Standardization of GNSS Threat reporting and Receiver testing through International Knowledge Exchange, Experimentation and Exploitation [STRIKE3]: Results from First Year of Monitoring

Björn Gabrielsson

FOI

European Global Navigation Satellite Systems Agency

HORIZON 2020

ENC 2017
European Navigation Conference 2017
May 9-12, **Lausanne**, Switzerland ■ www.enc2017.eu

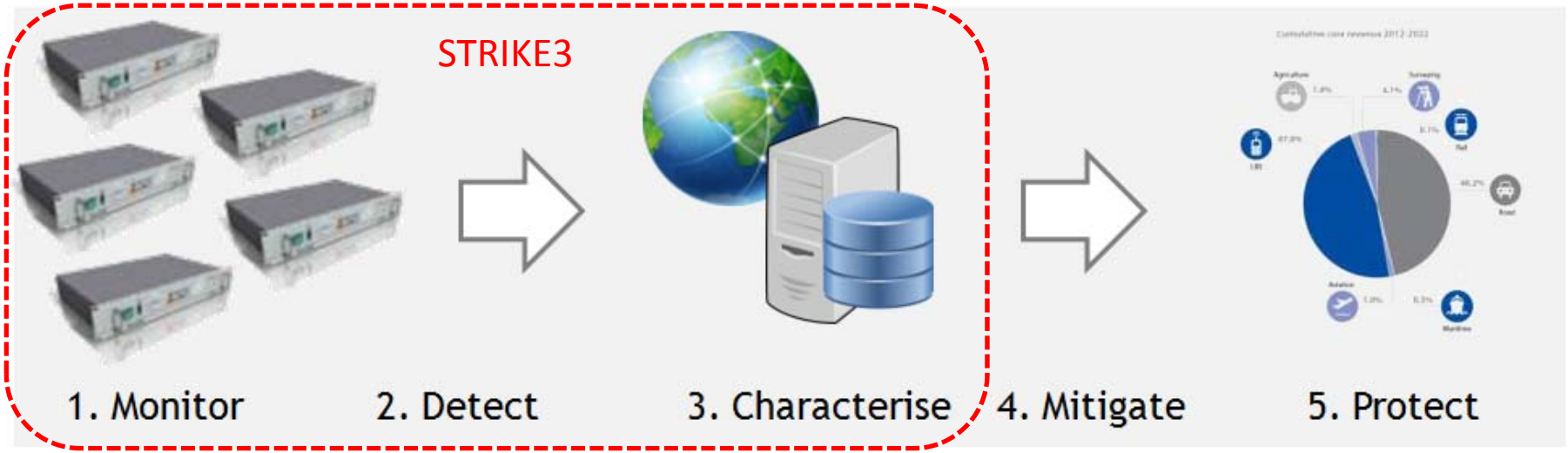
An initiative to protect our GNSS …

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

- Start date = 1 February 2016
- Duration = 3 years

STRIKE3 Project Rationale

- 6% of European GDP depends on GNSS (800BEuro)
- At the same time, GNSS vulnerabilities are being exposed and threats to degradation and denial of GNSS services are increasing.



- 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.

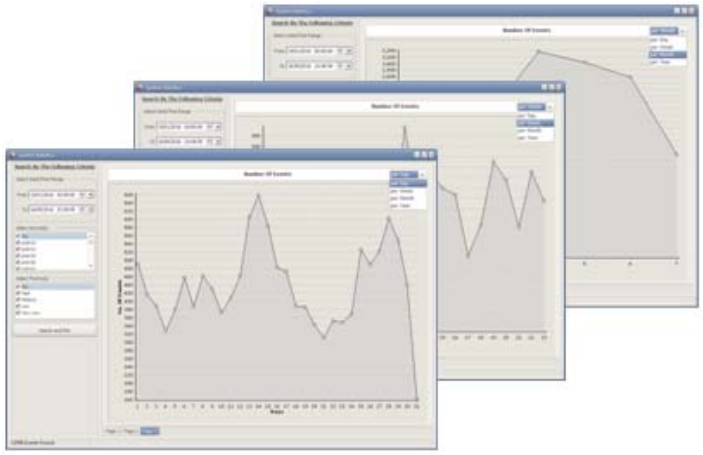
STRIKE3 “Stakeholders”

Range of entities/functions:

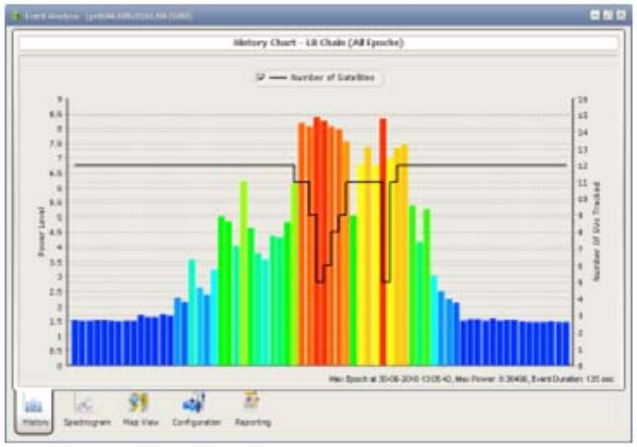
- Government agencies
- Frequency regulators
- Road operators
- Tolling operators
- Airport operators
- Air Navigation Service Providers
- Power grids

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?

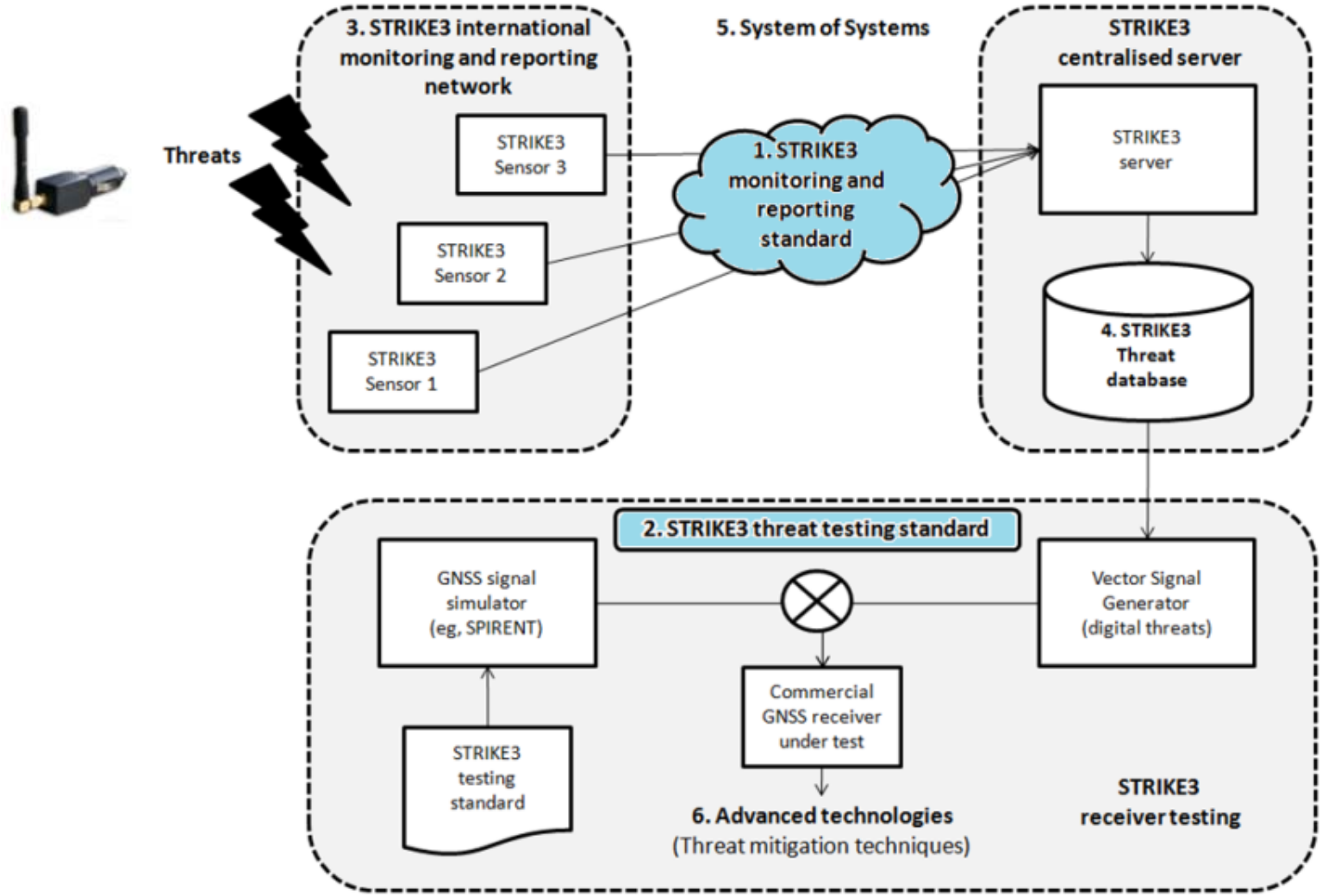


Number of events per location per time



Impact of an event on “Satellites in view”

Monitor, Detect & Characterise
= >
Mitigate & Protect



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

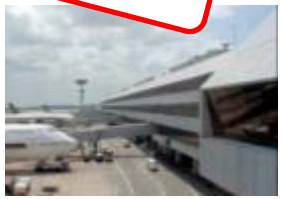
At a range of locations

- 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





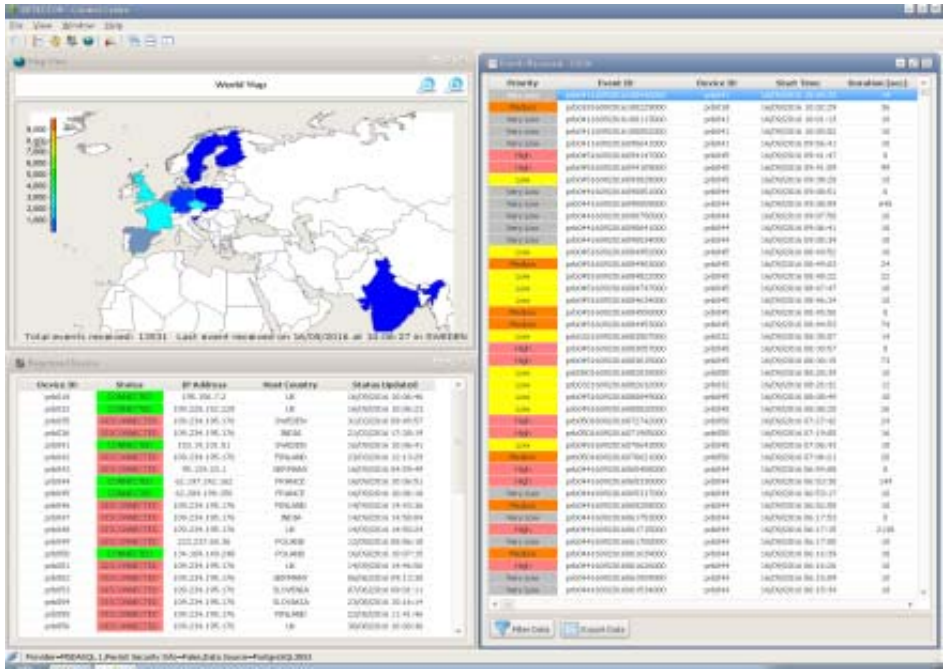


Monitoring Equipment - DETECTOR

- **GSS100D** – Interference detector
  - GPS/EGNOS/Galileo L1/E1

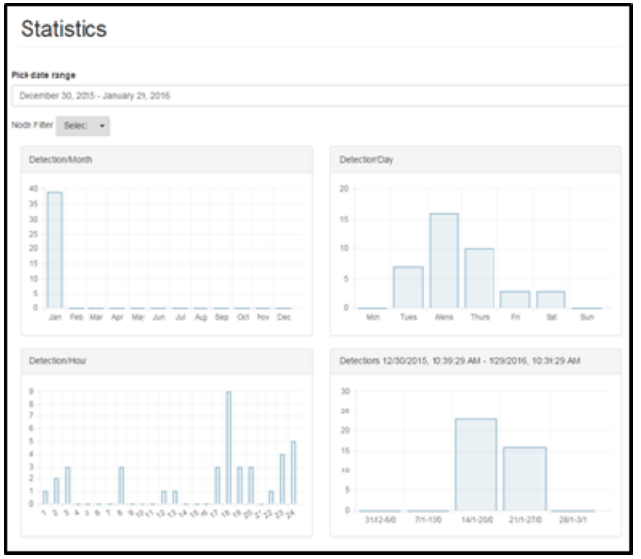
- **GSS200D** – Interference detector
  - GPS/Galileo/EGNOS/GLONASS L1/E1/G1

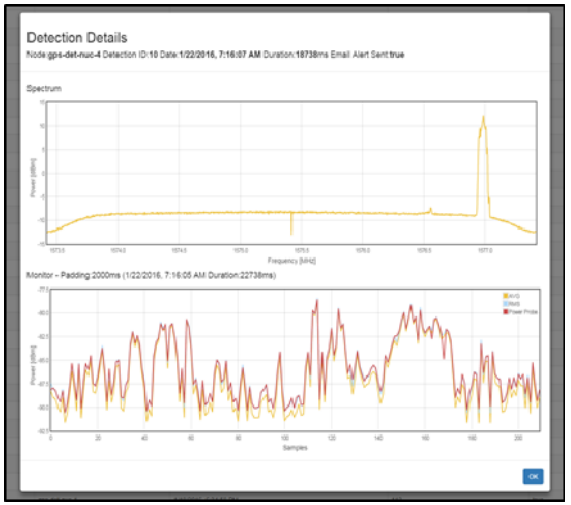
- **GSS200D'** – Interference detector
  - L1/L5 + ICAO/Eurocae interference masks
  - Spoofing detection



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

Monitoring Equipment – RF Oculus

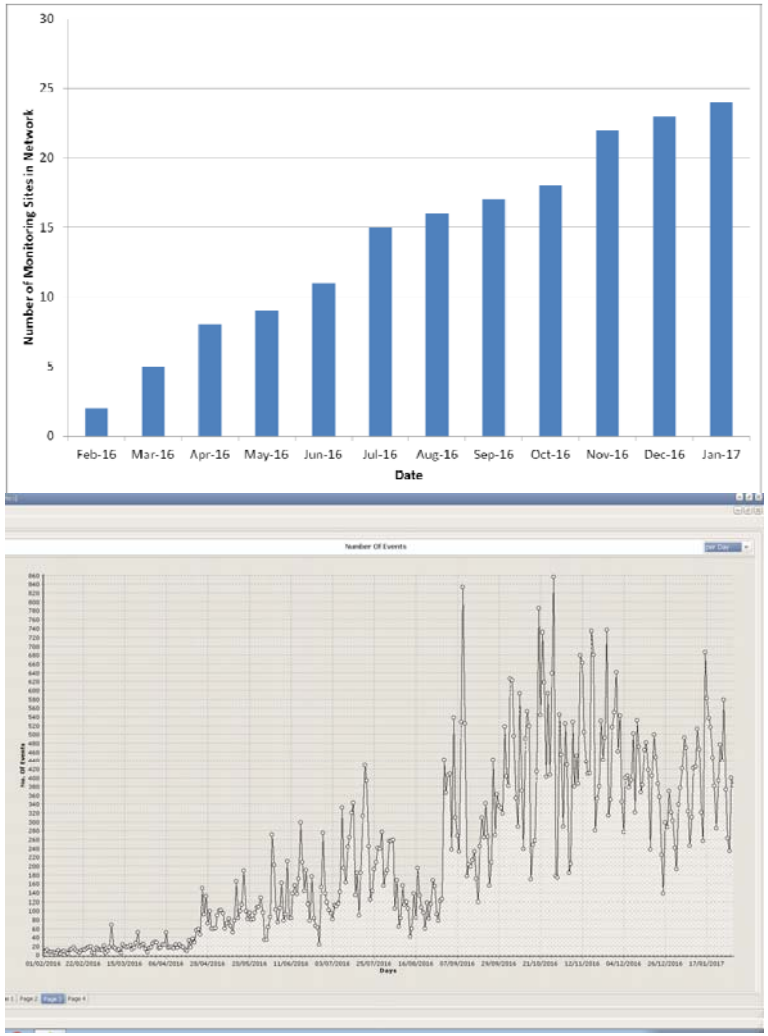




- **RF-Oculus**
  - GPS/SBAS/GALILEO L1/E1
  - Autonomous monitoring
  - Centralised server with web-interface

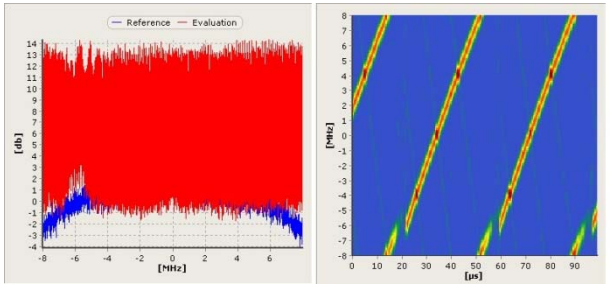
Summary of Monitoring from First Year

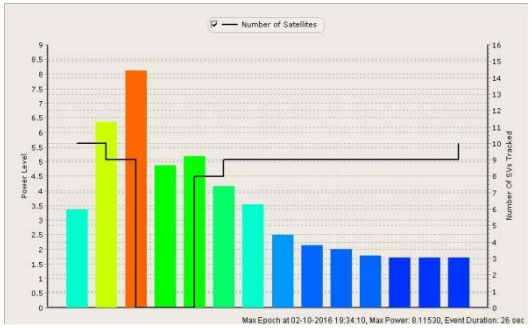
- Project KO – 1st Feb 2016
- Monitoring network a mix of pre-existing sites plus new installations
- Combined 140 months of data across all sites
- More than 80,000 events detected
  - Likely causes?
  - Intentional or unintentional
  - Comparison between sites
  - Impact on GNSS?



Intentional Events

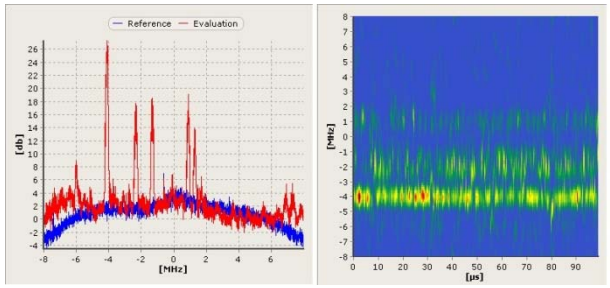
- ‘Chirp’ signals
- Power profile shows gradual rise / fall either side of peak
- Suggests mobile jammer

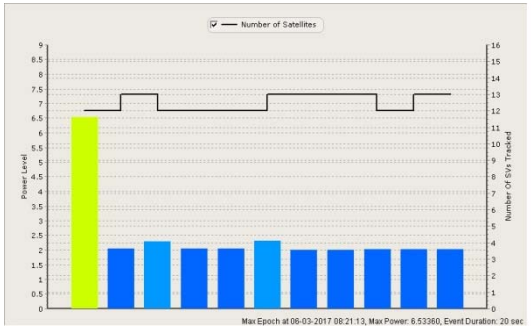




Unintentional Events

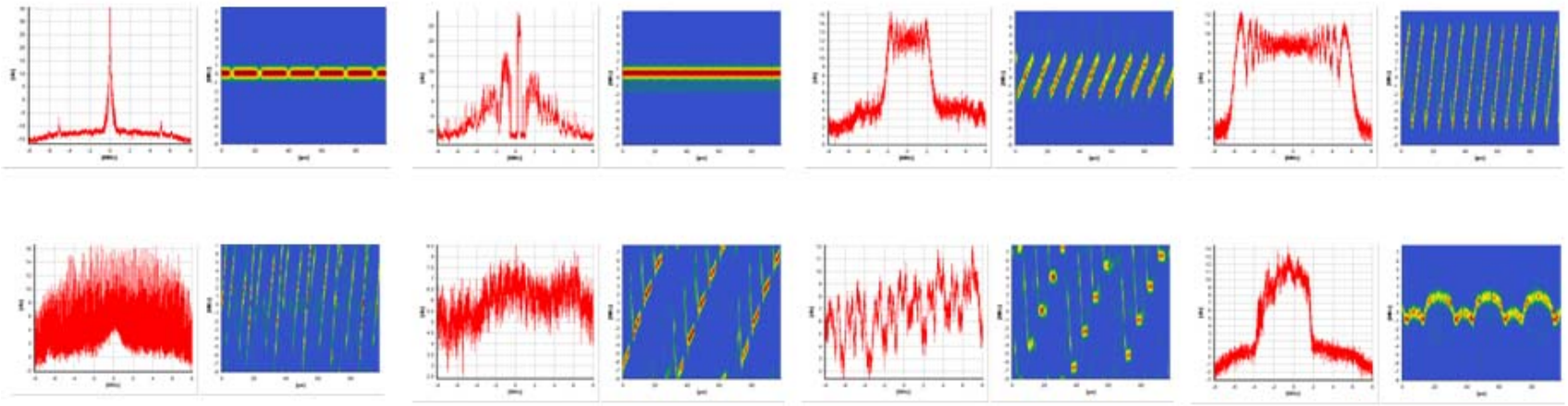
- Less structure to signals – not directly affecting GPS L1 centre frequency
- Power profile shows instantaneous peak in power
- Suggests not targeted at GPS L1





Unknown Events

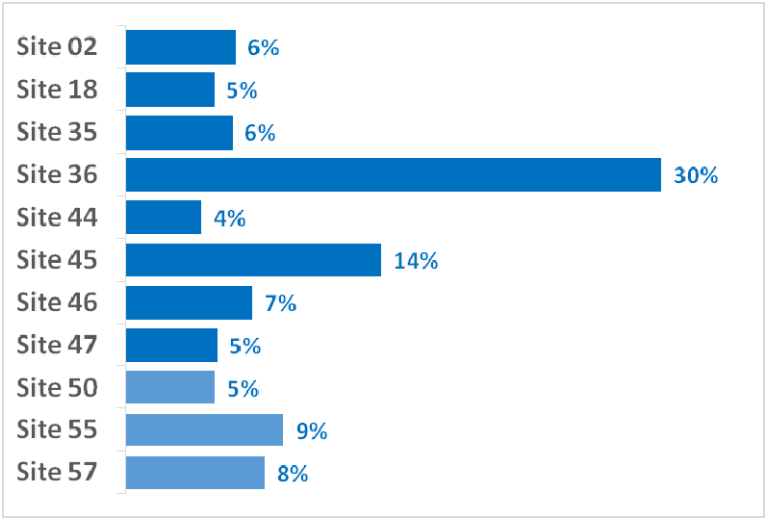
- Many more “RF threat waveforms” than reported in literature
- Large number of jammer “families” (varying complexity & impact)



- Growing need to share knowledge with international communities

Comparison Between Sites

- Variation in activity between different sites
  - City centre locations
    - Very active sites
    - Many chirp signals (jammers)
  - Major roads
    - Less overall activity than city centres
    - Still have many chirp events
  - Airports
    - Fewer chirp signals than other sites
    - Higher proportion of other types of signal with high power levels



Comparison Between Monitoring Equipment

- Co-location of RF Oculus and Detector V1 at one site
- Significant difference in total number of detections
  - Different thresholds for detection
  - Differences in bandwidth

7-week period Nov-16 to Jan-17

	Detector	RF Oculus
Total Number of Detections	392	118
Number of common detections	107	

- Good agreement for ‘significant’ detections
  - Chirp events detected by both systems
  - Timings of events similar (within a few seconds)

STRIKE3 Reporting Standards

- Key drivers
  - Ensure reports from different systems are compatible
  - Minimise changes to existing monitoring system equipment
  - Limit confidential / sensitive information that needs to be sent and stored
  - ‘Integrity’ of data and results
  - Flexibility in data provision and analysis

STRIKE3 Message Definition

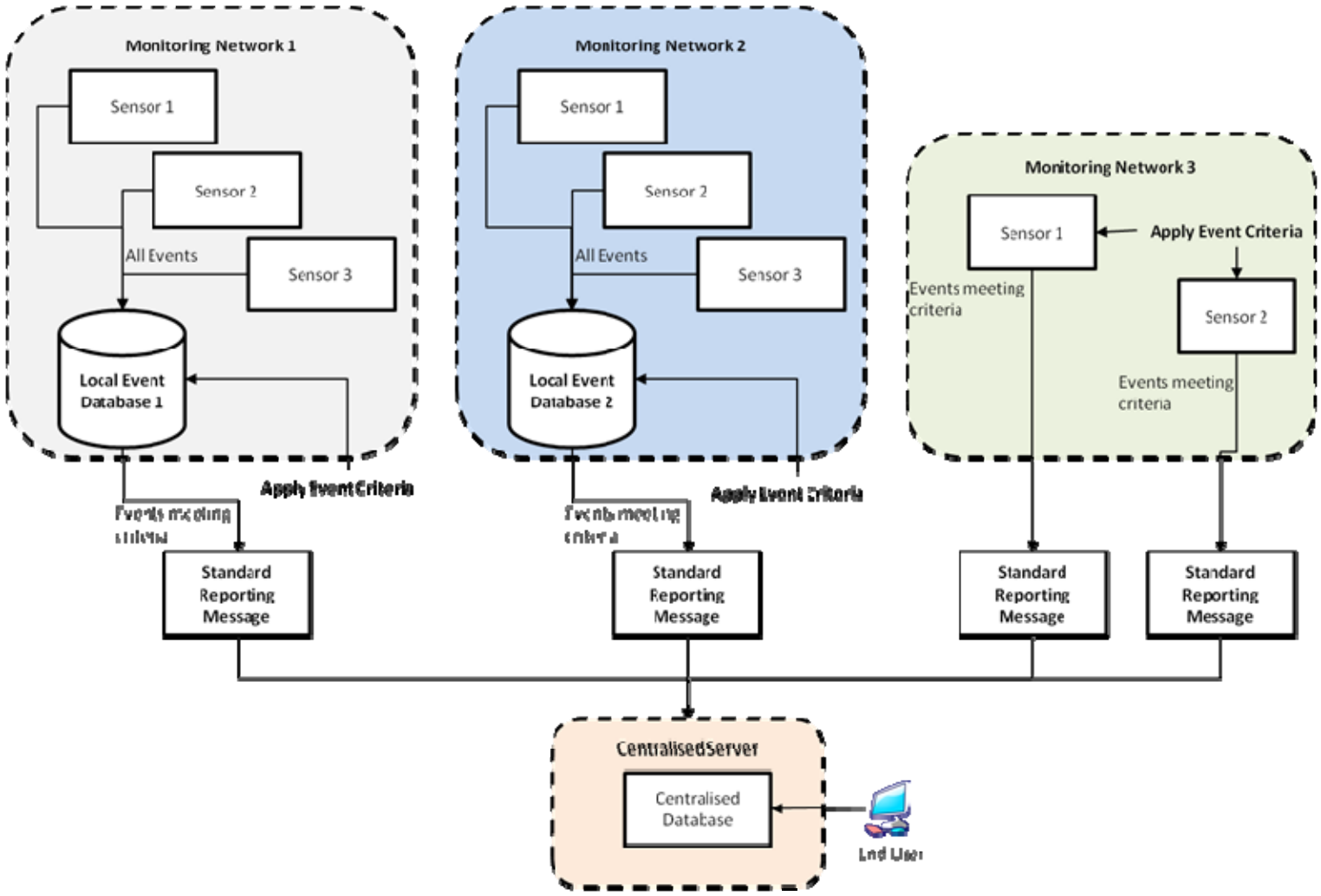
- Reporting Messages
  - Minimum reporting information
    - Per event: Id, event definition, frequency band, region, date
  - Optional additional information
    - Start time, duration, spectrum, delta power and reference noise figure, GNSS fix lost

STRIKE3 Event Definition

- Define standard event definition so that only events that meet criteria are reported:
  - Limit reporting to ‘significant’ events
  - Ensure consistency between detection systems
  - Can be applied post-detection, i.e. limit changes to detection equipment

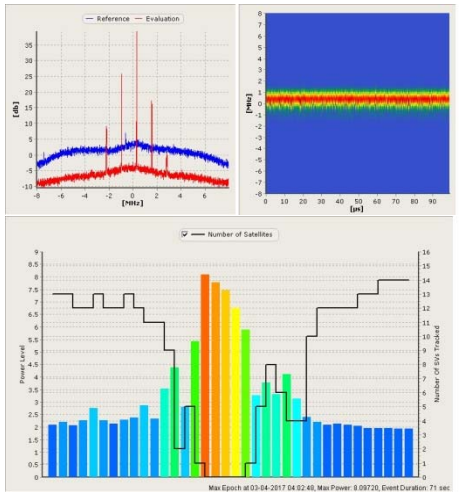
Type	Description
a	This event definition is intended for interference detection equipment that base the detection function on either power- or AGC-monitoring. If the received power is 5 dB (TBC) stronger than the expected noise power and if the received power is above this threshold for at least 5 (TBC) seconds, then an interference event has occurred. Where the noise power is the measured received power when there is no interference signal present at the input of the equipment. *Note: For AGC-monitoring systems this means a decrease of 5 dB in the AGC value and it should last at least for 5 seconds.*
b	This event definition is intended for interference detection equipment that base the detection function on GNSS-receivers. If the average C/N0, for used satellites in the positioning solution, is 10 dB (TBC) less than the expected C/N0 and if the C/N0 is below this threshold for at least 5 (TBC) seconds, then an interference event has occurred. Where the expected C/N0 is the measured average C/N0, for used satellites in the positioning solution, 1 minute before the event was triggered.

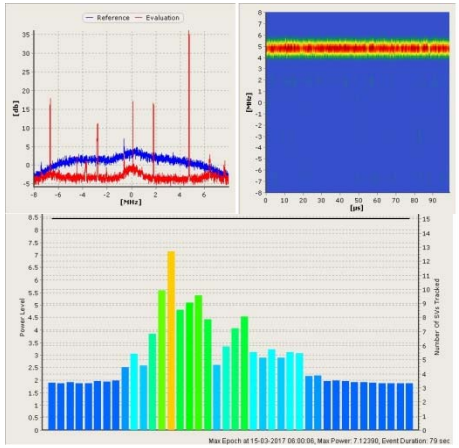
STRIKE3 Reporting System



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



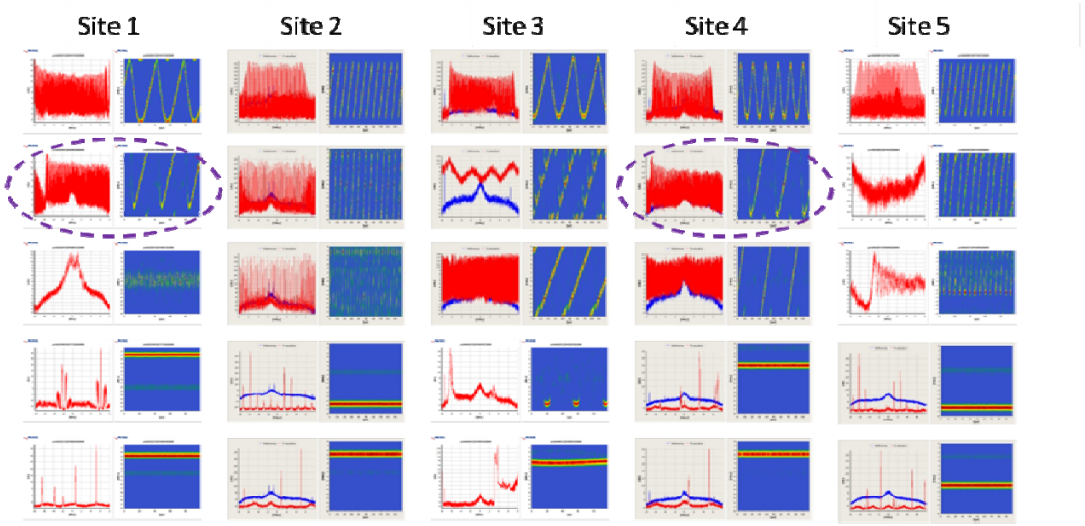


STRIKE3 Receiver Test Standards

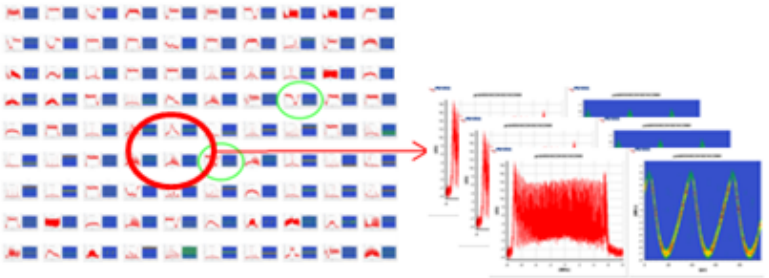
- The purpose is to assess GNSS receiver performance when subjected to “real-world” GNSS threats.
- Develop an outline test specification which can be used to assess performance of different GNSS receivers under a range of typical interference/jamming threats.
- The test standard shall be based on a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

STRIKE3 Database

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



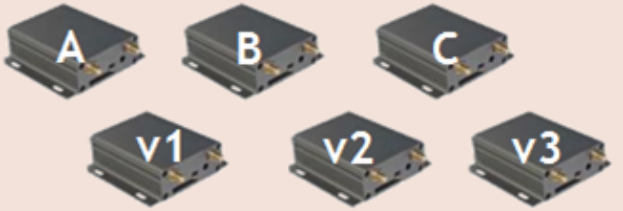
GNSS Receiver Testing



GNSS Threat "Test" Platform

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

STRIKE3 Test Plan



Devices under Test

GNSS Receiver
Vulnerability database

per threat battery, per application/market, per territory

Further Information

- www.gnss-strike3.eu
  - Project information
  - Draft standards for download
    - Reporting Standards
    - Test Standards

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)