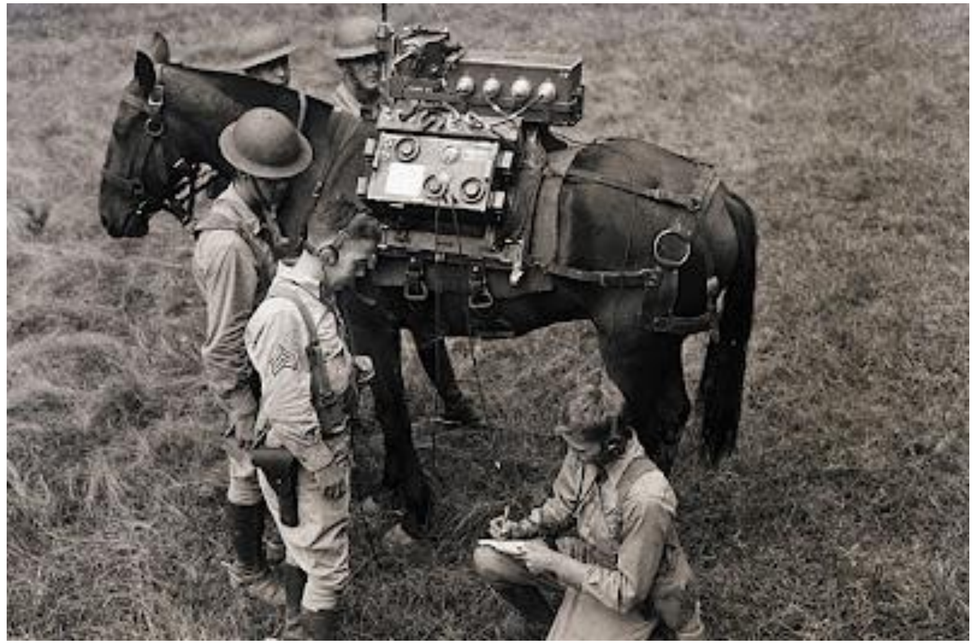
Introducción ás plataformas SDR e o seu emprego na industria

Iago Gómez. *igomez@gradiant.org*

www.gradiant.org

Índice

- Introdución SDR
- Usos amateurs (RTL-SDR)
- Usos profesionais



Introdución SDR

Definición SDR

Joseph Mitola → No seu traballo sobre radio cognitiva (**1991**), acuñaba o termo **SDR**:

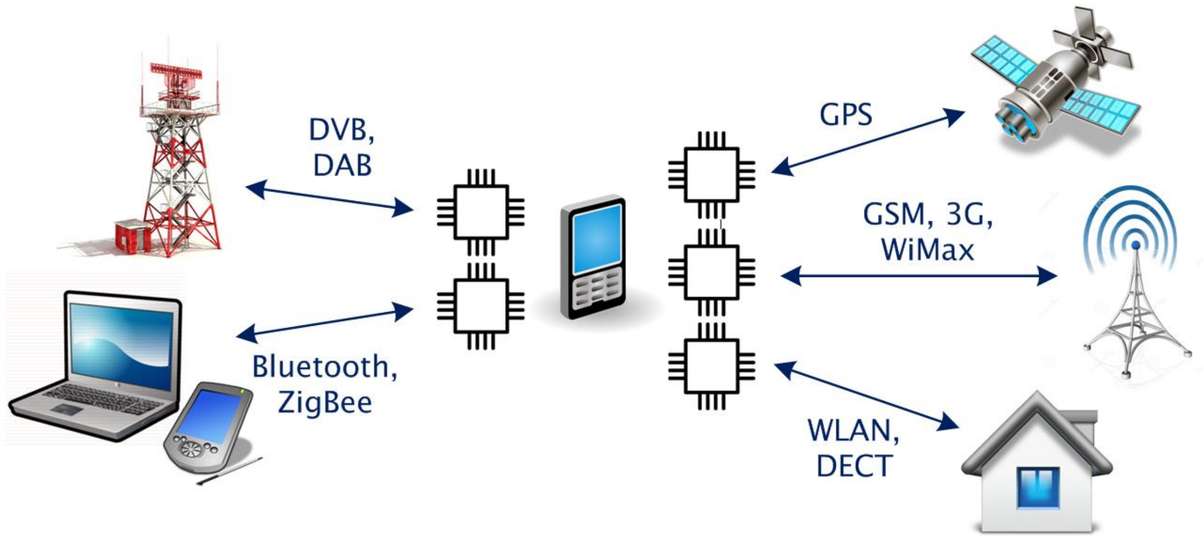
“Radios reprogramables ou reconfigurables que, sen modificar físicamente o seu hardware, poden desempeñar distintas funcións en diferentes instantes de tempo.

A selección dunha ou outra funcionalidade pódese realizar mediante software.”

Clasificación Radios Software

Wireless Innovation Forum (SDR Forum):

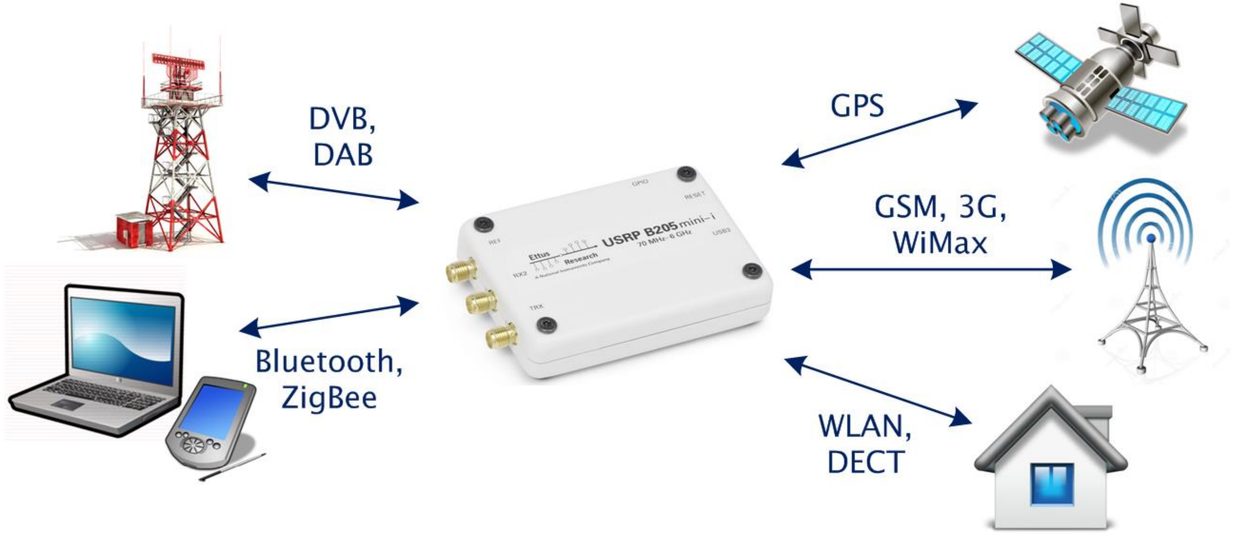
Tier	Nombre	Siglas
0	Hardware Radio	HR
1	Software Controlled Radio	SCR
2	**Software Defined Radio**	**SDR**
3	Ideal Software Radio	ISR
4	Ultimate Software Radio	USR



Clasificación Radios Software

Wireless Innovation Forum (SDR Forum):

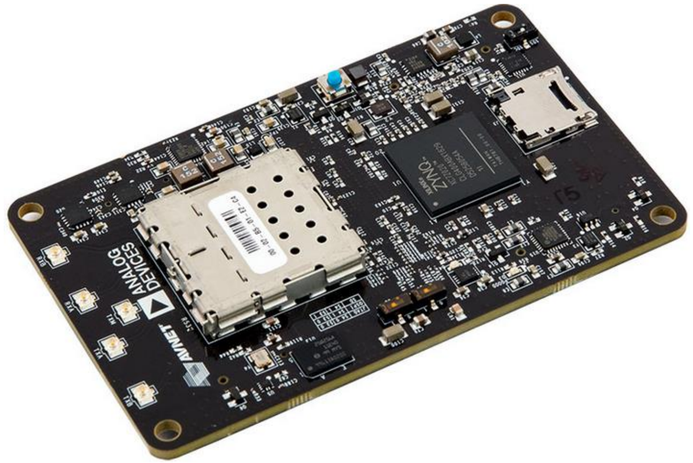
Tier	Nombre	Siglas
0	Hardware Radio	HR
1	Software Controlled Radio	SCR
2	**Software Defined Radio**	**SDR**
3	Ideal Software Radio	ISR
4	Ultimate Software Radio	USR



Plataformas SDR - Uso profesional

Ettus USRP B2xx

~800 €



PicoZed SDR

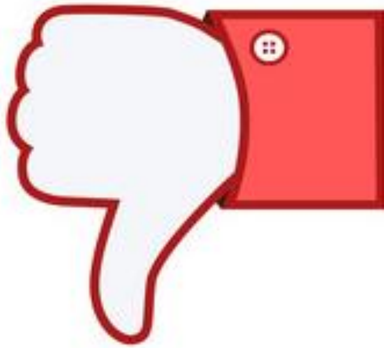
~500 €

Matchstiq

> 7.000 €

SDR - Pros & Cons

- Flexibilidade
- Multifuncionalidade
- Compatibilidade/Actualización
- Portabilidade
- Tempo y custo de desarrollo

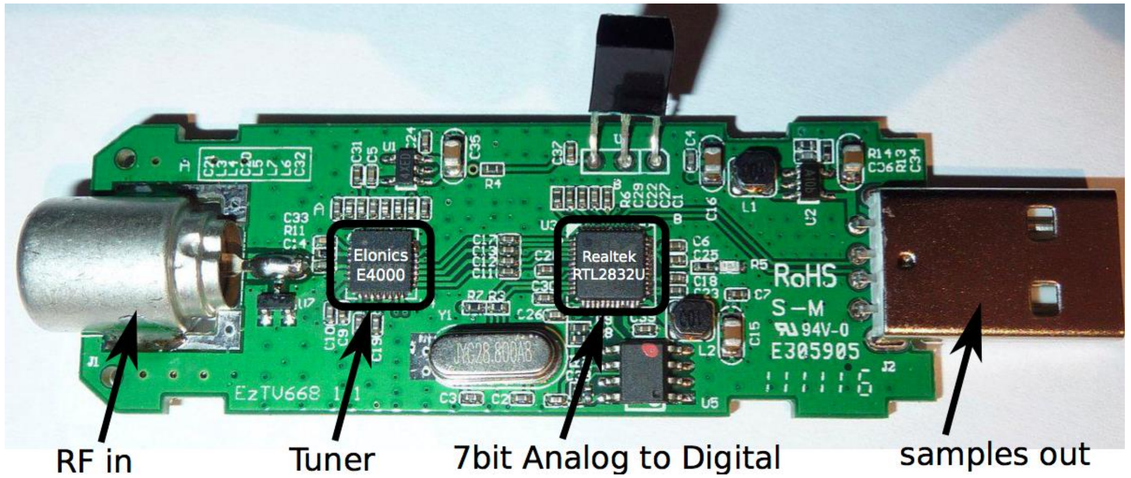


- Custo
- Curva de aprendizaxe media/alta
- Comunidade de desarrolladores amateur pequena
- Moitas veces HW/FW propietario

RTL-SDR

RTL-SDR

Orixinalmente fabricouse un **dongle USB** para a recepción e decodificación do **TDT en Europa**:



Formado principalmente por dous chips:

- **Sintonizador** de 60 a 1700 MHz: E4000.
- **Demodulador DVB-T** COFDM: **RTL**2832U.

Antti Palosaari, no 2011, descubriu que era posible **acceder directamente ás mostras I/Q** do chip RTL2832U, o que permitiría converter este sintonizador de TDT nunha SDR de banda ancha.

Este descubrimento supuxo un **gran avance** no ámbito da **radio amateur**, xa que podíanse conseguir estos dongle USB por apenas 20 $.

RTL-SDR

Dende entón:

- Proliferación do mercado.
- Amplia popularidade.
- Democratización do acceso ó espectro radio.
- Gran número de aplicacións.
- Maior cantidade de **software libre** neste ámbito.
- Aparición de comunidades específicas: www.rtl-sdr.com

Plataformas SDR – Uso amateur

RTL-SDR
~20 €

Pluto SDR
~85 €

LimeSDR mini
~130 €

HackRF One
~250 €

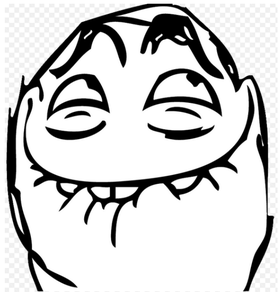
RTL-SDR - Usos

Podes:

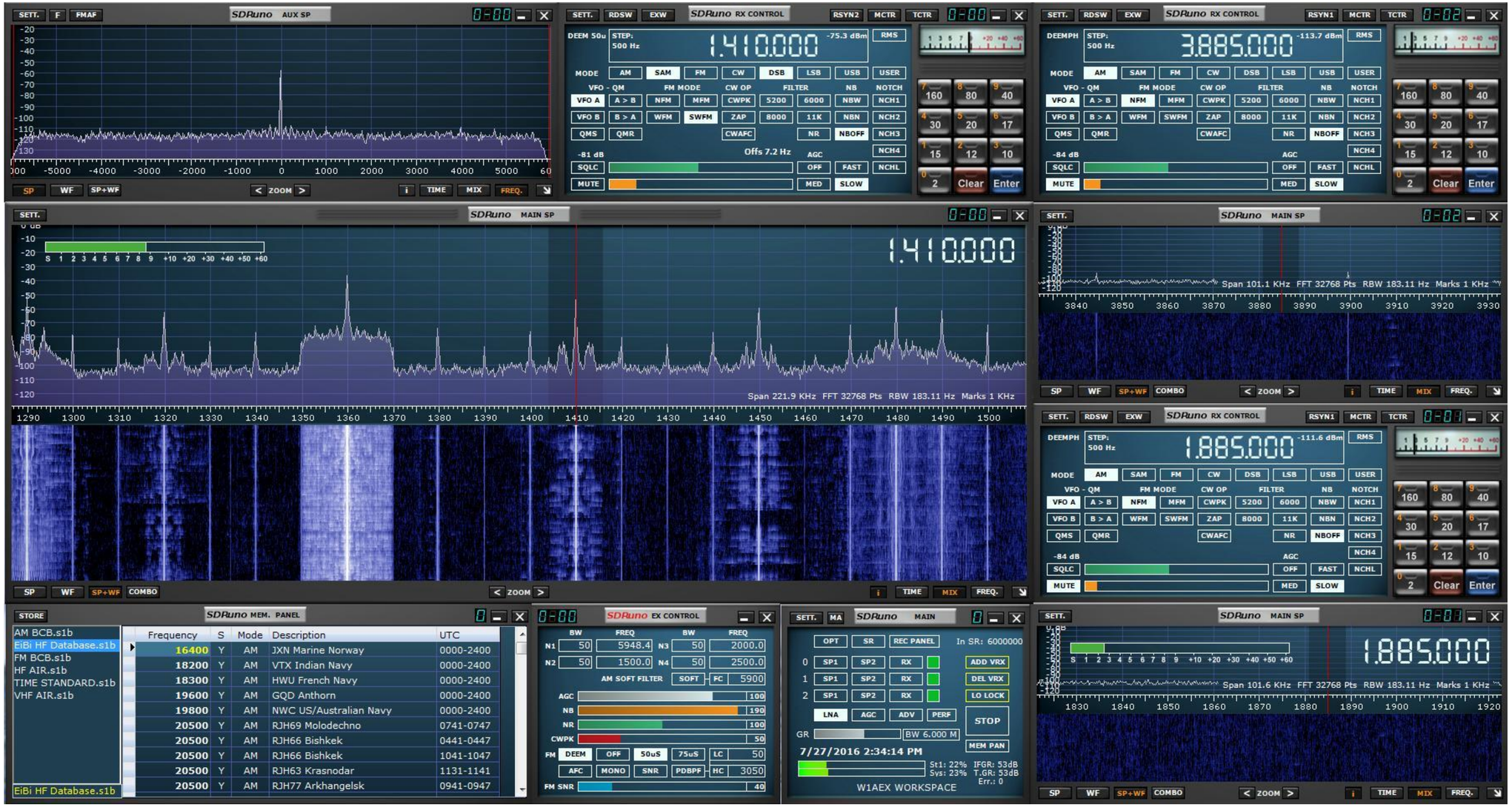
- Analizar o espectro
- Recibir todo tipo de sinais e decodificar protocolos abertos (GPS, radio AM/FM, etc)
- Transmitir en bandas non licenciadas (ISM)
- Aprender (uso educativo): SDR, RF, procesado de sinal, etc.

“Non deberías” trolear:

- Jamming
- Sniffing
- Spoofing
- Replay attacks
- Hijacking
- Reverse engineering
- Transmitir en bandas licenciadas

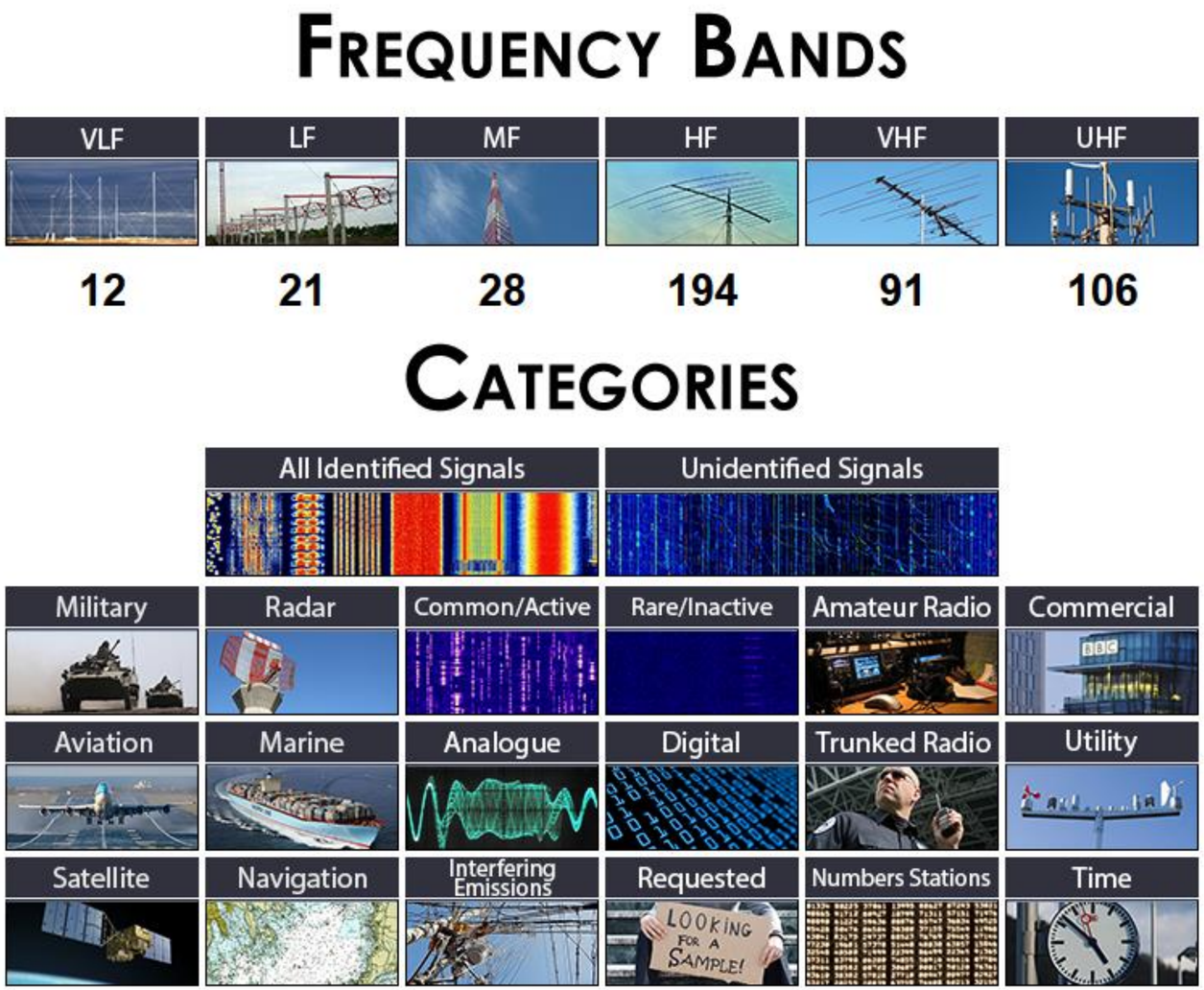


RTL-SDR – Analizador de espectro



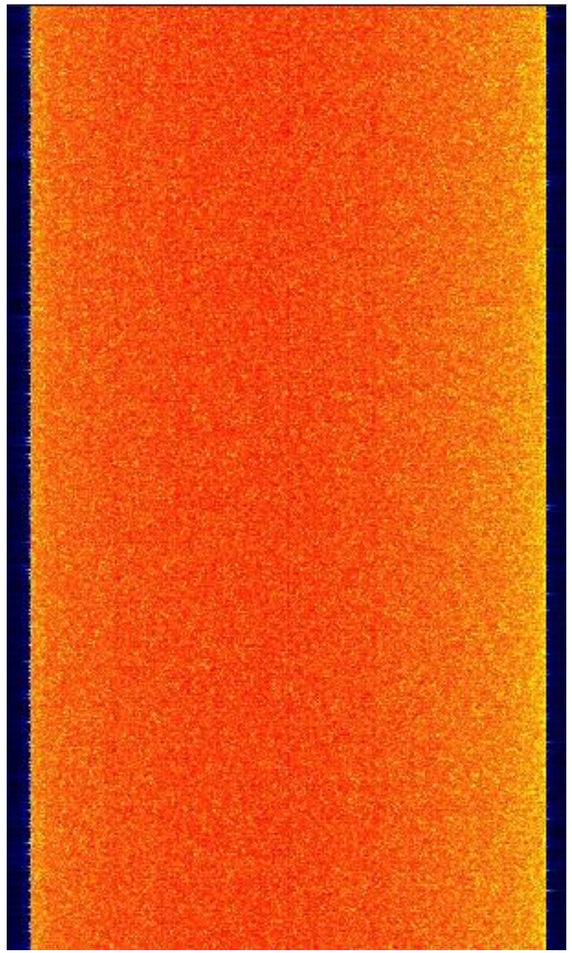
Fonte: SDRuno (OpenSource)

SIGIDWIKI

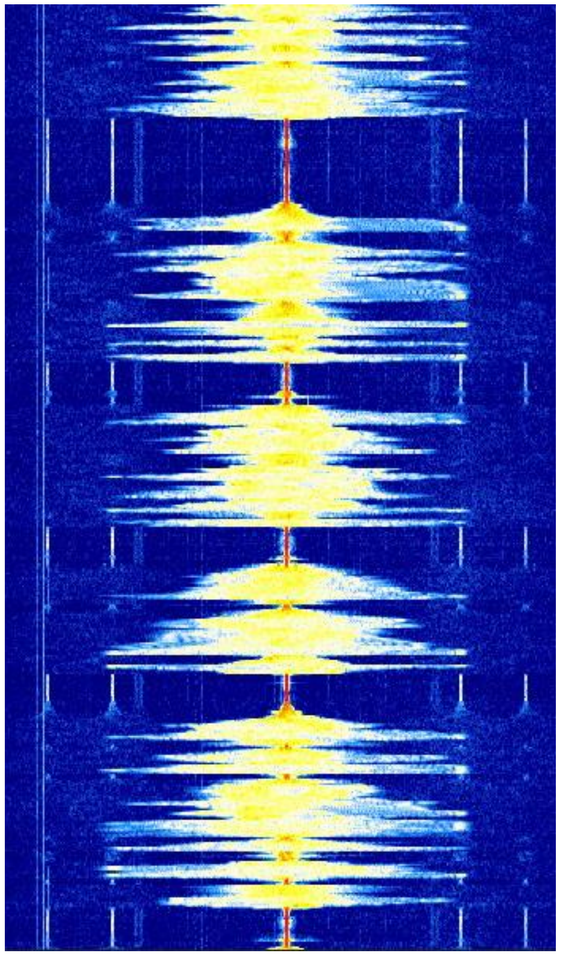


https://www.sigidwiki.com/wiki/Signal_Identification_Guide

RTL-SDR – sigidwiki (sinais identificadas)



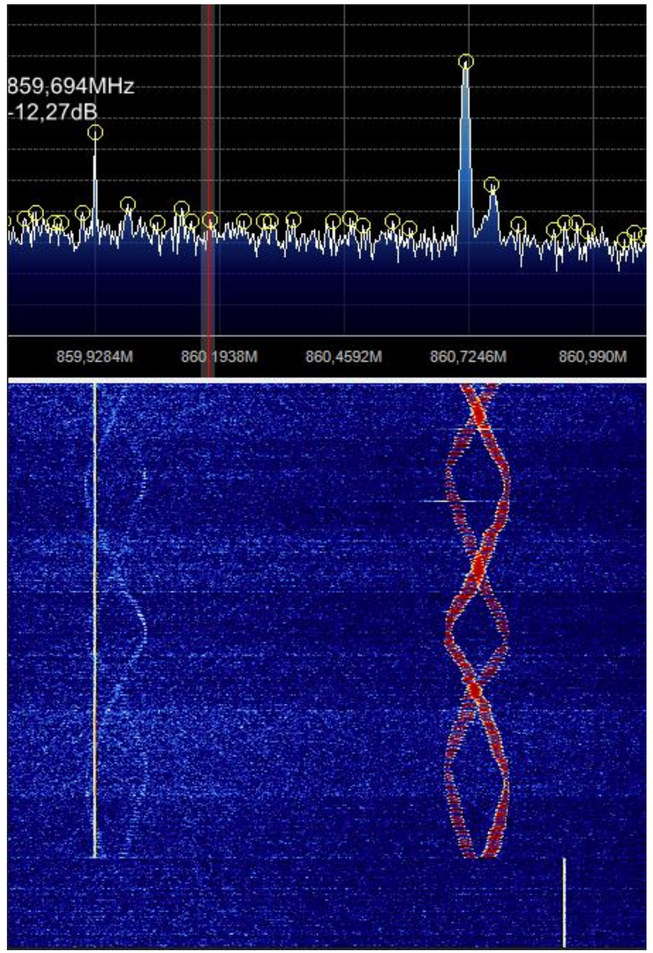
DVB-T



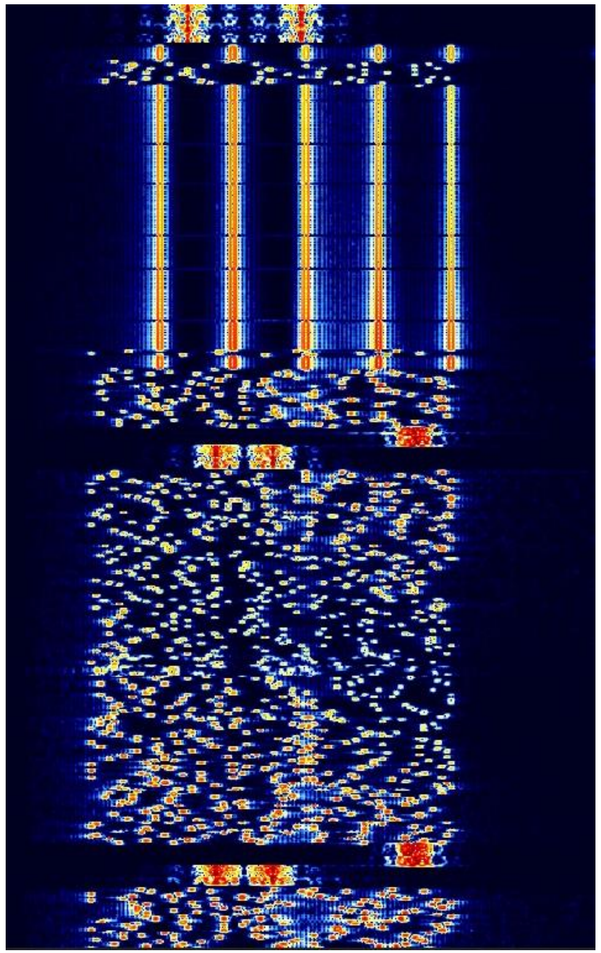
Radio FM

Morse

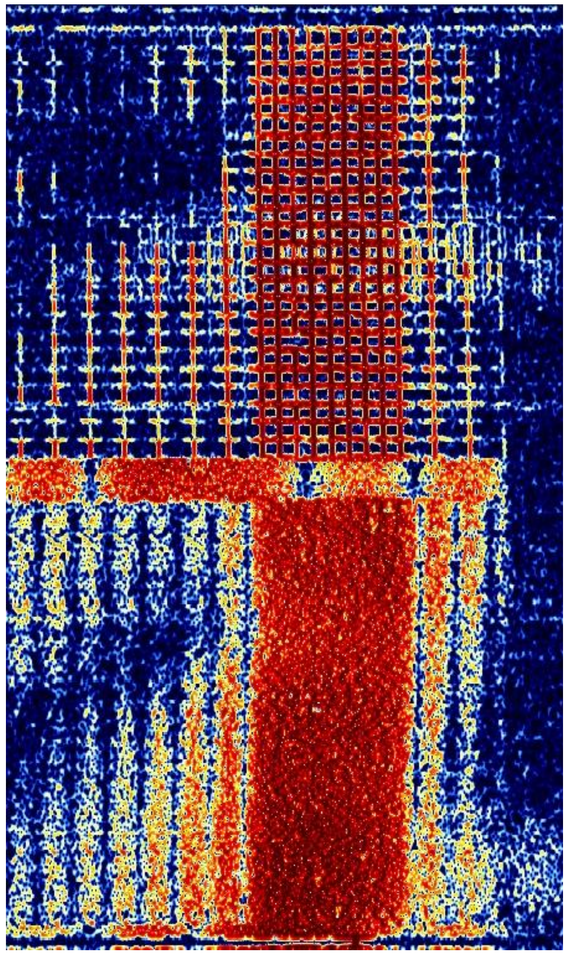
RTL-SDR – sigidwiki (sinais sen identificar)



¿?

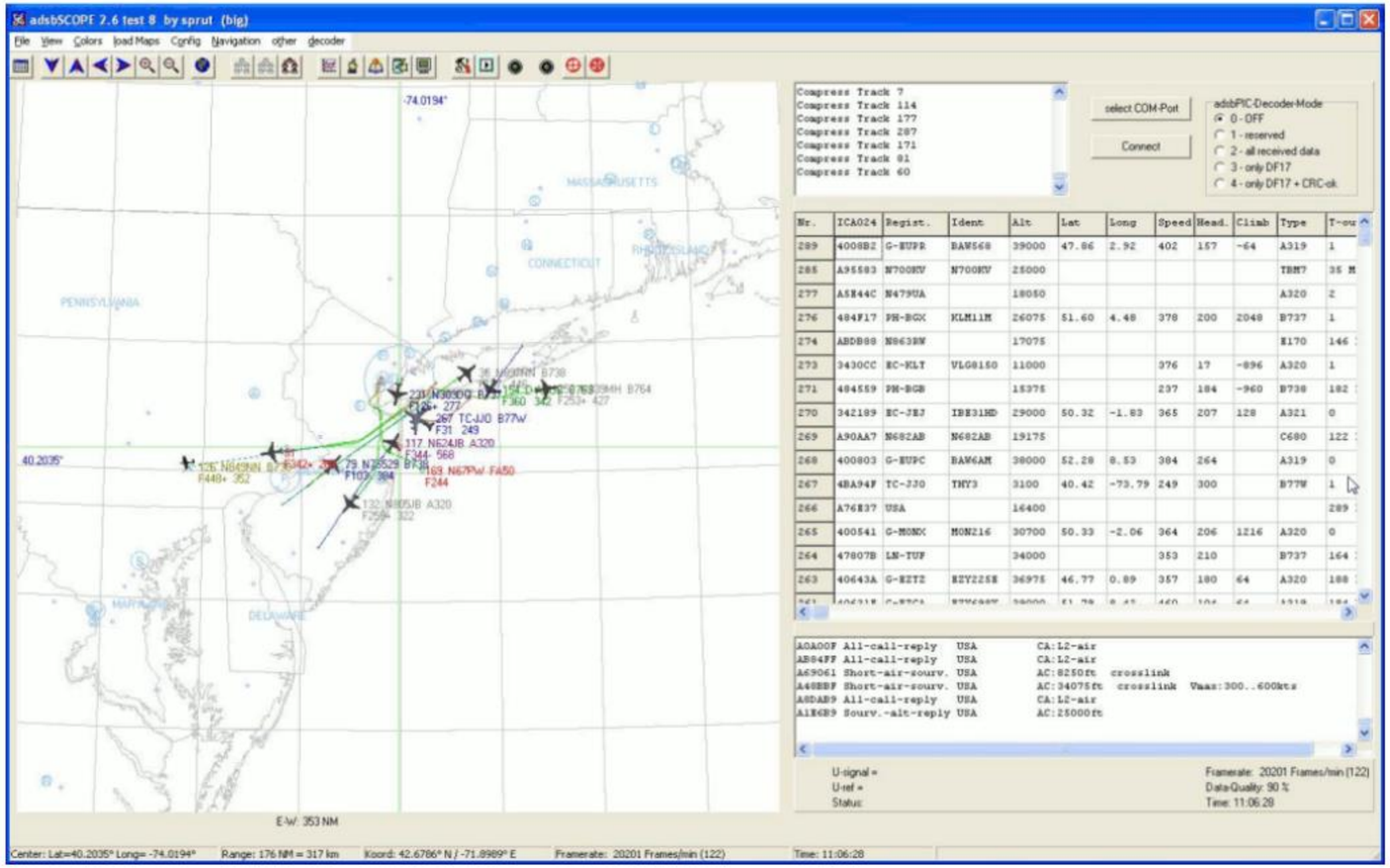


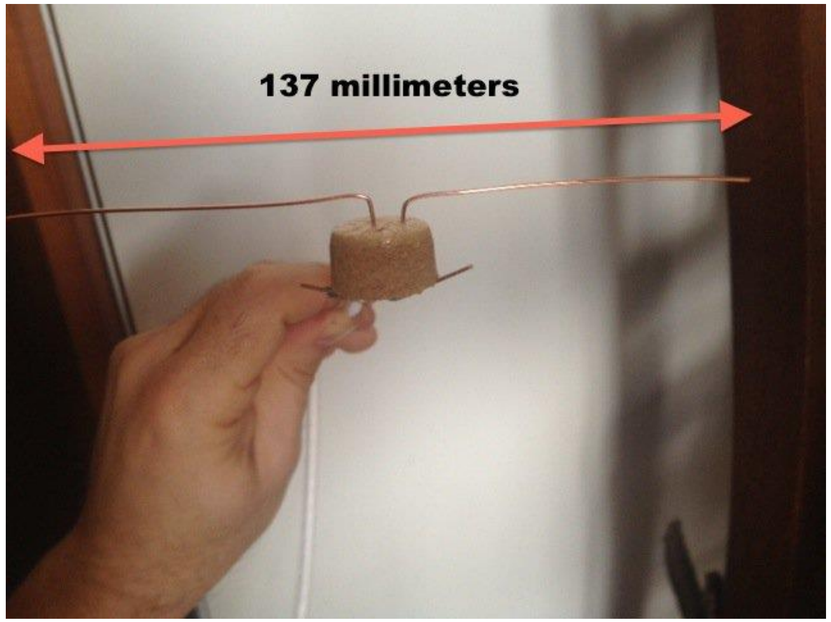
¿?



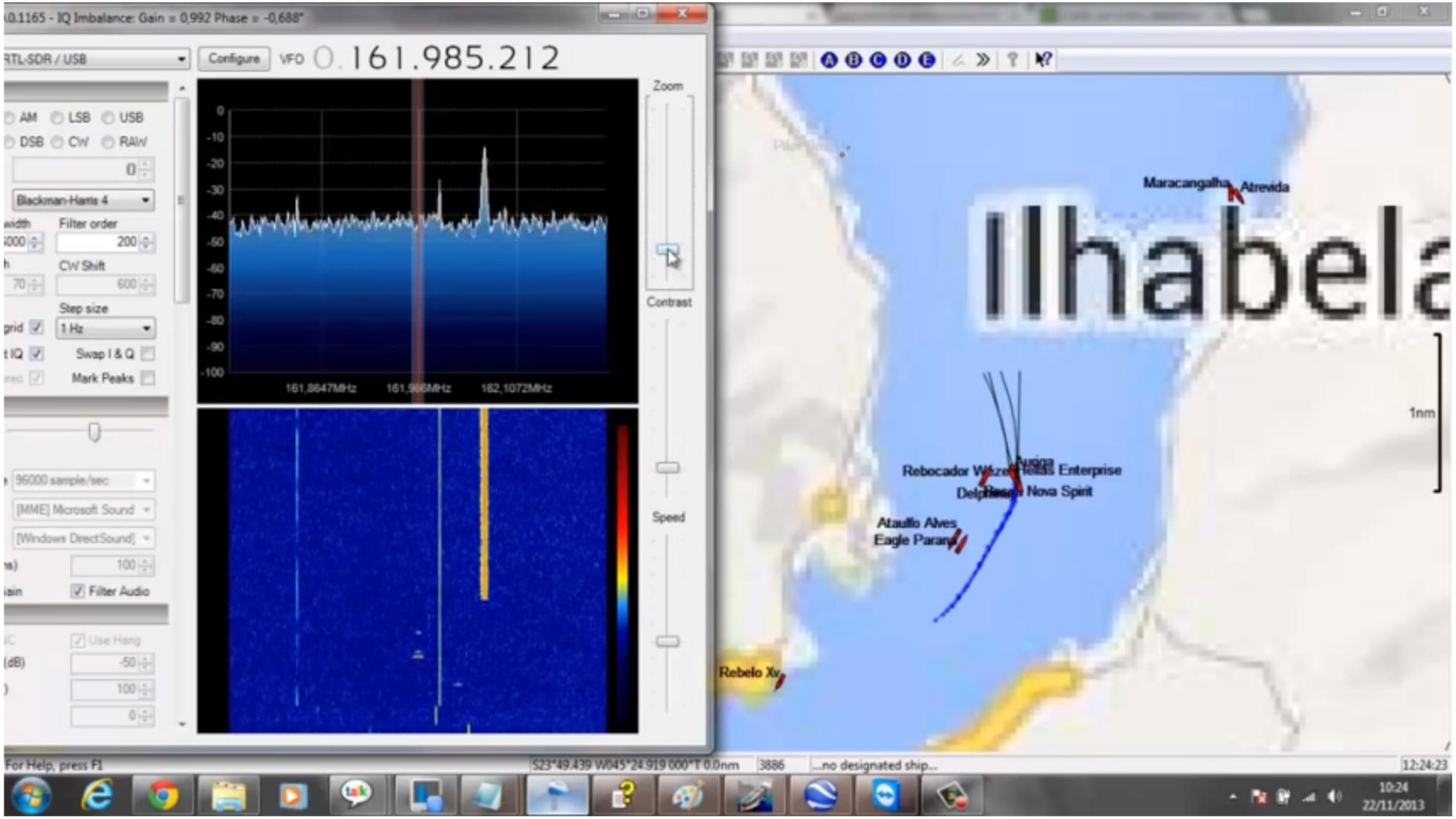
¿?

RTL-SDR – receptor ADS-B (“radar aeronáutico”)



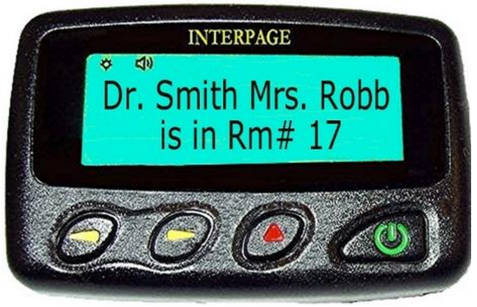


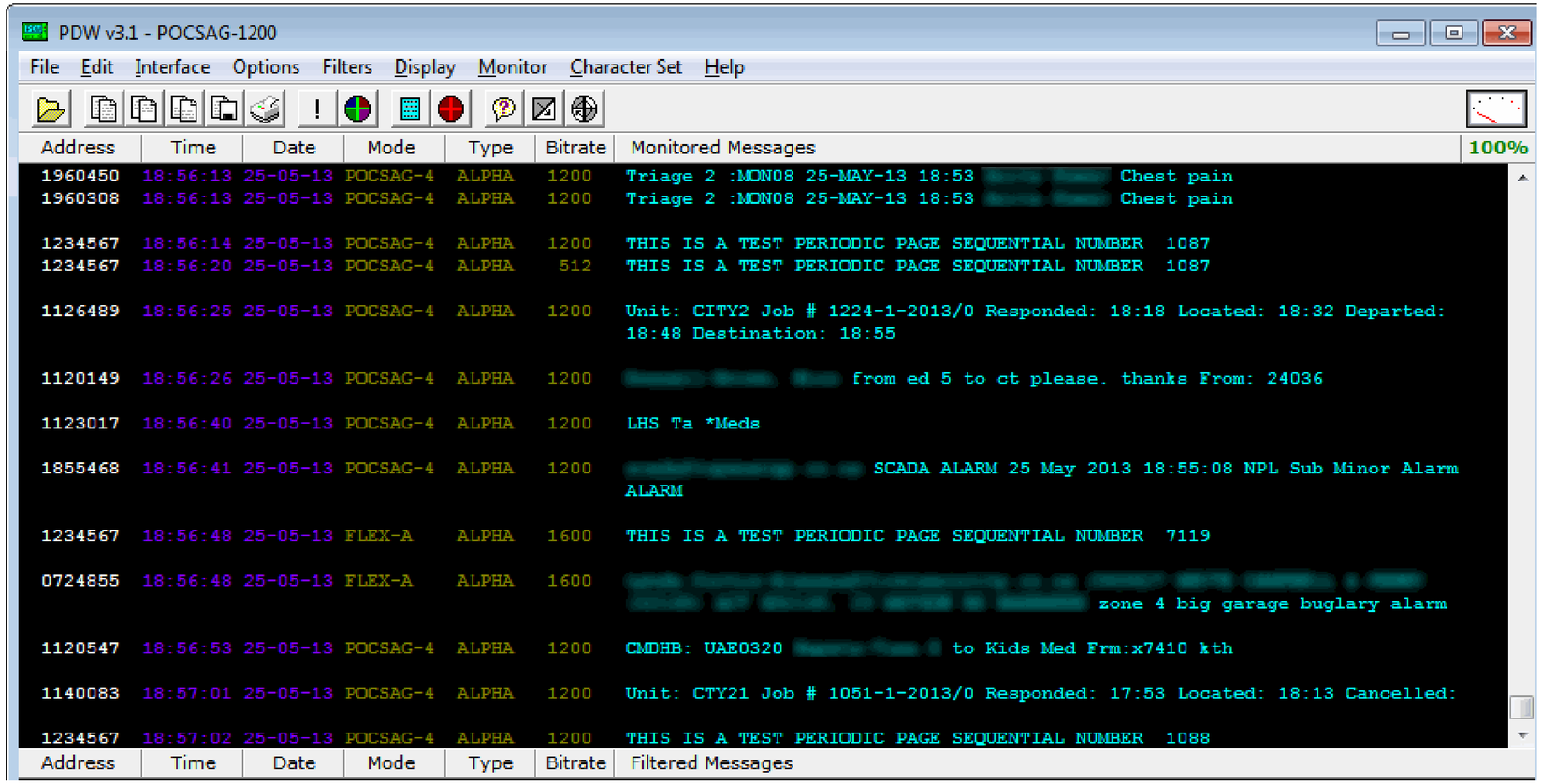
RTL-SDR – receptor AIS (“radar marítimo”)



Exemplos de aplicacións

Sniffing de información de pagers de hospitais, ambulancias, bombeiros:

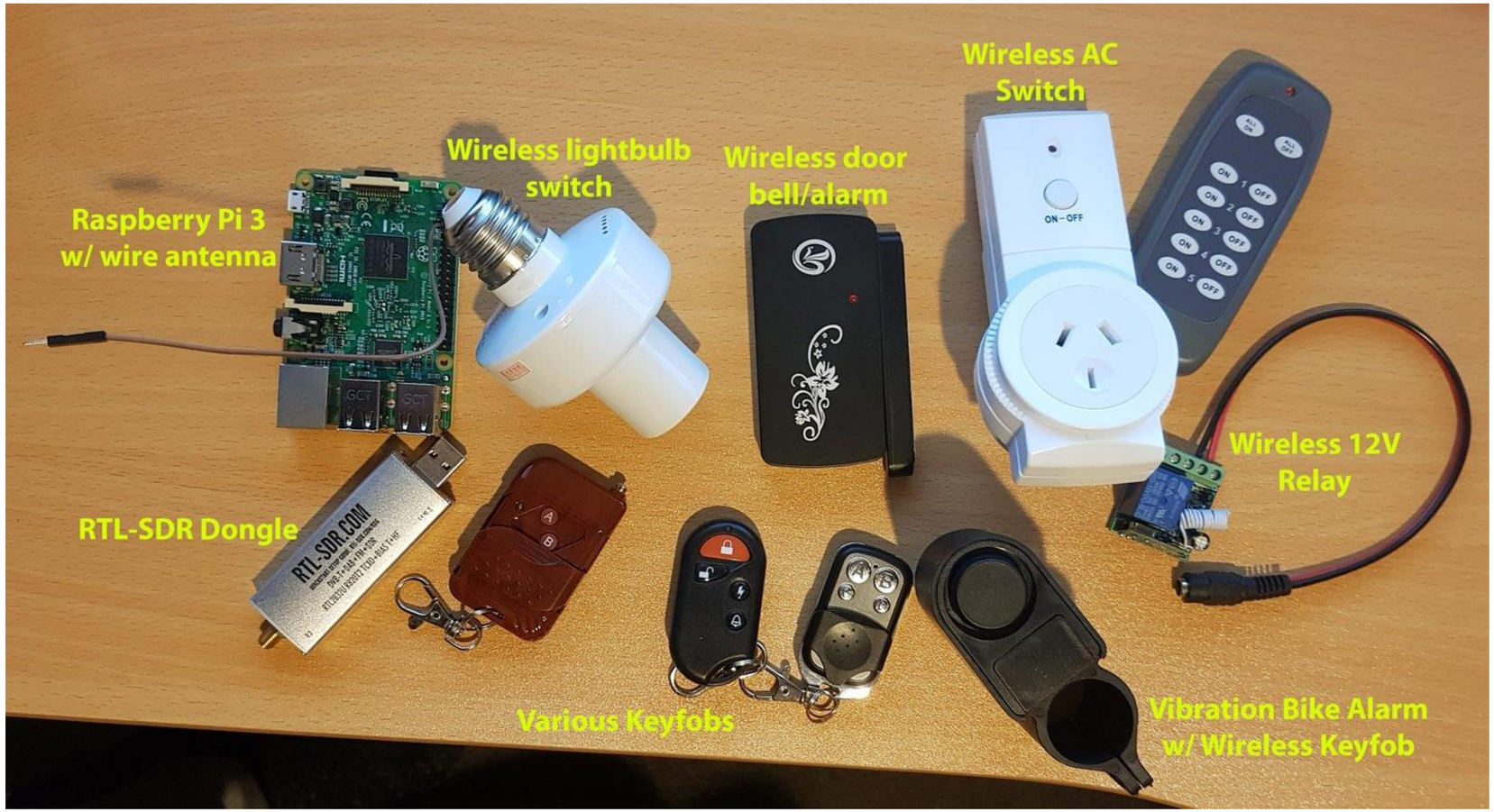




https://www.rtl-sdr.com/exposing-hospital-pager-privacy-breaches/

Exemplos de aplicacións

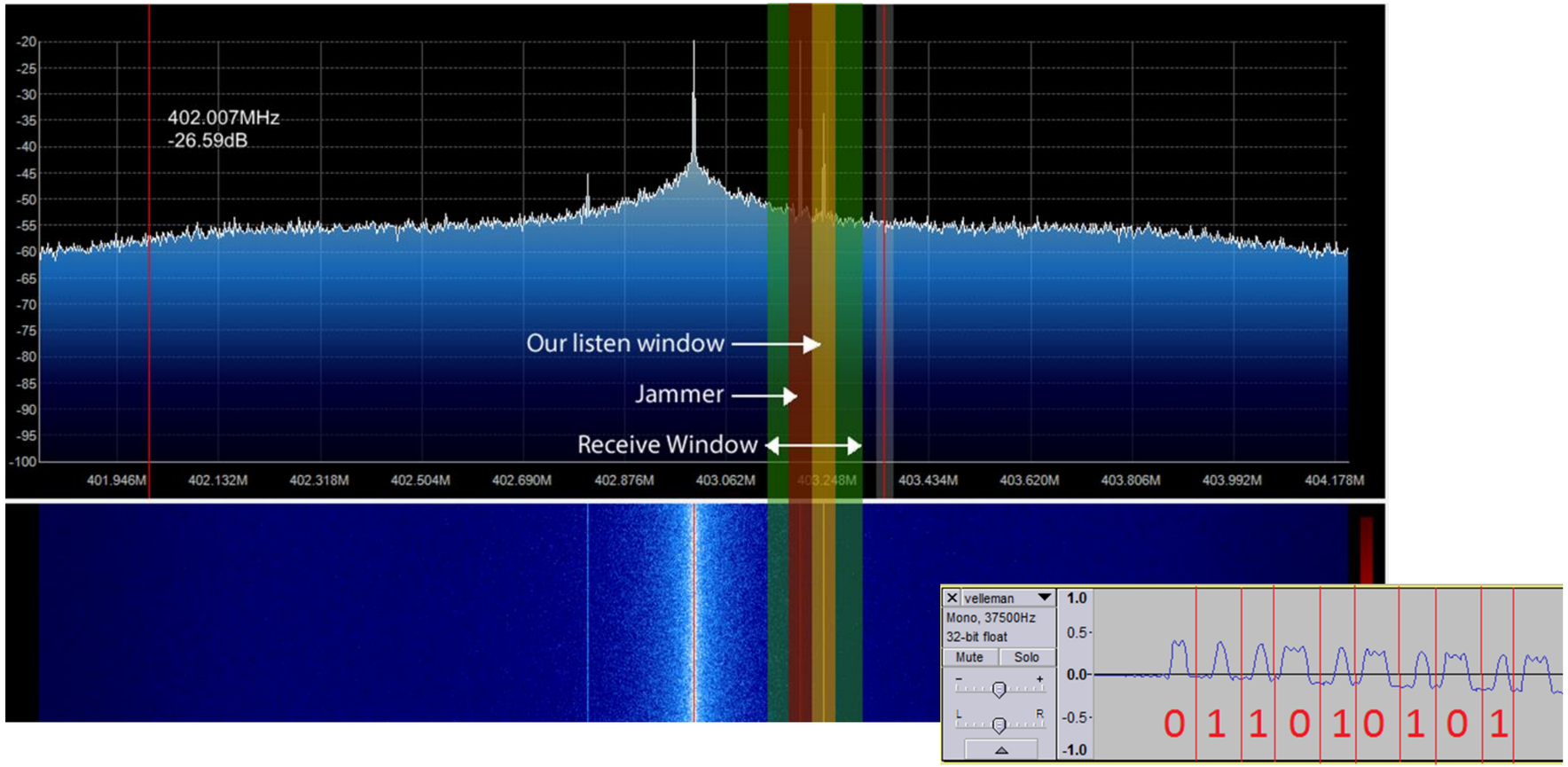
Replay attacks sobre distintos dispositivos inalámbricos:



https://www.rtl-sdr.com/tutorial-replay-attacks-with-an-rtl-sdr-raspberry-pi-and-rpitx/

Exemplos de aplicacións

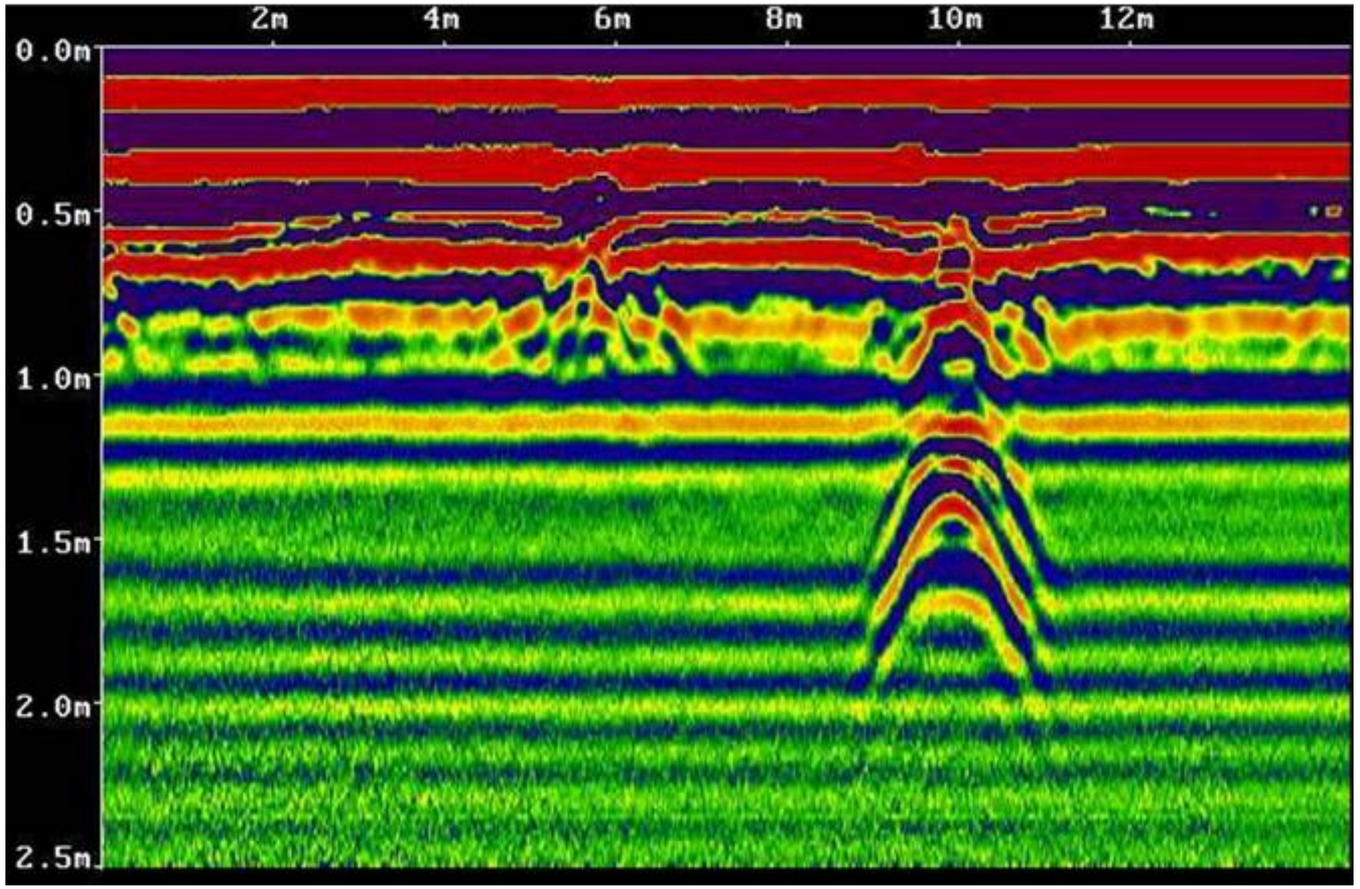
Jamming + Replay attack para abrir coches:



https://andrewmohawk.com/2016/02/05/bypassing-rolling-code-systems/

Thinking outside the box

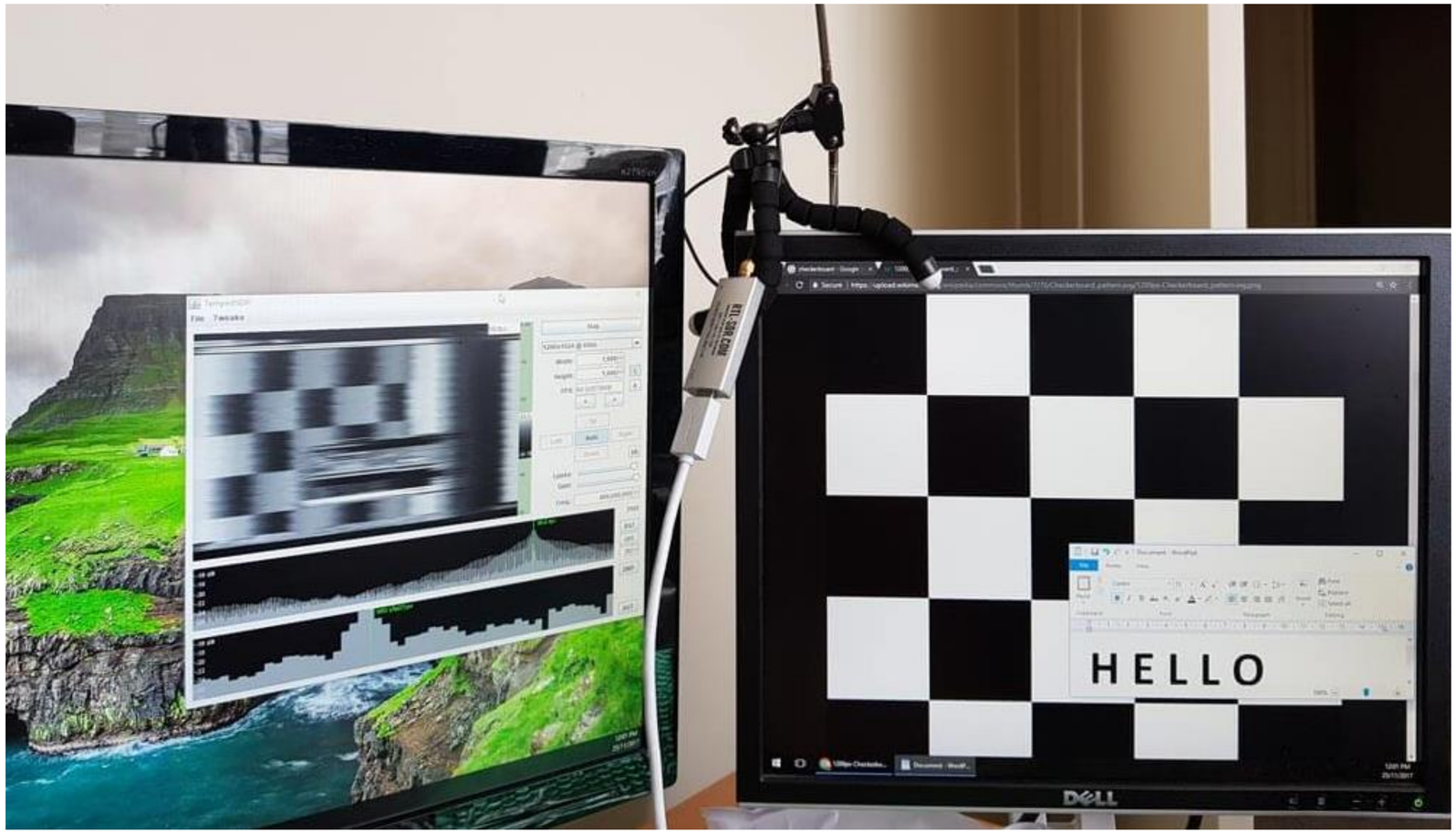
Detección de metais mediante radar de penetración terrestre (GPR):



https://www.rtl-sdr.com/an-rtl-sdr-based-ground-penetrating-radar-metal-detector/

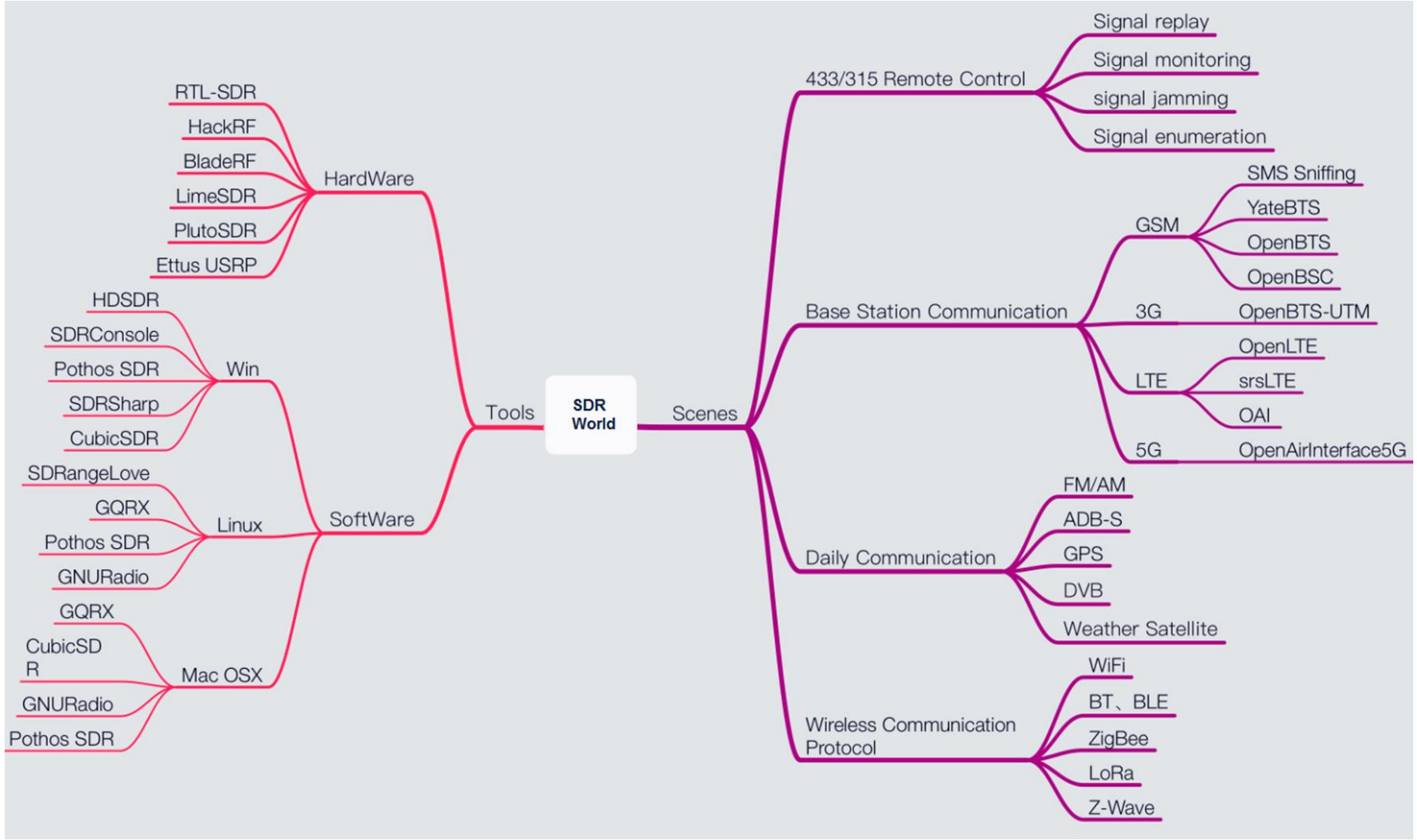
Thinking outside the box

Tempest (eavesdropping) dunha pantalla de ordenador:



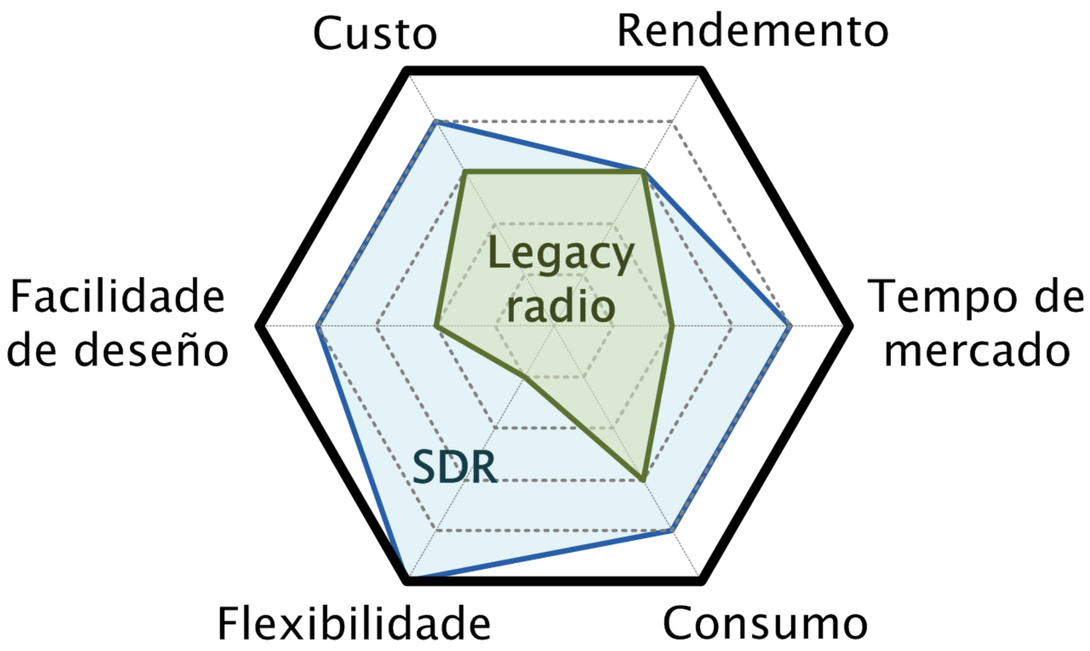
https://www.rtl-sdr.com/tempestsdr-a-sdr-tool-for-eavesdropping-on-computer-screens-via-unintentionally-radiated-rf/

Resumen SDR


SDR World
Tools
HardWare
RTL-SDR
HackRF
BladeRF
LimeSDR
PlutoSDR
Ettus USRP
SoftWare
Win
HDSDR
SDRConsole
Pothos SDR
SDRSharp
CubicSDR
Linux
SDRangeLove
GQRX
Pothos SDR
GNURadio
Mac OSX
GQRX
CubicSD R
GNURadio
Pothos SDR
Scenes
433/315 Remote Control
Signal replay
Signal monitoring
signal jamming
Signal enumeration
Base Station Communication
GSM
SMS Sniffing
YateBTS
OpenBTS
OpenBSC
3G
OpenBTS-UTM
LTE
OpenLTE
srsLTE
OAI
5G
OpenAirInterface5G
Daily Communication
FM/AM
ADB-S
GPS
DVB
Weather Satellite
Wireless Communication Protocol
WiFi
BT、BLE
ZigBee
LoRa
Z-Wave

Usos profesionais

¿Por que SDR?



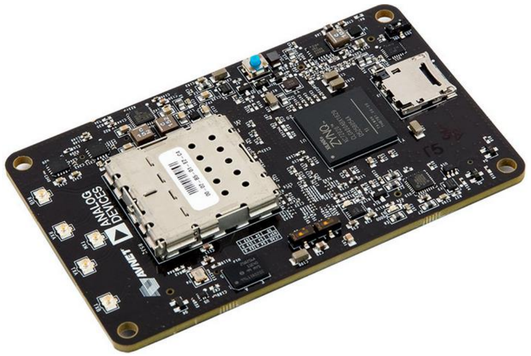
- Aplicacións profesionais (non de consumo, p.e. defensa) => custo e consumo non son críticos
- Produtos con tempos de obsolescencia reducidos (por exemplo telefonía)
- Tempos de desenrolo rápidos => Aprendizaxe
- Prototipos => Funcionalidade fronte a custo/consumo
- I+D => Flexibilidade fronte a custo/consumo

Recursos Gradiant

Ettus USRP B200mini

Ettus USRP N210

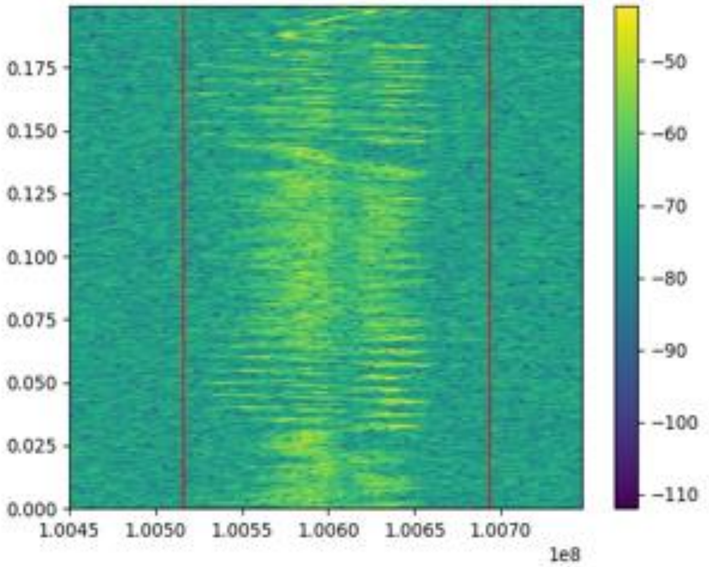
Ettus USRP E310

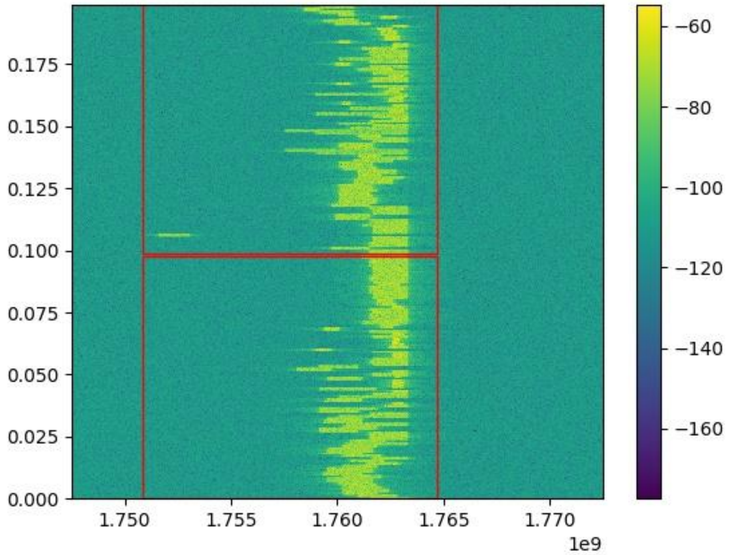


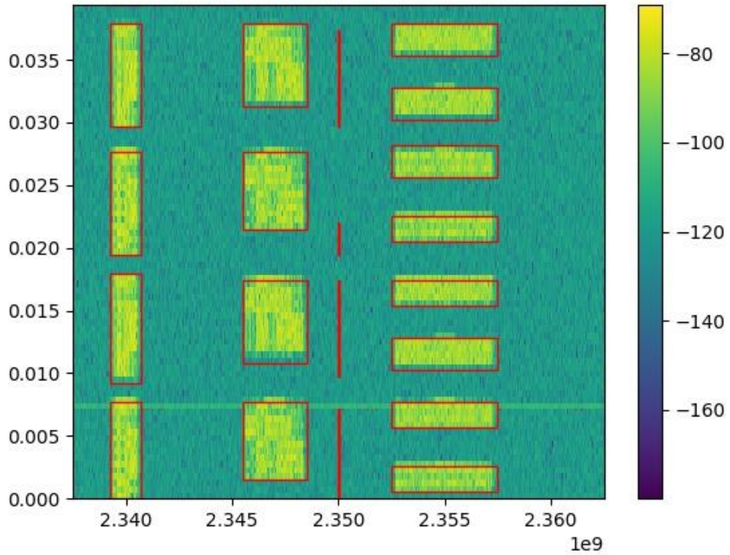
PicoZed SDR

Outras plataformas: E110, B210, B100, FPGA (con softcores) + ADCs

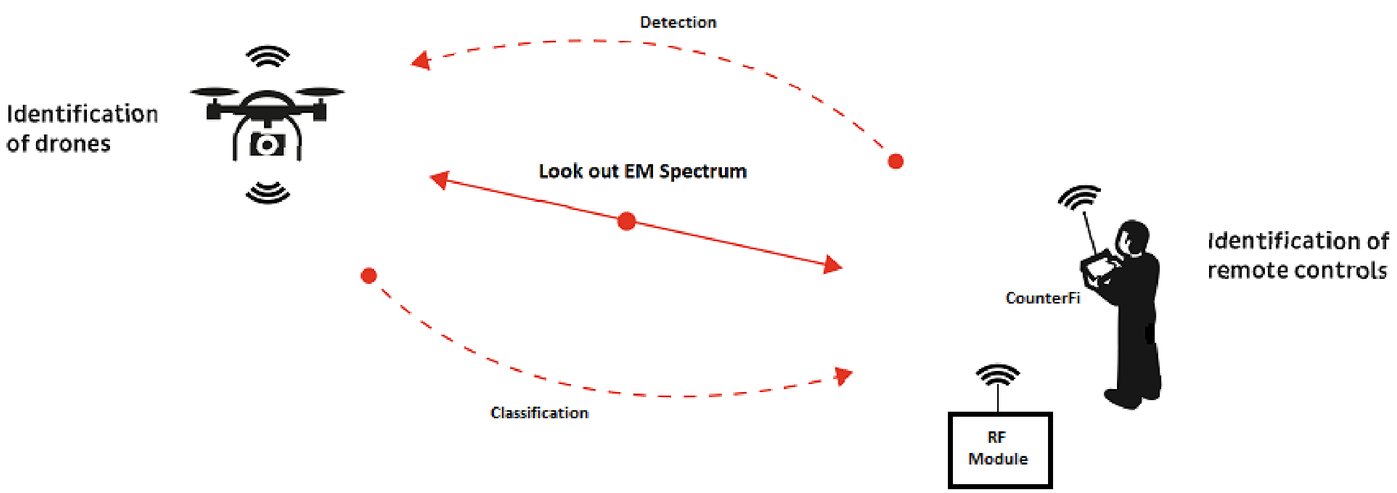
Test e medida – Detección e Identificación automática de sinais (interferencias)



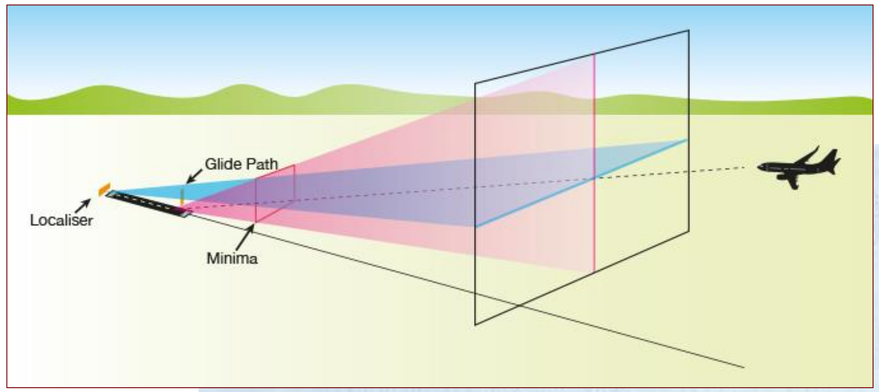


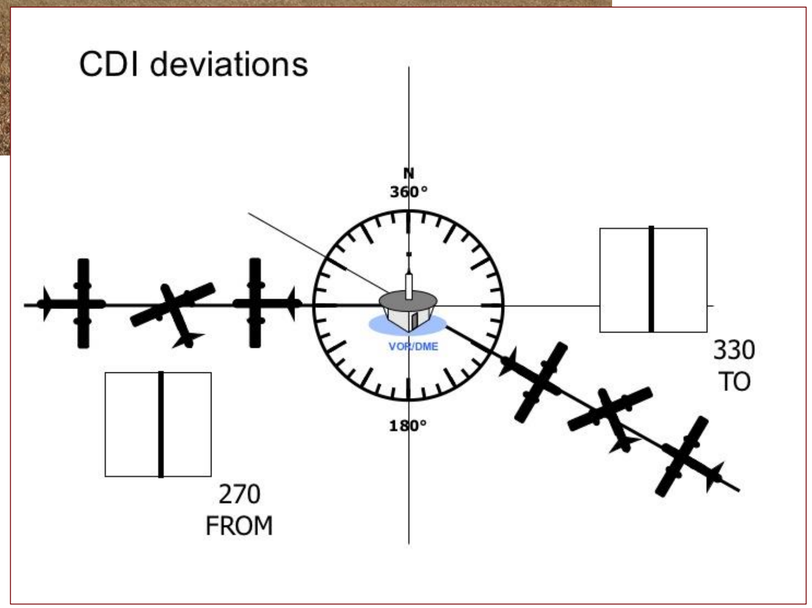


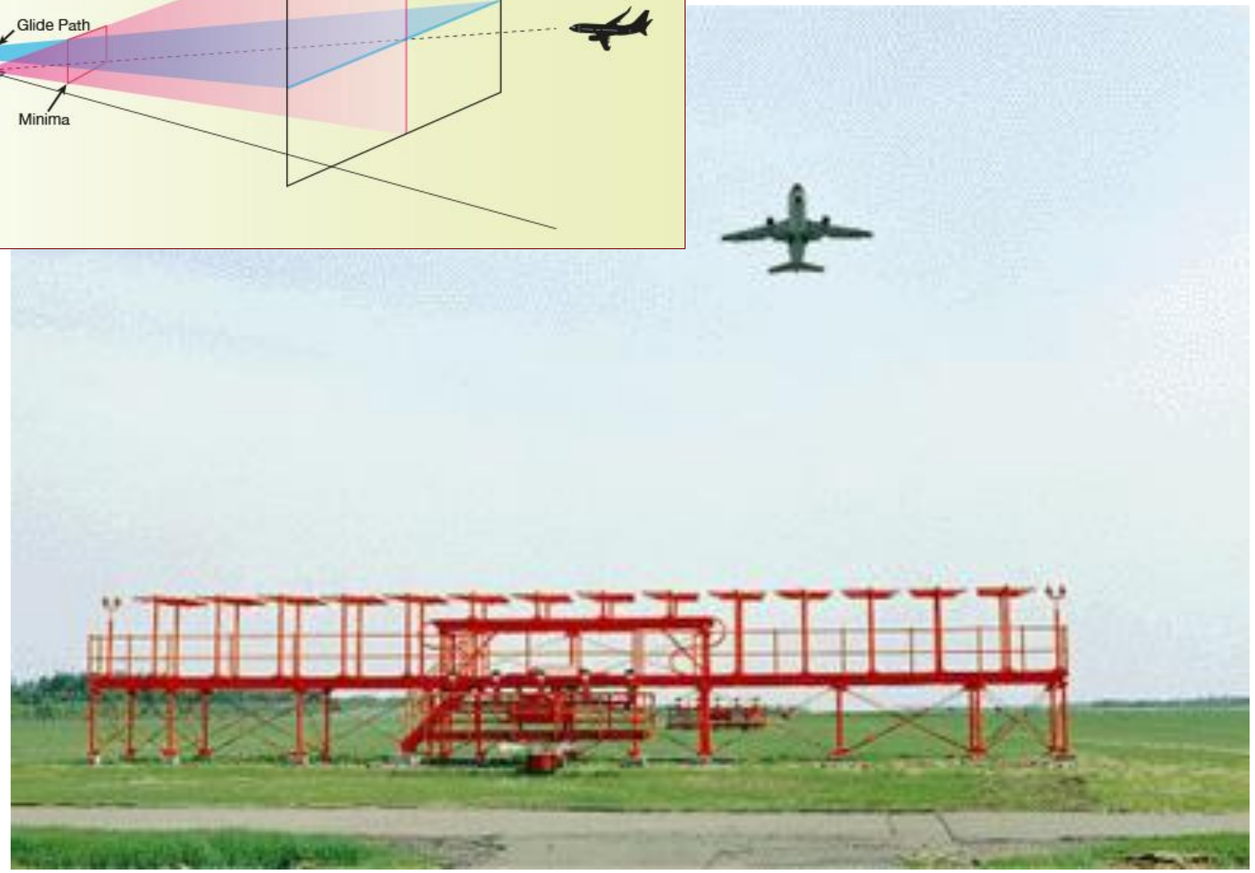
Detección e identificación de drons



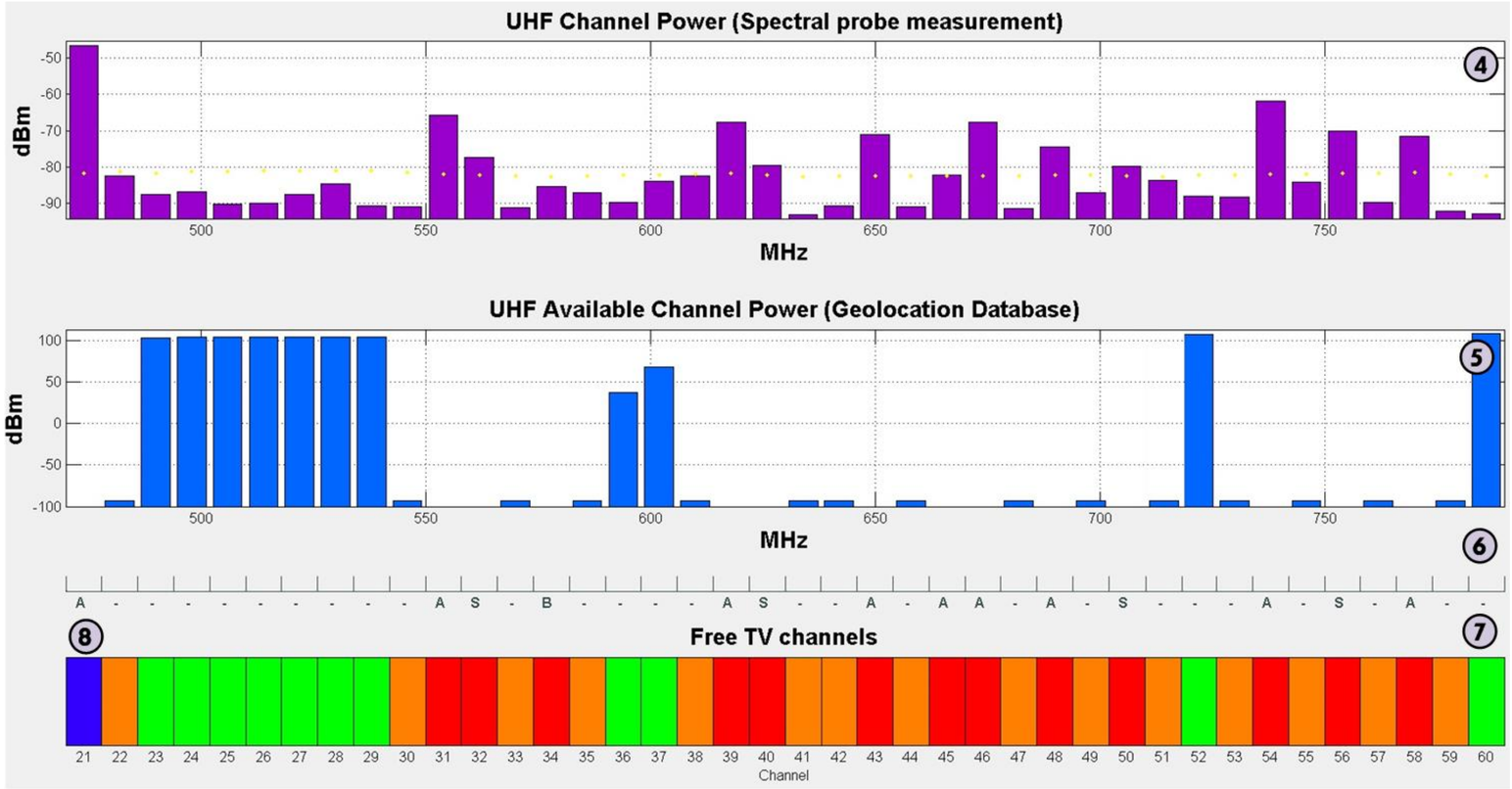
Test e medida – Radioaxudas para a navegación aérea

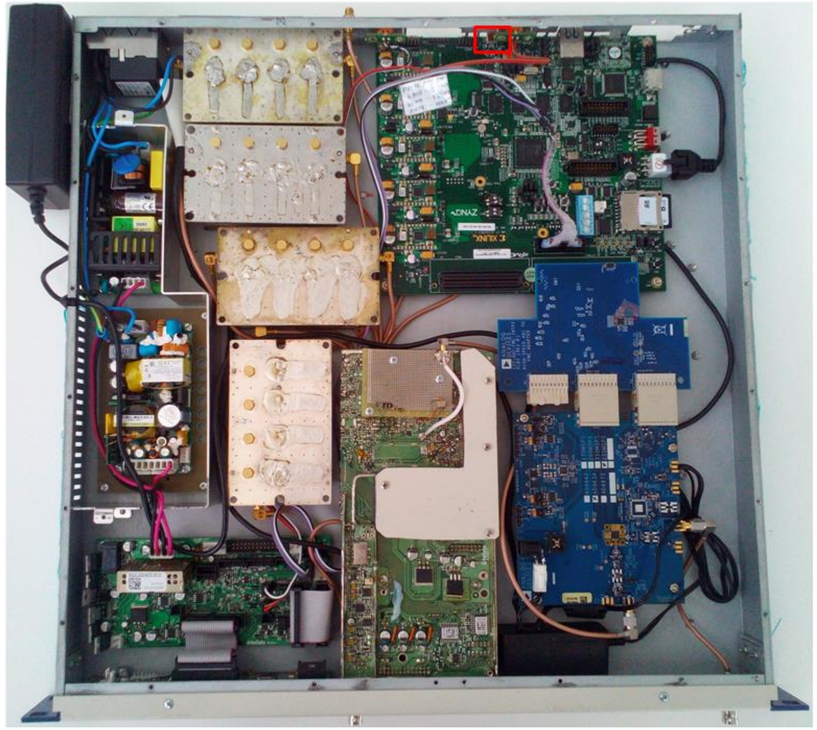


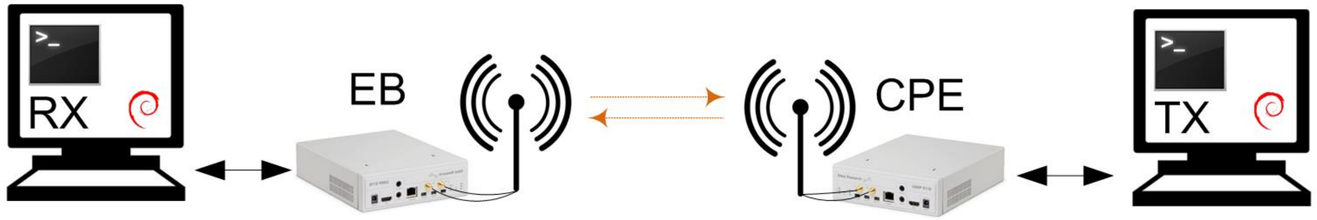




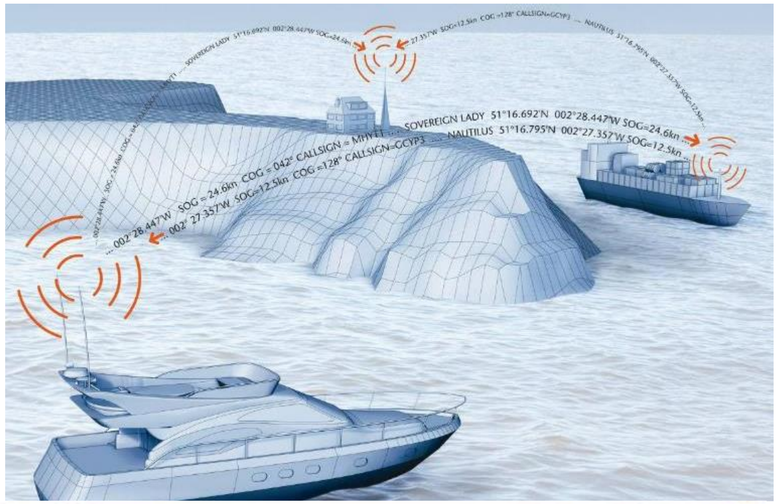
Radio cognitiva – Aproveitamento dos espazos brancos do espectro

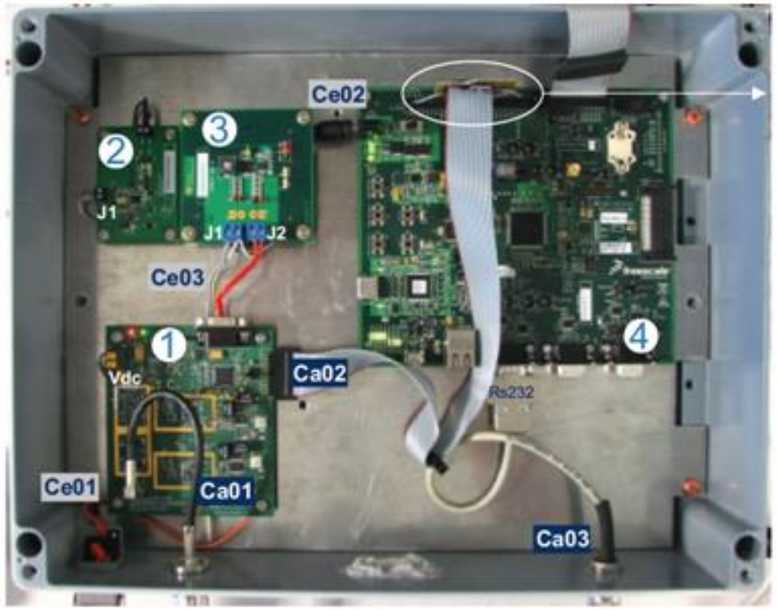




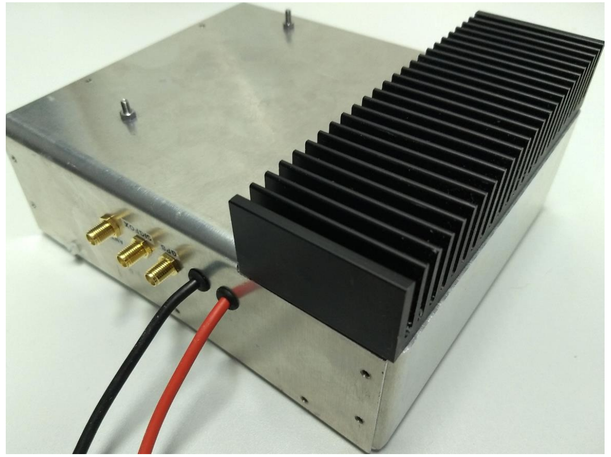


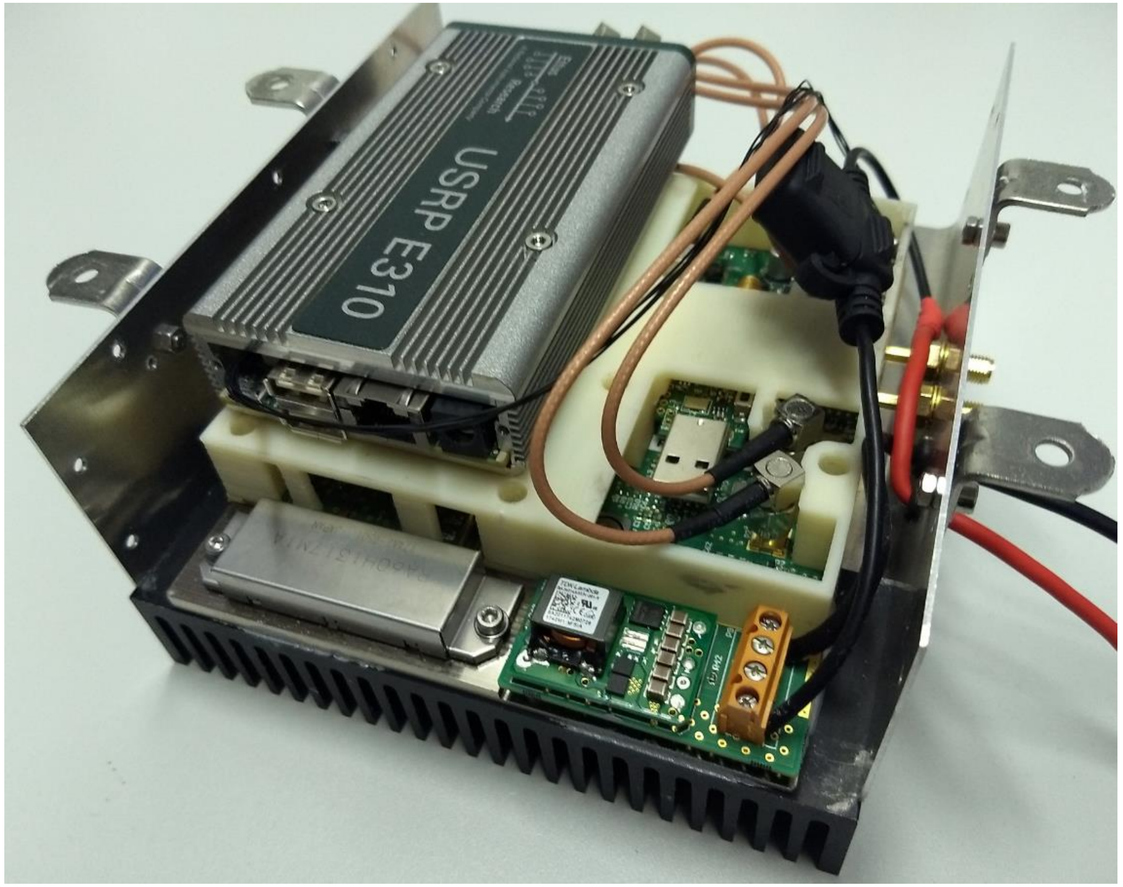
Comunicacións marítimas – AIS



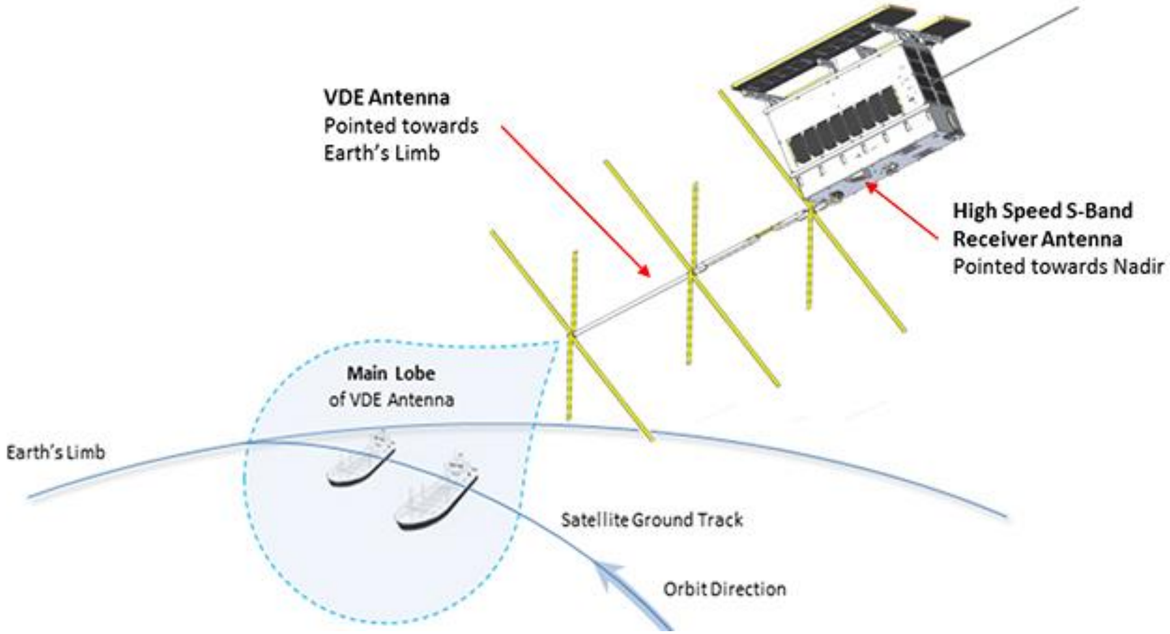


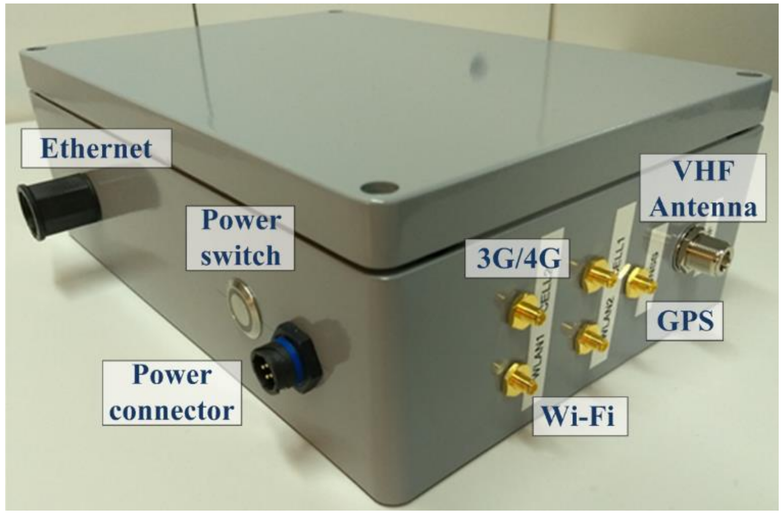
Comunicacións marítimas – Novo estándar VDES

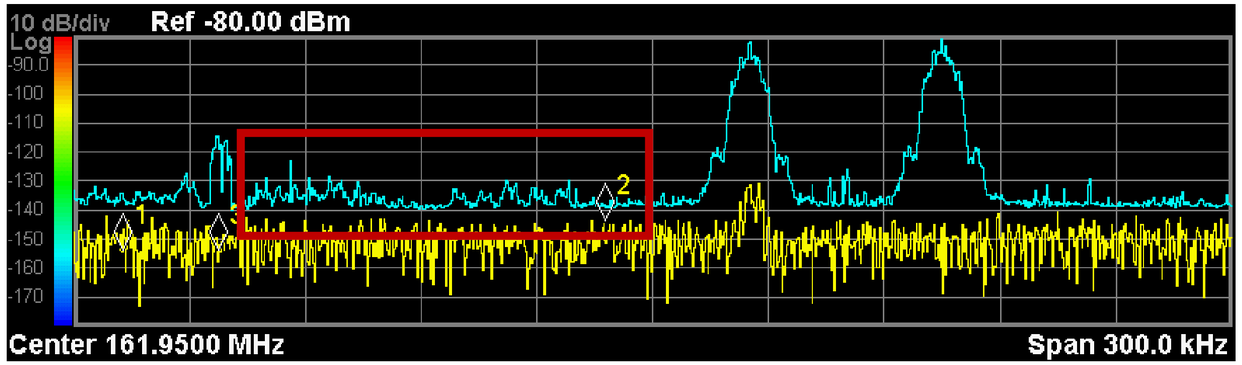




Comunicacións satelitais (marítimas) – VDES

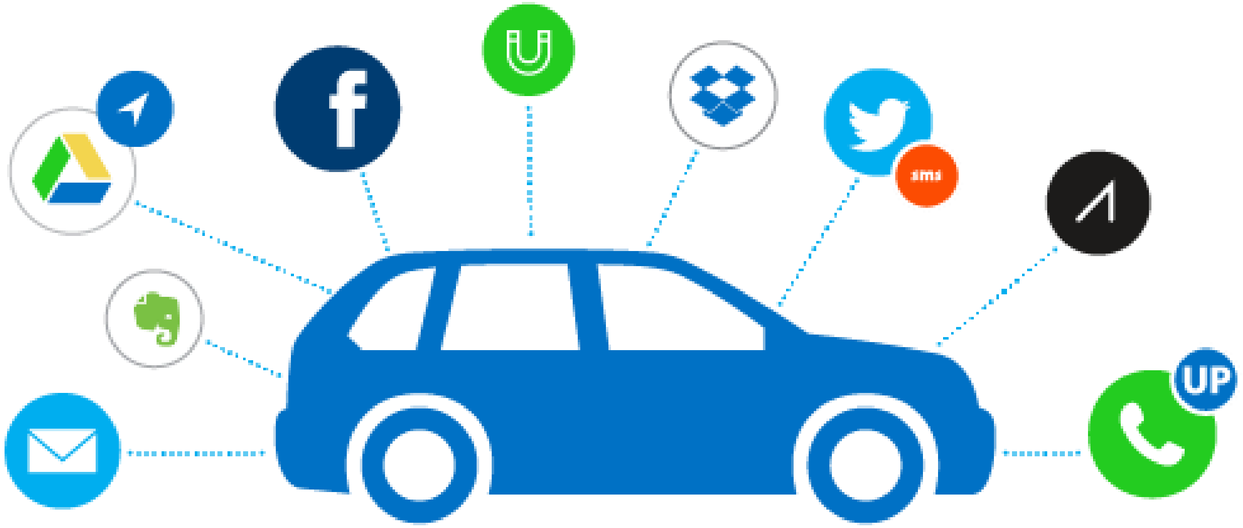


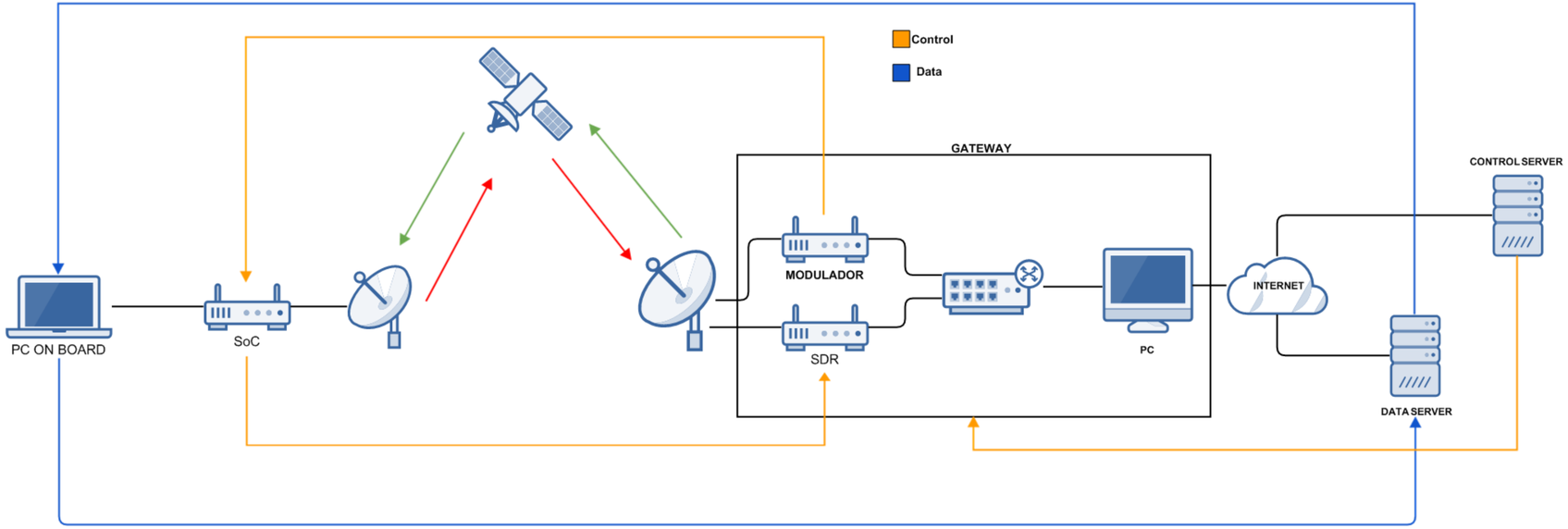




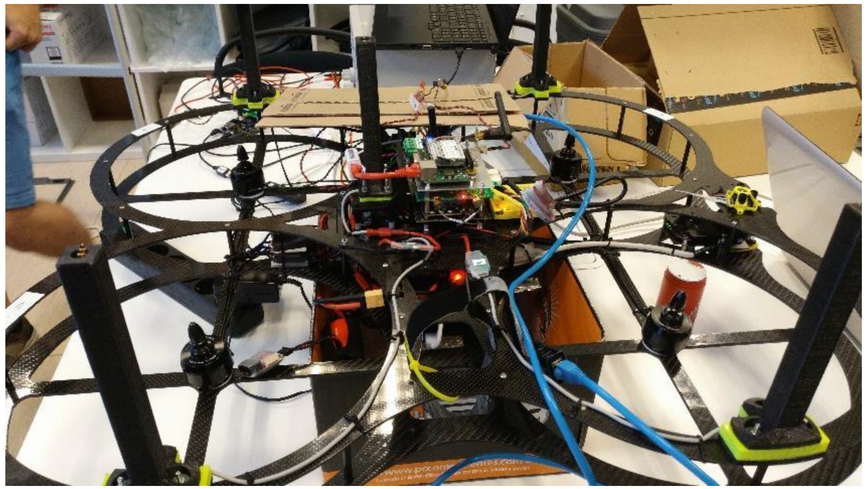
Comunicacións satelitais – Enlace de comunicacións para UAV

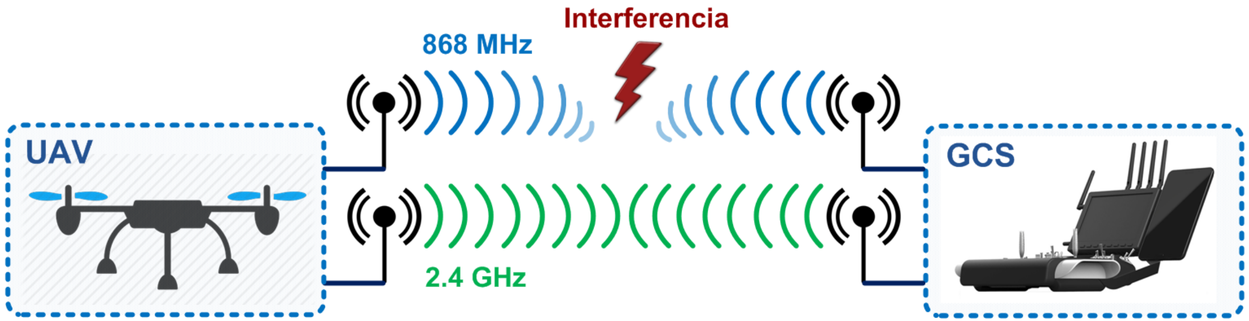
Comunicacións satelitais – Coche conectado

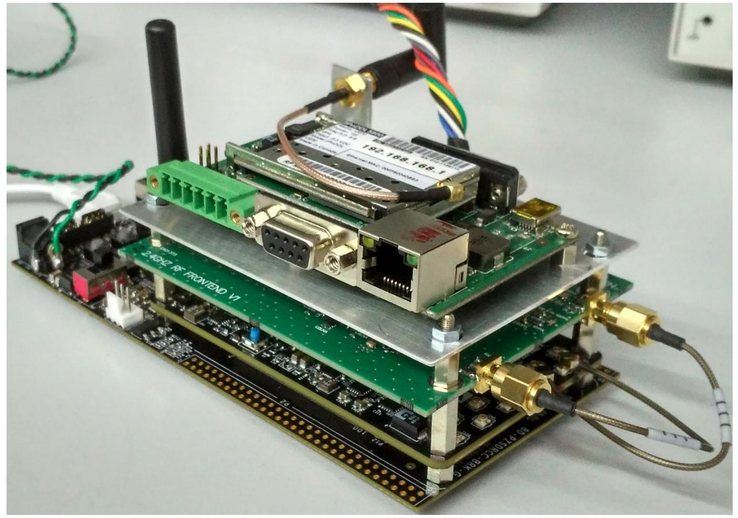




Enlaces de comunicacións robustos (FHSS)

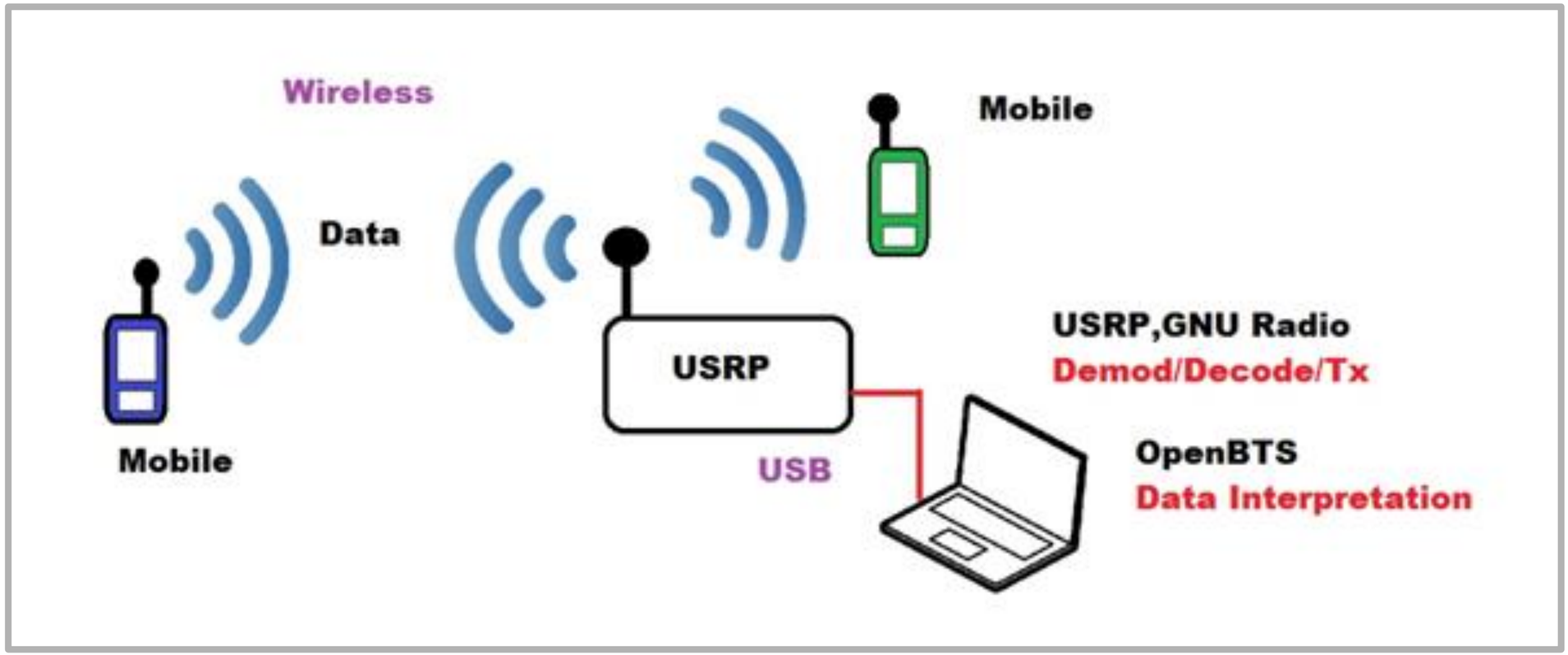




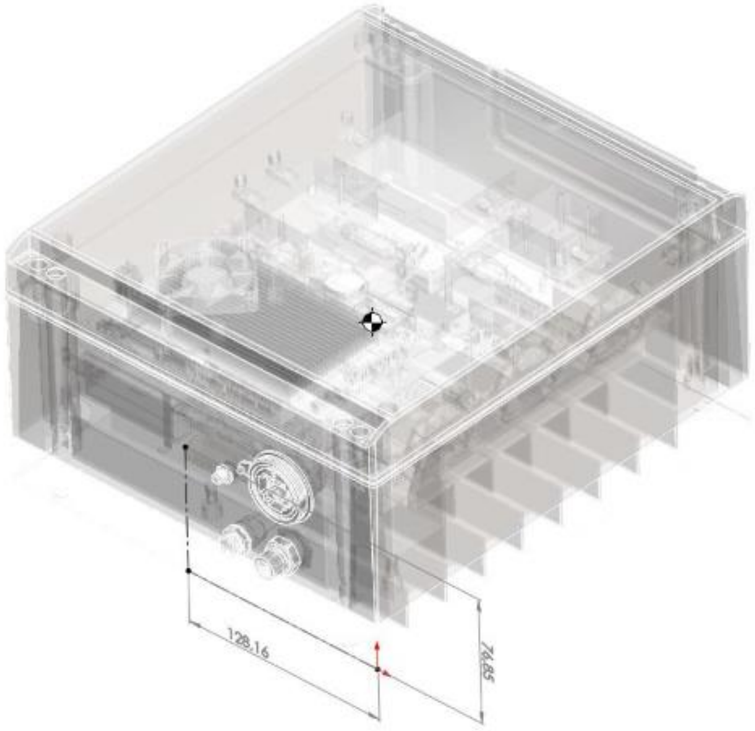


Estación base GSM

OpenBTS™



GPS spoofing



gradiant
Connectivity · Intelligence · Security
for your business

igomez@gradiant.org