

Le décodage ADS-B comme observable des propriétés physiques d'une antenne

Culture Sciences
de l'Ingénieur

La Revue
3E.I

Thomas ORTEGA¹

Édité le
07/07/2026

école —
normale —
supérieure —
paris—saclay —

¹ Lycée Militaire de Saint-Cyr l'Ecole - BTS CIEL IR option spécifique cyber-défense

Cette ressource fait partie du N° 120 de La Revue 3EI du 3^{ème} trimestre 2026.

Cet article a pour objet d'apporter les éléments d'une activité pédagogique pratique autour de la réception et du décodage des signaux ADS-B (Automatic Dependent Surveillance-Broadcast) émis par les aéronefs civils à 1090 MHz. Dans le contexte de l'enseignement en BTS CIEL, l'étude de ces signaux en radio logicielle avec GNU Radio permet aux étudiants de confronter les concepts enseignés en physique avec le concret.

L'idée centrale est ici d'utiliser le nombre d'avions détectés comme indicateur observable et motivant de la performance de chaque antenne réalisée.

En utilisant un récepteur de radio logicielle peu onéreux et le logiciel open-source GNU Radio, les étudiants construisent leurs propres antennes, reçoivent en temps réel les trames de position des avions, les décodent et comparent leurs résultats avec les données publiées par exemple par Flightradar24. Cette approche développe simultanément des compétences en propagation radio, en traitement du signal numérique, en protocoles de communication, en programmation Python et en cybersécurité.

La radio logicielle (Software Defined Radio, SDR) offre un terrain d'exploration exceptionnel pour le co-enseignement Physique-Informatique en BTS CIEL.

Cet article repose sur la mise en œuvre de GNU Radio en enseignement de physique par Thomas LAVARENNE qu'il a présentée en particulier à l'European GNU Radio Days [1].

1 - Intérêt pédagogique : pourquoi l'ADS-B en co-enseignement BTS CIEL ?

Le BTS CIEL (Cybersécurité, Informatique et réseaux, Électronique), dans ses deux options - option A (Informatique et réseaux) et option B (Électronique et réseaux) - place les enseignants devant un défi structurant : co-animer, à deux enseignants, des contenus de physique appliquée (propagation des ondes, antennes, chaîne de réception radio) avec des contenus informatiques (traitement numérique du signal, protocoles, programmation) autour des mêmes compétences. Le co-enseignement constitue une réponse naturelle, à condition de disposer d'un objet d'étude commun, concret et motivant pour les étudiants, et accessible aux deux enseignants.

L'ADS-B répond parfaitement à ces exigences, pour plusieurs raisons :

- accessibilité et gratuité du signal : émis avec une puissance de l'ordre de 200W, le signal est assez facile à recevoir pour tout avion commercial en vol au-dessus du lieu

d'enseignement. Le signal est non chiffré, non soumis à autorisation de réception, et disponible sans abonnement.

- résultat visible et vérifiable en temps réel : les avions décodés s'affichent sur une carte et peuvent être immédiatement comparés avec Flightradar24, ce qui procure une satisfaction immédiate et valide concrètement le travail des étudiants.
- fil directeur unique : le nombre d'avions détectés. Ce compteur synthétise en une seule grandeur l'ensemble de la chaîne (qualité de l'antenne, placement, gain RF, seuil de décodage) et constitue une métrique de performance objective et concrète accessible à tous les étudiants, quel que soit leur niveau.
- coût réduit : un clef USB RTL-SDR (~40 €) suffit pour une version allégée et des antennes fabriquées par les étudiants à partir d'un connecteur SMA, de câble coaxial et de fil de cuivre (~4 € chacune).
- richesse des contenus pluridisciplinaires : le TP mobilise la transmission des ondes électromagnétiques, la caractérisation temporelle et fréquentielle des signaux, les caractéristiques des antennes et le lien entre longueur d'onde et longueur de l'antenne, la transmission numérique en bande de base et le codage Manchester, les protocoles de communication, la vérification CRC, la programmation Python – autant de points inclus dans le référentiel BTS CIEL.

Plusieurs compétences du BTS CIEL option A ou option B sont susceptibles d'être mises en œuvre :

- Supports de propagation dans les réseaux informatiques (compétences C04 analyse et C05 conception).
- Caractéristiques des communications présentes dans les systèmes informatiques étudiés (compétences validation C06, installation C09 et exploitation C10).
- Principes de transmission en espace libre ou guidée dans les réseaux informatiques (compétences analyse C04 et conception C05).

La documentation réglementaire et technique peut aussi faire l'objet d'une exploitation en co-enseignement anglais (ESLA) en exploitant les documents techniques ou vidéo [2] en langue anglaise.

2 - Régulation du trafic aérien et transpondeurs

2.1 - Contexte historique : du radar primaire à l'ADS-B

La surveillance du trafic aérien repose historiquement sur deux technologies complémentaires :

- Le radar primaire (PSR, Primary Surveillance Radar) détecte les aéronefs par réflexion d'une impulsion radio (principe de l'écho). L'onde est émise par une antenne souvent en rotation continue. La différence de temps entre l'émission et la réception fournit la position angulaire et la distance – sans identification.
- Le radar secondaire (SSR, Secondary Surveillance Radar) interroge activement les transpondeurs des aéronefs à 1030 MHz en émettant deux ou trois impulsions radio. Ceux-ci répondent au code d'interrogation à 1090 MHz avec leur code d'identification (squawk ident en Mode A) et leur altitude telle que mesurée dans l'aéronef (par incrément de 100 pieds en mode C). La séparation temporelle entre les impulsions émises détermine le mode utilisé et donc la question posée.

Le Mode S (Mode Select Beacon System, développé au MIT Lincoln Laboratory dans les années 1970 et déployé dans les années 1990, améliore le SSR en ajoutant la fonctionnalité d'interrogation sélective de chaque aéronef via une adresse unique de 24 bits, identifiant fixé par l'Organisation de l'aviation civile internationale (OACI) (ICAO en anglais), capable d'adresser jusqu'à 16 777 216 aéronefs distincts. Les codes ICAO sont accessibles sur des bases en lignes comme OpenSky [3].

L'ADS-B (Automatic Dependent Surveillance-Broadcast) représente l'étape suivante : l'aéronef diffuse spontanément ses données de vol à intervalles réguliers, sans interrogation, sur la fréquence 1090 MHz. C'est précisément sur cette émission radio que repose la suite de cet article : il n'est pas nécessaire d'être à proximité d'un aéroport pour l'étudier.

L'acronyme ADS-B se décompose ainsi :

- *Automatic* : aucune action du pilote ni du contrôleur n'est requise ;
- *Dependent* : le système dépend des récepteurs GNSS embarqués par les aéronefs pour calculer la position ;
- *Surveillance* : il remplit une fonction de surveillance du trafic ;
- *Broadcast* : la diffusion est omnidirectionnelle, à destination de toute station capable de recevoir.

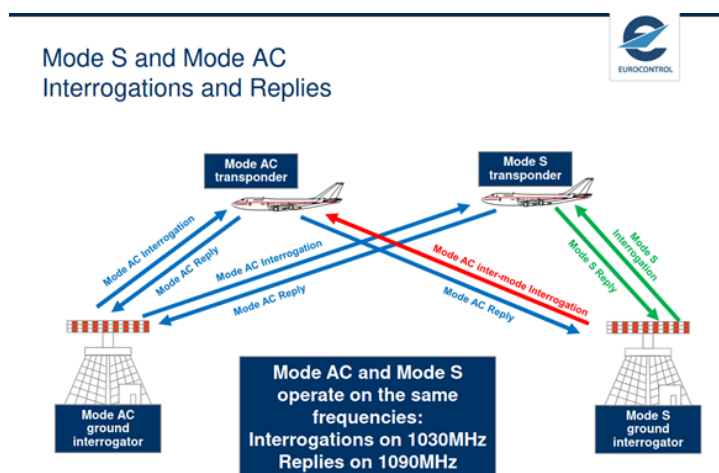


Figure 1 : Modes S et A/C, source ICAO [4]

En utilisant l'interrogation sélective, le protocole améliore considérablement la capacité de transfert de données sur le canal de la porteuse (1090MHz). Mais ce qui nous intéressera dans cet article, c'est une approche passive basée sur le décodage des informations émises en broadcast par les aéronefs.

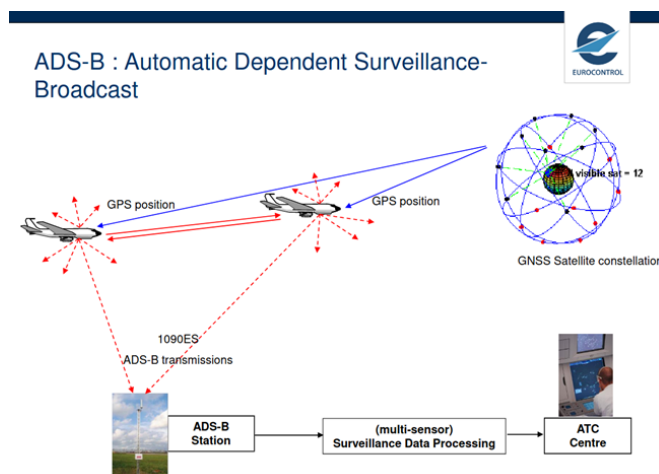


Figure 2 : ADS-B, source ICAO [4]

Encadré - Extrait de The 1090MHz Riddle (Second Edition) - Junzi Sun [5]

Automatic Dependent Surveillance-Broadcast (ADS-B) is a surveillance technology designed to allow aircraft to broadcast their flight state periodically without the need for interrogation.

The word automatic refers to the fact that no inputs from controllers or pilots are required.

The word dependent indicates this technology depends on information from other onboard systems, such as air data systems and navigation systems.

ADS-B only become possible because of Global Navigation Satellite Systems (GNSS), such as Global Positioning System (GPS), which is the first GNSS system made available for civil usage by the USA after the Korean Air Lines Flight 007 accident in 1983.

Common aircraft state parameters included in ADS-B are position, altitude, and speed.

The position is determined by GNSS and air data systems.

The velocity is derived from the GNSS position and the inertial measurement system.

The altitude information includes both barometric altitude and GNSS altitude. The barometric altitude is provided by the air data system.

In addition to these primary state parameters, ADS-B also allows other information to be broadcast, for example, aircraft call-sign, accuracy indicators, integrity indicators, and operational status.

It is worth emphasizing that ADS-B is a broadcast-based surveillance system. Unlike other types of Mode S surveillance, no surveillance interrogation is required. The decoding of ADS-B messages is also easier than other Mode S messages because the message type and structure are clear for each individual message.

Different types of ADS-B messages are identified by Type Codes. The structures of these messages are all defined in ICAO documents.

2.2 - Déploiement mondial et obligation réglementaire

Depuis le 7 juin 2020, tout aéronef civil qui navigue dans l'espace aérien européen au-dessus du plancher de vol FL245 (environ 7 500 m) doit être équipé d'un transpondeur ADS-B opérationnel (règlement d'exécution UE 2017/386) (https://eur-lex.europa.eu/eli/reg_impl/2017/386/oj/eng). Aux États-Unis, la réglementation FAA impose l'ADS-B Out depuis janvier 2020 pour les espaces aériens contrôlés. La quasi-totalité des avions commerciaux émet donc des signaux ADS-B en continu.

2.3 - Les sites de surveillance participative

Plusieurs sites dont Flightradar24, FlightAware ou OpenSky illustrent parfaitement le potentiel de l'ADS-B : il agrège les données de milliers de stations de réception réparties dans le monde entier (dont beaucoup sont des particuliers utilisant un simple récepteur radio logiciel RTL-SDR) pour afficher en quasi-temps-réel la position de tous les avions visibles. Cette infrastructure participative repose entièrement sur la réception passive du signal ADS-B - exactement ce que les étudiants mettent en œuvre dans ce TP. Ils constituent un outil externe de validation des montages des étudiants.



Figure 3 : Capture d'écran de FlightRadar24 montrant les aéronefs au-dessus de la France, source www.flightradar24.com

3 - Structure des trames ADS-B

3.1 - Les sites de surveillance participative

Le signal ADS-B est transmis à 1090 MHz avec une modulation PPM (*Pulse Position Modulation*) :

- Un bit «1» est représenté par une impulsion dans la première moitié de la période, suivie d'un silence ;
- Un bit «0» est représenté par un silence dans la première moitié, suivi d'une impulsion.

Le débit binaire est de 1 Mbit/s, soit une durée de bit $T_b = 1 \mu s$. Chaque trame est précédée d'un préambule fixe de 8 μs (séquence binaire 10100000 01000000, A040 en hexadécimal) permettant la synchronisation. Ce préambule sera utilisé ultérieurement avec GNU Radio pour identifier le début des trames à capturer.

Encadré - Codage Manchester et PPM

Le signal ADS-B utilise la Modulation d'impulsions en position ou PPM (*Pulse Position Modulation*), parfois assimilée au codage Manchester car les deux codages encodent chaque bit par une transition. En PPM stricte, c'est la position de l'impulsion au sein de la période bit qui porte l'information (première ou deuxième moitié), alors qu'en Manchester c'est la direction de la transition (montante ou descendante). Les deux approches nécessitent 2 échantillons par bit pour être décodées correctement, ce qui explique le taux d'échantillonnage de 2 MHz utilisé dans GNU Radio.

3.2 - Structure d'une trame ADS-B

Une trame ADS-B complète comporte **112 bits** organisés comme suit :

DF (5 bits)	CA (3bits)	ICAO (24 bits)	ME / DATA (56)	PI (24bits)
-------------	------------	----------------	----------------	-------------

Avec la décomposition suivante :

Champ	Bits	Description
DF	1-5	<i>Downlink Format</i> : pour les trames ADS-B mode S Extended Squitter des aéronefs civils, DF vaut 17 (10001 en binaire)
CA	6-8	<i>Capability</i> : capacité du transpondeur (0 à 7)
ICAO	9-32	Adresse unique de l'aéronef (24 bits, hexadécimal)
ME	33-88	<i>Message Extended squitter</i> : données de position, vitesse, identification
PI	89-112	<i>Parity/Interrogator</i> : CRC-24 pour contrôle d'intégrité

On retiendra de la valeur de CA :

CA=0 : transpondeur type 1

CA=4 : transpondeur type 2, l'aéronef est au sol

CA=5 : transpondeur type 2, l'aéronef est en vol

CA=6 ou 7 : l'aéronef est en vol ou au sol

Le détail complet des trames est détaillé dans l'ouvrage *The 1090 Megahertz Riddle* [5].

Les 5 premiers bits du champ ME constituent le Type Code (TC), qui identifie le type de message :

TC	Contenu
1-4	Identification et catégorie (indicatif)
5-8	Position en surface
9-18	Position en vol (altitude barométrique)
19	Vitesse en vol
20-22	Position en vol (altitude GNSS)
28	Statut aéronef
31	Statut opérationnel

3.3 - Contrôle d'intégrité : le CRC-24

Le champ PI de 24 bits est un **CRC** (*Cyclic Redundancy Check*) calculé sur les 88 premiers bits de la trame. Le polynôme générateur utilisé est :

$$G(x) = x^{24} + x^{23} + x^{22} + x^{17} + x^{10} + x^3 + x + 1$$

Ce CRC permet de détecter (mais pas de corriger) les erreurs de transmission. Un message dont le CRC ne correspond pas doit être rejeté. En pratique, avec la modulation PPM et le rapport

signal/bruit typique en réception, le taux d'erreur sur les trames reçues peut être significatif, surtout pour les aéronefs lointains.

3.4 - Exemple de décodage du début d'une trame

Prenons la trame binaire reçue par un récepteur :

10001 101 010010000100 000011010110 00100 0000010110011 00001101110001110000
110010110011100000 | 010101110110 000010011000 |

soit en hexadécimal : 8D4840D6 2202CC37 1C32CE0 576098

- DF = 10001 = 17 en décimal → Extended Squitter ADS-B ✓
- CA = 101 = 5 en décimal → transpondeur niveau 2 et l'aéronef est en vol
- ICAO = 4840D6 → adresse ICAO hexadécimale 24bit de l'aéronef.

La consultation de la base OpenSky Network, Flightradar24 ou mieux planespotter via l'URL : <https://www.planespotters.net/hex/4840D6> permet de confirmer qu'il s'agit bien d'un vol KLM , appareil Fokker 70 dont l'indicatif est PH-KZD

- TC (5 premiers bits de ME) = 00100 = 4 → message d'identification

Le décodage de cette partie sera suffisant pour l'activité proposée. Elle pourra toutefois être poursuivie avec le décodage de la position, l'altitude et la vitesse.

3.5 - Position, altitude, vitesse

Le décodage de la position géographique d'un avion à partir des trames ADS-B est un point intéressant qui peut être exploité en co-enseignement mathématique-informatique. En effet les messages de type TC=9 à 22 transmettent latitude et longitude non pas directement en degrés décimaux, mais dans un format compact appelé CPR (Compact Position Reporting).

Encoder une latitude avec une précision de 5 m au niveau mondial nécessiterait 26 bits pour chaque coordonnée, soit 52 bits pour la paire (latitude, longitude). Le format CPR permet d'atteindre la même précision avec seulement 17 bits par coordonnée (34 bits au total), en exploitant le fait que des messages successifs d'un même avion sont reçus à intervalles rapprochés et qu'on n'a donc pas besoin d'un repère absolu et univoque à l'échelle de la planète. On alterne deux grilles de codage légèrement différentes : la trame paire (F=0) et la trame impaire (F=1). La résolution globale résulte de la combinaison des deux trames [6].

Deux sources d'altitudes sont transmises : l'altitude calculée par l'aéronef à partir des constellations satellites GNSS et l'altitude barométrique issue des mesures de pression par l'aéronef. Ces deux modes de calcul de l'altitude seront utilisés aussi pour calcul la vitesse ascensionnelle dans la partie vitesse.

En ce qui concerne la vitesse, trois composants sont transmis par ADS-B :

- DEWS (10 bits) : composante Est-Ouest de la vitesse sol
- DNS (10 bits) : composante Nord-Sud de la vitesse sol
- VR (10 bits) : taux de montée/descente vertical

Il est donc aussi possible d'en faire calculer le cap de l'aéronef.

Le détail complet des trames est détaillé dans l'ouvrage *The 1090 Megahertz Riddle* [5].

4 - Evaluation de la réception théorique

4.1 - Propagation des ondes de la bande L

La fréquence 1090 MHz appartient à la bande L (définie par les fréquences de 1 à 2 GHz). Cette bande de fréquence est utilisée par des services de radio astronomie, des usages militaires, de la téléphonie mobile (LTE 1800), quelques radars spécifiques, une partie de radio numérique (DAB), les constellations satellites de positionnement GNSS (GPS/Galileo/GLONASS/Beidou) et ADS-B.

Pour la fréquence 1090 MHz, la longueur d'onde est $\lambda = \frac{c}{f} = \frac{3 \times 10^8}{1,09 \times 10^9} \approx 27,5 \text{ cm}$

Cette bande est caractérisée par propagation quasi-optique. La pluie et les nuages ont une atténuation négligeable à cette fréquence. Les obstacles (collines, bâtiments) créent des zones d'ombre importantes. C'est pourquoi l'élévation de l'antenne est le paramètre le plus critique pour maximiser le nombre d'avions détectés. Il faudra donc veiller à placer les antennes sur un même niveau pour avoir des résultats significatifs.

4.2 - Portée géométrique maximale

Le signal ADS-B utilise une porteuse à 1090 MHz. Cette fréquence est située dans la bande L qui est connue pour se propager en ligne de vue. En supposant l'absence d'obstacles et une puissance d'émission suffisante, la portée maximale est alors géométriquement limitée par la courbure de la Terre :

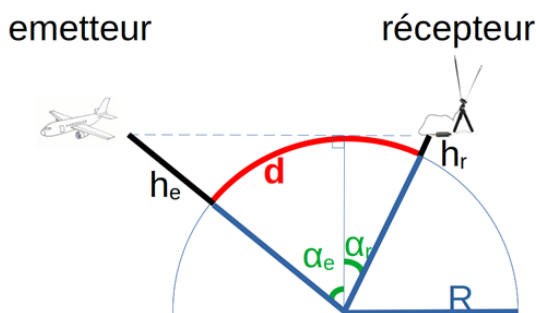


Figure 4 : Positions de l'émetteur et du récepteur sur la courbure de la Terre

Avec : $R = 6,371.10^6 \text{ m}$ (rayon terrestre moyen)

h_e = altitude de l'aéronef au-dessus du niveau de la mer (en m)

h_r = altitude de l'antenne réceptrice (en m)

Longueur l'arc de cercle $d = (\alpha_e + \alpha_r) \times R$

$$d = \left(\arccos\left(\frac{R}{R + h_r}\right) + \arccos\left(\frac{R}{R + h_e}\right) \right) \times R$$

Ainsi pour un récepteur placé à 50 m d'altitude et un avion à 10 km d'altitude, la distance maximale serait de l'ordre de 400 km :

$$d = \left(\arccos\left(\frac{6,371.10^6}{6,371.10^6 + 50}\right) + \arccos\left(\frac{6,371.10^6}{6,371.10^6 + 10^4}\right) \right) \times 6,371.10^6 \approx 397.10^3 \approx 397 \text{ km}$$

Cette portée théorique n'est cependant qu'un maximum géométrique. En conditions réelles, le modèle de Friis impose que la portée dépende aussi de la puissance d'émission, des gains d'antenne et des pertes de trajet.

4.3 - Bilan de liaison selon Friis

La formule de transmission de Friis donne la puissance reçue en espace libre :

$$P_r = P_e + G_e + G_r - \alpha$$

avec :

- P_r = Puissance reçue (dBm)
- P_e = Puissance émise (dBm)
- G_e = Gain d'antenne émission (dBi)
- G_r = Gain d'antenne réception (dBi)
- α = perte de propagation (dB) en espace libre $\alpha = 20 \times \log_{10} \frac{4\pi\delta}{\lambda}$

avec δ = Distance entre l'émetteur et le récepteur (en mètres)

λ = Longueur d'onde (en mètres)

4.4 - Application numérique

Puissance émise (P_e)



Figure 5 : Façade du transpondeur Garmin GTX™ 345

La fiche technique du transpondeur Garmin GTX 345 indique une puissance d'émission du signal de 200W soit, (en utilisant la formule de conversion $P(\text{dBm})=10\log_{10}(1000 \times P(\text{W}))$) $P_e=+53\text{dBm}$.

Gain des antennes

On peut dans un premier temps prendre comme approximation qu'une antenne d'émission a un gain nul ($G_e=3\text{dBi}$) car incluse dans le système du transpondeur et donc dans ses caractéristiques. On peut aussi prendre en approximation qu'une antenne de réception type spider $\lambda/4$ a un gain de 3dBi ($G_r=3\text{dBi}$). La qualité des antennes de réception pourra faire l'objet de mesures fines grâce à un équipement NanoVNA (Network Vector Analyzer de poche, accessible chez des fournisseurs habituels pour moins d'une centaine d'euros).

Sensibilité du récepteur

Des mesures effectuées sur les clefs RTL-SDR montrent une sensibilité de l'ordre de -129dBm à 1GHz. (cf blog RTL SDR <https://www.rtl-sdr.com/measurements-on-rtl-sdr-e4000-and-r820t-dvb-t-dongles-image-rejection-internal-signals-sensitivity-overload-1db-compression-intermodulation/>).

Dans des conditions de réception difficile, ou à titre d'extension de TP pour les élèves qui ont avancé plus rapidement, elle peut être augmentée d'environ 6 dB par l'ajout d'un amplificateur LNA (low-noise amplifier) externe généraliste, ou 16 dB avec un amplificateur LNA et un filtre passe bande centré sur 1090 MHz (ces équipements accessibles chez les fournisseurs habituels pour quelques dizaines d'euros).

Pour une distance émetteur-récepteur $\delta = 200$ km :

$$\alpha = 20 \times \log_{10} \frac{4 \times \pi \times 200,000}{0,275} = 20 \times \log_{10}(9,12 \cdot 10^6) \approx 139,2dB$$
$$P_r = 53 + 0 + 3 - 139,2 = -83,2dBm$$

La puissance du signal reçu est bien au-dessus du plancher de tous les récepteurs la détection est assurée.

Pour une distance émetteur-récepteur $\delta = 500$ km :

$$\alpha = 20 \times \log_{10} \frac{4 \times \pi \times 500000}{0,275} \approx 147,2dB$$
$$P_r = 53 + 0 + 3 - 147,2 = -91,2dBm$$

La puissance du signal reçu est supérieure au seuil de sensibilité des récepteurs mais elle sera conditionnée par le dégagement de l'antenne car on est à la limite géométrique pour un aéronef volant à 10 km d'altitude.

Conclusion du bilan de liaison de Friis : la portée Friis est presque toujours inférieure à la portée géométrique (sauf pour les avions très proches). Pour les avions en croisière (10 km d'altitude), la limite pratique avec un RTL-SDR et une antenne de type *spider* est de l'ordre de 350-400 km.

4.5 - Exploitation pédagogique

Les étudiants comprennent ici que la chaîne de réception a deux limites indépendantes – géométrique (courbure de la Terre) et énergétique (Friis) – et que c'est la plus contraignante qui s'impose. Pour les avions en croisière, c'est presque toujours la limite géométrique qui domine.

Les étudiants peuvent, à partir de la formule géométrique, prédire la portée maximale attendue depuis leur lycée en fonction de l'altitude des avions en croisière (typiquement 200km à 12200km). Ils tracent ensuite la courbe théorique et la comparent avec les données réellement reçues (position GPS des avions décodés). L'écart entre théorie et mesure ouvre la discussion sur les obstacles locaux, le relief et la qualité de l'antenne.

5 - Importance des antennes

5.1 - Pourquoi l'antenne est-elle le facteur clef ?

Dans la chaîne de réception ADS-B, le récepteur SDR est suffisamment performant pour ne pas être le maillon limitant. La **qualité de l'antenne** et son **placement** déterminent à eux seuls la majorité de la performance : une antenne bien accordée à 1090 MHz capte des avions bien au-delà de l'horizon, là où une antenne TNT désaccordée ou un simple fil ne reçoit que les avions proches.

C'est l'idée centrale du TP : **mesurer le nombre d'avions détectés sur une fenêtre de temps fixe** (par exemple 15 minutes) permet de comparer objectivement et de façon reproductible les performances de différentes antennes réalisées par les étudiants.

5.2 - Appel : longueur d'onde à 1090 MHz

$$\lambda = \frac{c}{f} = \frac{3 \times 10^8}{1,09 \times 10^9} \approx 27,5cm$$

Les longueurs caractéristiques des antennes accordées à 1090 MHz sont donc :

$\lambda/2 = 13,75 \text{ cm}$ (demi-onde, dipôle ou monopole)

$\lambda/4 = 6,875 \text{ cm}$ (quart d'onde, élément d'une antenne planaire)

5.3 - Types d'antennes réalisables par les étudiants

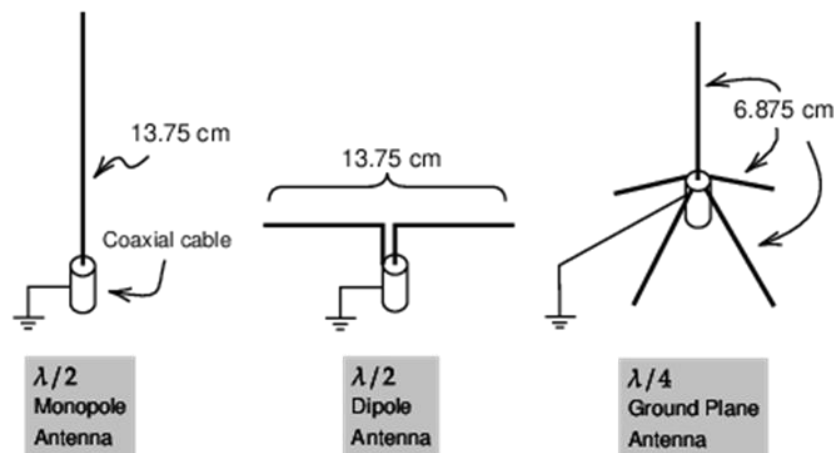


Figure 6 : Schéma des de différentes formes d'antenne, source The 1090MHz Riddle [5]

Antenne monopole $\lambda/2$: un simple fil de cuivre 13,75 cm soudé sur un connecteur SMA. Facile à réaliser, gain nul (0 dBi), directivité quasi-omnidirectionnelle dans le plan horizontal. C'est la référence de base.

Antenne dipôle $\lambda/2$: deux brins de 13,75 cm montés en opposition sur un câble coaxial, le brin central et la tresse formant les deux éléments. Gain théorique $\approx 2,15 \text{ dBi}$. Légèrement supérieure au monopole. L'utilisation d'un double domino à vis ou de deux connecteurs rapides type Wago simplifie le montage mécanique.

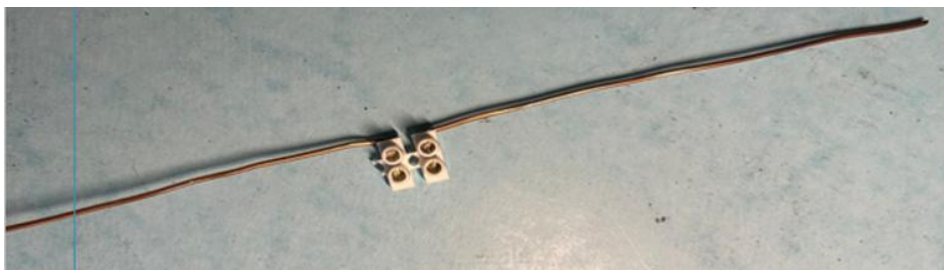


Figure 7 : Montage d'un dipôle à l'aide d'un domino

Antenne planaire quart d'onde (*Spider*) : un élément vertical central de $\lambda/4 = 6,875 \text{ cm}$ entouré de 4 à 6 radiaux horizontaux de même longueur. C'est l'antenne de référence pour la réception ADS-B. Gain $\approx 2-3 \text{ dBi}$, omnidirectionnel dans le plan horizontal, cette antenne est très adaptée à la réception depuis toutes les directions.

Antenne Yagi TNT de récupération : une antenne de télévision terrestre peut être détournée pour 1090 MHz si ses éléments sont approximativement accordés. Gain élevé (6-10 dBi) mais directionnelle : efficace uniquement dans la direction pointée, ce qui réduit le nombre d'avions vus. Les fréquences de la TNT sont comprises entre 470MHz et 790MHz ; ces antennes comportent souvent un filtre démontable plus ou moins facilement et dont on peut étudier l'influence.

Antenne planaire demi-onde : variante de l'antenne type *spider* avec des radiaux plus longs ($\lambda/2$), légèrement différente en termes de diagramme de rayonnement.

5.4 - Réalisation pratique par les étudiants

Matériaux nécessaires par groupe :

- 1 mètre de câble coaxial (pour limiter les soudures, on peut prendre un cordon avec un connecteur SMA déjà serti à une extrémité)
- 1 connecteur SMA mâle à souder par type d'antenne
- Fil de cuivre rigide 1,5 mm² (électricité)
- Étain et fer à souder
- Mètre ruban, pince coupante, dénudeur

Conseils pratiques :

- Les tolérances de ± 2 mm sont acceptables à 1090 MHz.
- Un multimètre en mode « continuité » permet de vérifier qu'il n'y a pas de court-circuit entre l'âme et la tresse.
- L'utilisation d'un analyseur d'antenne type NanoVNA, (*Network Vector Analyzer* de poche, accessible chez des fournisseurs habituels pour moins d'une centaine d'euros) permet de mesurer le taux d'onde stationnaire (TOS ou SWR) et les pertes par réflexion (Return Loss) d'une antenne en fonction de la fréquence. Pour les étudiants BTS CIEL, c'est un outil de validation expérimentale direct entre le calcul théorique et la performance mesurée.
- Dans notre contexte pédagogique, le NanoVNA valide le dimensionnement (cotes correctes) de l'antenne, et le comptage d'avions mesure la performance globale incluant le gain. Le NanoVNA est une aide précieuse pour l'accord des antennes :
 - **Résonance trop haute** (ex. : minimum SWR à 1150 MHz)
→ l'antenne est trop courte. Allonger légèrement les brins (+1 à 2 mm).
 - **Résonance trop basse** (ex. : minimum SWR à 1040 MHz)
→ l'antenne est trop longue. Raccourcir les brins.
 - **SWR minimum > 2 à 1090 MHz**
→ vérifier la qualité des soudures, la continuité et l'absence de court-circuit partiel.

On peut fixer comme objectif pour d'obtenir une mesure SWR < 1,5 à 1090 MHz

6 - Mise en œuvre de GNU Radio pour la réception des frames

6.1 - Présentation de GNU Radio

GNU Radio est un framework open-source de traitement du signal, disponible sous licence GPL. Il permet de construire des diagrammes de flux (*flowgraphs*) en connectant graphiquement des blocs de traitement dans l'interface GNU Radio Companion (GRC). Chaque diagramme génère automatiquement le code Python correspondant, exécutable en ligne de commande de manière indépendante.

GNUR Radio permet de mettre à disposition de manière simple et utilisable des outils puissants du traitement du signal.

Son installation sous Linux Ubuntu/Debian est simple : `sudo apt-get install gnuradio gr-osmosdr`

6.2 - La chaîne de traitement GNU Radio

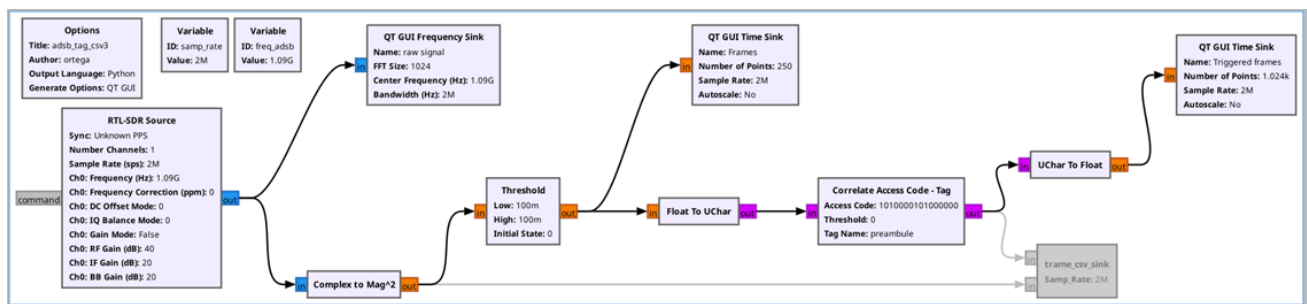


Figure 8 : Flowchart de la réception du signal sous GNU Radio Companion

La chaîne de traitement ADS-B dans GNU Radio comprend les étapes suivantes :

- Variables : `smp_rate` : le taux d'échantillonnage : $2 \cdot 10^6$
- Variables : `freq_adsb` : fréquence de la porteuse ADSB : $1090 \cdot 10^6$

Étape 1 - Source SDR (bloc **osmocom Source**) :

Fréquence centrale : `freq_adsb`
 Taux d'échantillonnage (`smp_rate`) : `smp_rate`
 Gain RF : 20-40 dB (à ajuster selon la configuration)
 Gain IF : 20 dB
 Gain BB : 20 dB

Étape 1bis - Affichage brut du signal reçu (bloc **QT GUI Frequency Sink**) :

On affiche le signal brut.

FFT Size 1024
 Center Frequency : `freq_adsb`
 Bandwidth : 2MHz

Étape 2 - Calcul de l'amplitude (bloc **Complex to Mag²**) :

Transforme le signal complexe I+jQ en amplitude instantanée
 C'est l'enveloppe du signal, qui révèle les impulsions PPM.

Étape 3 - Seuillage (bloc **Threshold**) :

Compare chaque échantillon à un seuil (typiquement 100 pour un niveau normalisé) et produit un signal binaire : 1 si l'amplitude est dans l'intervalle, 0 sinon. Cet intervalle doit être réglé expérimentalement selon le niveau de bruit ambiant. Cela permet de filtrer et d'extraire les bits d'information du bruit.

Étape 3bis - Affichage brut des trames reçues (bloc **QT GUI Time Sink**) :

Number of points 250 (on affiche 250 bits)
 Sample Rate : `smp_rate`

Étape 4 - Conversion de type (**Float to Uchar**) :

Conversion des flottants en caractères non signés pour le bloc de corrélation suivant.

Étape 5 - Corrélation avec le préambule (**Correlate Access Code - Tag**) :

Ce bloc central recherche dans le flux binaire la séquence fixe du préambule ADS-B : **10100000 01000000** (en représentation binaire sur 2 échantillons/bit : **1010000001000000...**)

Lorsque la séquence est reconnue, il attache un **tag** nommé « preamble» à la position correspondante du flux, signalant le début d'une trame.

Access Code : 1010000101000000

Treshold : 0

Tag Name : preamble

Étape 6 - Conversion de type (Uchar to Float) :

Conversion des caractères non signés en flottants pour le bloc d'affichage suivant.

Étape 7 - Visualisation (QT GUI Time Sink) :

Affiche en temps réel le signal après seuillage, avec un déclenchement synchronisé sur les tags «burst». L'étudiant peut observer visuellement la structure de la trame (préambule, champs DF/CA/ICAO, données).

Number of points 1024 (on affiche 1024 bits)

Sample Rate : samp_rate

Sample Rate : samp_rate

Trigger / Trigger Tag Keu : « Preamble »

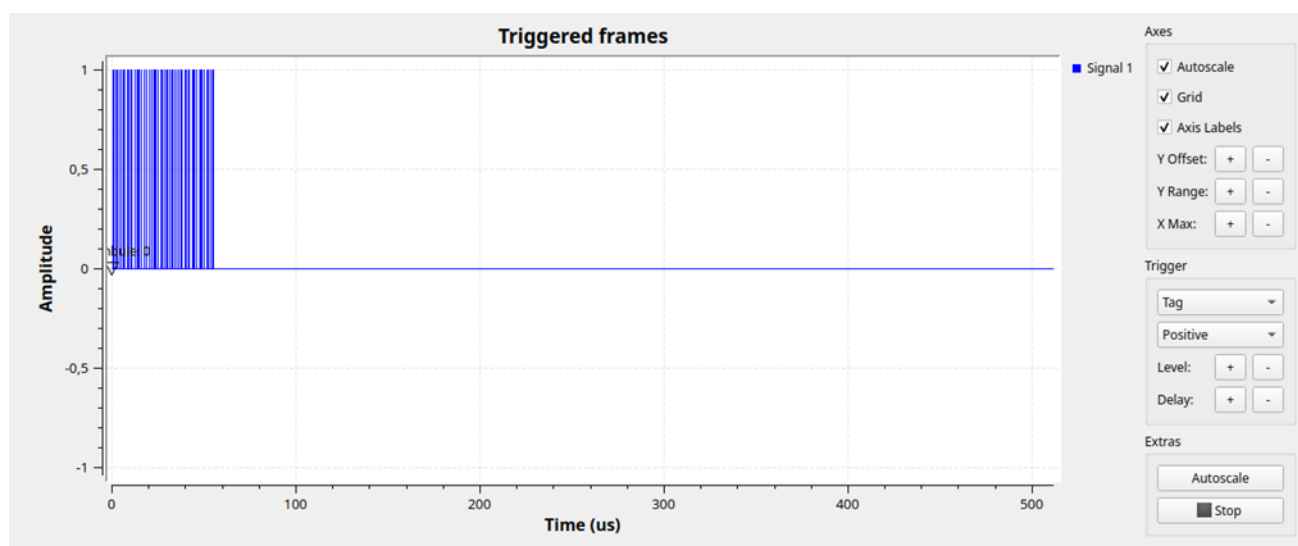


Figure 9 : Affichage des trames ADS B sous GNU Radio

6.3 - Réglage du gain et du seuil

Le réglage du gain est une étape empirique importante pour les étudiants : **trop peu de gain** → signal trop faible, peu de trames détectées ; **trop de gain** → saturation de l'ADC, distorsion, fausses détections. La procédure recommandée est :

- Démarrer GNU Radio avec le gain RF à 0.
- Observer le niveau de bruit de fond sur le QT GUI Time Sink.
- Augmenter progressivement le gain RF par pas de 10 dB jusqu'à observer des impulsions clairement au-dessus du bruit.
- Ajuster le seuil du bloc Threshold à environ 2-3 fois le niveau de bruit moyen.
- Vérifier que les préambules sont bien détectés dans l'affichage.

6.4 - Du signal reçu au décodage de la trame en Python

Les fichiers binaires enregistrés par GNU Radio sont ensuite traités par un programme Python dans le bloc `trame_csv_sink` (grisé dans le flowchart ci-dessus). Ce code spécifique peut être fourni aux étudiants ou faire l'objet d'un mini-projet.

Ce code spécialement développé :

- Surveille les tags `preamble` ;
- capture les échantillons suivant chaque tag,
- décode la modulation PPM du Mode S (1 bit = 1 µs ; impulsion dans la première demi-microseconde = 1, dans la deuxième = 0) ;
- lit les 112 bits de chaque trame enregistrée ;
- extrait les champs DF, CA, ICAO, TC selon la structure du tableau §2.2 ;
- vérifie le CRC-24 et ajoute `crc_ko` en cas d'erreur, `crc_ok` si la trame est valide et donc exploitable ;
- selon le Type Code et si le CRC est correct, converti la trame binaire en hexadécimal et affiche l'identification ICAO en hexadécimal ;
- stocke le résultat dans un fichier a format csv avec un horodatage.

```
horodatage;binaire;hexadecimal;df;icao;crc
20260705_114515;01010101010100101...101100100010010111;;10;;crc_ko
20260705_114515;10001101011100111...010100101110010111;8D7380C3EA25385D15
3F8C5D4B97;17;7380C3;crc_ok
20260705_114515;01011101011100101...010110100101001110;;11;;crc_ko
20260705_114516;10101001010100100...100011101100101001;;21;;crc_ko
20260705_114516;10101011110110100...011000101110010001;;21;;crc_ko
```

Figure 10 : Extrait du fichier csv de trames généré

7 - Mesure de la qualité de réception : le comptage d'aéronefs

7.1 - Principe de la métrique

L'idée centrale de ce TP est d'utiliser le nombre d'aéronefs ICAO distincts détectés sur une fenêtre de temps fixe comme indicateur de performance de la chaîne de réception. Cette métrique présente plusieurs avantages pédagogiques :

- Simple à mesurer : un programme Python comptant les adresses ICAO uniques suffit.
- Objective : elle intègre toute la chaîne (antenne, placement, gain, seuil, décodage).
- Reproductible : en testant les antennes dans les mêmes conditions de trafic (même créneau horaire, même durée), la comparaison est équitable.
- Motivante : les étudiants « voient » directement l'impact de leur réalisation d'antenne.

7.2 - Protocole de mesure

Il convient de fixer des conditions de mesure explicites pour tous les étudiants :

- Durée de mesure : 20 minutes minimum par antenne (pour obtenir une statistique représentative)
- Créneau horaire : 9h-11h ou 14h-16h (trafic commercial dense)
- Position du récepteur : identique pour toutes les antennes testées
- Gain RF GNU Radio : fixe (même valeur pour toutes les antennes)
- Seuil Threshold : fixe

7.3 - Evaluation

Une note peut être élaborée à partir des résultats des mesures selon les critères établis et annoncés par l'enseignant. L'évaluation sommative permettra de prendre en compte l'ensemble du travail réalisé par l'étudiant et son efficacité concrète.

7.4 - Extension : cartographie des avions détectés

La visualisation sur carte constitue une extension naturelle pour les étudiants avancés. La bibliothèque Python [folium](#) permet de générer une carte HTML interactive :

La comparaison de la carte obtenue avec celle de Flightradar24 au même instant valide le bon fonctionnement du décodage. Les écarts (avions présents sur Flightradar24 mais non détectés) permettent d'identifier les zones d'ombre liées aux obstacles locaux.

Il peut être aussi opportun d'intégrer une partie base de données pour exploiter le code OACI aéronef sur 24 bits et rechercher le numéro de vol, ses aéroports de départs et destination, ...

8 - Aspects cybersécurité

8.1 - Vulnérabilités inhérentes au protocole

L'ADS-B a été conçu pour la disponibilité et l'interopérabilité, sans considération initiale pour la sécurité. Cette réalité, discutée ouvertement dans la communauté de sécurité depuis les conférences DEFCON et Black Hat, présente plusieurs vulnérabilités :

- Absence d'authentification : n'importe quel émetteur SDR peut envoyer des trames ADS-B valides avec une adresse ICAO et une position arbitraire. Il n'existe aucun mécanisme cryptographique pour vérifier que le message provient bien de l'aéronef qu'il prétend être.
- Absence de chiffrement : toutes les données sont en clair, lisibles par quiconque dispose d'un récepteur. Les informations diffusées (position, vitesse, indicatif) peuvent révéler des informations sensibles sur certains vols.

Ces deux faiblesses du protocole ouvrent de nombreuses possibilités d'attaque :

- *Ghost aircraft injection* (injection de faux avions) : créer des trafics fantômes qui apparaissent sur les écrans de contrôle. Présenté à DEFCON 20 par Andrei Costin et Augustin Francillon [7]
- *Aircraft spoofing* (usurpation d'identité) : émettre avec l'adresse ICAO d'un vrai avion pour induire en erreur les systèmes de surveillance. [8],[9]
- *Replay attack* : rejouer des trames enregistrées précédemment.

- *DoS par saturation* : inonder la fréquence 1090 MHz de trames, saturant les récepteurs.

Avertissement légal : toute émission sur la fréquence 1090 MHz sans autorisation est strictement interdite en France par article L. 33-3-1 du Code des Postes et Communications Électroniques. Ce TP utilise exclusivement le mode réception passive (les clefs RTL SDR ne font que de la réception).

8.2 - Contre-mesures et mécanismes de détection

Plusieurs approches sont à l'étude ou déjà déployées pour sécuriser l'ADS-B :

- *MLAT (Multilateration)* : en combinant les temps d'arrivée du même signal sur plusieurs récepteurs géographiquement distants, il est possible de recalculer indépendamment la position de l'émetteur. Si la position calculée par MLAT ne correspond pas à la position déclarée dans le message, le message est suspect. [10]
- Détection d'anomalies par apprentissage machine : des travaux récents appliquent des réseaux de neurones récurrents (LSTM) pour détecter les séquences de messages incohérentes physiquement (vitesse impossible, trajectoire erratique).
- ADS-B version 2 : la version 2 du standard introduit des indicateurs d'intégrité (NIC, NAC, SIL) plus robustes, mais ne résout pas fondamentalement l'absence d'authentification.

9 - En 2026 : entretien avec un contrôleur aérien

En situation opérationnelle normale, ADS-B améliore-t-il votre travail de contrôleur aérien au quotidien ?

Le territoire français métropolitain (et plus largement le territoire européen) est assez bien couvert par de nombreux radars secondaires. Il persiste quelques zones blanches, notamment en zone montagneuse, mais les données radars sont celles privilégiées pour le contrôle aérien français (notamment pour des raisons d'intégrité). Ainsi, je travaillais avant dans un centre en route et je ne crois pas que les données ADS-B y étaient exploitées. Je crois cependant que cette technologie est aujourd'hui plus largement exploitée en Outre-Mer, où les radars sont moins nombreux et où la maintenance est plus compliquée. Les données ADS B permettent de travailler plus efficacement là où le contrôle aux procédures était la norme, et où le contrôle radar était l'exception.

Je crois aussi que des projets d'installation de Multilatération utilisant l'ADS-B sont en cours sur des grandes approches telles que l'aéroport Marseille, où le radar sol primaire ne suffit souvent pas à donner une image précise de la situation au sol. Ce serait alors un grand plus pour les contrôleurs aériens qui y travaillent.

Comment évaluez-vous la précision et la fiabilité des données ADS-B (position, vitesse, altitude) par rapport aux radars secondaires classiques ? Quels sont les avantages et les limites que vous observez ?

Les données ADS-B sont généralement considérées comme plus précises que les données radars, car provenant directement des systèmes de navigation bord. Et ces données sont également mises à jour plus régulièrement. Cependant, sans infrastructure sol pour vérifier l'information, c'est par sa fiabilité que le système ADS-B est limité. On est en effet dépendant de la qualité des données fournies, qui peut varier suivant des dysfonctionnements systèmes, des interférences, ... C'est pour ça que le système ADS-B n'est à ma connaissance pas utilisé comme seule source d'information et qu'il est redondé par d'autres infrastructures sol.

Bref, système précis, efficace et beaucoup plus économique à entretenir, mais qui n'est pas totalement fiable s'il n'est pas redondé par d'autres moyens de détection

Les pilotes remontent des problématiques de guerre électronique affectant la réception des signaux GNSS, avez-vous connaissance d'incidents similaires avec ADS-B ?

Il me semble qu'un vol en provenance de Beyrouth et à destination de Marseille avait été victime de leurrage et de brouillage GNSS à son départ (zone de conflits). Cela avait entraîné des perturbations sur la suite de son vol, notamment des alarmes injustifiées à bord. C'est probablement le cas de nombreux autres vols, et cela illustre le risque quant à la fiabilité de cet outil si utilisé seul.

Références :

[1]: Utilisation des "Tags" pour synchroniser un flux de données ; Application au décodage des signaux ADS-B. Thomas Lavarenne, <https://gnuradio-fr-18.sciencesconf.org/214676.html>

[2]: Document video : " PROGRESS IN AIR TRAFFIC CONTROL " 1973 U.S. AIR FORCE ATC EDUCATIONAL FILM XD94765, https://youtu.be/OTmwe3Vf_Y0?si=PlFZvfAoDS6PECOe

[3]: OpenSky <https://opensky-network.org/data/aircraft>

[4]: ICAO Technical Provisions for Mode S Services and Extended Squitter,
<https://www.icao.int/MID/Documents/2019/MICA/MICA-MID%20-%20WP%2002%20-%20Mode%20S%20Surveillance%20Principle.pdf>

[5]: The 1090MHz Riddle. An open-access book about decoding Mode-S and ADS-B data by Junzi Sun, <http://mode-s.org/decode/>

[6]: Formal analysis of the compact position reporting algorithm, Aaron Dutle, Laura Titolo, Mariano M. Moscato, César A. Muñoz, Gregory Anderson, Francois Bobot,
<https://cea.hal.science/cea-04491533v1>

[7]: Andrei Costin and Aurélien Francillon. "Ghost is in the Air(traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices". In: Black Hat USA. July 2012, pp. 1-12.

[8]: ADS-B spoofing attack detection method based on LSTM Jing Wang, Yunkai Zou, Jianli Ding

[9]: Detecting ADS-B spoofing attacks - using collected and simulated data Joakim Thorn, Alex Wahlgren

[10]: Non-Radar Surveillance ADS-B/MLAT/WAM Products -THALES,
https://www.icao.int/SAM/Documents/2017-ADSB/14%20THALES_%20NRS_Products_SEP_2017.pdf