STRIKE3
Standardization of GNSS Threat reporting and Receiver testing through International Knowledge Exchange, Experimentation and Exploitation

- Draft Standards for Receiver Testing –

Martin Pölöskey

aric automotive + rail innovation center aachen

European Global Navigation Satellite Systems Agency

HORIZON 2020

CERGAL 2017

DGON/ESOC
Darmstadt
06. July 2017

An initiative to protect our GNSS …

STRIKE3

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

STRIKE3

European Global Navigation Satellite Systems Agency

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

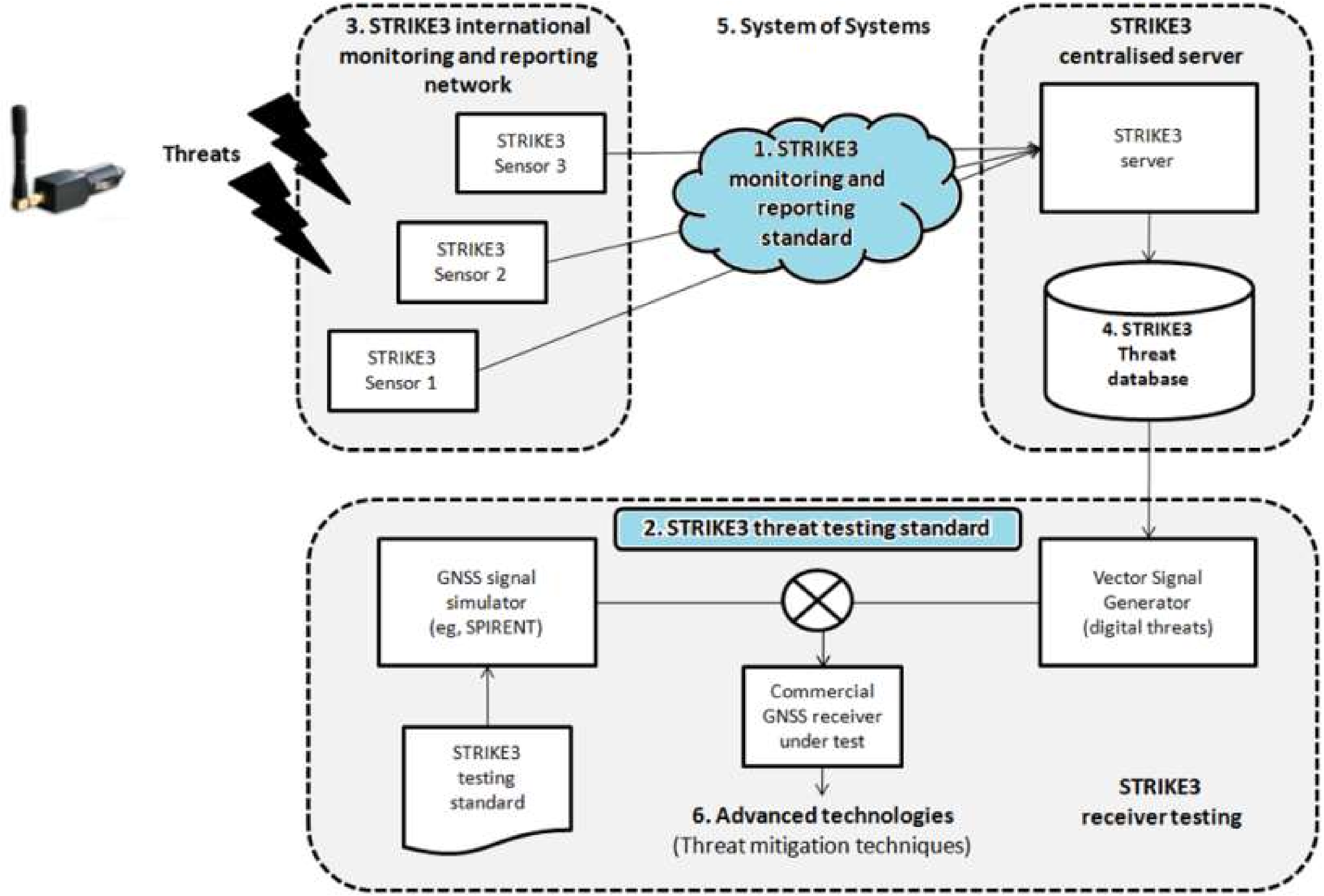
GNSS LABS

ETRI

Project Content & Structure

STRIKE3

Monitor, Detect & Characterise → Mitigate & Protect


Threats
3. STRIKE3 international monitoring and reporting network
STRIKE3 Sensor 3
STRIKE3 Sensor 2
STRIKE3 Sensor 1
5. System of Systems
1. STRIKE3 monitoring and reporting standard
STRIKE3 centralised server
STRIKE3 server
4. STRIKE3 Threat database
2. STRIKE3 threat testing standard
GNSS signal simulator (eg, SPIRENT)
Vector Signal Generator (digital threats)
Commercial GNSS receiver under test
STRIKE3 testing standard
6. Advanced technologies
(Threat mitigation techniques)
STRIKE3 receiver testing

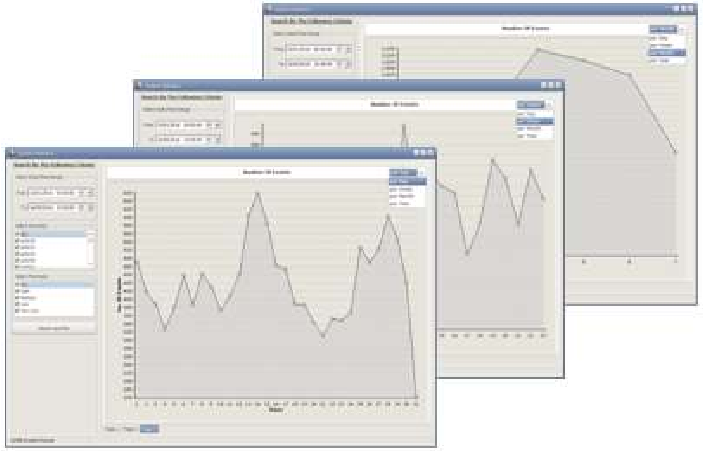
STRIKE3 “Stakeholders”

Range of entities/functions:

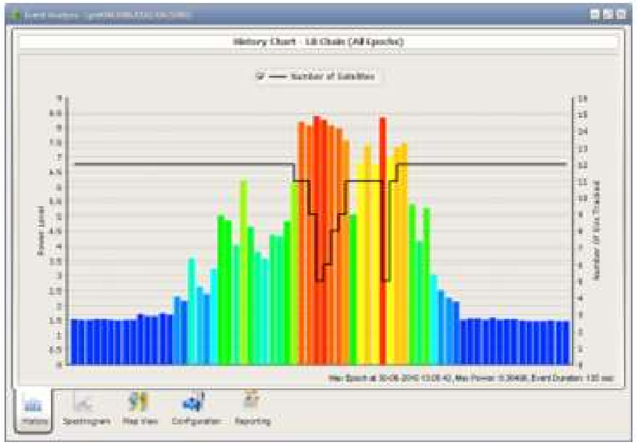
- Government agencies
- Frequency regulators
- Road + Tolling operators
- Airport operators
- Air Navigation Service Providers
- Power grids
- Time-Sync.

Range of concerns:

- What is the scale of the problem?
- How do the results compare at different locations?
- Are there any patterns at my site? At other sites?
- What is the impact on GNSS receivers in the vicinity?
- What is the risk and what options exist to reduce the risk?

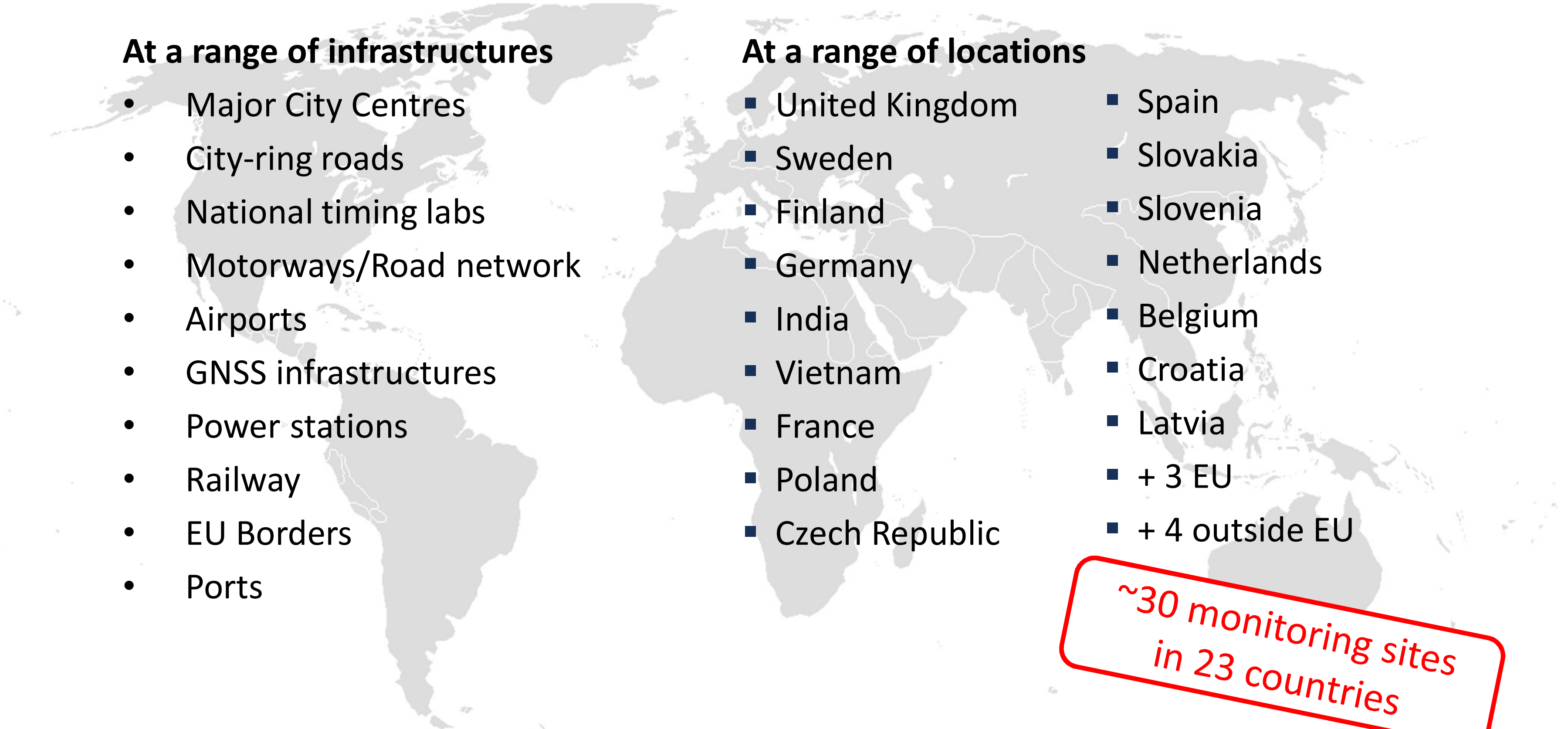


Number of events per location per time



Impact of an event on “Satellites in view”

STRIKE3 International Network



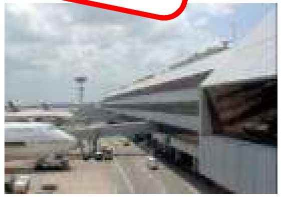
At a range of infrastructures

- 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



Monitoring Equipment

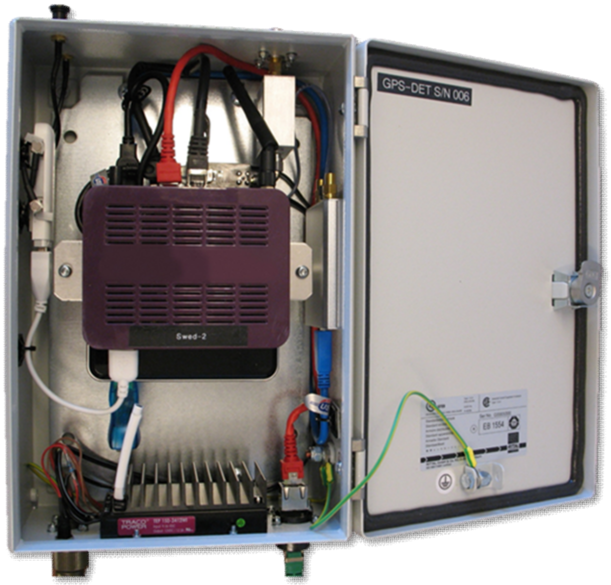
Detector

- **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

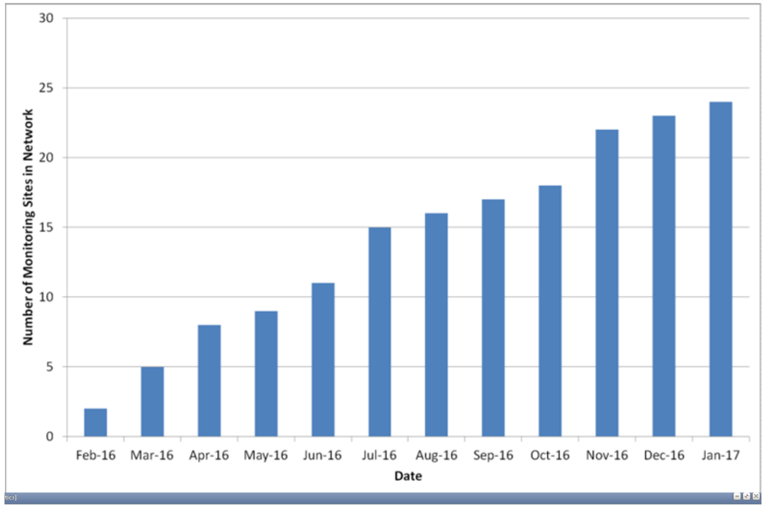


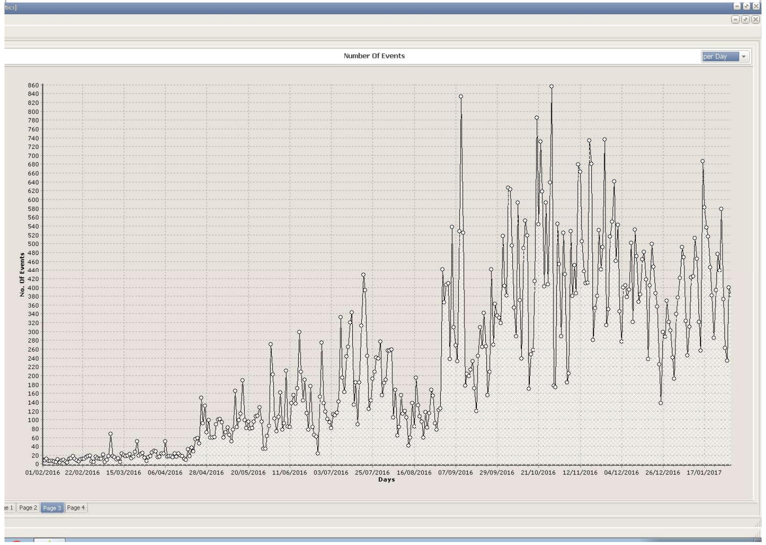
- GPS/SBAS/GALILEO L1/E1
- Autonomous monitoring
- Centralised server with web-interface

Summary of Monitoring from First Year

STRIKE3

- Project KO – 1st Feb 2016
- Monitoring network a mix of pre-existing sites plus new installations
- Combined 140 months of data across all sites
- More than 80,000 events detected
  - Likely causes?
  - Intentional or unintentional
  - Comparison between sites
  - Impact on GNSS?

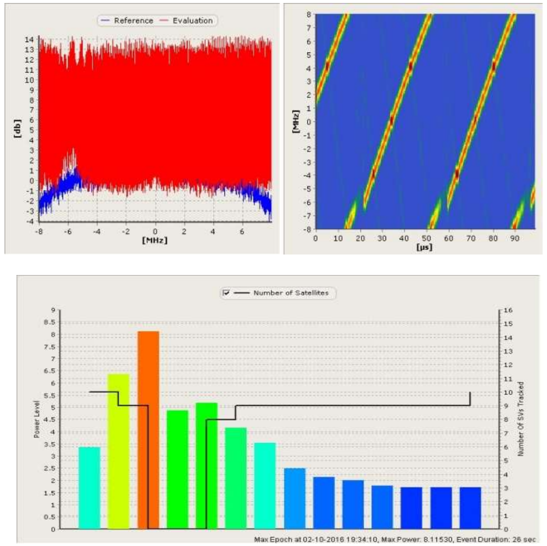


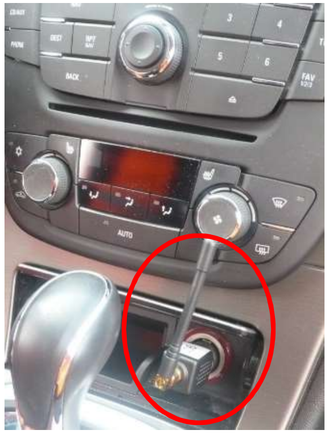


Events Classification

Intentional Events

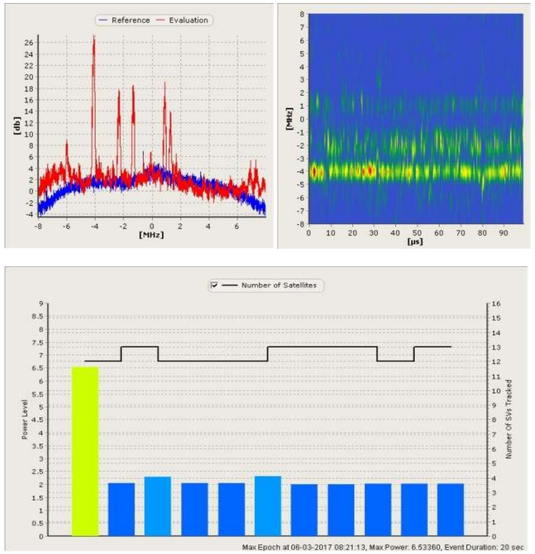
- ‘Chirp’ signals
- Power profile shows gradual rise / fall either side of peak
- Suggests mobile jammer





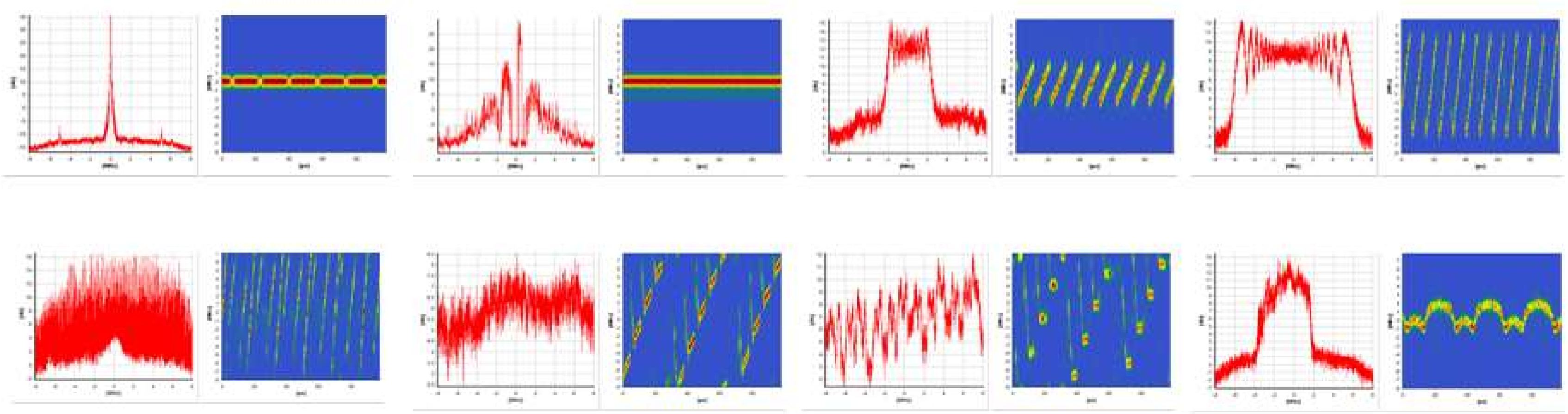
Unintentional Events

- Less structure to signals – not directly affecting GPS L1 centre frequency
- Power profile shows instantaneous peak in power
- Suggests not targeted at GPS L1



Unknown Events

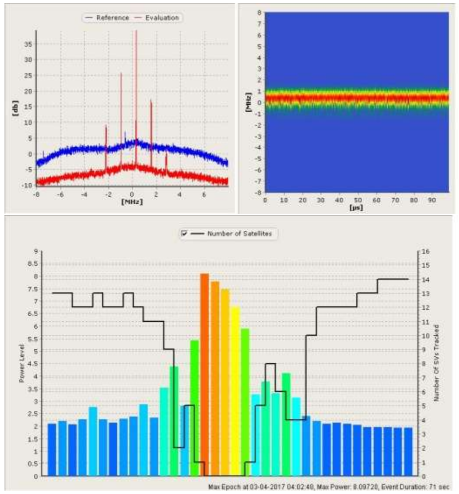
- Many more “RF threat waveforms” than reported in literature
- Large number of jammer “families” (varying complexity & impact)

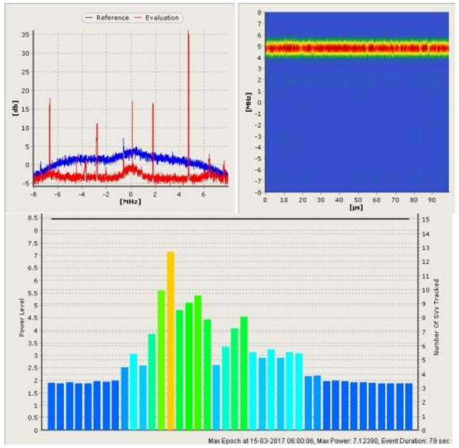


- Growing need to share knowledge with international communities

Impact on GNSS

- Monitoring sites may record impact on GNSS
- However, many factors affecting impact of interference signal:
  - Type and duration of interference
  - Emitter power
  - Distance from transmitter to receiving site
  - Shielding of interference and obstructions along path
  - Receiving antenna type
  - Type of receiver and specific set-up / configuration





STRIKE3 Monitoring & Reporting

STRIKE3

- Threat monitoring and reporting
  - Provides a lot of information and insights about existing interferences and disturbances on GNSS
  - Is the basis for mitigation and defence ("know your enemy")
- "Draft Standards for Threat Monitoring and Reporting"
  - Document is a key deliverable of STRIKE3 project
  - Contains definitions on events, events messages and system information messages
  - Is available for public (-> download at www.gnss-strike3.eu)
  - The signals and the knowledge about these interferences can be used to improve the robustness of receivers and systems

STRIKE3 Draft Receiver Test Standards

STRIKE3

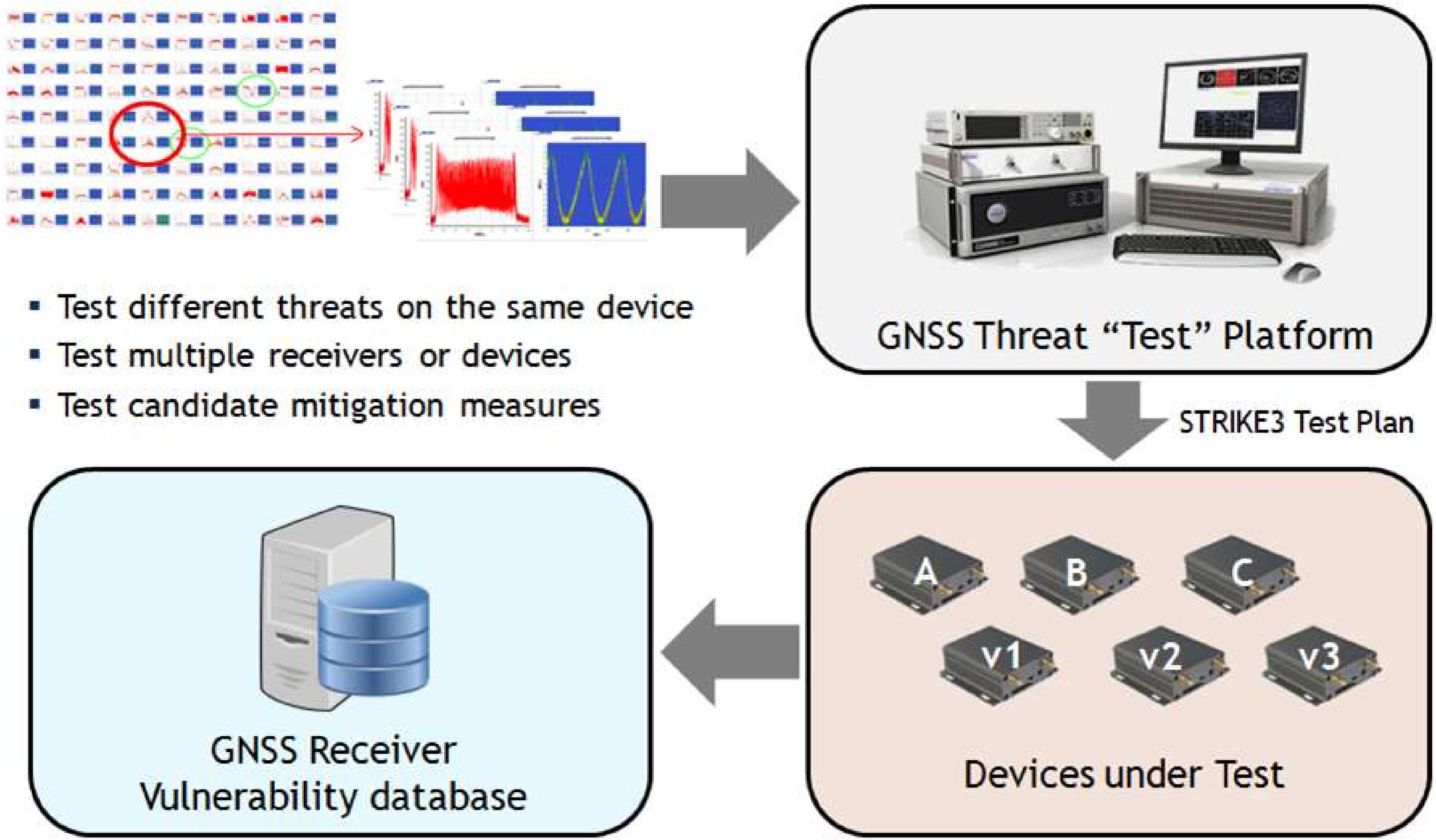
Ambition

- Propose standard methodology to test receivers against selected threats
- Define a standard set of threats for testing based on interference signals observed in the field, and propose a method to identify and select new threats for testing in the future

Application of standards

- Test standards envisaged as a guideline for standard bodies, application developers, receiver manufacturers, etc.
    - ➢ Test standards provide the framework and instructions for performing tests
    - ➢ Expected values of metrics and pass/fail criteria are defined by the relevant authority based on requirements.

GNSS Receiver Testing



- Test different threats on the same device
- Test multiple receivers or devices
- Test candidate mitigation measures

GNSS Threat "Test" Platform

STRIKE3 Test Plan

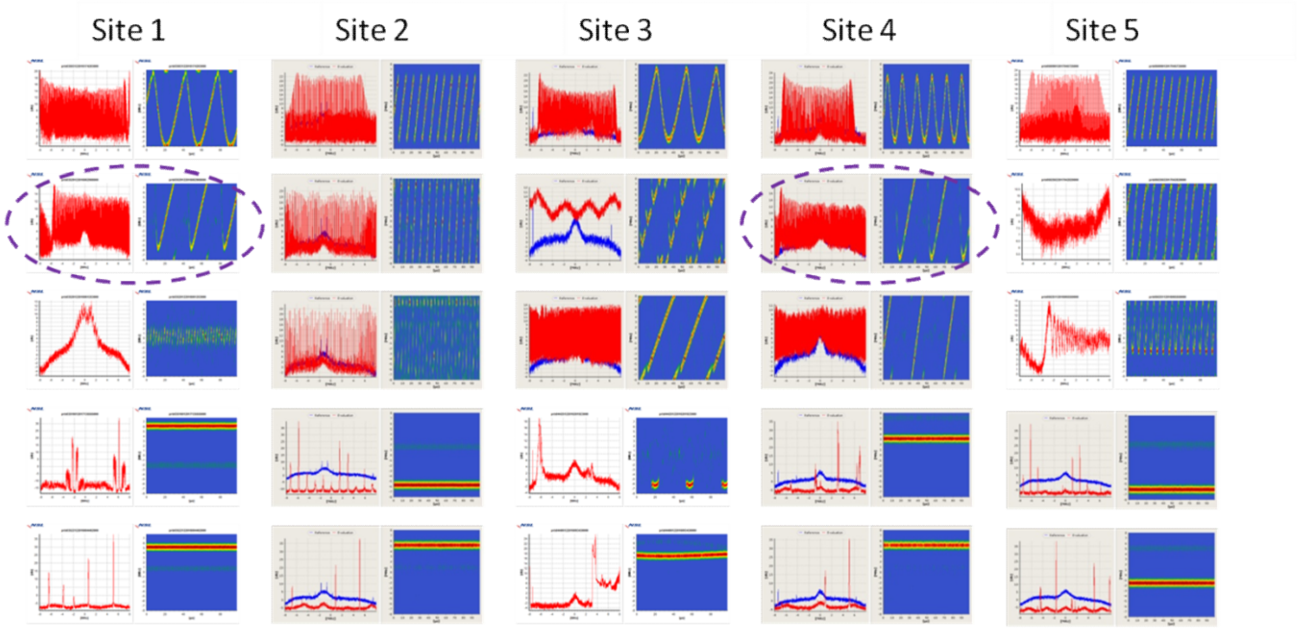
Devices under Test

GNSS Receiver Vulnerability database

per threat battery, per application/market, per territory

STRIKE3 Database

- Information about all detected events
  - Power level, duration, signal type, waveform
- Use knowledge of threats and waveforms for testing



Threat Selection

STRIKE3

- Test standards will focus on real threats from STRIKE3 event database
  - Thousands of events are available already

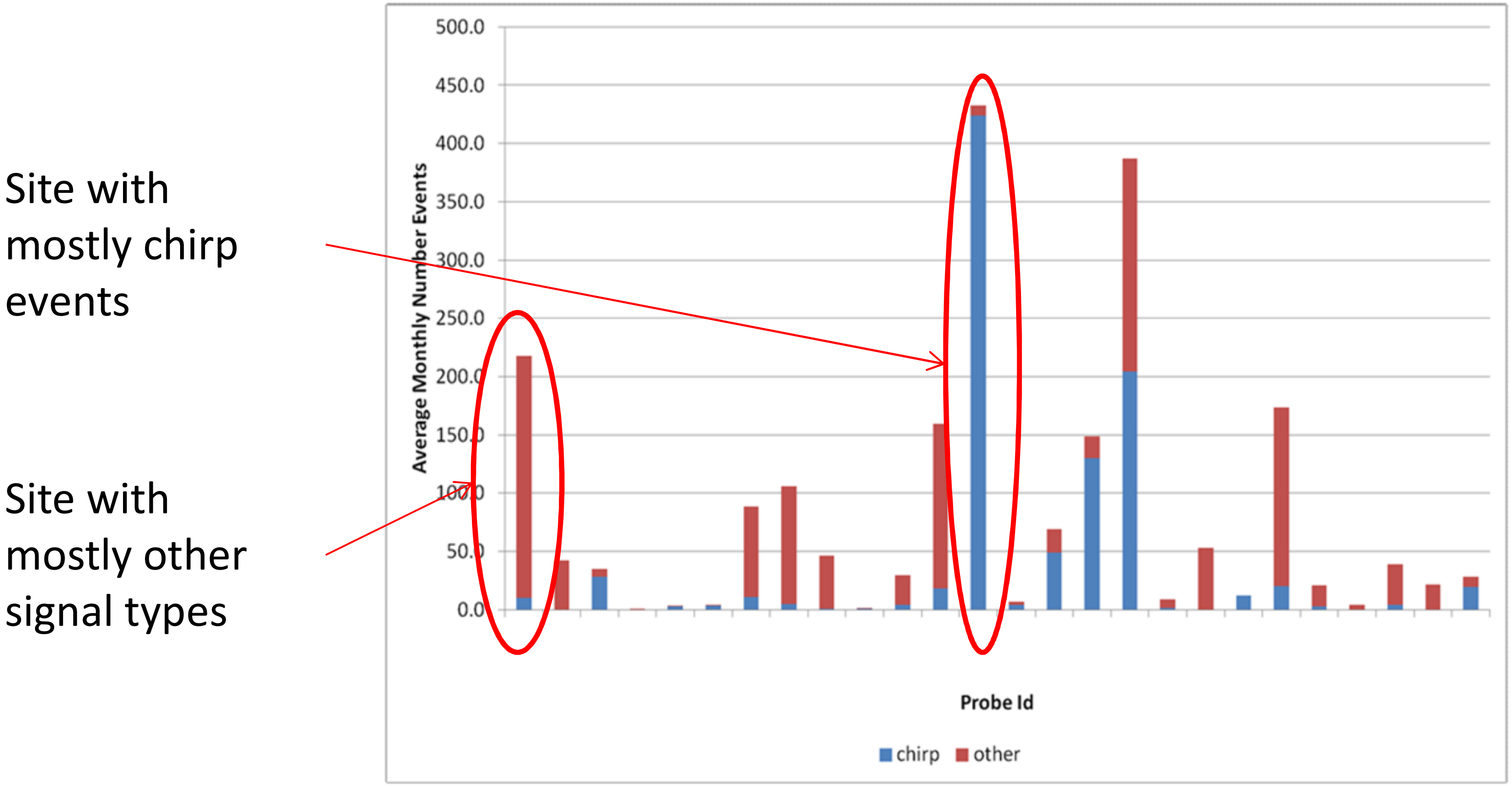
- Initial threat selection
  - Filter by power level (at least a certain power)
  - Select common signatures for different categories (chirp, NB, etc.)
  - Select some unusual signals anticipated to be difficult to mitigate

- Initial threats will be prepared and tested during the project
  - Final recommendation will produce baseline set of threats
  - Methodology to identify emerging threats for testing

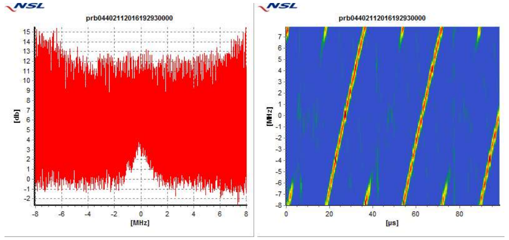
Comparison of Signal Types

STRIKE3

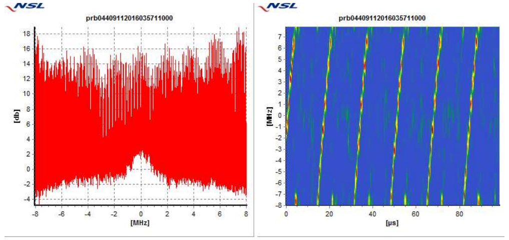
Number of events above minimum power level



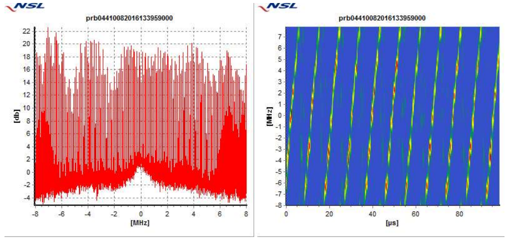
Types of Chirp Signals



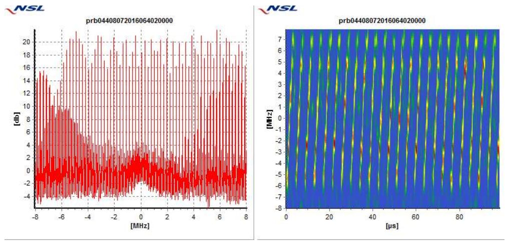
Wide sweep - slow



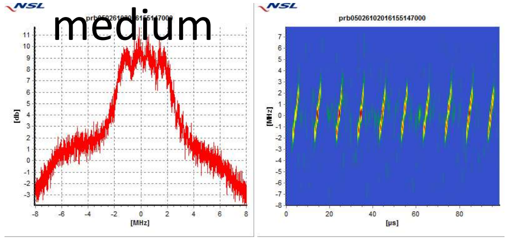
Wide sweep - medium



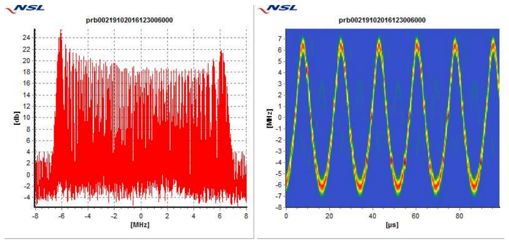
Wide sweep - fast



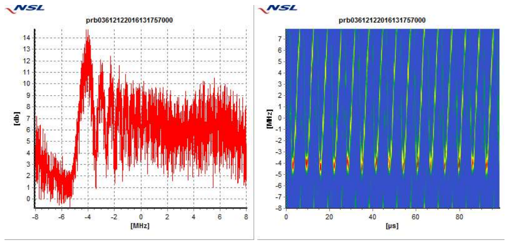
Wide sweep - rapid



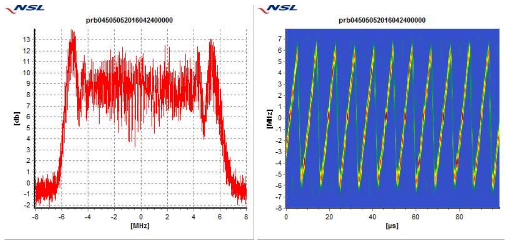
Narrow sweep



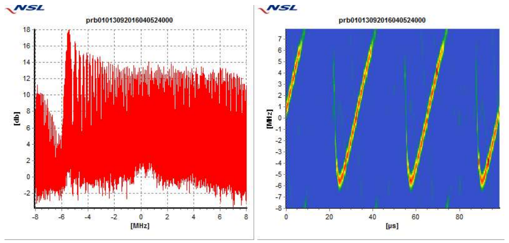
Triangular wave



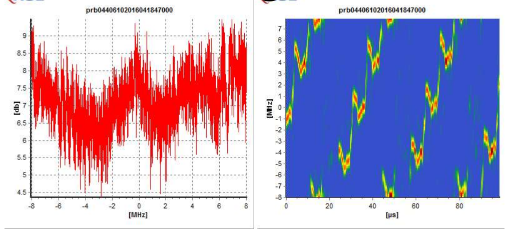
Triangular



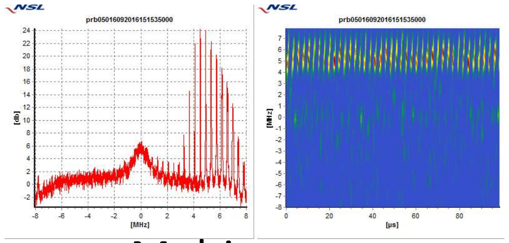
Sawtooth



Hooked sawtooth



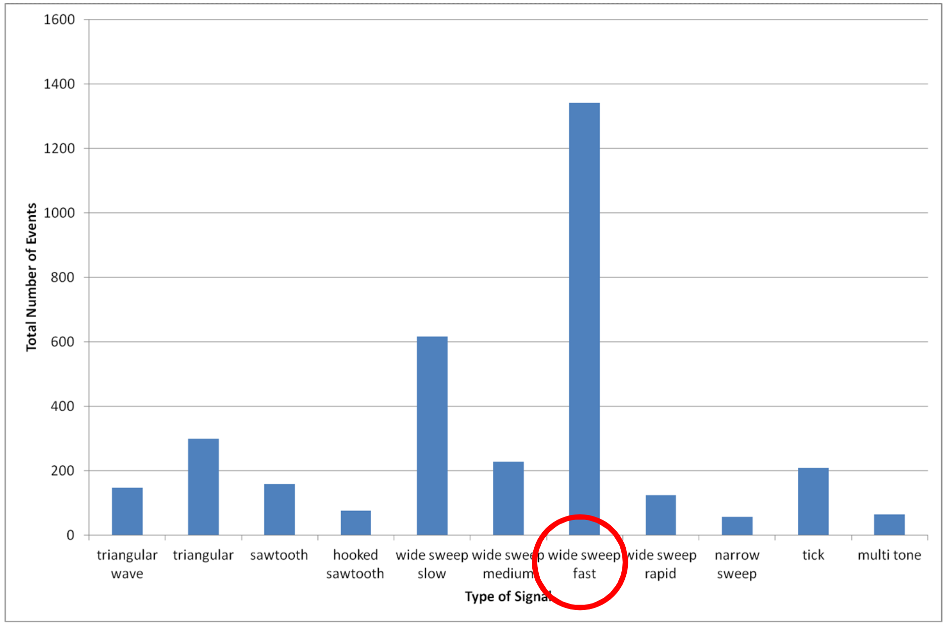
Tick



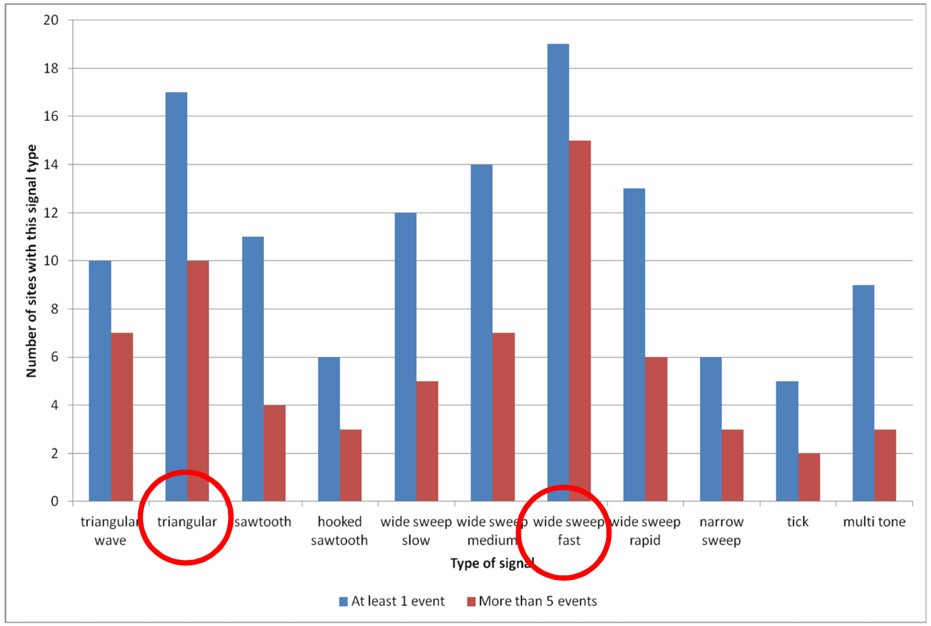
Multi-tone

Chirp Signal Type Analysis

Total number of events – different types of signal

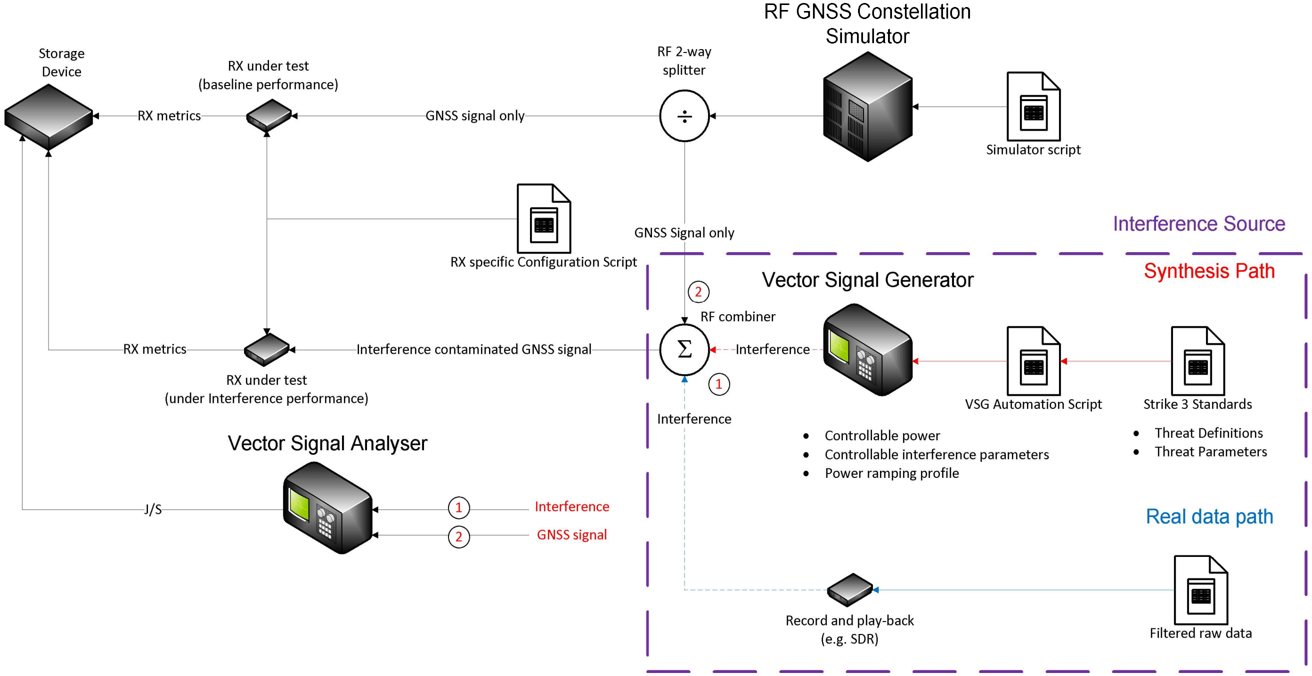


No. of sites detecting different types of signal



STRIKE3 Test Architecture Overview

- Lab tests based on simulated GNSS signals
  - Easy to control, repeatable
- GNSS signals mixed with interference signals



- Some differences depending on receiver type (mass-market, integrated, professional, timing)

Interference Signal Generation

STRIKE3

- Focus in STRIKE3 on GPS L1 interference
  - Standards can be extended to cover other frequencies
- Want test signals to be based on real interference from event database
- Two approaches under consideration
  - Synthetic signal (based on properties of real signal detected in the field)
  - Replay of raw data samples
- Both will be defined and tested in STRIKE3
- Best approach will be proposed as an outcome of the project

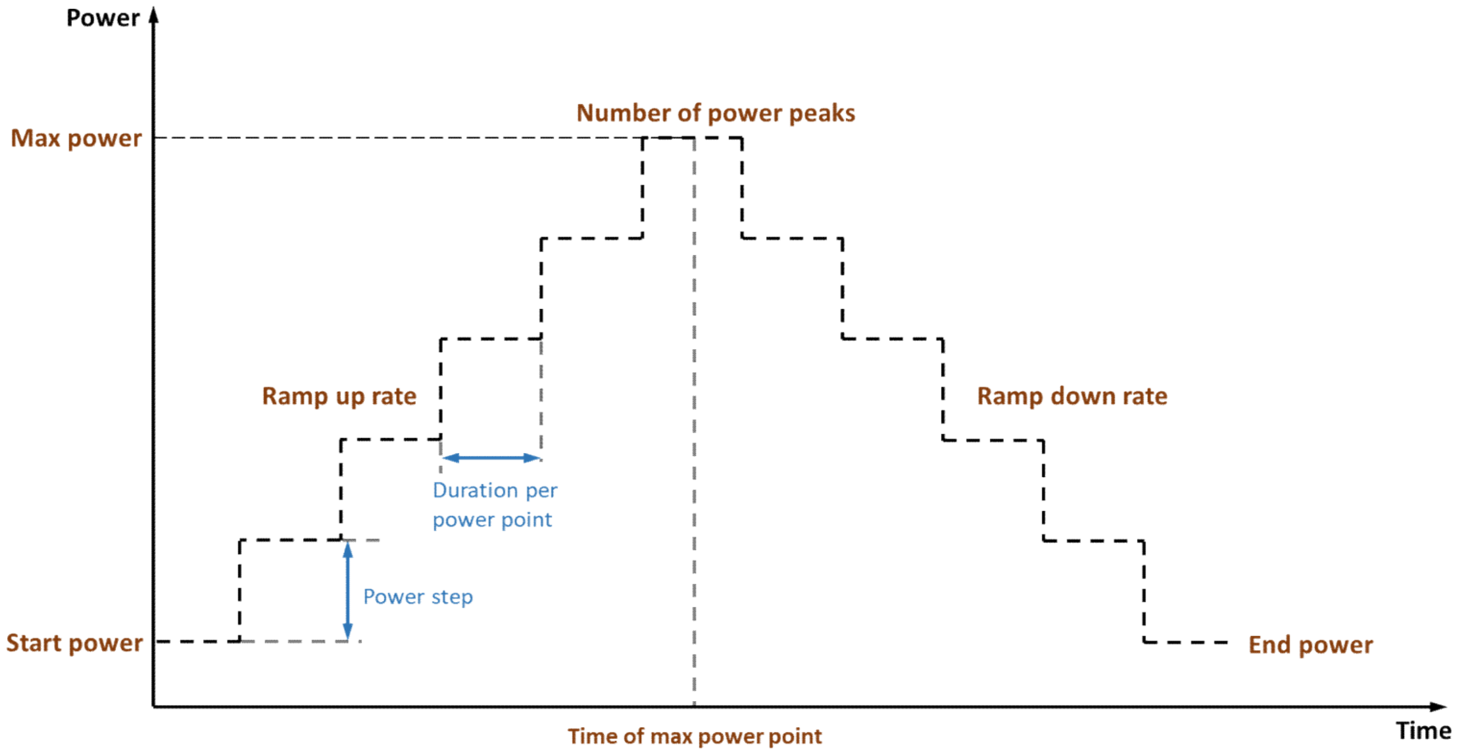
Test Cases

STRIKE3

- Time To First Fix
  - Assess time taken for receiver to recover after strong interference event
- Acquisition and tracking sensitivity (single peak and multi-peak ramp)
  - Assess behaviour of static receiver as interference level increases, including impact on position error, point at which tracking is lost, and point at which re-acquisition occurs
- Dynamic receiver test
  - Assess behaviour of dynamic receiver as interference level increases, in particular impact on position error
- Timing receiver test
  - Assess impact of interference on performance of timing receiver

Test Case Steps

- Steps for test cases will be defined:
  - Initial conditions for receiver (e.g. receiver in stable mode tracking all satellites)
  - Test times and durations
  - Times of test case events (e.g. start of interference, increase in power level, etc.)
  - Interference power levels at each time



Receiver Testing Campaign

- Test selection of receivers:
  - Mass-market, professional, integrated devices, timing receivers

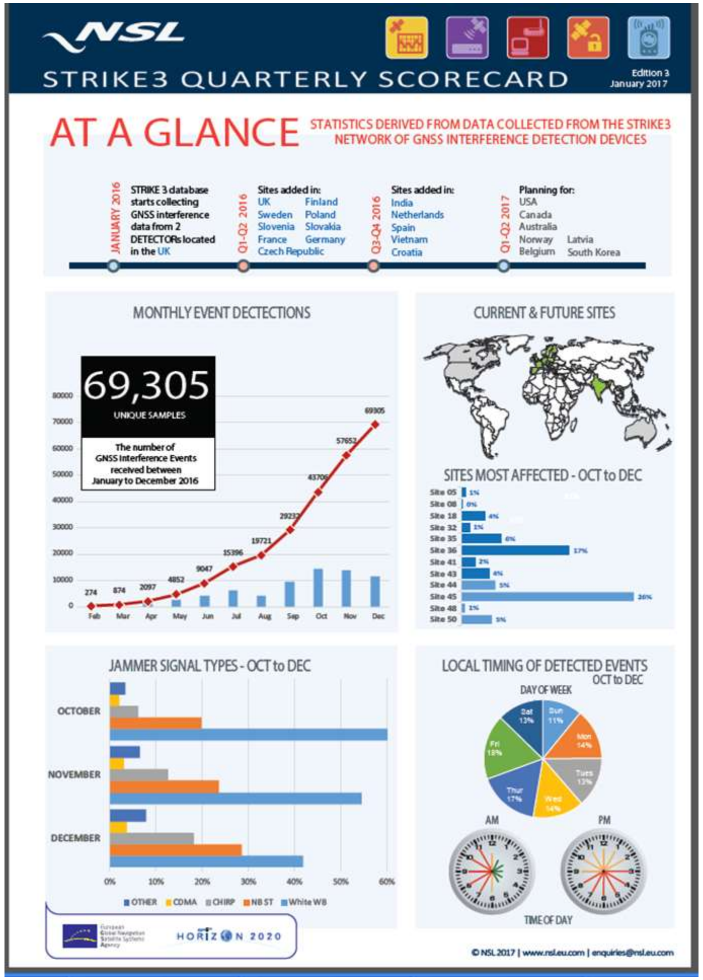
- Outputs
  - Consolidated draft test standards
  - Overview of receiver performance (anonymous)

- Future (beyond STRIKE3)
  - Improved mitigation / resilience to threats

STRIKE3 Further Information

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

- Project information
  - Information on threats and interferences
  - Quarterly score cards of monitoring results
- Draft standards for download
  - Threat Monitoring & Reporting Standards available now
  - Test Standards coming soon



STRIKE3 QUARTERLY SCORECARD

Edition 3
January 2017

AT A GLANCE

STATISTICS DERIVED FROM DATA COLLECTED FROM THE STRIKE3 NETWORK OF GNSS INTERFERENCE DETECTION DEVICES

JANUARY 2016: STRIKE 3 database starts collecting GNSS interference data from 2 DETECTORs located in the UK

Q1-Q2 2016: Sites added in: UK, Finland, Sweden, Poland, Slovenia, Slovakia, France, Germany, Czech Republic

Q3-Q4 2016: Sites added in: India, Netherlands, Spain, Vietnam, Croatia

Q1-Q2 2017: Planning for: USA, Canada, Australia, Norway, Latvia, Belgium, South Korea

MONTHLY EVENT DECTECTIONS

69,305

UNIQUE SAMPLES

The number of GNSS Interference Events received between January to December 2016

CURRENT & FUTURE SITES

SITES MOST AFFECTED - OCT to DEC

JAMMER SIGNAL TYPES - OCT to DEC

LOCAL TIMING OF DETECTED EVENTS OCT to DEC

© NSL 2017 | www.nsl.eu.com | enquiries@nsl.eu.com

Thank You for Your Attention!

STRIKE3

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

European
Global Navigation
Satellite Systems
Agency

HORIZON 2020

NSL FOI NLS FINNISH GEOSPATIAL RESEARCH INSTITUTE FGI aric automotive + rail innovation center aachen

CATAPULT Satellite Applications GNSS LABS ETRI

Contact: Martin Pölöskey Tel. +49-2432-93376-11 Mail: martin.poloskey@aric-research.de