**Proposition de projet technique**

Verbatim et liste matériels

**Classe de Première**

Parcours « Défense dans l’environnement électromagnétique et le Cyber (D2EC) »

Introduction

Dans le cadre du partenariat avec votre lycée, le 54e régiment de transmissions s’est vu attribué un élément du projet : la conception d’une télécommande sans fil.

Cette tâche implique la création d’un dispositif qui permettra aux utilisateurs l’envoi de commande simple, offrant la possibilité d’intégrer cette option dans d’autre élément. A travers ce mini-projet, les objectifs seront de comprendre le fonctionnement d’une transmission sans-fil, de concevoir une télécommande simplifiée, enfin d’être sensibiliser aux risques du « sans-fil ».

Suite au cadencement réalisé en fin 2023, il a été planifié que les cours seront répartis en trois blocs de quatre heures chacun, totalisant ainsi douze heures de cours au total.

La première participation de 4h00 a été définie à la date du 08 avril 2024. Suivra une intervention le 6 mai ainsi que le 3 juin.

A l’étape initiale, il me paraît probable que les élèves n’aient pas encore acquis les fondements requis pour appréhender de manière approfondie le concept de transmission sans-fil. Par conséquent, l’approche se fera initialement par des notions plus élémentaires. Des bases seront vues en s’appuyant sur des émissions radio publiques telles que les stations radio.

Le projet comporte plusieurs modules étalés sur un période de 3 mois. Dans ce cadre, l’intervention se déroulera en trois phrases :

* 4h : Vulgarisation de la chaîne de transmission
* 4h : Conception d’une télécommande et analyse de la chaine de transmission
* 4h : Sensibilisation aux risques du « sans-fil »

Les modules sont articulés comme suit :

08 avril 2024

* Présentation du projet global
* Initiation au domaine radio
* Présentation des différents modules de réceptions UHF
* Introduction aux outils Radioamateur
* Introduction à la notion de modulation/démodulation.
* Conception d’un module de réception pour la radio

06 mai 2024

* Prise en main de l’arduino et ses modules
* Conception d’un module d’émission/réception pour la radio
* Analyse de la phase d’émission

3 juin 2024

* Introduction au concept d’interception
* Audit de sécurité du système de transmission
* Démonstration d’exploitation des vulnérabilités

# 1er demi-journée – participation 54e RT

## Présentation du projet global

Le projet consistera à concevoir et programmer une télécommande sans fi fonctionnelle. A travers différentes observation, les élèves observeront les différentes phases nécessaires afin de transmettre une information. L’objectif final sera de réaliser une télécommande simplifiée à partir de module 433Mhz. Par la suite, ils observeront à l’aide d’outils SDR la communication de leurs modules respectifs.

## Initiation au domaine radio

La transmission radio est une technologie essentielle qui nous permet de communiquer sans fil sur de, plus ou moins, longue distance. Pour prendre en exemple le téléphone portable, la station radio de la voiture ou encore les balles de football connecté, la transmission radio est au cœur du fonctionnement de ces appareils.

Pour définir le concept, la transmission sans fil est un moyen de transférer des informations à travers l’espace en utilisant des ondes électromagnétiques. Ces ondes se déplacent à la vitesse de la lumière et peuvent traverser l’air, l’eau et même les murs.

## Présentation des différents modules de réceptions UHF

Bien que le fonctionnement puisse paraître mystérieux, il est le fruit d’une succession de principes simples. Dans le cadre de ce module, les station radio illustrent parfaitement le concept. On distingue donc quatre phases :

* Filtrage (passe bas, passe bande, passe haut)
* Amplification HF
* Démodulation
* Amplification audio

Le filtrage sert à séparer les différentes fréquences présentes dans le spectre radioélectrique afin de sélectionner uniquement les signaux désirés tout en éliminant les interférences et le bruit indésirable.

L'amplification HF est utilisée pour augmenter l'amplitude de ces signaux afin de les rendre suffisamment forts pour être traités par les circuits suivants du récepteur ou pour être émis avec une puissance adéquate. Les signaux peuvent subir des pertes lors de leur propagation à travers divers composants électroniques, câbles coaxiaux ou lignes de transmission. L'amplification HF compense ces pertes en augmentant l'amplitude du signal avant qu'il ne soit soumis à d'autres traitements ou avant d'être transmis à travers une ligne de transmission.

La démodulation est le processus consistant à extraire l'information utile, telle que la voix, les données ou tout autre contenu modulé sur une onde porteuse, à partir d'un signal modulé. Ce point sera abordé plus en détail par la suite.

## Introduction aux outils Radioamateur

Le radioamateur désigne l’ensemble des pratiques de la transmission sans fil de loisir. L’activité radioamateur permet d’acquérir ainsi des connaissances techniques dans le domaine de la radio et de l’électronique.

La radio logicielle, souvent désignée sous l’acronyme SDR (Software Defined Radio), représente une évolution majeure dans le domaine de la radiocommunication. Contrairement au radios traditionnelles qui dépendent d’un matériel spécifique pour fonctionner, les SDR utilisent des logiciels pour accomplir une grande partie du traitement des signaux radio, offrant ainsi une flexibilité et une adaptabilité sans précédent. On peut citer GNU Radio qui est incontestablement l’outils de référence dans cette discipline.

GNU Radio est un logiciel open-source ([gnuradio.org](https://www.gnuradio.org/)) et gratuit qui permet de concevoir et de simuler des systèmes de traitement numérique du signal pour la SDR. Les fonctionnalités sont multiples :

* Traitement Numérique du Signal : GNU Radio fournit un ensemble complet d'outils et de bibliothèques pour le traitement numérique du signal, permettant aux utilisateurs de concevoir et de mettre en œuvre une large gamme de fonctions de traitement des signaux.
* Conception Graphique : Une interface graphique intuitive permet aux utilisateurs de créer et de visualiser des flux de traitement du signal en les reliant par des blocs de traitement pré-conçus, ce qui facilite la conception et la simulation de systèmes de communication complexes.
* Support de Matériel : GNU Radio est compatible avec une variété de matériel SDR populaire tel que le RTL-SDR.
* Bibliothèques : GNU Radio comprend une vaste bibliothèque de blocs de traitement du signal, couvrant une gamme étendue de fonctions telles que la modulation, la démodulation, et de filtrage.

GNU Radio est utilisé dans de nombreuses applications, notamment :

* Radiocommunication amateure
* Radiodiffusion et télévision
* Réseaux de téléphonie mobile
* Surveillance du spectre radioélectrique
* Expérimentation et recherche dans le domaine des communications sans fil

GNU Radio est un outil puissant et polyvalent pour la conception et l'implémentation de systèmes de traitement du signal pour la radio logicielle et d'autres applications de radiocommunication. En tant que logiciel open-source, il offre aux utilisateurs une grande liberté et une flexibilité pour explorer et développer de nouvelles technologies dans ce domaine en constante évolution.

## Introduction à la notion de modulation/démodulation.

La modulation et la démodulation radio sont des concepts fondamentaux dans le domaine de la radiocommunication, qui permettent de transporter des signaux audio ou de données sur des ondes radio.

La modulation radio est le processus par lequel un signal de basse fréquence, tel que le son ou les données, est combiné avec une onde porteuse de haute fréquence pour être transmis efficacement à travers l'air. Cette technique permet de transporter les informations sur de longues distances en utilisant des ondes électromagnétiques. Elle implique la modification de certaines caractéristiques de l'onde porteuse, telles que son amplitude, sa fréquence ou sa phase, en fonction des variations du signal à transmettre. Cela permet d'imprimer les informations sur l'onde porteuse, créant ainsi un signal modulé qui peut être émis par une antenne et capté par un récepteur radio. Il existe plusieurs types de modulation, parmi lesquels les plus courants sont :

**Modulation d'Amplitude (AM) :** Dans ce type de modulation, l'amplitude de l'onde porteuse est modifiée en fonction du signal à transmettre.

**Modulation de Fréquence (FM) :** Ici, c'est la fréquence de l'onde porteuse qui est modulée en fonction du signal à transmettre.

**Modulation de Phase (PM) :** Dans ce cas, la phase de l'onde porteuse est modifiée en fonction du signal à transmettre. La modulation de phase est couramment utilisée dans les systèmes de communication numérique.

## Conception d’un module de réception pour la radio

**Objectif :** Concevoir et implémenter un récepteur radio FM (Frequency Modulation) en utilisant GNU Radio.

**Matériel nécessaire :**

* Un ordinateur avec GNU Radio installé.
* Une clé SDR (Software Defined Radio) compatible avec GNU Radio (par exemple, RTL-SDR).
* Antenne FM.
* Haut-parleurs ou casque audio pour écouter la station radio.

**Étapes du TP :**

* Configuration du matériel :
  + Installation des pilotes et logiciels nécessaire (GNU Radio, AirSpy)
* Présentation du GUI GNURadio
* Ajouter les blocs nécessaires pour :
  + Recevoir le signal radio FM à l'aide du bloc « RTL-SDR Source ».
  + Démoduler le signal FM à l'aide du bloc « Frequency Modulation ».
  + Convertir le signal audio à l'aide du bloc « WAV File Sink » ou « Audio Sink » pour l'écoute.
* Configuration des paramètres :
  + Configurer la fréquence de réception pour écouter une station de radio FM spécifique.
* Exécution et test
* Exploration avancée (facultatif) :
* Expérimenter avec différents paramètres de démodulation FM pour observer l'effet sur la qualité audio.
* Ajouter des fonctionnalités supplémentaires, comme la visualisation de la constellation, l'égalisation audio, etc.

À la fin du TD, les étudiants devraient avoir réussi à créer un récepteur radio FM fonctionnel en utilisant GNU Radio. Ils auront acquis une compréhension pratique des principes de base de la réception radio logicielle et seront en mesure d'explorer davantage les capacités de GNU Radio pour des applications de traitement du signal.

# 2er demi-journée – participation 54e RT

## Prise en main de l’arduino et ses modules

Ce module vise à fournir aux participants les connaissances de base nécessaires pour débuter avec l'Arduino et ses modules. À la fin du cours, les participants seront en mesure de comprendre les principes fondamentaux de l'Arduino, de réaliser des projets simples et d'utiliser différents modules pour étendre les fonctionnalités de leurs projets.

Pour commencer, il est important de comprendre les composants de base d'une carte Arduino, tels que le microcontrôleur, les broches d'entrée/sortie, les ports de communication, etc. Ensuite, il est recommandé de télécharger et d'installer le logiciel Arduino IDE, qui est l'environnement de développement intégré utilisé pour écrire, compiler et télécharger du code sur la carte Arduino.

Ensuite, les élèves peuvent commencer à explorer les fonctionnalités des capteurs compatibles avec Arduino.

La documentation officielle d'Arduino, ainsi que les nombreux tutoriels et exemples disponibles en ligne, sont des ressources précieuses pour apprendre à utiliser l'Arduino et ses modules de manière efficace. Avec de la pratique et de la persévérance, les débutants peuvent rapidement progresser et réaliser des projets électroniques passionnants avec l'Arduino.

## Conception d’un module d’émission/réception pour la radio

L’objectif de se module est de mettre en œuvre un émetteur radio en 433Mhz à l’aide d’un kit d’émission/réception pour Arduino.

Le kit émetteur-récepteur 433MHz est une option populaire pour la communication sans fil avec Arduino. Ce kit comprend généralement une paire de modules : un émetteur et un récepteur, chacun équipé d'une antenne pour la transmission et la réception des signaux à une fréquence de 433MHz.

La première étape consistera à connecter physiquement les différents modules entre eux. Une fois les connexions établies, on s’appuiera sur la bibliothèque VirtualWire compatible avec les modules émetteur-récepteur 433MHz pour émettre et recevoir des données entre les dispositifs Arduino.

Le code ci-dessous initialise la communication avec le module émetteur-récepteur 433MHz via la bibliothèque VirtualWire. Ensuite, dans la boucle principale, il envoie le message "Hello Word » à intervalles d'une seconde. Le message peut être personnalisé pour envoyer des codes précis (ex : 0 pour fermer et 1 pour ouvrir)

|  |
| --- |
| #include <VirtualWire.h>  const int transmitPin = 12; // Broche de transmission connectée à l'émetteur  const char\* message = "Hello World ; // Message à envoyer  void setup() {  // Initialise la bibliothèque VirtualWire avec la vitesse de transmission en bits par seconde  vw\_setup(2000); // Vitesse de transmission en bits par seconde  // Définir la broche de transmission comme sortie  pinMode(transmitPin, OUTPUT);  }  void loop() {  // Envoie le message  vw\_send((uint8\_t \*)message, strlen(message));  vw\_wait\_tx(); // Attente de la fin de la transmission  delay(1000); // Attente d'une seconde avant d'envoyer le message suivant  } |

## Analyse de la phase d’émission

L’idée de ce module est d’analyser l’émission du kit à l’aide d’outils SDR. On peut observer et analyser les caractéristiques du signal émis par le kit émetteur-récepteur 433MHz. Cela peut inclure des informations telles que la forme d'onde, la fréquence, la modulation, la puissance de transmission et d'autres paramètres. En s’appuyant sur la documentation de l’émetteur, l’idée est d’observer les concepts vus dans les modules précédents tels que la modulation, l’amplitude, la fréquence, etc.

L’analyse de la transmission de signal sera réalisée à l’aide d’une clé RTL-SDR. Cette approche utilise une clé USB RTL-SDR, qui est un récepteur radio logiciel économique capable de capturer et de traiter une large gamme de signaux radio.

L'avantage de cette méthode est sa polyvalence et sa capacité à fournir des informations détaillées sur le signal de la télécommande sans nécessiter de matériel spécialisé coûteux. De plus, les outils de traitement de signal disponibles avec les clés RTL-SDR offrent des fonctionnalités avancées telles que la démodulation, la détection d'interférences et l'analyse de protocoles de communication spécifiques.

# 3er demi-journée – participation 54e RT

## Introduction au concept d’interception

Ce module a pour dessein de présenter les techniques d'interception des signaux. L'interception des signaux consiste à capturer et à analyser les communications échangées entre des dispositifs sans fil, tels que les téléphones portables, les réseaux Wi-Fi, les systèmes de surveillance sans fil, et autres.

L'interception des signaux peut être réalisée à l'aide d'équipements spécialisés tels que les scanners radio, les antennes directionnelles, ou même des logiciels dédiés. Cette pratique peut être utilisée à des fins diverses, notamment la collecte de renseignements, le dépannage de réseaux sans fil, ou la recherche en sécurité informatique.

Dans ce module, nous explorerons les différentes techniques d'interception des signaux, y compris la surveillance passive et active, la détection des réseaux sans fil, la capture et l'analyse des paquets de données, ainsi que les mesures de protection contre l'interception.

Nous examinerons également les implications éthiques et légales de l'interception des signaux, ainsi que les moyens de protéger la confidentialité et la sécurité des communications sans fil.

En résumé, ce module vise à fournir une vue d'ensemble complète de l'interception des signaux, en mettant l'accent sur les techniques, les outils, les implications et les mesures de protection associées à cette pratique

## Audit de sécurité du système de transmission

L’objectif de ce module est d’aborder le concept de TEMPEST.

Le TEMPEST est un terme utilisé pour décrire les mesures de sécurité visant à protéger les systèmes informatiques contre les fuites d'informations par le biais d'émissions électromagnétiques involontaires.

Le TEMPEST vise à empêcher la divulgation non intentionnelle d'informations sensibles à partir d'équipements électroniques, tels que des ordinateurs, des écrans, des claviers et d'autres périphériques, en réduisant ou en contrôlant les signaux électromagnétiques qu'ils émettent.

Pour atteindre cet objectif, diverses techniques sont utilisées, notamment le blindage électromagnétique des équipements, la réduction de la puissance des signaux électromagnétiques émis, la modulation du spectre des signaux pour réduire les risques d'interception, et la conception de circuits et de dispositifs résistants aux attaques électromagnétiques.

Le TEMPEST est particulièrement important dans les environnements sensibles où la confidentialité des informations est primordiale, tels que les installations militaires, les agences gouvernementales, les centres de données sensibles et les entreprises traitant des données hautement confidentielles.

## Démonstration d’exploitation des vulnérabilités

Ce point conclue les différentes notions abordées.

Le rejeu d'un signal d'une télécommande consiste à intercepter le signal émis par une télécommande, puis à le reproduire pour effectuer la même action que celle initiée par l'utilisateur à l'origine. Cette technique est souvent utilisée pour contourner les systèmes de sécurité et accéder à des zones protégées ou des dispositifs contrôlés par une télécommande.

Pour réaliser le rejeu d'un signal de télécommande, un attaquant peut utiliser un récepteur radio (type RTL-SDR) pour capturer le signal émis par la télécommande lorsqu'un utilisateur appuie sur un bouton. Une fois le signal enregistré, l'attaquant peut le rejouer à l'aide d'un émetteur radio pour déclencher la même action que celle effectuée par l'utilisateur initial.

Cette technique de rejeu peut être utilisée pour diverses fins, y compris le vol de véhicules équipés de systèmes d'ouverture sans clé, le contournement des systèmes de sécurité des portes automatiques, des systèmes d'alarme ou des systèmes de contrôle d'accès.

Pour se protéger contre le rejeu de signal de télécommande, plusieurs mesures de sécurité peuvent être mises en place, telles que l'utilisation de télécommandes à code tournant qui génèrent un nouveau code à chaque pression de bouton, le chiffrement des signaux de télécommande pour éviter l'interception, ou l'ajout de mécanismes d'authentification supplémentaires pour vérifier l'identité de l'utilisateur

Matériels demandés :

* 1x Emetteur
  + Arduino
  + Module émetteur 433Mhz
  + Module bouton-poussoir
* 1x Récepteur
  + Arduino
  + Module récepteur 433Mhz
* Divers :
  + Plaque de montage rapide
  + Fil cuivré rigide FCR60
  + Assortiment de résistance
  + 1xClé RTL-SDR / élève