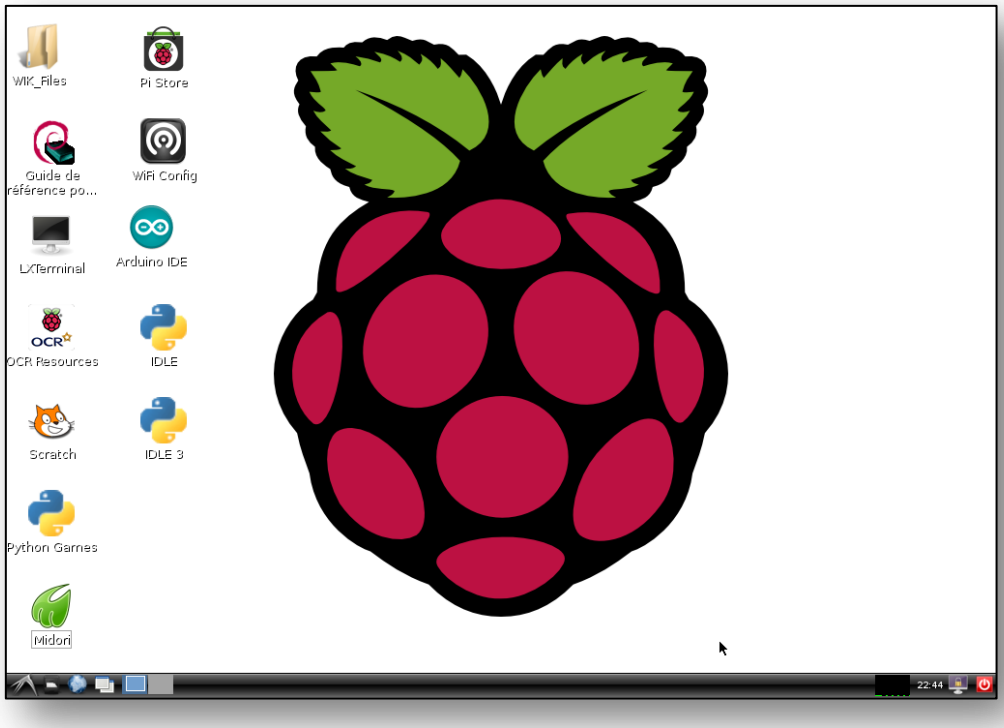
Pour faire communiquer l'arduino avec le module NFC Shield certaines bibliothèques sont nécessaires notamment RFID, SPI

II.5 Démarrage et configuration de la Raspberry Pi

Une fois la Raspberry Pi est alimentée, des informations de démarrage défilent à l'écran puis un login et un mot de passe sont demandés.

L'environnement graphique ne démarre pas de lui-même dans la plupart des distributions Linux pour Raspberry Pi. Afin de quitter la console en mode texte, on saisit la commande :
Startx

L'environnement de bureau graphique LXDE (*Lightweight X11 Desktop Environment*) propose une fenêtre simple qui ressemble à celle de Windows ou Mac OS X.



FigIV.2 : L'environnement graphique de la raspberry pi

À gauche du bureau, on trouve les raccourcis IDLE et IDLE3 pour le langage Python.
On trouve également le raccourci vers LXTerminal qui ouvre un terminal permettant d'émettre des commandes Linux dans une fenêtre en mode texte sans quitter l'interface graphique.

- **Attribuer une adresse IP statique pour le Raspberry PI :**

L'adresse IP est configurée dans le fichier /etc/network/interfaces et nous aurons besoin de modifier ce fichier pour la configuration de dynamique à statique. Pour cela on utilise la commande **`ifconfig`**

À partir du moment où l'adresse IP de la Raspberry Pi est connue, on peut s'y connecter à partir d'un autre poste informatique du réseau pour effectuer certaines opérations à distance.

➢ Installer un serveur Web sur la Raspberry Pi

Pour se faire on doit installer les modules suivant : Apache2, PHP5, SQLite3, RPI.GPIO et Pyserial.

✓ Installation du serveur Apache :

Avant d'installer le serveur on met à jour le raspbian, avec les commandes suivantes :

```
sudo aptitude update
sudo aptitude upgrade
```

Une fois raspbian mis à jour, nous allons installer le serveur Apache, avec la commande suivante :

```
sudo aptitude install apache2
```

✓ Installation de PHP sur le Raspberry

On Installe php5 avec la ligne de commande suivante :

```
sudo aptitude install php5
```

✓ Vérifier que PHP fonctionne :

Pour savoir si PHP fonctionne correctement, la méthode est relativement proche de celle employée pour Apache.

En premier lieu supprimer le fichier « index.html » dans le répertoire « /var/www » à laide de la commande suivante :

```
sudo rm /var/www/index.html
```

Puis on crée un fichier « index.php » dans ce répertoire, avec cette ligne de commande :

```
Sudo echo "<?php phpinfo.php ?>" /var/www/index.php
```

Pour vérifier le bon fonctionnement, on saisit l'adresse suivante dans notre navigateur web :http://192.168.1.2 (l'adresse statique attribuée à la Raspberry Pi)

✓ Installer un serveur de gestion de base de données SQLite 3

On installe SQLite3 avec la ligne de commande suivante :

```
sudo apt-get install sqlite3
```

- **Installer RPi.GPIO sur la Raspberry Pi**

On installe le module RPI.GPIO pour manipuler les broches de la Raspebry Pi.

- Décompresser l'archive puis l'installer

```
Sudo tar xzf RPi.GPIO-0.6.2.tar.gz
apt-get install RPi.GPIO
```

- **Installer pyserial sur la Raspberry Pi**

Ce module permet à la Raspebry Pi d'accéder au port série.

- Décompresser l'archive puis l'installer

```
Sudo tar xzf pyserial-3.0.1.tar.gz
apt-get install pyserial
```

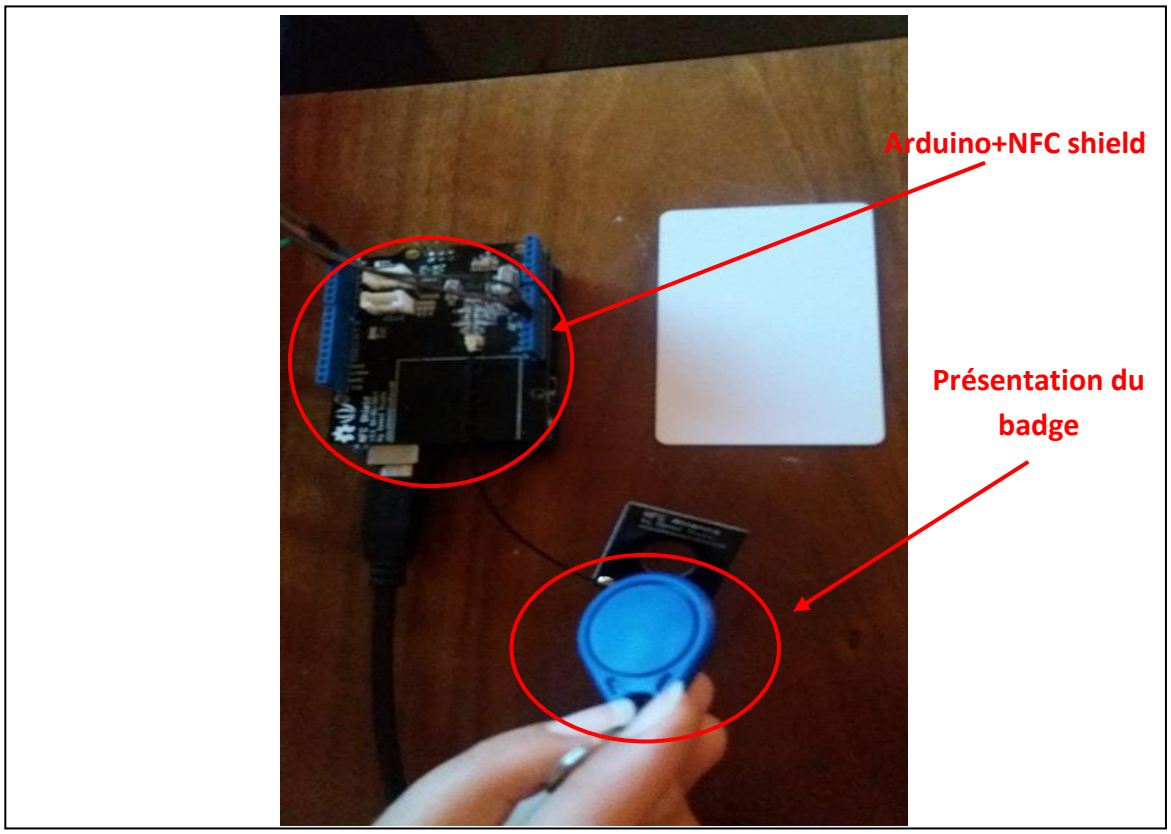
III. Les tests

Nous présentons dans cette partie les schémas de câblage de nos modules et les différents tests effectués sur ces derniers.

III.1 Le test récupération de l'identifiant

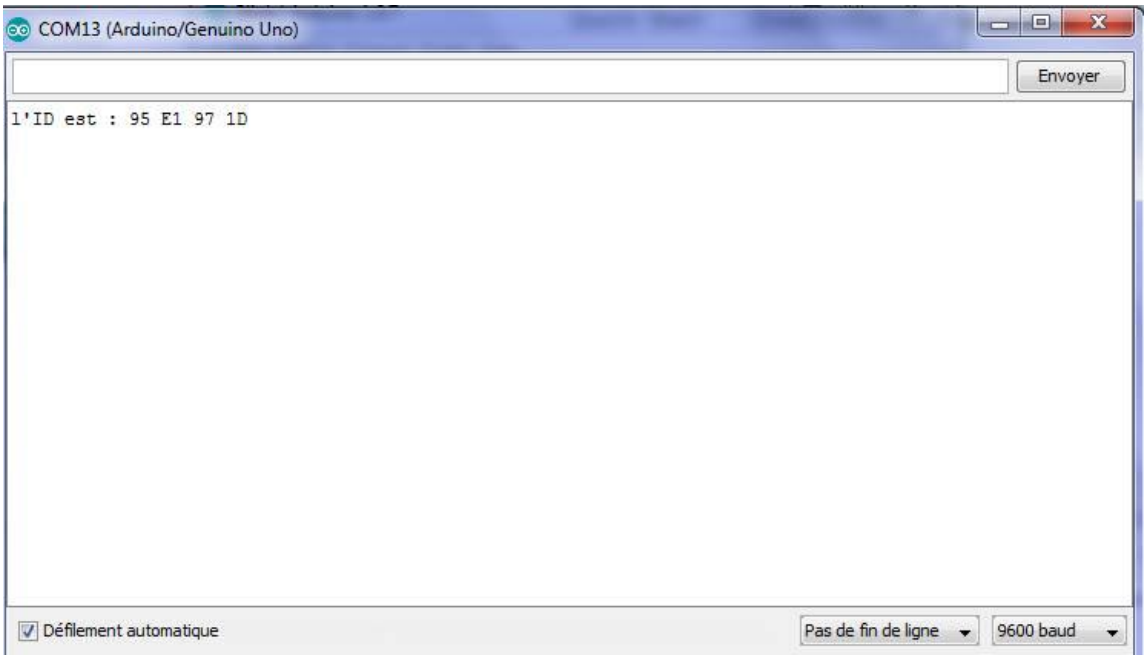
Comme il a été mentionné dans le chapitre précédent la récupération de l'identifiant se fait en reliant un lecteur RFID et une carte arduino, avec présentation du badge)

La figure suivante montre le test de récupération d'identifiant d'un badge RFID.



FigIV.3 Le test de récupération d'identifiant

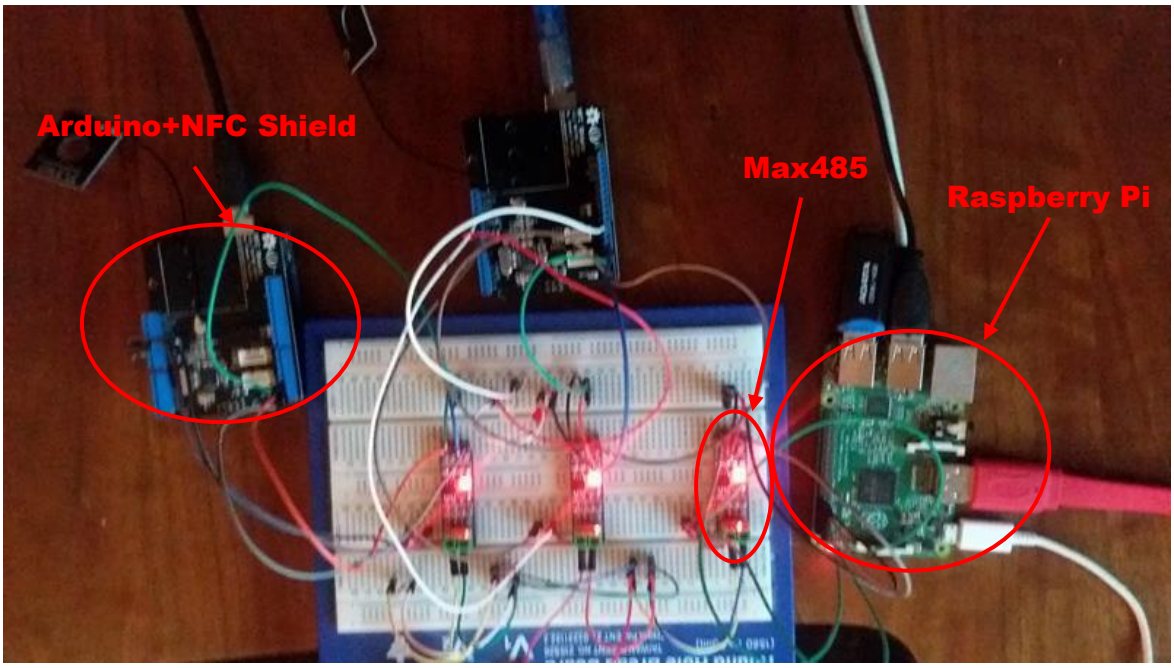
La figure fig IV.4 montre le résultat de présentation du badge au lecteur. On peut le voir ce résultat sur le moniteur série d'arduino



FigIV.4 le résultat de test récupération d'identifiant

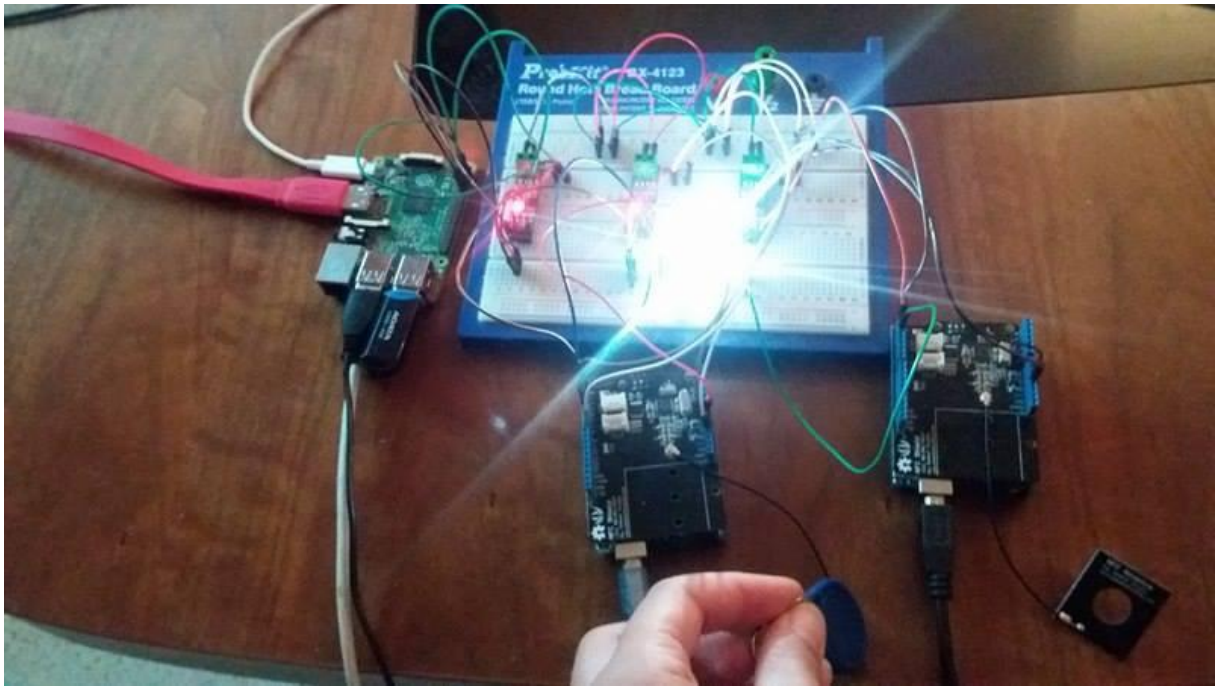
III.2 Le test de notre système

Ce test consiste à échanger des données entre la raspberry Pi et l'arduino en reliant ces composants via le bus RS485. Le branchement des composants est illustré par la figure suivante :



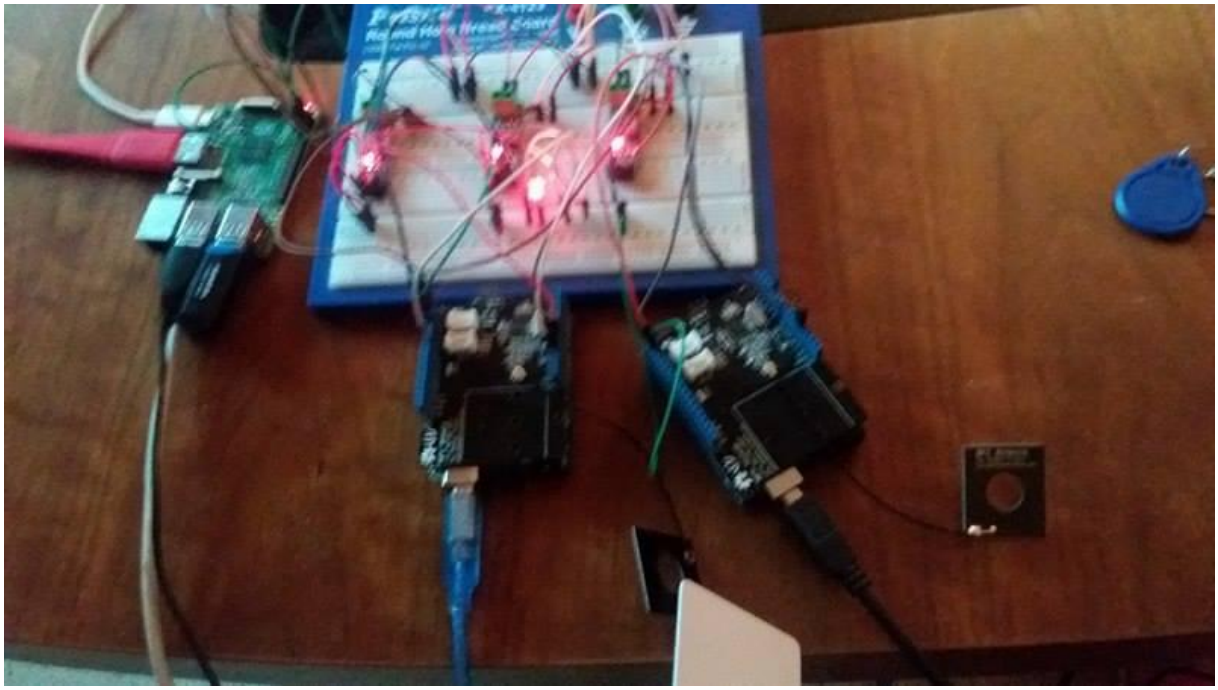
FigIV.5.Les branchements des composants de notre système

Sur la figure fig.IV.6 on peut voir l'allumage d'une led verte après présentation du badge qui signifie un accès accordé



FigIV.6 L'allumage d'une led verte

Sur la figure fig.IV.7 on peut voir l'allumage d'une led rouge après présentation du badge qui signifie un accès refusé



FigIV.7 L'allumage d'une led rouge

Comme il a été mentionné dans le chapitre précédent un logiciel de gestion est intégré dans la Raspberry Pi afin de gérer à distance notre système.

IV. Présentation de l'application :

- **Accéder au serveur:**

Pour accéder à notre logiciel de gestion, il faut entrer l'adresse IP de Raspberry Pi dans l'URL suivi du nom de fichier. Dans notre cas : 192.168.1.2/RFID

Une page d'authentification s'affiche comme suit :

Fig IV.8 Page d'authentification

- **Page d'accueil:**

Apres l'authentification la page d'accueil est la première page qui apparait à l'administrateur, elle contient tous les liens vers les autres pages.

Fig.IV.9 : La page d'accueil

- **Page Historique**

A partir de cette page l'administrateur peut s'avoir qui a accédé à la zone au quelle l'accès est contrôlé, dans quel jour à quel heure, et les tentatives d'accès

Identifiant_RFID	Nom	Prenom	Heure	Date	porte	Acces
E4 6B 18 C5	OTMANI	Nacera	01:15:23	03/07/16	5	Oui
E4 6B 18 C5	OTMANI	Nacera	01:15:33	03/07/16	4	Non
E4 6B 18 C5	OTMANI	Nacera	01:15:40	03/07/16	4	Non
E4 6B 18 C5	OTMANI	Nacera	01:15:46	03/07/16	4	Non
95 E1 97 1D	CHAFA	Tassadit	01:15:56	03/07/16	4	Oui
95 E1 97 1D	CHAFA	Tassadit	01:16:02	03/07/16	4	Oui
95 E1 97 1D	CHAFA	Tassadit	01:16:08	03/07/16	4	Oui
95 E1 97 1D	CHAFA	Tassadit	01:16:16	03/07/16	5	Non
E4 6B 18 C5	OTMANI	Nacera	01:16:24	03/07/16	5	Oui
95 E1 97 1D	CHAFA	Tassadit	01:16:30	03/07/16	4	Oui
95 E1 97 1D	CHAFA	Tassadit	01:20:53	03/07/16	4	Oui
95 E1 97 1D	CHAFA	Tassadit	01:21:04	03/07/16	4	Oui
95 E1 97 1D	CHAFA	Tassadit	01:21:10	03/07/16	5	Non
95 E1 97 1D	CHAFA	Tassadit	01:21:15	03/07/16	4	Oui
E4 6B 18 C5	OTMANI	Nacera	01:21:21	03/07/16	5	Oui
E4 6B 18 C5	OTMANI	Nacera	01:21:27	03/07/16	5	Oui
E4 6B 18 C5	OTMANI	Nacera	01:21:40	03/07/16	4	Non

FigIV.10 : La page Historique

L'ajout d'un nouveau utilisateur nécessite la connaissance de l'identifiant du badge attribué, donc une application d'ajout est nécessaire.

- **Application ajout :**

Cette application permet d'afficher l'identifiant lu à partir d'un lecteur RFID, puis la saisie des différentes informations concernant le nouveau utilisateur (Fig.IV.11)

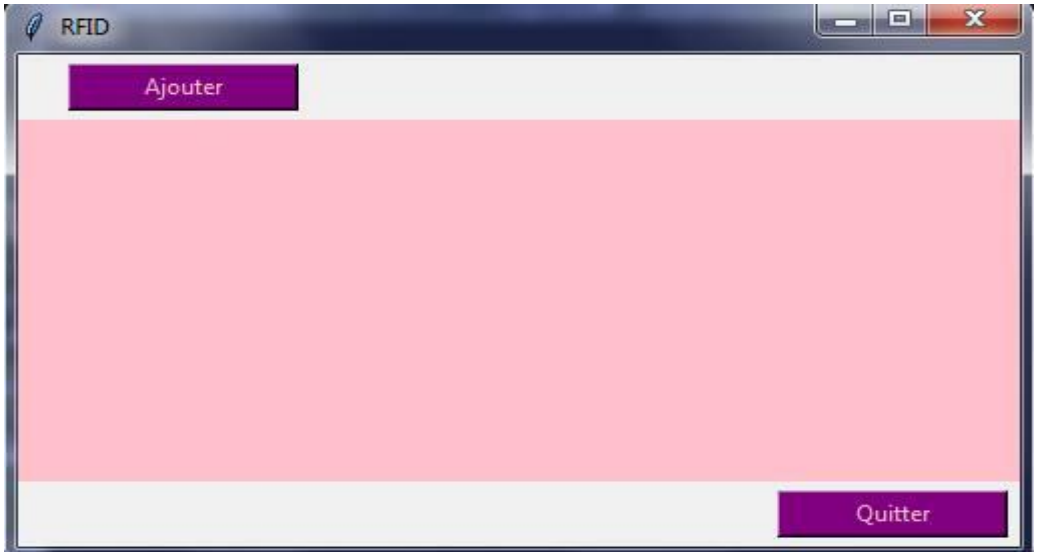
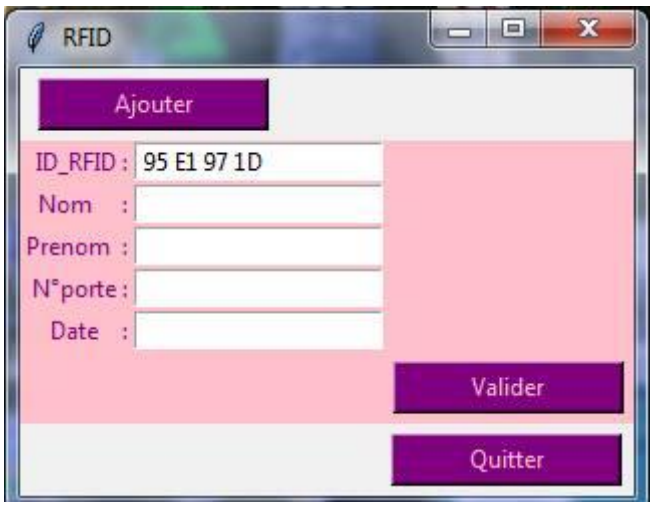


Fig.IV.11 : l'application d'ajout d'un utilisateur

- **La récupération de l'identifiant**

L'administrateur clique sur le lien Ajouter, un formulaire sera affiché, dont un identifiant sera récupéré (Après présentation du badge), l'administrateur le remplit puis il l'envoie**,** comme est illustré dans la figure suivante



FigIV.12 : Le formulaire Ajouter un utilisateur

V. Conclusion

Au cours de ce dernier chapitre, nous avons décrit l'étape de réalisation et de test de notre système. En premier lieu, nous avons présenté les outils de développement utilisés ainsi que les configurations matérielles effectuées. Ensuite, nous sommes passés à l'étape qui consiste à effectuer des tests sur notre système.
Comme nous l'avons mentionné, notre système offre à l'utilisateur de l'application les fonctionnalités nécessaires pour gérer les accès à la zone qu'il veut sécuriser.
En ayant les résultats attendus, on peut conclure que le système mise en place répond bien au besoin de contrôle d'accès.

Conclusion Générale

Conclusion général

L'objectif du présent travail étant de concevoir et de développer un système permettant de contrôler l'accès à des zones particulières. L'utilisation de nouvelles technologies d'identification rend l'échange d'informations plus rapide, notamment l'identification par radiofréquence (RFID) qui permet le contrôle d'accès et assure une meilleure traçabilité.
Ainsi, notre attention s'est orientée vers l'utilisation d'une application embarquée sur le Raspberry Pi en utilisant les technologies Web. Cette application permet la gestion du système

Afin de mieux cerner et comprendre les caractéristiques du matériel utilisé, nous avons présenté dans le premier chapitre des généralités sur les systèmes embarqués, leur architecture, leurs types et leurs utilisations. La technologie RFID et le contrôle d'accès ont été introduits au deuxième chapitre.

Pour développer notre système, nous avons suivi un cycle d'analyse, conception, implémentation, tests et déploiement. Les deux premières phases ont fait objet du troisième chapitre dans lequel les deux parties du système (logicielle et matérielle) ont été traitées et éclairés. Le quatrième chapitre a donc porté sur les dernières phases, l'implémentation et les tests.

Au terme de ce travail élaboré dans le cadre de notre projet de fin d'études, nous considérons que ce projet nous a été bénéfique vu qu'il nous a permis de consolider nos connaissances vers le développement d'un système embarqué qui sera utile dans le domaine de contrôle d'accès. En effet, l'apport de notre projet se résume surtout dans la découverte et la familiarisation avec les techniques de développement qui nous ont permis d'améliorer nos compétences et nos acquis en ce qui concerne la configuration Linux embarqué et la programmation.

Perspectives

Pour la suite de ce travail, nous avons comme perspectives : l'amélioration du matériels utilisés notamment le remplacement de la carte Arduino Uno par une Arduino Nano qui se caractérise par ses petites dimensions et un faible coût. L'utilisation d'un écran LCD pour l'affichage. L'acquisition d'une serrure électronique au lieu des leds. L'utilisation de la carte RFID et les empreintes digitales en même temps pour renforcer la sécurité. Contrôler l'accès par rapport à des jours et des horaires bien précis. Intégrer notre système dans des solutions embarquées finies qui pourraient être utilisée par exemple pour le contrôle d'accès au laboratoire LARI.

Bibliographie

[SE1] : Richard Grisel, Université de Rouen, Nacer Abouchi, ESCPE Lyon Les systèmes embarqués Introduction

[SE2] : Ramzi BOULKROUNE, Les Systèmes Embarqués, mémoire, , université d'Annaba, 2009.

[SE3] : http://www.technologuepro.com.

[SE4] : Didier DONSEZ, Systèmes d'exploitation pour l'embarqué, Université Joseph Fourier

[SE5] : Brique ROSE Samuel, Systèmes d'exploitation embarqués, École Nationale Supérieure des Télécommunications

[SE6] : pierre ficheux , Linux embarqué 2ème édition, Editions EYRO,2005

[SE7] Patrice Kadionik, Les systèmes embarqués : une introduction, Décembre 2005

[SE8] : http://www-igm.univ-mlv.fr/~dr/XPOSE2002/SE/architecture.html

[SE9] : Les mémoires, rapport, université Paul Sabatier

[SE10] : Anthony, processeur, article, 2014

[RF1] : Eric Schuler et Jean-François PILLOU, Article, de www.arvensys.com.

[RF2] : CNRFID, De l'innovation au déploiement de solution RFID et NFC, le centre national de référence

[RF3] : Jean de françoi, RFID (Radio Frequency Identification, septembre 2015

[RF4] : Noyel Mélanie Pisaneschi Thomas, Mise en place d'un système RFID pour une entreprise de panneaux laqués haute finition, Rapport de fin d'études, 2010 / 2011

[RF5]: https://rfid.ooreka.fr/comprendre/etiquette-rfid

[RF6]: L'identification par radio-fréquence Document réalisé par le collège Utilisateurs du CNRFID

[RF7]: Radio Frequency Identification, http://www.erasme.org/IMG/synthese

[RF8]:http://www.centrenational-rfid.com/classification-des-tags-rfid-article-19-fr-ruid 17.html

[RF9]: http://www.journaldunet.com/solutions/systemes-reseaux/dossier/rfid-10-applications-qui-montent/rfid-10-applications-qui-montent.shtml

[CA1]: http://www.itqsecurity.fr/controle-d-acces/

Bibliographie

[CA2]: http://www.silvaconsultants.com/introduction-to-access-control-systems.html

[Con1]: Jonathan W. Valvano,Embedded systems: introduction to ARM CORTEX: Microcontollers Volume , juin 2014

[rp1] : Matt Richardson,shawn Wallac , A la decouverte de la Raspberry Pi, livre, décembre 2014

[ard1]: https://www.arduino.cc/en/Main/Arduino

[ard2]: Livret Arduino en français par Jean-Noël Montagné, Centre de Ressources Art Sensitif, novembre 2006, sous licence CC.

[ard3] : Initiation Arduino http://oli.lab.perso.sfr.fr/cours%20Arduino

[ard4] : http://f-leb.developpez.com/tutoriels/arduino/univers_arduino/part1/

[nfc1]: http://www.gotronic.fr/art-shield-nfc-v2-0-113030001-19856.htm

[max1]: Lammert Bies, RS485 serial information, de http://www.lammertbies.nl/comm /info/RS-485.html

[RS1] : Présentation MODBUS via RS485 V1.1 - SOLIA Concept

[RS2] : http://xavier.fenard.free.fr/RS485.htm

[spi1] :http://wcours.gel.ulaval.ca/2011/a/GIF3002/default/5notes/SMI_C7_Periph_Interface_serie

[uart1] : J-M INGRE, la liaison série asynchrone(UART), cours AT90S8535, 2002