REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE M'HAMED BOUGARA-BOUMERDES

# Faculté de Technologie

## Département Ingénierie des Systèmes Electriques

## Mémoire de Master

Présenté par

**KHELIFI Yazid**

**RAHMOUNI Abderrahim**

**Filière :** Electronique

**Spécialité :** Electronique des Systèmes Embarqués

---

# *Système de surveillance à distance et de contrôle d'accès avec intégration de l'internet des objets*

---

**Soutenu le 03 /07/2024 devant le jury composé de:**

| | | | | |
|---|---|---|---|---|
| Kessassia | Karima | MCA | UMMB | Présidente |
| Riache | Samah | MCB | UMMB | Examinatrice |
| Kaouane | Mohamed | MCA | UMMB | Encadrant |

**Année Universitaire : 2023/2024**

# Dédicaces

Ce travail, et bien au-delà, je le dois à mes très chers parents qui mon élevés, soutenus et qui se sont sacrifiés pour moi tout au long de leur vies.

A mon frère Hakim et ma petite sœur Ines.

Je remercie infiniment mes cousins pour avoir cru en moi et pour m'avoir soutenu tout au long de mon projet.

Je remercie aussi toute ma famille grands parents, oncles, cousins et cousines pour leurs soutiens apportés chaque jour.

À mes très chers amis Samir et Mehdi pour leurs aides.

Je remercie également tous mes amis qui ont toujours été là pour moi et qui m'ont toujours apporté leurs aides et encouragement.

Je dédie ce travail à la mémoire de mon grand-père, Amar.

**KHELIFI Yazid**

# Dédicaces

Ce travail, et bien au-delà, je le dois à mes très chers parents qui mon élevés, soutenus et qui se sont sacrifiés pour moi tout au long de leur vies.

A mon frère Imed Eddine, Abdelghani et ma petite sœur Meriem

Je remercie infiniment mes chers parents pour avoir cru en moi et pour m'avoir soutenu tout au long de mon projet.

Je remercie aussi toute ma famille grands parents, oncles, cousins et cousines pour leurs soutiens apportés chaque jour. A mes très chers amis pour leurs aides.

Je remercie également tous mes amis qui ont toujours été là pour moi et qui m'ont toujours apporté leurs aides et encouragement.

**RAHMOUNI Abderrahim**

# Remerciement

Nous remercions énormément notre encadreur Monsieur M.KAOUANE, pour toute l'aide déterminante et l'intérêt qu'il nous a apporté tout au long de ce mémoire de fin d'étude, qu'il trouve ici notre profonde gratitude et toute notre reconnaissance et notre respect.

On tient à remercier aussi Monsieur N.MESSAOUDI pour tout son aide, sa disponibilité et ça générosité qui nous a permis de réalisée ce travail.

Nous témoignons notre gratitude à nos chers parents et à toutes les personnes ayant contribué de près ou de loin à la réalisation de ce travail et sans qui nous aurions jamais pu arriver à sa finalisation.

A nos amis (nos collègues du l'université) qui par leurs encouragements, on a pu surmonter tous les obstacles, et on a travaillé avec une ambiance enrichissant.

# Résumé

Au cours de ce mémoire, nous avons conçu et réalisé un système de surveillance intelligent pour une maison en utilisant une carte Raspberry Pi Pico pour la collecte des données. Notre système intègre un capteur de mouvement PIR, la technologie RFID et une caméra ESP32CAM connectée au WiFi. Les données sont accessibles en temps réel via une interface web hébergée sur un serveur dédié, incluant un journal d'événements avec des photos capturées lors de détections de mouvement ou d'erreurs d'identification RFID.

Ce projet reflète notre engagement à améliorer la sécurité résidentielle en utilisant une technologie robuste et accessible. La combinaison du capteur PIR pour la détection de mouvement et de la RFID pour l'identification offre une surveillance proactive et précise. La caméra ESP32CAM enrichit l'expérience en permettant la visualisation en temps réel et la capture d'images cruciales.

**Mots clés :**
Raspberry Pi Pico, vidéosurveillance, RFID, PIR, ESP32CAM.

# Abstract

During this thesis, we designed and implemented an intelligent surveillance system for a house using a Raspberry Pi Pico board for data collection. Our system integrates a PIR motion sensor, RFID technology, and an ESP32CAM camera connected via WiFi. Data is accessible in real-time through a web interface hosted on a dedicated server, including an event log with photos captured during motion detection or RFID identification errors.

This project reflects our commitment to enhancing residential security using robust and accessible technology. The combination of the PIR sensor for motion detection and RFID for identification provides proactive and precise surveillance. The ESP32CAM camera enhances the experience by enabling real-time visualization and capture of crucial images.

**Keywords:**
Raspberry Pi Pico, video surveillance, RFID, PIR, ESP32CAM.

# ملخص

خلال هذه الرسالة، قمنا بتصميم وتنفيذ نظام مراقبة ذكي لمنزل باستخدام بطاقة Raspberry Pi Pico لجمع البيانات. يدمج نظامنا مستشعر الحركةPIR ، وتكنولوجياRFID ، وكاميرا ESP32CAM المتصلة عبر WiFi. يمكن الوصول إلى البيانات في الوقت الحقيقي من خلال واجهة ويب مستضافة على خادم مخصص، بما في ذلك سجل الأحداث مع الصور الملتقطة أثناء اكتشاف الحركة أو أخطاء تحديد الهوية .RFID يعكس هذا المشروع التزامنا بتعزيز الأمن السكني باستخدام تكنولوجيا قوية ومتاحة. تجمع مزيج من مستشعر PIR لاكتشاف الحركة وتقنية RFID للتعرف على هوية الأشخاص على مراقبة نشطة ودقيقة. تعزز كاميرا ESP32CAM الخبرة بتمكين التصور في الوقت الحقيقي والتقاط الصور الحاسمة.

**الكلمات المفتاحية:**

Raspberry Pi Pico، مراقبة الفيديو، RFID، PIR، ESP32CAM

# Table des matières

**Dédicaces** .....

**Dédicaces** .....

**Remerciement** .....

**Résumé** ..... i

**Abstract** ..... i

**ملخص** ..... ii

**Liste des abréviations** ..... iii

**Liste des tableaux** ..... v

**Liste des figures** ..... vi

**Introduction générale** ..... 1

**Chapitre I : Généralités sur la vidéosurveillance** ..... 3

*I.1. Introduction* ..... *4*

*I.2. Principe de fonctionnement d'un système de vidéosurveillance* ..... *4*

*I.3. Les domaines d'application de la vidéosurveillance* ..... *4*

I.3.1. Contrôle et gestion de la circulation automobile ..... 5

I.3.2. Domaines industriels ..... 5

I.3.3. Domaines commerciaux ..... 5

I.3.4. Domaines médicaux ..... 5

*I.4. Les Composants essentiels d'un système de vidéosurveillance* ..... *5*

I.4.1. Caméras ..... 5

I.4.2. Moniteur ..... 5

I.4.3. Alarme ..... 6

I.4.4. Enregistreur de vidéosurveillance ..... 6

*I.5. Apparition des systèmes de vidéosurveillance* ..... *6*

*I.6. Évolution des systèmes de vidéosurveillance* ..... *6*

I.6.1. Système de vidéosurveillance classique CCTV ..... 7

I.6.2. Système de vidéosurveillance analogique avec magnétoscopes traditionnels ..... 7

I.6.3 Système de vidéosurveillance analogique avec enregistreur numérique ..... 8

I.6.4 Système de vidéosurveillance analogique avec enregistreur numérique réseau ..... 9

I.6.5 Système de vidéosurveillance sur IP avec serveur vidéo ..... 9
I.6.6 Système de vidéosurveillance sur IP avec caméras réseau ..... 10
I.6.7. Réseau sans fil ..... 10

*I.7. Intégration de l'intelligence artificielle dans les caméras de surveillance ..... 11*
I.7.1. Avantages de l'intégration de l'IA ..... 11
I.7.2 Utilisation des caméras de surveillance dotées d'IA ..... 13

*I.8. Les avantages de la vidéosurveillance dans les lieux publics ..... 14*
I.8.1. Dissuasion de la criminalité ..... 14
I.8.2. Aide à l'enquête criminelle ..... 14
I.8.3. Renforcement de la sécurité publique ..... 14
I.8.4. Gestion efficace des foules ..... 14
I.8.5. Prévention des actes de vandalisme ..... 14
I.8.6. Utilisation dans la gestion du trafic ..... 14

*I.9. Inconvénients de la vidéosurveillance ..... 15*
I.9.1. Problèmes de vie privée ..... 15
I.9.2. Questions juridiques et éthiques ..... 15
I.9.3. Limitations techniques ..... 16

*I.10. Difficultés et problématiques de la vidéosurveillance ..... 16*
I.10.1 Contraintes techniques ..... 16
I.10.2. Contraintes environnementales ..... 16
I.10.3. Contraintes sémantiques ..... 16

**Chapitre II: Conception matérielle du système de surveillance ..... 18**

*II.1. Introduction ..... 19*

*Dans ce chapitre, nous allons détailler la conception matérielle du système de surveillance à distance et de contrôle d'accès intégrant l'internet des objets. Chaque composant sélectionné pour ses caractéristiques spécifiques joue un rôle essentiel dans la mise en œuvre d'un système fonctionnel. ..... 19*

*II.2. Description du système de surveillance ..... 19*

*II.3. Unités de traitement et de communication ..... 21*
II.3.1. Carte de traitement ..... 21
II.3.1.2 Broches GPIO ..... 22
II.3.2. ESP32CAM ..... 24
II.3.2.1 Caractéristiques principales de L'ESP32-CAM ..... 25
II.3.2.2 Carte mémoire SD ..... 25
II.3.3. ATmega328 ..... 25
II.3.4. Module radio NRF24L01 ..... 27

*II.4. Unités de capteurs ..... 27*
II.4.1. Capteur de mouvement PIR ..... 27
II.4.2. Module RFID (Radio-Frequency Identification) ..... 28
II.4.3. Capteur à interrupteur magnétique de porte ..... 29

*II.5. Unité d'actionneurs (Relais et serrure électrique) ..... 29*

*II.6. Horloge en temps réel ..... 30*

*II.7. Bouton poussoir ..... 31*

*II.8 Partie de signalisation* ..... *31*
II.8.1. LED ..... 31
II.8.2. Buzzer ..... 31
*II.9. Partie d'affichage* ..... *32*
II.9.1. Écran TFT 1,77 pouces ..... 32
II.9.2. LCD 1602 (Liquid Crystal Display 1602) ..... 33
*II.10. Coût du Projet* ..... *34*
*II.11. Conclusion* ..... *36*
**Chapitre III : Conception logicielle du système de surveillance ..... 37**
*III.1 Introduction* ..... *38*
*III.2. Configuration de l'unité de traitement* ..... *38*
III.2.1 Sélection et installation de l'interpréteur ..... 38
*III.3. Configuration ESP32CAM* ..... *41*
III.3.1 Préparation de l'IDE Arduino ..... 41
III.3.2 Configuration matérielle ..... 43
III.3.3 Configuration de l'ESP32-CAM dans l'IDE Arduino ..... 43
III.3.4 Téléversement du Code ..... 44
III.3.5 Bibliothèque pour l'ESP32-CAM ..... 44
*III.4. Configuration des deux Atmega 328P (A et B)* ..... *46*
*III.5. Création du serveur web* ..... *49*
*III.6. Conception du serveur web* ..... *51*
*III.7. Conclusion* ..... *54*
**Chapitre IV : Tests pratiques et résultats ..... 55**
*IV.1. Introduction* ..... *56*
*IV.2. Outils pour la conception de circuits électroniques* ..... *56*
IV.2.1 Fritzing ..... 56
IV.2.2 KiCad ..... 57
IV.2.2.1 Schéma Électronique ..... 57
IV.2.2.2 Conception de PCB ..... 58
IV.2.2.3 Visualisation 3D ..... 63
*IV.3 Assemblage de la partie matérielle* ..... *65*
*IV.4 Résultats par les capteurs* ..... *66*
IV.4.1 Capteur PIR ..... 66
IV.4.2 Module RFID et serrure électrique ..... 67
IV.4.3 Capteur magnétique ..... 67
*IV.5 Interface web* ..... *67*
*IV.6. Résultats obtenu par les différents afficheurs* ..... *67*
IV.6.1 Afficheur LCD 1602 ..... 67
IV.6.2 Afficheur TFT 1.77 ..... 69

*IV.7. Analyse des résultats ..... 70*

*IV.8. Conclusion ..... 70*

**Conclusion générale ..... 71**

**Bibliographie .....**

# Liste des abréviations

ADC: Analog-to-Digital Converter

CCTV: Closed-circuit television

DC: Direct Current

DSP: Digital Signal Processor

FPGA: Field-Programmable Gate Array

GPIO: General Purpose Input/Output

GND: ground

HTML: HyperText Markup Language

IA: Intelligence Artificielle

IDE: Integrated Development Environment

I2C: Inter-Integrated Circuit

IOT: Internet of Things

IP: Internet Protocol

IOS: Input/Output System

IRA: Armée républicaine irlandaise

LAN: Local Area Network

LCD: Liquid Crystal Display

LED: Light-Emitting Diode

MP: MicroPython

NRF: Nordic Semiconductor Radio Frequency

PA: Power Amplifier

PC: Personal Computer

PCB: Printed Circuit Board

PIC: Peripheral Interface Controller

PIR: Passive infrared sensor

PWM: Pulse Width Modulation

RAM: Random Access Memory

RFID: Radio-Frequency Identification

RP Pico: Raspberry Pi

RPP: Raspberry Pi Pico

RST: Reset

RTC: Real-Time Clock

SD: Secure Digital

SPI: Serial Peripheral Interface

SRAM: Static Random Access Memory

SSID: Service Set Identifier

TFT: Thin-Film Transistor

UART: Universal Asynchronous Receiver/Transmitter

USB: Universal Serial Bus

URL: Uniform Resource Locator

VCC: voltage at the common collector

WIFI: Wireless Fidelity

WLAN: Wireless Local Area Network

# Liste des tableaux

Tableau II.1 : Caractéristiques principales de la carte Raspberry Pi Pico [17].....22
Tableau II.2 : Branchement de carte "A".....23
Tableau II.3 : Caractéristiques principales de l'ESP32-CAM.....25
Tableau II.4 : Branchement de carte "B.....26
Tableau II.5 : Spécification de l'Écran TFT 1,77 pouces [31].....32
Tableau II.6 : Spécification de l'écran LCD 1602.....34
Tableau II.7 : Spécifications techniques Carte « A » et « B ».....35
Tableau III.1 : Éléments constituant l'interface du serveur Web.....53
Tableau IV.1 : Les informations affichées sur LCD 1602.....68
Tableau IV.2 : Les informations affichées sur l'ecran TFT 1.77.....69

# Liste des figures

Figure I.1 : vidéosurveillance [1]....4
Figure I.2 : Architecture de vidéosurveillance classique CCTV....7
Figure I.3 : Architecture de vidéosurveillance analogique avec magnétoscopes traditionnels ....8
Figure I.4 : ARCHITECTURE DE VIDEOSURVEILLANCE ANALOGIQUE AVEC ENREGISTREUR NUMERIQUE ....8
Figure I.5 : ARCHITECTURE D'UN SYSTEME ANALOGIQUE AVEC ENREGISTREUR NUMERIQUE RESEAU ....9
Figure I.6 : Architecture de vidéosurveillance sur IP avec serveur vidéo....9
Figure I7 : Architecture de vidéosurveillance sur IP avec caméras réseau ....10
Figure I.8 : Architecture de réseau sans fil pour système de vidéosurveillance ....11
Figure I.9 : DETECTION DE MOUVEMENT [8]....12
Figure I.10 : Reconnaissance faciale et analyse biométrique [9]....12
Figure I.11 : Système de détection de vol à l'étalage dans un supermarché [10]....13
Figure I.12 : Système de classification d'objets [11]....13
Figure I.13 : Surveillance de masse ....15
Figure II.1 : Schéma synoptique "carte A"....20
Figure II.2 : Schéma synoptique "carte B" ....21
Figure II.3 : La carte Raspberry Pi Pico [16] ....21
Figure II.4 : ESP32-CAM [19]....24
Figure II.5 : Système de communication entre l'ATmega328 "A" et "B"....26
Figure II.6 : Module NRF24L01+PA [20]....27
Figure II.7 : Capteur de mouvement (PIR HC-SR501) [22] ....28
Figure II.8 : Module RFID RC522 [24]....28
Figure II.9 : MC-38 Capteur magnétique [26]....29
Figure II.10 : Serrure électrique....30
Figure II.11 : Module relais [27] ....30
Figure II.12 : DS1302 real-time clock (RTC) [29] ....31
Figure II.13 : Écran TFT 1,77 pouces [30]....32
Figure II.14 : Écran LCD 1602....33
Figure III.1 : Installation du Firmware MicroPython sur le Raspberry Pi Pico via Thonny....38
Figure III.2 : Sélection du MicroPython pour le Raspberry Pi Pico dans Thonny ....39
Figure III.3 : Installation de MicroPython pour le Raspberry Pi Pico via Thonny ....39
Figure III.4 : Diagramme du code téléversé sur le Raspberry Pi Pico....40
Figure III.5 : Ouverture de l'IDE et sélection des "Préférences" dans le menu "Fichier....41
Figure III.6 : Ajout de l'URL dans le champ "URL de gestionnaire de cartes supplémentaires....42
Figure III.7 : Installation du package "ESP32" via la fenêtre de recherche pour configurer l'environnement de développement....42
Figure III.8 : Sélection du type 'AI Thinker ESP32-CAM' après l'installation pour programmer notre ESP32CAM....43
Figure III.9 : AJOUT ET CONFIGURATION DES BIBLIOTHEQUES NECESSAIRES DANS L'IDE ARDUINO VIA LE MENU "CROQUIS" ....44
Figure III.10 : Diagramme de configuration de l'ESP32-CAM avec le serveur web ....45

Figure III.11 : Diagramme de code de l'ATmega A ..... 47
Figure III.12 : Diagramme de code de l'ATmega B ..... 48
Figure III.13 : L'interface web crée ..... 51
Figure IV.1 : plaques d'essai « A » ..... 56
Figure IV.2 : plaques d'essai « B » ..... 57
Figure IV.3 : Circuit de la carte "A" ..... 57
Figure IV.4 : Circuit de la carte "B" ..... 58
Figure IV.5 : Couche avant de la carte "A" ..... 58
Figure IV.6 : Couche arrière de la carte "A" ..... 59
Figure IV.7 : Couche silksceen et contour de la carte "A" ..... 59
Figure IV.8 : Plan de perçage de la carte "A" ..... 59
Figure IV.9 : Plan de perçage de la carte "A" ..... 60
Figure IV.10 : Carte PCB "A" Plan Avant et Arrière ..... 60
Figure IV.11 : Couche avant de la carte "B" ..... 61
Figure IV.12 : Couche arrière de la carte "B" ..... 61
Figure IV.13 : Couche silksceen et contour de la carte "B" ..... 61
Figure IV.14 : Plan de perçage de la carte "B" ..... 62
Figure IV.15 : Plan de perçage de la carte "B" ..... 62
Figure IV.16 : Carte PCB "B" Plan Avant et Arrière ..... 63
Figure IV.17 : Carte PCB "A" en 3D ..... 64
Figure IV.18 : Carte PCB "B" en 3D ..... 64
Figure IV.19: plaques d'essai "A" ..... 65
Figure IV.20 : plaques d'essai "B" ..... 65
Figure IV.21 : Carte PCB "A" ..... 66
Figure IV.22 : Carte PCB "B" ..... 66
Figure IV.23 : capteur d'écran l'interface web ..... 67

# Introduction générale

De nos jours, le besoin de systèmes de sécurité intelligents pour la protection des lieux et des personnes est devenu un enjeu majeur à l'échelle planétaire, entraînant un développement rapide de cette technologie. L'évolution des technologies analogiques vers le numérique pour les installations de vidéosurveillance révolutionne le marché mondial des applications vidéo, offrant des solutions de surveillance pour les logements, lieux de travail, établissements, villes, routes, etc., qui sont devenus des espaces de vie intelligents.

La vidéosurveillance, l'une des solutions de sécurité les plus anciennes et répandues, présente divers avantages, notamment en matière de sécurité publique et de protection des biens mobiliers ou immobiliers. Les caméras IP ont marqué le passage de la technologie analogique par télévision en circuit fermé (CCTV) vers les caméras numériques, fonctionnant par le biais d'un réseau informatique à l'aide de câbles ou d'un réseau wifi. Elles permettent l'installation de réseaux de vidéosurveillance avec un grand nombre de caméras, indispensables dans les lieux publics où des centaines de caméras de surveillance peuvent être déployées.

La surveillance humaine présente des limitations en raison des heures continues de surveillance, d'où l'intérêt des systèmes à caméras numériques IP conçus intelligemment pour répondre aux besoins futurs sans s'appuyer sur l'opérateur humain. L'avènement des microcontrôleurs et des systèmes embarqués à faible coût comme Arduino, Raspberry Pi, FPGA, avec leurs propres plateformes Open Source, a favorisé d'incroyables innovations et inventions électroniques qui ont changé nos vies, offrant un large espace de développement avec des possibilités d'implémentation vastes et diverses.

Dans le cadre de cette thèse de master, nous proposons l'architecture d'un système intelligent à faible coût, comprenant comme éléments intelligents la carte Raspberry Pi Pico et l'ESP32CAM. Ce système permettra la surveillance en temps réel, la réception d'alertes et la capture de photos de l'intrus à chaque de détection de mouvement ou de module RFID. Les événements enregistrés seront affichés dans une interface web permettant de visualiser le journal des événements enregistrés dans un fichier log.csv.

Ce mémoire est divisé en quatre chapitres. Le premier présente un état de l'art sur la technologie actuelle des systèmes de vidéosurveillance. Le deuxième chapitre décrit notre système à faible coût ainsi que les différentes composantes utilisées. Le troisième chapitre présente les étapes de réalisation du système, ses codes sources et ses modes de fonctionnement. Enfin, le quatrième chapitre est réservé à la description de la réalisation pratique. La conclusion générale clôture ce travail

# **Chapitre I :**
# Généralités sur la vidéosurveillance

## I.1. Introduction

La vidéosurveillance est devenue omniprésente dans notre société moderne, offrant un outil essentiel pour la sécurité et la surveillance dans une variété d'environnements, des espaces publics aux propriétés privées.

Dans ce chapitre, nous allons aborder les généralités sur la vidéosurveillance, en introduisant ces principes de fonctionnement, les domaines d'application, les composants, l'apparition et l'évolution de cette technologie, ses avantages et inconvénients, ainsi que l'intégration de l'IA dans ces systèmes.

## I.2. Principe de fonctionnement d'un système de vidéosurveillance

Un système de vidéosurveillance fonctionne en capturant des images à l'aide de caméras, qui peuvent être analogiques ou IP (Internet Protocol), et enregistre ces images sur un disque dur ou un autre type de stockage.

Les images peuvent être traitées pour améliorer leur qualité et filtrées pour supprimer les images non pertinentes. Les images enregistrées peuvent être visionnées sur un écran, un ordinateur ou un smartphone, et peuvent servir de preuve dans des situations de vol ou d'autres infractions.

**FIGURE I.1 :** VIDEOSURVEILLANCE [1]

La vidéosurveillance peut être utilisée dans des espaces publics ou privés et peut être utilisée pour des fins de sécurité publique, de contrôle du trafic, de surveillance de la criminalité, de contrôle des activités industrielles et de suivi de l'état de santé. [2]

## I.3. Les domaines d'application de la vidéosurveillance

La vidéosurveillance est largement utilisée dans divers domaines, offrant des solutions efficaces pour la sécurité, la gestion, et l'optimisation des processus. Voici quelques-uns des domaines d'application les plus courants : [3]

### I.3.1. Contrôle et gestion de la circulation automobile

La vidéosurveillance est utilisée pour le contrôle et la gestion du trafic automobile en milieu urbain et le long des axes routiers. Couplée à un centre de gestion du trafic, elle permet de dérouter la circulation, de fluidifier le trafic et d'adapter la signalisation en temps réel pour une meilleure gestion des flux de véhicules.

### I.3.2. Domaines industriels

Dans les industries, la vidéosurveillance est utilisée pour observer le matériel, les structures et les processus de production. Elle permet notamment la thermographie infrarouge, le contrôle des contraintes mécaniques et de l'état de dégradation, ainsi que l'optimisation de la sécurité et de l'efficacité des sites de production.

### I.3.3. Domaines commerciaux

Dans le secteur commercial, la vidéosurveillance est utilisée pour étudier et analyser l'activité, optimiser l'agencement des magasins, et améliorer l'expérience client. Elle offre également un aperçu instantané et dynamique des infrastructures et des sites touristiques.

### I.3.4. Domaines médicaux

En milieu médical, la vidéosurveillance est utilisée en salle d'opérations pour assister le personnel médical, permettant notamment le déport du champ opératoire pour l'anesthésiste et les infirmières. Elle est également utilisée en salle de réveil pour une surveillance permanente des patients.

## I.4. Les Composants essentiels d'un système de vidéosurveillance

L'installation d'un système de vidéosurveillance commence par une analyse minutieuse des emplacements des caméras et de la salle de contrôle. Une fois le plan établi, les caméras sont installées et connectées à la salle de contrôle via des câbles ou une connexion Wi-Fi. Les images capturées par les caméras sont transmises à un terminal, qui les affiche sur un écran. Un logiciel spécifique intégré dans le terminal permet de gérer les flux vidéo, offrant des fonctionnalités telles que la sélection des images à afficher et la configuration des préférences d'affichage.

En général, un système de vidéosurveillance de base comprend les composants suivants : [4]

### I.4.1. Caméras

Une ou plusieurs caméras filaires ou sans fil, analogiques ou IP, adaptées aux besoins spécifiques de surveillance, telles que les caméras infrarouges pour une vision nocturne ou les caméras avec détecteurs de mouvement, de chaleur, ou de fumée.

### I.4.2. Moniteur

Un écran de surveillance relié aux caméras par câble ou liaison radio, permettant de visualiser en direct les images capturées par les caméras installées dans les zones surveillées.

### I.4.3. Alarme

Une alarme connectée aux caméras, se déclenchant en cas de détection d'activité suspecte ou d'intrusion dans les zones surveillées, permettant ainsi une réaction rapide aux incidents.

### I.4.4. Enregistreur de vidéosurveillance

Un dispositif d'enregistrement numérique permettant de stocker les images capturées par les caméras. Cet enregistreur assure la conservation des données pour une analyse ultérieure ou comme preuve en cas d'incident.

## I.5. Apparition des systèmes de vidéosurveillance

La vidéosurveillance a connu un développement initial au Royaume-Uni en réaction aux attaques de l'IRA. Les premières initiatives des années 70 et 80 ont évolué vers des programmes d'envergure dans les années 1990. Ces succès ont encouragé le gouvernement à sensibiliser la population et à installer un grand nombre de caméras. Actuellement, les caméras sont largement déployées dans les centres-villes, les gares et les parkings au Royaume-Uni. Une étude a estimé qu'il y a environ 400 000 caméras à Londres et 4 000 000 au total au Royaume-Uni.

D'autres pays, comme la France, ont également adopté des systèmes de vidéosurveillance. En 1998, on recensait environ un million de caméras en France, dont 150 000 dans les lieux publics. Ces caméras sont installées dans divers endroits tels que les aéroports, les gares, les routes et les transports en commun, et commencent à se répandre dans les villes.

Les attentats du 11 septembre 2001 à New York et plus récemment ceux de juillet 2005 à Londres ont renforcé le sentiment d'insécurité dans la population. En réponse, de nombreux États ont opté pour la mise en place d'une surveillance généralisée. [5]

## I.6. Évolution des systèmes de vidéosurveillance

Les systèmes de vidéosurveillance ont évolué significativement depuis leur apparition environ 25 ans. Ils ont progressivement évolué de systèmes entièrement analogiques vers des technologies numériques. Voici une évolution des systèmes de vidéosurveillance : [6]

## I.6.1. Système de vidéosurveillance classique CCTV

Un système de vidéosurveillance CCTV classique utilise des caméras analogiques avec des sorties coaxiales qui sont reliées à un moniteur. Un opérateur doit être constamment présent devant le moniteur pour contrôler et intervenir en cas d'anomalies.

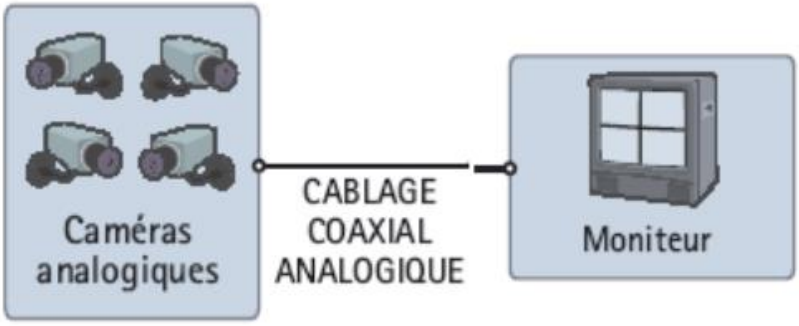



**FIGURE I.2 :** ARCHITECTURE DE VIDEOSURVEILLANCE CLASSIQUE CCTV

Les avantages de ce système sont une installation très simple et non professionnelle, ainsi qu'une manipulation des données assez simple et accessible à toute personne. Cependant, les inconvénients incluent un fonctionnement limité de la surveillance, la nécessité de réserver un opérateur pour le contrôle, l'absence d'enregistrement et l'impossibilité de déclencher la surveillance.

## I.6.2. Système de vidéosurveillance analogique avec magnétoscopes traditionnels

Ce système ancien de vidéosurveillance est encore actuellement le plus utilisé dans les entreprises, commerces et habitations de particuliers. Il est équipé d'une ou plusieurs caméras analogiques qui capturent des images et les envoyer à un enregistreur à durée limitée (type magnétoscope) par le biais d'un signal analogique, d'un moniteur (ou téléviseur) et d'un câblage (le transfert d'images se fait via un câble dit coaxial).

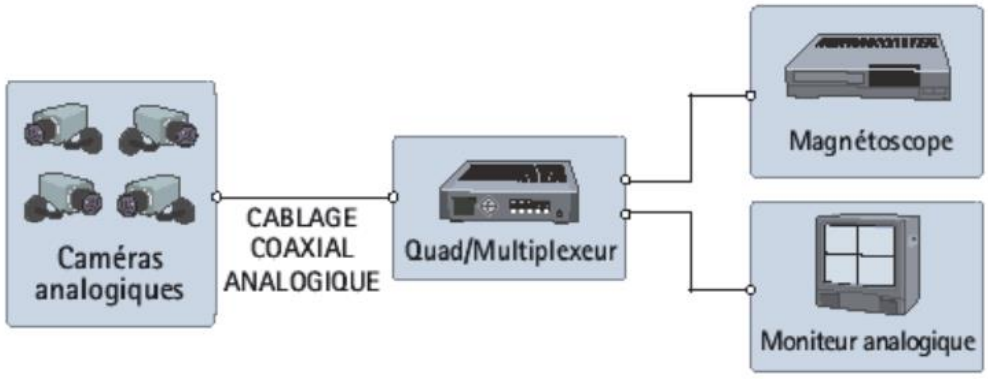



**FIGURE I.3 :** ARCHITECTURE DE VIDEOSURVEILLANCE ANALOGIQUE AVEC MAGNETOSCOPES TRADITIONNELS

Ces systèmes analogiques présentent généralement, un multiplexeur connecté entre la caméra et le moniteur, qui permet de visualiser et d'enregistrer le contenu de plusieurs caméras sur un même moniteur et magnétoscope.

## I.6.3 Système de vidéosurveillance analogique avec enregistreur numérique

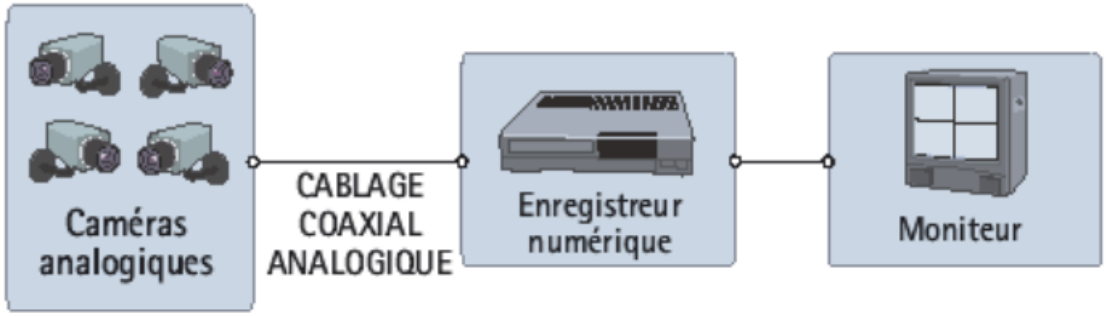



**FIGURE I.4 :** ARCHITECTURE DE VIDEOSURVEILLANCE ANALOGIQUE AVEC ENREGISTREUR NUMERIQUE

Avec un enregistreur vidéo numérique ou « digital », l'enregistrement ne se fait plus sur bandes magnétiques mais sur des disques durs où les séquences vidéo sont numérisées et compressées de telle façon à emmagasiner quotidiennement un volume important d'images.

## I.6.4 Système de vidéosurveillance analogique avec enregistreur numérique réseau

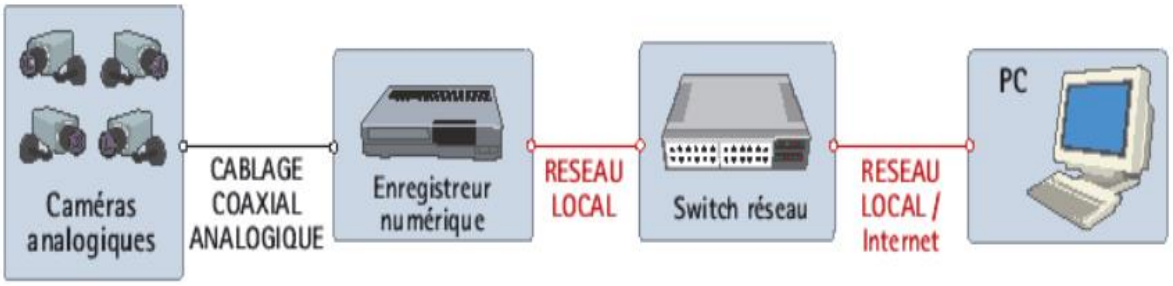



**FIGURE I.5 :** ARCHITECTURE D'UN SYSTEME ANALOGIQUE AVEC ENREGISTREUR NUMERIQUE RESEAU

C'est un système de vidéosurveillance analogique passant configurer par un enregistreur numérique en réseau par l'intermédiaire d'une connexion à travers un port Ethernet. La vidéo étant numérisée et compressée sur l'enregistreur numérique, les images sont visualisées sur PC à distance par un réseau informatique à l'aide d'un client Windows spécifique, ou simplement un navigateur web standard. Les enregistreurs numériques en réseau permettent donc la visualisation d'images vidéos à distance sur PC et le contrôle du système (de prise de vue/de la caméra) à distance.

## I.6.5 Système de vidéosurveillance sur IP avec serveur vidéo

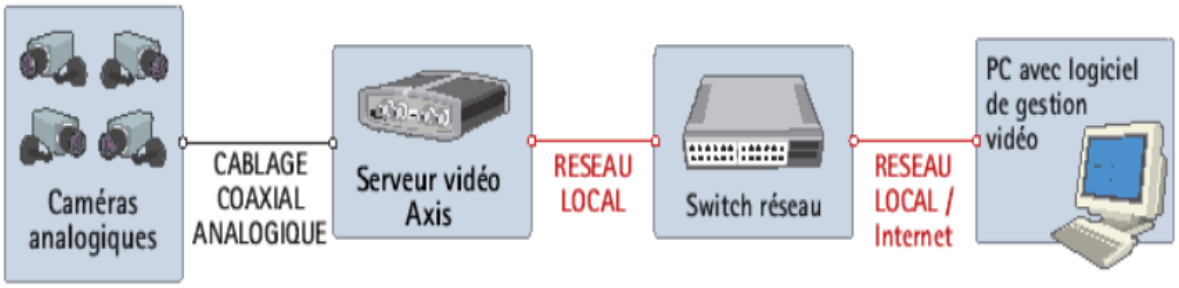



**FIGURE I.6 :** ARCHITECTURE DE VIDEOSURVEILLANCE SUR IP AVEC SERVEUR VIDEO

Les systèmes de vidéosurveillance actuels fonctionnent sur réseaux IP avec une association à un serveur vidéo qui assure la migration du système de vidéosurveillance analogique vers une solution de vidéosurveillance sur IP. Ainsi, la caméra analogique est branchée sur le serveur vidéo pour

assurer la numérisation et la compression des séquences vidéo. De son côté, le serveur vidéo est connecté sur le réseau informatique pour le transport des images vidéos vers un PC ou un serveur via un commutateur réseau. Les images vidéo sont alors enregistrées sur le disque dur du PC. Ce type de système permet l'enregistrement hors site, et de faire évoluer le système, une caméra à la fois.

### I.6.6 Système de vidéosurveillance sur IP avec caméras réseau

C'est un système entièrement numérique flexible et évolué, où les images vidéo sont transmises sur réseau IP à l'aide de caméras réseau. Une caméra réseau présente l'association d'une caméra numérique et un ordinateur, et permet la numérisation et la compression vidéo. Les images vidéo sont acheminées par réseau IP par l'intermédiaire des commutateurs réseau, pour être restituées et enregistrées sur un PC/serveur standard à l'aide d'outils de gestion vidéo.

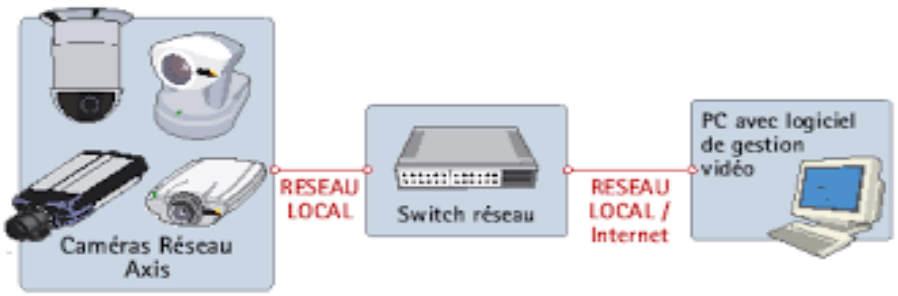



**FIGURE I.7 :** ARCHITECTURE DE VIDEOSURVEILLANCE SUR IP AVEC CAMERAS RESEAU

L'une des évolutions les plus probables de la vidéosurveillance est le rapprochement des enregistrements avec des données biométriques qui permettrait d'analyser les démarches inhabituelles des individus. De même, des recherches récentes misent sur la prévisibilité du comportement humain dans les espaces publics: un voleur ne se comporterait pas de la même façon qu'un usager. L'ordinateur peut identifier ce genre de mouvements et donner l'alerte.

### I.6.7. Réseau sans fil

Actuellement dans la plupart des bâtiments, la solution sans fil peut s'avérer la plus intéressante pour l'utilisateur, tant financièrement que sur le plan fonctionnel.

Pour le problème à certains bâtiments classés par exemple, où l'installation d'un câblage endommagerait inévitablement l'intérieur, ou à certains sites (commerces par exemple) pour lesquels la caméra doit être régulièrement déplacée et où l'on ne souhaite pas devoir tirer chaque fois de nouveaux câbles, la solution est l'utilisation courante de la technologie sans fil concerne les

bâtiments ou les sites que l'on souhaite relier sans pour autant devoir entreprendre de lourds et coûteux travaux au sol.

La technologie sans fil s'applique à la fois aux systèmes de vidéo sur IP et aux systèmes analogiques et se divise en deux catégories principales :

- LAN sans fil (Wireless LAN, ou WLAN) : définit un réseau local, c'est-à-dire sur de courtes distances et en principe à l'intérieur.

- Ponts sans fil : pour relier des bâtiments ou des sites par une liaison rapide, point à point longue distance et à grande vitesse.

Les technologies micro-ondes et laser sont couramment utilisées.

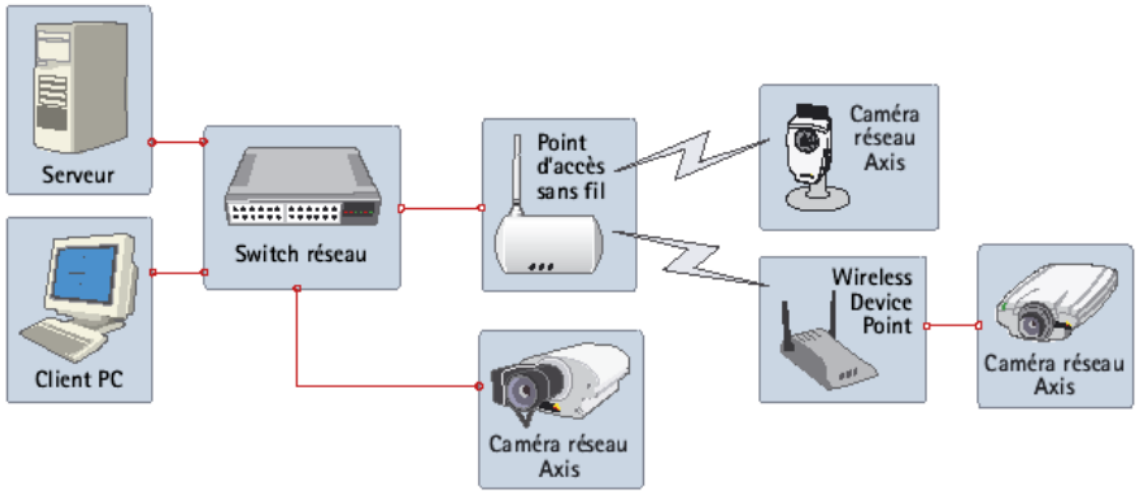



**FIGURE I.8 :** ARCHITECTURE DE RESEAU SANS FIL POUR SYSTEME DE VIDEOSURVEILLANCE

## I.7. Intégration de l'intelligence artificielle dans les caméras de surveillance

L'intégration de l'Intelligence Artificielle (IA) dans les caméras de surveillance représente une avancée majeure dans le domaine de la sécurité, offrant des capacités analytiques et une efficacité accrue par rapport aux systèmes traditionnels. Cette innovation repose sur l'utilisation de technologies avancées telles que le traitement d'image et l'apprentissage automatique pour analyser les flux vidéo en temps réel.

### I.7.1. Avantages de l'intégration de l'IA

Les caméras de surveillance intelligentes utilisent des algorithmes d'IA pour traiter et analyser les données vidéo de manière autonome, offrant plusieurs avantages significatifs : [7]

- Détection de mouvement avancée : Les caméras intelligentes peuvent distinguer les mouvements pertinents (comme une personne entrant dans une zone restreinte) des mouvements insignifiants (comme le vent soufflant dans les arbres), réduisant ainsi les fausses alertes.

**FIGURE I.9 :** DETECTION DE MOUVEMENT [8]

- Reconnaissance faciale : Grâce à l'apprentissage automatique, les caméras peuvent identifier et reconnaître les visages des individus. Cette capacité est utile pour des applications comme l'accès sécurisé et le suivi des personnes d'intérêt.

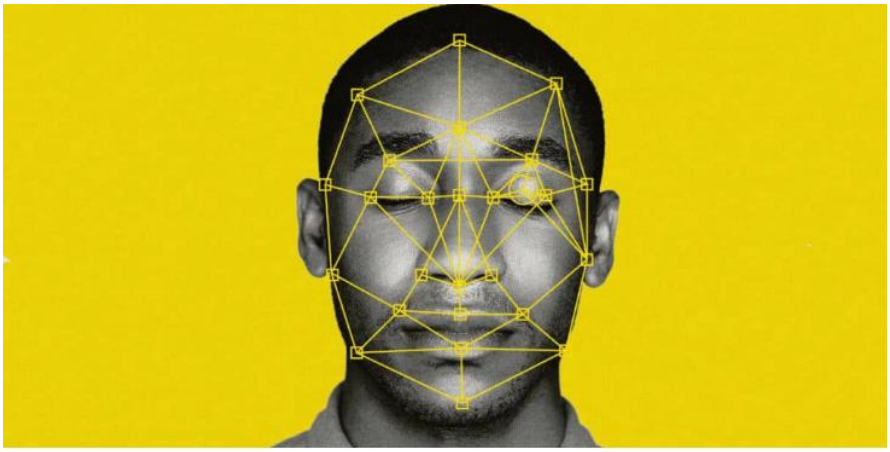


**FIGURE I.10 :** RECONNAISSANCE FACIALE ET ANALYSE BIOMETRIQUE [9]

- Analyse comportementale : Les systèmes d'IA peuvent analyser le comportement des individus pour détecter des actions suspectes ou anormales, telles que l'errance prolongée dans une zone sensible ou des comportements agressifs.

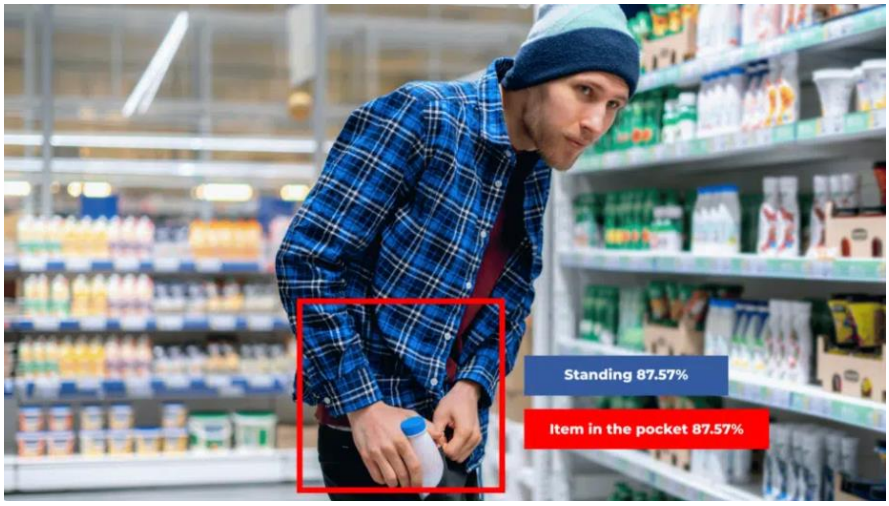



**FIGURE I.11 :** SYSTEME DE DETECTION DE VOL A L'ETALAGE DANS UN SUPERMARCHE [10]

- Classification d'objets : Les algorithmes d'IA peuvent identifier et classer différents objets (comme des véhicules, des sacs abandonnés, etc.) dans le champ de vision de la caméra, permettant une surveillance contextuelle et détaillée.

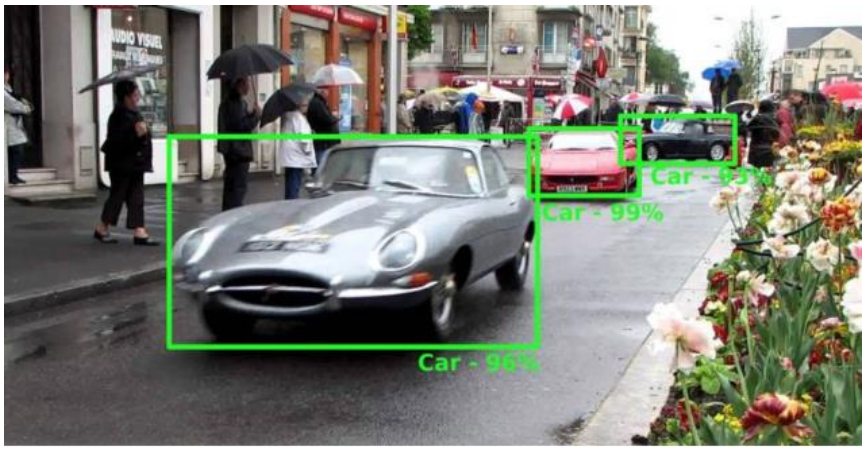



**FIGURE I.12 :** SYSTEME DE CLASSIFICATION D'OBJETS [11]

## I.7.2 Utilisation des caméras de surveillance dotées d'IA

Les caméras de surveillance dotées d'IA sont utilisées dans divers contextes pour améliorer la sécurité et l'efficacité :

- Sécurité urbaine : Les villes intelligentes utilisent des caméras d'IA pour surveiller les espaces publics, détecter les comportements suspects et réagir rapidement aux incidents.
- Sécurité des transports : Dans les gares, les aéroports et les systèmes de transport en commun, les caméras d'IA peuvent identifier les menaces potentielles, surveiller les flux de passagers et améliorer la sécurité

- Sécurité d'entreprise : Les entreprises utilisent des systèmes de surveillance intelligents pour protéger leurs installations, surveiller les activités des employés et prévenir les vols.
- Résidentiel : Les solutions de surveillance domestique intègrent l'IA pour identifier les visiteurs, surveiller les périmètres et alerter les propriétaires en cas d'activité suspecte.

## I.8. Les avantages de la vidéosurveillance dans les lieux publics

Un système de vidéosurveillance présente plusieurs avantages lorsqu'il est utilisé dans les lieux publics : [12]

### I.8.1. Dissuasion de la criminalité

La présence visible de caméras de vidéosurveillance peut dissuader les comportements criminels, offrant ainsi un environnement plus sûr pour les citoyens et contribuant à la réduction des taux de criminalité.

### I.8.2. Aide à l'enquête criminelle

Les enregistrements de vidéosurveillance fournissent des preuves essentielles pour les enquêtes criminelles, aidant à identifier les suspects, à reconstituer les événements, et à accélérer le processus d'enquête pour une justice plus rapide.

### I.8.3. Renforcement de la sécurité publique

La vidéosurveillance assure une surveillance continue des lieux publics, permettant une détection rapide des situations dangereuses, une intervention rapide en cas d'urgence, et contribuant ainsi à sauver des vies et à réduire les dommages.

### I.8.4. Gestion efficace des foules

Dans les lieux publics très fréquentés, comme les stades ou les centres commerciaux, la vidéosurveillance aide à gérer les foules en surveillant les flux de personnes, en détectant les comportements suspects et en permettant une intervention rapide pour maintenir l'ordre.

### I.8.5. Prévention des actes de vandalisme

La présence de caméras de vidéosurveillance dissuade les actes de vandalisme en identifiant les auteurs potentiels, réduisant ainsi les dommages matériels et contribuant à la préservation des biens publics.

### I.8.6. Utilisation dans la gestion du trafic

La vidéosurveillance est utilisée pour surveiller et gérer le trafic, détectant les embouteillages, surveillant les intersections, et améliorant ainsi la fluidité du trafic pour une meilleure mobilité urbaine.

## I.9. Inconvénients de la vidéosurveillance

Bien que la vidéosurveillance offre de nombreux avantages en matière de sécurité et de gestion des espaces publics et privés, elle présente également plusieurs inconvénients qu'il est important de considérer. [13]

### I.9.1. Problèmes de vie privée

1. Atteinte à la vie privée : L'un des principaux inconvénients de la vidéosurveillance est l'intrusion potentielle dans la vie privée des individus. Les caméras peuvent enregistrer des activités personnelles et quotidiennes sans le consentement des personnes filmées, ce qui soulève des préoccupations en matière de droits de l'homme et de liberté individuelle.
2. Surveillance de masse : L'installation généralisée de caméras dans les espaces publics peut conduire à une surveillance de masse, où les mouvements et les comportements de tous les citoyens sont constamment surveillés et analysés, ce qui peut être perçu comme une société de surveillance intrusive.

**FIGURE I.13 :** SURVEILLANCE DE MASSE

### I.9.2. Questions juridiques et éthiques

1. Cadre légal inadéquat : Dans de nombreux pays, la législation concernant l'utilisation de la vidéosurveillance n'est pas suffisamment développée pour protéger adéquatement les droits des individus. Il peut y avoir un manque de clarté sur qui ont accès aux enregistrements, comment les données sont stockées, et combien de temps elles sont conservées.
2. Abus potentiels : Les systèmes de vidéosurveillance peuvent être sujets à des abus, tels que la surveillance illégale, l'utilisation des images à des fins personnelles ou malveillantes, ou la manipulation des enregistrements pour accuser injustement quelqu'un.

### I.9.3. Limitations techniques

1. Coût élevé : Bien que le coût des équipements de vidéosurveillance ait diminué, l'installation, la maintenance et la mise à jour des systèmes peuvent représenter des dépenses importantes. De plus, l'intégration de technologies avancées comme l'IA peut nécessiter des investissements supplémentaires en matériel et en logiciels.
2. Failles de sécurité : Les systèmes de vidéosurveillance peuvent être vulnérables aux cyberattaques, comme le piratage ou les ransomwares. Les attaquants peuvent accéder aux flux vidéo, les manipuler ou les rendre indisponibles, compromettant ainsi la sécurité.
3. Fiabilité limitée : Les systèmes de vidéosurveillance peuvent être sujets à des pannes techniques, des erreurs de configuration, ou des interférences environnementales (comme les conditions météorologiques défavorables) qui peuvent affecter leur performance et leur fiabilité.

## I.10. Difficultés et problématiques de la vidéosurveillance

La conception et la mise en œuvre d'un système de vidéosurveillance se heurtent à plusieurs contraintes et difficultés, tant d'ordre technique qu'environnemental et sémantique : [14]

### I.10.1 Contraintes techniques

Résolution de l'image, taux de rafraîchissement de la vidéo, ajustement automatique de gain et placement des caméras sont des défis techniques à relever pour garantir la qualité et la précision des enregistrements.

### I.10.2. Contraintes environnementales

Les changements de luminosité, les conditions climatiques et la présence d'arrière-plan en mouvement sont autant de variables environnementales qui peuvent affecter la qualité des images capturées et la performance du système de vidéosurveillance.

### I.10.3. Contraintes sémantiques

La définition du contexte et la détermination de ce qui est considéré comme "normal" dans une scène donnée posent des défis sémantiques. Par exemple, la présence d'un piéton sur la route peut être considérée comme normale uniquement s'il se trouve sur un passage piéton.

Ces contraintes se traduisent par des problématiques complexes lors de l'analyse des données vidéo :

- La représentation en deux dimensions (2D) d'une scène tridimensionnelle (3D) entraîne une perte d'information relative à la profondeur, ce qui peut rendre la perception des objets dans l'image difficile et altérer la précision des mesures.

- Les conditions d'acquisition de l'image peuvent varier selon l'environnement, et les systèmes doivent être capables de s'adapter aux conditions environnementales changeantes, telles que les conditions météorologiques.
- Les occlusions, lorsqu'un objet est partiellement caché par un autre, peuvent rendre difficile l'extraction et le suivi d'objets dans la scène, nécessitant des algorithmes robustes pour gérer ces situations.
- La résolution de l'image et le taux de rafraîchissement influent sur le choix des descripteurs utilisés pour la reconnaissance ou le suivi des objets, tandis que les changements de luminosité, les conditions climatiques et la présence d'arrière-plan en mouvement posent des défis supplémentaires aux algorithmes de détection d'objets.

## I.11. Conclusion

Dans ce chapitre, nous avons abordé plusieurs notions fondamentales liées à la vidéosurveillance. Les vidéosurveillances intelligentes sont de plus en plus répandues à travers le monde, révolutionnant ainsi le domaine de la sécurité. Dans le chapitre suivant, nous aborderons la conception matérielle de notre système.

# **Chapitre** II: Conception matérielle du système de surveillance

## II.1. Introduction

Dans ce chapitre, nous allons détailler la conception matérielle du système de surveillance à distance et de contrôle d'accès intégrant l'internet des objets. Chaque composant sélectionné pour ses caractéristiques spécifiques joue un rôle essentiel dans la mise en œuvre d'un système fonctionnel.

## II.2. Description du système de surveillance

Le système se compose d'une unité de capteur, d'une carte de traitement, d'un circuit de visualisation et d'un circuit d'actionneur.

Nous allons réaliser un système de surveillance intelligente permettant d'acquérir les données de sécurité et de les transmettre vers une plateforme d'affichage.

Notre choix s'est porté sur le Raspberry Pi Pico, qui présente un ensemble d'avantages pour ce type d'acquisition. Le RP Pico, basé sur le microcontrôleur RP2040, est doté d'un processeur double cœur ARM Cortex-M0+ cadencé à 133 MHz avec 264KB de RAM. Il est relié grâce à ses différents ports d'entrées et sorties (GPIO) à l'unité de capteur, à la carte de commande et à la caméra ESP32CAM. [15]

Mais malgré cela, nous avons également rencontré un problème de manque de broches GPIO. Pour pallier ce problème, nous avons divisé notre système en deux cartes (carte A et carte B) en utilisant deux autres microcontrôleurs ATmega328, connectés via un module radio NRF24L01. Cette configuration permet une gestion optimisée et fiable des différents composants du système.

Les composants de chaque carte sont les suivants :

**A- Carte (Master)**

1) Raspberry Pi Pico (Master)
2) Module RFID RC522 + Tags
3) Capteur de mouvement (PIR HC-SR501)
4) RTC DS1302
5) Écran TFT 1,77pouces
6) RGB LED (02)
7) BUZZER
8) ATmega 328 "B"
9) Nrf24l01 module radio
10) ESP32CAM
11) Carte SD

**B- Carte (Slave)**

1) ATmega 328 "A"
2) Nrf24l01 module radio
3) MC-38 Capteur magnétique

4) Bouton poussoir (pour l'ouverture de la porte en interne)
5) Relais 5v
6) Serrure électrique
7) LCD 16x2
8) RGB LED

Les figures suivantes représentent les deux schémas synoptiques de notre système :

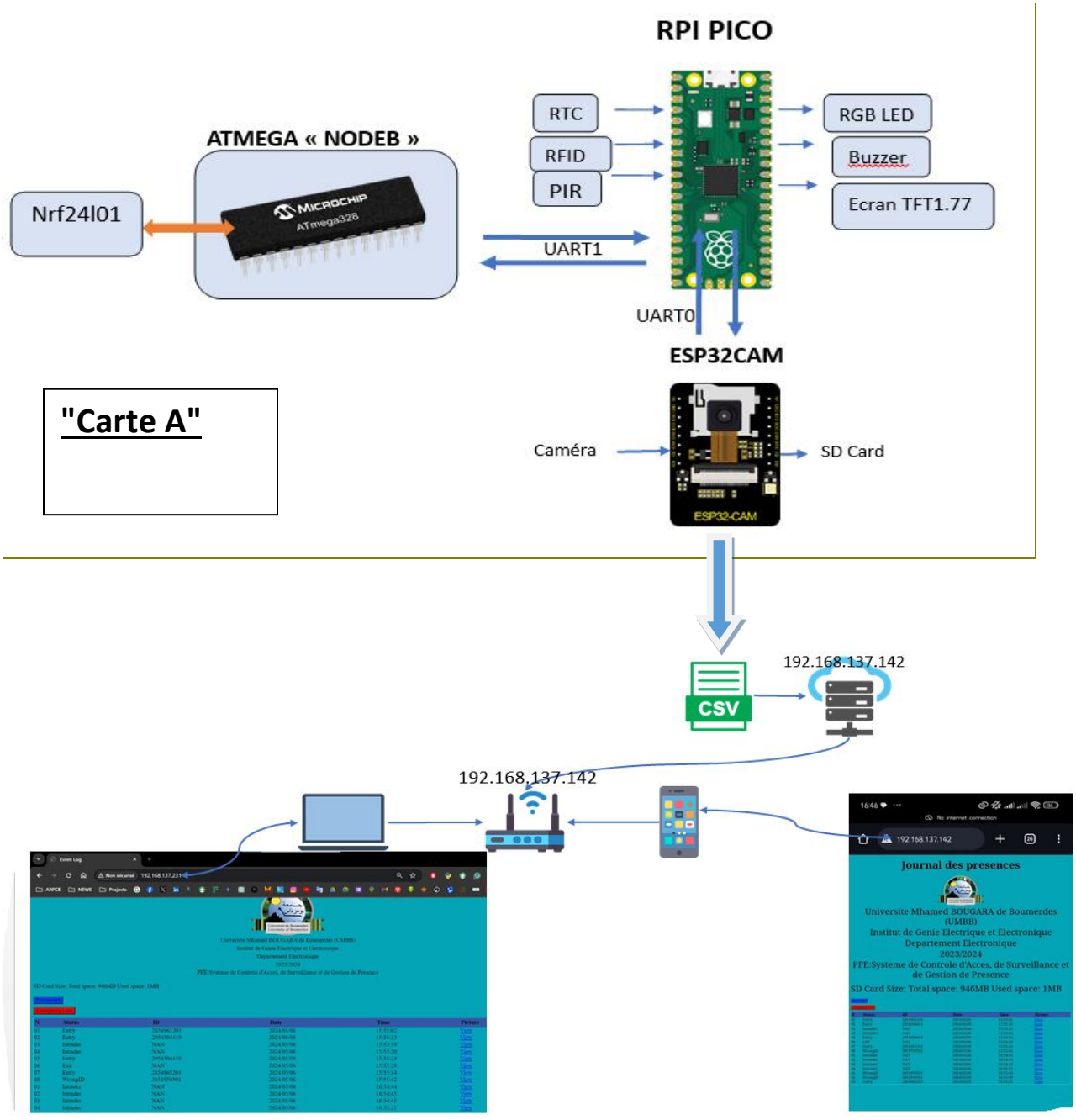



**FIGURE II.1 :** SCHEMA SYNOPTIQUE "CARTE A"

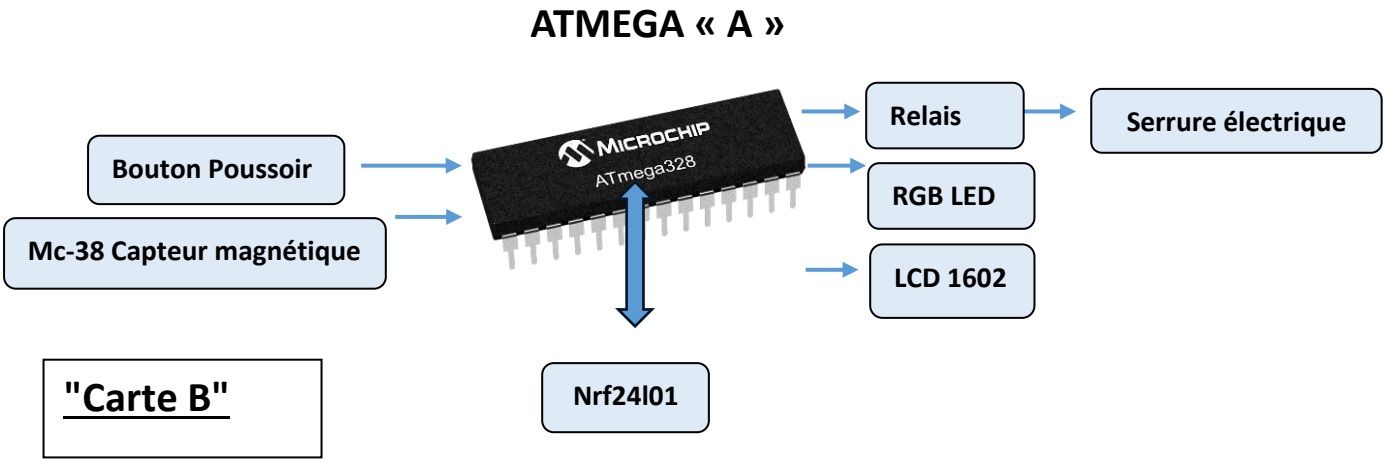



**FIGURE II.2 :** SCHEMA SYNOPTIQUE "CARTE B"

## II.3. Unités de traitement et de communication

Pour assurer une gestion efficace des différents capteurs et actionneurs, ainsi que pour faciliter la communication entre les composants du système de sécurité, nous avons intégré plusieurs unités de traitement et de communication. Ces unités sont cruciales pour le traitement des données, la coordination des actions et la transmission des informations au sein du système. Les principales unités utilisées sont le RPP, les microcontrôleurs ATmega328, l'ESP32CAM et le module radio NRF24L01. Chacune de ces unités joue un rôle spécifique et complémentaire pour garantir le bon fonctionnement du système global.

### II.3.1. Carte de traitement

Le RP Pico est au cœur de notre système de surveillance et de contrôle d'accès.

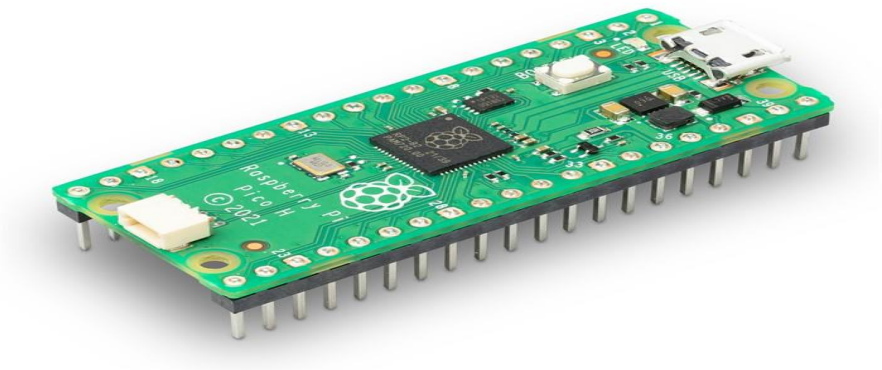


**FIGURE II.3 :** LA CARTE RASPBERRY PI PICO [16]

Le RPP collecte les données provenant des capteurs connectés, tels que le capteur PIR et le lecteur RFID. Lorsqu'un mouvement est détecté par le capteur PIR ou qu'une carte RFID est lue, il traite ces informations pour déclencher des actions appropriées, comme la capture d'images par l'ESP32CAM ou l'ouverture d'une serrure électrique. Il centralise également la gestion des communications avec les autres microcontrôleurs via le module radio NRF24L01, assurant ainsi une coordination efficace entre tous les composants du système.

### II.3.1.1 Caractéristiques principales de la carte

| Caractéristique | Description |
|---|---|
| Microcontrôleur | RP2040, conçu par Raspberry Pi |
| Processeur | ARM Cortex M0+ double cœur, horloge flexible jusqu'à 133 MHz |
| Mémoire | 264 Ko de SRAM, 2 Mo de mémoire Flash |
| E/S | 26 broches GPIO multifonctions |
| Interfaces | 2x SPI, 2x I2C, 2x UART, 3x ADC 12 bits, 16x canaux PWM contrôlables |
| Autres caractéristiques | Capteur de température, horloge et minuterie précises, bibliothèques à virgule flottante accélérées, 8x machines d'état d'entrée/sortie programmables (PIO) |
| Programmation | C/C++, MicroPython |
| Alimentation | 5V via micro-USB |
| Dimensions | 21mm x 51mm |
| Connectivité | Port micro-USB |

**TABLEAU II.1 :** CARACTERISTIQUES PRINCIPALES DE LA CARTE RASPBERRY PI PICO [17]

### II.3.1.2 Broches GPIO

Ces broches sont une interface physique entre le Pi et le monde extérieur. Sur les 40 broches, 26 sont des broches GPIO et les autres sont des broches d'alimentation ou de masse.

Ses branchements dans notre projet sont les suivants :

| N° | Composant | IN/OUTPUT PINS | Raspberry Pi Pico |
|---|---|---|---|
| **Carte « A »**Raspberry Pi Pico | | | |
| 01 | RTC DS1302 | SDA | GPIO11 |
| | | SCL | GPIO9 |
| | | RST | GPIO10 |
| | | **VCC** | **5v** |
| | | **GND** | **GND** |
| 02 | PIR HC-SR501 | Signal | GPIO3 |
| | | **VCC** | **5v** |
| | | **GND** | **GND** |
| 03 | TFT 1,77 | **LDEA** | **3.3v** |
| | | CS | GPIO21 |
| | | RS | GPIO20 |
| | | RES | GPIO22 |
| | | SDA | GPIO19 |
| | | SCK | GPIO18 |
| | | VCC | 5v |
| | | **GND** | **GND** |
| 04 | RFID RC522 | CS | GPIO5 |
| | | SCK | GPIO6 |
| | | MOSI | GPIO7 |
| | | MISO | GPIO4 |
| | | IRQ | / |
| | | RST | GPIO8 |
| | | VCC | 5v |
| | | **GND** | **GND** |
| 05 | Buzzer | Signal | GPIO12 |
| | | **GND** | **GND** |
| 06 | RGB LED | Red LED | GPIO15 |
| | | Green LED | GPIO13 |
| | | Blue LED | GPIO14 |
| | | **GND** | **GND** |
| 07 | ESP32CAM | GPIO3/RX | GPIO17/RX |
| | | GPIO1/TX | GPIO16/TX |
| | | **GND** | **GND** |
| 08 | ATmega 328P « B » | GPIO2/RX | GPIO5/RX |
| | | GPIO3/TX | GPIO4/TX |
| | | **GND** | **GND** |
| 09 | Nrf24l01 module radio | CE | D9 |
| | | CSN | D8 |
| | | SCK | D13 |
| | | MISO | D12 |
| | | MOSI | D11 |
| | | VCC | 3.3v |
| | | **GND** | **GND** |
| 10 | RGB LED | Red LED | D5 |
| | | Green LED | D6 |
| | | Blue LED | D7 |
| | | **GND** | **GND** |

**TABLEAU II.2 :** BRANCHEMENT DE CARTE "A"

## II.3.2. ESP32CAM

L'ESP32CAM est une carte basée sur le microcontrôleur ESP32, équipée d'une caméra OV2640. Ce module est capable de capturer des images et de les transmettre via une connexion WiFi. Le microcontrôleur ESP32 dispose de deux cœurs LX6, cadencés à 240 MHz, 520KB de SRAM, et intègre des interfaces de communication telles que SPI, I2C, UART, PWM, ADC, et DAC. La caméra OV2640 offre une résolution maximale de 2MP, permettant une capture d'images de haute qualité. [18]

Ce module dispose également d'un lecteur de carte SD pour enregistrer les images.

Dans notre système de sécurité, l'ESP32CAM joue un rôle crucial en assurant la surveillance visuelle. Il est responsable de la capture d'images en temps réel lorsqu'un mouvement est détecté par le capteur PIR ou lorsqu'un événement d'accès se produit. Les images capturées sont ensuite transmises via WiFi à une plateforme d'affichage ou à un serveur dédié pour être visualisées par les utilisateurs. Grâce à sa capacité de connexion WiFi, l'ESP32CAM permet une surveillance à distance, offrant aux utilisateurs la possibilité de vérifier l'état de sécurité de leur domicile ou de leur bureau en temps réel, où qu'ils se trouvent.

**FIGURE II.4 :** ESP32-CAM [19]

### II.3.2.1 Caractéristiques principales de L'ESP32-CAM

| Caractéristique | Description |
|---|---|
| Microcontrôleur | ESP32, double cœur Tensilica Xtensa LX3 à 32 bits |
| Fréquence d'horloge | Jusqu'à 240 MHz |
| Mémoire | 520 Ko de SRAM, 4 Mo de PSRAM externe |
| Connectivité sans fil | Wi-Fi 802.11 b/g/n/e/i (2,4 GHz) et Bluetooth 4.2 BLE |
| Caméra | OV2640, 2 mégapixels (MP), résolution d'image jusqu'à 1080p |
| Interfaces | SPI, I2C, UART, PWM, ADC, DAC |
| Consommation électrique | 200 mA maximum |
| Dimensions | 27 mm x 40,5 mm x 4,5 mm |
| Autres caractéristiques | Lecteur de carte Micro SD, GPIO programmables, faible consommation d'énergie |

**TABLEAU II.3 :** CARACTERISTIQUES PRINCIPALES DE L'ESP32-CAM

### II.3.2.2 Carte mémoire SD

Pour stocker les données enregistrées par le système, telles que les images capturées, nous avons utilisé une carte SD placée dans le lecteur de carte micro SD de l'ESP32CAM.

## II.3.3. ATmega328

Les microcontrôleurs ATmega328 sont utilisés pour pallier le manque de broches GPIO sur le Raspberry Pi Pico. Ils servent à gérer des tâches spécifiques, telles que le contrôle des actionneurs (comme la serrure électrique) et la communication avec les capteurs.

Connectés via le module radio NRF24L01, ils assurent une extension flexible et fiable des capacités du système principal.

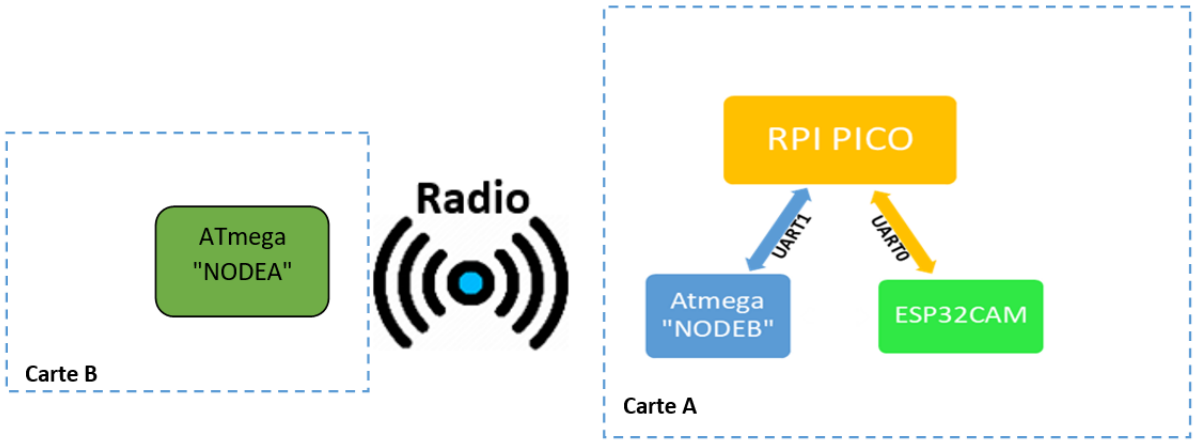



**FIGURE II.5 :** SYSTEME DE COMMUNICATION ENTRE L'ATMEGA328 "A" ET "B"

Ses branchements sont les suivants :

| N° | Composant | IN/OUTPUT PINS | Atmega 328P |
|---|---|---|---|
| **Carte « B »** ATmega 328P « A » | | | |
| 01 | Magnetic Switch MC-38 | Signal | D5 |
| | | **GND** | **GND** |
| 02 | Bouton Poussoir | Signal | D6 |
| | | **GND** | **GND** |
| 03 | Relais 5V | Signal | D7 |
| | | **VCC** | **5v** |
| | | **GND** | **GND** |
| 04 | Nrf24l01 module radio | CE | D9 |
| | | CSN | D8 |
| | | SCK | D13 |
| | | MISO | D12 |
| | | MOSI | D11 |
| | | VCC | 3.3v |
| | | **GND** | **GND** |
| 05 | RGB LED | Red LED | D3 |
| | | Green LED | D2 |
| | | Blue LED | D10 |
| | | **GND** | **GND** |
| 06 | LCD I2C | SDA | A4 |
| | | SCL | A5 |
| | | **VCC** | **5v** |
| | | **GND** | **GND** |

**TABLEAU II.4 :** BRANCHEMENT DE CARTE "B

## II.3.4. Module radio NRF24L01

Le module NRF24L01 est un choix populaire pour la communication sans fil. Il fonctionne dans la bande de fréquences ISM de 2,4 GHz et utilise la modulation GFSK pour la transmission des données. La tension de fonctionnement du module varie de 1,9 à 3,9V, et il dispose de broches logiques tolérantes à 5V.

Le module NRF24L01 est connecté à chaque microcontrôleur ATmega328 (ATmega A et ATmega B), permettant aux microcontrôleurs de s'envoyer des données et de se coordonner. Par exemple, lors de l'utilisation du badge via le module RFID sur la "Carte A", si le badge est correct, l'ATmega B envoie un signal à l'ATmega A via le module NRF24L01 pour déclencher l'ouverture de la serrure électrique contrôlée par le relais sur la "Carte B". Après que le capteur magnétique a détecté l'ouverture de la porte, l'ATmega A renvoie un signal à l'ATmega B via le module NRF24L01 pour indiquer que la porte est ouverte. Ensuite, l'ATmega B peut passer cette information au Raspberry Pi pour qu'il l'affiche dans l'écran TFT 1.77 via la "Carte A".

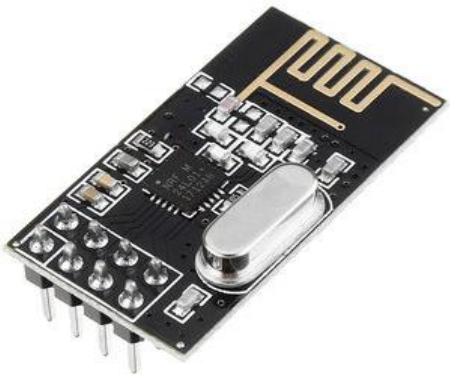


**FIGURE II.6 :** MODULE NRF24L01+PA [20]

## II.4. Unités de capteurs

Pour contrôler l'accès et la surveillance dans notre système de sécurité, nous avons utilisé différents capteurs. Les principaux capteurs utilisés sont le capteur PIR pour la détection de mouvement, le lecteur RFID pour l'identification des utilisateurs, et le capteur à interrupteur magnétique de porte pour surveiller l'état des portes.

## II.4.1. Capteur de mouvement PIR

Le capteur PIR (Passive InfraRed) détecte les mouvements en mesurant les variations de rayonnement infrarouge dans son champ de vision. Lorsqu'un corps chaud, comme un être humain, passe devant le capteur, il modifie le rayonnement infrarouge détecté, provoquant une détection de mouvement. Les capteurs PIR sont couramment utilisés pour des applications de sécurité en raison de leur sensibilité et de leur faible coût. [21]

Dans notre système de surveillance, le capteur PIR est connecté au Raspberry Pi Pico. Lorsqu'un mouvement est détecté, le capteur envoie un signal au microcontrôleur, qui déclenche alors une série d'actions, telles que la capture d'images par l'ESP32CAM et l'envoi de notifications aux utilisateurs. Le capteur PIR joue un rôle crucial dans la détection précoce des intrusions, permettant une réaction rapide du système de sécurité.

**FIGURE II.7 :** CAPTEUR DE MOUVEMENT (PIR HC-SR501) [22]

## II.4.2. Module RFID (Radio-Frequency Identification)

Pour renforcer la sécurité, nous avons intégré le capteur RFID RC522, qui fonctionne en émettant des ondes radio pour lire les informations stockées sur une puce RFID. Lorsqu'une carte ou un tag RFID est placé à proximité du capteur, celui-ci capte les données émises par la puce et les transmet au microcontrôleur pour vérification. Les systèmes RFID sont couramment utilisés pour le contrôle d'accès, car ils permettent une identification rapide et sécurisée des individus. [23]

Dans notre système, le capteur RFID RC522 est également connecté au Raspberry Pi Pico. Lorsque le capteur détecte une carte RFID, il envoie les informations au microcontrôleur, qui vérifie l'authenticité des données. Si l'identification est correcte, le système peut déclencher l'ouverture de la serrure électrique via le module de commande. Cette fonctionnalité assure un contrôle d'accès sécurisé et une gestion efficace des entrées et sorties des utilisateurs autorisés.

**FIGURE II.8 :** MODULE RFID RC522 [24]

## II.4.3. Capteur à interrupteur magnétique de porte

Le capteur à interrupteur magnétique de porte fonctionne en utilisant un aimant et un commutateur à lame souple. Lorsque la porte est fermée, l'aimant est aligné avec le capteur, maintenant le circuit fermé. Lorsque la porte est ouverte, l'aimant s'éloigne du capteur, ouvrant le circuit et déclenchant une alerte ou une action prédéfinie. Dans notre système de sécurité, le capteur à interrupteur magnétique de porte est connecté au microcontrôleur ATmega328 « A ». Lorsque la porte est ouverte, le capteur envoie un signal au microcontrôleur, qui peut alors déclencher une alerte en surveillant l'état des portes et en l'affichant sur les différents afficheurs. [25]

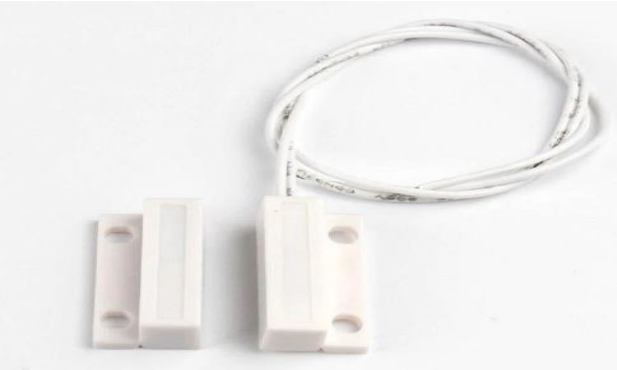


**FIGURE II.9 :** MC-38 CAPTEUR MAGNETIQUE [26]

## II.5. Unité d'actionneurs (Relais et serrure électrique)

Une serrure électrique fonctionne en utilisant un électroaimant pour verrouiller ou déverrouiller une porte. Dans notre système, le relais  joue un rôle crucial en contrôlant l'alimentation de la serrure électrique. Lorsque le relais est activé, il permet au courant électrique de passer à travers l'électroaimant de la serrure, créant ainsi un champ magnétique qui actionne le mécanisme de verrouillage. Cette configuration permet de contrôler l'accès de manière électronique et sécurisée. Les serrures électriques commandées par relais sont couramment utilisées dans les systèmes de sécurité pour offrir un contrôle d'accès pratique et fiable.

Dans notre système de sécurité, la serrure électrique est intégrée pour permettre le contrôle d'accès automatisé. Elle est connectée au microcontrôleur ATmega328 « A », qui reçoit les commandes de déverrouillage ou de verrouillage du RPP. Le relais 5V joue un rôle en gérant l'alimentation de la serrure électrique.

Lorsqu'un utilisateur est authentifié avec succès via le lecteur RFID, le RPP envoie un signal au microcontrôleur ATmega328. Ce dernier active le relais 5V, permettant au courant électrique de passer à travers l'électroaimant de la serrure, créant ainsi un champ magnétique qui actionne le mécanisme de verrouillage ou de déverrouillage, ouvrant ainsi la porte.

**FIGURE II.10 :** SERRURE ELECTRIQUE

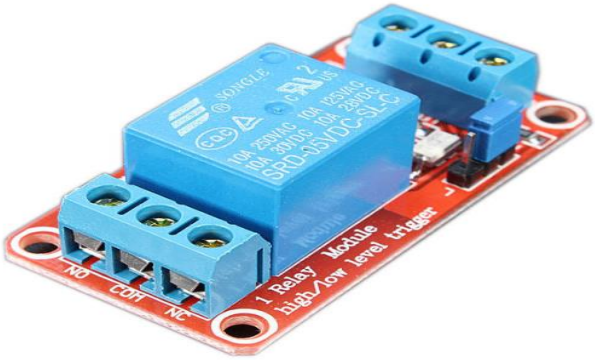



**FIGURE II.11 :** MODULE RELAIS [27]

## II.6. Horloge en temps réel

Nous allons intégrer un composant essentiel et pratique à tout système informatique : une horloge temps réel (Real-Time Clock). Une RTC permet à un système, tel que la Raspberry Pi, de maintenir en permanence l'heure de manière précise et exacte, même en l'absence de connexion Internet.

Ce module RTC est principalement constitué d'un oscillateur à quartz et d'une pile bouton de 3V, assurant ainsi que le module RTC reste alimenté même lorsque notre carte est éteinte, permettant ainsi de conserver l'heure en mémoire. Les RTC sont couramment utilisées dans les systèmes nécessitant une exécution précise des tâches selon des horaires définis, comme les ordinateurs. [28]

**FIGURE II.12 :** DS1302 REAL-TIME CLOCK (RTC) [29]

## II.7. Bouton poussoir

Pour ouvrir la porte intérieure, nous utiliserons un bouton-poussoir. Lorsqu'il est enfoncé, le microcontrôleur poussoir envoie un signal au relais 5V, qui à son tour active la serrure électrique pour ouvrir la porte.

## II.8 Partie de signalisation

La signalisation est une section cruciale de tout système, en particulier dans le domaine de sécurité. Elle fournit des informations essentielles sur l'état du système et aide les utilisateurs à prendre des décisions appropriées en fonction des conditions en cours. Dans notre projet, la signalisation comprend deux éléments principaux : la LED et le buzzer.

### II.8.1. LED

La LED est utilisée comme indicateur visuel pour les états du système

- LED rouge= danger
- LED verte= fonctionnement normal

### II.8.2. Buzzer

Le buzzer joue le rôle d'une alarme dans notre projet

- Si ça sonne = danger
- Sinon = fonctionnement normal

## II.9. Partie d'affichage

Pour fournir des informations visuelles aux utilisateurs, notre projet utilise deux types d'écrans: un écran LCD 16x2 pour l'intérieur et un écran TFT 1.77 pouces pour l'extérieur.

Chacun de ces écrans a des caractéristiques et des fonctionnalités spécifiques adaptées à leur environnement d'utilisation.

### II.9.1. Écran TFT 1,77 pouces

L'écran TFT (Thin-Film Transistor) de 1,77 pouce est un dispositif d'affichage compact et coloré, idéal pour les projets embarqués nécessitant une interface utilisateur visuelle. Il offre plusieurs avantages, notamment une résolution relativement élevée pour sa taille et la capacité d'afficher des graphiques, du texte, et des images en couleurs.

**FIGURE II.13 :** ÉCRAN TFT 1,77 POUCES [30]

Voici quelques caractéristiques techniques typiques de cet écran :

| Caractéristique | Spécification |
|---|---|
| Mode d'affichage | TFT/TN |
| Résolution | 128x160 |
| Angle de vue | 12 0'horloge |
| Connecteur | CPF |
| CI | ST7735S |
| Interface | IPS |
| Taille | 1,77 pouces |
| Mode d'affichage | TFT/TN |
| Température de fonctionnement | -20°C à 70°C |

**TABLEAU II.5 :** SPECIFICATION DE L'ÉCRAN TFT 1,77 POUCES [31]

Dans ce projet, l'écran TFT 1,77 pouces est utilisé pour afficher des informations critiques liées au contrôle d'accès et à la surveillance, telles que :

1. ACCESS_AUTORISE : Indique que l'accès a été accordé à un utilisateur valide.
2. ACCESS_REFUSE : Indique que l'accès a été refusé en raison d'un badge RFID non valide.
3. MOUVEMENT_DETECTE : Alerte lorsqu'un mouvement suspect est détecté par le capteur PIR.
4. INTRUSION : Signale une tentative d'intrusion, par exemple l'ouverture d'une porte sans badge RFID valide.
5. SORTIE : Indique que la porte a été ouverte de l'intérieur lorsque le bouton poussoir est appuyé.

## II.9.2. LCD 1602 (Liquid Crystal Display 1602)

Cet écran est un dispositif électronique utilisé pour afficher des données et des messages. Il est connu sous le nom d'écran LCD 1602. Comme son nom l'indique, il comporte 16 colonnes et 2 lignes, ce qui lui permet d'afficher 32 caractères. La couleur des caractères est blanche et l'écran a un fond bleu, ce qui le rend également lisible dans l'obscurité. Il utilise une interface parallèle pour la communication, ce qui le rend compatible avec une large gamme de microcontrôleurs. [32]

Dans ce projet, le LCD 1602 est utilisé sur la carte slave (ATmega328 A) pour afficher l'état de la porte (fermée ou ouverte).

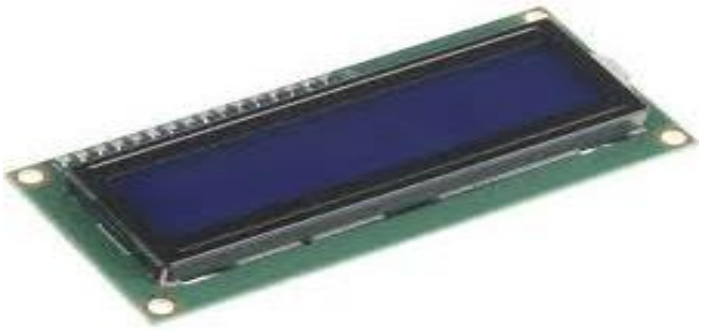


**FIGURE II.14 :** ÉCRAN LCD 1602

Voici quelques caractéristiques techniques typiques du LCD 1602 :

| Caractéristique | Spécification |
|---|---|
| Nombre de caractères | 2 lignes X 16 caractères |
| Tension | 5V CC |
| Taille du module | 80 mm x 35 mm x 11 mm |
| Taille de la zone d'affichage | 64,5 mm x 16 mm |

**TABLEAU II.6 :** SPECIFICATION DE L'ECRAN LCD 1602

Dans ce projet, le LCD 1602 est utilisé dans la carte slave (B) pour afficher l'état de la porte (fermée ou ouverte).

**Driver I2C pour LCD 1602 :** Le driver I2C pour LCD 1602 est un circuit intégré ou un module qui facilite la connexion et le contrôle du LCD 1602 à l'aide du protocole de communication I2C (Inter-Integrated Circuit). Ce driver agit comme une interface entre le microcontrôleur et le LCD, simplifiant ainsi la connexion et réduisant le nombre de broches nécessaires pour contrôler l'affichage.

## II.10. Coût du Projet

L'un des objectifs clés de ce projet était de concevoir un système de contrôle d'accès et de surveillance qui soit non seulement fonctionnel et efficace, mais également abordable. Les composants matériels sélectionnés ont été choisis en tenant compte de leur coût et de leur performance. Voici une estimation des coûts associés aux principaux composants et leurs spécifications techniques du projet :

| N° | Composant | Voltage | Consommation courant | Fréquence | Température | Communication | Dimensions | Prix |
|---|---|---|---|---|---|---|---|---|
| **Carte « A »** | | | | | | | | |
| 1. | RPI PICO | 1.8v – 5.5v | 2.5A | 133Mhz | -20°C – 85°C | UART1: Atmega B UART0 : ESP32CAM | 51x21mm | **2500 DA** |
| 2. | ESP32CAM | 5V | 2A | 160Mhz | -20°C – 85°C | UART0 : RPI PICO | 40x27mm | **2500 DA** |
| 3. | TFT 1.77 | 3.3v – 4.8v | 30mA | - | -20°C – 70°C | SPI | 55x34mm | **1950 DA** |
| 4. | PIRHC-SR501 | 5 – 20v | 65mA | - | -20°C – 85°C | Digital signal | 32x24mm | **750 DA** |
| 5. | RFID RC522 | 2.5 – 3.3v | 10 – 26mA | 13.56Mhz | -20°C – 85°C | SPI | 60x40mm | **1300 DA** |
| 6. | RTC DS1302 | 2 – 5.5v | 0.4 – 1.2mA | 32.7Khz | -0°C – 70°C | I2C | 43x23mm | **600 DA** |
| 7. | RGB LED | 2 – 3.2v | 5 – 30mA | - | -40°C – 85°C | Digital Signal (OUTPUT) | 5mm | **10 DA** |
| 8. | Buzzer | 4 – 8v | 80mA | - | -25°C – 60°C | Digital Signal (OUTPUT) | 12mm | **95 DA** |
| 9. | Atmega 328P « B » | 2.7 – 5.5v | 1.5mA | 16Mhz | -40°C – 125°C | UART1: RPI PICO Radio: ATmega A | 35x8mm | **720 DA** |
| 10. | Nrf24l01 module radio | 1.9 – 3.6v | 11.3 – 13.5mA | 2.4Ghz | -40°C – 85°C | SPI : ATmega B | 49x16mm | **450 DA** |
| **Carte « B »** | | | | | | | | |
| 1. | Atmega 328P « A » | 2.7 – 5.5v | 1.5mA | 16Mhz | -40°C – 125°C | Radio : SPI : ATmega B | 35x8mm | **720 DA** |
| 2. | Nrf24l01 module radio | 1.9 – 3.6v | 11.3 – 13.5mA | 2.4Ghz | -40°C – 85°C | SPI : ATmega A | 49x16mm | **450 DA** |
| 3. | MC-38 Door Sensor | 100v | 0.5A | - | - | Digital Signal (INPUT) | 27x14mm | **700 DA** |
| 4. | Relay 5v | 3.7 - 6v | 2 - 70mA | - | -40°C – 70°C | Digital Signal (OUTPUT) | 43x17mm | **500 DA** |
| 5. | Serrure électrique | 12v | 0.35A | - | - | Commandée par relais | 33x27mm | **1600 DA** |
| 6. | Push Button | - | - | - | - | Digital Signal (INPUT) | 12mm | **45 DA** |
| 7. | RGB LED | 2 – 3.2v | 5 – 30mA | - | -40°C – 85°C | Digital Signal (OUTPUT) | 5mm | **10 DA** |
| 8. | LCD1602 | 7v | 2.5mA | - | 0°C – 50°C | Via I2C module | 80x36mm | **850 DA** |
| 9. | LCD I2C | 2.5- 6v | | - | -20°C – 70°C | I2C | 42x19mm | **1300 DA** |

**TABLEAU II.7 :** SPECIFICATIONS TECHNIQUES CARTE « A » ET « B »

Le coût des composants est d'environ 18 000 DA, et nous avons effectué l'assemblage nous-mêmes, ce qui reste beaucoup moins cher que l'installation des systèmes traditionnels.

## II.11. Conclusion

Dans ce chapitre, nous avons détaillé la conception matérielle de notre système de surveillance à distance et de contrôle d'accès intelligent, basé sur RFID avec intégration IoT pour la gestion de présence. Nous avons exploré les différentes unités du système, notamment l'unité de traitement, l'unité de capteur, et l'unité de commande, en décrivant leurs composants et leur intégration. Dans le chapitre suivant, nous aborderons la conception logicielle de notre système, en expliquant comment programmer et configurer les divers composants pour assurer un fonctionnement harmonieux et efficace.

# **Chapitre III :**
# Conception logicielle du système de surveillance

## III.1 Introduction

Dans ce chapitre, nous allons détailler la conception logicielle de notre projet de système de surveillance. Nous commencerons par la configuration de la carte de traitement, le Raspberry Pi Pico. Ensuite, nous aborderons la configuration de l'ESP32-CAM et des deux ATmega328. Enfin, nous terminerons par la création et la description de notre serveur web pour l'affichage des données en temps réel.

## III.2. Configuration de l'unité de traitement

Nous avons choisi Thonny pour la programmation en langage MicroPython pour notre projet en raison de sa vaste disponibilité de bibliothèques adaptées à notre prototype. De plus, MP optimise l'utilisation des ressources matérielles, assurant une performance élevée et une faible consommation d'énergie.

Après avoir téléchargé et installé la dernière version de Thonny sur thonny.org, nous suivons les instructions suivant pour installer le Firmware MP spécifique au Raspberry Pi Pico :

### III.2.1 Sélection et installation de l'interpréteur

1. Ouvrez le logiciel Thonny ou l'outil que vous utilisez pour programmer en MP.
2. Accédez au menu "Outils" dans le logiciel.
3. Sélectionnez l'option "Options" ou une option similaire qui vous permet de configurer les paramètres du logiciel.
4. Dans l'onglet "Interpréteur" ou une section similaire, recherchez une option appelée "Install MP" ou similaire dans un menu déroulant.
5. Sélectionnez cette option pour installer l'interpréteur MP dans le logiciel, ce qui permettra au logiciel de communiquer avec la carte RPP ou tout autre périphérique compatible avec MP.

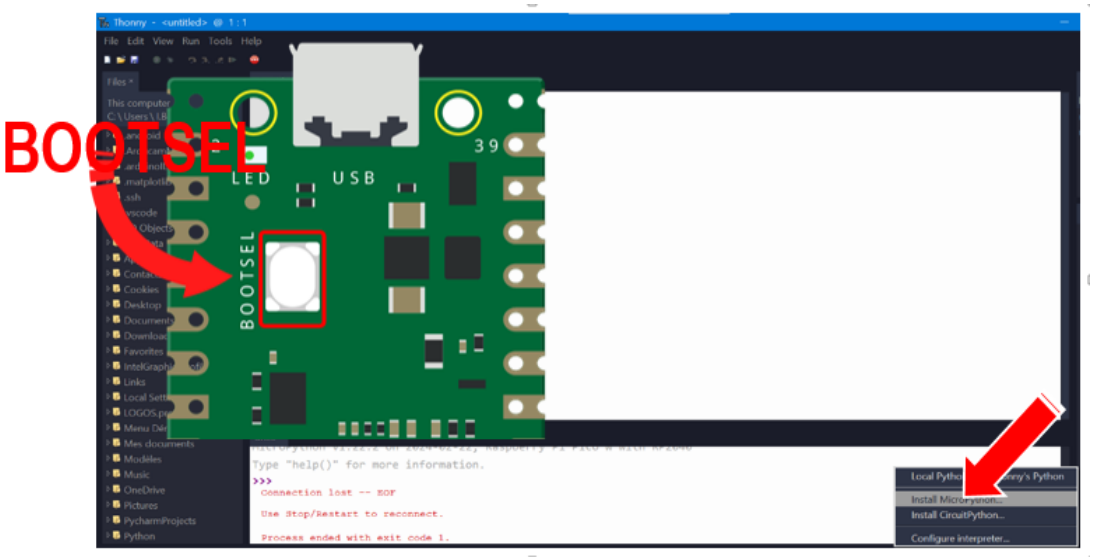



**FIGURE III.1 :** INSTALLATION DU FIRMWARE MICROPYTHON SUR LE RASPBERRY PI PICO VIA THONNY

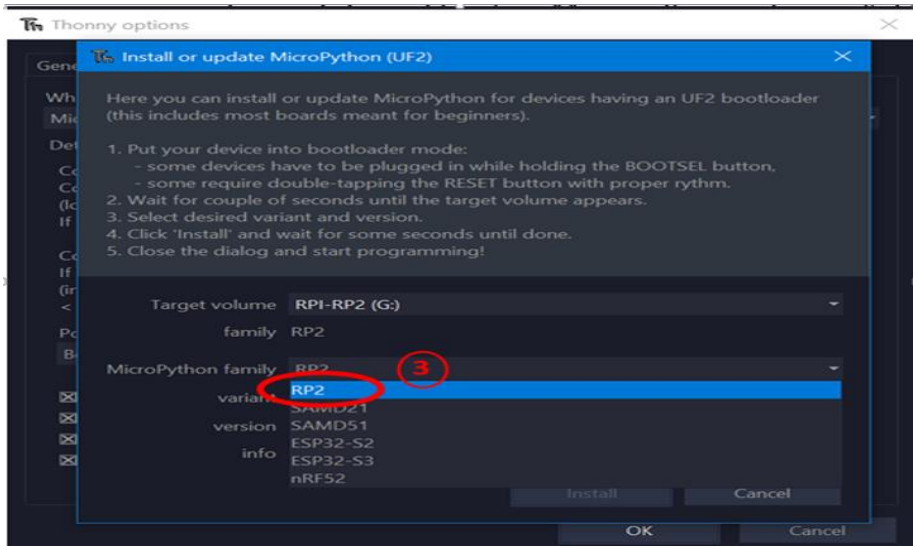



**FIGURE III.2 :** SELECTION DU MICROPYTHON POUR LE RASPBERRY PI PICO DANS THONNY

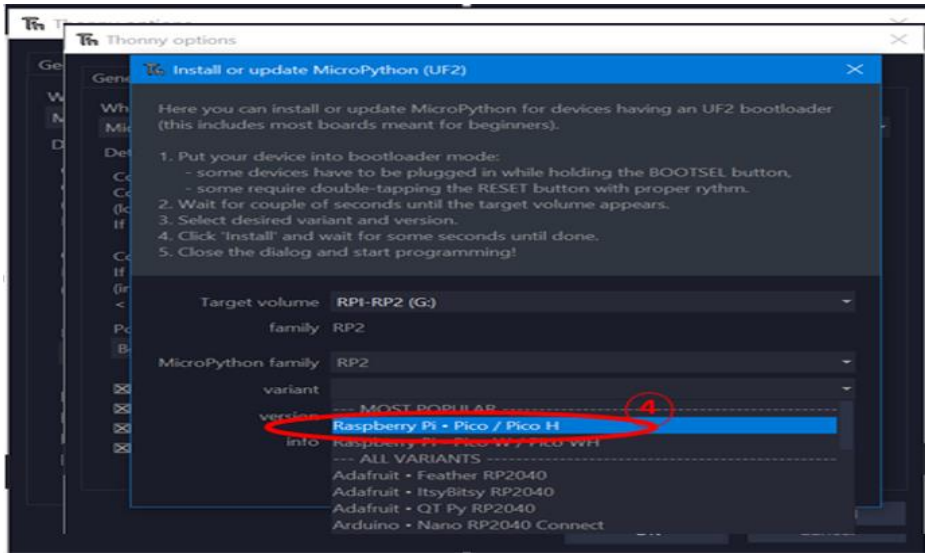



**FIGURE III.3 :** INSTALLATION DE MICROPYTHON POUR LE RASPBERRY PI PICO VIA THONNY

Après avoir sélectionné et installé l'interpréteur MP, nous pouvons commencer à écrire notre code pour la carte RPP. Voici les étapes générales que nous pourrions suivre :

1. **Configurer notre environnement de développement :** il faut que notre logiciel de programmation soit prêt à être utilisé avec MP et qu'il est connecté à notre carte RPP.
2. **Ouvrir un nouveau fichier :** Créons un nouveau fichier dans notre logiciel de programmation pour commencer à écrire notre code.
3. **Écrire notre code MicroPython :** Utilisons les bibliothèques et les fonctions de MP pour écrire le code qui réalisera les fonctionnalités que nous souhaitons pour notre projet. Nous

pouvons nous référer à la documentation de MP pour obtenir des informations sur les bibliothèques et les fonctions disponibles.

4. **Tester notre code :** Avant de transférer notre code sur notre carte RPP on doit le tester dans notre environnement de développement pour vérifier s'il fonctionne comme prévu.
5. **Transférer le code sur la carte :** Une fois que nous sommes satisfaits de notre code, nous pouvons le transférer sur notre carte RPP en utilisant les fonctionnalités de téléchargement ou de transfert de notre logiciel de programmation.

Voici le diagramme du code téléversé sur le Raspberry Pi Pico :

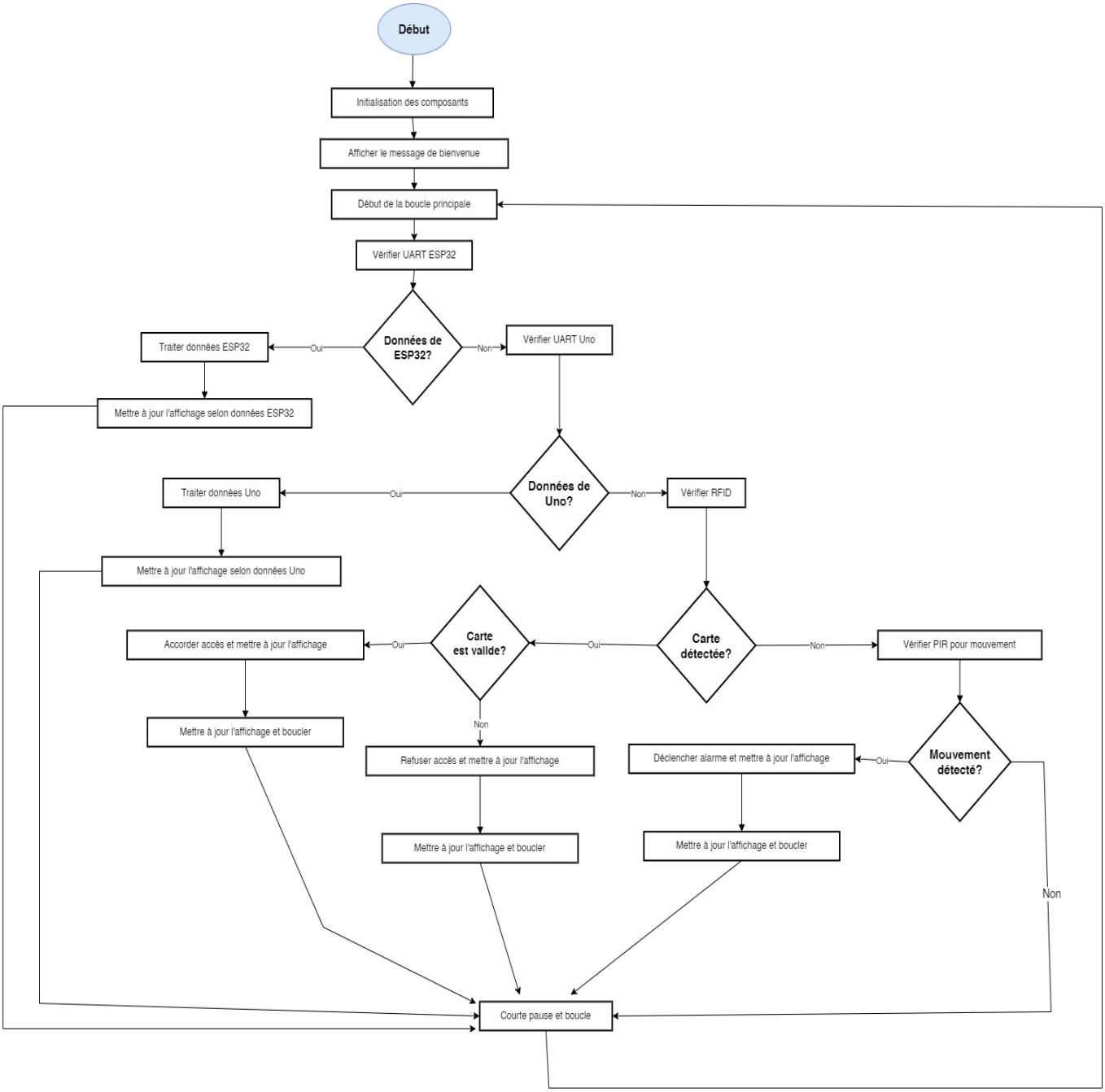



**FIGURE III.4 :** DIAGRAMME DU CODE TELEVERSE SUR LE RASPBERRY PI PICO

6. **Exécuter notre code sur la carte :** Après avoir transféré notre code, nous devrions pouvoir l'exécuter sur notre carte RPP pour le voir en action.

## III.3. Configuration ESP32CAM

Pour configurer l'ESP32-CAM avec l'IDE Arduino, suivez ces étapes :

## III.3.1 Préparation de l'IDE Arduino

### III.3.1.1 Installer l'ESP32 Core

- Ouvrez l'IDE Arduino.
- Allez dans Fichier > Préférences.

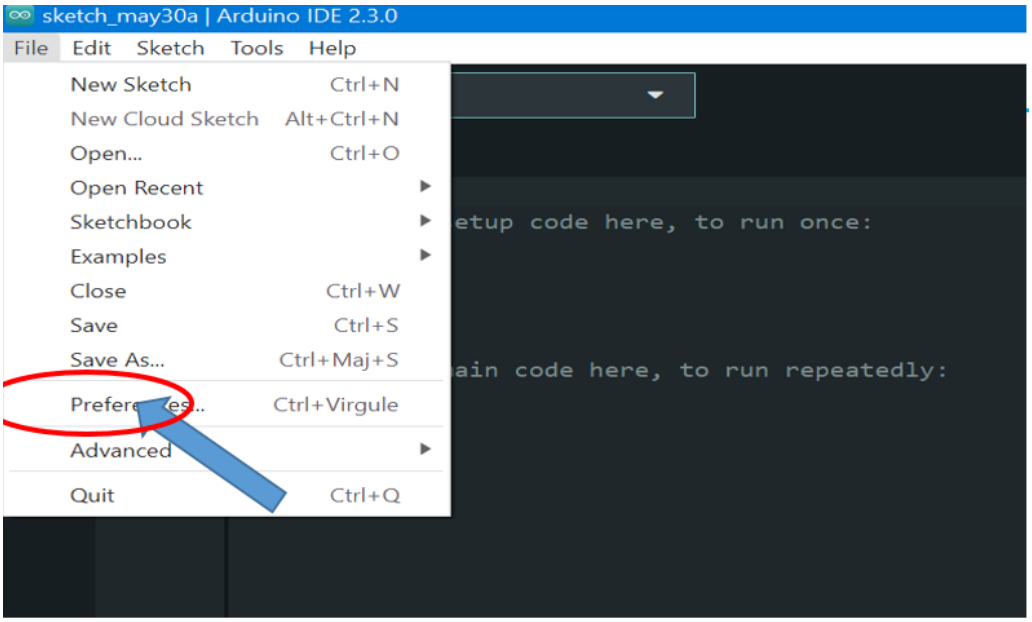



**FIGURE III.5 :** OUVERTURE DE L'IDE ET SELECTION DES "PREFERENCES" DANS LE MENU "FICHIER

Dans le champ "**URL de gestionnaire de cartes supplémentaires**", on ajoute l'URL suivant :

https://raw.githubusercontent.com/espressif/arduino-esp32/gh-pages/package_esp32_index.json

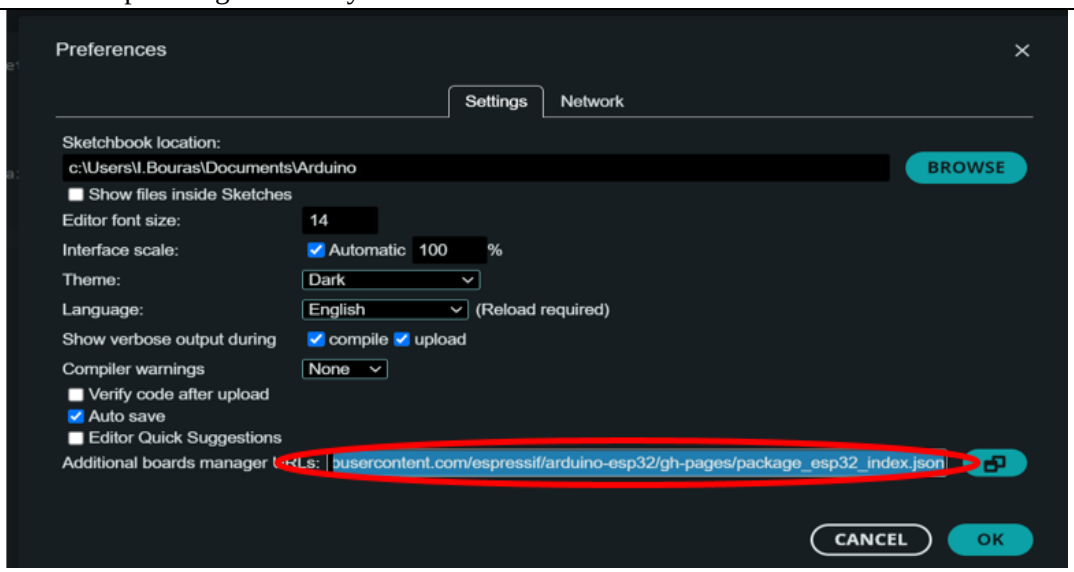



**FIGURE III.6 :** AJOUT DE L'URL DANS LE CHAMP "URL DE GESTIONNAIRE DE CARTES SUPPLEMENTAIRES

Ensuite, en accédant au menu "**Outils**" de l'environnement de développement intégré (IDE). À cet endroit, le choix se porte sur l'option "**Type de carte**", suivie d'un clic sur "**Gestionnaire de cartes**".

Recherchez "**esp32**" et installez "**esp32 by Espressif Systems**".

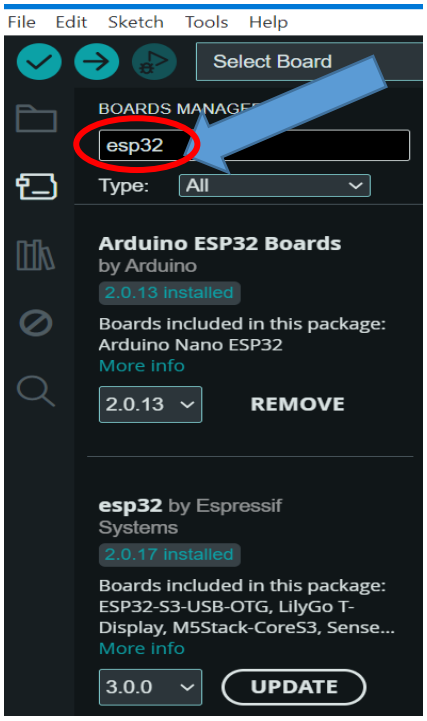



**FIGURE III.7 :** INSTALLATION DU PACKAGE "ESP32" VIA LA FENETRE DE RECHERCHE POUR CONFIGURER L'ENVIRONNEMENT DE DEVELOPPEMENT

## III.3.1.2 Sélectionner la Carte ESP32-CAM

1 - Une seule fois l'installation est terminée nous prouvons sélectionner le type '**AI Thinker ESP32-CAM**' pour programmer notre ESP32CAM.

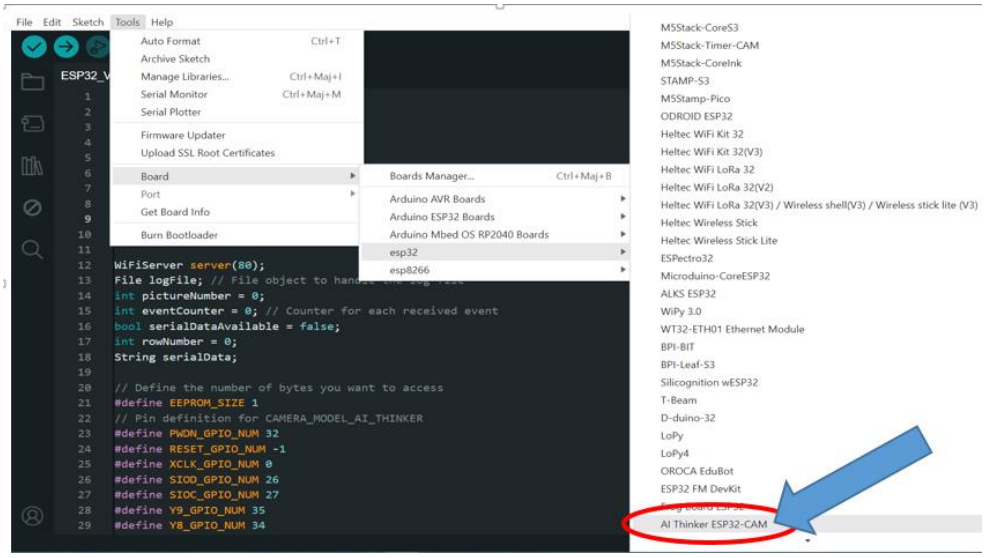



**FIGURE III.8 :** SELECTION DU TYPE 'AI THINKER ESP32-CAM' APRES L'INSTALLATION POUR PROGRAMMER NOTRE ESP32CAM

## III.3.2 Configuration matérielle

1. **Connexion de l'ESP32-CAM**

- Connecter l'ESP32-CAM à l'ordinateur en utilisant un adaptateur FTDI (USB vers UART).

2. **Brancher le module FTDI**

- Brancher le module FTDI à votre ordinateur via USB.

## III.3.3 Configuration de l'ESP32-CAM dans l'IDE Arduino

1. **Paramètres de l'ESP32-CAM**
   - Allez dans Outils et configurez les options comme suit :
     - **Type de carte**: AI Thinker ESP32-CAM
     - **Port**: Sélectionnez le port COM correspondant à votre module FTDI.
     - **Processeur**: ESP32
     - **Flash Mode**: QIO
     - **Flash Frequency**: 40MHz
     - **Partition Scheme**: Huge APP (3MB No OTA/1MB SPIFFS)

2. **Charger le code**

    - Allez dans Fichier > Exemples > ESP32 > Camera > CameraWebServer.
    - Ouvrez l'exemple CameraWebServer.

## III.3.4 Téléversement du Code

1. **Mettre en mode flash**
    - Assurez-vous que le pin IO0 est connecté à GND.
    - Cliquez sur le bouton Téléverser dans l'IDE Arduino.
    - Lorsque le téléversement commence, appuyez sur le bouton Reset de l'ESP32-CAM.
2. **Déconnecter IO0**
    - Après le téléversement réussi, déconnectez le pin IO0 de GND.
    - Appuyez sur le bouton Reset de l'ESP32-CAM.

## III.3.5 Bibliothèque pour l'ESP32-CAM

Une fois la carte ESP32 installée dans l'IDE Arduino, nous devons ajouter et configurer les bibliothèques nécessaires pour la compilation de notre code. Pour ce faire, on ouvre l'IDE Arduino et dans le menu "**Croquis**", on sélectionne "**Inclure une bibliothèque**" et "**Gérer les bibliothèques**".

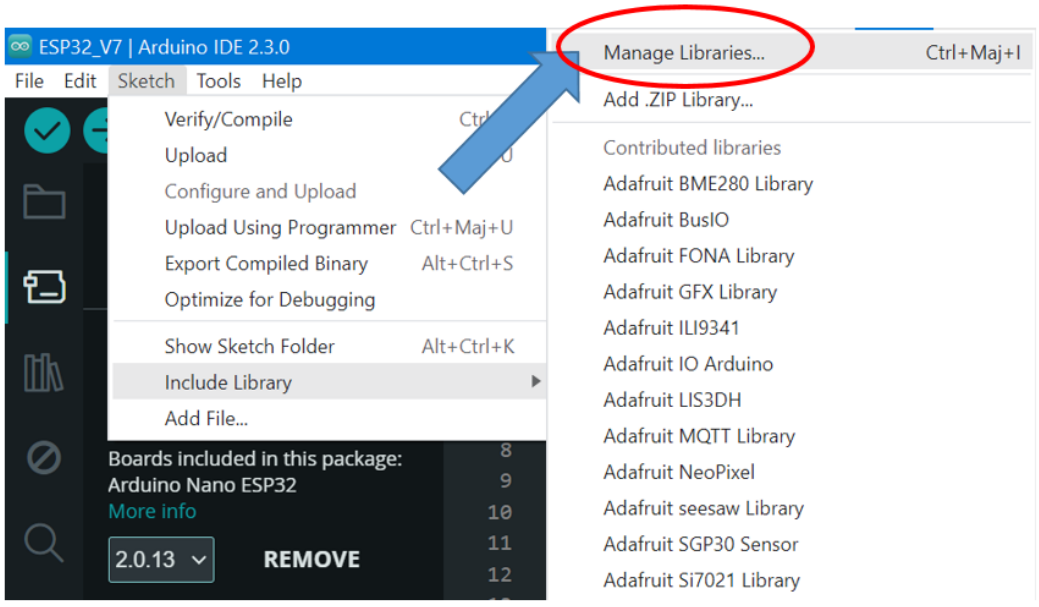



**FIGURE III.9 :** AJOUT ET CONFIGURATION DES BIBLIOTHEQUES NECESSAIRES DANS L'IDE ARDUINO VIA LE MENU "CROQUIS"

Dans la fenêtre du gestionnaire de bibliothèques, on recherche et on installe les bibliothèques nécessaires pour la compilation du sketch (code).

Voici le diagramme de configuration de l'ESP32-CAM avec le serveur web :

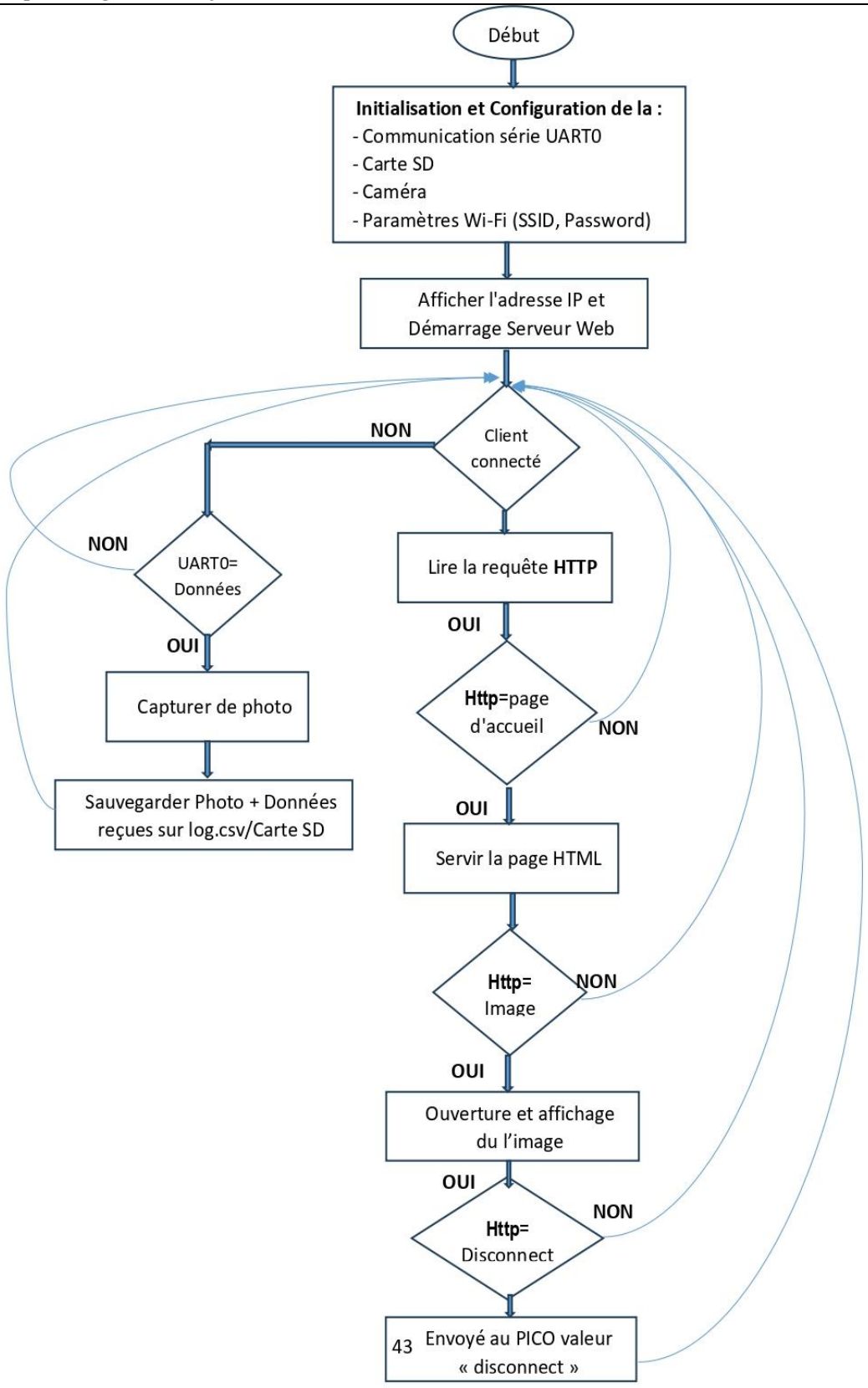



**FIGURE III.10 :** DIAGRAMME DE CONFIGURATION DE L'ESP32-CAM AVEC LE SERVEUR WEB

## III.4. Configuration des deux Atmega 328P (A et B)

Pour configurer l'Atmega 328P pour utiliser le module radio NRF24L01, nous devons d'abord connecter les broches du module aux broches correspondantes au microcontrôleur comme indiqué dans le tableau dans le chapitre 2.

Ensuite, nous installons les bibliothèques nécessaires dans l'IDE Arduino. Pour cela, nous ouvrons l'IDE, puis nous allons dans **Croquis**>**Inclure une bibliothèque**>**Gérer les bibliothèques**. Nous avons recherché et installé les bibliothèques **nRF24L01** et **RF24**. Ces bibliothèques nous permettent de contrôler le module radio et de gérer les communications sans fil de manière efficace.

Le code télévisé pour microcontrôleur A et B est représenté sur les diagrammes suivants :

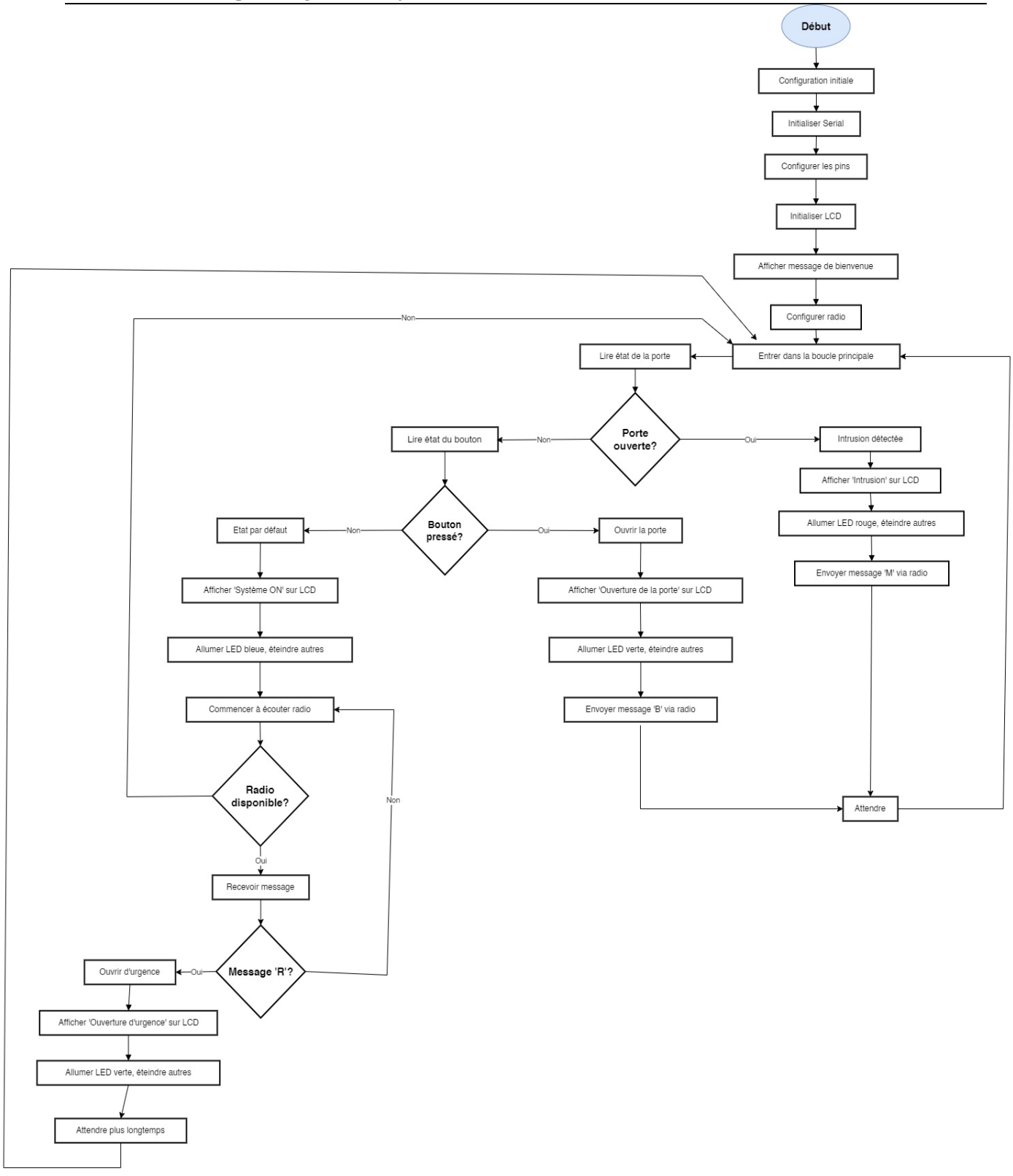



**FIGURE III.11 :** DIAGRAMME DE CODE DE L'ATMEGA A

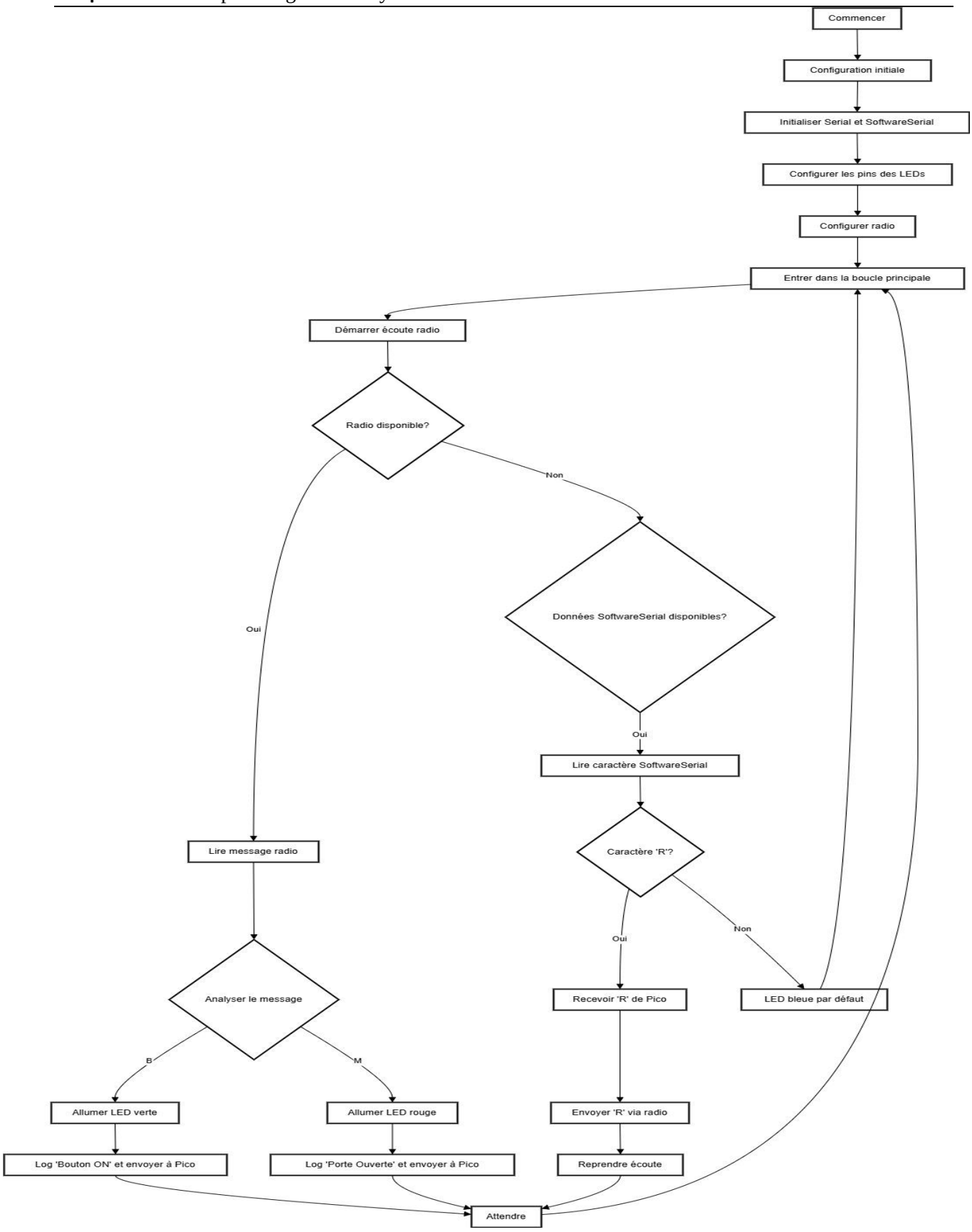



**FIGURE III.12 :** DIAGRAMME DE CODE DE L'ATMEGA B

## III.5. Création du serveur web

Le serveur web est créé et géré à l'aide de la classe « **WiFiServer** » dans la fonction setup. Le serveur écoute les requêtes clients entrantes sur le port 80, et lorsqu'un client se connecte, il traite ces requêtes dans la fonction « ***handleClientRequests*** ». Les réponses à ces requêtes incluent du code HTML, qui est généré à divers endroits du code.

Dans le serveur web plusieurs éléments ont été utilisés en l'occurrence :

**Structure du document :**

Les éléments de base de la structure HTML sont utilisés :

- **<!DOCTYPE html>** : Définit le type de document comme étant HTML.
- **<html> :** Élément racine du document HTML.
- **<head> :** Contient des métadonnées sur le document (titre dans ce cas).
- **<body> :** Contient le contenu visible de la page Web.

Le début de la page HTML commence par la ligne suivante :

```
client.println("<!DOCTYPE html><html>");
```

Cette ligne indique que le document est en HTML5 et marque le début de la page HTML.

**1- Titre**

Le titre de la page web est spécifié dans la section **<head>** du HTML. Voici comment il est défini dans le code :

```
client.println("<head><title>Journal des presences</title></head>");
```

**Explication :** Cette ligne définit le titre de la page web à "Journal des presences". Le titre est affiché sur l'onglet du navigateur.

**NB :** de même manière les autres titres ont été créés.

**2- Style**

`<body style="background-color: #03A4B6;">` : Définit la couleur d'arrière-plan de la page Web en bleu clair.

**3- En-têtes :**

- **<h1>** : Définit un titre de niveau 1 (le plus grand) pour le titre "Journal des présences".
- **<h2>** : Définit un titre de niveau 2 pour d'autres sections.

**4- Logo**

L'image de l'université de Boumerdès (logo) est incluse dans la section **<body>** du HTML et est servie par le serveur lorsqu'elle est demandée. Voici comment elle est intégrée dans le HTML :

```
client.println("<img src=\"/logo.png\" alt=\"Logo\" style=\"display: block; margin: 0 auto; max-width: 200px; height: auto;\">");
```

**Explication** : Cette ligne ajoute une image à la page web. La source de l'image est /logo.png et elle est stylisée pour être centrée et limitée à une largeur maximale de 200 pixels. L'image du logo est effectivement servie par la fonction **sendLogoFile**.

### 5- Bouton

Les boutons sont créés comme faisant partie des formulaires HTML. Voici un exemple de bouton :

```
- client.println("<form action=\"/disconnect\" method=\"post\">");
- client.println("<input type=\"submit\" value=\"DECONNECTER\" style=\"margin-bottom: 10px; background-color: #fcba03;\">");
- client.println("</form>");
```

**Explication** : Cette partie illustre la création d'un bouton étiqueté "DECONNECTER". Lorsqu'on clique dessus, il envoie une requête POST à l'endpoint /disconnect, ce qui déclenche la fonction « ***handleDisconnect*** ».

### 6- Tableau

**Structure du tableau**

- **<table>** : Définit un tableau pour afficher les informations sur les événements.
- **<thead>** : Définit la rangée d'en-tête du tableau.
- **<th> :** Définit les cellules d'en-tête pour chaque colonne (Événement, ID, Date, etc.).
- **<tbody>** : Définit le corps du tableau où les lignes de données sont ajoutées.
- **<tr>** : Définit une ligne de tableau.
- **<td>** : Définit une cellule de données dans une ligne de tableau.

Le journal des événements est affiché dans un tableau. Voici un exemple de la création des en-têtes de tableau :

```
- client.println("<table style=\"border-collapse: collapse; width: 100%; border: 2px solid #000000;\">");
- client.println("<thead style=\"background-color: #3358A7;\">");
- client.println("<tr>");
- client.println("<th style=\"text-align: left; padding: 4px;\">N</th>");
- client.println("<th style=\"text-align: left; padding: 4px;\">EVENEMENT</th>");
- client.println("<th style=\"text-align: left; padding: 4px;\">ID</th>");
- client.println("<th style=\"text-align: left; padding: 4px;\">DATE</th>");
- client.println("<th style=\"text-align: left; padding: 4px;\">HEURE</th>");
- client.println("<th style=\"text-align: left; padding: 4px;\">IMAGE</th>");
- client.println("<th style=\"text-align: left; padding: 4px;\">OPTION</th>");
- client.println("</tr>");
- client.println("</thead>");
```

**Explication** : Ce morceau de code crée un tableau avec des en-têtes pour diverses colonnes telles que :

- "**N**" : présente le numéro de l'évènement ;

- "**EVENEMENT**" : cette colonne contient les différents types d'évènement enregistrés sur la carte SD ;
- "**ID**" : le numéro d'identification des carte RFID ;
- "**DATE**" : date de l'événement ;
- "**HEURE**" : l'heure de l'évènement ;
- "**IMAGE**" : image prise lors l'évènement ;
- "**OPTION**" : un bouton qui permettre de supprimer la ligne entier de l'évènement enregistré.

**7- Liens :**

<a href="/image?path=filename"> : Crée un lien vers un autre fichier image enregistré sur la carte SD de l'ESP32-CAM avec le nom de fichier spécifié.

La partie du code HTML permet de créer une interface utilisateur simple et efficace pour la gestion des présences. Il comprend des éléments de structure, de style, des images, des boutons et des tableaux pour une présentation organisée et interactive des données.

## III.6. Conception du serveur web

Voici l'interface de serveur Web crée :

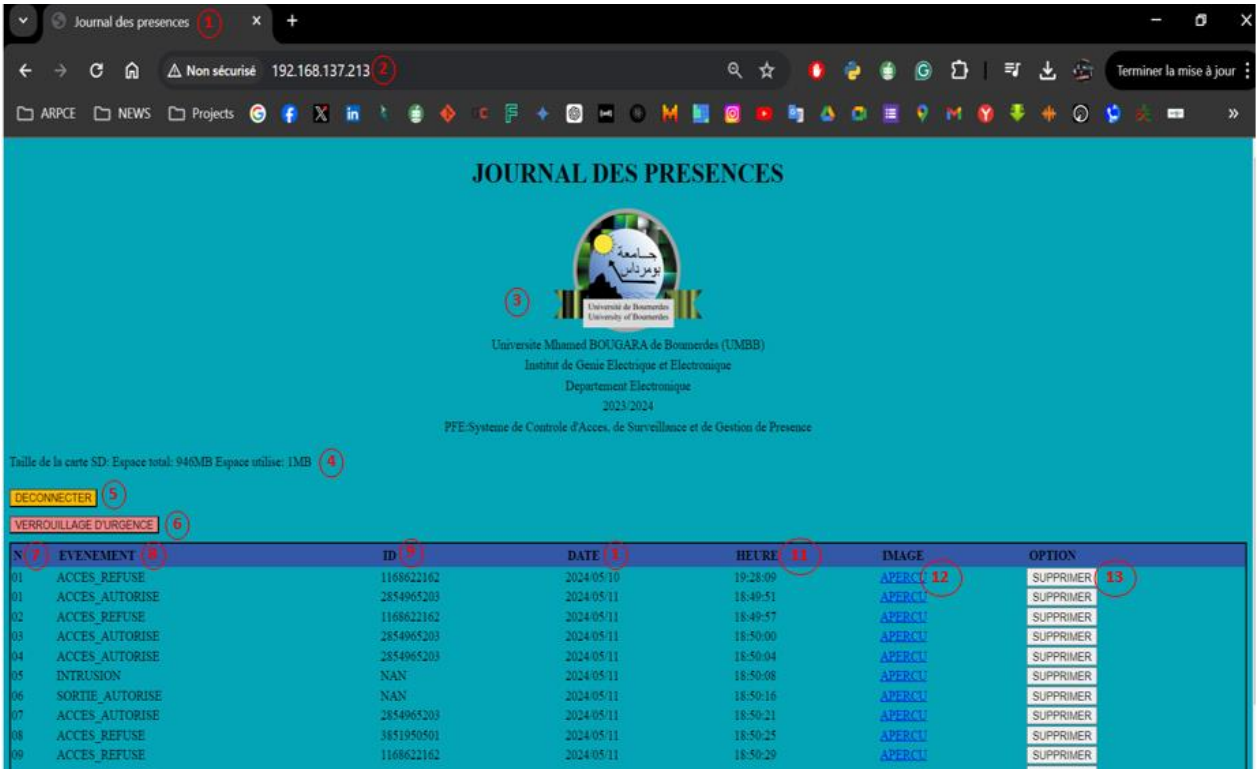



**FIGURE III.13 :** L'INTERFACE WEB CRÉE

**Description de l'interface du serveur web**

Le tableau ci-dessous présente les éléments qui constituent l'interface de serveur Web :

| N° | Elément | Description |
|---|---|---|
| **1** | **Nom de page** | Nom de la page « Journal d'évènement ». |
| **2** | **Adresse IP** | @IP généré par l'ESP32CAM pour afficher les données stockées sur la carte SD. |
| **3** | **Entête et logo** | Entête et logo et d'autres informations présentatives. |
| **4** | **Info carte SD** | Affichage de la taille de la carte SD total et l'espace utilisé |
| **5** | **Bouton « Déconnecter »** | Ce bouton permet l'utilisateur de se déconnecter du serveur web pour permettre l'insertion des données sur le fichier CSV localisé dans la carte SD. |
| **6** | **Bouton « Verrouillage d'urgen** | **Le Verrouillage d'urgence est utilisé pour verrouiller/déverrouiller le système dans le cas d'urgence.**<br>- **Verrouillage :** la porte est inaccessible pour tous les utilisateurs porteurs de cartes RFID valide et son qui ont en interne.<br>- **Déverrouiller :** la porte est maintenue ouverte dans le cas d'un incendie par exemple sans besoin de présenter une carte RFID valide ou d'activer le mécanisme d'ouverture en interne. |
| **7** | **Tableau des évènements** | Les évènements sauvegardés sur le ficher CSV dans la carte SD sont affichées sous format d'un tableau contenant 7 colonnes. |
| | **N** | **Colonne N :** Indique le numéro d'événement incrémenté (si le serveur est redémarré le conteur des évènements **N** sera initialisé indiquant que lESP32CAM a été mise hors alimentation). |
| **8** | **Evènement** | **La colonne 'Evènement'** porte différent type d'événements mentionnés précédemment. |
| **9** | **ID** | **La colonne 'ID'** porte les numéros d'identification des cartes RFID soit valide (Autorisé par l'Admin) ou non autorisé (Carte RFID non autorisé par l'Admin). **NOTE** : Si survient un événement non lié à l'utilisation d'une carte RFID le système prend la valeur NAN par défaut. |
| **10** | **Date** | **La colonne 'Date'** cette colonne contient la date réelle à laquelle l'évènement s'est produit. |
| **11** | **Heure** | **La colonne 'Heure'** cette colonne présente l'heure actuelle de l'évènement. |
| **12** | **Bouton « Aperçu »** | **Le Bouton « Aperçu »** permet de visualiser la photo prise lors de l'évènement. |
| **13** | **Bouton « Supprimer »** | **Le Bouton « Supprimer »** permet de supprimer l'évènement indésirable par l'Admin. |

**TABLE III.1 :** ÉLEMENTS CONSTITUANT L'INTERFACE DU SERVEUR WEB

## III.7. Conclusion

Dans ce chapitre, nous avons détaillé les différentes étapes de configuration logicielle nécessaires à la réalisation de notre système de surveillance. Nous avons configuré et programmé les composants essentiels, tels que le Raspberry Pi Pico, l'ESP32CAM, et les deux ATmega 328, pour assurer une surveillance en temps réel.

Dans le chapitre suivant, nous aborderons la partie pratique de notre projet. Nous effectuerons les tests de chaque capteur, procéderons à l'assemblage, et afficherons les résultats obtenus.

# **Chapitre IV :** Tests pratiques et résultats

## IV.1. Introduction

Dans ce chapitre, nous allons présenter les tests pratiques réalisés pour valider le fonctionnement de notre système de surveillance. Nous détaillerons l'assemblage de la partie matérielle, les résultats fournis par les capteurs, ainsi que les données affichées sur différents dispositifs. Ces tests nous permettront de vérifier la fiabilité et l'efficacité de notre système en conditions réelles.

## IV.2. Outils pour la conception de circuits électroniques

### IV.2.1 Fritzing

Fritzing est un logiciel open source de conception de circuits électroniques, particulièrement apprécié pour sa facilité d'utilisation et son interface intuitive. Il permet aux utilisateurs de créer des schémas électroniques, de prototyper des circuits sur des plaques d'essai virtuelles, et de concevoir des circuits imprimés (PCB). Fritzing offre une bibliothèque étendue de composants électroniques, ce qui simplifie grandement le processus de conception et de prototypage. [33]

Nous avons utilisé Fritzing pour concevoir les deux plaques d'essai. Ces conceptions nous ont permis de visualiser et de valider nos circuits avant de les fabriquer. Les cartes sont représentées comme suit :

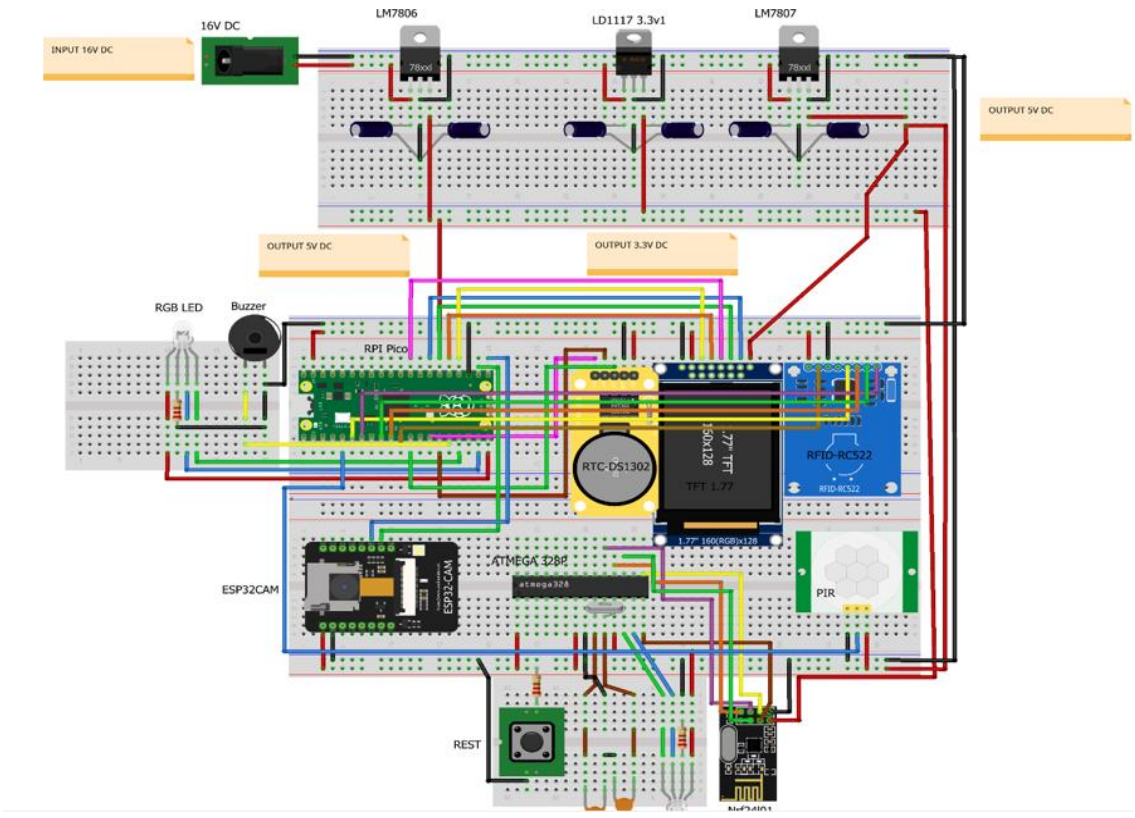



**FIGURE IV.1 :** PLAQUES D'ESSAI « A »

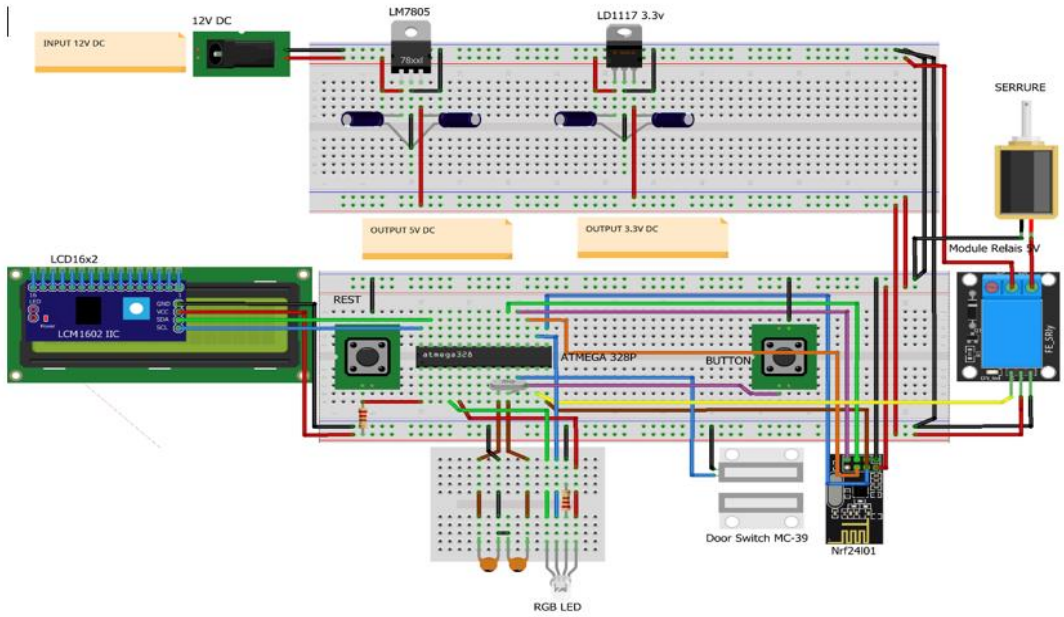



**FIGURE IV.2 :** PLAQUES D'ESSAI « B »

## IV.2.2 KiCad

KiCad est une suite logicielle open-source utilisée pour la conception de circuits électroniques. Elle permet aux ingénieurs et aux amateurs de créer des schémas électroniques et des circuits imprimés (PCB). Voici les fonctionnalités principales que nous avons utilisées avec KiCad, illustrées par des figures issues de notre projet : [33]

### IV.2.2.1 Schéma Électronique

C'est un schéma qui permet de dessiner et de documenter des circuits électroniques.

Voici les schémas de deux cartes :

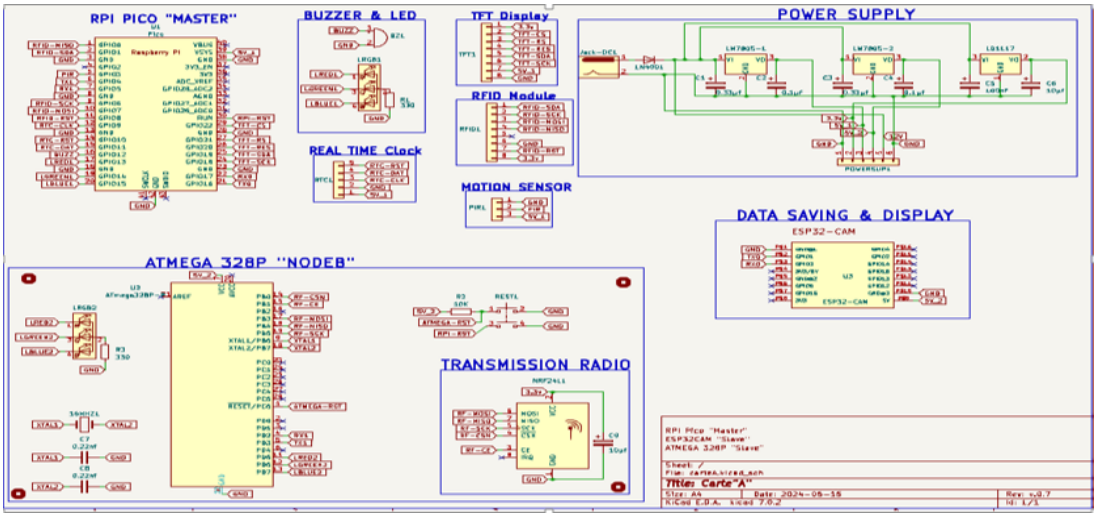



**FIGURE IV.3 :** CIRCUIT DE LA CARTE "A"

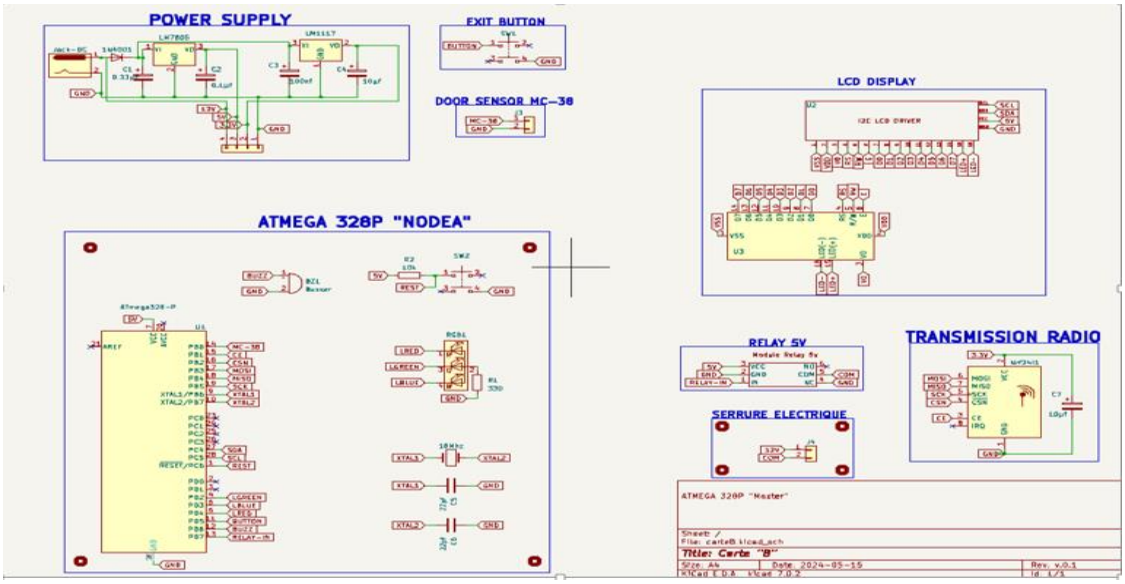



**FIGURE IV.4 :** CIRCUIT DE LA CARTE "B"

## IV.2.2.2 Conception de PCB

Elle permet de concevoir des circuits imprimés, de placer des composants et de tracer des pistes.

Voici les figures correspondantes à la carte PCB "A" de notre projet :

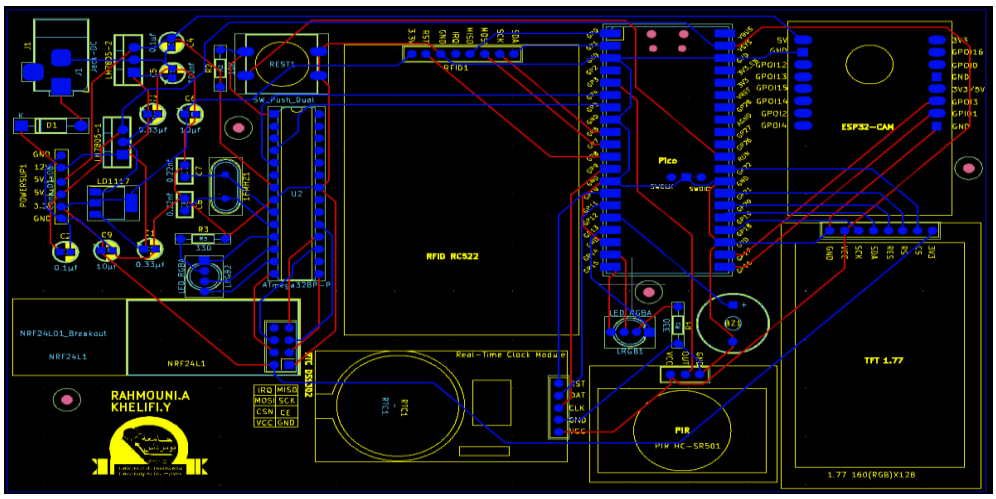



**FIGURE IV.5 :** COUCHE AVANT DE LA CARTE "A"

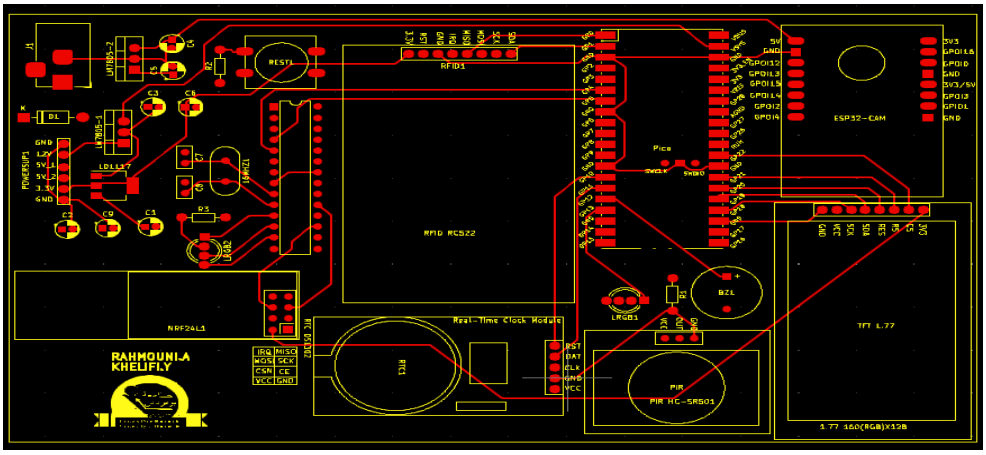



**FIGURE IV.6 :** COUCHE ARRIERE DE LA CARTE "A"

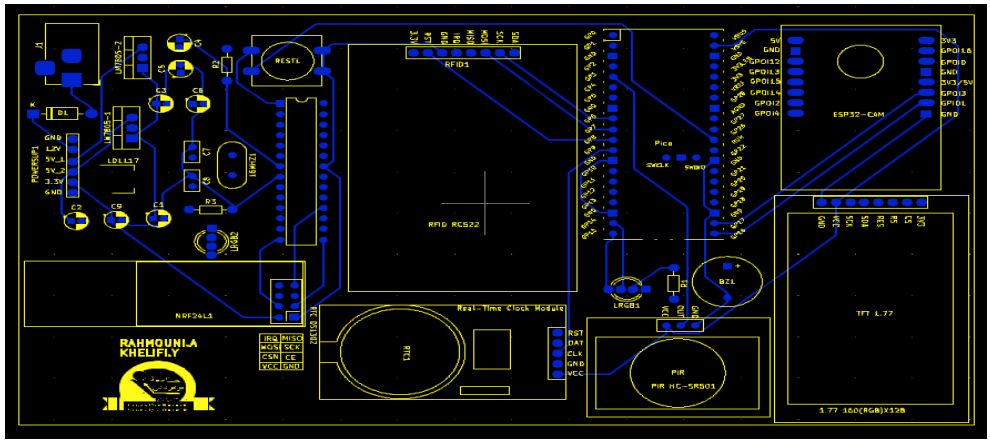



**FIGURE IV.7 :** COUCHE SILKSCEEN ET CONTOUR DE LA CARTE "A"

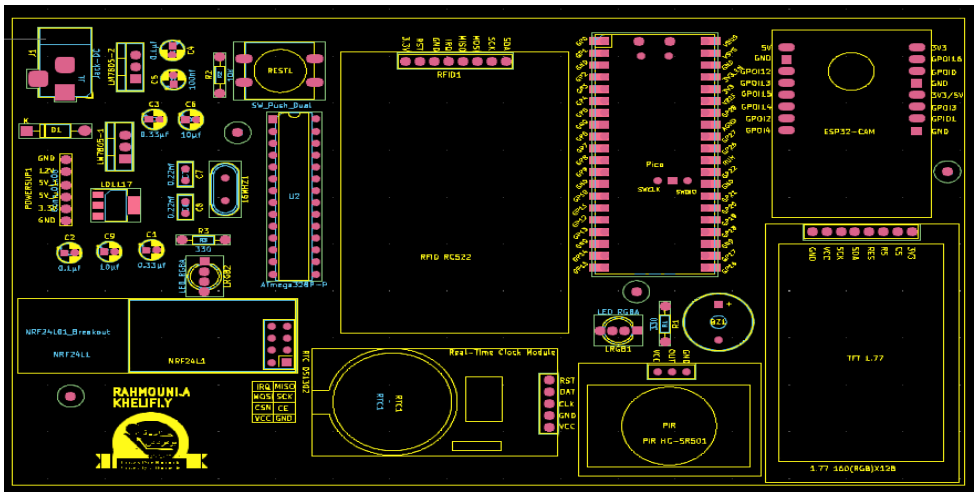



**FIGURE IV.8 :** PLAN DE PERÇAGE DE LA CARTE "A"

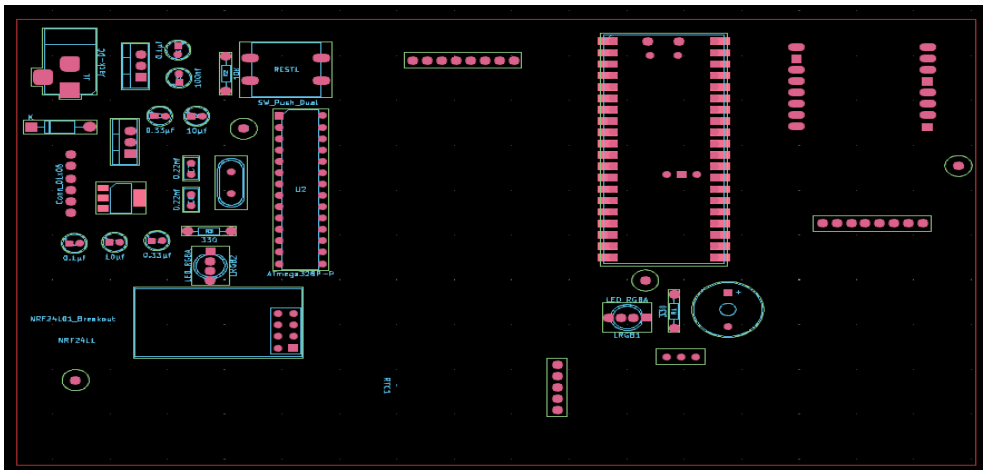


**FIGURE IV.9 :** PLAN DE PERÇAGE DE LA CARTE "A"

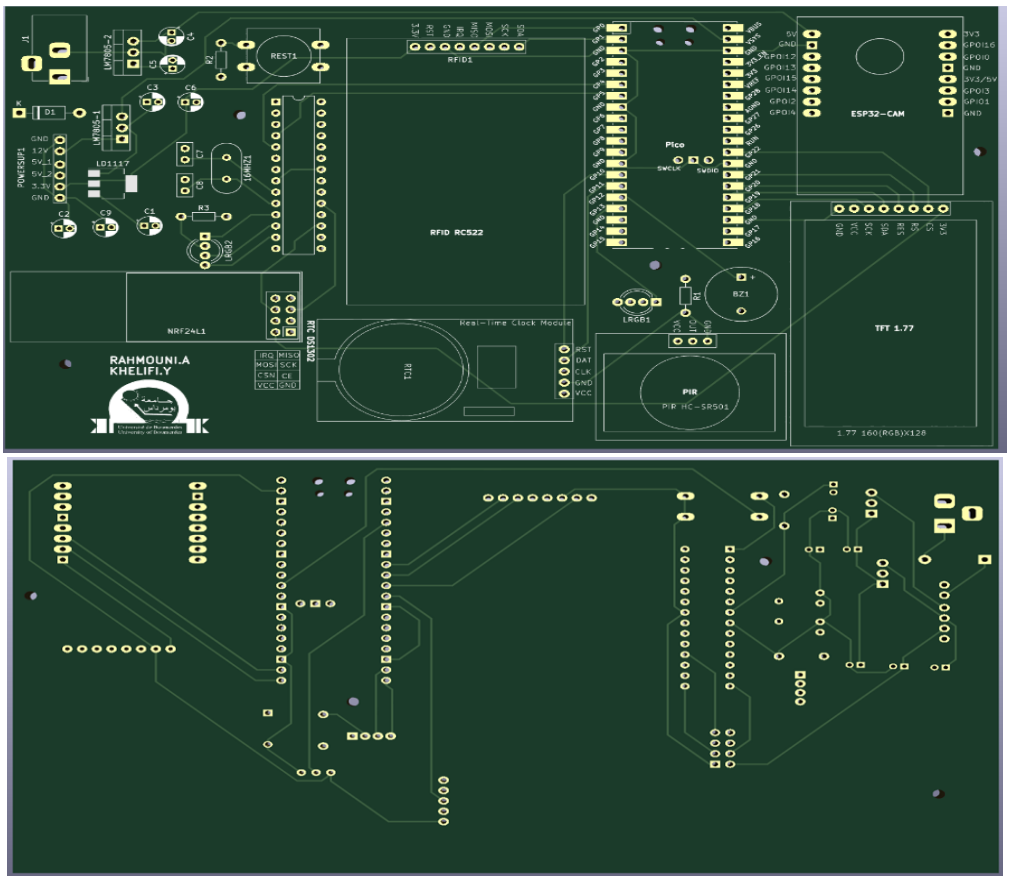



**FIGURE IV.10 :** CARTE PCB "A" PLAN AVANT ET ARRIERE

Voici les figures correspondantes à la carte PCB "B" de notre projet :

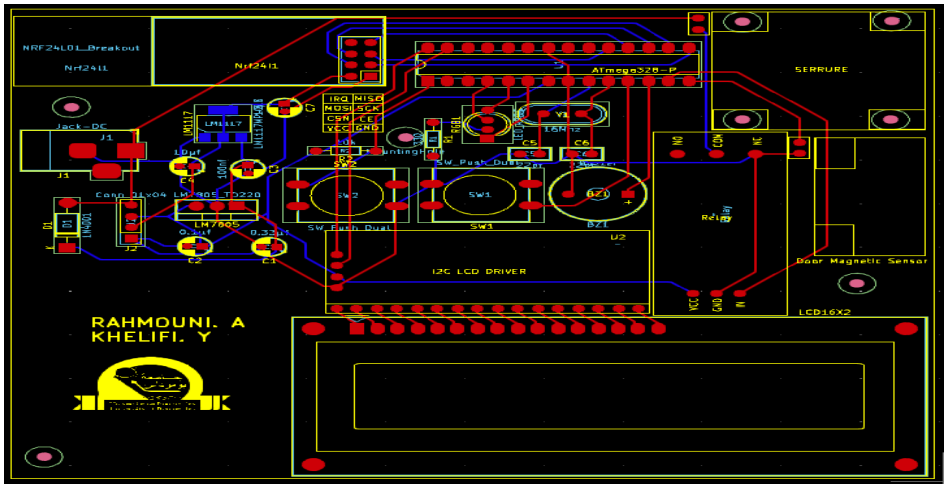



**FIGURE IV.11:** COUCHE AVANT DE LA CARTE "B"

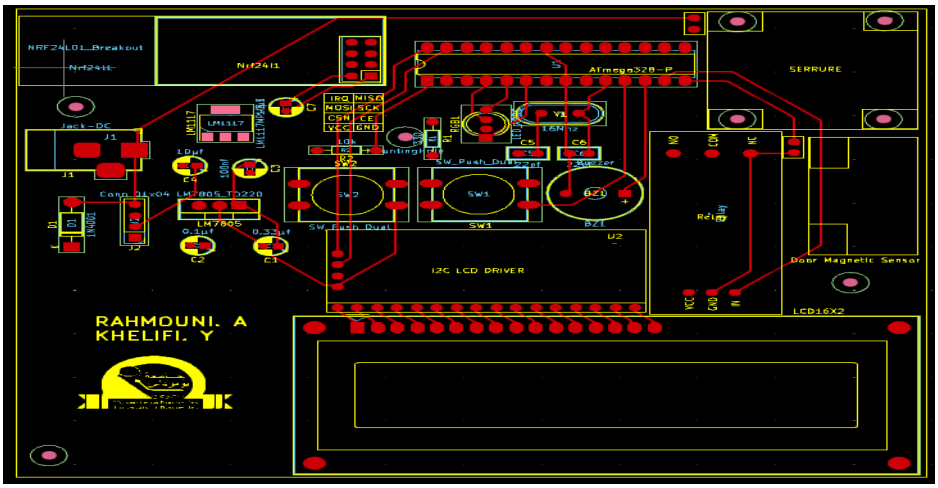



**FIGURE IV.12 :** COUCHE ARRIERE DE LA CARTE "B"

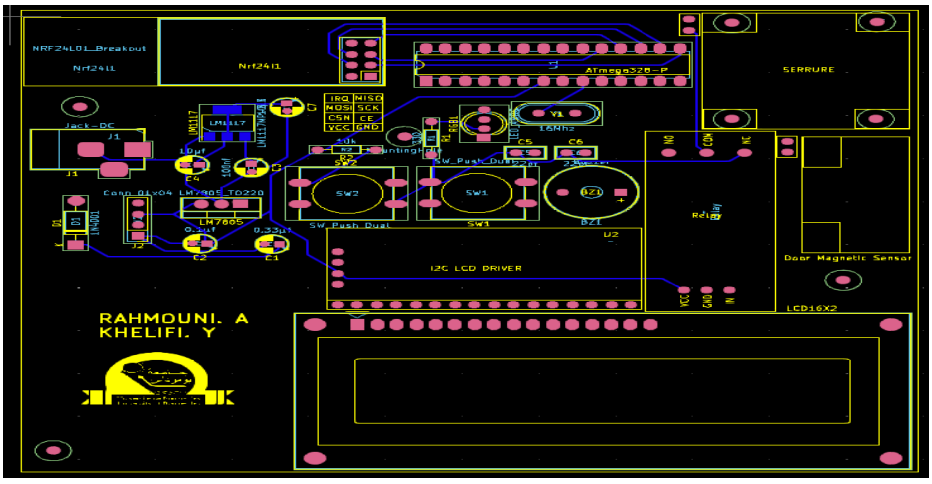



**FIGURE IV.13 :** COUCHE SILKSCEEN ET CONTOUR DE LA CARTE "B"

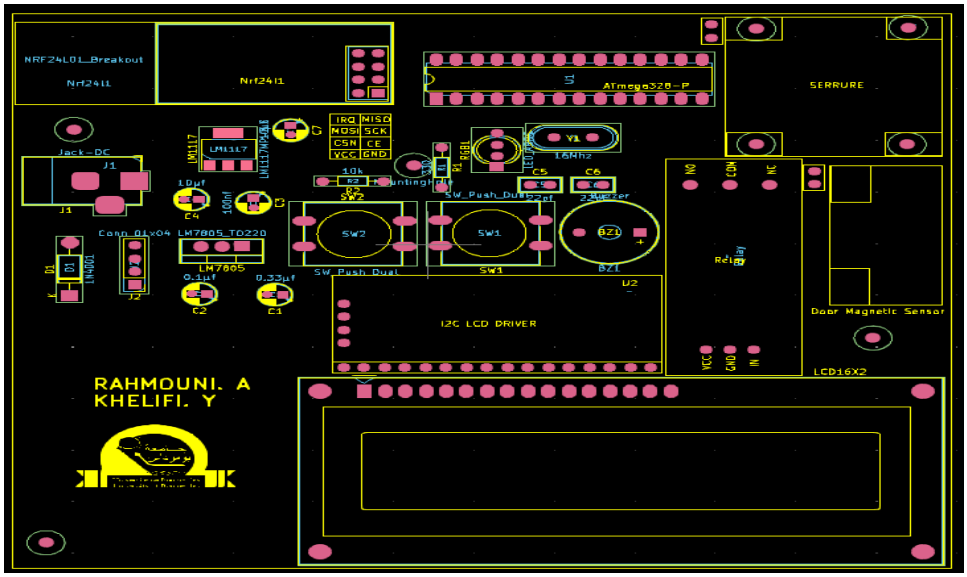



**FIGURE IV.14 :** PLAN DE PERÇAGE DE LA CARTE "B"

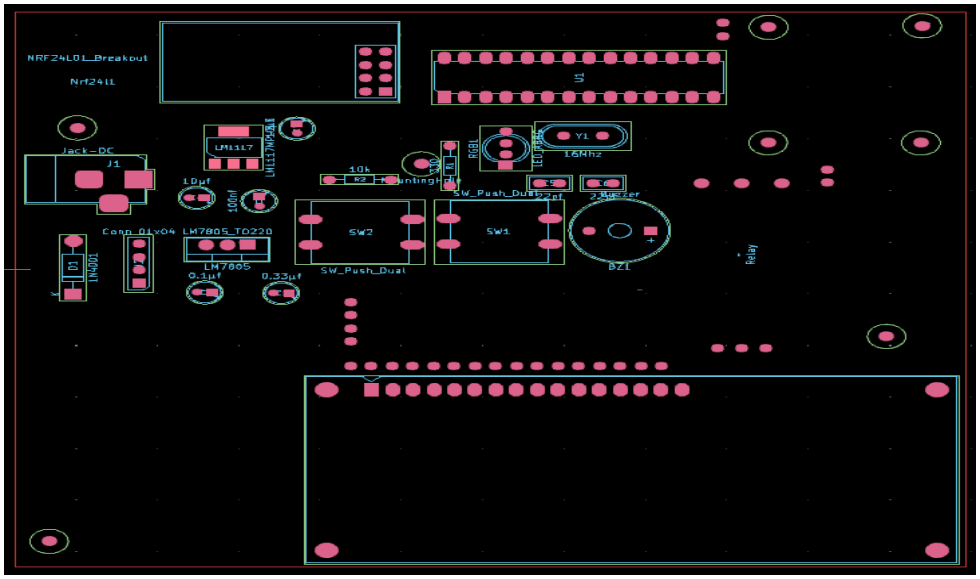



**FIGURE IV.15 :** PLAN DE PERÇAGE DE LA CARTE "B"

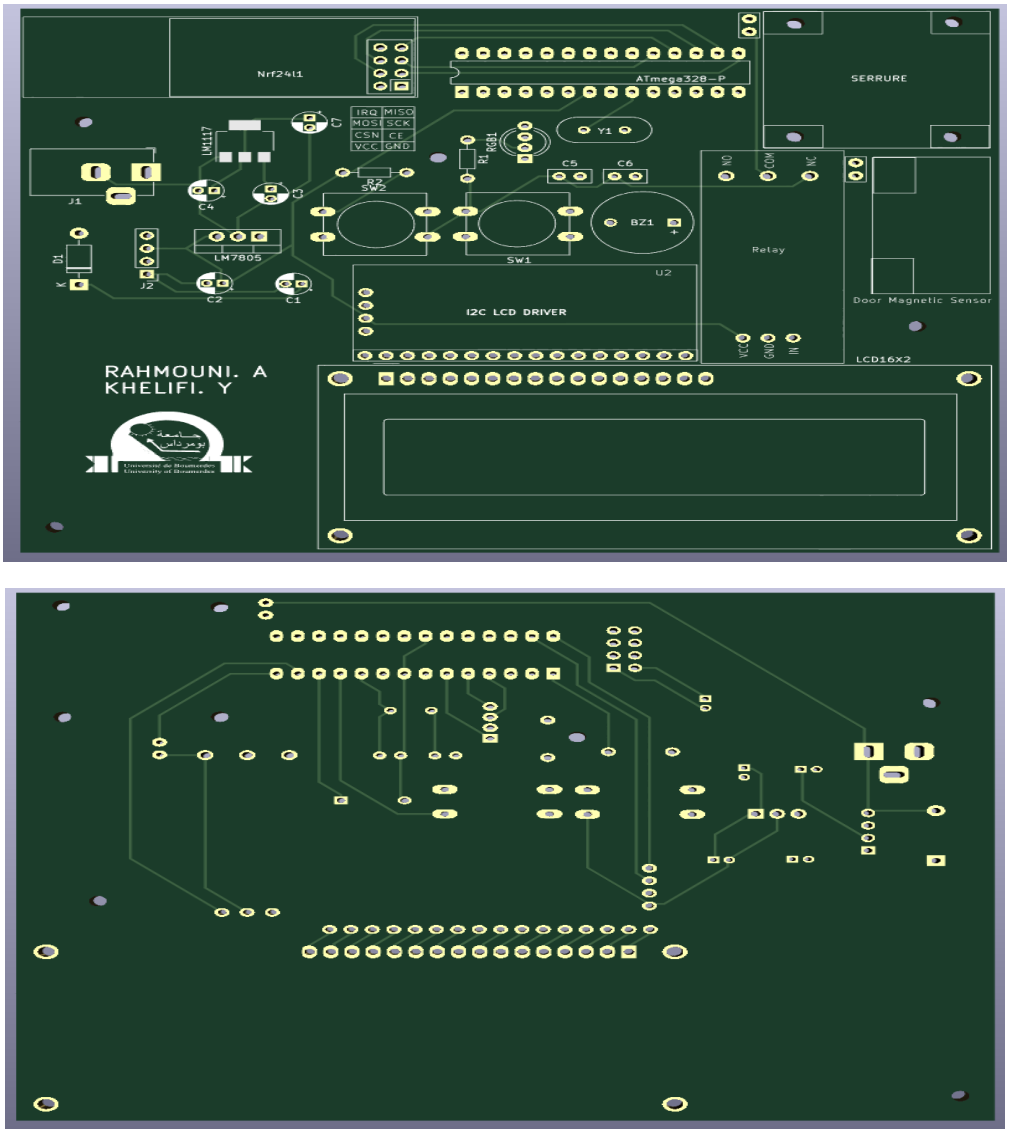



**FIGURE IV.16 :** CARTE PCB "B" PLAN AVANT ET ARRIERE

## IV.2.2.3 Visualisation 3D

Elle permet de visualiser le PCB en 3D pour vérifier le placement des composants, l'agencement général et le contour de deux cartes A et B, comme illustré par les figures suivantes :

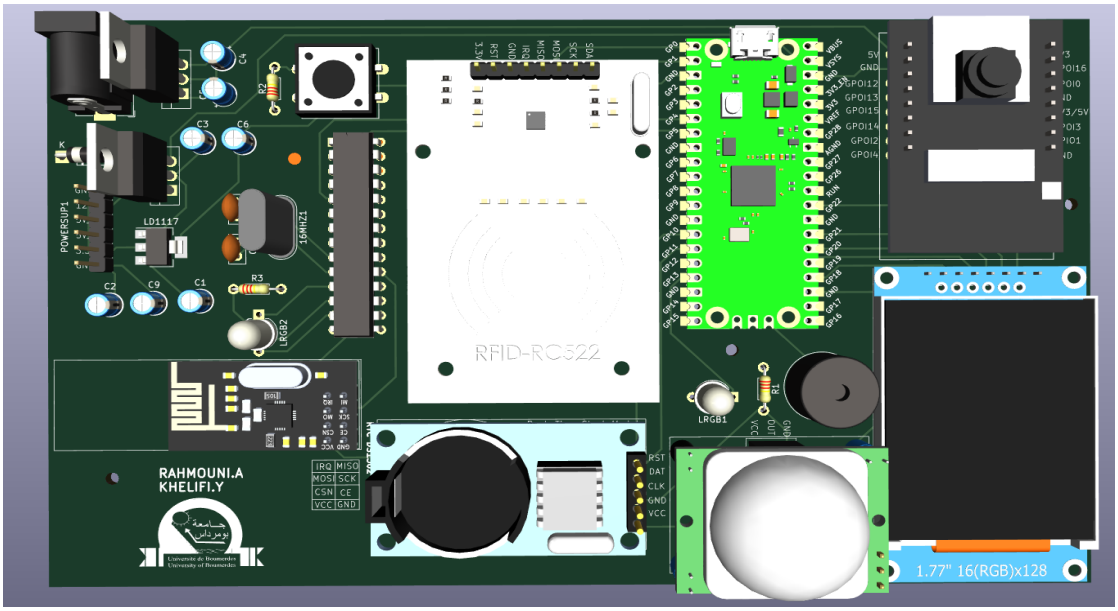



**FIGURE IV.17 :** CARTE PCB "A" EN 3D

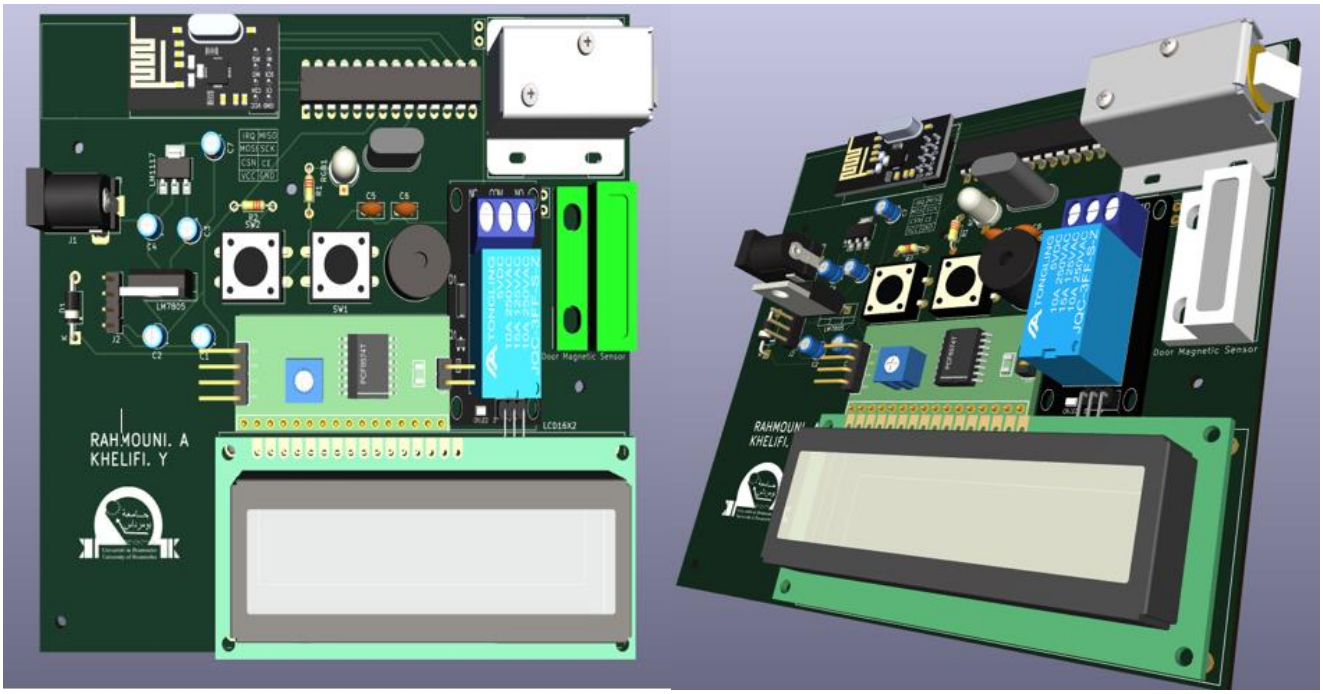



**FIGURE IV.18 :** CARTE PCB "B" EN 3D

## IV.3 Assemblage de la partie matérielle

Dans cette partie, nous nous concentrons sur l'assemblage physique de notre système, où nous disposons les composants sur les plaques d'essai et puis sur les deux plaques de circuit imprimé (PCB). Cette étape cruciale illustre la concrétisation de nos schémas électroniques préalablement conçus, garantissant ainsi une intégration précise et fonctionnelle de notre système de surveillance et de contrôle d'accès.

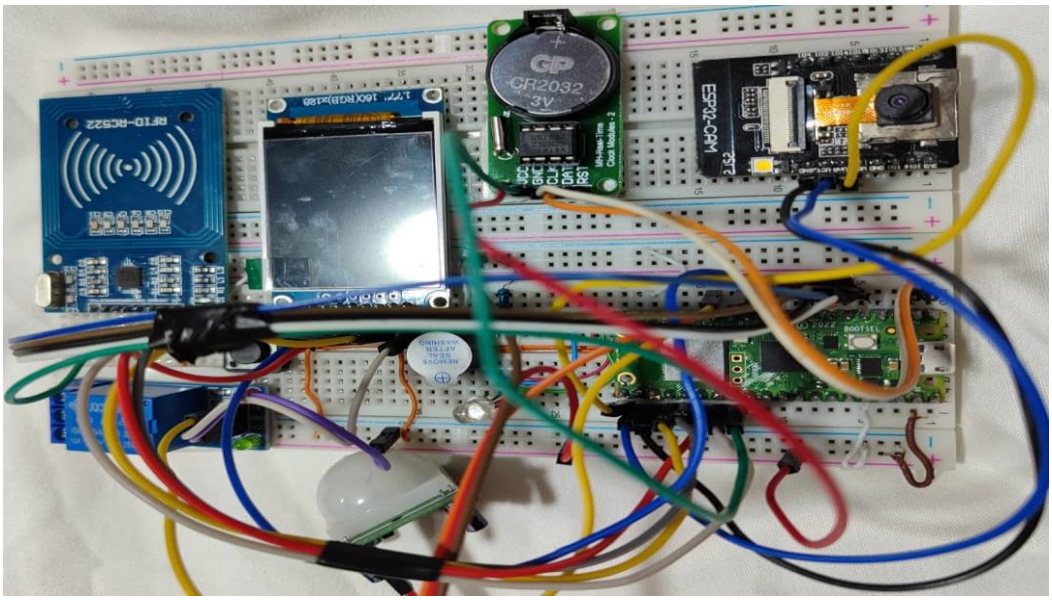



**FIGURE IV.19 :** PLAQUES D'ESSAI "A"

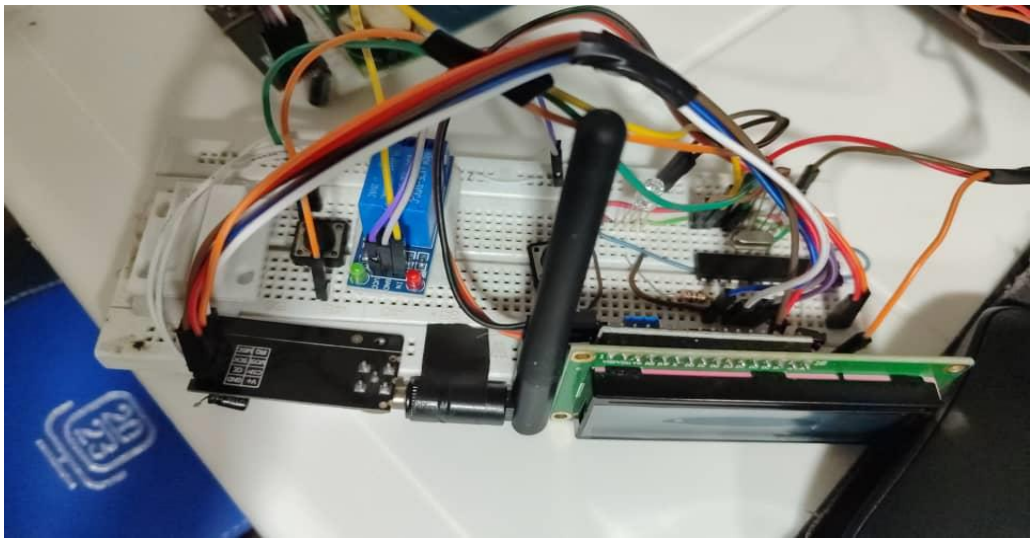


**FIGURE IV.20:** PLAQUES D'ESSAI "B"

**FIGURE IV.21:** CARTE PCB "A"

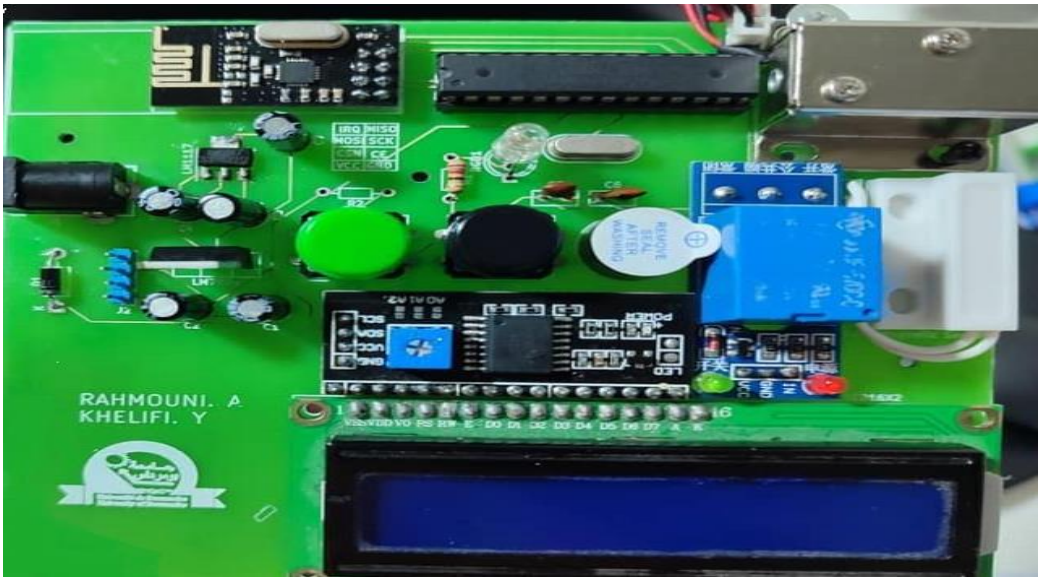



**FIGURE IV.22:** CARTE PCB "B"

## IV.4 Résultats par les capteurs

### IV.4.1 Capteur PIR

Le capteur PIR est utilisé pour détecter les mouvements. Les résultats montrent les notifications envoyées aux afficheurs et sur l'interface web lorsqu'un mouvement est détecté, ainsi que les images capturées par l'ESP32-CAM.

## IV.4.2 Module RFID et serrure électrique

Le module RFID permet la vérification de l'identité des individus autorisés à accéder au système sécurisé et l'activation de la serrure électrique pour les accès autorisés. Les résultats montrent les lectures de tags RFID et l'enregistrement des accès sur l'interface web, ainsi que les images capturées par l'ESP32-CAM.

## IV.4.3 Capteur magnétique

Le capteur magnétique détecte l'ouverture et la fermeture des portes et fenêtres. Les notifications sont affichées sur les différents afficheurs.

## IV.5 Interface web

Notre interface web affiche les photos capturées par l'ESP32-CAM et fournit des alertes en temps réel. La figure ci-dessous illustre des exemples de résultats envoyés par les différents capteurs :

| N | Status | ID | Date | Time | Picture |
|---|---|---|---|---|---|
| 01 | Entry | 2854965203 | 2024/05/06 | 15:55:02 | View |
| 02 | Entry | 2954304410 | 2024/05/06 | 15:55:13 | View |
| 03 | Intruder | NAN | 2024/05/06 | 15:55:19 | View |
| 04 | Intruder | NAN | 2024/05/06 | 15:55:20 | View |
| 05 | Entry | 2954304410 | 2024/05/06 | 15:55:24 | View |
| 06 | Exit | NAN | 2024/05/06 | 15:55:28 | View |
| 07 | Entry | 2854965203 | 2024/05/06 | 15:55:34 | View |
| 08 | WrongID | 3851950501 | 2024/05/06 | 15:55:42 | View |
| 01 | Intruder | NAN | 2024/05/06 | 16:54:44 | View |
| 02 | Intruder | NAN | 2024/05/06 | 16:54:45 | View |
| 03 | Intruder | NAN | 2024/05/06 | 16:54:45 | View |
| 04 | Intruder | NAN | 2024/05/06 | 16:55:21 | View |

**FIGURE IV.23:** CAPTEUR D'ECRAN L'INTERFACE WEB

## IV.6. Résultats obtenu sur les différents afficheurs

Nous allons voir les différents résultats obtenus pour chaque afficheur :

## IV.6.1 Afficheur LCD 1602

Ce tableau montre tous les messages affiché sur L'afficheur LCD 1602 :

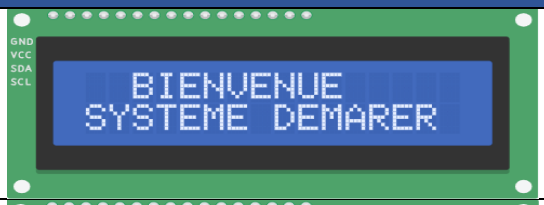
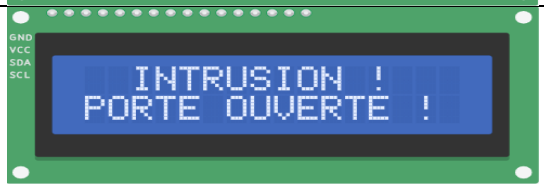
| N° | Phase | Condition | Action |
|---|---|---|---|
| 01 | Démarrage Système | Aucune<br>(SETUP) |  |
| 02 | Evènement = « INTRUSION » lorsque « Porte Ouverte » | SI MC-38 = HIGH |  <br>Red LED = ON<br>Green LED =OFF<br>Blue LED = OFF<br>RADIO ENVOI « M » |
| 03 | Evènement = « SORTIE » lorsque le bouton est appuyé « Ouverte de la Porte » | SI BUTON = LOW | <br>Green LED = ON<br>Red LED =OFF<br>Blue LED = OFF<br>RELAIS (SERRURE) = HIGH<br>RADIO ENVOI « B » |
| 04 | Evènement = « ENTREE » lorsqu'une carte RFID valide est scannée « Ouverte de la Porte » | SI RADIO RECOIT = « E » | <br>Green LED = ON<br>Red LED =OFF<br>Blue LED = OFF<br>RELAIS (SERRURE) = LOW |
| 05 | Pas d'événement et le système est en marche | Aucune<br>(LOOP) | <br>Blue LED = ON<br>Red LED =OFF<br>Green LED = OFF<br>RELAIS (SERRURE) = LOW |

**TABLE IV.1 :** LES INFORMATIONS AFFICHEES SUR LCD 1602

## IV.6.2 Afficheur TFT 1.77

Ce tableau montre tous les messages affichés sur L'afficheur TFT 1.77

| N° | Phase | Condition | Action | Affichage |
|---|---|---|---|---|
| 01 | Démarrage Système | Aucune<br>(SETUP) | Connection **ESP32CAM** au **WIFI**<br>Initialisation **RFID, RTC**<br>Green LED = ON<br>Red LED = OFF<br>Blue LED = OFF<br>Buzzer = OFF | |
| 02 | Evènement = « INTRUSION » lorsque « Porte Ouverte » | Si RADIO '**NODEB**' reçoit = « M » | **Prise de photo et** enregistrement d'évènement su la carte SD<br>Green LED = OFF<br>Red LED = ON<br>Blue LED = ON<br>Buzzer = OFF | |
| 03 | Evènement = « SORTIE » lorsque le Bouton est appuyé « Ouverte de la Porte » | Si RADIO '**NODEB**' reçoit = « B » | **Prise de photo et** enregistrement d'évènement su la carte SD<br>Green LED = ON<br>Red LED = OFF<br>Blue LED = OFF<br>Buzzer = ON | |
| 04 | Evènement = « ACCESS_AUTORISE » lorsqu'une carte RFID valide est scannée « Ouverte de la Porte » | Si une carte RFID valide est scannée | **Prise de photo et** enregistrement d'évènement su la carte SD<br>RADIO '**NODEB**' envoi « E »à '**NODEA**'<br>Green LED = ON<br>Red LED = OFF<br>Blue LED = OFF<br>Buzzer = ON | |
| 05 | Evènement = « MOUVEMENT » lorsqu'une carte RFID valide est scannée « Ouverte de la Porte » | Si PIR = 'HIGH' pendent 5 seconds && aucune carte RFID n'a été scannée | Enregistrement d'évènement su la carte SD<br>Green LED = ON<br>Red LED = OFF<br>Blue LED = OFF<br>Buzzer = ON | |
| 06 | Evènement = « Verrouillage » lorsqu'une carte RFID valide est scannée « Ouverte de la Porte » | Si le Verrouillage est activé sur l'interface web | Verrouillage Système<br>RADIO '**NODEB**' envoi « V »à '**NODEA**'<br>Green LED = ON<br>Red LED = OFF<br>Blue LED = OFF<br>Buzzer = OFF | |
| 07 | Evènement = « Déverrouillage » lorsqu'une carte RFID valide est scannée « Ouverte de la Porte » | Si le Déverrouillage est activé sur l'interface web | Déverrouillage Système<br>RADIO '**NODEB**' envoi « D »à '**NODEA**'<br>Green LED = ON<br>Red LED = OFF<br>Blue LED = OFF<br>Buzzer = OFF | |
| 08 | Pas d'événement et le système est en marche | Aucune<br>(LOOP) | Green LED = OFF<br>Red LED = OFF<br>Blue LED = OFF<br>Buzzer = OFF | |

**TABLE IV.2 :** LES INFORMATIONS AFFICHEES SUR L'ECRAN TFT 1.77

## IV.7. Analyse des résultats

Nous avons analysé les résultats obtenus pour vérifier la fiabilité des détections et la performance du système. Les résultats montrent un taux de réussite élevé pour les détections de mouvement et les lectures RFID, ainsi qu'un temps de réponse rapide du serveur web.

## IV.8. Conclusion

Dans cette partie, nous avons présenté la maquette finale de notre projet ainsi que les résultats obtenus suite aux divers tests effectués. Grâce aux outils et méthodes utilisés pour la conception des circuits électroniques, nous avons pu valider les différentes fonctionnalités de notre système. Nous passons maintenant à la conclusion générale, où nous aborderons les perspectives et les recommandations futures.

# Conclusion générale

Après une étude approfondie des différents systèmes de surveillance disponibles, nous avons mis en œuvre un système visant à renforcer la sécurité des biens et des personnes, en le rendant plus efficace et fiable. Car cella offre un moyen d'améliorer la sécurité, de réduire les risques d'intrusion et de simplifier la gestion des accès dans divers environnements.

Notre projet repose sur l'utilisation d'une carte Raspberry Pi Pico pour collecter les données de surveillance, tandis que l'ESP32CAM se charge de la connexion au réseau WiFi et de l'affichage des données en temps réel via une interface web hébergée sur notre serveur dédié.

Cette interface permet de consulter un journal d'événements, comprenant des photos capturées en cas de détection de mouvement ou d'identification RFID incorrecte.

Notre projet est certainement perfectible, donc nous avons envisagé des perspectives d'amélioration et d'autres idées pour le développer davantage.

Par exemple, en intégrant la reconnaissance faciale pour une identification plus précise, en ajoutant des capteurs supplémentaires pour une surveillance plus complète ou en développant une application mobile pour un accès à distance plus facile.

La réalisation de ce projet nous a permis d'approfondir nos connaissances et nos compétences acquises tout au long de notre formation à l'université M'hamed Bougara, et d’autre part de préparer notre intégration à la vie professionnelle.

Nous espérons que notre système de surveillance intelligent trouvera des applications pratiques dans divers domaines, tels que la sécurité résidentielle, la surveillance industrielle et la gestion des accès dans les bâtiments publics et privés.

# Bibliographie

[1] R. Capdepon, « Vidéoprotection à Marseille : l'audit qui accuse », *Laprovence*, 12 février 2022. [En ligne]. Disponible sur : https://www.laprovence.com/article/sorties-loisirs/6657860/le-grand-deballage.html. Consulté le 15 avril 2024

[2] « Comment fonctionne un système de vidéosurveillance ? », *AT-Electronics*, 14 août 2017. https://www.at-electronics.lu/comment-fonctionne-un-syst%C3%A8me-de-vid%C3%A9osurveillance. Consulté le 15 avril 2024

[3] « REALISATION D'UNE APPLICATION DE VIDEOSURVEILLANCE VIA MOBILE (ANDROID) » , mémoire de master, Université d'IBN KHALDOUN-Tiaret, 2015. [En ligne]. Disponible sur : http://dspace.univ-tiaret.dz/bitstream/123456789/4902/1/TH.M.INF.FR.2015.05.pdf. Consulté le 15 avril 2024

[4] « REALISATION D'UNE APPLICATION DE VIDEOSURVEILLANCE VIA MOBILE (ANDROID) » , mémoire de master, Université d'IBN KHALDOUN-Tiaret, 2015. [En ligne]. Disponible sur : http://dspace.univ-tiaret.dz/bitstream/123456789/4902/1/TH.M.INF.FR.2015.05.pdf. Consulté le 25 avril 2024

[5] «  Vidéosurveillance : définition et explications », *Techno-Science.net*. https://www.techno-science.net/definition/11698.html. Consulté le 25 avril 2024

[6] R. B. Chehida, « Cours vidéosurveillance », *Technologue Pro. Évolution des systèmes de vidéosurveillance*, https://www.technologuepro.com/cours-videosurveillance/Chapitre-3-evolution-des-systemes-de-videosurveillance.html. Consulté le 25 avril 2024

[7] AMIRA.F, « Ce qu'apporte l'IA à la surveillance domestique », *Lesoirdalgerie*, 2022. https://www.lesoirdalgerie.com/beta/supplement-ia/ce-qu-apporte-l-ia-a-la-surveillance-domestique-111978. Consulté le 25 avril 2024

[8] MySecurite, « Detecteur de mouvement d'une alarme : quels résultats ? », *MySecurite*, 13 janvier 2017. https://www.mysecurite.com/alarmes/dossiers/comment-placer-les-detecteurs-de-votre-alarme-maison. Consulté le 26 avril 2024

[9] J. Robert, « Reconnaissance faciale : Décryptage de son fonctionnement », *Formation Data Science | DataScientest.com*, 9 novembre 2023. https://datascientest.com/reconnaissance-faciale-tout-savoir. Consulté le 26 avril 2024

[10] « Algorithme et IA pour sécuriser les commerces », *Veesion*. https://veesion.io/algorithme-et-ia-en-matiere-de-videosurveillance-comment-lintelligence-artificielle-securise-les-

commerces/. Consulté le 26 avril 2024

[11] J.-C. Risch et J.-C. Risch, « Segmentation et détection d'objets en temps réel avec Tensorflow », *ActuIA*, 29 juillet 2022. https://www.actuia.com/contribution/jeancharlesrisch/segmentation-et-detection-dobjets-en-temps-reel-avec-tensorflow/. Consulté le 27 avril 2024

[12] « Avantages et inconvénients de la vidéosurveillance en lieu public ». https://www.tike-securite.fr/securite-maison/42-les-avantages-et-les-inconvenients-de-la-videosurveillance-dans-les-lieux-publics.Consulté le 28 avril 2024

[13] « Les avantages et les inconvénients de la vidéosurveillance dans les espaces publics – Wayfe » , 10 juillet 2023. https://www.wayfe.net/2023/07/10/les-avantages-et-les-inconvenients-de-la-videosurveillance-dans-les-espaces-publics/. Consulté le 30 avril 2024

[14] « REALISATION D'UNE APPLICATION DE VIDEOSURVEILLANCE VIA MOBILE (ANDROID) », mémoire de master, Université d'IBN KHALDOUN-Tiaret, 2015. [En ligne]. Disponible sur : http://dspace.univ-tiaret.dz/bitstream/123456789/4902/1/TH.M.INF.FR.2015.05.pdf. Consulté le 30 avril 2024

[15] G. Tronic, « Carte Raspberry Pi Pico », *GO TRONIC*. https://www.gotronic.fr/art-carte-raspberry-pi-pico-33027.htm. Consulté le 1 mai 2024

[16] E. ZDNet, « Raspberry Pi Pico ; W ; : "W" pour Wi-Fi » , *ZDNET*, 25 avril 2024. [En ligne]. Disponible sur : https://www.zdnet.fr/guide-achat/raspberry-pi-pico-w-w-pour-wi-fi-39944240.htm. Consulté le 1 mai 2024

[17] Raspberry Pi Pico Documentation," Raspberry Pi Foundation. [Online]. Disponible: https://www.raspberrypi.com/documentation/microcontrollers/raspberry-pi-pico.html. . Consulté le 1 mai 2024

[18] « ESP32-CAM Camera Module », *Components101*. https://components101.com/modules/esp32-cam-camera-module. Consulté le 2 mai 2024

[19] « ESP32-CAM | BinaryTech Electronique Algérie », *Binarytech Electronique Algérie*. https://binarytech-dz.com/produit/arduino-raspberry/cartes-diveres/esp32-cam-avec-ov2640-camera/. Consulté le 2 mai 2024

[20] Aranacorp," nRF24L01 Module Image, Aranacorp. [Online Image]. Available: https://www.aranacorp.com/wp-content/uploads/module-nrf24l01.jpg. . Consulté le 3 mai 2024

[21] Alexis, « Capteur infrarouge en MicroPython : détecter les mouvements facilement sur la Pico », *uPesy*, 23 juin 2023. https://www.upesy.com/blogs/tutorials/ir-sensor-module-pico-on-micropython-tutorial?shpxid=4deba352-e7fa-43d2-ad26-e3c5e6adbd1e. Consulté le 3 mai 2024

[22] SZ Kuongshun," Image of Electronic Component, SZ Kuongshun. [Online Image]. Available: https://fr.sz-kuongshun.com/Content/File_Img/S_Product/2016-08-27/20160827101008690263 5.jpg. Consulté le 3 mai 2024

[23] RFID Contrôle d'accès par badge avec Arduino," Electronique Mixte. [Online]. Available: https://www.electronique-mixte.fr/microcontrolleurs/rfid-controle-dacces-par-badge-avec-arduino. Consulté le 4 mai 2024

[24] « KIT RFID-RC522 ». https://www.orbit-dz.com/product/kit-rfid-rc522/. Consulté le 4 mai 2024

[25] Melopero Electronics, « Magnetic contact switch (door sensor) - Melopero Electronics », *Melopero Electronics*, 9 mai 2023. https://www.melopero.com/fr/shop/sensori/proximit%C3%A9/magn%C3%A9tiquecontactsinterrupteurportecapteur/. Consulté le 4 mai 2024

[26] « MC-38 Magnetic Contact Switch sensor », *Cytron Technologies Malaysia*. https://my.cytron.io/c-others-sensor/p-mc-38-magnetic-contact-switch-sensor. Consulté le 10 mai 2024

[27] « Module relais 10A 1 canal optocoupleur | Binarytech Electronique Algérie », *Binarytech Electronique Algérie*. https://binarytech-dz.com/produit/composants-electronique/composants/relais/module-relais-10a-1-canal-optocoupleur/. Consulté le 10 mai 2024

[28] Alicia, « Module RTC DS3231, horloge en temps réel. » , *Le Disrupteur Dimensionnel*, 27 septembre 2022. https://ledisrupteurdimensionnel.com/arduino/module-rtc-ds3231-horloge-en-temps-reel/. Consulté le 10 mai 2024

[29] Amazon," Product Image. [Online Image]. Available: https://m.media-amazon.com/images/I/51FRPQM+ukL._SX522_.jpg. Consulté le 10 mai 2024

[30] AZ-Delivery," 1.77-Zoll SPI TFT Display Image, AZ-Delivery. [Online Image]. Available: https://www.az-delivery.de/cdn/shop/products/177-zoll-spi-tft-display-und-128x160-pixeln-kompatibel-mit-arduino-und-raspberry-pi-480689.jpg?v=1679397950&width=1200. Consulté le 12 mai 2024

[31] « Fabricants et fournisseurs et usine d’écrans LCD couleur TFT de 1,77 pouces personnalisés - ENRICH ». https://fr.enrichlcddisplay.com/tft-lcd/tft-lcd-displays/1-77-inch-tft-color-lcd.html. Consulté le 12 mai 2024

[32] YoupiLab, « LCD 16X2 Rétroéclairage bleu | YoupiLab Components ». https://youpilab.com/components/product/lcd-16x2-retroeclairage-bleu. Consulté le 12 mai 2024

[33] Isaac, « Fritzing : le logiciel pour les makers et l'électronique (et les alternatives) » , *Hardware Libre*, 18 mars 2022. [En ligne]. Disponible sur : https://www.hwlibre.com/fr/friture/. Consulté le 10 juin 2024

[34] « KICAD | 5.1 | Français | Documentation | KICAD » , *KiCad | 5.1 | Français | Documentation | KiCad*. https://docs.kicad.org/5.1/fr/kicad/kicad.html. Consulté le 10 juin 2024