UNIVERSITY OF PASSAU

# Security-Analyse der Eurobalise

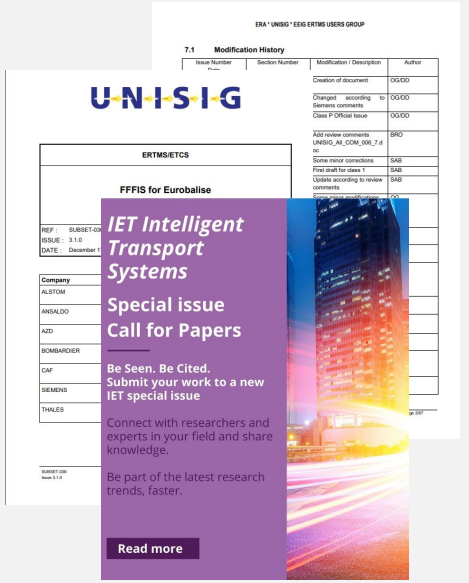
DRSS
Digital Rail Summer School

*Alexander Braml*
*Andreas Weber*
*Ilnaz Tayebi*
*Jannes Mennenga*
*Lukas Knobel*

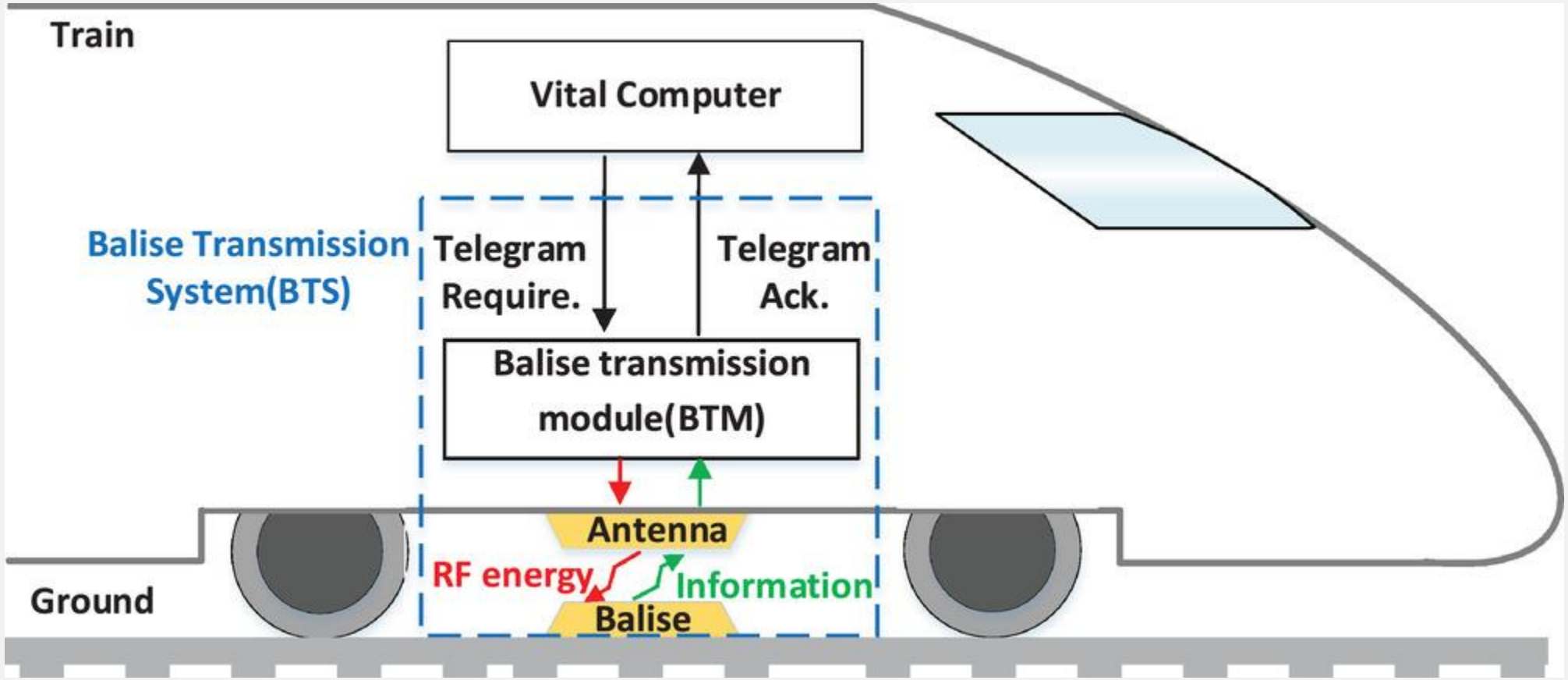
***Betreuer: Simon Unger***

# Artefacts


HackRF One
GREAT SCOTT GADGETS

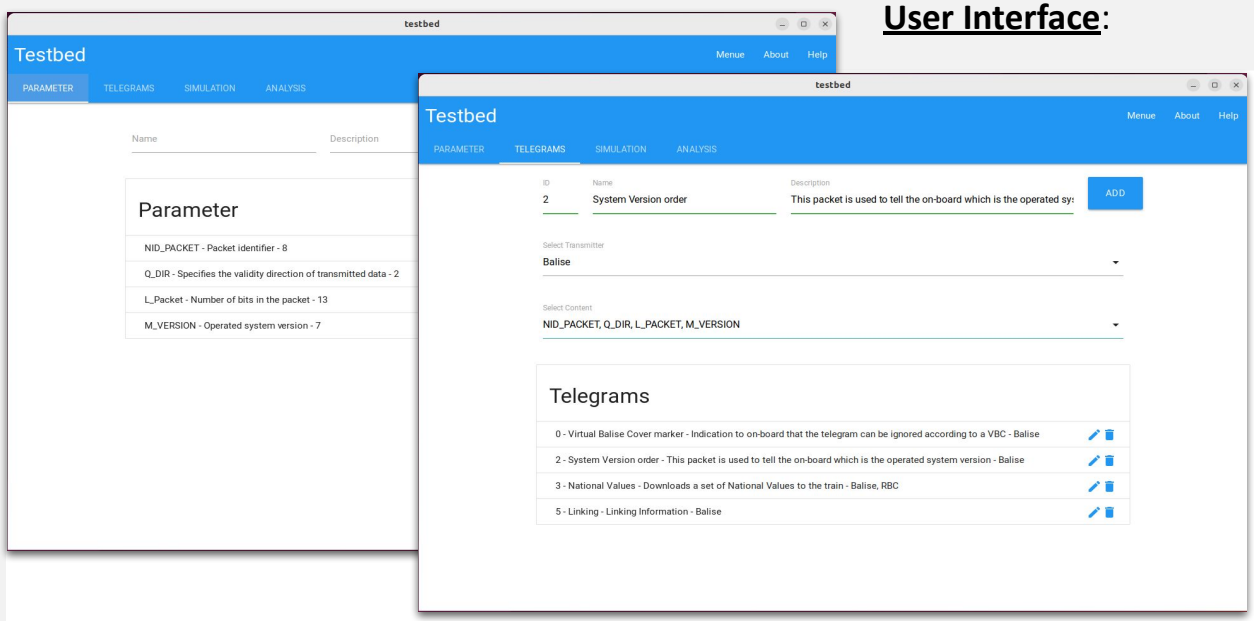

ERA * UNISIG * EEIG ERTMS USERS GROUP
7.1 Modification History
UNISIG
ERTMS/ETCS
FFFIS for Eurobalise
IET Intelligent Transport Systems
Special issue
Call for Papers
Be Seen. Be Cited.
Submit your work to a new IET special issue
Connect with researchers and experts in your field and share knowledge.
Be part of the latest research trends, faster.
Read more

# EU Train Control System (ETCS)

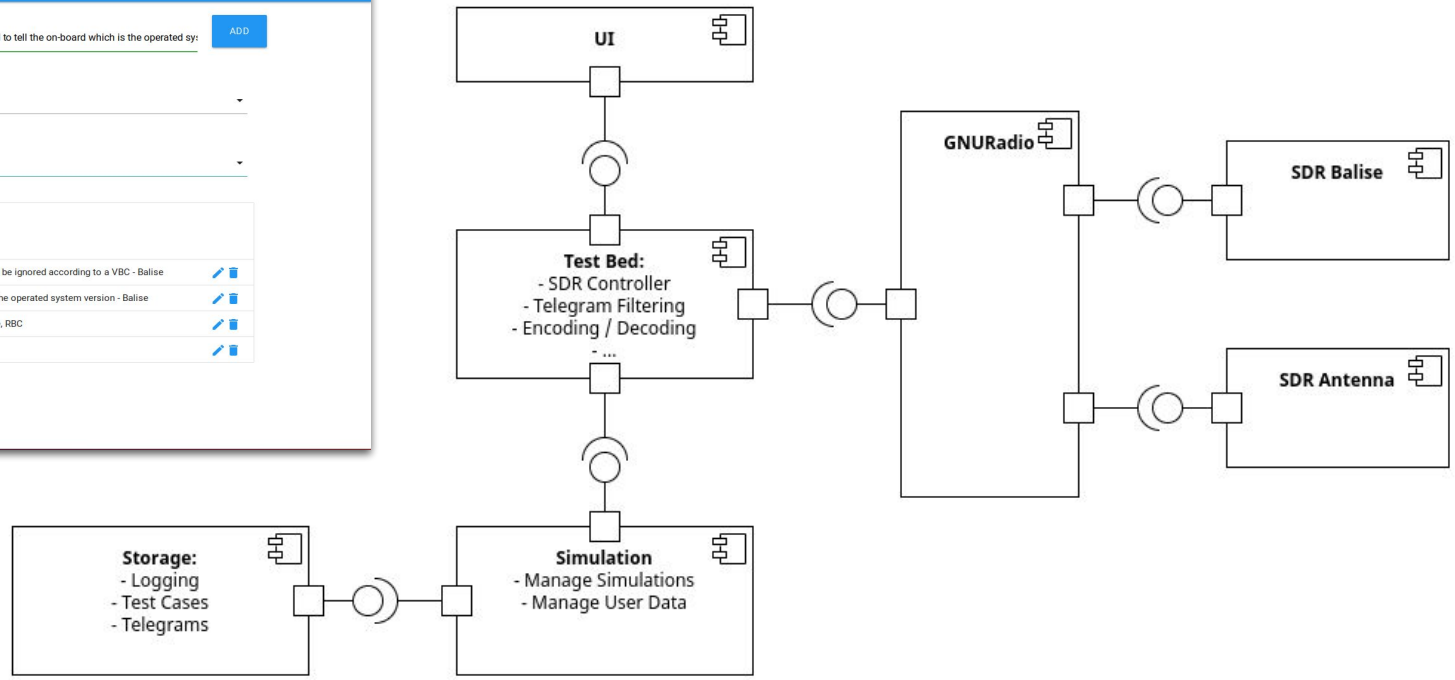


# Implementation of Testbed

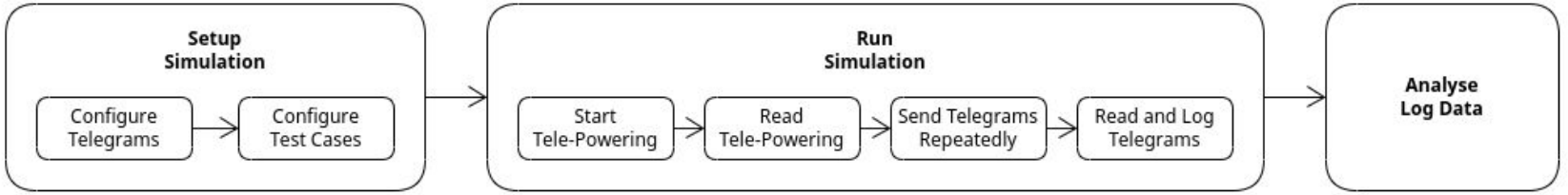
**User Interface**:




**Architecture**:

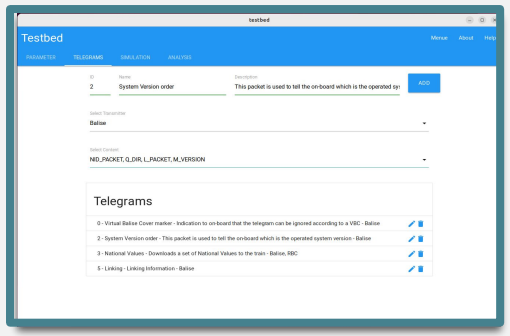



**Workflow**:



# Planned Setup

Software Testbed

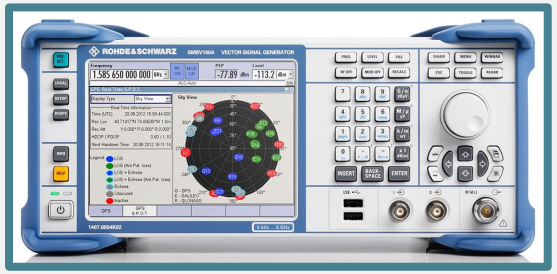



Python Interface of GNU-Radio


FSK

PWM Signal

Signal Generator




HF Linear Amplifier

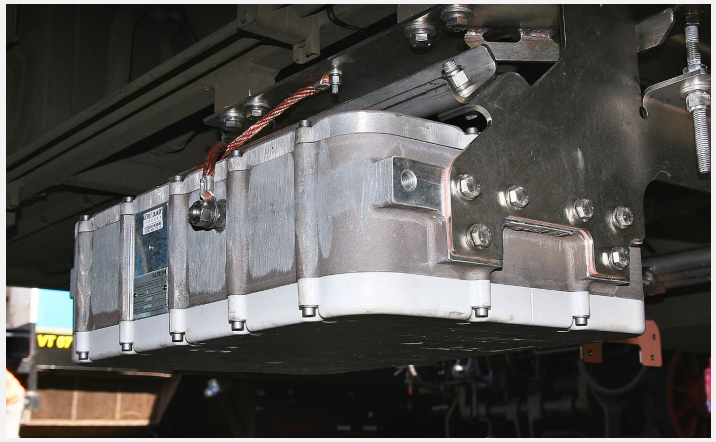
Inductor Coil

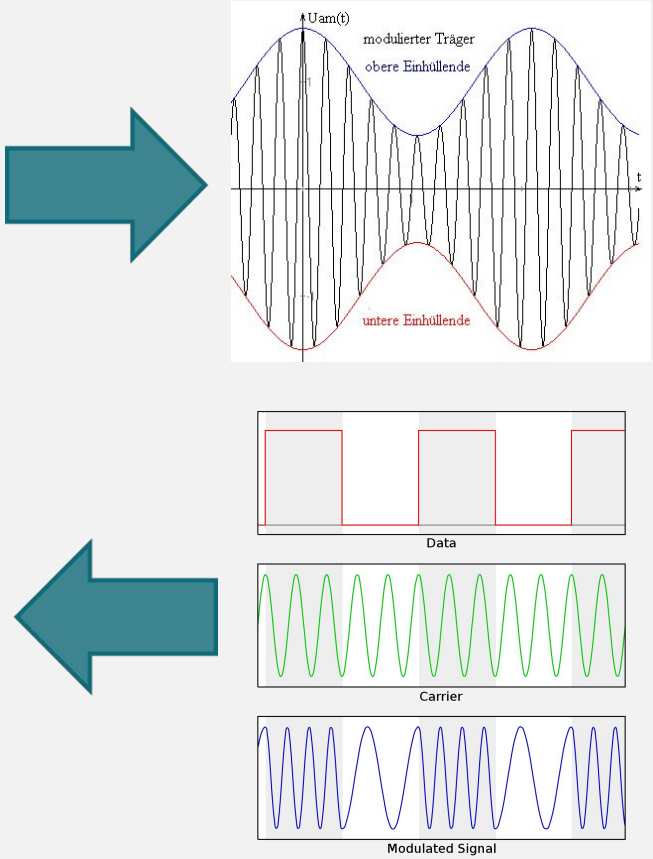
AM

Inductive Powering

# Communication between Balise and BTM Antenna

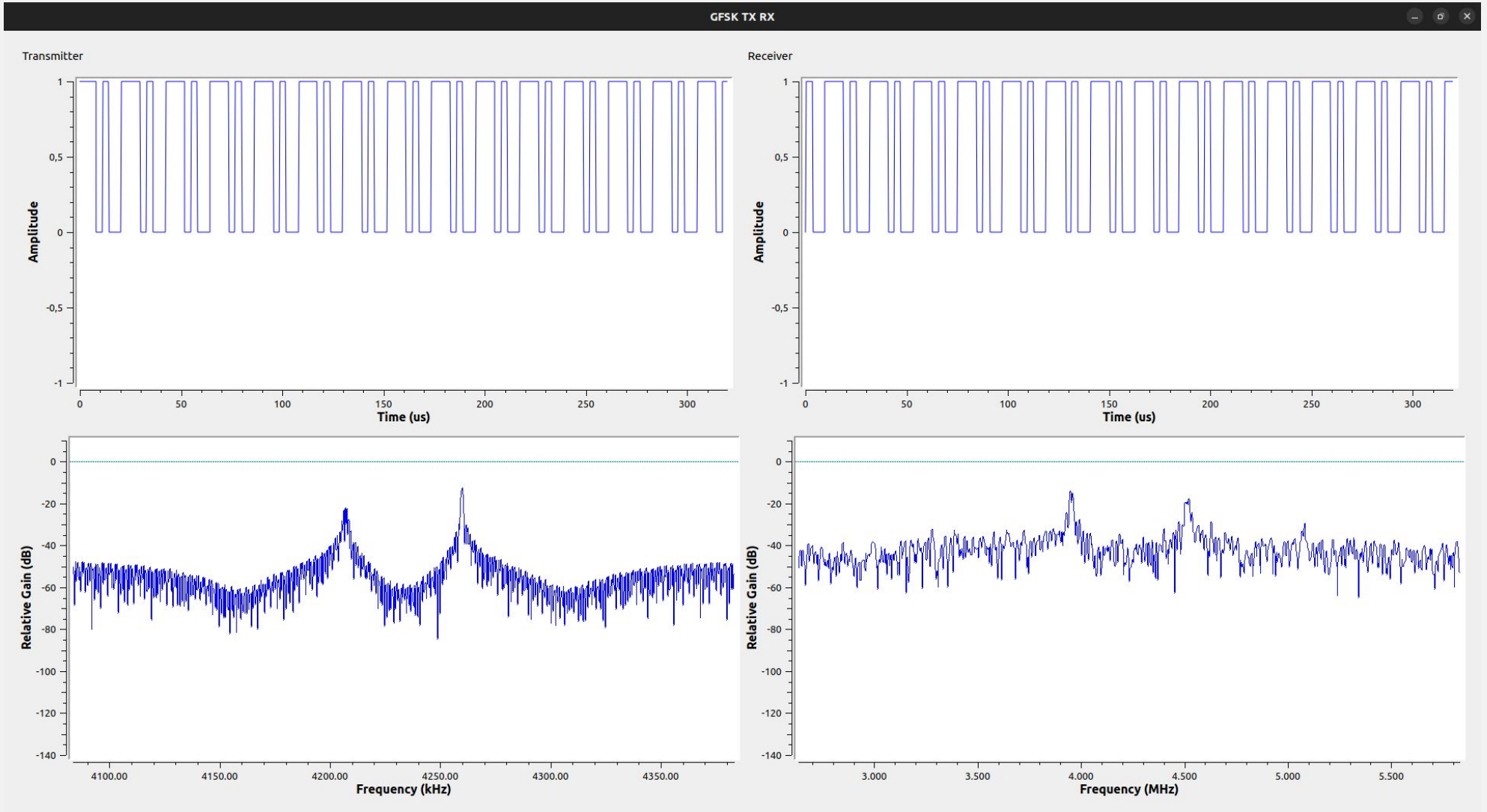
**Amplitude Modulation (AM) for Downlink**
**27.095 MHz inductive powering**



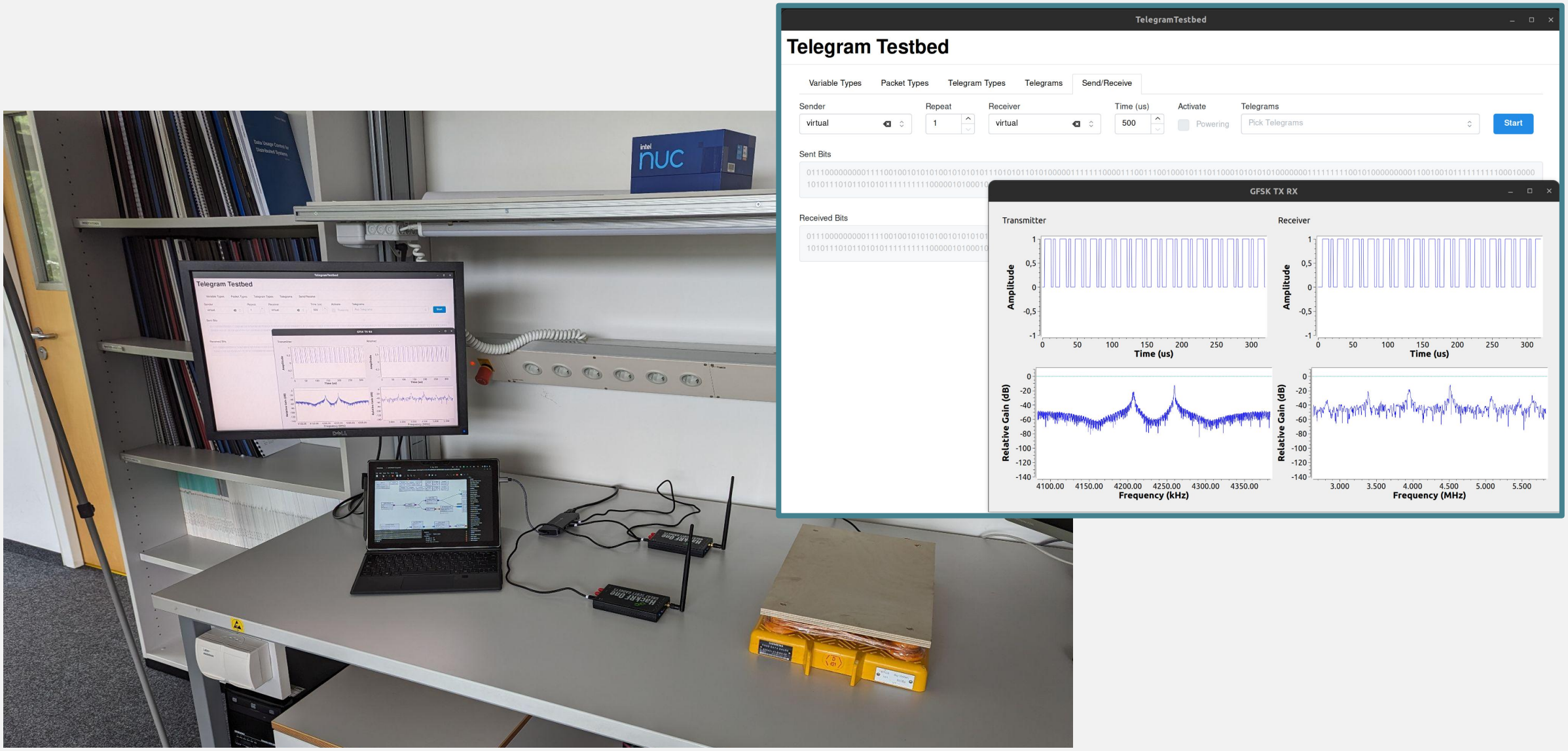



**Frequency Shift Key Modulation (FSK) for the Uplink**
**3.951 MHz for 0, 4.516 MHz for 1**

# Emulation of Balise and BTM Antenna



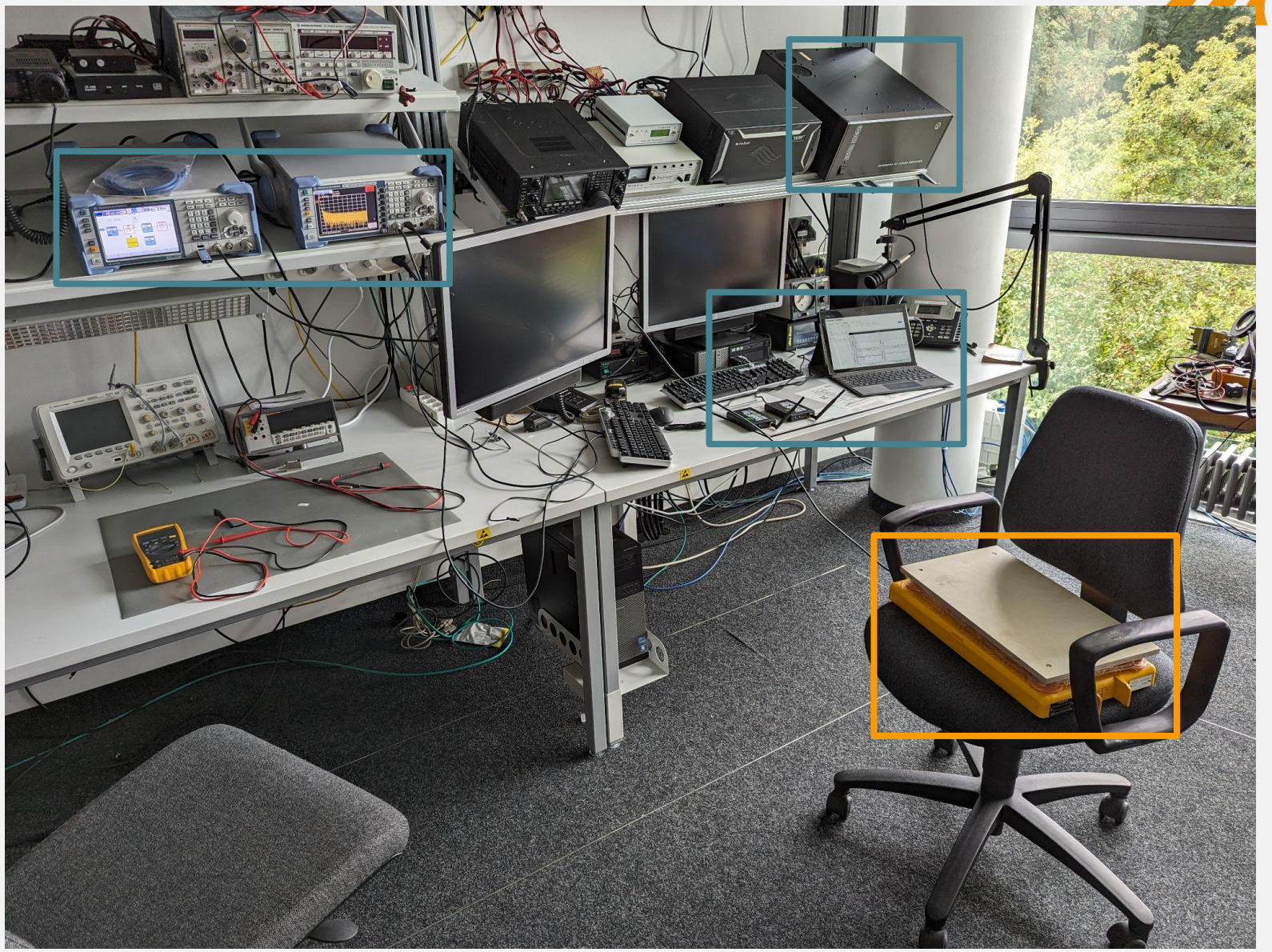
# Emulation of Balise and BTM Antenna



# Challenges

- **Setup for Powering the Balise**
  - Handling and filtering noise
  - Handling legal and technical restrictions
  - Constructing a fitting antenna
- **Lack of …**
  - Data to simulate air-gap noise
  - Publicly available documentation
  - Knowledge about the field and equipment

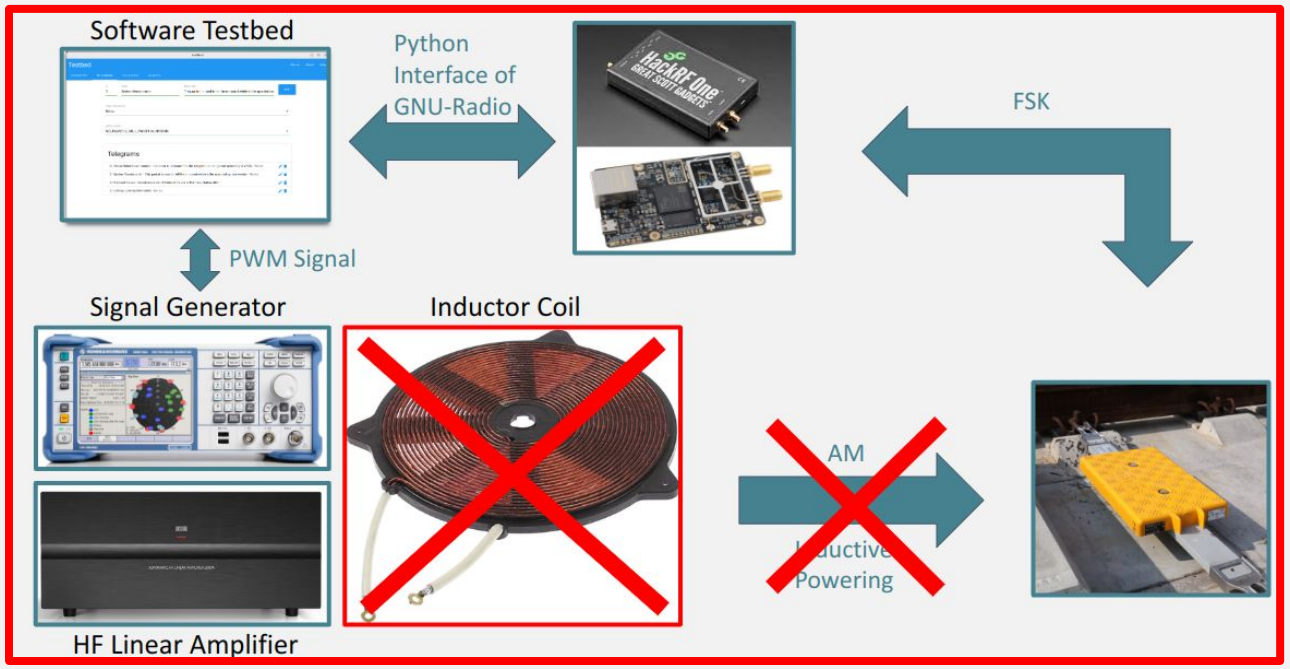
# Final Setup

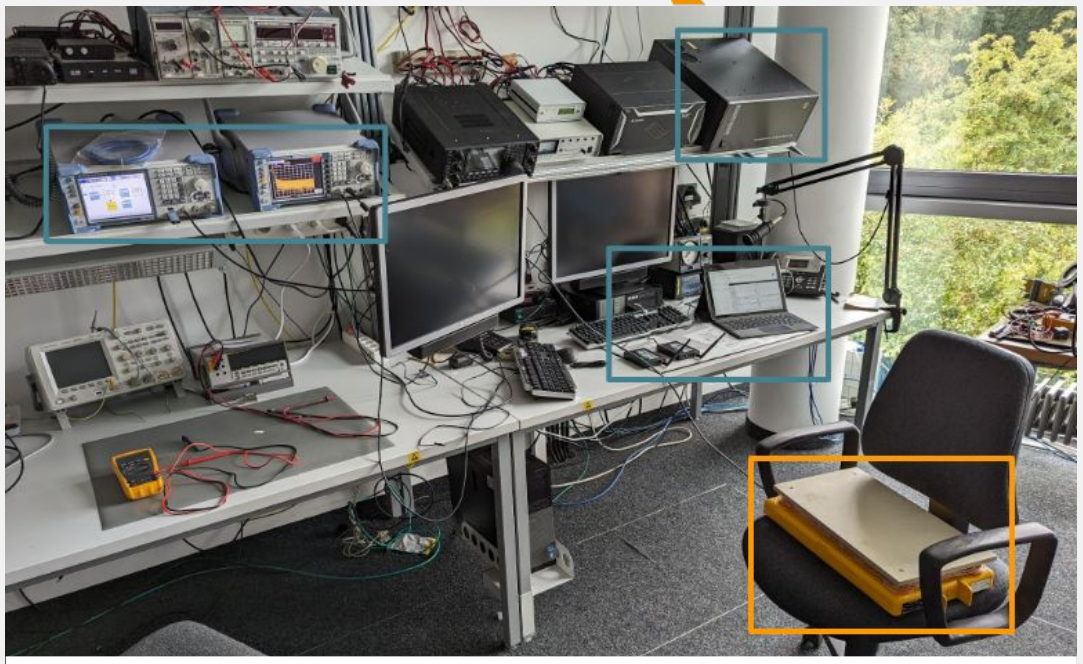


# Results

**Reading the Balise only with SDRs is not possible**

- Fitting equipment
- As well as knowledge in the field is necessary



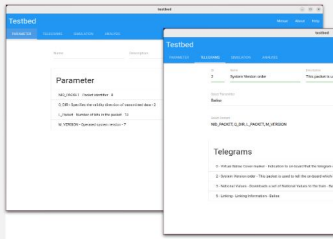



# Thank you!

UNIVERSITY OF PASSAU

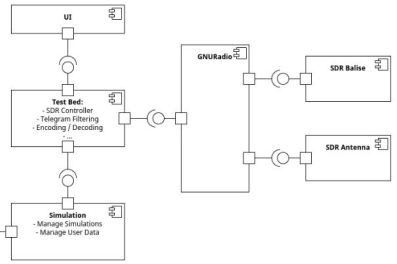
## Implementation of Testbed

UNIVERSITY OF PASSAU

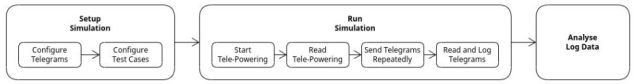



**User Interface:**

**Architecture:**



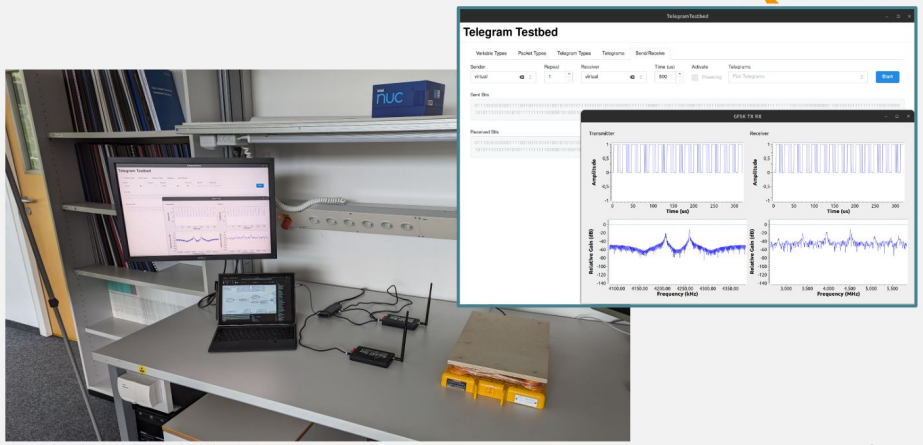

**Workflow:**






## Emulation of Balise and BTM Antenna

UNIVERSITY OF PASSAU






## Task 6: Final Setup

UNIVERSITY OF PASSAU

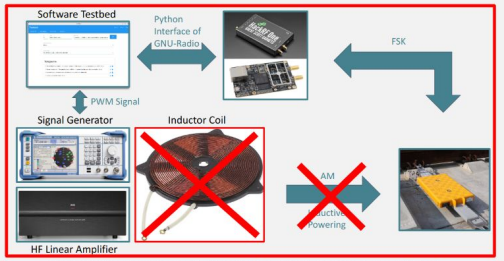


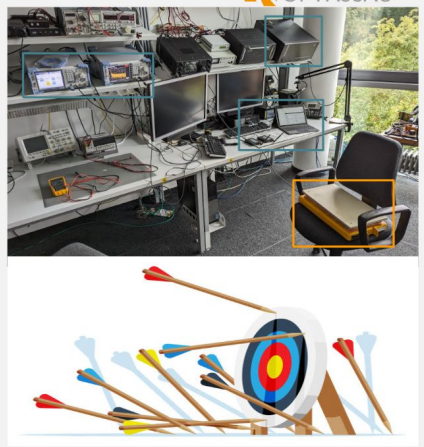
## Results

UNIVERSITY OF PASSAU

**Reading the Balise only with SDRs is not possible.**

- Fitting equipment
- As well as knowledge in the field is necessary.



# Literature


**[1]** Modelling and performance analysis of Balise under dynamic energy harvesting in high-speed railway, Li et. al, 2022

**[2]** Modeling and Simulation of Balise Up-Link Data Transmission Based on Finite Element Method, Zhao et. al, 2012

**[3]** Position Manipulation Attacks to Balise-Based Train Automatic Stop Control, Wu et. al, 2018

**[4]** Vulnerabilities, Attacks, and Countermeasures in Balise-Based Train Control Systems, Wu et. al, 2016

**[5]** Modeling and Data Analysis of the Balise System, Zhang et. al, 2018

**[6]** Archived - Set of specifications 3 (ETCS B3 R2 GSM-R B1)