STRIKE3

Outcomes of Long Term Monitoring of GNSS Threats and Receiver Testing

Michael Pattinson

NSL

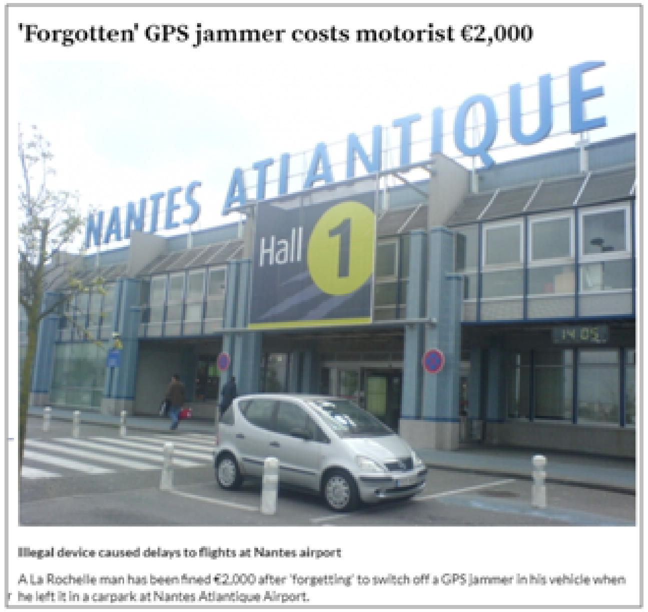
European
Global Navigation
Satellite Systems
Agency

HORIZON 2020

Baska
6-9 May 2018

GNSS Needs Protection

1. GNSS air navigation



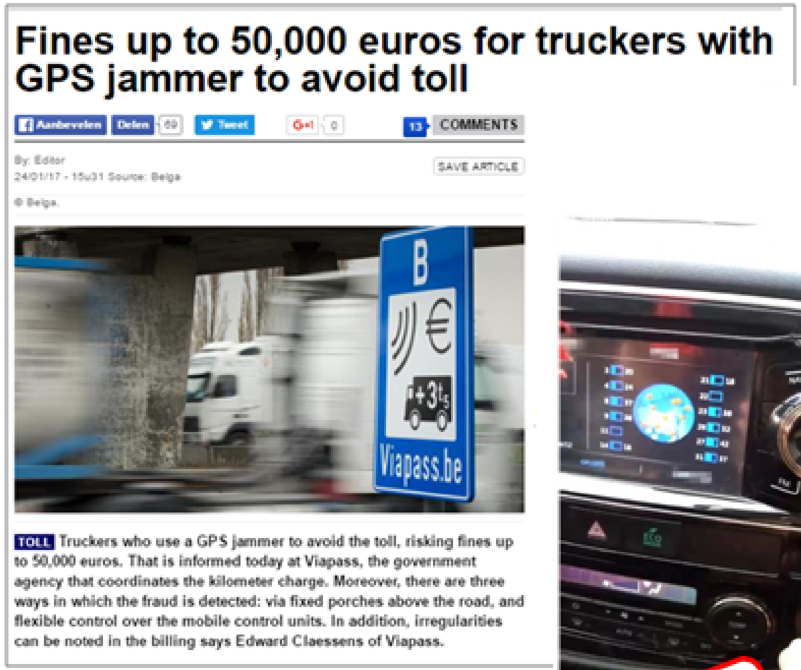
'Forgotten' GPS jammer costs motorist €2,000

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

2. GNSS road pricing



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

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

© 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

An initiative to protect our GNSS ...

STRIKE3

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

STRIKE3

HORIZON 2020

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

NSL FOI NLS FINNISH GEOSPATIAL RESEARCH INSTITUTE FGI

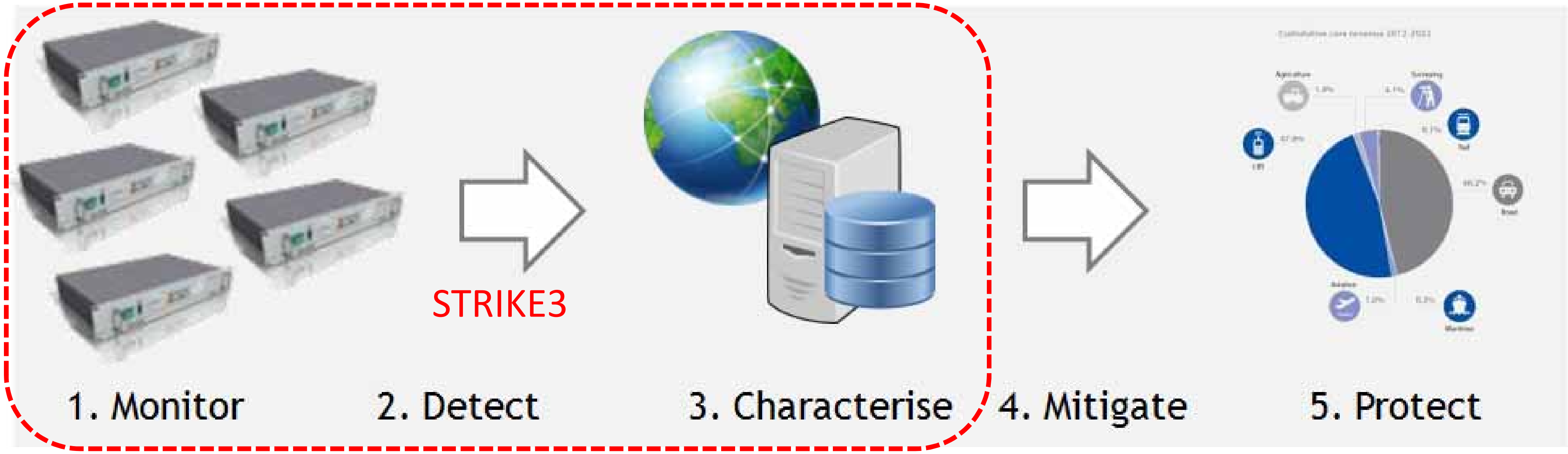
aric automotive + rail innovation center aachen

CATAPULT Satellite Applications

GNSS LABS ETRI

STRIKE3 Project Overview

STRIKE3



STRIKE3

1. Monitor
2. Detect
3. Characterise
4. Mitigate
5. Protect

- STRIKE3 provides a response at an international level to ensure that there is:

i. a standard for GNSS threat reporting and analysis

ii. a standard for assessing the performance of GNSS receivers and applications under threat.

STRIKE3 Monitoring Equipment

STRIKE3

DETECTOR

GSS100D – Interference detector

- ➢ GPS/EGNOS/Galileo L1/E1

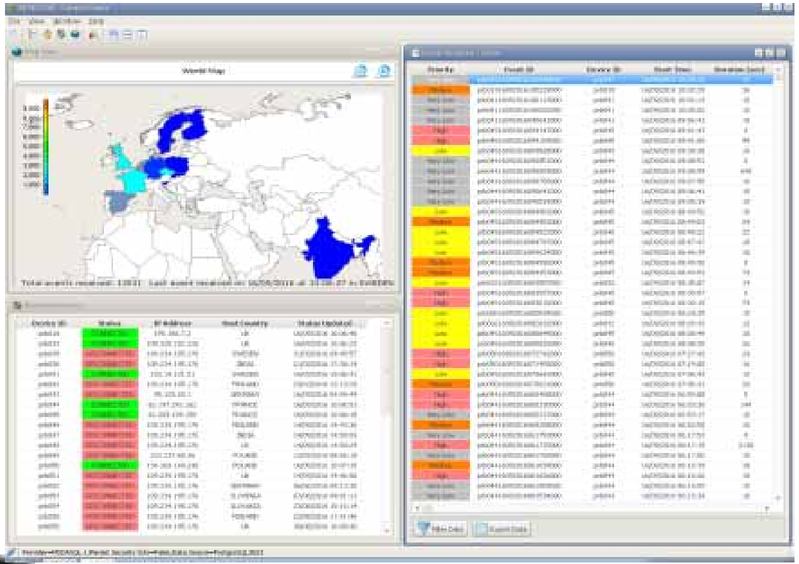
GSS200D – Interference detector

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

GSS200D' – Interference detector

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

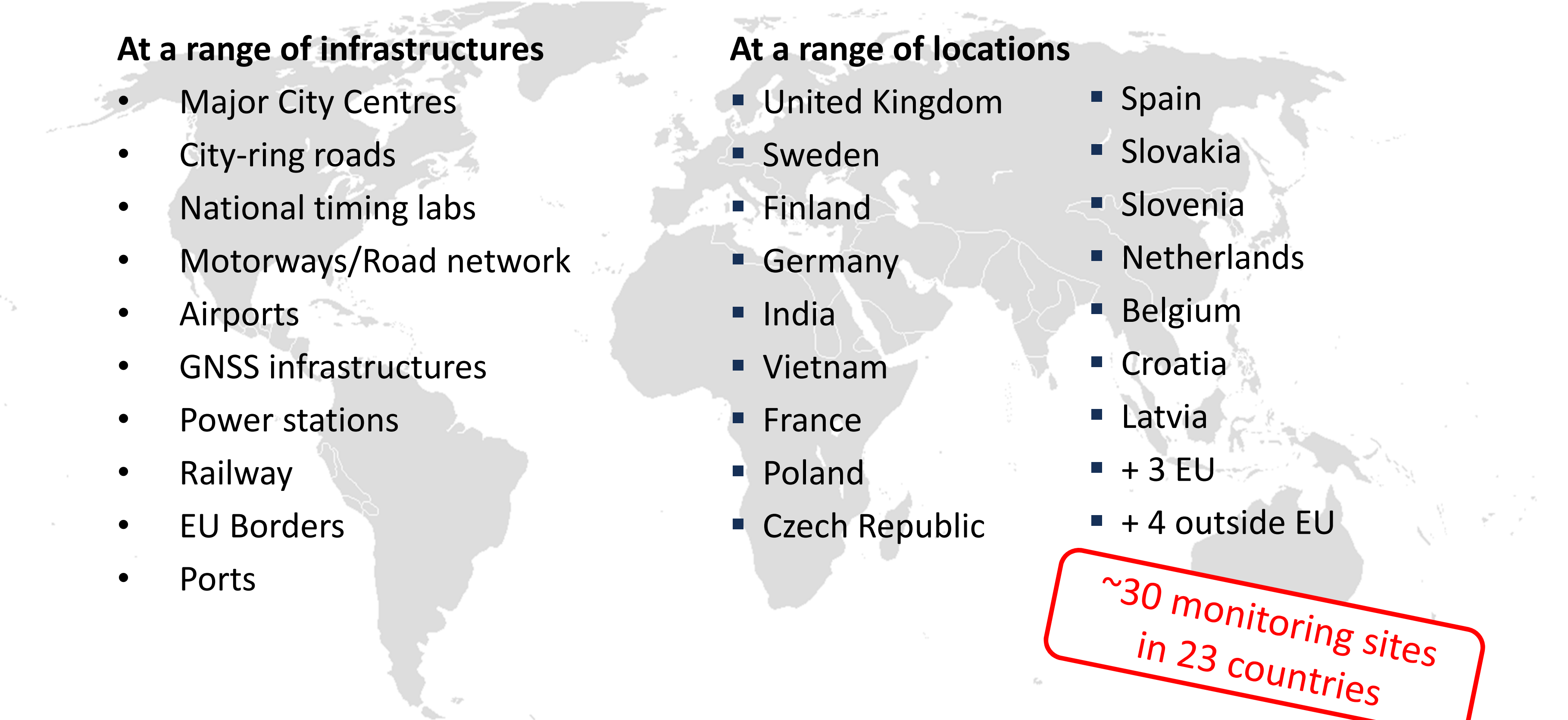
RF-Oculus



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

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

STRIKE3 International Network



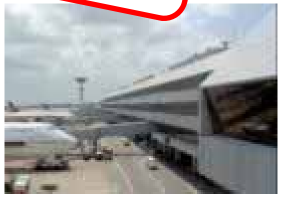
At a range of infrastructures

- 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

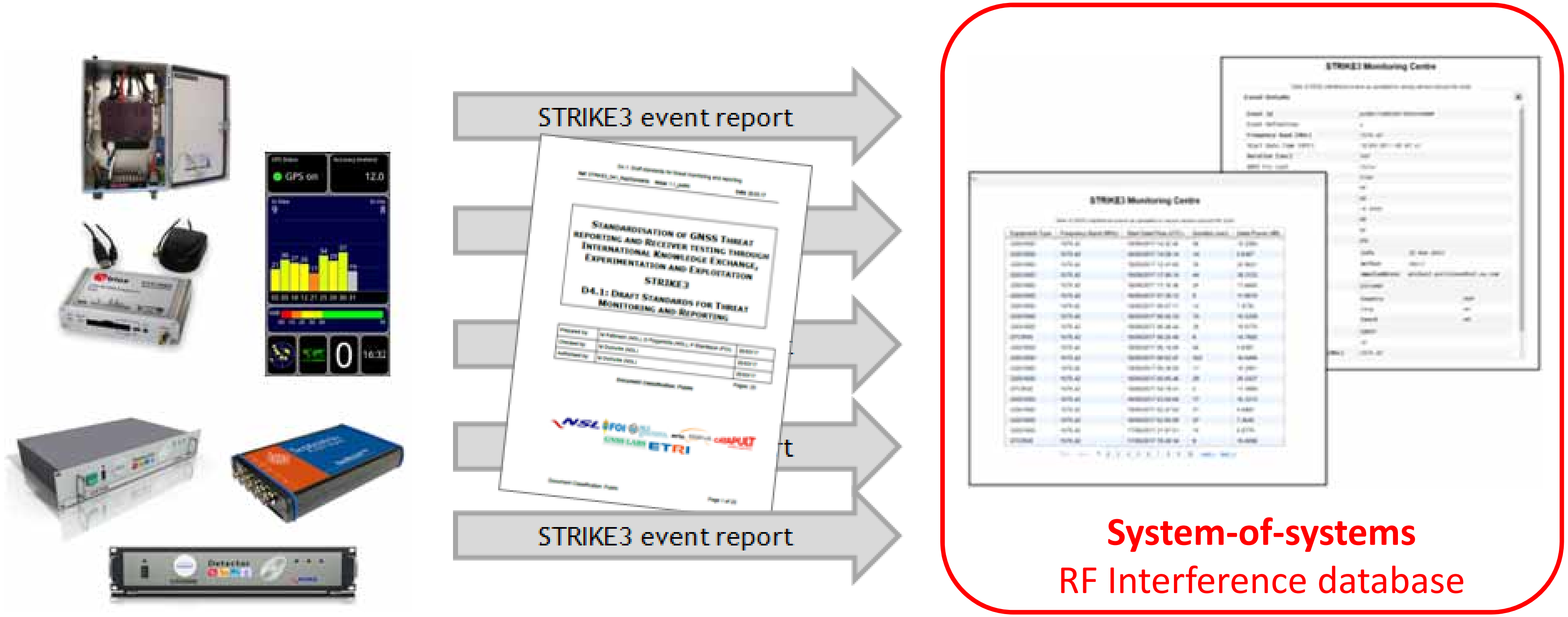
- United Kingdom
- Sweden
- Finland
- Germany
- India
- Vietnam
- France
- Poland
- Czech Republic
- Spain
- Slovakia
- Slovenia
- Netherlands
- Belgium
- Croatia
- Latvia
- + 3 EU
- + 4 outside EU

~30 monitoring sites in 23 countries



STRIKE3 “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



STRIKE3 event report

STANDARDISATION OF GNSS THREAT REPORTING AND RECEIVER TESTING THROUGH INTERNATIONAL KNOWLEDGE EXCHANGE, EXPERIMENTATION AND EXPLOITATION

STRIKE3

D4.1: DRAFT STANDARDS FOR THREAT MONITORING AND REPORTING

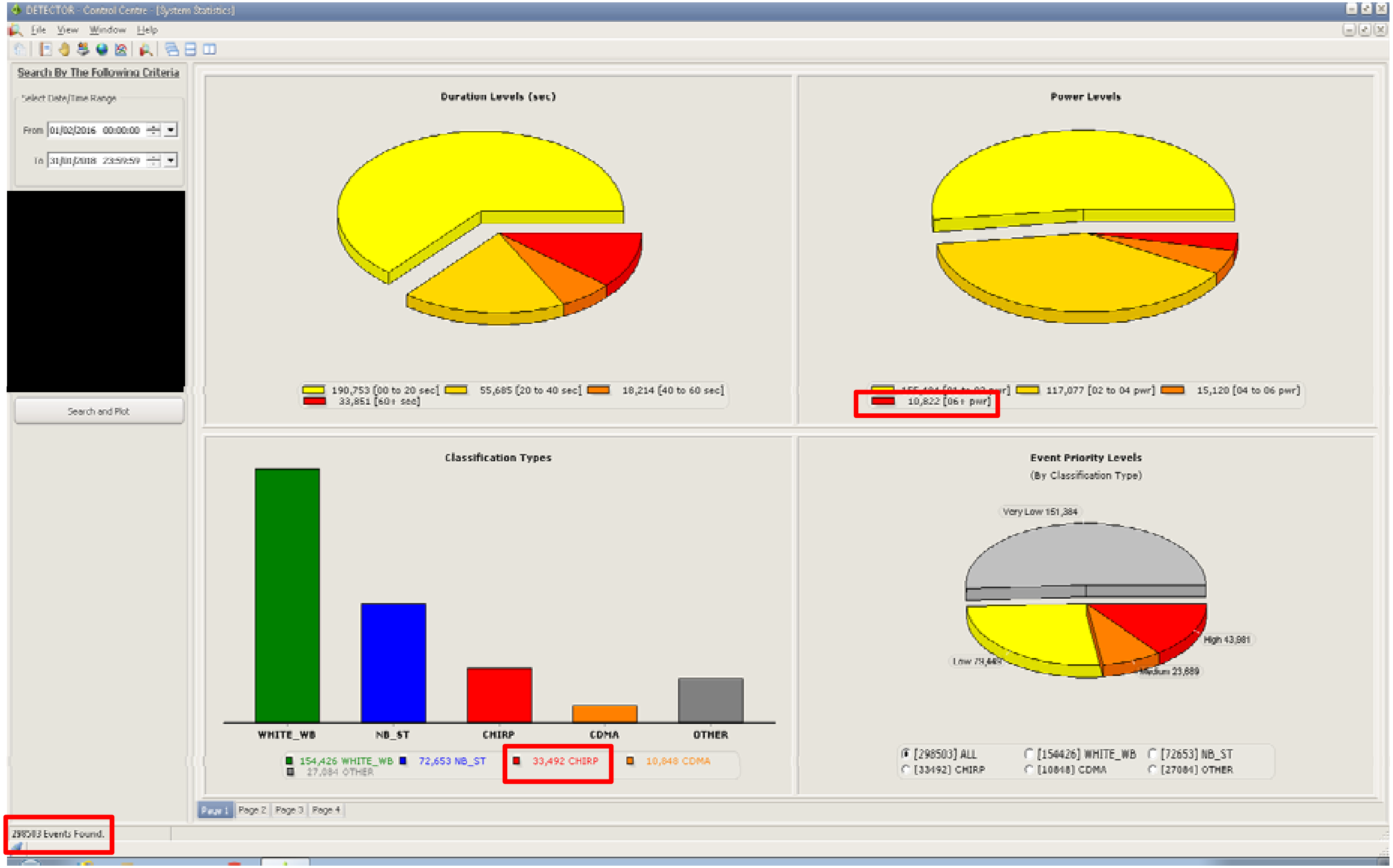
STRIKE3 event report

System-of-systems

RF Interference database

Overall 2-Year Activity

STRIKE3



DETECTOR - Control Centre - [System Statistics]

Search By The Following Criteria

Select Date/Time Range

From 01/02/2016 00:00:00

To 31/01/2018 23:59:59

Duration Levels (sec)

🟨 190,753 [00 to 20 sec] 🟨 55,685 [20 to 40 sec] 🟧 18,214 [40 to 60 sec] 🟥 33,851 [60+ sec]

Power Levels

🟨 155,484 [01 to 02 pwr] 🟨 117,077 [02 to 04 pwr] 🟧 15,120 [04 to 06 pwr] 🟥 10,822 [06+ pwr]

Classification Types

🟩 154,426 WHITE_WB 🟦 72,653 NB_ST 🟥 33,492 CHIRP 🟧 10,848 CDMA ⬛ 27,084 OTHER

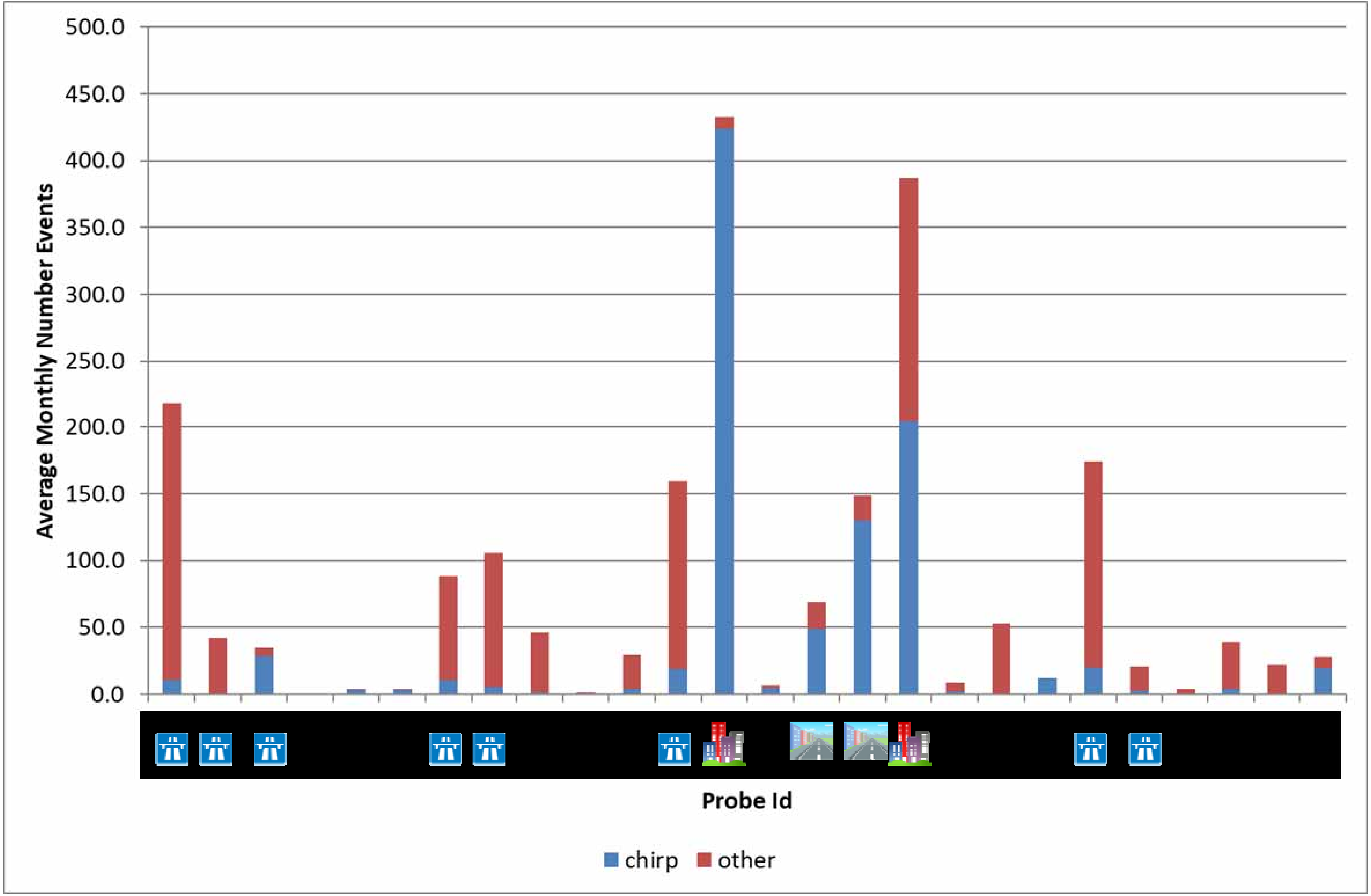
Event Priority Levels
(By Classification Type)

● [298503] ALL ○ [154426] WHITE_WB ○ [72653] NB_ST
○ [33492] CHIRP ○ [10848] CDMA ○ [27084] OTHER

298503 Events Found.

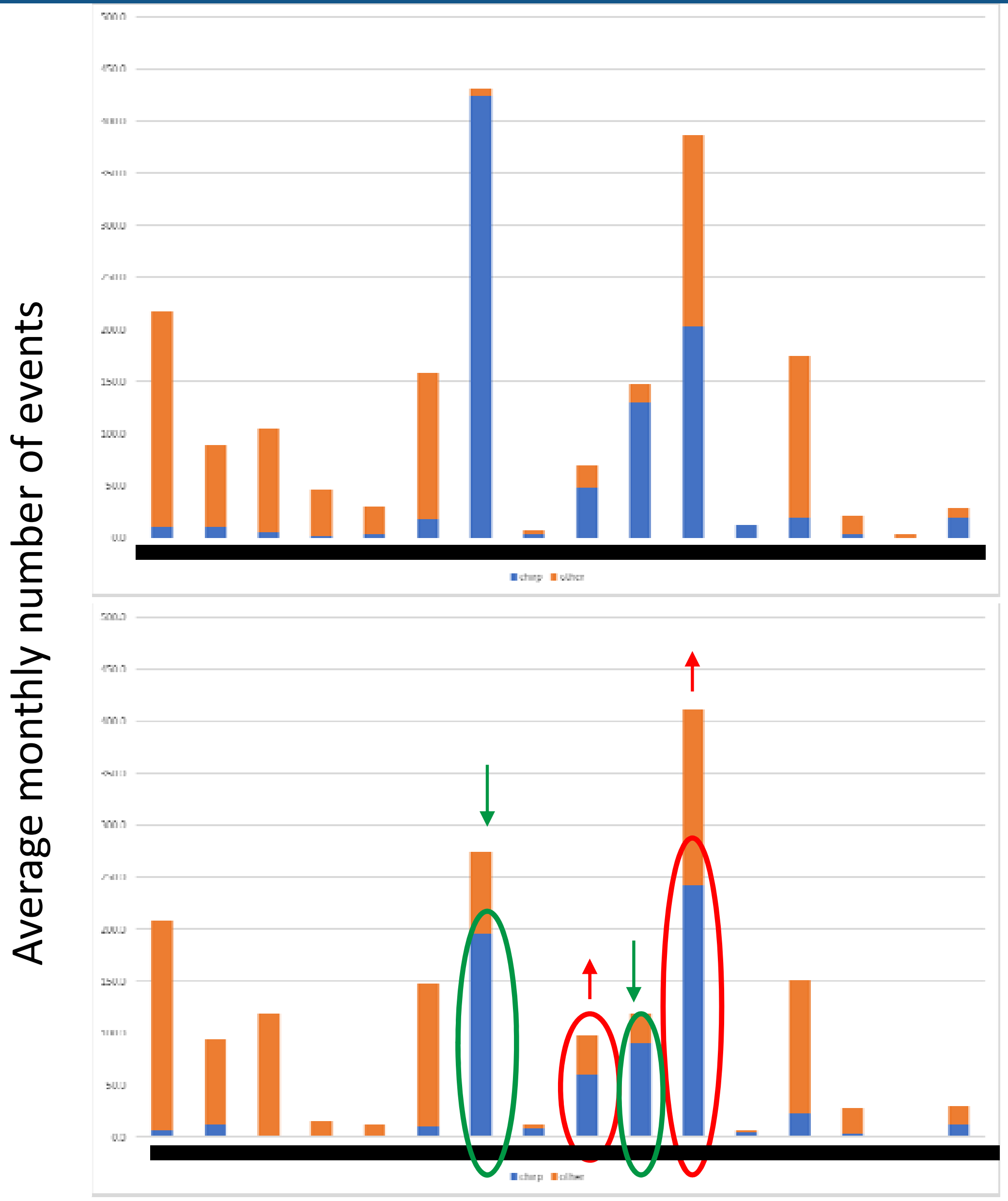
Comparison between Multiple Sites

STRIKE3



Comparison of Site Activity over Time

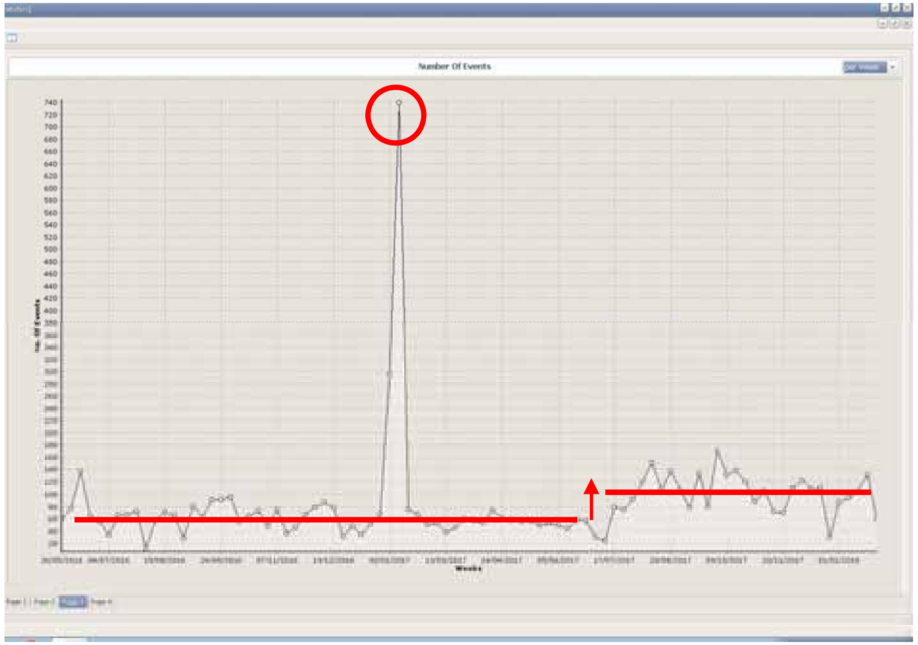
STRIKE3

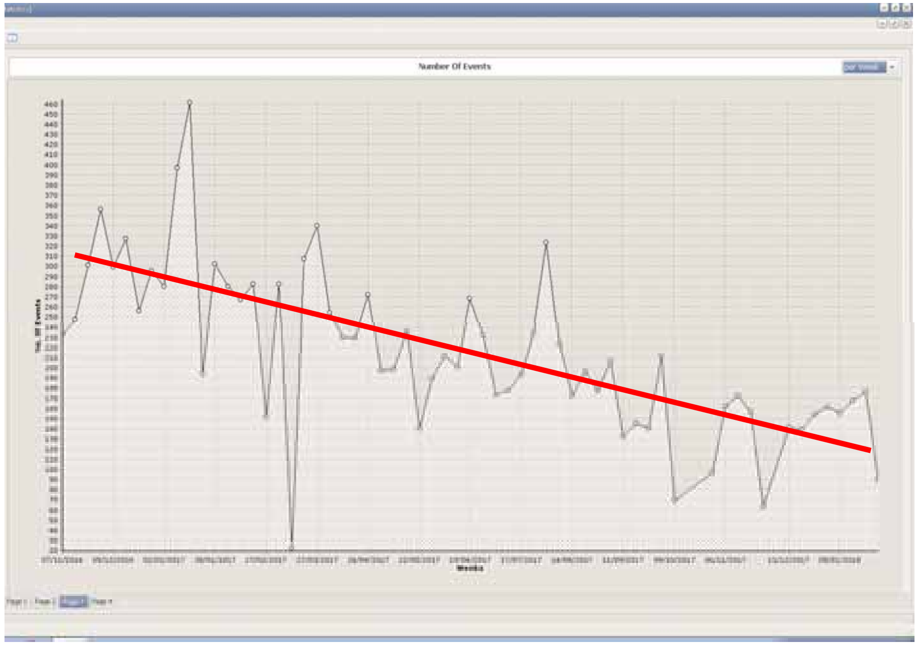


Year 1

Year 2

Example Changes in Site Activity



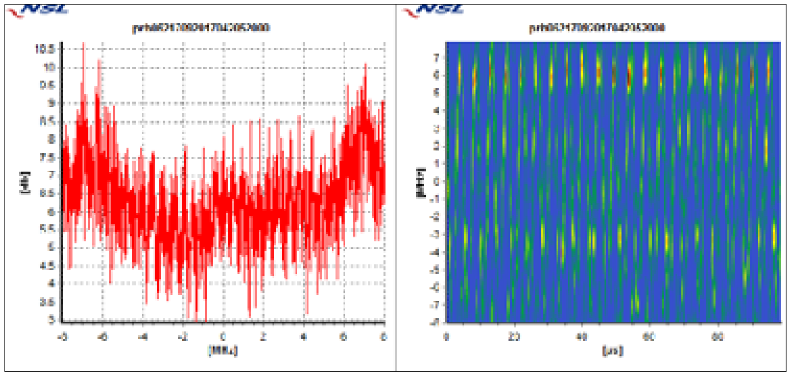


- City Centre Site
- One week with very high activity (>700 events!)
- General increase in weekly activity after Oct 2017 (from 60 to 100 per week)

- City Centre Site
- Gradual decrease in weekly activity since installation
  - From 300 to 150 per week

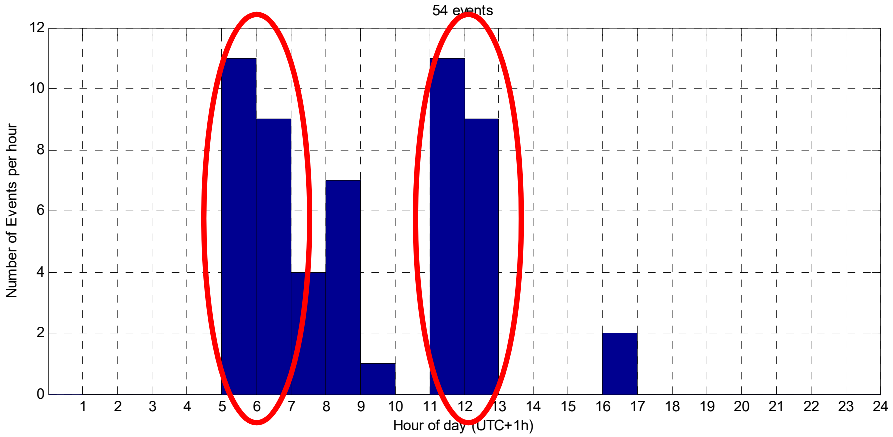
Repeating Jammer at a Site

Example event on 17/09/2017 recorded at 04:21:18 UTC

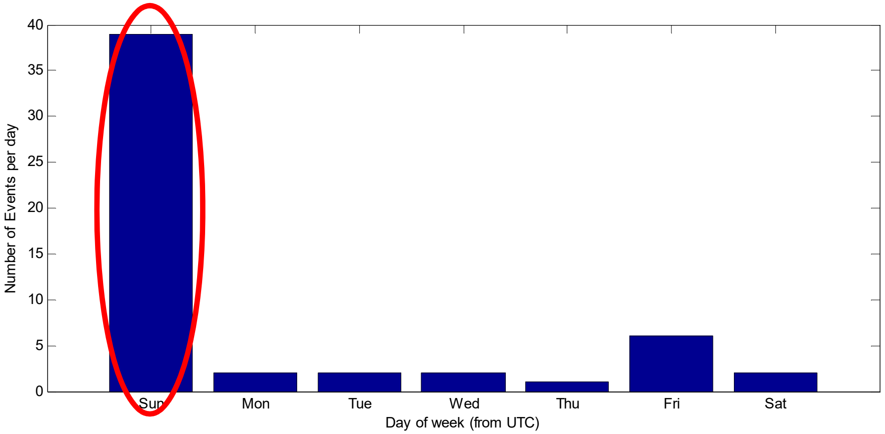


(a)

- Jamming signal at airport site
- Detected almost exclusively on Sundays
- Usually twice per day – morning and early afternoon



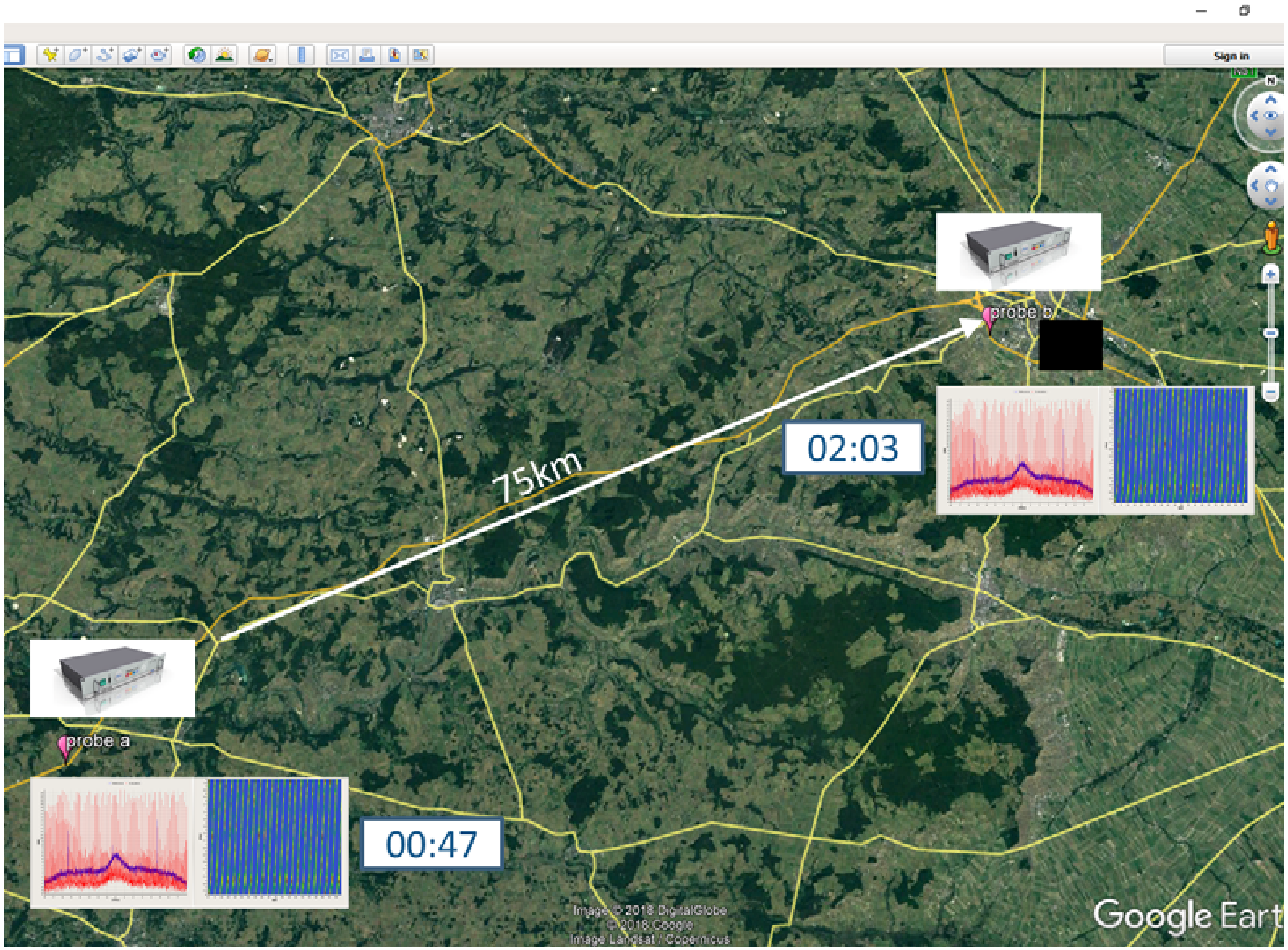
(b)



(a)

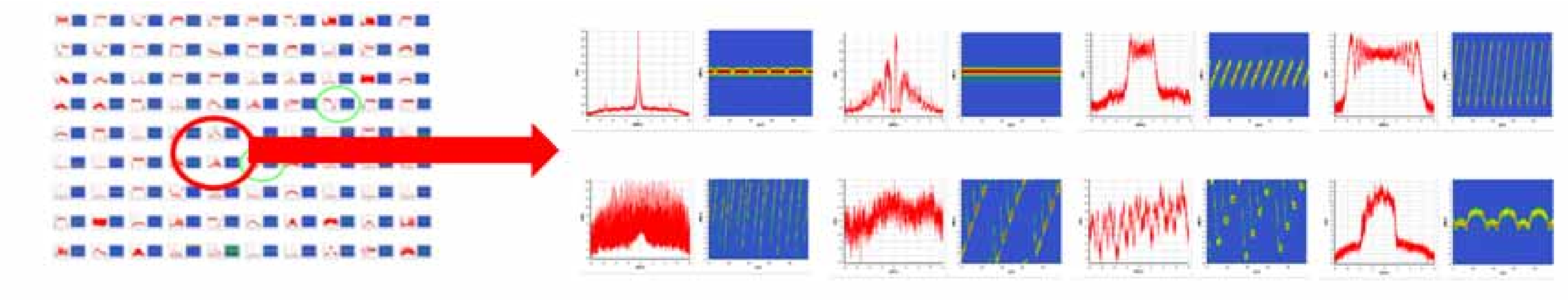
Track-a-jammer

STRIKE3

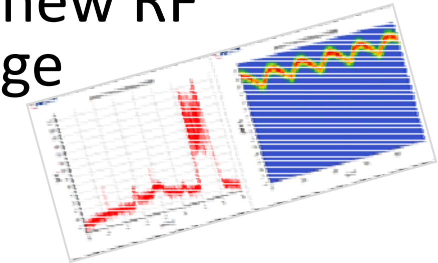


STRIKE3 Receiver Test Standards

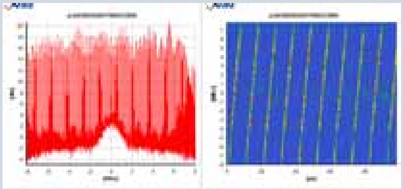
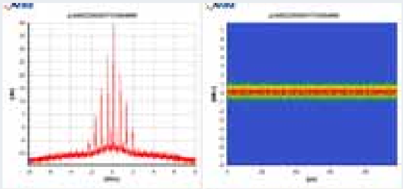
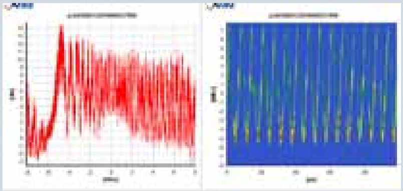
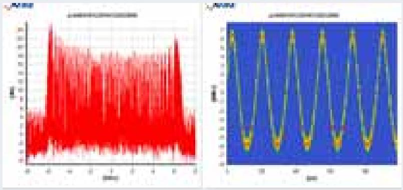
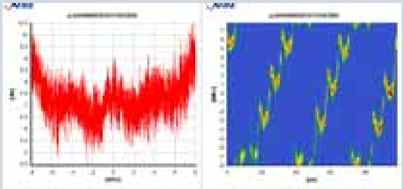
- The purpose is to assess GNSS receiver performance when subjected to “real-world” GNSS threats.
- Develop an outline test specification which can be used to assess performance of different GNSS receivers under a range of typical interference/jamming threats.



- 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

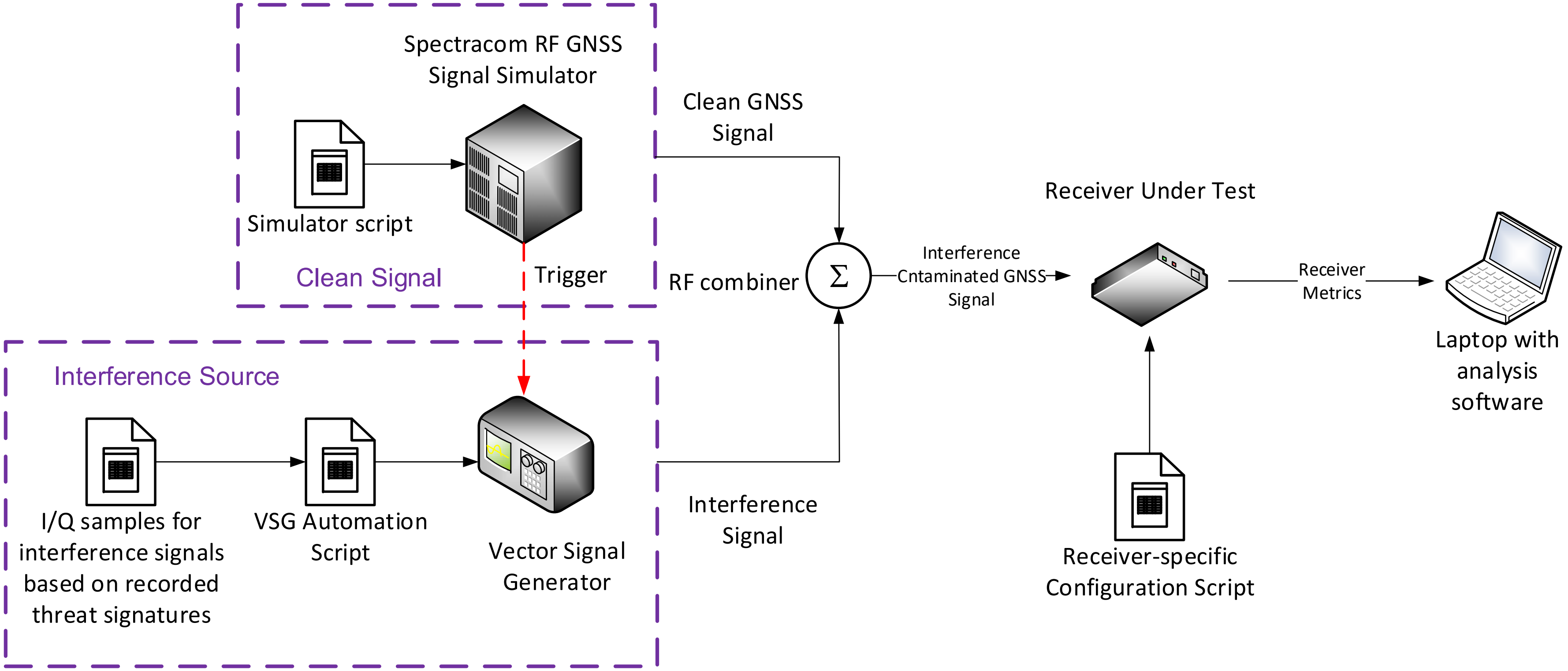


Selected Threat Signatures for Testing

Type of signal	Example Plots	Reason for choice
Wide Sweep – fast repeat rate		Very common (total number of events, and number of sites)
Narrow band at L1		Example unintentional signal – this type seen on multiple occasions and at multiple sites
Triangular		Common (and number of sites)
Triangular wave		Common (and number of sites)
Tick		Quite common. Evolving threat (new type).

STRIKE3 Test Architecture Overview

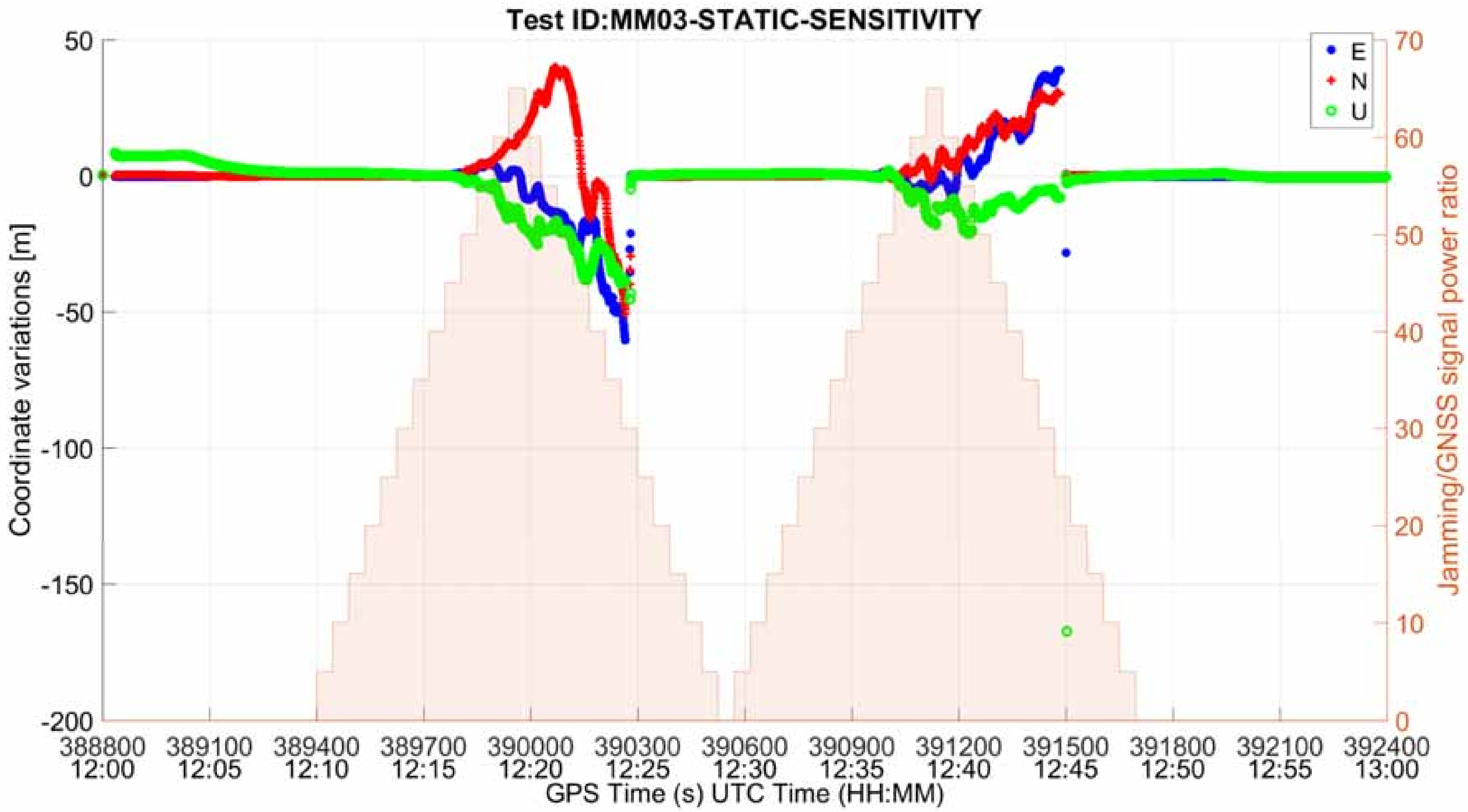
- Lab tests based on simulated GNSS signals
  - Easy to control, repeatable
- Interference signals added to clean GNSS signals


Spectracom RF GNSS Signal Simulator
Simulator script
Clean Signal
Trigger
Clean GNSS Signal
RF combiner
Σ
Interference Cntaminated GNSS Signal
Receiver Under Test
Receiver Metrics
Laptop with analysis software
Interference Source
I/Q samples for interference signals based on recorded threat signatures
VSG Automation Script
Vector Signal Generator
Interference Signal
Receiver-specific Configuration Script

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

STRIKE3

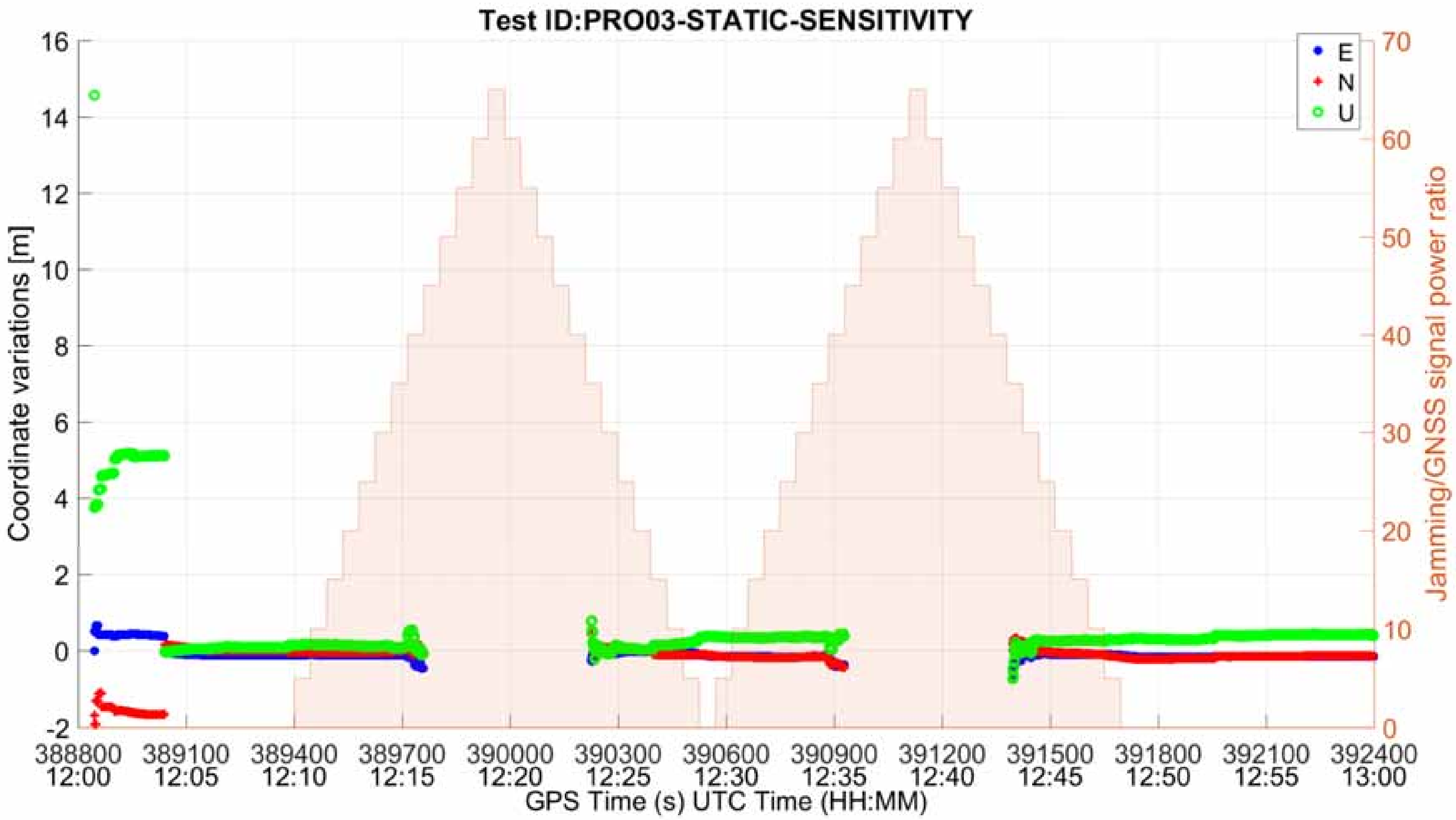
No C/N0 masking in PVT



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

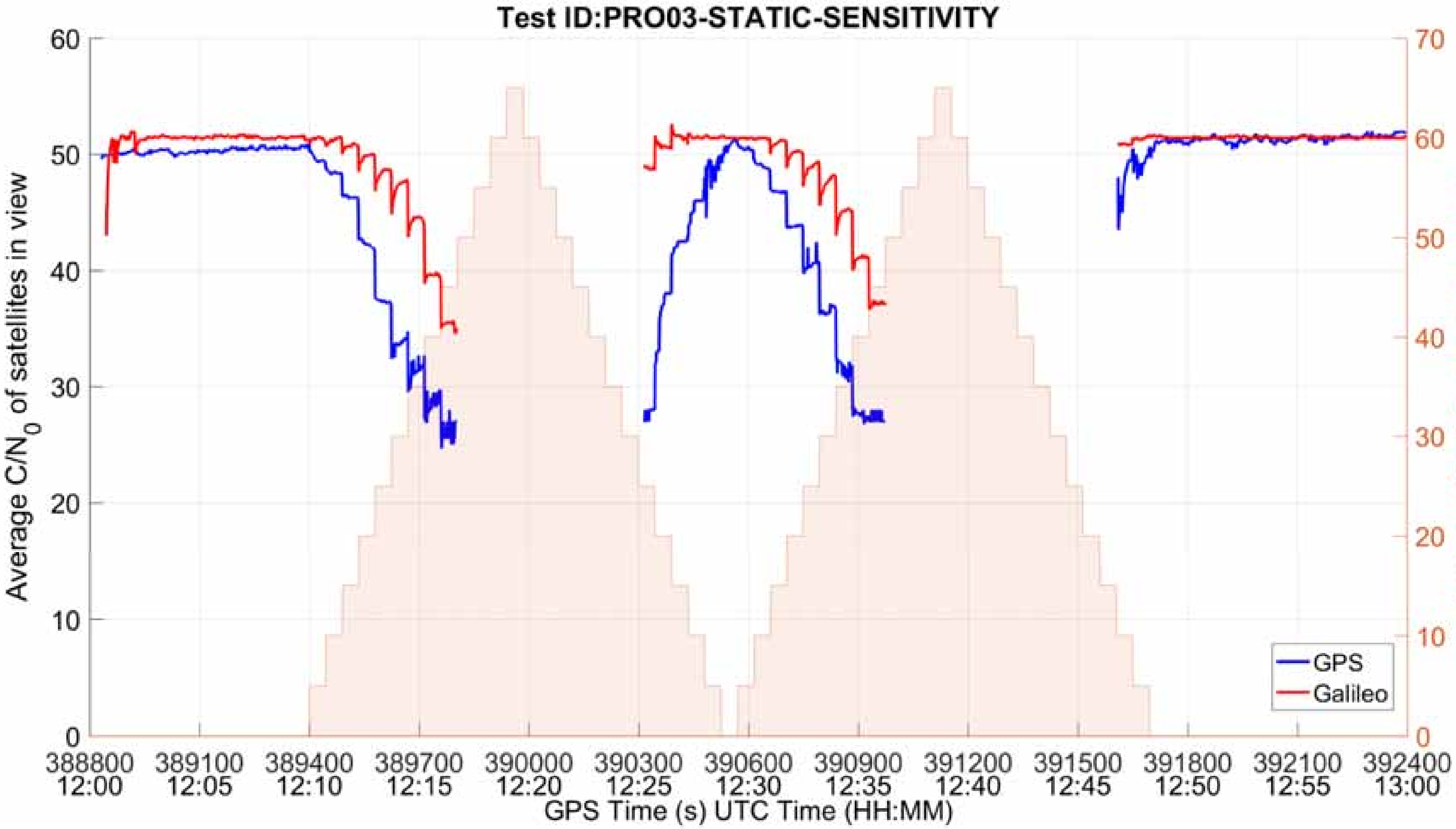
STRIKE3

Default C/N0 masking in PVT



PRO03-STATIC-SENSITIVITY: Average C/No

STRIKE3



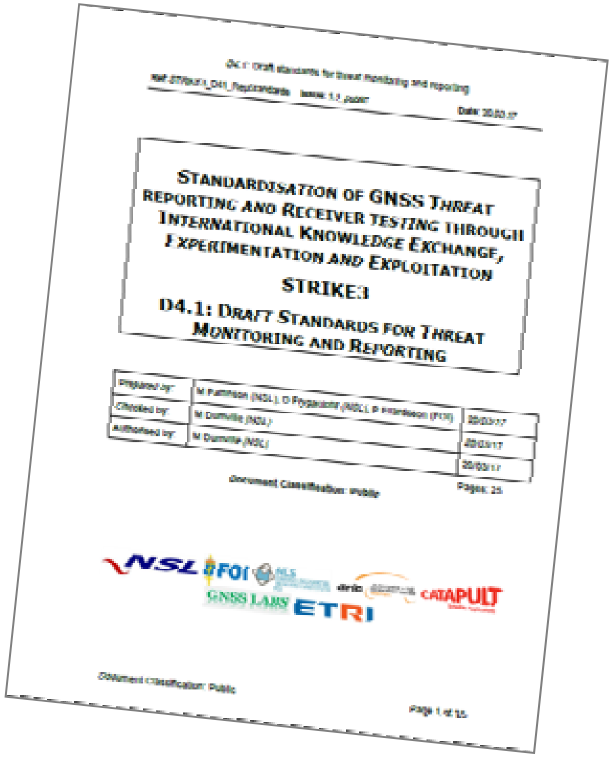
Conclusions

STRIKE3

- There are RFI threats to GNSS
- Long term monitoring can help us understand and quantify the threat
- Receiver testing against real threats can help assess receiver resilience and develop better mitigation

Available from:

<u>www.gnss-strike3.eu</u>



D4.1: Draft standards for threat monitoring and reporting

Ref: STRIKE3_D41_Reportstandards Issue: 1.1_public

Date: 20.03.17

STANDARDISATION OF GNSS THREAT REPORTING AND RECEIVER TESTING THROUGH INTERNATIONAL KNOWLEDGE EXCHANGE, EXPERIMENTATION AND EXPLOITATION

STRIKE3

D4.1: DRAFT STANDARDS FOR THREAT MONITORING AND REPORTING

Prepared by:	M Pattinson (NSL), D Fryganiotis (NSL), P Eliardsson (FOI)	20/03/17
Checked by:	M Dumville (NSL)	20/03/17
Authorised by:	M Dumville (NSL)	20/03/17

Document Classification: Public Pages: 25

Document Classification: Public

Page 1 of 25

D4.2: Draft standards for receiver testing against threats

Ref:STRIKE3_D42_Teststandards Issue: 1.0

Date: 03.02.17

STANDARDISATION OF GNSS THREAT REPORTING AND RECEIVER TESTING THROUGH INTERNATIONAL KNOWLEDGE EXCHANGE, EXPERIMENTATION AND EXPLOITATION

STRIKE3

D4.2: DRAFT STANDARDS FOR RECEIVER TESTING AGAINST THREATS

Prepared by:	Steve Hill, Satellite Applications Catapult Ltd [illegible] Ameer, Satellite Applications Catapult Ltd Sanguk Lee, ETRI Venkatesh Manikundalam, GNSS Labs	03.02.17
Checked by:	M Pattinson (NSL)	03.02.17
Authorised by:	M Dumville (NSL)	03.02.17

Document Classification: Public Pages: 50

Document Classification: Public

Page 1 of 50

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

European
Global Navigation
Satellite Systems
Agency

HORIZON 2020

NSL

FOI

NLS
FINNISH GEOSPATIAL
RESEARCH INSTITUTE
FGI

arlo automotive + rail innovation center

CATAPULT
Satellite Applications

GNSS LABS

ETRI