****

**I**nstitut **S**upérieur d’**I**nformatique

**M**odélisation et de leurs **A**pplications

1, Rue de la Chebarde

TSA 60125

CS 60026

63178 Aubière Cedex

France

*Rapport de Projet*

*3ème année d’élève ingénieur*

*Filière 5 – Réseaux et Sécurité Informatique*

2015/2016

Création d’une radio pirate à l’aide de la radio logicielle



Présenté par : HOANG Jimmy

JOUGLA Benoit

Tuteur de projet : TILMANT Christophe

Enseignant Référent : CHEMINAT Michel

Remerciements

Nous remercions Mr Christophe Tilmant, pour sa disponibilité et de son aide durant ce projet, ainsi que toutes les personnes qui nous ont aidé.

Table Figure et Illustrations

Résumé

Abstract

Table des matières

Glossaire

Introduction

Dans notre vie quotidienne, nous sommes entourés d’ondes. En passant par la radio FM, au service de météo, à la téléphonie et plus récemment aux objets connectés, de nombreux objets utilisent les ondes pour échanger des informations.

Dans le cadre des portes ouvertes de l’Isima, afin de représenter la filière F5, Réseaux et sécurité, nous devions présenter une application de radio logicielle.

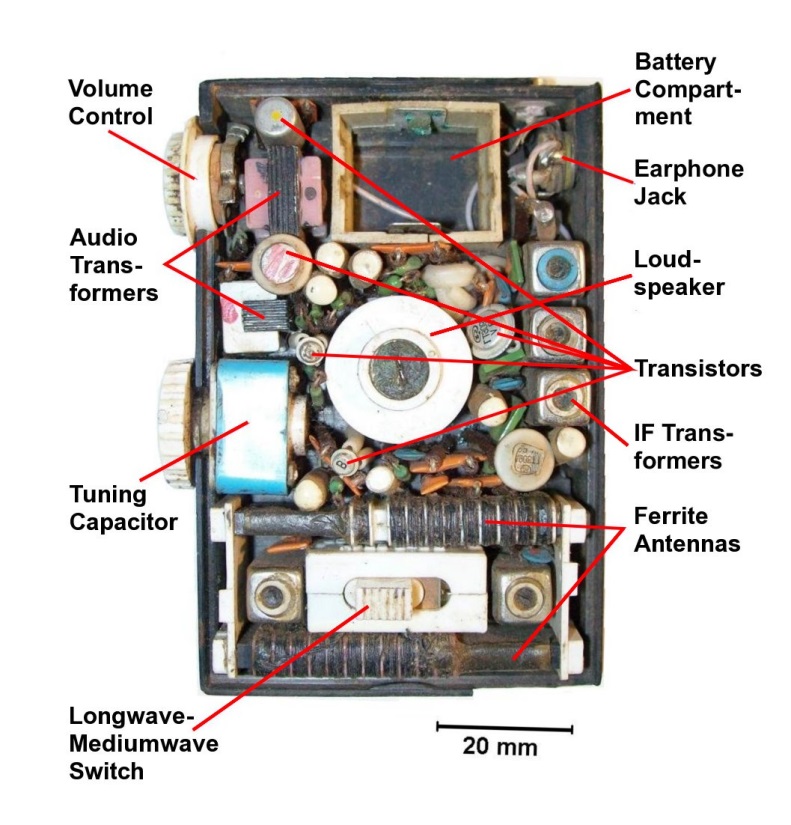
Ce projet a pour but de mettre en avant la filière F5 aux portes ouvertes de l’Isima.

Etant donné le nombre infini d’applications, qu’il est possible de réaliser, nous nous sommes concentré sur la réalisation d’une radio « pirate ».

Dans ce rapport nous allons tout d’abord nous intéresser à la définition de la radio logicielle et à certaines applications existantes. Ensuite nous présenterons les outils que nous avons utilisé dans le cadre ce projet ainsi que l’application que nous avons réalisé.

# I - Qu'es ce que la radio logicielle ?

La radio classique est un assemblage complexe de composant électronique dont le but est de traiter un signal, aussi bien à la réception qu'à l'émission, afin de transmettre et de recevoir des informations. Le système radio est spécifique à un signal.



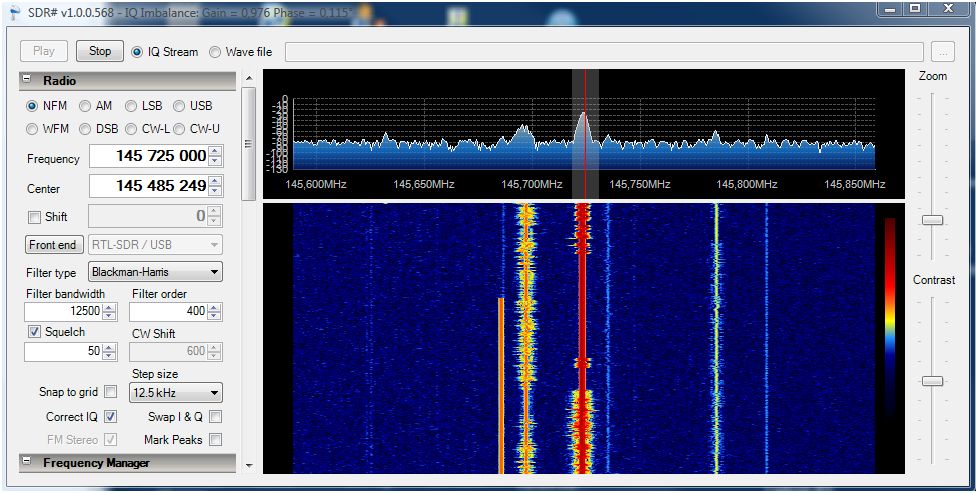
Une radio logicielle, au contraire, fonctionne de façon numérique à l'aide d'un processeur classique d'ordinateur. Un convertisseur analogique-numérique, lié à une antenne, permet de recevoir ou d'émettre sur une large bande de fréquences. Les signaux reçues seront ensuite traiter selon le type d'application. Il est donc possible d'utiliser le même équipement pour traiter une multitude de signaux, sous différentes formes et fréquences, en ne changeant que la partie logicielle.



La radio logicielle est beaucoup plus adaptable que la radio classique.

## Applications de réception

Les applications sont nombreuses et variées. Il est possible à l'aide d'une antenne adaptée de récupérer des informations de satellites, d'avions, de bateaux, … Il est possible de récupérer les signaux de n'importe quelle application qui émet des ondes. Par exemple, il est possible de récupérer les messages envoyés par les smartphones, messages envoyés par les services publiques comme la police, les pompiers, informations des avions, ...



## Applications d’émission

Pour émettre des ondes, cela est plus compliquées car les ondes sont protégées et réglementées. Il n'est pas possible de faire tout ce qu'on veut sous peine de sanction. Les fréquences radioélectriques appartiennent au domaine public de l'Etat. L'ANFR, l'Agence Nationale des Fréquences, gère et contrôle l'utilisation de ces fréquences. Par exemple, il est possible de contrôler un drone avec un PC via une interface radio, ouvrir fermer une porte de garage, …



# II – Les outils

## Gnu radio :

Afin de réaliser des applications de radio logicielle, nous avons utilisé une suite logicielle dédiée à leurs implémentations, Gnu Radio. L'utilisation du logiciel s'articule autour de blocs qu'il suffit d'interconnecter les uns aux autres. Les blocs comprennent des sources (récepteur radio, fichier, …), des blocs de traitements de signal, de l'affichage graphique, ainsi que des blocs de sorties (audio, graphique, …).

Pour réaliser une chaîne de traitement du signal, il est possible de le réaliser en le codant dans un des nombreux langages pris en charge par le logiciel, c++, python, … ou en utilisant une interface graphique, Gnu Radio Companion, qui permet d'assembler les modules graphiquement.

La sonde spatiale internationale Cometary Explorer, qui a été lancé en 1978 par la NASA pour surveiller l’activité du soleil, est actuellement sous le contrôle de GNU RADIO. En 1999, la NASA abandonna le satellite sur l’orbite du soleil. En 2008, le satellite était toujours opérationnel, un groupe de scientifique et de programmeur réussirent à reprendre le contact du satellite, en 2014, en adaptant GNU RADIO au protocole utilisé dans les années 1970.

## HackRF One :

Le HackRF One est un émetteur-récepteur pour la radio logicielle. Il couvre avec les antennes adaptées les fréquences de 1MHz à 6GHz.

# III - Radio "pirate"

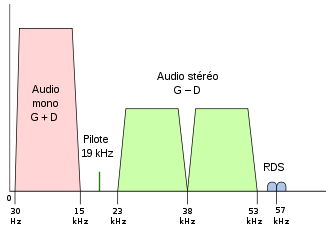
Dans le cadre de ce projet, nous avons décidé de développer une radio "pirate". L'application permet de diffuser de la musique et de diffuser des messages.

## Principe

Au départ, la radiodiffusion consistait à moduler en fréquence la porteuse par un signal audio monophonique, d’une largeur de 15kHz. Avec l’arrivé de la stéréophonie et d’autres services, tels que le RDS (Radio Data System), le signal est devenu un signal multiplexe.

Pour garder la compatibilité avec les récepteurs monophoniques, un signal est émis sans modulation de 30Hz à 15kHz. Dans les émissions en stéréo, ce signal monophonique représente en réalité des deux canaux stéréo gauche et droite (G+D). De cette façon un récepteur monophonique dispose bien de l’ensemble des sons émis. En stéréo, la différence des voies (G – D) est en plus transmise en modulant une sous-porteuse à 38kHz. Un signal pilote à 19kHz est ajouté au signal pour indiquer la présence de la stéréo et permettre le décodage de sous-porteuse sans risque de déphasage du son. Pour obtenir les voies gauche ou droite, le récepteur stéréophonique effectue respectivement la somme ou la différence des deux signaux G+D et G-D. La somme permet d’obtenir le résultat 2G et la différence 2D.

Les informations du RDS sont transmises sous forme numérique, via une sous porteuse à 57kHz.

[](https://commons.wikimedia.org/wiki/File:Modulation_radiodiffusion_FM.svg?uselang=fr)

## Protocole RDS

Le protocole RDS est un service de transmission de données, il permet l’écoute d’une station sans interruption lors d’un déplacement, en prenant en charge automatiquement le passage d’une fréquence à l’autre, il fournit une identification des stations par leur nom, des messages textuels, des flashes routier, etc.

### Trames RDS

La transmission d’une trame RDS est constituée de 4 blocs de données. Ils sont transmis en continu sans interruption. Un bloc est constitué d’une donnée sur 16 bits associée à un mot de contrôle de 10 bits. Les blocs sont transmis dans l’ordre A, B, C et D. Ces 4 blocs forment un groupe. Un groupe fait donc 104 bits (4\*26).

Le bloc A est utilisé pour transmettre le code d’identification de la radio, le bloc B permet d’identifier le type de données transmis et les blocs C et D contiennent les données.