République Algérienne Démocratique Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Ibn Khaldoun – Tiaret

Faculté des Mathématiques et d'Informatique

Département Informatique

Thème

LA CONCEPTION ET LA RÉALISATION D'UN SYSTÈME D'ALARME ET CONTRÔLE D'ACCÈS

Pour l'obtention du diplôme de Master

Spécialité : Réseaux et télécommunication

Réalisé : -El Besri charaf eddine A. Rahman.

- Belghithare Merouan

Dirigé par : Mr. Daoud Bachir.

Année Universitaire : 2015-2016

Remerciements

*Avant toute chose je tiens à remercier le grand « **Dieu** « de nous avoir donné le courage et la volonté qui nous ont permis de réaliser ce modeste travail.*

*Nos remerciements particuliers à **Mr Daoud Bachir** pour ses remarques pertinentes et son optimisme qui nous fait parfois défaut. En outre ses qualités d'encadreur, nous ont toujours permis d'avancer à un rythme régulier dans notre travail, nous encourageant à persévérer. Nous exprimons toute notre gratitude à nos examinateurs*

Merci également à l'ensemble des enseignants du département Informatique Université Tiaret.

Enfin, nous ne saurions terminer ces remerciements sans y associer toute personne qui, de près ou de loin, nous a apporté son aide ou sa sympathie.

Liste des abréviations

CMSI : Centralisateur de Mise en Sécurité Intrusion

DAI : Détecteur Automatique d'Intrusion

DAS : Dispositif Actionné de Sécurité

DM : Déclencheur Manuel

DS : Diffuseur Sonore

DTMF : Double Tonalité Multifréquences

ECS : Équipement de Contrôle et de Signalisation

ERP : Établissement Recevant du Public

SDI : Système de Détection d'Intrusion

SSI : Système de Sécurité Intrusion

SMSI : Système de Mise en Sécurité Intrusion

CCTV : Closed Circuit Television

PIR : Passive Infra Red Sensor

GLCD : Graphic Liquid Crystal Display.

ICSP : In Circuit Serial Programming

LED : Diode Electro-Luminescente.

SD : Secure Digital Memory

USART : Universal asynchronous receiver/transmitter

MMC : Multimedia Memory Card

MSSP: Master Synchronous Serial Port

RAM: Read Access Memory

EEPROM: Electrically Erasable Programmable Read-Only Memory

PCB: Printed Circuit Board.

PLCC: Plastic Leaded Chip Carrier.

SPI: Serial Peripheral Interface.

I2C: Inter Integrated Circuit

PSP: Parallel Slave Port

CAN: Convertisseur Analogique Numérique.

PCMIA: Personal Computer

Manufacturer Interface Adaptor

ADCON: Analog Digital Converter.

MCLR: Master Clear.

Liste des figures

Liste des tableaux :

S O M M A I R E

Chapitre 03 : généralité Sur La téléphonie

Chapitre 04 : Conception du système de surveillance et control d'accès

Chapitre 05 : Réalisation du système de surveillance et 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 menaces

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 lointains.

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-autorisée pour des salles d'entrainement, ou à circuler dans les différents départements de l'entreprise est certainement très attrayante.

Toutefois l'électronique moderne et la technologie informatique ont apporté à la surveillance un tout nouveau champ d'application.

Notre objectif est de "concevoir un système de surveillance et de contrôle d'accès qui répond à des besoins bien spécifiques et dictés par le cahier des charges".

Ce système de surveillance et contrôle d'accès englobe un système d'alarme contre intrusion, un système de contrôle d'accès, dont l'ensemble est lié à un système d'appel téléphonique permettant d'informer les personnes concernées et se trouvant à distance, des différentes situations, par des messages vocaux.

Chapitre 01 : L'évolution des réseaux

1. Introduction :

Un système de communication, ou réseau, désigne tout ensemble d'éléments capables de véhiculer de l'information d'une source vers une destination. Le téléphone en est la meilleure illustration. Apparus plus récemment, de nouveaux types de réseaux transportant d'autres formes d'informations, telles que les données informatiques ou la vidéo. Ces systèmes ont pratiquement toujours été astreints à des supports fixes.

Au début des années 80, la CEPT (Conférence Européenne des Postes et Télécommunications) crée un groupe de travail, le GSM (Global System for Mobile Communication ou, groupe spécial mobile), pour définir un système numérique de communication avec les mobiles à vocation internationale pour l'horizon 1990. L'année 1992 a vu la commercialisation réelle des premiers systèmes GSM [1].

La norme GSM est adoptée dans de nombreux pays. C'est l'unique norme numérique de téléphonie cellulaire 2G (2ème Génération) acceptée en Europe. Dans la plupart des autres régions du monde, elle est en concurrence avec d'autres normes de radiotéléphonie numérique, en général originaires des Etats-Unis (Interim Standard IS-95) ou du Japon (Personal Digital Cellular PDC) [2]

Dans ce chapitre, nous parlerons de l'architecture d'un réseau GSM et l'évolution de ce dernier

2- Architecture du réseau GSM

Le réseau GSM est composé de 3 parties essentielles :

• Le sous-système radio BSS (Base Station Subsystem).

• Le sous-système réseau NSS (Network Sub-System).

• Le système réseau de gestion NMS (Network Management System) ou connu sous une autre appellation, le sous-système d'exploitation et de maintenance OSS (Opération and Maintenance Sub System).

2-1- Le sous-système radio (BSS)

Ce sous-système est constitué de stations de base BTS (Base Transreceiver Station), qui assure le lien radioélectrique avec les abonnés mobiles MS. Les BTS sont gérées par un contrôleur de stations de base BSC (Base Station Controller), qui assure également la fonction de concentration du trafic. Le BSC est connecté à un sous-multiplexeur transcodeur TCSM (TransCoder Sub-Multiplexer) qui rend compatible le réseau GSM avec les réseaux numériques fixes publics avec une adaptation du débit des circuits de parole.

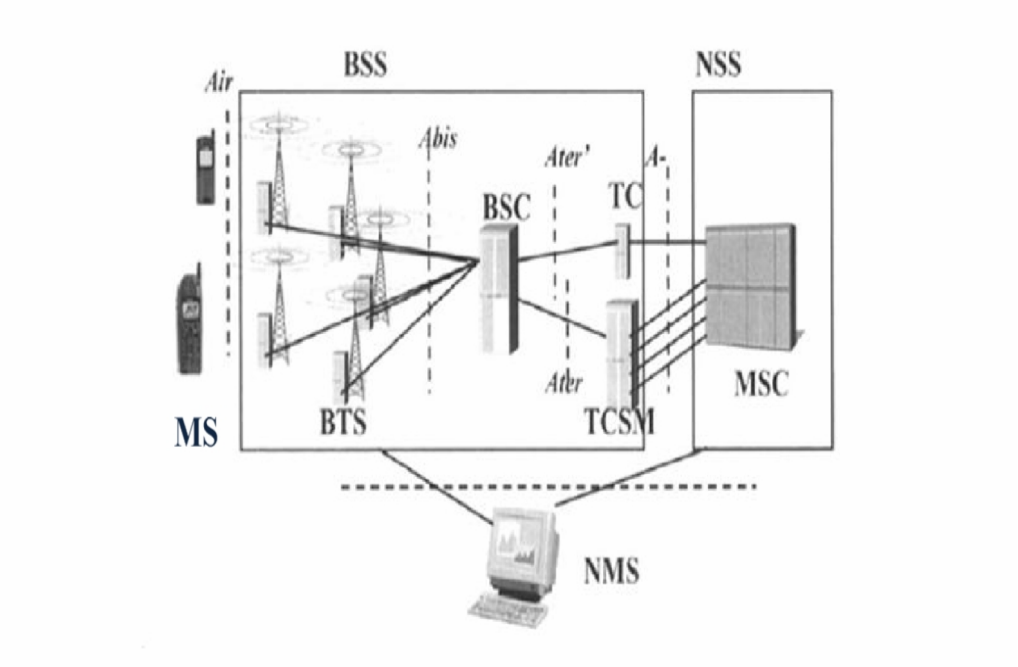


Figure1 : Architecture d'un réseau Gsm

2-2- Le sous-système réseau NSS

C'est une interface entre le réseau GSM et le réseau fixe public, elle regroupe toutes les fonctions de commutation et de routage, localisées dans le MSC (Mobile-services Switching Center). Les données de référence, propre à chaque abonné sont enregistrées dans une base de données répartie sur des enregistreurs de localisation HLR (Home Location Register) afin de minimiser les accès aux VLR (Visitor Location Register).

2-3-Le sous-système d'exploitation et de maintenance NMS

Il est utilisé par l'opérateur pour administrer son réseau, de manière locale par des OMC (Operation and Maintenance Centre), et de manière générale par les NMC (Network Management Centre). Les fonctions de sécurité et de contrôle d'accès au réseau sont assurées par le centre d'authentification AUC (AUthentication Centre) et l'enregistreur des identités des équipements EIR (Equipment Identity Register).

2-4-La station mobile (MS)

La station mobile MS (Mobile Station) désigne un équipement terminal muni d'une carte SIM (Subscriber Identity Module) qui permet d'accéder aux services de télécommunications d'un réseau mobile GSM. La carte SIM d'un abonné est généralement du format d'une carte de crédit, parfois même juste du format de la puce (plug-in). Elle contient toutes les informations nécessaires au bon fonctionnement du mobile :

- Ses identités
  - ✓ Universelle et unique IMSI (international Mobile Subscriber Identity).
  - ✓ Temporaire et valable seulement au sein d'un VLR : TMSI (Temporary Mobile Subscriber Identity).
- Eventuellement un code PIN (bloquant la carte après trois essais).
- Sa clé de chiffrement.
- Sa clé d'authentification.
- les algorithmes de chiffrement et d'authentification.

Le terminal est muni d'une identité particulière, l'IMEI (International Mobile Equipment Identity). Cette identité permet en particulier de déterminer le constructeur d'équipement.

2-5-Le canal physique (L'interface Air)

Les différentes interfaces dans un réseau GSM :

- L'interface Air.
- Interface Abis, reliant BTS au BSC
- Interface Ater, reliant BTS au TC (Transcoder) et au TCSM.
- Interface A-, reliant BSS au NSS.

L'interface Air est l'interface centrale, c'est la plus importante interface dans n'importe quel système GSM, car la station mobile est exposée directement à cette interface, et la qualité de cette interface est nécessaire pour la réussite du réseau GSM. Elle dépend directement de l'utilisation efficace du spectre de fréquence assigné à cette dernière. L'interface radio, ou l'interface Air, permet la connexion sans fil du terminal et du réseau. Elle est constituée de mécanisme permettant l'émission et la réception de signaux de radiofréquence de manière efficace et sûre, quelles que soient les conditions de propagation. Cette couche physique inclus des moyens permettant d'établir, de maintenir et de relâcher, mais également de particulariser les différents types de liens établis entre le terminal mobile et le réseau. Elle regroupe tous les moyens mis en œuvre dans un système de communication pour transmettre les informations d'un émetteur vers un récepteur. Dans un système radio mobile, la couche physique gère l'émission et la réception des signaux radio. Pour éviter que les signaux radio de différents utilisateurs proches ne se perturbent les uns les autres, le système de communication définit les règles d'accès au médium. Il peut s'agir des techniques d'accès multiples, dont les plus répandues sont le TDMA (Time Division Multiple Access), ou de versions hybrides telles que F-TDMA (Frequency-TDMA). L'information n'est pas transmise en une fois, il faut la découper et la transmettre au moyen de plusieurs trames consécutives.

En GSM, l'accès radio s'appuie sur la F-TDMA. Sur plusieurs bandes de fréquences se trouve une trame TDMA. Pour augmenter la diversité fréquentielle, il est possible de mettre en œuvre le saut de fréquence. Dans ce cas, chaque trame TDMA est transmise à une fréquence différente de la précédente, le jeu de fréquences utilisé étant connu à la fois de l'émetteur et du récepteur, et les trames TDMA se partagent les bandes de fréquences

disponibles. Les voies montantes (du mobile vers la station de base) et descendantes (de la station de base vers le mobile) sont séparées en fréquences, c'est ce qu'on appelle écart duplex. L'écart duplex est de 45 MHz pour le GSM 900 et de 95 MHz pour le GSM 1800. La bande de fréquences est découpée en canaux de 200 kHz. Ainsi, il existe 125 canaux montants dans la bande 890-915 MHz et 375 dans la bande 1710-1785 MHz. Ces canaux sont partagés entre les opérateurs.

L'accès TDMA est assuré par la découpe temporelle d'un canal de 200 kHz en huit intervalles de temps élémentaires appelés slots, numéroté de 0 à 7. La période d'un slot est de 577 µs et celle de la trame de 4.615 ms. Le débit binaire sur cette trame est environ 270 Kbit/s grâce à une modulation non linéaire, la GMSK (Gaussian Minimum Shift Keying). Les voies montantes et descendantes utilisent une structure TDMA identique mais avec un décalage temporel de trois slots. Cela évite qu'un mobile reçoit et transmet en même temps, ce qui serait techniquement réalisable, mais au prix de terminaux plus onéreux.

Un canal physique est défini par l'occurrence d'un timeslot, sur une fréquence particulière. Les canaux physiques permettent de transporter différents types de canaux logiques de débits variés. Pour mettre en œuvre cette variété de débits, une notion de multitrame a été introduite, permettant d'obtenir des périodes d'apparition spécifiques pour chaque type d'information : une multitrame à 26 trames, d'une durée totale de 120 ms, et une autre multitrame à 51 trames, d'une durée totale de 235,38 ms.

En fonction du canal logique transporté, le slot est organisé en burst. Un burst représente l'agencement des informations dans le signal transmis dans un slot TDMA. Il existe plusieurs types de bursts, dédiés à des fonctions particulières, telles que la synchronisation, l'accès initial, ou la transmission de données. Ce dernier burst, appelé burst normal, est illustré par la figure 2.

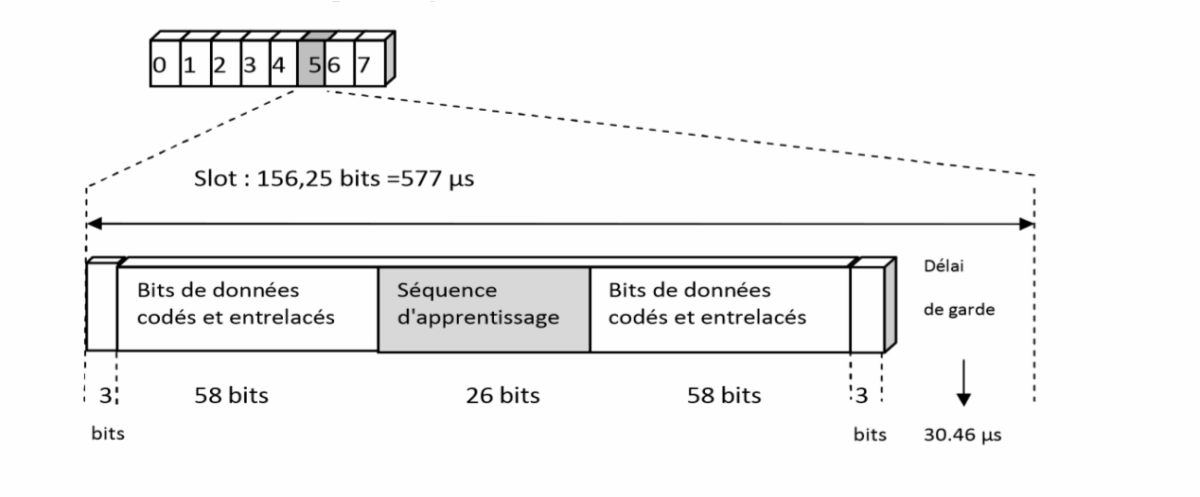


Figure2 : format d'un brust d'information

2-6-Les canaux logiques

Les canaux logiques permettent de distinguer les différents types d'informations circulant dans le système, il existe deux catégories de canaux logiques, les canaux communs, partagés par tous les utilisateurs, et les canaux dédiés, réservés à un utilisateur spécifique. Le tableau 1-1 présente tous les canaux logiques du GSM avec leurs fonctions. La manière avec laquelle les canaux logiques utilisent les canaux physiques pour le transport des informations est appelée le mapping, ou l'association des canaux logiques et des canaux physiques.

2-7-Le codage

Pour s'opposer aux erreurs, le GSM combine deux types de codes :

• **Les codes en blocs** : Appelés aussi CRC (Cyclic Redundancy Check), sont des codes cycliques utilisés pour détecter la présence d'erreur. Il en a été défini plusieurs sortes en fonction du type de canal logique transporté.

• **Les codes convolutifs** : Ils sont utilisés pour corriger les erreurs de transmission.

2-8-La modulation utilisée

La modulation des signaux utilisée dans les réseaux GSM est la modulation GMSK (Gaussian Minimum Phase-shift Keying), c'est une modulation angulaire dérivée de la modulation MSK appartenant à la famille de modulation des fréquences (FM) numérique. L'inconvénient majeur de la MSK est son large spectre d'opération.

La GMSK est choisie comme une méthode de modulation travaillant avec deux fréquences entre lesquelles elle transite facilement. L'avantage important de cette méthode est qu'elle ne module pas l'amplitude, et que la largeur de bande de transmission de fréquence est de 200 kHz, qui est une largeur de bande utilisée par les standards.

2-9-Les protocoles

L'interface radio du GSM permet la transmission sans fil entre le réseau et le mobile, d'une manière fiable et efficace. La communication d'un mobile doit cependant pouvoir être acheminée vers son destinataire à travers le réseau de l'opérateur mobile et le réseau téléphonique commuté public. De façon similaire, l'opérateur mobile doit connaître à tout moment l'état et l'emplacement du mobile de façon à pouvoir le contacter en cas d'appel. La mobilité à proprement parler doit être gérée, que le terminal soit en communication (cas du Handover), ou qu'il se connecte à un réseau autre que celui de l'opérateur d'origine (on parle dans ce cas de roaming).

1. Alarme d'intrusion

1.1. Système de détection des intrusions.

Dans le domaine des systèmes de sécurité industrielle, la méthode de protection est tout à fait différente. Elle se divise en trois parties :

- Détection
- Retardement
- alarme

Les systèmes d'alarme industriels résultent d'une intégration de plusieurs systèmes de capteurs. Le plus important pour les grandes installations serait la barrière extérieure sur laquelle est placé un capteur. Il permettrait de détecter et de retarder l'intrus avant même qu'elles n'atteignent le bâtiment lui-même. Comme décrit ci-dessous, il y a un certain nombre de barrages équipés par différents types de capteurs, chacun ayant ses qualités et ses défauts.

Autre que les capteurs montés sur les barrières, d'autres capteurs peuvent être disposés sur le dessus d'un mur ou enfouis dans le sol pour créer une ligne de défense cachée. Cela permet au système de sécurité de détecter des intrus, mais ne pas les retarder.

Un autre choix pour la détection est en circuit fermé de télévision (CCTV). La détection peut être manuelle (un gardien surveille les écrans vidéo, par exemple) ou automatique grâce à des logiciels de détection automatique de mouvement dans l'endroit vidéo-surveillé.

Cependant, le CCTV reste peu efficace en tant que capteur autonome dans des applications externes, parce qu'il est souvent affecté par les conditions météorologiques (brouillard épais, pluie, neige).

La dernière ligne de protection est le bâtiment lui-même. Il peut être protégé par des capteurs infrarouges, capteurs micro-ondes, les serrures à puce ou des portes équipées par des détecteurs magnétiques.

1.2. Types d'alarme d'intrusion à l'intérieur

Ces types de capteurs sont conçus pour une utilisation en intérieur. L'utilisation à l'extérieur ne serait pas recommandée en raison de la vulnérabilité de fausses alarmes et la durabilité du temps.

1.2.1. Détecteurs à infrarouge passif

Le détecteur infrarouge passif (Passive Infra Red : PIR) est l'un des détecteurs les plus courants dans les environnements domestiques et les petites entreprises, car il offre des fonctionnalités fiables et abordables. Le terme "passif" désigne que le détecteur est capable de fonctionner sans avoir besoin de générer et émettre sa propre énergie (contrairement aux capteurs à ultrasons et à micro-ondes qui sont des détecteurs d'intrusion volumétrique "actifs").

Les PIR sont capables de distinguer si un objet émetteur infrarouge est présent d'abord par la détection de la température ambiante de l'espace surveillé, puis par la détection d'un changement dans la température causée par la présence de cet objet.

En utilisant le principe de différenciation, qui se traduit par une vérification de la présence ou non-présence, le PIR permet de décider si un intrus ou un objet est réellement là.

Parmi ces zones, il y a des zones de non-sensibilité (zones mortes) qui sont utilisées par le capteur pour la comparaison.

1.2.2. Détecteurs à ultrasons

Utilisant des fréquences entre 25 kHz et 75 kHz, ces détecteurs à ultrasons actifs émettent des ondes sonores inaudibles par l'être humain.

Émises par l'émetteur, ces ondes sonores sont réfléchies par des objets solides (tels que le sol, le mur et le plafond), puis captés par le récepteur.

Le principe de l'effet Doppler est à la base de son fonctionnement. En effet, les ondes ultrasonores sont presque complètement réfléchies par les objets à surface rigide alors que les objets à surface molle (comme le corps humain) ont tendance à absorber une partie de l'énergie de ces ondes et entraînent un changement de leur fréquence.

Ainsi, un objet en mouvement introduit un changement de fréquence des ondes émises dont la détection implique une intrusion dans l'espace surveillé. . Deux conditions doivent se produire pour détecter avec succès un événement par effet Doppler :

- Il doit y avoir un mouvement d'un objet dans l'axe du récepteur.
- Ce mouvement doit provoquer un changement de la fréquence des ultrasons captés par le récepteur par rapport à la fréquence d'émission.

1.3. Types d'alarmes d'intrusion à l'extérieur (En plein air)

Ces types de capteurs se trouvent souvent montés sur des barrières ou installés sur le périmètre de la zone protégée.

1.3.1. Vibreur

Ces dispositifs sont montés sur les obstacles et sont surtout utilisés pour détecter une attaque sur la structure elle-même. La technologie repose sur une configuration instable mécanique qui fait partie du circuit électrique. Quand un mouvement ou vibration se produit, la partie instable du circuit se déplace et brise le flux de courant, qui produit un signal d'alarme. La technologie des appareils varie et peut être sensible aux différents niveaux de vibration. Le milieu de la transmission des vibrations doit être correctement sélectionné pour le capteur spécifique.

Un type assez nouveau et non prouvée de capteurs utilise des composants piézo-électriques plutôt que de circuits mécaniques, qui peuvent être ajustées pour être très sensibles aux vibrations.

Avantages : capteurs très fiables, à faible taux de fausses alarmes et de prix abordables.

Inconvénients : Le prix assez élevé dissuade de nombreux clients, mais son efficacité compense son prix élevé.

1.3.2. Détection passive du champ magnétique

Ce système de sécurité enterré, est basé sur le principe de détection des anomalies magnétiques de l'opération. Le système utilise un générateur de champ électromagnétique alimenté par deux câbles en parallèle. Les deux fils passent le long du périmètre et sont généralement installés à environ 5 cm au-dessus d'un mur ou d'environ 30 cm sous terre. Les

fils sont connectés à un processeur de signal qui analyse tout changement dans le champ magnétique.

Avantages : Taux de fausse alarme très faible permettant de détecter les cambrioleurs réels.

Inconvénients : ne peut pas être installé à proximité de lignes à haute tension, les radars ou les aéroports.

1.3.3. Détection active du champ électromagnétique

Ce système de proximité peut être installé sur le périmètre du bâtiment, des clôtures et des murs. Il offre aussi la possibilité d'être installé sur des poteaux autoportants dédié. Le système utilise un générateur de champ électromagnétique alimentant un fil, avec un autre fil de détection parallèle. Les deux fils passent le long du périmètre et sont généralement installés, près de 800 mm, l'un par rapport à l'autre. Le fil de la sonde est relié à un processeur de signal qui analyse :

- Le changement de taux électromagnétique (mouvement des intrus)
- Le temps des perturbations

Ces paramètres caractérisent le mouvement de l'intrus et quand les trois sont détectés simultanément, un signal d'alarme est généré.

La barrière peut fournir une protection contre le sol à environ 4 mètres d'altitude. Il est généralement configuré dans les zones de longueurs allant jusqu'à 200 mètres selon le nombre de fils de capteur installé.

Avantage : peut être complètement discret.

Inconvénient : - coût élevé

1.3.4. Détecteur à fibre optique

Un détecteur à fibre optique peut être utilisé pour détecter les intrusions en mesurant la différence de la quantité de lumière envoyée par le noyau de la fibre. Si la fibre est perturbée, une partie de la lumière sera perdue et le récepteur détecte cette fuite. La détection peut porter aussi, non pas sur la quantité de la lumière reçue, mais sur le changement de polarisation causé par le mouvement survenu sur la fibre.

Le support portant la fibre peut être attaché directement à une clôture ou lié à une bande en acier barbelé qui est utilisé pour protéger le haut des murs et des clôtures.

Avantages : très semblable au système microphonique, configuration simple, facile à installer. Peut protéger des longues distances (de plusieurs km).

Inconvénients : taux élevé de fausses alarmes.

1.3.5. Champ électromagnétique de perturbation

Ce système utilise un principe de champ électromagnétique de perturbation basée sur deux câbles coaxiaux non blindée enterrés à environ 1015 cm de profondeur et situé à environ 2,1 mètres. L'émetteur émet une Radio Fréquence (RF) sur le premier câble, cette fréquence est reçue par le second câble. Lorsque le changement de l'intensité du champ diminue en raison de la présence d'un objet et atteint un seuil préétabli inférieure,

Une condition d'alarme est générée. Le système est discret quand il est installé correctement.

Avantages : caché comme une forme enterrée.

Inconvénients :

- sensible au bruit RF
- Taux élevé de fausses alarmes.
- Difficile à installer.

2. Contrôle d'accès

2.1. L'accès physique

En matière de sécurité physique, le terme contrôle d'accès désigne le fait de restreindre l'entrée d'une propriété, d'un bâtiment ou d'une salle aux personnes autorisées. Le contrôle d'accès physique peut être réalisé par un gardien, par des moyens mécaniques tels que des serrures à clés, ou par des moyens technologiques tels que les systèmes automatiques de contrôle d'accès, comme le vestibule de contrôle d'accès.

Le contrôle d'accès physique doit avoir des réponses aux questions : Qui ?, Où ? Et Quand ?

Un système de contrôle d'accès détermine qui est autorisé à entrer ou sortir, où ils sont autorisés à entrer ou à sortir, et quand ils sont autorisés à entrer ou sortir.

Historiquement, cela a été partiellement réalisé au moyen de clés et de serrures. Quand une porte est verrouillée, uniquement celui qui possède une clé peut entrer par la porte. Les serrures mécaniques à clés ne permettent pas des restrictions sur les moments et les dates d'accès. Elles ne fournissent pas aucun

Autre moyen de contrôle en ce qui concerne la copie des clés ou sur les personnes qui les ont utilisées.

Quand une clé mécanique est perdue ou le détenteur de la clef n'est plus autorisé à utiliser la zone protégée, les verrous doivent être retapées.

Le contrôle d'accès électronique utilise des systèmes plus intelligents pour éviter ce type de défauts en offrant un large éventail de pouvoirs qui peut être utilisé pour remplacer des touches mécaniques.

Le contrôle électronique accorde l'accès en se basant sur les informations d'identifications présentées. Lorsque l'accès est accordé, la porte est déverrouillée pendant une durée prédéterminée et la transaction est comptabilisée. Lorsque l'accès est refusé, la porte reste verrouillée et la tentative d'accès est enregistrée. Le système peut également surveiller la porte et déclenche une alarme si la porte est forcée ou maintenue ouverte trop longtemps après avoir été déverrouillée.

2.2. Fonctionnement d'un système de contrôle d'accès

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.

2.3. Composants du système de contrôle d'accès

Un point de contrôle d'accès, tel qu'une porte, une barrière de parking, un ascenseur, ou toute autre barrière physique commandée électriquement, peut contenir plusieurs éléments. À la base, il y a une serrure électrique autonome qui se déverrouille par une opération de commutation.

Pour surveiller la position de la porte un interrupteur de porte magnétique est utilisé.

2.3.1. Types de lecteurs

La borne comporte souvent un lecteur qui pourrait être un clavier, un lecteur de carte magnétique 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 RS-232, 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 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.

Conclusion

Dans ce chapitre nous avons parlé des systèmes d'intrusion de leurs types, de leur structure, et des périphériques (capteurs, détecteurs, sirènes…). Des avantages et inconvénients de ses différents périphériques.

De même nous avons donne une vue globale sur les systèmes de contrôle d'accès, leur utilisations, leur rôle, et les différents types valables.

Dans ce qui suit nous allons parler de la ligne téléphonique et de sa caractéristique afin de pouvoir englober tous les systèmes nécessaires pour notre système de surveillance et de contrôle d'accès.

À travers ce chapitre, nous présentons quelques notions générales de la téléphonie ainsi qu'un bref aperçu sur les principes de la commutation téléphonique et les signaux échangés lors d'une communication, ce qui nous aidera dans l'étude et le montage de la partie, de notre système, liée à la transmission de l'information.

1. Principe de base de la téléphonie :

Initialement, l'objectif de la téléphonie était la transmission à distance de la voix humaine. Cette transmission nécessite la transformation de l'énergie acoustique en énergie électrique.

L'énergie acoustique (voix) se transforme en énergie mécanique sous l'effet de la vibration de la membrane du microphone, qui la transforme en énergie électrique qui sera, ensuite, amplifiée pour qu'elle soit transmise ensuite à l'autre bout du circuit, où elle sera reconvertit en énergie mécanique puis acoustique grâce à la membrane vibrante d'un haut-parleur (voir schéma de la figure 3).

Dans ce qui suit, nous nous intéressons à la description de la transmission téléphonique.

1.1. Bande utile :

C'est la bande de fréquence transmise pendant une conversation. Pour une conversation courante, la bande de fréquence transmise d'après la recommandation de la CCITT (Comité Consultatif internationale Téléphonique et Télégraphe) est de 300Hz à 3400Hz.

1.2. La signalisation

La connaissance des caractéristiques d'une ligne téléphonique telles que ses états, ainsi les diverses tensions sont fondamentales, pour la conception, le dimensionnement et la mise en œuvre de tout système de transmission, de gestion ou de communication téléphonique.

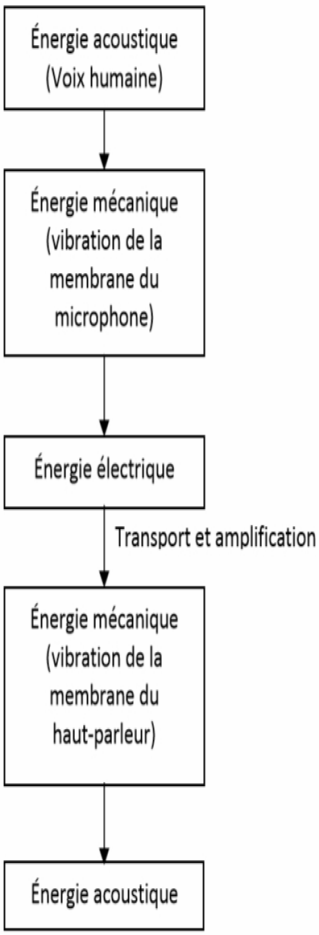


Figure3 : les étapes de transformation de l'énergie acoustique en énergie électrique

La mise en œuvre d'un réseau téléphonique automatique implique l'existence de moyens d'échanges d'informations, d'une part, entre les différents autocommutateurs et d'autre part entre autocommutateurs et terminaux.

Ces moyens d'échanges et l'ensemble des procédures associées constituent la signalisation téléphonique. On distingue en général, la signalisation terminale qui est échangée entre le poste téléphonique et le réseau, et la signalisation entre autocommutateurs.

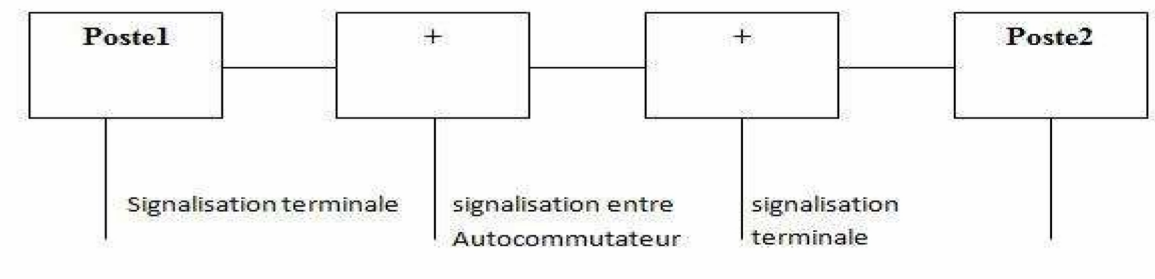


Figure 4 : signalisation terminale échangée entre abonné et autocommutateur

1.3. Ligne d'abonné :

La ligne téléphonique nécessite deux fils conducteurs qui servent comme support de la transmission, à la fois :

- Du courant d'alimentation.
- Du signal utile porteur de la conversation.
- D'un certain nombre de signaux de service (signal d'occupation, d'invitation à transmission, retour d'appel).

La ligne d'abonné est constituée de deux fils métalliques, cuivre ou bronze, reliant le poste d'abonné à son central, ce qui permet de réaliser un circuit fermé sur la boucle du poste d'abonné. Chaque abonné a donc une paire de fils réservée à son seul usage.

1.4. Échange de signaux entre postes demandeur et demandé :

1.4.1. Invitation à la numérotation :

Lorsque l'autocommutateur est prêt à recevoir la numérotation, il envoie sur la ligne de l'abonné une tonalité d'invitation à numéroter sous forme d'un signal permanent d'une fréquence de 440Hz. Cette tonalité se transforme en "occupation" si aucun numéro n'a été composé dans les vingt secondes (ligne classée en faux appel).

La numérotation peut être transmise sous deux formes selon le type du poste téléphonique.

Si le poste de l'abonné demandeur est équipé d'un cadran, les chiffres constituant le numéro de l'abonné demandé seront transmis sous forme de trains d'impulsions. Une impulsion est constituée d'une ouverture de la boucle d'une durée de 66 ms. Deux impulsions successives d'un même train sont séparées par une fermeture de la boucle d'une

durée de 33 ms, le nombre d'impulsions constituant un train est égal au chiffre à transmettre sauf le zéro qui correspond à dix impulsions.

La durée entre deux trains consécutifs est supérieure ou égale à 200 ms.

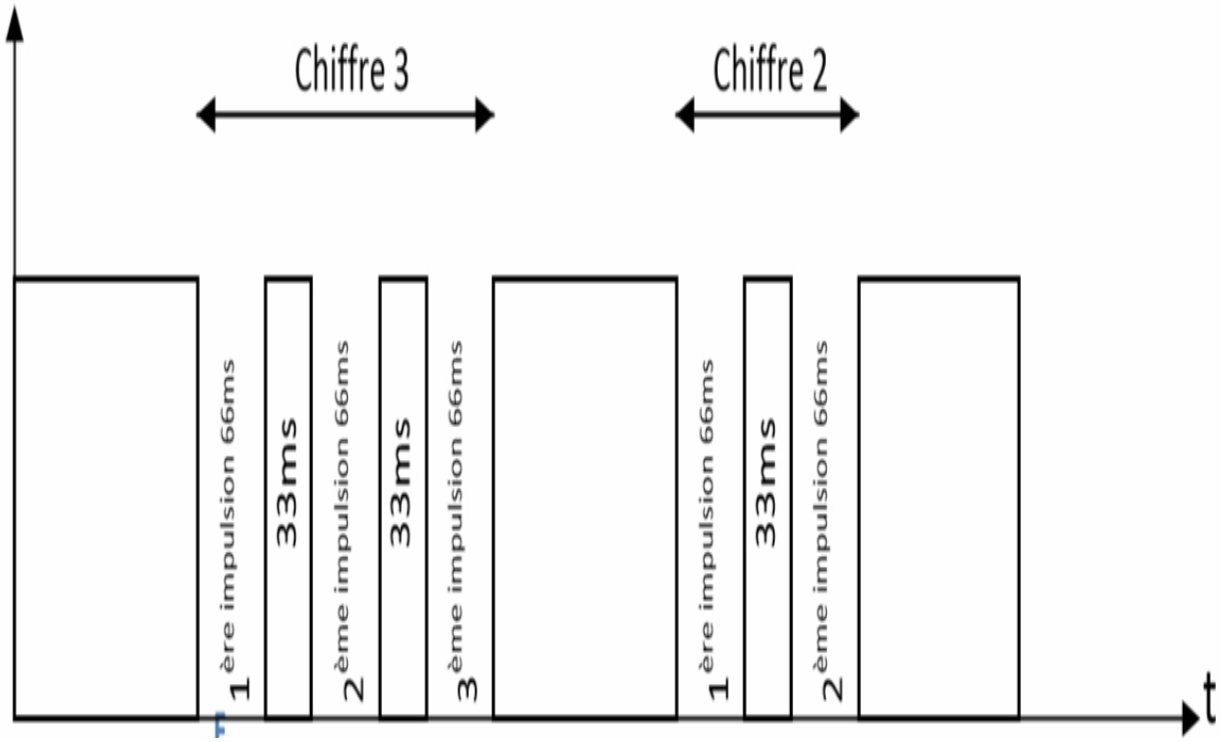


Figure5 : transmission du numéro 32 par trains d'impulsions

Par contre, si le poste de l'abonné demandeur est équipé d'un clavier, chaque chiffre sera transmis sous forme d'impulsions bi-fréquences dont la durée dépend du temps d'enfoncement de la touche correspondante.

Les claviers les plus répandus sont de type multifréquences, autrement dit "DTMF"(Double Tonalité Multi-Fréquences) ou à fréquences vocales : à chaque touche correspond une paire de fréquences : l'une fait partie d'un groupe de hautes fréquences et l'autre appartenant au groupe des basses fréquences (voir Table 1).

Contrairement aux impulsions décimales, ces signaux bi-fréquences peuvent être reçus par votre correspondant si vous actionnez le clavier au cours de la communication. On peut ainsi faire très souvent l'économie d'un boîtier à couplage acoustique.

Fréquences (Hz)	1209	1336	1477
697	1	2	3
770	4	5	6
852	7	8	9
941	*	0	#

Table1 : fréquences utilisées pour les différentes touches du clavier d'un poste téléphonique

1.4.2. État de la ligne

À la fin d'une numérotation, et lorsque la ligne du correspondant est libre, le demandeur reçoit le retour d'appel, sinon une tonalité d'occupation est entendue dans son récepteur.

La tonalité de retour d'appel est émise vers l'abonné demandeur par l'autocommutateur de rattachement de l'abonné demandé. Elle est constituée de la fréquence 440Hz émise à la même cadence et, en principe, en phase avec le courant d'appel qui provoque une sonnerie du poste appelé, c'est-à-dire 1.7 seconde d'émission et 3.3 secondes de silence.

Dans le cas où la ligne serait occupée ou si un encombrement est rencontré dans l'accès à celle-ci, la tonalité d'occupation est envoyée à l'abonné demandeur. Elle est constituée de la fréquence 440Hz émise à une cadence de 0.25s d'émission et 0.25s de silence. Si la ligne appelée est inaccessible pour une autre raison que l'occupation, un enregistrement vocal sera émis vers le demandeur, lui précisant la cause d'inaccessibilité.

Généralement, l'autocommutateur, qui constate cette inaccessibilité émet l'enregistrement vocal.

1.4.3. Retour d'appel

- **Réponse de l'abonné demandé**

Au moment de décrochage de l'abonné demandé, la tonalité de retour d'appel disparaît. Cette tonalité est constituée de fréquence de 440Hz émise à la cadence de 1.2s d'émission et de 1.2s de repos. Lorsque le poste demandé décroche, l'autocommutateur arrête l'envoi du courant d'appel et de la tonalité de retour d'appel. Par contre, si au bout de 30s, le poste demandé n'aurait pas décroché, l'autocommutateur émet un signal d'occupation sur la ligne du demandeur.

- **Caractéristiques des signaux du demandeur**

Au repos, une ligne téléphonique présente, entre ses deux fils une tension continue de 48 à 50v, dont l'un des pôles est relié à la terre. Pour faire sonner le poste, le central peut superposer, à cette alimentation continue, une tension alternative d'environ 80V et de 50Hz. Un simple condensateur permet de séparer ces deux tensions lorsque ceci est nécessaire.

Lorsqu'on décroche le poste (ou lorsque un système automatique prend la ligne), un circuit approprié consomme un courant d'environ 35mA sur la ligne, ce qui fait chuter la tension à 7V.

- **Cas d'arrivée d'un appel**

La ligne appelée étant au repos, elle est alimentée normalement par son autocommutateur par une tension de 48V, qui passe à près de 100V à la sonnerie.

Lorsque la communication est enfin établie, il faut que l'injection et le prélèvement des signaux sur la ligne se fasse sous une impédance de 600, avec une puissance largement inférieure au milliwatt, et dans la bande 300-3400Hz.

1.4.4. Tonalités

Les différentes tonalités échangées entre le poste demandé et le poste demandeur se caractérisent par :

- la fréquence
- la cadence
- et le niveau sonore

Elles sont données par la table 2 :

	Fréquence	**Cadence**	**Niveau**
Tonalité d'invitation à numéroter	425±2Hz	Continue	-12 dB
Tonalité d'occupation	425±2Hz	émission 0.25s, repos 0.25s	-12 dB
Tonalité de retour d'appel	425±2Hz	émission 1.2s, repos 4.65s	-12 dB
Tonalité d'encombrement	425±2Hz	émission 0.25s, repos 0.25s	-12 dB

Table 2 : Les différentes tonalités

Conclusion

À travers ce chapitre, nous avons présenté les spécifications techniques, et les contraintes qui en découlent, et dont nous aurons besoin pour comprendre et faire fonctionner un module de transmission via une ligne téléphonique fixe et commutée.

Le principe de fonctionnement, les fonctionnalités du système conçu et tout ce qui a rapport avec la conception du système sera étudié en détail dans les chapitres suivants.

Référence **[3]**

1. Structure du système

Le système de surveillance et contrôle d'accès est constitué de plusieurs modules (figure 6), chacun accomplit une ou plusieurs fonctions qui lui sont propres. On y distingue :

• le module central qui prend en charge de commander et de recevoir les instructions des autres modules, c'est lui qui gère et qui maintient le fonctionnement du circuit. Il contient un écran graphique à cristaux liquides et un clavier comme périphériques d'interfaçage humain.

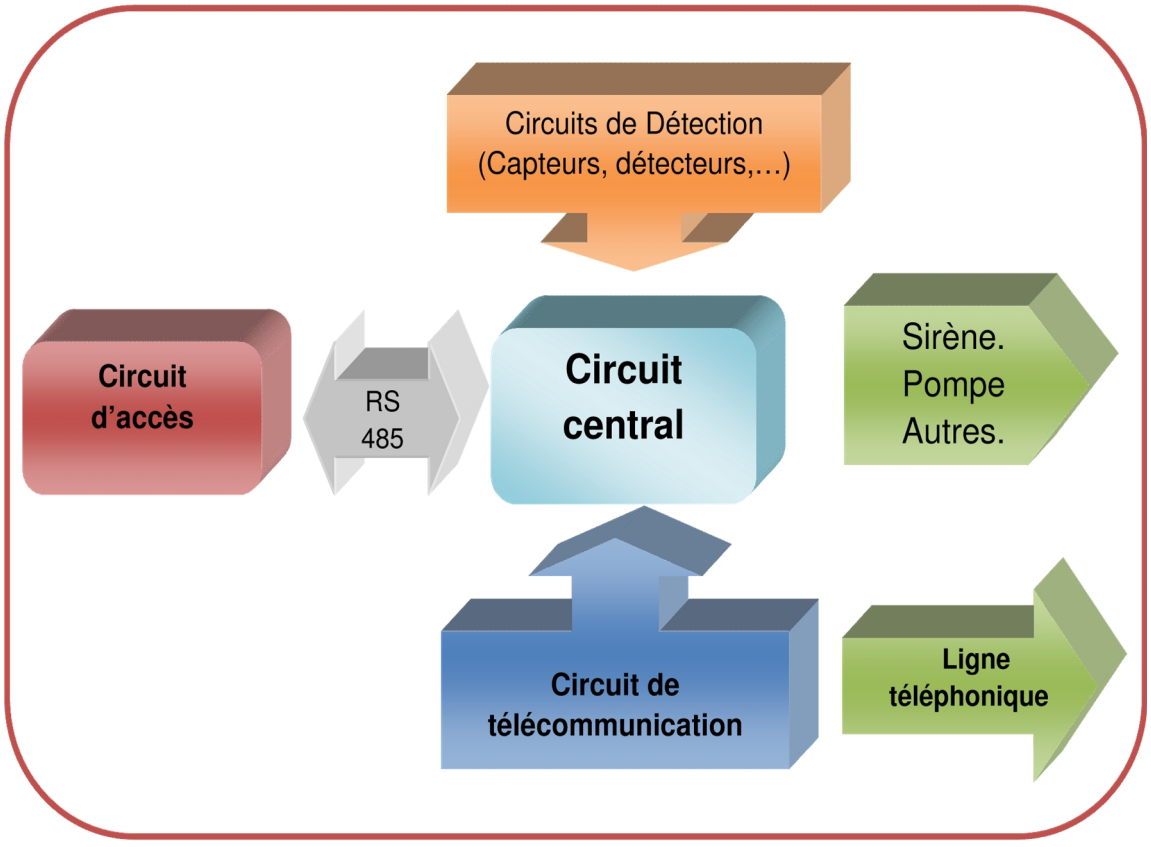


Figure 6 : schéma bloc de système.

• Le module d'accès : il est constitué d'un clavier et d'un écran LCD à deux lignes, il assure la saisie du code d'accès, et ensuite autorise ou non l'accès à un endroit spécifique en

commandant une porte à verrouillage électrique. Il est connecté au module central à travers le Protocol RS485.

- Le module de télécommunication : il sert à assurer le transfert des informations concernant l'état de l'alarme aux personnes désignées à travers une ligne téléphonique. Il est constitué d'un combiné téléphonique réduit et d'un circuit d'émission vocale.

Le déclenchement d'une alarme évoque l'établissement d'un appel via la ligne téléphonique. Ce module compose un des numéros de téléphone prédéterminés dans le système, pour que la (ou les) personne(s) concernées soit tenue informée de la situation en faisant émettre, par le circuit vocal, le message approprié sur la ligne téléphonique.

2. Principaux éléments constituants de chaque module

2.1. Module central :

Il constitue le cœur du système. Il est maître des autres modules desquels il reçoit les informations et vers lesquels il envoie ses commandes.

Pour des raisons de sécurité, l'accès au contenu logiciel de ce module serait protégé par un code formé d'au moins 4 caractères.

Ce module accomplit les tâches suivantes :

- Marche et arrêt de tout le système.
- Activation et désactivation de la surveillance de chacune de zones de sécurité.
- basculer entre mode "silencieux" ou "non silencieux" des alarmes.
- Changement de mot de passe
- Changement des numéros de téléphones
- Affichage de tous les changements effectués et les modes choisis.

Pour assurer ses fonctions, le module central serait muni

- d'une unité de traitement à base d'un processeur gérant toutes les commandes
- d'un clavier qui transmettra les commandes de l'utilisateur au processeur
- d'un écran qui affiche l'état de chaque zone

• bien sûr, des ports d'Entrée/Sortie pour faire la connexion avec les détecteurs et les organes de commande.

Puisque ce circuit doit piloter un système d'alarme d'incendie et de détection d'intrusion dans un vaste espace qui constitue la menuiserie, nous avons eu recours à une partition minimale de cet espace en 16 zones différentes.

Pour communiquer avec le module de contrôle d'accès, nous devons nous servir d'un module RS485 qui est capable d'assurer la communication pour des distances relativement longues (300m).

En résumé, le module central comporte :

- un microcontrôleur PIC 16F877A
- un clavier 4x3,
- un écran graphique à cristaux liquide 128x64,
- un circuit d'interface série avec l'écran LCD,
- un circuit d'interfaçage avec la sirène et gyrophare

2.2. Module d'accès

Ayant le rôle de contrôler l'accès à un endroit à protection renforcée, ce module vérifie le code fourni par le demandeur d'accès, et s'il est correct, commande électriquement l'ouverture d'une porte.

Un utilisateur possédant le code, peut changer ce dernier, s'il connait un chiffre supplémentaire qu'il doit taper suivi du nouveau code.

Ce module utilise le protocole RS485 pour communiquer avec le module central, ce qui lui permet de se placer à une longue distance (de valeur maximale de 300m) par rapport au module central. Ce protocole de communication se contente d'une seule paire de fils en cuivre, ce qui simplifie le câblage.

Entre autre, cette connexion permet, après trois essais d'accès refusés, de transmettre au module central un signal codé comprenant l'adresse du module d'accès concerné, pour l'informer de la situation.

Le module central peut, selon le cas, répondre convenablement à chaque situation, soit par un appel téléphonique au responsable, soit par le déclenchement de la sirène, soit les deux à la fois.

Ce module peut servir, aussi, à activer ou désactiver, à distance, l'ensemble du système de surveillance, ce qui évite à l'utilisateur un déplacement inutile jusqu'au module central.

2.3. Module de télécommunications

Suite à un changement d'état du système (déclenchement d'alarme, tentation d'intrusion frauduleuse, …), ce module reçoit une demande de la part du module central pour établir un contact téléphonique avec le ou les numéros des responsables désignés pour leur signaler ce changement sous forme d'un message vocal.

Ce module utilise une ligne téléphonique fixe, les numéros sont composés en DTMF. Un générateur des signaux DTMF est donc nécessaire pour pouvoir établir un appel téléphonique.

Pour répondre à ces besoins, nous avons choisi d'utiliser l'émetteur-récepteur

MT88890C (Integrated DTMF Transceiver with Adaptive Micro Interface) capable d'émettre et de recevoir les paires de tonalités DTMF et qui est muni d'une liaison avec microcontrôleur.

Le microcontrôleur envoie au MT88890C la commande de composer un numéro téléphonique puis il lui envoie ce numéro ;

Le MT88890C décroche la ligne téléphonique et compose le numéro, si la ligne n'est pas occupée, et il attend que l'appelé accepte l'appel :

- si l'appel est accepté, le MT88890C en informe le microcontrôleur pour générer le message vocal convenable.

- si l'appelé ne répond pas ou si sa ligne est occupée, le MT88890C en informe le microcontrôleur qui attend un certain temps avant de recommencer. 3 essais consécutifs avec un délai de temps court après le premier appel et plus long entre le second et le troisième appel, et ce avant de passer à d'autres numéros s'il y en a. Ayant, au moins, 16 états pour les

16 zones différentes de l'espace surveillé, le microcontrôleur du module central a à gérer au moins, 16 messages vocaux.

3. Critères de choix des composants

Les composants choisis pour réaliser ce projet sont les suivants :

- Deux microcontrôleur PIC 16F877A.
- Un écran à cristaux liquides (LCD).
- Un générateur récepteur des signaux DTMF
- claviers à 12 touches.
- Un amplificateur LM386

a) Le choix du microcontrôleur repose sur plusieurs critères :

Nombre d'entrées sorties : Le microcontrôleur doit pouvoir se connecter à :

- un LCD qui nécessite 6 entrées/sorties, et un clavier à 9 touches qui nécessite 7 entrées/sorties
- une interface USART nécessaire pour le Protocol RS485. (2sortie)
- Les détecteurs infrarouges (1 entrée et 1 sortie).
- La sirène, (1sortie).
- Deux moteurs (2 sorties)
- Bouton de fermeture (1 entrée)
- Es circuits de PIC (2 entrées et 2 sorties)

Ainsi, le total des entrées/sorties nécessaires s'élève donc à 26. D'où la nécessité d'utiliser un microcontrôleur PIC16F877A qui répond à nos critères. Mais il n'a que 36 entrées/sorties.

Un microcontrôleur suffisamment rapide pour pouvoir exécuter la tâche de lire un fichier de son de type « wav » en temps réel ou presque.

Compatibilité avec le langage C, ce qui facilite sa programmation.

4. Présentation du microcontrôleur utilisé

Un microcontrôleur est un composant programmable. Il regroupe dans un seul boîtier compact un processeur de calcul, de la mémoire vive (RAM), de la mémoire permanente (FLASH, EEPROM), des périphériques. Il en existe des dizaines de modèles.

Les exemples les plus courants sont : les 8051 d'Intel, les 68HC11 de Motorola...

Et les PIC de Micro chip.

a. Familles de PIC

La société Micro chip propose plusieurs familles de PIC :

- 10F, 12F, 16F : Architecture sur 8 bits, leur utilisation est réservée à des simples applications.
- 18 F : Architecture sur 8 bits, les PIC de cette famille sont assez semblables à ceux de la famille 16F, mais ils sont optimisés pour la programmation en langage C, grâce à un plus grand nombre d'instructions assembleur. Ainsi, ils tendent à remplacer, de plus en plus, les 16F.
- PIC 24 : Tout en restant dans le même type d'application que les 18F, les PIC24 offrent de bien meilleures performances grâce à leur architecture 16 bits, tout en conservant un grand nombre de périphériques.
- dsPIC : En combinant architecture 16 bits, cœur de calcul DSP et périphériques plus performants et plus variés, le dsPIC est le choix idéal pour des applications complexes de contrôle, de traitement du signal, ...
- PIC32 : Ce sont aujourd'hui les produits les plus évolués de la gamme Microchip. Leur utilisation est réservée à des applications complexes et gourmandes en ressources.

b. Architecture interne d'un pic

Le schéma de la figure 7 présente les principaux blocs fonctionnels présents à l'intérieur d'un PIC. Nous les décrivons succinctement comme suit :

• Mémoire flash : C'est une mémoire réinscriptible qui conserve ses données lorsque le PIC n'est pas alimenté. Elle est utilisée pour stocker le programme.

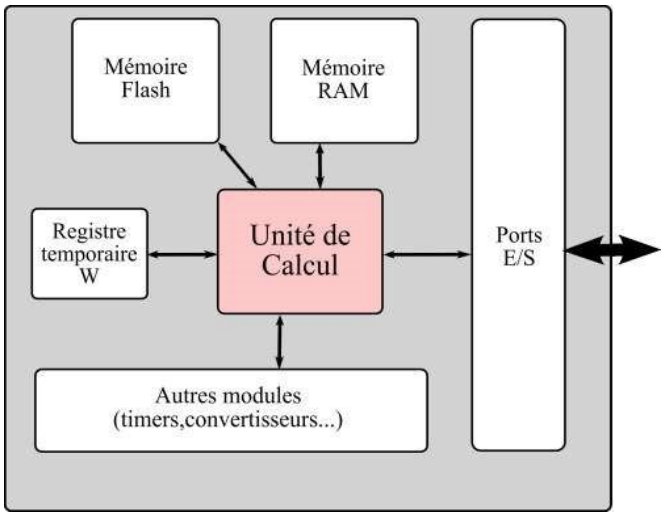


Figure 7 : Architecture interne d'un pic

• Mémoire RAM : C'est une mémoire volatile qui s'efface quand le PIC n'est plus alimenté. Les variables utilisées lors de l'exécution du programme sont stockées à cet endroit.

• Unité de Calcul : C'est le cœur du microcontrôleur. Ici se déroulent toutes les opérations arithmétiques et logiques.

• Registre temporaire W : C'est l'accumulateur du microcontrôleur, là où est stockée une des opérandes d'une opération de calcul.

• Ports E/S (Entrées/Sorties) : Ce sont les circuits électriques à travers lesquels le PIC communique avec son environnement externe.

• Modules annexes : tels que minuterie, comparateurs, convertisseurs analogiques/ numériques, et autres.

Référence **: [**4**]**

c. Le microcontrôleur PIC16F877A

• Caractéristiques

De la famille 16F, le microcontrôleur PIC16F877A, qui se présente dans un boîtier de 40 broches PDIP, est caractérisé par :

Mémoire du programme flash : 64 kB (65536 bytes).

Mémoire EEPROM : 1 kB (1024 bytes).

Mémoire RAM : 3,875 kB (3968 bytes).

Fréquence maximale de l'horloge : 40 MHz.

Ports parallèles : A, B, C, D et E.

Entrées/sorties : 36.

Oscillateur interne : 8 MHz / 32 MHz.

Entrées/sorties séries : EUSART (CSA*), SPI (CSS*), MI^{2}C (CSS*).

Port parallèle esclave : PSP.

CAN* 10 bits: 13 pins.

ICSP : programmation série en circuit (le microcontrôleur est programmé sans nécessité de le détacher du circuit.) Nombre d'Instructions : 75.

Boîtiers : 40 PIN DIP, 44 PIN PLCC, 44 PIN TQFP.

Compatibilité avec le langage C.

- Configuration des broches (voir figure 8)

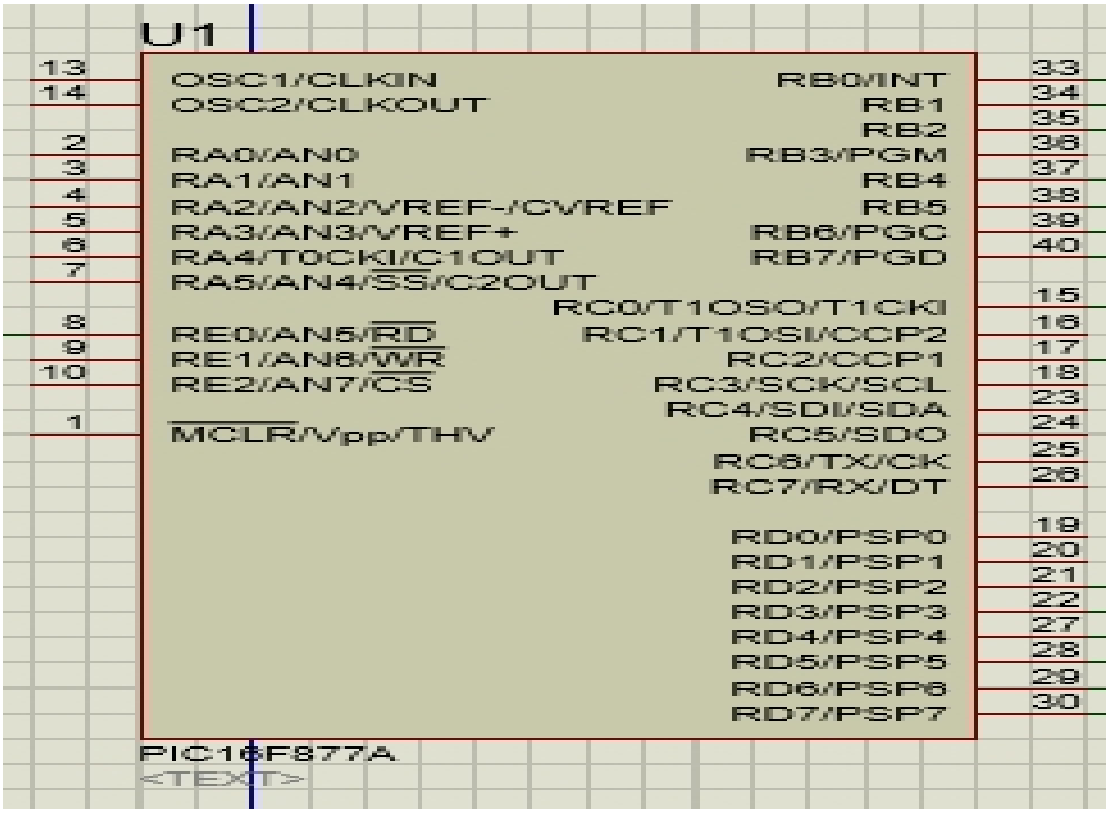


Figure 8 : configuration du pic 16F877A

.

- Schéma bloc

Le schéma bloc de la figure9 est constitué de quatre blocs principaux :

Bloc A : représente le cœur du microcontrôleur, il comporte l'unité arithmétique et logique, le pointeur, les mémoires ROM et RAM et les mémoires d'adresse, ainsi que le décodeur d'instructions et de contrôle, c'est dans ce bloc que se font les opérations arithmétiques et logiques.

Bloc B : les ports d'entrées/sorties du microcontrôleur référencés de A à E se trouvent dans ce bloc. Chacun de ces ports renferme huit pattes à l'exception des ports D et E qui en contiennent seulement quatre. Par défaut, ces ports sont utilisés comme étant des entrées/sorties pour le microcontrôleur. Pour les utiliser pour les interfaçages des USART, SPI, I2C…, une configuration interne du microcontrôleur est nécessaire.

Bloc C : renferme toutes les interfaces qu'on peut appliquer au microcontrôleur par une simple configuration du microcontrôleur. Parmi ces interfaces figurant dans le bloc C,

on a utilisé le MSSP pour connecter le MCP23S17 au microcontrôleur suivant le protocole SPI.

Bloc D : comprend les oscillateurs internes du microcontrôleur, le chien de garde (Watchdog), le Reset, la minuterie…

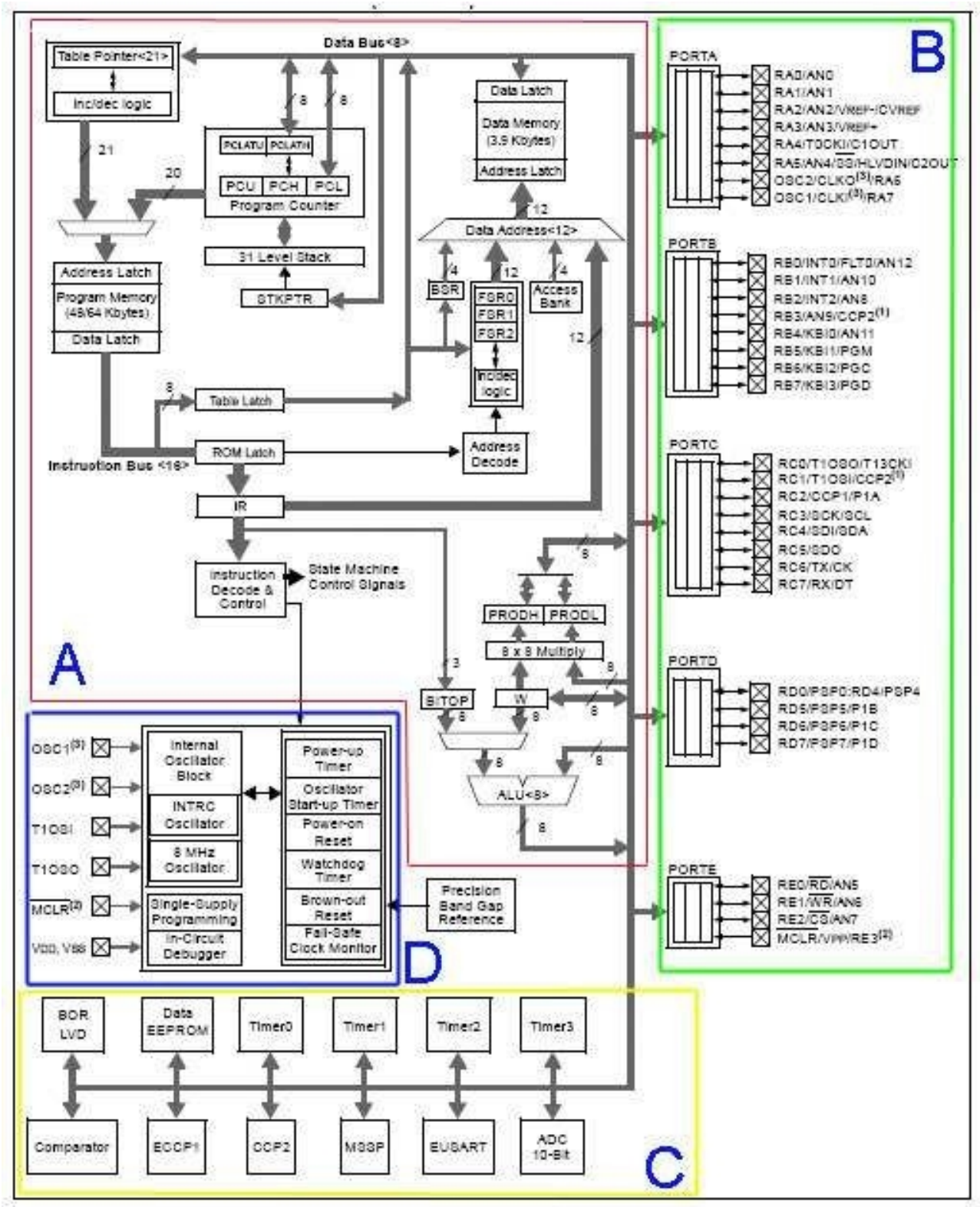


Figure 9 : Schéma bloc PIC16F877A

- Oscillateur externe

Le PIC16F877A comme tout autre microcontrôleur, comprend d'une horloge interne ou externe. L'horloge interne maximale de notre pic est de 8 MHz. Ce qui est relativement lent. Pour cela on a eu recours à utiliser un oscillateur externe.

L'oscillateur que nous avons réalisé (circuit à la figure 10) est de type HS (High speed) quartz ou résonateur céramique 20 MHz.

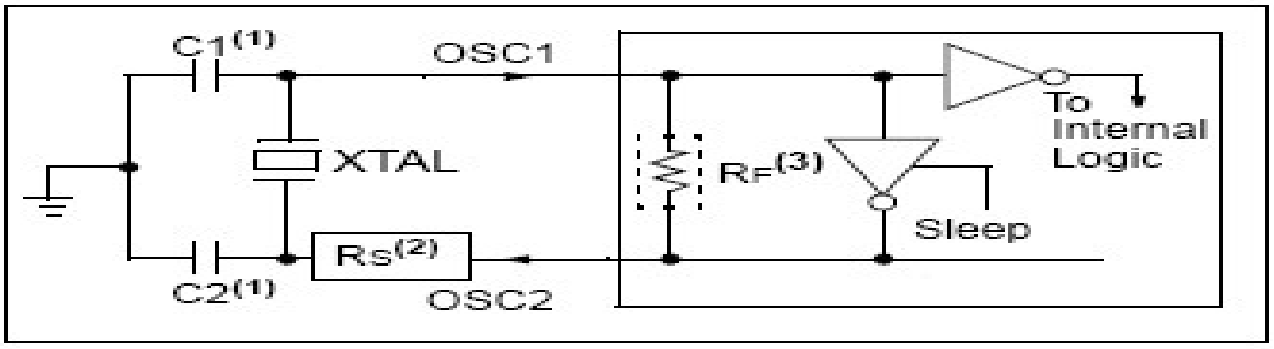


Figure 10 : oscillateur externe

- Initialisation matérielle du microcontrôleur :

La patte permet une initialisation externe du microcontrôleur en la reliant à zéro, comme le montre le circuit de la figure. Parfois il arrive que le système arrête de fonctionner normalement, on dira que le microcontrôleur est bloqué et ne répond pas correctement aux périphériques. Dans ce cas il faut initialiser le système en reliant la patte à zéro. Or en fonctionnement normal doit être relié à VDD, alors on place une résistance et une diode pour ne pas avoir un court-circuit en reliant à zéro.

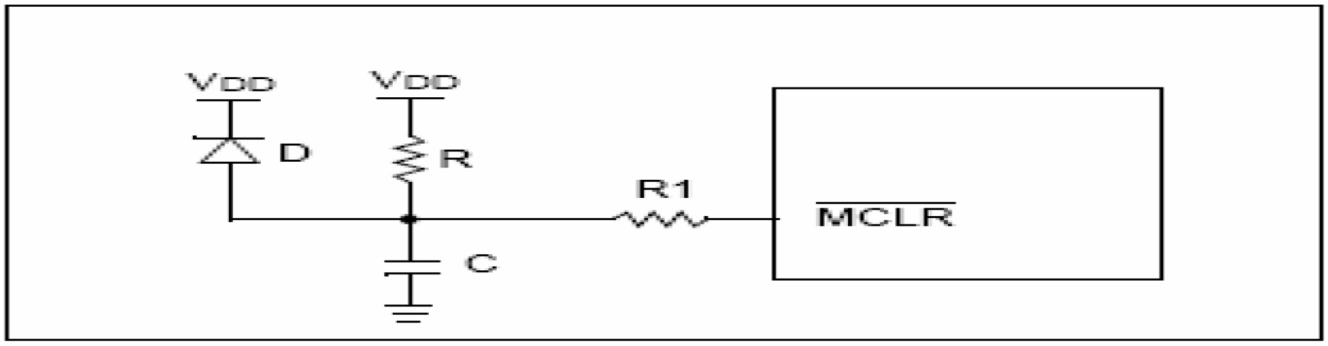


Figure 11 : Initialisation du microcontrôleur

- Initialisation des registres

Les périphériques du microcontrôleur disposent de registres spéciaux qui sont utilisés pour configurer les différents états de ces périphériques.

Les bits PCFG3 à PCFG0 sont les 4 bits de poids les plus faible du registre ADCON1 dont la configuration interne est illustrée dans la table 3.

ADCON1	-	-	VCFG1	VCFG0	PCFG3	PCFG2	PCFG1	PCFG0
	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0

Table 3 : Configuration du registre ADCON1

Nous avons choisi de convertir toutes les entrées de AN0 à AN12 en numérique, en se référant à la dernière ligne de la table 3, on trouve que pour que tous les ports analogiques soient numériques, il faut que les quatre bits LSB soient remis à « 1 », ce qui donne une valeur de 0x0F à écrire dans le registre ADCON1.

• Communication série synchrone : SPI

Une liaison SPI* est un bus de donnée série synchrone. Les circuits communiquent selon un schéma de maître-esclaves, où le maître s'occupe totalement de la communication. Plusieurs esclaves peuvent coexister sur un bus, la sélection du destinataire se fait par une ligne dédiée entre le maître et l'esclave appelée chip select.

Une transmission SPI typique est une communication simultanée entre un maître et un esclave, le maître génère l'horloge et sélectionne l'esclave avec qui il veut communiquer, l'esclave répond aux requêtes du maître.

À chaque coup d'horloge le maître et l'esclave s'échangent un bit. Après huit coups d'horloge le maître aurait transmis un octet à l'esclave et vice-versa. La vitesse de l'horloge est réglée selon des caractéristiques propres aux périphériques.

De même, le module SPI est nécessaire pour la connexion avec la mémoire statique (MMC). La carte MMC est connectée, à travers 4 fils, aux 4 broches suivantes de SPI :

- Le module USART (Universal Synchronous Asynchronous ReceiverTransmitter).

Le module USART est un périphérique Synchrone ou Asynchrone utilisable pour la transmission et la réception des données, en mode synchrone semi duplex, le module USART utilise le protocole RS485, où on trouve la configuration émettrice réceptrice, pour l'échange d'information.

L'émetteur et le récepteur doivent fonctionner à la même vitesse de transmission. La communication démarre toujours à l'initiative de l'émetteur. Le nombre d'émetteur/récepteurs peut atteindre 32 et où chacun aura une adresse unique,

La configuration des réseaux locaux est une communication multipoint. La vitesse de transmission de données est relativement grande (35 Mbit / s jusqu'à 10 m et 100 kbit / s à 1200 m). Il utilise un différentiel de ligne symétrique sur paires torsadées, et peut s'étendre sur des distances relativement grandes (jusqu'à 4000 pieds ou un peu plus de 1200 mètres).

- Initialisation du clavier

On a utilisé le port B comme port d'entrées pour le microcontrôleur, et sur lesquelles seront connectées les sorties du clavier.

Les instructions suivantes permettent de faire cette configuration et d'initialiser le clavier.

TRISB = 0xff, tous les pins du port B sont configurés en entrées.

Keypad_Init (&PORTB) : initialisation du clavier via le port B.

Référence **: [**5**]**

5. La carte mémoire

Une carte mémoire est l'unité de stockage la plus légère dont on peut se servir dans ce type de projet pour y stocker des données numériques sous forme de fichiers.

Il existe différents types de cartes :

- La *carte SD* ou Secure Digital. Au premier semestre 2010, elle est la plus répandue et offre une capacité maximale de 64 Go (les capacités théoriques maximales sont de 2 Go pour les SD de première génération, de 32 Go pour les versions SDHC, et de 2 To pour les SDXC)
- La *carte CF* ou Compact Flash. Autrefois la plus répandue, elle est progressivement abandonnée dans le cadre d'un usage grand public, mais reste cependant privilégiée par les professionnels. Elle offre en septembre 2008 une capacité maximale de 100 Go. La capacité théorique maximale était limitée à 137 Go jusqu'en 2010.
- La *carte MS* ou Memory Stick offre un stockage maximal de 16 Go fin 2008. Elle est surtout utilisée par les APN (Appareil Photo Numérique) de la marque Sony. Il y en a plusieurs variantes (Pro duo, micro...). Sony a annoncé au CES 2010 qu'il commençait à produire des cartes au format SD et micro SD.
- La *carte XD* ou XD-Picture Card offre un stockage maximal de 2 Go en septembre 2006. Elle est surtout utilisée par les APN des marques Olympus et Fujifilm
- La *carte SM* ou Smart Media Card (Olympus et Fuji), très mince, d'une capacité maximale de 128 Mo, est abandonnée
- La *carte MMC* ou MultiMedia Card
- La *carte PCMCIA*, d'un gabarit plus important, se connectant directement sur le port PCMCIA des ordinateurs portables.

Référence **: [**9**]**

6. Écran graphique

L'écran utilisé (figure 12) dans notre système est un écran graphique à cristaux liquides LCD de type KS0108. Il a les dimensions de 128x64 pixels.

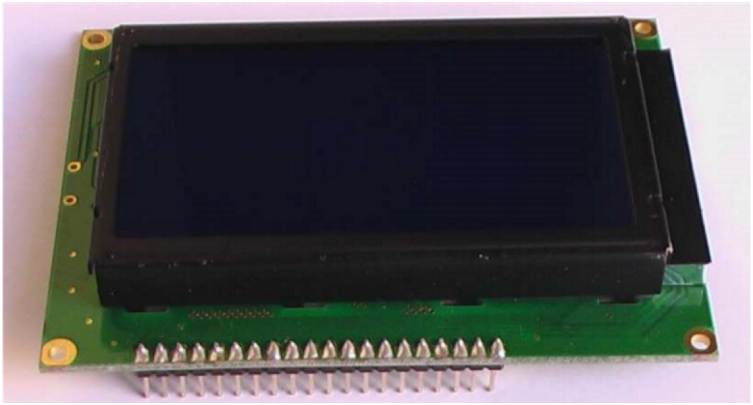


Figure12 : LCD

L'écran à cristaux liquides est le composant d'affichage le plus utilisé actuellement dans un grand nombre de dispositifs portables.

Il utilise la polarisation de la lumière grâce à un système de filtre polarisant dont on peut faire varier l'orientation en fonction du champ électrique.

Du point de vue optique, l'écran à cristaux liquides est un dispositif passif, dont on peut faire varier la transparence. Il n'émet pas de lumière et doit être éclairé ou rétroéclairé.

Référence **: [**10**]**

7. Clavier

Le clavier est de type matriciel quatre lignes quatre colonnes (4x3), ce qui nécessite huit broches de connexion. Il comporte 12 touches (figure 13) dont 10 pour les chiffres (de 0 à 9) ainsi que les deux symboles '*' et '#'.

Figure13 : clavier a 12 touches

Sa connexion avec le microcontrôleur peut se faire comme le montre la figure14

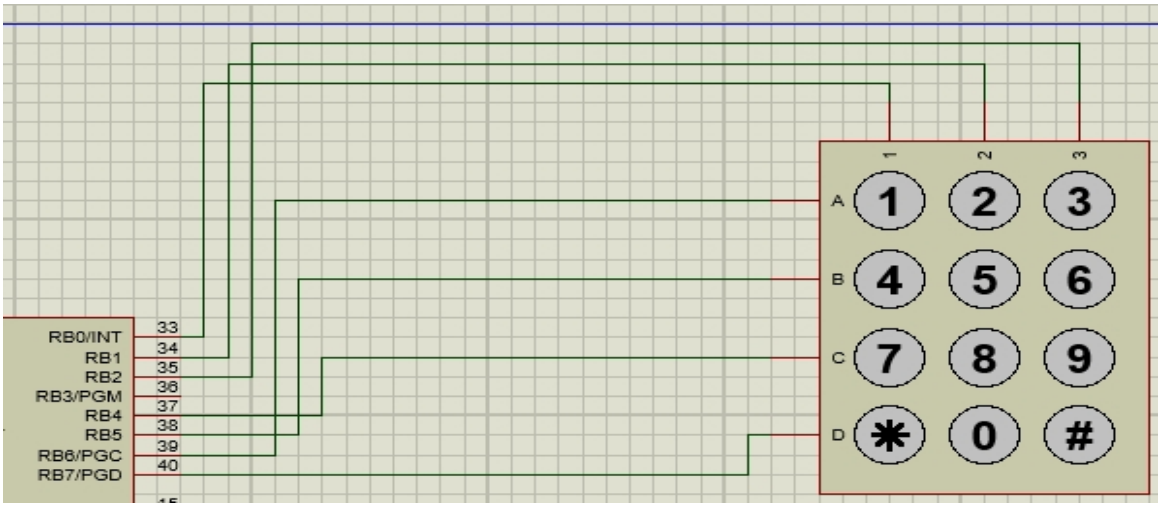


Figure14 : Brochage d'un clavier.

En appuyant sur une touche on relie une ligne à une colonne ce qui permet au microcontrôleur de détecter la touche appuyée.

Référence **: [**11**]**

8. L'amplificateur LM386

Le signal audio que produit le microcontrôleur est un signal digital dont on le transforme en signal analogique à l'aide d'un convertisseur numérique analogique du type R2R, ce signal est d'amplitude et de puissance faible.

Pour le transmettre sur la ligne téléphonique on utilise l'amplificateur LM386.

Caractéristiques :

Un minimum de parties externes

Une large gamme de tension

Un faible courant de drainage : 4 mA

Gain de tension de 20 à 200

Une entrée à référence terrestre

Une sortie à voltage auto centrée

Une faible distorsion

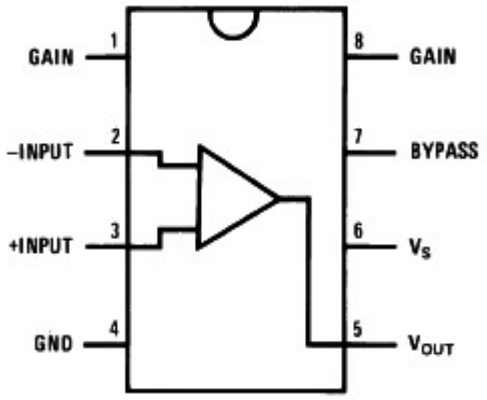


Figure15 : brochage de l'amplificateur LM386

12. Conclusion

Dans ce chapitre, nous avons passé en revue l'architecture matérielle de notre système de surveillance et contrôle d'accès ainsi que les principales caractéristiques des composants qui vont le constituer et pour lesquels, nous avons justifié leurs sélections. De même, nous avons présenté leurs configurations externes et internes et la manière avec laquelle, chacun d'eux, peut être connecté avec les autres.

Chapitre 05 : Réalisation du système de surveillance et contrôle d'accès.

Introduction

Après avoir fait l'étude du système de surveillance et contrôle d'accès, la réalisation d'un prototype se fait à 2 niveaux : matériel et logiciel.

1. Déroulement de la réalisation

1.1. Réalisation matérielle

La réalisation matérielle est faite en premier lieu. Chaque module du prototype est réalisé et &testé séparément.

Les montages sont d'abord construits sur des "breadboard" ou cartes de montage expérimental.

Après les avoir expérimentés et adoptés séparément, nous les avons regroupés et réalisés sur deux circuits imprimés. Ces derniers sont faits en se servant du logiciel "Isis" [11]

1.1.1. Circuit du système d'accès.

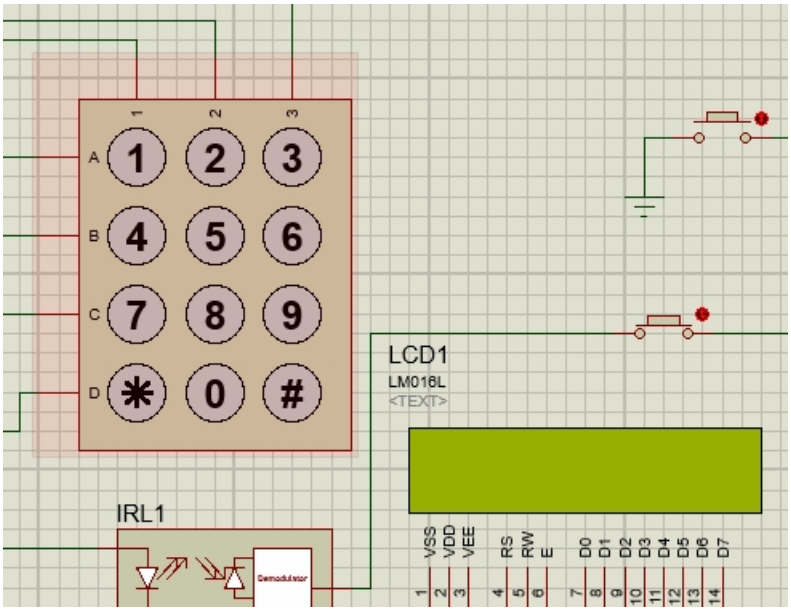


Figure 16 : système d'accès sans boitier

Le premier circuit électronique qui englobe le système d'accès se divise en 6 blocs principaux :

- L'alimentation à courant continu.

- Le microcontrôleur.
- L'écran à cristaux liquide.
- Le clavier.
- Les relais de commande
- Le module de programmation sur place

L'alimentation à courant continu est composée d'un transformateur 220V/12V 1000mA, suivi d'un pont à Diodes dont la sortie redressée est Filtrée à l'aide d'un condensateur de

470µF puis régulée à 5V par le régulateur de tension 7805. Estreservee

Le microcontrôleur est muni d'un oscillateur externe de fréquence 20MHz.

Toutes les entrées/sorties sont configurées comme numériques à l'aide du registre ADCON1.

Le PORT B, configuré comme entrée, est réservé au clavier.

Les pattes RD4, RD5, RD6, RD7 configurées comme sorties, sont réservées pour l'écran à cristaux liquides. Le pin RA1 est réservé pour le buzzer

Les pattes RC2, RB0 configurées comme sortie sont réservées pour l'infrarouge

La patte RC0 est réservée pour le Moteur 1 ,La patte RE0 pour désactiver le system d'alarme

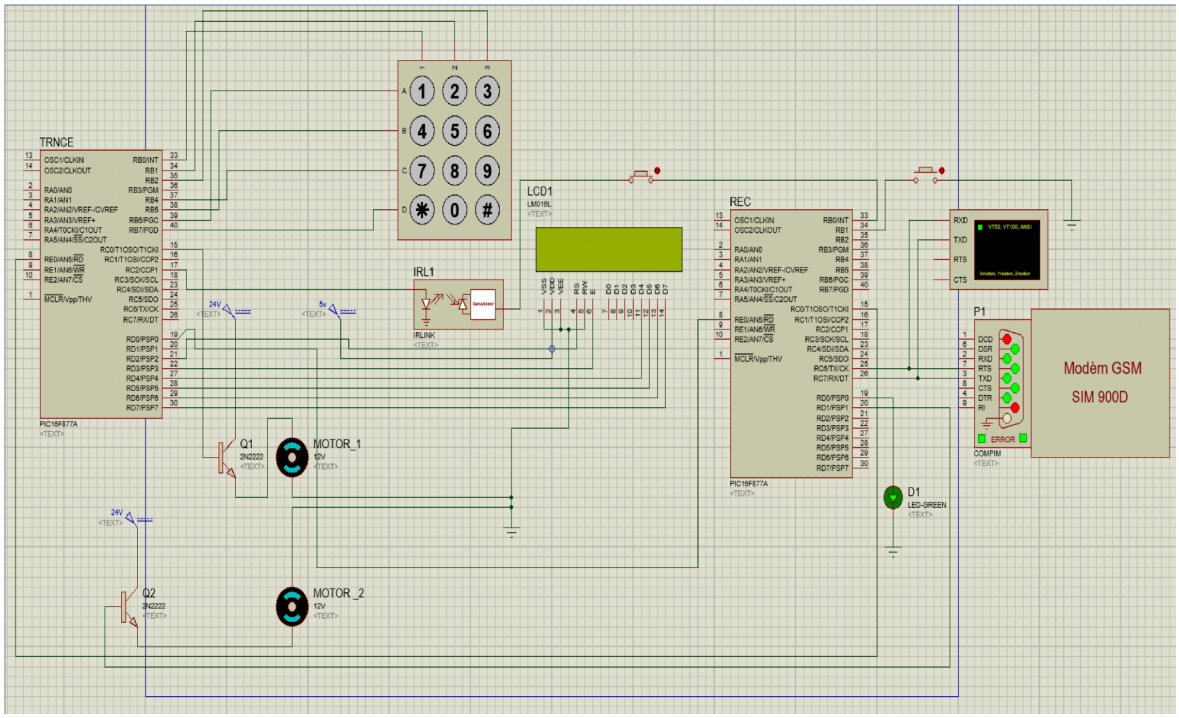


Figure 17 : Système de surveillance et contrôle d'accès final

1.1.2. Circuit du système d'alarme d'incendie et d'intrusion

Le second circuit électronique qui englobe le système d'alarme et d'intrusion se divise en 13 blocs principaux :

- L'alimentation à courant continu.
- Le microcontrôleur.
- L'écran à cristaux liquide.
- Le clavier.
- L'amplificateur.
- Les extensions de ports.
- Le convertisseur Numérique Analogique.
- Le module de connexion sur la ligne téléphonique.
- Le module de lecture d'un fichier audio.
- Le module de commande des sirènes, pompes et autres éléments de sécurité.
- Le module de connexion des capteurs.

- Le module de programmation sur place.

1.2. Réalisation logicielle

La partie logicielle consiste en un programme développé à l'aide du logiciel MikroC (compilateur C de MikroElectronica, conçu pour les microcontrôleurs PIC surtout les familles 16F et comprend une librairie très riche) sous Windows et qui sera exécuté par le microcontrôleur.

Le système comporte deux microcontrôleurs, l'un pour le système d'accès et l'autre pour la carte mère (Pour notre prototype, nous avons développé un seul boitier d'accès, mais le système complet doit comporter un nombre plus important de ces cartes d'accès pouvant atteindre 32). Nous avons développé un programme propre à chacun des deux microcontrôleurs.

1.2.1. Le programme du système d'accès permet à l'utilisateur de :

- Introduire le mot de passe pour avoir accès au lieu protégé.

- Changer le mot passe par les personnes possédant déjà le mot de passe.

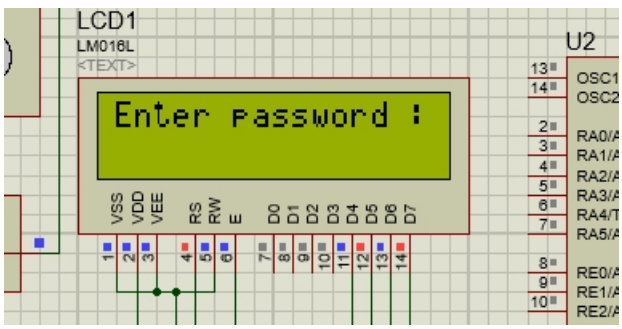
- Sauvegarder le mot de passe dans la mémoire EEPROM.

- Afficher sur l'écran les différents messages d'invitation et/ou de réponse..

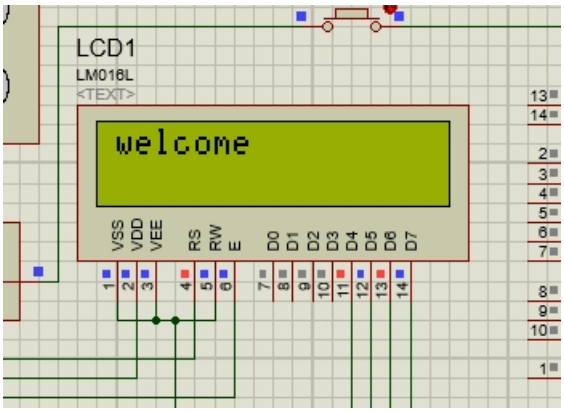
-Déclencher l'alarme après trois essais erronés de saisie de code.

1.2.2. Déroulement de processus

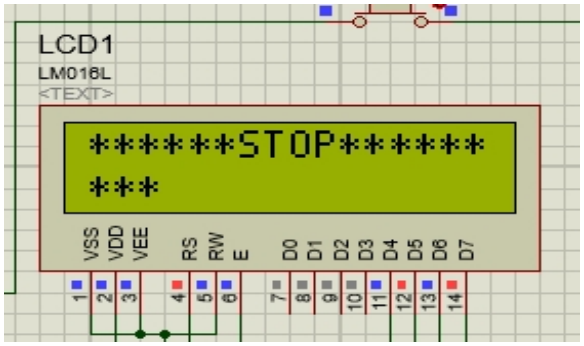
Une fois le module est sous tension l'écran affiche « initializing…. » En attendant que le module soit prêt.



Quand l'utilisateur entre le code, l'écran affiche, pour chaque touche appuyée, une étoile. Quand le code est complètement saisi.



Si le code saisi est correct, l'écran affiche « Welcome» et la porte s'ouvre, Si le code est refusé pour 3 fois, le système d'accès envoie un signal d'alarme au module central.



L'utilisateur peut changer le code d'accès, et cela de la manière suivante :

1.2.3. Le programme du module central permet à l'utilisateur de :

- Introduire le mot de passe pour avoir accès au système.
- Changer le mot passe par les personnes possédant déjà le mot de passe.
- Sauvegarder le mot de passe dans la mémoire EEPROM.
- Afficher sur l'écran les différents messages d'invitation et/ou de réponse.

- Activer ou désactiver le système de surveillance par les personnes autorisées.
- Changer le mode de l'alarme (silencieux, général, avec appel téléphonique, sans appel téléphonique).
- Introduire et modifier les numéros de téléphones des personnes responsables.

2. Organigramme du programme principal.

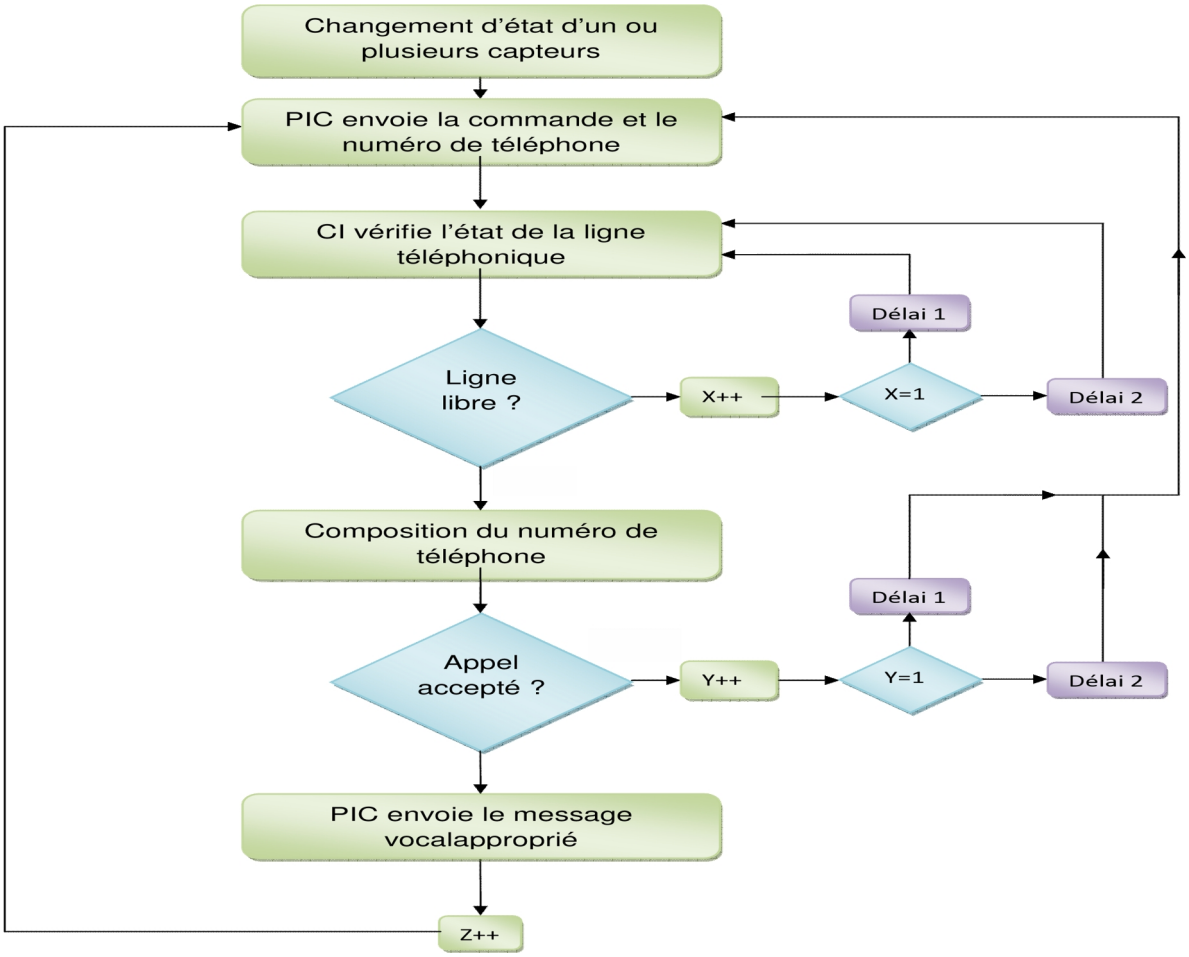


Figure 18 : Organigramme du système de surveillance et contrôle d'accès

3. Fonctionnement du système.

3.1 Configurations nécessaires

Pour faire fonctionner le système, plusieurs réglages, installations et configurations sont nécessaires. Parmi ceux-ci, nous citons :

- Installation des capteurs : Les différents capteurs doivent être mis en place dans les endroits désignés afin de couvrir l'ensemble des zones surveillées, puis ils doivent être connectés au module central.

Plusieurs capteurs peuvent être reliés en parallèle pour former une zone unique, chaque zone est reliée à l'une des 16 entrées du module central réservées aux capteurs et détecteurs d'intrusion.

Les capteurs et détecteurs doivent être calibrés et ajustés convenablement pour réduire au minimum la probabilité des fausses alarmes.

Les boitiers du système d'accès sont tous reliés sur le même câble car ils sont adressables et ils émettent les informations accompagnées du code du module d'accès émetteur

Avant leur activation, nous devons configurer chacun des modules d'accès, en introduisant le code d'accès valide correspondant. Ce code peut être modifié par la (ou les) personne(s) autorisée(s) selon la procédure déterminée dans le programme du module.

- Enregistrement et chargement des messages vocaux, relatifs à chaque zone, sur la carte mémoire. Ces messages doivent être numérisés au format '.wav' mono, à 8 bits/échantillon, et à 11025 Hz de fréquence d'échantillonnage.

- Connexion de la ligne téléphonique au module de télécommunications, et configuration du module central, en ce qui concerne :

La mémorisation des numéros de téléphones à appeler pour chaque type de situation, et éventuellement s'il y en plus qu'un numéro, l'ordre dans lequel ils doivent être appelés, et, le choix du mode de fonctionnement de l'alarme.

3.2 Fonctionnement typique en situation alarmante

Lorsque le système est configuré en mode "actif", à la réception d'un signal d'alarme transmis par, le module central localise le lieu du capteur d'où provient le signal et après un certain délai instauré pour vérifier qu'il ne s'agit pas d'un signalement instable et fugitif, le module central réagit en déclenchant l'alarme selon la procédure établie pour la zone concernée et selon le type d'alarme signalée (incendie, intrusion, tentative d'accès non autorisée,…).

8. Conclusion

Dans ce chapitre, nous avons décrit le processus de la réalisation matérielle et logicielle du prototype de notre application. Nous avons évoqué les principales difficultés que nous avons dues affronter lors de cette phase.

C O N C L U S I O N

Dès l'aube de l'humanité, l'homme cherche à se protéger et à protéger ses propriétés contre toute sorte de risques naturels ou humains.

Noun nous sommes intéressés à travers ce projet à développer un outil permettant d'aider l'entreprise pour laquelle nous travaillons à protéger ses propriétés contre les incendies, les voleurs et l'intrusion, et de maîtriser davantage l'accès à des endroits spécifiques.

La méthode utilisée repose sur le fait d'installer des capteurs à multi-paramètres (fumée, température, infrarouge, mouvement, bris de vitre …), et les relier à un module centralisé qui gère l'ensemble de ces détecteurs et déclenche, en fonction de la situation, une certaine signalisation d'alarme et agist convenablement à chaque événement détecté. La présence d'une ligne téléphonique permet au système d'appeler le responsable sur son téléphone et lui informer de la situation grâce à des messages vocaux numériques préconfigurés.

Conçu pour une utilisation commerciale, notre système permet de gérer jusqu'à 104 entrées analogiques, et 32 cartes d'accès utilisant le protocole RS485. Le système scrute les entrées analogiques, et les cartes d'accès et active une sirène en cas d'alarme général puis compose les numéros de téléphones des responsables pour les informer. L'alarme peut être silencieux c.à.d. sans activation de la sirène.

La réalisation matérielle et logicielle de ces maquettes suivie d'une phase de validation et de tests a donné des résultats satisfaisants

REFERENCES BIBLIOGRAPHIQUES

[1] Alagha ,Pujolle, Vivier. "Réseaux de Mobile et Réseaux sans fil". Eyrolles, 2001.

[2] Khaldoun Alagha & Co. "Réseaux sans fil et mobile". Lavoisier, 2004.

[3] http://fr.wikipedia.org/wiki/contrôle_d'accès , Articles : contrôle d'accès, Auteurs : http://fr.wikipedia.org/w/index.php?title=Contrôle_d'accès &action=history

[4] http://elec4you.blogspot.com/2009/05/alarme-telephonique-base-dupic16f84a.html, Auteur: « Hicham Bouzouf », titre: alarme téléphonique base du pic

[5] Titre : PIC18F2525/2620/4525/4620, Auteur : Microchip

[6] http://ww1.microchip.com/downloads/en/DeviceDoc/21952b.pdf , : MCP23017/MCP23S17, Auteur : Microchip

[7] http://www.lammertbies.nl/comm/info/RS-485.html#intr , Titre : RS485 serial information, Auteur : Lammert Bies

[8] www.chipcatalog.com/Zarlink/MT8889C.htm , titre : Integrated DTMF Transceiver with Adaptive Micro Interface, Auteur : Zarlink Semiconductor

[9] http://www.interfacebus.com/Secure_Digital_Card_Pinout.html , Titre : Secure Digital Card Pinout , Auteur : Leroy Davis

[10] http://www.datasheetarchive.com/KS0107-datasheet.html , Titre : écran graphique à cristaux liquide, Auteur : winstar.

[11] Help du MikroC; Keypad Library

http://fr.wikipedia.org/wiki/contrôle_d'accès , Articles : contrôle d'accès, Auteurs : http://fr.wikipedia.org/w/index.php?title=Contrôle_d'accès &action=history

Dédicace :

Je dédie ce modeste travail ;

A mes très chers parents ;

A mes frères ; A mes Sœurs ;

A mon amis gheribi Madjid ;

A ma chère Si Bachir Ikram ; A ma Belle Sœur Ikram

A Farid ;

Pour la gentillesse, la générosité, la joie de vivre, la patience et la volonté dont vous m'avez toujours entourée et que vous m'avez transmise.

Je vous remercie également du fond du cœur pour m'avoir encouragée et conseillé durant mes études.

A mon binôme Mr. Belghithare Merouan pour les beaux moments que je les passés avec-il et toute sa famille ;

Je n'oublierai pas d'adresser ma gratitude à tous mes amies et à tous mes camarades pour leur soutien et encouragements.

Merci !!