STRIKE3

Standardization of GNSS Threat reporting and Receiver Testing through International Knowledge Exchange, Experimentation and Exploitation:

Validation of Reporting and Testing Standards

Martin Pölöskey

aric automotive + rail innovation center research GmbH

European Global Navigation Satellite Systems Agency

HORIZON 2020

ENC 2018

The European Navigation Conference 2018

Gothenburg
16. May 2018

An initiative to protect our GNSS …

- Project funded by European GNSS Agency (GSA) under the H2020 Framework Programme for R&D

- Duration: 3 years (1. Feb. 2016 to 31.01.2019)
- Main subjects: Standardization of GNSS
  - ➢ Threat Reporting and Receiver Testing

GNSS Needs Protection

1. GNSS air navigation

'Forgotten' GPS jammer costs motorist €2,000

NANTES ATLANTIQUE

Hall 1

Illegal device caused delays to flights at Nantes airport

A La Rochelle man has been fined €2,000 after 'forgetting' to switch off a GPS jammer in his vehicle when he left it in a carpark at Nantes Atlantique Airport.

Airport operations suspended for 75 minutes due to GPS jammer

In car cigar lighter supply

2. GNSS road pricing

Fines up to 50,000 euros for truckers with GPS jammer to avoid toll

Aanbevelen Delen 69 Tweet G+1 0 13 COMMENTS

By: Editor
24/01/17 - 15u31 Source: Belga

SAVE ARTICLE

© Belga.

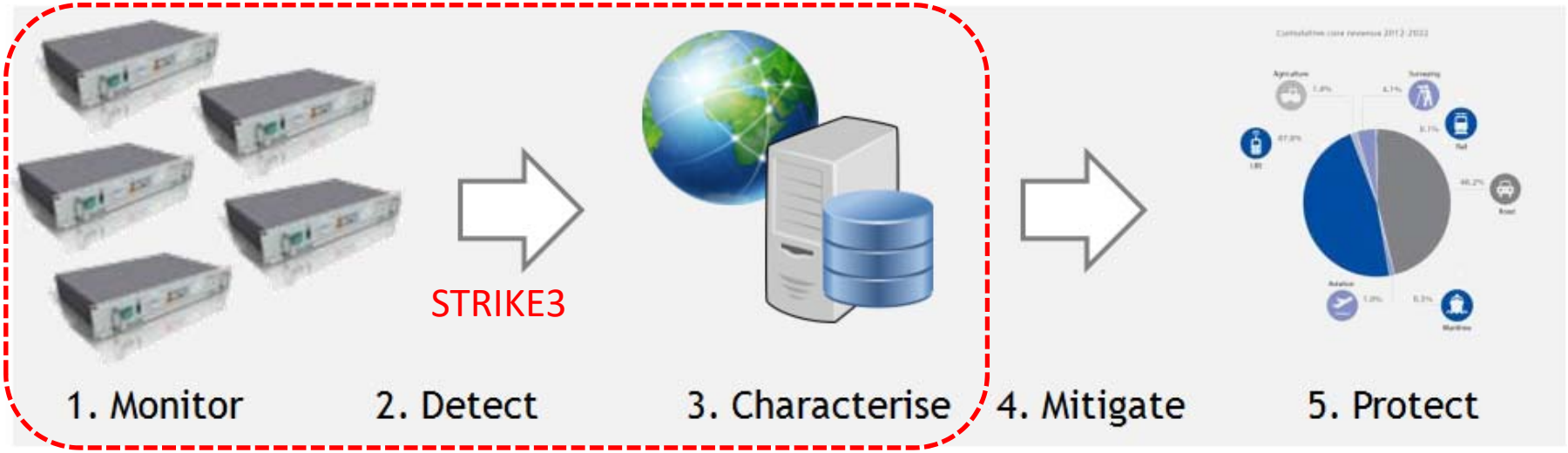
TOLL Truckers who use a GPS jammer to avoid the toll, risking fines up to 50,000 euros. That is informed today at Viapass, the government agency that coordinates the kilometer charge. Moreover, there are three ways in which the fraud is detected: via fixed porches above the road, and flexible control over the mobile control units. In addition, irregularities can be noted in the billing says Edward Claessens of Viapass.

3. New GNSS Jammers

New

USB powered Jammer
L1 + L2 frequency

STRIKE3 Project Overview



- STRIKE3 provides a response at an international level to ensure that there is:
  i. a standard for GNSS threat reporting and analysis based on monitoring and analysis of interference signals
  ii. standard for assessing the performance of GNSS receivers and applications under threat.

STRIKE3 Monitoring Equipment

DETECTOR

GSS100D – Interference detector

- GPS/EGNOS/Galileo L1/E1

GSS200D – Interference detector

- GPS/Galileo/EGNOS/GLONASS L1/E1/G1

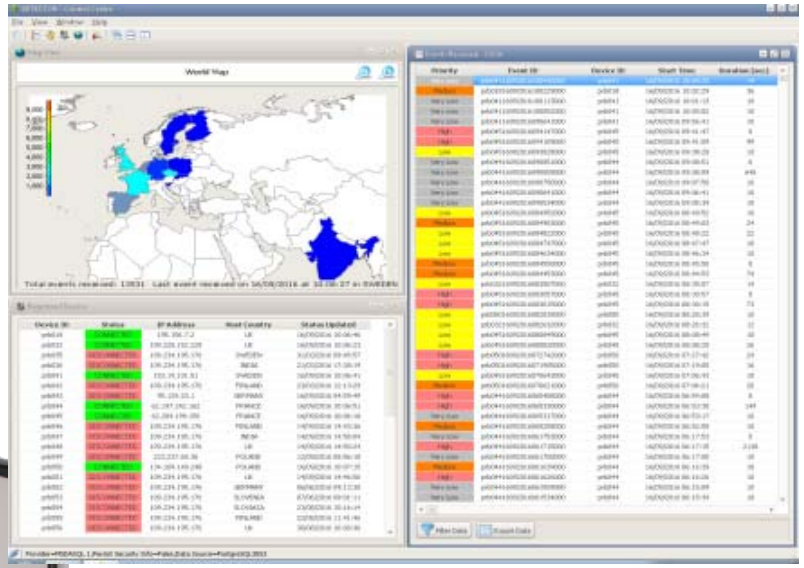
GSS200D' – Interference detector

- L1/L5 + ICAO/Eurocae interference masks
- Spoofing detection

RF-Oculus

- GPS/SBAS/GALILEO L1/E1
- Autonomous monitoring
- Centralised server with web-interface

STRIKE3 Data-base Server



- Dedicated STRIKE3 project server
- Autonomous and persistent monitoring
- Records events in secure database

ICAO = International Civil Aviation Organization

STRIKE3 International Network

At a range of infrastructures

- Major City Centres
- City-ring roads
- National timing labs
- Motorways/Road network
- Airports
- GNSS infrastructures
- Power stations
- Railway
- EU Borders
- Ports

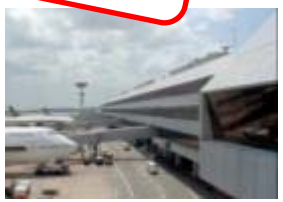
At a range of locations

- United Kingdom
- Sweden
- Finland
- Germany
- India
- Vietnam
- France
- Poland
- Czech Republic
- Spain
- Slovakia
- Slovenia
- Netherlands
- Belgium
- Croatia
- Latvia
- + 3 EU
- + 4 outside EU

~30 monitoring sites in 23 countries



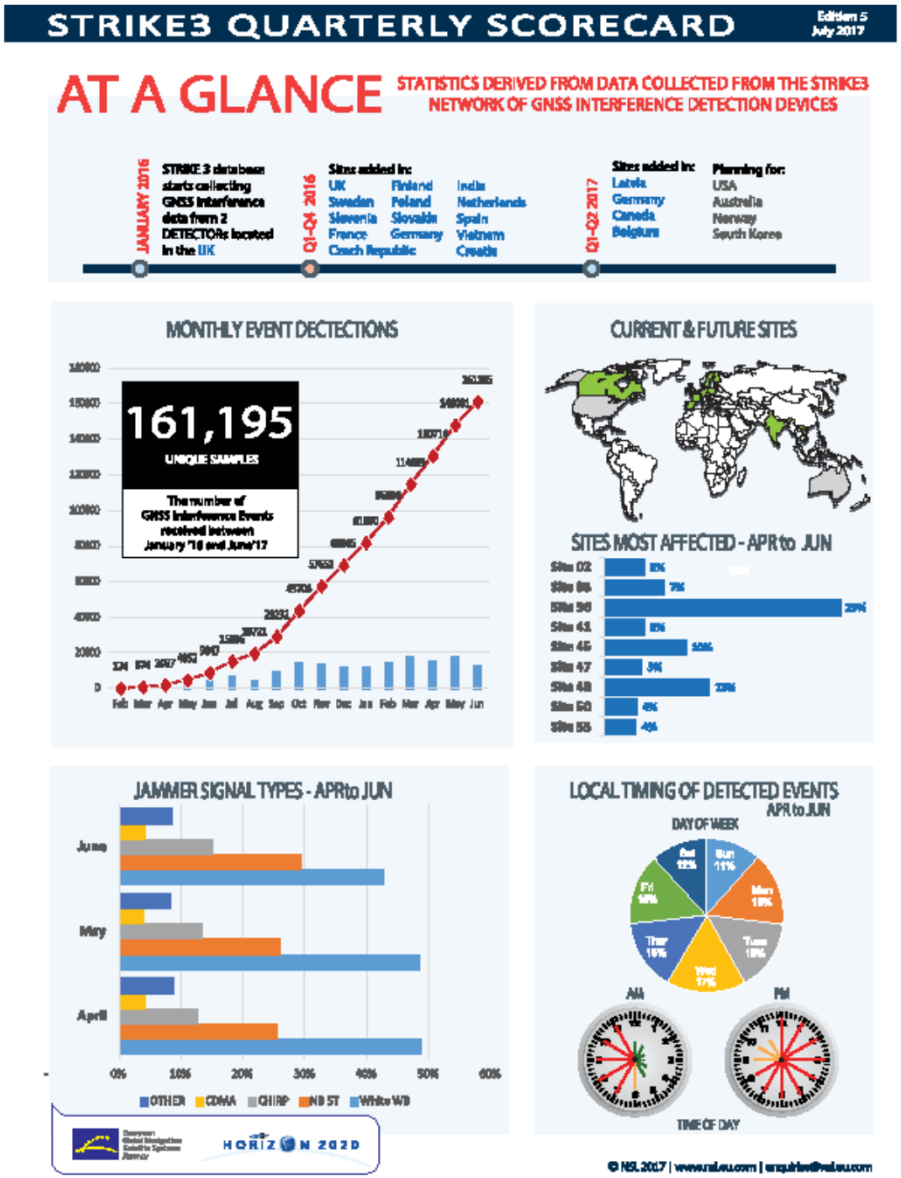




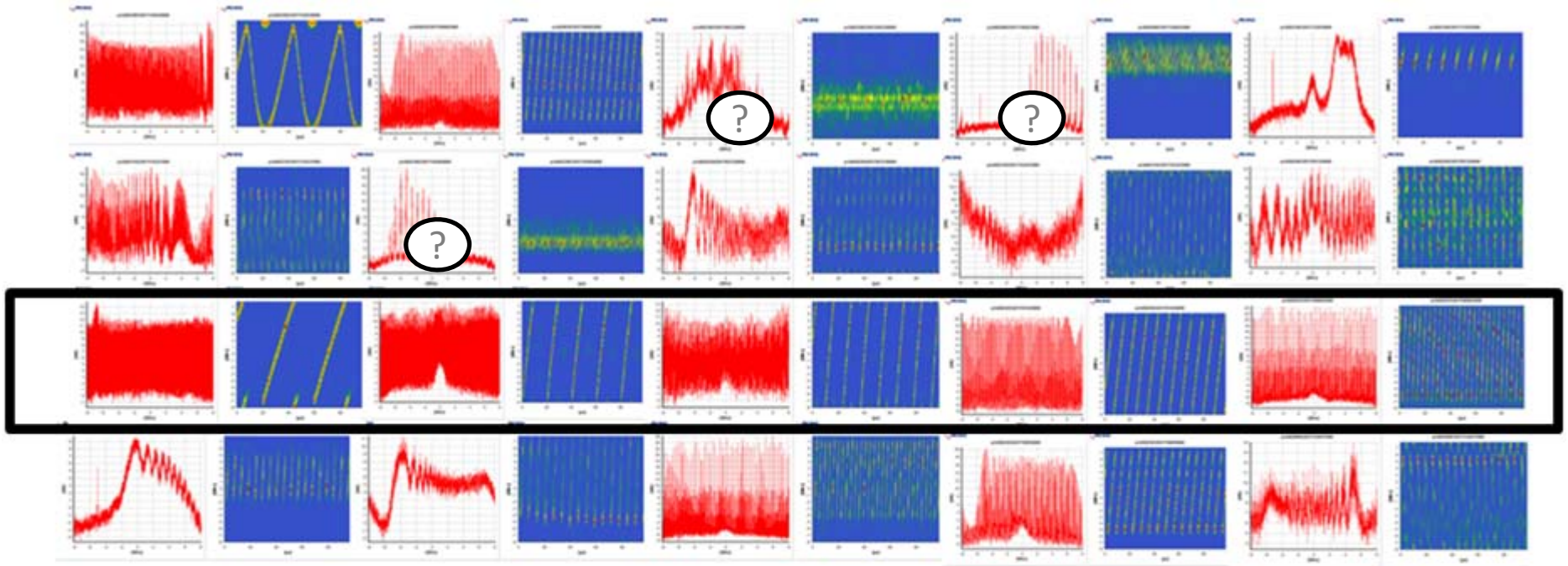
STRIKE3 International Network

Up-to-date nearly 300.000 interference signals recorded

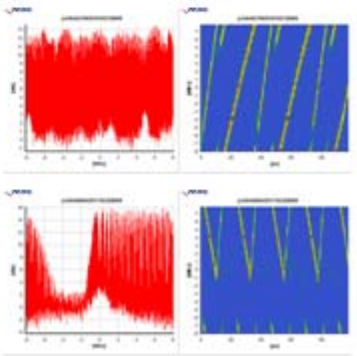
STRIKE3 Score Card available from project web page www.gnss-strike3.eu



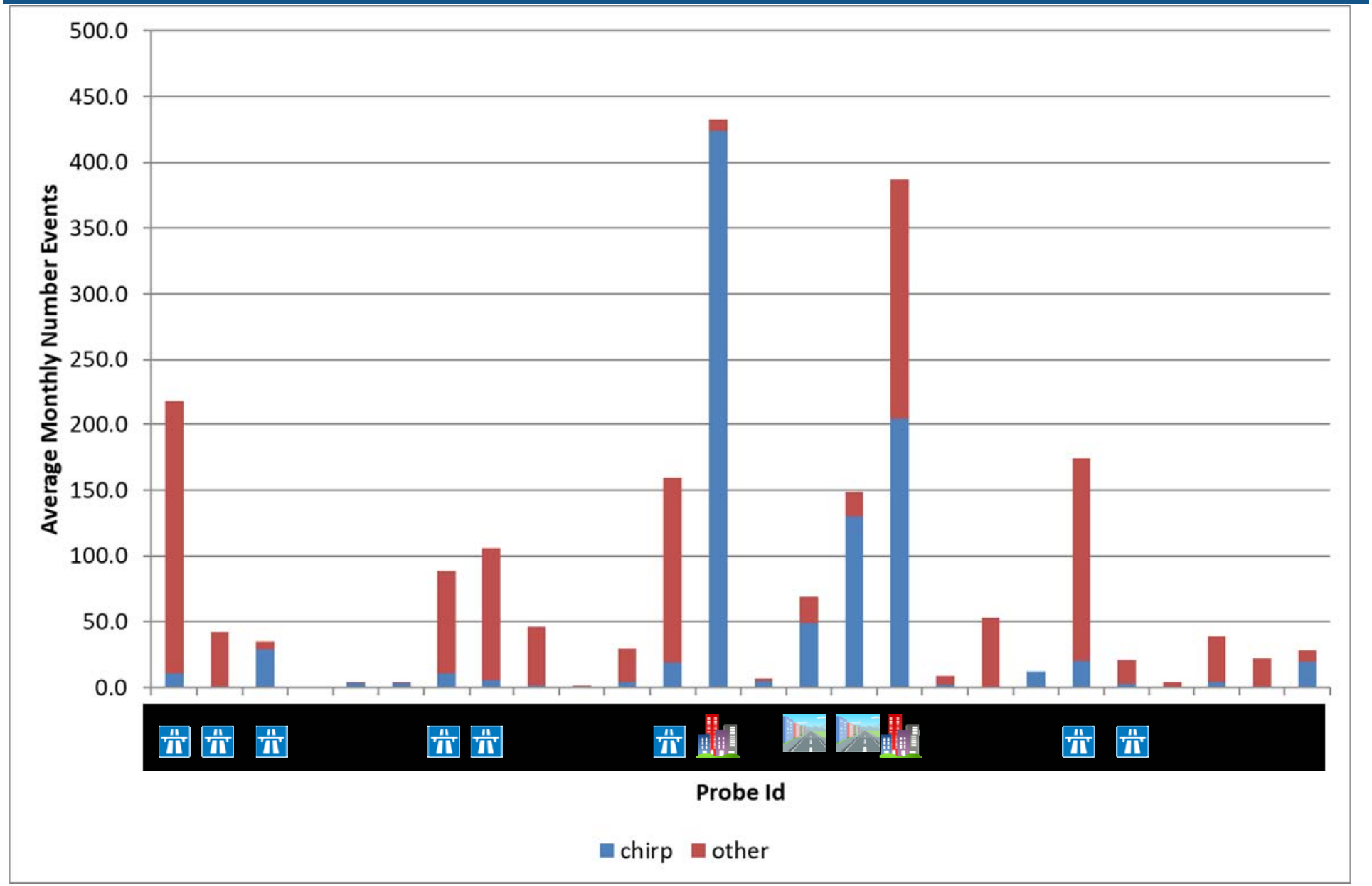
Typical “Chirp” Jammer Waveforms



- **There are lots of jammer waveforms, characterised by:**
  - Bandwidths, power, centre frequency, signal(s)
  - Additional parameters: sweep rate, direction, return

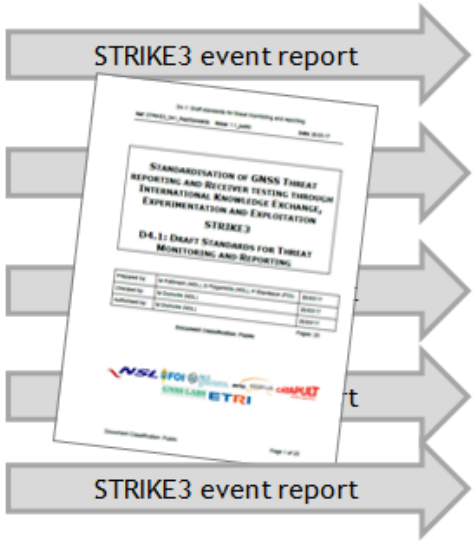


Comparison between Multiple Sites



STRIKE3 “Systems of Systems” Database

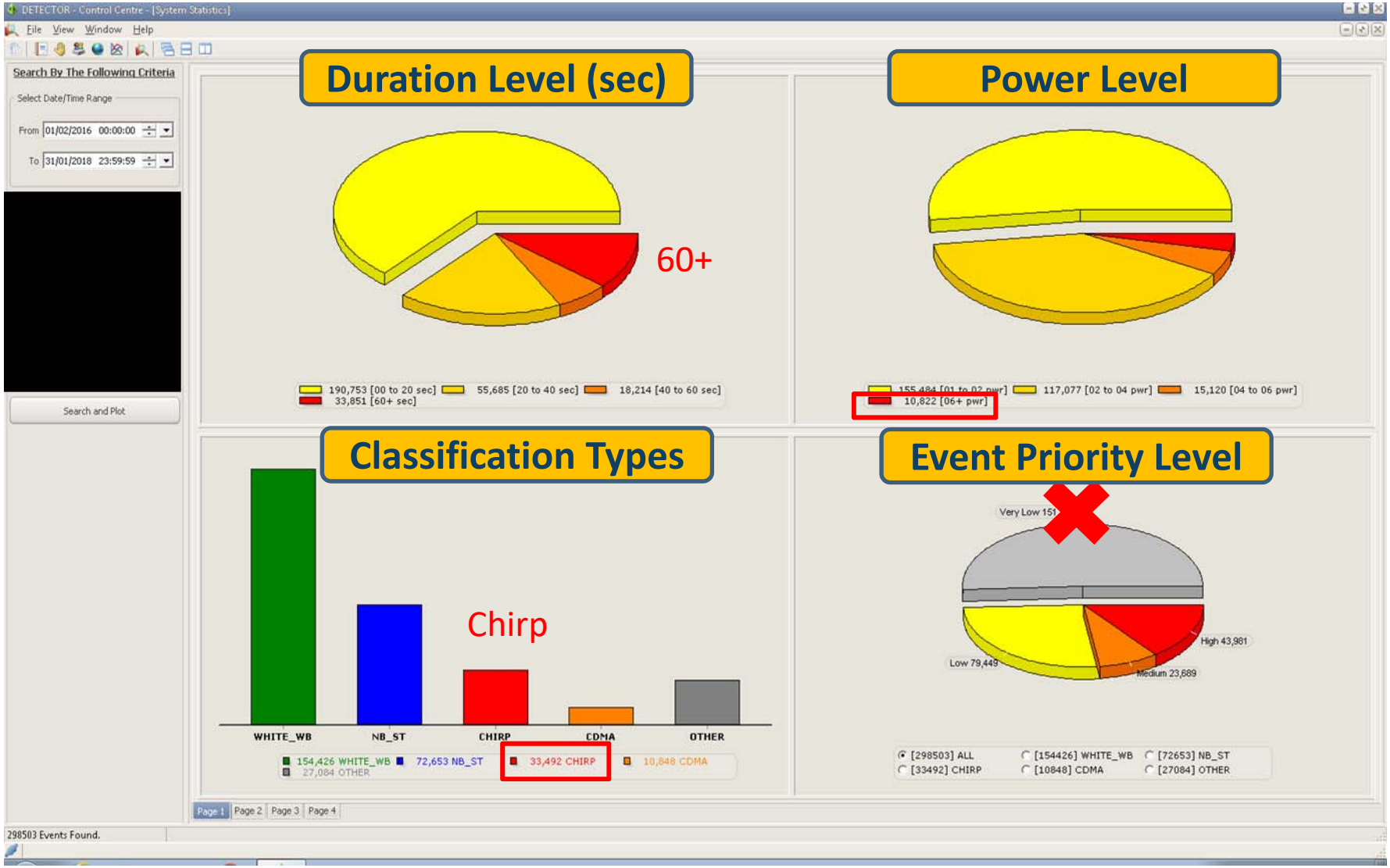
- Ensure event reports from different monitoring systems are compatible
- Minimise changes to existing monitoring system equipment
- Limit “sensitive” information that needs to be sent (and stored)
- Protect against data “Integrity” issues (copies/changes)
- Flexibility in data provision and analysis



System-of-systems
RF Interference database

„Draft Standards for Threat Monitoring and Reporting“ available from www.gnss-strike3.eu

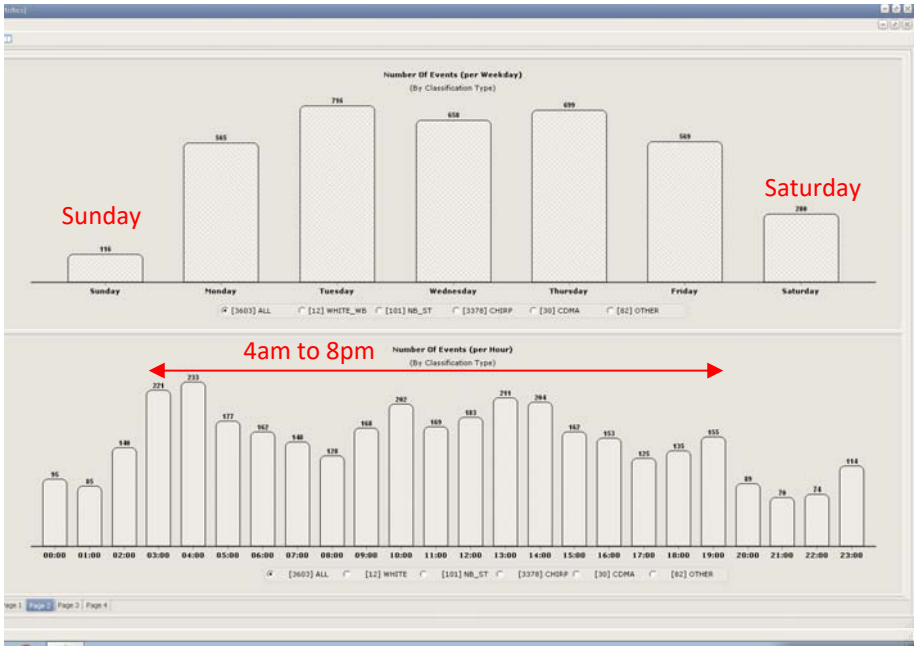
Overall 2-Year Activity



Example Event Time Analysis

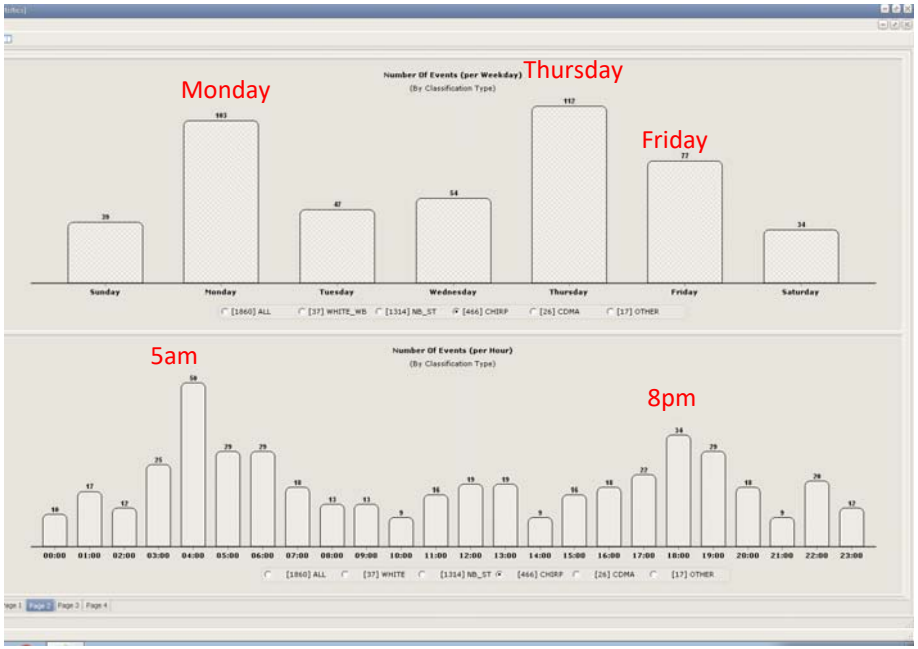
Example I: City Centre Site

- Very active
- Clearly reduced activity at weekends
- Generally increased activity during the day

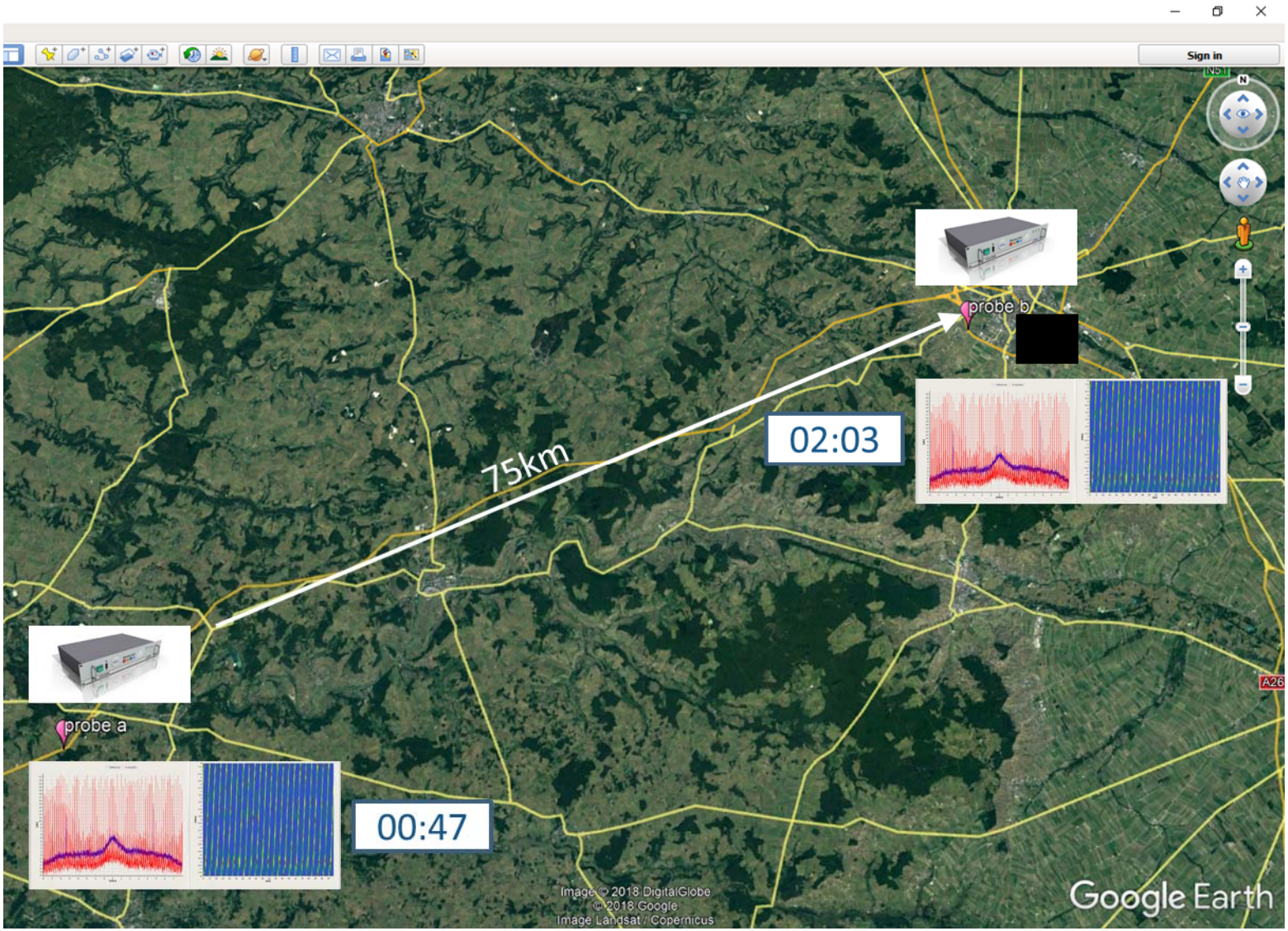


Example II: Highway Site

- Fairly active
- Shows increased activity on certain days
- Shows morning and evening peaks

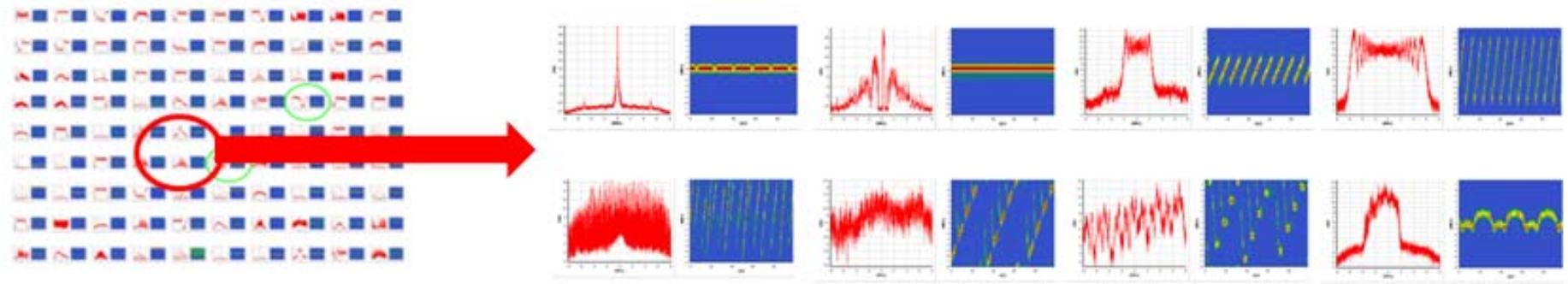


Track-a-jammer

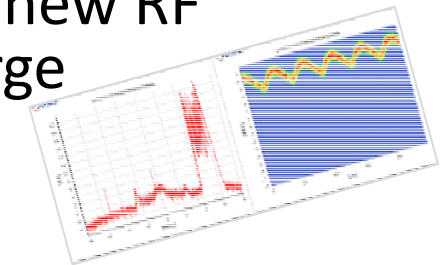


STRIKE3 Receiver Test Standards

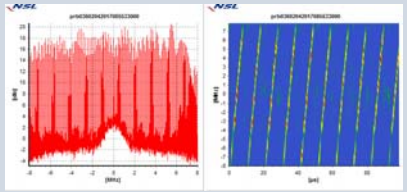
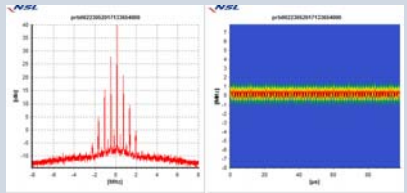
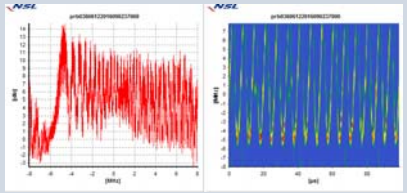
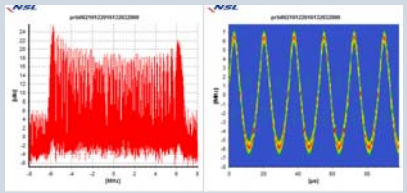
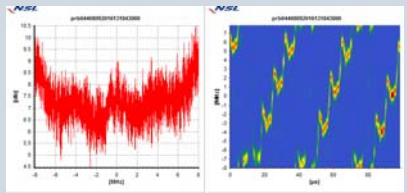
- The purpose is to assess GNSS receiver performance when subjected to “real-world” GNSS threats.
- Develop an outline test specification which can be used to assess performance of different GNSS receivers under a range of typical interference/jamming threats.



- The test standard shall be based on a generic series of threats as detected during the monitoring campaign.
- The test standard should evolve to incorporate new RF interference and jamming threats as they emerge

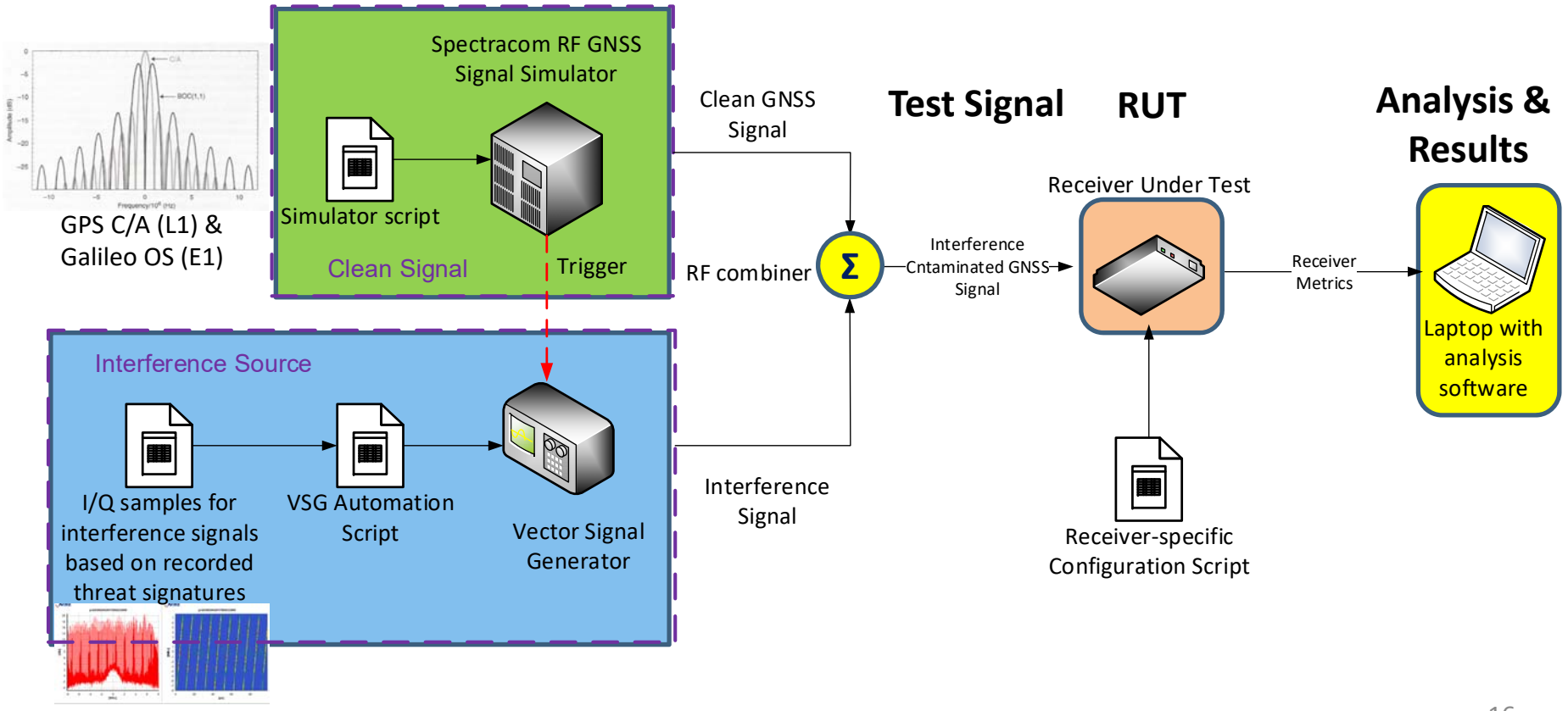


Selected Threat Signatures for Testing

Type of signal	Example Plots	Reason for choice	Options
Wide Sweep – fast repeat rate		Very common (total number of events, and number of sites)	1. Raw I/Q data from Detector 2. Synthetic I/Q data to represent real signal
Narrow band at L1		Example unintentional signal – this type seen on multiple occasions and at multiple sites	1. Raw I/Q data from Detector 2. Synthetic I/Q data to represent real signal
Triangular		Common (and number of sites)	1. Raw I/Q data from Detector 2. Synthetic I/Q data to represent real signal
Triangular wave		Common (and number of sites)	1. Raw I/Q data from Detector 2. Synthetic I/Q data to represent real signal
Tick		Quite common. Evolving threat (new type).	1. Raw I/Q data from Detector

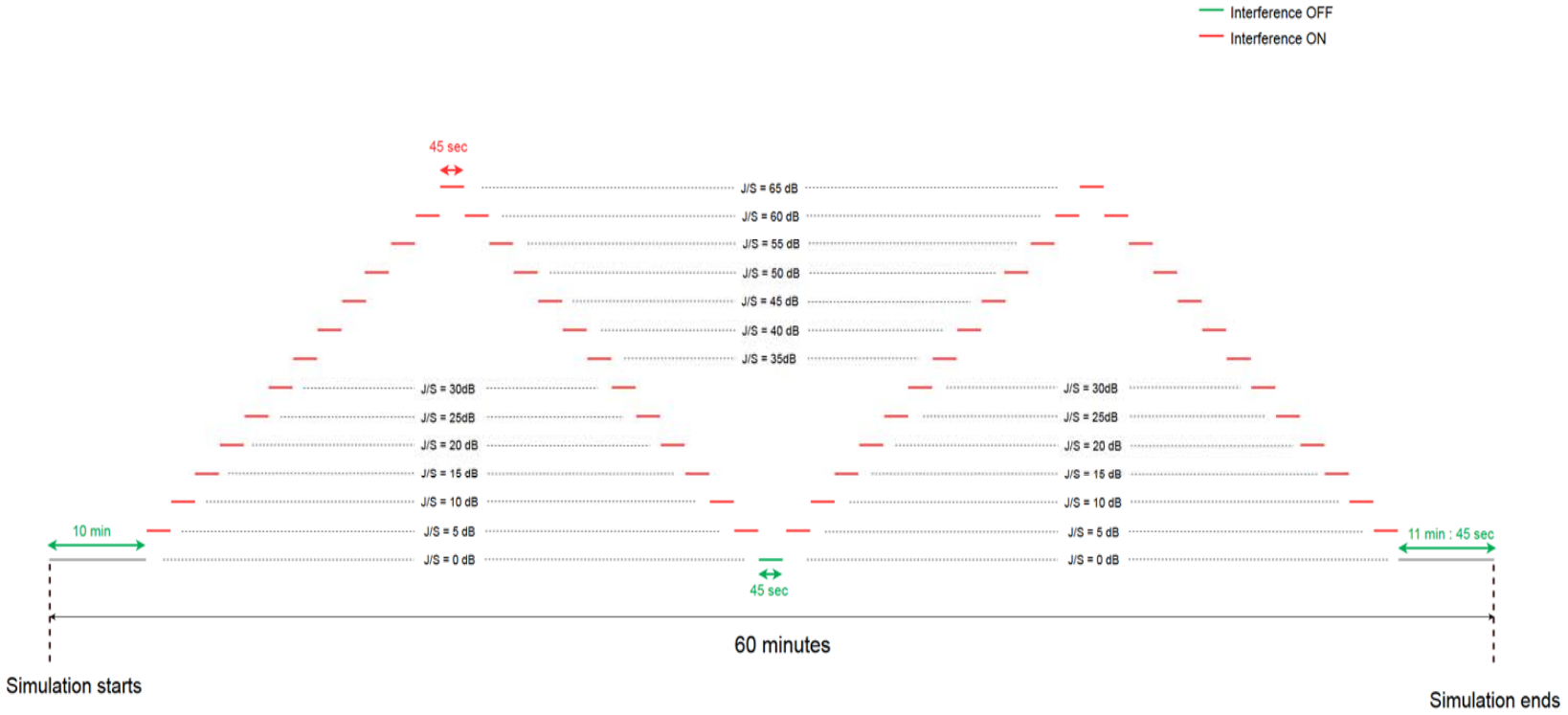
STRIKE3 Test Architecture Overview

- Lab tests based on simulated GNSS signals (60°N / 24°E / 30m)
  - Easy to control, repeatable
- Interference signals added to clean GNSS signals (as recorded in real life)



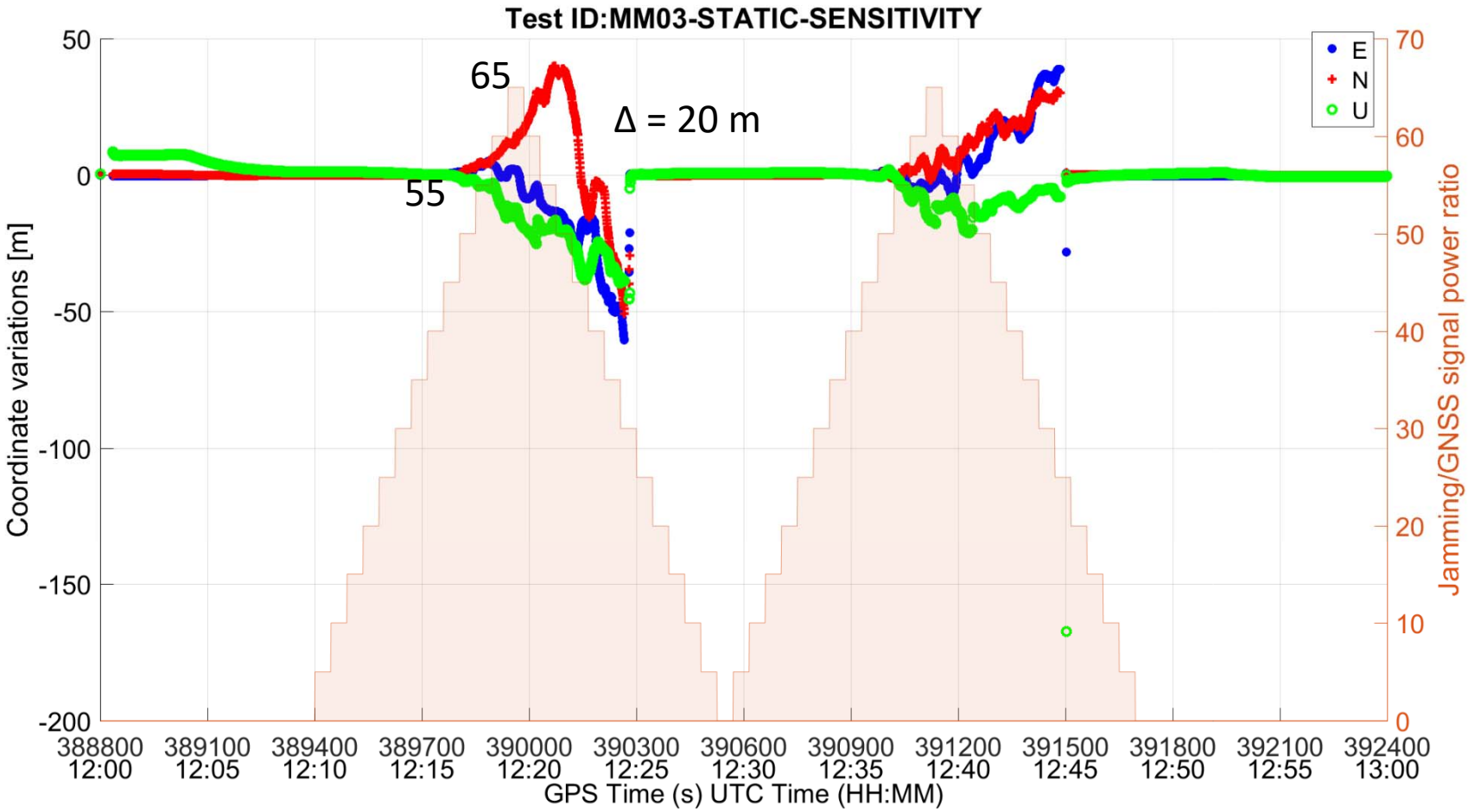
Test methodology: Sensitivity

This test is conducted by varying the power of the interference test signal. The interference is switched on 10 minutes after the simulation starts. The initial interference power is such that J/S is 5 dB, and then the interference power is increased by 5 dB every 45 seconds, up to a maximum J/S of 65 dB. Then, the interference power is decreased by 5 dB every 45 seconds. This is done twice. The total duration of the test is 60 minutes.



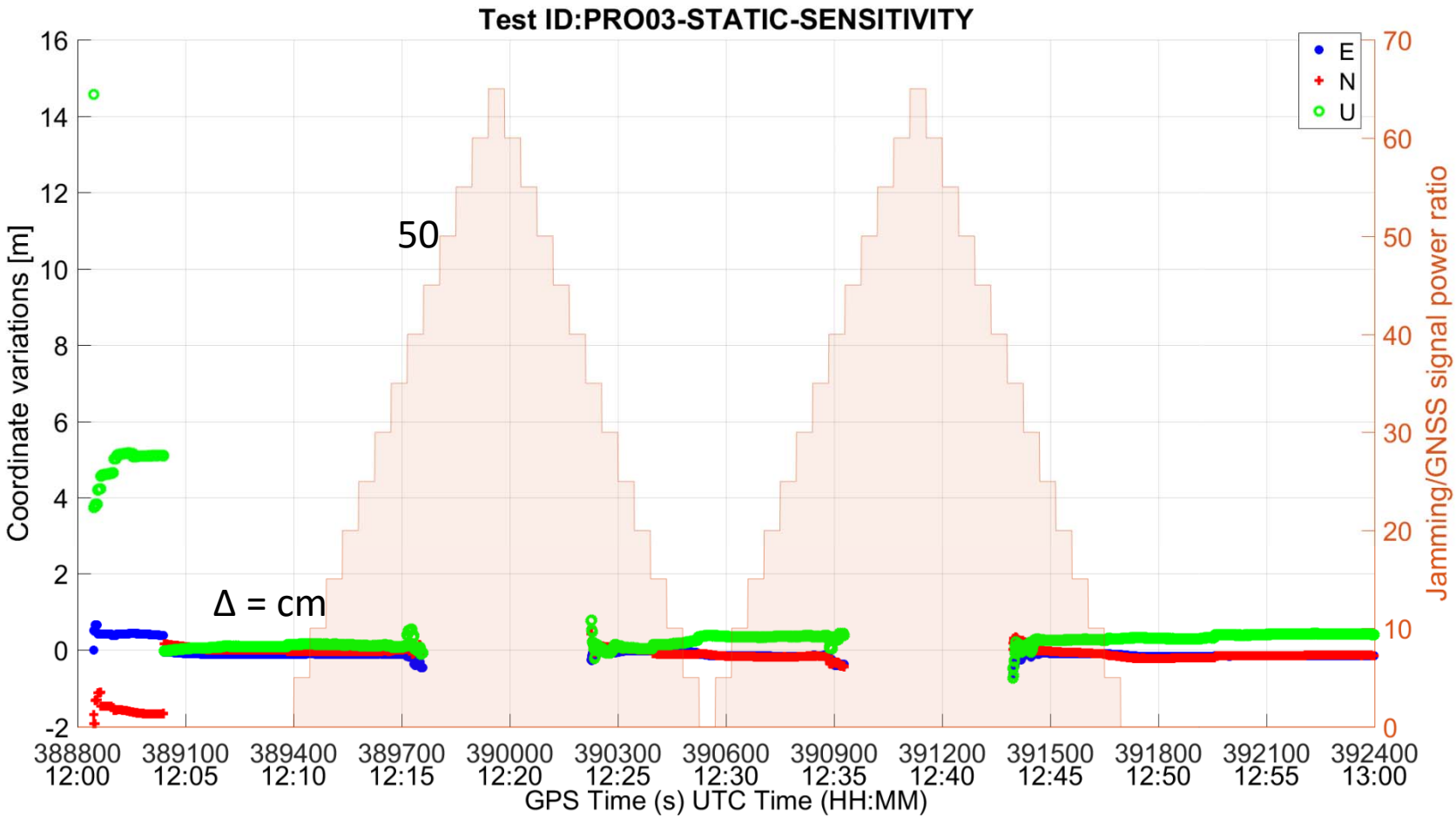
MM03-STATIC-SENSITIVITY:
ENU variations with respect to true position

RUT Mass Market Receiver



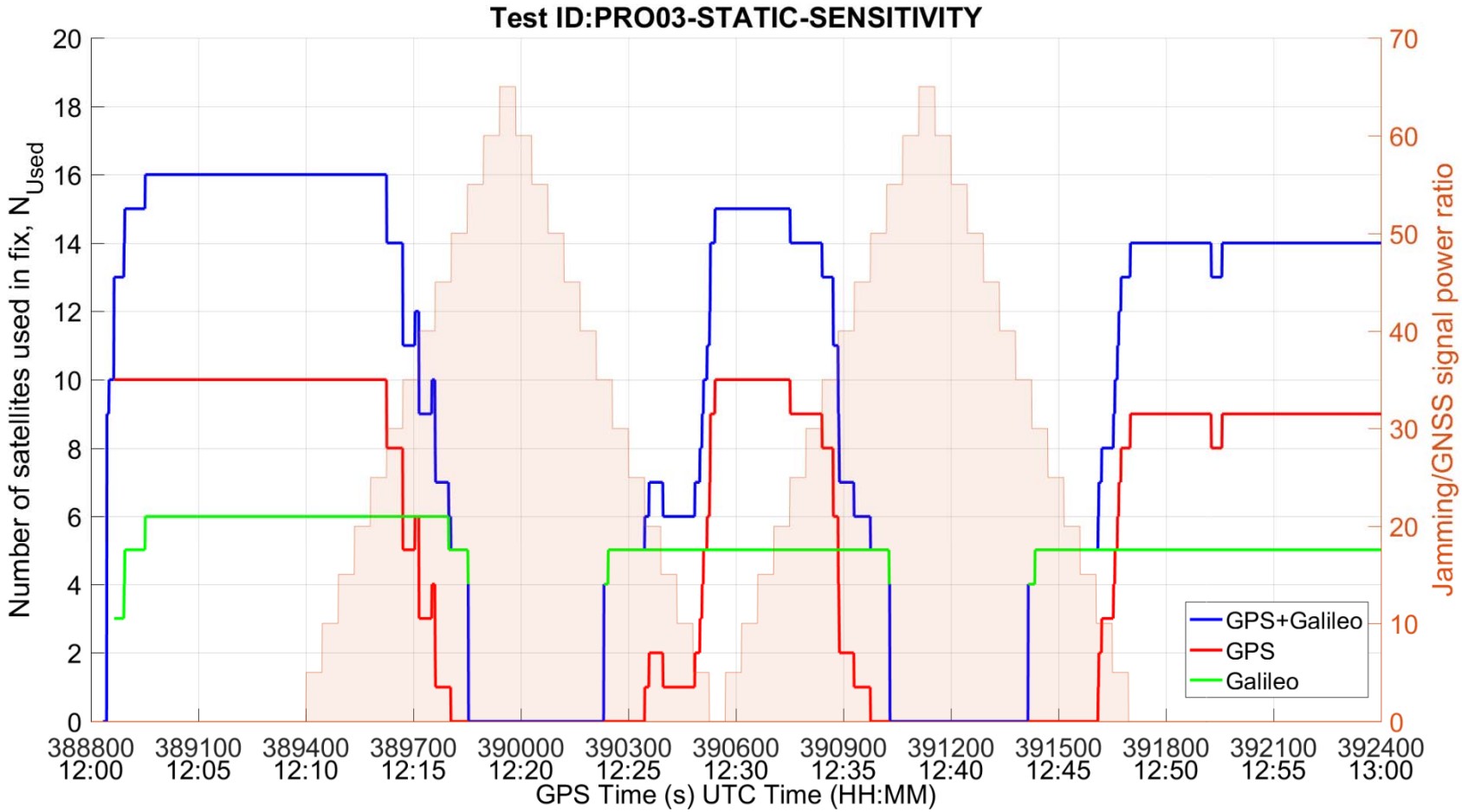
PRO03-STATIC-SENSITIVITY:
ENU variations with respect to true position

RUT Professional Grade Receiver



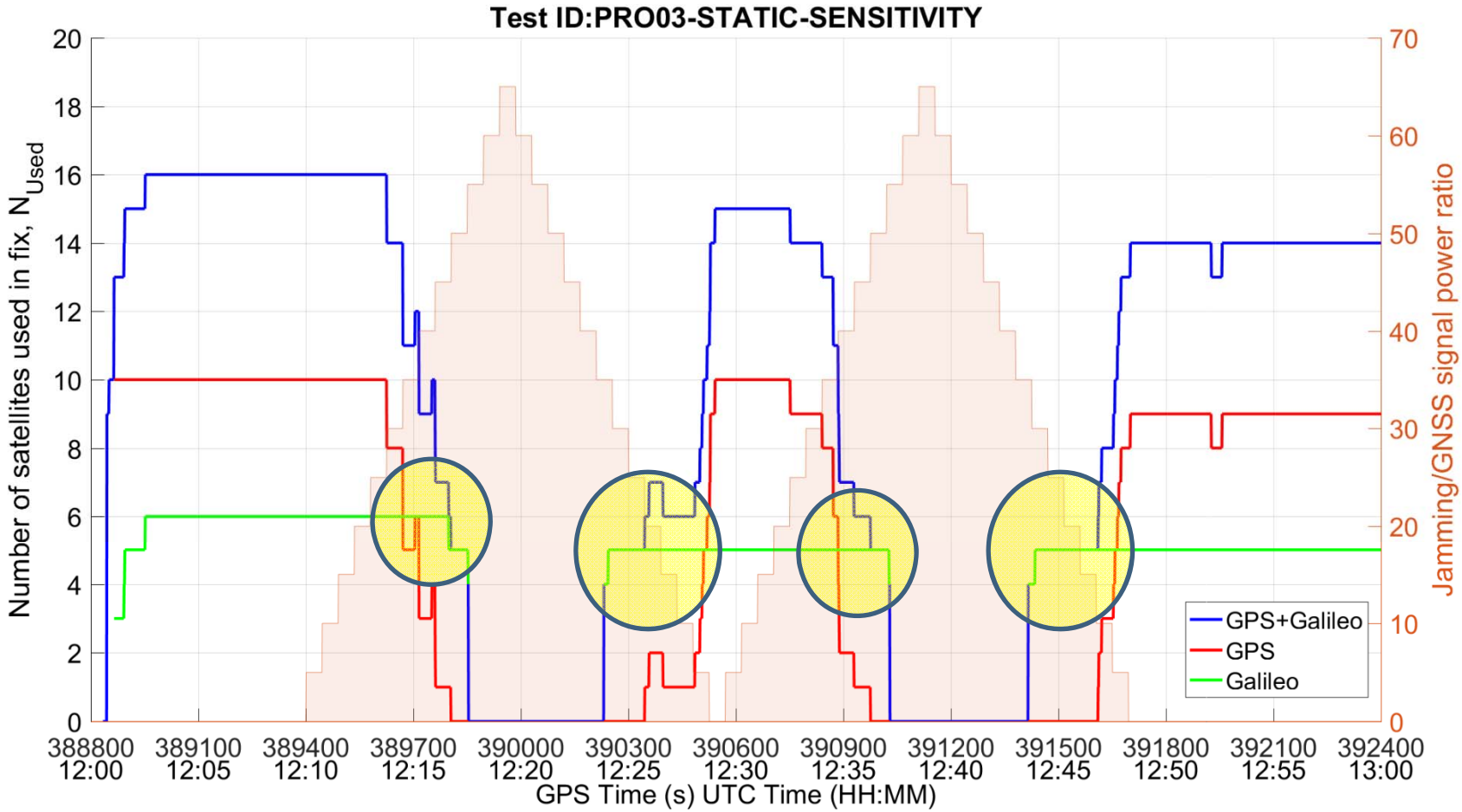
PRO03-STATIC-SENSITIVITY: Number of Satellites used in Fix (N_{Used})

RUT Professional Grade Receiver



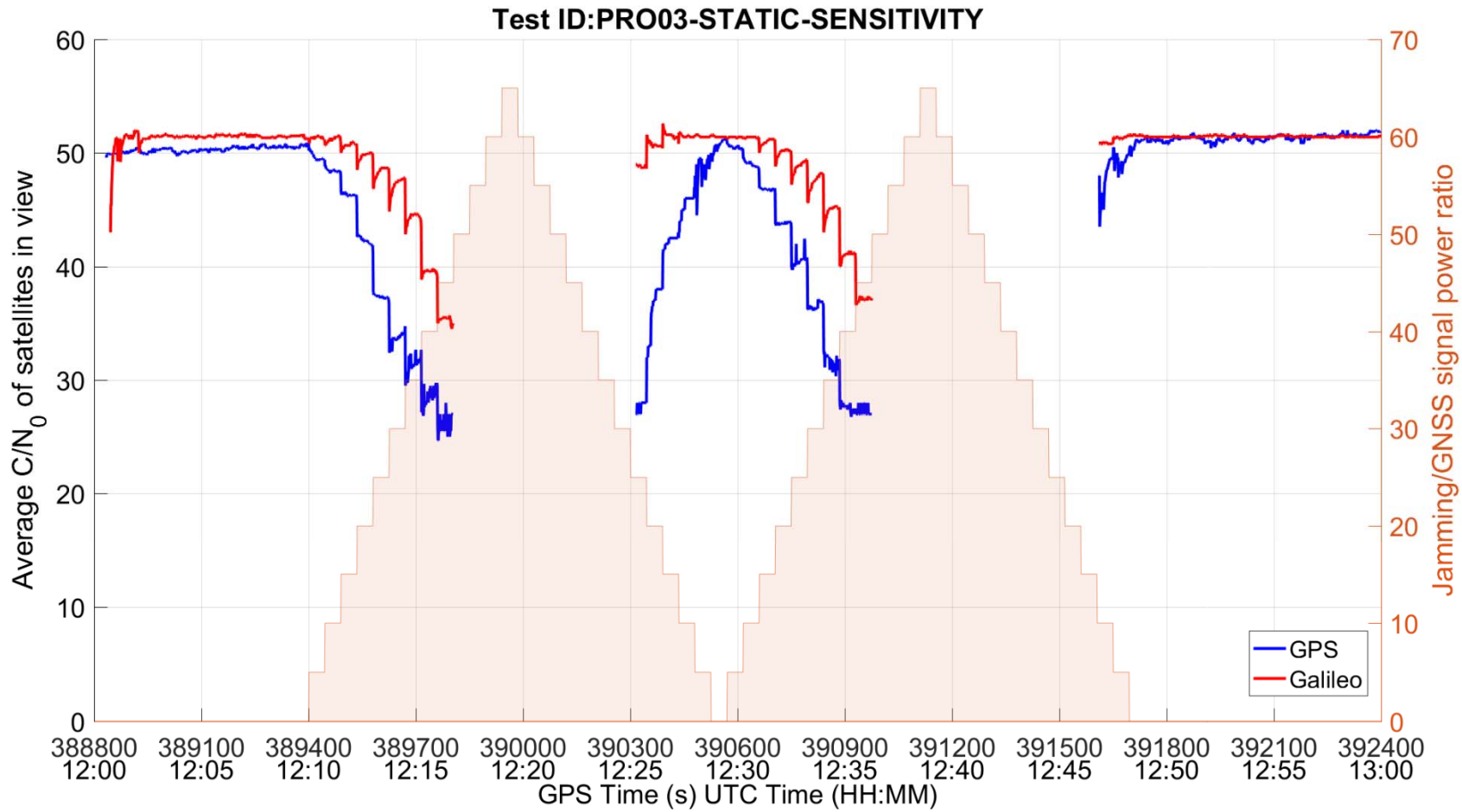
PRO03-STATIC-SENSITIVITY: Number of Satellites used in Fix (N_{Used})

RUT Professional Grade Receiver



PRO03-STATIC-SENSITIVITY: Average C/No

RUT Professional Grade Receiver



STRIKE3 Draft Standards

- **Draft Standards for Threat Monitoring and Reporting**
- **Draft Standards for Receiver testing against threats**
  - Both available from www.gnss-strike3.eu

How you can contribute:

- Review draft standards
- Provide Feedback to Project team
  - Send mail to info@gnss-strike3.eu
- Use Project Forum for Discussions, Comments, Questions, ….
  - Recently installed at www.gnss-strike3.eu/forum

Thank You for Your Attention!

The work presented in this paper has been co-funded under the H2020 programme through the European GNSS Agency (GSA)

Project info at web: www.gnss-strike3.eu