

**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:	Michael Pattinson, NSL Sanguk Lee, ETRI Zahidul Bhuiyan and Sarang Thombre, NLS Venkatesh Manikundalam, GNSS Labs Steve Hill, SAC	27.11.17
Checked by:	M Pattinson (NSL)	27.11.17
Authorised by:	M Dumville (NSL)	27.11.17

Pages: 55

Document Classification: Public



## Change Record

Issue Rev	Date	§: Change Record	Author(s)
1.0	03.02.2017	First version of document delivered for Requirements Review	SH, GA, SL, VM
2.0	27.11.2017	<p>Updated version delivered for Deployment Readiness Review at end of WP7: Receiver Testing Validation Platforms covering DRS comments from RBR and other necessary updates arising from implementation of the test platforms:</p> <ul style="list-style-type: none"> <li>• Use of GNSS constellation simulator to provide time synchronization of equipment and scenarios explained in section 2.2 (DRS Id 1)</li> <li>• Some clarification added to section 2.3.1 about frequencies and constellations to test</li> <li>• Some clarification about interference signals to test added to section 2.4.1</li> <li>• Added some more details on output messages from receivers (NMEA) and on metric calculation in section 3.2.2</li> <li>• Completed test procedures to remove TBCs and insert proposed values in section 4 (DRS Id 2)</li> <li>• Completed section on timing error test method in section 4.5 (DRS Id 3)</li> <li>• Completed section on threat selection in section 5 (DRS Id 4)</li> <li>• Updated section 6 to be consistent with final approach from other sections</li> <li>• Added information on baseline threat selection to Annex A</li> <li>• Corrected broken link to reference document in section 3.2.2</li> </ul>	MP, SL, ZB, ST

## Table of Contents

1	Introduction .....	7
1.1	Purpose of Document .....	7
1.2	STRIKE3 Overview .....	7
1.3	Document Overview .....	8
1.4	References.....	8
1.4.1	Applicable Documents .....	8
1.4.2	Reference Documents .....	9
1.5	Acronyms.....	9
2	Test Architecture.....	11
2.1	Introduction .....	11
2.2	Test Setups.....	12
2.2.1	Introduction .....	12
2.2.2	Mass Markets Receivers Test .....	13
2.2.3	Integrated Devices Test .....	14
2.2.4	Professional Multi-Constellation Receivers Test.....	15
2.2.5	Timing Receivers Test .....	16
2.3	General Scenario Settings .....	17
2.3.1	Frequencies / Constellations for Clean Signals .....	17
2.4	Other scenario settings .....	18
2.4.1	Types of interference .....	18
2.4.2	Atmospheric Modelling .....	19
3	Performance Metrics.....	20
3.1	Possible Metrics .....	20
3.1.1	Outputs from Measurement Devices .....	20
3.1.2	Outputs from GNSS Receivers .....	20
3.2	Analysis and justification of Metrics .....	20
3.2.1	Outputs from Measurement Devices .....	20
3.2.2	Outputs from GNSS Receivers .....	21
3.3	Selected Metrics.....	24
4	Test Methodology .....	25

## D4.2: Draft standards for receiver testing against threats

Ref: STRIKE3\_D42\_TestStandards

Issue: 2.0

Date: 27.11.17

---

4.1	Test Methodology Overview .....	25
4.1.1	Test Parameters .....	25
4.2	TTFF Test Method .....	27
4.3	Acquisition and tracking sensitivity test method.....	28
4.3.1	Single Peak Ramp Profile .....	31
4.3.2	Multi-Peak Ramp Profile .....	32
4.4	Receiver Dynamics Test Method.....	33
4.5	Timing Error test method.....	34
5	Criteria and Procedure for Selecting Threats.....	36
5.1	Overview of Proposed Approach.....	36
5.2	Procedure for Threat Selection.....	36
5.2.1	Introduction to Threat Selection .....	36
5.2.2	Process for Initial Threat Selection.....	36
5.2.2.1	Initial Filtering Based on Power Level.....	37
5.2.2.2	Identification of Different Chirp Signal Types .....	37
5.2.2.3	Selection Based on Common Signal Types.....	37
5.2.2.4	Selection of Evolving Signal Types.....	38
5.2.3	Description of Baseline Set of Threats .....	38
5.2.4	Receiver Testing and Impact Considerations .....	39
5.3	Use of Real Signatures for Threat Testing.....	40
5.3.1	Overview.....	40
5.3.2	Use of Synthetic I/Q Data.....	41
5.3.3	Replay of Raw Sample Data .....	41
5.4	Future Considerations.....	42
6	Application of Proposed Test Standards.....	43
Annex A:	Details on Threat Selection .....	45
	Definitions .....	45
	Chirp Signal Analysis – Number of Events .....	51

## List of Tables

Table 1-1: Applicable Documents.....	8
Table 1-2: Reference Documents.....	9
Table 1-3: Acronyms and Abbreviations.....	10
Table 2-1: GNSS Frequencies and Power Levels.....	18
Table 3-1: Performance Metrics.....	24
Table 4-1: TTFF Test Parameters.....	28
Table 4-2: Parameters of Interference Power Profile.....	29
Table 4-3: Key Parameters for Receiver Dynamics.....	33
Table 5-1: Descriptions of Baseline Set of Selected Threats.....	39

## List of Figures

Figure 2-1 : Test setup for Mass-Market receivers.....	13
Figure 2-2 : Test setup for Mobile (integrated) receivers.....	14
Figure 2-3 : Test setup for a professional multi-frequency, multi-constellation receiver ....	15
Figure 2-4 : Test setup for GNSS timing receivers.....	16
Figure 2-5: GNSS Constellations / Frequencies .....	17
Figure 4-1 Test Methodology Overview .....	26
Figure 4-2 : TTFB Test Profile .....	27
Figure 4-3: Interference Single Peak Ramp Profile.....	31
Figure 4-4: Example of a multi-peak power profile.....	32
Figure 5-1: Overview of Interference Signal Generation for Testing .....	41
Figure 6-1 Use of Standard Flow Diagram .....	44
Figure A-1: Number of Chirp Events of each type at Each Site .....	51
Figure A-2: Total Number of Events of each type from All Sites .....	52
Figure A-3: Number of Sites that Detect Each Type of Event .....	53

# 1 Introduction

## 1.1 Purpose of Document

This document is the Draft Standards for Receiver Testing against Threats. The main objectives of this document are to:

- Propose Strike 3 Receiver Test Architecture.
- Propose Strike 3 Test Methodology
- Assess performance metrics which will be logged from receivers under test and analysed against defined acceptable performance
- Describe method for selecting threats from Strike 3 and define set of baseline threats to test receivers against.
- Propose method for using real threats in receiver testing.

The overall intention is to provide a standard methodology for testing receivers against real interference signals collected in the field. Test authorities and application developers can then take these standards as the basis for creating application / equipment specific tests, with suitable thresholds for performance, for example.

This deliverable is prepared as part of WP4: Draft Standards Development.

The lead partner for WP4 is SAC. Contributions have also been provided by NSL, FOI, NLS, SAC, ETRI and GNSS labs, with review and comment from AGIT.

## 1.2 STRIKE3 Overview

The objective of the STRIKE3 project is to develop international standards in the area of GNSS threat reporting and GNSS receiver testing. This will be achieved through international partnerships. GNSS threat reporting standards are required to ensure that international GNSS threat databases can be developed. GNSS receiver test standards are required to ensure new applications can be validated against the latest threats. Both standards are missing across all civil application domains and are considered a barrier to the wider adoption and success of GNSS in the higher value markets.

STRIKE3 will persistently monitor the international GNSS threat scene to capture the scale and dynamics of the problem and shall work with international GNSS partners to develop, negotiate, promote and implement standards for threat reporting and receiver testing. This is being achieved through the deployment and operation of an international GNSS interference monitoring network.

### 1.3 Document Overview

This document is arranged in the following sections:

- **Section 1** the current section, is an introduction that describes the purpose, scope and structure of the document.
- **Section 2 *Test Architecture***. This section defines the test system architecture utilised to assess the performance of GNSS receivers in the presence of interference signals derived from the Strike 3 database.
- **Section 3 *Performance Metrics***. This section considers how interference impacts a GNSS receiver and which metrics should be logged and observed to assess that impact. It also suggests suitable levels of performance.
- **Section 4 *Test methodology***. This section describes the method for carrying out the testing against the proposed standard.
- **Section 5 *Criteria and Procedure for Selecting Threats***. This section considers the basis for how threats should be selected from the Strike 3 database for addition to the Standard and how the threats can be parameterised for utilisation within the test system.
- **Section 6 *Application of Proposed Test Standards***. This section considers how the user would utilise the standard to assess the performance of their GNSS receiver equipment and the associated systems.
- **Annex A *Details of Threat Selection***. This section describes the process that was followed for assessing and selecting threats from the Detector database for use in receiver testing.

### 1.4 References

#### 1.4.1 Applicable Documents

Ref.	Document title	Document reference	Issue	Date
AD1	STRIKE3 Grant Agreement	Grant Agreement - 687329	-	26/01/2016

**Table 1-1: Applicable Documents**



## 1.4.2 Reference Documents

No.	Reference
RD1	W.J. Riley, "Handbook of Frequency Stability Analysis." NIST Special Publication 1065, National Institute of Standards and Technology, Boulder, CO, USA, July 2008

**Table 1-2: Reference Documents**

## 1.5 Acronyms

Acronym	Definition
AD	Applicable Document
ADC	Analogue to Digital Convertor
AGC	Automatic Gain Control
AWGN	Additive Gaussian White Noise
BDS	BeiDou Navigation Satellite System
C/N0	Carrier to Noise ratio
CW	Continuous Wave
DME	Distance Measuring Equipment
DMB	Digital Multimedia Broadcasting
DOCXO	Double Oven Crystal Controlled Oscillator
FDMA	Frequency Division Multiple Access
FOC	Full Operational Capability
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
IF	Intermediate Frequency
IOC	Initial Operational Capability
IRIG-B	Inter-Range Instrumentation Group time codes
IRNSS	Indian Regional Navigation Satellite System
J/S	Jammer to Signal power ratio
LNA	Low Noise Amplifier

## D4.2: Draft standards for receiver testing against threats

Ref: STRIKE3\_D42\_TestStandards

Issue: 2.0

Date: 27.11.17

---

<b>Acronym</b>	<b>Definition</b>
NB	Narrow Band
PPS	Pulse Per Second
RD	Reference Document
RF	Radio Frequency
RX	Receiver
SDR	Software Defined Radio
SNR	Signal to Noise Ratio
SV	Satellite Vehicle
TACAN	Tactical Air Navigation System
TTFF	Time To First Fix
TX	Transmitter
VSG	Vector Signal Generator
WB	Wide Band

**Table 1-3: Acronyms and Abbreviations**

## 2 Test Architecture

### 2.1 Introduction

The aim of this section is to establish a test architecture necessary for testing receivers in the presence of RF interference that is comprehensive, repeatable and covers the main sets of receiver types, defined as follows:

- **Professional receivers:**

Professional receivers are usually higher cost, are optimized for precise measurements and positioning, and often can handle multiple different frequencies and constellations.

  - *Multi Constellation*
    - *FOC: GPS, GLONASS, IRNSS*
    - *IOC: Galileo, BDS(BeiDou System)*
  - *Multi Frequency (Civil)*
    - *L1 & E1*
    - *E5a & L5*
  - *Carrier Phase*
  - *Differential modes*
  - *Bandwidth : wide*
  
- **Mass-market receivers:**

Mass-market receivers are typically lower cost, with lower power consumption, and are optimized for signal and solution availability (e.g. tracking high sensitivity). They are typically single frequency (L1), although they may be multi-constellation.

  - *Low cost, low power*
  - *GPS L1 +GLONASS L1 + Galileo E1 + BDS (B1)*
  - *Includes chipsets e.g. Qualcomm Snapdragon 800 series*
  - *Bandwidth : narrow*
  
- **Integrated receivers:**

Integrated receiver are those devices where the antenna and receiver are integrated in a single unit. These are typically consumer devices e.g. phones but can also be in ruggedized form for e.g. maritime applications

  - *Antenna+Receiver*

- *Mass-market chipsets are integrated into antenna built-in receiver module as integrated receivers.*
  
- **Timing Receivers:**

Timing receivers are specifically designed to provide precise time information and precise reference timing signal to timing infrastructure such as mobile communications base station, terrestrial DMB station, DBS station, financial trade system, smart grid for power plant etc. Some of timing receiver equipped with precise oscillator like DOCXO for maintain timing requirement during outage of GNSS timing service.

## 2.2 Test Setups

### 2.2.1 Introduction

When defining the test set-up the key considerations were:

- It must be possible to test all the appropriate GNSS constellations and signals.
- The test set-up must be repeatable and, if possible, some level of automation is useful.
- The results of tests from different receivers or for a single receiver against different types of interference must be consistent and comparable.
- Metrics gathered from either measuring devices and/or receiver output

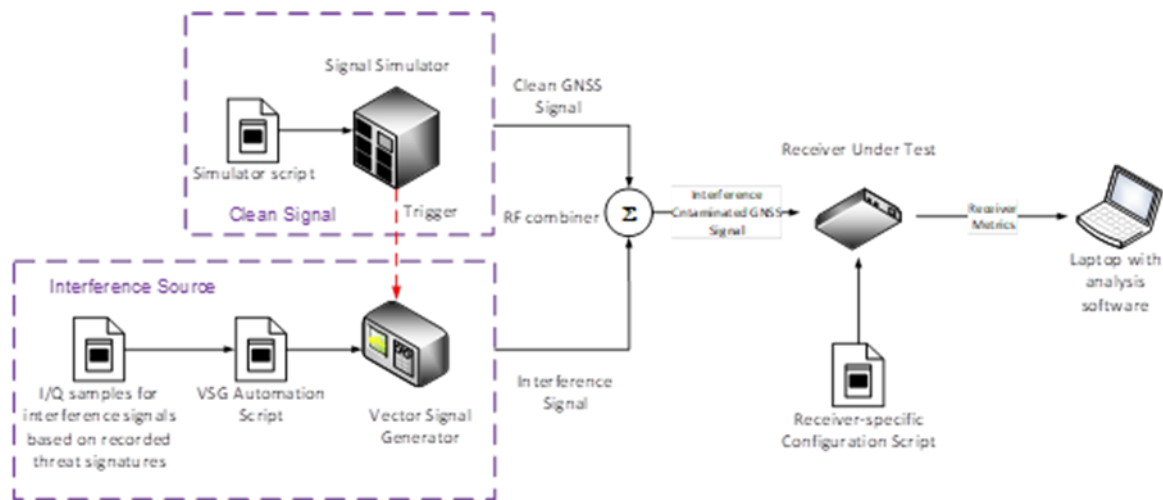
Based on the above, the main features of the test setups are as follows:

- It is preferable to use a GNSS constellation simulator, though GNSS record/replay device could be acceptable if the recorded signal was of sufficient 'quality' e.g. no multipath, obscuration or interference.
- Interference signals based on those from real detected events are utilized to test the receiver performance. This could be implemented as either synthetic representations of real signals or by replaying the raw samples of the interference itself through a signal generator.
- Architecture would support extension for spoofing and meaconing interference classes in the future.
- There are 4 setups defined, one for each of the main receiver classes listed above.
- GNSS simulator, Interference replay and Receiver configurations should be scripted to ensure repeatability and traceability of testing.
- GNSS constellation simulator is used to provide reference time information to the other equipment to ensure synchronization of the interference scenarios.

- All defined (Section 3) receiver metrics should be recorded for later analysis against applied GNSS and interference signals.
- Automation of the tests is desirable.

### 2.2.2 Mass Markets Receivers Test

In test scenario-1 illustrated in Figure 2-1, the GNSS signal is generated from a constellation simulator such as a Spirent Simulator. In the optimal set-up, the output is split two ways to feed the receiver under test with a clean GNSS signal in the absence of interference to allow measurement of the baseline performance, while the split signal is added to a controllable interference signal and fed to the same model and make of receiver to measure performance in presence of interference<sup>1</sup>.



**Figure 2-1 : Test setup for Mass-Market receivers**

Note that since the signal is generated from an RF constellation simulator and thus is repeatable, the tests with and without interference can also be performed in series if only one receiver is available, although doing the test in parallel saves time as the test is run only once.

In this set-up, the interference is generated using a Vector Signal Generator (VSG). To create the interference, I/Q sample data is used as input to the VSG. This can either be I/Q data for a synthetic signal that is representative of a real signal, or it can be raw I/Q data

<sup>1</sup> Note that it is possible to replace the RF GNSS Constellation simulator with a record and playback device for the GNSS signals if a RF constellation simulator is not available. However, the user would need to ensure the recording was of good quality and not contaminated with interference, multipath, obscuration etc.)

recorded in the field for a real event. Strike 3 will assess and compare the two options for adding interference and make recommendations for a future approach on the interference sources.

Scripts are input into the vector signal generator and the RF GNSS constellation simulator to automate the testing process. When completed, this test standard will propose which threats to test against and provide the parameters to the automation script of the vector signal generator.

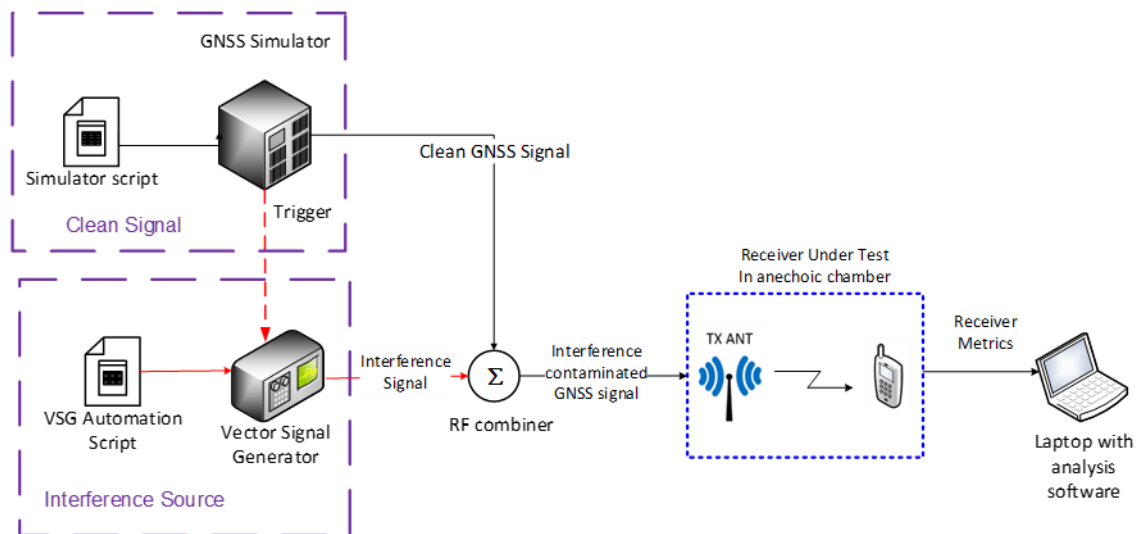
The time-tagged receiver metric outputs and the J/S are stored on a storage device.

Once the test system is assembled, the system must be calibrated to ensure that the simulated GNSS signal appears at a power level of -130dBm at the input to the receiver. It is less important to calibrate the interference signal as this is variable. However, it must be possible to measure and record the interference power level at the input to the receiver throughout the test (i.e. J/S).

Note that there should be synchronisation between the GNSS constellation simulator and the interference generator to ensure repeatability of the tests, e.g. by using time-tagged triggering function.

### 2.2.3 Integrated Devices Test

Figure 2-2 shows the test setup for integrated receivers. In this test, the GNSS signal from a constellation simulator is added to an interference signal generated by a vector signal generator and then radiated within an anechoic chamber using a standard antenna. Similar to the first test scenario, it would be advantageous to measure the baseline performance without interference. It is recommended that the test be done in series, as a single anechoic chamber would be required.



**Figure 2-2 : Test setup for Mobile (integrated) receivers**

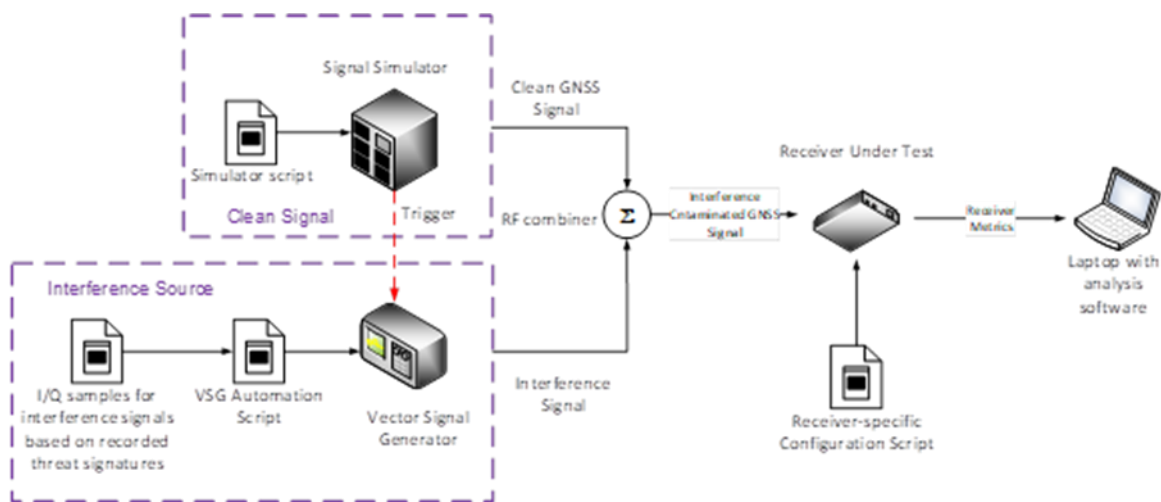
It might be necessary to compensate for loss through cables and the antenna gain inside

the anechoic chamber. This can be achieved by adjusting the output of the vector signal generator /SDR such that the output corresponds to the required level.

### 2.2.4 Professional Multi-Constellation Receivers Test

When testing the performance of professional receiver under interference, it is paramount that the testing accounts for the different capabilities of the receivers, for example, a dual frequency receiver should be tested using signals on both frequencies it supports. Similarly, a receiver which is multi-constellation should be tested using clean signals for the different constellation/frequencies it supports. As a minimum, interference should be generated in GPS L1 / Galileo E1 frequency band for all equipment - that is the baseline for the STRIKE3 project and is the situation described in these draft standards. Nevertheless, in the future it could be foreseen that testing of interference on multiple frequency bands (either individually or simultaneously) could be of benefit.

Figure 2-3 shows the general test setup for a multi-constellation and/or multi-frequency receiver.



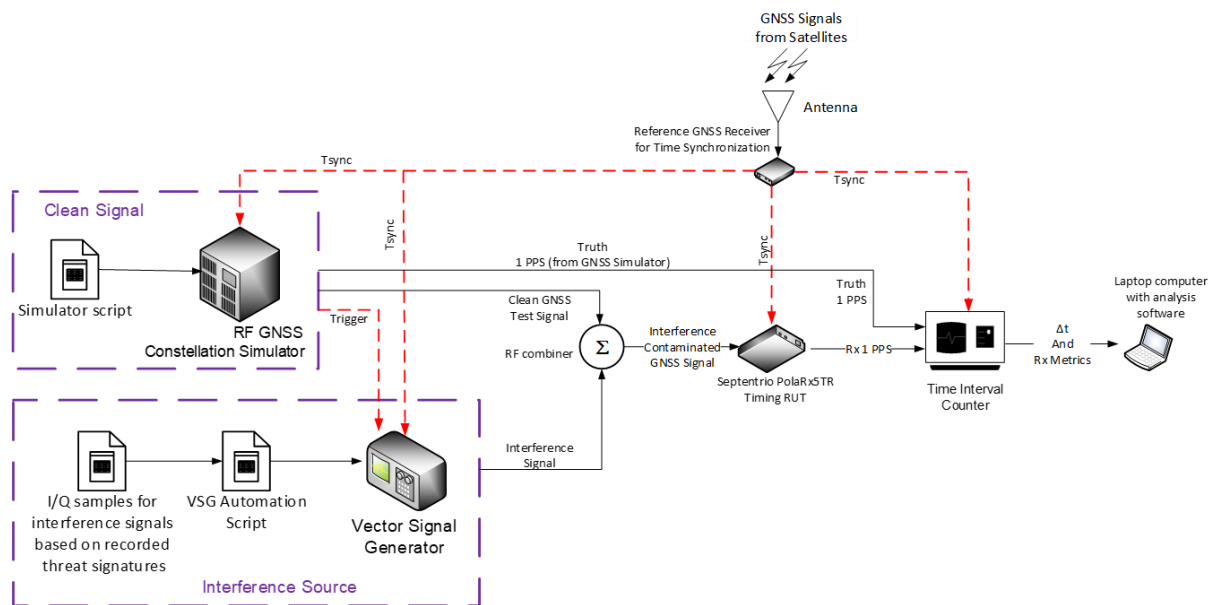
**Figure 2-3 : Test setup for a professional multi-frequency, multi-constellation receiver**

As illustrated in Figure 2-3, the baseline case includes generation of interference on GPS L1 using a single VSG. If generation of interference on multiple frequency bands at the same time was required then additional VSG capability would be necessary.

As with the previous test setups, Strike 3 test standards with a set of threat definitions are inputted into the vector signal generator via an automation script.

## 2.2.5 Timing Receivers Test

GNSS timing receivers provide timing signal outputs such as one pulse per second (1 PPS) and IRIG-B that can be used to synchronise other devices and systems. To be able to confirm the accuracy of the receiver derived pulses, it is essential that they are compared against a truth signal. This can be generated by the use of a GNSS constellation simulator. The test setup is shown in Figure 2-4.



**Figure 2-4 : Test setup for GNSS timing receivers**

As illustrated in Figure 2-4, a GNSS Constellation simulator is used to provide a simulated GNSS signal and is fed by a script to configure the simulation. It also provides a truth 1PPS signal as a reference to assess the accuracy of the timing signal from the receiver under test.

In this case the test is performed twice – once with a clean signal (no interference) to measure baseline performance for the receiver under test, and then a second time with the interference signal added to the clean signal and fed to the same receiver to measure its metrics under interference.

An time interval counter is used to compare the reference 1PPS signal generated by the simulator and the timing signals generated by the receivers with and without interference. Under no interference it would be expected that the timing signal from the receiver under test would be synchronised with the truth 1PPS signal with little jitter. With interference applied, the jitter displayed by the receiver under test timing signal will increase and its accuracy thus impacted.



## 2.3 General Scenario Settings

### 2.3.1 Frequencies / Constellations for Clean Signals

The key recommendation is that the testing should cover the constellation/frequency capabilities of the receiver under test. This would almost certainly cover the L1 band for the majority of receivers but other frequency bands are supported, especially in high end professional receivers. As a minimum, the constellation / frequency combination required for the basic operation of the receiver for the target application should be tested, i.e. if a receiver will be used in GPS+Galileo L1/E1 mode then clean signals for GPS+Galileo L1/E1 should be generated by the constellation simulator. Note that it could be envisaged where all supported frequencies are tested simultaneously, though the test system would need enhancement to support this configuration.

The diagram and table below show the frequency bands used in each constellation together with the power level of each signal which must be achieved at the receiver input during the tests.

#### ■ Frequency Offsets ( Inband/Out of band) w.r.t. Center Frequency

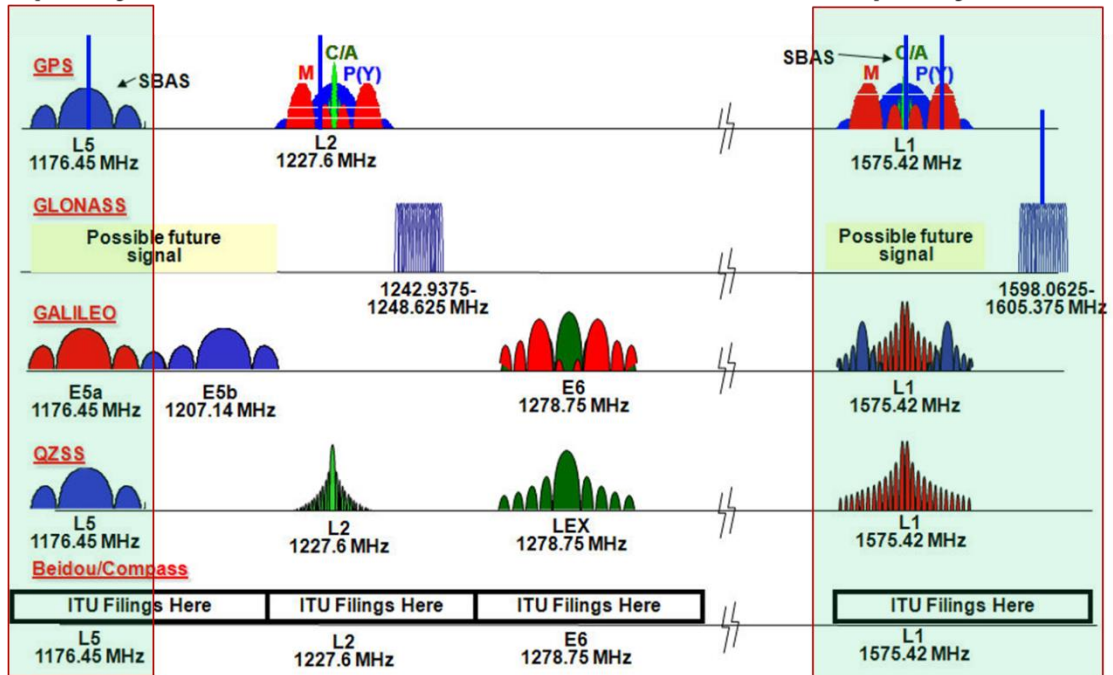


Figure 2-5: GNSS Constellations / Frequencies

Table 2-1: GNSS Frequencies and Power Levels

Constellation	Centre Frequency (MHZ)	Min Power (dBm)	Notes
GPS L1, L1C	1575.42	-128.5 (C/A) -127 (L1C)	
GPS L2, L2C	1227.6	-134.5 -> 131.5	Increasing power with newer satellites
GPS L5	1176.45	-127.9	
GLONASS L1	1598.0625 – 1605.375	-131	FDMA
GLONASS L2	1242.9375 – 1248.625	-137	FDMA
GALILEO E1 (OS)	1575.42	-127	
GALILEO E5a	1191.795	-125	
GALILEO E5b	1176.45	-125	1207.14 combined centre freq.
GALILEO E6 (CS)	1278.75	-125	
QZSS L1	1575.42	-128.5 (C/A) -127 (L1C) -131 (SAIF)	
QZSS L2	1227.6	-130	
QZSS LEX	1278.75	-125.7	
QZSS L5	1176.45	-127.9	
BEIDOU B1	1575.42	-133	
BEIDOU B2	1207.14	-133	Similar band to E5
BEIDOU B3	1268.52	-133	Similar band to E6

## 2.4 Other scenario settings

### 2.4.1 Types of interference

GNSS receivers could potentially, experience the following interference types:

- Jamming (intentional or unintentional)
- Meaconing

- Spoofing

Whilst spoofing and meaconing are bona-fide threats to GNSS receiver operation, they as yet, are not commonly encountered. They require specialist knowledge and equipment to undertake which in turn suggests a very specific motive. However, GNSS jamming is relatively common and can occur for a variety of reasons:

- Deliberate jamming
- Secondary effects of 'personal protection devices' afflicting adjacent users
- Poorly designed, installed or faulty electronic equipment.
- User close to high power transmitting equipment.

Therefore, this document considers jamming interference only in GPS L1 / Galileo E1 frequency band.

It is noted that constellation simulators and signal generators have the capability to generate all kinds of interference at different frequencies and with different characteristics. The purpose of these standards generated as part of the STRIKE3 project are to test receivers against interference that has been observed in the real world through a dedicated interference monitoring network. The selection and generation of interference test signals in this proposed test standard will be based on real signals detected in the field and is described in more detail in Section 5.

## **2.4.2 Atmospheric Modelling**

The GNSS simulator should include atmospheric modelling capability as the receivers under test will compensate for these effects, especially single frequency receivers. The common models utilised are:

- Ionosphere: Klobuchar (default parameters)
- Troposphere: Saastamoinen (default parameters)

# **3**

## 3 Performance Metrics

This section considers the receiver observations, measurements and outputs that can be utilised to assess the performance of the receiver in the presence of interference. Receivers vary in terms of the outputted metrics but the standard proposes to use the most routinely available metrics for the purpose of performance assessment. There are two main types of metric: either from measurement devices like frequency counter and oscillator or those output directly from receivers.

### 3.1 Possible Metrics

#### 3.1.1 Outputs from Measurement Devices

Performance of receiver under threat from interferences can be assessed by measuring jamming signal level, timing error.

- Jamming Signal Level(J/S dB) (using Oscilloscope/Spectrum Analyser)
- Time Error(ns) ( using frequency counter/Oscilloscope )

#### 3.1.2 Outputs from GNSS Receivers

Metrics that routinely available from typical receivers are as follows

- Position Accuracy in meters (rms)
- Values of C/N0 for each SVs
- Number of SVs used/Number of SVs visible
- TTFF for GPS Fix
- Total outage of GNSS signal due to interference.
- Timing error(ns)

### 3.2 Analysis and justification of Metrics

#### 3.2.1 Outputs from Measurement Devices

Metrics obtained from measuring devices are very good for GNSS test against GNSS interference like jamming. However, it is quite expensive and dependent on availability of the expensive measuring device.

- Jamming Signal Level(J/S dB) from Oscilloscope

- Jamming to Signal level indicator is used to reference the input signal level to the receiver in order to characterise the scenario. It is not a performance metric of the receiver
  - J/S is essential metric for measuring interference power level & its shape during the GNSS receiver test against GNSS interference like Jamming.
  - Jamming signal level exposed to the tested receiver is essential for test of GNSS receiver against GNSS interference like jamming.
  - Jamming level should be calibrated with respect to GNSS signal such as around -130 dBm (it varies for the frequency band)
  - Jamming signal level can be established for position error exceeding 10 meter (in RMS), 95meter(in RMS), Loss of GPS Fix, hand-over for timing receiver, GPS Fix, back to normal for timing receiver during ramp profile test.
- Time Error (ns) from frequency counter or oscilloscope.
    - Frequency counter or oscilloscope can measure time error of GNSS timing receiver.
    - Jamming level should be calibrated with respect to GNSS signal such as ~ -130 dBm (it varies depending upon the frequency band and constellation (see Table 2-1: GNSS Frequencies and Power Levels ).

### 3.2.2 Outputs from GNSS Receivers

- Position Accuracy (error) in meter (rms)
  - Position accuracy (error) with respect to a known position is very important performance metric and it is dependent on DOP, C/N0 of each of SVs, number of visible SVs etc.
  - GNSS interference like jamming signal degrades a GNSS receiver positioning accuracies and eventually causes outage of GNSS positioning, navigation and timing services.
  - This metric is selected for GNSS receiver test against interference.
  - Use NMEA output from receiver (GGA)
- Values of C/N0 (SNR) for each SVs
  - This value is crucial to accuracy of pseudo-range. If some of C/N0 values are poor with respect the others, then position error obtained from those pseudo-ranges is also poor.
  - The level of C/N0 for SVs are very important metrics for performance of receivers in positioning, navigation and timing services. Overall

- performance metrics can be positioning error or timing error.
- Use NMEA output from receiver (GSA and GSV)
- Number of SVs used/Number of SVs visible
  - Number of SV visible is derived theoretically by considering geometry at the receiver vicinity.
  - Number of SV used means that number of SV signals which are used for obtaining navigation solution.
  - As GNSS interference power level is increased, C/N0 for the SVs decreases. As the value decreases towards zero, then the position fix cannot be maintained.
  - The metric is selected as it allows the user to check nominal receiver performance without interference.
  - Use NMEA output from receiver (GSA and GSV)
- TTFF for GPS Fix total outage of GNSS signal due to Jamming
  - Definition: Time to first fix (TTFF, seconds) from GNSS signal acquisition, tracking and obtaining navigation solution (GPS Fix).
  - TTFF can be calculated from GGA data in NMEA-0183

**GGA Global Positioning System Fix Data. Time, Position and fix related data for a GPS receiver**

```

      1           2           3 4           5 6 7 8 9 10 | 11 12 13 14 15
      |           |           | |           | | | | | | | | | | |
$--GGA,hhmmss.ss,l1l1.l1,a,yyyyy.yy,a,x,xx,x.x,x.x,M,x.x,M,x.x,xxxx*hh

```

- 1) Time (UTC)
- 2) Latitude
- 3) N or S (North or South)
- 4) Longitude
- 5) E or W (East or West)
- 6) GPS Quality Indicator,
  - 0 - fix not available,
  - 1 - GPS fix,
  - 2 - Differential GPS fix

- TTFF can be measured by time in UTC from epoch 1(hhmmss.ss1; fix not available) to epoch 2(hhmmss.ss2; GPS Fix) in seconds.
- Timing error (ns)
  - Timing receivers provide 1 PPS output.
  - Timing error is computed by comparing the GNSS timing receiver 1 PPS output with the 1 PPS reference/truth signal from the signal source (GNSS simulator).

- This comparison is performed in a timing interval counter which continuously measures the time offset between the two pulses.
- Based on this time offset, stability metrics can be computed for the timing receiver performance. Two stability metrics that are commonly used are the Time Allan Deviation (TDEV) and the Maximum Time Interval Error (MTIE).
- TDEV is computed from  $M$  frequency error measurements  $\delta f_i, i = 1, \dots, M$ , for analysis interval  $\tau$  as:

$$TDEV(\tau) = \frac{\tau}{m^2 \sqrt{6(M-3m+2)}} \sqrt{\sum_{j=1}^{M-3m+2} \left( \sum_{i=j}^{j+m-1} \left( \sum_{k=i}^{i+m-1} (\delta f_{k+m} - \delta f_k) \right) \right)^2}$$

where the integer  $m$  denotes the number of measurements corresponding to the averaging time  $\tau$  [RD.1].

- Alternatively, TDEV can be evaluated using  $(M+1)$  time offset measurements  $\Delta t_i$  as:

$$TDEV(\tau) = \frac{1}{m \sqrt{6(M-3m+2)}} \sum_{j=1}^{M-3m+2} \left( \sum_{i=j}^{j+m-1} (\Delta t_{i+2m} - 2\Delta t_{i+m} + \Delta t_i) \right)^2.$$

- MTIE refers to the largest variation of the time offset within one analysis period of length  $\tau$ , expressed mathematically as:

$$MTIE(\tau) = \max_k \left( \max_{(k-1)m+1 \leq i \leq km} \Delta t_i - \min_{(k-1)m+1 \leq i \leq km} \Delta t_i \right).$$

- For normal operational environment, timing error should be within 30 ns according to Galileo system specifications.
- Hold-over mode is a situation when the receiver is unable to produce a valid timing solution due to unavailability of GNSS signals (due to signal outage or interference). In this situation, the receiver output is driven by its internal clock, whose drift is not anymore compensated by GNSS time solution.
- Hold-over time is the amount of time it takes for the receiver to cross the maximum timing error threshold when the receiver is in hold-over mode.

This can be a very useful parameter even though it is not a performance metric of timing receivers.

### 3.3 Selected Metrics

It is recommended that the complete set of metrics is obtained and recorded for each test (with the exception of timing error for non-timing receiver). This allows maximum visibility of the performance achieved by the receiver during the testing.

**Table 3-1: Performance Metrics**

Metric	Description	Measure / Output / Derived	Normal	Receiver type	Test Type
<b>J/S</b>	Jammer to Signal Ratio	M	0dB	All	All
<b>Timing Error</b>	Error in e.g. 1PPS or IRIG-B signal measured with scope or counter	M	10~20ns	Timing Receiver	All
<b>C/No</b>	Carrier to noise density	O	~55dB-Hz	All	All
<b>Accuracy</b>	Accuracy of the position determined by processing GNSS signals.	O	H: 3 – 5m V: 7.5 – 12m	All	All
<b>Number of Visible SVs</b>	Number of available signals from visible SVs.	O	12	All	All
<b>Number of SVs in use</b>	Number of SV signals that are processed by receiver to produce a position.	O	4 – 12*	All	All
<b>TTFF (Reacquisition only)</b>	Time to first fix receiver position during reacquisition.	O	1 sec (or as stated in receiver specification)	All	All
<b>Timing Error</b>	As measured by receiver	O	10~20ns	Timing Receiver	Timing
<b>Tracking Sensitivity</b>	Signal tracking capability in weak or noisy signal environment.	D		All	All
<b>Reacquisition Sensitivity</b>	Signal reacquisition capability in weak or noisy signal environment.	D		All	All

\*4 Satellites are needed for a GPS fix.



## 4 Test Methodology

### 4.1 Test Methodology Overview

Figure 4-1 shows an overview of the test methodology including the test methods, their variants and the key parameters that describe these test methods.

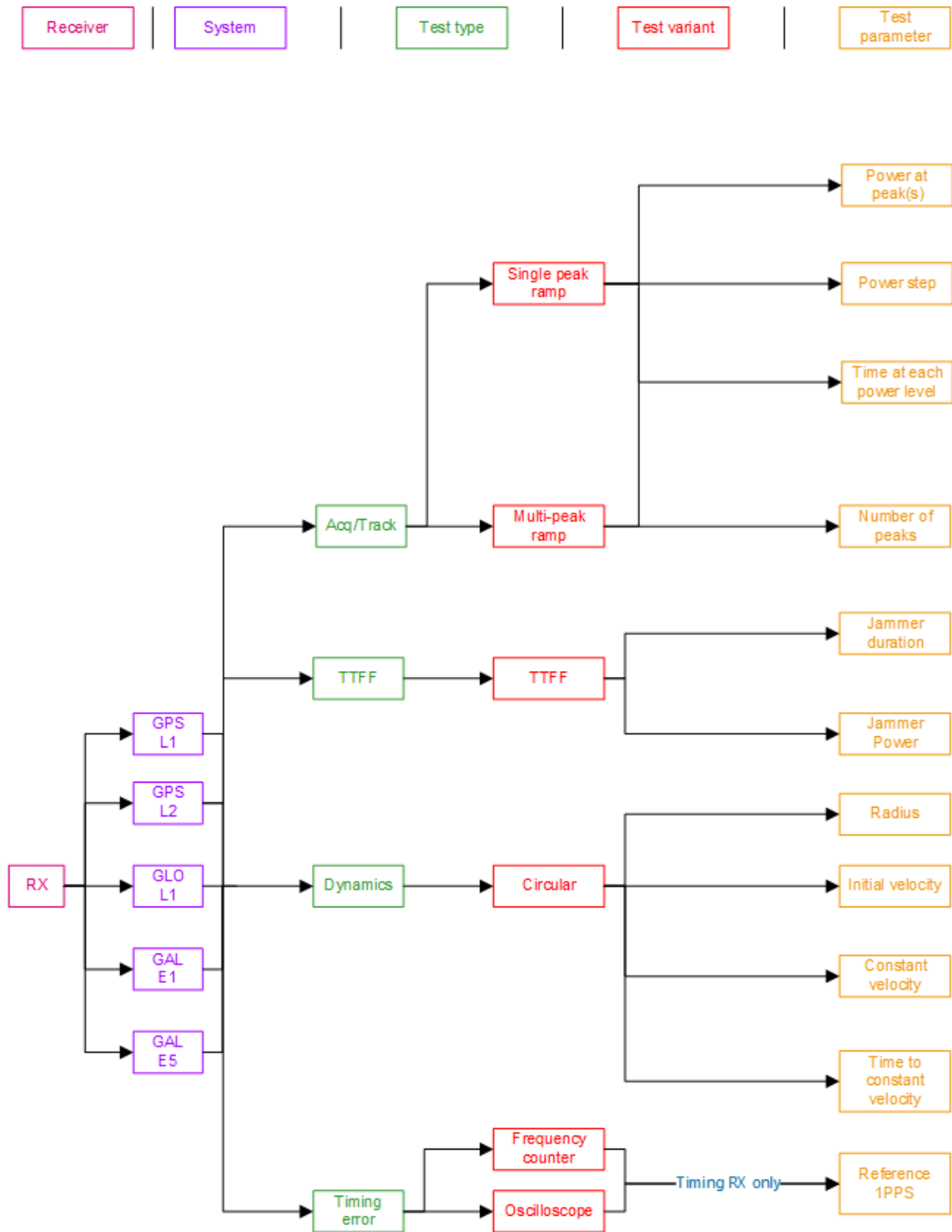
Note that the receiver type does not usually affect the test methodology, so is omitted from the diagram and subsequent descriptions. The exception to this is timing receivers where a specific test method is described in section 4.6.

#### 4.1.1 Test Parameters

The following parameters need consideration and configuration before carrying out testing:

- Receiver type
- Number of visible SVs: 12, number of used SVs: more than 8, and C/N0s are larger than 40 dB-Hz for prerequisite condition for normal operation without interference.
- Constellations and frequencies
- Max Incident power level (consideration of LNA, AGC, ADC)
- Interference type(s)
- Interference (I/Q data for synthetic signal or real signal)
- Parameters specific to the test methods: e.g. TTFF, Dynamic and Static tests
- Receiver parameters (via script – user/application specific)
- Receiver parameters (via script – required metrics)

Figure 4-1 Test Methodology Overview



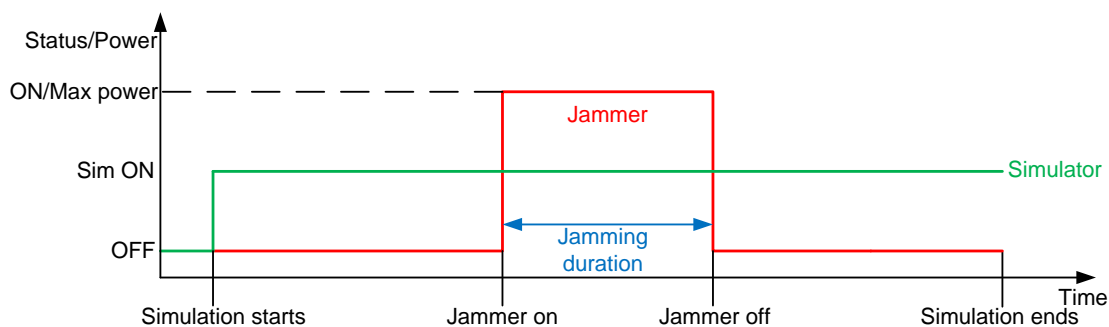
## 4.2 TTFF Test Method

This test is used to measure the time taken for a receiver to recover immediately after a strong interference event. By utilising this time measurement and the time taken to acquire and position fix in nominal conditions, the behaviour of the receiver immediately after interference can be assessed.

Follow the steps below to perform this test:

1. Setup the receiver under test and the required equipment according to the receiver type by following the appropriate test setup description from **Section 2: Test Architecture**.
2. Prepare to record the appropriate set of metrics from the receiver (see section 3) for the duration of the test.
3. Refer to Figure 4-2 for a definition of the parameters required for this test method and their recommended values. Baseline values for the parameters such as the Jamming duration, and maximum jamming power level are defined in Table 4-1
4. Record the simulation start time
5. With a GNSS simulator switched on and no interference source, run the simulation for the defined time period and record the time taken until the receiver has its first position fix from starting the simulation.
6. At the defined jammer start time, start the interference source at the defined maximum power level.
7. Switch the interference source off at the end of the selected jamming duration.
8. Keeping the GNSS simulator on, record the time it took the receiver to reach a position fix after switching off the interference source.

The profile of this test is illustrated in Figure 4-2 .



**Figure 4-2 : TTFF Test Profile**

As shown in Figure 4-2, the receiver under test establishes a position solution from a GNSS simulator and the TTFF is recorded. The interference source is then turned on at a sufficient power level such that the receiver loses position solution and that interference is applied for a time defined as the jamming duration. After that duration, the interference source is switched off and the simulator continues to operate until the receiver has its first fix. The time taken between switching off the interference source and the first fix is recorded as the TTFF after interference and is compared with the TTFF in nominal conditions.

Parameter	Description	Format / Unit	Value
<b>Simulation Start</b>	The start time of simulation	Hh:mm:ss	00:00:00
<b>Simulation End</b>	The end time of the simulation	Hh:mm:ss	00:30:00
<b>Jammer on</b>	The start time of interference	Hh:mm:ss	00:14:00
<b>Jammer off</b>	The end time of interference	Hh:mm:ss	00:15:30
<b>Jamming duration</b>	The duration of the interference	Seconds (s)	90 sec as default
<b>Jammer Max Power</b>	The Maximum power of the jammer	dB	90 in J/S As default

**Table 4-1: TTFF Test Parameters**

### ***4.3 Acquisition and tracking sensitivity test method***

This test is conducted by keeping the simulated location of the receiver static and varying the power of the interference test signal. There are two reasons why this is desirable:

- a) Assess how the receiver reacts to interference power levels of different magnitudes from noise level through to saturation. This allows us to measure the point at which the receiver under test fails to track enough satellites to produce a position (tracking sensitivity) and the point at which the receiver under test starts to track enough satellites to produce a position (acquisition sensitivity). It also allows study

- of any undesirable behaviour under these conditions e.g. the generation of erroneous data.
- b) Emulate in a simple way how the receiver under test reacts to a moving interference test signal with respect to a stationary/ receiver (or vice versa).

Figure 4-3 and Figure 4-4 show a recommended power profile and the key parameters that define it highlighted in red for single peak and multi-peak scenarios. These parameters should be programmed into the interference generator. The table below describes the main parameters of the suggested power profiles

**Table 4-2: Parameters of Interference Power Profile**

Parameter	Description	Format/Unit	Value	Comments
<b>Start time</b>	The starting time of interference	hh:mm:ss hh – two-digit hour mm – two digit minutes ss – two digit seconds	00:03:00	Allow the RUT to form a stable position fix before starting the interference
<b>Start Power</b>	The absolute power level to start from	dBm	-120	
<b>Number of power peaks</b>	The number of power peaks in the profile	Signed Integer	1-5	1 if single peak > 1 multi-peak
<b>Total Number of power points</b>	The total number of power points in the simulation	Signed Integer	13 [up] + 13 [down]	Range of interference power = -120 dBm to -60 dBm with 5 dB steps
<b>Power step [up] to peak [#N]</b>	The step in power between each power point	dB	5	[up] defines direction of sweep [#N] only applicable if multi-peak
<b>Duration per power step [up] to peak</b>	Duration between power steps seconds	Seconds	30 seconds	

D4.2: Draft standards for receiver testing against threats

Ref: STRIKE3\_D42\_TestStandards

Issue: 2.0

Date: 27.11.17

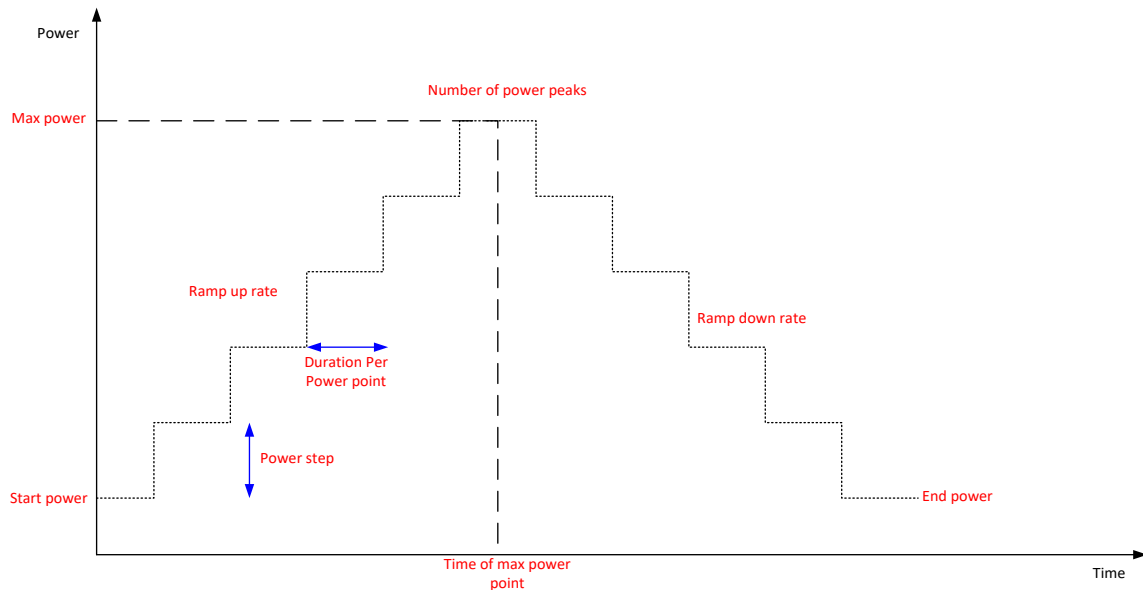
Parameter	Description	Format/Unit	Value	Comments
<b>[#N]</b>				
<b>Time of peak #N</b>	The time of the peak number N	hh:mm:ss (see parameter 1)	Peak 1 at 00:09:30. Peak N (N>1) at (00:09:30 + 00:13:00 * (N-1))	First peak at 9.5 minutes. Every next peak after 13 minutes interval.
<b>Power level at peak #N</b>	The power level in of the peak N	dBm	-60	
<b>Power step [down] from peak [#N]</b>	The step in power going down from peak N	dB	5	Applicable only if the power step down is different from step up
<b>Duration per power step [down] from peak [#N]</b>	The duration between power steps going down from peak N	Seconds	30 seconds	Applicable only if the duration per power step down is different from step up
<b>End power</b>	The simulation end power	dBm	-120	
<b>End time</b>	The simulation end time	hh:mm:ss (see parameter 1)	(00:16:00 + 00:13:00 * (N-1))	Depending on the number of peaks. Every peak is 13 minutes long + 3 minutes at the beginning.

When power of jamming signal is increased, values of C/N0s for SVs are gradually decreased and number of used SVs is decreased at the same time. When number of used SVs turns to 3, then 3D Fix turns to 2D Fix. If its value turns 2, then it gives No Fix.

If we do the similar steps reversely, number of use SVs turns 1(one) then it means signal acquisition. Its value reaches up 3 and gives 2D Fix, 4 and 3D Fix and then most of C/N0 values reaches up to more than 40 dB-Hz when Jamming signal goes down to zero.

### 4.3.1 Single Peak Ramp Profile

To assess the baseline performance of a receiver in terms of acquisition and tracking sensitivity, it is recommended that a power profile shown in Figure 4-3 is incorporated in the suite of tests.



**Figure 4-3: Interference Single Peak Ramp Profile**

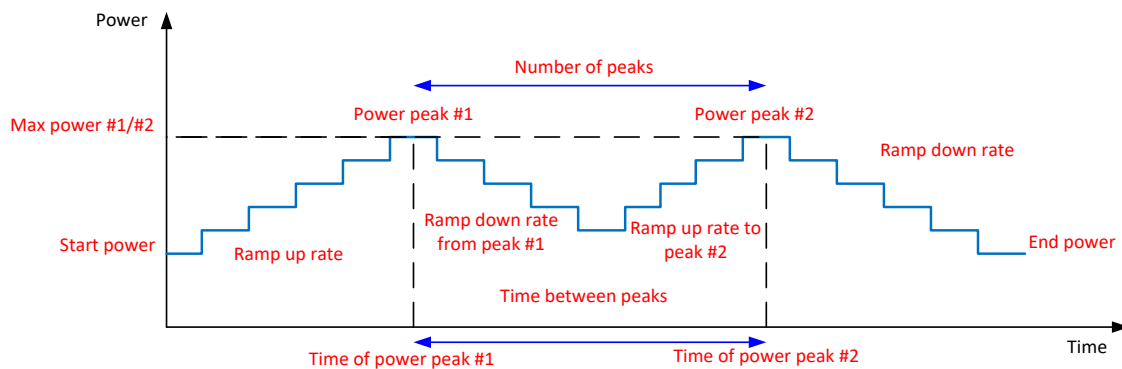
Follow the steps below to perform this test:

1. Setup the receiver under test and the required equipment according to the receiver type by following the appropriate test setup description from **Section 2: Test Architecture**
2. Refer to figure Figure 4-3 for a definition of the parameters required for this test method and to Table 4-2 for the recommended values that should be chosen.
3. Prepare to record the appropriate set of metrics from the receiver (see section 3) for the duration of the test.
4. Record the simulation start time
5. With a GNSS simulator switched on and no interference source, run the simulation until the receiver has its first position fix, record the time taken to reach the first fix from starting the simulation.
6. Run the interference source for the defined duration per power level, increasing the power level by the defined power step each time

7. Record the power level (in dBm) at which the receiver cannot produce a position fix and continue increasing the power level until you reach the defined maximum power level defined to confirm total loss of position
8. Reduce the power level gradually by defined power step with the defined power level duration interval and observe when the receiver starts to reacquire, track and produce its initial position solution, record the power level (in dBm) when each of those events occur

### 4.3.2 Multi-Peak Ramp Profile

To assess the performance of a receiver to rapidly recurring power peaks in the incident interference signal, it is recommended that a power profile shown in Figure 4-4 is incorporated in the suite of tests.



**Figure 4-4:** Example of a multi-peak power profile

Follow the steps below to perform this test:

1. Setup the receiver under test and the required equipment according to the receiver type by following the appropriate test setup description from **Section 2: Test Architecture**
2. Refer to figure Figure 4-4 for a definition of the parameters required for this test method and to Table 4-2 for the recommended values that should be chosen.
3. Prepare to record the appropriate set of metrics from the receiver (see section 3) for the duration of the test.
4. Record the simulation start time
5. With a GNSS simulator switched on and no interference source, run the simulation until the receiver has its first position fix, record the time taken to each the first fix from starting the simulation.
6. Start the interference source at your chosen starting power



7. Increase the power level by the defined power step taking into account a the defined dwell duration per power step
8. Record when the receiver loses its position fix and continue increasing the power until reaching the first power peak to confirm the complete loss of position fix
9. Reduce the power level from the first power peak until the receiver reacquires, tracks and regains its position fix, record the power levels( in dBm) when each such event occur
10. Repeat steps 7 to 9 with the subsequent power peaks taking into account the different ramp up or ramp down rates and record any differences in the power level at which the receiver starts to lose position fix and the power level at which the receiver reacquires.

#### **4.4 Receiver Dynamics Test Method**

This test is used to assess impact of interference on a moving receiver. In this test, a RF GNSS constellation simulator generates the GNSS signal together with simulated receiver motion. A circular or similar motion is highly dynamic as the receiver is constantly changing direction.

Note that the combination of receiver motion and change in interference power level is not designed to simulate a specific use case – the vehicle motion in the simulation is introduced simply to assess the behaviour of the position engine within the receiver in cases where interference is introduced.

The receiver motion configuration is described in the table below.

**Table 4-3: Key Parameters for Receiver Dynamics**

<b>Parameter</b>	<b>Description</b>	<b>Format / Unit</b>	<b>Value</b>
<b>Radius</b>	The radius of the motion (if circular)	Meters (m)	100
<b>Initial velocity</b>	The initial speed of the vehicle	rad/s	0
<b>Constant Velocity</b>	The eventual constant velocity of the vehicle around the track (if circular)	rad/s	0.1
<b>Time to reach Constant Velocity</b>	Time between start and reaching Constant Velocity, defines acceleration of vehicle	Seconds(s)	60

The interference test itself takes the form of the multi-peak tracking/acquisition test, with the only difference that the receiver is simulated to be in motion rather than static.

Follow the steps below to perform this test

1. Setup the receiver under test and the required equipment according to the receiver type by following the appropriate test setup description from **Section 2: Test Architecture**
2. Refer to figure Figure 4-4 for a definition of the parameters required for this test method and the recommended values that could be chosen. Decide on the values for the parameters such as the starting power level of jamming, duration per power level, power step and number of power peak.
3. Set the constellation simulator generation script to include the dynamic receiver motion described in the table above
4. Prepare to record the appropriate set of metrics from the receiver (see section 3) for the duration of the test.
5. Record the simulation start time
6. With a GNSS simulator switched on and no interference source, run the simulation until the receiver has its first position fix, record the time taken to reach the first fix from starting the simulation.
7. Start the interference source at your chosen starting power
8. Increase the power level by the defined power step taking into account the defined dwell duration per power step
9. Record when the receiver loses its position fix and continue increasing the power until reaching the first power peak to confirm the complete loss of position fix
10. Reduce the power level from the first power peak until the receiver reacquires, tracks and regains its position fix, record the power levels (in dBm) when each such event occur
11. Repeat steps 7 to 9 with the subsequent power peaks taking into account the different ramp up or ramp down rates and record any differences in the power level at which the receiver starts to lose position fix and the power level at which the receiver reacquires.

## 4.5

### 4.5 *Timing Error test method*

To do the receiver validation tests for timing errors and the effect of external threats on the general behavior of timing receivers, the following series of steps are performed. Please

note that point number 7 (introduction of threat scenarios) can be performed in accordance to the series of steps given in .

1. A GNSS signal simulator is used as a source of the test signal. The RF GNSS signals are provided to the timing receiver under test (RUT). The simulator also provides a 1 PPS signal as a second output.
2. The timing receiver under test processes the GNSS RF input from the simulator and provides a 1PSS output. This is obtained by maintaining a fixed position within the receiver and computing only the time component of the overall PVT solution.
3. The 1 PPS signals from the simulator is the truth/reference while the 1 PPS signal from the timing receiver under test is the output which has to be validated.
4. These two 1 PPS signals are compared in a timing interval counter, which measures very accurately the time difference (also called time offset) between the corresponding 1 PPS signals.
5. A high-quality stable time source such as a professional grade GNSS receiver or an oven controlled oscillator is used as a 10 MHz frequency reference to synchronize the three components of the validation platform – simulator, RUT, and interval counter.
6. The result of the timing test is the magnitude and temporal variation of this time offset. With external computations, the stability metric such as Maximum Time Interval Error (MTIE) and Time Deviation (TDEV) can be computed for this time offset.
7. The same validation test can be run under different threat scenarios to record the effect of interferences on the timing receiver under test.

## 5 Criteria and Procedure for Selecting Threats

### 5.1 Overview of Proposed Approach

Existing receiver test standards that consider interference tend to use definitions of various types of synthetic signal to check receiver behaviour and impact of such threats. The advantage of such an approach is that different receivers can be tested in a standardised way against particular threat vectors to assess their resilience. However, such definitions suffer from the fact that they may not be directly linked to real threats that occur in the operational RF environment, and the definition of the threats is static and cannot reflect the evolving nature of threats and interference. The purpose of the threat monitoring and selection in STRIKE3 is to identify real signals that pose a genuine threat to GNSS receivers and to quantify the impact of such threats on receivers. By using real threats that have been detected in the field this enables interested parties (e.g. certification bodies, application developers, receiver manufacturers, etc.) to better assess the risk to GNSS performance during operations, and to develop appropriate counter-measures.

In addition, by continuously monitoring for threats in the field this enables the evolution of GNSS threats to be monitored to see if new threats evolve and need to be countered. This is analogous to the monitoring for threats and development of anti-virus technology in the software domain.

The purpose of the STRIKE3 test standards therefore is not to propose a fixed set of threats to covering all the types of signal in existing test standards, but instead to develop draft standards for testing receivers against threats that have been detected in the field, and for proposing an approach for choosing how to assess and select new threats in the future (out of the many examples that will be detected).

### 5.2 Procedure for Threat Selection

#### 5.2.1 Introduction to Threat Selection

The intention within the STRIKE3 project is to define a baseline set of threats for receiver testing, and to propose a method for selecting and new threats that could be added to the test standards. The baseline set of threats and selection approach for new threats will be an outcome at the end of the STRIKE3 project.

In working towards that goal, STRIKE3 must identify candidate threats and assess them in order to define a reference set of threats. this section describes the process that has been followed to identify and select the baseline set of threats for testing, and describes the baseline threats.

#### 5.2.2 Process for Initial Threat Selection

With many thousands of potential threats being detected by a monitoring network, it is impractical to test receivers against all detected threats. Therefore an initial threat

selection process is proposed to identify a baseline set of threats that are worthy of further consideration.

The different steps taken to perform this initial threat selection are described below.

### **5.2.2.1 Initial Filtering Based on Power Level**

With so many events in the database it is impossible to analyse them all in detail. Therefore, as an initial step, the chirp events from each site are filtered so that only those that have received power above a medium power level are considered. This has the effect of reducing the numbers of events to analyse to a more manageable level. It also has the following additional advantages:

- The classification of event type has higher confidence for higher power signals, and so there is less chance that the signals that meet the power level criteria have been mis-classified as chirp;
- For signals with higher power levels, the characteristics of the signal structure (such as frequency range, frequency rate of change, chirp repeat rate, etc.) are more clearly identifiable in the data.

The remaining events that have passed the initial power level filter are then analysed in more detail.

### **5.2.2.2 Identification of Different Chirp Signal Types**

In the next step, the chirp events that have passed the initial power level filter are analysed for each site independently. Each event is analysed in terms of its interference signal structure in order to group events that have similar chirp signals. Various broad groupings for chirp signals are defined and each event is then allocated to the particular type which is the best fit. Once all chirp events at a site are grouped according to similar signals, it is then possible for each site to see which types of chirp signal are most common. An overview of the broad types of chirp signal used for this analysis is provided in Annex A.

### **5.2.2.3 Selection Based on Common Signal Types**

Once the chirp signals at each monitoring site have been grouped, further analysis is performed to identify the most common signal types. Choosing the most common signals is felt to be an effective way to cover the biggest threat to receivers, as the most common signals are those most likely to be encountered by a receiver in the field.

This analysis is performed in two parts: firstly, the chirp signal types are assessed in terms of the total number of events detected to see which are most commonly detected, and secondly the chirp signal types are assessed for how widespread they are, i.e. how many different sites detect the same type of signal. From both parts of this analysis, the top signals (in terms of number of events and number of sites) are selected as the most common signals that pose the widest threat to receivers in the field. Some figures from the initial analysis are provided in Annex A.

### 5.2.2.4 Selection of Evolving Signal Types

As well as picking just the most common types of signal, some consideration is given to evolving threats. These are threats that may not necessarily be the most common but can be seen to be becoming more common over time. This may be seen either through increasing numbers of events / numbers of sites over time, or a sudden appearance at one or more sites in significant numbers.

### 5.2.3 Description of Baseline Set of Threats

After following the steps described above for the Detector event database in STRIKE3, a baseline set of 5 types of chirp threats have been selected for inclusion in the draft test standard for receiver testing. These are described below

Type of signal	Example Plots	Reason for choice
Wide Sweep – fast repeat rate		Very common (total number of events, and number of sites)
Wide sweep – medium repeat rate		Very common (total number of events, and number of sites)
Triangular		Common (number of sites)

Type of signal	Example Plots	Reason for choice
Triangular wave		Common (number of sites)
Tick		Quite common. Evolving threat (new type).

**Table 5-1: Descriptions of Baseline Set of Selected Threats**

### 5.2.4 Receiver Testing and Impact Considerations

The set of threats selected for testing have been chosen based on how widespread they are in the real-world, as this defines the likelihood that a receiver will be exposed to that threat. However, this analysis does not say anything about the impact each threat will have on a receiver in terms of GPS tracking performance. Therefore in order to establish a final set of threats for a test standard, and to identify new threats that should be added to the standard, candidate threats that have been selected from the database will be used in receiver testing to assess the impact. This will help to inform the choice of which threats should form part of the test standard, and also to help identify any new threats that should be added to the reference set of threats at a later date.

The testing of receivers against the selected threats has two main purposes:

1. To assess the impact of the selected threats on receiver performance (different types of receiver and different manufacturers) in order to identify those threats that are important to consider for test standards.
2. To assess impact of different signals in order to determine if there is any correlation between impact and particular signal characteristics.

The first of these is important to establish a baseline set of threats. The choice of which threats to consider may be based on several factors, e.g. signals that have a significant impact on all receivers under test, or signals that have the biggest range of impacts on different types of receiver, etc.

The second of these is important to help refine the threat selection criteria to be used in the future for identifying new threats to be added to the standards. If there is a clear correlation between signal characteristics (other than power level) and receiver impact then this can be used in the future to help optimise the threat selection process (described in section 5.2.2) from continuous monitoring of GNSS interference events.

## **5.3 Use of Real Signatures for Threat Testing**

### **5.3.1 Overview**

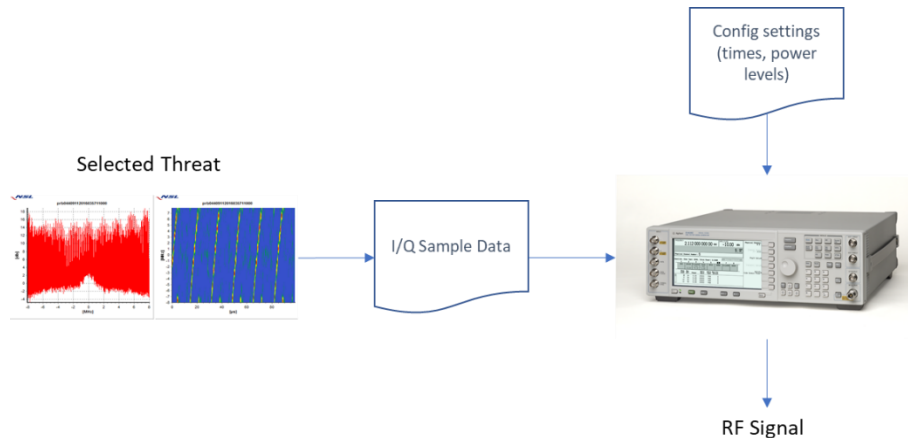
The purpose of using real threats that have been detected in the field is to assess receivers against interference signals they may realistically encounter during operations, rather than checking against some theoretical worst case signal that will have a significant impact on receiver performance but is only generated in a laboratory environment. Nevertheless, it is acknowledged that the detection of a particular interference event – and the characteristics associated with that event (power levels, duration, etc.) – are dependent on the interference detection equipment, thresholds and location relative to the interference source. Therefore, as far as possible, those site/sensor specific aspects should be removed from the process, i.e. it is the interference signal that is being tested and not the characteristics of the event itself. In practical terms this means that:

- It shall be possible to replay a signal with the characteristics of that detected in the field (in terms of centre frequency, frequency variation, pulse repeat rate, etc.);
- It shall be possible to modify the power level of the interference signal, i.e. to replay the test threat signal at lower or higher power than what was detected in the field;
- It shall be possible to modify the duration of the interference signal, i.e. to replay the test threat signal with short or longer event duration than what was detected in the field;
- It shall be possible to replay only the interference test signal, i.e. to ignore the status of the GNSS signals themselves (e.g. what signals being tracked, at what power level, appearance of multipath or other errors, etc.) at the time of the real event.

In order to fulfil these objectives, two alternative approaches are currently considered – replay of synthetic signal and replay of raw sample data. It is noted that these alternative approaches are currently both under consideration within the STRIKE3 project and will be compared during testing within the project with a view to proposing a recommended approach.

Both approaches are similar in that they use a Vector Signal Generator (VSG) to generate the interference for testing. Using a VSG has advantages for testing in that the type of signal and the interference event characteristics (e.g. power level, duration) can be well controlled through the VSG, and a repeatable signal can be generated for adding to the GNSS signals (through a signal combiner). This is illustrated in the following figure.





**Figure 5-1: Overview of Interference Signal Generation for Testing**

The baseline format of the I/Q data is as follows:

- Format: "Double"
- Sample: Complex, I and Q interleaved (In a data file you will have: I(n), Q(n), I(n+1), Q(n+1),...)
- Sampling frequency: 16MSps
- Duration of the time series samples: 200ms

The difference between the two approaches is in how the I/Q data is created.

### 5.3.2 Use of Synthetic I/Q Data

The first option for using real threats for testing is the generation of synthetic data to represent the real threat. In this approach, a synthetic I/Q data sample is generated to represent the real signal. This is done through manually creating a signal in a VSG with properties that are representative of the real signal. The I/Q data that goes with this synthetic signal is then used to generate interference signals for testing.

The advantage of this approach is that the generated signal is 'clean' and hence free of multipath and GNSS PRN codes that could otherwise cause problems when adding the interference signal to GNSS RF data generated by a constellation simulator.

However, this approach has limitations when the original signal is complex and difficult to re-create synthetically as the resultant interference signal may not accurately reflect the real signal, and hence the impact on receiver performance may be different.

### 5.3.3 Replay of Raw Sample Data

An alternative approach to generating a synthetic signal is to replay the raw sample data

itself through a VSG as a re-creation of the detected threat.

The advantage of this approach is that for more complex threat signals this could potentially provide a more accurate reconstruction of the detected threat. However, in order to replay the raw data and meet the requirements for the test there are a number of factors to consider.

Firstly, the raw sample data must be captured with appropriate characteristics or else the replay will not give an accurate representation of the interference signal.

Secondly, the sample capture will only be for a short duration and so the sample must be repeated to enable it to replay for a longer duration.

Thirdly, the raw sample data will contain the satellite information (PRN codes) as well as the information about the interference signal and so these must be filtered out before replaying the signal so as to not contaminate the interference signal with the GNSS satellite information.

Therefore some pre-processing of the raw signal is necessary before it can be used for replay.

## **5.4 Future Considerations**

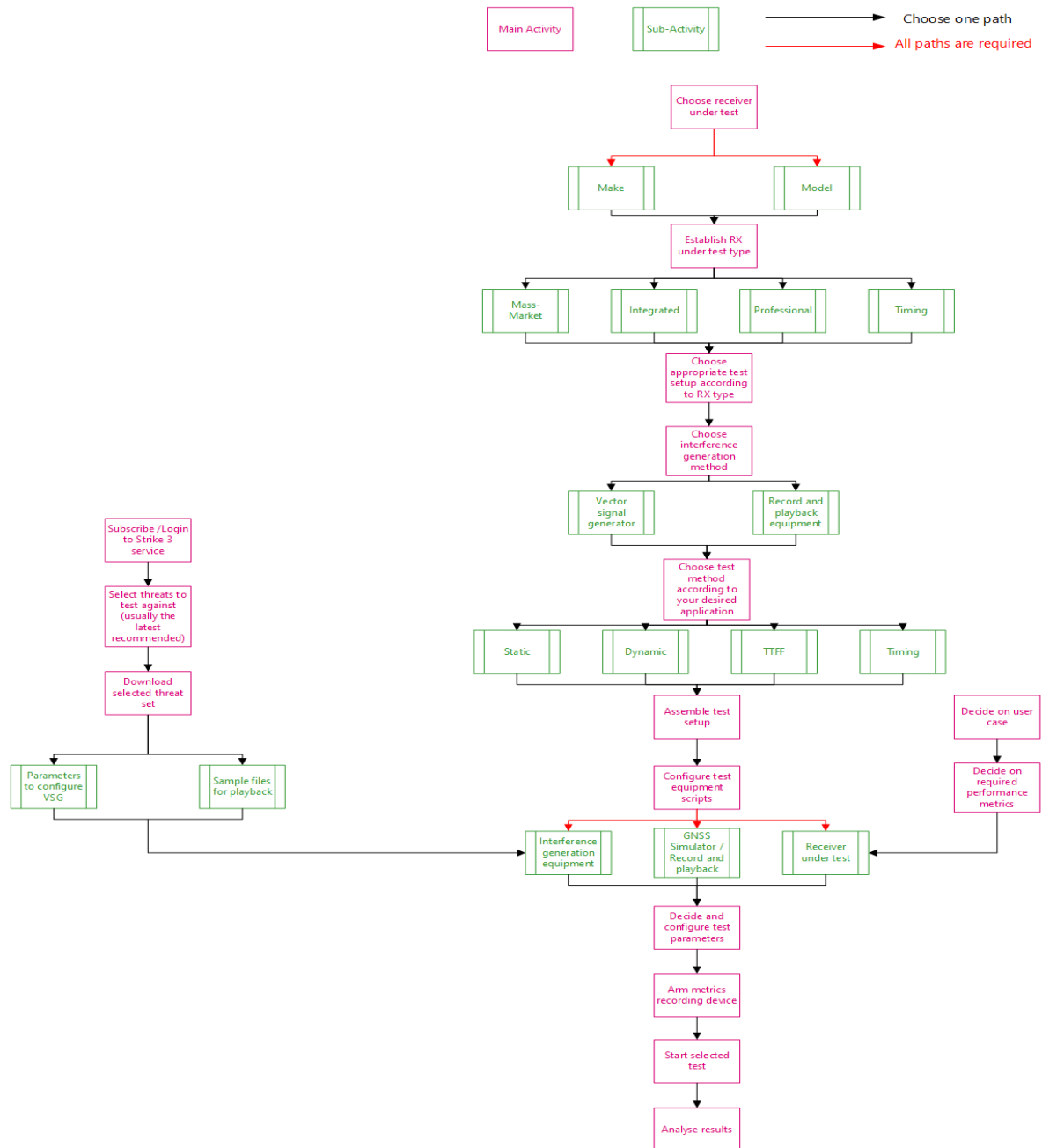
The objective of the STRIKE3 project is to define a baseline set of threats – based on real signals detected in the field - for receiver testing, and to propose a method for identifying and selecting new threats to add to the test standard. In addition, a recommended method for using real threats in receiver testing (playback of representative synthetic signal or raw sample playback) will be proposed. The alternative approaches for using real threats in receiver testing (parameterisation and raw sample playback) will be compared in STRIKE3 in order to trade-off the impact at receiver level vs. the practicalities of the approaches – both for the test process itself as well as for the original data capture.

## 6 Application of Proposed Test Standards

This section explains how the test standard should be utilised in the assessment of GNSS receiver performance. A flow diagram (**Figure 6-1 Use of Standard Flow Diagram**) is included to support the explanation.

1. Select the receiver for testing
2. Establish the make and model of the receiver
3. Establish the type of receiver (Mass Market, Professional, Integrated, Timing). This will determine the test architecture (see section 2) and the test parameters /methodology (see section 4)
4. Decide on interference generation method; vector signal generator with I/Q samples from representative synthetic signal or real samples
5. Based upon the needs of your application, select the test to undertake (TTFF, Static, Dynamic, Timing). See section 3.
6. Assemble the test configuration based upon the gathered information above and section 2.
7. Configure the various equipments forming the test setup. This will commonly be in the form of scripts:
  - For receiver under test:
    - i. Configure parameters consistent with the application of the receiver together with parameters specific to the required tests e.g. constellations/frequencies and performance metrics (see section 3)
  - For the GNSS Constellation Simulator
    - i. Configure parameters to carry out a specific test (section 3)
    - ii. Ensure that GNSS power level at the input to the receiver is in accordance with the specific GNSS constellation and frequency under test (see Table 2 1: GNSS Frequencies and Power Levels )
  - For the Interference Generation Equipment
    - i. For the interference signal under test, load samples into playback equipment. Note that each interference signal should be tested in turn.
    - ii. See section 5 for more detail.
8. Configure any Test Parameters specific to the test to be carried out which are not already configured (see Section 4).
9. Arm device for recording metrics
10. Conduct specific test(s)
11. Analyse results and compare against required performance.

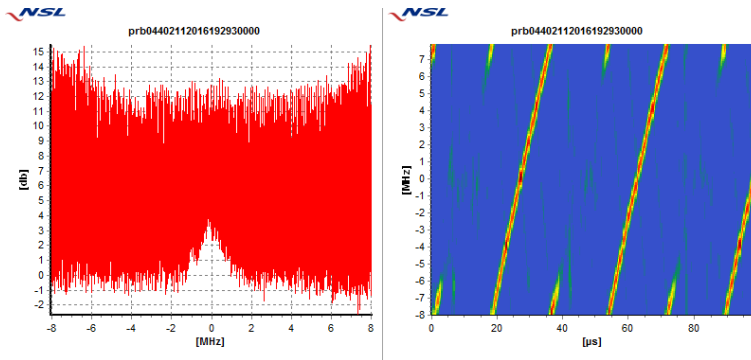
Figure 6-1 Use of Standard Flow Diagram

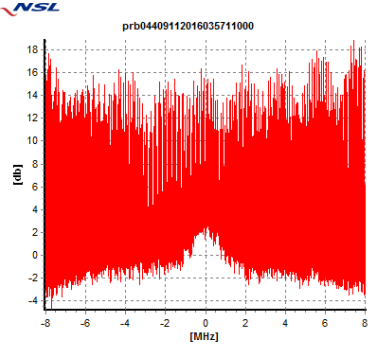
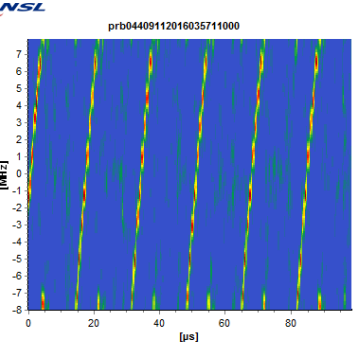
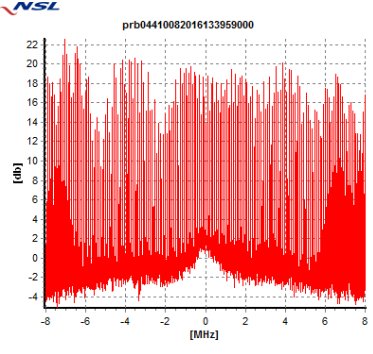
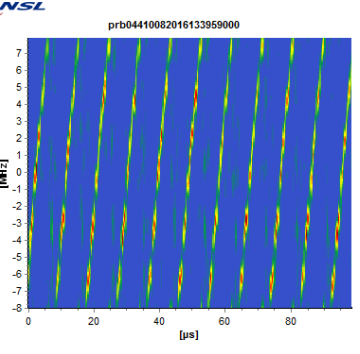


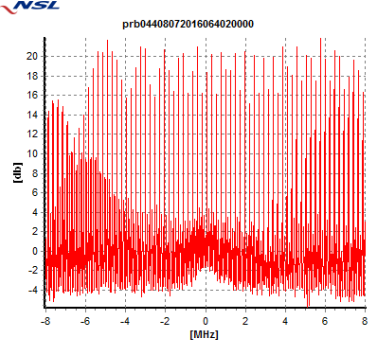
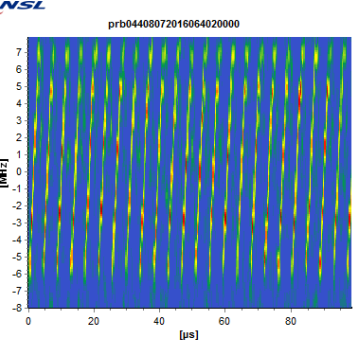
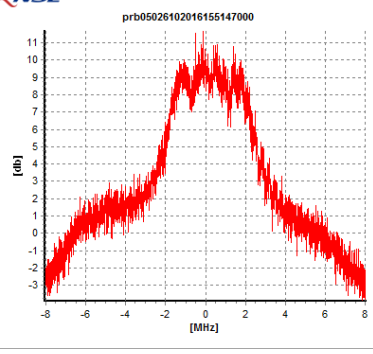
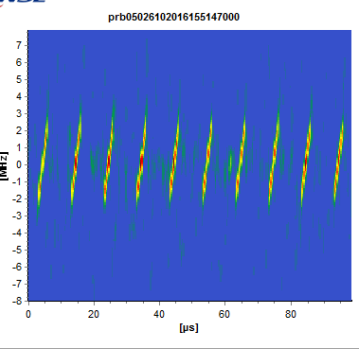
## Annex A: Details on Threat Selection

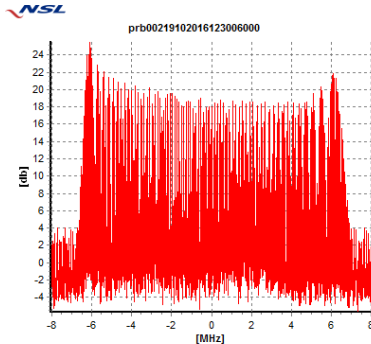
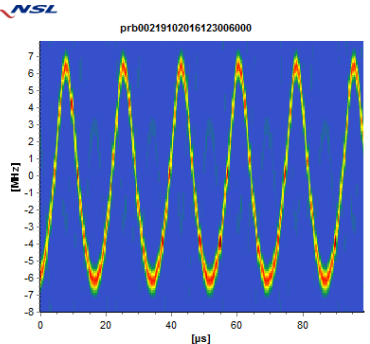
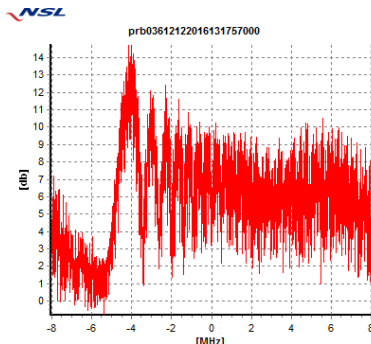
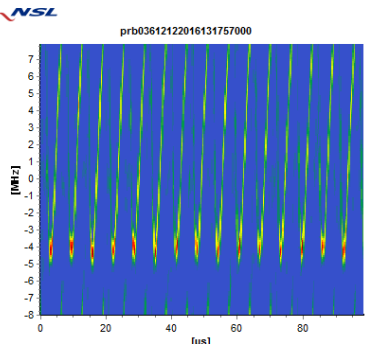
### Definitions

There are many different types of signal that are characterised as ‘chirp’. The following table contains the definitions of the different categories that are used in the analysis of chirp signals for threat selection.

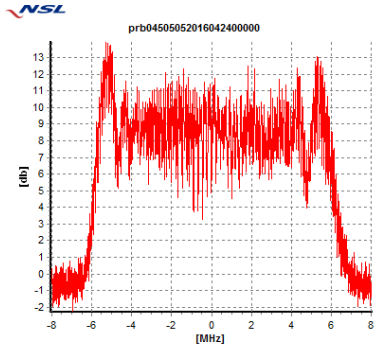
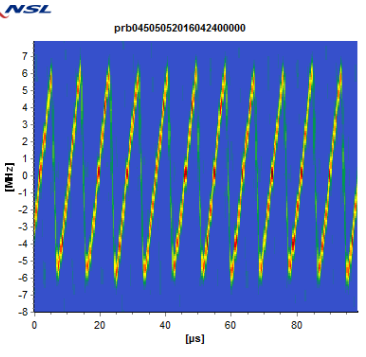
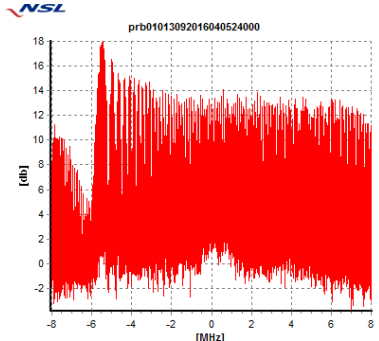
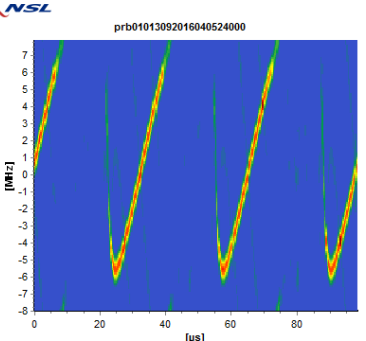
Name	Features	Example
Wide sweep - slow	<p>Spectrum plot</p> <ul style="list-style-type: none"> <li>- show wide variation in power levels at all frequencies</li> <li>- Often see shape of reference spectrum defining bottom edge of power levels</li> </ul> <p>Spectrogram</p> <ul style="list-style-type: none"> <li>- Clearly defined and separated linear (or slightly curved) diagonal lines across wide frequency range</li> <li>- Most commonly show frequency increasing with time</li> <li>- Slow sweeps are characterised as 2 to 3 chirps per 100 <math>\mu</math>s</li> </ul>	 <p>The example section contains two plots. The left plot is a spectrum plot with a red signal, showing power levels in dB on the y-axis (ranging from -2 to 15) and frequency in MHz on the x-axis (ranging from -8 to 8). The signal shows a wide variation in power levels across the frequency range. The right plot is a spectrogram with a blue background and yellow diagonal lines, showing frequency in MHz on the y-axis (ranging from -8 to 7) and time in <math>\mu</math>s on the x-axis (ranging from 0 to 80). The diagonal lines represent chirps, showing frequency increasing with time.</p>

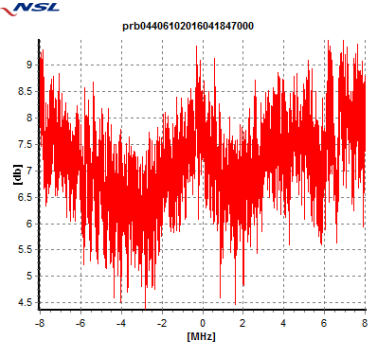
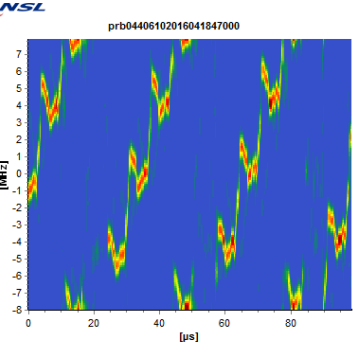
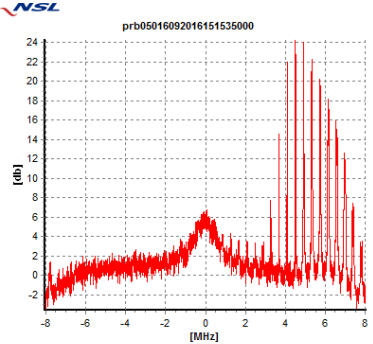
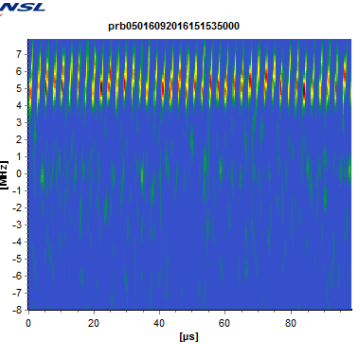
Name	Features	Example	
Wide sweep - medium	<p>Spectrum plot</p> <ul style="list-style-type: none"> <li>- show wide variation in power levels at all frequencies</li> <li>- Often see shape of reference spectrum defining bottom edge of power levels</li> </ul> <p>Spectrogram</p> <ul style="list-style-type: none"> <li>- Clearly defined and separated linear (or slightly curved) diagonal lines across wide frequency range</li> <li>- Most commonly show frequency increasing with time</li> <li>- Medium sweeps are characterised as 4 to 6 chirps per 100 <math>\mu</math>s</li> </ul>	 <p>A spectrum plot showing power levels in dB on the y-axis (ranging from -4 to 18) versus frequency in MHz on the x-axis (ranging from -8 to 8). The plot shows a dense, noisy signal with a clear lower-frequency component that tapers off towards higher frequencies.</p>	 <p>A spectrogram showing frequency in MHz on the y-axis (ranging from -8 to 7) versus time in microseconds on the x-axis (ranging from 0 to 80). The plot displays several distinct, slightly curved diagonal lines (chirps) against a blue background, indicating frequency increasing over time.</p>
Wide sweep - fast	<p>Spectrum plot</p> <ul style="list-style-type: none"> <li>- show wide variation in power levels at all frequencies</li> <li>- Often see shape of reference spectrum defining bottom edge of power levels</li> </ul> <p>Spectrogram</p> <ul style="list-style-type: none"> <li>- Clearly defined and separated linear (or slightly curved) diagonal lines across wide frequency range</li> <li>- Most commonly show frequency increasing with time</li> <li>- Fast sweeps are characterised as 8</li> </ul>	 <p>A spectrum plot showing power levels in dB on the y-axis (ranging from -4 to 22) versus frequency in MHz on the x-axis (ranging from -8 to 8). The plot shows a dense, noisy signal with a clear lower-frequency component that tapers off towards higher frequencies.</p>	 <p>A spectrogram showing frequency in MHz on the y-axis (ranging from -8 to 7) versus time in microseconds on the x-axis (ranging from 0 to 80). The plot displays several distinct, slightly curved diagonal lines (chirps) against a blue background, indicating frequency increasing over time.</p>

Name	Features	Example	
Wide sweep - rapid	<p>to 12 chirps per 100 <math>\mu</math>s</p> <p>Spectrum plot</p> <ul style="list-style-type: none"> <li>- show wide variation in power levels at all frequencies</li> <li>- Often see shape of reference spectrum defining bottom edge of power levels</li> </ul> <p>Spectrogram</p> <ul style="list-style-type: none"> <li>- Clearly defined and separated linear (or slightly curved) diagonal lines across wide frequency range</li> <li>- Most commonly show frequency increasing with time</li> <li>- Fast sweeps are characterised as more than 12 chirps per 100 <math>\mu</math>s (typically we see 16 or more)</li> </ul>	 <p>prb04408072016064020000</p> <p>The spectrum plot shows a dense collection of vertical red lines across a frequency range from -8 MHz to 8 MHz. The power levels vary significantly, with a higher concentration of power between -4 MHz and 0 MHz.</p>	 <p>prb04408072016064020000</p> <p>The spectrogram displays a series of parallel, slightly upward-sloping diagonal lines in yellow and green against a blue background. These lines represent individual chirps occurring over a time interval of 0 to 80 <math>\mu</math>s.</p>
narrow sweep	<p>Spectrum plot</p> <ul style="list-style-type: none"> <li>- show increase in power levels across narrow frequency range</li> </ul> <p>Spectrogram</p> <ul style="list-style-type: none"> <li>- Clearly defined and separated linear (or slightly curved) diagonal lines covering small frequency range</li> <li>- Most commonly show frequency increasing with time</li> </ul>	 <p>prb05026102016155147000</p> <p>The spectrum plot shows a single, broad peak of power centered around 0 MHz, with a range from approximately -8 MHz to 8 MHz. The power is highest in the center and tapers off towards the edges.</p>	 <p>prb05026102016155147000</p> <p>The spectrogram shows several distinct, parallel diagonal lines in yellow and green, indicating narrow sweeps. These lines are spaced out over the 0 to 80 <math>\mu</math>s time interval.</p>

Name	Features	Example	
<p>Triangular wave</p>	<p>Spectrum plot</p> <ul style="list-style-type: none"> <li>- wide range of powers over affected frequency range</li> </ul> <p>Spectrogram</p> <ul style="list-style-type: none"> <li>- Wave pattern showing clear continuous increase and decrease in frequency with time</li> </ul>		
<p>Triangular</p>	<p>Spectrum plot</p> <ul style="list-style-type: none"> <li>- more likely to see raised power over affected frequency range</li> </ul> <p>Spectrogram</p> <ul style="list-style-type: none"> <li>- Clearly see decrease and increase in frequency with time</li> <li>- Gradient and power level of downward and upward slopes are more equal than in sawtooth case</li> </ul>		



Name	Features	Example	
Sawtooth	<p>Spectrum plot</p> <ul style="list-style-type: none"> <li>- Raised power over affected frequency range</li> </ul> <p>Spectrogram</p> <ul style="list-style-type: none"> <li>- Linear sweeps in frequency across wide range</li> <li>- See decrease in frequency with time as well as the increase</li> <li>- Gradient of downward slope is much sharper than main upward slope, and less well defined</li> </ul>	 <p>NSL prb0450505201604240000</p>	 <p>NSL prb0450505201604240000</p>
Hooked sawtooth	<p>Spectrum plot</p> <ul style="list-style-type: none"> <li>- similar to plot for wide sweeps with high variation in power levels across wide frequency range, but usually with a notch of reduced power</li> </ul> <p>Spectrogram</p> <ul style="list-style-type: none"> <li>- similar to wide sweep case, but with additional hook at lower end to make a partial sawtooth effect</li> </ul>	 <p>NSL prb01013092016040524000</p>	 <p>NSL prb01013092016040524000</p>

Name	Features	Example	
Tick	<p>Spectrum plot</p> <ul style="list-style-type: none"> <li>- general increased power across the spectrum</li> </ul> <p>Spectrogram</p> <ul style="list-style-type: none"> <li>- underlying slow wide sweep (2-3 sweeps per 100 <math>\mu</math>s)</li> <li>- Additional structure and variation (taking form of a tick) overlaying the underlying slow sweep</li> </ul>	 <p>NSL prb04406102016041847000</p> <p>[dB] vs [MHz]</p>	 <p>NSL prb04406102016041847000</p> <p>[MHz] vs [<math>\mu</math>s]</p>
Multi tone	<p>Spectrum plot</p> <ul style="list-style-type: none"> <li>- Multiple distinct tones with high power at different frequencies</li> </ul> <p>Spectrogram</p> <ul style="list-style-type: none"> <li>- multiple closely spaced near vertical lines in the region of affected frequency</li> </ul>	 <p>NSL prb05016092016151535000</p> <p>[dB] vs [MHz]</p>	 <p>NSL prb05016092016151535000</p> <p>[MHz] vs [<math>\mu</math>s]</p>

Types of signal that do not easily fall into these categories are marked unusual.

## Chirp Signal Analysis – Number of Events

The first plot shows for each site the number of chirp signals of different types (above the minimum power threshold) that were detected at that site during the monitoring period. The longer the bar, the greater the number of events. Each type of chirp signal is indicated by a different colour.

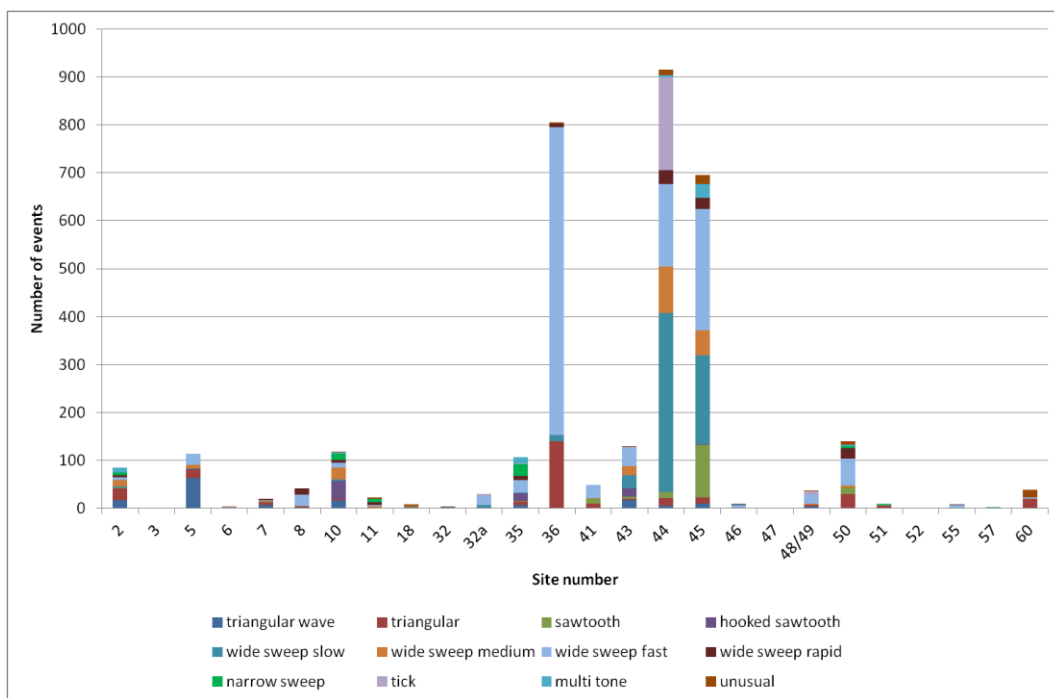


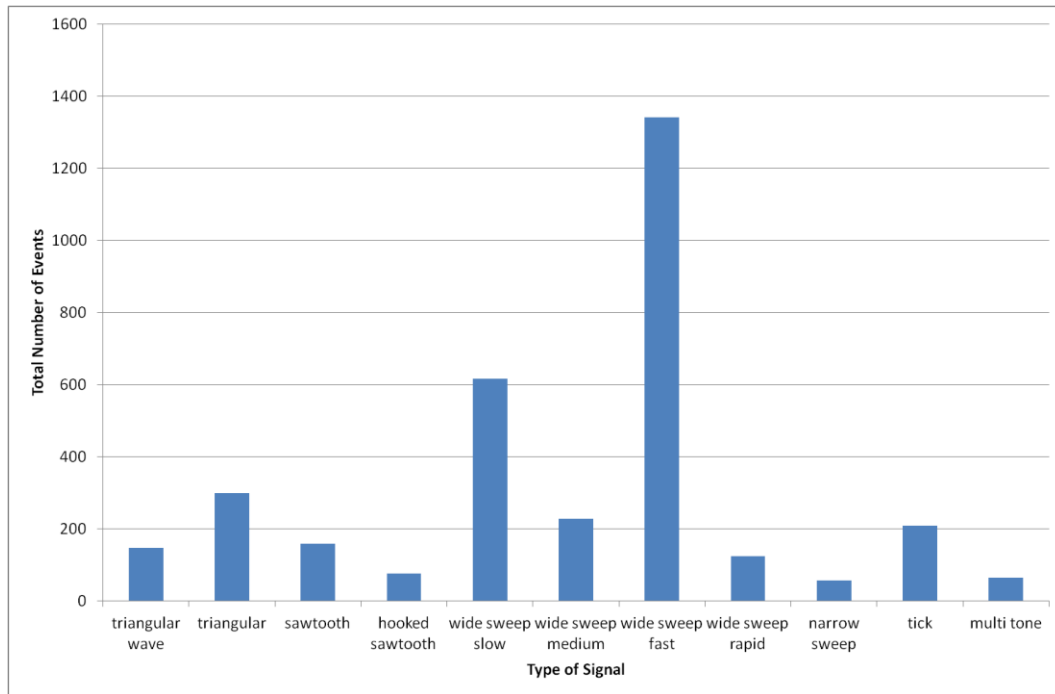
Figure A-1: Number of Chirp Events of each type at Each Site

It can be seen from the results that all of the sites that detect chirp signal see a variety of different types. Also, a lot of the types are common to a lot of different sites. However, it can also be seen that the relative proportions of different types of jammer are quite different for each site. For example, probe36 sees a very large proportion of wide sweep fast events and a lot of triangular, but few others. Probe44 on the other hand sees quite a few different events, but also a much higher proportion of the 'tick' type signals than any other site.

There are several possible reasons for these differences. It could be that different types of jammer are more prevalent in some countries than others. Alternatively it could be that certain sites are affected by just a few jammers that travel past the monitoring site a number of times each day on their way to/from work.

Therefore in identifying which type of chirp signals are most common and offer the

greatest threat we need to consider several things. One option is to look at total number of events from all sites for each jammer category.

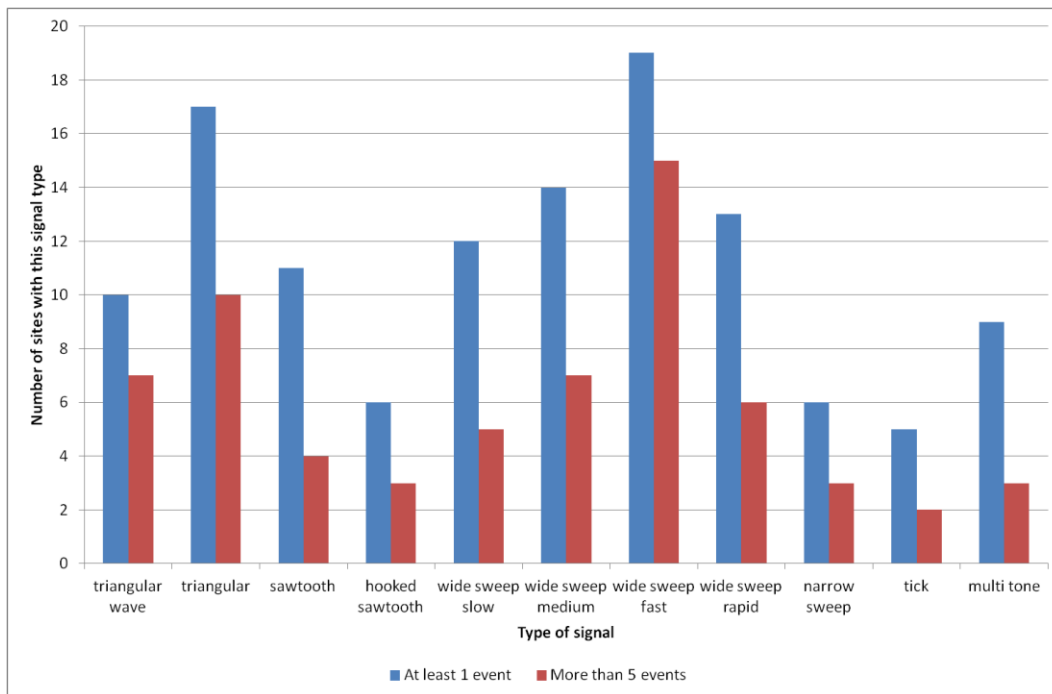


**Figure A-2: Total Number of Events of each type from All Sites**

From this we can see that the most common type of chirp signal is a wide sweep with fast repeat rate (8-12 sweeps per 100  $\mu$ s). The next most common in order are wide sweep with slow repeat rate, triangular, wide sweep with medium repeat rate and 'tick'.

However, this analysis is influenced by the site activity and how long the site has been in place, so may be skewed if certain active sites see a high proportion of a particular type. Therefore this is not the best way to determine how widespread a signal is and how likely it is to be encountered at any site.

An alternative approach is to look at how many sites detect each type of signal as this shows how common it is in a general sense. The following plot shows for each signal type how many sites detected it. Two numbers are shown – the number of sites that detected the signal type at least once, and the number of sites that had at least 5 detections with that signal type. This second one is used in case a single detection at a site was a fluke or misclassification.



**Figure A-3: Number of Sites that Detect Each Type of Event**

This plot shows that the most common type of signal (in terms of the number of sites it is detected at) is the wide sweep with fast repeat rate. This was also the most common type of signal in terms of total number of detections and so this type does indeed appear to be one that is widespread and therefore poses a threat.

The next most common is the triangular type of signal, which was also one of the most common in terms of total numbers. Again therefore this appears to be an important type of signal to consider in testing.

After that there is less agreement between the two different plots. For example, 'tick' type signals were quite common in terms of total number of events but are detected at the fewest sites. In fact almost all the detections of this type were at a single site (probe44) and this has been seen only rarely at other sites. However, it does appear to show an evolution of chirp signals as this type has not been seen in previous studies.

On the other hand the triangular wave type of signal is only the 6<sup>th</sup> most common type of signal in terms of total number of detections, but is seen on more than 5 occasions at 7 different sites, which is the third most common.

Overall therefore it seems that the most typical types of chirp signal – and ones that should therefore form the basis for the threats for testing – are wide sweep (various speeds), triangular and triangular wave. Of the others there may be some benefit in picking ones that look like a new type of threat or may have a significant impact on GNSS performance. Certainly the 'tick' type would fall into this category as it is common at one site, seems more advanced than the swept type, and analysis of events at probe44 shows it has a

## D4.2: Draft standards for receiver testing against threats

**Ref:** STRIKE3\_D42\_TestStandards

**Issue:** 2.0

**Date:** 27.11.17

---

bigger impact on GPS satellite tracking than other types of chirp signal for the same power level.

D4.2: Draft standards for receiver testing against threats

**Ref:** STRIKE3\_D42\_TestStandards

**Issue:** 2.0

**Date:** 27.11.17

---

**END OF DOCUMENT**