STRIKE3 project
Standardisation of GNSS threat reporting and Receiver Testing

Mark Dumville

General Manager, NSL

6th UN ICG Interference Detection and Mitigation Workshop

9 May, Krk Island, Croatia

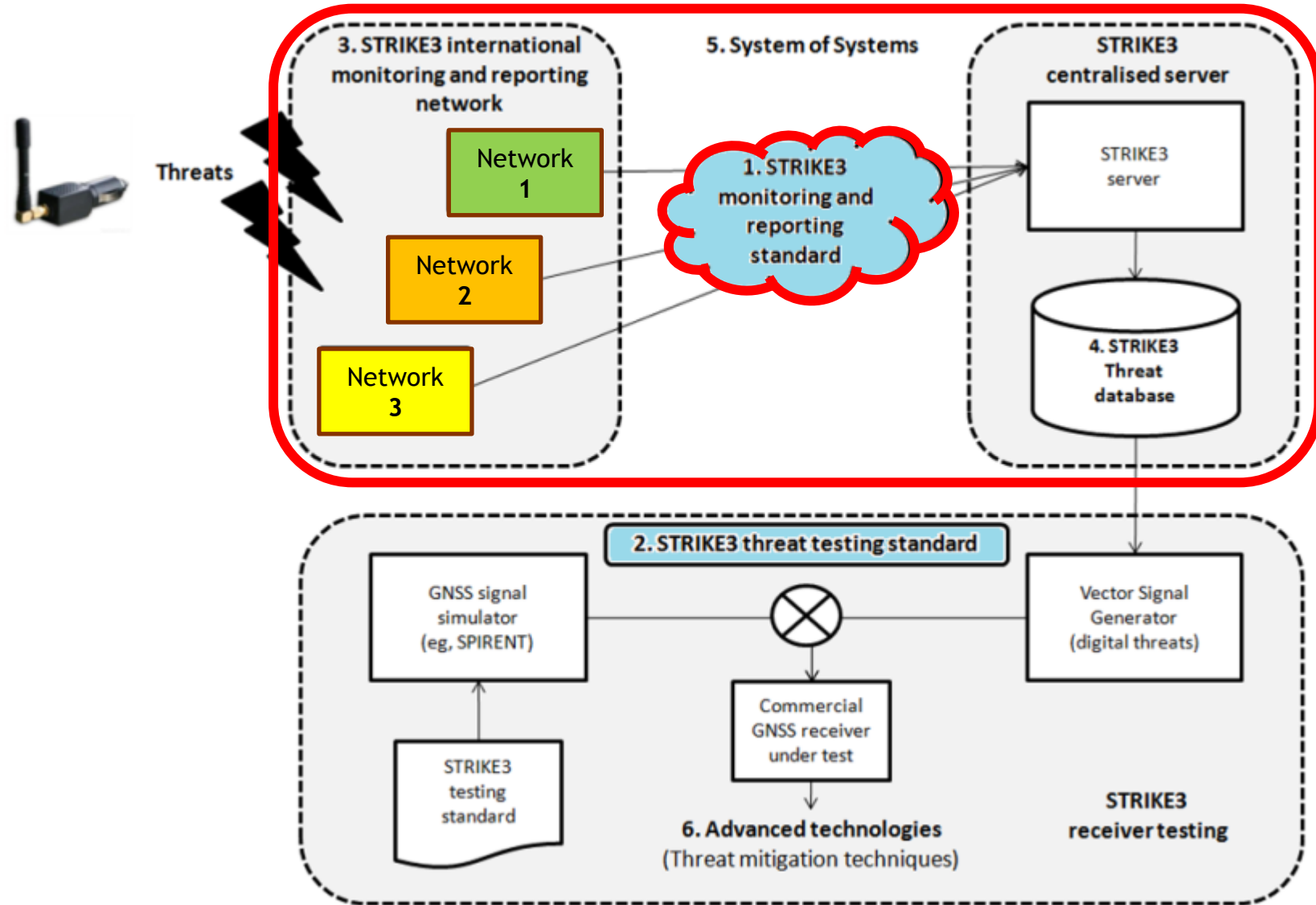www.nsl.eu.com

STRIKE3 is a project to protect GNSS…

- **S**tandardisation of GNSS **T**hreat reporting and **R**eceiver testing through **I**nternational **K**nowledge **E**xchange, **E**xperimentation and **E**xploitation [STRIKE3]

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


- Start date = 1 February 2016
- Duration = 3 years
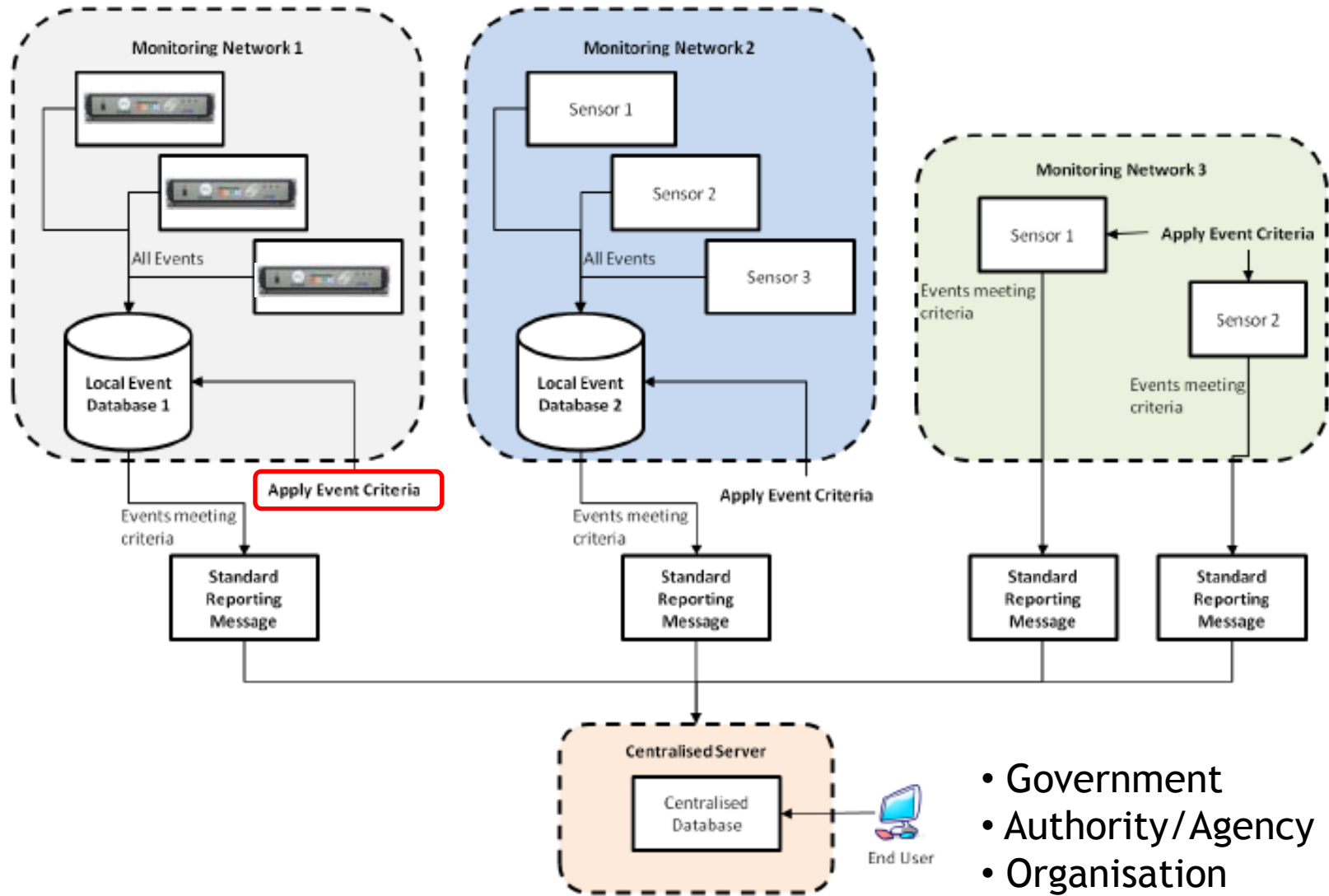
STRIKE3 Threat Reporting Standard

STRIKE3

3. STRIKE3 international monitoring and reporting network

Threats

Network 1

Network 2

Network 3

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)

STRIKE3 testing standard

Commercial GNSS receiver under test

Vector Signal Generator (digital threats)

6. Advanced technologies (Threat mitigation techniques)

STRIKE3 receiver testing

STRIKE3 Threat Reporting Standard

- 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
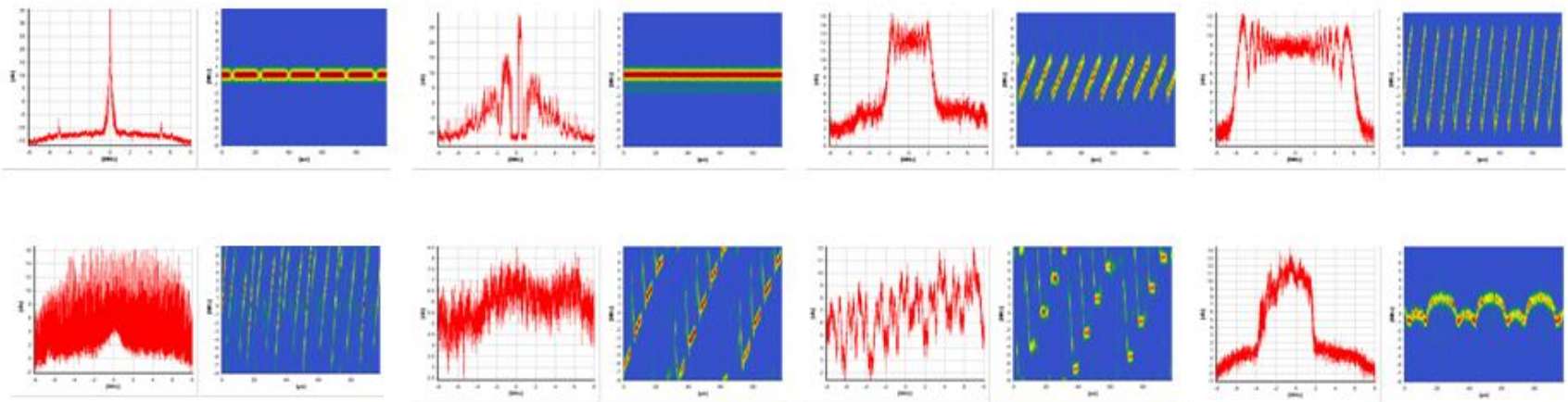
- Multiple RFI monitoring systems exist, with different features
- Any standard should reflect a minimum level of data
  - Suppliers and vendors can offer advanced features
  - Minimum requirement for monitoring and exchange

STRIKE3 Threat Monitoring and Reporting System Concept

STRIKE3 Reporting Requirements

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

www.nsl.eu.com

STRIKE3 Message Definition

- One message per event

- **Minimum content** (mandatory)
  - ID
  - Event definition
  - Frequency band
  - Geographic Region*
  - Date

- Optional content
  - Start time, duration
  - Spectrum
  - Power
  - GNSS fix lost

- Manufacturers content (not available)
  - Waveform Classification
  - Spectrogram
  - NMEA/GNSS data
  - Acquisition/Tracking performance
  - IQ data

www.nsl.eu.com

STRIKE3 Event Definition

- Define standard event definition so that only events that meet **specific criteria** are reported:
  1. Generated by a wide set of equipment (dedicated and general)
  2. Restrict report generation to **"significant"** events
  3. Ensure consistency between detection systems
  4. Can be applied post-detection, i.e. reduce changes to detection equipment

Event Type A - Dedicated (Power)

Event Type B - General (SNR)
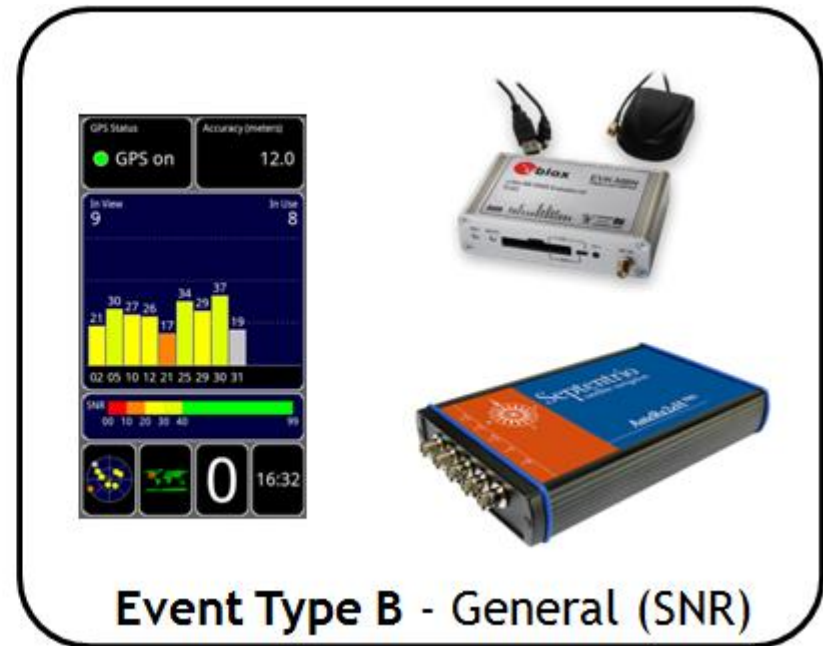
Comparison between RFI Monitoring Equipment

|	DETECTOR	RF OCULUS
Total Number of Detections	392	118
Number of common detections	107	

Collocation of DETECTOR and RF OCULUS - 7-week period Nov-16 to Jan-17

- Significant difference in total number of detections
  - Different "thresholds" used for interference detection
  - Differences in "monitored" bandwidths

- Good agreement for "significant" events
  - Chirp jammer events were detected by both systems
  - Timings of events similar (within a few seconds)
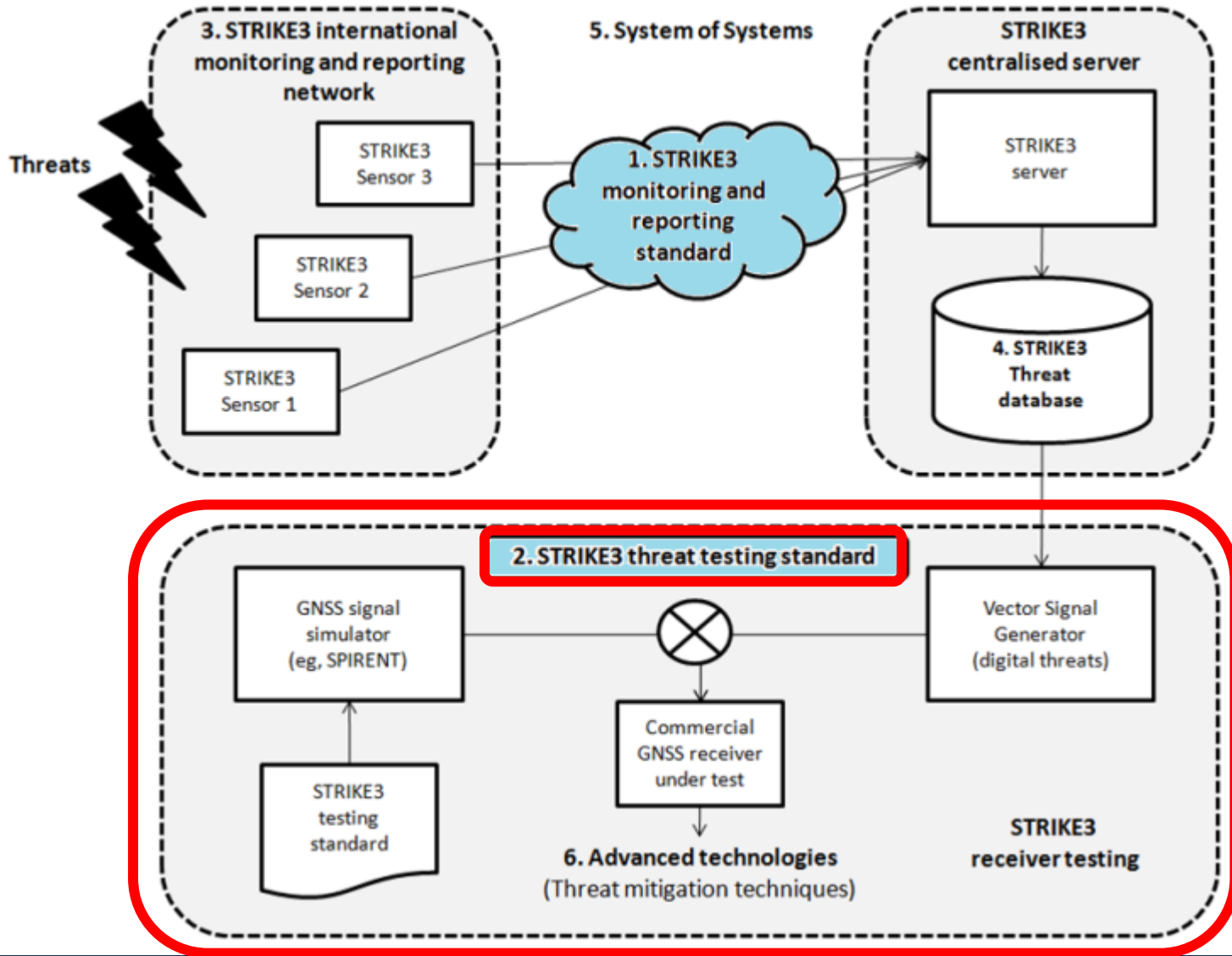
www.nsl.eu.com

Optional Content

- STRIKE3 Reporting Standard permits monitoring sites to report impact on GNSS

- However, many factors affect the impact of interference on GNSS
  - Type of interference (frequency, bandwidth)
  - Duration of interference
  - Emitter power
  - Distance from transmitter to monitoring site
  - Shielding of interference and obstructions along path
  - Receiving antenna type
  - Type of receiver and specific set-up / configuration

- STRIKE3 allows for optional content to be included
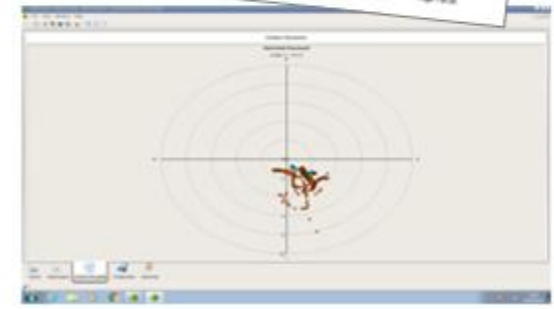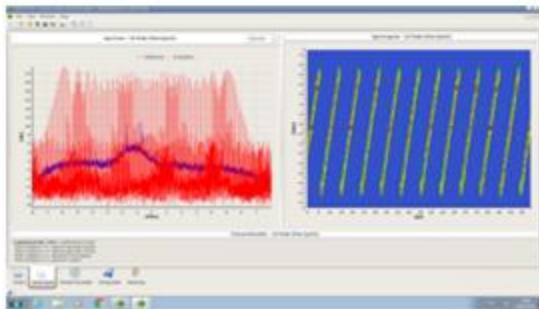
Examples: Start, Duration, Spectrum, Power, GNSS lost

www.nsl.eu.com

STRIKE3 Threat Reporting Standard

STRIKE3 Receiver Test Standards

France

airports

Extract the most relevant RFI threats:

- Per period (year)
- Per region (country)
- Per infrastructure
- Per domain (aviation)
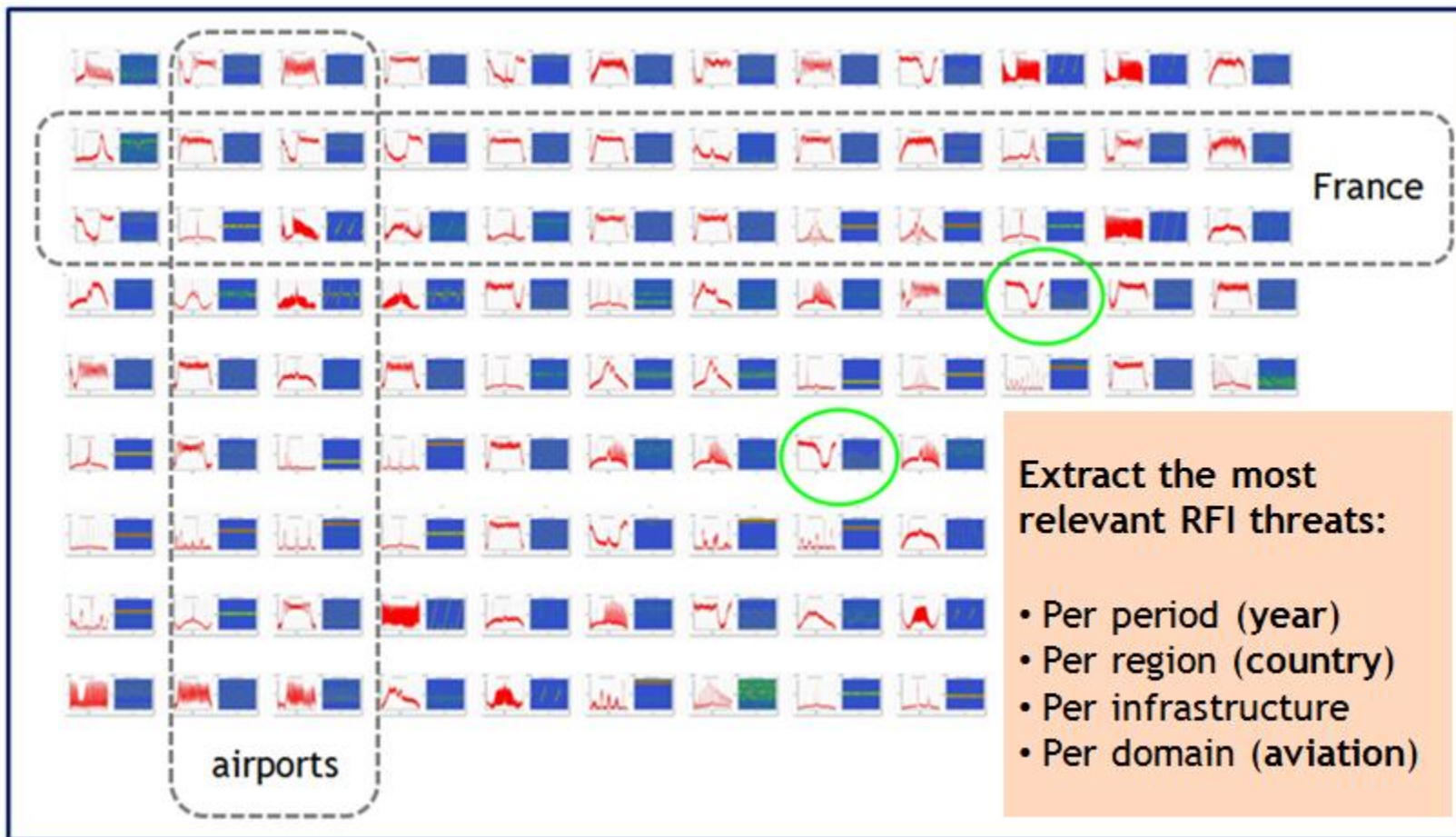
Most probable events, most severe, longest durations, new waveform etc…

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.
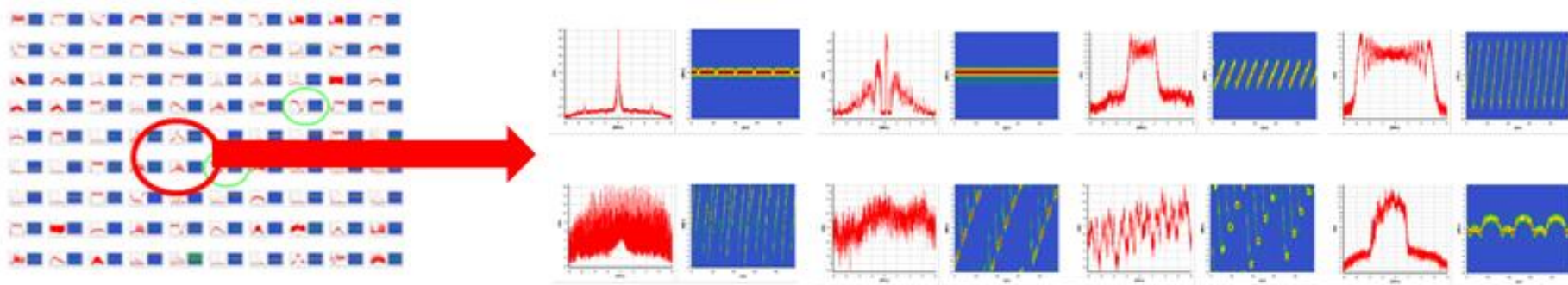

- The test standard shall be based on a generic series of threats as detected during the monitoring campaign.

- The test standard should evolve to incorporate new RF interference and jamming threats as they emerge

www.nsl.eu.com
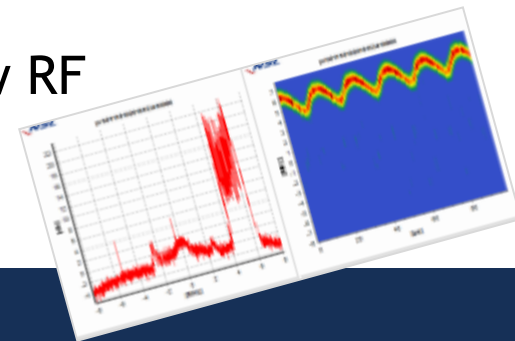
Test Considerations

1. Applicable to all GNSS systems and signals.
2. Must be applicable to all RFI threats
3. Repeatable process
4. Highly automated (preferable)
5. Results should be comparable
6. Standard metrics
   - Electronic measuring equipment
   - GNSS receiver output (eg NMEA values)
7. Applicable to different GNSS receivers
   - Mass-market (integrated antenna)
   - Professional grade
   - Safety of Life
   - Timing receiver
   - Integrated receiver (with other sensors)
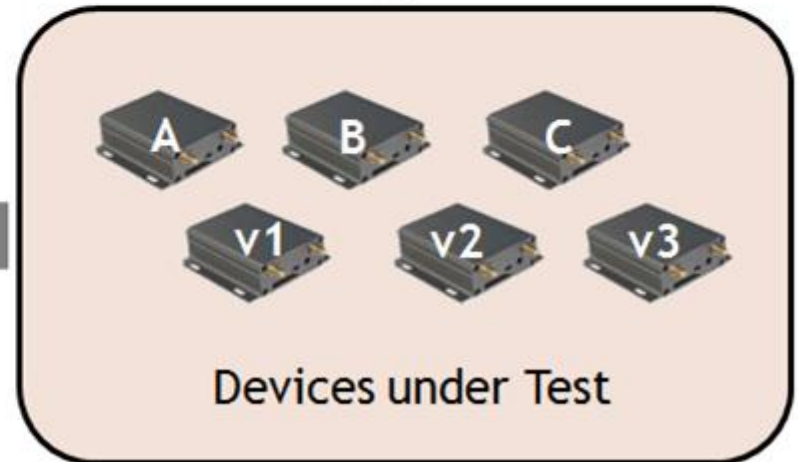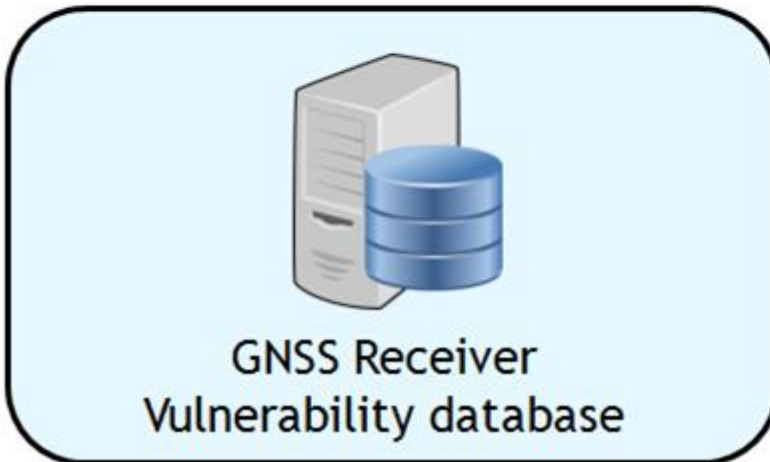
www.nsl.eu.com
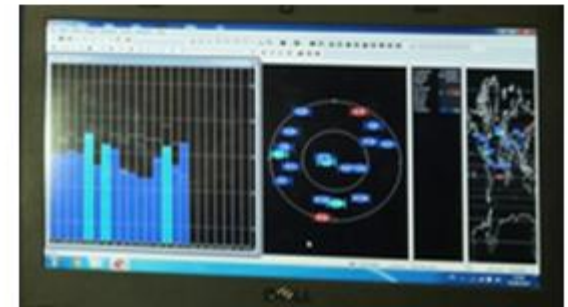
STRIKE3 Receiver Test
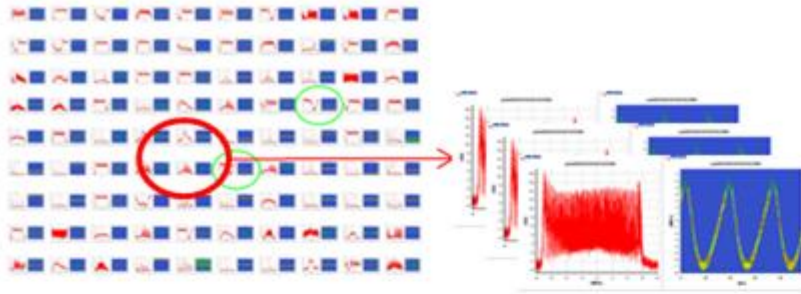
- Test different threats on the same device
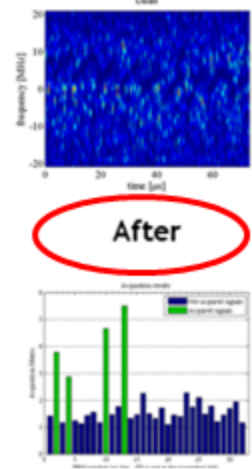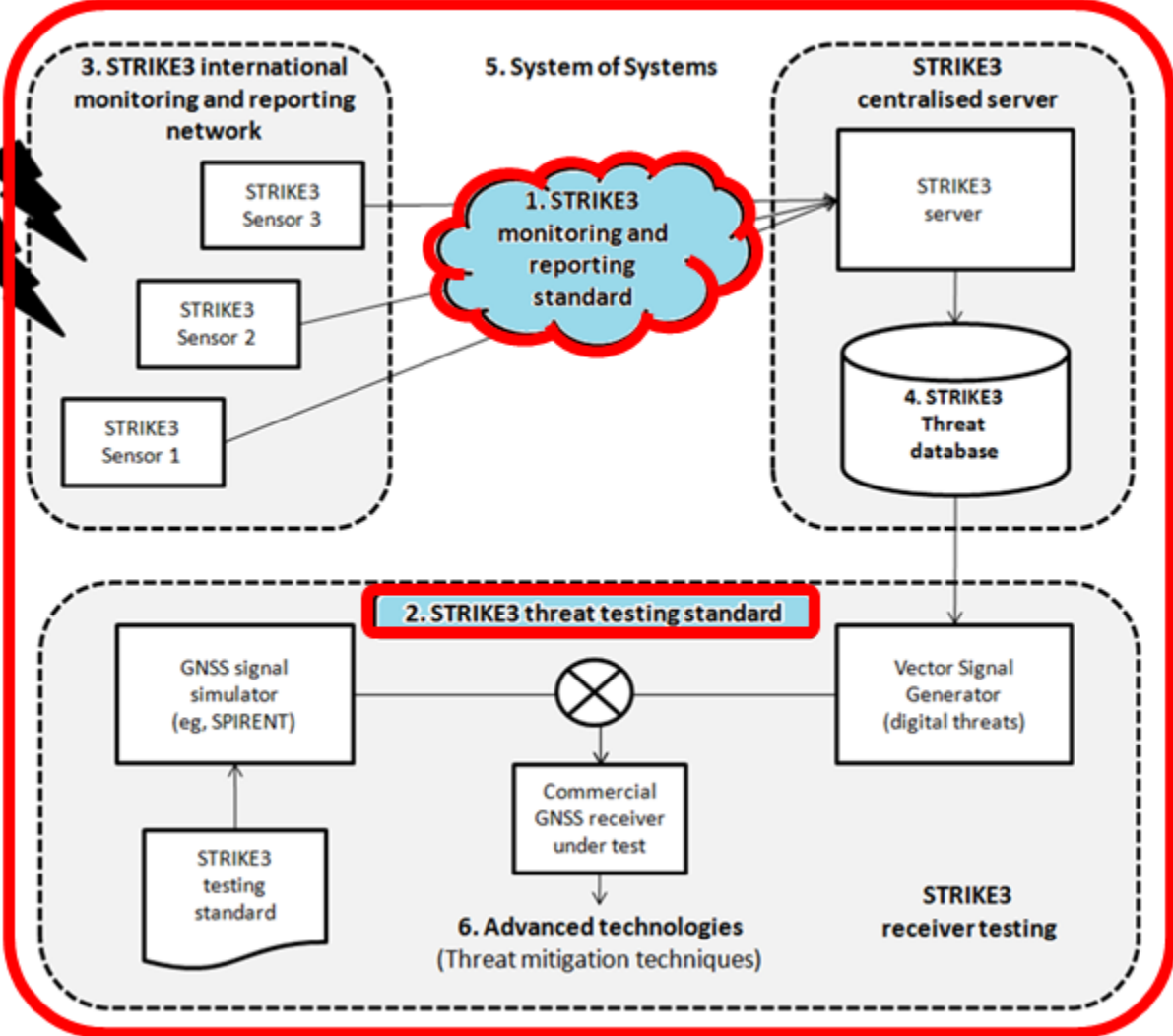- Test multiple receivers or devices
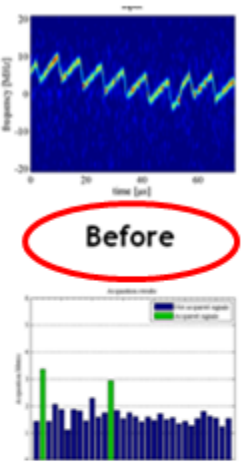- Test candidate mitigation measures

GNSS Threat "Test" Platform

STRIKE3 Test Plan

A   B   C

v1   v2   v3

Devices under Test

GNSS Receiver
Vulnerability database

per threat battery, per application/market, per territory

www.nsl.eu.com

STRIKE3 Threat Reporting & Testing Standards

Mitigation techniques are being developed outside the STRIKE3 project

STRIKE3 Threat Reporting & Testing Standards

- Standards for Threat Monitoring and Reporting
- Standards for Receiver testing against threats

Available from: www.gnss-strike3.eu

thank you

mark.dumville@nsl.eu.com