



HAL
open science

Conception et installation d'un système de surveillance dans une menuiserie avec émission d'alarme à distance

Nassif Matta

► **To cite this version:**

Nassif Matta. Conception et installation d'un système de surveillance dans une menuiserie avec émission d'alarme à distance. Electronique. 2010. dumas-00594324

HAL Id: dumas-00594324

<https://dumas.ccsd.cnrs.fr/dumas-00594324v1>

Submitted on 19 May 2011

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Conservatoire National des Arts et Métiers
Institut des Sciences Appliquées et Économiques
ISAE – Cnam Liban

Mémoire
présenté en vue d'obtenir
le diplôme d'ingénieur Cnam
en
Électronique
par
Nassif Matta

**Conception et installation d'un système de
surveillance dans une menuiserie avec émission
d'alarme à distance**

Soutenu le 10/11/2010 devant le jury composé de :

Président: M. Michel Terré

Membres: M. Imad Mougharbel
M. Haissam Hajjar
M. Chaouki Diab
M. Khaled Itani
M. Nazih Matta

Résumé

La conception et la réalisation d'un système de surveillance et contrôle d'accès font l'objet de ce mémoire. L'objectif de ce système est de surveiller le bâtiment où il est installé contre l'incendie et l'intrusion. En se servant des capteurs et des détecteurs. D'autre part il assure un contrôle d'accès pour les bureaux et les salles dont l'accès est limité pour certaines personnes.

Le système est capable de gérer un certain nombre d'appel téléphonique à distance pour informer les responsables de tous genres de détection, à travers des messages vocaux numérisés stockés sur une carte mémoire.

Le système comporte 16 entrées / sorties extensibles jusqu'à 112 au maximum, le nombre de numéros téléphoniques et des messages vocaux numériques est illimité, comme ils sont sauvegardés sur la carte mémoire SD de capacité maximale 2 GO. Le nombre maximal des palettes du contrôle d'accès est 32, qui peuvent être réparties autour du module central et sur une distance maximale de 300m.

Ce système est muni d'un écran graphique LCD, qui facilite la mise en marche et la configuration du système, et qui permet d'afficher l'état des différents périphériques.

Les palettes du système de contrôle d'accès sont, à leur tour, munies d'un écran LCD et d'un clavier pour faciliter l'usage.

Un prototype est réalisé dans ses deux aspects matériel et logiciel. Après validation, ce système a donné une bonne performance et un taux très réduit de fausses alarmes comparées à d'autres types d'alarmes présents sur le marché tout en gardant un coût de fabrication très abordable.

Mots-clés : Surveillance, Contrôle d'accès , Alarme d'incendie, Détection d'intrusion, Microcontrôleur PIC, Messagerie vocale, Extension de ports, RS485, DTMF, carte mémoire SD.

Summary

The conception and the implementation of a surveillance system and access control are the subject of this report. The objective of this system is to supervise the building where it is installed against the fire and the intrusion while using the sensors and detectors. On the other hand it assures an access control for the offices and the rooms whose access is limited for some people.

The system is capable to manage a certain number of telephonic call to inform the responsible persons of all kinds of detection, using saved digital audio files on the memory SD card.

The system includes 16 inputs/outputs expandable to 112 maximum, the number of telephonic number and audio messages is unlimited, and as they are saved on the SD memory card of maximum capacity 2 GO. The units of access control can reach 32 maximum and can be placed for a distance of 300m.

This system is provided with a graphic LCD, that facilitates the starting up and the configuration of the system and it displays the state of the peripherals.

The units of access control are provided with LCD screen and a keyboard to facilitate the use.

A prototype is achieved in both hardware and software aspects. After validation, this system gave a good performance and a very reduced rate of false alarms compared to other types of alarms presents on the market while keeping manufacturing costs very affordable.

Keywords: System of surveillance and access control, Fire alarm, intrusion alarm, access control, telephonic call, PIC micro controller, graphic liquid crystal display (GLCD), ports Extension, RS485, DTMF, SD memory card.

Remerciements

Tout d'abord, je tiens à remercier le président du jury M. le Professeur Michel Terré, Directeur de l'Eicnam, pour avoir bien voulu accepter de présider le jury.

Que les membres du jury,

- M. Imad Mougharbel, Professeur à la Faculté de Génie de l'Université Libanaise,*
- M. Haissam Hajjar, maître de conférences à l'Institut Universitaire de Technologie de l'Université Libanaise et,*
- M. Nazih Matta, Architecte et propriétaire de la menuiserie « multiwood »*

soient remerciés pour leur présence et pour le temps qu'ils ont bien voulu consacrer pour l'évaluation de ce travail.

J'exprime ma profonde gratitude à M. Chaouki Diab qui a suivi ce travail, pour son soutien et ses conseils.

Je remercie M. Elias El Hachem, le Directeur de l'ISAE – Cnam Liban, ainsi que le chef du département Génie électrique M. Khaled Itani et tout le corps enseignant pour leurs soutiens et leurs efforts au service des auditeurs du Cnam au Liban.

Sommaire

Introduction	1
<i>Chapitre 1 : Le Cahier des charges</i>	3
1. Introduction	3
2. Le système doit assurer les fonctionnalités suivantes :	3
2.1. Surveillance et protection contre les incendies	3
2.2. Contrôle d'accès aux locaux, afin d'assurer un certain degré de sécurité	3
3. Du point de vue technique, le système doit être:	4
4. Conclusion	4
<i>Chapitre 2 : Généralités sur les systèmes d'alarme d'incendie</i>	5
1. Les systèmes d'Alarme-incendie	5
1.1. Types de systèmes de sécurité incendie	5
1.1.1. Systèmes de type 4	5
1.1.2. Systèmes de type 3	5
1.1.3. Systèmes de type 2	6
1.1.4. Systèmes de type 1	6
1.2. Structure générale d'une alarme d'incendie	7
1.2.1. Le système de détection incendie (SDI) :	7
1.2.2. Le traitement de l'acquisition et des informations :	7
1.2.3. Le système de mise en sécurité incendie (SMSI) :	7
1.3. Les étapes de la sécurisation.	8
1.3.1. Détecter et signaler	8
1.3.2. Mettre en sécurité :	8
1.3.3. Intervenir	8
1.4. Matériels utilisés dans le SDI	8
1.4.1. Déclencheur manuel	9
1.4.2. Détecteur automatique	9
1.5. Matériels utilisés dans le S.M.S.I	14
1.5.1. Alarme sonore	14
1.5.2. Compartimentage	14
<i>Chapitre 3: Généralités sur les systèmes d'alarme d'intrusion et contrôle d'accès</i>	16
1. Alarme d'intrusion	16
1.1. Système de détection des intrusions.	16

1.2. Types d'alarme d'intrusion à l'intérieur	16
1.2.1. Détecteurs à infrarouge passif	17
1.2.2. Détecteurs à ultrasons	17
1.2.3. Détecteur à micro-ondes	18
1.2.4. Détecteur à faisceaux lumineux modulés	18
1.2.5. Détecteurs de bris de vitre	18
1.3. Types d'alarmes d'intrusion à l'extérieur (En plein air)	19
1.3.1. Vibreur	19
1.3.2. Détection passive du champ magnétique	19
1.3.3. Détection active du champ électromagnétique	20
1.3.4. Clôture à micro-ondes :	20
1.3.5. Les systèmes microphoniques	21
1.3.6. Détecteur à fibre optique	21
1.3.7. Champ électromagnétique de perturbation	21
2. Contrôle d'accès	22
2.1. L'accès physique	22
2.2. Fonctionnement d'un système de contrôle d'accès	23
2.3. Composants du système de contrôle d'accès	23
2.4. Types de lecteurs	23
Conclusion.....	24
Chapitre 4 : Généralités sur la téléphonie	25
Introduction.....	25
1. Principe de base de la téléphonie:	25
1.1. bande utile :	25
1.2. La signalisation	25
1.3. ligne d'abonné:	27
1.4. Échange de signaux entre postes demandeur et demandé :	27
1.4.1. Invitation à la numérotation:	27
1.4.2. État de la ligne :	29
1.4.3. Retour d'appel :	29
1.4.4. Tonalités :	31
Conclusion.....	31
Chapitre 5 : Conception du système de surveillance et contrôle d'accès	32

1. Structure du système	32
2. Principaux éléments constituant de chaque module	33
2.1. Module central :	33
2.2. Module d'accès	34
2.3. Module de télécommunications	35
3. Critères de choix des composants	37
4. Présentation du microcontrôleur utilisé	39
a. Familles de PIC	39
b. Architecture interne d'un pic	40
c. Le microcontrôleur PIC18F4620	41
5. Le circuit d'extension de ports : MCP23S17	48
6. Le circuit de connexion : Max485	49
Référence [7] :.....	50
7. Le circuit générateur/récepteur DTMF : MT8889C	51
8. La carte mémoire	52
8.1. Carte SD :	53
9. Écran graphique	54
10. Clavier	55
11. L'amplificateur LM386	56
12. Conclusion	57
Chapitre 6: Réalisation du système de surveillance et contrôle d'accès	58
1. Introduction	58
2. Déroulement de la réalisation	58
2.1. Réalisation matérielle	58
2.1.1. Circuit du système d'accès	58
2.1.2. Circuit du système d'alarme d'incendie et d'intrusion	61
2.2. Réalisation logicielle	65
2.2.1. Le programme du système d'accès permet à l'utilisateur de :	65
2.2.2. Déroulement de processus	66
2.2.3. Le programme du module central permet à l'utilisateur de :	67
2.2.4. De plus ce logiciel gère les fonctions suivantes :	67
3. Aperçu sur le programme du système	70
4. Fonctionnement du système	71

4.1. Configurations nécessaires	71
4.2. Fonctionnement typique en situation alarmante	72
5. Problèmes de réalisation	72
6. Validation et tests :	75
7. Installation	75
8. Conclusion	76
Chapitre 7 : Comparaison avec d'autres systèmes	78
1. Introduction	78
2. Coût matériel de notre système.	78
3. Qualités et défauts	79
4. Systèmes du marché.....	80
a. Selon le prix :	80
b. Selon la fonctionnalité :	81
5. Table comparative entre notre système et les systèmes présentés ci-dessus	83
6. Conclusion.....	84
Conclusion	85
Bibliographie	87
Annexe	88

Liste des figures

Figure 1: Centrale d'alarme d'incendie et ses périphériques.....	8
Figure 2: Courbe du développement du feu.....	10
Figure 3 : Réaction des détecteurs en fonction de l'évolution du feu.....	10
Figure 4 : Équipement pour alarme sonore.....	14
Figure 5 : Ventouses pour fermeture de portes.....	15
Figure 6 : les étapes de transformation de l'énergie acoustique en énergie électrique et vice-versa.....	26
Figure 7 : Signalisation terminale échangée entre abonné et autocommutateur	27
Figure 8 : transmission du numéro 32 par trains d'impulsions.....	28
Figure 9 : schéma bloc du système.....	32
Figure 10 : Architecture interne d'un pic.....	40
Figure 11 : Configuration du PIC4620.....	42
Figure 12: Schéma bloc du PIC4620.....	43
Figure 13 : oscillateur externe (avec $C_1=C_2=22\text{pF}$)	44
Figure 14 : Initialisation du microcontrôleur ($R=10\text{ k}\Omega$).....	44
Figure 15 : Topologie du réseau RS485.....	47
Figure 16 : Brochage du MCP23S17.....	48
Figure 17 : Schéma bloc du MCP23S17.....	49
Figure 18 : Schéma bloc du CI MAX 485.....	49
Figure 19 : Configuration des broches du CI MT8889.....	51
Figure 20 : Broches de la carte mémoire SD.....	53
Figure 21 : GLCD.....	54
Figure 22: Clavier à 16 touches.....	55
Figure 23 : Brochage d'un clavier.....	56
Figure 24 : brochage de l'amplificateur LM386	56
Figure 25 : Système d'accès sans boîtier.....	59
Figure 26 : Circuit imprimé du système d'accès.....	60
Figure 27 : Schéma électronique du système d'accès.....	60
Figure 28 : Système de surveillance et contrôle d'accès final.....	61
Figure 29 : Circuit imprimé du système de surveillance.....	65
Figure 30 : PICKIT2.....	68
Figure 31 : Brochage du PICKIT2.....	68
Figure 32 : Organigramme du système de surveillance et contrôle d'accès.....	69
Figure 33 : Organigramme du système.....	70
Figure 34 : plan de menuiserie - étage 2.....	76
Figure 35: Sensaphone Model FGD 6700 Express II.....	81
Figure 36: VAP-416 M ALARM PANEL.....	82
Figure 37: ELMO NET432	83

Liste des tables

Table 1 : Détermination de la surface de détection pour un détecteur linéaire de fumée	13
Table 2 : Détermination de la surface de détection pour un détecteur de flamme.....	14
Table 3 : Fréquences utilisées pour les différentes touches du clavier d'un poste téléphonique.	28
Table 4 : Tableau de récapitulation des signaux téléphoniques.....	30
Table 5 : Différentes tonalités pour différents messages téléphoniques.....	31
Table 6 :ADCON1.....	45
Table 7: Configuration du registre ADCON1.	45
Table 8 : Rôle de chacune des broches du MT8889.	52
Table 9 : brochage de la carte SD.....	54
Table 10: Brochage du GLCD.....	55
Table 11 : Repartition de détecteurs	76
Table 12: Coût estimé des composants du module central.....	78
Table 13 : Coût estimé des composants de la carte de contrôle d'accès.	79
Table 14: Comparaison entre les systèmes	83

Liste des abréviations

APN :	Appareil Photo Numérique.
BAAS :	Bloc Autonome d'Alarme Sonore
CCITT :	Comité Consultatif International Téléphonique et Télégraphe
CMSI :	Centralisateur de Mise en Sécurité Incendie
DAI :	Détecteur Automatique d'Incendie
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'Incendie
SSI :	Système de Sécurité Incendie
SMSI :	Système de Mise en Sécurité Incendie
CCTV:	Closed Circuit Television
PIR:	Passive Infra Red Sensor
GLCD:	Graphic Liquid Crystal Display.
DIP:	Dual In-line Package.
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.
TQFP:	Thin Quad Flat Pack.
SPI:	Serial Peripheral Interface.
I2C:	Inter Integrated Circuit

PSP:	Parallel Slave Port
CAN:	Convertisseur Analogique Numérique.
CF:	Compact Flash
MS:	Memory Stick
XD:	Extreme Digital
SM:	Smart Media
PCMIA:	Personal Computer Manufacturer Interface Adaptor
ADCON:	Analog Digital Converter.
CI :	Circuit Intégré.
MCLR:	Master Clear.

Avant propos

La conception et l'implantation d'un système de surveillance et de contrôle d'accès fait l'objet de ce mémoire. L'objectif de ce système est de surveiller l'endroit concerné de toute sorte d'incendie et d'intrusion.

"Multiwood", une grande menuiserie, dont les locaux sont situés à Mkalles (Mont-Liban Nord) où ils s'étendent sur 3 étages d'une superficie totale de 1200 m², a pressenti le besoin de s'équiper d'un outil de surveillance capable de détecter et régir rapidement à tout risque. En plus d'un magasin de stockage, ces locaux abritent un atelier bien équipé et un bureau d'étude et de conception (design) situé au second étage.

Ce besoin est devenu très pressant suite à plusieurs accidents d'incendie, heureusement d'une faible gravité, survenus dans les locaux de l'entreprise l'année passée.

Etant le responsable de l'entretien électrique de cette entreprise, ses propriétaires m'ont confié la mission d'étudier et de mettre en œuvre un système de détection d'incendies en premier lieu, de surveillance et de contrôle d'accès en second lieu. D'où est née l'idée d'un système intégrant ces 2 fonctions.

Lors de sa conception, j'ai tenu à rendre ce système déployable et adaptable à n'importe quel type d'espace à surveiller.

Pour simplifier son usage par les utilisateurs, le système sera complètement autonome et indépendant de tout autre matériel (ordinateur ou autre). Son fonctionnement demande une simple alimentation électrique du secteur (220V-50Hz), une ligne téléphonique, et plusieurs capteurs de types différents selon les types de risques à prendre en charge.

Afin d'avoir un outil évolutif, notre système est conçu de manière le rendant extensible à d'autres éventuelles fonctionnalités.

Introduction

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 lointains.

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'entraînement, 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 se résume par : "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 d'alarme contre incendie et 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.

Ce mémoire est formé de cinq chapitres, à travers lesquels nous décrivons le travail effectué pour la conception et la réalisation de notre système:

Dans le premier chapitre, nous présentons les spécifications du cahier des charges sur lequel nous nous sommes basés dans la réalisation de ce projet.

Dans le second chapitre, nous donnons une vue sommaire sur les différents

systemes de surveillance, d'alarme, d'incendie et de contrôle d'accès existants actuellement sur le marché.

Dans le chapitre 3, nous abordons les différents aspects de la communication via une ligne téléphonique fixe et dont nous aurons besoin dans l'élaboration de notre système pour la transmission des messages vocaux.

Le chapitre 4 décrit la phase de conception du système. On y décrit les principales composantes constituant ce système tout en justifiant leurs choix.

Le chapitre 5 présente les étapes de réalisation et d'implantation du système. On y découvre les schémas électroniques détaillés des différentes parties du système, ses modes de fonctionnement, ainsi que la mise en place de la partie logicielle.

Avant de conclure, nous présentons, dans le dernier chapitre, une comparaison entre notre système et les systèmes disponibles sur le marché en termes de qualité et de prix.

Chapitre 1 : Le Cahier des charges

1. Introduction

La menuiserie «Multiwood» cherche à mettre en place un système autonome de détection de chaleur afin de se protéger contre les incendies. Ce système devra être équipé d'un moyen de communication permettant de transmettre une signalisation d'alarme à ceux qui doivent intervenir en cas d'incendie.

De plus, le bureau d'études de cette menuiserie doit être protégé par un système d'alarme muni par des détecteurs de mouvement, d'ouverture de portes, ...etc.

Ce même bureau devrait être équipé d'un système de contrôle d'accès pour la porte principale.

Le but de ce projet consiste à étudier un système électronique capable d'assurer cette mission en respectant le cahier des charges suivant:

2. Le système doit assurer les fonctionnalités suivantes :

2.1. Surveillance et protection contre les incendies

- Détection de la chaleur dans les endroits susceptibles d'être des foyers d'incendie.
- Dans le cas d'une détection de chaleur suspecte, le système doit effectuer les opérations suivantes :
 - Coupure du courant électrique.
 - Activation d'une sirène.
 - Mise en action de l'extincteur dans la ou les zone(s) concernée(s).
 - Émission d'un signal d'alarme vocale par voie téléphonique pour avertir les sapeurs pompiers ainsi que les propriétaires.

2.2. Contrôle d'accès aux locaux, afin d'assurer un certain degré de sécurité

- Porte à digicodes pour l'accès aux bureaux

- Détecteur d'intrusion dans l'atelier (capteur magnétique, infrarouge, ...).
- Dans le cas d'une détection d'intrusion, le système doit émettre un signal d'alarme vocale par voie téléphonique pour avertir, à la fois, la police et les propriétaires.

3. Du point de vue technique, le système doit être:

- Autonome, indépendant d'aucun autre système-hôte
- Facilement configurable à travers un écran GLCD offrant à la fois la simplicité de la configuration et la visualisation des informations que le système doit fournir à l'administrateur.
- Fiable, avec une probabilité de fausse alarme infiniment petite.
- Alimenté par le courant du secteur avec une alimentation de secours non interruptible.
- d'un coût relativement abordable par rapport aux systèmes disponibles dans ce domaine.

4. Conclusion

Pour répondre au cahier des charges détaillé ci-dessus, le système de surveillance et contrôle d'accès serait divisé principalement en trois modules, le module central, le module de télécommunication et le module de contrôle d'accès que nous détaillerons à partir du chapitre 4

Avant d'entrer dans ces détails, nous présentons dans les deux chapitres suivants les résultats d'un travail bibliographique que nous avons effectué dans le cadre de ce projet et qui nous a éclairés sur plusieurs aspects que nous avons dû aborder dans notre démarche.

Chapitre 2 : Généralités sur les systèmes d'alarme d'incendie.

Les alarmes d'incendies sont des dispositifs permettant de détecter la présence de feu. Il existe plusieurs types d'alarme d'incendie, allant du moins au plus développé.

Dans ce chapitre on parlera des types des alarmes incendies, de leur structure générale, et des détecteurs utilisés par ces systèmes.

1. Les systèmes d'Alarme-incendie

Une alarme-incendie 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.

En France la réglementation a fait adapter les SSI (Systèmes de Sécurité Incendie) selon les établissements dans lesquels ils sont installés avec la création de catégories. La catégorie de SSI détermine le type d'alarme installé allant du type 4 à 1 (plus on se rapproche de 1, plus le dispositif est développé).

1.1. Types de systèmes de sécurité incendie

1.1.1. Systèmes de type 4

Pour les ERP (Etablissement Recevant du Public) les moins importants, les systèmes de sécurité incendie se composent soit :

- d'une centrale à alimentation autonome (sur pile) intégrant un diffuseur sonore (DS) et un déclencheur manuel (DM),
- ou d'une centrale pouvant gérer une à deux lignes de DM et une ligne de DS.

1.1.2. Systèmes de type 3

Ces systèmes se composent d'un ou plusieurs BAAS (Blocs Autonomes d'Alarme Sonore) reliés entre eux, et qui peuvent gérer chacun une boucle de déclencheurs

manuels. Les BAAS* comportent chacun un diffuseur sonore et une batterie pour pouvoir fonctionner en cas de coupure de l'alimentation "secteur". Ils sont reliés entre eux de façon à ce que lorsqu'un BAAS passe en position d'alarme, tous les autres se déclenchent également.

1.1.3. Systèmes de type 2

Les systèmes d'alarme type 2 se différencient dans deux catégories:

Catégorie 2a

Les systèmes de cette catégorie se composent d'un CMSI (Centralisateur de Mise en Sécurité Incendie) relié à plusieurs boucles de déclencheurs manuels, et à des DAS (Dispositifs Actionnés de Sécurité) et des DS*.

Catégorie 2b

Les systèmes de cette catégorie sont équipés avec un BAAS type Pr: c'est un BAAS qui intègre un panneau de commande qui gère jusqu'à huit boucles de déclencheurs manuels, et parfois un contact auxiliaire pour un DAS*. Un BAAS Pr ne peut être raccordé qu'à des BAAS et non des DS*.

1.1.4. Systèmes de type 1

Ils se composent d'un SDI (Système de Détection d'Incendie) qui peut être relié à un CMSI*. C'est le seul type d'équipement d'alarme qui peut comporter des détecteurs automatiques d'incendie (ou DAI). Le SDI peut se distinguer par deux installations différentes: le SDI conventionnel et le SDI adressable.

SDI conventionnel:

Les détecteurs d'incendie et les déclencheurs manuels sont reliés par des boucles à la centrale (Équipement de Contrôle et de Signalisation ou ECS), donc en cas d'alarme, la signalisation et le traitement correspondant s'effectuent par zone. Ce type d'installation est adapté à des ERP* de petite ou moyenne taille et moins onéreux qu'un SDI adressable.

SDI adressable:

Les détecteurs d'incendie et les déclencheurs manuels sont reliés à l'ECS* sur une seule boucle par un système numérique que l'on appelle "bus". En cas d'alarme feu, l'élément de détection peut-être localisé individuellement et avec précision sur

un écran. Un SDI adressable est beaucoup plus onéreux qu'un SDI conventionnel, mais beaucoup plus adapté à un ERP* de grande taille.

1.2. Structure générale d'une alarme d'incendie

On distingue trois parties essentielles (figure 1) :

1.2.1. Le système de détection incendie (SDI) :

Il permet de localiser le sinistre. Il est composé de détecteurs automatiques (DA) ou de déclencheurs manuels (DM).

1.2.2. Le traitement de l'acquisition et des informations :

Permet de traiter les informations reçues par les détecteurs, pour commander les systèmes nécessaires pour lutter contre l'incendie, et sauver la vie des personnes sur scène.

1.2.3. Le système de mise en sécurité incendie (SMSI) :

Permet d'assurer les fonctions d'évacuation, de compartimentage, de désenfumage grâce aux portes coupe-feu, aux trappes de désenfumage déjà en place et aux diffuseurs sonores (DS) ou aux blocs autonomes d'alarmes sonores (BAAS).

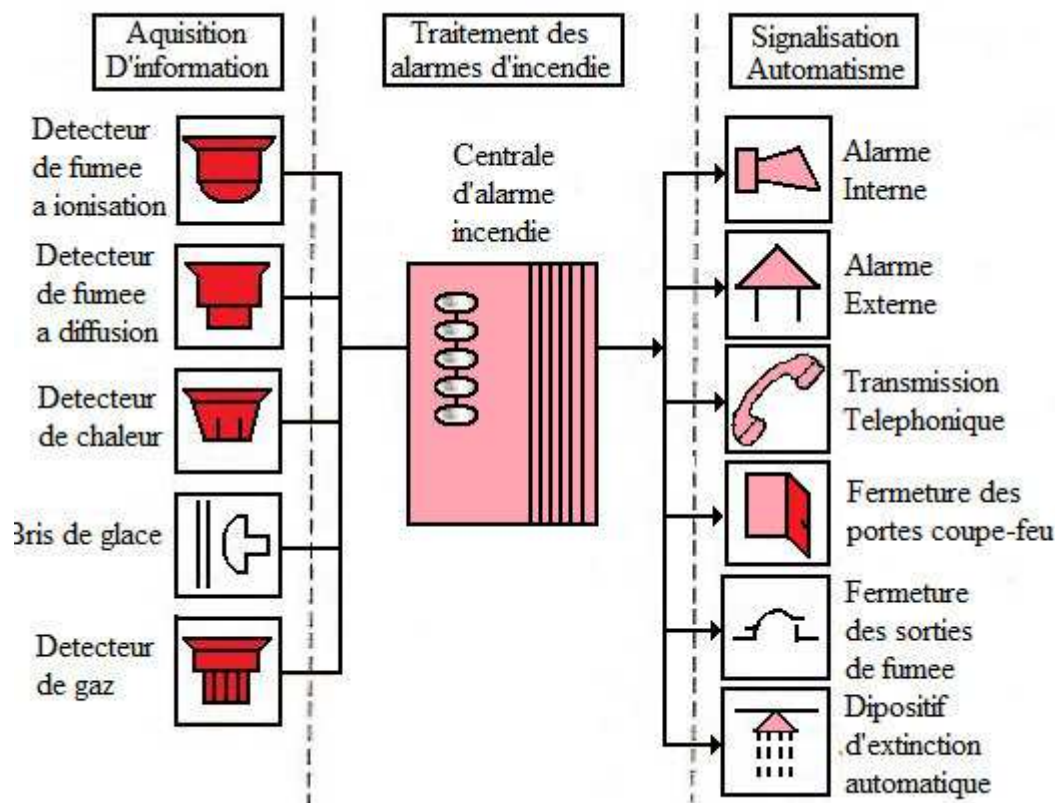


Figure 1:Centrale d'alarme d'incendie et ses périphériques.

1.3. Les étapes de la sécurisation.

1.3.1.Détecter et signaler

Détecter le feu au plus tôt et signaler la localisation au personnel de surveillance pour agir convenablement selon des procédures bien déterminées afin d'assurer la sécurité des personnes et de limiter les dégâts dans le bâtiment surveillé.

1.3.2.Mettre en sécurité :

Plusieurs actions doivent être menées pour sécuriser les personnes et les biens. Par ordre chronologique, elles sont les suivantes:

- **Évacuer**

Informé le public à l'aide de signaux visuels et sonores et libérer les issues de secours.

- **- Compartimenter**

Limité la propagation du feu et des fumées afin de faciliter l'évacuation du public et réduire les dégâts dans le bâtiment et ce, en actionnant la fermeture des portes coupe-feu grâce à des ventouses électromagnétiques.

- **Désenfumer**

Protéger les personnes des fumées et faciliter l'évacuation en commandant l'ouverture d'un exutoire de fumée par le biais d'un tableau de mise en sécurité.

1.3.3.Intervenir

Faciliter l'intervention des secours en :

- Signalant la localisation du feu et l'état des organes de mise en sécurité
- Mettant à disposition les organes de commande permettant de limiter la propagation du feu et des fumées et de couper le courant électrique dans la zone sinistrée et ceci pour éviter, d'une part, les courts circuits et les risques d'explosion et pour protéger, d'autre part, les services de secours.

1.4. Matériels utilisés dans le SDI

1.4.1. Déclencheur manuel

Le déclencheur manuel est équipé d'une vitre (bris de glace) ou d'une membrane déformable.

Ils sont placés :

- à 1.30m du sol ;
- à chaque étage et proches des escaliers ;
- au rez-de-chaussée à proximité des sorties ;
- près des issues de secours

Les déclencheurs sont câblés sur une même boucle avec un câble type C2 de 8/10 mm; ils sont de couleur :

- Rouge (commande du signal d'évacuation)
- Verte (Commande de gestion des issues)
- Jaune (commande de compartimentage)
- Blanche (commande de désenfumage).

On distingue deux types de déclencheurs manuels :

- Le déclencheur manuel à membrane simple dont le déclenchement se fait par pression sur la membrane. La déformation nette de celle-ci indique que le produit a été actionné.
- Le déclencheur manuel avec indicateur mécanique de l'état ce qui permet une visualisation claire et rapide de son état (actionné ou en veille).

Le déclencheur manuel adressable est équipé d'un indicateur mécanique et d'un voyant lumineux. L'indicateur mécanique renseigne sur l'état du déclencheur (actionné ou en veille) et le voyant indique si la centrale a pris en compte ou non l'information.

1.4.2. Détecteur automatique

Les détecteurs automatiques permettent de détecter un éventuel départ du feu grâce à leur sensibilité à la fumée, à la flamme ou à la température. La figure 2 schématise les étapes de développement du feu.

Il existe différents types de détecteurs automatiques selon le risque à surveiller. Ainsi, ils seront choisis en fonction du type d'incendie visé ou probable:

- les feux ouverts qui engendrent flammes et chaleur.
- les feux couvrants qui engendrent fumées et gaz combustible.

La figure 3 décrit la sensibilité de certains types de détecteurs à la température et à la fumée; chaque détecteur a sa propre marge de détection et agit soit à la

température soit à la fumée;

Parmi ces détecteurs, nous citons:

- Le détecteur optique de fumée
- Les détecteurs de chaleur
- Le détecteur linéaire de fumée
- Le détecteur de flamme

Dans ce qui suit, nous décrivons brièvement, le principe de fonctionnement et les principales caractéristiques de chacun d'eux.

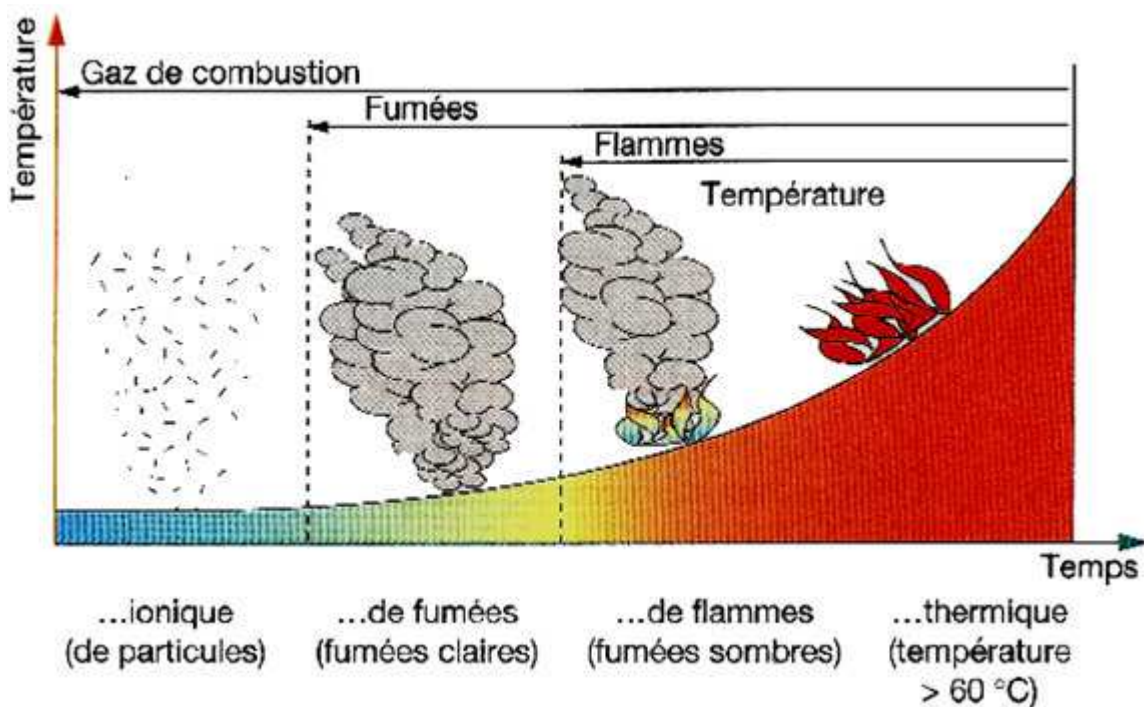


Figure 2: Courbe du développement du feu

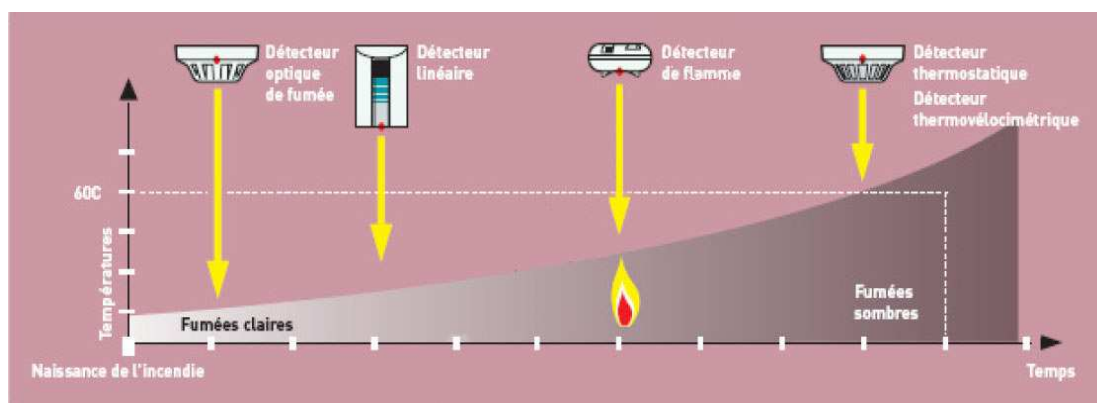


Figure 3 : Réaction des détecteurs en fonction de l'évolution du feu.

1.4.2.1. Le détecteur optique de fumée

Il est sensible à tous les types de fumées et d'aérosols car il utilise la technique « détection de particules ». Par contre il n'est pas sensible au feu sans fumée (feu d'alcool). Son avantage est qu'il détecte rapidement le début d'un incendie avant la formation de flamme.

Il est utilisé dans les endroits où il n'y a pas de fumée d'exploitation en fonctionnement normal.

Utilisation

Ce type de détecteurs assure une protection sur une surface ne dépassant pas les 60 m² et d'une hauteur maximale de 12 m.

Sa température d'utilisation peut varier entre -20 °C et +60 °C.

Son bon fonctionnement est entravé par des éléments perturbants tels que :

- le développement intense et soudain de poussières.
- un dispositif de cuisson
- la vapeur d'eau
- la condensation et le givre.

Dans les circulations, il faut installer un détecteur à 5 m maximum de chaque extrémité puis respecter un intervalle de 10 m maximum entre détecteurs.

1.4.2.2. Les détecteurs de chaleur

1.4.2.2.1. Type Thermo vélocimétrique

Ce type de détecteur réagit lorsque la température atteint un certain seuil, en prenant en compte la vitesse d'élévation de la température.

Il transmet l'alarme dès que la température dépasse le seuil fixé.

Utilisation

Généralement, ce type de détecteur assure une protection sur une surface maximale de 30 m², d'une hauteur maximale de 4 m, et à une distance standard maximale de 4.4m.

Sa température d'utilisation peut varier entre -20 °C et +90 °C, son bon fonctionnement est entravé par des éléments perturbants tels que :

- une température ambiante supérieure à 90 °C
- une chambre frigorifique
- des locaux en partie ouverts

1.4.2.2.2. Type Thermostatique

Il est activé dès que la température dépasse un seuil fixé sans qu'il tienne en compte la vitesse de variation de cette température.

Utilisation

Généralement, ce type de détecteur assure une protection sur une surface maximale de 18 m², d'une hauteur maximale de 4 m, et à une distance standard maximale de 3.6 m.

Sa température d'utilisation peut varier entre -20°C et +70°C

Son bon fonctionnement est entravé par des éléments perturbants tels qu'une température ambiante supérieure à 70°C

Conclusion

Les valeurs généralement admises sont : 60 m² pour la surface, et 5 m de distance entre un détecteur et l'endroit le plus éloigné de la zone à surveiller pour le détecteur de fumée. Pour le détecteur thermo-vélocimétrique, les valeurs sont de 30 m² de surface 4 m de distance

1.4.2.3. Le détecteur linéaire de fumée

Il est sensible aux fumées blanches ou noires qui traversent le faisceau laser émis par le boîtier et renvoyé par le réflecteur.

Son intérêt réside dans la couverture de grandes distances évitant ainsi l'emploi de plusieurs détecteurs de fumée ponctuels et offrant une solution simple d'installation dans le cas de grandes hauteurs de plafond ou de points de fixation inaccessibles et non souhaités (hall, entrepôt ...) pour des détecteurs ponctuels.

Comme pour le détecteur optique de fumée, il doit être utilisé dans les locaux où il n'y a pas de fumée en mode de fonctionnement normal.

Utilisation

Il assure une surveillance sur des longues distances allant de 30 à 100 m sur une largeur de 10 m et pour une hauteur de local de 5 à 12 m (voir table no. 1).

Sa température d'utilisation peut varier entre -10°C et +55°C.

Son bon fonctionnement est entravé par des éléments perturbants tels que :

- vapeur d'eau
- poussières

- aérosols
- obstacle de toute nature

A noter que la coupure complète du faisceau laser est signalée comme un défaut.

Il faut prévoir son implantation sur un support stable et non dilatable pour éviter les variations du faisceau en position.

Il ne faut avoir aucun obstacle entre le détecteur et son réflecteur.

Hauteur du local (m)	Hauteur de détecteur sous plafond (m)	Largeur de surveillance par rapport à l'axe du faisceau (m)
$H \leq 5$	$0.3 \leq H \leq 0.5$	4
$5 < H \leq 12$	$0.5 < H \leq 2$	5

Table 1 : Détermination de la surface de détection pour un détecteur linéaire de fumée

1.4.2.4. Le détecteur de flamme

Il est sensible au rayonnement infrarouge émis par les flammes d'un foyer ainsi qu'à la présence du CO_2 résultant.

Il détecte un foyer à une distance allant jusqu'à 17 m, pour les moins performants d'entre eux. Son angle de vision est de $\pm 45^\circ$ par rapport à son axe optique, soit un cône de 90° . Pour un détecteur monté sur plafond entre 3,5 et 7 m de haut, la surface couverte est de 150 m^2 . Elle varie en fonction de l'inclinaison et de la hauteur sous-plafond du détecteur. Le détecteur doit être installé à un emplacement permettant une liaison visuelle de la zone à surveiller aussi courte que possible et exempt d'obstacle.

Il faut prévoir son implantation sur un support stable. La zone à surveiller doit toujours être à la vue directe du détecteur et sans obstacles.

La surface minimale surveillée dépend de la hauteur d'implantation de détecteur (F) et de son inclinaison (V) – voir Table no. 2.

Utilisation

Il est utilisé lorsque le paramètre à détecter est la présence de flammes émises par la combustion de solides, liquides ou gaz carbonés (bois, fuel, butane...).

Il est très adapté à la détection de feux ouverts et peut remplacer les détecteurs de fumée lorsque les conditions d'environnement empêchent

l'utilisation de ces derniers.

Ce détecteur est sensible aux phénomènes perturbants suivants :

- rayonnement direct du soleil, éclairage artificiel intense ou vacillant
- réflexion de lumière sur des plans d'eau, vitrages, parties mobiles ou machine ...
- vibration du point de fixation du détecteur
- tout mouvement produisant une modulation de la lumière captée par le détecteur.

F = hauteur de fixation du détecteur (m)	Surface maximale surveillée au sol en m ²			
	V= angle d'inclinaison par rapport à la verticale			
	0° < V < 15°	15° < V ≤ 30°	30° < V ≤ 45°	45° < V ≤ 60°
F ≤ 1,5	10	15	25	30
1,5 < F ≤ 3,5	40	60	60	60
3,5 < F ≤ 7	150	120	100	70
7 < F ≤ 10	300	250	250	250
10 < F ≤ 20	550	440	350	250

Table 2 : Détermination de la surface de détection pour un détecteur de flamme.

1.5. Matériels utilisés dans le S.M.S.I

1.5.1. Alarme sonore

L'évacuation des personnes peut être soit provoquée par la diffusion d'un signal sonore (figure 4) soit organisée, dans certains cas, par le personnel de l'établissement.

L'alarme sonore doit être audible en tout point du bâtiment :

- Par sirène ou diffuseur sonore qui peuvent être autonomes ou non.

Par un bloc autonome d'alarme sonore (BAAS)



Figure 4 : Équipement pour alarme sonore.

1.5.2. Compartimentage

Le dispositif actionné de sécurité (DAS) par fermeture automatique des portes coupe-

feu utilise des ventouses électromagnétiques qui réagissent à une coupure ou à l'établissement d'une tension électrique (figure 5).



Figure 5 : Ventouses pour fermeture de portes.

Conclusion

Nous avons décrit les différents types d'alarme d'incendie, leur structure générale et les différents périphériques de ces systèmes, leur utilisation les avantages et les inconvénients.

Dans ce qui suit, nous allons voir les systèmes d'alarme d'intrusion et les systèmes de contrôle d'accès.

Référence [1] :

Chapitre 3: Généralités sur les systèmes d'alarme d'intrusion et contrôle d'accès.

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.

Cette technologie est considérée comme démodée par de nombreux

professionnels d'alarme, et n'est plus fréquemment utilisée.

1.2.3. Détecteur à micro-ondes

De même principe que le précédent, ce détecteur émet des micro-ondes et les détecte après qu'elles soient réfléchies tout en mesurant leur intensité. L'émetteur et le récepteur sont généralement combinés dans un seul boîtier pour les applications intérieures, et sont dans des boîtiers séparés pour les applications extérieures.

Ainsi, ce détecteur fonctionne comme un dispositif actif volumétrique qui répond à:

- Un changement de fréquence Doppler quart de travail.
- Un décalage de phase de fréquence.
- Un mouvement entraînant une réduction de l'énergie reçue.

1.2.4. Détecteur à faisceaux lumineux modulés.

Le système à faisceau photoélectrique détecte la présence d'un intrus par l'émission visible ou infra rouge des faisceaux lumineux dans une zone. Pour améliorer la surface de détection, les faisceaux sont souvent employés en deux ou plus.

Toutefois, si un intrus est conscient de la présence de la technologie, il peut l'éviter.

Le système de détection peut se montrer efficace, s'il est installé dans des piles de trois ou plus, lorsque les émetteurs /récepteurs sont répartis en nombre suffisant pour pouvoir créer une barrière de manière qu'il serait inévitable de s'en passer par tout intrus.

Ce type de systèmes est valable aussi bien pour des applications internes qu'externes.

Pour empêcher une attaque discrète en utilisant une source secondaire de lumière afin de maintenir le détecteur dans un état de fermeture, la plupart des systèmes utilisent une source de lumière modulée.

1.2.5. Détecteurs de bris de vitre

Le détecteur de bris de verre peut être utilisé pour la protection du périmètre de construction interne. Quand le verre se casse il génère du son dans une large bande de fréquences (couvrant les fréquences sonores audibles et ultrasonores inaudibles, allant de quelques Hz à plus de 20 kHz). Les détecteurs de bris de verre acoustiques sont montés à proximité des vitres et ils écoutent

les fréquences sonores causées par le bris du verre.

Un autre type de détecteurs de bris de vitres peut être utilisé : Ce sont les détecteurs sismiques qui diffèrent des détecteurs de type précédent par le fait qu'ils sont installés sur la vitre. Quand le verre se casse il produit un choc de fréquences bien déterminées qui se propagent à travers le verre et souvent par l'intermédiaire du cadre de fenêtre, les murs et le plafond.

En règle générale, les fréquences les plus intenses sont générés entre 3 et 5 kHz, selon le type de verre et de la présence d'un intercalaire en plastique. Les détecteurs sismiques de bris de verre sentent ces fréquences aux chocs et à leur tour génèrent un état d'alarme.

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 abordable.

Inconvénients: Doit être monté clôture. 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:

- la variation d'amplitude du champ
- 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.

Inconvénients: - coût élevé

- peu fiable (taux élevé de fausses alarmes, incapable de distinguer un chat d'un homme, trop dépendant des conditions météorologiques, ...etc.).

1.3.4. Clôture à micro-ondes :

Le fonctionnement d'une barrière à micro-ondes est très simple. Ce type de dispositif produit un faisceau électromagnétique utilisant des ondes à hautes fréquences qui passent de l'émetteur au récepteur, ce qui crée un mur invisible, mais sensible à l'intrusion. Lorsque le récepteur détecte un changement dans le faisceau reçu (dû à une éventuelle intrusion), le système démarre une analyse détaillée de la situation et peut déclencher, le cas échéant, un signal d'alarme.

Avantages: faible coût, facile à installer, barrière périmétrique invisible (limites inconnues à l'intrus).

Inconvénients: très sensible aux conditions météorologiques (pluie, neige et brouillard, par exemple, entraîneraient une rupture du fonctionnement des capteurs), nécessité d'un espace complètement dégagé (pas d'obstacle de toute sorte (arbre, ...)).

1.3.5. Les systèmes microphoniques

Les systèmes microphoniques sont variés, mais ont, en commun, la capacité de détecter le bruit causé par l'intrusion. Habituellement, les capteurs sont attachés aux clôtures rigides, mais pour certaines versions plus sophistiquées, ils peuvent également être enfouis sous terre.

Selon le type choisi, le système peut être sensible à différents niveaux de bruit ou de vibrations.

Avantages: très bon marché, configuration simple, facile à installer.

Inconvénients: certains systèmes sont peu fiables (taux élevé de fausses alarmes dû à une forte sensibilité des capteurs utilisés).

1.3.6. 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.

1.3.7. Champ électromagnétique de perturbation

Ce système utilise un principe de champ électromagnétique de perturbation basée sur deux câbles coaxiaux non blindée enterrés à environ 10-15 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 retapés.

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'identification 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.

2.4. 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 donné 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.

Référence **[2]** :

Chapitre 4 : Généralités sur la téléphonie

Introduction

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 6).

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.

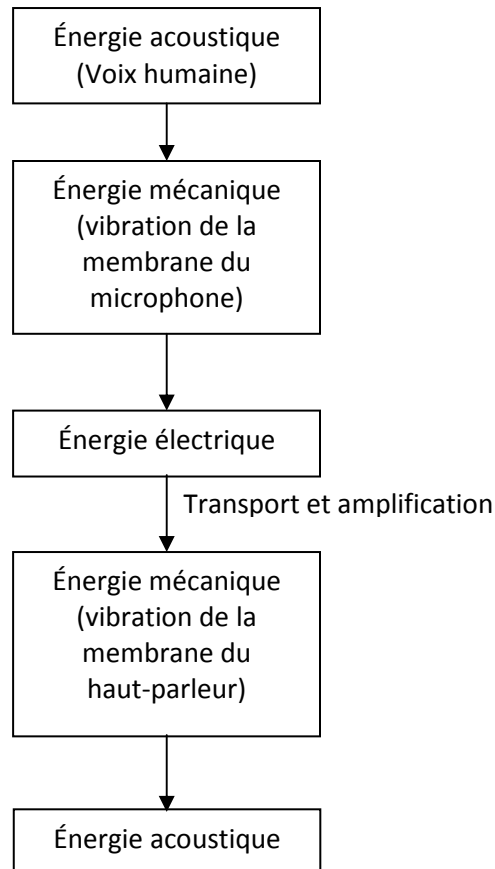


Figure 6 : les étapes de transformation de l'énergie acoustique en énergie électrique et vice-versa.

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.

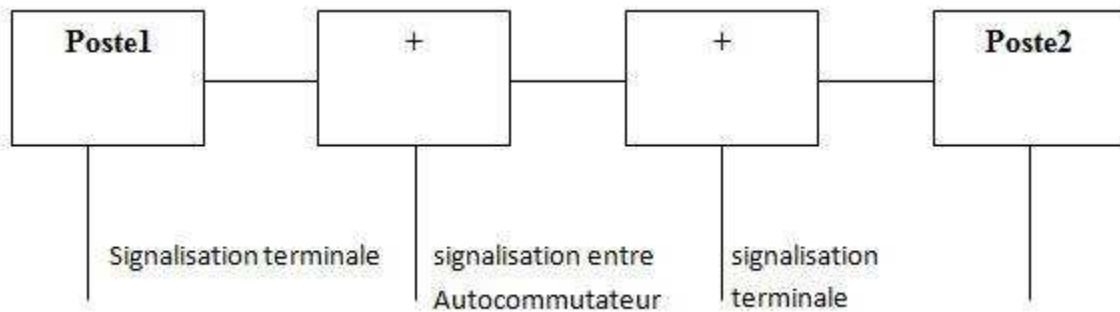


Figure 7 : Signalisation terminale échangée entre abonné et autocommutateur

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 numérotter 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.

Courant de ligne i

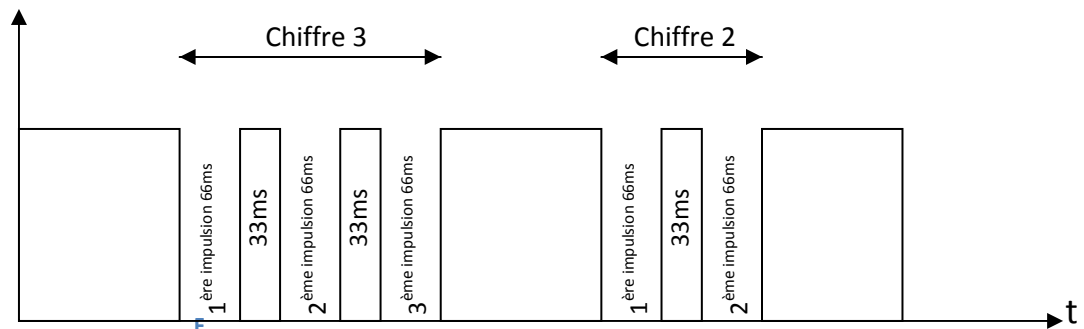


Figure 8 : transmission du numéro 32 par trains d'impulsions.

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 3).

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	1633
697	1	2	3	A
770	4	5	6	B
852	7	8	9	C
941	*	0	#	D

Table 3 : 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 la 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 600Ω , avec une puissance largement inférieure au milliwatt, et dans la bande 300-3400Hz.

La Table 4 récapitule l'ensemble des échanges de signaux qui peuvent avoir lieu pendant l'établissement d'une connexion téléphonique entre deux abonnés.

Signification du signal	Détection signal demandeur commutateur demandé	Nature du signal	
		Signal électrique	Tonalité
Appel	→	Ligne bouclée	425 Hz
Invitation à numéroté	←	Rupture de boucle	
Numérotation	→		
Occupation du demandé (demandeur ?)	←		425Hz (0.25s /0.25s)
Sonnerie	→	25Hz	
Retour d'appel	←		425Hz (1.2s/4.65s)
Réponse du demandé	←	Ligne bouclée	
Raccrochage du demandé	←	Rupture de boucle	
Raccrochage du demandeur	→	Rupture de boucle	425Hz

Table 4 : Tableau de récapitulation des signaux téléphoniques.

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 5.:

	Fréquence	Cadence	Niveau
Tonalité d'invitation à numéroté	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 5 : Différentes tonalités pour différents messages téléphoniques.

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]

Chapitre 5 : Conception du système de surveillance et contrôle d'accès

1. Structure du système

Le système de surveillance et contrôle d'accès est constitué de plusieurs modules (figure 9), 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. Tous les capteurs sont connectés à ce module.

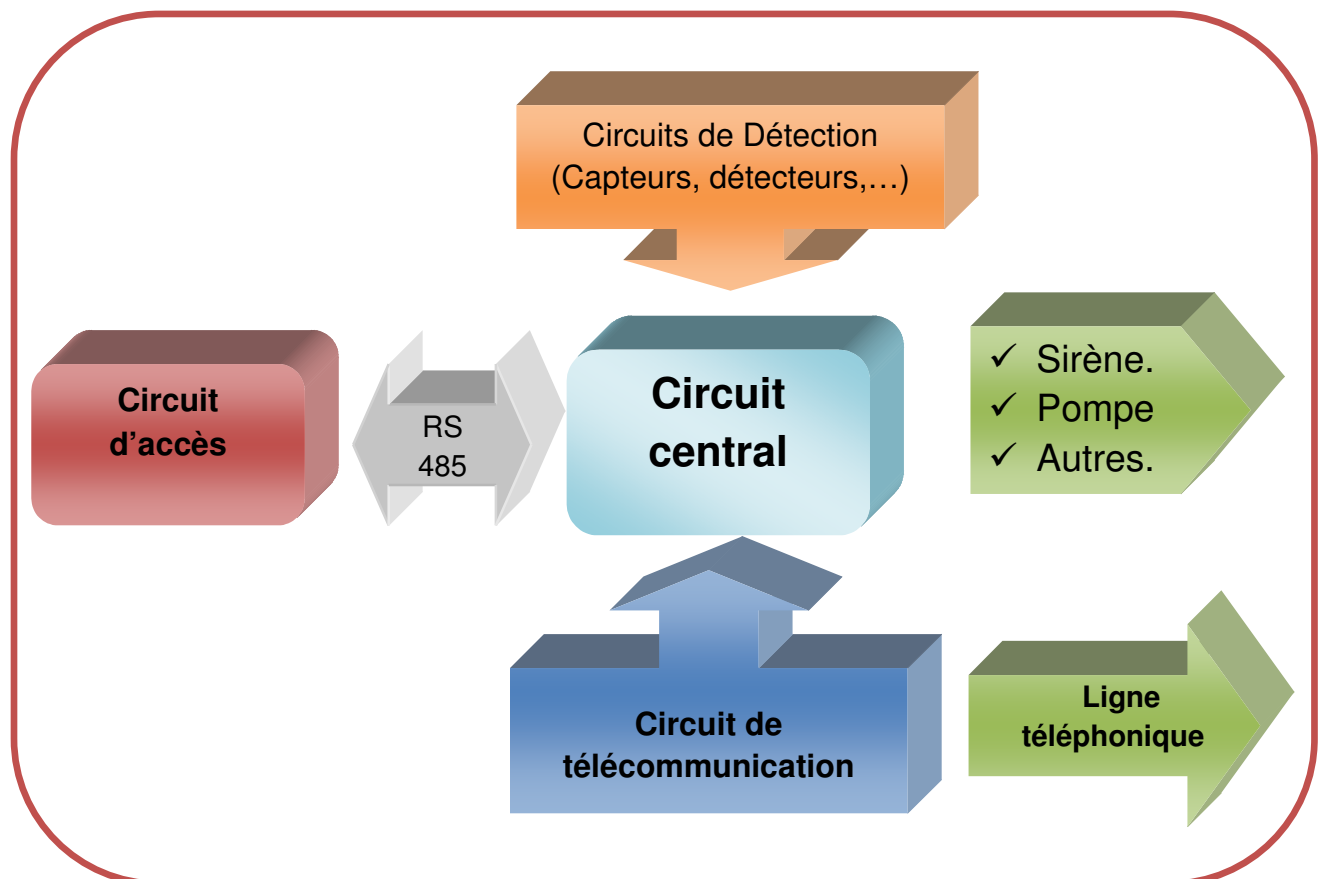


Figure 9 : schéma bloc du système.

- 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 constituant 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 des 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,
- et 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 18F4620,
- un clavier 4x4,
- un écran graphique à cristaux liquide 128x64,
- un circuit pour le protocole RS 485,
- un circuit d'interface série avec l'écran LCD, et
- un circuit d'interfaçage avec la sirène.

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 connaît 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.

Pour assurer son rôle, ce module doit comporter:

- un microcontrôleur, qui gère la saisie et les commandes
- un écran pour l'affichage des messages, et
- un clavier pour saisir le code..,

En résumé, ce module comporte :

- un microcontrôleur PIC 18f4620
- un clavier
- un écran LCD à 2 lignes pour l'affichage, et
- un module pour le protocole RS485.

2.3. Module de télécommunications

Suite à un changement d'état du système (déclenchement d'alarme, tentative 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 ce 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.

Donc, une carte mémoire multimédia pour le stockage des fichiers qui contiennent les messages vocaux est nécessaire pour stocker ces messages. Cette mémoire sera, bien sûr, contrôlée par le microcontrôleur.

Nous avons choisi d'enregistrer les messages vocaux en format "wav" à 8 kHz, sur une carte mémoire SD (Secure Digital), connectée au microcontrôleur à travers le Protocol SPI (Serial Protocol interface).

Pour convertir les contenus binaires des fichiers ",wav" en une forme sonore analogique afin de les transmettre, ensuite, sous forme d'un message vocal sur une ligne téléphonique, le module doit se servir :

- d'un convertisseur numérique analogique (CNA) et,
- d'un amplificateur LM 386 de gain 200

Le microcontrôleur lit le fichier approprié de la carte mémoire SD, octet par octet et envoie chaque octet sur le port D connecté à un pont de résistances R2R servant comme un convertisseur digital analogique.

Ce signal est ensuite filtré puis amplifié par l'amplificateur LM386 avant qu'il soit livré sur la ligne téléphonique connectée.

3. Critères de choix des composants

Les composants choisis pour réaliser ce projet sont les suivants :

- Deux microcontrôleur PIC 18F4620.
- Les circuits intégrés MCP23S17 pour l'extension des ports.
- Un écran graphique à cristaux liquides (GLCD).
- Un écran à cristaux liquides (LCD).
- Un générateur récepteur des signaux DTMF
- Deux claviers à 16 touches.
- Un circuit Max485 pour l'interfaçage du Protocol RS485.
- Une carte mémoire flash (SD)
- Un amplificateur LM386

a) Le choix du microcontrôleur repose sur plusieurs critères :

- Nombre d'entrées sorties: Le microcontrôleur doit pouvoir se connecter à:
 - un GLCD qui nécessite 14 entrées/sorties,
 - un clavier à 16 touches qui nécessite 8 entrées/sorties
 - un générateur/récepteur des signaux DTMF qui nécessite 9 entrées/sorties.
 - un circuit Max485 qui nécessite 3 entrées/sorties
 - une interface USART nécessaire pour le Protocol RS485.
 - une carte mémoire flash (MMC) qui nécessite 5 entrées/sorties et l'interface MSSP (Master Synchronous Serial Port)

- Les détecteurs de mouvement, de chaleur, de fumée, et autres (au moins 16 entrées).
- La sirène, la ligne téléphonique et les autres commandes de sortie (5 sorties).
- Le module de conversion digitale analogique (8 sorties).

Ainsi, le total des entrées/sorties nécessaires s'élève donc à 68. D'où la nécessité d'utiliser un microcontrôleur qui supporte au moins 68 entrées/sorties.

- Taille des mémoires statique et volatile suffisamment large pour éviter d'avoir recours à des mémoires externes.
- 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.
- Interfaces intégrées dans le microcontrôleur pour la communication avec l'extérieur.
- Type du boîtier: on préfère travailler avec un microcontrôleur de type DIP (dual in-line package) qui est plus facile à implémenter et à souder sur PCB que celui dont le boîtier est de type TQFP (Thin Quad Flat Pack).

Le microcontrôleur PIC 18F4620 de Microchip, que nous avons choisi, répond à la plupart de ces critères mais il n'a que 36 entrées/sorties.

Pour remédier à l'insuffisance des entrées/sorties, deux solutions se présentent :

- La première consiste à chercher un microcontrôleur offrant un plus grand nombre d'entrées/sorties.
- La deuxième consiste à ajouter un module d'extension d'entrées/sorties comme le MCP23S17 de Microchip.

La première solution aurait dû nous amener à un microcontrôleur dont le boîtier est de type TQFP (Thin Quad Flat Pack) au lieu du DIP. Pour éviter des contraintes liées à sa soudure sur PCB, nous avons opté pour la seconde

solution qui s'avère plus facile à implémenter.

- b) Le choix du MCP23S17 repose sur deux paramètres :
- la librairie du langage C permet de s'interfacer et de communiquer facilement avec le MCP23S17.
 - Ce circuit autorise une communication- série avec le microcontrôleur.
- c) L'écran LCD est choisi de type graphique (GLCD) pour pouvoir afficher le plan de la menuiserie et indiquer la zone affecté.
- d) un clavier à 16 touches a été sélectionné: ce clavier suffit pour faire saisir un code (qui peut être de 14 chiffres différents) et offre aussi la possibilité d'entrer le code pour activer et désactiver le système de surveillance, ainsi que pour faire de changement de configuration tel que le menu, les modes et numéros de téléphone à appeler.
- e) Le choix du générateur et récepteur DTMF MT8889C se justifie par sa simplicité à s'interfacer avec le microcontrôleur d'une part, et la qualité du signal DTMF, et la détection de la progression d'appel.
- f) Le circuit d'interfaçage Max485 est choisi pour sa compatibilité avec le protocole RS485 qui permet la transmission de données sur une paire de fils torsadés,.
- g) Le choix de la carte mémoire MMC se justifie par sa grande capacité de stockage.

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 Microchip.

a. Familles de PIC

La société Microchip 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 10 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.

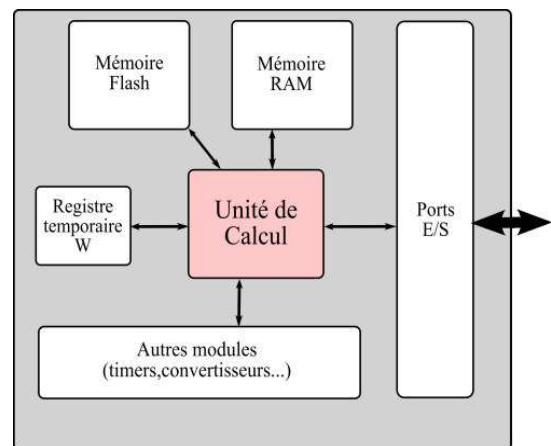


Figure 10 : Architecture interne d'un pic.

- 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 opérands 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 PIC18F4620

- Caractéristiques

De la famille 18F, le microcontrôleur PIC18F4620, 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 kHz.
 - ✓ Entrées/sorties séries: EUSART (CSA*), SPI (CSS*), MI²C (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 11)

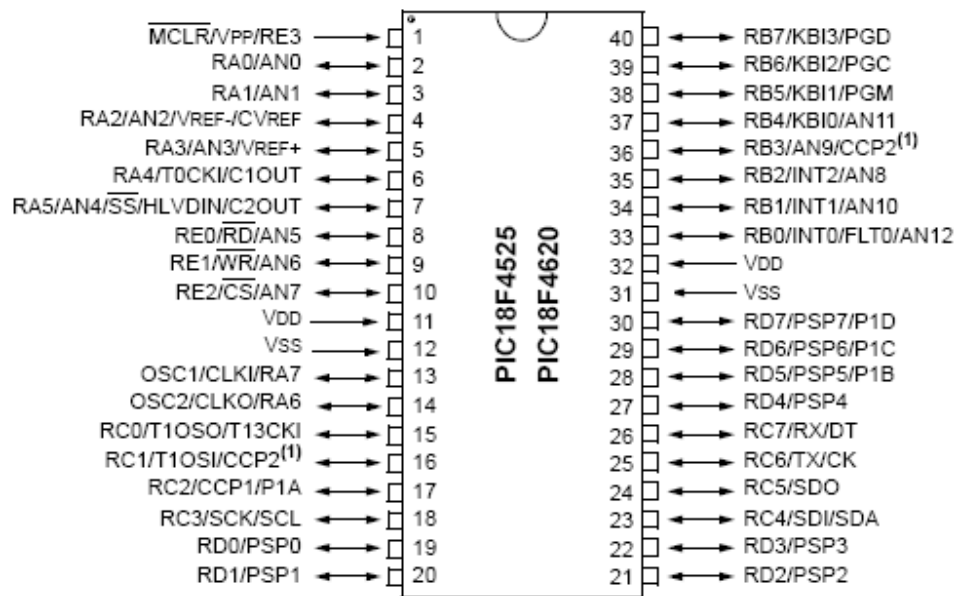


Figure 11 : Configuration du PIC4620.

- Schéma bloc

Le schéma bloc de la figure 12 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...

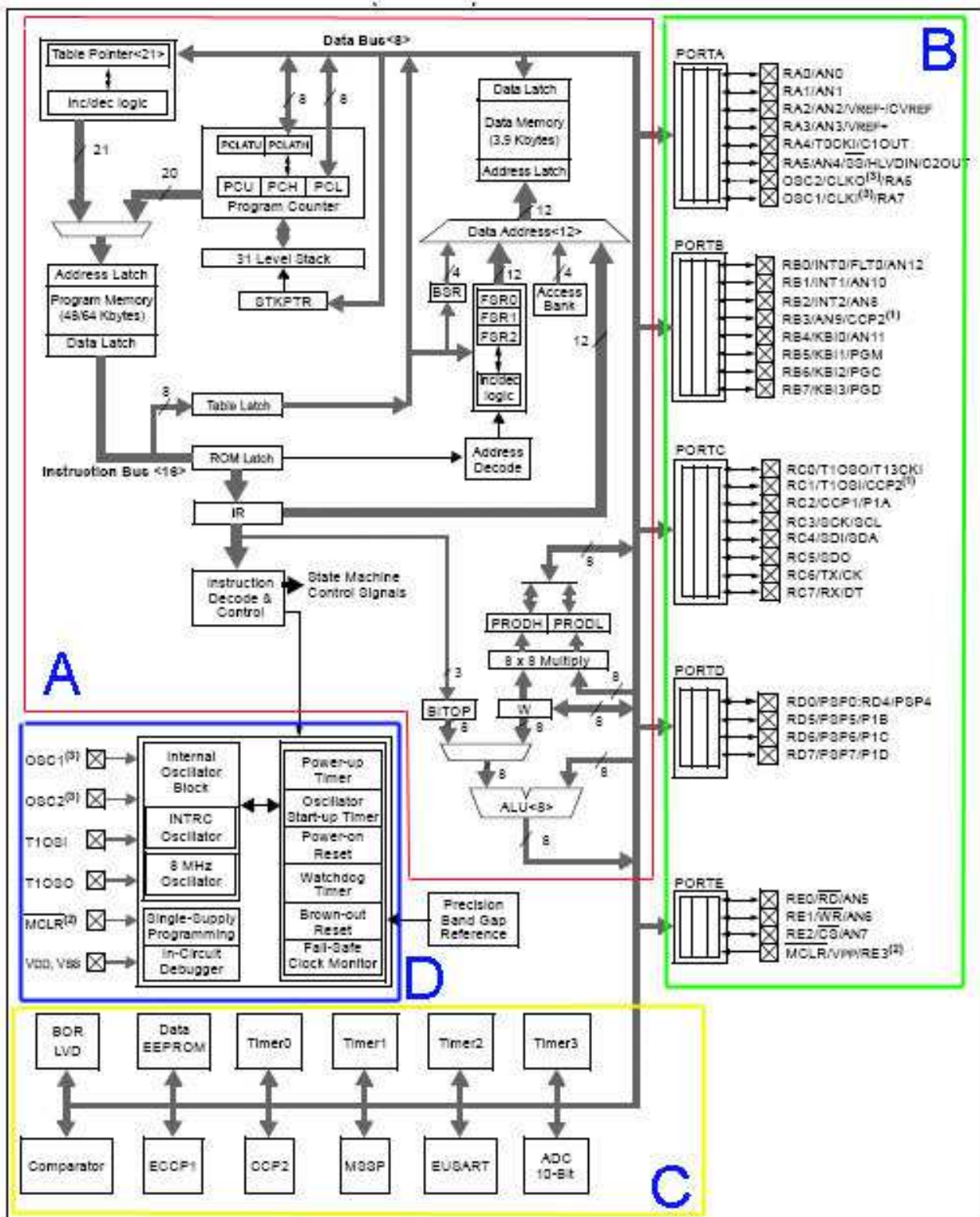


Figure 12: Schéma bloc du PIC4620.

- Oscillateur externe

Le PIC18F4620 a besoin, comme tout autre microcontrôleur, 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 13) est de type HS (High speed) quartz ou résonateur céramique 20 MHz.

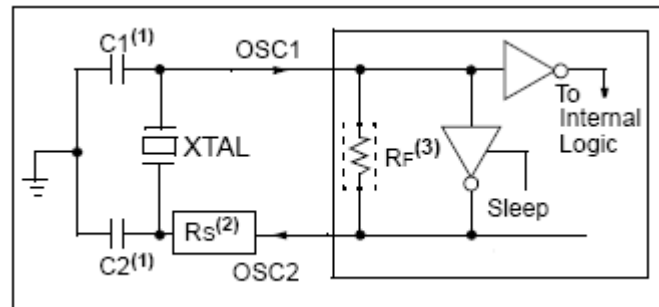


Figure 13 : oscillateur externe (avec $C_1=C_2=22\text{pF}$)

- Initialisation matérielle du microcontrôleur: \overline{MCLR}

La patte \overline{MCLR} permet une initialisation externe du microcontrôleur en la reliant à zéro, comme le montre le circuit de la figure 14. 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 \overline{MCLR} à zéro. Or en fonctionnement normal \overline{MCLR} doit être relié à VDD, alors on place une résistance et une diode pour ne pas avoir un court circuit en reliant \overline{MCLR} à zéro.

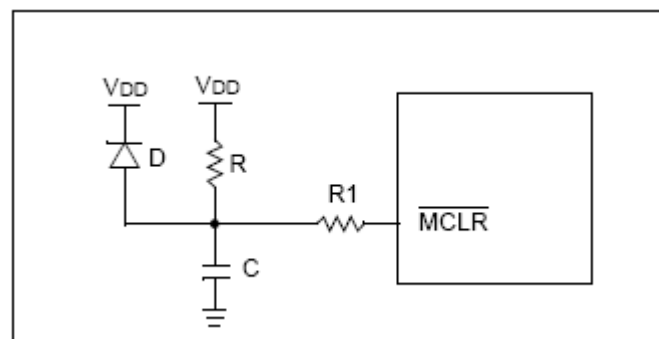


Figure 14 : Initialisation du microcontrôleur ($R=10\text{ k}\Omega$).

- Initialisation des registres

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

Le registre de contrôle analogique numérique ADCON1 sert à convertir les entrées ou les sorties analogiques en numérique. La table 6 montre comment se fait cette conversion.

PCFG3: PCFG0	AN12	AN11	AN10	AN9	AN8	AN7 ⁽²⁾	AN6 ⁽²⁾	AN5 ⁽²⁾	AN4	AN3	AN2	AN1	AN0
0000 ⁽¹⁾	A	A	A	A	A	A	A	A	A	A	A	A	A
0001	A	A	A	A	A	A	A	A	A	A	A	A	A
0010	A	A	A	A	A	A	A	A	A	A	A	A	A
0011	D	A	A	A	A	A	A	A	A	A	A	A	A
0100	D	D	A	A	A	A	A	A	A	A	A	A	A
0101	D	D	D	A	A	A	A	A	A	A	A	A	A
0110	D	D	D	D	A	A	A	A	A	A	A	A	A
0111 ⁽¹⁾	D	D	D	D	D	A	A	A	A	A	A	A	A
1000	D	D	D	D	D	D	A	A	A	A	A	A	A
1001	D	D	D	D	D	D	D	A	A	A	A	A	A
1010	D	D	D	D	D	D	D	D	A	A	A	A	A
1011	D	D	D	D	D	D	D	D	D	A	A	A	A
1100	D	D	D	D	D	D	D	D	D	D	A	A	A
1101	D	D	D	D	D	D	D	D	D	D	D	A	A
1110	D	D	D	D	D	D	D	D	D	D	D	D	A
1111	D	D	D	D	D	D	D	D	D	D	D	D	D

A = Analog input

D = Digital I/O

Table 6 :ADCON1.

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 7.

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

Table 7: 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 6, 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

totallement 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:

- SPI_Output,
 - SPI_Input,
 - SPI_SLK, et
 - CS.
- Le module USART (Universal Synchronous Asynchronous Receiver-Transmitter).

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).

- Topologie du réseau avec le RS485

La topologie du réseau est, probablement, la meilleur dans l'acquisition de données et les applications de contrôle. En effet, il est l'unique interface capable de faire fonctionner plusieurs émetteurs et récepteurs dans un même réseau. Quand on utilise les récepteurs RS485 avec une résistance d'entrée, il est possible de connecter 32 dispositifs au réseau.

La figure 15 nous permet de voir la topologie générale du réseau du RS485.

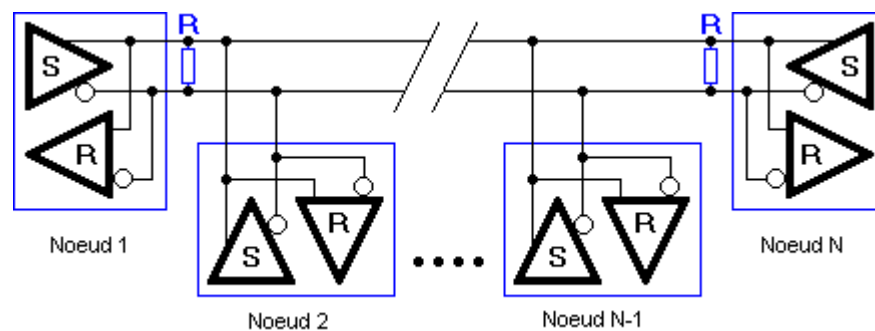


Figure 15 : Topologie du réseau RS485

N nœuds sont connectés dans un réseau RS485 à multipoint. Pour des vitesses plus élevées et des lignes plus longues, les résistances de terminaison sont nécessaires sur les deux extrémités de la ligne pour éliminer les réflexions.

Dans le cas de notre projet, il s'agit d'un simple réseau de communication RS485, de type d'opération simplex, dans lequel le RS485 du module d'accès est l'émetteur (c'est-à-dire le maître) et celui de la centrale principale est le récepteur (c'est-à-dire l'esclave).

- 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. Le circuit d'extension de ports : MCP23S17

Le MCP23S17 est une extension de ports. Le boîtier que nous avons choisi est de type DIP de 28 broches. Il comporte deux ports de huit bits chacun. Ces bits sont bidirectionnels (entrées/sorties).

Sa vitesse maximale est de l'ordre de 10 MHz. Il utilise le protocole SPI* maître-esclave. Le microcontrôleur joue le rôle du maître, le MCP23S17 est l'esclave.

Nous avons utilisé le MCP23S17 comme interface série entre le microcontrôleur et le GLCD. La figure 15 présente la configuration des broches de ce circuit. Sa configuration interne est représentée sur la figure 16, où on trouve, à gauche, les terminaux de commande de l'extension des ports MCP23S17 suivants:

- Cs : sélection du circuit (Chip Select)
- Sck : horloge
- Si : entrée de données série
- So : sortie de données série
- A0, A1, A2 : lignes d'adresses du circuit
- Reset : Remise à 0
- intA : interruption pour le port A
- intB : interruption pour le port B

À droite, on trouve les nouveaux ports, ajoutés au microcontrôleur, chacun de 8 bits, ainsi que des convertisseurs série/parallèle et parallèle /série, une unité de contrôle, un décodeur,...etc.

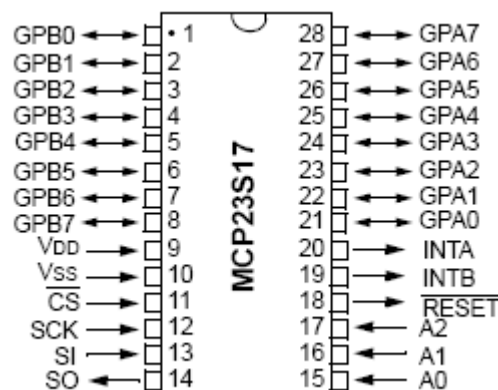


Figure 16 : Brochage du MCP23S17.

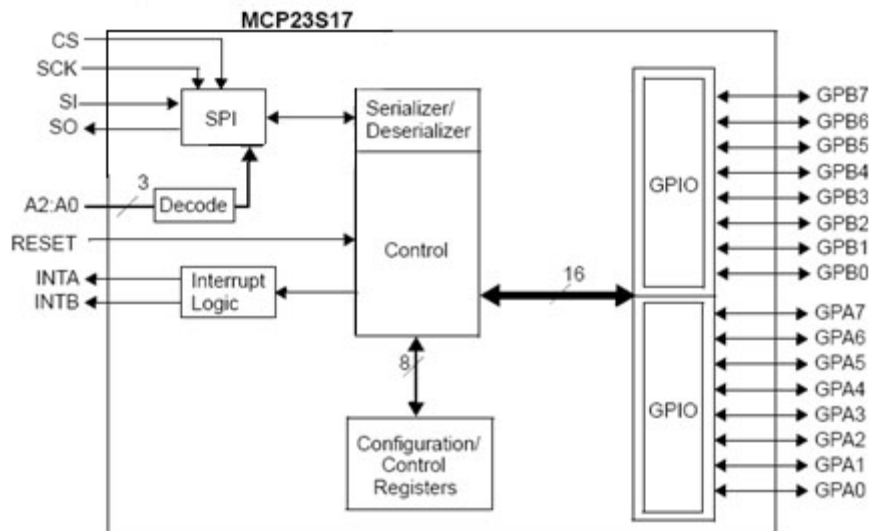


Figure 17 : Schéma bloc du MCP23S17.

Référence : [6]

6. Le circuit de connexion : Max485

Dans notre réseau de communication RS485, nous avons utilisé le Max 485 (Fig.17), qui est un émetteur/récepteur à bus/ligne différentiel de basse puissance $300\mu\text{A}$, conçu pour les applications du standard RS485 dans la transmission de données à multipoint, avec une portée étendue du mode commun (12V jusqu'à -7V).

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

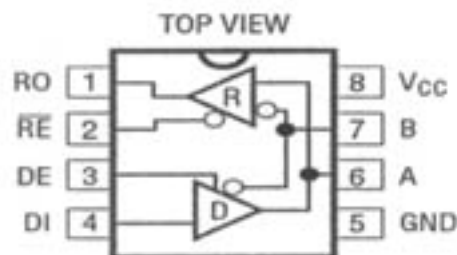


Figure 18 : Schéma bloc du CI MAX 485.

6.1. Le protocole de communication 485

La communication se fait à travers des paquets de 8 octets, repartit de la façon suivante :

Octet de début = 10010110
Octet d'adresse
Octet Datalen
Octet de Donnée1 (s'il existe)
Octet de Donnée2 (s'il existe)
Octet de Donnée3 (s'il existe)
CRC
Octet d'arrêt = 10010110

6.2. Configuration du Max485

- ✓ RE (Broche2) : Validation de la sortie du récepteur. Un niveau bas valide la sortie du récepteur RO. Un niveau haut met la sortie du récepteur dans un état de haute impédance.

- ✓ A (Broche6) : Sortie de l'émetteur/Entrée du récepteur.

- ✓ B (Broche7) : Sortie de l'émetteur/Entrée du récepteur.

- ✓ RO (Broche 1) : Sortie du récepteur. Si la sortie du récepteur est validée (RE au niveau bas), RO sera au niveau haut si $A > B$ de 200 mV ?, . Sinon, elle sera au niveau bas.

- ✓ DE (Broche3) : Validation des sorties du « driver ». Un niveau haut sur DE valide la sortie du « driver ». A, B et le LTC485 fonctionnent comme émetteur de la ligne. Un niveau bas mettra les sorties du « driver » dans un état de haute impédance et le LTC485 fonctionne comme récepteur de la ligne.

- ✓ DI (Broche4) : Entrée de l'émetteur. Si les sorties de l'émetteur sont validées (DE au niveau haut), un niveau bas sur DI mettra A au niveau bas et B au niveau haut, alors qu'un niveau haut sur DI, mettra A au niveau haut et B au niveau bas.

- ✓ GND (Broche5) : Connexion à la terre.

- ✓ Vcc (Broche8) : Alimentation positive ; $4.75 < V_{cc} < 5.25$.

Référence [7] :

7. Le circuit générateur/récepteur DTMF : MT8889C

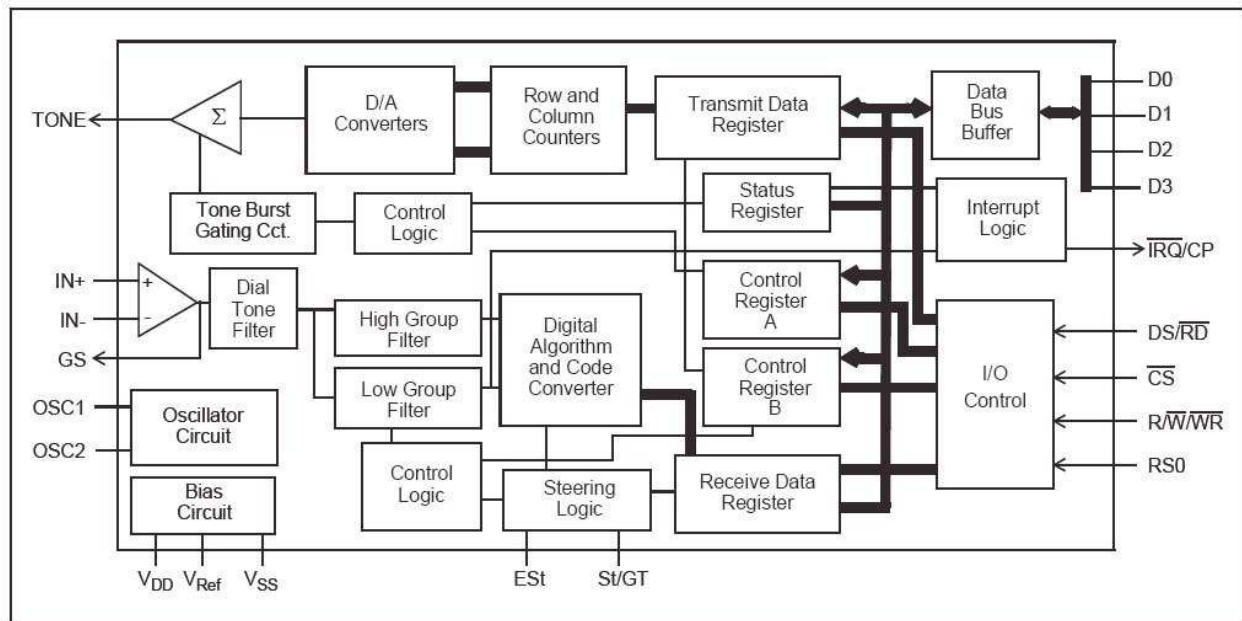


Figure 19 : Schéma bloc du MT8889

Le MT8889C est un émetteur-récepteur monolithique DTMF avec filtrage à la progression de l'appel. Il est fabriqué en technologie CMOS offrant une faible consommation et haute fiabilité.

La partie réceptrice est identique au circuit MT8870 (récepteur standard DTMF), le transmetteur utilise un convertisseur Digital Analogique à faible distorsion, et une signalisation DTMF de haute précision. Un compteur interne fournit un mode "rafale" tels que les tonalités peuvent être transmises avec un temps précis. Un filtre d'appel en progrès peut être sélectionné pour permettre à un microprocesseur d'analyser les tonalités.

Le MT8889C utilise une interface adaptative micro, qui permet au dispositif d'être relié à un certain nombre de microcontrôleurs populaires.

La figure 18 représente le schéma bloc du CI MT8889 alors que la figure 19 représente la configuration de ses broches dont le rôle de chacune est résumé par la Table 8.

Référence [8] :

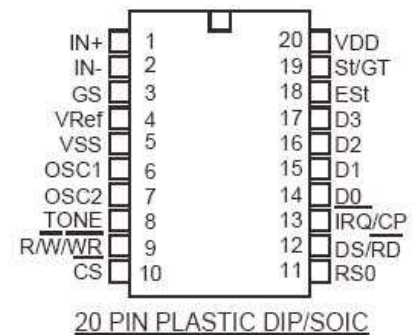


Figure 19 : Configuration des broches du CI MT8889.

Broche	Nom	Description
1	IN+	Entrée ampli-op non inverseuse
2	IN-	Entrée ampli-op inverseuse
3	GS	Gain de sortie
4	VRef	Référence de tension de sortie (VDD / 2).
5	VSS	Masse
6	OSC1	Entrée d'oscillateur (horloge DTMF). Une résistance de 4.7MΩ doit être connectée à VSS si un oscillateur à cristal est utilisé.
7	OSC2	Sortie de l'oscillateur. Un cristal de 3.579545 MHz connecté entre OSC1 et OSC2 complète le circuit oscillateur interne. Lorsque OSC1 est entraîné à l'extérieur, la broche doit rester ouverte.
8	TONE	La sortie interne de l'émetteur DTMF
9	R/W (WR)	lecture/écriture (pour μp Motorola) ou entrée Écriture (pour μp Intel). Compatible avec TTL.
10	CS	Entrée sélection du CI. Ce signal doit être qualifié à l'extérieur soit par l'adresse stroboscopique (AS), l'adresse mémoire valide (VMA) ou l'adresse latch enable (ALE) du signal,
11	RS0	Entrée sélection du registre
12	DS (RD)	Data Strobe (pour μp Motorola) ou (Intel) entrée Lecture (pour μp Intel). L'activité sur cette entrée est seulement nécessaire lorsque le circuit est en cours d'accès. Compatible TTL.
13	IRQ/CP	Demande d'interruption (drain ouvert) de sortie. En mode d'interruption, cette sortie passe au niveau bas quand une rafale de tonalité DTMF valide est transmise ou reçue. En mode de progression d'appel, cette broche de sortie sera un signal rectangulaire représentatif du signal d'entrée appliqué à l'entrée de l'ampli-op. Le signal d'entrée doit être dans les limites de bande passante du filtre à progression d'appel.
14-17	D0-D3	Bus de données du microprocesseur. haute impédance lorsque CS=1 ou DS=0 (Motorola) ou RD=1 (Intel). Compatible TTL.
18	Est	Early Steering output. Présente un niveau logique haut lorsque l'algorithme numérique détecte une paire de tonalité valide (état du signal). Toute perte momentanée du signal entraîne Est à un niveau logique bas.
19	St/GT	Steering Input/Guard Time output (bidirectionnel). Une tension supérieure à VTSt détectée à St amène le dispositif à enregistrer la paire de tonalité détectée et à mettre à jour la Sortie latch. Une tension inférieure à VTSt libère le dispositif pour devenir prêt à accepter une nouvelle paire de tonalité.
20	VDD	Alimentation positive (5V typique).

Table 8 : Rôle de chacune des broches du MT8889.

8. 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]

8.1. Carte SD :

Pour notre prototype, nous avons choisi d'utiliser une carte mémoire de type SD. La famille des cartes SD disponibles sur le marché comporte plusieurs types qui sont:

- Secure Digital
- Mini Secure Digital
- Micro Secure Digital
- Secure Digital High Capacity

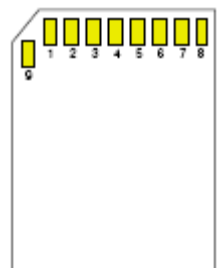


Figure 20 : Broches de la carte mémoire SD.

La carte SD utilisée dans notre projet est de type Secure Digital (figure 20). La configuration de son brochage est donnée dans la table 9.

Broche	Symbole	Fonction SD Mode	Fonction SPI Mode
1	DAT3/CS	Data Line 3	Chip Select/Slave Select
2	CMD/DI	Command Line	Master Out/Slave In
3	VSS1	Ground	Ground
4	Vdd	Voltage Supply [2.7V or	Voltage Supply [2.7V or
5	Clock	Clock	Clock [SCK]
6	Vss2	Ground	Ground
7	DAT0/D0	Data Line 0	Master In Slave Out
8	DAT1/IRQ	Data Line 1	Unused or IRQ
9	DAT2/NC	Data Line 2	Unused

Table 9 : brochage de la carte SD.

9. Écran graphique

L'écran utilisé (figure 21) dans notre système est un écran graphique à cristaux liquides GLCD* de type KS0108. Il a les dimensions de 128x64 pixels.

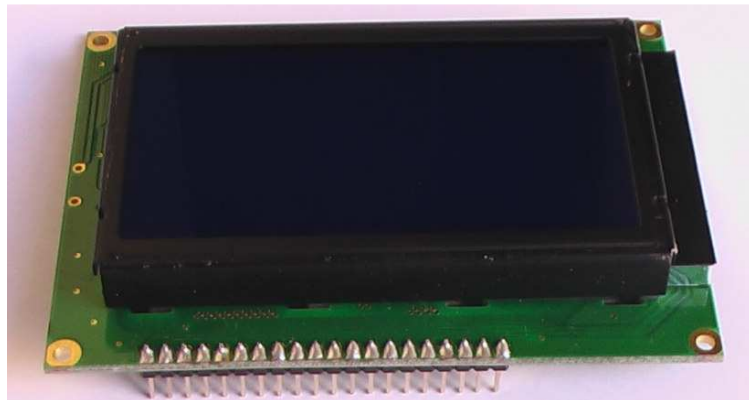


Figure 21 : GLCD.

Son brochage est donné dans la table 10:

Broche numéro	Symbole	Fonction
1	Vss	Masse
2	Vdd	Alimentation (+ 5V)
3	V0	Ajustement du contraste
4	D/I	Data/Instruction
5	R/W'	Data Read/Write'
6	E	H→L Enable
7	DB0	Data Bus Line
8	DB1	Data Bus Line
9	DB2	Data Bus Line
10	DB3	Data Bus Line
11	DB4	Data Bus Line
12	DB5	Data Bus Line

13	DB6	Data Bus Line
14	DB7	Data Bus Line
15	CS1	Chip Select for IC1
16	CS2	Chip Select for IC2
17	RST'	RESET (remise à zéro)
18	Vee	Tension de sortie négative
19	A	Alimentation LED +4.2V
20	K	Alimentation LED 0V

Table 10: Brochage du GLCD

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 rétro-éclairé.

Référence : [10]

10. Clavier

Le clavier est de type matriciel quatre lignes quatre colonnes (4x4), ce qui nécessite huit broches de connexion. Il comporte 16 touches (figure 22) dont 10 pour les chiffres (de 0 à 9) ainsi que les lettres A, B, C, et D et les deux symboles '*' et '#'.

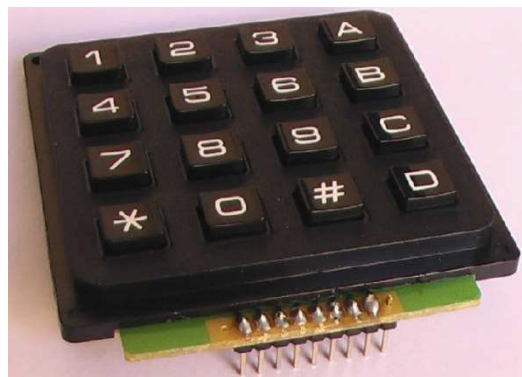


Figure 22: Clavier à 16 touches.

Sa connexion avec le microcontrôleur peut se faire comme le montre la figure 23.

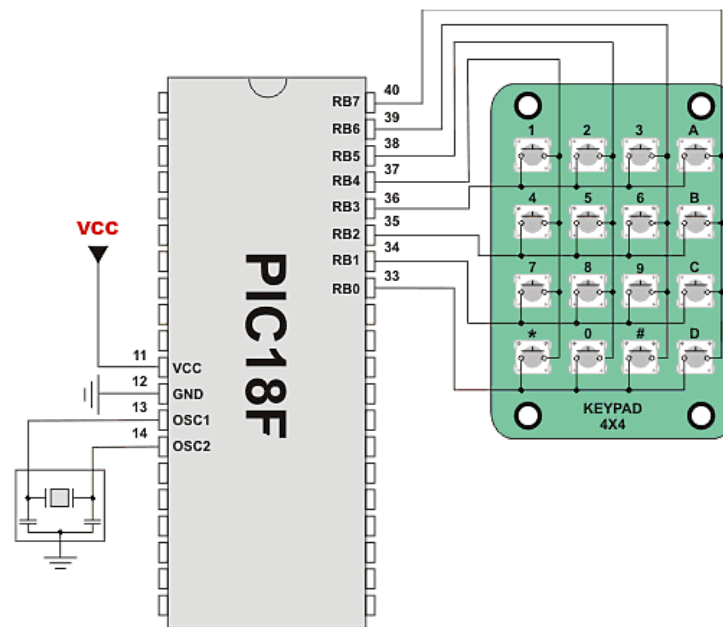


Figure 23 : Brochage d'un clavier.

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

Référence : [11]

11. L'amplificateur LM386

Le signal audio que produit le microcontrôleur est un signal digitale 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

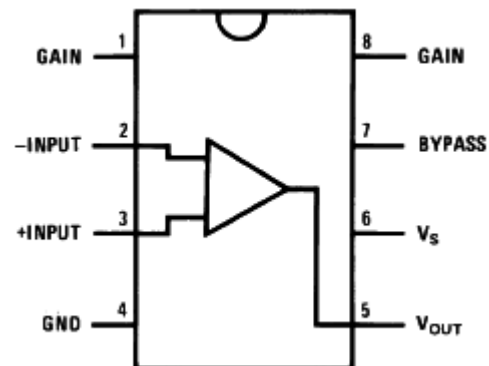


Figure 24 : brochage de l'amplificateur LM386

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

1.Introduction

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

Une fois la réalisation est achevée, une phase de validation sera nécessaire. Nous testons la fonctionnalité du prototype en vérifiant sa réponses aux détections d'alarme et/ou d'intrusion.

2.Déroulement de la réalisation

2.1. 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 (voir figures 26 et 29). Ces derniers sont faits en se servant du logiciel "Eagle" [12] (programme de dessin des schémas électroniques avec routage automatique; il est assez intuitif et comporte une librairie assez riche en composants).

Les schémas des circuits électroniques ainsi conçus sont présentés sur les figures 27 et 28.

À ce niveau, un autre test est fait pour vérifier le bon fonctionnement des circuits imprimés ainsi réalisés

2.1.1. Circuit du système d'accès.

Le premier circuit électronique qui englobe le système d'accès (figure 25) se divise en 6 blocs principaux:

- L'alimentation à courant continu.
- Le microcontrôleur.
- L'écran à cristaux liquide.
- Le clavier.
- Le module RS485.
- 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 470 μ F puis régulée à 5V par le régulateur de tension 7805.

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 D, configuré comme entrée, est réservé au clavier.

Les pattes RB4, RB5, RB6, RB7 configurées comme sorties, sont réservées pour l'écran à cristaux liquides.

Les pattes RC2, RC6, RC7 sont configurées pour la communication série avec le CI MAX485.

Le pin RA1 est réservé pour le buzzer

Le pin RB0 est réservé pour la commande du relais.



Figure 25 : Système d'accès sans boîtier.

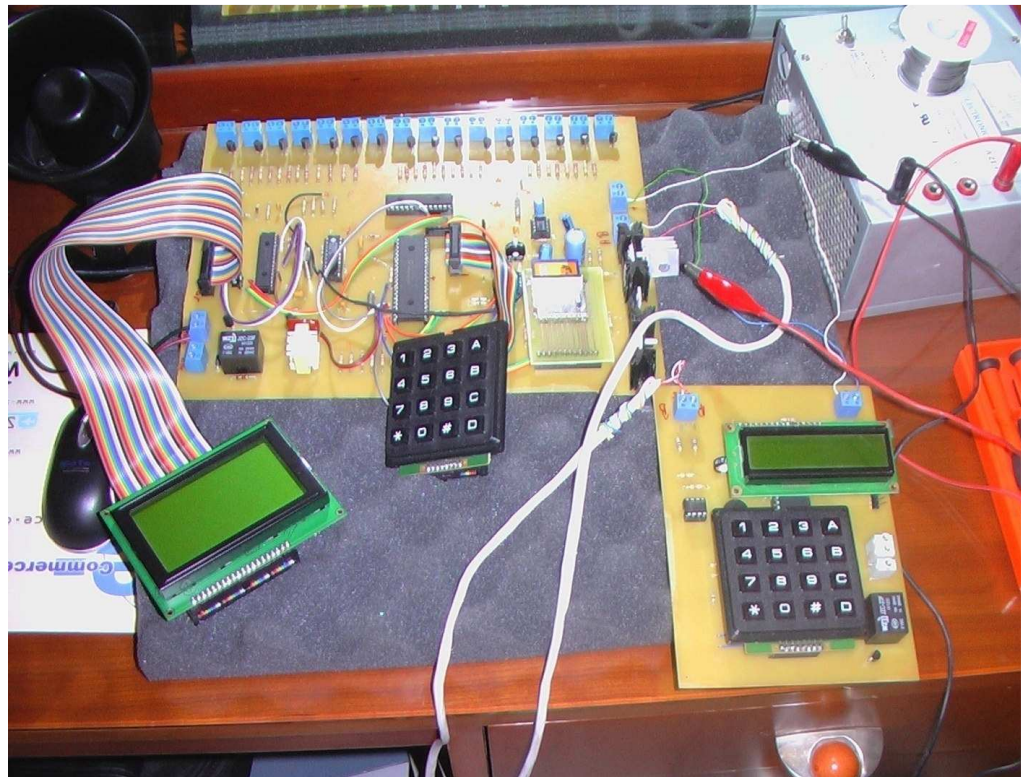


Figure 28 : Système de surveillance et contrôle d'accès final.

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

Le second circuit électronique qui englobe le système d'alarme et d'intrusion (figure 28) se divise en 13 blocs principaux:

- L'alimentation à courant continu.
- Le microcontrôleur.
- L'écran à cristaux liquide.
- Le clavier.
- Le module RS485.
- L'amplificateur.
- Les extensions de ports.
- La carte SD.
- 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.

L'alimentation à courant continu est composée d'un transformateur 220V/12V 3000mA, suivi d'un pont à diodes dont la sortie redressée est filtrée à l'aide d'un condensateur de 470 μ F puis régulée à 5V par le régulateur de tension 7805 et en 12 volt par le régulateur de tension 7812.

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.

Le PORT D, configuré comme sortie, est réservé pour le convertisseur numérique analogique R2R.

Les PORTS A et E, sont configurés comme sorties, et servent pour commander le module de connexion à la ligne téléphonique (Module de télécommunication).

Les pattes RB6, RB7 configurées comme entrées, sont utilisées de plus pour la programmation sur place du microcontrôleur.

Les pattes RC2, RC6, RC7 sont configurées pour la communication série avec le CI MAX485.

Les pattes RC0, RC1, RC3, RC4, RC5 sont configurées pour la communication série avec les CI MCP23S17 (extension de port). Chaque CI offre deux nouveaux ports, le nombre de CI MCP23S17 que l'on peut utiliser est limité à huit car chacune est adressée par 3 bits.

Le CI MCP23S17 d'adresse 000 est utilisé pour l'écran graphique à cristaux liquides.

Le CI MCP23S17 d'adresse 001 est utilisé comme récepteur pour 16

capteurs différents.

Les autres CI peuvent être ajoutés pour jouer le rôle d'extension de ports pour usage multiple.

Les pattes RC2, RC3, RC4, RC5 sont utilisées pour la connexion de la carte SD (Secure Digital).

Les pattes GPA6, GPA7 sont utilisées pour la sirène et pour le relais téléphonique pour raccrocher et décrocher.

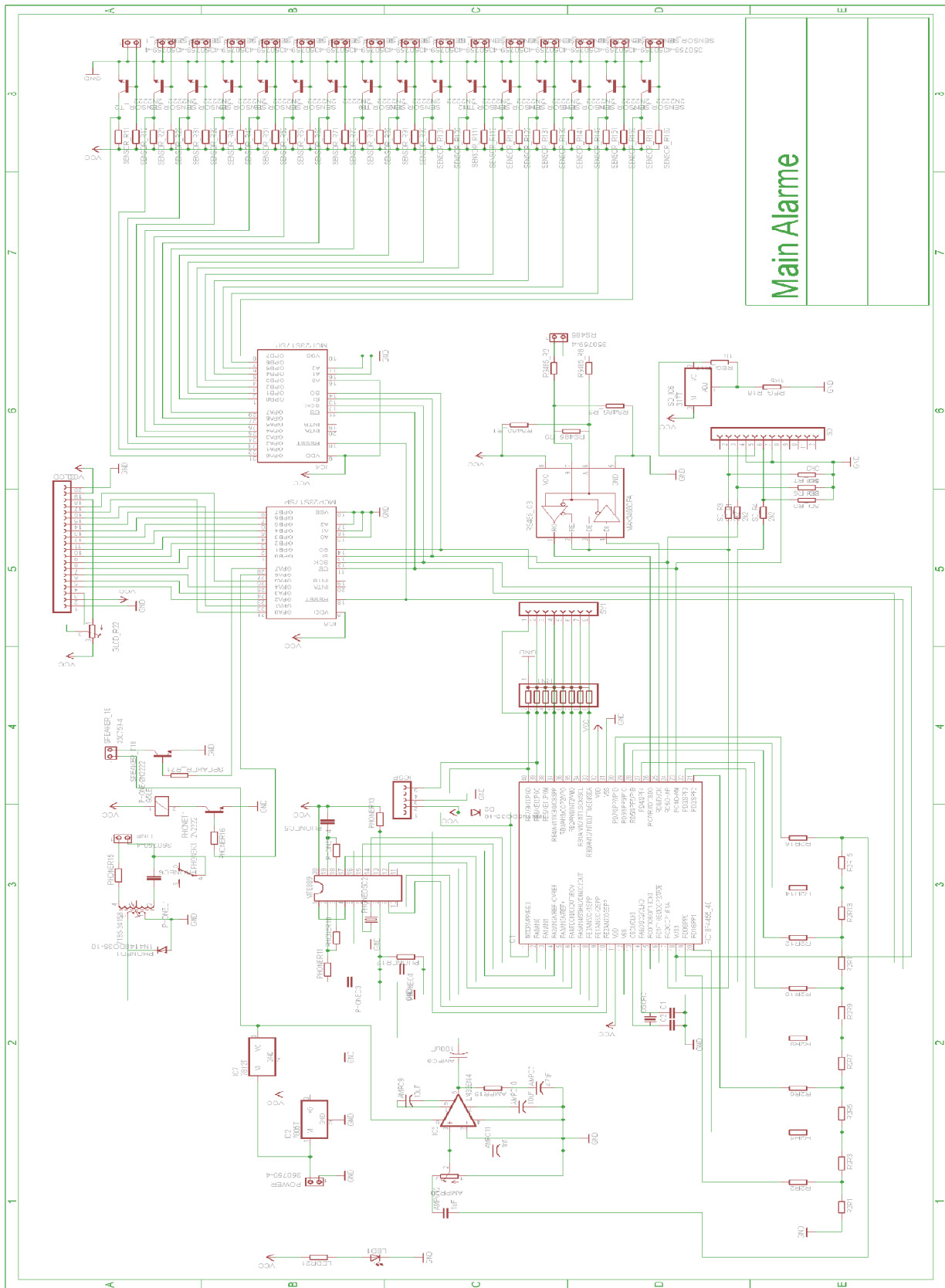


Figure 28 : schéma électronique du système de surveillance.

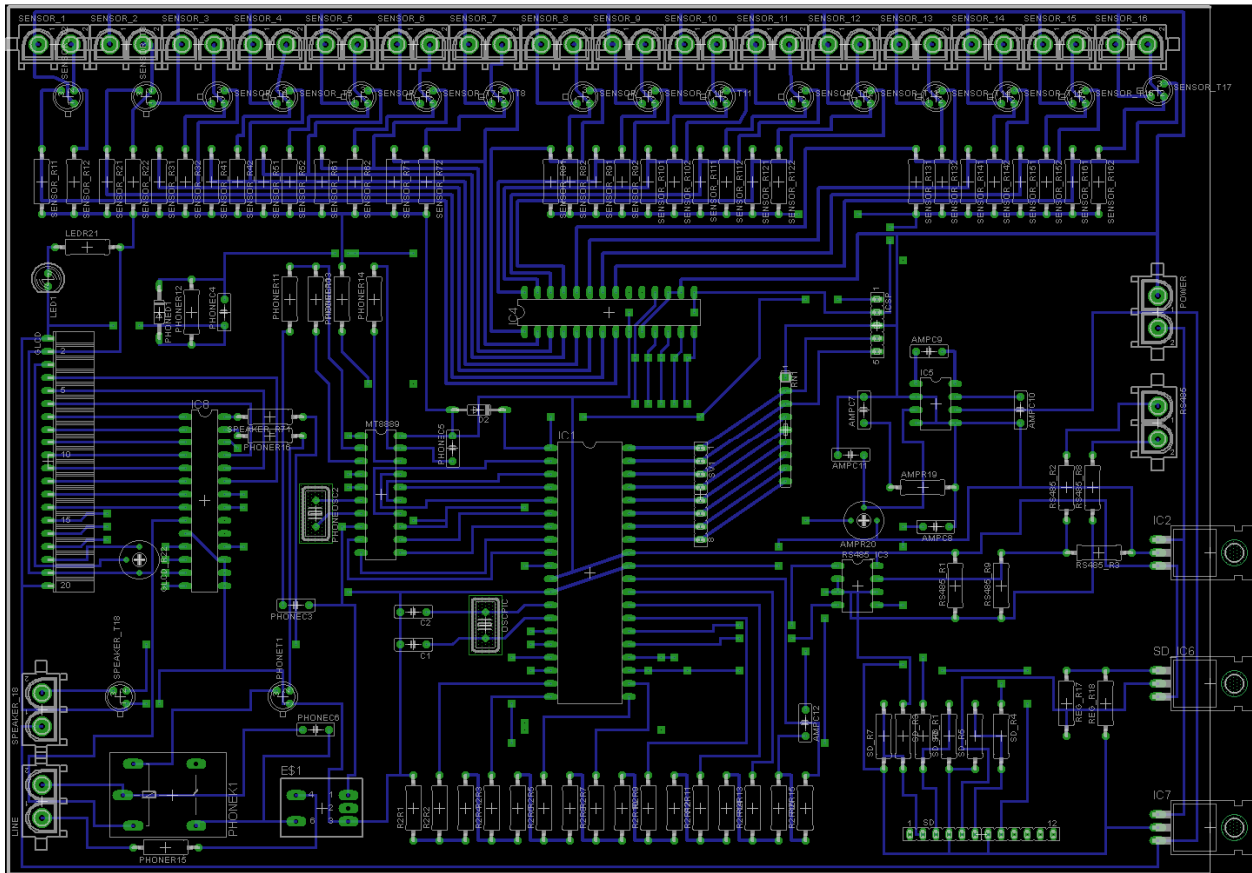


Figure 29 : Circuit imprimé du système de surveillance.

2.2. 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 18F et comprend une librairie très riche) sous Windows et qui sera exécuté par le microcontrôleur.

Le chargement de ce programme sur le microcontrôleur est effectué grâce à l'interface pickit2 de la société Microchip.

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 boîtier 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.

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

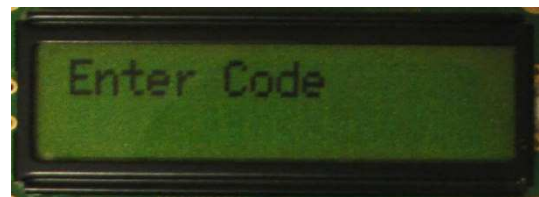
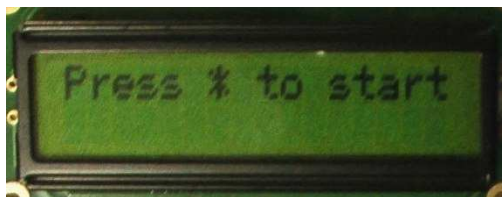
- Introduire le mot de passe pour avoir accès au lieu protégé.
- Changer le mot passe par les personnes possédant déjà le mot de passe.
- Sauvegarder le mot de passe dans la mémoire EEPROM.
- Afficher sur l'écran les différents messages d'invitation et/ou de réponse.
- Activer ou désactiver le le système de surveillance.
- Déclencher l'alarme après trois essais erronés de saisie de code.

2.2.2. Déroulement de processus

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



Lorsqu'il devient prêt, l'écran affiche « press * to start ». Après avoir appuyée la touche "étoile" (*), l'écran affiche "Enter code".



Quand l'utilisateur entre le code, l'écran affiche, pour chaque touche appuyée, une étoile. Quand le code est complètement saisi, l'utilisateur doit appuyer sur la touche (#) pour la confirmation.



Si le code saisi est correct, l'écran affiche « Access granted » et la porte s'ouvre, sinon l'écran affiche « Access denied » et nous revenons au début.



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 :

Supposons que le code est « 1234 » et l'utilisateur voudra le changer en « 9876 ». Alors quand l'écran affiche « enter code », l'utilisateur fait entrer le code ancien suivi du nombre 5, exemple « 12345# », l'écran affiche « enter new code » alors l'utilisateur fait entrer le nouveau code par exemple « 9876# »

2.2.3. 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.
- Activer ou désactiver les entrées des multiples capteurs.
- Afficher en cas d'alarme le lieu du feu ou d'intrusion.

2.2.4. De plus ce logiciel gère les fonctions suivantes :

- ✓ gère la connexion avec le clavier 4x4.
- ✓ Commande l'écran graphique à cristaux liquides à travers l'extension de port série le MCP23S17.
- ✓ Reçoit les signaux d'alarmes provenant des capteurs à travers l'extension

de port série le MCP23S17.

- ✓ Communique avec les bornes distribuées du système d'accès (32 au maximum).
- ✓ Pilote le CI MT8889 pour établir les communications téléphoniques en fonction de l'état des systèmes et selon les directives déjà introduites dans le système.
- ✓ Lit et transmet les messages vocaux stockés dans la carte mémoire SD.

L'algorithme correspondant à ce programme est décrit graphiquement par l'organigramme de la figure 32.

Ces programmes ont été développés sur un ordinateur sous Windows en utilisant le logiciel de développement en MikroC. Les programmes sont ensuite transférés au système pour qu'ils soient exécutés par les microcontrôleurs.

Le transfert est effectué grâce à l'interface Pickit2 (figure 30) de Microchip. Cette interface est conçue pour pouvoir programmer les microcontrôleurs pic déjà opérationnels sur un circuit. [5]

Une connexion matérielle doit être réalisée entre le pickit2 et le microcontrôleur. De l'autre côté, le pickit2 doit être connecté à l'ordinateur à travers un port USB.

Ainsi, nous avons ajouté au circuit du système une extension pour l'interfacer au pickit2. Le brochage du PICKIT2 se fait selon la figure 31.



Figure 30 : PICKIT2.

- 1- Etats des LEDs.
- 2- Bouton poussoir.
- 3- Connexions.
- 4- Connexions port USB.
- 5- marqueur de la broche 1.
- 6- Connecteur pour la programmation.

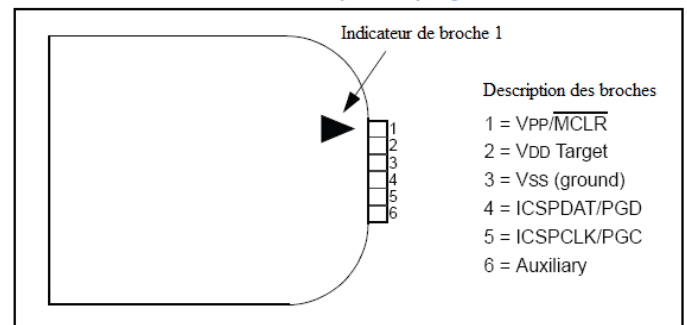


Figure 31 : Brochage du PICKIT2.

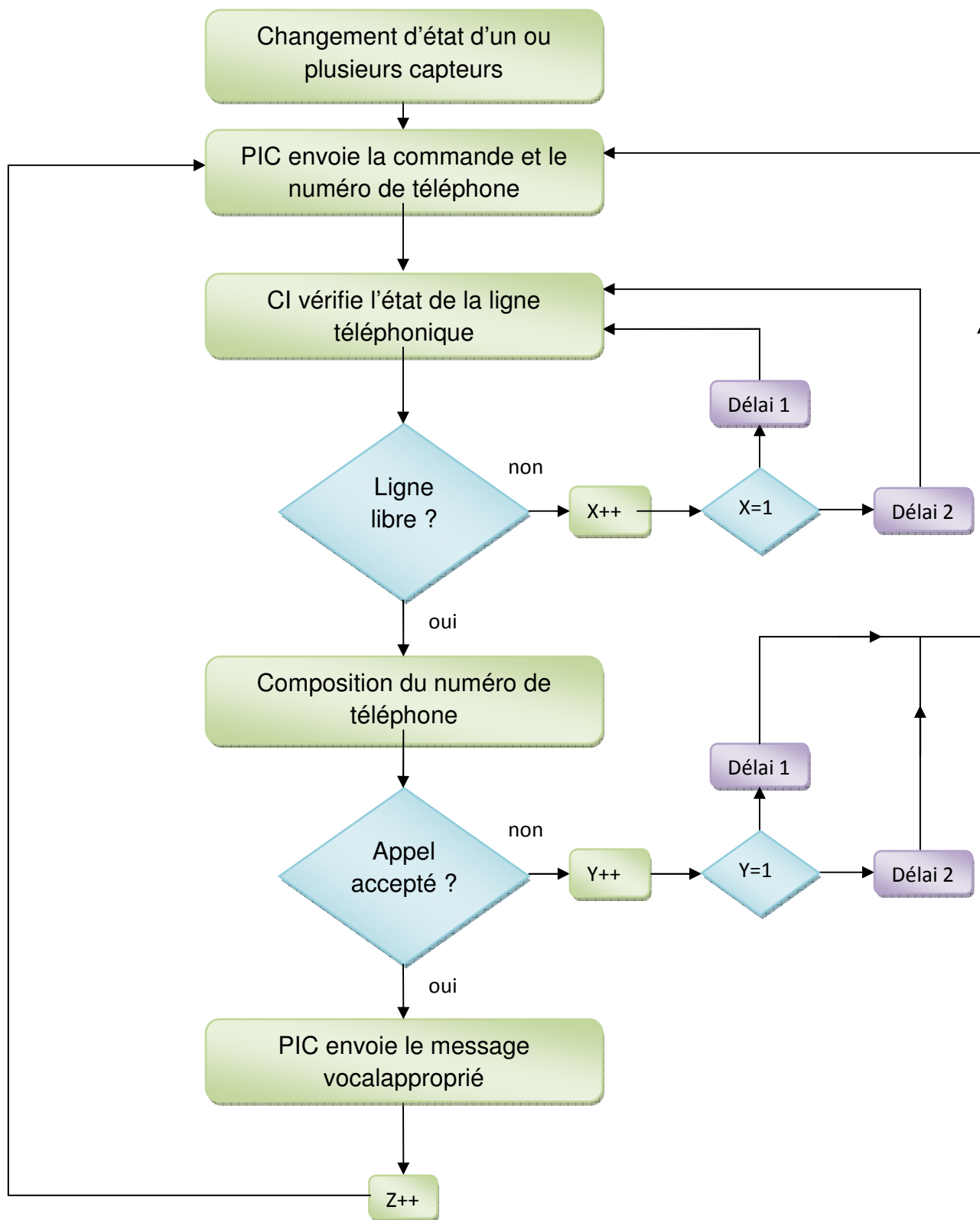


Figure 32 : Organigramme du système de surveillance et contrôle d'accès.

3. Organigramme du programme principal.

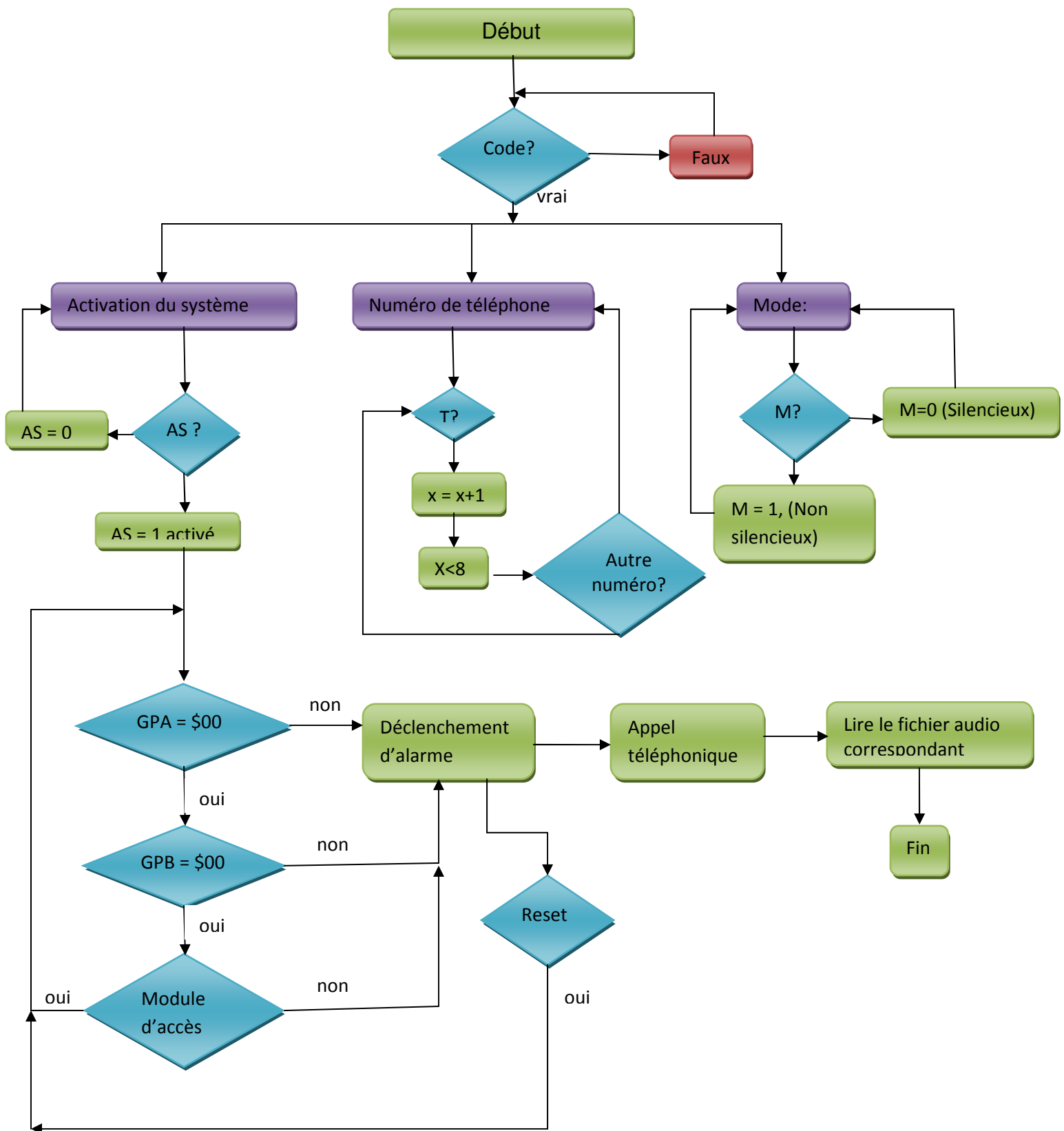


Figure 33 : Organigramme du système

4. Fonctionnement du système.

4.1. 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.

- Installation des boîtiers de contrôle d'accès dans les endroits désirées, où chacun doit être connecté d'une part à la porte (ou autre élément d'accès) concernée par la commande d'accès, et d'autre part, au module central par deux paires de fils en cuivre: la première paire est pour l'alimentation, alors que la seconde sert à transmettre le signal émis par le module d'accès

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

4.2. 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,...).

Si cette procédure prévoit d'envoyer un message vocal à quiconque, le module central transmet la commande au module de télécommunication suivi par le numéro à composer. Si la communication téléphonique est établie, le module central lit le message vocal correspondant et termine la communication avant de procéder, le cas échéant, à établir un autre appel.

Pour désactiver l'alarme il faut entrer le code correspondant, puis choisir: désactivation.

Notons enfin que, tous les modules sont normalement alimentés sur le secteur. Cependant, et pour éviter toute coupure du courant, nous les avons équipés par des batteries de secours capables de les maintenir sous tension en cas de la coupure de l'électricité.

5. Problèmes de réalisation

La réalisation pratique du prototype n'était pas sans difficultés. Parmi ces difficultés, on cite:

- ✓ Le choix du module vocal, n'était pas si évident: Dans un premier temps,

nous avons choisi le circuit APR9600, qui enregistre 8 messages vocaux pour une durée totale de 60 secondes. Pour lire ces messages le CI est équipé de 8 boutons poussoirs.

Ce choix ne convenait pas à notre système pour plusieurs raisons :

- Nombre et durée des messages insuffisants
- la commande de lecture d'un message se fait à travers un bouton poussoir, ce qui va nous obliger à consacrer un ligne de commande du microcontrôleur pour la lecture de chaque message.

Le second choix s'est orienté vers le CI APR6016 qui est capable d'enregistrer jusqu'à 16 minutes; il utilise la connexion série avec le microcontrôleur pour l'enregistrement et la lecture, le microcontrôleur envoie l'adresse de début pour commencer l'enregistrement ou la lecture. Ces caractéristiques sont plutôt acceptables pour notre prototype, mais aux premiers essais, nous avons constaté une certaine incompatibilité avec le microcontrôleur que nous utilisons, qui rend son utilisation non fiable à cause d'une instabilité dans le CI APR9600.

Ensuite, nous nous sommes orientés vers un programme gratuit qu'on peut trouver sur l'internet: le « btc » qui lit un message vocal et le transforme en binaire avec un format qui lui est spécifique. Cette forme binaire sera enregistrée dans la mémoire du système et à chaque que le microcontrôleur souhaite lire le message vocal, il n'a qu'à lire le contenu du fichier binaire, bit par bit, et les envoyer vers une sortie où est placé un filtre RC pour reproduire le son vocal.

Ce choix peut être valable techniquement mais il souffre de deux inconvénients majeurs pour notre application:

- Tout d'abord la qualité du son est médiocre
- les fichiers binaires sont trop volumineux de sorte que la mémoire

interne du microcontrôleur ne puisse supporter plus de 80 secondes (cette solution a été envisagée initialement avant d'avoir recours à la carte mémoire).

Son principal avantage est qu'il utilise une seule broche pour la sortie.

La décision finale était d'introduire une carte mémoire « SD » dont la capacité peut atteindre 2 GO, ce qui veut dire qu'il n'y aura pas de limitation pour le nombre de messages vocaux.

La lecture se fait, alors, octet par octet du fichier «.wav» enregistré sur la carte mémoire. Chaque octet lu est ensuite envoyé vers le PORT D du microcontrôleur où un convertisseur numérique analogique R2R convertit le message en analogique, avant qu'il soit amplifié par l'amplificateur LM386 ayant un gain de 200 fois et livré sur la ligne téléphonique à travers un transformateur isolateur 1:1 .

- ✓ La seconde difficulté était dans la génération du signal DTMF, qui a été résolue grâce à l'utilisation du CI MT8889 qui offre la précieuse possibilité de s'interfacer avec le microcontrôleur. Ainsi, son mode de fonctionnement devient complètement programmable et piloté par le microcontrôleur qui lui envoie les chiffres du numéro à composer sous forme binaire et le MT8889 génère le signal DTMF correspondant.
- ✓ Un troisième problème se résume par le manque du nombre des entrées sorties du microcontrôleur. C'est une des raisons qui nous ont amené à essayer de remplacer ce microcontrôleur par un autre (le PIC 18F97J60) disposant de 70 entrées/sorties.

Or, ce dernier pose un problème technique de montage sur le circuit imprimé. Il est de type TQFP et de dimensions réduites, ce qui nous oblige à faire appel à un atelier spécialisé, chose qui n'est pas facilement accessible sur le marché libanais et ce qui pourrait augmenter considérablement le coût de réalisation de notre produit.

L'autre alternative que nous avons choisie consiste à ajouter au PIC une extension de ports. La société Microchip offre une gamme riche de ces extensions. Dans cette gamme on trouve deux familles d'extension de ports; la première utilise le protocole SPI, et la seconde utilise le protocole I2C. Le choix du protocole n'était pas difficile car le logiciel MikroC est muni d'une très bonne librairie qui utilise le protocole SPI pour connecter un écran GLCD au PIC. Ainsi, l'utilisation du MCP23S17, comme un composant d'extension de ports, était pour nous la solution optimale.

6. Validation et tests :

Après avoir achever le premier prototype, la phase de test est nécessaire pour s'assurer du bon fonctionnement du système.

Le système est munie d'un programme qui test les différents parties du système dès la mise en marche, si un ou plusieurs module n'est pas fonctionnel un message apparait sur l'écran GLCD pour informer l'utilisateur.

Le système est testé pendant 24heures avec les périphériques suivants, les capteurs et les détecteurs sont remplacés par des interrupteurs, la sirène est en place, et le module d'accès et la ligne téléphonique sont connectés.

Les résultats sont satisfaisantes le système fonctionne comme prévu, si n'importe quel interrupteur est activé la sirène se met en marche, la module d'appel compose le numéro de téléphone et le message approprié est transmis. L'écran affiche le numéro du port en activation. Le module d'accès active l'alarme après trois essais consécutifs non acceptés du code.

7. Installation

La menuiserie est formée de trois étages, le premier étage est utilisé comme dépôt dont la superficie ne dépasse pas les 100m², le second et le troisième étage sont identiques et de 300m² de superficie chacun.

Le second étage comporte les bureaux où il faut placer le module d'accès, et l'autre partie (Quelle partie) c'est le milieu(????) de travail.

Le troisième étage abrite l'atelier (????).

La figure 34 montre la répartition des détecteurs de chaleur, des détecteurs de mouvement, du module d'accès et du circuit central au second étage.

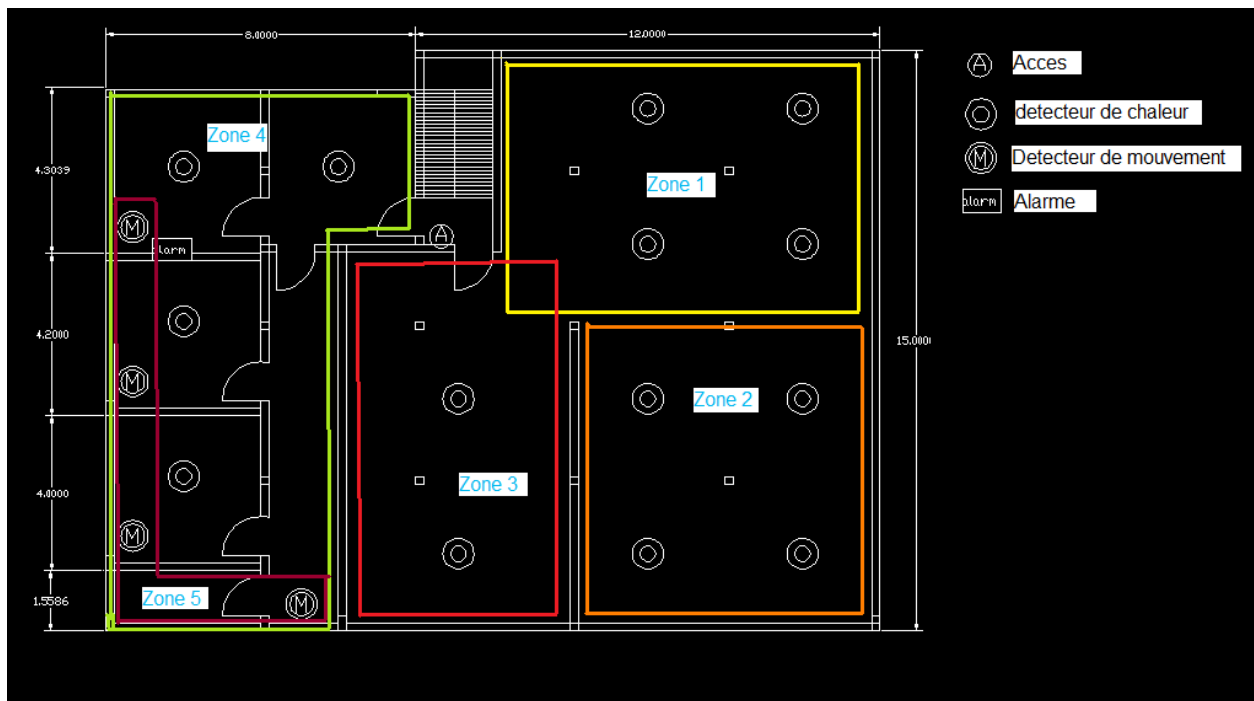


Figure 34 : plan de menuiserie - étage 2

Le choix des détecteurs de chaleur est imposé par l'environnement de la menuiserie caractérisé par une forte présence de la poussière, qui rend impossible l'utilisation des détecteurs de fumée, étant connu que la poussière forme une couche isolante semblable à la fumée qui pourrait déclencher l'alarme.

Le nombre de détecteurs est réparti suivant la table 11 :

Étage	Détecteur de chaleur	Détecteur de mouvement	Module d'accès	Zone	Circuit central
1	3	-	-	1	-
2	14	4	1	5	1
3	14	-	-	4	-

Table 11 : Répartition de détecteurs

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.

Dans le chapitre suivant, nous présentons une étude comparative entre les systèmes de surveillance et d'accès actuellement disponibles sur le marché et notre prototype, de point de vue "prix" et "qualité".

Chapitre 7 : Comparaison avec d'autres systèmes

1. Introduction

La réalisation matérielle et logicielle des maquettes du système de surveillance et contrôle d'accès des circuits intégrés suivie d'une phase de validation et de tests a donné des résultats approuvables.

Pour compléter notre étude, nous allons aborder dans ce qui suit l'aspect commercial en évaluant le coût de réalisation de notre système, son prix de revient ainsi que ses qualités par rapport à quelques systèmes commercialisés sur le marché libanais.

2. Coût matériel de notre système.

Construit autour d'un microcontrôleur « PIC18F4620 », le prototype de notre système comporte les périphériques et les composants donnés dans les tables 11 et 12.

2.1. Le module central:

Composants	Quantité	Prix d'unité \$	Coût estimé \$
PIC18F4620	1	10	10
Clavier	1	4	4
Mémoire SD	1	20	20
GLCD	1	25	25
MT8889	1	10	10
MCP23S17	2	4	8
LM 386	1	5	5
Max485	1	3	3
Transformateur	1	3	3
Pont diodes	1	0.5	0.5
Régulateur	3	1	3
Circuit imprimé	1	10	10
Quartz	2	1	2
Transistors 2n2222	18	0.1	1.8
Autres			4
Total			120 \$

Table 12: Coût estimé des composants du module central.

2.2. La carte de contrôle d'accès :

Composants	Quantité	Prix d'unité \$	Coût estimé \$
PIC18F4620	1	10	10
Clavier	1	4	4
LCD 2 lignes	1	10	10
Max485	1	3	3
Transformateur	1	3	3
Régulateur	1	1	1
Circuit imprimé	1	5	5
Quartz	1	1	1
Relais	1	1	1
Autres			2
Total			40\$

Table 13 : Coût estimé des composants de la carte de contrôle d'accès.

Le coût matériel de ce prototype (Module central + 1 module de contrôle d'accès) ne doit dépasser pas 160 US\$

N'oublions pas le coût de notre travail de développement logiciel ainsi que le coût de la main d'œuvre de réalisation. Tenant compte de tous ces aspects, nous pensons que, dans un objectif commercial, le prix de revient de notre système ne doit pas dépasser les 300 US\$.

3. Qualités et défauts

Il est vrai que le système, tel que nous l'avons décrit, souffre des points faibles qui limitent, selon l'environnement dans lequel il serait utilisé, sa compétitivité vis-à-vis d'autres systèmes de haut de gamme.

Parmi ces points faibles, nous citons:

- La méthode d'appel étant basée sur la ligne téléphonique, une panne de celle ligne, pour n'importe quelle raison, rend le système incapable de prévenir les autorités compétentes, ce qui prive le système de l'un ses points forts.
- Le système doit avoir un journal (log file), pour garder une trace de l'ensemble des événements.
- Le système n'est pas accessible via l'internet.

Malgré ceci, ce système a plusieurs points forts qui lui permettent de se distinguer de nombreux systèmes commercialisés sur le marché. Parmi ces qualités nous citons :

- Son autonomie: le système fonctionne indépendamment d'un ordinateur-hôte.
- Microcontrôleur programmable sur place, sans besoin de le détacher du circuit.
- Temps de réponse très court (moins d'une seconde)
- Utilisation d'une mémoire SD allant jusqu'à 2 MO, pour sauvegarder les messages vocaux, d'où pas de limitation pour ces messages.
- Détection et localisation des zones en cas d'alarme.
- Affichage sur écran graphique a cristaux liquide pour toutes les situations.
- Facile à configurer, comme il utilise un écran graphique pour afficher les résultats et le menu.
- Système facilement extensible : Plus d'une centaine de zones peut être surveillée 100, et le nombre de modules d'accès pouvant aller jusqu'à 32.
- Utilisation du protocole RS485 pour la connexion distante des modules du système de contrôle d'accès.
- Dispositif à prix abordable.

La plupart de ces qualités sont identifiées en comparant notre système aux systèmes existants sur le marché libanais et dont nous présentons quelques-uns dans le paragraphe suivant.

4. Systèmes du marché

Un tour effectué chez les principaux distributeurs de ce type de produit sur le marché libanais et en ligne via les sites internet, nous a permis d'avoir une idée assez globale du matériel existant actuellement dans le domaine des système de surveillance. Ce que nous avons constaté peut être résumé comme suit:

a. Selon le prix :

Les systèmes de surveillance du marché sont relativement chers, malgré qu'ils soient, pour la plupart, non accompagnés d'un système de contrôle d'accès.

Le système de surveillance sans système d'accès le moins cher (environ 360 US\$) du marché se contente de 16 capteurs, et la limitation du message

vocale pour 60 seconde pour 4 messages au maximum et 4 numéros de téléphone.

Le plus cher (de l'ordre de 1800\$) est capable d'accepter jusqu'à 40 détecteurs, et supporte 48 messages vocaux. Un écran LCD 2 lignes pour l'affichage, et peut être programmé via téléphone.

b. Selon la fonctionnalité :

Nous considérons ici, 3 types de systèmes qui sont classés parmi les meilleurs sur le marché, et pour lesquels nous allons citer les principales caractéristiques fonctionnelles:

➤ Sensaphone Model FGD 6700 Express II (figure 35) :

Offre un ensemble complet de surveillance et de contrôle, ainsi que des options d'expansion de sorte que vous pouvez personnaliser le système pour vos besoins spécifiques ou ajouter à mesure que vos applications se développent.



Figure 35: Sensaphone Model FGD 6700 Express II

Ce système de surveillance et de contrôle dispose de :

- 8 entrées configurables
- 32 canaux supplémentaires d'entrée / sortie d'expansion
- Système anti coupure d'électricité, volume sonore ajustable
- Relais de sortie pour commutation manuelle ou automatique
- Enregistrement vocal numérique permettant à l'utilisateur d'enregistrement personnalisé des messages d'entrée.
- Accès complet de programmation en utilisant le clavier local ou à distance via téléphone à clavier.
- Possibilité de composer jusqu'à 48 numéros programmables par l'utilisateur.
- Alarme à numérotations spécifiques et des listes téléphoniques permettant à l'utilisateur de personnaliser le processus de numérotation.

- Face avant LCD et LED indiquent l'état d'entrée pour le personnel sur place

Son prix est de l'ordre 1800 \$.

Référence : [14]

➤ TEKNIM VAP-416 M ALARM PANEL (figure 36):

Ce système d'alarme est muni de 16 entrées, et peut être étendu pour supporter 16 entrées en plus, il a besoin d'un clavier et d'un module pour la ligne téléphonique.



Figure 36: VAP-416 M ALARM PANEL

- 16 zones, extensible à 32 zones
- 4 Raccordement numériques de clavier.
- Armer /désarmer,
- Panneau de contrôle et les sorties à distance par téléphone
- Technologie intelligente pour division, en utilisant chaque division comme des systèmes indépendants.
- Appel à deux stations centrales avec des numéros secondaires
- 8 utilisateurs, 4 Téléphone central
- Mémoire de 256 lignes des événements avec date et heure d'information
- 3 sorties programmables peut être augmentée à 8 sorties
- 1 sortie sirène

Son prix est de l'ordre 500 \$.

Référence : [15]

➤ ELMO NET432 (figure 37) :

Unité de contrôle à microprocesseur comportant la fonction d'assistance à distance, 4 zones équilibrées extensibles à 8 (à 32 avec max 3 concentrateurs River), sortie de relais pour intrusion et alarme d'autoprotection des dispositifs de contrôle:

- Clavier,
- 2 Zones programmables pour détecteurs,
- Transmetteur téléphonique multifonction avec la voix / mode de fonctionnement des données (FSK V21),
- Le contrôle de 10 codes utilisateur et de 4 partitions.
- Alimentation secteur AC230V de 14,5 V/1.5A

Son prix est de l'ordre 800 \$.

Référence : [16]

5. Table comparative entre notre système et les systèmes présentés ci-dessus

Caractéristique	Notre Système	Sensaphone FGD 6700	TEKNIM VAP-416 M	ELMO NET432
Alarme intrusion	✓	✓	✓	✓
Alarme Incendie	✓	✓	✓	✓
Alarme d'accès	✓	X	X	X
RS485	✓	X	X	X
Nombres d'entrées Max	104 + 32	40	32	32
Affichage	GLCD	LCD	LED	LED
Nombres de message vocaux	illimité	48	8	2
Autonomie	✓	✓	✓	✓
Aspect	Commercial	Commercial	Commercial	Commercial
Microcontrôleur programmable sur place	✓	X	X	X
Prix	300 US\$	1800US\$	500 US\$	800 US\$

Table 14: Tableau comparatif entre les systèmes



Figure 37: ELMO NET432

6. Conclusion

Finalement, nous constatons que le système de surveillance et contrôle d'accès que nous avons développé assure une bonne performance avec un prix abordable comparé aux systèmes qui existent sur le marché, et offre une flexibilité d'extension facile, et un système d'accès intégré unique et de ce point de vue, il peut être compétitif si on souhaite le commercialiser.

Conclusion

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.

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 agit 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:

En termes de qualité et de prix, ce système assure une bonne performance comparée à d'autres types présents sur le marché tout en gardant un coût de fabrication très abordable. Ceci nous permet d'envisager sa commercialisation sur le marché libanais.

De même, une extension du système reste envisageable afin :

- ✓ d'offrir une alternative pour la ligne téléphonique.
- ✓ De créer un fichier pour enregistrer tout changement de n'importe quel

capteur ou détecteur et surtout les modules d'accès, afin d'avoir une référence gardée sur la carte mémoire.

- ✓ D'utiliser le transmetteur récepteur mt8889c comme récepteur d'où la possibilité de commander le système à travers la ligne téléphonique, après avoir entré le code de sécurité.
- ✓ D'installer une interface USB pour connecter un ordinateur, pour lire et écrire sur la carte mémoire sans avoir à la détacher.
- ✓ De connecter le système sur internet.

Bibliographie

- [1] Catalogue LEGRAND France pour L'année 2010
- [2] 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
- [3] <http://elec4you.blogspot.com/2009/05/alarme-telephonique-base-du-pic16f84a.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
- [12] <http://www.cadsoft.de/> Titre: Eagle PCB Help, auteur : Eagle cadsoft
- [14] <http://www.alarms247.com/sensaphone-expressii.aspx> , Titre : FGD6700 - Sensaphone Express II , Auteur : Sensaphone
- [15] <http://www.teknim.com/UrunDetay.asp?ID=13> , Titre : VAP-416 M ALARM PANEL, Auteur : teknim
- [16] <http://www.elmospa.com/products.aspx?item=NET432> , Titre : INTRUSION DETECTION, Auteur : Elmo

Annexe

