

ENSEIGNEMENT SUPÉRIEUR ET UNIVERSITAIRE
INSTITUT SUPÉRIEUR TECHNIQUE ADVENTISTE DE GOMA
« ISTAGO »



Email: uago2015@gmail.com

[Site web: www.uagom.com](http://www.uagom.com)

B.P: 116 GOMA

Département de science et technologie

Option : réseau et infrastructure

« Mise en place d'un système de sécurité physique pour la détection des mouvements au niveau du coffre-fort » Cas de l'Equity Bank

Par : **ISHIMWE MWEMERANKIKO Jean-Pierre**

Mémoire de fin de cycle présenté en vue de l'obtention
du diplôme de Master en Réseau et Infrastructure.

DIRECTEUR : Dr. Djousse Marcelle, PhD

Année Académique 2023

DÉCLARATIONS DE L'ÉTUDIANT

Je soussigné, ISHIMWE MWEMERANKIKO JEAN-PIERRE, étudiant en réseau et infrastructure à l'Institut Supérieur Adventiste de Goma (ISTAGO), déclare solennellement ce qui suit concernant la rédaction de mon mémoire de master :

1. Je confirme que le présent mémoire de master est le résultat de mes propres recherches et efforts, menés sous la supervision de mon directeur de mémoire.
2. Je m'engage à respecter les principes d'intégrité académique et d'éthique dans toutes les phases de la rédaction de mon mémoire, en évitant toute forme de plagiat, de tricherie ou de falsification de données.
3. Je reconnais l'importance de citer et de référencer correctement les sources utilisées dans mon mémoire, en accordant une reconnaissance appropriée aux travaux et aux idées d'autres chercheurs.
4. Je suis conscient de l'impact potentiel de mes recherches et de mes conclusions sur mon domaine d'étude, et je m'engage à mener une analyse rigoureuse et impartiale des données pour garantir la fiabilité et la validité de mes résultats.
5. Je suis ouvert aux commentaires, aux critiques constructives et aux suggestions de mon directeur de mémoire et des membres de mon comité d'évaluation, et je suis prêt(e) à apporter les modifications nécessaires pour améliorer la qualité de mon mémoire.
6. Je suis conscient de l'importance de respecter les délais fixés par mon établissement d'enseignement pour la soumission de mon mémoire et je m'engage à respecter ces échéances, tout en maintenant la qualité et la rigueur de mon travail.
7. Je m'engage à présenter les résultats de ma recherche de manière claire, cohérente et professionnelle, en utilisant les normes de présentation et de formatage spécifiées par mon établissement d'enseignement.
8. Je reconnais que la rédaction d'un mémoire de master peut être un processus exigeant, tant sur le plan intellectuel qu'émotionnel, et je m'efforce de maintenir un équilibre entre mon travail académique et ma santé personnelle.
9. Je suis reconnaissant envers mon établissement d'enseignement, mes enseignants et mes pairs pour leur soutien et leur contribution à mon parcours académique, et je m'engage à valoriser cette opportunité en produisant un mémoire de master de haute qualité.
10. Je comprends que la réussite de mon mémoire de master repose sur mon engagement, ma persévérance et ma volonté de repousser les limites de la connaissance dans mon domaine d'étude, et je suis déterminé à faire de mon mieux pour atteindre cet objectif.

Je confirme que toutes les déclarations ci-dessus sont véridiques et que je suis prêt à assumer la responsabilité de mes actes en tant qu'étudiant rédigeant un mémoire de master.

ISHIMWE MWEMERANKIKO Jean-Pierre

ÉPIGRAPHE

« La seule limite à notre réalisation de demain sera nos doutes d'Aujourd'hui »

Franklin D. Roosevelt

ISHIMWE MWEMERA Jean-Pierre

DÉDICACE

Nous dédions ce présent travail à nos très chers parents BATESI et NYIRAMBABAZI.

ISHIMWE MWEMERA Jean-Pierre

REMERCIEMENTS

Au terme de ce projet de recherche, Nos remerciements les plus distingués s'adressent à la famille BATESI et la Famille NKURUNZIZA pour leur aide financière tant morale, courage, courtoisie et amour pendant nos études, qui fait un moment inoubliable dans le parcours de notre vie.

Je tiens à remercier sincèrement le Directeur Dr. Djousse PhD, a joué un rôle crucial en fournissant des conseils éclairés, une guidance précieuse et un soutien constant tout au long de cette recherche.

Aux autorités académiques de l'Institut Supérieur Techniques Adventiste de Goma (ISTAGO) en général et celle de la faculté de Gestion Informatique, PhD Dr. Elias SEMAJERI recteur de l'uago sans oublier le CT Josué KALEMA qui ne cessent de nous apporter soutiens, directives et conseils pour nous permettre d'atteindre le niveau de standard mondial et d'être compétitif au marché de l'emploi.

En fin, je souhaite remercier ma famille en général, mes camarades et mes amis pour leurs soutiens indéfectibles tout au long de cette recherche. Leurs encouragements constants et leurs présence réconfortante ont été une source de motivation inestimable.

En somme, la réussite de ce projet a été rendue possible grâce à l'engagement, l'expertise et le soutien de toutes les personnes mentionnées. Leur contribution a été déterminante pour la mise en place du système de sécurité physique et performant pour le coffre-fort.

ISHIMWE MWEMERA Jean-Pierre

SIGLES ET ABRÉVIATIONS

PERT	:	Program Evaluation and Review Technique
MT	:	Marge Totale
ML	:	Marge Libre
DAT	:	Date au Plût-tôt
DAP	:	Date au plut-Tard
ISTAGO	:	Institut Supérieur Technique Adventiste de Goma

LISTE DES TABLEAUX

Tableau 1 TABLEAU DES ANTÉCÉDENTS	28
Tableau 2 Estimation du coût de main d'œuvre.....	29
Tableau 3 Estimation de coût des matériels	30
Tableau 4 Coût global du projet.....	30

LISTE DES FIGURES

<i>Figure 1 Les Capteur de Mouvement</i>	<i>Erreur ! Signet non défini.</i>
<i>Figure 2 Le détecteur de mouvements à infrarouge</i>	<i>Erreur ! Signet non défini.</i>
<i>Figure 3 Les détecteurs de mouvement ultrasonique</i>	<i>Erreur ! Signet non défini.</i>
<i>Figure 4 Câblage</i>	20
<i>Figure 5 fonctionnement des capteurs Ultrason</i>	21
<i>Figure 6 buzzer</i>	22
<i>Figure 7 Le réseau PERT</i>	32
<i>Figure 8 date plus tôt et date plus tard</i>	34
<i>Figure 9 Chemin critique</i>	36
<i>Figure 10 Diagramme de Gantt</i>	37
<i>Figure 11 Calendrier du Project</i>	37
<i>Figure 4 Carte Uno</i>	18
<i>Figure 5 Câblage</i>	20
<i>Figure 6 fonctionnement des capteurs Ultrason</i>	21
<i>Figure 7 buzzer</i>	22
<i>Figure 8 Quit RFID</i>	24
<i>Figure 9 Le réseau PERT</i>	32
<i>Figure 10 date plus tôt et date plus tard</i>	34
<i>Figure 11 Chemin critique</i>	36
<i>Figure 12 Diagramme de Gantt</i>	37
<i>Figure 13 Calendrier du Project</i>	37
<i>Figure 14 Schéma complet d'interconnexion entre les composants du projet</i>	41
<i>Figure 15 Schéma d'interconnexion entre les composants du projet</i>	41
<i>Figure 16 Architecture du système</i>	42
<i>Figure 17 déclaration des bibliothèques et déclaration des variables</i>	42
<i>Figure 18 Déclaration des fonctions du buzzer</i>	43
<i>Figure 19 Initialisations des variables</i>	43
<i>Figure 20 Exécution du code (si une carte est connu le système est désactivée)</i>	43
<i>Figure 21 Exaction du système (si une autre carte est reconnu le système est réactiver avec le buzzer</i>	43
<i>Figure 22 l'affichage de la partie pour le coffre-fort</i>	44
<i>Figure 23 l'image de démonstration pour le lecteur RFID et Le capteur</i>	44
<i>Figure 24 démonstration des branchement des câbles du système et la câble d'alimentation</i>	44
<i>Figure 25 l'image complet du système de sécurité</i>	45

RÉSUMÉ

La mise en place d'un système de sécurité physique basé sur arduino pour la détection du mouvement au niveau du coffre-fort a été réalisée. Ce système vise à renforcer la sécurité des biens stockés dans le coffre-fort en détectant toute activité suspecte.

Lorsqu'un mouvement est détecté, le système active une sirène pour alerter les responsables de sécurité. Cependant, afin d'éviter les fausses alarmes, le propriétaire du coffre-fort a la responsabilité de s'identifier à l'aide d'une Carte RFID spécifique. Le système est conçu pour écouter pendant quelques secondes après la détection d'un mouvement afin de permettre au propriétaire du coffre-fort de présenter sa carte RFID. Si une carte valide est détectée pendant cette période, aucune alarme ne sera déclenchée. En revanche, si aucune carte RFID valide n'est présentée dans le délai imparti, le système déclenche la sirène pour signaler un mouvement suspect. Les responsables de sécurité peuvent alors prendre les mesures nécessaires pour protéger les biens et garantir la sécurité des clients. Ce système offre une solution efficace et pratique pour sécuriser les coffres-forts de l'institutions financières, en réduisant les risques de vols et d'intrusions. Il constitue une mesure de sécurité supplémentaire pour protéger les actifs des clients et maintenir la confiance dans la banque.

La mise en place de ce système de sécurité physique repose sur l'utilisation de la technologie Arduino, qui permet une intégration facile et une flexibilité dans la conception des fonctionnalités. De plus, l'utilisation des cartes RFID offre une méthode d'identification rapide et sécurisée pour les propriétaires de coffres-forts.

Dans l'ensemble, ce projet a pour objectif d'améliorer la sécurité des coffres-forts de la banque en combinant la détection des mouvements avec l'identification par la carte RFID. Il s'agit d'une solution efficace qui allie technologie, praticité et protection des biens.

SUMMARY

The implementation of a physical security system based on arduino for motion detection at the safe level was carried out. This system aims to enhance the security of goods stored in the safe by detecting any suspicious activity.

When movement is detected, the system activates a siren to alert security officials and customers present in the bank. However, in order to avoid false alarms, the owner of the safe is responsible for identifying himself using a specific RFID Card. The system is designed to listen for a few seconds after motion is detected to allow the safe owner to present their RFID card. If a valid card is detected during this period, no alarm will be triggered. On the other hand, if no valid RFID card is presented within the allotted time, the system triggers the siren to signal a suspicious movement. Security managers can then take the necessary measures to protect assets and ensure the safety of customers. This system offers an effective and practical solution for securing the safes of financial institutions, reducing the risk of theft and intrusion. It serves as an additional security measure to protect customer assets and maintain trust in the bank.

The implementation of this physical security system is based on the use of Arduino technology, which allows easy integration and flexibility in the design of functionalities. Additionally, the use of RFID cards provides a quick and secure method of identification for safe owners.

Overall, this project aims to improve the security of bank safes by combining motion detection with RFID card identification. It is a complete solution that combines technology, practicality and property protection.

CHAPITRE PREMIER : INTRODUCTION

I.1. Contexte de l'étude

Les coffres-forts sont utilisés depuis des siècles pour stocker des biens précieux tels que de l'argent, des bijoux ou des documents importants. Bien que ces coffres soient conçus pour offrir une protection contre le vol et l'incendie, ils peuvent toujours être vulnérables aux attaques malveillantes. Il est donc important de disposer de systèmes de sécurité efficaces pour protéger ces biens précieux (Snow, 2012). La détection de mouvement est une technologie largement utilisée dans de nombreux domaines tels que la sécurité, la surveillance, l'automatisation industrielle et la robotique. Les différentes technologies utilisées pour la détection de mouvement comprennent des capteurs, des caméras, des détecteurs infrarouges, des détecteurs ultrasoniques, des détecteurs de pression, des détecteurs de vibration, etc. La sélection de la méthode appropriée dépend du contexte d'utilisation (intérieur ou extérieur), de la sensibilité requise, de l'angle de détection et des coûts (Lin, 2014).

Les applications de la détection de mouvement sont nombreuses et incluent la sécurité et la surveillance des bâtiments, la surveillance de la production industrielle, la détection de mouvement dans les systèmes robotiques et la surveillance environnementale (System M. D., 2017). Cependant, la détection de mouvement peut rencontrer des limitations telles que des fausses alarmes, des angles morts et des coûts élevés.

Les cambriolages de coffres-forts sont de plus en plus fréquents dans le monde entier. En effet, les voleurs utilisent maintenant des techniques sophistiquées qui leur permettent de contourner les systèmes de verrouillage traditionnels des coffres-forts. Il est donc essentiel de disposer de systèmes de sécurité modernes et efficaces pour protéger les biens précieux des individus et des entreprises (RoJansky, 2016).

Au niveau mondial et continental, la sécurité des banques et des institutions financières est devenue un enjeu majeur ces dernières années. Les technologies de pointe ont été mises en place pour sécuriser les locaux bancaires, les coffres-forts, ainsi que les données et les transactions financières. La gestion de la sécurité prend en compte plusieurs aspects tels que la protection physique, l'intégrité des données, la surveillance continue et la récupération en cas d'incident (Ray, 2019).

Les banques et les institutions financières ont tendance à être hautement ciblées par les criminels, en particulier dans les zones où la criminalité est élevée. Ces criminels cherchent souvent à voler ou à saboter les coffres-forts ou à voler les caisses des agences bancaires. Compte tenu des pertes financières conséquentes que cela peut entraîner pour les banques, les institutions financières et les clients, il est donc impératif pour les banques de mettre en place des mesures de sécurité fortes pour protéger leurs infrastructures, leurs coffres-forts et les biens de leurs clients.

(Hanlon, 2006).

Au niveau continental, l'Afrique est confrontée à des défis uniques en matière de sécurité bancaire, coopératives et les institutions financières, notamment en raison de l'instabilité politique, de la corruption généralisée, de la criminalité organisée et de la faible couverture en matière de sécurité civile. L'Union Africaine a mis en place une politique de sécurité pour renforcer les capacités de sécurité et de défense des États membres. Cette politique vise à réguler la vente d'armes légères et de petit calibre, à combattre le terrorisme et la criminalité transnationale, ainsi qu'à renforcer la sécurité de la navigation maritime en Afrique. (Moyo, 2016)

En ce qui concerne la République Démocratique du Congo (RDC), les secteurs bancaires et financiers sont confrontés à des problèmes de sécurité similaires aux autres pays africains. Les niveaux de criminalité sont élevés et l'instabilité politique est un facteur clé de l'insécurité dans certaines régions du pays. Les banques et les institutions financières ont également été touchées par des actes de vandalismes ou de vol avec violence (Li, 2017).

C'est dans ce contexte que l'Equity Banque, qui est l'une des principales banques opérant en RDC, nous a intéressé de penser sur la mise en place d'un système de sécurité physique pour la détection des mouvements au niveau du coffre-fort dans sa succursale à Goma. L'objectif de ce système est de protéger les actifs de l'établissement financier et de ses clients contre les actes de vol ou d'effraction.

En conclusion, nous pouvons dire que la sécurité est un enjeu majeur pour les banques et les institutions financières du monde entier, en particulier dans les zones où la criminalité est élevée. Les banques doivent prendre des mesures proactives pour protéger leurs locaux et leurs actifs afin de garantir la sécurité de leurs clients. Au niveau continental, l'Union Africaine travaille pour renforcer les capacités de sécurité et de défense des États membres. En RDC, les banques ont été touchées par des actes de vandalismes ou de vol avec violence,

ce qui rend nécessaire la mise en place de mesures de sécurité supplémentaires pour protéger les biens de l'établissement financier et de ses clients.

I.2. Énoncé du problème ou La Problématique

Il est indéniable que l'informatique représente la plus grande révolution et l'innovation la plus marquante de l'histoire de l'humanité moderne. Les origines de l'informatique remontent à l'aube de l'humanité, lorsque l'homme a commencé à utiliser ses mains pour compter et à exploiter ses ressources et ses richesses. Le premier objectif des systèmes d'information en entreprise était d'automatiser les tâches opérationnelles. Aujourd'hui, les logiciels et les réseaux informatiques offrent des solutions pour tous les aspects de la vie, qu'il s'agisse de domaines professionnels ou d'applications personnelles. Le développement de ces systèmes a conduit à l'émergence de nouvelles technologies qui améliorent leur sécurité et leur offrent des fonctionnalités de plus en plus étendues.

Toutefois, il a été observé que malgré la mise en place de systèmes de sécurité automatisés au sein de nombreuses entreprises et des banques, ces derniers ne sont pas toujours efficaces. En cas de danger, les individus ne sont pas informés en temps et en heure. De plus, l'absence de mesures de sécurité adéquates peut entraîner des problèmes imprévus au sein des coffres forts des entreprises, des banques et des institutions financières (Anderson, 2008).

Le principal défi de cette recherche est la méthode la plus appropriée pour détecter le mouvement d'un coffre-fort tout en minimisant les coûts et en assurant la fiabilité du système. Il est également important de trouver une méthode qui peut être installée facilement et qui ne nécessite pas d'entretien coûteux.

Le problème à résoudre dans cette étude porte sur la sécurité du coffre-fort de l'Equity Banque à Goma. En effet, les coffres-forts des banques et des institutions financières sont souvent ciblés par les malfaiteurs, qui cherchent à voler les biens précieux qui y sont conservés. 0

Dans ce contexte, il est essentiel que la banque et l'institution financière dispose d'un système de sécurité fiable pour détecter toute tentative d'intrusion ou de vol. Cependant, l'absence d'un système de sécurité adéquat peut mettre en danger la sécurité des biens des clients de la banque et de l'institution financière elle-même.

C'est pourquoi cette étude vise détecter tous les mouvements et les risques liés au coffre-fort pour proposer des solutions concrètes et renforcer la sécurité des biens en gardant en sécurité les biens qui sont dans le coffre-fort de l'Equity Banque à Goma.

I.3. But et objectifs

1. Objectif Général

L'objectif général de cette étude est de mettre en place un système de sécurité physique basé sur arduino capable de détecter les mouvements Au niveau du coffre-fort de l'Equity Bank à Goma et de déclencher la sirène en cas de Mouvement suspecte, afin de garantir la sécurité des biens des clients de la banque et de l'institution elle-même.

2. Les objectifs Spécifiques

Les objectifs spécifiques incluent :

- Analyser les besoins spécifiques au niveau de la succursale de l'Equity Bank à Goma en matière de sécurité physique pour la détection des mouvements au niveau du coffre-fort..
- Concevoir et développer un système de sécurité basé sur Arduino qui utilise des capteurs de mouvement pour détecter toute présence suspecte.
- Assurer une réactivité immédiate en cas de détection de mouvement en déclenchant directement une sirène d'alerte.
- Proposer des recommandations pour l'optimisation du système, par exemple en intégrant d'autres fonctionnalités de sécurité telles que la surveillance Vidéo ou en renforçant la résistance aux tentatives de sabotage.

I.4. Méthodes et Techniques

I.4.1. La Méthodologie

Dans notre Travail de la recherche nous nous sommes servis de la méthode **PERT** : (Program Évaluation and Review Technique) qui nous permettra de décrire l'enchaînement des tâches en tenant compte des contraintes d'ordonnancement qui les relie. Cette méthode introduit la notion des tâches fictives de durée égale à 0 au début et la fin, la tâche fictive de début reliant toutes les tâches sans prédécesseurs à la tâche fictive de fin reliée sans successeur.

1.4.2. Les techniques

- **Technique d'observation** : Qui nous à faciliter une observation libre sur les différentes institutions financières et des banques, la façon dont se déroulent les mouvements au niveau du coffre-fort.
- **Technique documentaire** : Cette technique est la source des connaissances, elle nous a inspiré à travers des Toutes les travaux scientifique, livres, document et beaucoup d'autres ouvrages qui cadrent avec notre sujet de recherche.

I.5. Choix et Intérêt du sujet

Le choix du sujet de renforcement de la sécurité d'un coffre-fort de banque est pertinent et important car il concerne la protection des biens des clients, des dépôts et des actifs financiers détenus dans ces coffres forts. La sécurité est une préoccupation majeure pour les banques, en particulier dans les régions où le taux de criminalité est élevé. La sécurité des coffre-fort est l'une des priorités les plus importantes des établissements bancaires, car elle peut avoir un impact significatif sur leur réputation, leur responsabilité morale et leur crédibilité. Les techniques identifiées pour renforcer la sécurité peuvent aider à prévenir les vols, les cambriolages et les pertes financières. Il est donc crucial de mettre en place des mesures de sécurité efficaces pour garantir la sécurité des biens des clients et renforcer la confiance des clients envers la banque.

I.6. Délimitation de la Recherche

Il est affirmé qu'un travail scientifique, pour être bien précis, doit être délimité. Raison pour laquelle, Nous n'allons pas aborder toutes les questions liées à la mise en place d'un système des sécurités pour la détection de mouvement car elle paraît une matière très complexe. Ainsi nous avons pensés limiter Notre étude dans l'espace en mettant en place un système de sécurité pour la détection des mouvements au niveau du coffre-fort. Au niveau de succursale de l'Equity Banque Qui se localise physiquement en RDC, province du Nord-Kivu, Ville de Goma.

Dans le temps, ce travail porte sur la période allant de Février 2022 à octobre 2023, mais le nouveau système servira pour une période indéterminée.

I.7. Importance de la Recherche

En somme, cette recherche vise à proposer une solution efficace pour la détection de mouvement de coffre-fort qui répond aux besoins des utilisateurs. En développant des systèmes de sécurité fiable

I.8. Subdivision du Travail

Le présent travail est subdivisé en cinq chapitres structures comme suit :

Chapitre i : Introduction

Chapitre ii : Étude théorique et revue de la littérature

Chapitre iii. Analyse du système d'information existant

Chapitre iv. Modélisation du système futur

Chapitre v. Présentation du système réalisé

DEUXIÈME CHAPITRE : ÉTUDE THÉORIQUE ET REVUE DE LA LITTÉRATURE

II.1. Introduction

Dans ce chapitre nous allons parler sur la revue de la littérature et définir quelques concepts fondamentaux sur lequel se base notre étude.

II.1. Revue de la littérature empirique (État de la question)

Cette section présente une synthèse des études antérieures menées sur le même sujet de recherche.

Dans cette optique, plusieurs travaux de recherche ont été menés pour développer des systèmes de sécurité pour le coffre-fort. Par exemple,

1. Une étude menée par **Carlier et Johnson. (2014)** ont présenté un travail scientifique sur un système de sécurité innovant basé sur des capteurs et des caméras pour détecter les mouvements suspects au niveau du coffre d'une voiture. Les chercheurs ont utilisé une approche multidisciplinaire en combinant des techniques de traitement d'images, de vision par ordinateur et de reconnaissance de formes pour analyser en temps réel les images capturées par les caméras. Cela leur a permis d'identifier et de signaler tout mouvement suspect pouvant indiquer une tentative de vol ou d'intrusion dans le coffre. (Johnson, 2014)
2. L'efficacité des mesures de sécurité **selon** (BOUREGHIDA ZAKARIA, 2021) Une étude menée par Conception et Réalisation d'une serrure électronique codée équipée par un Système d'alerte à base d'Arduino. Leurs projet s'intéressé à la sécurité domestique en particulier aux systèmes de verrouillage de porte, il avait fait L'étude et la réalisation d'une serrure de porte codée équipée d'un système d'alerte SMS. Le système était basé sur la plate-forme Arduino. Il garantira un accès sans clé car le code pin était entré à l'aide d'un clavier, Si le code pin est correct la porte s'ouvrira automatiquement sinon l'alarme sera activée après trois fausses tentatives... De plus, la serrure de porte était équipée d'un système SMS (module GSM) la porte peut être ouverte à distance simplement en envoyant un message texte, De plus, elle envoie des messages d'alerte lorsque le mot de passe est modifié ou après trois mauvaises tentatives (BOUREGHIDA ZAKARIA, 2021)
3. Une autre étude menée par **Martinez Garcia et Lopez. (2019)** ont proposé un système de sécurité basé sur l'utilisation de capteurs de pression pour détecter les tentatives d'ouverture du coffre-fort. Ils ont proposé un système de sécurité novateur basé sur des capteurs d'inertie pour détecter les mouvements suspects au niveau du coffre et ils ont utilisé des capteurs MEMS (Micro Electro-Mechanical Systems) pour mesurer les accélérations et les inclinaisons

du coffre. Ces données ont été analysées en temps réel à l'aide d'un algorithme de détection de mouvement spécialement conçu pour identifier les activités suspectes, telles que les tentatives de vol ou d'effraction. Les résultats ont montré que le système était capable de détecter avec précision ces mouvements suspects (Lopez, 2019).

4. L'article intitulé « Systèmes de sécurité pour la détection des mouvements dans les coffres-forts » par Dupont et Martin, publié dans le journal of Security Technology, se concentre sur les différents systèmes de sécurité utilisés pour détecter les mouvements au niveau des coffres-forts. Les auteurs explorent diverses technologies telles que les capteurs des pressions, les capteurs de vibration, les capteurs infrarouges et les systèmes de vision par ordinateur. L'article examine en détail les avantages et les limites de chaque technologie, ainsi que leur application pratique dans les situations réelles (Martin D. e., 2016).
5. Dans l'article intitulé « Évaluation des performances des systèmes de sécurité pour la détection des mouvements dans les coffres-forts » Renaud Lambert et Lefebvre réalisent une évaluation approfondie des performances des différents systèmes de sécurité utilisés pour la détection des mouvements dans les coffres-forts. Les auteurs présentent une méthodologie complète pour évaluer la fiabilité, la précision et la sensibilité de ces systèmes. Ils fournissent également des recommandations pour améliorer les performances des systèmes existants et développer de nouvelles solutions plus efficaces (Lefebvre, 2021).

Le point de divergence ou de démarcation entre ton travail et ceux qui existe

Partant de tous ces travaux précités, notre projet de recherche se base sur le système de sécurité physique pour la détection des mouvements au niveau du coffre-fort qui est basé sur la carte arduino qui est connectée sur une sirène. Lorsqu'il y a la n'importe quel détection de mouvement le système se déclenche automatiquement. Ce pendant pour identifier le propriétaire du coffre-fort à tous les mouvements nous avons essayé d'utiliser la carte RFID pour désactiver le système à la présence de l'utilisateur et le réactive lors de sa sortie

II.2. Revue de la littérature théorique

Après la lecture des nombreux chercheurs qui ont traité sur le thème de systèmes de sécurité pour la détection des mouvements il est constaté que les solutions pour la détection des mouvements peuvent être classées en plusieurs manières. Dont on peut avoir le système de sécurité à l'aide des caméras de surveillance, Systèmes d'alerte à l'aide de module GSM et déclencher une alerte sonore avec une sirène. Partant des manières du système nous sommes inspirés par Mise en place d'un système de sécurité physique pour la détection des mouvements au niveau du coffre-fort « cas de l'Equity Bank ».

Notre recherche vise à répondre quelque problème qui survient lorsqu'il s'agit de renforcer la sécurité en utilisant la carte arduino Nano et les capteurs pour détecter les mouvements et déclencher d'une manière automatique une alerte sonore à l'aide d'une sirène. Elle offre une solution abordable, flexible et automatisée pour la surveillance et la prévention des intrusions au niveau du coffre-fort.

C'est à la fin de notre recherche, que nous allons proposer à l'institution financier « L'Equity Bank » un système de sécurité pour la détection de mouvement au niveau de leurs coffre-fort.

II.4. Définition des Concepts

Cette section définit les concepts clés liés à la question de recherche. Pour notre sujet, cette section peut inclure des définitions de termes tels que "système de sécurité", "détection de mouvement" et "coffre-fort".

II.4.1. Système de sécurité

Un système de sécurité est défini comme "un ensemble d'éléments interconnectés qui fonctionnent ensemble pour détecter, prévenir, dissuader et répondre aux menaces, aux perturbations ou aux incidents pouvant affecter la sécurité d'une personne, d'une propriété, d'un lieu ou d'un système". (Dolan, 2017)

voici les différentes définition du système de sécurité selon les auteurs

1. Selon le livre "Sécurité des systèmes d'information" un système de sécurité est défini comme "l'ensemble des moyens techniques, organisationnels et humains mis en place pour prévenir, détecter et réagir face aux menaces qui pèsent sur les informations et les systèmes informatiques (Festor, 2018)."

2. Dans son ouvrage "Gestion des risques : principes et pratiques", Gérard Friesé définit le système de sécurité comme "l'ensemble des mesures et des actions mises en place pour prévenir, détecter et réagir face aux risques susceptibles d'affecter la sécurité des biens et des personnes dans un environnement donné". (Friesé, 2016)

3. Le livre "La sécurité privée en France" par Georges Feneuil et Thierry Obrist, publié par Larcier en 2014, propose la définition suivante : "Le système de sécurité est l'ensemble des installations et des mesures prises afin d'assurer la protection des biens, des personnes et de l'information contre les actes malveillants ou les accidents (Obrist, 2014)."

4. Dans "Sécurité informatique et malwares : Analyse des menaces et mise en œuvre des contre-mesures", Pierre-Paul Allard donne la définition suivante : "Un système de sécurité est l'ensemble des dispositifs techniques et des procédures utilisés pour protéger les systèmes informatiques contre les attaques, les intrusions et autres incidents de sécurité (Allard, 2016).

5. Le livre "Management et Contrôle de la Sécurité des Systèmes d'Information" de Jean-Louis Rochet, publié par Lavoisier en 2019, propose la définition suivante : "Le système de sécurité est un ensemble intégré de politiques, de procédures, de mesures techniques et organisatrices mises en place pour protéger les systèmes d'information contre les menaces qui les affectent (Rochet, 2019)."

Quels sont les avantages d'un système de sécurité domestique ?

Protection D'abord et avant tout, un système de sécurité domestique vise à protéger votre propriété et les personnes qui s'y trouvent contre les cambriolages, les intrusions dans la maison, les incendies et autres catastrophes environnementales telles que les tuyaux éclatés. Les services de surveillance professionnels le font, que vous soyez conscient du problème ou non, et ils peuvent également vous aider en cas d'urgence médicale. Si un système de sécurité représente une dépense importante, le coût d'un cambriolage est en moyenne de 2 400 \$ par victime, sans parler de l'impact psychologique qu'il peut avoir.

Quels sont les différents types de sécurité informatique ?

Les risques informatiques sont devenus l'une des inquiétudes capitales de la majorité des entreprises, quelle que soit leur taille et leur domaine d'activité. Les menaces liées au piratage et à la privation de données restent les secondes menaces les plus graves après le risque d'interruption d'activité. Les pirates informatiques utilisent des techniques de plus en plus sophistiquées. C'est pourquoi la protection de vos actifs numériques et de votre équipement réseau est essentielle (System C. , 2023).

1. La sécurité du réseau et la sécurité Internet

Les sécurités du réseau sont utilisées pour éviter que des utilisateurs malveillants entrent dans vos réseaux. Cela permet de garantir la disponibilité, la fiabilité et l'intégrité du réseau. Ces types de sécurité sont nécessaires pour empêcher les pirates d'accéder aux données du réseau. Cela les empêche également d'avoir un impact négatif sur les capacités de l'utilisateur

à atteindre ou à utiliser les réseaux. La cybersécurité devient de plus en plus complexe à mesure que les entreprises augmentent le nombre de terminaux qu'elles utilisent et migrent leurs services vers un cloud public. La sécurité Internet concerne la protection des informations envoyées et reçues dans le navigateur, ainsi que la sécurité des applications Web. Ces défenses sont mises en place pour contrôler les trafics Internet et rechercher les programmes malveillants et les mouvements intrus. Ces protections peuvent se présenter sous la forme des pare-feux, de préceptes anti-logiciel offensif et de système anti-logiciel dénonciateur (System C. , 2023).

2. La sécurité de point d'extrémité et sécurité en nuage

La sécurité des terminaux offre une protection au niveau de l'appareil. Les appareils pouvant bénéficier de la sécurité des terminaux incluent les téléphones portables, les tablettes, les ordinateurs portables et les ordinateurs de bureau. La sécurité des points de terminaison empêche vos appareils d'accéder à des réseaux malveillants qui peuvent constituer une menace pour votre organisation. Les logiciels avancés de protection contre les logiciels malveillants et de gérance des outils sont l'exemple des sécurités du point d'extrémité. Les applications, les données et les identités sont migrées vers le cloud, ce qui signifie que les utilisateurs sont connectés directement à Internet, sans protection par les piles de sécurité traditionnelles. La sécurité du cloud rend l'utilisation des applications ou logiciels en tant que service et des clouds publics plus sûrs (System C. , 2023).

3. La sécurité des applications

Avec la sécurité des applications, les applications sont particulièrement codées lors de l'ouvrage pour être aussi protégées afin qu'elles ne soient pas fragiles aux effractions. Ces couches de sécurisation complémentaire incluent les évaluations des codes de l'application et l'identification des vulnérabilités potentielles au niveau logiciel (System C. , 2023).

La sécurité physique du Coffre-fort : fait référence aux dispositifs et aux mécanismes mis en place pour protéger le contenu du coffre-fort contre les accès non autorisés, le vol, l'incendie ou d'autres dangers potentiels. Cela comprends l'utilisation de matériaux résistants, de systèmes de verrouillage complexes, de systèmes de surveillance vidéo et de systèmes d'alarme pour assurer la protection des objets de valeur, documents importants et autres biens essentiels stockés dans le coffre-fort (Sravani Bhattacharjee, 2019).

II.4.2. Détection des mouvements

1. Selon le livre "Traitement du signal pour la détection et la localisation d'objets" par Jean-Philippe Farrugia, publié par ISTE Editions en 2013, la détection des mouvements est décrite comme "le processus consistant à détecter et à suivre les changements de position ou d'état d'un objet par rapport à son environnement, en utilisant des capteurs ou des caméras, afin de fournir des informations sur le mouvement." (Farrugia, 2013)
2. Dans "Vision par ordinateur : Algorithmes et applications" de Richard Szeliski, publié par Dunod en 2014, la détection des mouvements est définie comme "l'extraction d'informations relatives aux mouvements des objets dans une séquence d'images ou une vidéo, généralement basée sur l'analyse des différences entre images successives." (Szeliski, 2014)
3. Dans le livre "Analyse vidéo par vision artificielle" de Abdelaziz Bensrhair et Djamel Eddine Benzaoui, publié par Hermès Science Publications en 2003, la détection des mouvements est décrite comme "la tâche consistant à extraire des informations de mouvement à partir d'une séquence vidéo, afin de détecter les objets en mouvement, leur direction et leur vitesse." (Benzaoui, 2003)

Voici quelques types de détection des mouvements couramment utilisés, accompagnés de leurs définitions et caractéristiques.:

1. Détection des mouvements par différences d'images (background subtraction) : Cette méthode consiste à soustraire une image d'arrière-plan fixe à une image en mouvement afin de détecter les objets en mouvement. Les points forts de cette approche sont sa simplicité et sa rapidité. Cependant, elle peut être sensible aux variations de luminosité ou aux changements d'éclairage. (Szeliski, 2010)

2. Détection des mouvements par flux optique : Il s'agit de suivre le déplacement apparent des pixels entre deux images consécutives pour détecter les mouvements. Le flux optique peut être calculé en utilisant différentes méthodes comme la méthode basée sur la luminance ou celle basée sur les gradients. Cette approche est efficace pour détecter les petits mouvements et peut fournir des informations sur la direction et la vitesse des objets en mouvement. (Prince, 2012)

3. Détection des mouvements par modélisation statistique : Cette technique repose sur la modélisation statistique du mouvement pour identifier les anomalies ou les événements

intéressants dans une séquence vidéo. Elle utilise souvent des modèles probabilistes tels que les modèles occlusions, les modèles de mélange gaussien, ou les modèles de Markov cachés (Halasan, 2013).

Voici quelques caractéristiques générales des méthodes de détection des mouvements :

1. Sensibilité au mouvement : Les méthodes de détection des mouvements peuvent varier en termes de sensibilité, c'est-à-dire leur capacité à détecter avec précision les petits ou les grands mouvements (Sarkar, 2013).

2. Robustesse aux variations d'éclairage : Certaines méthodes peuvent être plus robustes que d'autres lorsqu'il s'agit de détecter les mouvements dans des conditions d'éclairage variables, telles que des changements de luminosité ou des ombres (Bouwman, 2014).

3. Capacité de suivi du mouvement : Certaines techniques de détection des mouvements peuvent également suivre le mouvement d'un objet dans le temps, permettant ainsi de déterminer sa trajectoire et sa vitesse (Panwar, 2013).

4. Complexité et ressources requises : Les différentes méthodes de détection des mouvements peuvent varier en termes de complexité algorithmique et des ressources informatiques nécessaires pour les exécuter. Certaines méthodes sont plus simples et moins exigeantes en termes de calcul, tandis que d'autres peuvent nécessiter des ressources plus importantes (Kiani, 2017).

5. Précision et taux de fausses détections : La précision d'une méthode de détection des mouvements détermine sa capacité à détecter correctement les objets en mouvement sans générer de fausses alarmes. Un bon équilibre entre la détection des vrais mouvements et la minimisation des fausses détections est important (Aliaga, 2014).
 Veuillez noter que ces caractéristiques peuvent varier en fonction des approches spécifiques utilisées dans la détection des mouvements.

Comment fonctionne un détecteur de mouvement ?

Le principe du détecteur de mouvement est simple : déclencher un type d'action précis lors de la détection de mouvements dans sa zone d'opérations. Ces actions peuvent consister à allumer ou à éteindre la lumière, déclencher une alarme, ou envoyer un signal à un appareil électronique, comme un smartphone ou un ordinateur.

Il est composé d'un minuteur qui permet de faire le décompte de la durée de l'action. Cette dernière est renouvelée à chaque détection, qui est assurée par les capteurs dans l'appareil. En fonction de la technologie utilisée dans le détecteur, le capteur peut être passif ou à infrarouge. Il peut également avoir un système laser ou mixte.

II.4.3. Les capteurs

Les capteurs sont les dispositifs ou les instruments permettant de mesurer, de détecter ou de transmettre une grandeur physique ou chimique. Ils convertissent ces grandeurs en signaux électriques exploitables par d'autres systèmes. Les capteurs peuvent être utilisées dans de nombreux domaines tels que l'industrie, l'environnement, la santé, l'automobile, etc. (Mondon, 2016)

Voici les définitions des capteurs données par différents auteurs en langue française, avec les informations de livres, auteurs, dates et maisons d'édition correspondantes :

- le capteur comme "un dispositif destiné à recevoir des informations sur l'environnement dans lequel il est placé, à les traiter pour en extraire la grandeur utile et à les convertir en un signal exploitable par un système électronique" (2007, Dunod). (Dulau, 2007)
- "Dispositif qui permet de mesurer une grandeur physique et de la convertir en signal électrique" (française, 1992)
- Selon le site Techno-Science.net, un capteur est un "dispositif capable de transformer une grandeur physique (température, pression, lumière, etc.) en un signal électrique utilisable par un système électronique de mesure, de commande ou de contrôle" (consulté en avril 2023).
- Dans "Les systèmes de mesure", Jean-Paul Corriou définit le capteur comme "un élément transducteur prenant des stimuli physiques ou chimiques d'origine extérieure et les convertissant en signaux électriques ou électroniques" (2001, Dunod).

II.4.4. Coffre-fort

Un coffre-fort : est un dispositif de sécurité conçu pour protéger des objets de valeur, des documents importants ou de l'argent contre le vol, l'incendie ou d'autres dommages. Il est généralement fabriqué en acier résistant et est équipé de mécanismes de verrouillage sécurisés tels que des serrures à combinaison ou des serrures électroniques. Les coffres fors sont souvent utilisées dans les banques, les entreprises, les hôtels, les résidences et d'autres lieux nécessitant une protection accrue des biens précieux (Perrot, 2016).

Comment bien choisir son coffre-fort ?

Comme le cambriolage est, un fléau dont un bon nombre de personne est victime chaque jour, trouver un moyen de prévenir une telle catastrophe est le seul moyen d'y échapper. Certainement, vous avez chez vous des biens de valeur que vous voulez protéger à tout prix des regards curieux et des mains baladeuses, pour conserver vos affaires personnelles, misez sur la performance d'un **coffre-fort**. Mais avant l'acquisition de cet équipement, il est bon de préciser quelques points essentiels. Tout d'abord, il est très important de savoir le niveau de sécurité de chaque coffre-fort disponible sur le marché. Avec l'évolution de la technologie, presque tous les coffre-fort peuvent résister à une montée de la température lors d'un incendie ou encore peuvent conserver son contenu d'une inondation. Hautement sécurisés, les modèles de coffre-fort à encastrer proposent un niveau de sécurité avancé vu qu'ils ne sont accessibles que par une seule face (Bourgoin, 2018).

Coffre-fort à encastrer : Est un équipement de sécurité conçu pour être intégré dans une structure solide telle qu'un mur, un sol ou un meuble, offrant ainsi une protection supplémentaire contre le vol. il est généralement fabriqué en acier robuste et possède des systèmes de verrouillage avancés, tels que des serrures à combinaison. Les caractéristiques spécifiques peuvent varier en fonction du fabricant et du modèle choisi (Lebel, 2010).

Ensuite, il faut voir la capacité de stockage d'un coffre-fort. Pour les modèles à poser, ils peuvent contenir beaucoup plus que des objets de valeurs ou des documents confidentiels. Vous pouvez y mettre aussi un vos pistolets de protections ou encore vos données numériques. Cette contenance dépend, en général, du besoin que vous voulez évaluer. Pour le poids d'un **coffre-fort**, les petits modèles à encastrer peuvent peser quelques kilos et pour les types de coffre-fort à poser utilisés dans les institutions bancaires, leurs poids peuvent atteindre des tonnes. Enfin, le dernier point à éclaircir est la vérification du modèle de serrure d'un coffre-fort. Cette serrure peut fonctionner sous différents aspects. Certaines serrures peuvent être déverrouillées avec une clé manuelle, mais il en existe aussi qui ne s'ouvrent que par le biais d'un code digital. Il y a aussi des serrures mixtes pour renforcer la sécurité de son contenu (Widmer, 2014).

II.4.5. Mise en place

La mise en place désigne l'ensemble des actions et des préparatifs nécessaires pour organiser et mettre en œuvre quelque chose. Il s'agit de planifier, d'ordonnancer et de mettre en pratique les différentes étapes ou composantes d'un projet, d'un processus ou d'une activité.

La mise en œuvre vise à assurer une exécution efficace et harmonieuse de ce qui a été conçu ou décidé au préalable. (Lambert, 2012)

II.4.7. PERT

« Program Evaluation Review Technique » (technique d'évaluation et d'examen de programmes) Le diagramme de PERT ou appelé « diagramme d'antériorité de tâches » a été développé par la marine américaine dans les années 1950 et a permis de gagner un an sur la construction d'un bateau. À partir d'un projet découpé en objectifs et en tâches, il permet de schématiser sous forme de réseau l'ordre d'enchaînement des actions qui composent le projet en faisant apparaître leurs liens de dépendance et leur chronologie pour aboutir au résultat du projet. En affectant un délai de réalisation sur chaque tâche ou action, ce diagramme permet de calculer la durée minimale de réalisation du projet en faisant apparaître le « chemin critique », c'est-à-dire le chemin le plus long en terme de délai, pour finir votre projet. Il permet d'optimiser la répartition des tâches dans le temps en autorisant par exemple, leurs réalisations en parallèle ou encore, en menant une réflexion sur les ressources à affecter au projet en accord avec les délais et étapes à suivre. Cet outil est donc aussi intéressant en management de projet. En aval du PERT on peut ensuite préparer un Diagramme de GANTT qui permet de gérer au quotidien son projet (Joseph J. Moder, 2014)

II.4.8. Une Plaque d'essais

Une plaque d'essais est un support permettant de réaliser des montages électroniques temporaires à des fins de prototypage ou de tests. Elle est composée d'un réseau de trous permettant d'insérer et de connecter facilement des composants électroniques, tels que des résistances, des condensateurs, des transistors etc. Les plaques d'essais offrent une grande flexibilité et facilitent l'expérimentation lors du développement de circuits électriques. (Initiation à l'électronique en partant de Zéro, 2019)

II.4.8. Une Sirène

Une sirène est un dispositif acoustique utilisé pour émettre des signaux sonores puissants et caractéristiques. Elle est généralement composée d'un moteur électrique entraînant un disque rotatif à plusieurs pales. Lorsque le disque tourne, il crée une vibration qui génère un son strident et perçant. Les sirènes sont couramment utilisées dans des domaines tels que la sécurité publique, les systèmes d'alerte d'incendie ou encore en navigation maritime. (Lavandier, 2015)

TROISIÈME CHAPITRE : MÉTHODOLOGIE DE RECHERCHE

III.1. INTRODUCTION

Dans ce chapitre, partant des différents problèmes rencontrés concernant le système de sécurité, pour arriver à pallier à tous ces problèmes, nous nous attacherons à analyser le système en présentant une estimation des coûts du projet et des matériaux pour sa réalisation.

III.2. Le projet

Un projet est un processus unique, consistant en un ensemble d'activités coordonnées et maîtrisées comportant des dates de début et de fin, entrepris dans le but d'atteindre un objectif conforme à des exigences spécifiques, incluant des contraintes de délais, de coûts et de ressources (Chasseray, 2019).

III. 3. Détermination des objectifs

Pour réaliser tout projet, il est nécessaire d'établir les objectifs pouvant aider à la détermination des tâches qui seront exécutées dans ce projet ainsi que le délai par le quel ce projet sera exécuté. Dans ce projet nous allons nous concentrer sur le système de sécurité physique pour la détection des mouvements au niveau du coffre-fort.

III.4. CHOIX DES OUTILS

III.4.1. Introduction

Dans ce contexte cette partie porte sur la présentation des matériels tels la carte Arduino, la sirène, la carte RFAID et le capteur mouvements et les autres composants périphériques.

III.4.2 Description Matériel

Pour réaliser Notre projet de mettre en place un système de sécurité pour la détection des mouvements au sein du coffre-fort nous avons besoin :

- Carte Arduino Uno.
- Capteur ultrasons.
- Capteur de Mouvement
- Buzzer
- Led
- Carte RFAID

III.4.2.1 Définition Matériel

1. Carte Arduino :

Est une carte de développement open-source largement utilisée dans le monde de l'électronique et de la programmation. Elle a été conçue par un groupe des chercheurs italiens dirigé par **Massimo Banzi**. Grâce à sa taille compacte et à sa facilité d'utilisation, elle est idéale pour les débutants et les amateurs. (Shilon, 2014)

Elle comprend le nécessaire pour que le processeur fasse son travail, il suffit de la connecter à un ordinateur via USB ou au courant électrique à travers d'un transformateur.

(Smith, 2019)

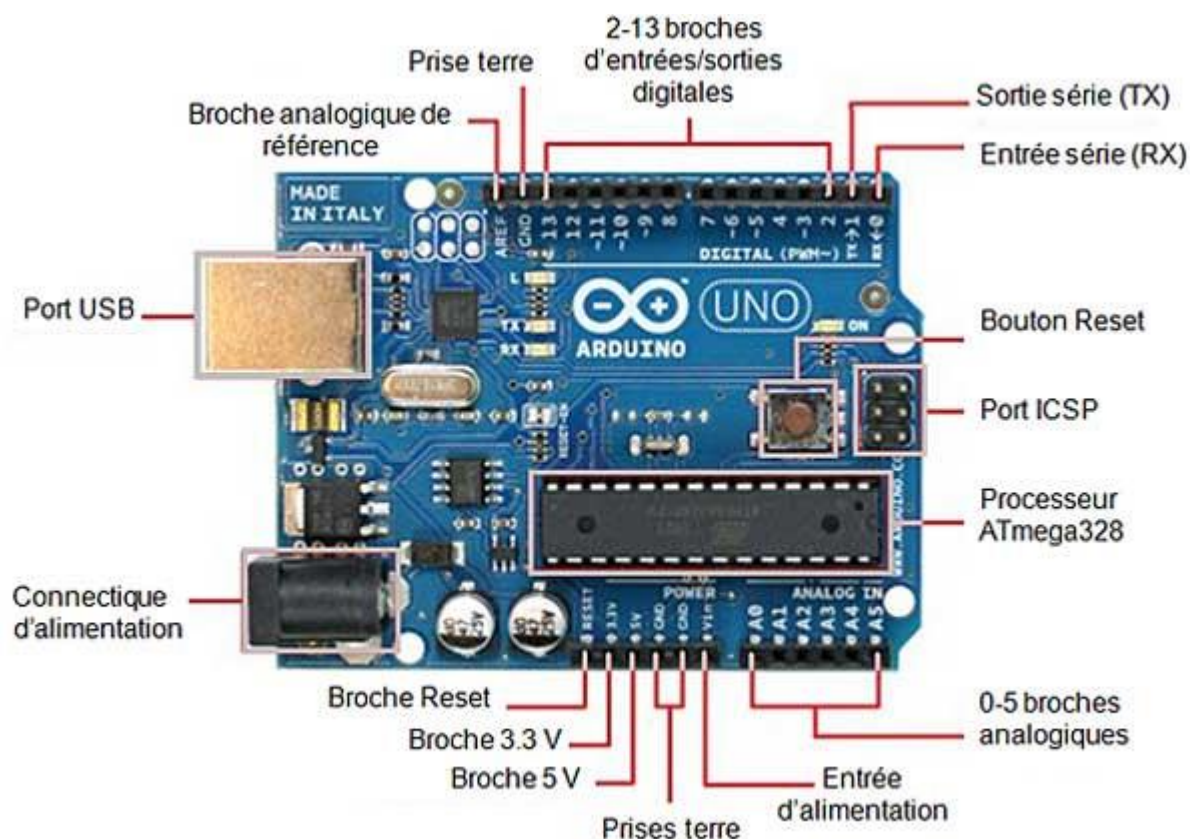


Figure 1 Carte Arduino

Composants de la carte Arduino UNO

Caractéristiques basiques :

- Microcontrôleur ATmega328 de 8 bits à 16 MHz que fonctionne à 5 V. **Mémoire flash** -> 32 KB. **EEPROM** -> 1 KB. **SRAM** -> 2 KB.

- Contient 14 pins numériques dont 6 peuvent être utilisés comme sorties PWM.
- 6 pins analogiques qui peuvent travailler dans un intervalle d'intensité jusqu'à 40 mA.
- Port USB.
- Connectique d'alimentation.
- Crystal 16 MHz.

2. **Capteur Ultrasons** : Est un dispositif électronique utilisé pour détecter la distance entre le capteur et un objet en utilisant des ondes sonores à haute fréquence. Il émet des impulsions ultrasoniques et mesure le temps écoulé entre l'émission et la réception de l'écho pour calculer la distance (Schmidt, 2015).

Capteur de distance à Ultrasons

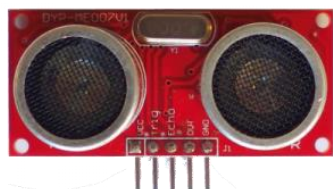


Figure 3. Capteur de distance à Ultrasons

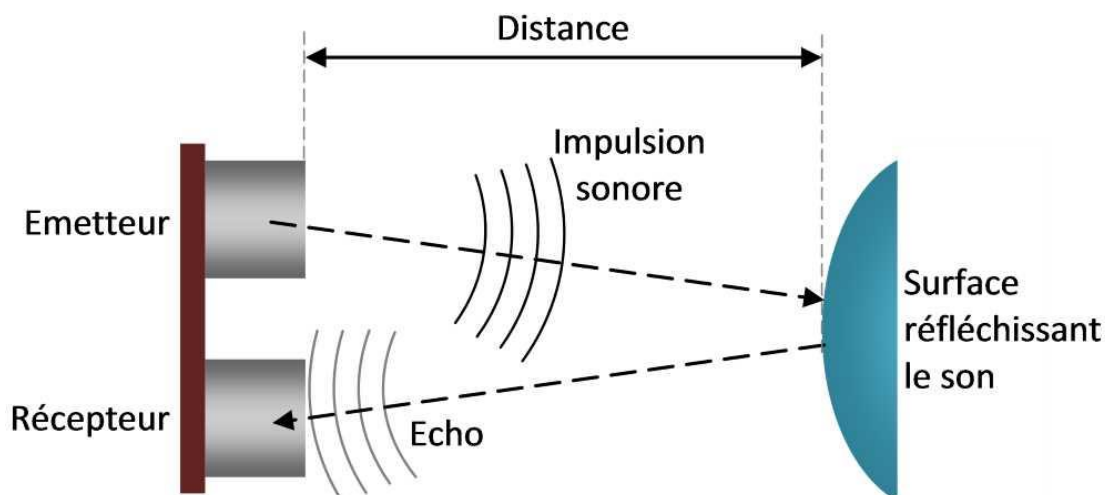
Principe

Les **capteurs de distance à ultrasons** utilisent le principe de l'**écho** pour déterminer la distance à laquelle se trouve un objet :

Un court signal sonore est envoyé (inaudible car dans le domaine des ultrasons – environ 40kHz) ;

Le son est réfléchi par une surface et repart en direction du capteur : c'est l'**écho** ;

Une fois revenue à son point de départ, l'onde sonore est détectée par le capteur.



Démonstration des Capteur de distance à Ultrasons

La **durée** entre l'instant de l'émission et l'instant de la réception peut être mesurée. Le signal ayant parcouru 2 fois la **distance** entre le capteur et la surface (un aller-retour), on peut la calculer ainsi :

$$\text{Distance} = \frac{1}{2} \times \text{vitesse du son} \times \text{durée}$$

Remarque la vitesse du son est environ égale à 340 m/s.

Câblage

Comme la plupart des composants actifs, les capteurs de distance à ultrasons doivent être alimentés (5V le plus souvent).

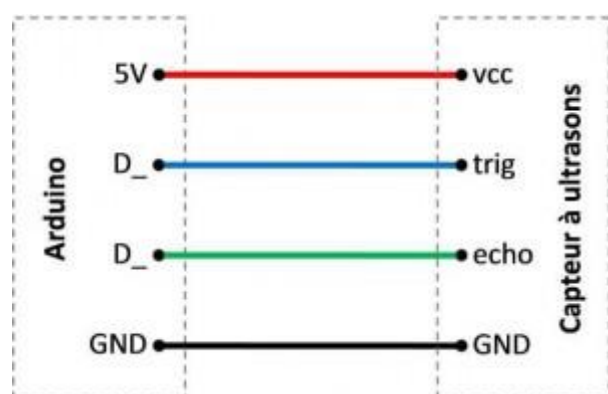


Figure 2 Câblage

Ils fonctionnent de la manière suivante :

- L'Arduino envoie au capteur par un port numérique une courte impulsion (10µs environ) à l'entrée « trigger » du capteur ;
- Cela déclenche l'émission d'un **signal sonore** très court (8 oscillations environ) ;

- Lorsque ce signal est parti, la sortie « *echo* » du capteur passe à l'état HIGH ;
- Dès que le signal sonore revient, il est détecté par le capteur dont la sortie « *echo* » repasse à LOW

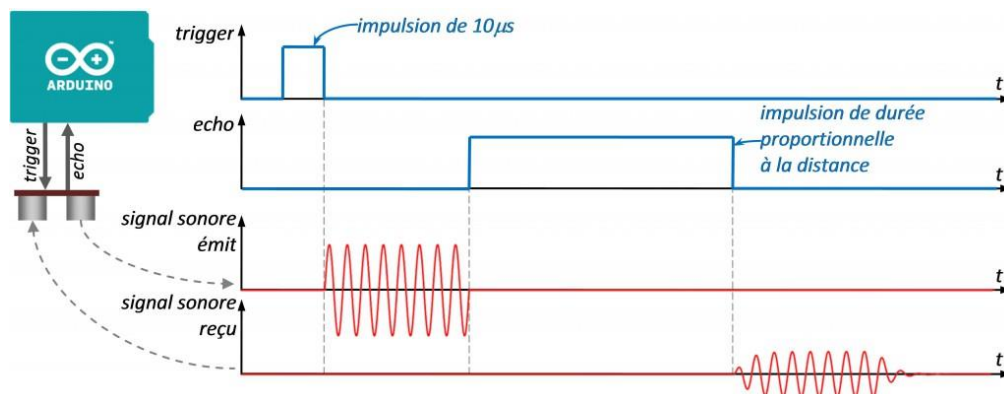


Figure 3 fonctionnement des capteurs Ultrason

Remarque : si le signal retour n'est pas détecté, la durée du signal « echo » est limitée à 36 ms environ (cela dépend des modèles), soit 6m environ.

- 3. Buzzer :** Est un composant électronique qui convertit un signal électrique en un son audible. Il est souvent utilisé pour émettre des alarmes ou des avertissements sonores (Gates, 2017).

Qu'est-ce qu'un buzzer : son fonctionnement et ses applications

Il existe de nombreuses façons d'interagir entre l'utilisateur et le produit. L'un des meilleurs moyens consiste à communiquer vocalement à l'aide d'un circuit intégré de sonnerie. Ainsi, comprendre certaines technologies de configuration pendant le processus de conception est très utile. Cet article présente donc un aperçu d'un appareil doté d'un signal audio tel qu'un bip ou un buzzer et de son fonctionnement avec les applications.

Qu'est-ce qu'un Buzzer ?

Un dispositif de signalisation sonore tel qu'un bip ou un buzzer peut être électromécanique, piézoélectrique ou mécanique. Sa tâche principale est de convertir le signal du son en son. Il fonctionne généralement sous tension continue et est utilisé dans les minuteriers, les alarmes, les imprimantes, les ordinateurs, etc. Dans différents modèles, il peut produire différents sons, tels qu'une alarme, de la musique, une cloche et une sirène.



Figure 4 buzzer

Buzzer Pin Configuration

La configuration des broches du buzzer est indiquée ci-dessous.

Il possède deux broches, positive et négative. Sa borne positive est marquée d'un symbole "+" ou d'une fiche plus longue. Cette broche est alimentée en 6 volts, tandis que la broche négative est représentée par un symbole "-" ou une broche courte et est connectée à la broche GND.

Histoire

L'histoire du sondeur électromécanique et du dispositif piézoélectrique est discutée ci-dessous.

Électromécanique

Ce buzzer a été mis au point par le scientifique américain Joseph Henry en 1831, mais a été utilisé dans les sonnettes de porte jusqu'à son retrait en 1930 au profit de cloches musicales à un seul ton.

Piézoélectrique

Ces buzzers ont été inventés par des fabricants japonais et ont été installés sur une grande variété d'équipements dans les années 1970 et 1980. Cette évolution est donc principalement due à la coopération des entreprises manufacturières japonaises. En 1951, ils ont reconnu le Comité de recherche appliquée sur le titanate de baryum, permettant ainsi aux entreprises de rivaliser et de produire de nombreuses créations piézoélectriques.

Informations techniques

Les spécifications du buzzer incluent les informations suivantes.

- La couleur est noire
- La plage de fréquences est de 3 300 Hz
- La température de fonctionnement est comprise entre -20°C et 60°C
- La tension de fonctionnement varie de 3 V à 24 V CC
- Le niveau de pression acoustique est de 85 dBA ou 10 cm
- Le courant d'entrée est inférieur à 15 mA

Types des buzzers

Il existe différents types de buzzers disponibles, notamment les suivants.

- Piézoélectrique
- Électromagnétique
- Mécanique
- Électromécanique
- Magnétique

4. **Led (Light Emitting Diodes)** : Sont les dispositifs électroniques qui émettent de la lumière lorsqu'un courant électrique les traverse. Elles sont utilisées dans de nombreux domaines tels que l'éclairage, les écrans d'affichage, les téléviseurs et les indicateurs lumineux (Tran-Thanh, 2017).
5. **Carte RFAID** : Est Une carté équipé d'une puce et d'une antenne qui permettent la communication sans fil avec des systèmes RFID. Elles sont utilisées pour diverses les applications telles que le contrôle d'accès, le suivi des marchandises et le paiement sans contact (Mohammad, 2018).

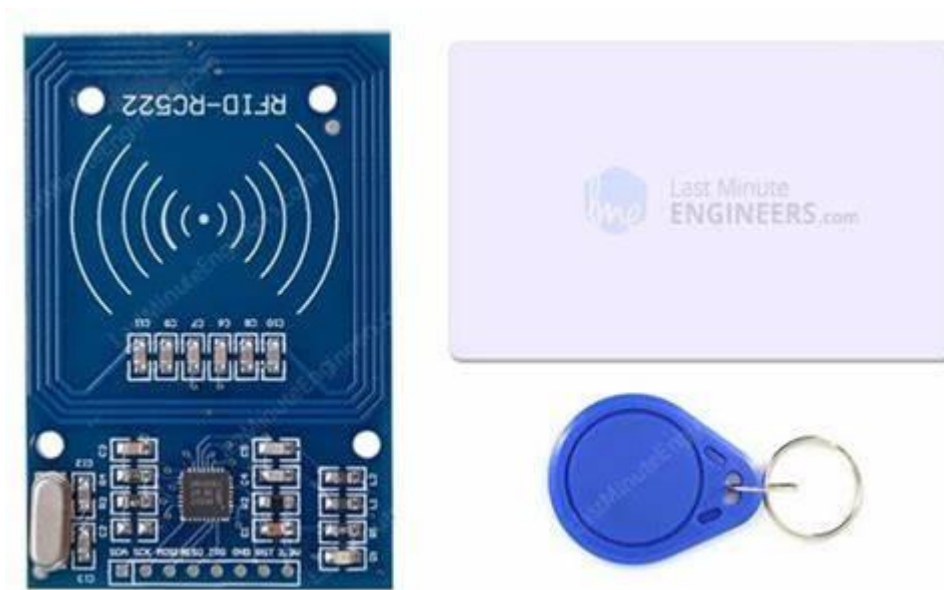


Figure 5 Quit RFID

III .5. Méthode D'ordonnement

Les méthodes d'ordonnement : Elle désigne l'ensemble des techniques et des procédures utilisées pour planifier et organiser les activités au sein d'une entreprise. Ces méthodes permettent de déterminer l'ordre dans lequel les tâches doivent être effectuées, en tenant compte des contraintes de temps, des ressources disponibles et des objectifs à atteindre (Kelleher, 2011).

La méthode Pert Est une méthode de gestion de projet qui s'appuie sur des techniques probabilistes pour évaluer la durée et l'ordonnement des activités dans un projet. Elle permet d'identifier les tâches critiques, c'est-à-dire celles qui ont un impact direct sur la durée totale du projet et de prévoir des marges de temps pour faire face à d'éventuels retards (Kerzner, Project Management : A Systems Approach to Planning, Scheduling, and Controlling, 2017).

Le diagramme de Gantt est un outil visuel utilisé dans la gestion de projet pour planifier et suivre l'avancement des différentes tâches d'un projet. Il permet de représenter graphiquement les dates de début et de fin de chaque tâche, ainsi que les dépendances entre elles (Institute, A Guide to the Project Management Body of Knowledge (PMBOK Guide), 2017).

III.6. PLANNING PRÉVISIONNEL DU PROJET

"Le planning prévisionnel du projet est un outil de gestion qui consiste à planifier et organiser les différentes tâches, étapes, ressources et délais nécessaires à la réalisation d'un

projet. Il permet d'anticiper les activités à effectuer et d'établir une séquence logique pour leur réalisation, tout en tenant compte des contraintes et des dépendances entre les différentes actions." (Crabé, 2018)

Mais aussi "Le planning prévisionnel du projet est un document synthétique qui répertorie toutes les activités à réaliser, leur durée prévue, les ressources nécessaires et les dates de début et de fin estimées. Il sert de référence pour planifier et suivre l'avancement du projet, en permettant d'anticiper les éventuels retards ou écarts par rapport au calendrier initial." (Portny, 2016)

En outre "Le planning prévisionnel du projet est un outil de planification qui permet de définir et d'organiser chronologiquement les différentes tâches et étapes nécessaires à la réalisation d'un projet. Il inclut également la gestion des ressources, des délais et des interdépendances entre les différentes activités, afin de garantir la performance et l'efficacité du projet." (Dufau-Joël, 2014)

ÉTAPES DU PLANNING PROVISIONNEL DU PROJET

- Identifier les tâches : Décomposez le projet en une liste de tâches nécessaires à sa réalisation.
- Estimer la durée de chaque tâche : Il s'agit d'estimer la durée optimiste, la durée pessimiste et la durée probable de chaque tâche. Ces estimations permettent de prendre en compte les aléas et les incertitudes liés au projet.
- Identifier les dépendances entre les tâches : Déterminez les relations de dépendance entre les différentes tâches du projet, telles que les tâches qui doivent être terminées avant de commencer d'autres tâches.
- Créer le réseau PERT : Utilisez les informations collectées précédemment pour créer un diagramme du réseau PERT. Ce diagramme représente les tâches sous forme de nœuds interconnectés par des flèches représentant les relations de dépendance.
- Calculer les dates au plus tôt et au plus tard : À l'aide des durées estimées et des dépendances identifiées, calculez les dates au plus tôt et au plus tard pour chaque tâche. La date au plus tôt indique la date à laquelle une tâche peut commencer, tandis que la date au plus tard indique la date limite à laquelle une tâche doit être terminée sans retarder le projet.
- Identifier le chemin critique : Identifiez les tâches qui se trouvent sur le chemin critique, c'est-à-dire les tâches dont tout retard entraînerait un retard dans le calendrier global du projet.

- Élaborer le calendrier du projet : Utilisez les informations du réseau PERT pour élaborer le calendrier du projet, en spécifiant les dates de début et de fin de chaque tâche.
- Réviser et ajuster : Comme pour toute planification prévisionnelle, il est important de réviser et d'ajuster régulièrement le planning PERT en fonction de l'avancement du projet et des changements rencontrés.

La méthode PERT permet de visualiser les relations et les dépendances entre les différentes tâches du projet, ainsi que d'identifier le chemin critique qui nécessite une attention particulière pour respecter le calendrier. Estimer la durée de chaque tâche, Identifier les dépendances entre les tâches, Créer le réseau PERT, Calculer les dates au plus tôt et au plus tard, Identifier le chemin critique, Élaborer le calendrier du projet et Réviser et ajuster

III.6.1. IDENTIFIER LES TÂCHES

- Analyse des besoins,
- Recherche et sélection des capteurs,
- Conception technique,
- Développement du logiciel,
- Intégration des matériels,
- Test et validation,
- Documentation et manuel d'utilisation,
- Formation des utilisateurs,
- Mise en œuvre et déploiement,
- Suivi et maintenance.

III.6.2. IDENTIFIER LES DÉPENDANCES ENTRE LES TÂCHES

À partir des durées des tâches que nous avons fournies, voici les dépendances potentielles entre les tâches :

- La tâche I ne nécessite aucune condition préalable pour être effectuée. Elle ne possède pas l'antériorité
- La tâche "Recherche et sélection des capteurs" dépend de la tâche "Analyse des besoins", car il est nécessaire de comprendre les besoins avant de pouvoir procéder à la recherche et à la sélection des capteurs.

Donc La tâche II nécessite que la tâche I soit réalisée. Donc la tâche II possède la tâche I comme antériorité

- La tâche "Conception technique" dépend de la tâche "Recherche et sélection des capteurs", car les spécifications techniques dépendent des capteurs choisis.

La tâche III nécessite le finissage de la tâche I et II. Donc la tâche III possède la tâche II comme l'antériorités,

- La tâche "Développement du logiciel" peut commencer une fois que la tâche "Conception technique" est terminée, car il faut d'abord avoir les spécifications techniques pour guider le développement du logiciel.

La tâche IV nécessite le finissage de la tâche III,

- La tâche "Intégration des matériels" peut commencer une fois que la tâche "Recherche et sélection des capteurs" et la tâche "Développement du logiciel" sont terminées, car il faut connecter les capteurs au logiciel développé.

La tâche V nécessite le finissage de la tâche II et IV,

- La tâche "Test et validation" doit être effectuée après l'intégration des matériels, car il faut s'assurer que les capteurs fonctionnent correctement avant de procéder aux tests.

La tâche VI possède la tâche V comme antériorités,

- La tâche "Documentation et manuel d'utilisation" peut être réalisée en parallèle avec les autres tâches, ou elle peut dépendre de toutes les tâches précédentes pour collecter les informations nécessaires à la rédaction de la documentation.

La tâche VII il est réalisée en parallèle avec les tâches précédentes pour collecter les information,

- La tâche "Formation des utilisateurs" peut commencer une fois que la tâche "Documentation et manuel d'utilisation" est terminée, car il faut disposer de la documentation finale pour former efficacement les utilisateurs.

La tâche VIII nécessite le finissage de la tâche VI,

- La tâche "Mise en œuvre et déploiement" peut commencer après la formation des utilisateurs, car il est préférable de former les utilisateurs avant de déployer pleinement le système.

La tâche IX possède la tâche VII comme antériorité,

- La tâche "Suivi et maintenance" peut être effectuée en parallèle avec les autres tâches ou

peut dépendre de toutes les tâches précédentes pour assurer un suivi et une maintenance appropriés.

En fin la tâche X peut dépendre de toutes les tâches précédentes pour assurer un suivi et une maintenance appropriés.

Ces dépendances permettent d'organiser les tâches dans un ordre logique, en tenant compte des prérequis et des contraintes du projet. Toutefois, il est important de noter que ces dépendances peuvent être ajustées en fonction des besoins spécifiques et des contraintes de votre projet.

III.6.3. TABLEAU DES ANTÉCÉDENTS

Tableau des antécédents : Est un outil utilisé dans la gestion de projet pour identifier et visualiser les relations de dépendance entre les tâches d'un projet. Il permet de représenter graphiquement les prérequis et les contraintes entre les différentes activités, afin de planifier efficacement l'ordre d'exécution des tâches (Institute, PMBOK Guide, 2017).

Code	Tâches	Antécédent immédiate	durée estime (en jrs)
I	Analyse des besoins	Aucune	2
II	Recherche et sélection des capteurs	I	3
III	Conception technique	II	5
IV	Développement du logiciel	III	6
V	Intégration des matériels	IV	4
VI	Test et validation	V	3
VII	Documentation et manuel d'utilisation	VI	3
VIII	Formation des utilisateur	VII	6
IX	Mise en place et déploiement	VIII	1
X	Suivie et maintenance	IX	3
TOTAL			36 JOURS

Tableau 1 **TABLEAU DES ANTÉCÉDENTS**

Cela signifie que chaque tâche doit être complétée après l'achèvement de ses tâches antérieures respectives. Par exemple, la tâche II ne peut commencer qu'après l'achèvement de la tâche I. de même, la tâche III ne peut commencer qu'après l'achèvement de la tâche II, et ainsi de suite.

III.6.4. ESTIMATION DU COÛT

L'estimation du cout d'un projet est une étape cruciale dans la planification et le suivi des ressources financières nécessaires à sa réalisation. Elle permet d'évaluer les dépendances prévues en matière de gestion des finances. (Vigneron, 2007)

III.6.4.1. Estimation du coût de main d'œuvre

Estimation du coût de la main d'œuvre : est un processus utilisé dans la gestion de projet pour déterminer les dépenses associées aux ressources humaines nécessaires à la réalisation d'un projet. Cela inclut le calcul des salaires, des charges sociales, des avantages sociaux et autre coûts liés à la main d'œuvre utilisée pour les différentes tâches du projet (Jr., 2011).

Code	Tâches	Antécédent précédente	durée estime	Nbre de personnes	CU en \$	CT en \$
I	Analyse des besoins	Aucune	2	3	10	60
II	Recherche et sélection des capteurs	I	3	3	10	90
III	Conception technique	II	5	3	10	150
IV	Développement du logiciel	III	6	1	10	60
V	Intégration des matériels	IV	4	2	10	80
VI	Test et validation	V	3	2	10	60
VII	Documentation et manuel d'utilisation	VI	3	1	10	30
VIII	Formation des utilisateur	VII	6	1	10	60
IX	Mise en place et déploiement	VIII	1	2	10	20
X	Suivie et maintenance	IX	3	1	10	30
TOTAL			36 jrs			640\$
IMPRÉVUE (10%)						64\$
COUT TOTAL GENERAL						704\$

Tableau 2 Estimation du coût de main d'œuvre

III.6.4.2. Estimation de coût des matériels

Estimation de coût de matériels : est une activité de planification financières qui consiste à évaluer les dépenses liées à l'acquisition ou à la location de matériel nécessaire à la réalisation d'un projet. Cela comprend les coûts d'achat, de location, de maintenance, de Transport et

Autres Frais associés aux équipements et aux matériaux utilisés dans le cadre du projet (Burnett, 2020).

MATÉRIEL	CARACTÉRISTIQUE	NOMBRE	PU	PT
Arduino	Arduino LLC	1	100\$	100\$
Capteurs	Détecteur de Mouvement	2	50\$	100\$
Câble	Câble	4	50\$	200\$
Système d'alerte	Sirène	1	80\$	80\$
Ordinateur	Laptop	2	500\$	1000\$
Plaque d'essais	Plaque d'essais	1	50\$	50\$
Jumps	Jumps	1	10\$	10\$
Résistance	Résistance	1	10\$	10\$
Étain	Étain	3	10\$	30\$
Moyen de déplacement	Transport		100\$	100\$
Système de conc	Carte RFAID	1	50\$	50\$
Accessoire	IMPRÉVUE		600\$	600\$
Total				2330\$

Tableau 3 Estimation de coût des matériels

III.6.4.3. Coût global du projet

Le coût Global d'un projet : est la somme de tous les coûts estimés, y compris les coûts de la main-d'œuvre, des matériels, des frais indirects, des frais de gestion et d'autres dépenses nécessaires à la réalisation du projet. Il représente ainsi le montant total que l'entreprise ou l'organisation devra investir pour mener à bien le projet (Wysocki, 2013).

Numéro	Désignation	Montant
1	Main d'œuvre	704\$
2	Coût des matériels	2330\$
Coût total général du projet		3034\$

Tableau 4 Coût global du projet

III.6.5 Créer le réseau PERT

Pour créer le réseau PERT, nous allons utiliser les tâches que nous avons énumérées ci-haut et les dépendances identifiées précédemment. Voici le réseau PERT pour votre projet :

1. Tâche I : Analyse des besoins (2 jours)
 - Aucune dépendance
2. Tâche II : Recherche et sélection des capteurs (3 jours)
 - Dépendance avec Tâche I
3. Tâche III : Conception technique (5 jours)
 - Dépendance avec Tâche II
4. Tâche IV : Développement du logiciel (6 jours)
 - Dépendance avec Tâche III
5. Tâche V : Intégration des matériels (4 jours)
 - Dépendance avec Tâche II et Tâche IV
6. Tâche VI : Test et validation (3 jours)
 - Dépendance avec Tâche V
7. Tâche VII : Documentation et manuel d'utilisation (3 jours)
 - Aucune dépendance
8. Tâche VIII : Formation des utilisateurs (6 jours)
 - Dépendance avec Tâche VII
9. Tâche IX : Mise en œuvre et déploiement (1 jour)
 - Dépendance avec Tâche VIII
10. Tâche X : Suivi et maintenance (3 jours)
 - Dépendance avec Tâche VII, Tâche VIII, et Tâche IX

Ce réseau PERT représente les différentes tâches de ce projet, avec leurs durées respectives et les dépendances entre elles. Il permet de visualiser l'enchaînement logique des tâches et d'identifier les tâches critiques, c'est-à-dire celles qui doivent être réalisées dans les délais pour que le projet soit terminé à temps.

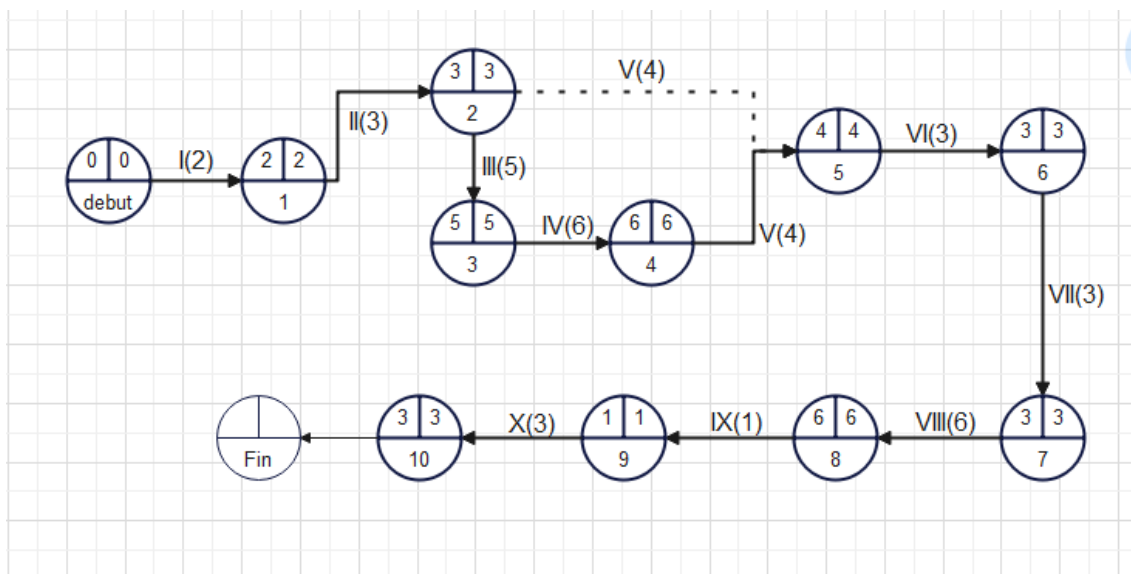


Figure 6 Le réseau PERT

III.6.6. Détermination de la date au plus tôt, date au plus tard, marge libre et marge total

III.6.6.1. Date au plus tôt

Date au plus tôt (DAT) : est une notion utilisée dans la gestion de projet pour déterminer le moment le plus précoce auquel une activité peut être planifiée ou achevée sans compromettre le calendrier global du Projet. C'est la date à laquelle une activité peut commencer dès que toutes ses contraintes de précédence et de ressources sont satisfaites (Institute, A Guide to the Project Management Body of Knowledge (PMBOK Guide), 2017).

Les dates au plus tôt (DAT) sont synonymes de début des dates au plus tôt « Les calculs des dates commencent tout d'abord par les DAT.

Pour une étape donnée, cette information détermine à quelle date minimum depuis le début du projet sera atteinte, au plus tôt, l'étape considérée. Pour ce faire, on se base sur l'estimation de la durée des tâches.

On part de l'étape du début, pour laquelle la DAT est initialisée à 0, et on parcourt le réseau en suivant l'agencement des tâches déterminé auparavant.

Pour calculer les dates d'une tâche, on procède de la manière suivante : ce que nous devons savoir est qu'il y a un seul chemin possible pour atteindre l'étape ; la date au plus tôt vaut la DAT antérieure à laquelle on ajoute la durée de la tâche liant les étapes :

Pour plusieurs tâches il y a plusieurs chemins possibles pour atteindre l'étape. On applique le procédé décrit ci-dessus (pour une seule tâche) pour chacune des tâches antérieures ; la date au plus tôt vaut le maximum parmi ces résultats :

Formule : $DAT = \text{Max}(DAT \text{ des activités précédentes}) + \text{Durée de l'activité}$

- $DAT I = 0$ (début du projet)
- $DAT II = DAT I + \text{durée I} = 0 + 3 = 3$ (début de la Tâche II)
- $DAT III = DAT II + \text{durée II} = 3 + 3 = 6$ (début de la Tâche III)
- $DAT IV = DAT III + \text{durée III} = 6 + 5 = 11$ (début de la Tâche IV)
- $DAT V = DAT IV + \text{durée IV} = 11 + 6 = 17$ (début de la Tâche V)
- $DAT VI = DAT V + \text{durée V} = 17 + 4 = 21$ (début de la Tâche VI)
- $DAT VII = DAT VI + \text{durée VI} = 21 + 3 = 24$ (début de la Tâche VII)
- $DAT VIII = DAT VII + \text{durée VII} = 24 + 3 = 27$ (début de la Tâche VIII)
- $DAT IX = DAT VIII + \text{durée VIII} = 27 + 6 = 33$ (début de la Tâche IX)
- $DAT X = DAT IX + \text{durée IX} = 33 + 1 = 34$ (fin de la Tâche X)

III.6.6.2. Date au plus tard

Les dates au plus tard (DPT) : est une notion utilisée dans la gestion de projet pour déterminer la dernière date possible à laquelle une activité doit être terminée sans retarder le projet dans son ensemble. C'est la date limite avant laquelle une activité doit être terminée pour éviter tout impact négatif sur le calendrier global du Projet (Kerzner, Project Management : A systems Approach to Planning, Scheduling, and Controlling, 2017).

Les dates au plus tard signifie la date début au plus tard et la date de fin au plus tard « Pour une étape donnée, cette information détermine à quelle date maximum, depuis le début du projet, doit être atteinte, au plus tard, l'étape considérée, afin que le délai de l'ensemble du projet ne soit pas modifié. Pour ce faire, on se base sur l'estimation de la durée des tâches. On part de l'étape de fin, pour laquelle la date au plus tard est initialisée à la même valeur que la date au plus tôt détermine précédemment, et on parcourt le réseau en suivant réagencement inverse de tâche.

- $DAP I = DAT II - \text{durée I} = 2 - 0 = 2$
- $DAP II = DAT III - \text{durée II} = 5 - 3 = 2$
- $DAP III = DAT IV - \text{durée III} = 10 - 5 = 5$
- $DAP IV = DAT V - \text{durée IV} = 16 - 6 = 10$
- $DAP V = DAT IV - \text{durée IV} = 20 - 4 = 16$

- DAP VI = DAT V – durée V = 23 – 3 = 20
- DAP VII = DAT VI – durée VI = 26 – 3 = 23
- DAP VIII = DAT VII + durée VII = 32 – 6 = 26
- DAP IX = DAT VIII – durée VIII = 33 – 1 = 32
- DAP X = DAT IX – durée IX = 36 – 3 = 33

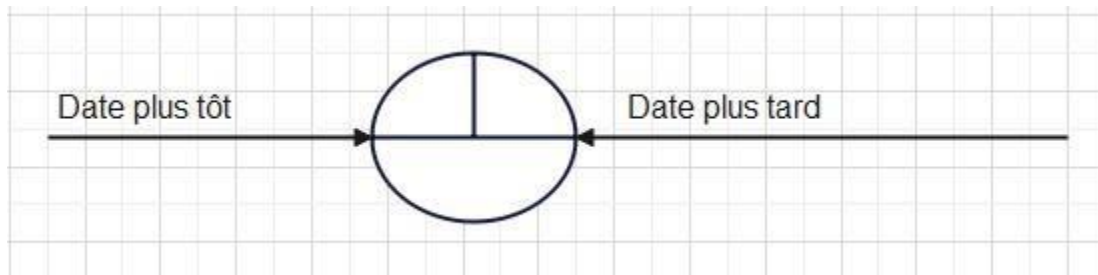


Figure 7 date plus tôt et date plus tard

III.6.6.2. Calcul des marges

On appelle « marge » d'une tâche le retard qu'il est possible de tolérer dans la réalisation de celle-ci, sans que la durée optimale prévue du projet global en soit affectée. Il s'agit donc de la possibilité qu'a une tâche d'être retardée sans pour autant impacter sur le chronogramme du projet. Deux sortes de marges sont à distinguer ici : la marge libre (ML) et la marge totale (MT)

III.6.6.2.1. La marge libre (ML)

La marge libre d'une tâche indique le retard que l'on peut admettre dans la réalisation de cette tâche sans modifier les dates au plus tôt des tâches suivantes et sans allonger la durée optimale du projet. Cette marge se calcule par la formule

$$ML = DAP - DAT$$

Pour notre projet, voici les marges libres de différentes tâches :

$$ML(I) = 2 - 0 = 2$$

$$ML(II) = 3 - 1 = 1$$

$$ML(III) = 5 - 5 = 0$$

$$ML(IV) = 10 - 10 = 0$$

$$ML(V) = 16 - 16 = 0$$

$$ML(VI) = 20 - 20 = 0$$

$$ML(VII) = 23 - 23 = 0$$

$$ML(VIII) = 26 - 26 = 0$$

$$ML(\text{IX}) = 32 - 32 = 0$$

$$ML(\text{X}) = 33 - 33 = 0$$

III.6.6.2. La marge totale

Le marge totale d'une tâche indique le retard maximal que l'on peut admettre dans la réalisation de cette tâche sans allonger la durée optimale du projet. Ainsi, pour notre projet, Bref : La marge totale est égale à la date au plus tard moins la date au plus tôt. Les marges totales de différentes tâches se présentent comme suit :

$$MT(\text{I}) = 2 + 2 = 4$$

$$MT(\text{II}) = 1 + 3 = 4$$

$$MT(\text{III}) = 0 + 5 = 5$$

$$MT(\text{IV}) = 0 + 6 = 6$$

$$MT(\text{V}) = 0 + 4 = 4$$

$$MT(\text{VI}) = 0 + 3 = 3$$

$$MT(\text{VII}) = 0 + 3 = 3$$

$$MT(\text{VIII}) = 0 + 6 = 6$$

$$MT(\text{IX}) = 0 + 1 = 1$$

$$MT(\text{X}) = 0 + 3 = 3$$

III.6.7. Détermination du chemin critique

On appelle chemin critique du réseau PERT, la succession des tâches pour lesquelles aucun retard n'est possible sans remettre en cause la durée optimale du projet. Il s'agit donc d'un chemin qui reprend les tâches pour lesquelles la date au plus tôt est égale à la date au plus tard.

C'est le chemin le plus long du projet

Ainsi, le chemin critique est trouvé en calculant la marge libre et la marge totale de chaque tâche. De ce fait, le chemin critique est le chemin du graphe passant par les tâches dont les marges libres et les marges totales sont nulles.

Dans le cadre de ce travail, les tâches du chemin critique sont : I, II, III, IV, V, VI, VII, VIII, IX et X tel qu'illustré sur la figure ci-dessous :

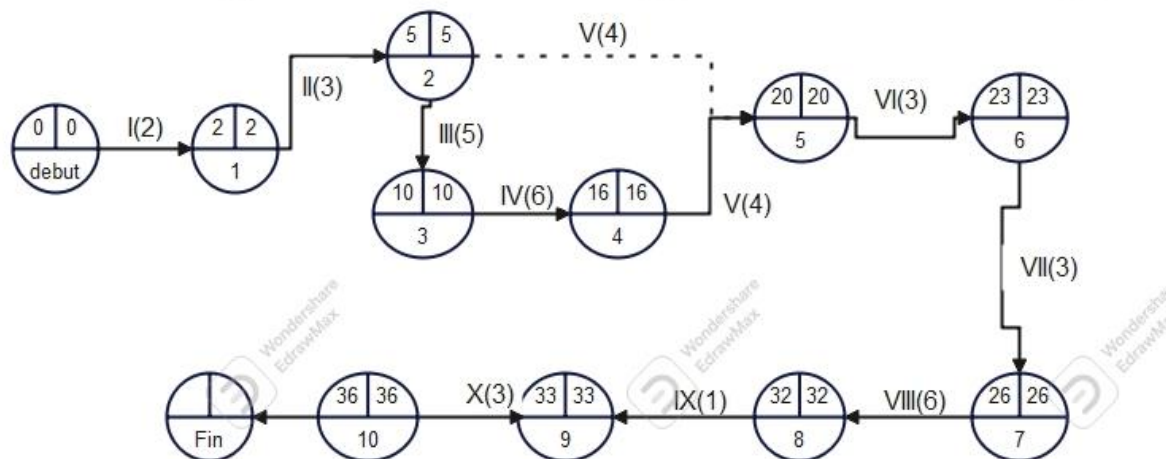


Figure 8 Chemin critique

III.6.8. Diagramme de gant

Le diagramme de Gant est un outil de gestion de projet qui permet de représenter graphiquement les différentes tâches d'un projet, ainsi que leur chronologie. Il est composé d'un axe horizontal qui représente la durée totale du projet, divisée en tranches égales ou inégales correspondant aux différentes tâches. Chaque tâche est représentée par une barre horizontale dont la longueur indique sa durée prévue. Les tâches peuvent être liées entre elles par des dépendances, ce qui permet de visualiser les relations et les contraintes dans la planification du projet.

Couramment utilisé en gestion de projet, est l'un des outils les plus efficaces pour représenter visuellement l'état d'avancement des différentes activités (tâches) qui constituent un projet. La colonne de gauche du diagramme énumère toutes les tâches à effectuer, tandis que la ligne d'en-tête représente les unités de temps les plus adaptées au projet (jours, semaines, mois etc.). Chaque tâche est matérialisée par une barre horizontale, dont la position et la longueur représentent la date de début, la durée et la date de fin. Ce diagramme permet donc de visualiser d'un seul coup d'œil :

- Les différentes tâches à envisager
- La date de début et la date de fin de chaque tâche
- La durée escomptée de chaque tâche, le chevauchement éventuel des tâches, et la durée de ce chevauchement

- La date de début et la date de fin du projet dans son ensemble, le diagramme de Gantt répertorie toutes les tâches à accomplir pour mener le projet et indique la date à laquelle ces tâches doivent être effectuées (le planning).

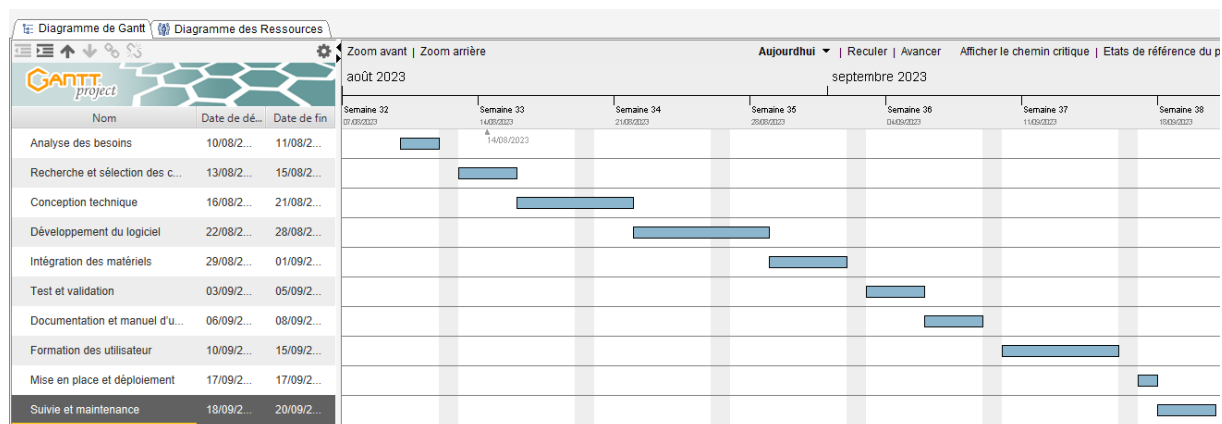


Figure 9 Diagramme de Gantt

III.6.9. CALENDRIER DU PROJET

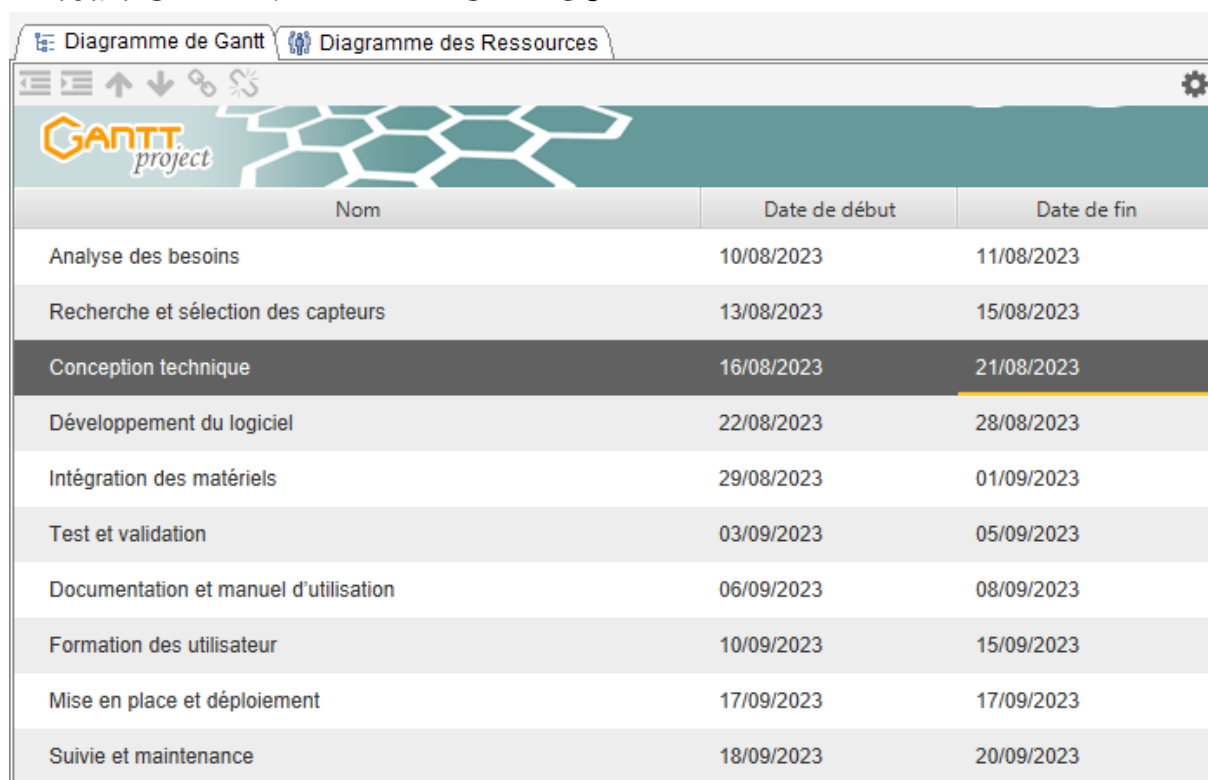


Figure 10 Calendrier du Project

III.6.10. Diagramme d'activité

Le diagramme d'activité est l'un des diagrammes dynamiques proposés par UML. Il représente les flots de données et de contrôle entre les actions. Il est majoritairement utilisé pour l'expression de la logique de contrôle et d'entrées/sorties.

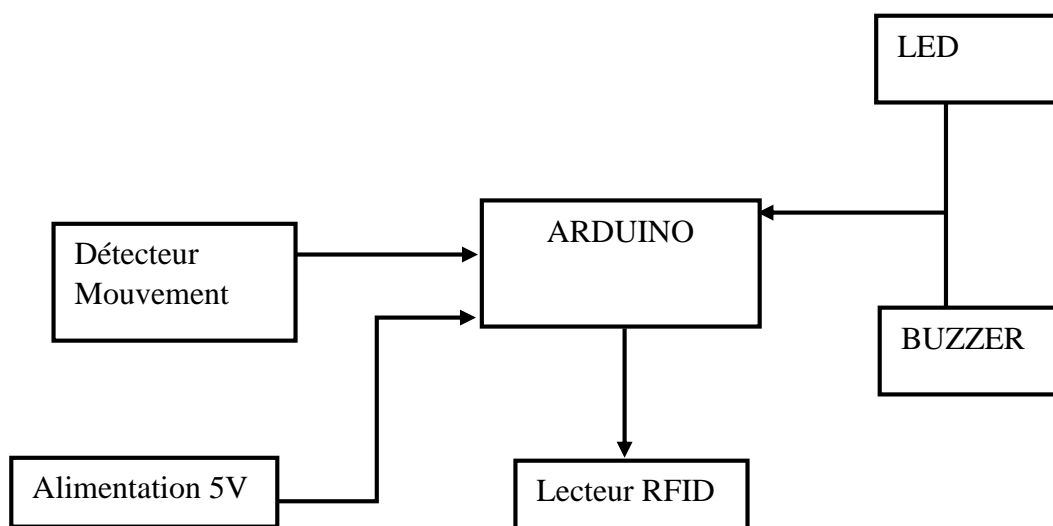
Les éléments de base du diagramme d'activité sont les suivants :

- **Des actions** : l'action est l'unité fondamentale de spécification comportementale en UML. Elle représente un traitement ou une transformation. **Des flots de contrôle entre actions.**

- **Des décisions (aussi appelées branchements conditionnels)** : Une décision est un nœud de contrôle structuré représentant un choix dynamique entre plusieurs conditions qui doivent être mutuellement exclusives.

- **Un début** et une ou plusieurs fins possibles.

1. Présentation de diagramme d'activités



III.6.10. Diagramme de cas d'utilisation

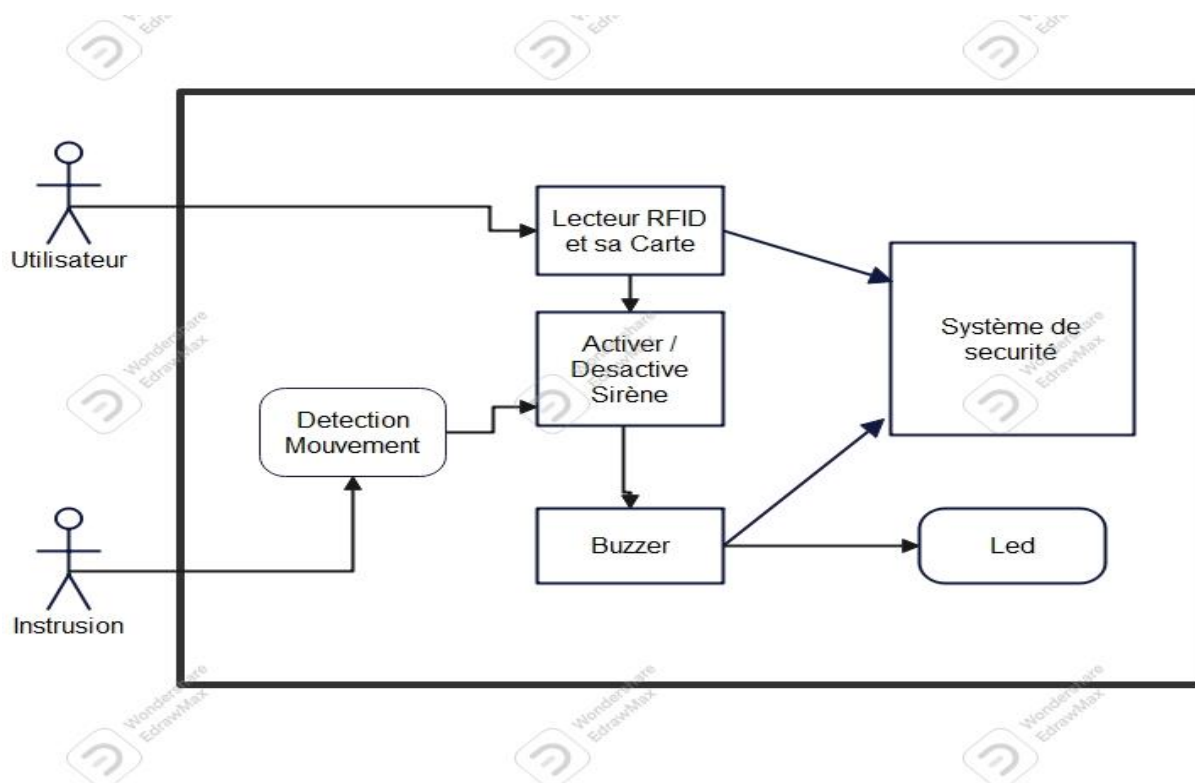
Un diagramme de cas d'utilisation est un outil de modélisation utilisé en génie logiciel pour représenter les fonctionnalités ou les interactions entre un système et ses acteurs. Il décrit les actions que le système peut effectuer et les utilisateurs qui interagissent avec le système.

Les fonctionnalités principales du diagramme de cas d'utilisation sont les suivantes :

1. **Identification des acteurs** : Le diagramme de cas d'utilisation permet d'identifier les différents acteurs qui interagissent avec le système. Les acteurs peuvent être des utilisateurs, des systèmes externes ou d'autres entités qui jouent un rôle dans l'utilisation du système.
2. **Description des acteurs** : Les cas d'utilisation représentent les différentes fonctionnalités ou actions que le système peut effectuer. Chaque cas d'utilisation décrit une séquence d'actions qui sont effectuées par le système et/ou par les acteurs.

3. **Relation entre les acteurs et les cas d'utilisation** : Le diagramme de cas d'utilisation montre les relations entre les acteurs et les cas d'utilisation. Un acteur peut être associé à plusieurs cas d'utilisation, et un cas d'utilisation peut impliquer plusieurs acteurs.
4. **Hierarchie des cas d'utilisation** : Le diagramme de cas d'utilisation peut également montrer la hiérarchie des cas d'utilisation. Par exemple, un cas d'utilisation peut être subdivisé en sous-cas d'utilisation pour détailler davantage les fonctionnalités.
5. **Inclusion et extension des cas d'utilisation** : Le diagramme de cas d'utilisation peut indiquer les relations d'inclusion et d'extension entre les cas d'utilisation. L'inclusion permet d'inclure un cas d'utilisation dans un autre cas d'utilisation. L'extension permet d'étendre ou de modifier le comportement d'un cas d'utilisation existant.
6. **Scénarios alternatifs** : Le diagramme de cas d'utilisation peut inclure les scénarios alternatifs ou des exceptions qui se produisent lorsque certaines conditions ne sont pas remplies ou lorsque des erreurs se produisent.
7. **Attributs du cas d'utilisation** : Les cas d'utilisation peuvent également inclure des attributs pour capturer des informations supplémentaires telles que des préconditions, des post conditions, les exigences spécifiques etc.

En fin, un diagramme de cas d'utilisation aide à visualiser les fonctionnalités d'un système et les interactions entre les acteurs et le système. Il fournit une vue globale des actions que le système peut effectuer et comment ces actions sont liées aux acteurs impliqués (Roques, UML 2 Par la pratique, 2009).



CHAP. PRÉSENTATION DES RÉSULTATS

IV.1 Environnement Matériel et Étude de Logiciels de programmation

IV.1.1 Environnement Matériel

Pendant l'exécution de notre projet, nous avons employé le matériel suivant :

Appareil	Unité	Caractéristiques
Ordinateur Portable HP DESKTOPRDEF7IO ISHIMWEJEAN-PIERRE	Processeur	Intel(R) Core(TM) i5-2520M CPU @ 2.50GHz 2.50 GHz
	RAM	4,00 Go
	Disque dur	500Go SSD
	Ecran	1920 x1080
	Systeme d'exploitation	Édition Windows 10 Professionnel Version 22H2 Installé le 23/06/2023 ID de périphérique : 322E6F90-18E2-4509-9900-D4B0AD87050C ID de produit :00331-10000-00001-AA228 Type du système Système d'exploitation 64 bits, processeur x64 Stylet et fonction tactile La fonctionnalité d'entrée tactile ou avec un stylet n'est pas disponible sur cet écran Build du système d'exploitation 19045.3208

IV.1.2 Étude de Logiciels de programmation

IV.1.2.1. Schéma d'interconnexion entre les composants

La carte Arduino effectue des lectures à travers les ports numériques, ensuite détecte l'angle du capteur et donne le signal au buzzer avec le Led.

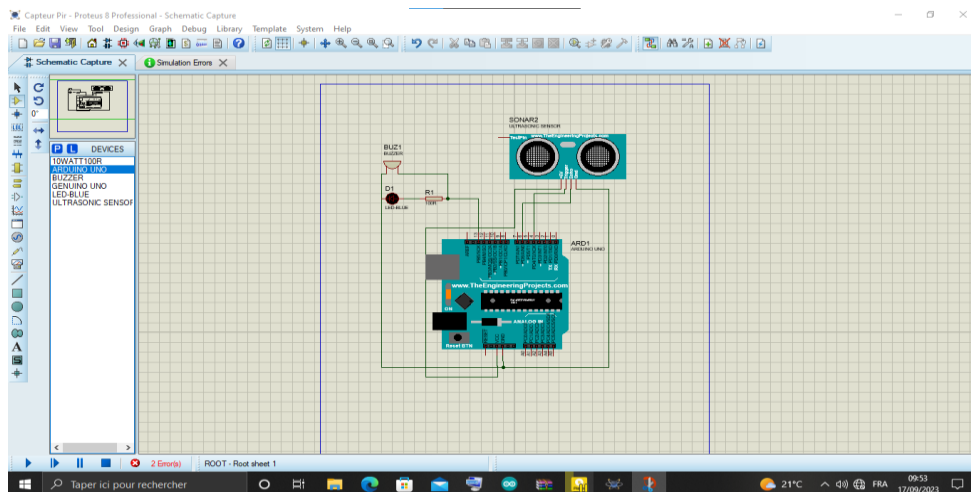


Figure 11 Schéma complet d'interconnexion entre les composants du projet.

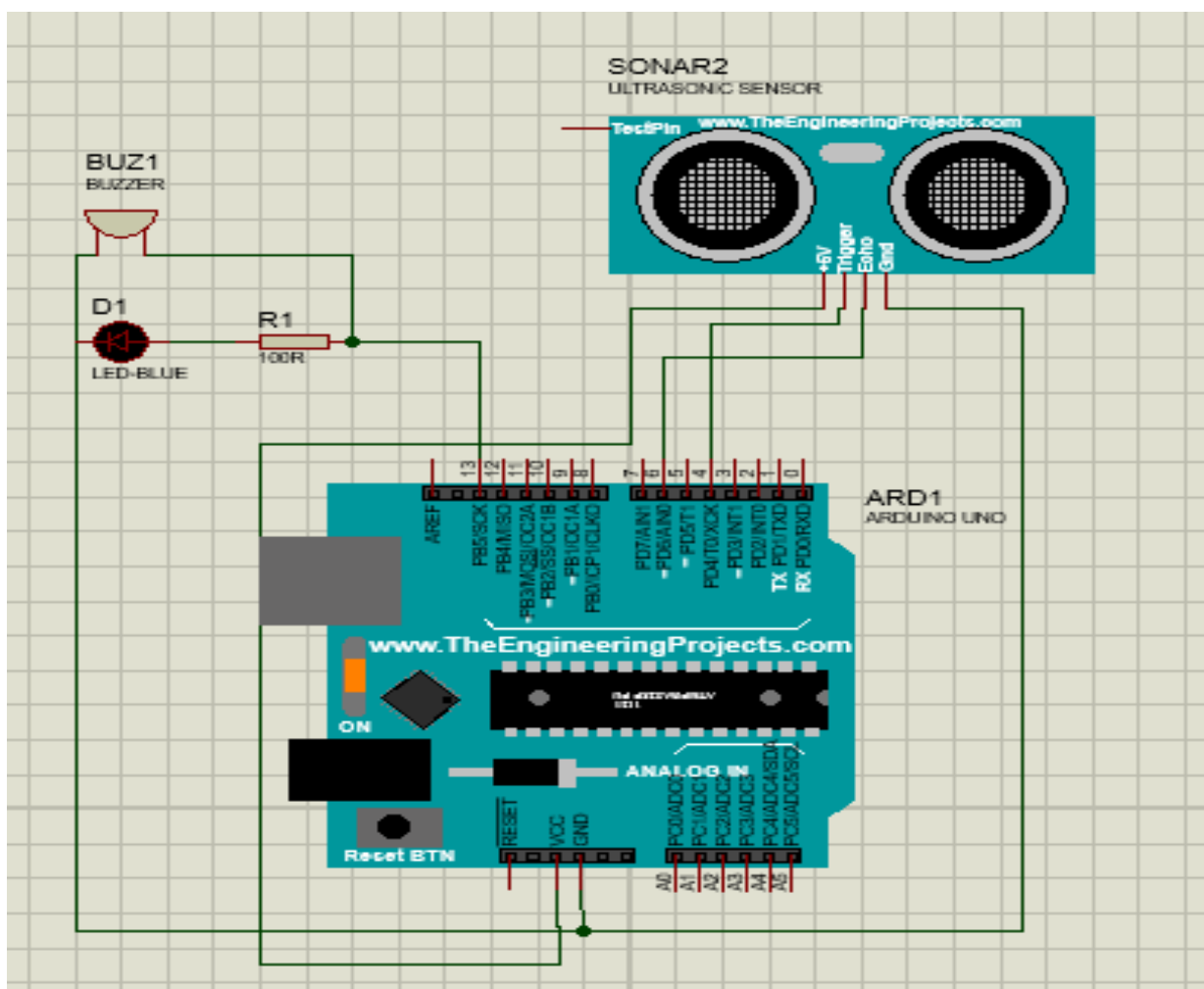


Figure 12 Schéma d'interconnexion entre les composants du projet.

Architecture du système : cette figure montre comment sont l'interconnection des objet du système

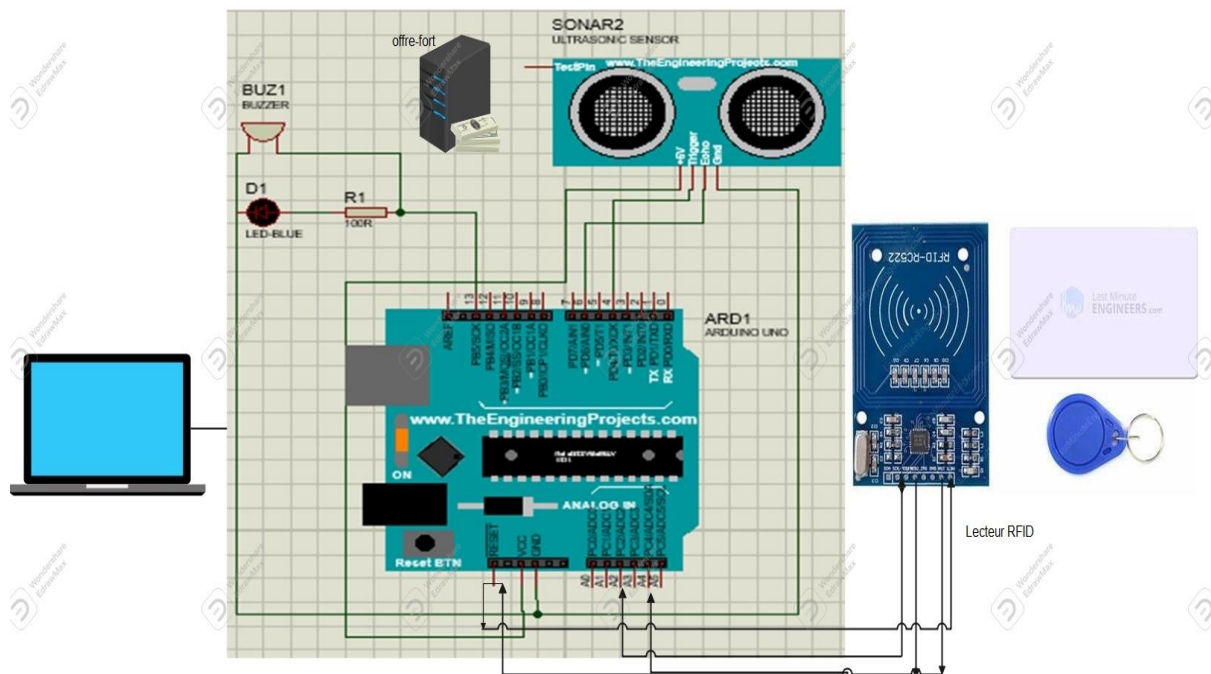


Figure 13 Architecture du système

IV.1.2.1 Interface de programmation Arduino

Notre travail vise à comprendre les différents mécanismes et techniques utilisés pour détecter les mouvements indésirables dans un environnement sécurisé. Il englobe des concepts tels que l'utilisation de capteurs pour détecter les changements de position, donc analyser tous les mouvements et la prise de décision pour déclencher une alerte. Maintenant en présentant les captures du logiciel utilisé il serait possible de montrer comment cette théorie est mise en pratique, en mettant en évidence les fonctionnalités spécifiques du logiciel qui facilitent la détection des mouvements suspects.

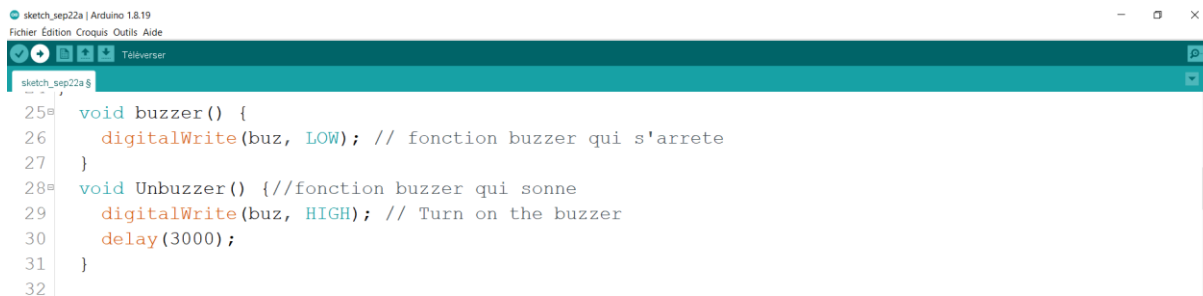
```

sketch_sep22a | Arduino 1.8.19
Fichier Edition Croquis Outils Aide

sketch_sep22a.g
1 //partie pour inclure les bibliotheque et declare les variables
2 #include <MFRC522.h>
3 #define SS_PIN 10
4 #define RST_PIN 9
5
6 MFRC522 mfc522(SS_PIN, RST_PIN); // Create MFRC522 object
7
8 int buz = 5; // Pin for the buzzer
9 int led1 = 4; // Pin for the green LED
10 int led2 = 3; // Pin for the red LED
11 #define TRIG_PIN 7
12 #define ECHO_PIN 8

```

Figure 14 déclaration des bibliothèques et déclaration des variables

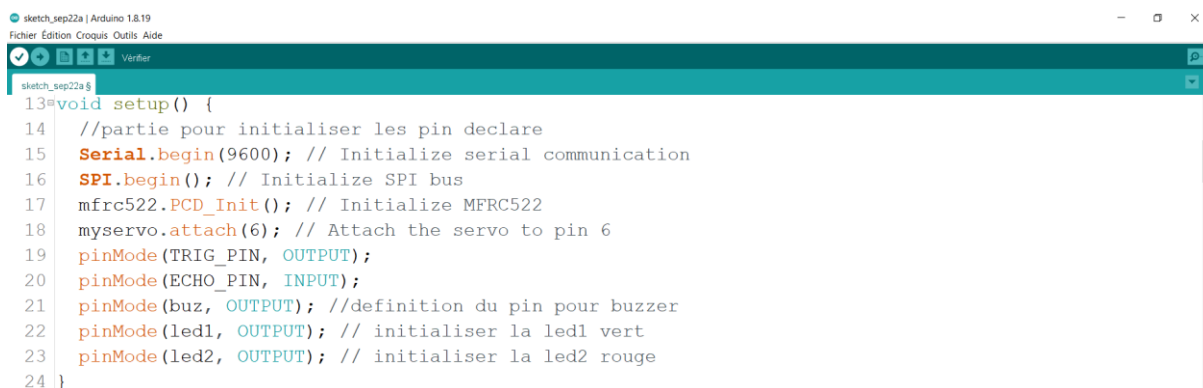


```

sketch_sep22a | Arduino 1.8.19
Fichier Edition Croquis Outils Aide
sketch_sep22a.g
25 void buzzer() {
26   digitalWrite(buz, LOW); // fonction buzzer qui s'arrete
27 }
28 void Unbuzzer() { //fonction buzzer qui sonne
29   digitalWrite(buz, HIGH); // Turn on the buzzer
30   delay(3000);
31 }
32

```

Figure 15 Déclaration des fonctions du buzzer



```

sketch_sep22a | Arduino 1.8.19
Fichier Edition Croquis Outils Aide
sketch_sep22a.g
13 void setup() {
14   //partie pour initialiser les pin declare
15   Serial.begin(9600); // Initialize serial communication
16   SPI.begin(); // Initialize SPI bus
17   mfr522.PCD_Init(); // Initialize MFRC522
18   myservo.attach(6); // Attach the servo to pin 6
19   pinMode(TRIG_PIN, OUTPUT);
20   pinMode(ECHO_PIN, INPUT);
21   pinMode(buz, OUTPUT); //definition du pin pour buzzer
22   pinMode(led1, OUTPUT); // initialiser la led1 vert
23   pinMode(led2, OUTPUT); // initialiser la led2 rouge
24 }

```

Figure 16 Initialisations des variables.

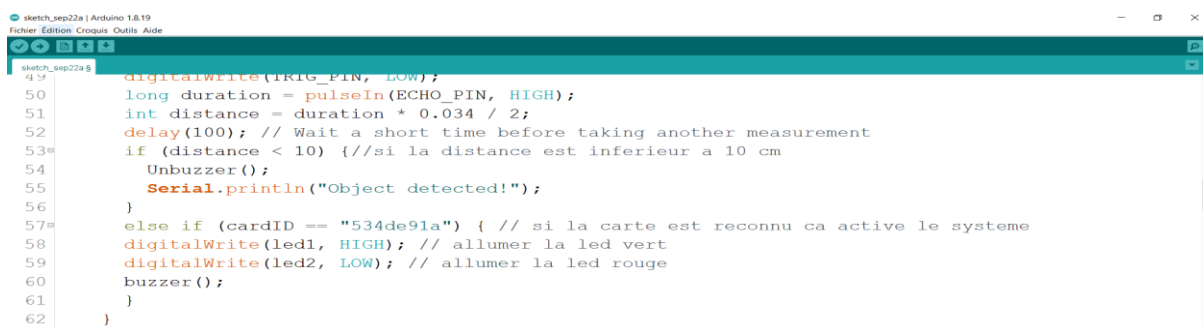


```

sketch_sep22a | Arduino 1.8.19
Fichier Edition Croquis Outils Aide
sketch_sep22a.g
32
33 void loop() {
34
35   if (mfr522.PICC_IsNewCardPresent() && mfr522.PICC_ReadCardSerial()) { // Check for RFID card
36     String cardID = "";
37     for (byte i = 0; i < mfr522.uid.size; i++) { // Read the RFID card ID
38       cardID.concat(String(mfr522.uid.uidByte[i] < 0x10 ? "0" : ""));
39       cardID.concat(String(mfr522.uid.uidByte[i], HEX));
40     }
41     while(cardID == "554ad83f") { // si la carte est reconnu
42       digitalWrite(led2, HIGH); // la led est allume
43       digitalWrite(led1, LOW); //la led est etteinte
44       buzzer();
45       digitalWrite(TRIG_PIN, LOW);
46       delayMicroseconds(2);
47       digitalWrite(TRIG_PIN, HIGH);
48       delayMicroseconds(10);

```

Figure 17 Exécution du code (si une carte est connu le système est désactivée)



```

sketch_sep22a | Arduino 1.8.19
Fichier Edition Croquis Outils Aide
sketch_sep22a.g
49       digitalWrite(TRIG_PIN, LOW);
50       long duration = pulseIn(ECHO_PIN, HIGH);
51       int distance = duration * 0.034 / 2;
52       delay(100); // Wait a short time before taking another measurement
53       if (distance < 10) { //si la distance est inferieur a 10 cm
54         Unbuzzer();
55         Serial.println("Object detected!");
56       }
57       else if (cardID == "534de91a") { // si la carte est reconnu ca active le systeme
58         digitalWrite(led1, HIGH); // allumer la led vert
59         digitalWrite(led2, LOW); // allumer la led rouge
60         buzzer();
61       }
62     }

```

Figure 18 Exaction du système (si une autre carte est reconnu le système est réactiver avec le buzzer).



Figure 19 l'affichage de la partie pour le coffre-fort

Cette figure montre comment est le projet en général mais l'espace le plus visible c'est le place pour le coffre-fort.

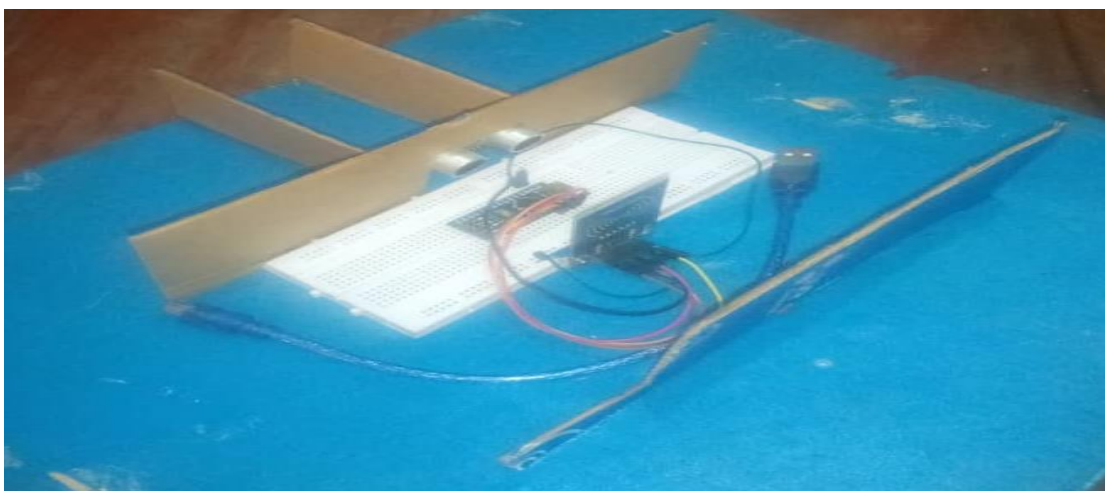


Figure 20 l'image de démonstration pour le lecteur RFID et Le capteur

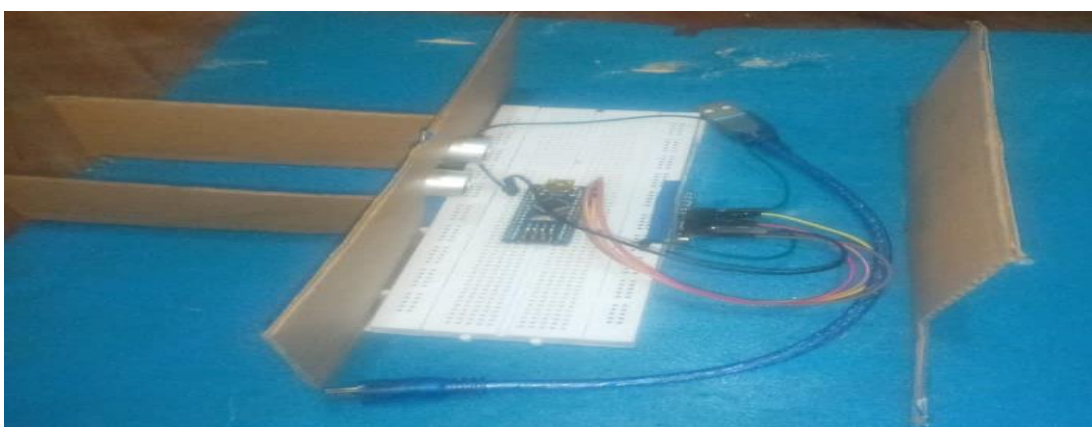


Figure 21 démonstration des branchement des câbles du système et la câble d'alimentation

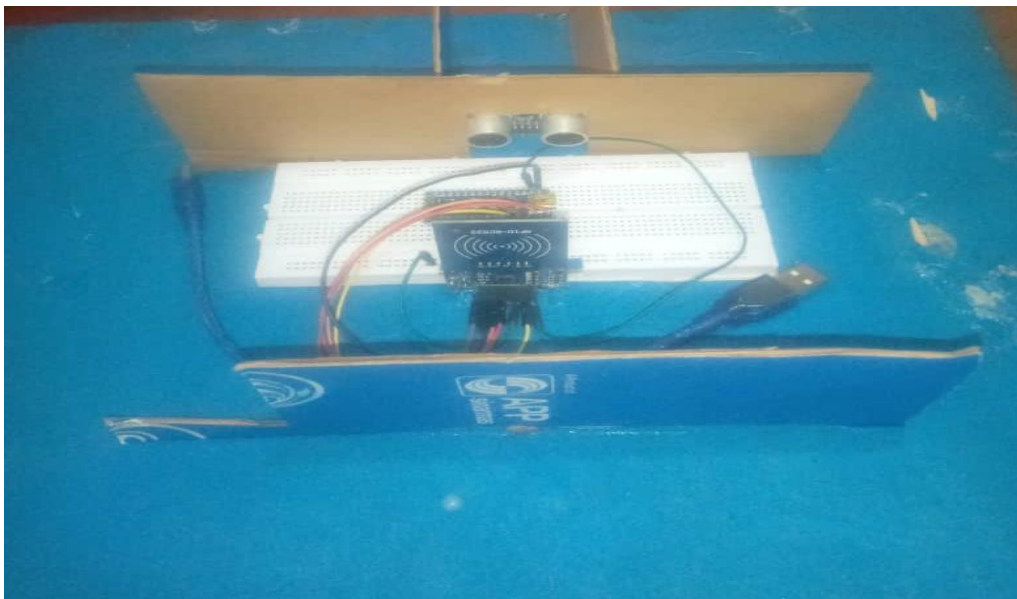


Figure 22 l'image complet du système de sécurité

IV.2 Présentation des codes

```
//partie pour inclure les bibliotheque et declare les variables
#include <MFRC522.h>
#define SS_PIN 10
#define RST_PIN 9

MFRC522 mfrc522(SS_PIN, RST_PIN); // Create MFRC522 object

int buz = 5; // Pin for the buzzer
int led1 = 4; // Pin for the green LED
int led2 = 3; // Pin for the red LED
#define TRIG_PIN 7
#define ECHO_PIN 8
void setup() {
  //partie pour initialiser les pin declare
  Serial.begin(9600); // Initialize serial communication
  SPI.begin(); // Initialize SPI bus
  mfrc522.PCD_Init(); // Initialize MFRC522
```

```

myservo.attach(6); // Attach the servo to pin 6
pinMode(TRIG_PIN, OUTPUT);
pinMode(ECHO_PIN, INPUT);
pinMode(buz, OUTPUT); //definition du pin pour buzzer
pinMode(led1, OUTPUT); // initialiser la led1 vert
pinMode(led2, OUTPUT); // initialiser la led2 rouge
}
void buzzer() {
    digitalWrite(buz, LOW); // fonction buzzer qui s'arrete
}
void Unbuzzer() { //fonction buzzer qui sonne
    digitalWrite(buz, HIGH); // Turn on the buzzer
    delay(3000);
}

void loop() {

    if (mfr522.PICC_IsNewCardPresent() && mfr522.PICC_ReadCardSerial()) { // Check for
RFID card

        String cardID = "";
        for (byte i = 0; i < mfr522.uid.size; i++) { // Read the RFID card ID
            cardID.concat(String(mfr522.uid.uidByte[i] < 0x10 ? "0" : ""));
            cardID.concat(String(mfr522.uid.uidByte[i], HEX));
        }
        while(cardID == "554ad83f") { // si la carte est reconnu
            digitalWrite(led2, HIGH); // la led est allume
            digitalWrite(led1, LOW); //la led est etteinte
            buzzer();
            digitalWrite(TRIG_PIN, LOW);
            delayMicroseconds(2);
            digitalWrite(TRIG_PIN, HIGH);

```



```
delayMicroseconds(10);
digitalWrite(TRIG_PIN, LOW);
long duration = pulseIn(ECHO_PIN, HIGH);
int distance = duration * 0.034 / 2;
delay(100); // Wait a short time before taking another measurement
if (distance < 10) { //si la distance est inferieur a 10 cm
    Unbuzzer();
    Serial.println("Object detected!");
}
else if (cardID == "534de91a") { // si la carte est reconnu ca active le systeme
digitalWrite(led1, HIGH); // allumer la led vert
digitalWrite(led2, LOW); // allumer la led rouge
buzzer();
}
}
// Unknown RFID card and no object detected
buzzer(); // Activate the buzzer
digitalWrite(led1, HIGH); // allumer la led vert
digitalWrite(led2, HIGH); // allumer la led rouge

mfrc522.PICC_HaltA(); // Stop communication with the RFID card
mfrc522.PCD_StopCrypto1();
Serial.println("Waiting for RFID card...");
}
}
```

CINQUIÈME CHAPITRE. RECOMMANDATION

La sécurité physique est d'une importance cruciale lorsqu'il s'agit de protéger les biens de valeur tels que le coffre-forts de la Banque. Dans cette esprit, cette recommandation vise à mettre en place un système de détection des mouvements physiques complet et fiable pour garantir une protection maximale contre les intrusions et les tentatives de vol.

Voici quelques recommandations pour la mise en place du système :

1. Étude préliminaire approfondie : Avant d'installer un système de surveillance, réalisez une étude préliminaire complète pour évaluer les caractéristiques spécifiques de la zone réservée au Coffre-fort. Cela comprend la collecte de données historiques sur le système de sécurité, l'analyse des risques potentiels et la cartographie précise des zones à haut risque.

2. Sélection des capteurs adaptés : Choisissez des capteurs de mouvement de haute qualité et adaptés aux conditions de la zone réservée pour garder le coffre-fort. Optez pour des capteurs à la fois sensibles et précis, capables de détecter toutes les mouvements rapidement et avec fiabilité. Les capteurs électrochimiques peuvent être envisagés en fonction des besoins spécifiques de la zone du coffre-fort.

3. Installation stratégique des capteurs : Disposez les capteurs de manière stratégique dans toute la zone du coffre-fort pour assurer une couverture maximale. Placez-les à des endroits où tous les mouvements sont susceptibles de se produire facilement, tels que les points d'entrée dans la chambre du coffre-fort. Assurez-vous également de positionner les capteurs de manière à minimiser les sources d'interférences potentielles.

4. Système de communication fiable : Mettez en place un système de communication fiable pour transmettre les signaux des capteurs à un contrôleur Arduino Uno. Cela peut impliquer l'utilisation de câbles ou de réseaux sans fil, en fonction de la configuration de la zone sécurisée. Assurez-vous que le système de communication est robuste et résistant aux interférences pour garantir une transmission de données continue.

5. Analyse en temps réel des données : Utilisez des logiciels d'analyse des données en temps réel pour traiter les informations collectées par les capteurs. Ces logiciels peuvent détecter les tous les mouvements d'intrusion et générer des alertes automatiques pour une action rapide. Les paramètres des alertes doivent être configurés en fonction des normes de sécurité et de la réglementation en vigueur.

6. Maintenance régulière du système : Planifiez des activités de maintenance régulières pour assurer le bon fonctionnement continu du système de surveillance. Cela comprend des vérifications périodiques des capteurs, des calibrations régulières et des procédures de remplacement des capteurs défectueux. Établissez également un plan de formation pour le personnel responsable de la maintenance.

7. Améliorations continues : Restez à jour avec les dernières avancées technologiques dans le domaine de la surveillance de mouvement au niveau du coffre-fort. Recherchez constamment de nouvelles méthodes et technologies pour améliorer les performances du système de surveillance et réduire les risques liés au coffre-fort.

CONCLUSION GÉNÉRALE

Nous voici au terme de ce travail de fin de cycle portant sur « Mise en place d'un système de sécurité physique pour la détection des mouvements au niveau du coffre-fort. »

Vu que le monde évolue toujours dans la technologie nous avons eu la motivation de traité sur le système de sécurité physique pour la détection des mouvements au niveau du coffre-fort de l'Equity Bank.

Les objectifs suivant ont été fixe pour arriver atteindre à la réalisation de notre projet :

L'objectif général de cette étude est de mettre en place un système de sécurité physique basé sur arduino capable de détecter les mouvements Au niveau du coffre-fort de l'Equity Bank à Goma et de déclencher la sirène en cas de présence suspecte, améliorant ainsi la sécurité globale de la banque, afin de garantir la sécurité des biens des clients de la banque et de l'institutions elle-même.

Les objectifs Spécifiques

Les objectifs spécifiques incluent :

- Analyser les besoins spécifiques au niveau de la succursale de l'Equity Bank à Goma en matière de sécurités physique pour la détection des mouvements au niveau du coffre-fort..
- Concevoir et développer un système de sécurité basé sur Arduino qui utilise des capteurs de mouvement pour détecter toute présence suspecte.
- Assurer une réactivité immédiate en cas de détection de mouvement en déclenchant directement une sirène d'alerte.
- Teste et Évaluer la précision et la fiabilité du système de détection de mouvement afin de minimiser les fausses alertes et d'assurer une détection précise des intrusions.
- Proposer des recommandations pour l'optimisation du système, par exemple en intégrant d'autres fonctionnalités de sécurités telles que la surveillance Vidéo ou en renforçant la résistance aux tentative de sabotage.
- Garantir une mise en place efficace du système de sécurité en évaluant les ressources nécessaires, en formant le personnel de la banque à son utilisation, suivi régulière et en assurant sa maintenance régulière.

Pour atteindre nos objectifs nous sommes servis des méthodes et techniques suivantes :

Pour analyser le système existant et concevoir le futur système d'information au sein de cette entreprise financière nous avons faire recours à la méthode **PERT**. Technique documentaire, Technique d'observation libre et la Technique d'interview

La concrétisation de notre étude est aboutie à Mise en place d'un système de sécurité physique pour la détection des mouvements au niveau du coffre-fort « cas de l'Equity Banque » qui a été capable de produire les résultats suivants :

- Détecter toutes les Mouvement lors de l'ouverture de la porte
- Identification de l'Utilisateur à l'aide de la carte RFID
- Déclencher une alerte d'une manière automatique lors de la détection d'intrusion qui se présente.

C'est ainsi que nous encourageons tout chercheur qui voudras nous en boiter les pas à aller plus loin que nous nous sommes arrêtes.

Bibliographies

- AFITEP. (2000). *Dictionnaire de management de proje* (éd. 4e édition). Afnor.
- Aghiles, S. J. (2018). *Etude et réalisation d'un radar détections à base de la carte Arduino*. UNIVERSITE MOULOUD MAMMARI DE TIZI-OUZOU.
- Aliaga, D. G. (2014). *Evaluation of Background Subtraction Methods on the Wallflower Dataset*. Consulté le 08 09, 2023
- Allard, P.-P. (2016). *Sécurité informatique et malwares : Analyse des menaces et mise en œuvre des contre-mesures* (éd. ENI). (P.-P. Allard, Éd.) ENI. Consulté le 08 08, 2023
- Alpaydin, E. (2010). *Introduction to Machine learning*.
- Anderson, R. J. (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems*. (éd. 2ème Edition). Chichester, Royaume-Uni : Wiley.
- B.Cottenceau. (s.d.). *Carte ARDUINO Uno Microcontrôleur ATmega328 , Microcontrôleurs E13 Option AGI* .
- Benzaoui, A. B. (2003). *Analyse vidéo par vision artificielle*. Hermès Science Publications. Consulté le 08 09, 2023
- BERNARD, A. (s.d.). *Technologie-Science.net*. Consulté le Mai 26, 2023, sur <https://www.technologie.net/glossaire-definition/Radar.html>
- BOUREGHIDA ZAKARIA, S. A. (2021).
- Bourgoin, S. (2018). *Coffres-forts : Histoire, Technique et Usage*. Consulté le 08 10, 2023
- Bouwman, T. (2014). *Background Subtraction Techniques: A Review*. Consulté le 08 09, 2023
- BRENNI, P. (s.d.). *Universalis.fr*. Consulté le Mai 26, 2023, sur <https://www.universalis.fr/encyclopedie/radar-en-bref/>
- Burnett, J. M. (2020). *Construction Project Management : A Managerial Approach* (éd. 7ème édition). (Wiley, Éd.) Hoboken, NJ: Wiley. Consulté le 09 05, 2023
- Charles, J.-P. (s.d.). *la sécurité du coffre fort*. Consulté le 09 10, 2023
- Chasseray, C. (2019). *Gestion de Projet : Fondamentaux, Méthodes et Outils*. Dunod. Consulté le 8 05, 2023
- Crabé, M. F. (2018). *Projet Management - Les Fondamentaux pages 45-46*.
- Decouverte_arduino. (s.d.). *techmania.fr*. Récupéré sur http://www.techmania.fr/arduino/Decouverte_arduino.pdf
- DELPRATO, J. (2016). *Analyse de la stabilité d'impulsion à impulsion*. -: UNIVERSITE DE LIMOGES.
- DIOT, J.-C. (2006). *Conception et réalisation d'un radar Ultra Large*. -: UNIVERSITE DE LIMOGES.
- DJAHID, L. (2017). *Emulation de Système SCADA pour le Contrôle et Distribution d'eau*. Université Badji Mokhtar Annaba.
- Djalal, D. M. (2016). *Étude et réalisation d'une Carte Arduino*. Algerie: Université A.MIRA de Bejaia.

- Djamel, B. (2023). *techniques_radars*. Consulté le 05 26, 2023, sur http://staff.univ-batna2.dz/sites/default/files/benatia_djamel/files/techniques_radars.pdf
- Dolan, P. O. (2017). *Introduction to Security*. Pearson Education. Consulté le juillet 19, 2023
- Dounya, D. N. (2017). *Étude et réalisation d'un RADAR de détection*. -: Université Aboubakr Belkaïd-Tlemcen .
- Dounya, D. N. (2017). *Étude et réalisation d'un RADAR de détection*. Tlemcen. Algérie: Université Aboubakr Belkaïd.
- Dreuillet, P. (s.d.). Défense et Sécurité L'ONERA DEVOILE RAMSES-NG. Dans *UN NOUVEAU SYSTEME DE DETECTION EMBARQUE ULTRA-PERFORMANT QUI EXPLOITE TOUT LE POTENTIEL DE LA SYNERGIE RADAR/OPTRONIQUE*. -: L'ONERA. Consulté le Avril 23, 2023, sur <http://www.onera.fr/podcasts/index.php#8>
- Dufau-Joël, J.-Y. M. (2014). *Gestion de Projet - Méthodologie et Outils pages 92-93*.
- Dulau, J. D. (2007). *Introduction aux capteurs*. Dunod.
- Eddine, A. B. (2023). *Etude et simulation d'un radar de détection*. UNIVERSITÉ BADJI MOKHTAR - ANNABA.
- Farrugia, J. P. (2013). *Traitement du signal pour la détection et la localisation d'objets* (éd. ISTE). ISTE. Consulté le 08 09, 2023
- Festor, E. D. (2018). *Sécurité des systèmes d'information*. Consulté le 08 08, 2023
- française, L. D. (1992). *Le Dictionnaire de l'Académie française* . Paris: 9ème édition.
- Frank Ervin, «. ». (2023). *Arduino-based Object Detection System*. Consulté le Avril 27, 2010
- Friesé, G. (2016). *Gestion des risques : Principes et Pratiques*. paris, France. Consulté le 08 08, 2023
- Fry, [. R. (2014). *Processing: A Programming Handbook for Visual Designers and Artists(Second Edition)* (Vol. II). The MIT Press.
- Fry, R. a. (2014). *Processing: A Programming Handbook for Visual Designers and Artists (Second Edition)*. The MIT Press.
- Gates, E. (2017). *Introduction To Electronics*. Massachusetts, Etats-Unis. Consulté le 09 08, 2023
- Grevisse, Y. R. (2019). *METHODES DE CONDUITE DES*. Institut Supérieur de Commerce. Récupéré sur <https://hal.science/cel-02004689>
- Halasan, C. M. (2013). *Statical Methods and Applications in Forestry and Environmental Sciences*. (Springer, Éd.) Consulté le 08 09, 2023
- Hanlon, B. (2006). *Banking Security in an Era of Violence*. American Bankers Association.
- Hgh-infrared. (s.d.). <https://hgh-infrared.com/fr/>. (hgh-infrared) Consulté le Juin 03, 2023, sur [https://hgh-infrared.com/Applications/Sécurité/Surveillance des frontières](https://hgh-infrared.com/Applications/Sécurité/Surveillance%20des%20fronti%C3%A8res)
- <https://content.cegos.com>. (s.d.). *La planification du projet*. Consulté le 07 14, 2023, sur <https://content.cegos.com/>: https://content.cegos.com/ecourses/mh092_b/ca/sup_files/mh092-synthesis-ca.html

- Initiation à l'électronique en partant de Zéro* (éd. Eyrolles). (2019). Eyrolles. Consulté le 08 20, 2023
- Institute, P. M. (2017). *A Guide to the Project Management Body of Knowledge (PMBOK Guide)* (éd. 6ème Edition). (P. M. Institute, Éd.) Newtown Square, PA, Etats-Unis: Project Management Institute. Consulté le 09 05, 2023
- Institute, P. M. (2017). *A Guide to the Project Management Body of Knowledge (PMBOK Guide)* (éd. 6ème édition). (P. M. Institute, Éd.) Newtown Square, PA, Etats-Unis : Project Management Institute. Consulté le 09 05, 2023
- Institute, P. M. (2017). *A Guide to the Project Management Body of Knowledge (PMBOK Guide)* (éd. 6ème Edition). (P. M. Institute, Éd.) Newtown Square. PA, Etats-Unis: Project Management Institute. Consulté le 09 06, 2023
- Johnson, D. C. (2014). Mise en place d'un système de sécurité pour la détection de mouvement au niveau du coffre d'une voiture.
- Joseph J. Moder, C. R. (2014). *Project Management with CPM, PERT and Precedence Diagramming*. Consulté le 08 14, 2023
- Jr., J. R. (2011). *Project Management : A Managerial Approach* (éd. 8ème édition). (Wiley, Éd.) Hoboken, NJ, Etats-Unis : Wiley. Consulté le 09 05, 2023
- Kadam D.B, P. Y. (2017). *Arduino Based Moving Radar System* (Vol. 3). Récupéré sur www.ijisnet.org
- KALLUM, E. (2022). *Gestion de projet informatique*. Goma: Université Adventiste de Goma.
- Kelleher, S. W. (2011). *Gestion de la production et des opérations* (éd. 11ème édition). Pearson. Consulté le 08 05, 2023
- Kerzner, H. (2017). *Project Management : A systems Approach to Planning, Scheduling, and Controlling* (éd. 12e Edition). (Wiley, Éd.) Hoboken, NJ, Etats-Unis: Wiley. Consulté le 09 06, 2023
- Kerzner, H. (2017). *Project Management : A Systems Approach to Planning, Scheduling, and Controlling* (éd. 12e édition). (Wiley, Éd.) Hoboken, Etats-Unis : Wiley. Consulté le 09 05, 2023
- Kiani, H. U. (2017). *Real-Time Background Subtraction Using CUDA*. Consulté le 08 09, 2023
- Lambert, J. (2012). *Gestion de Projet: Les meilleures méthodes*. Consulté le 08 20, 2023
- Lavandier, M. (2015). *Technologie des équipements audiovisuels* (éd. Dunod). Dunod. Consulté le 08 20, 2023
- Lebel, J.-F. (2010). *Les coffres-forts : Histoire, Techniques et Utilisations*. XYZ. Consulté le 09 07, 2023
- Lefbvre, R. L. (2021). Evaluation des performances des systèmes de sécurités pour la détection des mouvements dans les coffres forts. *Journal of Security Engineering*, 42(3), 256 - 275. Consulté le 08 07, 2023
- Li, D. B. (2017). *Banking in the Democratic Republic of Congo: Key opportunities and Challenges*. African Development Bank Group.
- Lin, T.-H. (2014). *Motion Detection Algorithms and Applications for Smart Cameras*. Springer.

- Lopez, M. G. (2019). Système de sécurité basé sur l'utilisation des capteurs des pressions pour detecter les tentatives d'ouverture du coffres forts. *La technologie de Sécurité Avancée* .
- Martin, B. (2019). *Coffres-forts et protection physique des valeurs*. Consulté le 08 10, 2023
- Martin, D. e. (2016). Système de sécurité pour la detection des mouvements dans les coffres-forts. *Le journal of Security Technology*(numéro 2), 145 - 162. Consulté le 08 07, 2023
- Meriem, M. Z. (2019/2020). *Simulation et réalisation d'un radar de détection d'objets à base d'arduino*. Algérie : Université Echahid Hamma Lakhdar El-Oued.
- Mohammad, S. A. (2018). *RFID Handbook : Applications, Technology, Security and Privacy*. Floride, Etats-Unis: Boca Raton. Consulté le 09 08, 2023
- Mondon, J. R.-Y. (2016). *Capteurs et Instrumentation*. Consulté le 08 20, 2023
- Moyo, I. (2016). *Africa's Security Challenges*. Routledge.
- Obrist, G. F. (2014). *La sécurité privée en France*. (Larcier, Éd.) paris, France. Consulté le 08 08, 2023
- P.Rojansky, M. (2016). *The New Russian Foreign Policy*. Brookings Institution Press.
- Panwar, P. (2013). *Object Tracking: A Survey*. Consulté le 08 09, 2023
- Perrot, O. (2016). *conception de la sécurité*. Consulté le 08 10, 2023
- Plamen Angelov, C. G. (2011). *Motion Sensors: Theory, Design and Applications*. (éd. John Wiley et Sons). Chichester, Royaume-Uni: John Wiley et Sons. Consulté le 09 12, 2023
- Portny, S. (2016). *Gestion de Projet pour les Nuls pages 78-79*. .
- Prince, S. J. (2012). *Computer Vision: Models, Learning, and Inference*. (C. U. Press, Éd.) Consulté le 08 09, 2023
- processing.pdf, C. (2017, 11 29). www.flossmanualsfr.net. Consulté le Août 23, 2023, sur <https://www.flossmanualsfr.net/media/files/processing/processing.web.pdf>
- Ray, I. (2019). *Banking and Financial Institutions* . 425 - 440: Oxford University Press.
- Rima, A. W. (2019/2020). *Conception d'un radar de contrôle de la circulation routières pour la détection des véhicules en excès de vitesse*. REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE: Université Mohamed Larbi Ben M'hidi - Oum El bouaghi.
- Rochet, J.-L. (2019). *Management et Contrôle de la Sécurité des Systèmes d'Information*. (Lavoisier, Éd.) Consulté le 08 08, 2023
- RoJansky, M. P. (2016). *The New Russian Foreign Policy*. Brookings Institution Press.
- Roques, P. (2009). *UML 2 Par la pratique*. Paris, France: Eyrolles. Consulté le 09 10, 2023
- Roques, P. (2019). *UML par la pratique: Etudes de cas et exercices corrigés*. Consulté le 08 29, 2023
- SALEME, J. (2022). *mise en place dun systeme de detection et prevention dinstruction dans un reseau informatique* . GOMA.
- Sangaré, A. (2019). *The Impact of Information and Communication Technologies in the Third World Countries*:. Springer.

- Sarkar, R. R. (2013). *Motion Detection Techniques for Video Surveillance*. Consulté le 08 09, 2023
- Schmidt, M. (2015). *Arduino : A Quick-Start Guide*. Raleigh, Caroline du Nord, Etats-Unis : Prmatic Bookshelf. Consulté le 09 08, 2023
- Shakir, M. M. (2016). *A Short Range Radar System*. Turkey: University of Turkish Aeronautical Association Ankara.
- Shilon, M. B. (2014). *Getting Started with Arduino*. (M. Banzi, Trad.) Californie, Etats-Unis: Sebastopol. Consulté le 09 08, 2023
- Smith, M. (2019). *Arduino Uno: A Beginner's Guide* (éd. 2nd Edition). (I. Plateform, Éd.) New-York, Etats-Unis: CreateSpace Independent Publishing Plateform. Consulté le 09 12, 2023
- Snow, R. L. (2012). *Handbouk of Accssible Archievement Test for All Students*. Routledge.
- Sravani Bhattacharjee, P. (2019). *Pratical Indistrial lot Security: A practitionner's guide to securing connected industries* (éd. Apress). New-Yprk, S, Etats-Unis: Apress.
- System, C. (2023). *La sécurité de TI*. Consulté le 08 09, 2023, sur <https://www.cisco.com/c/fr/products/security/what-is-it-security.html>
- System, M. D. (2017). *Huiying Liu, Junwei Cao, Jiansheng Chen* (éd. 1ère Edition). Hershey: 1ère Edition.
- Szeliski, R. (2014). *Vision par Ordinateur : Algorithmes et Applications*. (Dunod, Éd.) Consulté le 08 09, 2023
- Sziliski, R. (2010). *Computer Vision : Algorithms and Applications*. (Springer, Éd.) Consulté le 08 09, 2023
- THALESGROUP. (s.d.). *THALES Contrusion ensemble un avenir meilleur*. Consulté le mai 25, 2023, sur <https://www.thalesgroup.com/fr/surveillance-des-frontieres-action>
- Tran-Thanh, K. (2017). *Understading Led Illumination*. Rijeka, Croatie. Consulté le 09 08, 2023
- V.K, V. (2003). *Guide du référentiel des connaissances en gestion de projet*. PMI.
- Vigneron, B. F. (2007). *Maîtriser les coûts et les performances cachees p 78-105*. Dunod.
- Vinel, A. (2015). *Motion Detection and Sensor Techniques and Applications* (éd. CRC Press). Boca Raton, Etats-Unis: CRC Press. Consulté le 09 12, 2023
- Wernerfelt, B. (1984). Based View of the firm. *Strategic Management Journal*, 5, 171-180.
- Widmer, P. (2014). *La Sécurité des biens dans les coffres-forts*. Consulté le 08 10, 2023
- Wolff, C. (s.d.). *radartutorial.eu*. Consulté le Mai 26, 2023, sur <https://www.radartutorial.eu/01.basics/Principe%20du%20Radar.fr.html>
- Wysocki, R. K. (2013). *Effective Project Management : Traditional, Agile, Extreme* (éd. 6ème edition). (Wiley, Éd.) Indianapolis, IN, Etats-Unis: Wiley. Consulté le 09 05, 2023
- Yacine, B. Y. (2016/2017). *Étude et réalisation d'un Radar électronique « Radar à ultrason»*. Université Djilali Bounaama Khemis Miliana.