NKG SCIENCE WEEK 2024

Jammertest 2023

Oscar Isoz

Outline

- Introduction
- Jammertest
- Analysis of the impact on position and internal parameters of a Ublox F9p
- Results from other GNSS receivers

Our motivation for the trip

RISE uses GNSS for time comparison (NMI)

- We have need to understand how our receivers manages interference
- Show that we take the jamming issue seriously
- Be part of the Jammerfest from the start.

RISE does research regarding safe transport systems

- Learn from other people in the field
- Gain experiences that can be applied to lab based experiments
- Gain experience for future research proposals

RI.
SE

Who else was there?

- Armed forces
- State organisation
- Geodata/Navigation
- Receiver/Simulators
- Communication/timing
- Vehicle
- University/State research
- GNSS interference detection

Edited from TestNor

~ 60 companies/organisation & ~200 persons

Focus on Saftey

Mandatory Hi-Vis clothing outside

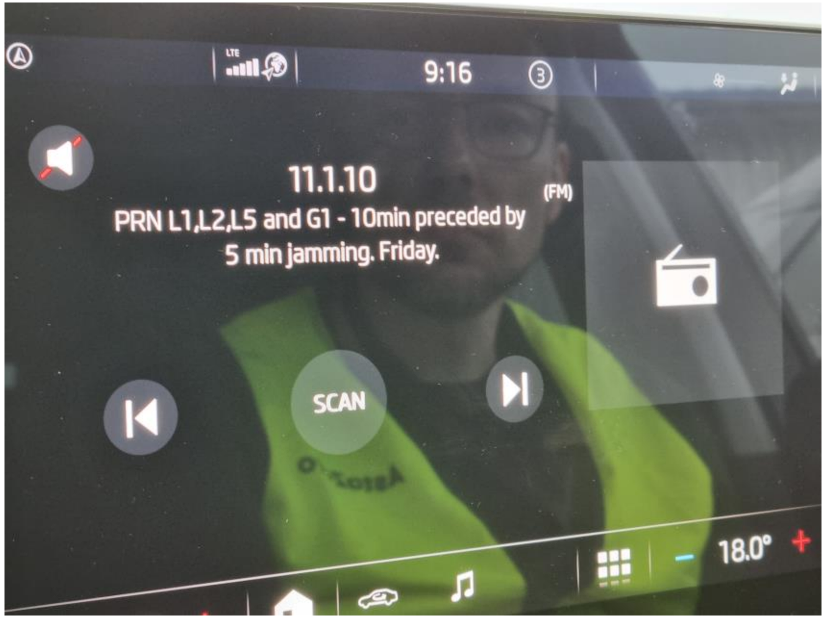
Reduced speed on the main ”jamming road”

But also on networking

Really good fika!

Test support systems

- Access to (uninterfered) RTK corrections
- Accurate timing by cable (unfortunately not to our “remote” office)
- Event chat channel for real-time messaging
- FM radio 99.0 - Radio Noise
- Realtime information via RDS
- MQTT broker with test information
- Testplan (pdf) with all planned tests described



Example of a RDS message

RI.
SE

What type of jamming were offered?

- Jamming (0.1uW->200W(!?))
  - L1/E1,G1, B1, L2,G2,L5, E5b, E6
  - CW, Swept CW, PRN-isch, PRN
- Spoofing
  - E1,L1, L2C, E5, L5
  - Coherent/Incoherent
  - With/without initial jamming
  - Static/dynamic spoofing
- Meaconing (0.1, 10W)
  - L1/E1, L2
- 100+ test scenarios at “base-camp”
- ~ 500+ jamming cases

Coherent spoofing = Transmission of simulated GNSS signals using true/broadcast ephemerides and where signal reception *at a designated target location* is code-phase aligned with live sky signals to better than half the code chip length[2].

Incoherent spoofing = Reception of transmitted simulated GNSS signals that are *not* code-phase aligned with live sky signals[3].

RI. SE

Our measurement sites

AirBnb

Ublox F9p

Main “office”

- Septentrio - Mosaic-T
- Septentrio - PolarX
- USRP-B210 SDR for realtime spectrum
- USRP-B205 SDR for RF data collection

Jamming antenna (mainly advanced spoofing)

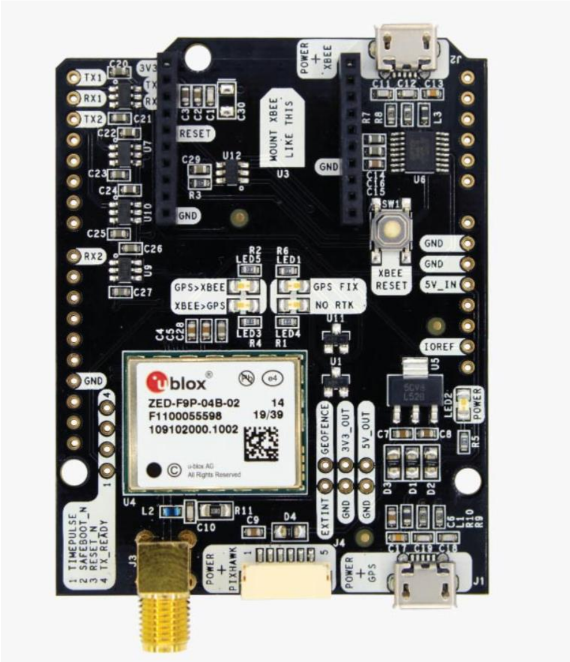
Our ”office” for the week

Main antenna

Main GNSS antenna farm outside the house

RI.
SE

Ublox F9p



Ardusimple RTK2B module
(~170€)

- L1/L2 reception (L1/L5 does also exist)
- Support for RTCM v3 messages
- Carrier phase capable
- GPS/Galileo/Glonass/Beidou
- NMEA and Ubx (binary) data format.

RI.
SE

Test (in refe	Date	Start UTC time	Stop UTC	Tx power [dBr	Sp
6.1.1	***2023-09-18***	***14:22:58***	***14:23:08***	***-41***	
6.1.1	2023-09-18	14:23:08	14:23:18	-39	
6.1.1	2023-09-18	14:23:18	14:23:28	-37	
6.1.1	2023-09-18	14:23:28	14:23:38	-35	
6.1.1	2023-09-18	14:23:38	14:23:48	-33	
6.1.1	2023-09-18	14:23:48	14:23:58	-31	
6.1.1	2023-09-18	14:23:58	14:24:08	-29	
6.1.1	2023-09-18	14:24:08	14:24:18	-27	
6.1.1	2023-09-18	14:24:18	14:24:28	-25	
6.1.1	2023-09-18	14:24:28	14:24:38	-23	
6.1.1	2023-09-18	14:24:38	14:24:48	-21	
6.1.1	2023-09-18	14:24:48	14:24:58	-19	
6.1.1	2023-09-18	14:24:58	14:25:08	-17	
6.1.1	2023-09-18	14:25:08	14:25:18	-15	
6.1.1	2023-09-18	14:25:18	14:25:28	-13	
6.1.1	2023-09-18	14:25:28	14:25:38	-11	
6.1.1	2023-09-18	14:25:38	14:25:48	-9	
6.1.1	2023-09-18	14:25:48	14:25:58	-7	
6.1.1	2023-09-18	14:25:58	14:26:08	-5	
6.1.1	2023-09-18	14:26:08	14:26:18	-3	
6.1.1	2023-09-18	14:26:18	14:26:28	-1	
6.1.1	2023-09-18	14:26:28	14:26:38	1	
6.1.1	2023-09-18	14:26:38	14:26:48	3	
6.1.1	2023-09-18	14:26:48	14:26:58	5	
6.1.1	2023-09-18	14:26:58	14:27:08	7	
6.1.1	2023-09-18	14:27:08	14:27:18	9	
6.1.1	2023-09-18	14:27:18	14:27:28	11	

Transmission log - provided by Nkom

6.1 Preconditions and setup

The main objective is to observe how the J/S signal affect the loss of PNT, and/or how it produces inaccurate PNT data, and at which power level. This will allow for evaluation of the sensitivity thresholds for various systems. The transmitted power will be ramped up and down from 0.1 µW to 20 W EIRP for each test with 10 seconds hold time for each power level, with ramping steps of 2 dB. The modulation will be PRN.

The attendees should be at a stationary location with a known distance to the jammer, so they can observe how different levels will affect the PNT. Comparing the ramping tests from both Cemetery (6) and Ramnan (7), will give the opportunity to compare signals arriving from different angles and also to see the difference between signals going along earth/ground and coming from above.

The jammer will be placed at the cemetery, north of Bleik. This is point A in 26.2.

Each test will last for 13.67 minutes, with a 15-minute break between each test. The jammer employed will be "Porcus Major", see appendix26.9.19. The last step, from 42 dBm to 43.0103 dBm (20 W), will be a 1.0103 dB increment, not a 2 dB increment.

Test Area: 1
Operational Contact: Nicolai Gerrard, Nkom
Technical Contact: Anders Rødningsby, FFI
Time estimate: 2 hours

6.1.1 Test: 0.1 µW to 20 W, 2 dB increments PRN: L1

6.1.2 Test: 0.1 µW to 20 W, 2 dB increments PRN: L1, G1

6.1.3 Test: 0.1 µW to 20 W, 2 dB increments PRN: L1, G1, L2

6.1.4 Test: 0.1 µW to 20 W, 2 dB increments PRN: L1, G1, L2, L5

26.9.19 Technical details on the high-power jammer “Porcus Major” F8.1

The high-power jammer can provide jamming signals with up to 20 W EIRP simultaneously on eight GNSS bands. Figure 24.1 shows the block diagram of the high-power jammer. The jammer uses two USRP X410 SDR from Ettus Research as exciters. Each SDR have four output channels covering the frequency range of 1 MHz to 7.2 GHz, with maximum 400 MHz instantaneous bandwidth. The SDRs have an internal gain range of 60 dB in 1 dB steps. Each of the exciter output signals are fed to the corresponding channel of the programmable step-attenuator. The attenuator has an attenuation range of 95 dB in 0.25 dB steps. The output signal from the attenuators is then fed to the power amplifiers. The amplifiers connect to eight individual antennas via a 10 m coax. The antennas are directional helical antennas with right hand circular polarization (RHCP) and 10 dB gain.

An overview of the jammer signal modulations is given in Table 25.1.

Frequency band name	CW	PRN		Sweep/chirp		
	Frequency (MHz)	Center freq (MHz)	BPSK modulated chip rate (MHz)	Center freq (MHz)	Sweep rate (kHz)	Frequency band (MHz)
L1	1575.42	1575.42	10	1575.42	100	± 3
L2	1227.6	1227.6	10	1227.6	100	± 3
L5	1176.45	1176.45	10	1176.45	100	± 3
G1	1602	1602	5*	1602	100	± 3
G2	1246	1246	3	1246	100	± 3
E5b	1207.14	1207.14	10	1207.14	100	± 3
E6	1278.75	1278.75	10	1278.75	100	± 3
B1I	1561.098	1561.098	3	1561.098	100	± 3

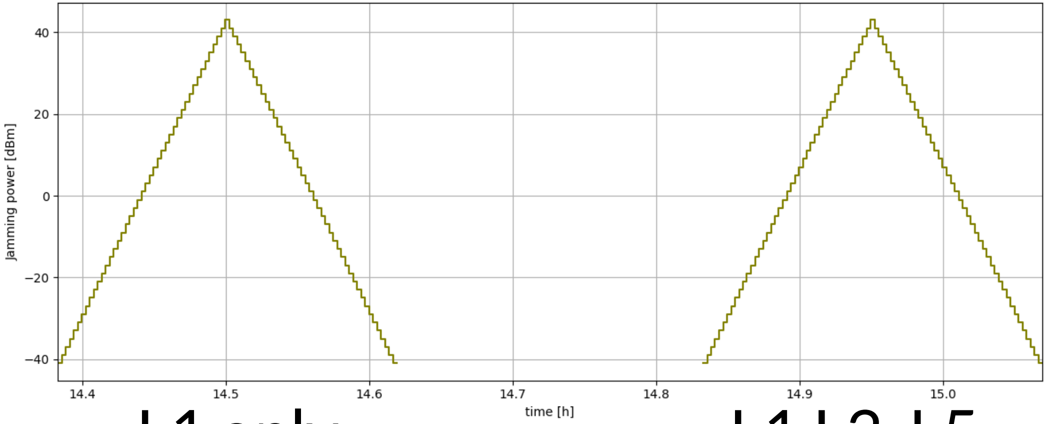
*3MHz may be used in the pyramid jamming (test groups 9 and 10).

RI.
SE

Jamming case 6.1.1,6.1.4

10MHz PRN Power ramp

Max power 43dBm ~ 20W



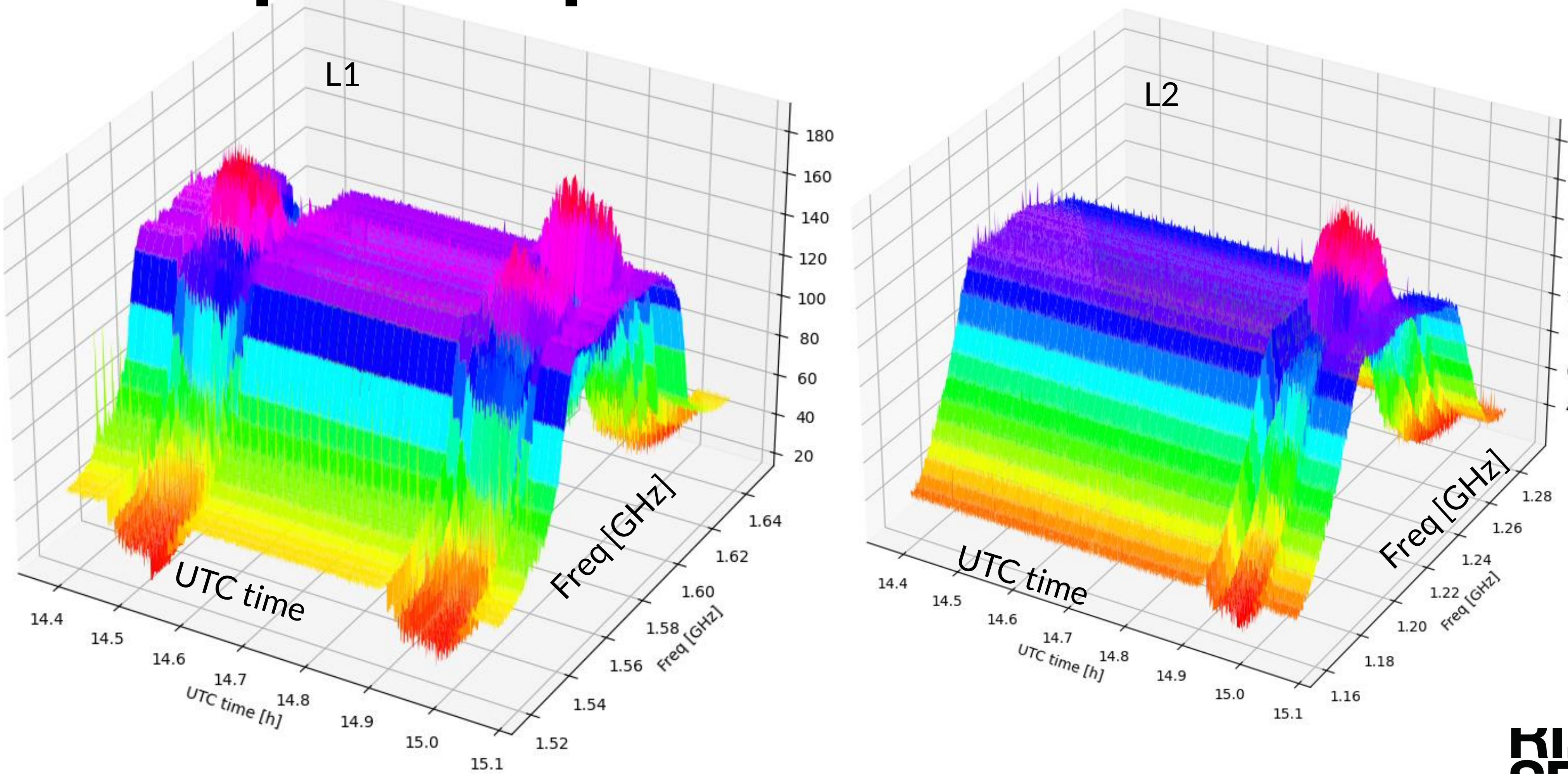
L1 only

L1,L2, L5

Min power - 41dBm ~ 80 nW

Distance to transmitter ~1.4km

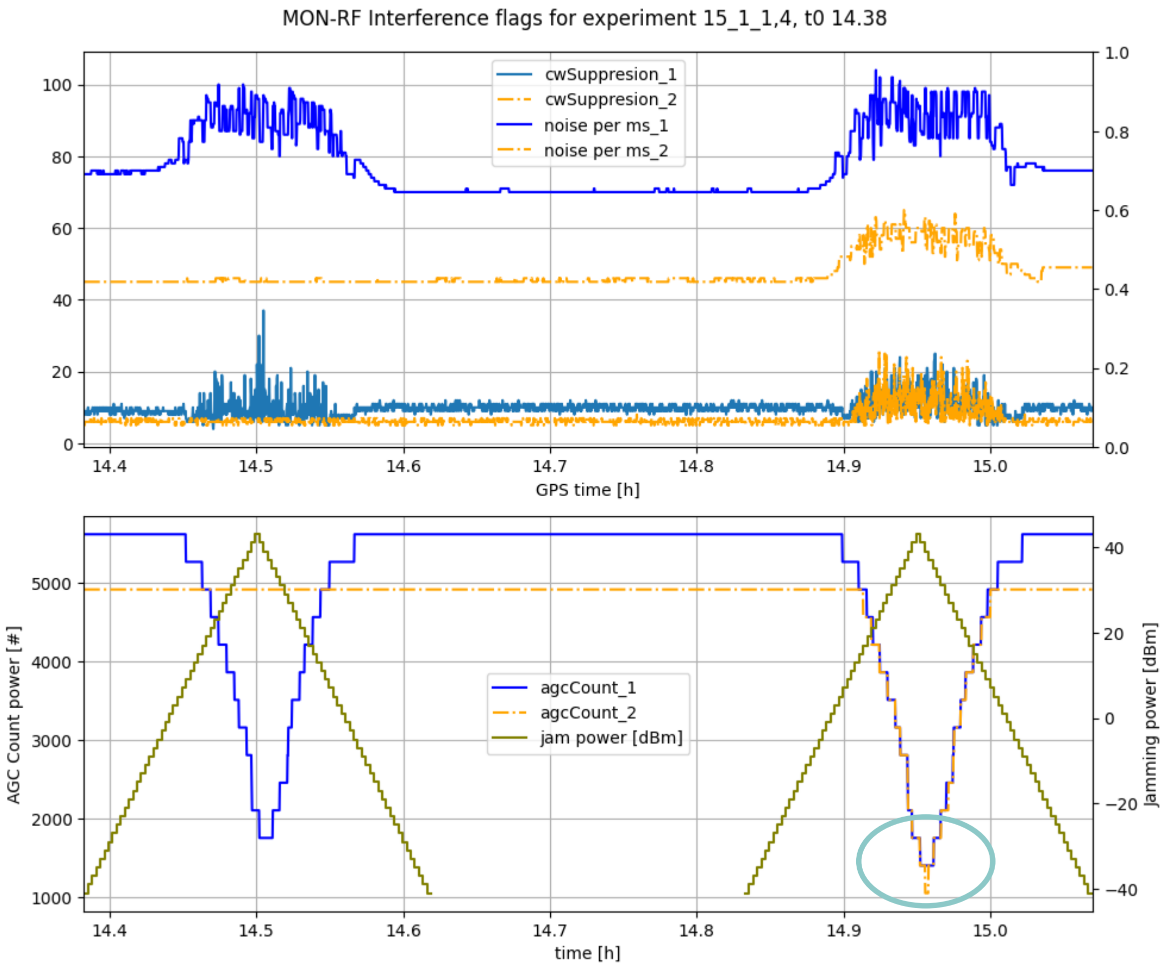
Reported spectrum



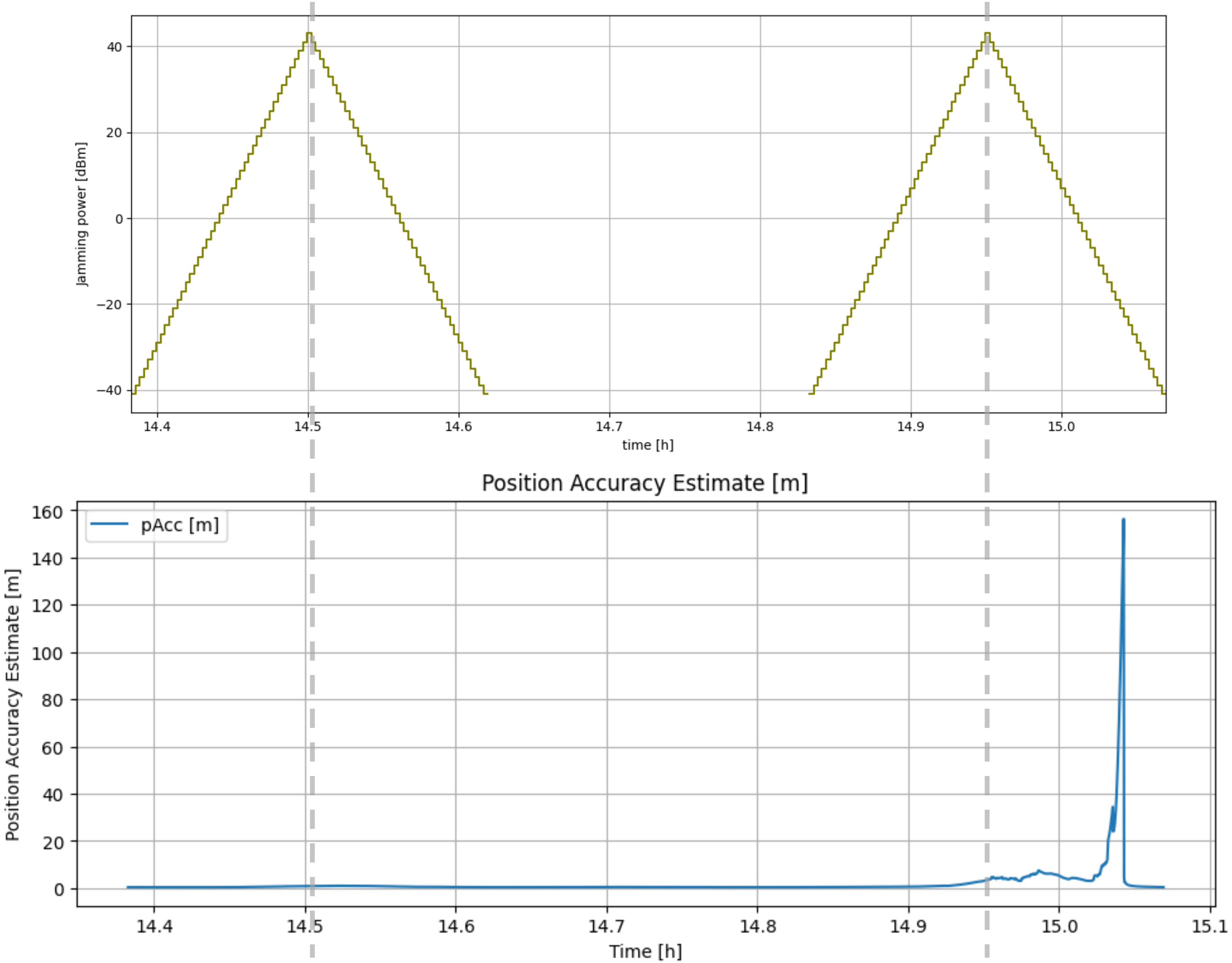
Recorded Ublox spectrum

RI.
SE

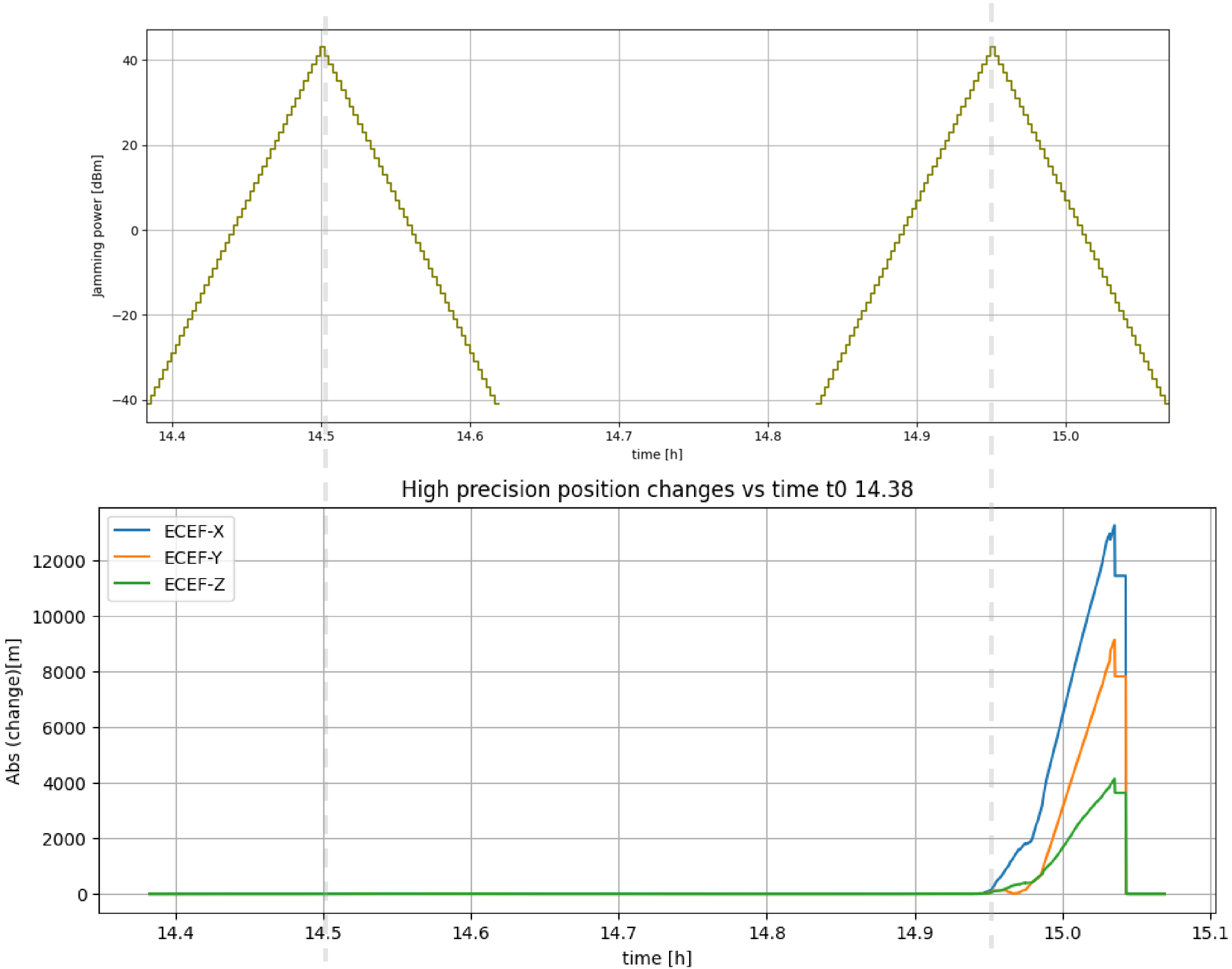
Impact on internal RFI flags



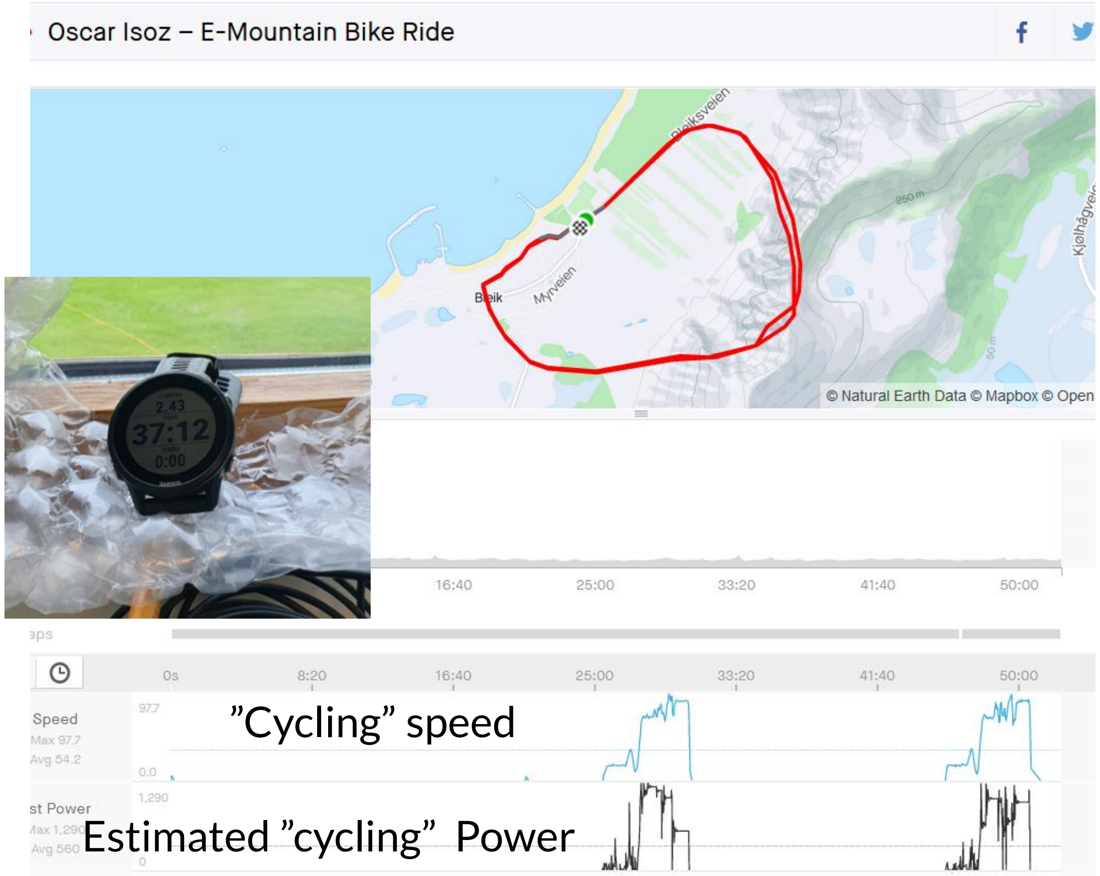
Interference level vs Estimated accuracy



Interference level vs ECEF-Position



Garmin FR 955 (L1,L5) vs
L1,L2C, L5 and E1, E5 spoofing
proceeded by jamming



L1,L2C,L5

E1,E5

Modern car (Skoda Enyaq) and Samsung S10
vs L1,L2C, L5 spoofing

Spoofed Route

Same location

Estimated location

Takk, Takk, Kitos, Aitäh, Paldies, Dėkoju, Tak, Tack

Oscar.isoz@ri.se

RI. SE

image TestNor

End of presentation