
DARK TERRITORY
Abusing legacy railroad signaling systems



**David Meléndez Cano**
@TaiksonTexas

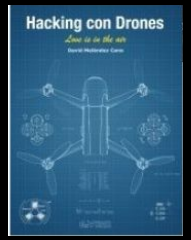
I+D & Embedded Software Engineer
Red Team en Innotec Security
Drone and Robot Builder
(Atropos & Interceptor Drones + Texas Ranger ROV)

Author of the book
"Hacking con Drones"



**Gabriela García**
@constrainterror

Security Software Developer
Hacker and hacking communities co-organizer
Coding & Cybersecurity instructor & mentor
Hardware Hacking Enthusiast



# DARK TERRITORY

In the railway sector, "dark territory" refers to a section of railway track that lacks remotely controlled railway signals or automatic block systems. In these areas, communication and coordination of train traffic rely exclusively on railway operators through radio communication and other non-automated methods, instead of using electronic signals or automated control systems to manage the safety and movement of trains.

The term has also gained popularity outside the railway context, especially in popular culture and information technology, to describe areas or sectors that lack supervision, regulation, or control, often symbolizing an environment of uncertainty, danger, or lack of control.


REC
FUN WITH
trains

Railway Block: A block is a section of railway track in which normally no more than one train can be present at a time, in order to prevent a collision between two trains.



Block Section Between Stations: a section of railway track in which normally no more than one train can be present at a time, in order to prevent a collision between two trains



Block Section Between Signals: A block section between signals is a section of railway track in which normally no more than one train can be present at a time, in order to prevent a collision between two trains.





# Axle Counter

**A railway axle counter is a system of sensors installed on train tracks to detect and count the axles of the train cars.**



Fun with trains

# Track Blocking

**A procedure by which the movement of trains on a track in a specific direction is authorized.**

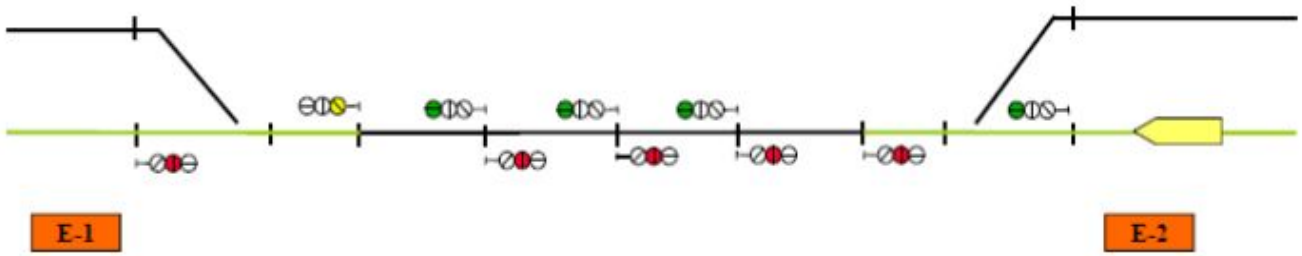


Token Block


Telephone Block

Fun with trains

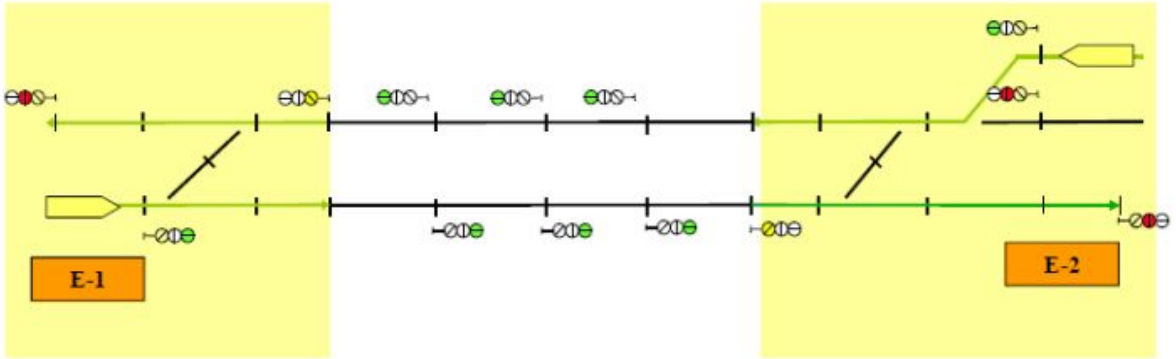
# Electronic Track Blocking




Automatic Blocking on Single Track (B.A.U.)

Fun with trains

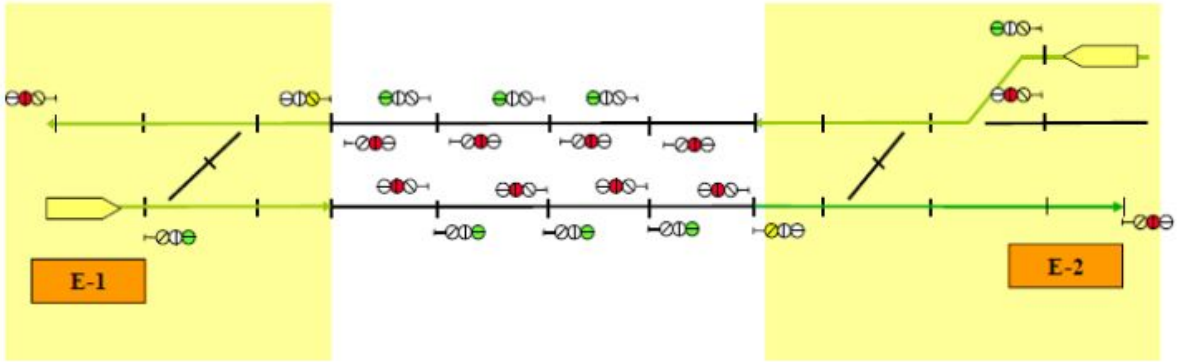
# Electronic Track Blocking




Automatic Blocking on Double Track (B.A.D.)

Fun with trains

# Electronic Track Blocking




Bidirectional Automatic Blocking (B.A.B.)

Fun with trains

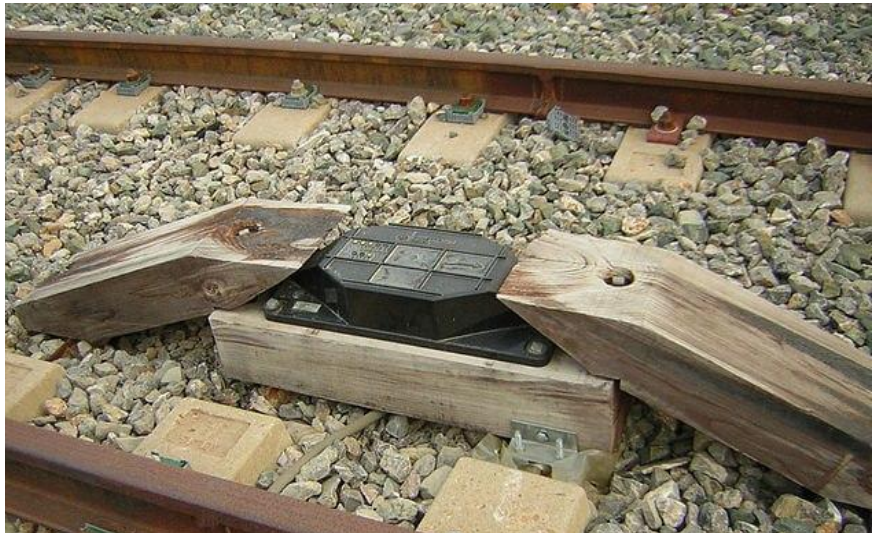
# Centralized Traffic Control




Fun with trains

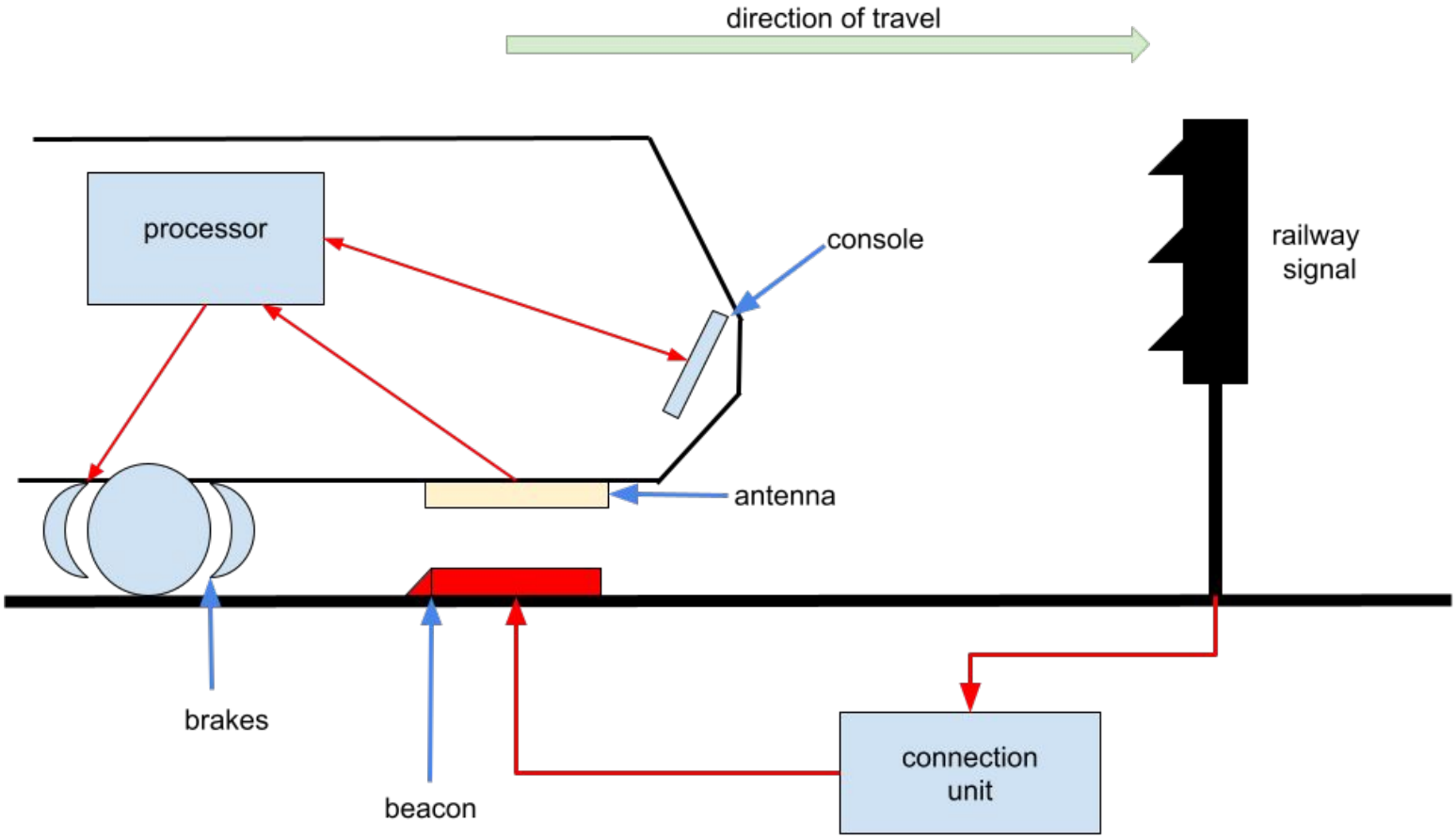
# ASFA (Anuncio de Señales y Frenado Automático)
## *Announcement of Signals and Automatic Braking*

**This is the oldest support system for train circulation and is installed on almost the entire Spanish railway network. It is designed to reduce human errors. The system is based on a coil-capacitor circuit connected to the signal, which, depending on the signal aspect, transmits one frequency or another to the onboard equipment.**





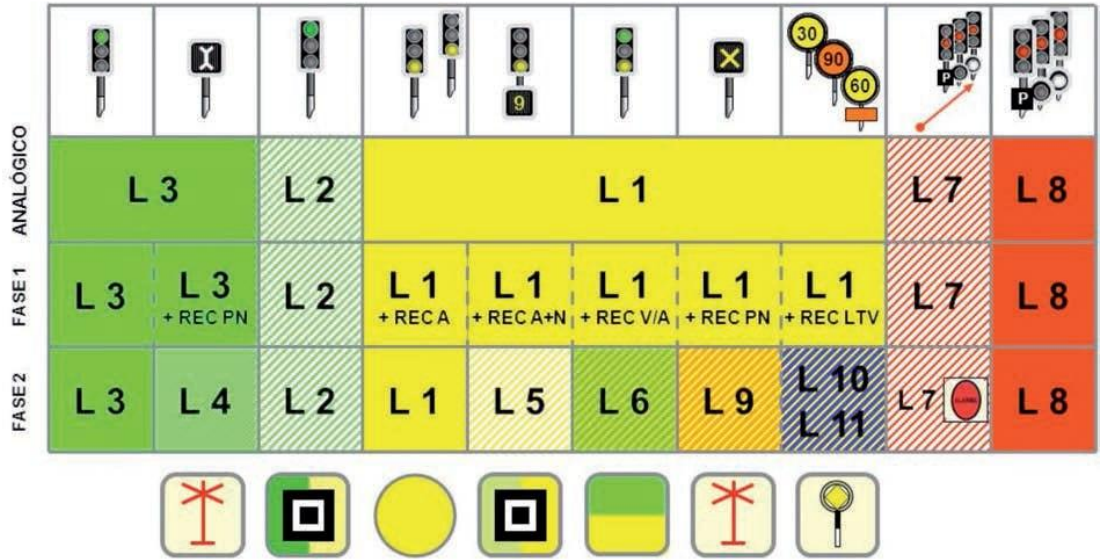
Fun with trains


direction of travel
processor
console
railway signal
antenna
brakes
beacon
connection unit

# ASFA - Types

Beacons with Fixed Aspect - Example: Level Crossing Beacon

Beacons with Variable Aspect - Example: Signal Beacon

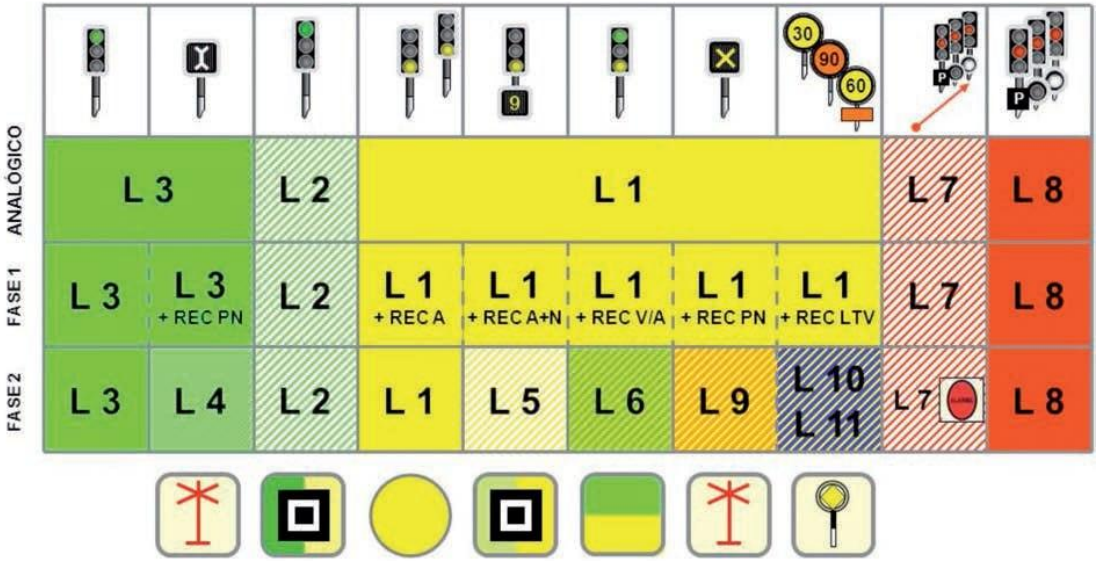


# ASFA - Signal Frequencies

## 6.2. Frecuencias utilizadas en el sistema A.S.F.A.

Las frecuencias actualmente utilizadas son las siguientes:

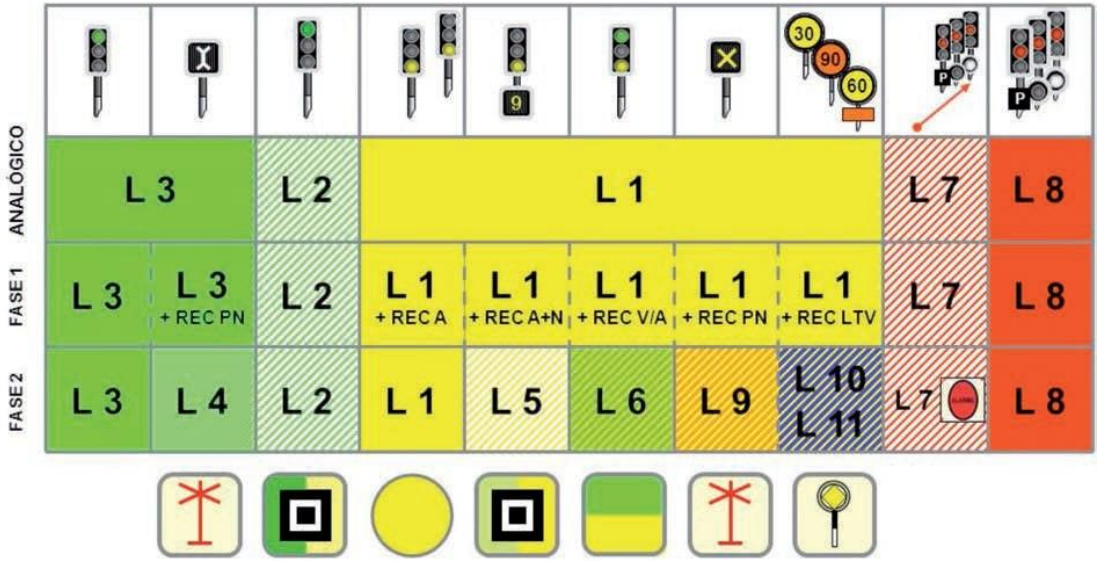
| | |
|---|---|
| L1—AMARILLO; VERDE-AMARILLO; AMARILLO DESTELLANTE | 60.000 Hz. |
| L2—VERDE DESTELLANTE | 64.020 Hz. |
| L3—VERDE | 68.310 Hz. |
| L7—CONTROL DE VELOCIDAD | 88.540 Hz. |
| L8—ROJO | 95.500 Hz. |




Fun with trains

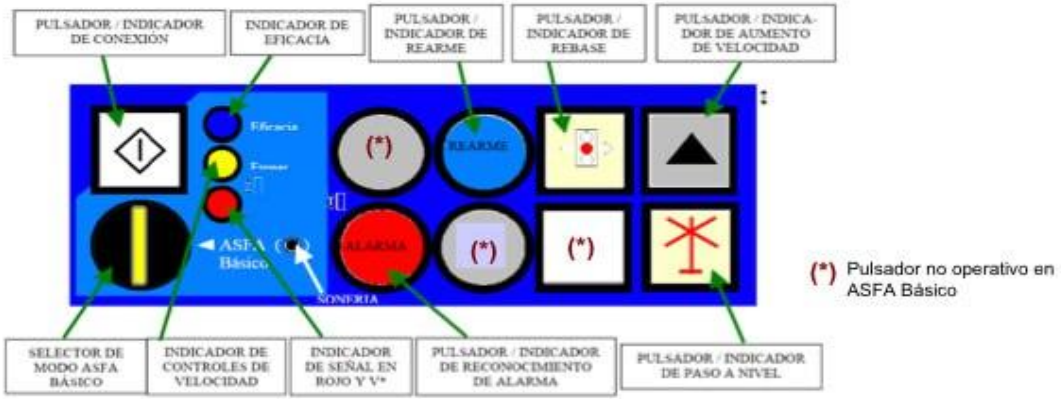
# ASFA (Anuncio de Señales y Frenado Automático) - *Announcement of Signals and Automatic Braking*

**Problem 1 - In Analog ASFA, the Same Aspect (e.g., L1 or L3) Indicates Multiple Signals**



# ASFA - What the Train Driver Sees

## Panel ASFA Digital




## Pulsadores adicionales de reconocimiento




**L1:** Anuncio de parada, anuncio de parada inmediata, preanuncio de parada, anuncio de precaución, paso a nivel desprotegido, anuncio de limitación temporal de velocidad.

Fun with trains

# ASFA - Lo que ve el maquinista




DARK TERRITORY

DN NAVARRA ACTUALIDAD DEPORTES OPINIÓN CULTURA Y OCIO VIVIR SERVICIOS DN Iniciar Sesión Suscríbete



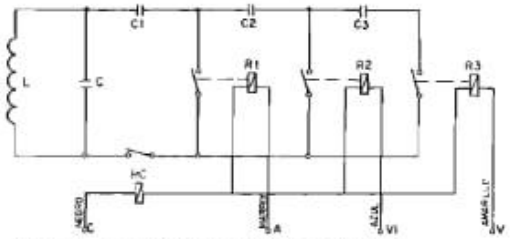
# Uharte Arakil: 25 años del mayor desastre ferroviario de Navarra

**El intercity 'Miguel de Unamuno' descarriló en Uharte Arakil con 248 pasajeros, de los que 18 fallecieron. La tragedia marcó a una generación**

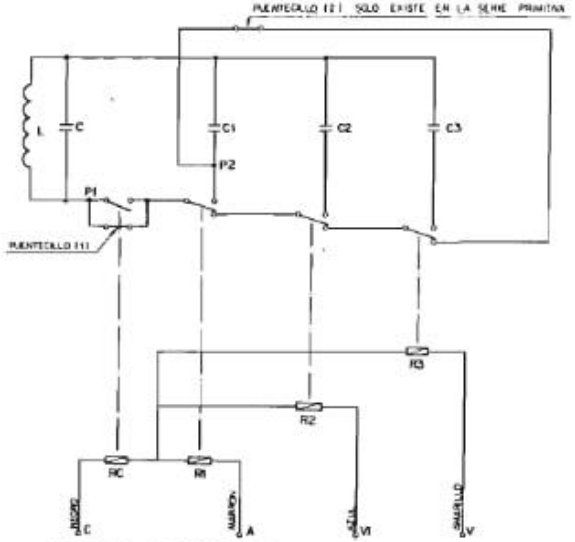


CIRCUITOS TIPICOS DE BALIZAS

Fig. 2




a) BALIZAS DE FONDO ROJO O CONTROL DE VELOCIDAD



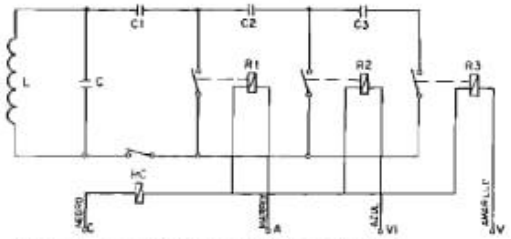

b) BALIZAS DE FONDO DOBLE

NOTA.- En las balizas de fondo doble que no son de la serie primitiva están unidos los puntos P1 y P2 con tan sólo el puentecillo (1), coincidiendo el punto P1 con la posición de un contacto en reposo de RC y no pasando el camino hacia P2 por los contactos de R1, R2 y R3.

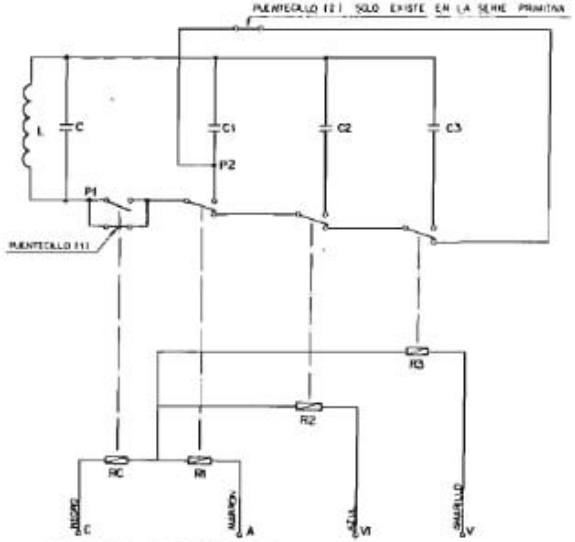


CIRCUITOS TIPICOS DE BALIZAS

Fig. 2



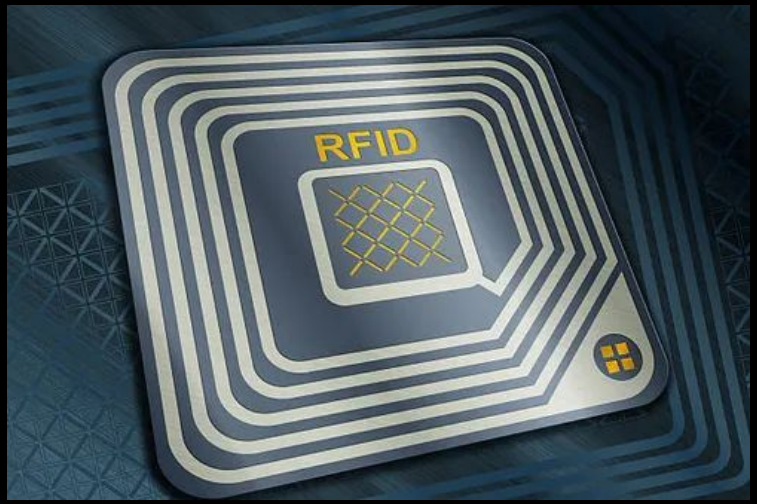

a) BALIZAS DE FONDO ROJO O CONTROL DE VELOCIDAD



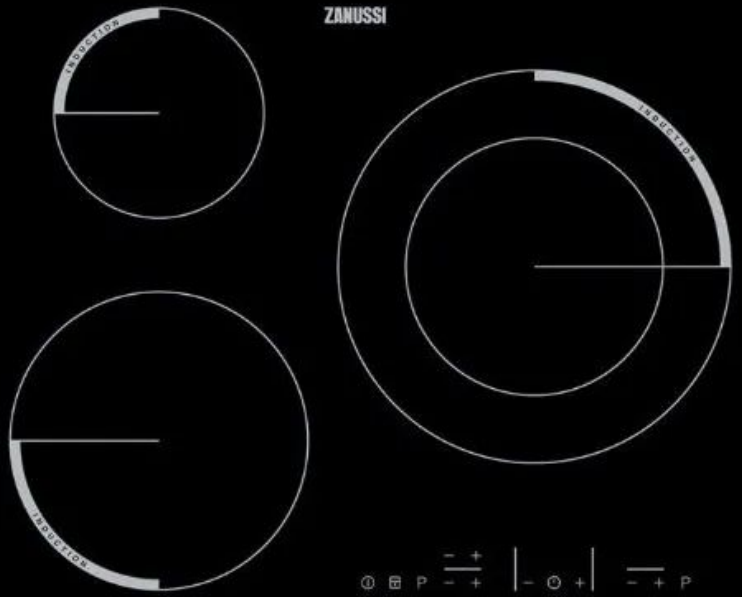

b) BALIZAS DE FONDO DOBLE

NOTA.- En las balizas de fondo doble que no son de la serie primitiva están unidos los puntos P1 y P2 con tan sólo el puentecillo (1), coincidiendo el punto P1 con la posición de un contacto en reposo de RC y no pasando el camino hacia P2 por los contactos de R1, R2 y R3.

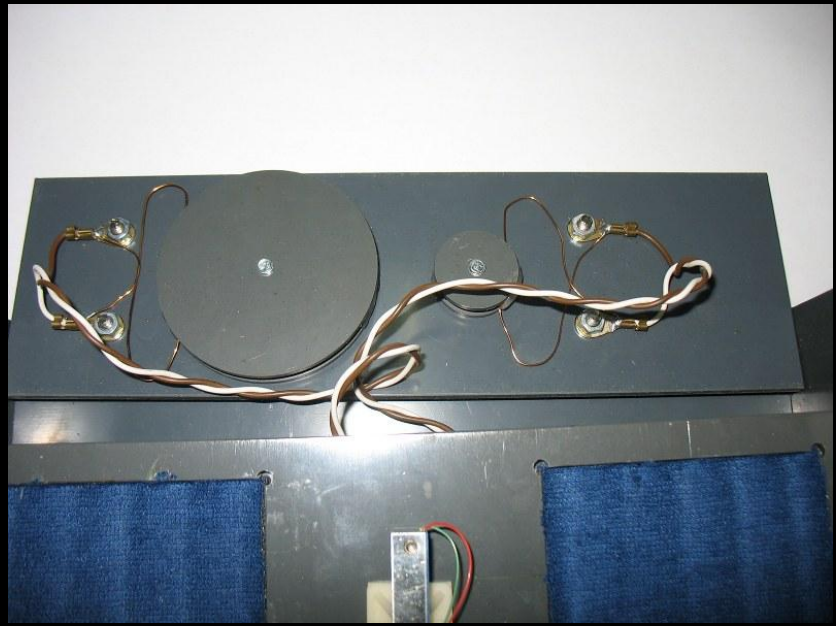



RFID




ZANUSSI


ON/OFF
Equipo
Comprobador
Balizas
CARGADOR
SEÑAL
LED
DME TRONIC

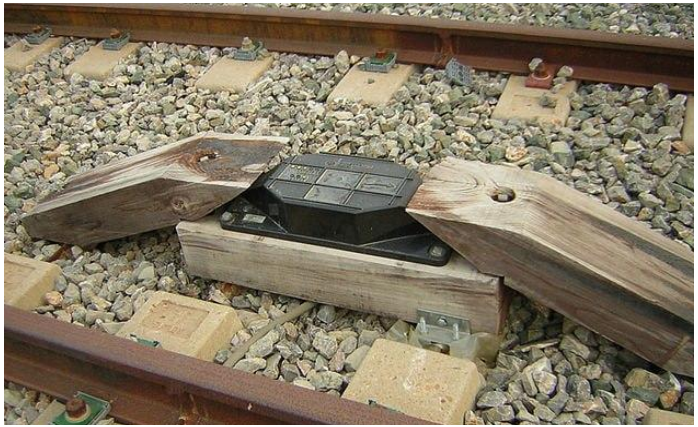


Possible Attacks:

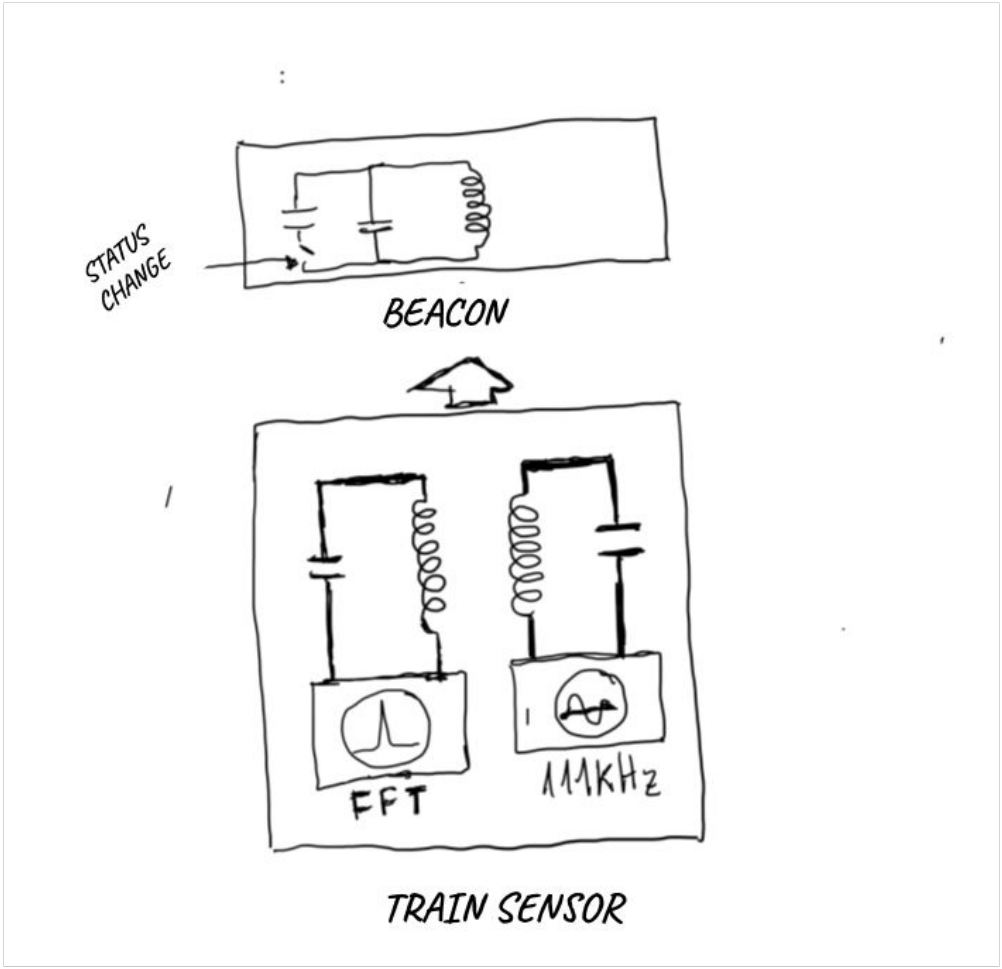
- Use a circuit with a coil and capacitor to induce the frequency we want the train to pick up to emulate a beacon.
- Replicate the beacon.

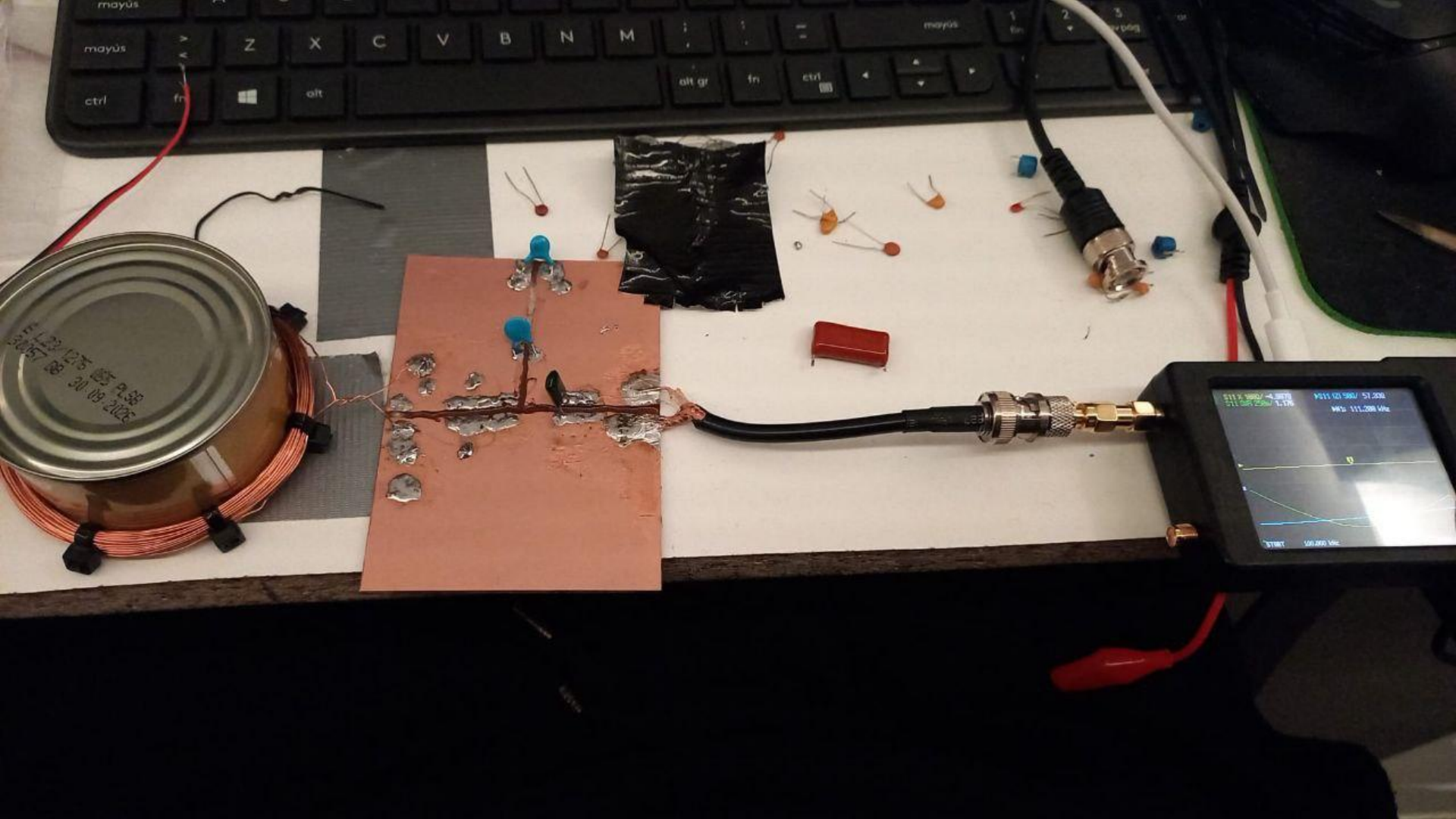
Requirements:

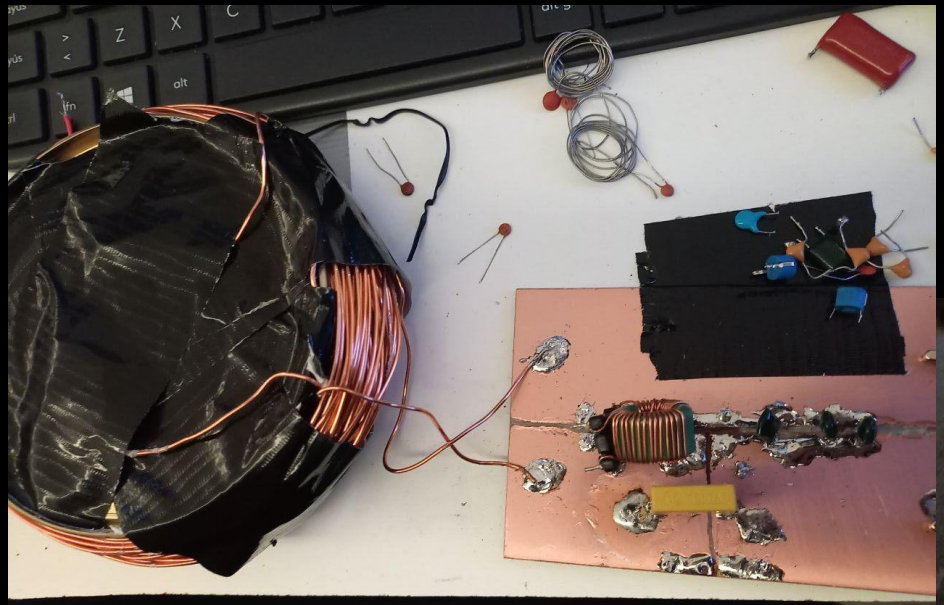
- Inductance of the coil
- Capacitance of the capacitor






STATUS
CHANGE
BEACON
FFT
111KHz
TRAIN SENSOR






S11 X 100Ω/ 13.68Ω
S11 SWR 250m/ 1.580
▶S11 IZI 500/ 75.89Ω
▶M1: 74.050 kHz
START 50.000 kHz
bw:1000Hz 101p STOP 115.000 kHz

AND WHAT IF . . .


production line and onto the feet
reputation for durability has become fo
in making things to last is as strong as it's eve


PORT 1
S11
+10dBm RF
10VDC Max
S21
PORT 2
S11 X 1000/ 14.98Ω
S11 |Z| 50Ω/ 72.46Ω
S11 SWR 250m/ 1.535
S21 LOGMAG 10dB/ -86.66dB
M1: 95.360 kHz
START 50.000 kHz
BW 1000Hz
STOP 122.000 kHz

# Thank You!

Acknowledgments:

Irene Cotillas

Pablo Trujillo

Matías

Pedro Candel (Saur0n)

@TaiksonTexas

@constrainterror