black hat®
EUROPE 2025

Breaking The Rails

Taking Control Over Legacy And ERTMS/ETCS Railroad Signaling Systems

DAVID MELÉNDEZ

RnD Engineer &
Co-Founder, TechFrontiers

GABRIELA GARCIA

Security Engineer &
Co-Founder, TechFrontiers

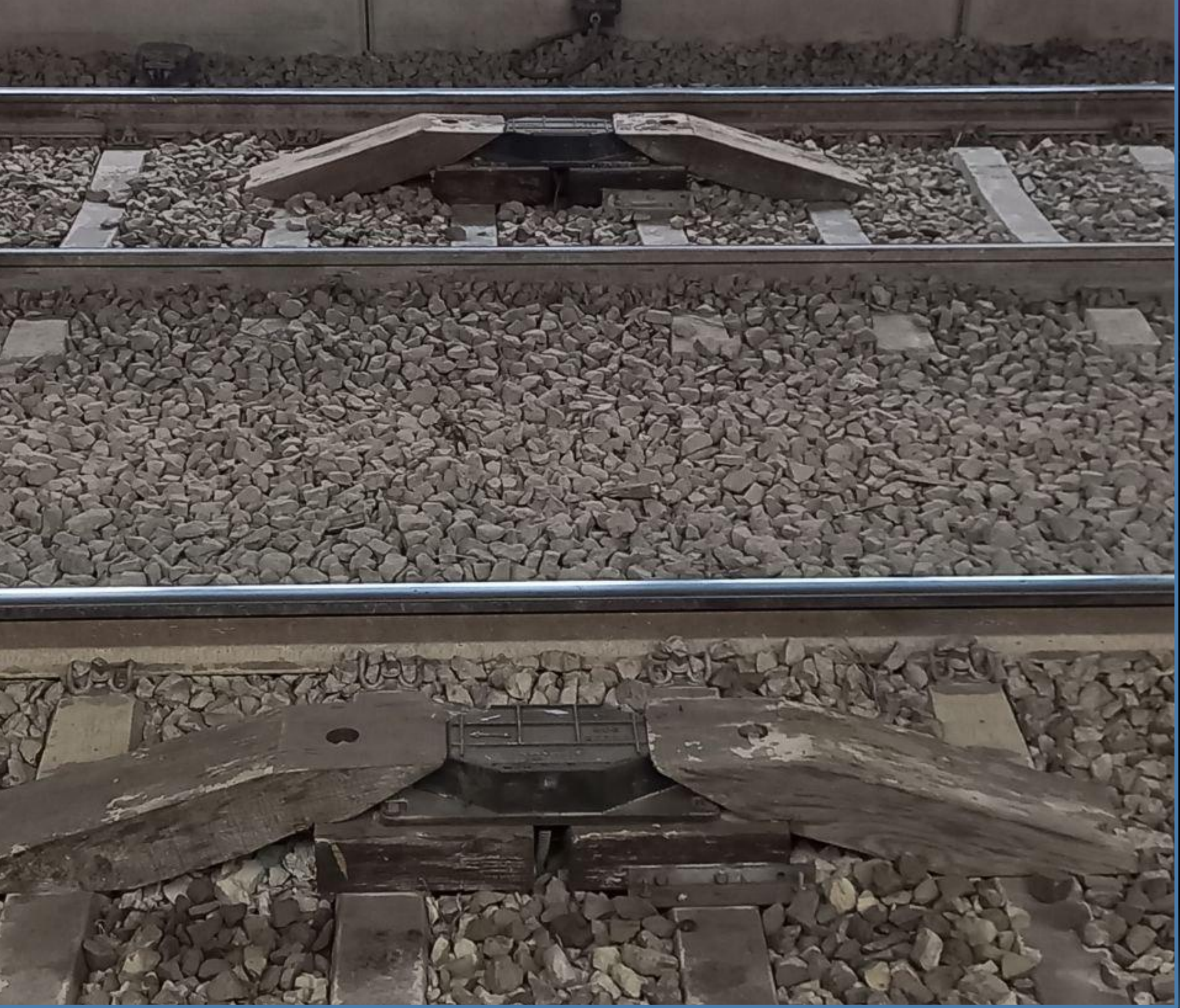
black hat
EUROPE 2025

WHY THE RAILWAY?

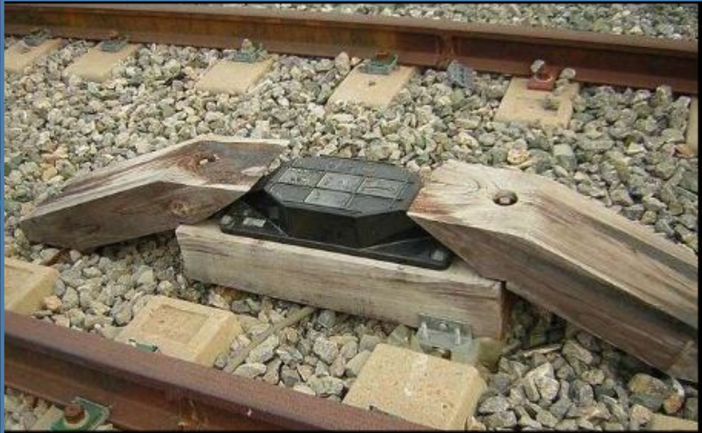
black hat EUROPE 2025

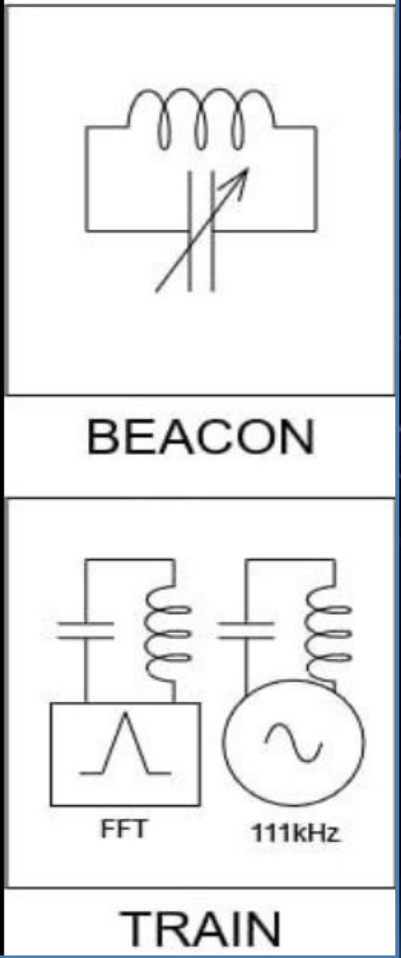
ASFA

Anuncio de Señales y Frenado Automático

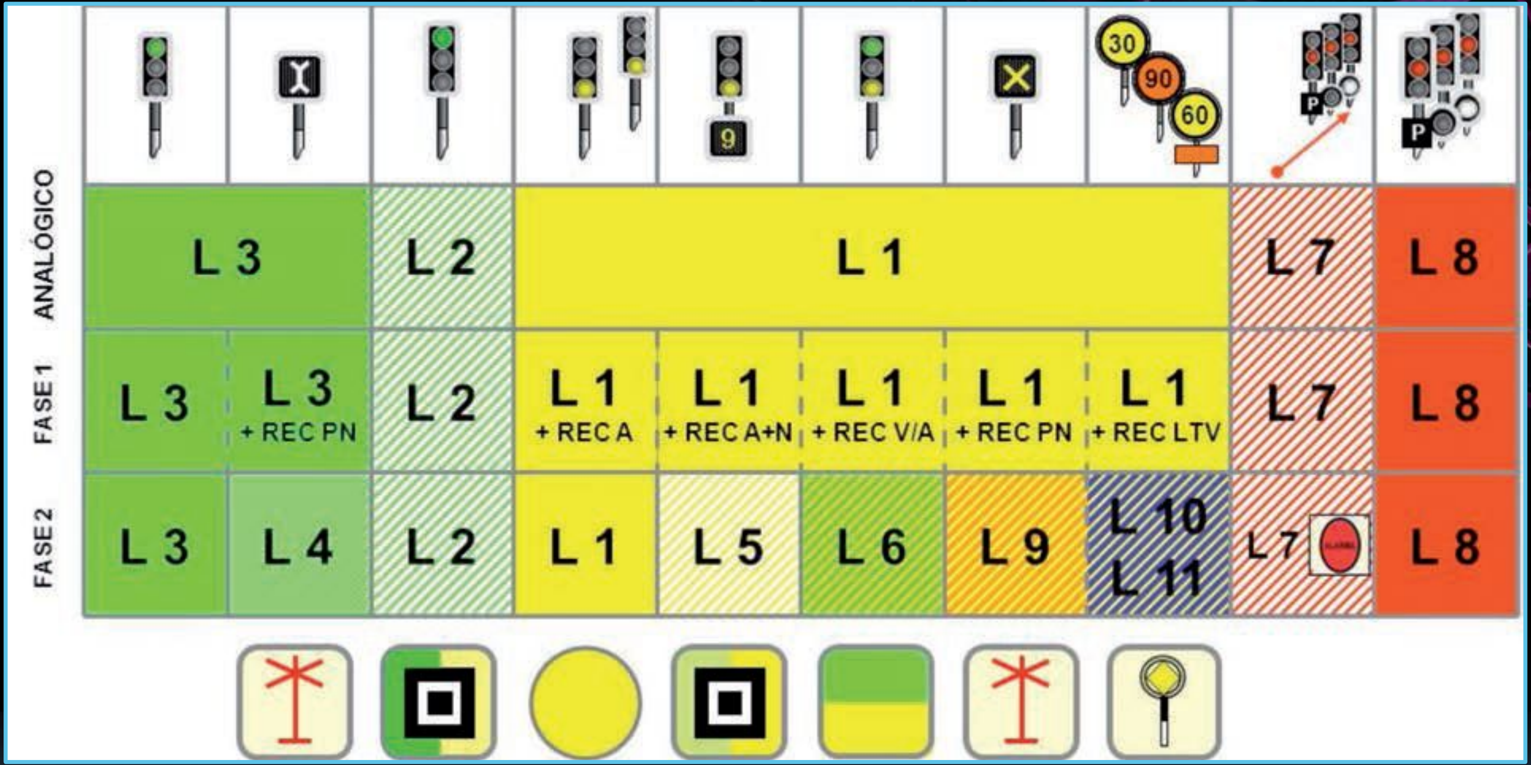


BEACONS ON THE TRACK (balises)

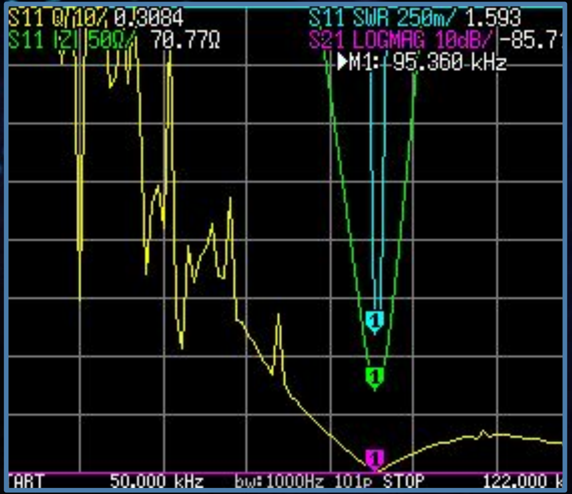


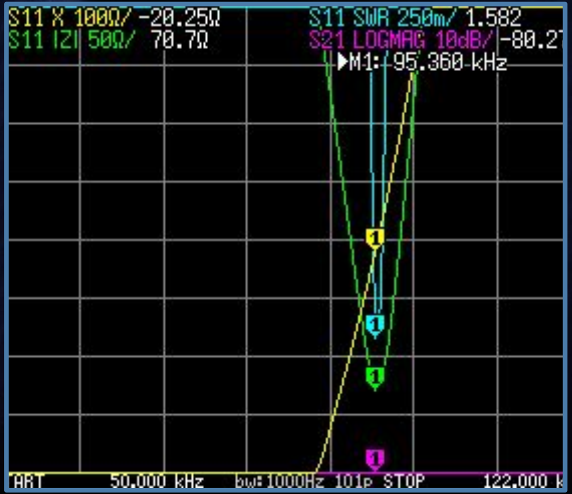

BEACON
FFT
111kHz
TRAIN

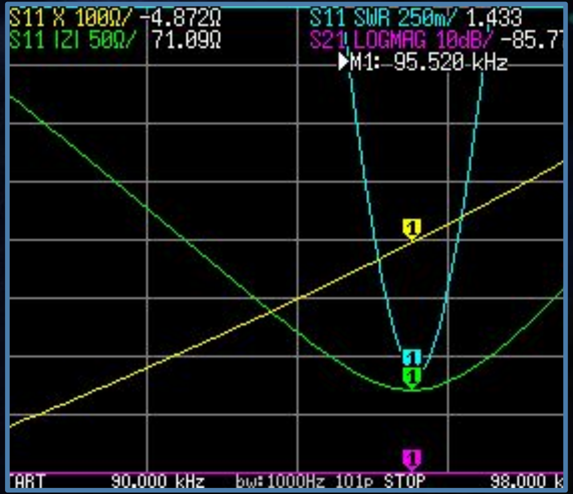
ASFA FREQUENCIES AND SIGNALS

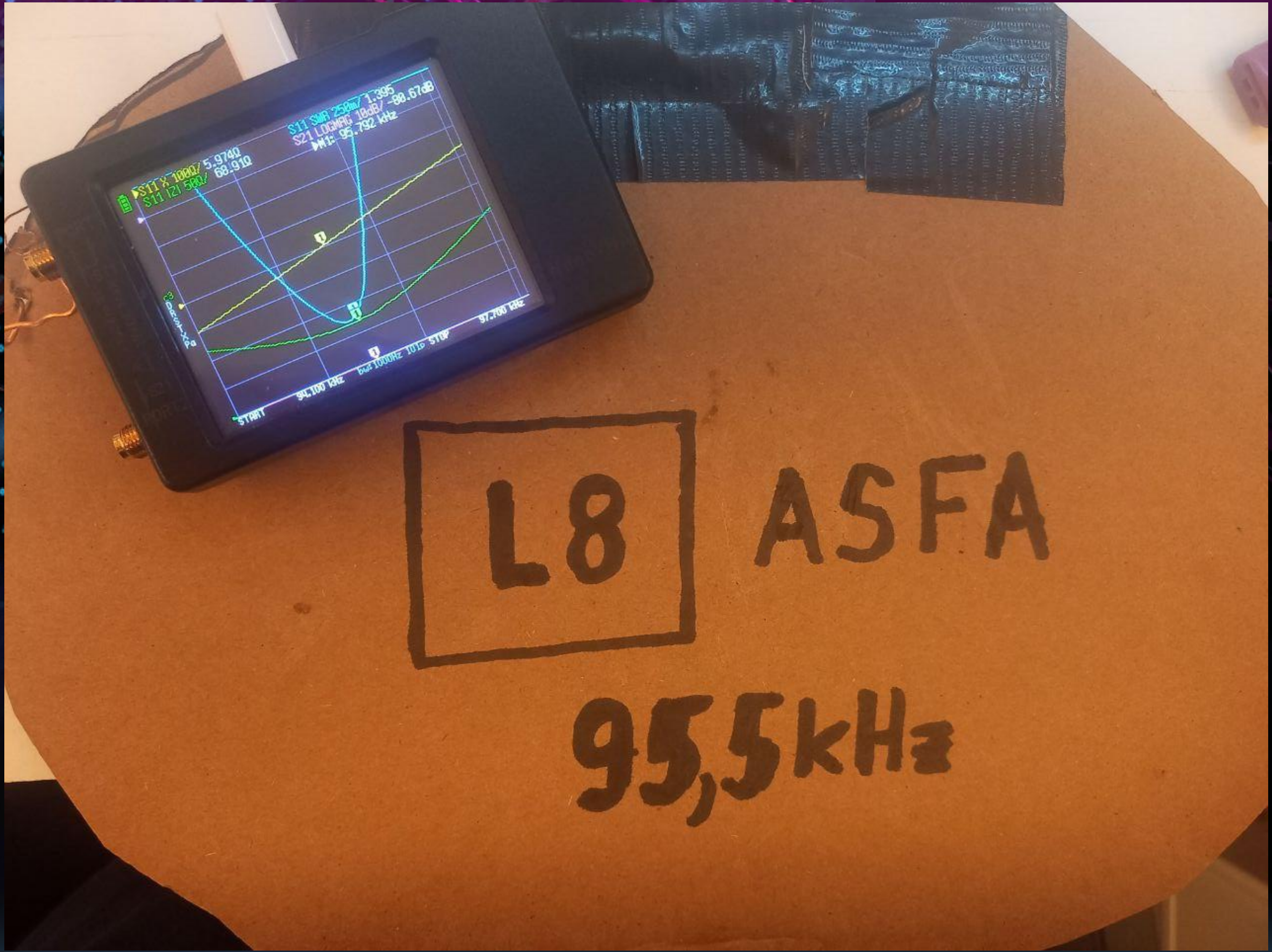


ANALÓGICO	L 3		L 2	L 1					L 7	L 8
FASE 1	L 3	L 3 + REC PN	L 2	L 1 + REC A	L 1 + REC A+N	L 1 + REC V/A	L 1 + REC PN	L 1 + REC LTV	L 7	L 8
FASE 2	L 3	L 4	L 2	L 1	L 5	L 6	L 9	L 10 L 11	L 7	L 8


S11 Q/10/ 0.3084
S11 |Z| 50Ω/ 70.77Ω
S11 SWR 250m/ 1.593
S21 LOGMAG 10dB/ -85.71
M1: 95.360 kHz
1
ART 50.000 kHz bw:1000Hz 101p STOP 122.000 k


S11 X 100Ω/ -20.25Ω
S11 |Z| 50Ω/ 70.7Ω
S11 SWR 250m/ 1.582
S21 LOGMAG 10dB/ -80.27
M1: 95.360 kHz
1
ART 50.000 kHz bw:1000Hz 101p STOP 122.000 k


S11 X 100Ω/ -4.872Ω
S11 |Z| 50Ω/ 71.09Ω
S11 SWR 250m/ 1.433
S21 LOGMAG 10dB/ -85.77
M1: 95.520 kHz
1
ART 90.000 kHz bw:1000Hz 101p STOP 98.000 k

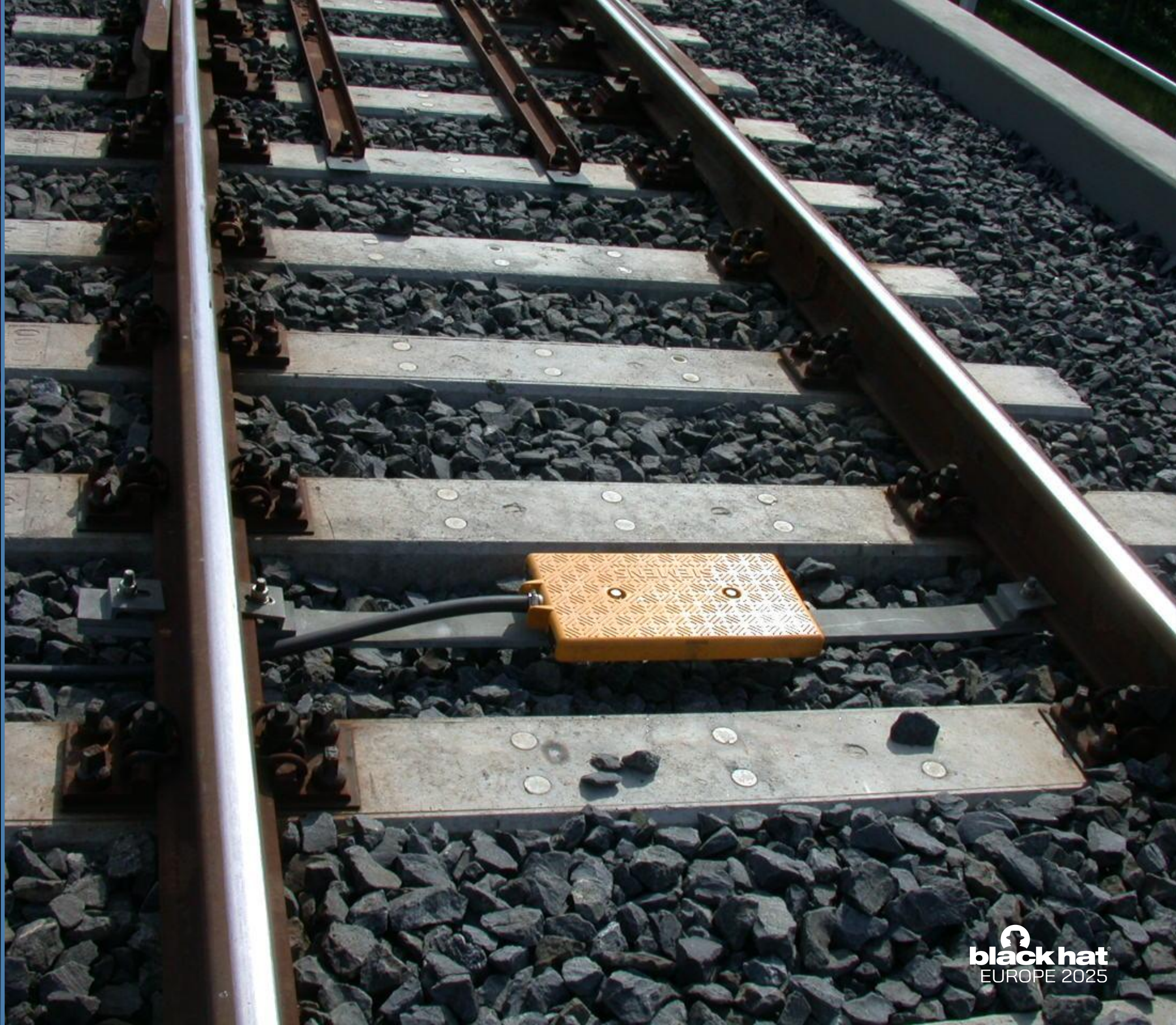


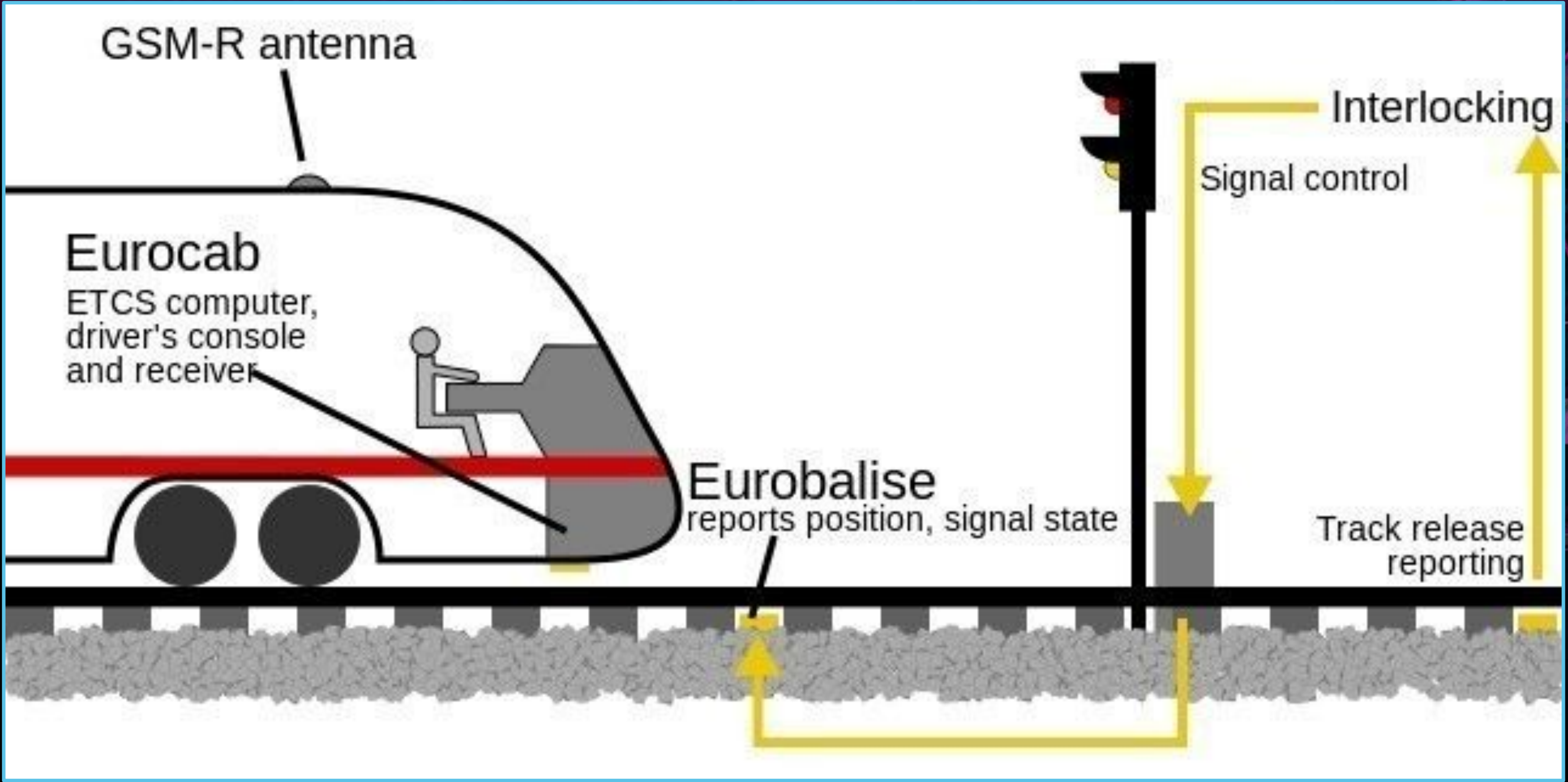
S11 X 100Ω/ 5.974Ω
S11 |Z| 50Ω/ 68.91Ω
S11 SWR 250m/ 1.395
S21 LOGMAG 10dB/ -80.67dB
M1: 95.792 kHz
START
94.100 kHz
bw:1000Hz 101p STOP
97.700 kHz
L8
ASFA
95,5kHz

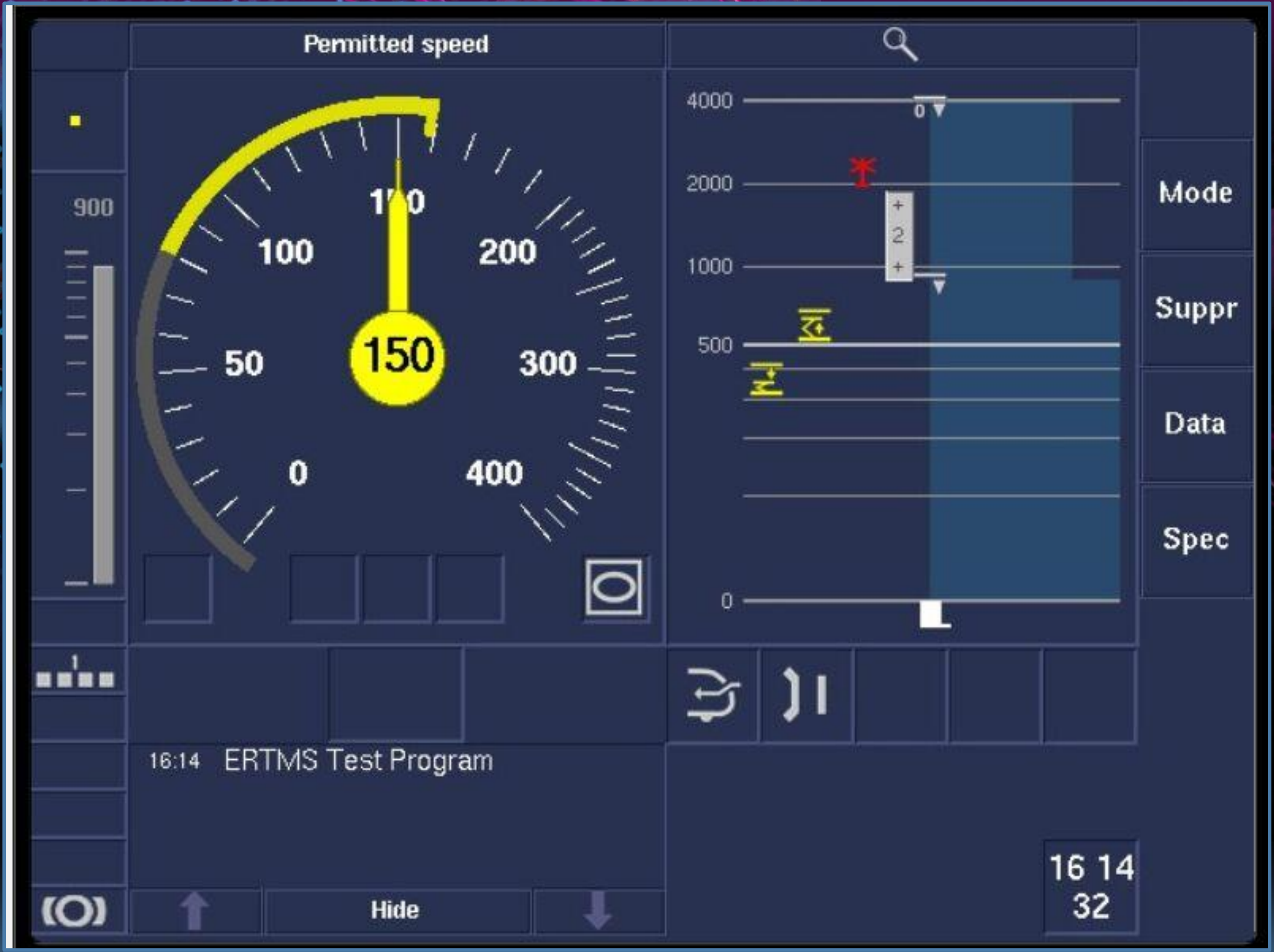
ERTMS

European Rail Traffic Management System

NEW ON-TRACK BALISES




GSM-R antenna
Eurocab
ETCS computer, driver's console and receiver
Eurobalise
reports position, signal state
Interlocking
Signal control
Track release reporting



16:14 ERTMS Test Program

16 14
32

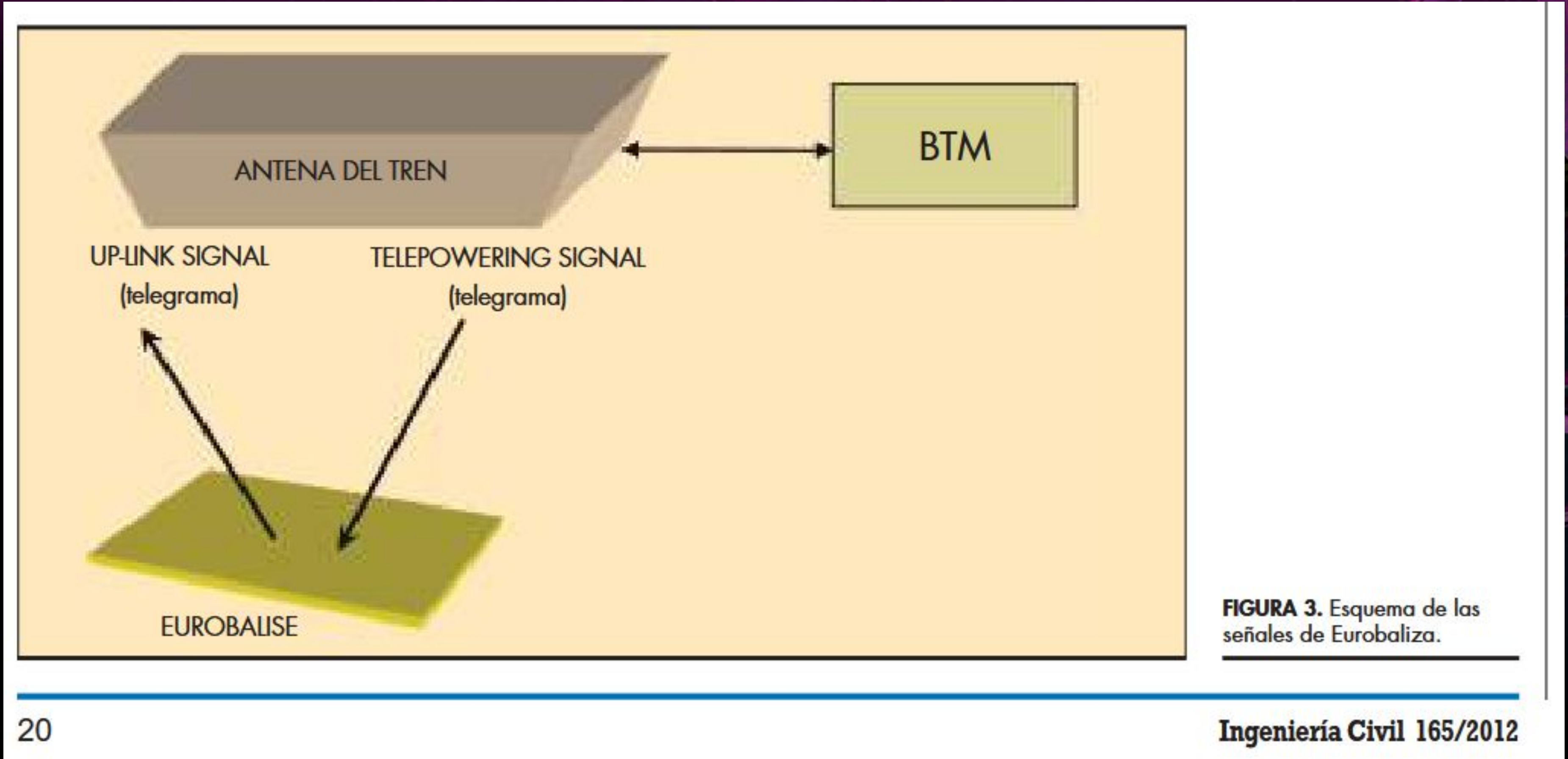
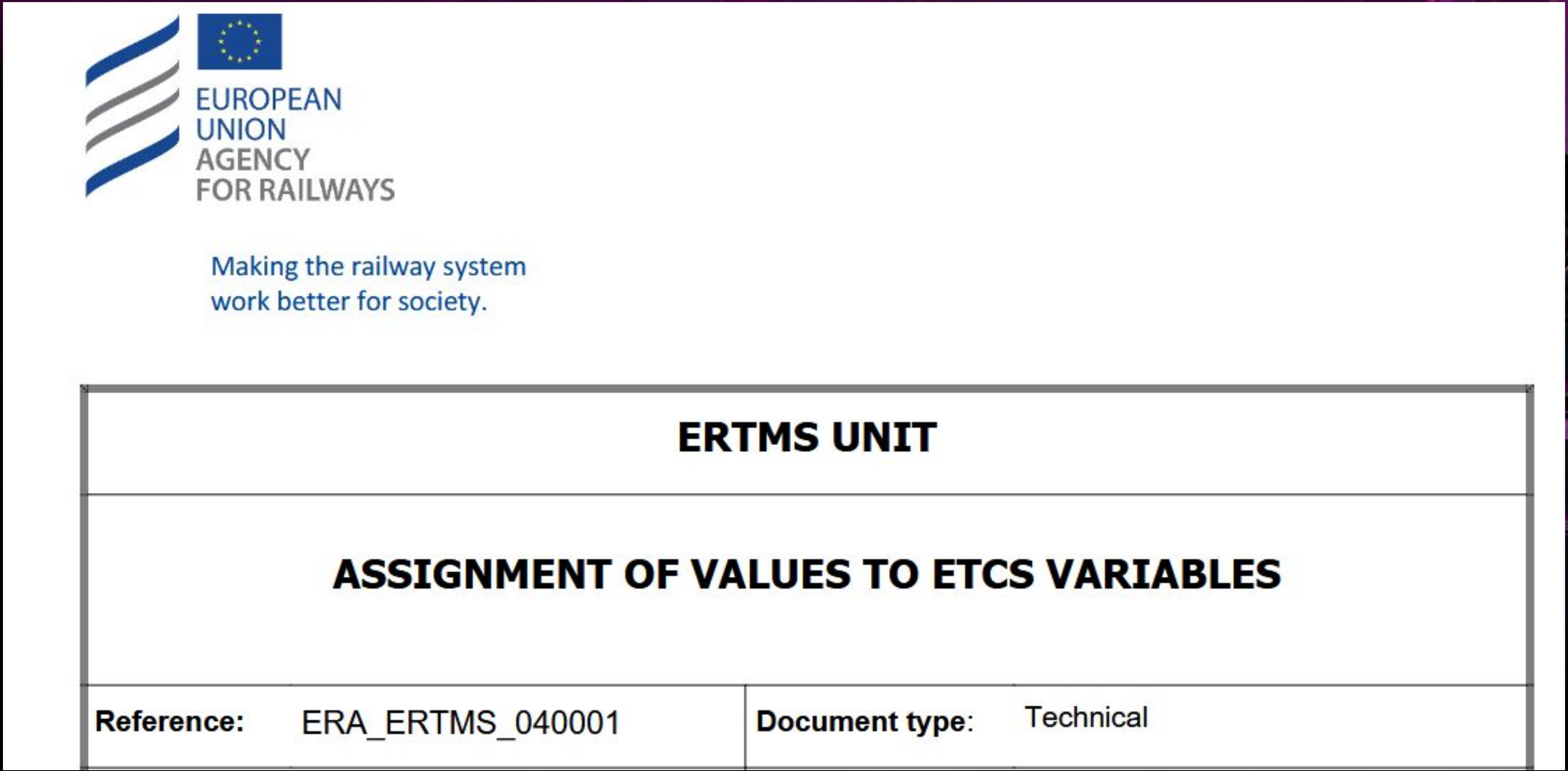


FIGURA 3. Esquema de las señales de Eurobaliza.

20

Ingeniería Civil 165/2012



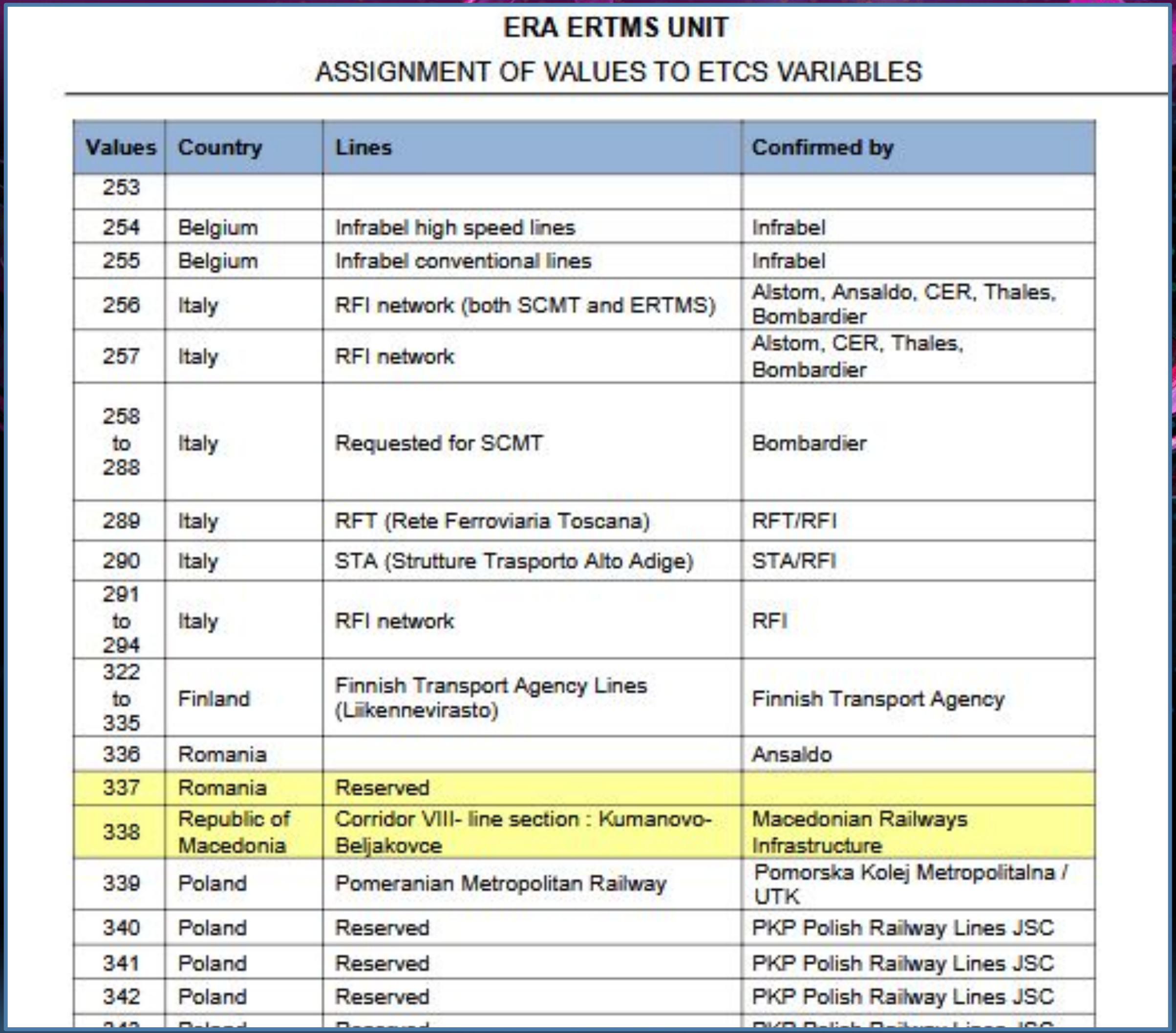
EUROPEAN
UNION
AGENCY
FOR RAILWAYS

Making the railway system
work better for society.

ERTMS UNIT
ASSIGNMENT OF VALUES TO ETCS VARIABLES

Reference:	ERA_ERTMS_040001	**Document type**:	Technical

PUBLIC DOCUMENTS VALUES



ERA ERTMS UNIT

ASSIGNMENT OF VALUES TO ETCS VARIABLES

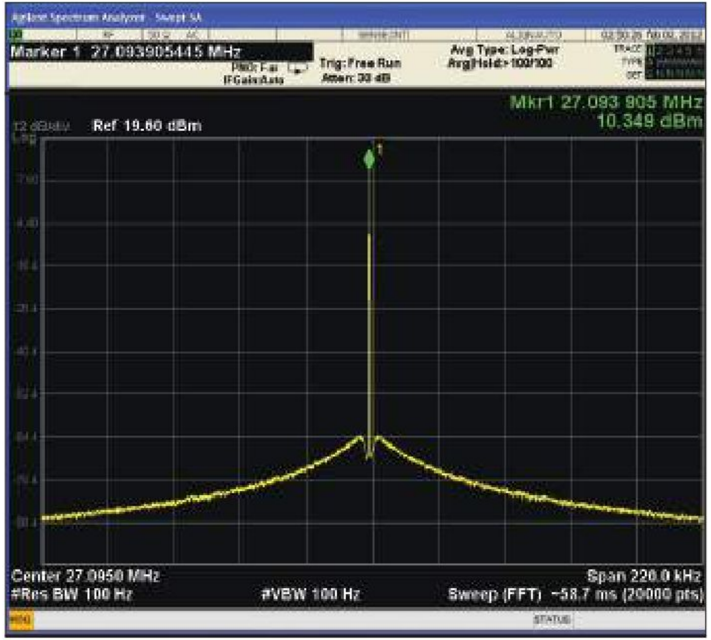
Values	Country	Lines	Confirmed by
253			
254	Belgium	Infrabel high speed lines	Infrabel
255	Belgium	Infrabel conventional lines	Infrabel
256	Italy	RFI network (both SCMT and ERTMS)	Alstom, Ansaldo, CER, Thales, Bombardier
257	Italy	RFI network	Alstom, CER, Thales, Bombardier
258 to 288	Italy	Requested for SCMT	Bombardier
289	Italy	RFT (Rete Ferroviaria Toscana)	RFT/RFI
290	Italy	STA (Strutture Trasporto Alto Adige)	STA/RFI
291 to 294	Italy	RFI network	RFI
322 to 335	Finland	Finnish Transport Agency Lines (Liikennevirasto)	Finnish Transport Agency
336	Romania		Ansaldo
337	Romania	Reserved	
338	Republic of Macedonia	Corridor VIII- line section : Kumanovo-Beljakovce	Macedonian Railways Infrastructure
339	Poland	Pomeranian Metropolitan Railway	Pomorska Kolej Metropolitalna / UTK
340	Poland	Reserved	PKP Polish Railway Lines JSC
341	Poland	Reserved	PKP Polish Railway Lines JSC
342	Poland	Reserved	PKP Polish Railway Lines JSC

DATA OBTAINED FROM PUBLIC DOCUMENTS

- TELEPOWERING 27,095 MHz ± 5 kHz
- (other documents: 27,115 MHz)

- DOWNLINK – 2-FSK
- δ_central = 4,2 MHz

- b_0 @ 3,951 MHz
- b_1 @ 4,516 MHz



Agilent Spectrum Analyzer - Swept SA

Marker 1 27.093905445 MHz

PNO: Fast
IFGain:Auto

Trig: Free Run
Atten: 30 dB

Avg Type: Log-Pwr
Avg|Hold:>100/100

Mkr1 27.093 905 MHz
10.349 dBm

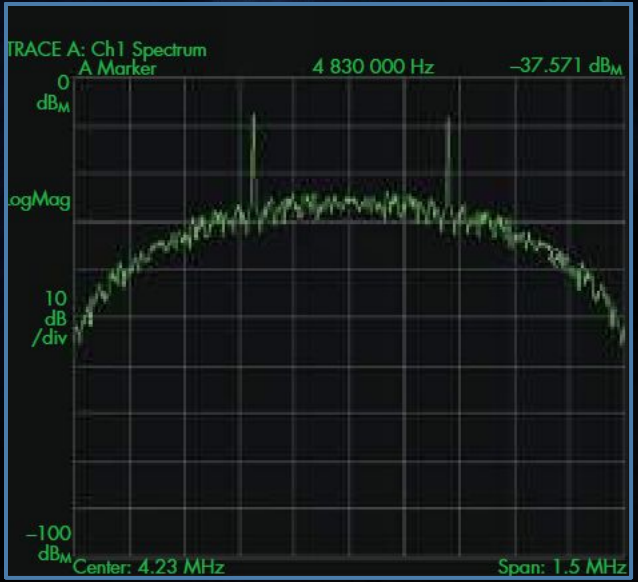
Ref 19.60 dBm

Center 27.0950 MHz
#Res BW 100 Hz

#VBW 100 Hz

Span 220.0 kHz
Sweep (FFT) ~58.7 ms (20000 pts)

FIGURA 20. Ejemplo de resultado del ensayo de características de la señal de telepowering.

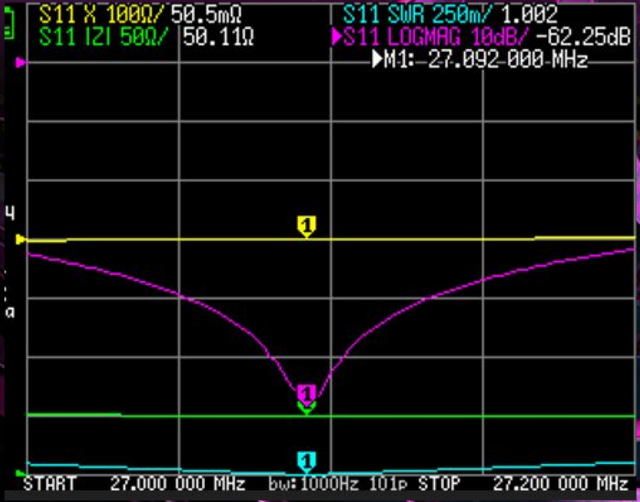


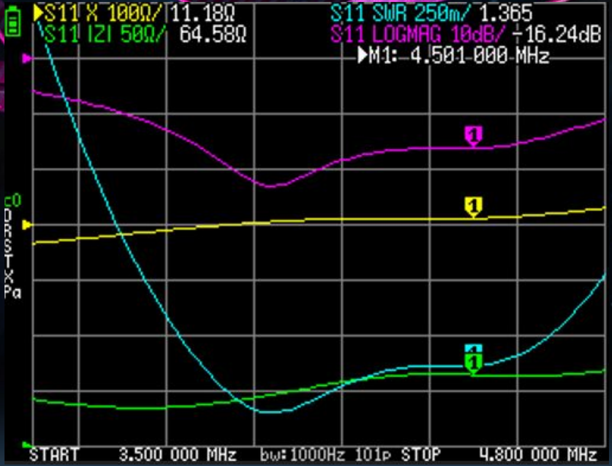
TRACE A: Ch1 Spectrum
A Marker 4 830 000 Hz –37.571 dB_M

Center: 4.23 MHz

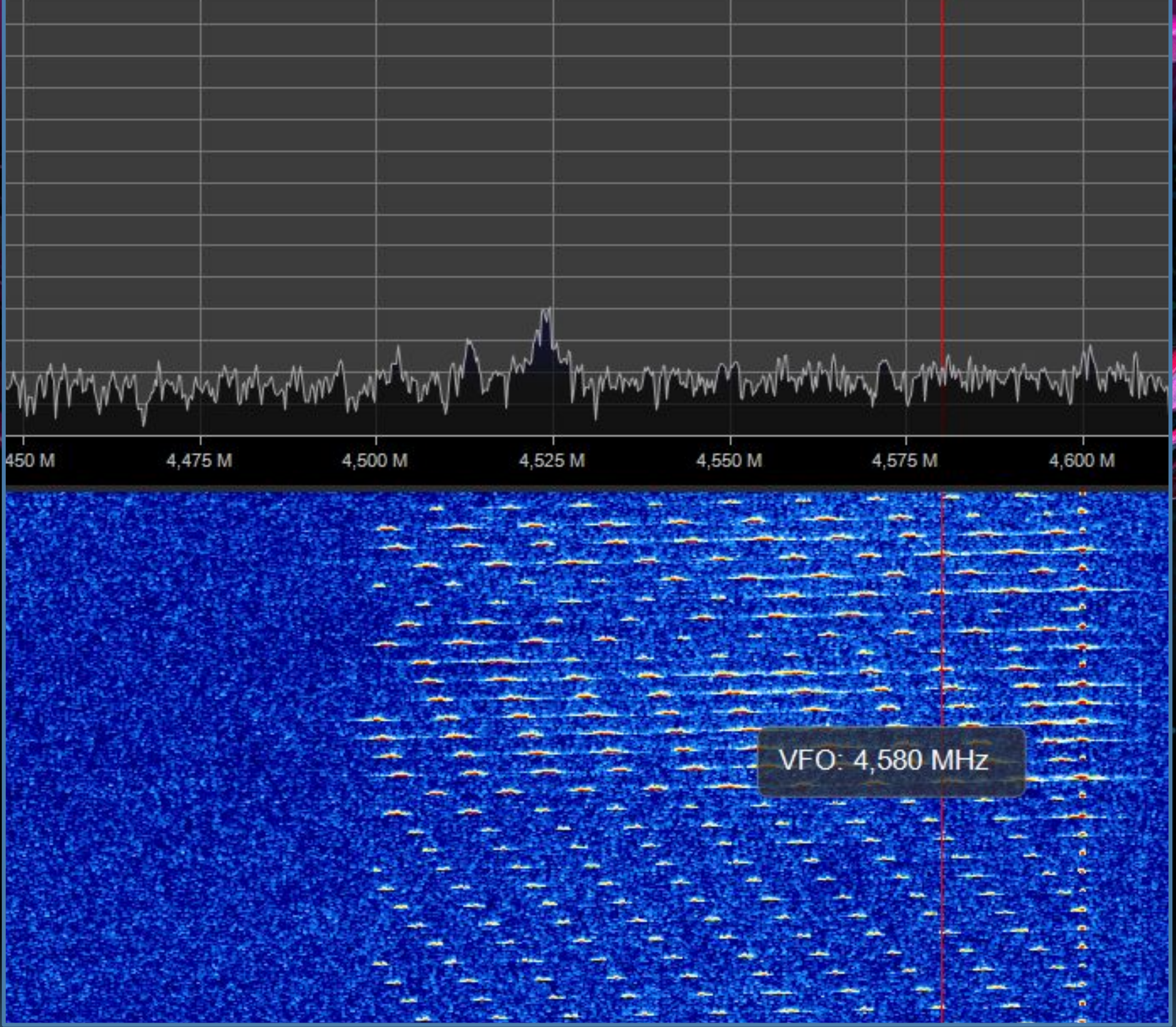
Span: 1.5 MHz

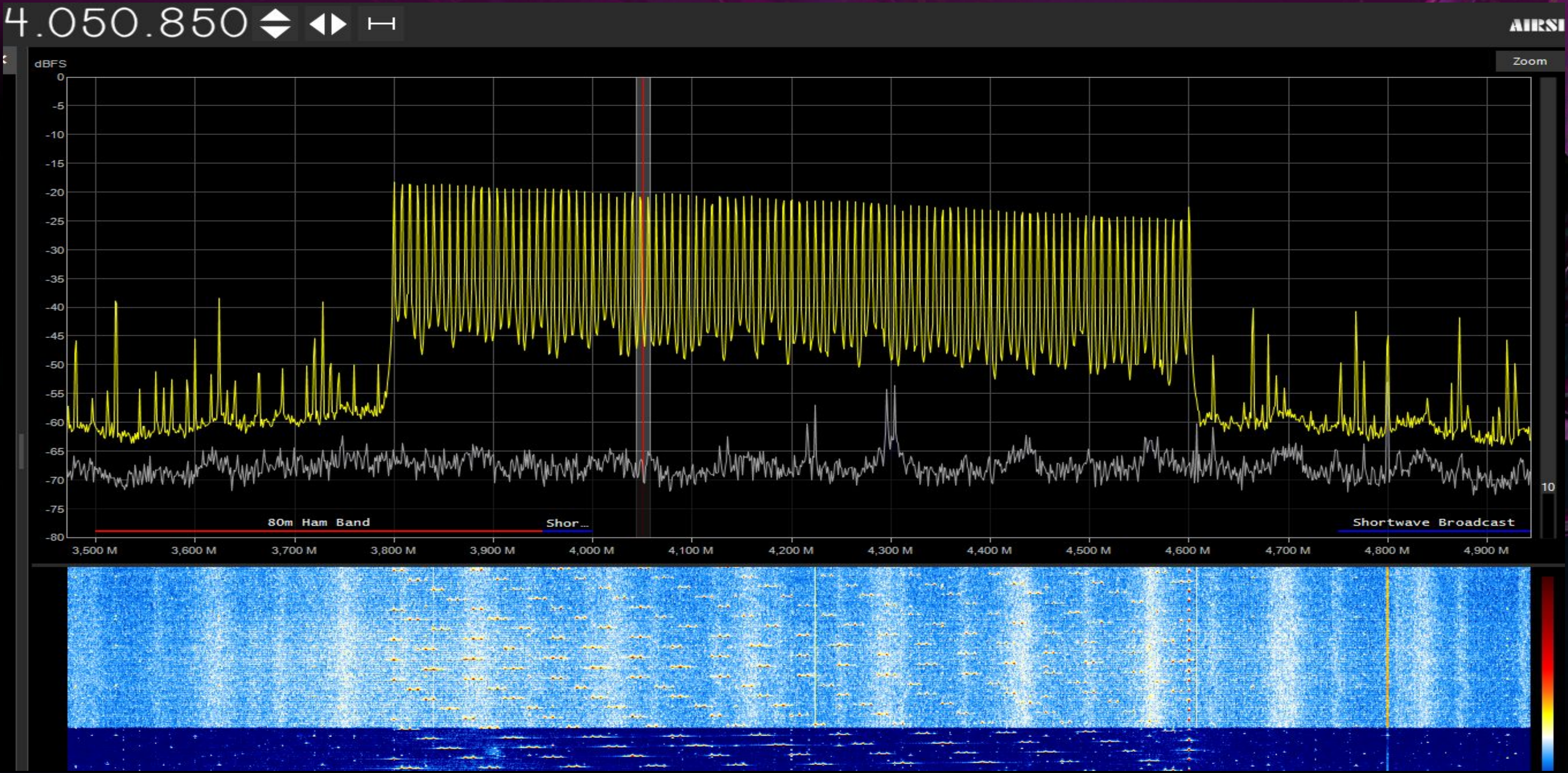
TX and RX ANTENNA PERFORMANCE

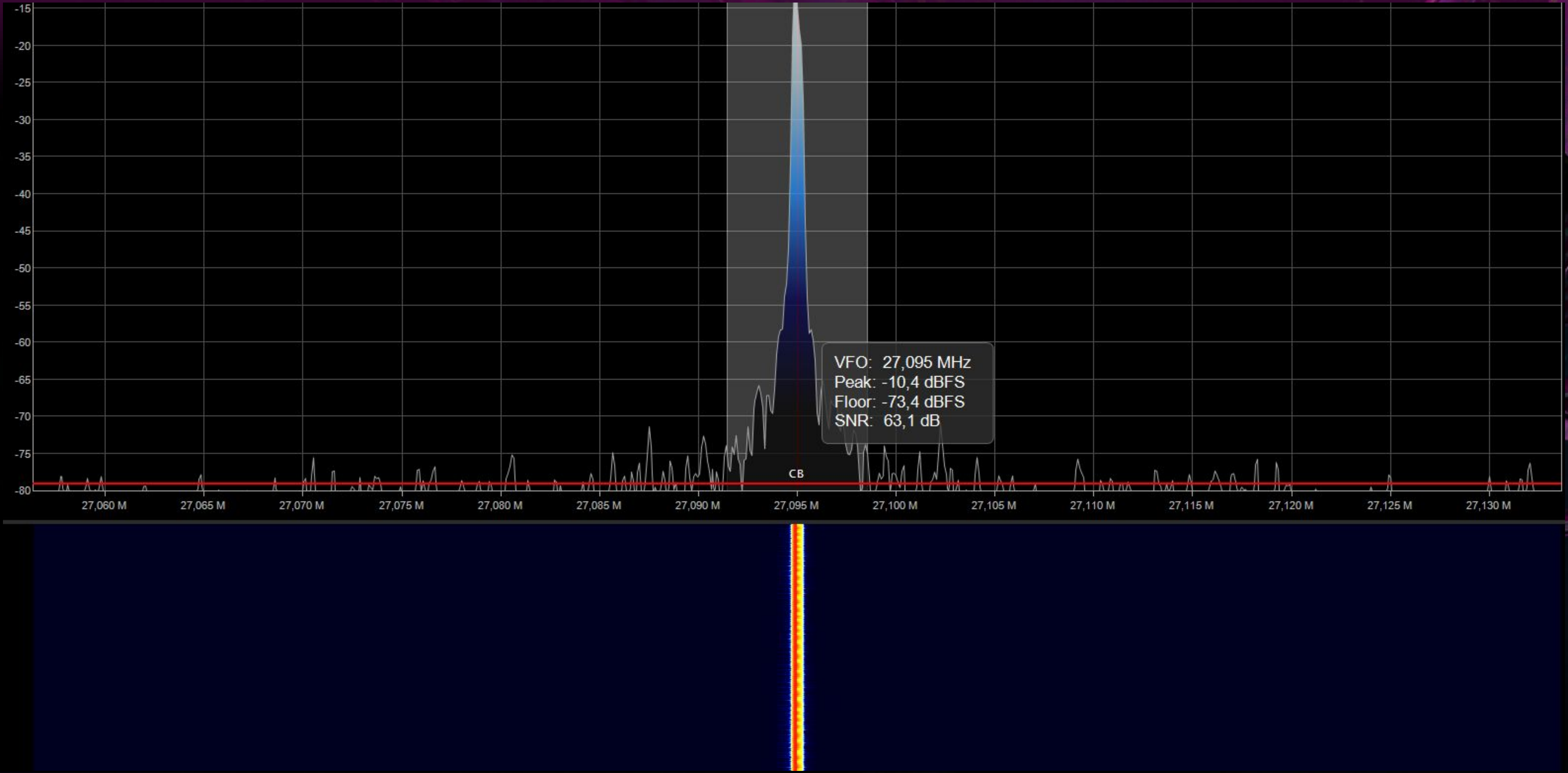




RX TESTING WITH VNA PINGS

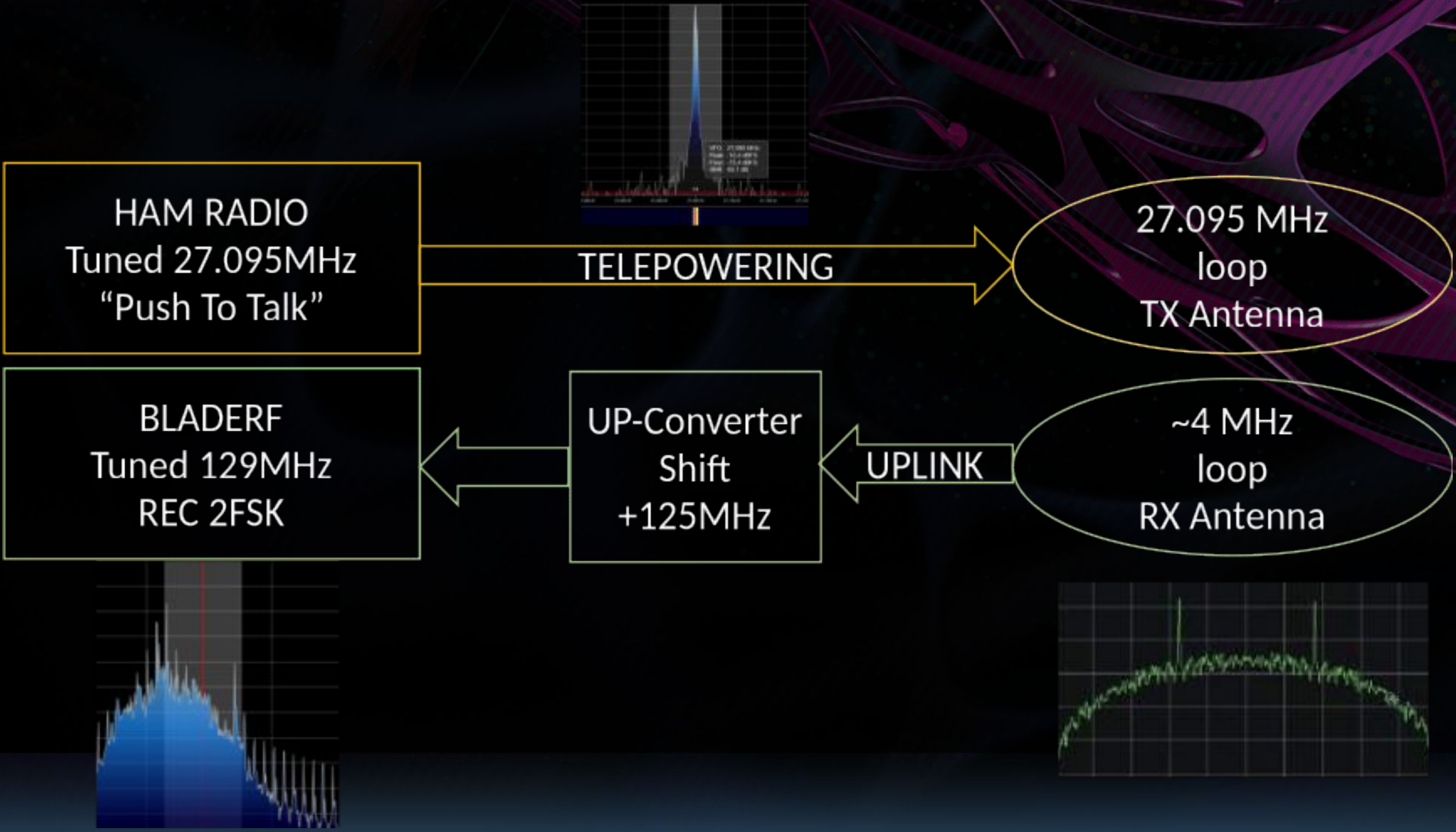



4.050.850
AIRSI
Zoom
dBFS
0
-5
-10
-15
-20
-25
-30
-35
-40
-45
-50
-55
-60
-65
-70
-75
-80
80m Ham Band
Shor…
Shortwave Broadcast
3,500 M
3,600 M
3,700 M
3,800 M
3,900 M
4,000 M
4,100 M
4,200 M
4,300 M
4,400 M
4,500 M
4,600 M
4,700 M
4,800 M
4,900 M
10



VFO: 27,095 MHz
Peak: -10,4 dBFS
Floor: -73,4 dBFS
SNR: 63,1 dB

ERTMS SNIFFER SETUP



HAM RADIO
Tuned 27.095MHz
“Push To Talk”

TELEPOWERING

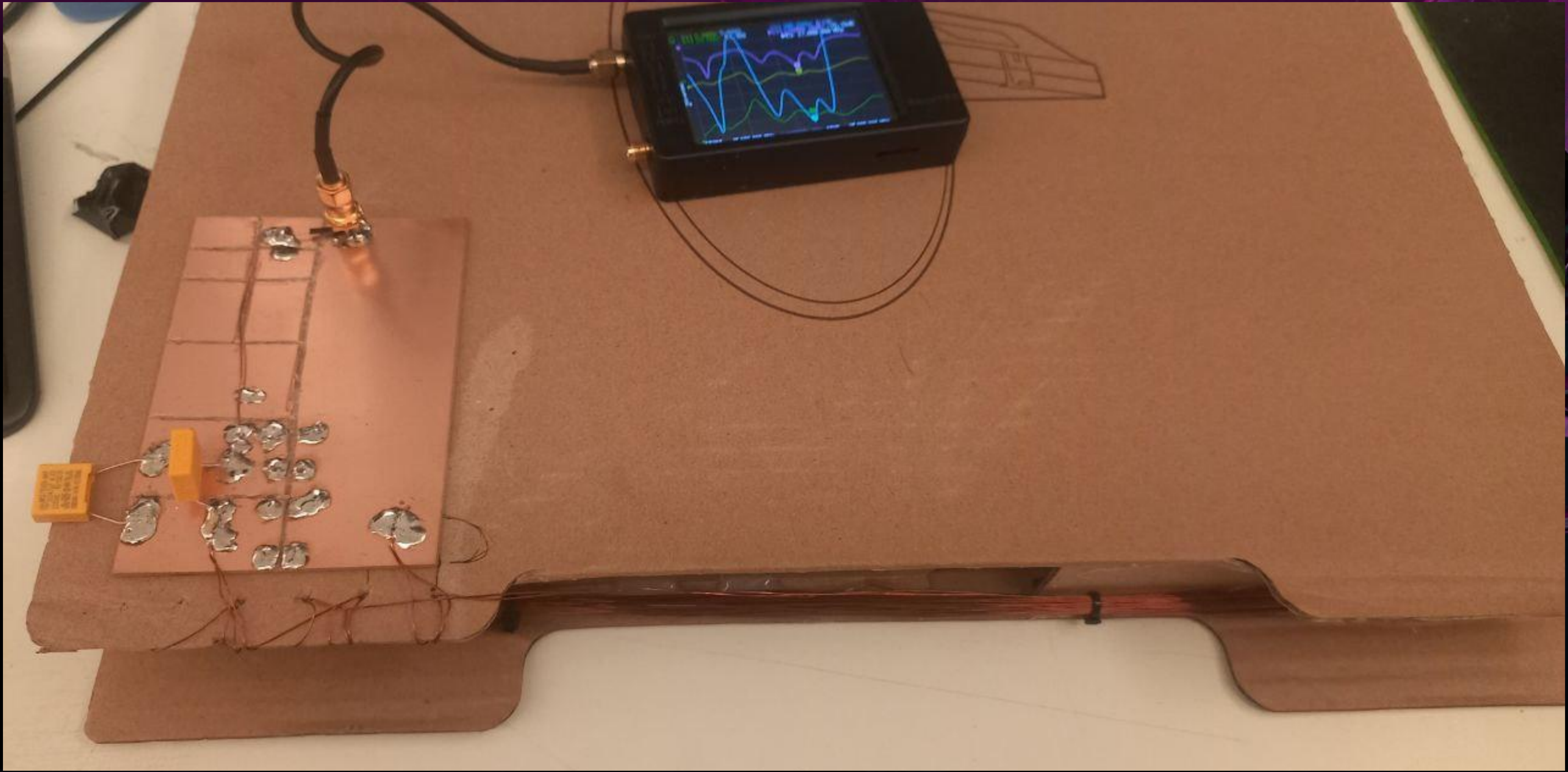
27.095 MHz
loop
TX Antenna

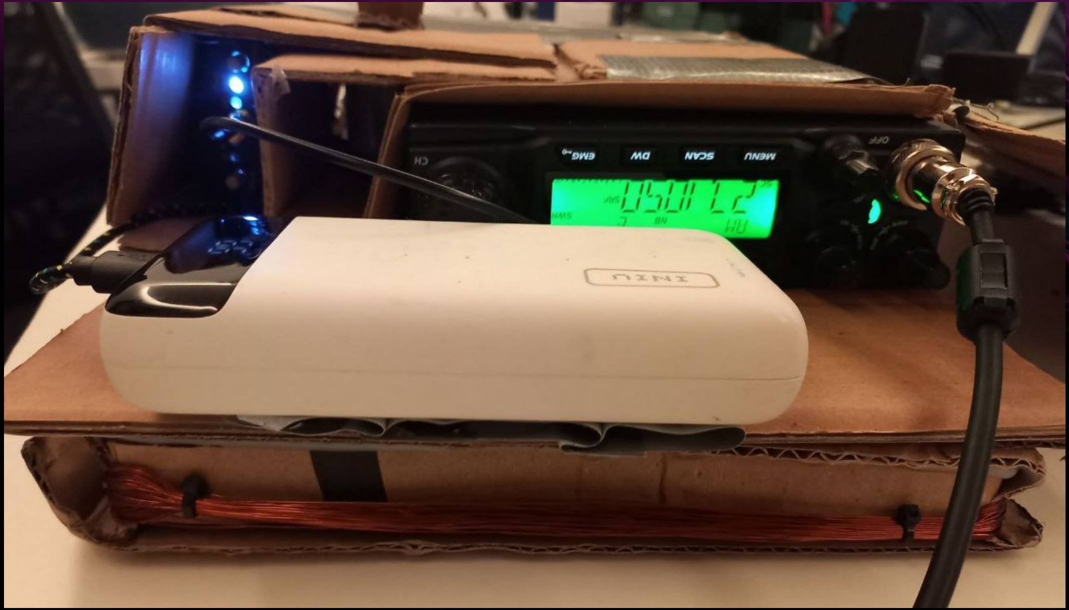
BLADERF
Tuned 129MHz
REC 2FSK

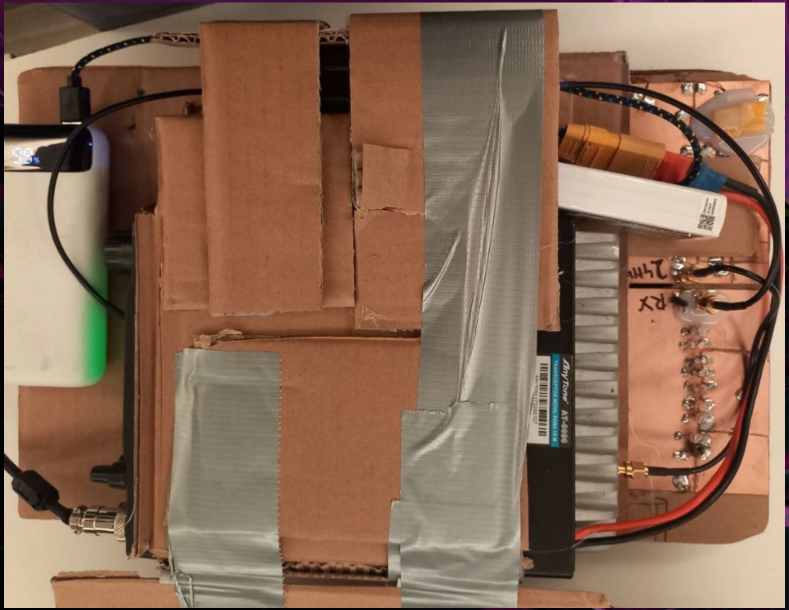
UP-Converter
Shift
+125MHz

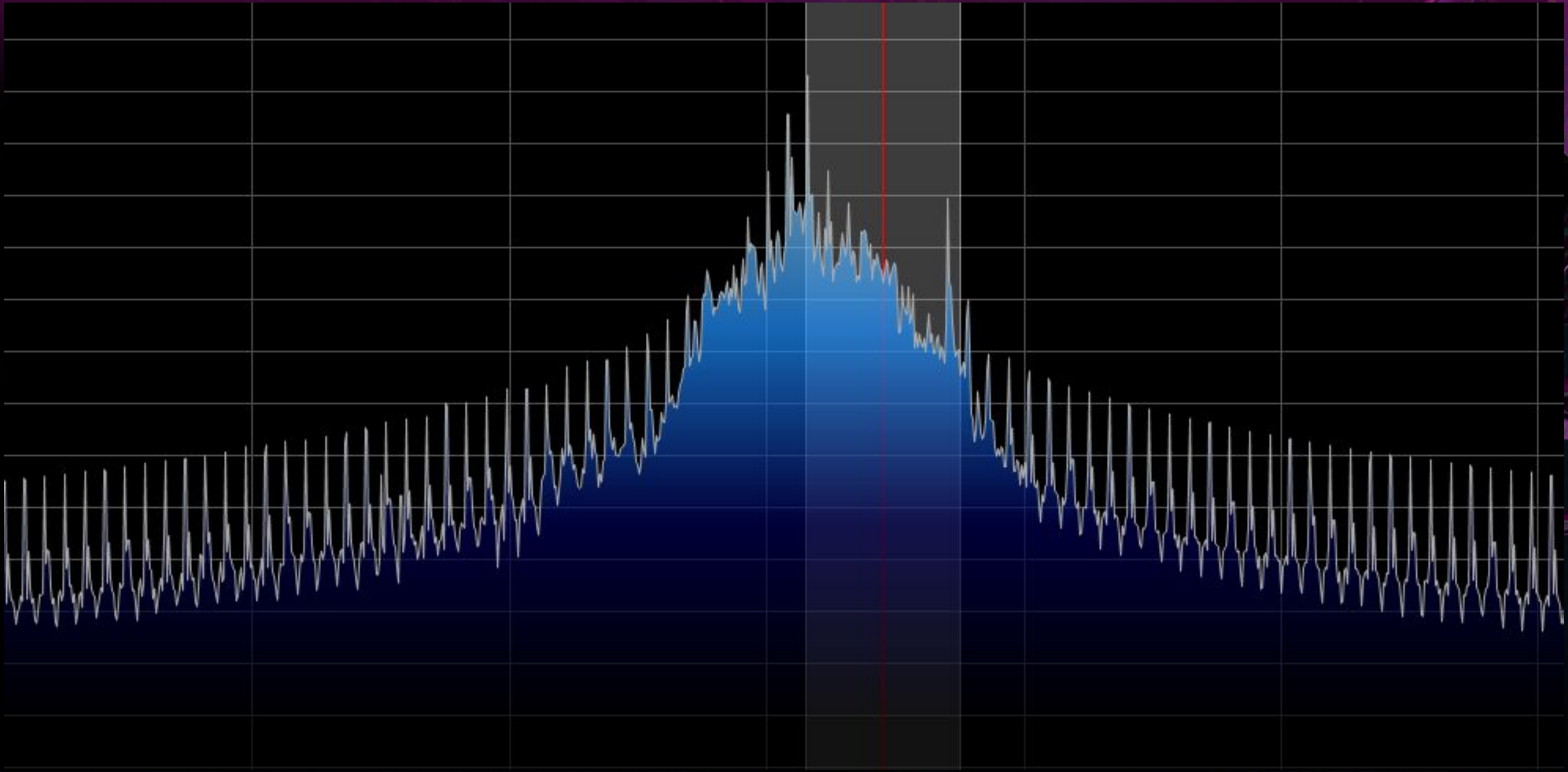
UPLINK

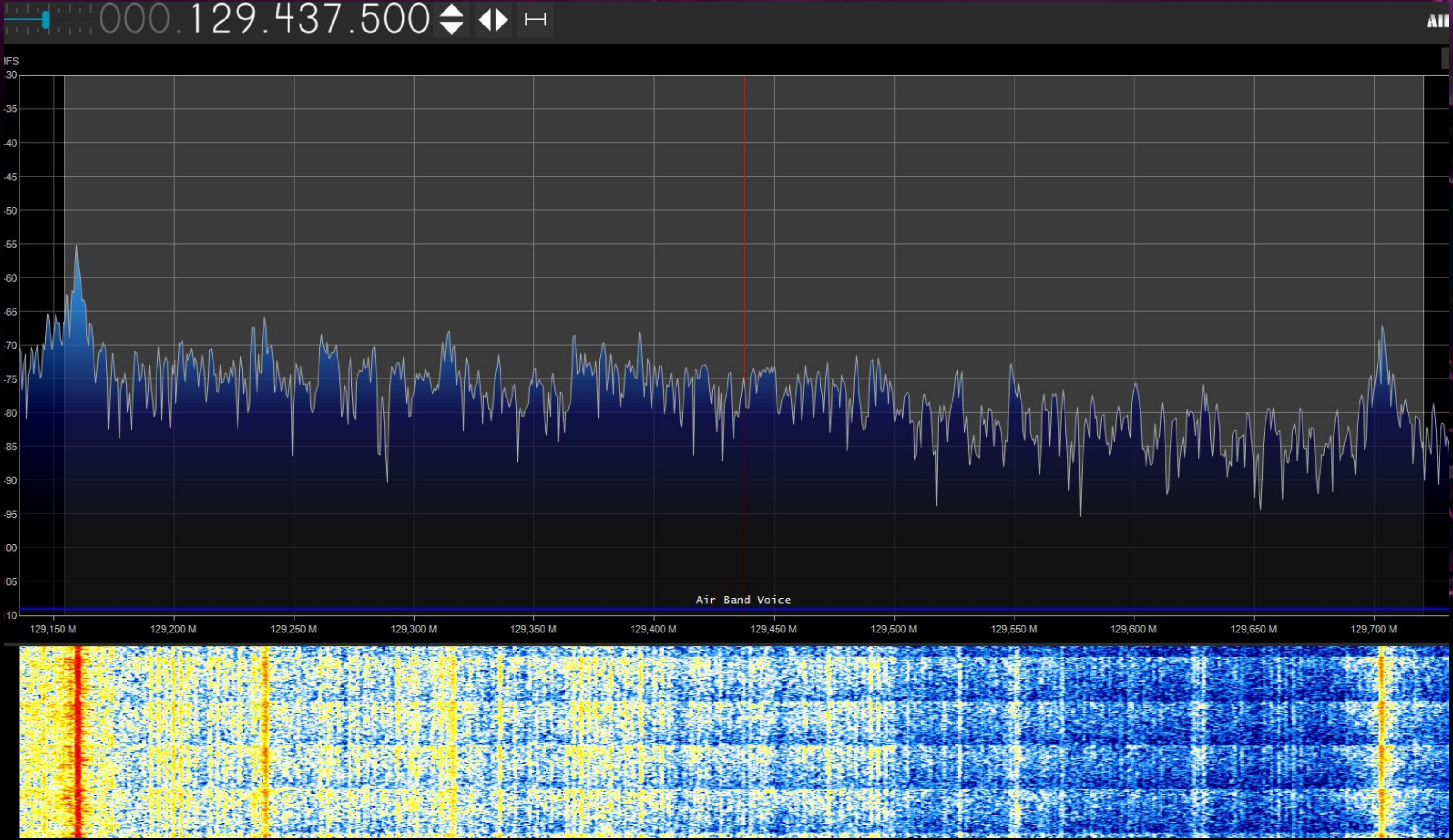
~4 MHz
loop
RX Antenna




CH
EMG
DW
SCAN
MENU
OFF
INIU


AnyTone AT-6666
24M
RX





000.129.437.500
AII
FS
-30
-35
-40
-45
-50
-55
-60
-65
-70
-75
-80
-85
-90
-95
00
05
10
Air Band Voice
129,150 M
129,200 M
129,250 M
129,300 M
129,350 M
129,400 M
129,450 M
129,500 M
129,550 M
129,600 M
129,650 M
129,700 M

Acknowledgments:

Alberto Rodriguez
RootedCON Staff, RootedCON

Jaime Esquivias
OSINT researcher expert, TechFrontiers

Joel Serna
IoT/ICS Pentest Engineer, TechFrontiers

black hat®
EUROPE 2025

DECEMBER 8-11, 2025
EXCEL LONDON / UNITED KINGDOM

Questions?

David Meléndez
RnD Engineer & Co-Founder, TechFrontiers
@TaiksonTexas

Gabriela García
Security Engineer & Co-Founder, TechFrontiers
@constrainterror
linkedin.com/in/itsgabsgarcia

Follow us on X: @_techfrontiers_

black hat®
EUROPE 2025

DECEMBER 8-11, 2025
EXCEL LONDON / UNITED KINGDOM