GNSS Jamming Detection and Mitigation in the EPCIP Framework

ICG WG-A, Vienna 10 June 2015
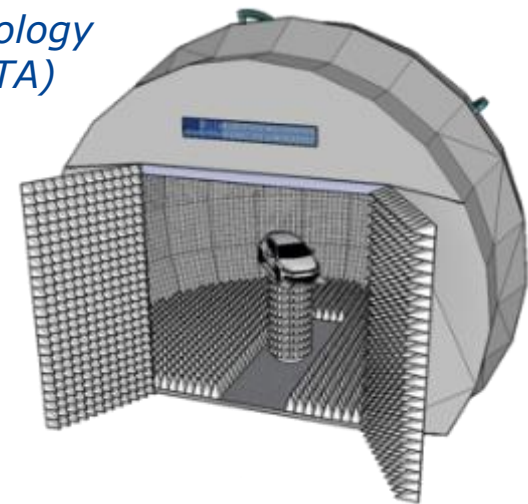**Daniele Borio**

Security Technology Assessment (STA) Unit

Joint Research Centre (JRC)

European Commission

Ispra, Italy

The European Commission's in-house science service
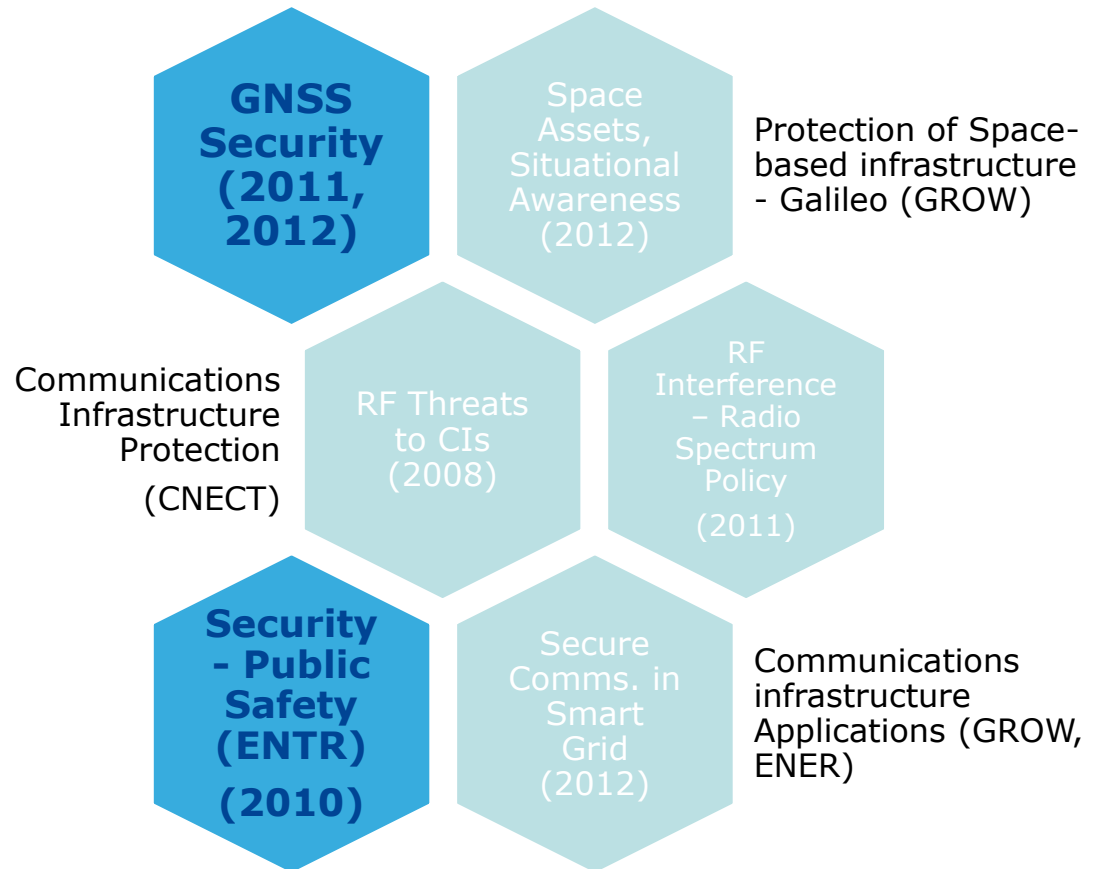
Protection of Critical Infrastructures

EPCIP: European Programme for Critical Infrastructure Protection

funded by DG HOME
(European Commission)

Several critical sectors

transport, energy, space, communications, GNSS, …

GNSS related projects:
EPCIP 2010, 2011 and **2012**

GNSS Security (2011, 2012)

Space Assets, Situational Awareness (2012)

Protection of Space-based infrastructure - Galileo (GROW)

Communications Infrastructure Protection (CNECT)

RF Threats to CIs (2008)

RF Interference – Radio Spectrum Policy (2011)

Security - Public Safety (ENTR) (2010)

Secure Comms. in Smart Grid (2012)

Communications infrastructure Applications (GROW, ENER)

Joint Research Centre

Critical Infrastructures

"Equipment and systems required for supporting critical functions that satisfy basic societal needs and provide public safety"

- ✓ Power generation and distribution
- ✓ Water supply
- ✓ Transportation system
- ✓ Financial services (banking)
- ✓ …

- **Several CIs rely on GNSS**

Over-reliance and Vulnerabilities:
Need for Protection

RF Threats to GNSS

EPCIP 2011

Activity A5: Communication and Navigation Infrastructure Protection (CONIP)
Identify, characterize and mitigate the impact of potential threats to Communications and Navigation CIs

Focus on: Jamming and Spoofing

EPCIP 2012

Action A2: Vulnerability and Protection of High Precision Positioning, Navigation and Timing (PNT) Services for Critical Infrastructure

Continuation of the CONIP activities

Focus on: Signal spoofing
GNSS signal authentication

Jammer Characterisation

Signal Characterization: identify the main characteristics of signals broadcast by a GNSS jammer

Impact on GNSS receivers:
- GPS and Galileo
- Analysis of possible countermeasures

In-vehicle characterization:
- Impact of vehicles (shielding, attenuation, …)
- Vehicle signature
- Detection range requirements
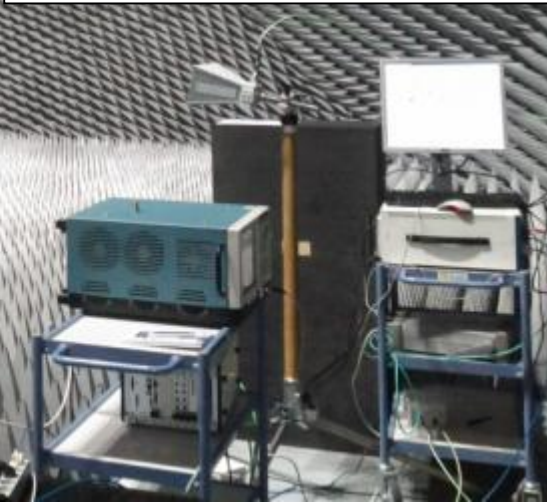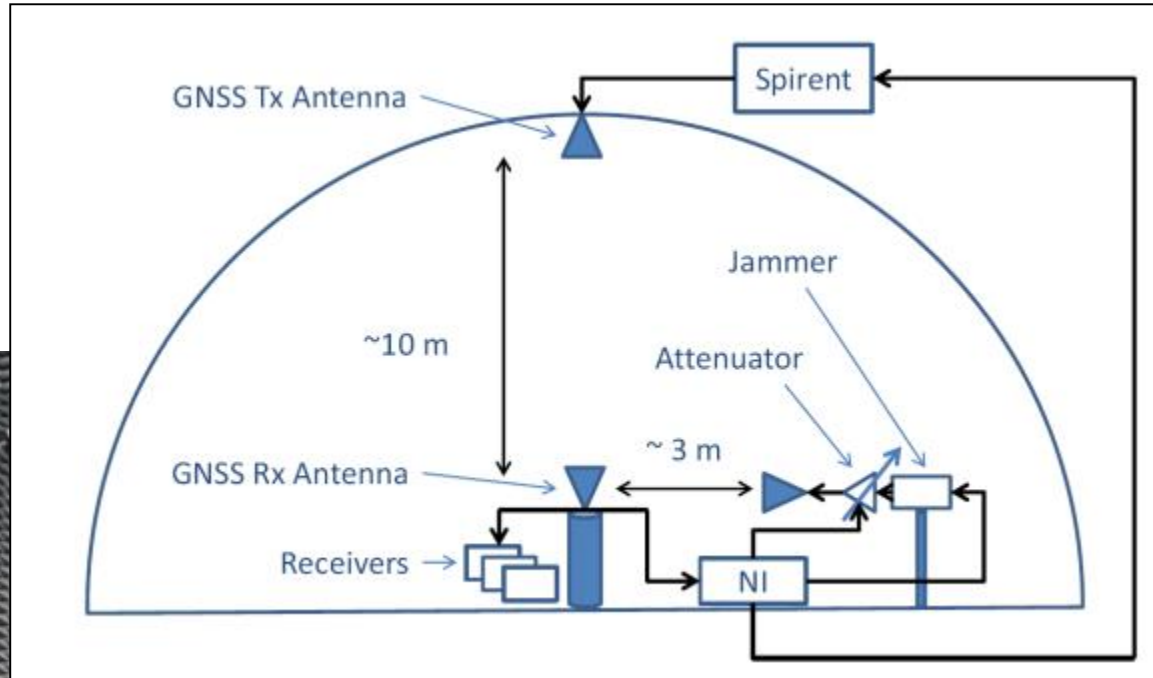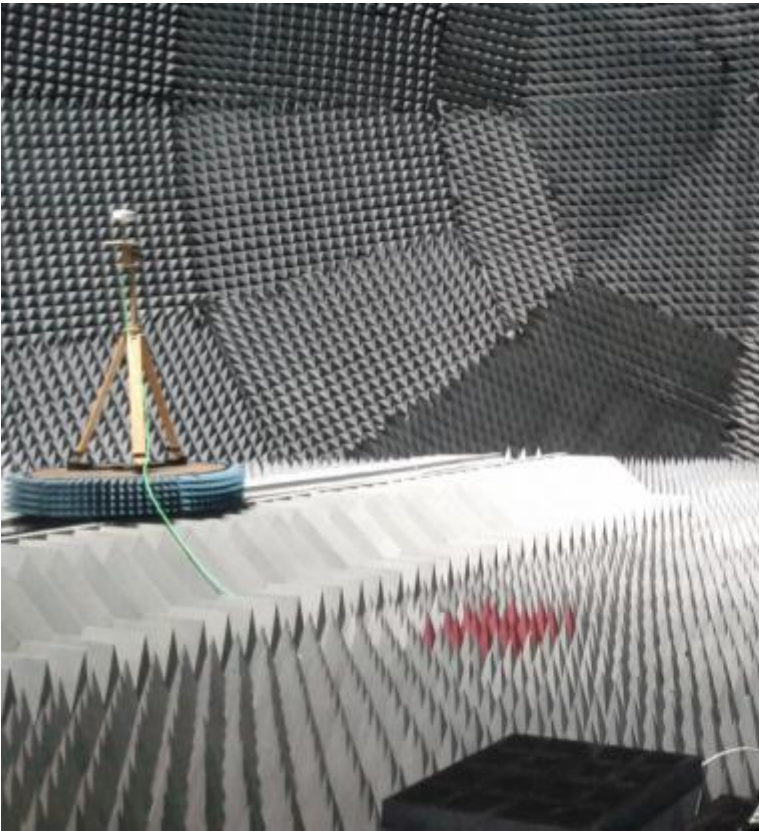
7 different jammers, all GNSS bands, 1 GSM jammer

2011WP5.2
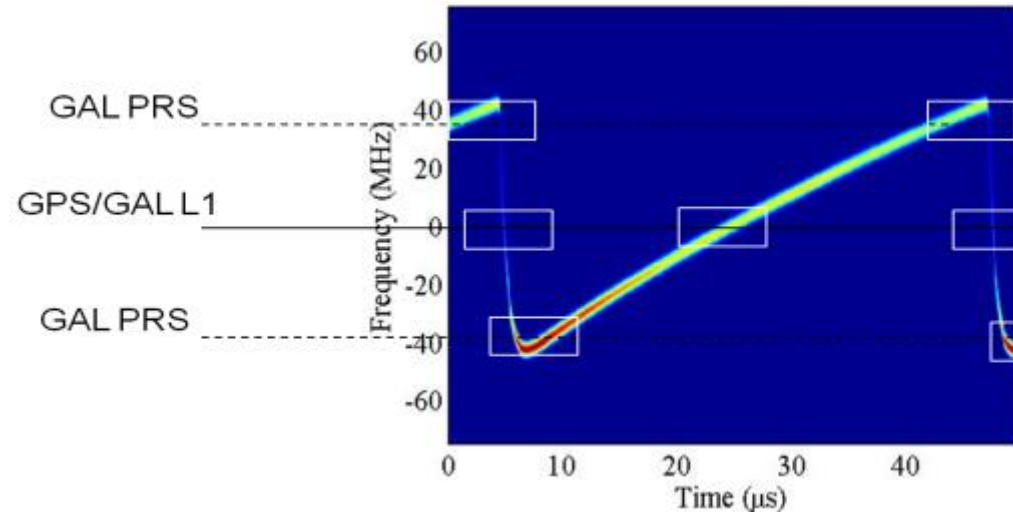
Impact on GNSS Receivers

Impact of jammers on commercial and software-based GNSS receivers

Development and implementation of a dedicated experimental setup in the EMSL

2011WP5.2

Jamming Detection

Development of **low-cost** jamming detectors based on COTS components (GPS receivers)

Design based on the fact that in the presence of jamming, all the C/N_0 measurements are affected by **correlated changes**
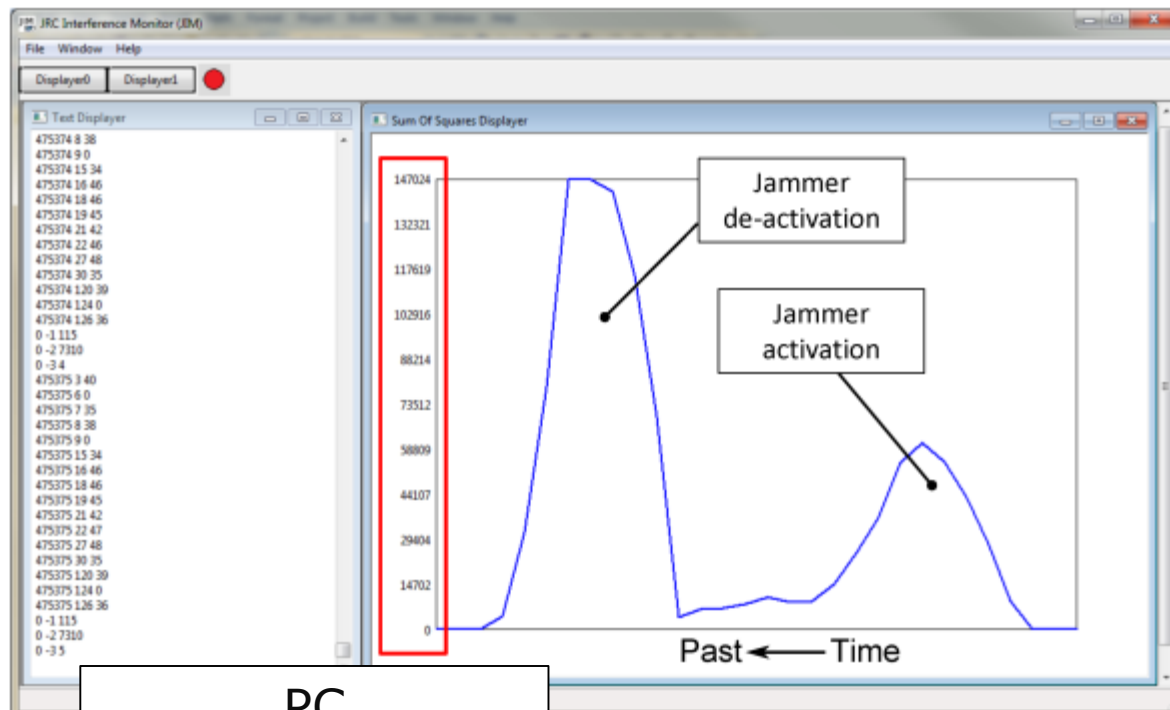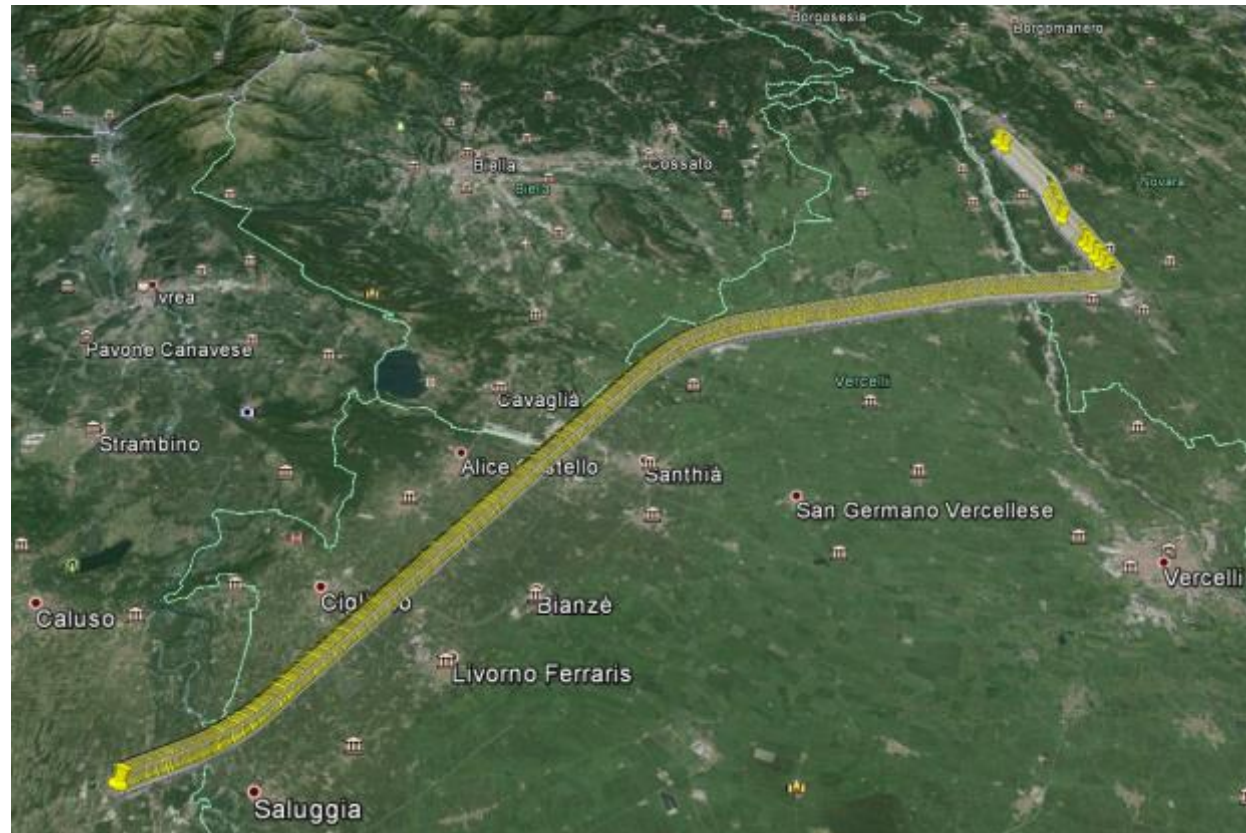

PC implementation

Android implementation

On the Road

Car test of approximately 30 min (~65 Km)
Highway test: **open sky conditions** – no obstructions or tunnels

PDOP < 2.5

Android phone used to **collect data** and to perform **jamming detection**

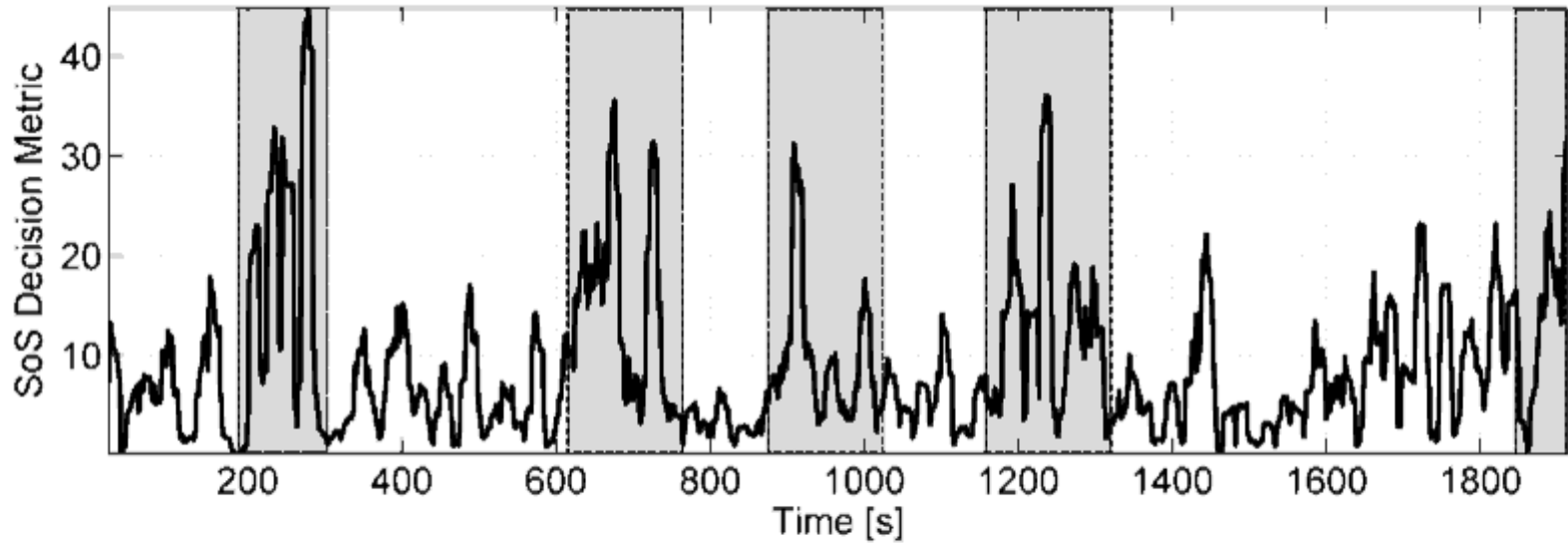Possible jamming events detected comparing a **decision statistic** with a **decision threshold**
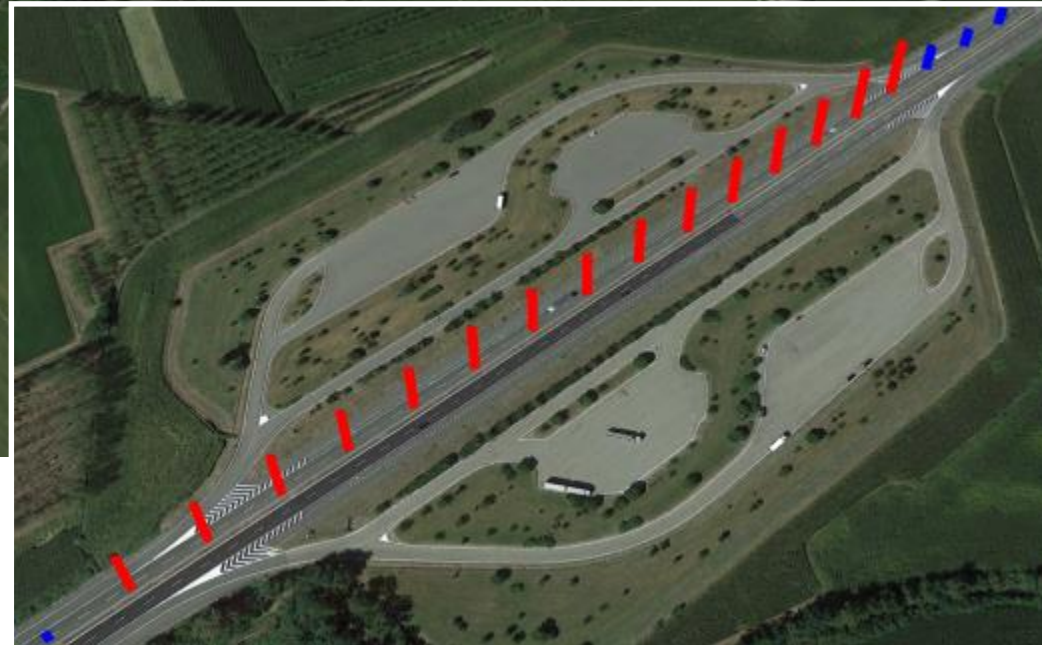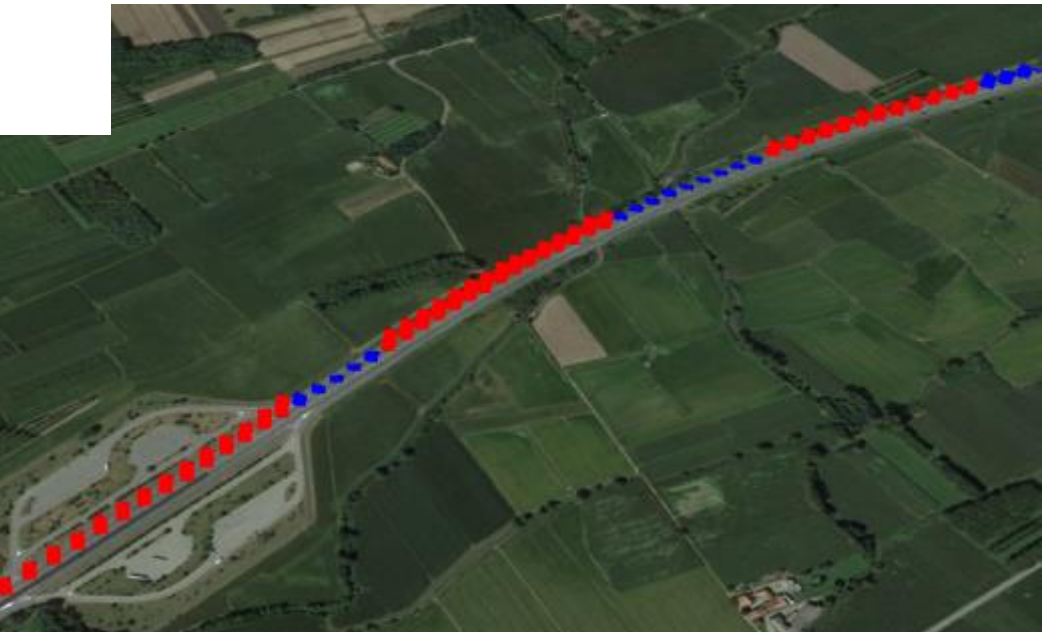
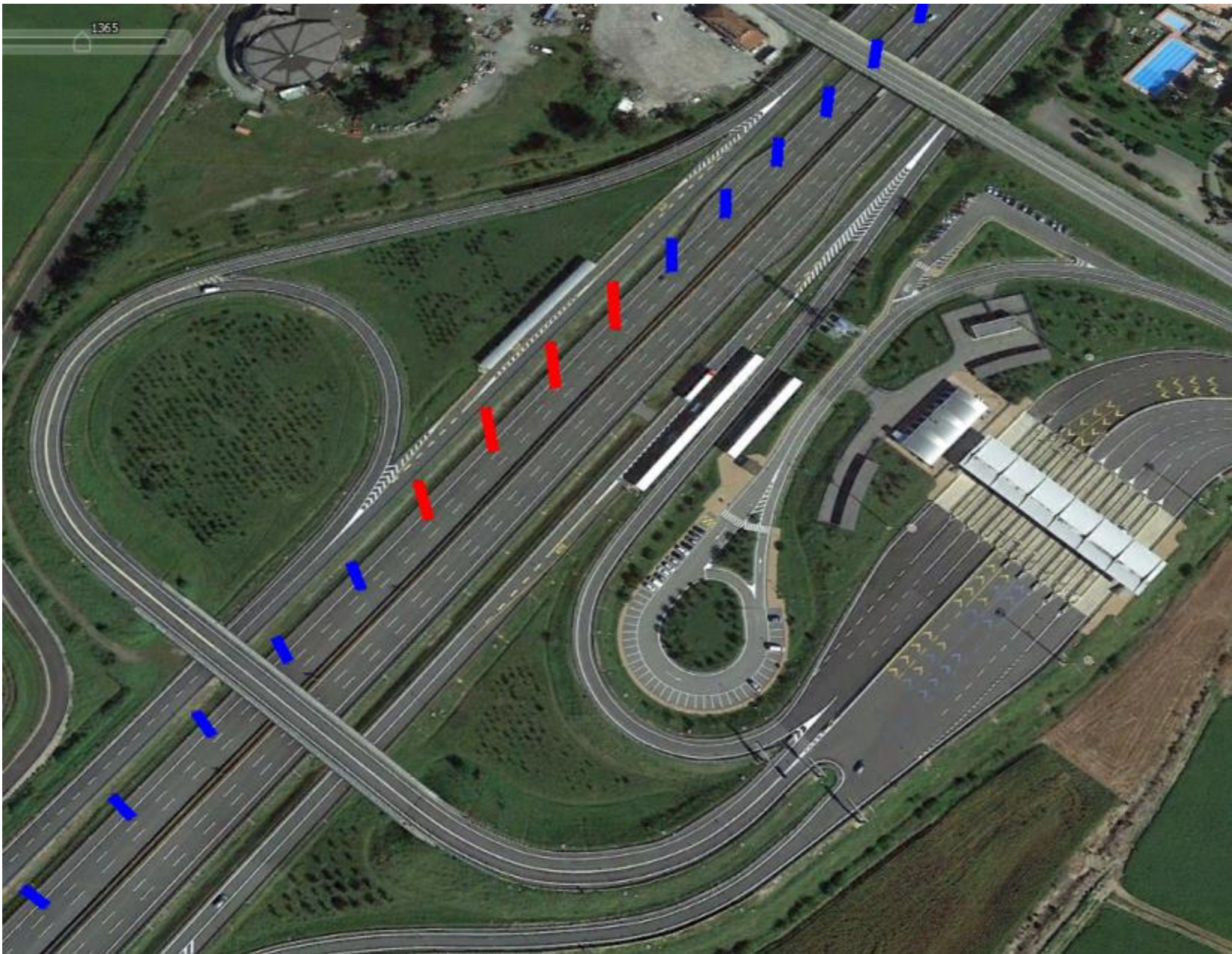# Sample Results

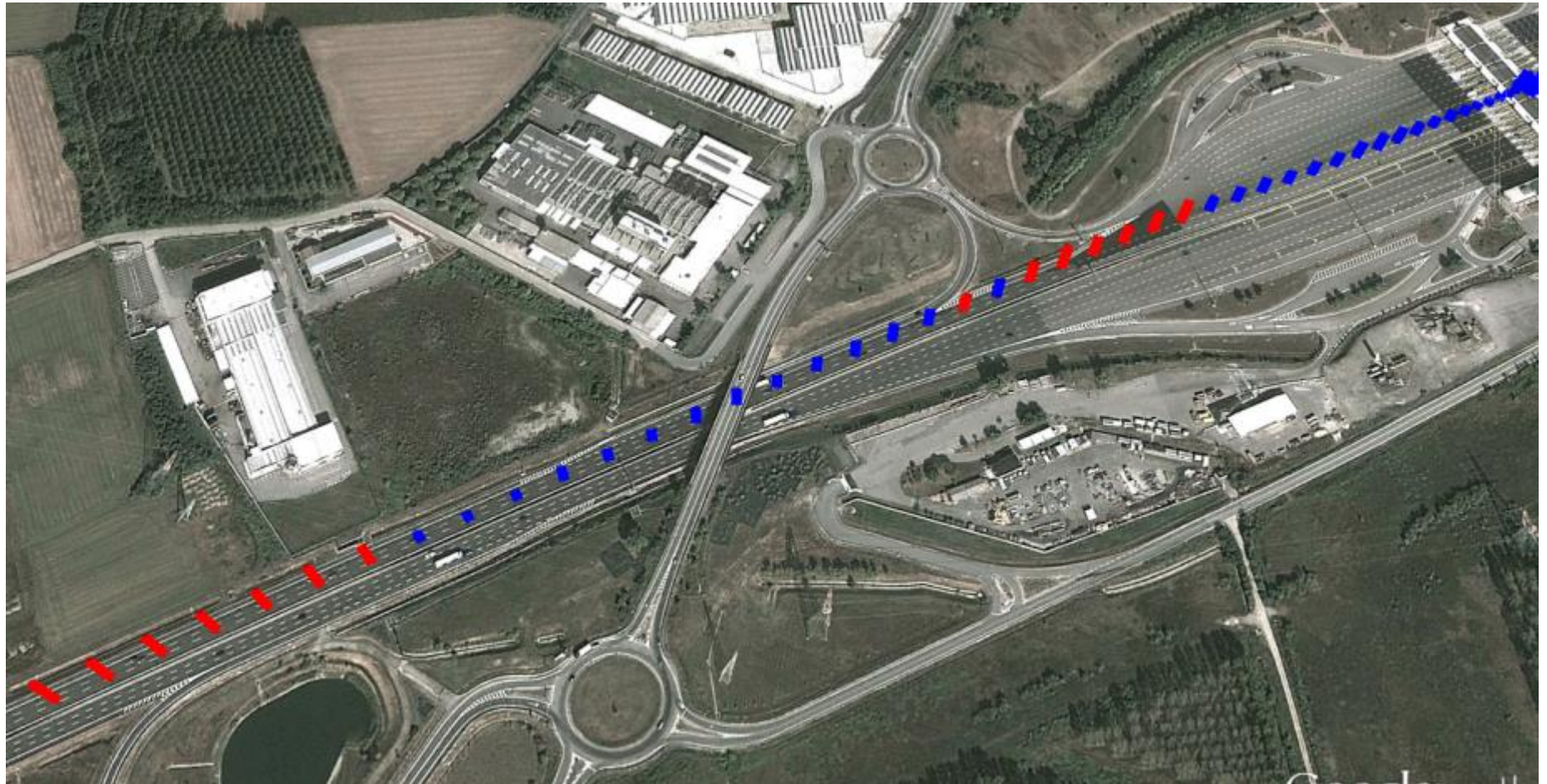

Highway Test
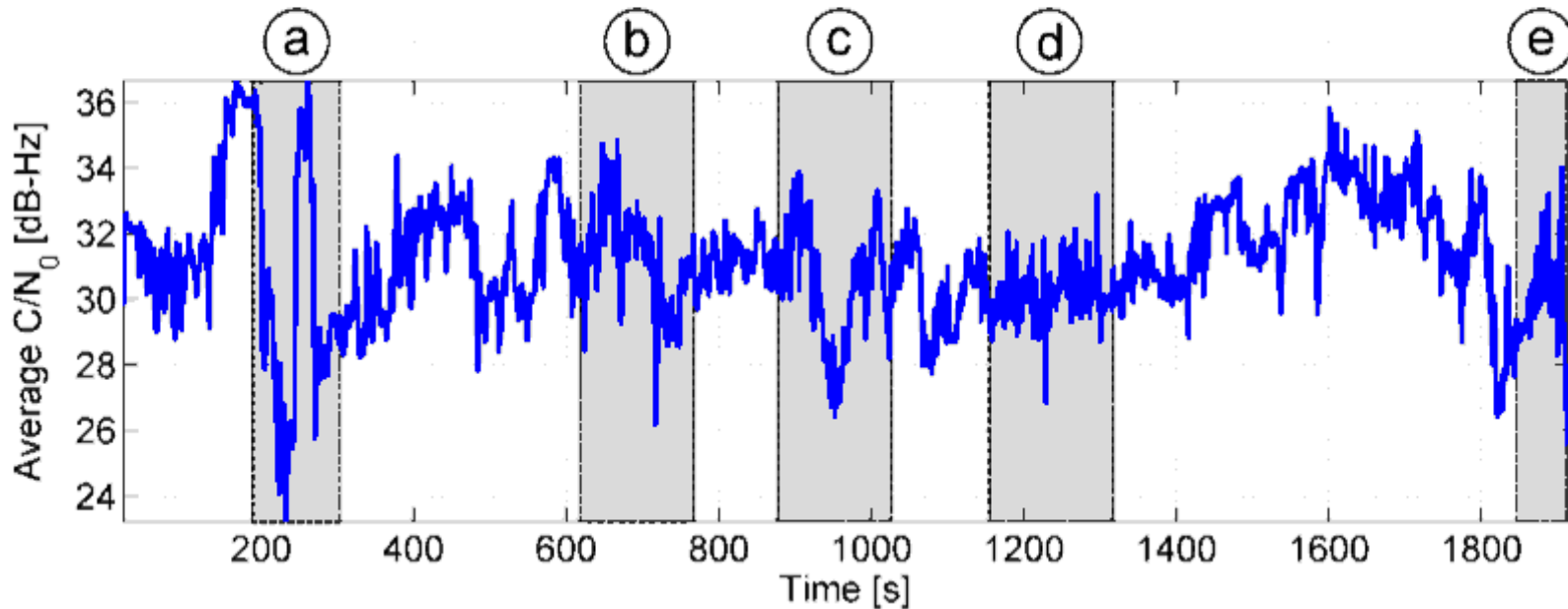
Highway test a)

Highway test b) & c)

Highway test d)

Highway test e)

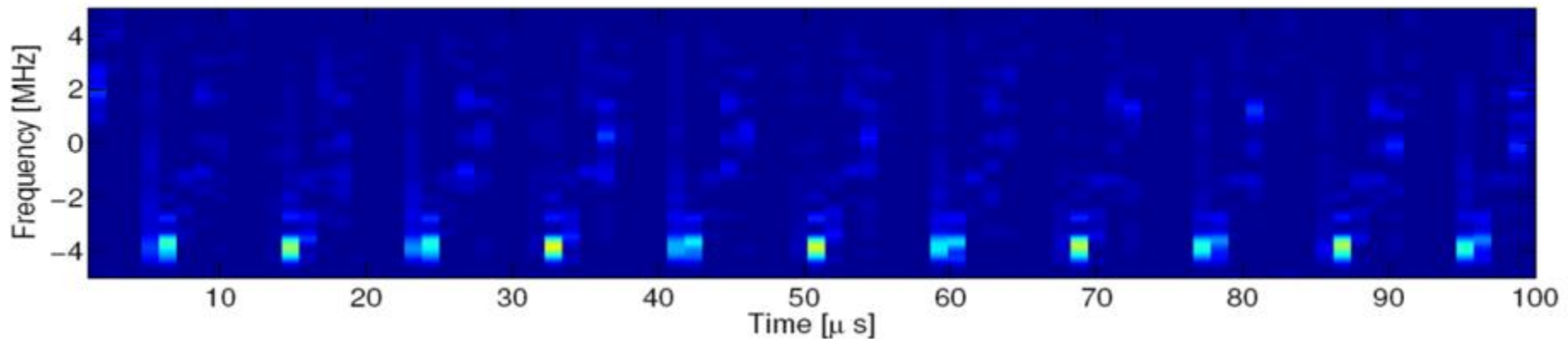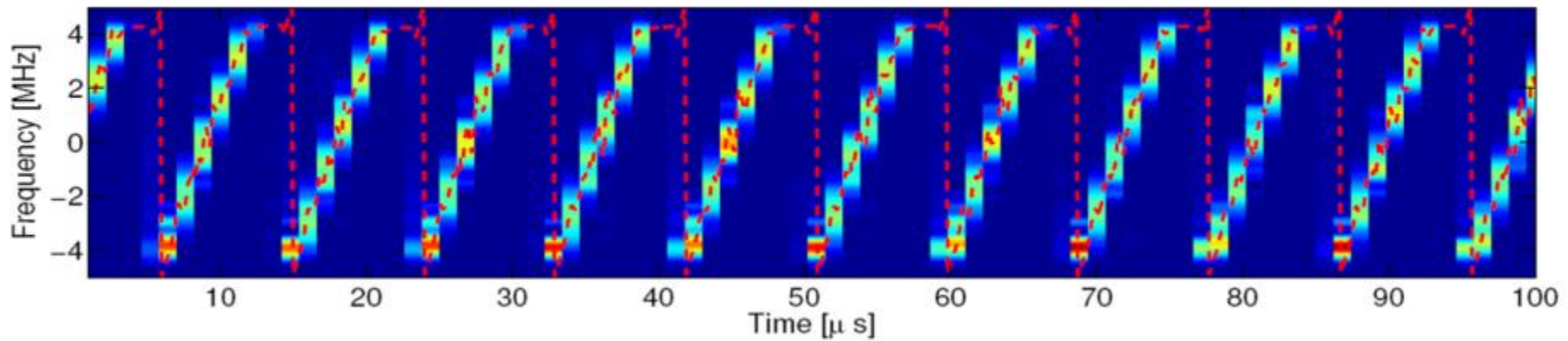Possible jamming events detected in the vicinity of packing spots

Platform for Interference Mitigation

Development of a technical platform for **interference detection** and **mitigation**
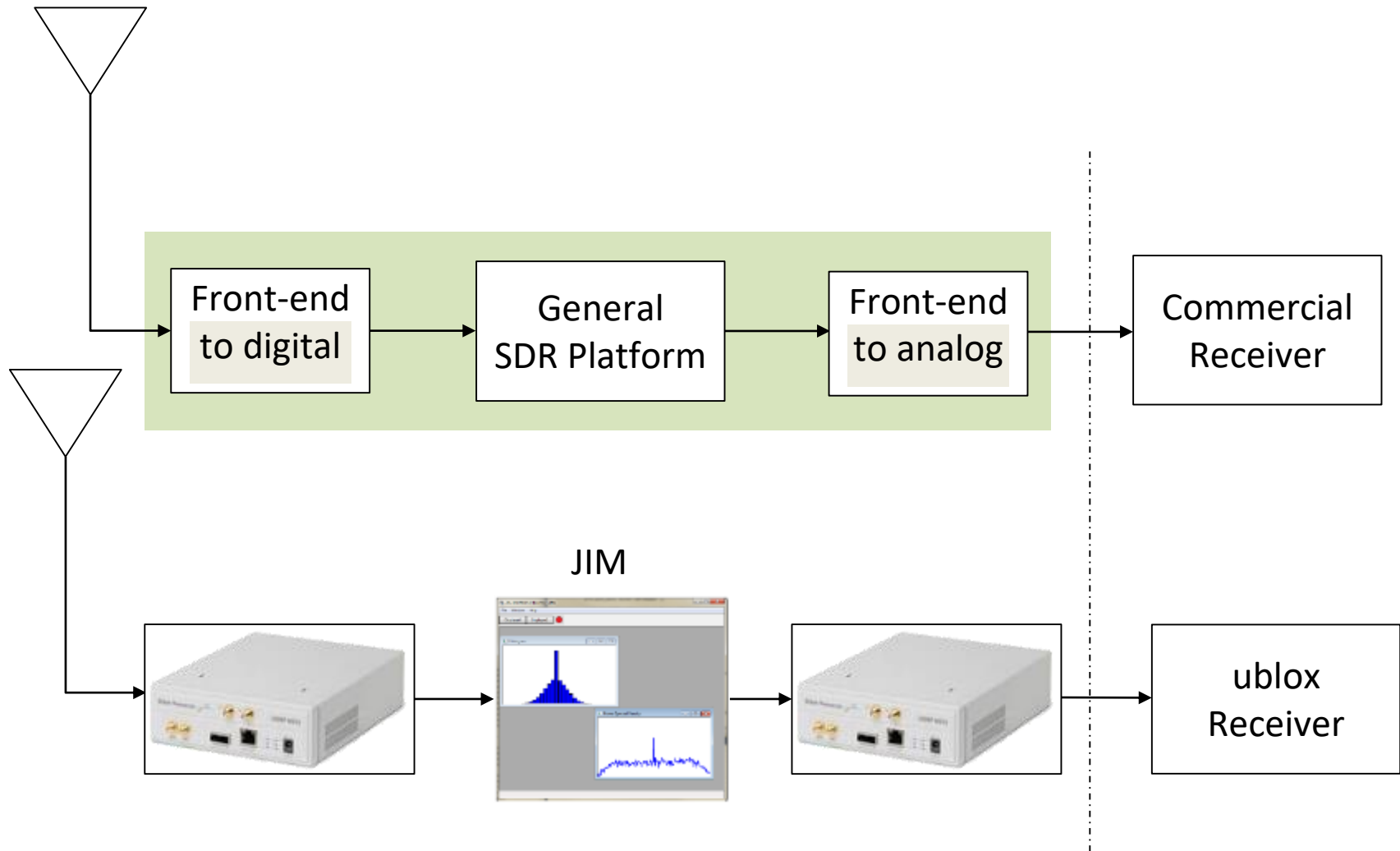
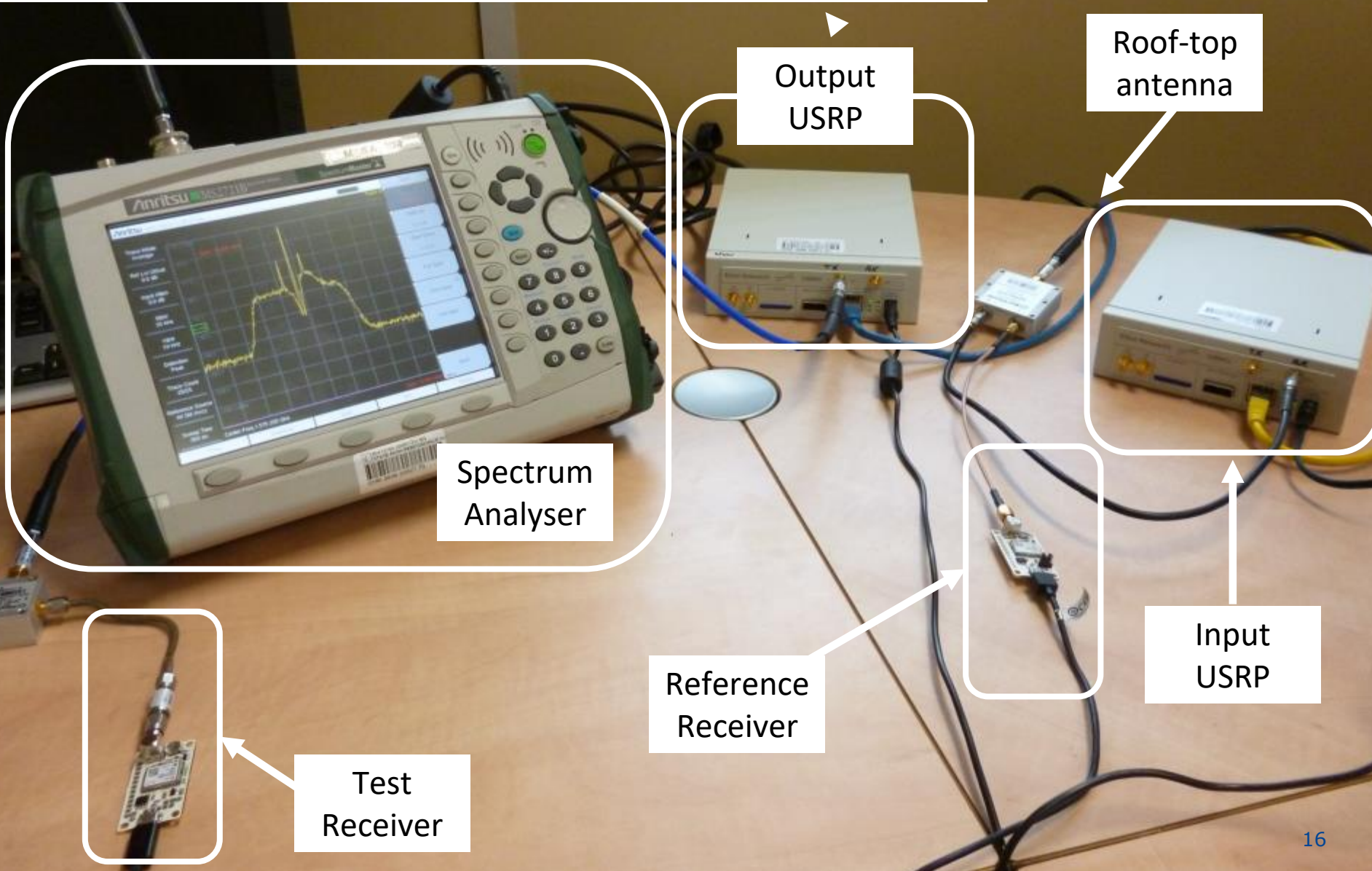Development of dedicated algorithms: **adaptive notch filters**

Real-time Interference Mitigation

Real-time Interference Sanitizer

Output USRP

Roof-top antenna

Spectrum Analyser

Reference Receiver

Input USRP

Test Receiver

Conclusions

- ✓ **JRC GNSS** activities started as part of the EPCIP program: GNSS fundamental element of several **CIs**

- ✓ **EPCIP** has given the JRC the opportunity to create a **state-of-the-art laboratory for GNSS security** (stakeholders and projects: DG GROW, GSA,…)

- ✓ Special focus on **interference detection** and **mitigation**

- ✓ Evaluation of **GNSS threats**: impact on European policy (e.g. the **DETECTOR** project, deployment of detection units on highways)

- ✓ Developments of **prototypes** for jamming detection and mitigation: **improved resilience**