

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

**STRIKE3**

**D6.2: THREAT DATABASE ANALYSIS REPORT**

Prepared by:	Oliver Towlson (NSL) David Payne (NSL) Patrik Eliardsson (FOI) Venkatesh Manikundalam (GNSS labs)	25/01/2019
Checked by:	Michael Pattinson (NSL)	25/01/2019
Authorised by:	Mark Dumville (NSL)	25/01/2019

Pages: 95

Document Classification: Public



## Change Record

Issue Rev	Date	§: Change Record	Author(s)
v1.0	25/01/2019	First version delivered to GSA.	Oliver Towlson (NSL) David Payne (NSL) Patrik Eliardsson (FOI) Venkatesh Manikundalam (GNSS labs)

## Table of Contents

List of Tables.....	5
List of Figures .....	6
1 Introduction.....	9
1.1 Purpose of Document .....	9
1.2 STRIKE3 Overview .....	9
1.3 Document Overview.....	9
1.4 References.....	10
1.4.1 Applicable Documents .....	10
1.4.2 Reference Documents .....	10
1.5 Acronyms.....	10
2 Overview of Threat Reporting Validation Process .....	12
2.1 Introduction .....	12
2.2 STRIKE3 Reporting Standards.....	12
2.3 Types of Equipment .....	16
2.3.1 Detector .....	16
2.3.2 RF Oculus.....	20
2.3.3 GNSS Receivers.....	21
2.4 Monitoring Sites .....	21
3 Standardised Monitoring Results .....	29
3.1 Introduction .....	29
3.2 Analysis of Standardised Reports from STRIKE3 Server .....	29
3.2.1 Overview.....	29
3.2.2 Total Events.....	29
3.2.3 Site Analysis .....	36
3.3 Assessment of Standard Event Definitions and Thresholds .....	41
3.3.1 Event type 'a' .....	41
3.3.2 Event Type 'b' .....	50
3.3.3 Multiple Events.....	56
3.3.4 Other Considerations .....	57
4 Detailed Database Analysis .....	58
4.1 Introduction .....	58

## D6.2: Threat Database Analysis Report

**Ref:** STRIKE3\_D62\_DatabaseRep

**Issue:** 1.0

**Date:** 25.01.19

---

4.2	Long-Term Validation Period (01/12/17 to 31/10/18) .....	58
4.2.1	Overview of Activity in Long-Term Monitoring Period .....	58
4.2.2	Comparison of Site Activity in Long-Term Monitoring Period.....	60
4.3	Analysis of Entire STRIKE3 Project Duration .....	68
4.3.1	Overall Activity in Entire Project Duration .....	68
4.3.2	Comparison of Site Activity during Entire Project Duration .....	70
4.4	Types of Signal .....	76
4.4.1	Period 1 .....	81
4.4.2	Period 2 .....	84
4.4.3	Period 3 .....	86
4.4.4	Unusual Signals .....	88
5	Summary and Conclusions .....	91

## List of Tables

Table 1-1: Applicable Documents.....	10
Table 1-2: Reference Documents.....	10
Table 1-3: Acronyms and Abbreviations.....	11
Table 2-1: Different types of event definitions.....	14
Table 2-2: Description of the information shared for each detected event. ....	16
Table 2-3: Summary of Sites used for Long-Term Monitoring within WP6 of the STRIKE3 project .....	26
Table 2-4 - Summary of Additional Sites used prior to Long-term Monitoring within the STRIKE3 project.....	28
Table 3-1: List of Reported interference events from the co-located sensors to the STRIKE3 database.....	44
Table 3-2: List of Events Detected by GSS100D at site 9a during Monitoring Period .....	50
Table 3-3: List of RF Oculus Events at Monitoring Site.....	55
Table 4-1: Site information ordered by monthly average intentional activity.....	72
Table 4-2: Comparison of Average Activity for High Activity Sites in Different Monitoring Periods .....	74
Table 4-3: Description of Chirp Jammer Categories .....	81

## List of Figures

Figure 2-1: Overview of DETECTOR System for Initial STRIKE3 Monitoring.....	17
Figure 2-2: Detector V1 Field Probe .....	18
Figure 2-3: DETECTOR V0 Field Probe (for Detection).....	18
Figure 2-4: DETECTOR V0 Field Hub (for comms) .....	19
Figure 2-5: Example Spectrum and Spectrogram viewed through the Web Portal.....	20
Figure 2-6: RF Oculus monitoring system. Developed for research activities. ....	21
Figure 3-1: Growth of detected interference events reported to the STRIKE3 database during the measurement campaign.....	30
Figure 3-2: Total number of detected events per month reported to the STRIKE3 database during the measurement campaign.....	31
Figure 3-3: Number of active sensors per month during the measurement campaign. ....	32
Figure 3-4: Distribution of detected interference events among the different sites per month. The central mark indicates the median, and the bottom and top edges of the box indicate the 25th and 75th percentiles, respectively. The whiskers extend to the most extreme data points not considered outliers, and the outliers are plotted individually using the '+' symbol and limited to 200 for scaleability. ....	33
Figure 3-5: Detected interference events distributed on countries. ....	34
Figure 3-6: Number of detected interference events distributed on the day of week. The central mark indicates the median, and the bottom and top edges of the box indicate the 25th and 75th percentiles, respectively. The whiskers extend to the most extreme data points not considered outliers, and the outliers are plotted individually using the '+' symbol and limited to 100 for scaleability.....	35
Figure 3-7. Number of detected interference events distributed in the hour of the day. The central mark indicates the median, and the bottom and top edges of the box indicate the 25th and 75th percentiles, respectively. The whiskers extend to the most extreme data points not considered outliers, and the outliers are plotted individually using the '+' symbol and limited to 90 for scaleability reasons. ....	36
Figure 3-8: Number of detected events per site during the measurement campaign. ....	37
Figure 3-9: Active sites per month. An active site is marked with green whilst an inactive site is marked with red. ....	38
Figure 3-10: Detection statistics for site no. 13. ....	39
Figure 3-11: Detection statistics for site no. 5. ....	39
Figure 3-12: Detection statistics for site no. 12. ....	40
Figure 3-13: Detection statistics for site no. 16. ....	40
Figure 3-14: Detection statistics for site no. 33a. ....	41

## D6.2: Threat Database Analysis Report

Ref: STRIKE3\_D62\_DatabaseRep

Issue: 1.0

Date: 25.01.19

---

Figure 3-15. Reported interference events by the Detector sensor.....	42
Figure 3-16: Reported interference events by the RF-Oculus sensor. ....	43
Figure 3-17 Power received in RF Oculus, and reported incidents from the Detector node. The RF Oculus did not report any incident during this time interval. Example from April 24 2018. ....	45
Figure 3-18 Frequency spectrum of incident detected on April 24 2018. Interference occurs outside of RF Oculus received bandwidth but within the Detector received bandwidth. .....	45
Figure 3-19 Power received in RF Oculus, and reported incidents from the two co-located nodes. Example from Sep. 19 2018.....	47
Figure 3-20 Frequency spectrum of incident detected on Sep 19 2018. ....	47
Figure 3-21: SNR Values at CORS Receiver close to RF Oculus Equipment on 17/08/1856	
Figure 4-1: Overview of data from long-term monitoring period .....	59
Figure 4-2: Time distribution of events for long-term monitoring throughout the day.....	60
Figure 4-3: (a) Total number of events with normalised power over 3.5 for each DETECTOR site active during WP6; (b) Total number of events with normalised power over 3.5 for each DETECTOR site active during WP6 – reduced axis; (c) No. of intentional events divided by total no. of total events.....	<b>Error! Bookmark not defined.</b>
Figure 4-4: Monthly average no. of events for each DETECTOR site in WP6. (a) shows the full range and in (b) the y-axis has been truncated to show more detail for lower activity sites.....	63
Figure 4-5: Totals of Reported and Unreported Intentional and Unintentional Events at each site.....	65
Figure 4-6: % of Intentional and Unintentional Events at each site that meet the event criteria and are reported to the STRIKE3 database .....	66
Figure 4-7: Impact of intentional and unintentional signals across the sites .....	67
Figure 4-8: % of Impacting intentional and unintentional signals across the sites .....	67
Figure 4-9: Overview of all signals across all time .....	69
Figure 4-10: Number of events throughout the day in local time .....	70
Figure 4-11: Monthly average events for all sites active in period 1 .....	73
Figure 4-12: Monthly average events for all sites active in period 2.....	73
Figure 4-13: Monthly average events for all sites active in period 3. The y-axis has been truncated to allow easier comparison with the other periods.....	74
Figure 4-14: Bar chart showing how the total event detection rate changes over time for seven sites that appear in all three monitoring periods .....	75
Figure 4-15: Plot showing Decrease in Jammer Activity at site 10.....	75
Figure 4-16: Plot showing Decrease in Jammer Activity at site 26.....	76

## D6.2: Threat Database Analysis Report

**Ref:** STRIKE3\_D62\_DatabaseRep

**Issue:** 1.0

**Date:** 25.01.19

---

Figure 4-17: Monthly Average Number of Chirp Events of each type at Each Site .....	81
Figure 4-18: Total Number of Events of each type from All Sites.....	82
Figure 4-19: Number of Sites that Detect Each Type of Event.....	83
Figure 4-20: Breakdown of chirp types by site for period 2. Monthly averages. ....	84
Figure 4-21: Breakdown of the total number of chirp types in period 2 .....	85
Figure 4-22: Breakdown of the spread of occurrences of various chirp types for period 2	86
Figure 4-23: Monthly average chirp types seen across the six sites under consideration .	87
Figure 4-24: Monthly average chirp type breakdown for each site. ....	88
Figure 4-25: Example Unusual Chirp Signals with Downward Sweep .....	89
Figure 4-26: Example Unusual Chirp Events with Multiple Signals .....	89
Figure 4-27: Example Unusual Non-Chirp Signals .....	90



# 1 Introduction

## 1.1 Purpose of Document

This document is the STRIKE3 threat database analysis report. The main purpose of this document is to present a summary of the results of the long-term monitoring and validation of the draft standards for threat monitoring and reporting. This deliverable is prepared as part of WP6: Threat Reporting Validation Process. The lead partner of WP6 is FOI. This document has been prepared with contributions from FOI, NSL, AGIT and GNSS Labs.

## 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 which describes the purpose, scope and structure of the document.
- **Section 2** provides an overview of international threat collection activities.
- **Section 3** provides a detailed review of the standard reports from the centralised STRIKE3 server.
- **Section 4** contains a detailed analysis of activity and signals across the whole of the STRIKE3 project.
- **Section 5** contains a summary and conclusions

## 1.4 References

### 1.4.1 Applicable Documents

The following documents, of the exact issue shown, form part of this document to the extent specified herein. Applicable documents are those referenced in the Contract or approved by the Approval Authority. They are referenced in this document in the form [AD X]:

Reference	Title	Document Reference	Version	Date
AD 1.	STRIKE3 Grant Agreement	Grant Agreement Number 687329	-	26/01/2016
AD 2.				

**Table 1-1: Applicable Documents**

### 1.4.2 Reference Documents

The following documents, although not part of this document, amplify or clarify its contents. Reference documents are those not applicable and referenced within this document. They are referenced in this document in the form [RD X]:

Reference	Title	Author(s)	Date
RD 1.	STRIKE3 D4.1 Draft Standards for Threat Monitoring & Reporting	NSL & FOI	20/03/2017
RD 2.	STRIKE3 D4.2 Draft Standards for Receiver Testing Against Threats	NSL, ETRI, NLS, GNSS Labs & SAC	28/02/2017

**Table 1-2: Reference Documents**

## 1.5 Acronyms

Acronym	Definition
AD	Applicable Documents

## D6.2: Threat Database Analysis Report

Ref: STRIKE3\_D62\_DatabaseRep

Issue: 1.0

Date: 25.01.19

<b>Acronym</b>	<b>Definition</b>
CORS	Continuously Operating Reference Station
COTS	Commercial Off The Shelf
EGNOS	European Geostationary Navigation Overlay Service
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
NB	Narrow Band
RD	Reference Document
RF	Radio Frequency
RFI	Radio Frequency Interference
RINEX	Receiver Independent Exchange format
SDR	Software Defined Radio
SNR	Signal to Noise Ratio (similar to C/N0)
ST	Single Tone
STRIKE3	Standardisation of GNSS Threat Reporting and Receiver Testing through International Knowledge Exchange, Experimentation and Exploitation
UTC	Coordinated Universal Time
VNB	Very Narrow band
WB	Wide Band

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

## 2 Overview of Threat Reporting Validation Process

### 2.1 Introduction

The Threat Reporting Validation Process is a 12-month activity running from November 2017 to October 2018. This activity addresses the need to validate the draft STRIKE3 threat reporting standard by deploying monitoring systems at key sites and demonstrating the population of a common and centralised STRIKE3 server and database with global GNSS threat reports. The main objectives are to:

- Deploy STRIKE3 compliant monitoring systems at key sites, replacing the initial setups
- Connect monitoring systems to the STRIKE3 server and database
- Carry out a long-term monitoring campaign to generate a unified STRIKE3 threat database
- Enable other threat monitoring systems to implement the STRIKE3 standard and to connect to the STRIKE3 infrastructure
- Develop a STRIKE3 ecosystem of stakeholders, suppliers and users

This enables a real-world validation of the STRIKE3 systems and infrastructure. The long-term monitoring also enables detailed analysis and assessment of the threat scene within different environments.

This report contains the results and analysis of long-term monitoring using the draft reporting standards to validate their use and to assess the long-term threat scene.

In addition, summary analysis of all data from the entire STRIKE3 period is provided to show more detail on the level of activity, changes over time, and types of signal that have been detected.

### 2.2 STRIKE3 Reporting Standards

The main purpose of the proposed draft reporting standards is to allow a mechanism for different types of equipment to identify and report on interference events in a standard way. This allows consistency in the results from different types of equipment so that wider analysis can be performed to get a better idea of the general level of activity.

The main elements of the reporting standard and the implementation within STRIKE3 are:

- Standard event definition criteria, so that a detected interference event is only reported if it is above a certain power level for a certain duration. The purpose of this is to prevent reporting of many thousands of low-level noise events, and also to ensure that different equipment can filter possible events in the same way
- Standard Event message definition, with minimum reporting information. This ensures that all different types of equipment report a minimum set of common information so that standard analysis can be performed.

## D6.2: Threat Database Analysis Report

**Ref:** STRIKE3\_D62\_DatabaseRep

**Issue:** 1.0

**Date:** 25.01.19

- Registration of data providers to try to provide some control over who is providing data to the database, and prevent junk and spam data being sent that would skew the results and analysis
- Use of centralized server to store standard reports and make the data available for inspection and analysis. Within STRIKE3 a database is hosted by NSL and a simple user app has been developed to demonstrate the sort of analysis that can be performed.

The event definition criteria are shown in the following table.

Type	Description
a	<p>This event definition is intended for interference detection equipment that base the detection function on either power- or AGC-monitoring.</p> <p>If the received power is 5 dB stronger than the expected noise power and if the event duration is greater than 5 seconds, then an interference event should be reported. Where:</p> <ul style="list-style-type: none"> <li>• the expected noise power is the measured received power when there is no interference signal present at the input of the equipment</li> <li>• the event duration is the difference between the start and end times of an event.</li> <li>• the start time of the event is the time at which the received power first exceeds the 5 dB threshold for increase</li> <li>• the end time of the event is the time at which the received power falls below the 5 dB threshold for increase and stays below the threshold for the following 10 seconds</li> </ul> <p><i>Note: For AGC-monitoring systems this means a decrease of 5 dB in the AGC value and it should last at least for 5 seconds.</i></p>
b	<p>This event definition is intended for interference based on GNSS-receivers without AGC enabled, where measured C/N0 is compared against expected C/N0 to detect events.</p> <p>If the measured C/N0 for all satellites in view is 6 dB less than the expected C/N0 and if the duration is greater than 10 seconds, then an interference event should be reported. Where:</p> <ul style="list-style-type: none"> <li>• the expected C/N0 is the value that would be expected when there is no interference signal present at the input of the equipment,</li> <li>• the event duration is the difference between the start and end times of an event</li> <li>• the start time of the event is the time at which the drop in C/N0 for all satellites in view first exceeds the 6 dB threshold</li> </ul>

## D6.2: Threat Database Analysis Report

Ref: STRIKE3\_D62\_DatabaseRep

Issue: 1.0

Date: 25.01.19

	<ul style="list-style-type: none"> <li>the end time of the event is the time at which at the C/N0 for at least one of the satellites in view increases above the detection threshold and stays above the threshold for the following 10 seconds</li> </ul>
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

**Table 2-1: Different types of event definitions.**

The contents of the event message are described in the next table. There is a non-optional part of the message, which contains information about the detected event that must be reported. There is though an opportunity, for some of the fields, to be vague if it sensitive to share that sort of information. For example, the region field, it is required to report in what country the event was detected but one can choose to report a city or a location (approximate latitude and longitude) to give more detailed information.

In the optional part of the message more detailed information about the detected event is provided. With that information together with the mandatory part of the message it would be possible the make deeper analysis of the interference event. Hopefully will many of the interference monitoring networks be able to provide both parts of the message to the centralised server.

Field	Description	Optional
Id	A unique identifier of the event. With the id it should be possible to go back to the interference monitoring network and sensor that reported this event in order to obtain more detailed information. The link back to the originating systems is only available to users authorized by that system.	No
Equipment Type	The name of the type of detection equipment that has detected this event. This is required in order to be able to link each event to the type of detection equipment that detected it.  The detection equipment type name should match one of the sensor types registered for the network.	No
Event definition	One of the two provided event definitions must be selected and followed. Selection of type a) or b).  <i>Note: See event definition section Table 2-1 for a definition of the different types.</i>	No
Frequency band	The frequency band where this interference event was detected. The current options are; 1575.42 MHz  <i>Note: This could be extended in the future to cover other frequency bands that are not supported at this moment.</i>	No

## D6.2: Threat Database Analysis Report

Ref: STRIKE3\_D62\_DatabaseRep

Issue: 1.0

Date: 25.01.19

Field	Description	Optional
Region	The region of where this interference event was detected. The region can be reported in different levels of detail. The minimum level of detail is at country basis. However, if the region is not sensitive information this can be reported more precise such as specific city or coordinates.	No
Date	The date (relative UTC) of when this event was detected.	No
Start time	The UTC timestamp of when this event was detected. <i>Note: Start time is not required as mandatory, but it is highly recommended that the start time is reported for the event.</i>	Yes
Duration	The duration of this event, when the selected event definition is true, in seconds.	Yes
GNSS fix lost	A GNSS-receiver, at the location of the detection system, lost their position fix during this event; Yes or No.	Yes
Spectrum	A frequency spectrum of the detected event. A frequency and power vector (with equal length) shall be reported. <i>Note: The user interface will render the spectrum figure in the same format for all different types of interference detection systems.</i>	Yes
Raw data available	A flag that indicates whether or not raw data (I/Q data) is available at the local event database.	Yes
Antenna type	The used antenna type.	Yes
Noise figure	The reference noise figure for the sensor (dBm). <i>Note: This value is used as the reference point of the reported "Delta power" and is only applicable when event definition type a) is used.</i>	Yes
Delta power	Maximum delta power in decibel (dB) above systems noise floor at the specific monitoring site. <i>Note: This is only applicable when event definition type a) is used.</i>	Yes
Baseline C/N0	The baseline C/N0 (dB-Hz) is the value that would be expected when there is no interference signal present at the input of the equipment <i>Note: This value is used as the reference point of the reported "Delta C/N0" and is only applicable when event definition type b) is used.</i>	Yes

Field	Description	Optional
Delta C/N0	<p>Maximum decrease in C/N0 in decibel (dB) relative the C/N0 without interference of the receiver at the specific monitoring site.</p> <p><i>Note: This is only applicable when event definition type b) is used.</i></p>	Yes

**Table 2-2: Description of the information shared for each detected event.**

Full details of the reporting standards, including further description and justification of the event definition and message contents, can be found in the draft reporting standards [RD.1].

## 2.3 Types of Equipment

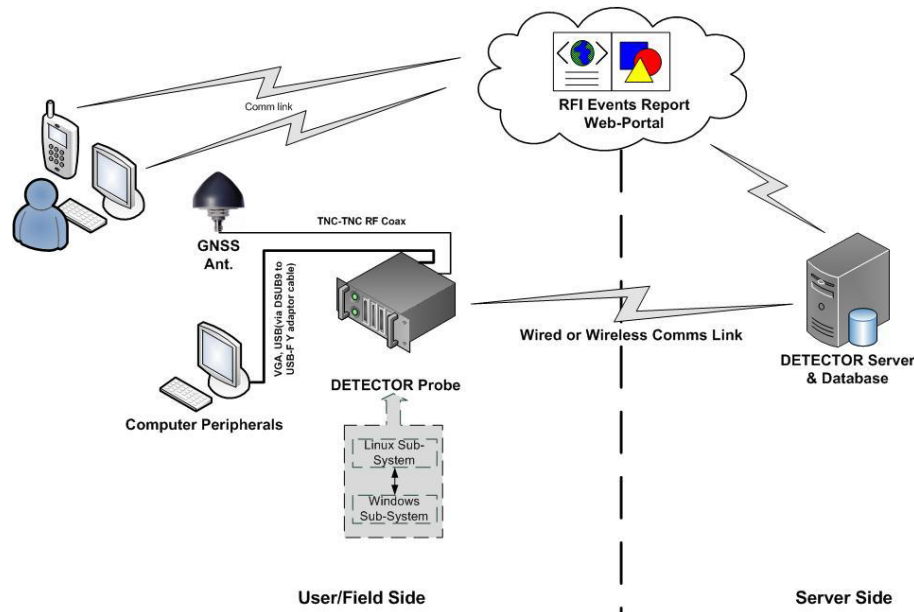
A number of different monitoring systems are brought to the STRIKE3 project by the consortium for use in the Threat Reporting Validation Process. Having different types of equipment is important for STRIKE3 where the aim is to develop reporting standards that are not tied to a particular product and can be supported by multiple interference monitoring systems. The types of monitoring system used in this activity are described in the following sections. It is noted that the different equipment works independently to detect interference events, and has been modified to report to a central STRIKE3 database using the draft reporting standards defined in RD.1. This means that there is a central database of standardised events from all sites, as well as individual records of all events stored locally for each type of detection system.

### 2.3.1 Detector

DETECTOR is a commercially available system for GNSS interference monitoring and characterization. The prototype system was originally developed in the DETECTOR project (funded by the GSA under the FP7 programme), which was led by NSL. Since then, NSL have further developed the system and it is now sold as a commercial product through Spirent (<http://www.spirent.com/Products/GSS100D-Detector>). This version is hereafter referred to as Detector v1.

The DETECTOR system consists of several components, as illustrated in the figure below.





**Figure 2-1: Overview of DETECTOR System for Initial STRIKE3 Monitoring**

Within STRIKE3 NSL host a single Detector server and database and two types of field probe report into it.

#### *GSS100D Field Probe*

This field probe is a 19" rack mounted unit that contains a software defined radio (SDR), a COTS GNSS receiver and a computer. The SDR front-end samples the civilian L1 GNSS continuously. Both pre- and post-correlation techniques are used to check for interference. Once interference is detected, this triggers an event and the power readings and GNSS Rx tracking information are logged for the duration of the event, as well as the start and end time and a digital sample of the raw data. Once the interference is no longer detected, the event is closed and the event message is sent to the remote back-office. The event message contains the following information:

- Device Id: Id of the device sending the report
- Start time: Start time of the event
- For each few seconds throughout the event:
  - Time
  - Power reading
  - GPS position
  - Information on GPS satellites tracked
- For the epoch with maximum power reading, the raw data sample is logged and included in the message.



**Figure 2-2: Detector V1 Field Probe**

#### *Detector V0 Field Probe*

This is the prototype Detector system, hereafter referred to as Detector V0. These prototypes are the same as those that were developed in the DETECTOR project (funded by the GSA under the FP7 programme), which was led by NSL.

The main difference to the GSS100D is that the Detector V0 field installation has a separate probe (with the RF front end and GPS receiver) and hub (to handle the comms with the back office), as illustrated in the following figures.



**Figure 2-3: DETECTOR V0 Field Probe (for Detection)**



**Figure 2-4: DETECTOR V0 Field Hub (for comms)**

Apart from the differences in the field unit HW, other functionalities are the same as GSS100D, and so the same information, results and analysis is available at the Detector back office as for GSS100D.

#### *Back-office Server/Database*

The DETECTOR back-office is a remote facility that receives, processes and stores events from multiple field probes. SW at the back-office processes the data sample to generate spectrum and spectrogram plots, and to perform classification of the signal type. The information about each event is stored in a database and analysis tools are available to provide statistics about events. Events are categorised as follows:

##### **I. Priority Level**

This is a metric determined by the power *and* type of interference. Interference which is clearly identifiable as a chirp jammer is ranked higher than those where there is less structure or there is less confidence in the attributed type. Power levels are divided into ranges, with the higher ranges leading to a higher priority.

##### **II. Device**

Selecting data from all or some of the available probe or probes

##### **III. Classification type**

IV. Selecting according to the signal type of the interference events. The categories include types such as Narrow Band (NB), Single Tone (ST), Wide Band (WB), CDMA, and various CHIRP types.

**V. Power**

Selecting according to the maximum power level of the detected event

**VI. Duration**

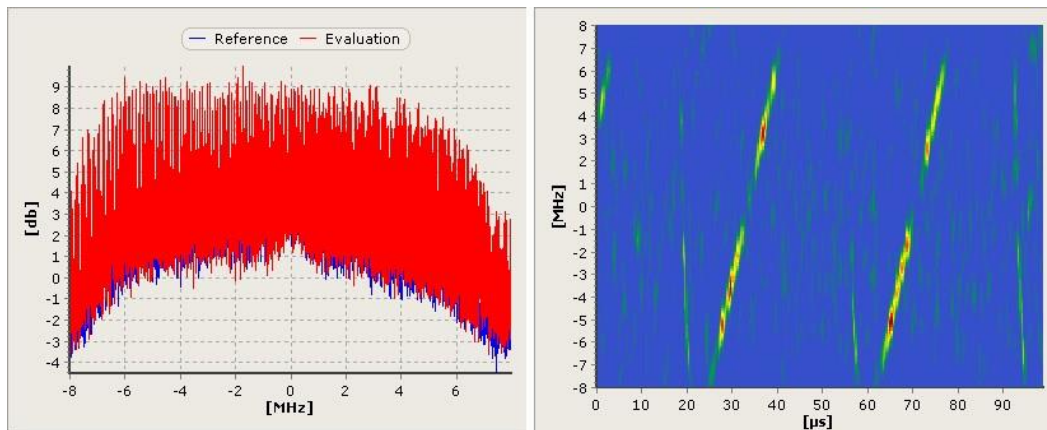
Selecting according to the duration of the detected event (period of time over which the power level of the interference remains above the threshold)

**VII. Event Type**

Allows differentiation between automatically generated events and manually triggered data grabs used to determine reference signal reception conditions.

*Web Portal*

The back-office for DETECTOR is managed centrally and is not open to all users. However, users with field probes can gain access to results for their device through a web portal. This allows users to view a summary of all events detected at their probe, as well as more detailed information on the signal. Summary tables of results can be exported and downloaded as CSV files.



**Figure 2-5: Example Spectrum and Spectrogram viewed through the Web Portal**

**2.3.2 RF Oculus**

RF-Oculus, is based on low cost commercial-off-the-shelf (COTS) components, see Figure 2-6. The measurement system consists of a software defined radio (SDR), a GNSS receiver and an Intel NUC computer. The SDR front-end samples the civilian L1 GNSS continuously with the instantaneous bandwidth of 4 MHz. The complex baseband signal is used for interference detection and classification. An energy detector is used to detect interference event and an Impulsiveness ratio (IR) detector is used to classify the interference.

A database in each node stores the GPS C/N0, received power from the SDR front end, IR value and current position. In case of an interference event start time, stop time and a frequency spectrum is stored to the database. The corresponding baseband signal for the

interference event is also stored at the nodes hard disk.

Several nodes can be connected to a central server. The central server also runs a web-server. The web application at the central server displays detection statistics, detailed information of interference event etc.



**Figure 2-6: RF Oculus monitoring system. Developed for research activities.**

### 2.3.3 GNSS Receivers

As well as using dedicated RF monitoring equipment, the reporting standards allow for the use of standard GNSS receivers to report interference based on C/N0 monitoring. Therefore, in this activity, analysis of GNSS data from a selection of CORS sites has been performed to see how it compares with the results from the dedicated RF monitoring equipment.

## 2.4 Monitoring Sites

Across the STRIKE3 project as a whole there have been 48 monitoring sites across 21 different countries. The sites have been chosen as they contribute to or satisfy the following requirements for the activity:

- Deployments in different countries to establish a wide area network
- Deployments at sites at different types of location with different local interference environment (e.g. city areas, major roads, etc.)
- Deployments at sites with different uses (e.g. timing, airports, power grids, etc.) to cover different types of infrastructure and engage with different potential stakeholders

Some sites have had continuous monitoring for over 2 years+, whilst others have been in place for just a short time, sometimes being moved around to other sites in order to build up a bigger picture. The following tables summarise the different monitoring sites that have been used. Note that those sites that have been active during the Reporting Platform Validation Process activity (and hence contribute standardised reports to the centralised STRIKE3 server) are separated from those that were active earlier in the project (and hence have just local event databases).

## D6.2: Threat Database Analysis Report

**Ref:** STRIKE3\_D62\_DatabaseRep

**Issue:** 1.0

**Date:** 25.01.19

---

For each site the main things noted in the table are:

- Type of equipment at the site
- Approximate dates of operation
- Site infrastructure
  - This is interesting to know as certain types of infrastructure may have other systems installed (e.g. comms systems) that may potentially cause unintentional interference with GPS
- Local environment
  - This is useful to know as the level of interference (unintentional and intentional) is often related to human activity, and so whether the site is in a busy city location or in a quiet field, for example, may well impact the level of activity we see
- Distance to roads (minor / major)
  - The major source of intentional interference is thought to come from in-vehicle jammers, and so verifying the activity against distance from roads is a good way to confirm this.

## D6.2: Threat Database Analysis Report

Ref: STRIKE3\_D62\_DatabaseRep

Issue: 1.0

Date: 25.01.19

Site No	Infrastructure	Local Environment	Distance to minor road	Distance to major road	Type of Equipment Installed	Start of Data	End of Data	Comments
1	Power Grid	Near intercity motorway	15 metres	300 metres	Detector V0	July 2016	September 2018	
2	Power Grid	Urban	140 metres	1.35 miles	Detector V0	Middle of February 2016	April 2018	
3	Gantry	Inter-city motorway	-	9 metres	Detector V0	February 2016	February 2018	
4	Gantry	Inter-city motorway	-	17 metres	Detector V0	July 2016	February 2018	
5	Airport	City motorway	-	119 metres	Detector V1	August 2017	Currently Active	
6	Airport	Airport	200 metres	1.1 miles	Detector V1	June 2016	Currently Active	
7	Boat/Port	Sea / port	NA	NA	Detector V1	December 2017	April 2018	Moved around the coast so no fixed distance from roads
8	Office	Urban	21 metres	2.5km	Detector V1	May 2018	Currently Active	
9a	Port	Port	140 metres	230 metres	Detector V1	April 2018	Currently Active	Both a Detector unit and a RF Oculus are set up at this site.
9b	Port	Port	140 metres	230 metres	RF Oculus	April 2018	Currently Active	
10	Office	City centre	29 metres	260 metres	Detector V1	November 2016	May 2018	



D6.2: Threat Database Analysis Report

Ref: STRIKE3\_D62\_DatabaseRep

Issue: 1.0

Date: 25.01.19

Site No	Infrastructure	Local Environment	Distance to minor road	Distance to major road	Type of Equipment Installed	Start of Data	End of Data	Comments
11	Office	Urban	114 metres	350 metres	Detector V1	Middle of May 2016	Currently Active	
12	Office	City motorway	30 metres	150 metres	Detector V1	June 2016	Currently Active	
13	Office	City centre	65 metres	178 metres	Detector V1	End of April 2016	Currently Active	
14	Airport	Airport	70 metres	400 metres	Detector V1	July 2017	January 2018	
15	Office	City Centre	-	4 metres	Detector V1	April 2018	May 2018	
16	Airport	City Centre	-	45 metres	Detector V1	June 2018	July 2018	
17	Office	City Centre	-	40 metres	Detector V1	August 2018	September 2018	
18	Airport	Airport	300 metres	4.5 km	Detector V1	September 2018	October 2018	
19	Airport	Airport	500 metres	4 km	Detector V1	October 2018	Currently active	
20	Office	Urban	65 metres	250 metres	Detector V1	November 2016	February 2017	Probe swap on 03/02/17
	Office	Urban	65 metres	250 metres	Detector V1	February 2017	February 2018	
21	Office	Business Park	30 metres	460 metres	Detector V1	March 2018	Currently Active	
22	Office / Airport	Inter-city motorway	1.3 km	45 metres	Detector V1	September 2016	Currently Active	
23	Office	Business Park	10 metres	70 metres	Detector V1	January 2017	Currently Active	



D6.2: Threat Database Analysis Report

Ref: STRIKE3\_D62\_DatabaseRep

Issue: 1.0

Date: 25.01.19

Site No	Infrastructure	Local Environment	Distance to minor road	Distance to major road	Type of Equipment Installed	Start of Data	End of Data	Comments
24	Airport	Airport	-	120 metres	Detector V1	December 2017	March 2018	
25	Office	Inter-city motorway	-	30 metres	Detector V1	July 2018	October 2018	
26	Toll booth	Inter-city motorway	-	45 metres	Detector V1	September 2016	June 2017	Probe was replaced due to problem.
	Toll booth	Inter-city motorway	-	45 metres	Detector V1	August 2017	Currently Active	Nature of site has also changed with removal of tolls in April 2018
27	Airport	Airport	100 metres	350 metres	Detector V1	July 2018	Currently Active	
28	Airport	Inter-city motorway	-	70 metres	Detector V1	July 2017	April 2018	
29	Airport	Airport	86m	150m	Detector V1	August 2017	Currently Active	
30	Airport	Airport	200 metres	1.15 miles	Detector V1	April 2017	Currently Active	
31	Office	City centre	70 metres	250 metres	Detector V1	April 2018	May 2018	
32	Airport	Near city motorway	-	100 metres	Detector V1	June 2017	Currently Active	
33a	Airport	Near a motorway	-	30 metres	RF Oculus	March 2016	Currently Active	
33b	Airport	Near a motorway	-	10 metres	RF Oculus	March 2016	Currently Active	
33c	Airport	Near a motorway	-	5 metres	RF Oculus	March 2016	Currently Active	

D6.2: Threat Database Analysis Report

Ref: STRIKE3\_D62\_DatabaseRep

Issue: 1.0

Date: 25.01.19

Site No	Infrastructure	Local Environment	Distance to minor road	Distance to major road	Type of Equipment Installed	Start of Data	End of Data	Comments
34	Office	Business park	70 metres	70 metres	RF Oculus	End of June 2018	Currently Active	

**Table 2-3: Summary of Sites used for Long-Term Monitoring within WP6 of the STRIKE3 project**

Site No	Infrastructure Active in WP3	Local Environment	Distance to minor road	Distance to major road	Type of Equipment Installed	Start of Data	End of Data	Comments
35	Office	Business park	50 metres	750 metres	Detector V1	End of April 2016	Mid-August 2016	
36	House	Urban	110 metres	400 metres	RF Oculus	March 2016	November 2017	Both a Detector unit and a RF Oculus are set up at this site.
37	House	Urban	110 metres	400 metres	Detector V1	Middle of August 2016	November 2017	
38	Office	Business park	50 metres	700 metres	Detector V0	Middle of March 2016	May 2017	
39	Gantry	Inter-city motorway	-	0 metres	Detector V0	July 2016	October 2017	

D6.2: Threat Database Analysis Report

Ref: STRIKE3\_D62\_DatabaseRep

Issue: 1.0

Date: 25.01.19

Site No	Infrastructure Active in WP3	Local Environment	Distance to minor road	Distance to major road	Type of Equipment Installed	Start of Data	End of Data	Comments
40	Gantry	Inter-city motorway	-	0 metres	Detector V0	July 2016	October 2016	
41	Office	Business park	19 metres	500 metres	Detector V1	August 2016	Mid-September 2016	
42	Power Grid	City motorway	-	200 metres	Detector V1	Mid-August 2016	November 2017	
43	Office / Railway	Urban	100 metres	450 metres	Detector V1	November 2016	June 2017	
44	Gantry	Border crossing, motorway	-	30 metres	Detector V1	November 2016	April 2017	
45	House	Inter-city motorway	-	14 metres	Detector V1	December 2016	May 2017	
46	Office	Port	40 metres	100 metres	Detector V1	January 2017	August 2017	
47	Airport	Inter-city motorway	-	80 metres	Detector V1	April 2017	August 2017	

D6.2: Threat Database Analysis Report

Ref: STRIKE3\_D62\_DatabaseRep

Issue: 1.0

Date: 25.01.19

Site No	Infrastructure Active in WP3	Local Environment	Distance to minor road	Distance to major road	Type of Equipment Installed	Start of Data	End of Data	Comments
48	Office	Inter-city motorway	45 metres	60 metres then 140 metres	Detector V1	July 2017	September 2017	Probe changed buildings end of July to September 2017
49	Office	Port	340 metres	50 metres	Detector V1	November 2016	June 2017	

**Table 2-4 - Summary of Additional Sites used prior to Long-term Monitoring within the STRIKE3 project**

## 3 Standardised Monitoring Results

### 3.1 Introduction

This section provides a review of the results generated using the draft reporting standards. This includes a summary of the results and analysis available at the centralised STRIKE3 server from the long-term monitoring campaign, as well as a more detailed assessment of the suitability of the event criteria, through comparing events reported by different equipment.

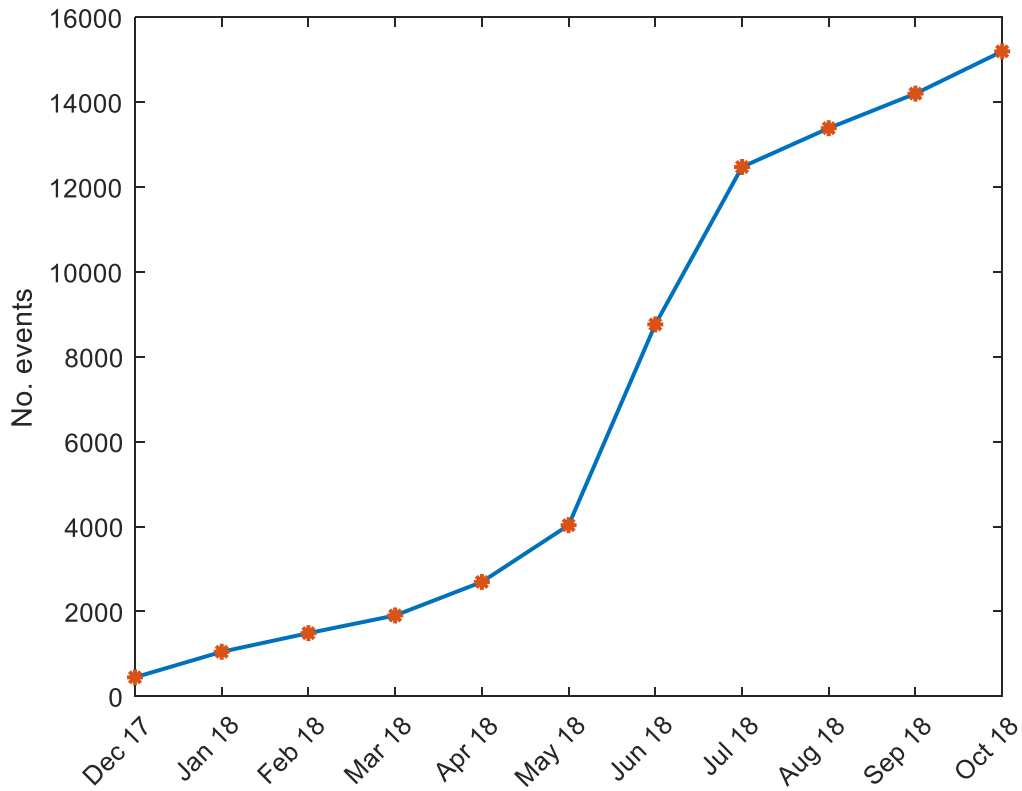
### 3.2 Analysis of Standardised Reports from STRIKE3 Server

#### 3.2.1 Overview

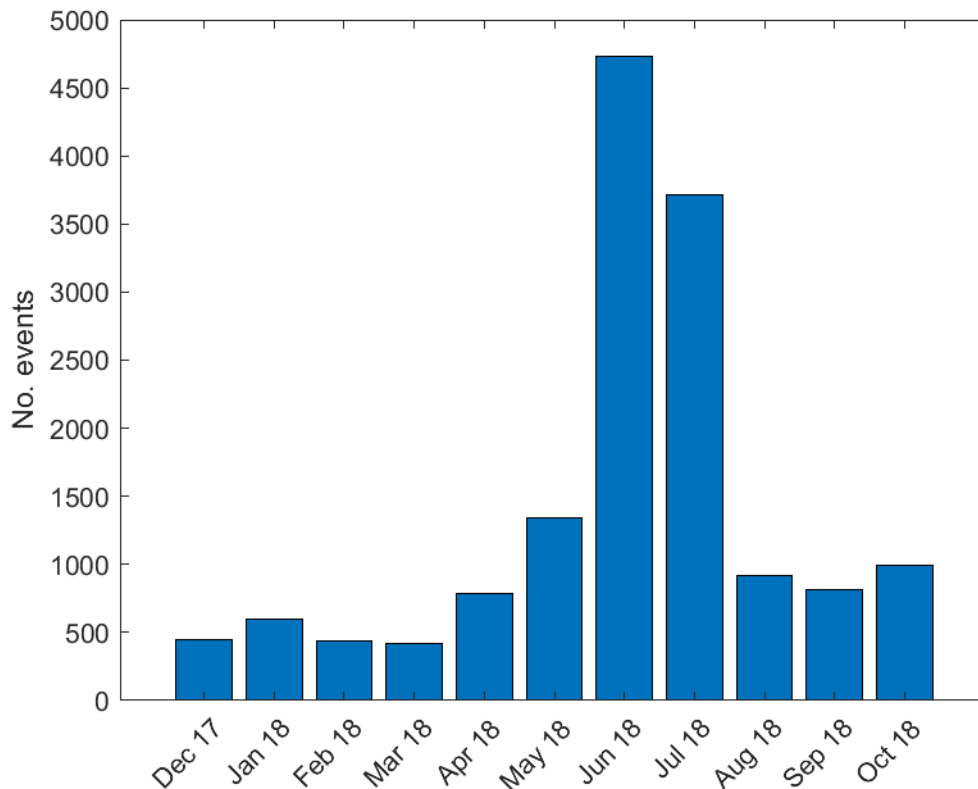
In this section, interference events sent to the STRIKE3 database through the standardised message are analysed in terms of number of events per month, country, day of week and hour of day. The database consists of tens of thousands interference events from sensors both from NSL and FOI. For some selected sites, the number of detected events is analysed deeply. The purpose of this section therefore is to show examples of the sort of analysis that can be performed using the information provided through standardised reporting, and to highlight some interesting or noteworthy findings.

#### 3.2.2 Total Events

During the entire measurement campaign, 2017-12-01 to 2018-10-31, there were in total 15 200 detected interference events reported by the STRIKE3 network to the centralised database through the standard reports, see Figure 3-1. In the beginning of the measurement campaign the number of events grew with approximately 500 events per month and in the end of the period the number of events per month were approximately 1000. Three months of the measurement period, May, June and July, have an outstanding number of events well above 1000 events each month, see Figure 3-2.

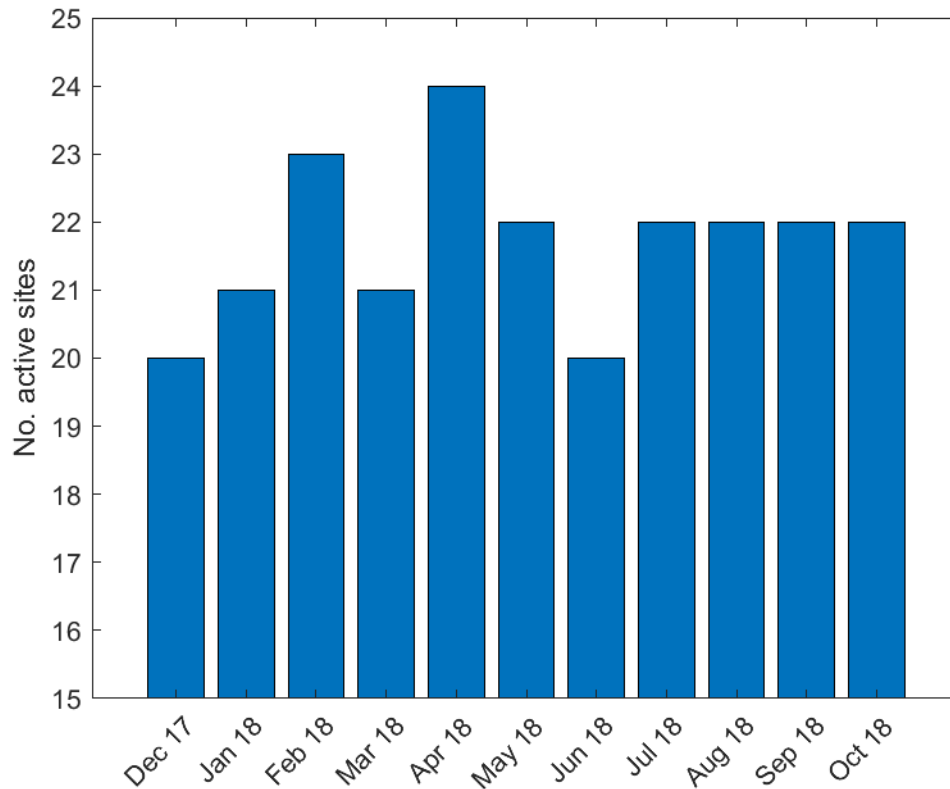


**Figure 3-1: Growth of detected interference events reported to the STRIKE3 database during the measurement campaign.**



**Figure 3-2: Total number of detected events per month reported to the STRIKE3 database during the measurement campaign.**

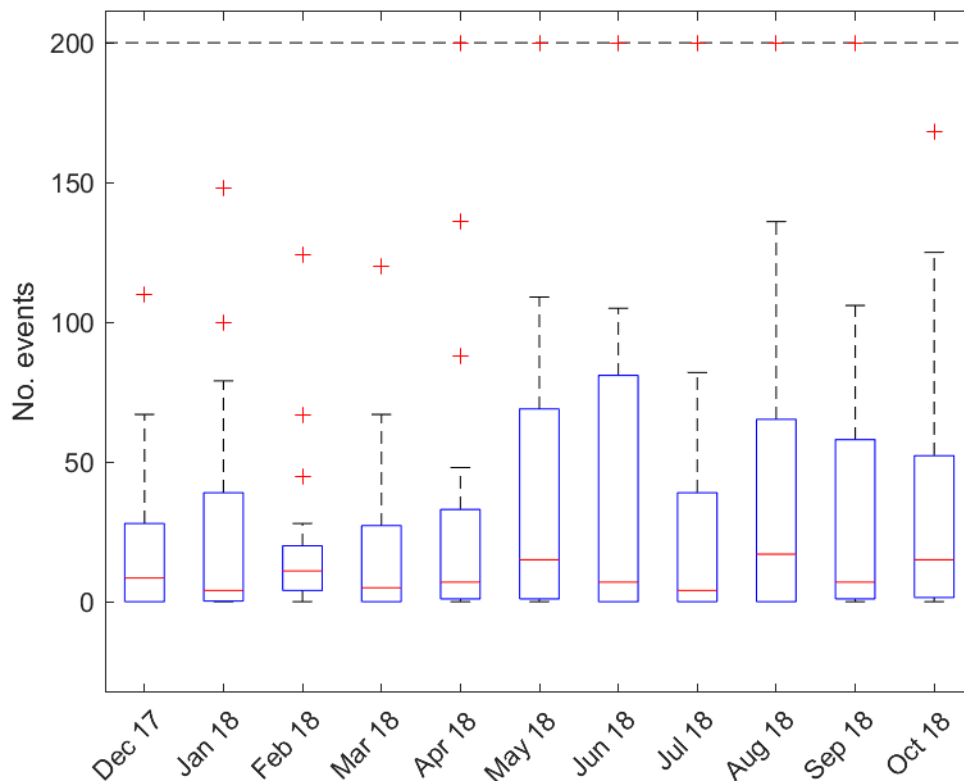
The increased growth of detected events is not an effect of the number of active sites during the period. In fact, when there were most detected events in June, then there was the least number of active sites. Figure 3-3 shows the number of active sites per month during the measurement period. By comparing Figure 3-2 and Figure 3-3 this phenomenon can be understood. Worth a note here is that the number of active sites is not available in the STRIKE3 database. Instead the number of active sites is based on separate notes from NSL and FOI about their respective systems. The reason why there are outstanding many events in especially June and July is because site no. 16 was active during these months and this site has many events, see section 3.2.3.



**Figure 3-3: Number of active sensors per month during the measurement campaign.**

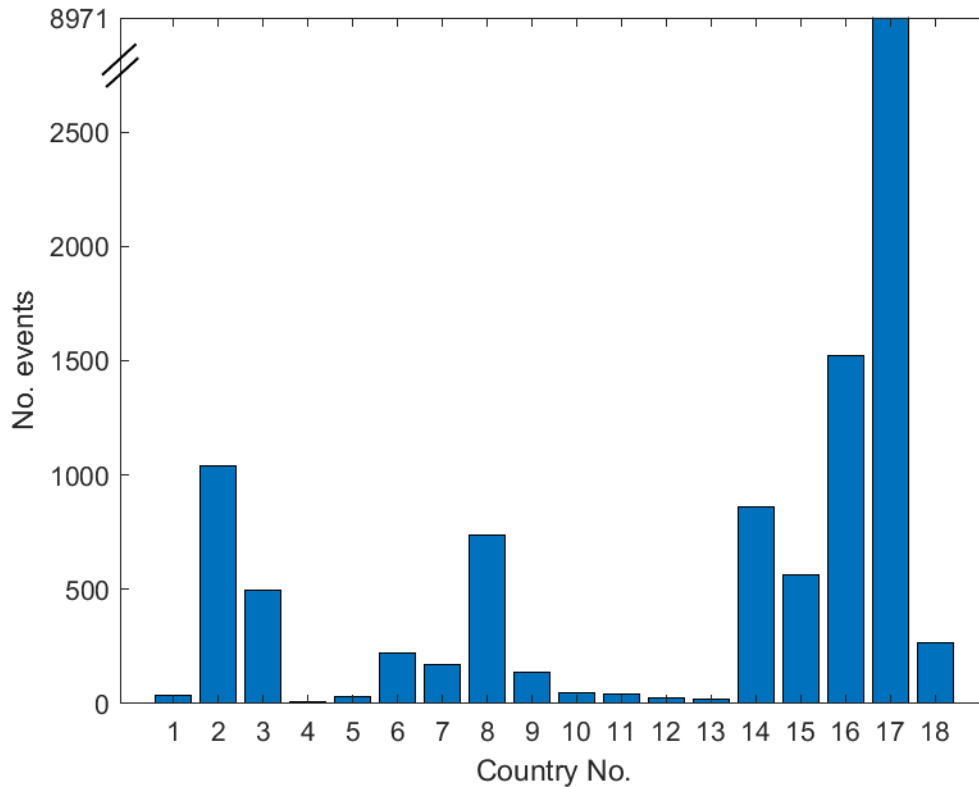
Looking at the distribution of the events among the different sites per month, the median value is around 10 events per month, see the red horizontal line in Figure 3-4. The horizontal edges of the blue box in Figure 3-4 indicate the 25<sup>th</sup> and the 75<sup>th</sup> percentiles, respectively. The whiskers in the figure extend to the number of events not considered outliers, and the outliers are limited to 200 and plotted individually using the '+' symbol. From Figure 3-4 we can conclude that there are sites that have zero events per month, and sites that have around 100 or more events, which means more than 3 events per day on average for those sites.





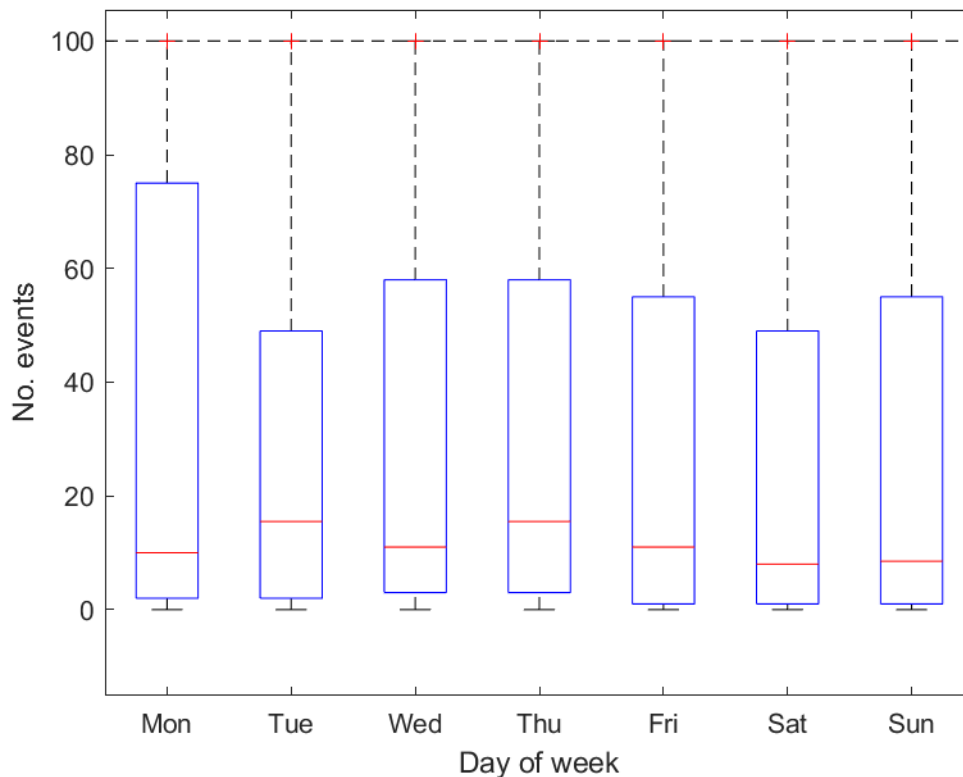
**Figure 3-4: Distribution of detected interference events among the different sites per month. The central mark indicates the median, and the bottom and top edges of the box indicate the 25th and 75th percentiles, respectively. The whiskers extend to the most extreme data points not considered outliers, and the outliers are plotted individually using the '+' symbol and limited to 200 for scaleability.**

In the measurement campaign 18 different countries are represented with various numbers of sites per country. Figure 3-5 shows the distribution of detected events among the different countries during the measurement campaign. The number of events per country is not scaled with the number of sites per country in this figure, which means that some countries might be more prone to have GPS interference because there were more measurements sites in that country and thus higher probability to detect the interferences. Also, the selected type of site (motorway, airport, city centre, etc.) per country is crucial for the number of detected events per country. So, one should be careful to say that a specific country has bigger problems with GPS interference than another country based on the results shown in Figure 3-5.



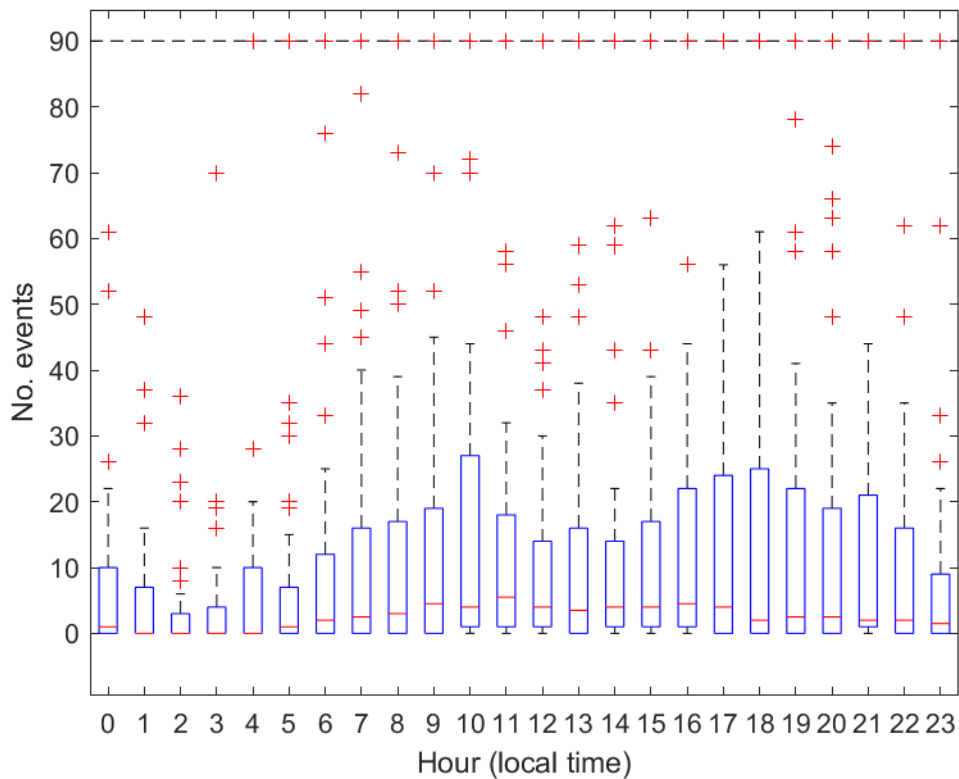
**Figure 3-5: Detected interference events distributed on countries.**

Figure 3-6 shows the distribution of the detected events with respect to the day of the week. It is seen in the figure that the median number of detected events for Monday to Friday is larger than respective number for Saturday and Sunday. This indicates that the detected events might have a correlation to business days, where more people and vehicles are active. For some sites the business might be the same for the entire week and therefore we see almost the same median number of detected events for the business days and for the weekend.



**Figure 3-6: Number of detected interference events distributed on the day of week. The central mark indicates the median, and the bottom and top edges of the box indicate the 25th and 75th percentiles, respectively. The whiskers extend to the most extreme data points not considered outliers, and the outliers are plotted individually using the '+' symbol and limited to 100 for scaleability.**

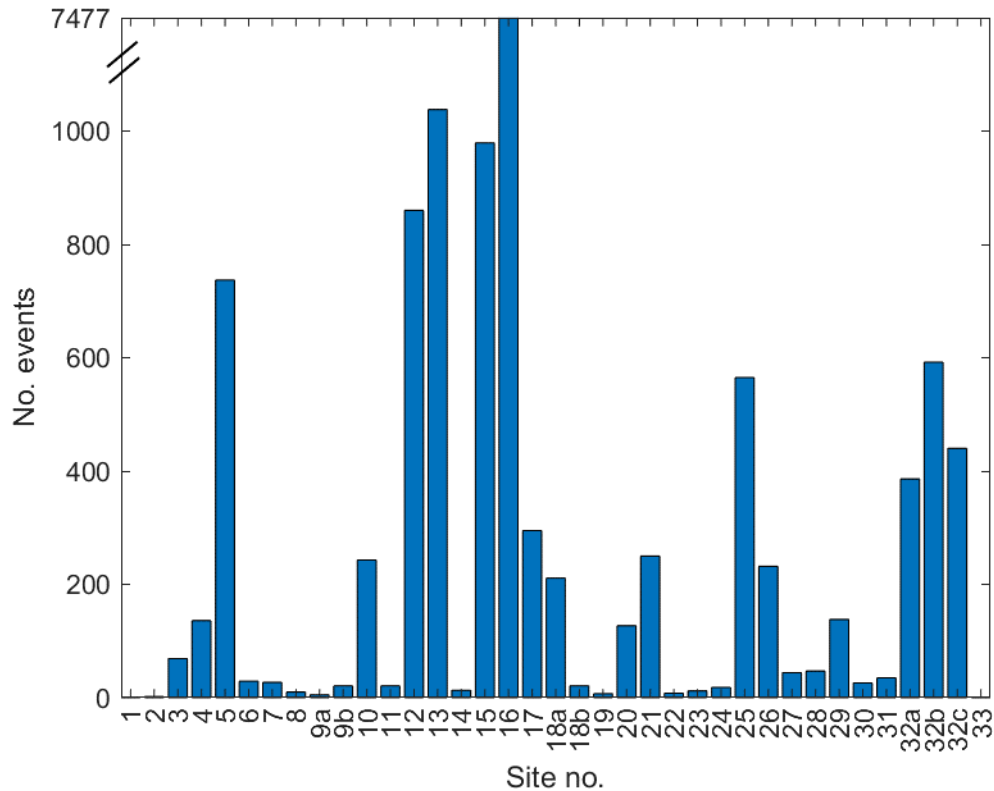
A stronger correlation between detected events and human activity can be seen in Figure 3-7, which shows the distribution of detected events over the hour of the day in local time. From the median number of events in the figure, it is seen that there are few or zero events per hour from midnight to early in the morning (around 5 a.m. to 7a.m). Largest median number of events per hour can be seen during business hours (9 a.m. to 5 p.m.) and from evening (6 p.m.) to midnight there is slow decay of the number of events per hour.



**Figure 3-7. Number of detected interference events distributed in the hour of the day. The central mark indicates the median, and the bottom and top edges of the box indicate the 25th and 75th percentiles, respectively. The whiskers extend to the most extreme data points not considered outliers, and the outliers are plotted individually using the '+' symbol and limited to 90 for scalability reasons.**

### 3.2.3 Site Analysis

The total number of detected events per site for the entire measurement campaign from December 2017 to the end of October 2018 varies a lot between the sites. It is seen in Figure 3-8 that the total number of events can be from less than 100 up to several thousands. Of course, the number of detected events depends on how long period each site was active, but it is not obviously the site with most events that is active for the longest period. Take as an example site no. 16, which has in total 7477 detected events but was only active for two months. Another example, site no. 6 was active for eleven months and reported 29 events during that time period. Which month each site was active in is seen in Figure 3-9 (NB remember that this information is not available from the STRIKE3 database at the moment. Information about when each site was active is from separate notes from NSL and FOI).



**Figure 3-8: Number of detected events per site during the measurement campaign.**

To exemplify the difference in number of detected events and when those events are detected, five different sites are selected. Three of them were active during the entire measurement period, one of them just two months and the last one almost the entire period. The sites are geographically spread from different countries in Europe to a country in Asia. The following will show detection statistics for those sites and highlight significant statistics for each site.

D6.2: Threat Database Analysis Report

Ref: STRIKE3\_D62\_DatabaseRep

Issue: 1.0

Date: 25.01.19



Figure 3-9: Active sites per month. An active site is marked with green whilst an inactive site is marked with red.

Site no. 13 was active during the entire measurement campaign and is located in a city centre. Figure 3-10 shows detection statistics for this site. From Figure 3-10 (a) it is seen that the number of events was almost constant for seven months in the beginning of the period. In July, the number of detected events was suddenly half as many, in August even less, and in the following month the number of events started to increase again. This phenomenon might be a correlation with the summer holidays in that area. During night time at this site, less interference events are detected, see the hourly distribution of events in Figure 3-10 (b). On Wednesdays and in the weekend there are less events compared to the other weekdays for this site, see the day of week distribution in Figure 3-10 (c).

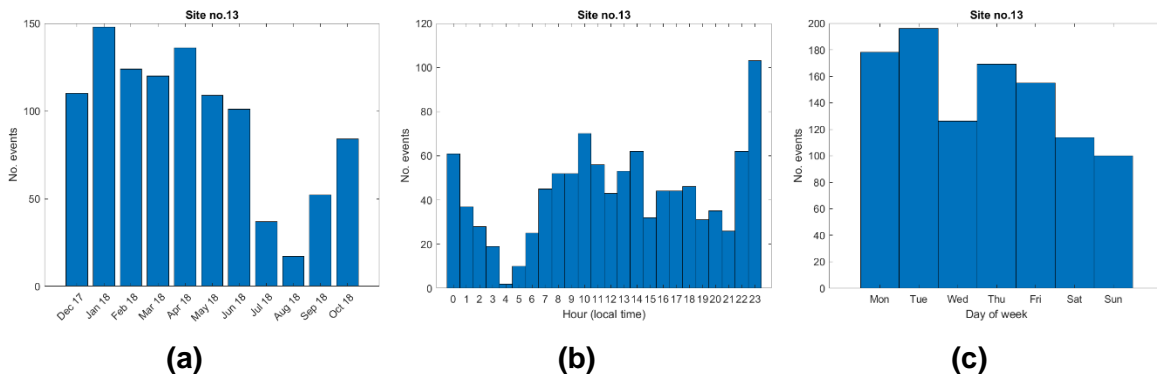


Figure 3-10: Detection statistics for site no. 13.

Another site that was active during the entire measurement campaign is site no. 5. This site is located along a motorway close to an airport. Figure 3-11 shows detection statistics for this site. It is seen in Figure 3-11 (a) that the number of events is almost constant for all months but not for January, February and March, where the number is less. In the morning there is a peak in the number of detected events, the number of events then decays to the evening and is low during the night, see Figure 3-11 (b). The day of week distribution of events is almost constant for all days but Wednesday, see Figure 3-11 (c).

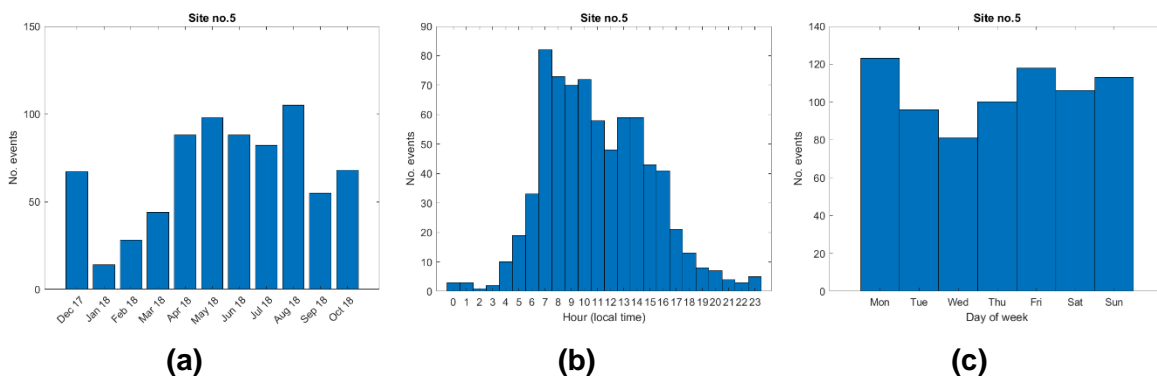


Figure 3-11: Detection statistics for site no. 5.

Near a city motorway site no. 12 is located. This site was active during the entire measurement campaign. In Figure 3-12 (a) it is seen that the number of events each month

is almost constant, but with a dip in August. For September and October there is an increasing trend in the number of events. This site has relatively many detected events during night time. The majority of events are though detected during daytime, see Figure 3-12 (b). Most of the events are detected during the weekdays and on Saturday and Sunday the numbers are much less, see Figure 3-12 (c).

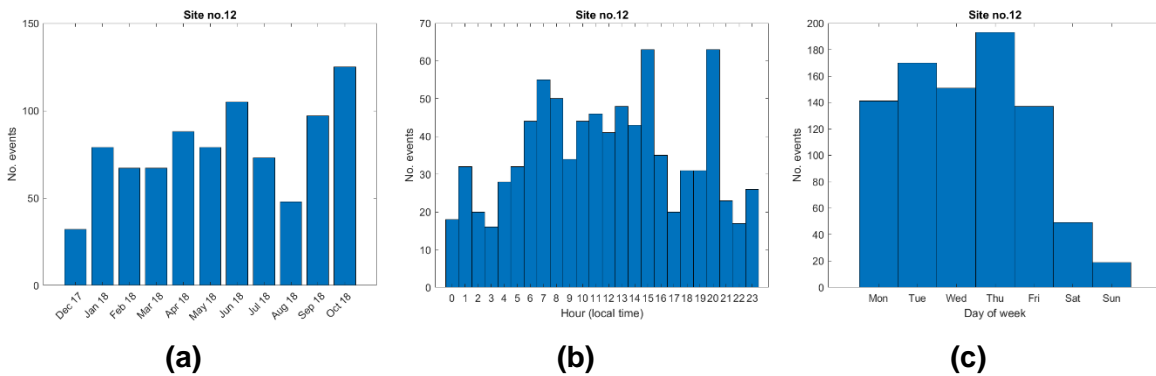


Figure 3-12: Detection statistics for site no. 12.

Site no. 16 is the site with the most detected interference events during the entire measurement campaign. This site was only active for two months, June and July, before the sensor was moved to another site. During these two months, 7477 events were detected at this site, see Figure 3-13 (a). The location of this site was at a city centre close to an airport. There are two peaks, one around morning (6 a.m. – 8 a.m.) and one around evening (5 p.m. – 7 p.m.), in the hourly distribution of events, see Figure 3-13 (b). This might be because there are more departure and arrival flights in the morning and evening in general at an airport, meaning a higher density of cars (with potential jammers) in the surrounding. The number of events distributed over day of week is seen in Figure 3-13 (c) and number of events each day of week is almost constant for this site.

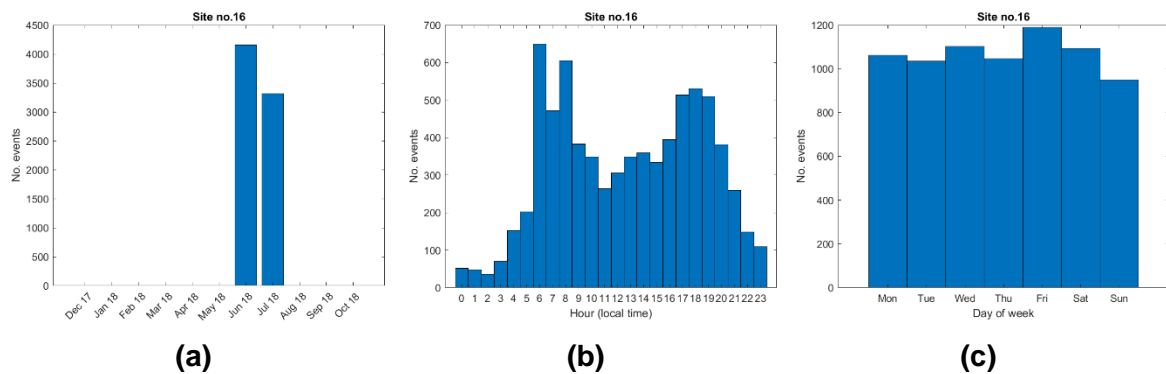


Figure 3-13: Detection statistics for site no. 16.

Another airport site is site no. 33a. In Figure 3-14 (a) it is seen that the number of detected events for each month has increased almost every month from the beginning until August



and then started to decrease until the end in October. The main bulk of the events are detected around evening (4 p.m. – 9 p.m.), but there are also many in-between the morning and noon, see Figure 3-14 (b). Wednesdays have approximately twice as many detected events compared with other weekdays, see Figure 3-14 (c). It is also seen in Figure 3-14 (c) that Saturday has least number of detected events.

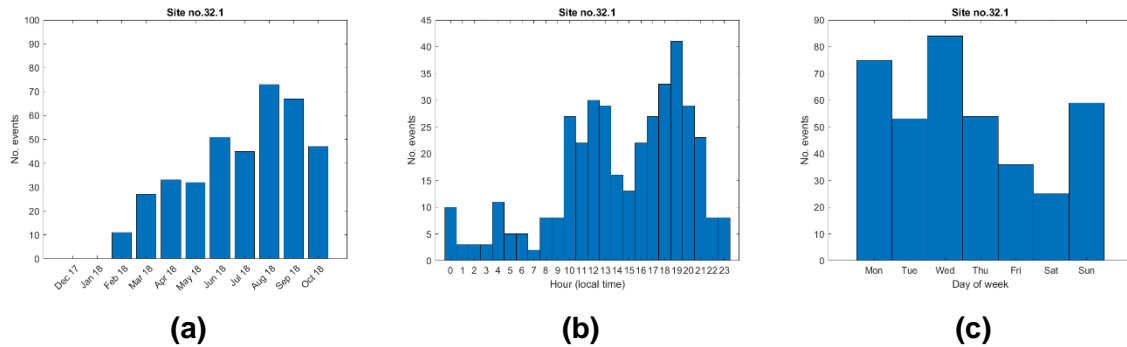


Figure 3-14: Detection statistics for site no. 33a.

### 3.3 Assessment of Standard Event Definitions and Thresholds

In this section, a selection of events are analysed in more detail to assess the defined event criteria and thresholds to determine if the current definitions are suitable to fulfil their objectives or if changes are required.

#### 3.3.1 Event type 'a'

Event type 'a' is applicable to monitoring equipment that detects interference based on power in the RF spectrum. This applies to both Detector and RF Oculus. The purpose of having a standard event definition is to try to ensure that different equipment will report the same events, and we will not have one set reporting far more events than the other.

Sites number 9a and 9b are co-located Detector and RF Oculus sensors respectively in a harbour area. Both sensors were set up in April 2018 but were disconnected for some weeks during June and July. The number of reported incidents is quite small at the current location, but there are enough events to make a decent comparison of the reported incidents between the two sensors. Figure 3-15 and Figure 3-16 show the number of reported interference events per month by the Detector and RF Oculus sensor respectively, and Table 3-1 show detailed information of each event.

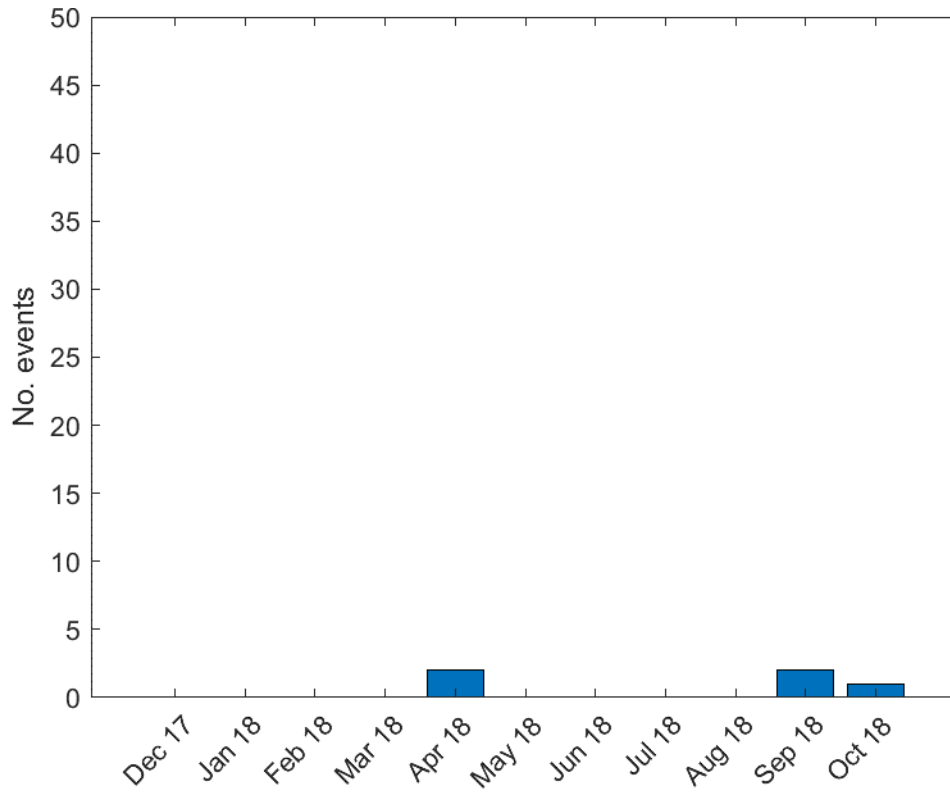
## D6.2: Threat Database Analysis Report

Ref: STRIKE3\_D62\_DatabaseRep

Issue: 1.0

Date: 25.01.19

---



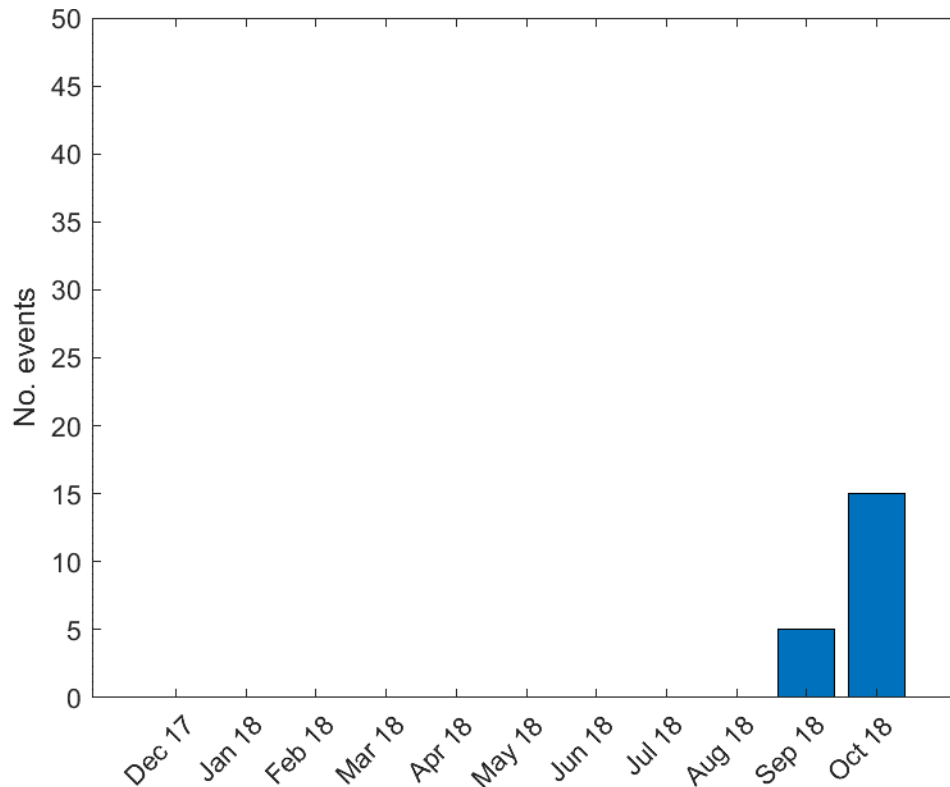
**Figure 3-15. Reported interference events by the Detector sensor.**

## D6.2: Threat Database Analysis Report

Ref: STRIKE3\_D62\_DatabaseRep

Issue: 1.0

Date: 25.01.19



**Figure 3-16: Reported interference events by the RF-Oculus sensor.**

Site ID	Equip.Type	Date	Time (UTC)	Duration (s)
9a	GSS100D	2018-04-24	18:30:34	6
9a	GSS100D	2018-04-24	18:30:54	8
9b	RF Oculus	2018-09-19	04:24:16	10
9b	RF Oculus	2018-09-19	04:24:29	264
9a	GSS100D	2018-09-19	04:24:45	10
9a	GSS100D	2018-09-19	04:25:58	8
9b	RF Oculus	2018-09-19	05:54:20	16
9b	RF Oculus	2018-09-24	18:41:16	16
9b	RF Oculus	2018-09-24	18:50:52	11
9b	RF Oculus	2018-10-02	17:30:56	32
9b	RF Oculus	2018-10-02	17:54:35	9
9b	RF Oculus	2018-10-02	17:54:55	6
9b	RF Oculus	2018-10-08	18:17:41	8
9b	RF Oculus	2018-10-08	19:15:42	16
9b	RF Oculus	2018-10-14	18:10:15	7
9b	RF Oculus	2018-10-14	18:10:25	7

## D6.2: Threat Database Analysis Report

Ref: STRIKE3\_D62\_DatabaseRep

Issue: 1.0

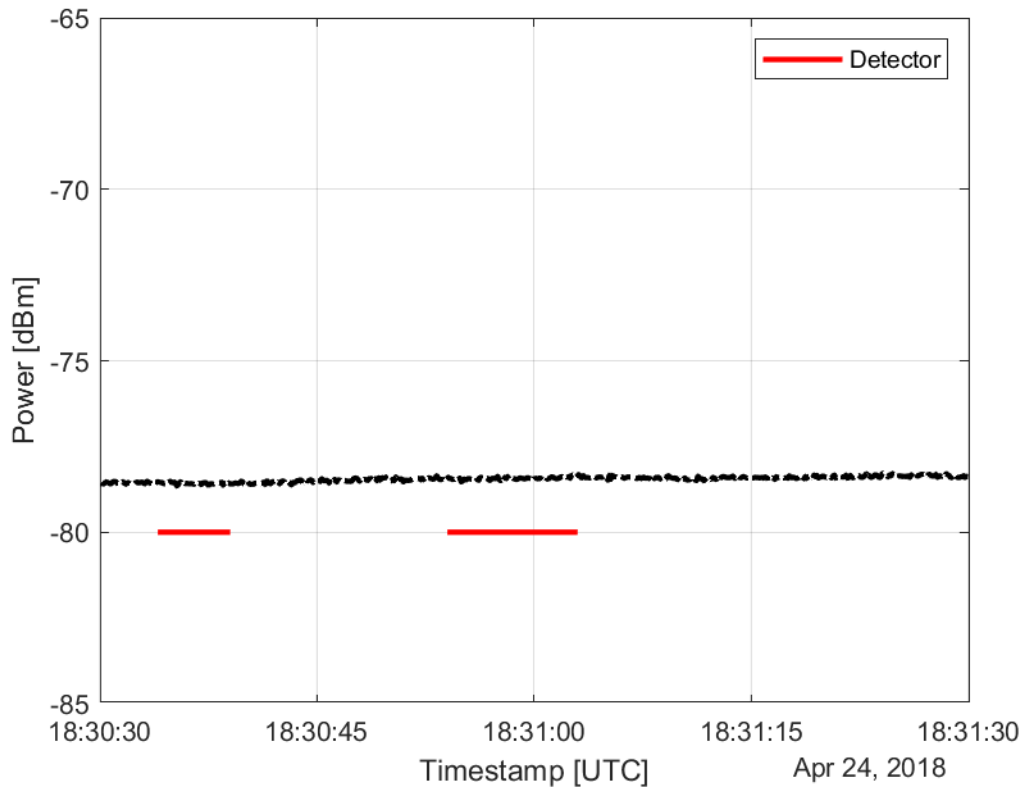
Date: 25.01.19

Site ID	Equip.Type	Date	Time (UTC)	Duration (s)
9b	RF Oculus	2018-10-14	18:03:12	12
9b	RF Oculus	2018-10-21	04:37:57	17
9b	RF Oculus	2018-10-23	17:39:31	6
9b	RF Oculus	2018-10-25	17:39:49	15
9b	RF Oculus	2018-10-25	17:41:07	14
9b	RF Oculus	2018-10-25	17:44:33	201
9b	RF Oculus	2018-10-25	19:03:33	153
9b	RF Oculus	2018-10-25	19:03:39	15
9a	GSS100D	2018-10-25	18:30:34	8

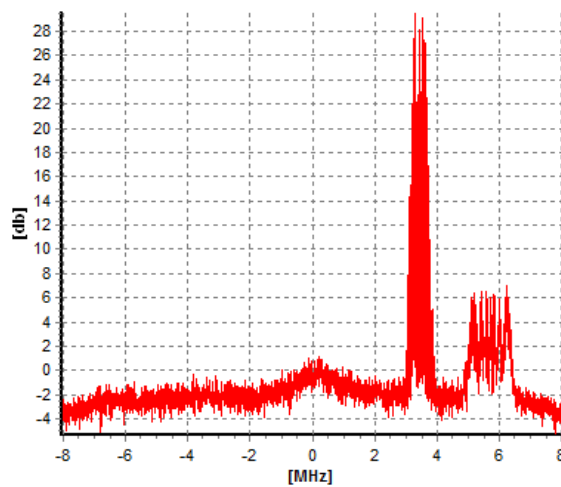
**Table 3-1: List of Reported interference events from the co-located sensors to the STRIKE3 database.**

From this list we can see that there is good agreement on some events, but there are also some occasions where one or other of the sensors reports an event but the other one does not. The main reason for this is likely to be the different monitoring bandwidths of RF Oculus and the GSS100D. The receiver bandwidth of the Detector is larger than that of the RF Oculus. This will affect the detection of interference incidents in a few different ways.

Firstly, interference events that occur outside of the received bandwidth of the RF Oculus, but within the received bandwidth of the Detector, can of course be reported by the Detector but not by the RF Oculus. An example of such an event is shown in Figure 3-17 and Figure 3-18. Figure 3-17 shows the power received by the RF Oculus (within its receiver bandwidth) and the interference events reported by the Detector. Figure 3-18 shows the frequency spectrum of the reported interference event. It is clear that the interference is outside of the 4 MHz bandwidth of the RF Oculus, but within the 16 MHz bandwidth of the Detector, which explains why the incident is reported by the Detector but not by the RF Oculus.



**Figure 3-17 Power received in RF Oculus, and reported incidents from the Detector node. The RF Oculus did not report any incident during this time interval. Example from April 24 2018.**



**Figure 3-18 Frequency spectrum of incident detected on April 24 2018. Interference occurs outside of RF Oculus received bandwidth but within the Detector received bandwidth.**

Secondly, the larger bandwidth of the Detector will affect the reporting threshold. The decision threshold is set, according to the standard, to be 5 dB above the receiver noise level. A larger bandwidth also gives a larger noise power within the received frequency band. That is, the decision threshold of the Detector system is in effect set higher than the decision threshold of the RF Oculus, according to the standard, since it has a larger measurement bandwidth. As a consequence, the RF Oculus reports interference incidents that are bandwidth limited to within the receiver bandwidth with slightly weaker power than the Detector. This is illustrated through the following figures.

Figure 3-19 shows the power received by the RF Oculus sensor, as well as the time duration of detected incidents by the two co-located sensor nodes during a six-minute time period on September 19. It is seen in the figure that the RF Oculus reported a 264 seconds long incident. During the same time interval, the Detector sensor reported two shorter incidents when the interference power increased significantly. This shows that for this particular interference event, the RF Oculus sensor reported an incident at a slightly lower interference power than the Detector sensor. This can be explained by the difference in receiver bandwidth.

Figure 3-20 shows the frequency spectrum of the interference incident as experienced by the Detector sensor. This particular interference signal is band limited to approximately 4 MHz, which is within the receiver bandwidth of the RF Oculus. That is, Figure 3-19 and Figure 3-20 confirm that the RF Oculus reports a rather narrow band interference signal at a lower power level, due to the smaller receiver bandwidth, than the Detector.

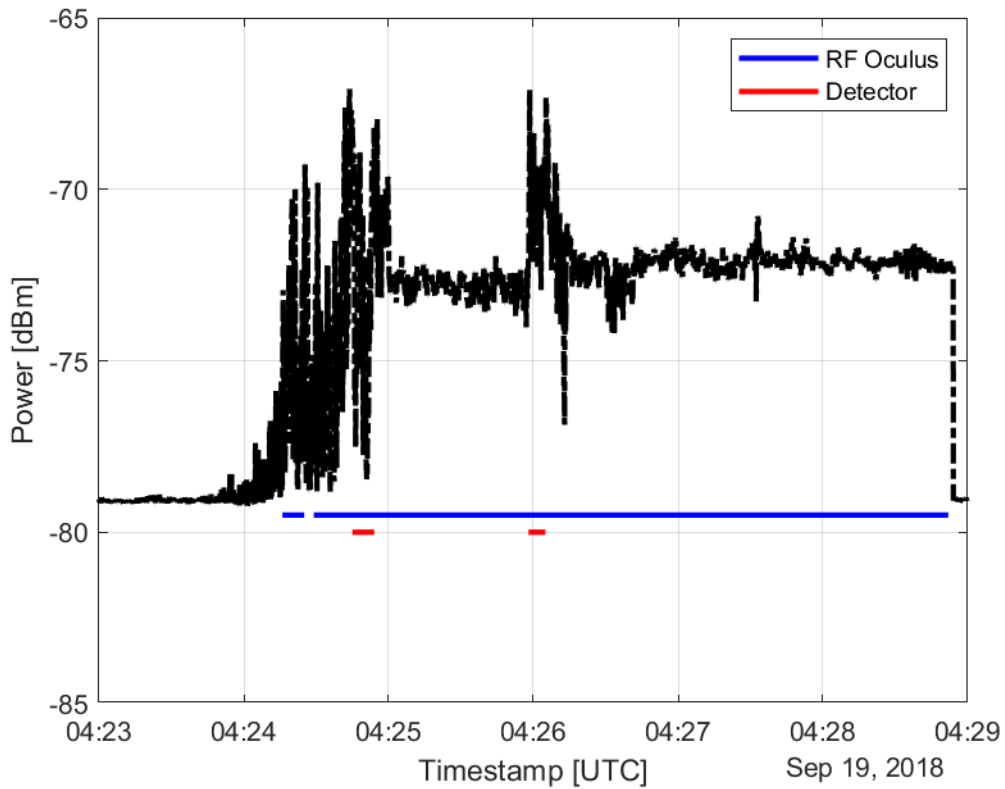


Figure 3-19 Power received in RF Oculus, and reported incidents from the two co-located nodes. Example from Sep. 19 2018.

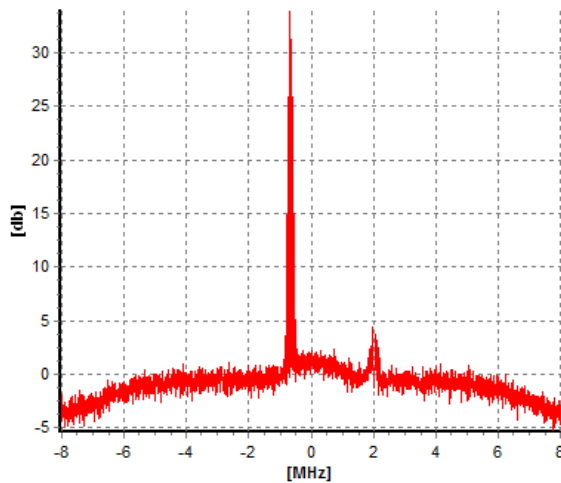


Figure 3-20 Frequency spectrum of incident detected on Sep 19 2018.

If we look at the raw Detector database (rather than the central database) we can see two

## D6.2: Threat Database Analysis Report

Ref: STRIKE3\_D62\_DatabaseRep

Issue: 1.0

Date: 25.01.19

main things. Firstly, that there are a lot of other low power events that are detected and not reported, which is one purpose of the standards (to filter out those that are low-level noise). Secondly, that all other the events reported by RF Oculus are also detected by the GSS100D but the apparent increase in power level is not high enough for the event to be reported. This demonstrates that the current event definition is a good first start to creating common event reporting, but perhaps a modification to the event 'a' criteria to take into account different bandwidths of equipment is necessary to get even better consistency in reporting.

Priority	Start Time	Duration (sec)	Class Type	Max Power
Low	28/10/2018 05:25	35	WHITE_OR_WB	2.5144
Low	27/10/2018 16:22	59	NB	2.8653
Medium	25/10/2018 19:01	197	VNB	4.6046
Low	25/10/2018 18:47	368	ST	2.2308
High	25/10/2018 17:39	489	ST	5.4304
Low	24/10/2018 04:17	32	WHITE_OR_WB	2.9881
Low	23/10/2018 04:39	54	VNB	2.1611
Low	23/10/2018 04:37	70	ST	2.5974
Medium	21/10/2018 18:43	127	VNB	4.7878
Medium	21/10/2018 18:02	219	VNB	3.7146
Medium	14/10/2018 18:09	99	VNB	3.9881
Medium	14/10/2018 15:31	412	WHITE_OR_WB	4.2521
Low	08/10/2018 19:17	441	ST	2.7536
High	08/10/2018 19:15	112	VNB	5.4666
Low	04/10/2018 16:21	65	NB	2.0412
Low	02/10/2018 17:58	100	ST	2.7911
Medium	02/10/2018 17:53	223	VNB	3.5173
Low	02/10/2018 17:53	14	VNB	2.4837
Low	02/10/2018 17:33	19	NB	2.1803
Medium	02/10/2018 17:30	102	NB	3.8028
Medium	24/09/2018 18:50	69	NB	3.7967
Low	24/09/2018 18:49	38	NB	2.0382
Medium	24/09/2018 18:41	40	VNB	4.0132
Low	19/09/2018 05:53	145	NB	2.5715
High	19/09/2018 04:24	296	VNB	5.2988
Low	18/09/2018 05:29	38	WHITE_OR_WB	2.3475
Low	18/09/2018 03:47	49	WHITE_OR_WB	2.4963
Medium	16/09/2018 18:18	24	CDMA	4.1372
Low	16/09/2018 17:52	34	WHITE_OR_WB	2.5421
Low	05/09/2018 06:11	50	WHITE_OR_WB	2.1066
Medium	31/08/2018 15:52	34	VNB	3.1295



## D6.2: Threat Database Analysis Report

Ref: STRIKE3\_D62\_DatabaseRep




Issue: 1.0

Date: 25.01.19

Priority	Start Time	Duration (sec)	Class Type	Max Power
High	25/08/2018 06:07	27	PULSEDCHIRPTRIANGULAR	3.1428
Medium	02/07/2018 04:39	40	WHITE_OR_WB	3.3621
Low	02/07/2018 04:39	22	WHITE_OR_WB	2.188
Low	01/07/2018 05:05	42	NB	2.1741
Low	07/06/2018 19:25	22	WHITE_OR_WB	2.0636
Low	07/06/2018 19:22	66	WHITE_OR_WB	2.7694
Medium	07/06/2018 18:51	40	WHITE_OR_WB	3.2066
Low	07/06/2018 04:25	34	SPECPERUNK	2.4873
Low	01/06/2018 18:57	221	WHITE_OR_WB	2.2865
Low	01/06/2018 18:54	56	WHITE_OR_WB	2.3069
Medium	01/06/2018 18:31	46	WHITE_OR_WB	4.4911
Medium	01/06/2018 04:40	40	WHITE_OR_WB	3.9643
Medium	30/05/2018 19:19	243	WHITE_OR_WB	3.3303
Low	30/05/2018 19:19	18	WHITE_OR_WB	2.0308
High	30/05/2018 18:33	53	WHITE_OR_WB	5.3165
Medium	30/05/2018 04:28	54	WHITE_OR_WB	3.1153
Medium	21/05/2018 20:24	42	WHITE_OR_WB	3.1202
Medium	17/05/2018 15:01	73	VNB	3.9065
Medium	17/05/2018 14:54	139	VNB	3.6231
Medium	17/05/2018 14:46	141	VNB	3.7067
Medium	17/05/2018 14:38	139	VNB	3.6027
Medium	17/05/2018 14:31	139	VNB	3.4817
Medium	17/05/2018 14:23	141	VNB	3.9014
Low	17/05/2018 14:15	142	VNB	2.5448
Low	03/05/2018 19:02	24	WHITE_OR_WB	2.292
Medium	03/05/2018 18:26	26	WHITE_OR_WB	3.3872
Low	03/05/2018 18:25	69	WHITE_OR_WB	2.3907
Medium	29/04/2018 18:52	46	NB	3.2395
High	26/04/2018 04:38	77	WHITE_OR_WB	6.6629
Low	26/04/2018 04:08	14	WHITE_OR_WB	2.0767
Low	24/04/2018 19:05	34	WHITE_OR_WB	2.5524
Medium	24/04/2018 19:03	77	WHITE_OR_WB	4.7479
Low	24/04/2018 18:31	44	WHITE_OR_WB	2.1394
High	24/04/2018 18:30	51	WHITE_OR_WB	6.4555
Low	24/04/2018 04:37	24	WHITE_OR_WB	2.6589
Low	22/04/2018 04:33	30	ST	2.1239
Low	20/04/2018 13:07	38	WHITE_OR_WB	2.0061
Medium	16/04/2018 04:39	46	WHITE_OR_WB	4.4835

Priority	Start Time	Duration (sec)	Class Type	Max Power
High	10/04/2018 04:45	44	WHITE_OR_WB	6.2532
Low	10/04/2018 04:45	26	WHITE_OR_WB	2.1187
Medium	06/04/2018 18:30	63	SPECPERUNK	3.6367

**Table 3-2: List of Events Detected by GSS100D at site 9a during Monitoring Period**

	Reported by both GSS100D and RF Oculus
	Reported by GSS100D only
	Reported by RF Oculus only

### 3.3.2 Event Type 'b'

Event type 'b' is applicable to COTS GNSS equipment that reports C/N0 measurements, either in raw observation data (e.g. RINEX files) or NMEA messages. The intention is that this will allow normal GNSS receivers (of which there are many more than dedicated RFI monitoring equipment) to detect and report interference events.

The current definition in the reporting standards [RD.1] is if the measured C/N0 for all satellites in view is 6 dB less than the expected C/N0 and if the duration is greater than 10 seconds, then an interference event should be reported. Where:

- the expected C/N0 is the value that would be expected when there is no interference signal present at the input of the equipment,
- the event duration is the difference between the start and end times of an event
- the start time of the event is the time at which the drop in C/N0 for all satellites in view first exceeds the 6 dB threshold
- the end time of the event is the time at which at the C/N0 for at least one of the satellites in view increases above the detection threshold and stays above the threshold for the following 10 seconds

For this analysis, five days of RINEX data from January 2018 has been analysed to find out whether any type 'b' interference events occurred. The expected C/N0 is taken as the measured average C/N0 for 1 minute before the event was triggered.

Using the above definition as the reference C/N0, and applying the definition for event type b, the following were the events detected.

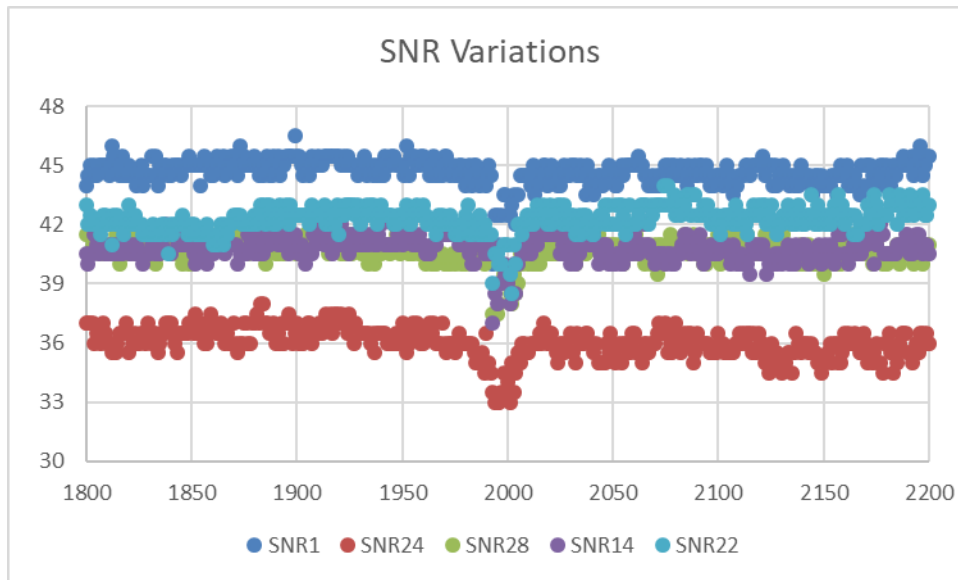
1. Jan 2<sup>nd</sup>, 2018 starting around 5:33:13 – 7 satellites are experiencing a 3-5dB dip in SNR, while 4 satellites dropped out of tracking for 1s (at least they were not reported). This did not quite meet the criteria for reporting but did show a possible event.

## D6.2: Threat Database Analysis Report

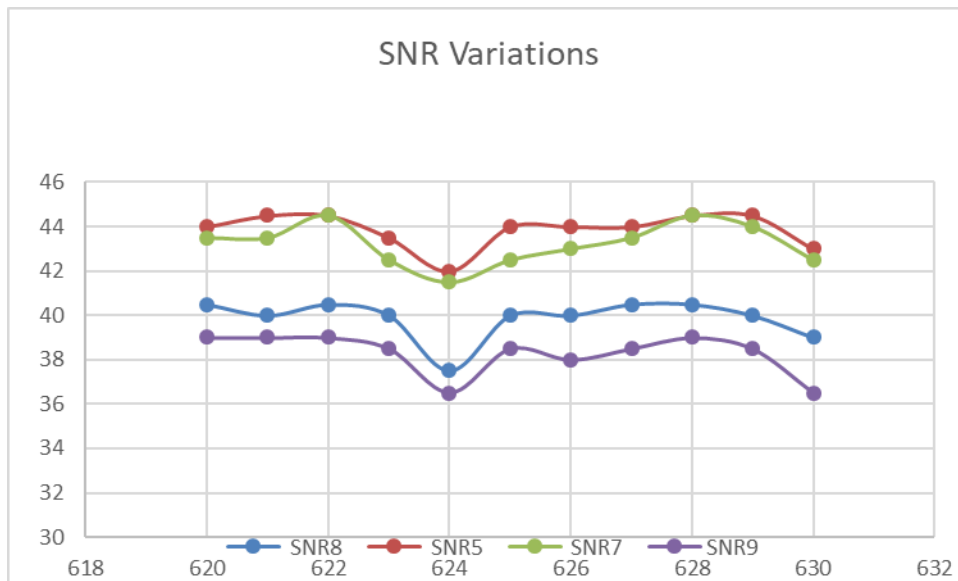
Ref: STRIKE3\_D62\_DatabaseRep

Issue: 1.0

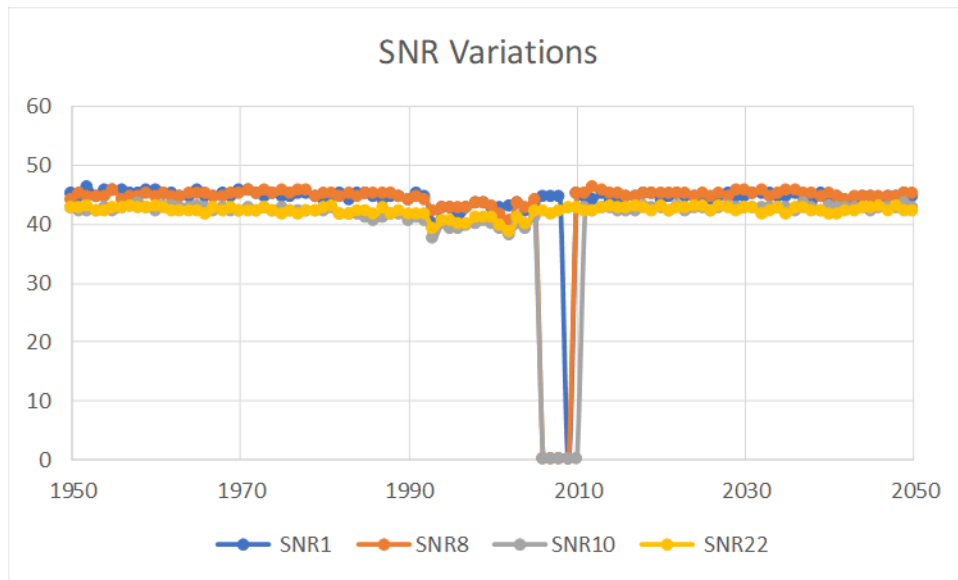
Date: 25.01.19



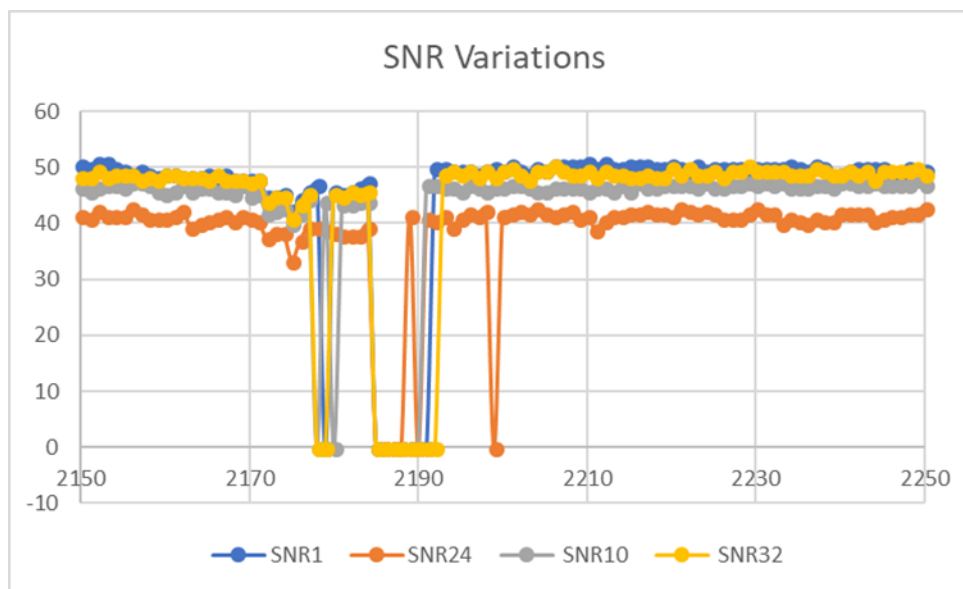
2. Jan 2<sup>nd</sup>, 2018 at 14:10:24 all satellites have a 1-2dB dip for 1s. Again, this did not quite meet the criteria for reporting but did show a possible event.



3. Jan 2<sup>nd</sup>, 2018, starting around 15:04:38 satellites start to fail in track and around 15:04:45 number of satellites are reduced to 3. Though the SNR dip is only around 4-5dB for those satellites that remain in track this is a major event as other satellites are not recovered for almost 7s.



4. Jan 3<sup>rd</sup> 2018, starting around 05:36:15 an event happens that results in 8 satellites losing lock at 05:36:19, recovering to 12 satellites by 05:36:21. A couple of seconds later, there seems to be another (or probably continuation of the same) event that results in no satellites being tracked for 3s from 05:36:26. Full recovery happens after 05:36:33.



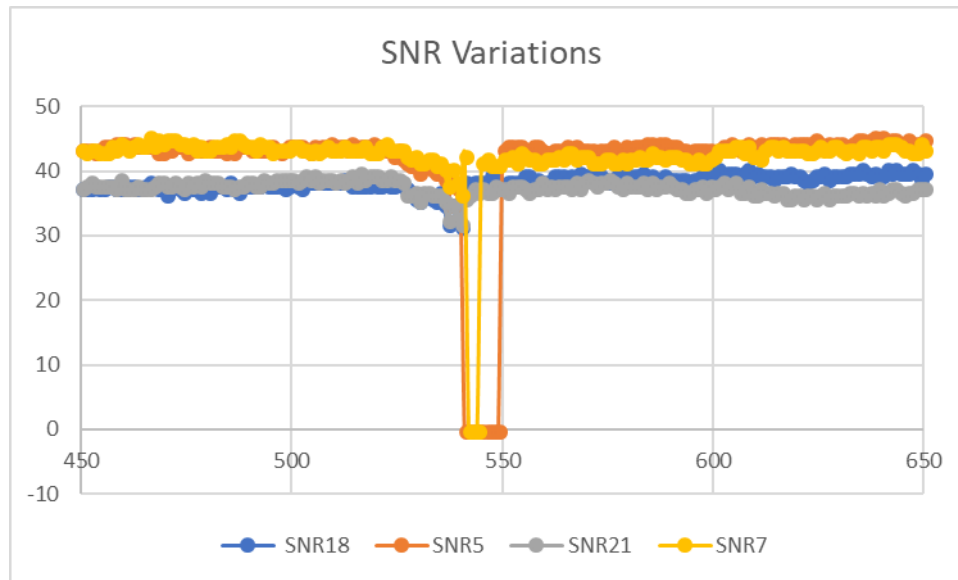
## D6.2: Threat Database Analysis Report

Ref: STRIKE3\_D62\_DatabaseRep

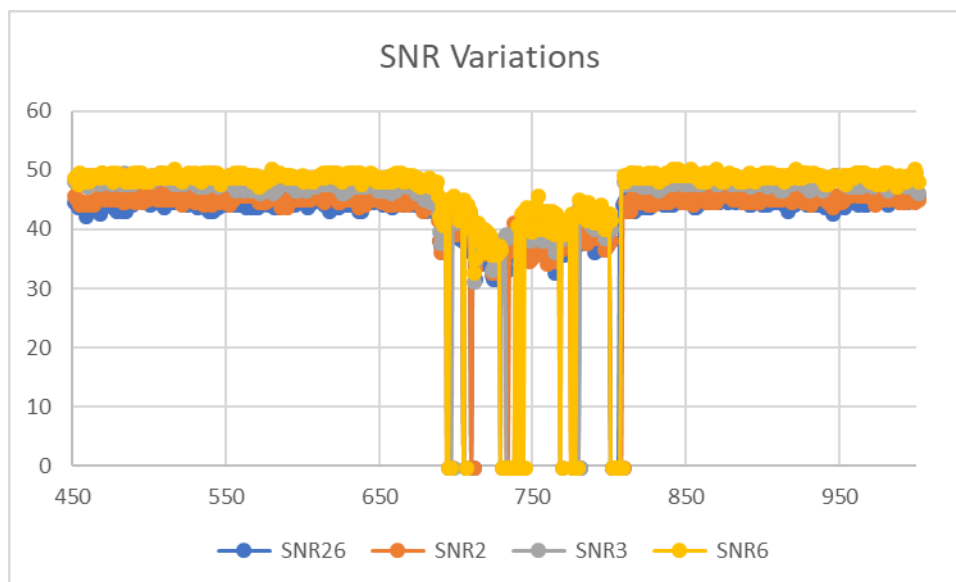
Issue: 1.0

Date: 25.01.19

5. Jan 3<sup>rd</sup>, 2018 starting around 15:08:58 an event started to affect the tracking resulting in the number of satellites being tracked reduced to just 3 at 15:09:04. The event appears to have subsided after around 15:09:10.



6. 5<sup>th</sup> Jan 2018 starting around 10:11:34 an event is seen which lasts for more than 100s. Satellites are continuously losing lock and tracking with a lower SNR. This would have triggered the event type 'b' criteria for reporting.



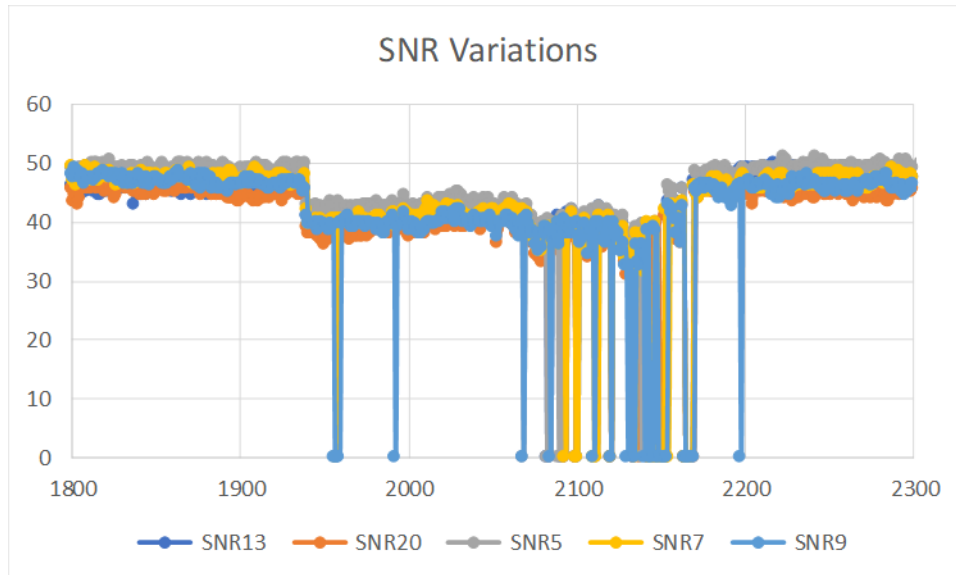
## D6.2: Threat Database Analysis Report

Ref: STRIKE3\_D62\_DatabaseRep

Issue: 1.0

Date: 25.01.19

7. 5<sup>th</sup> Jan 2018 starting around 13:32:30 an event starts that continues for almost 4min. SV's are dropped from tracking and less than expected C/N0 is reported. This would have triggered the event type 'b' criteria for reporting.



As this analysis showed some potential events, it was decided to proceed with the installation of the RF Oculus and then a more detailed comparison of the consistency of reports from RF Oculus and CORS data could be carried out. A full list of the events detected by RF Oculus at this site following installation are provided in the following table.

id	duration (ms)	start date (UTC)	start time (UTC)	stop date (UTC)	stop time (UTC)
1	101	14/07/2018	17:25:20.898	14/07/2018	17:25:20.999
2	201	29/07/2018	08:15:59.694	29/07/2018	08:15:59.895
3	101	29/07/2018	13:22:38.124	29/07/2018	13:22:38.225
4	100	29/07/2018	13:25:11.734	29/07/2018	13:25:11.834
5	101	29/07/2018	13:37:31.057	29/07/2018	13:37:31.158
6	101	29/07/2018	13:47:45.599	29/07/2018	13:47:45.700
7	100	29/07/2018	14:25:15.465	29/07/2018	14:25:15.565
8	101	04/08/2018	02:34:46.977	04/08/2018	02:34:47.078
9	101	05/08/2018	10:12:50.613	05/08/2018	10:12:50.714
10	201	05/08/2018	10:18:29.791	05/08/2018	10:18:29.992
11	201	05/08/2018	10:20:05.828	05/08/2018	10:20:06.029
12	502	05/08/2018	10:21:18.018	05/08/2018	10:21:18.520
13	101	05/08/2018	10:23:48.540	05/08/2018	10:23:48.641

## D6.2: Threat Database Analysis Report

Ref: STRIKE3\_D62\_DatabaseRep

Issue: 1.0

Date: 25.01.19

id	duration (ms)	start date (UTC)	start time (UTC)	stop date (UTC)	stop time (UTC)
14	100	05/08/2018	10:26:18.817	05/08/2018	10:26:18.917
15	101	05/08/2018	10:29:01.619	05/08/2018	10:29:01.720
16	101	10/08/2018	06:29:01.562	10/08/2018	06:29:01.663
17	101	10/08/2018	06:30:34.079	10/08/2018	06:30:34.180
18	101	10/08/2018	06:37:33.612	10/08/2018	06:37:33.713
19	101	12/08/2018	03:52:45.163	12/08/2018	03:52:45.264
20	2206	14/08/2018	07:57:13.977	14/08/2018	07:57:16.183
21	3710	17/08/2018	16:56:37.373	17/08/2018	16:56:41.083
22	3811	17/08/2018	16:56:56.971	17/08/2018	16:57:00.782
23	1806	17/08/2018	17:03:54.508	17/08/2018	17:03:56.314
24	2108	17/08/2018	17:04:21.114	17/08/2018	17:04:23.222
25	100	18/08/2018	08:48:41.372	18/08/2018	08:48:41.472
26	4111	18/08/2018	08:48:54.126	18/08/2018	08:48:58.237
27	201	23/08/2018	20:00:16.104	23/08/2018	20:00:16.305
28	101	23/08/2018	20:02:43.872	23/08/2018	20:02:43.973
29	101	23/08/2018	21:56:43.634	23/08/2018	21:56:43.735
30	101	26/08/2018	14:38:12.887	26/08/2018	14:38:12.988
31	101	05/09/2018	15:29:24.103	05/09/2018	15:29:24.204
32	101	08/09/2018	14:03:55.741	08/09/2018	14:03:55.842
33	101	20/09/2018	12:11:02.159	20/09/2018	12:11:02.260
34	101	02/10/2018	04:38:59.769	02/10/2018	04:38:59.870
35	2408	02/10/2018	04:46:10.122	02/10/2018	04:46:12.530
36	101	03/10/2018	13:14:37.065	03/10/2018	13:14:37.166
37	5315	04/10/2018	05:28:12.489	04/10/2018	05:28:17.804
38	101	04/10/2018	05:28:28.555	04/10/2018	05:28:28.656
39	1004	07/10/2018	10:31:58.310	07/10/2018	10:31:59.314
40	124	14/10/2018	09:30:47.121	14/10/2018	09:30:47.245
43	101	30/10/2018	06:53:40.974	30/10/2018	06:53:41.075
41	2308	27/10/2018	08:51:00.923	27/10/2018	08:51:03.231
42	702	27/10/2018	17:12:08.406	27/10/2018	17:12:09.108

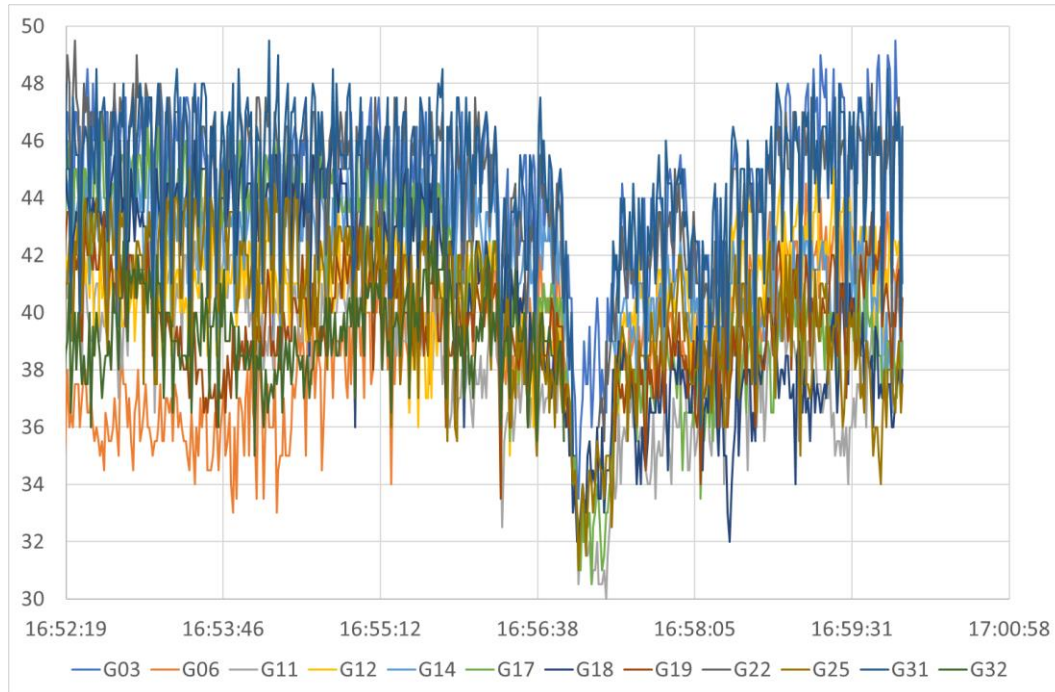
**Table 3-3: List of RF Oculus Events at Monitoring Site**

The first thing to note is that there are not many events, with only 42 detections in over 3 months. Also, the vast majority are very short and in fact there are only 10 events that last longer than 1 second, and only one that lasts for longer than 5 seconds (which is the trigger for reporting for event type 'a').

In this case the RF Oculus and the CORS receiver are not exactly co-located – they do not

share the same antenna – and so there may not be an exact match up of events. Nevertheless, as they are very close by, we should expect to see that strong RFI events detected by RF Oculus also can be seen in the SNR values at the CORS receiver.

One such example to look at is 17/08/18 where two events just before 17:00 are detected by RF Oculus. The plot below shows the SNR values at the CORS receiver for the same time period.



**Figure 3-21: SNR Values at CORS Receiver close to RF Oculus Equipment on 17/08/18**

It can be seen that there is a clear drop in the SNR values on all satellites corresponding with the second of the events. The drop also seems to last for longer than the 3 seconds indicated by RF Oculus. It is possible this is because the receiver takes some time to recover after the interference event. However, it can also be seen that although the drop is significant it would probably not trigger the threshold because the SNR values are quite noisy before and after the interference and so it is more difficult to be certain this is a real drop.

Other potential events showed the same behaviour with some drop in SNR corresponding to the RFI events, but the generally noisy SNR values making it more difficult to differentiate true events from general noise in SNR values.

### 3.3.3 Multiple Events

Figure 3-19 show that both the RF Oculus and the Detector sensor reported two events each, during slightly different time intervals, of what is most likely an interference event coming from the same source. One might argue that it would be more reasonable if both



sensor nodes had reported this as a single, long duration, event. However, for a type 'a' event this ambiguity would always occur, only that the exact occurrences depend on what power level the decision threshold is set. As set by the standard definitions, both types of sensor have been shown to detect an interference incident at such a low power level that a co-located GNSS receiver is still unaffected. Therefore, the event definitions are reasonable.

The only way to refine the event definitions in such a way that the sensors would report, for example, the incident shown in Figure 3-19 as a single long duration event would be to require some sort of signal analysis to see if the waveform of the interference is actually the same during this time interval. Such requirement would be an unreasonable extension for both types 'a' and 'b' event definitions and is rather something that could be done in post-processing of reported events if necessary.

### 3.3.4 Other Considerations

We became aware that some information about sites may be missing for each event in the STRIKE3 database when we did the statistical analysis of the collected events. With the message contents, as is, it is only possible to do analysis on country basis. There is neither no information about how many sites there are per country, which might result in statistics showing that a country has many events just because it was many sites in that specific country. However, it is possible to extract a 'probe Id' from the reported 'event Id', which tells which sensor equipment that detected the event. This is useful as long as no sensor is moved to another site. Therefore, we propose that information about a site is added to the STRIKE3 database and that every reported event is connected to a site.

Another experience from the analysis of the data in the STRIKE3 database has to do with the numbers of reported events per month for a specific site or sensor. If there are no reported events for a given month, what is the reason for that? Were there no events or was the sensor or site inactive that particular month? This is crucial information to be able to make the right conclusions. If there were no events and the site was active during the entire month, this means that there were no jamming events in that area. But if the site was inactive the entire month, there could have been many jamming events in that area, which never was reported to the database. The statistics would in that case show that there were no jamming events, if the information about site activity is not available. Therefore, we propose that information about site activity is added to the database. In the conducted measurement campaign each partner kept notes about when their sites were active or not. Therefore, it was possible to do the overview analysis of the collected data.

With regards event type 'a', we see some differences in the events that are reported due to the fact that the different bandwidths of the equipment create in effect different power levels for the same event. Therefore, the event definition criteria could be modified slightly to take account of the bandwidth so that the power level thresholds are more consistent.

Finally, with regards event type 'b', we see some difficulties differentiating real events when the reference SNR values are noisy. Perhaps this may limit the sites and equipment that can reliably be used.

## 4 Detailed Database Analysis

### 4.1 Introduction

The previous section has shown the results from the STRIKE3 central database where the standardised reports from the monitoring network are maintained. This shows the sort of analysis that would be possible using only the information that is included in the standard messages.

For other users, more detailed analysis and specific investigations may be necessary that require additional information over and above the information in the standard reports. As well as the STRIKE3 central database, a Detector specific database is also maintained that includes all events report by the Detector probes (even those events that do not meet the standard event criteria) and include additional information about the signals. This section therefore contains an analysis considering all events reported by the Detector probes. This is presented both for the long-term monitoring period in WP6 (and consistent with the analysis in section 3), as well as for any sites that have been monitored throughout the entire STRIKE3 project duration since 1<sup>st</sup> February 2016.

### 4.2 Long-Term Validation Period (01/12/17 to 31/10/18)

#### 4.2.1 Overview of Activity in Long-Term Monitoring Period

Over the long-term monitoring period a total of 232,973 events were detected by the Detector probes. This is a very high number of events and is far higher than the 15,200 events that met the event criteria in the reporting standards and were reported to the central STRIKE3 database. This apparent discrepancy is explained when we look at the breakdown of the signals in Figure 4-1.

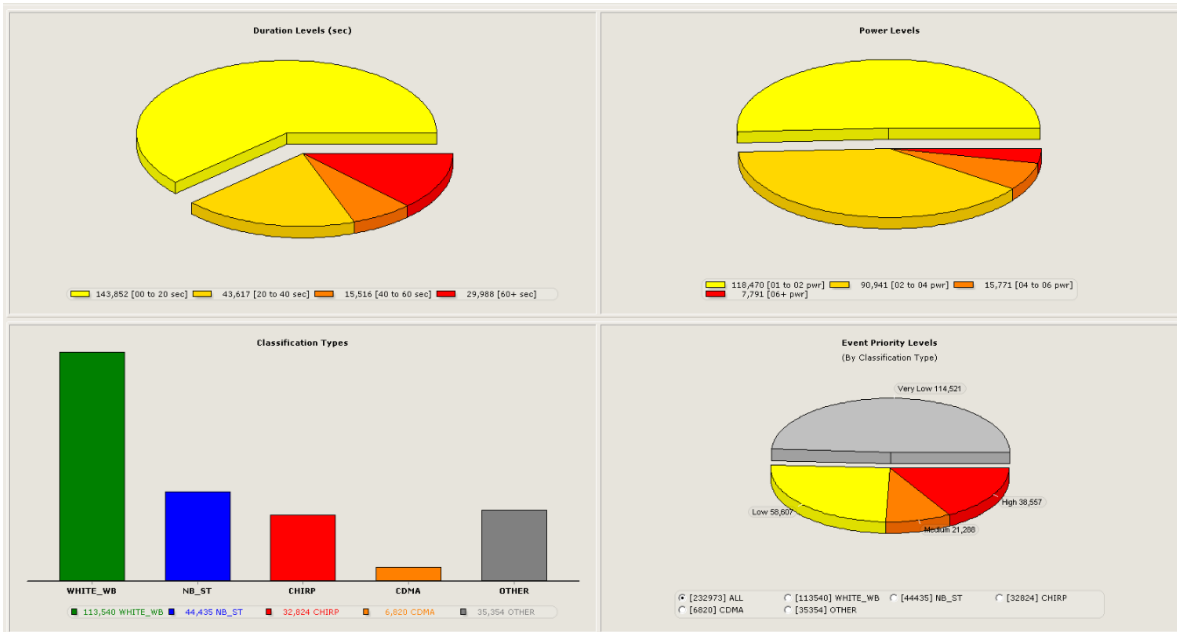


Figure 4-1: Overview of data from long-term monitoring period

Considering the overall results for this period, it can be seen that at least half of the events are short duration and are detected with low power levels – mostly these are classified as white noise and are given very low priority as they have no noticeable impact on the GPS tracking and position positioning calculations. Hence they do not meet the criteria for reporting and so are not sent to the central STRIKE3 database. Again, this is a validation that the event criteria that have been defined are doing their job in terms of filtering out as many of these low priority events as possible.

The next largest category of signal types, narrow band signals, are a bit more interesting as they can arise from other equipment unintentionally interfering with local receivers. Unlike the white noise the narrow band signals have a much more diverse range of priorities and more than 10% of the NB signals have high enough power levels to be deemed high priority.

The third category of signal to consider are chirp type signals. These are intentionally generated and are typical of in-vehicle jammers. In the right conditions they can jam all signals needed to calculate a unit’s position. These signals make up nearly 33,000 events, which is about 11% of the total number of events, which is a significant number but shows that unintentional interference events are far more common.

As well as the types of signal present, it is useful to consider at what time of day these events occur. From Figure 4-2 we see that the number of events rises throughout the times of peak human activity. This would suggest that the signals are generated by equipment operational only when people are awake. There also seem to be a larger number of intentional signals generated in the early morning than late at night. The proportion of intentional to unintentional events stays fairly consistent throughout the day however, which is interesting.

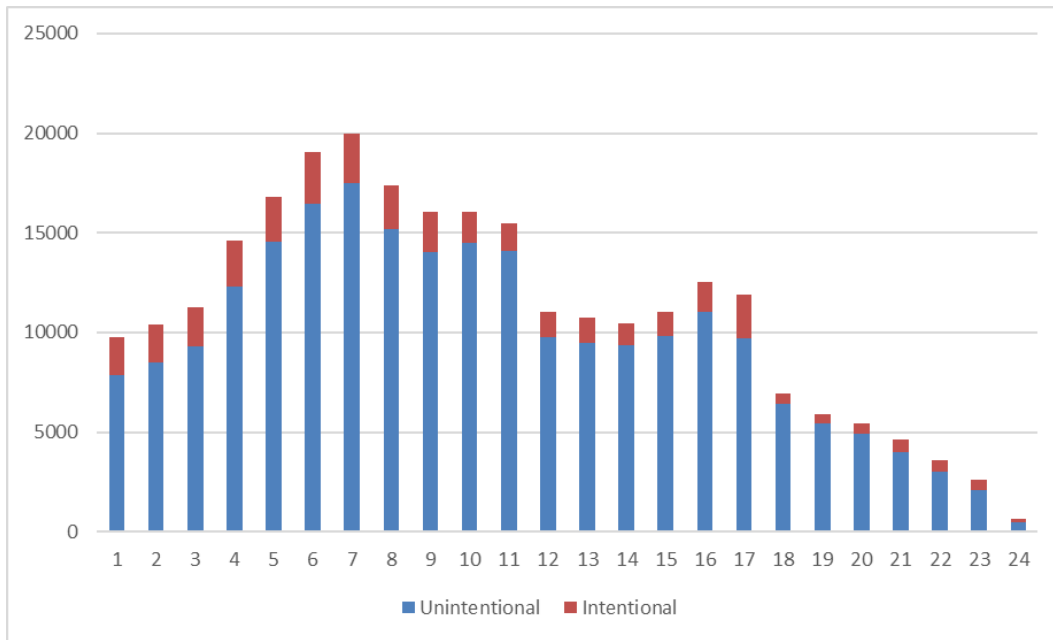


Figure 4-2: Time distribution of events for long-term monitoring throughout the day

#### 4.2.2 Comparison of Site Activity in Long-Term Monitoring Period

The previous section shows combined results considering all sites together during the monitoring period. However, the sites themselves are not the same and so some further analysis looking at individual site activity is presented.

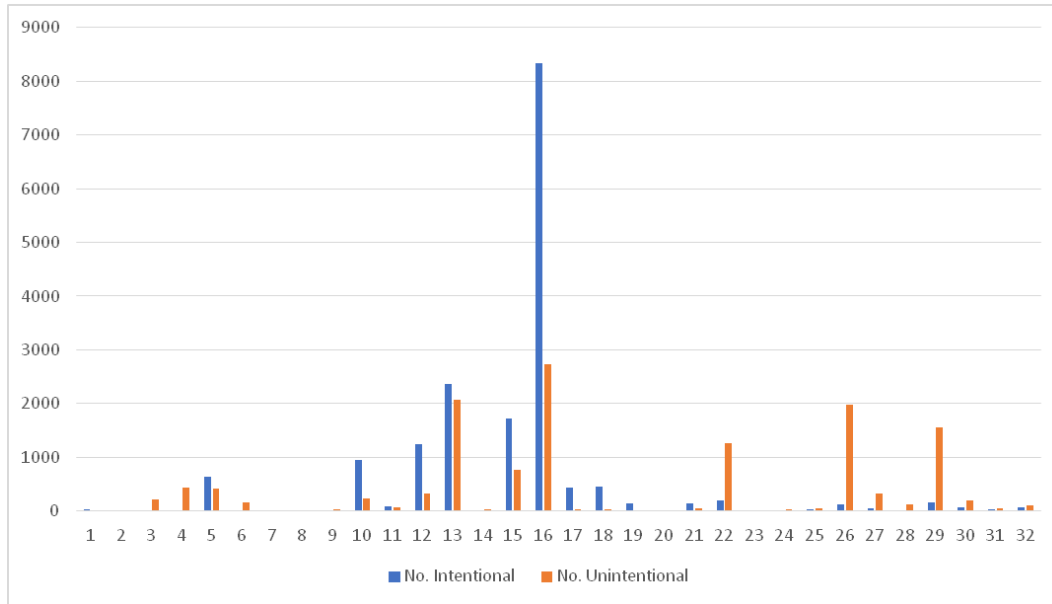
**Error! Reference source not found.** below shows the total number of detected events above a power level of 3.5 and the proportions of intentional to unintentional events for each site. This helps to identify those sites that have contributed a lot of events to the database and what sort of events are seen at those sites. Note that a power level of 3.5 is used because below that level it is difficult to properly characterise events as intentional (chirp) or unintentional (non-chirp).

## D6.2: Threat Database Analysis Report

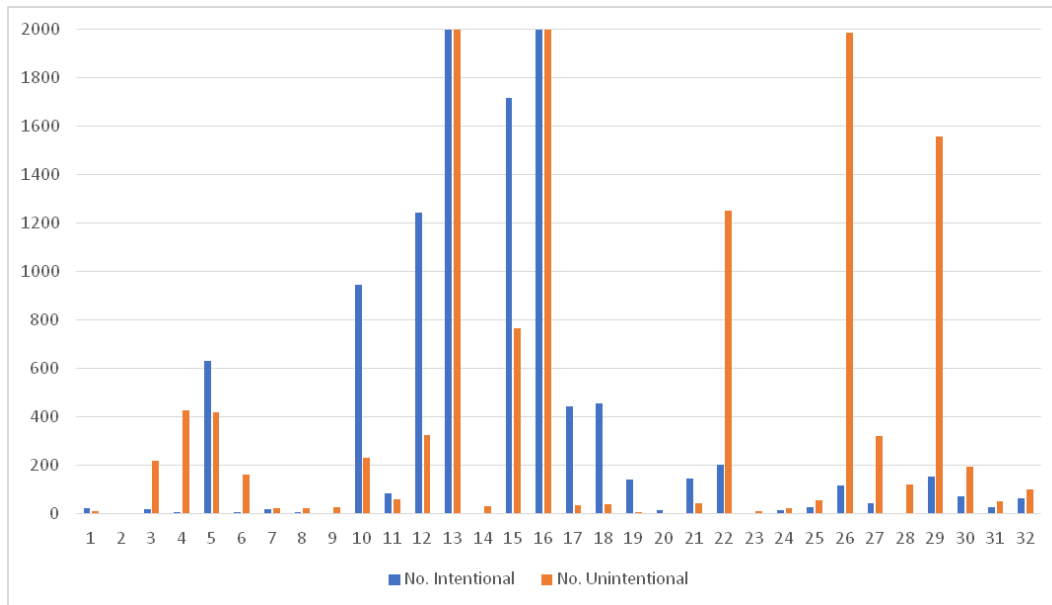
Ref: STRIKE3\_D62\_DatabaseRep

Issue: 1.0

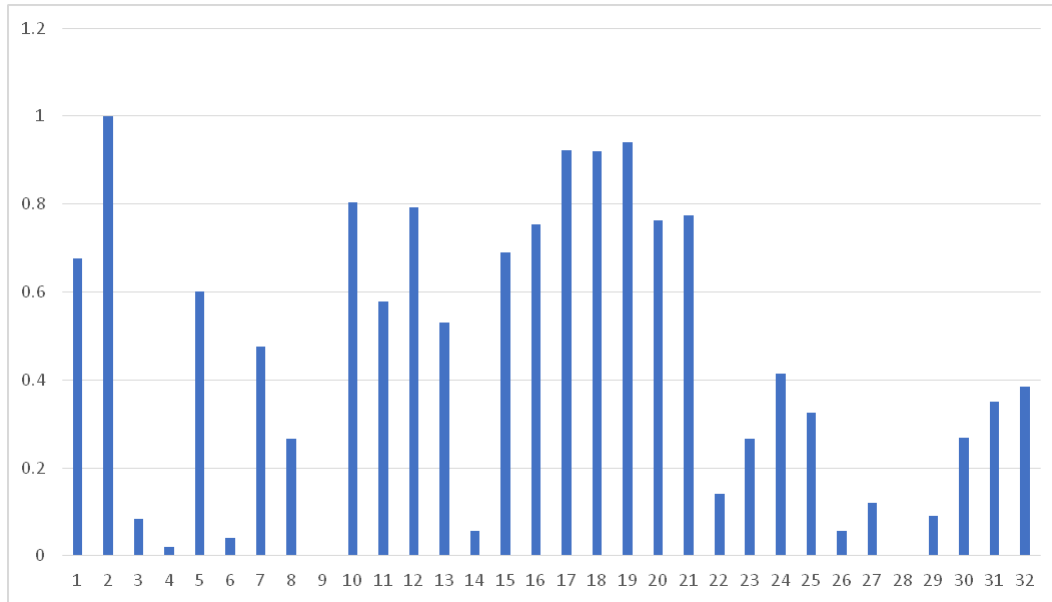
Date: 25.01.19



(a)



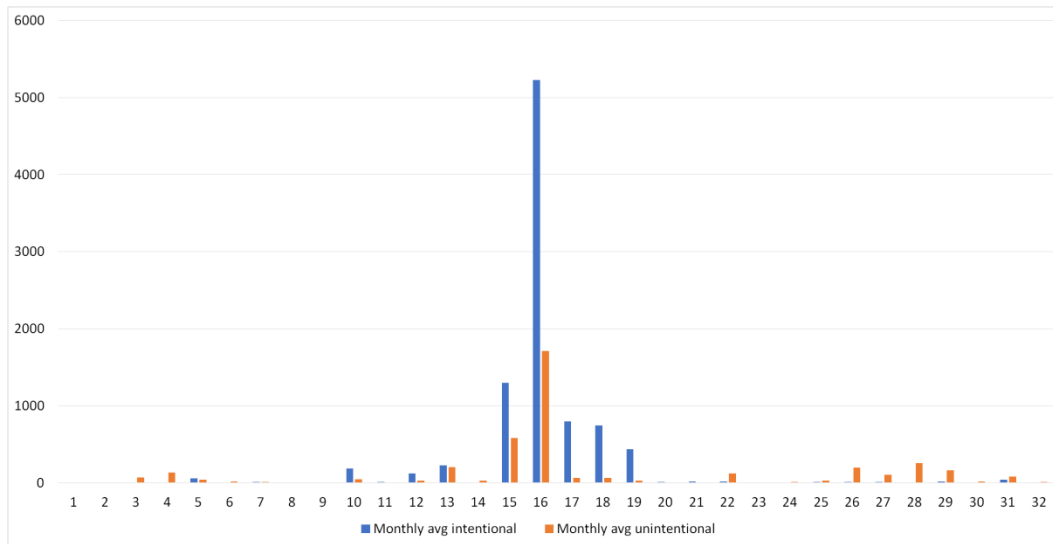
(b)



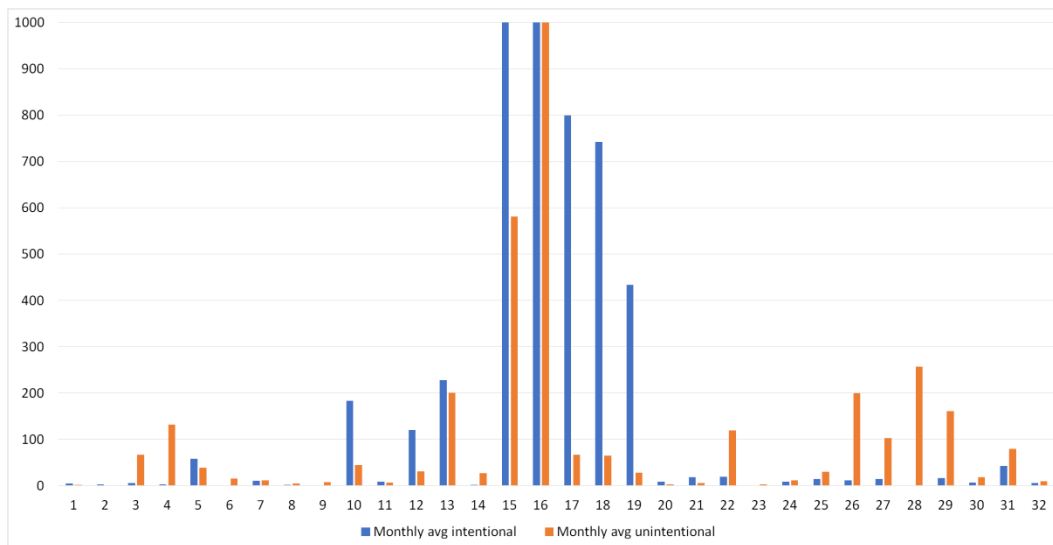
(c)

**Figure 4-3: (a) Total number of events with normalised power over 3.5 for each DETECTOR site active during WP6; (b) Total number of events with normalised power over 3.5 for each DETECTOR site active during WP6 – reduced axis; (c) No. of intentional events divided by total no. of total events.**

It can be seen from the figures that every site has some interference – none are entirely clean – but there is a huge difference in the numbers of events detected at each site, with some have very few at that power level and others have many thousands. However, as the sites have been active for different lengths of time the total number of events does not always give a true reflection of activity. Therefore Figure 4-4 below shows these numbers but divided by the number of active months (accounting for any equipment outages) in order to obtain normalised figures defined as monthly average number of events.



(a)



(b)

**Figure 4-4: Monthly average no. of events for each DETECTOR site in WP6. (a) shows the full range and in (b) the y-axis has been truncated to show more detail for lower activity sites**

From the results we can see that site 16 is by far the most active in terms of intentional events, with sites 15, 17, 18 and 19 also showing very high levels of activity.

After that the most active for intentional events are 10, 12 and 13 with then a drop down to sites 5 and 31.

Looking at Table 2-3 where the sites used are described, it can be seen that the most active sites are city centre and city motorway locations. Perhaps surprisingly motorway locations

## D6.2: Threat Database Analysis Report

**Ref:** STRIKE3\_D62\_DatabaseRep

**Issue:** 1.0

**Date:** 25.01.19

---

are not so active in terms of intentional events, but that maybe due to the different type of traffic, and the different traffic patterns – as cities and urban motorways will get many repeated journeys on the same day and from day to day.

In terms of unintentional interference, some of the city centre locations also have high numbers of events but there are some differences on the next level down. Sites such as 3, 4 and 26, have far more unintentional than intentional interferences and these are gantries and toll booths on motorways, so perhaps the infrastructure itself is causing interference. Also, sites 22, 27, 28 and 29 have quite high levels of unintentional interference and these are close to airports so perhaps there are some other systems causing unintentional interference.

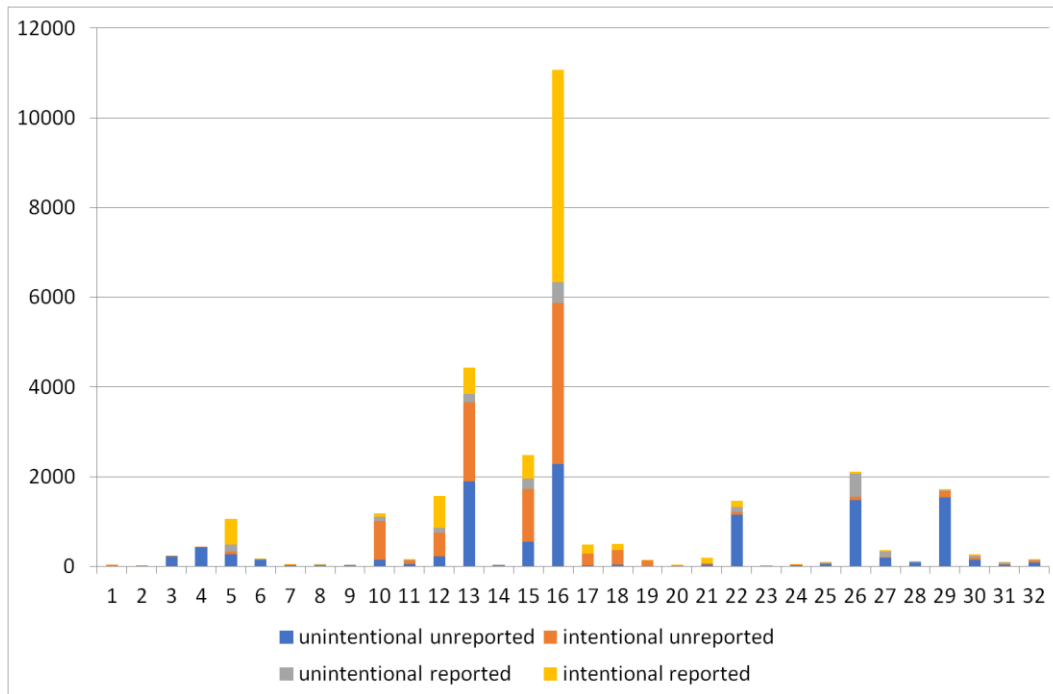
Finally, it is interesting to look at the impact of the events at each site to see which are most at risk. This is done in three steps:

- Firstly, the number of events – intentional and unintentional – at each site from the full database are identified
- Then the reported events (those that met the criteria) are checked
- Finally, the impact of the reported events is extracted. In this sense impact is defined as loss of GNSS positioning.

It is noted this criteria for impact is quite a high level – there will be many other events where there was an impact on C/N0 or number of satellites tracked even though a position solution was still possible. Also, this impact relates only to the COTS receiver in the Detector probe – other receivers at the same site may have been affected differently. Nevertheless, it gives a quick, clear metric to analyse.

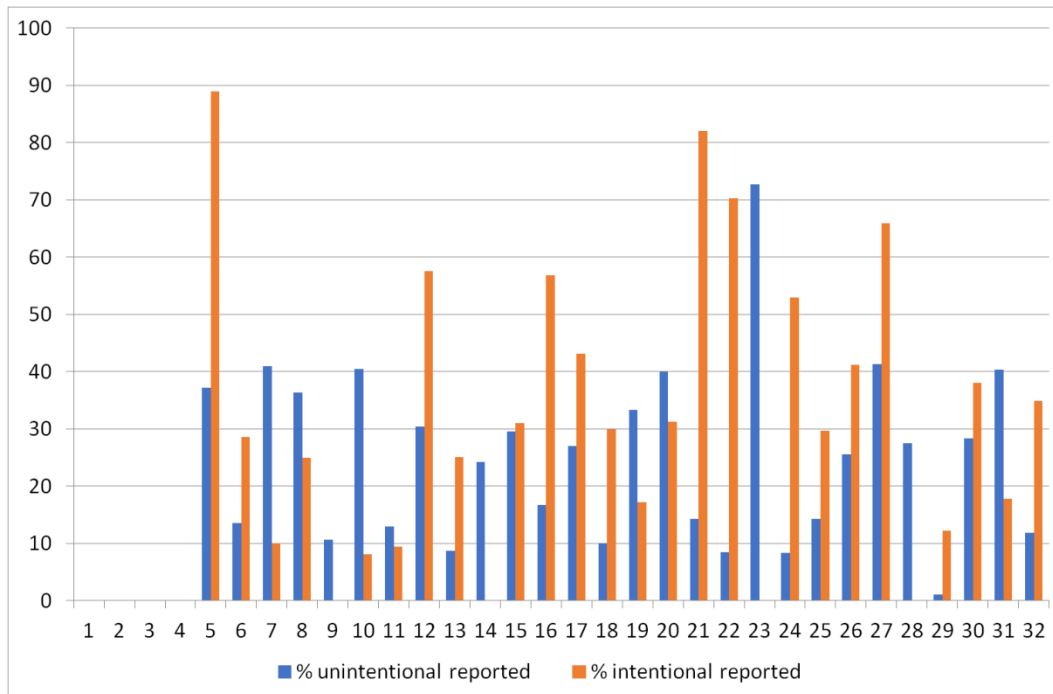
The first chart shows the total numbers of events at the site and whether they were intentional or unintentional and whether or not they met the criteria to be reported.





**Figure 4-5: Totals of Reported and Unreported Intentional and Unintentional Events at each site**

From this we can see of course that the results are dominated by the same active sites. However, there are some quite big differences in the proportions of events that meet the criteria and are reported. For example, at site 29 it appears that most of the events – both intentional and unintentional – are not reported, whereas at site 5 there are a high number of intentional events that are reported. This is shown in more detail by looking at the proportion of each type of event (intentional and unintentional) that are reported at each site.



**Figure 4-6: % of Intentional and Unintentional Events at each site that meet the event criteria and are reported to the STRIKE3 database**

From this we can see some interesting results. For example, site 10 (which is a city centre location) has a high number of events detected, but only a low % of the intentional events are detected with high enough power and long enough duration to be reported. This may be because the antenna is on a roof and so detects lots of events from a long way away that are at quite low power. On the other hand, site 5 has a very high % of intentional events reported, which probably means that there is a single close by source of jammers (a major road) that are usually all detected with high power. It is noted that the ones with highest % of reported intentional events tend to be close to a single major road which is likely to be the major (or only) source of jammers in the vicinity. Sites that are further from roads detect events at a lower power level, hence they are not reported, and sites in cities (that have multiple possible sources of interference from different distances) will detect some jammers from nearby and some from far away and so not all events meet the threshold to be reported.

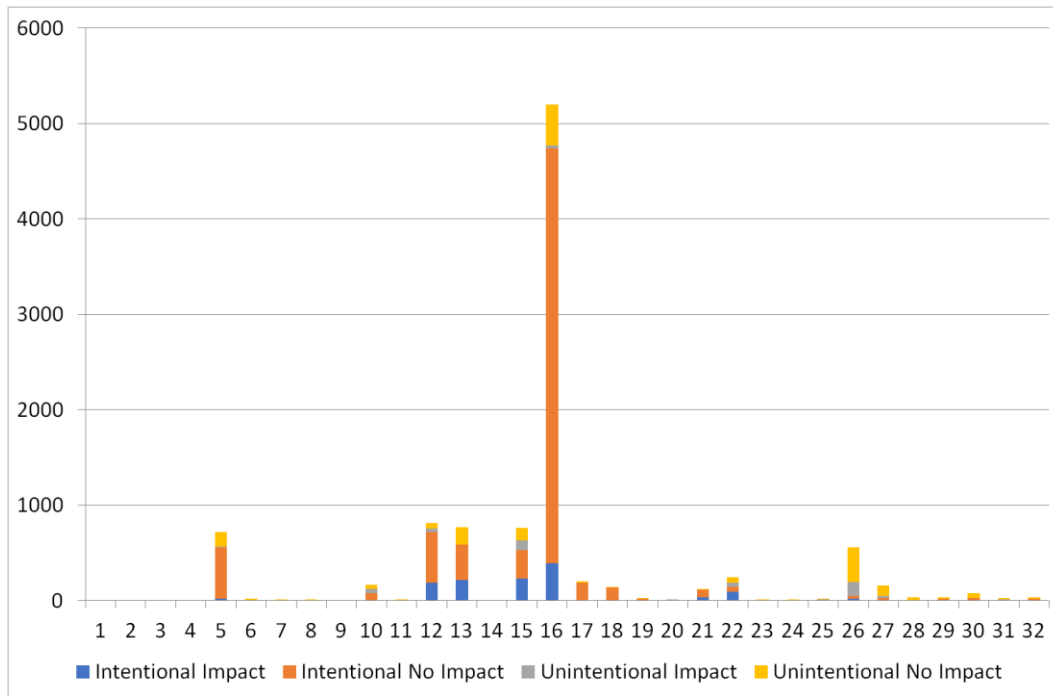
If we look at the impact we can also see differences between sites. The first plot shows number of reported events (intentional and unintentional) that do or do not have an impact (i.e. loss of GPS position).

## D6.2: Threat Database Analysis Report

Ref: STRIKE3\_D62\_DatabaseRep

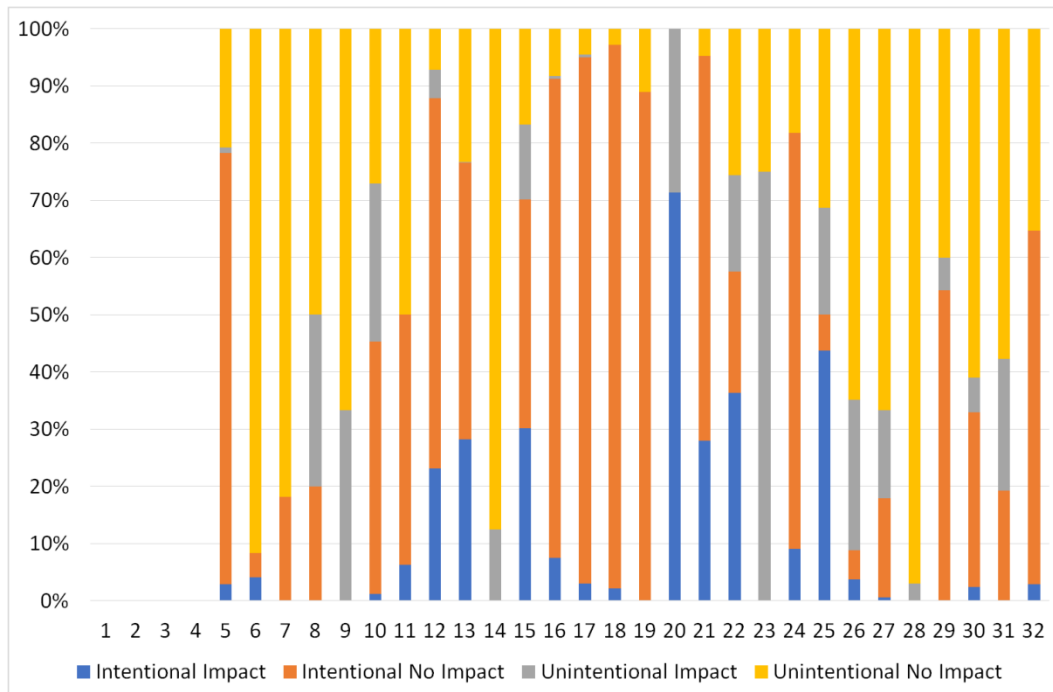
Issue: 1.0

Date: 25.01.19



**Figure 4-7: Impact of intentional and unintentional signals across the sites**

The % of reported events that are impacting and not impacting at each site are also shown.



**Figure 4-8: % of Impacting intentional and unintentional signals across the sites**

It can be seen that at most sites, the vast majority of signals – be they unintentional or intentional – do not cause loss of positioning for the GPS receiver in the Detector probe. At one level this is re-assuring, (at least for the immediate site) but in some ways it is troubling as it can indicate that GNSS jammers are not only in the areas where detectors were installed but also widespread around the local region. In terms of sites that are specifically at risk, site 26 seems particularly at risk from unintentional signals as it has a high number of events and a relatively high proportion that cause loss of GPS, whereas sites 12, 13, 15 and 22 have quite high numbers of intentional signals as well as a high proportion that cause impact.

For site 26, it is known there are transmitters close by to the site so these may be causing unintentional interference, but it is also very close to a motorway and so there could be unintentional interference from vehicles. Sites 12, 13, 15 and 22 on the other hand are in areas known to be susceptible to jammers (city centres and motorways) but are also very close to roads, and hence sources of jammers, and so the events tend to be received with higher power and have greater impact.

### **4.3 Analysis of Entire STRIKE3 Project Duration**

This section considers the entire duration of monitoring within STRIKE3, including all sites that have been monitored since 1<sup>st</sup> Feb 2016.

#### **4.3.1 Overall Activity in Entire Project Duration**

Over the all monitoring periods a total of 495,587 events were detected. Considering the signal classifications from Figure 4-9, the most common signal type seen is white noise. Such signals make up around 50% of all the events. These signals are usually or very low priority, meaning they have a small impact on the positioning calculations. This is due to their lack of power and duration. The next largest category, narrow band signals, can be caused by effects such as other equipment unintentionally interfering with local receivers. The third category of signal to consider are chirp type signals. These are intentionally generated and typical of in-vehicle jammers. Overall the proportions of signal types, different power levels and event duration are very similar for the entire period and for just the long-term monitoring in WP6, despite the fact that they include different sites.

One interesting thing to note is that although the majority of events are low power and short duration, there are a number of events that last for much longer and hence pose a higher risk. There are 7191 events that last for more than 5 minutes, 1112 events that last for more than 30 minutes, 610 events that last for more than 1 hr, and 5 events that last for more than 1 day. The longest event was 5 days in duration! This can happen for example when a vehicle with a jammer parks close by to the Detector probe and the driver leaves without switching off the jammer. These sorts of events, although rare, could potentially cause far more disruption than the more common shorter duration events.

## D6.2: Threat Database Analysis Report

Ref: STRIKE3\_D62\_DatabaseRep

Issue: 1.0

Date: 25.01.19

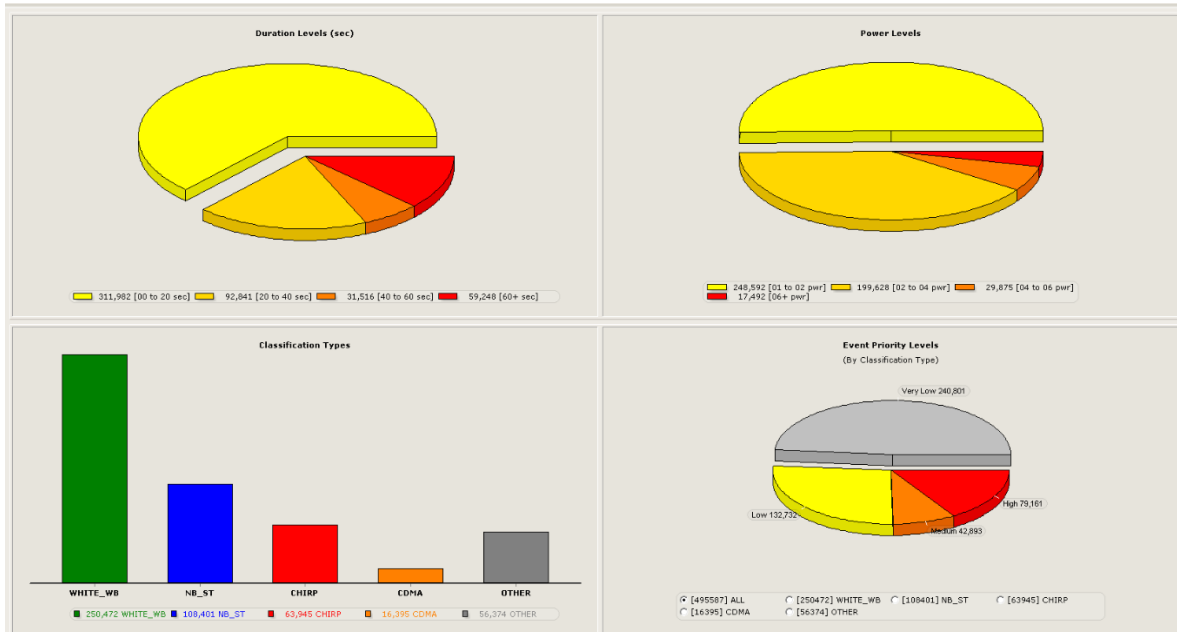


Figure 4-9: Overview of all signals across all time

Figure 4-10 demonstrates that there were many more events detected during the day than overnight. As such it is expected that the majority of events are as a direct result of human activity. The peaks at 7am and 4pm are consistent with those seen in Figure 4-10. The proportion of intentional to unintentional events is also very similar. There seems to be no change between monitoring periods in the time of day that signals are being detected.

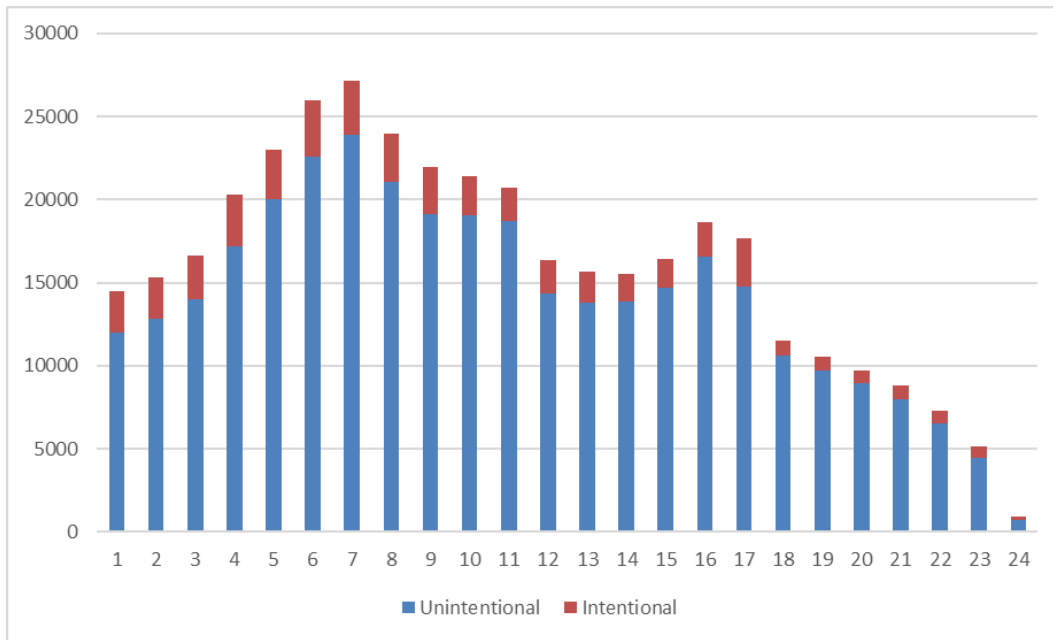


Figure 4-10: Number of events throughout the day in local time

### 4.3.2 Comparison of Site Activity during Entire Project Duration

In this section we look at entire monitoring period (since 1<sup>st</sup> Feb 2016) to include all sites.

Firstly, we present a table showing the sites ranked in descending order of activity for intentional events with normalised power greater than 3.5.

Site number	Monthly avg. no. chirps	Infra-structure	Local environment	Distance to minor road	Distance to major road
16	5227.800646	Airport	City centre	-	45 metres
15	1298.975261	Office	City centre	-	4 metres
17	799.3028203	Office	City centre	-	40 metres
18	742.3686946	Airport	Airport	300 metres	4.5 km
19	433.9995226	Airport	Airport	500 metres	4 km
47	421.3333333	Airport	Inter-city motorway	-	80 metres
10	252.1503831	Office	City centre	29 metres	260 metres
13	220.7717622	Office	City centre	65 metres	178 metres
12	117.4520601	Office	City motorway	30 metres	150 metres
42	55.42857143	Power Grid	City motorway	-	200 metres
5	53.5577328	Airport	City motorway	-	119 metres
31	42.69451162	Office	City centre	70 metres	250 metres

## D6.2: Threat Database Analysis Report

Ref: STRIKE3\_D62\_DatabaseRep

Issue: 1.0

Date: 25.01.19

Site number	Monthly avg. no. chirps	Infra-structure	Local environment	Distance to minor road	Distance to major road
22	20.53483069	Office / Airport	Inter-city motorway	1.3 km	45 metres
21	19.16863641	Office	Business park	30 metres	460 metres
1	14.74592662	Power Grid	Near intercity motorway	15 metres	300 metres
25	14.33994051	Office	Inter-city motorway	-	30 metres
27	14.06185683	Airport	Airport	100 metres	350 metres
26	13.84152161	Toll booth	Inter-city motorway	-	45 metres
29	12.20182177	Airport	Airport	86m	150m
32	11.58500658	Airport	Near city motorway	-	100 metres
3	10.96656368	Gantry	Inter-city motorway	-	9 metres
30	9.946253877	Airport	Airport	200 metres	1.15 miles
39	9.7	Gantry	Inter-city motorway	-	0 metres
20	7.468911859	Office	Urban	65 metres	250 metres
11	7.373682818	Office	Urban	114 metres	350 metres
24	6.044980701	Airport	Airport	-	120 metres
28	5.437095125	Airport	Inter-city motorway	-	70 metres
14	5.4	Airport	Airport	70 metres	400 metres
46	4	Office	Port	40 metres	100 metres
7	3.968348453	Boat/Port	Sea / port	NA	NA
4	3.902477097	Gantry	Inter-city motorway	-	17 metres
2	3.08689295	Power Grid	Urban	140 metres	1.35 miles
45	3	House	Inter-city motorway	-	14 metres
37	2.692307692	House	Urban	110 metres	400 metres
44	1.8	Gantry	Border crossing, motorway	-	30 metres
8	1.693695578	Office	Urban	21 metres	2.5km
6	0.986173768	Airport	Airport	200 metres	1.1 miles
35	0.75	Office	Business park	70 metres	70 metres
43	0.4	Office / Railway	Urban	100 metres	450 metres
23	0.264256471	Office	Business park	10 metres	70 metres

## D6.2: Threat Database Analysis Report

Ref: STRIKE3\_D62\_DatabaseRep

Issue: 1.0

Date: 25.01.19

Site number	Monthly avg. no. chirps	Infra-structure	Local environment	Distance to minor road	Distance to major road
38	0.230769231	Office	Business park	50 metres	700 metres
9	0	Port	Port	140 metres	230 metres
40	0	Gantry	Inter-city motorway	-	0 metres
49	0	Office	Port	340 metres	50 metres

**Table 4-1: Site information ordered by monthly average intentional activity.**

The first thing to see is that there is a huge variation in the activity between sites, with some sites seeing virtually no jammers but others averaging hundreds, or even thousands of jammers detected per month.

To draw some conclusions from the above, we study the top 15 and bottom 15 active sites for chirp (intentional) events. For the top 15 most active sites, we observe that

- All city centre locations are among the most active sites
- There are motorway sites – particularly city motorways

For the 15 least active chirp sites, we observe that:

- None are in city centre locations.
- Less active sites tend to be urban areas, business parks and ports

Taken together these observations suggest that inter-city motorways less active than city centres/motorways. This may be due to differences in the type of traffic on these roads, with city centres and city motorway having more taxis, deliveries and commuters, who repeat their journeys every day (or several times a day) and hence any jammers are seen multiple times.

Next we split the period into three to be able to spot differences in the same sites over time. The periods chosen are:

1. February 2016 – April 2017
2. May 2017 – Jan 2018
3. February 2018 – October 2018

The first set of plots show average monthly numbers of events (total and chirp, i.e. intentional) at each site.



## D6.2: Threat Database Analysis Report

Ref: STRIKE3\_D62\_DatabaseRep

Issue: 1.0

Date: 25.01.19

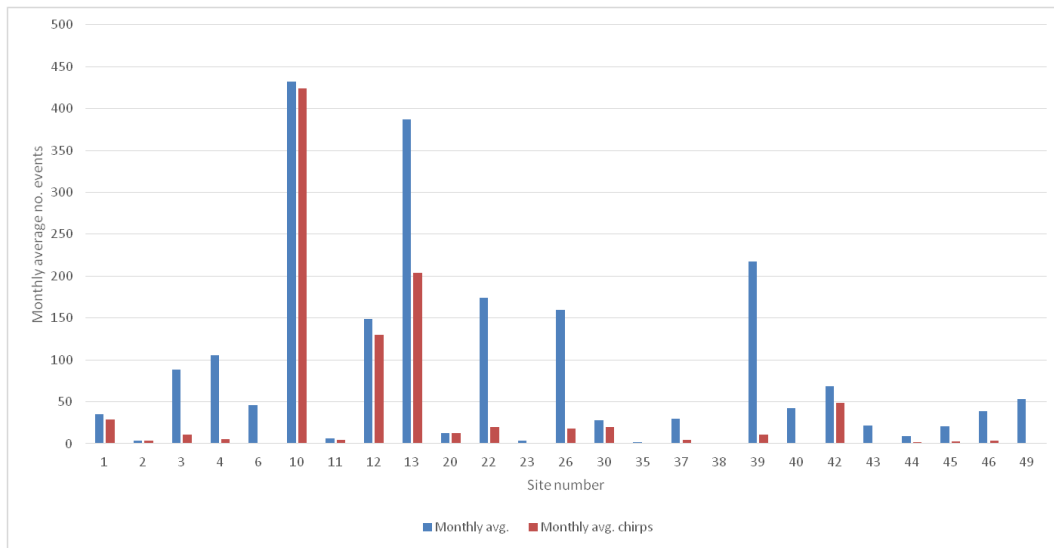


Figure 4-11: Monthly average events for all sites active in period 1

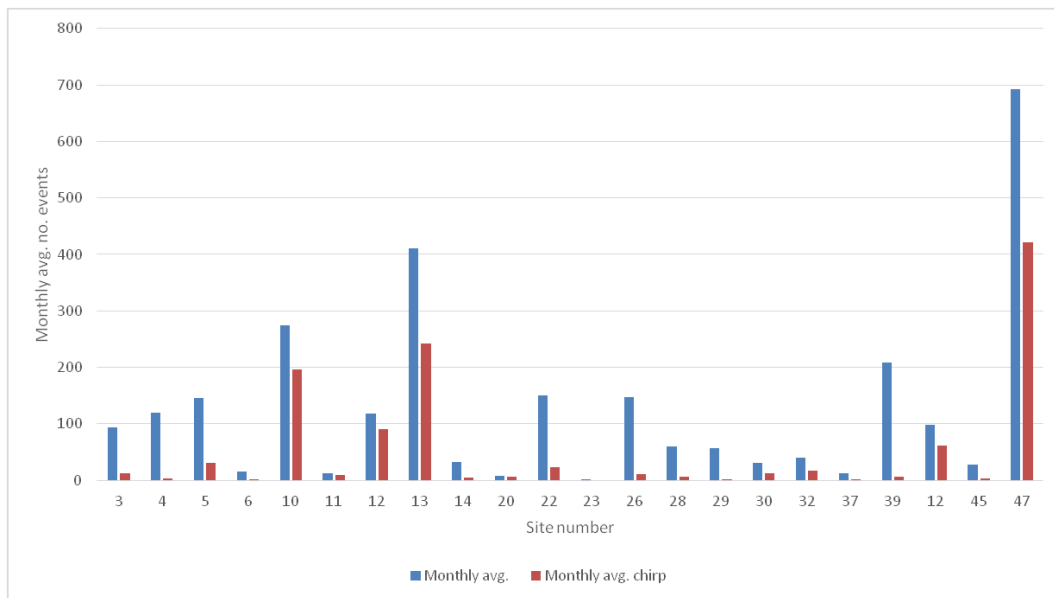
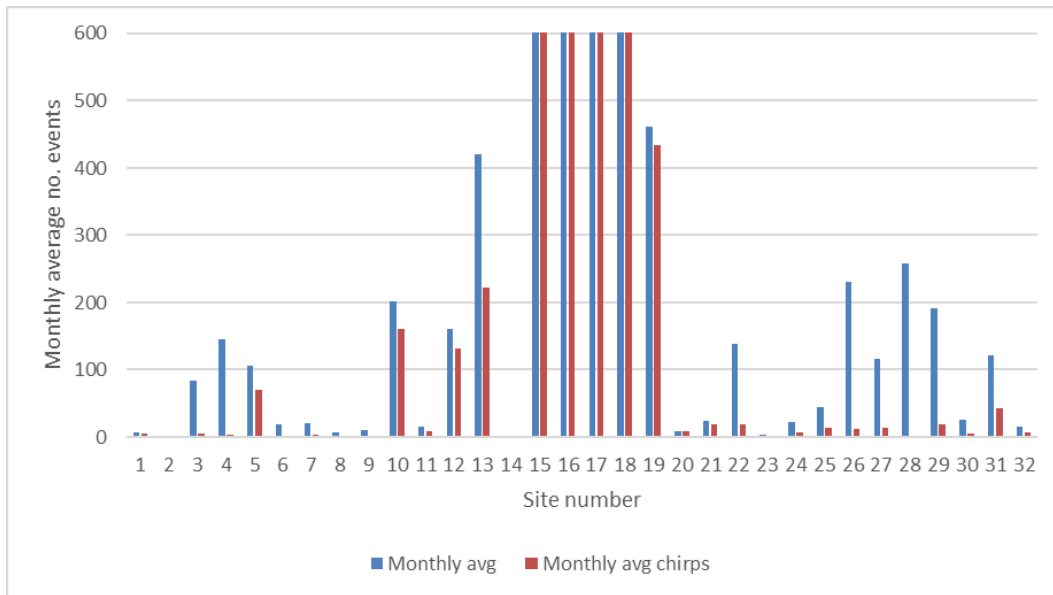


Figure 4-12: Monthly average events for all sites active in period 2

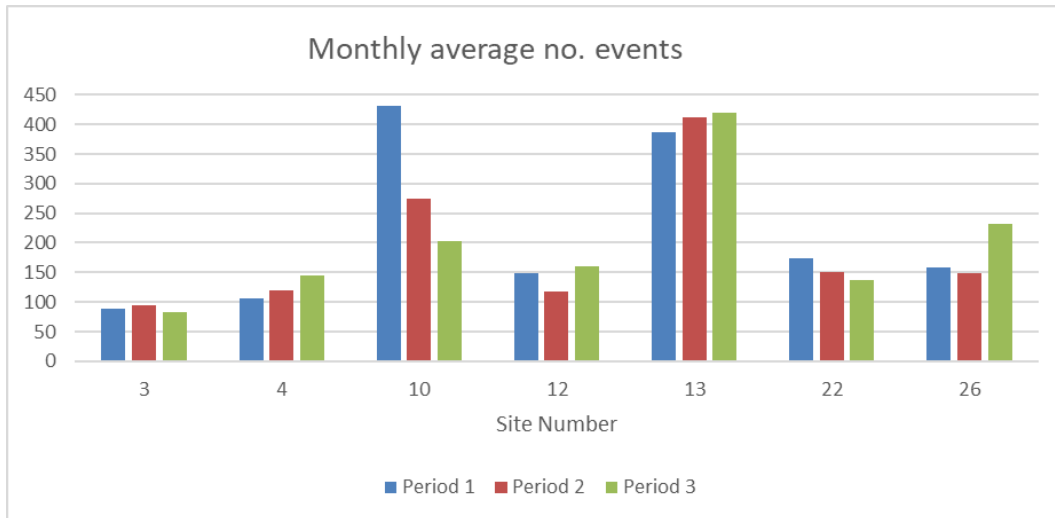


**Figure 4-13: Monthly average events for all sites active in period 3. The y-axis has been truncated to allow easier comparison with the other periods**

Some sites are common between periods and so we can compare the performance to see how the activity has changed over time. Some high activity sites are presented in every period to see how their activity changes over time, and also consider their infrastructure and environs (as we did for WP6) to spot any broad trends.

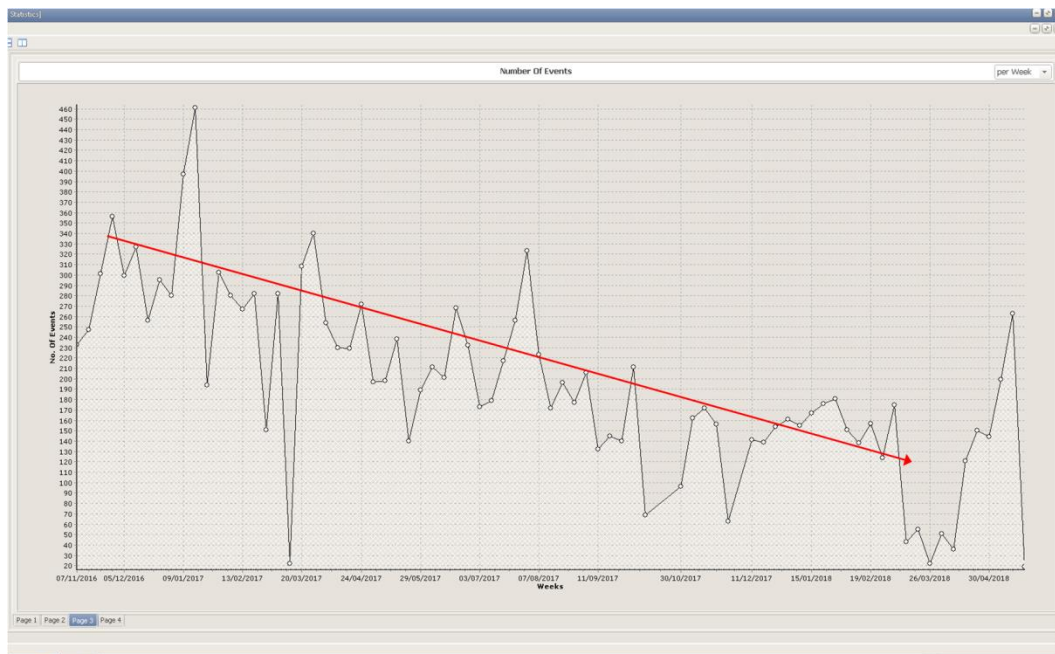
Site No	Infrastructure	Local Environment	Distance to minor road (m)	Distance to major road (m)	Monthly avgs in period (rounded)		
					1	2	3
3	Gantry	Inter-city motorway	-	9	89	94	83
4	Gantry	Intercity motorway	-	17	106	120	145
10	Office	City centre	29	260	432	274	202
12	Office	City motorway	30	150	149	118	161
13	Office	City centre	65	178	387	411	420
22	Office & Airport	Inter-city motorway	-	45	174	151	138
26	Gantry	Intercity motorway	-	45	159	148	231

**Table 4-2: Comparison of Average Activity for High Activity Sites in Different Monitoring Periods**



**Figure 4-14: Bar chart showing how the total event detection rate changes over time for seven sites that appear in all three monitoring periods**

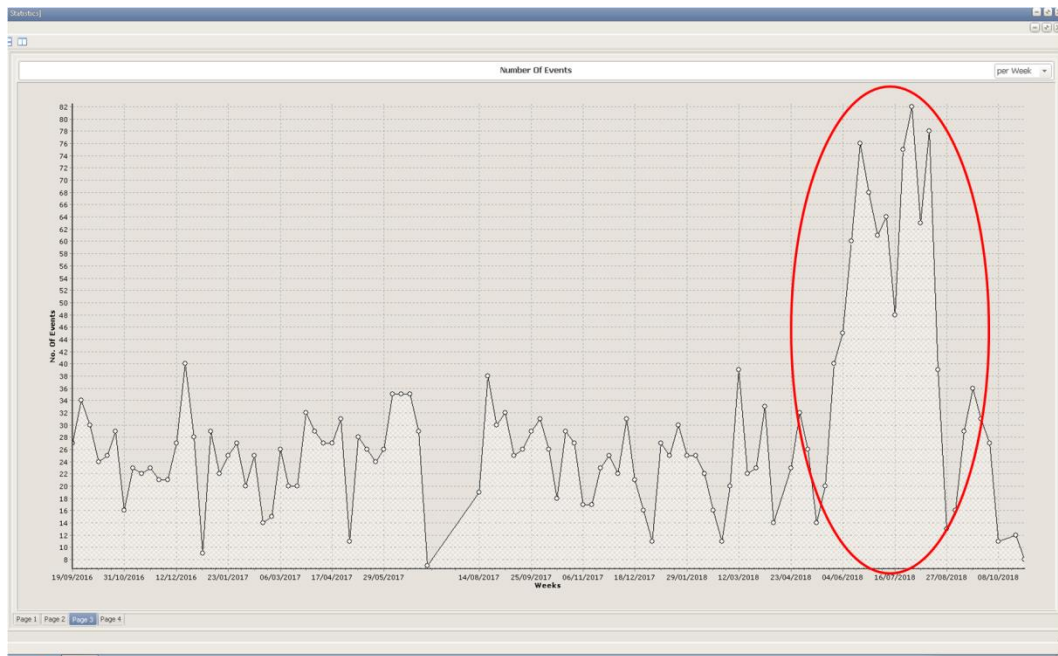
The analysis reveals that site 10 has significantly decreased over the STRIKE3 project duration. This is a city centre location and the time series of weekly numbers of high priority events are shown in the figure below.



**Figure 4-15: Plot showing Decrease in Jammer Activity at site 10**

It can be seen that over the period there was a gradual decrease in high priority events rather than a sudden change. The reduction is in chirp events rather than unintentional. This suggests a gradual reduction in jammer usage in this vicinity – although whether that reflects a general reduction in the city or just a change in behaviour of particular vehicles in that area is hard to say.

On the other hand, site 26 shows an increase in activity over the period. The time series of weekly activity for this site is shown below.



**Figure 4-16: Plot showing Decrease in Jammer Activity at site 26**

It can be seen that in this case the level of activity (which is mainly high-power unintentional signals) is reasonably constant except for a period in 2018 where there is a sudden increase in activity lasting for several months before dropping again.

#### 4.4 Types of Signal

Assessing the types of signal is important as it allows us to identify those signals that pose the greatest threat, i.e. those that are most common and hence most likely that the receiver will encounter. This knowledge then feeds into the receiver testing standards [RD.2] to decide which signals should be included in the test scenarios.

In this section we study the various subcategories of jammer signal, specifically the chirp signal across different sites and monitoring periods. In the section below, we have used the same three monitoring periods as mentioned in section 4.3.2. For this version of the document, we have only studied the distribution of the most powerful events seen at each

## D6.2: Threat Database Analysis Report

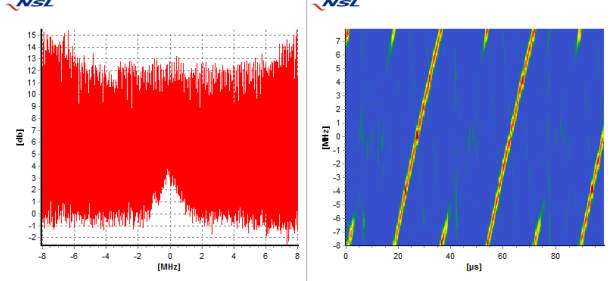
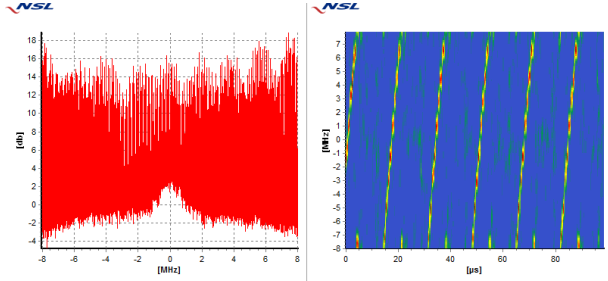
Ref: STRIKE3\_D62\_DatabaseRep

Issue: 1.0

Date: 25.01.19

site. This required using different power thresholds.

From the results we can see many hundreds of different types of chirp jammer. However, we can divide them into 11 broad categories for classification and analysis:

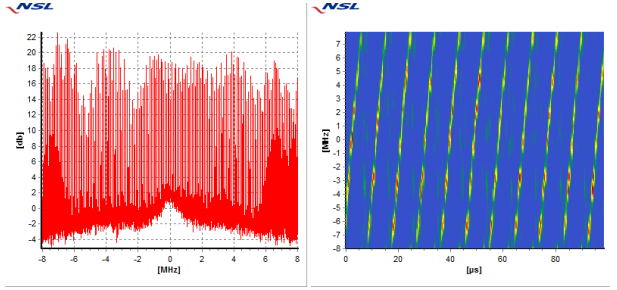
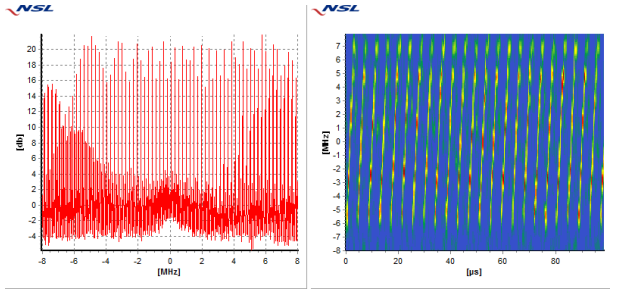
Name	Features	Example
Wide sweep - slow	<p>Spectrum plot</p> <ul style="list-style-type: none"> <li>- show wide variation in power levels at all frequencies</li> <li>- Often see shape of reference spectrum defining bottom edge of power levels</li> </ul> <p>Spectrogram</p> <ul style="list-style-type: 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>	
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>	

## D6.2: Threat Database Analysis Report

Ref: STRIKE3\_D62\_DatabaseRep

Issue: 1.0

Date: 25.01.19

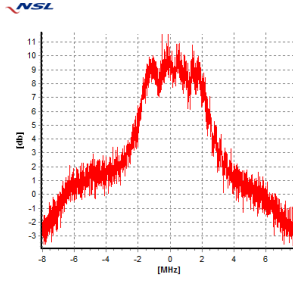
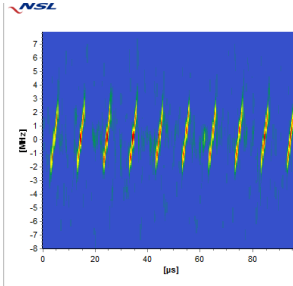
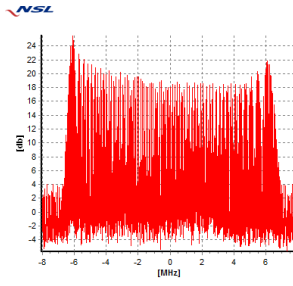
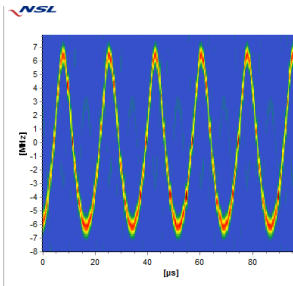
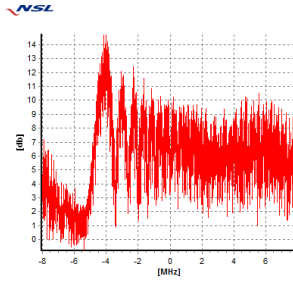
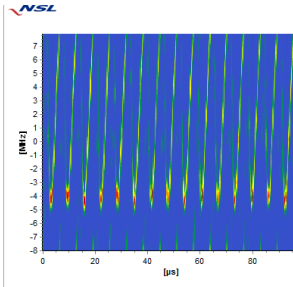
Name	Features	Example
<p>Wide sweep - fast</p>	<p>Spectrum plot</p> <ul style="list-style-type: none"> <li>- show wide variation in power levels at all frequencies</li> <li>- Often see shape of reference spectrum defining bottom edge of power levels</li> </ul> <p>Spectrogram</p> <ul style="list-style-type: 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 8 to 12 chirps per 100 <math>\mu</math>s</li> </ul>	
<p>Wide sweep - rapid</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>	

## D6.2: Threat Database Analysis Report

Ref: STRIKE3\_D62\_DatabaseRep

Issue: 1.0

Date: 25.01.19

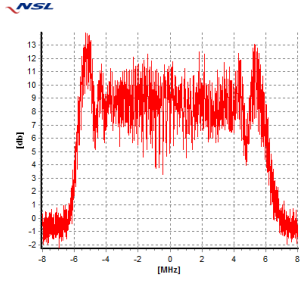
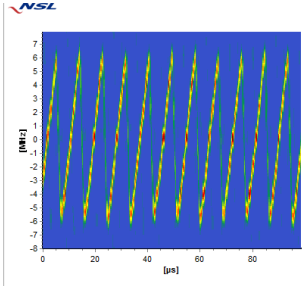
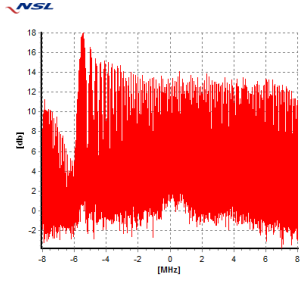
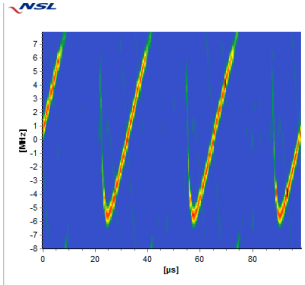
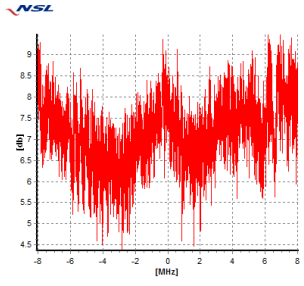
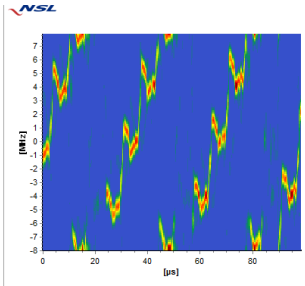
Name	Features	Example	
narrow sweep	<p>Spectrum plot</p> <ul style="list-style-type: none"> <li>- show increase in power levels across narrow frequency range</li> </ul> <p>Spectrogram</p> <ul style="list-style-type: none"> <li>- Clearly defined and separated linear (or slightly curved) diagonal lines covering small frequency range</li> <li>- Most commonly show frequency increasing with time</li> </ul>		
Triangular wave	<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>		
Triangular	<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>		

## D6.2: Threat Database Analysis Report

Ref: STRIKE3\_D62\_DatabaseRep

Issue: 1.0

Date: 25.01.19

Name	Features	Example	
<p>Sawtooth</p>	<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>Hooked sawtooth</p>	<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>Tick</p>	<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 µs)</li> <li>- Additional structure and variation (taking form of a tick) overlaying the underlying slow sweep</li> </ul>		



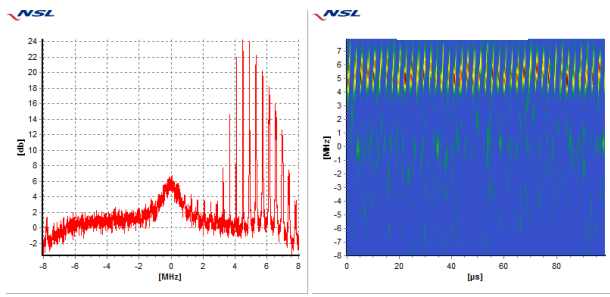
Name	Features	Example
Multi tone	<p>Spectrum plot</p> <ul style="list-style-type: none"> <li>- Multiple distinct tones with high power at different frequencies</li> </ul> <p>Spectrogram</p> <ul style="list-style-type: none"> <li>- multiple closely spaced near vertical lines in the region of affected frequency</li> </ul>	

Table 4-3: Description of Chirp Jammer Categories

### 4.4.1 Period 1

This period covers February 2016 – April 2017. At first there were few sites but as the period went on more and more sites were installed.

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.

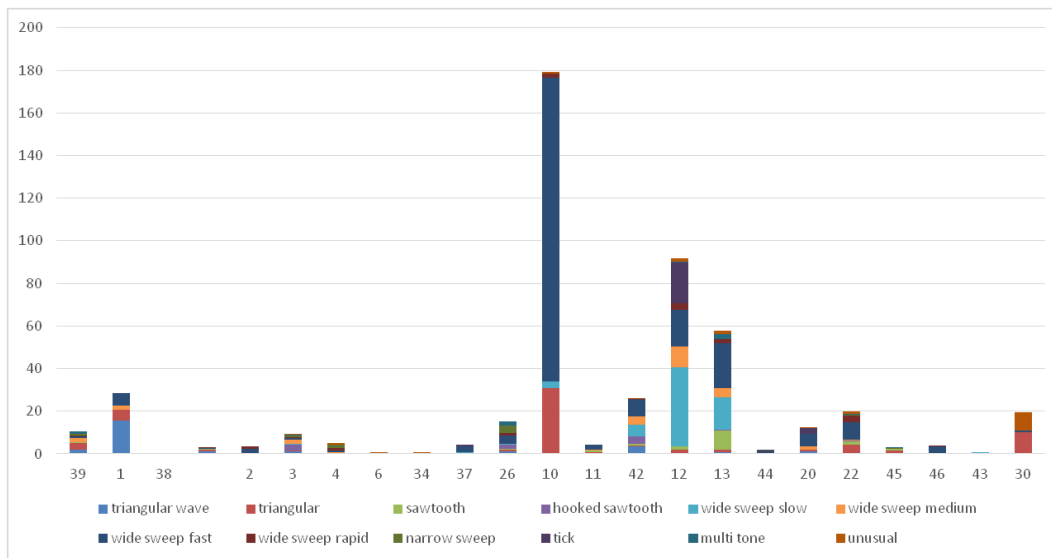


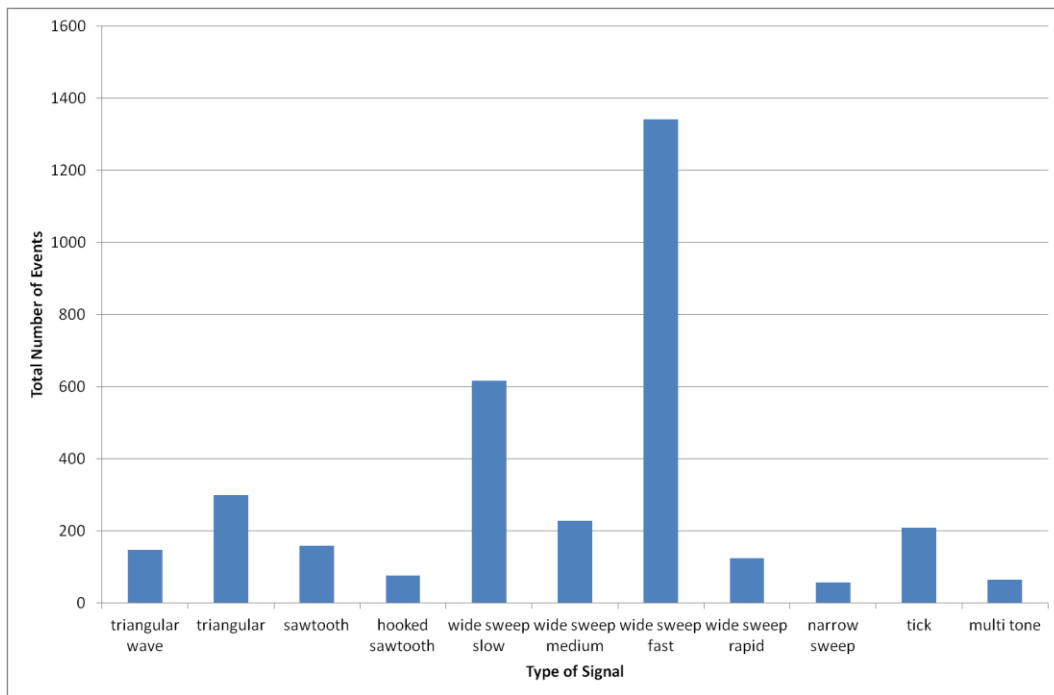
Figure 4-17: Monthly Average Number of Chirp Events of each type at Each Site

It can be seen from the results that all of the sites that detect chirp signals 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, site 10 sees a very large proportion of wide sweep fast events and a lot of triangular, but few others. Site 12 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.



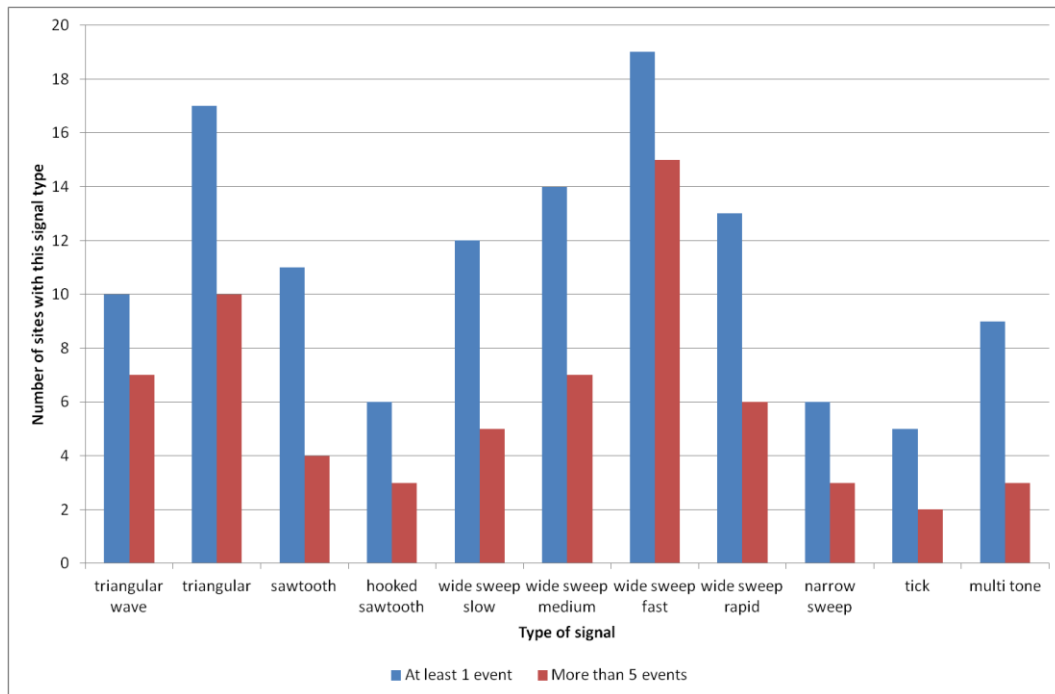
**Figure 4-18: Total Number of Events of each type from All Sites**

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 μs). 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 one-off or misclassification.



**Figure 4-19: 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 (site 12) and this has been seen only rarely at other sites.

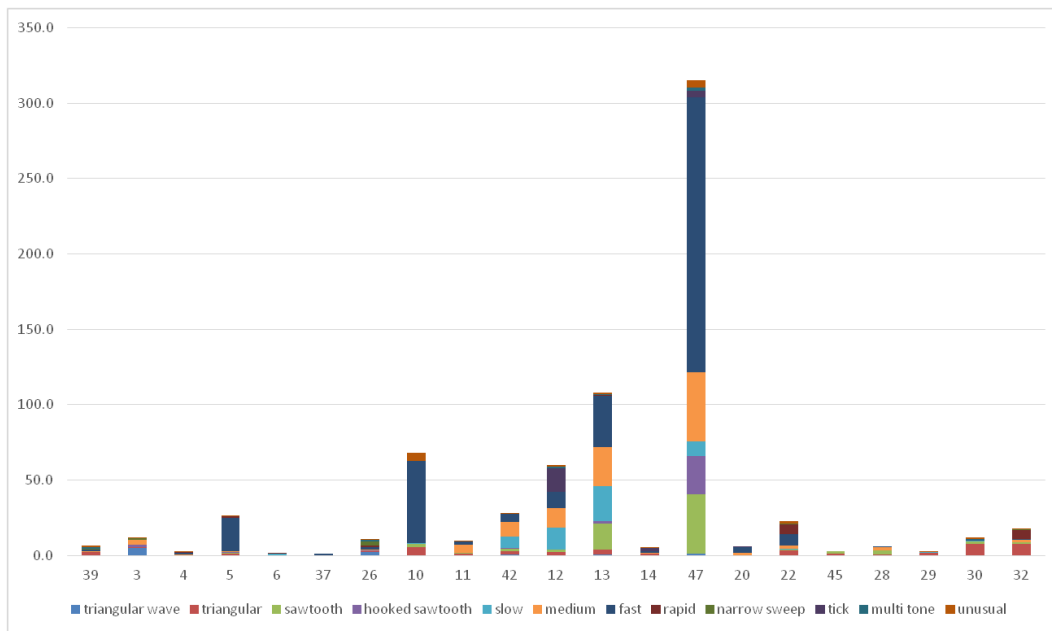
On the other hand, the triangular wave type of signal only the 6<sup>th</sup> most common type of signal in terms of total number of detections, but is seen on more than 5 occasions at 7 different sites, which is the third most common.

Overall therefore it seems that the most typical types of chirp signal are wide sweep (various speeds), triangular and triangular wave.

### 4.4.2 Period 2

Period 2 runs from May 2017 – Jan 2018. In this period some of the sites continued monitoring from period 1 but there were also some new sites.

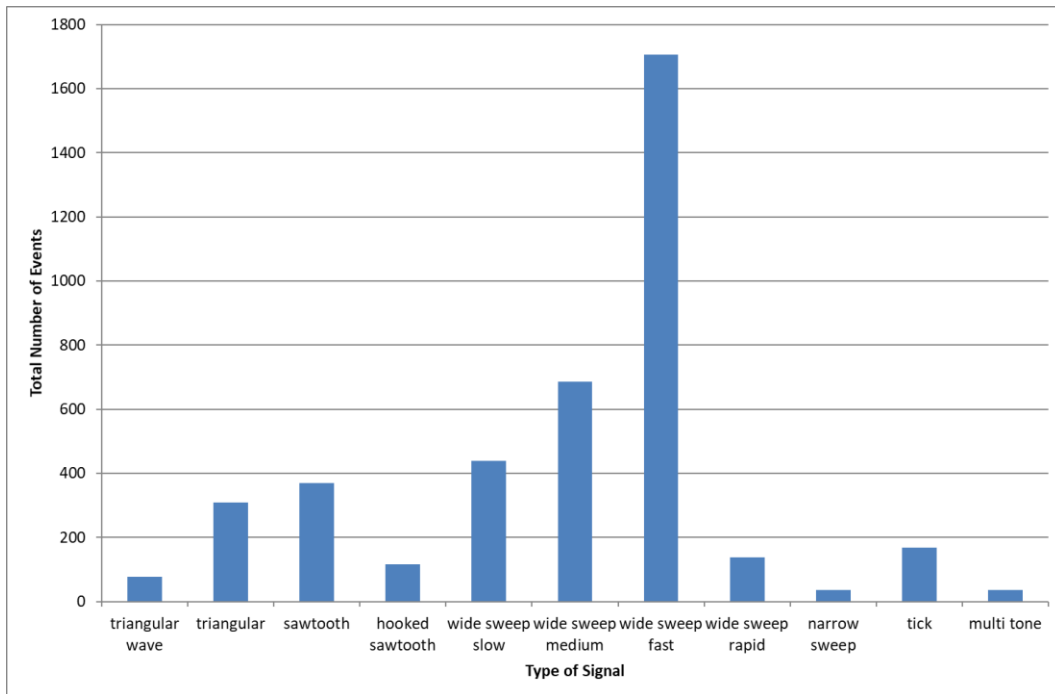
In the first plot we see for each site the number of chirp signals of different types (above the minimum power threshold) that were detected at that site during the monitoring period. The longer the bar, the greater the number of events. Each type of chirp signal is indicated by a different colour.



**Figure 4-20: Breakdown of chirp types by site for period 2. Monthly averages.**

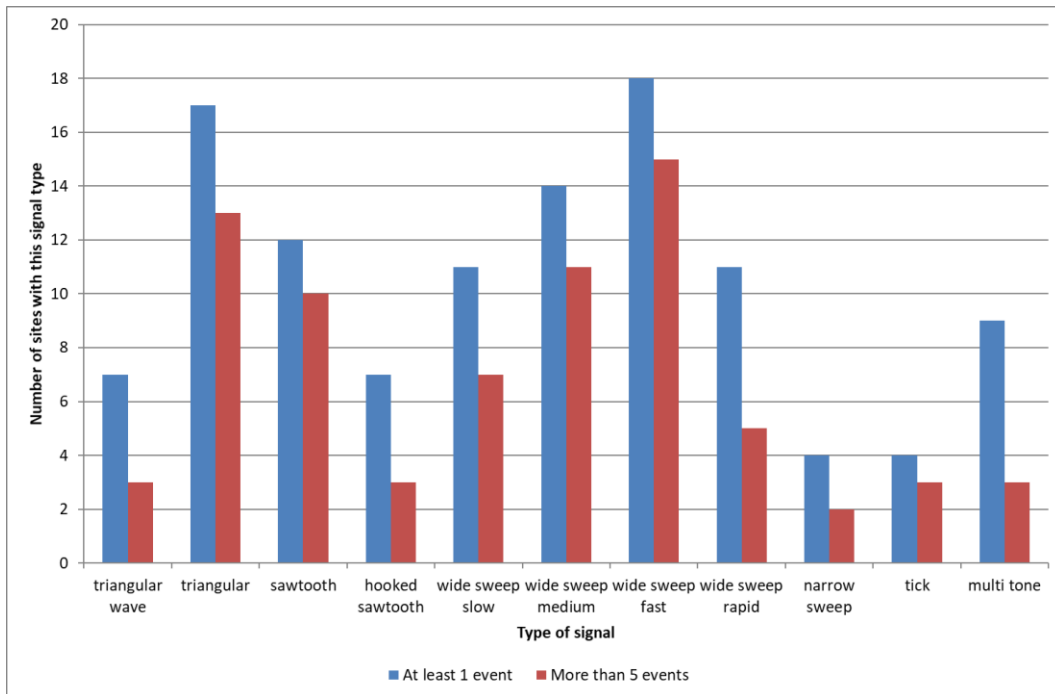
Like in period 1 we see a lot of variation between the sites – both in rate of detection of chirp jammers, and in the proportion of chirp signal types at each site. This time we can see that sites 10 and 12, which were previously the most active, now have reduced in activity whereas site 13 has increased. Now though a new site (site 46) is the most active and sees a wide variety of jamming signal types. It is also interesting to note that we observe similar proportions of the same event types at sites 12, 13 and 46. This is despite sites 12 and 13 being city centre locations and 46 being on an airport close to a motorway as noted.

Looking at the total activity for each chirp signal type we can see which have been detected the most frequently.



**Figure 4-21: Breakdown of the total number of chirp types in period 2**

As before the wide sweep with fast repeat rate is most commonly detected. We also can 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 one-off or misclassification.

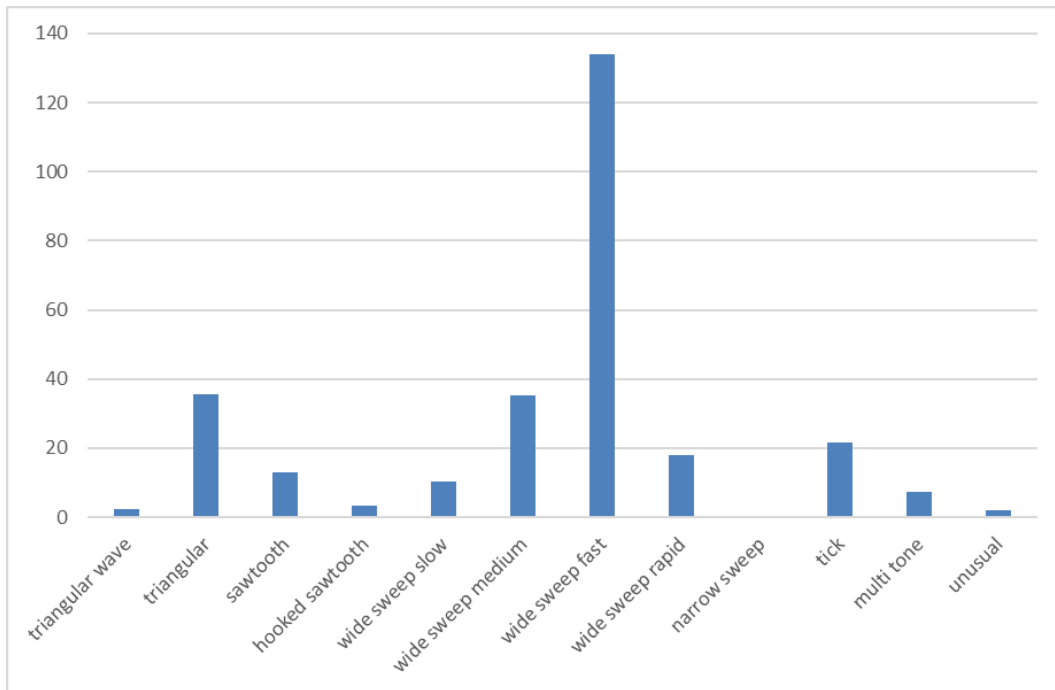


**Figure 4-22: Breakdown of the spread of occurrences of various chirp types for period 2**

Again we see the wide sweep fast and triangular as being very common. In fact, comparing between the first two periods there are very similar patterns to which signals are the most common. The few differences we see are that sawtooth seem more common and triangular wave less common in the second period. The triangular wave appears less common because some sites that saw it in the first period are no longer monitored in the second period. Conversely, the sawtooth is relatively common at some sites that are monitored in the second period but not in the first. This implies these signals are a bit less widespread than things like swept signals and triangular as those are still common in both periods despite using some different sites.

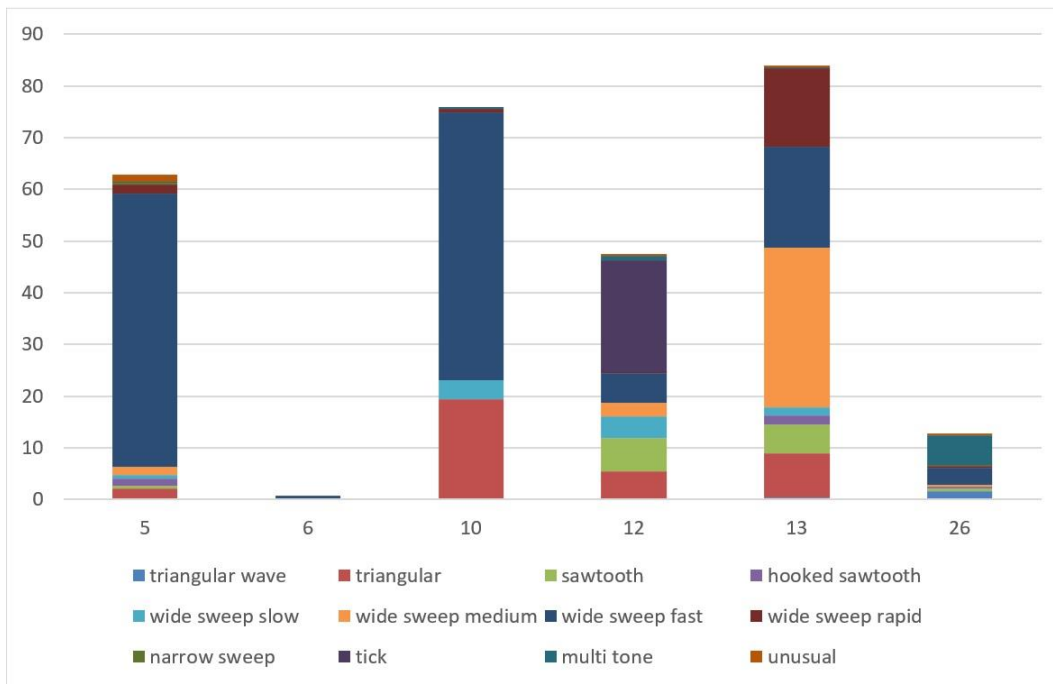
#### 4.4.3 Period 3

For the final period, we consider only the sites with high chirp activity that have also been active throughout the whole monitoring period: sites 5, 6, 10, 12, 13 and 26.



**Figure 4-23: Monthly average chirp types seen across the six sites under consideration**

Note that the values are lower than those in period 2 (Figure 4-21) simply because fewer sites are being considered. Overall though, the pattern is very similar, indicating that the distribution has remained fairly constant. However, relatively speaking, we have seen more tick, triangular and rapid sweep chirps in this period.



**Figure 4-24: Monthly average chirp type breakdown for each site.**

Comparing the above figure to Figure 4-20, it is immediately obvious that:

- The activity of site 5 has increased. This is largely down to fast sweep chirps
- Site 10 has seen an increase in triangular chirps
- Site 12 has seen a sharp increase in tick chirps. The vast majority of this type of chirp occurred at this site, particularly in this period.

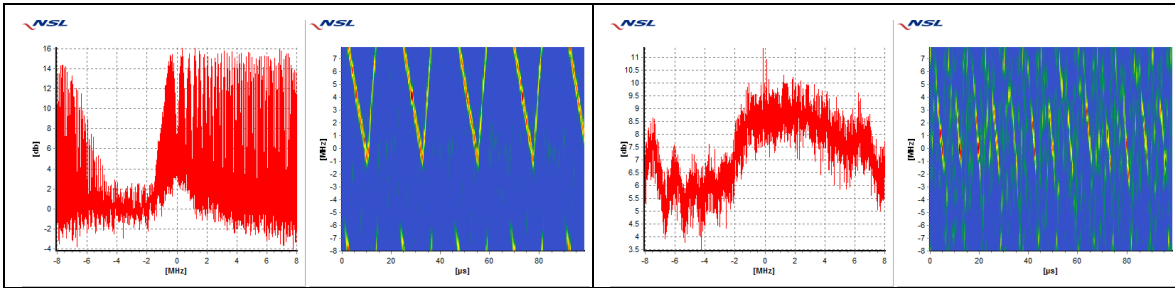
Across all three periods, it seems that the wide fast sweep chirp is by far the most common type.

#### 4.4.4 Unusual Signals

It is also interesting to point out some of the unusual signals characterized as chirp that have been detected at the sites. These unusual signals are seen only rarely – some of them only once or twice in the entire period – so they are not included in specific analysis of signals but they are interesting nonetheless.

Some of the unusual events show chirp events with swept signals in the opposite direction to usual.

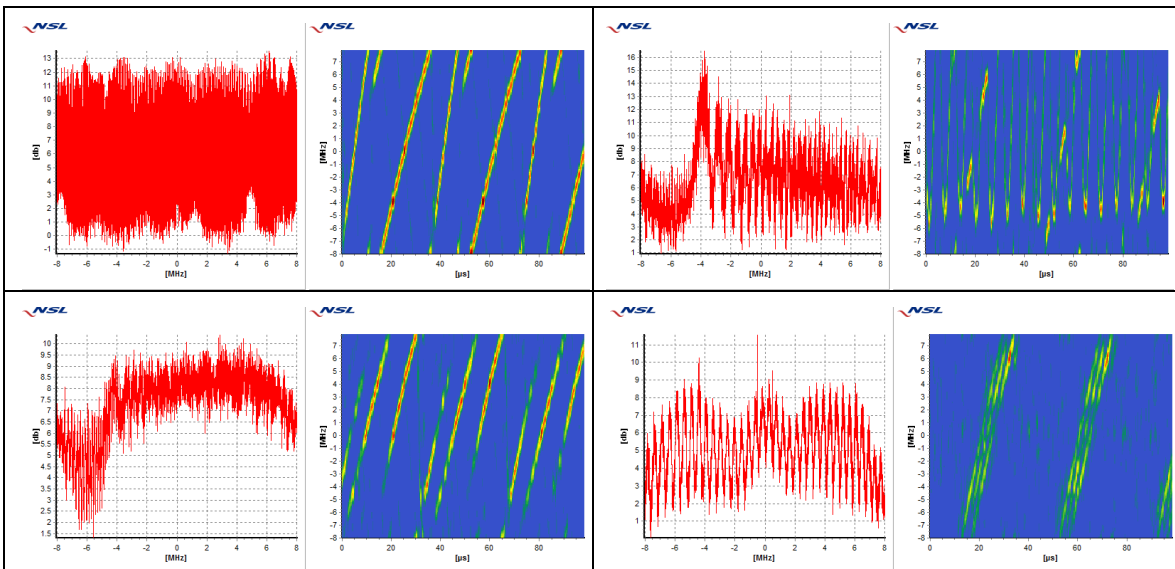




**Figure 4-25: Example Unusual Chirp Signals with Downward Sweep**

Others appear to show multiple signals in the same plot. Possible reasons for this could be:

- Detection of two different jammers in two different vehicles that happen to be passing the monitoring unit at the same time
- Possible multipath of the interference signal
- A user intentionally deploying two jammers in the same vehicle. The spectrum and spectrogram in the top right of the figure below is a good example of this because the same signature was seen on multiple days.



**Figure 4-26: Example Unusual Chirp Events with Multiple Signals**

Others are completely different and do not in fact appear to be chirp signals, but the strange nature of their structure obviously makes it difficult for the algorithms to classify them reliably.

## D6.2: Threat Database Analysis Report

Ref: STRIKE3\_D62\_DatabaseRep

Issue: 1.0

Date: 25.01.19

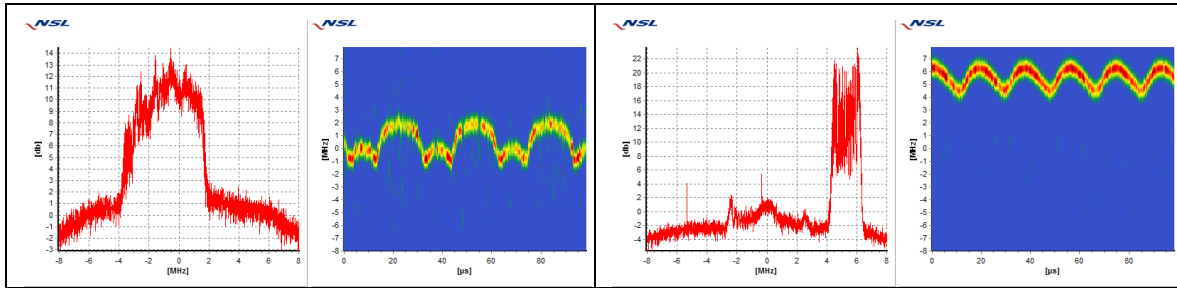


Figure 4-27: Example Unusual Non-Chirp Signals

## 5 Summary and Conclusions

The long-term monitoring at a global network of sites has provided a lot of information and allowed a thorough analysis of the interference environment at many locations.

Considering the long-term validation of the reporting standards themselves, the main conclusions are as follows:

- During the entire measurement campaign, 2017-12-01 to 2018-10-31, there were in total 15 200 detected interference events reported by the STRIKE3 network to the centralized database. In the beginning of the measurement campaign the number of events grew with approximately 500 events per month, and in the end of the period the number of events per month were approximately 1000. The number of events drastically increased for June and July. However, this is not a general trend it is because of a very noisy site which was active this time period and therefore dominates the overall results. Therefore, it could be misleading to look at the number of events per month without considering site activity. The median number of detected events per hour of the day, has good agreement with human activity. There are more events from 6 a.m. to 11 p.m. and less during the night.
- From the data collected to the centralized database it is possible to do high level trend analysis. But it is not possible to do analysis on site level, as the information about sites is not available in the database. If anonymous site information is added to the database, it is important to add information about the sensors status at the site. With sensor status it would be possible to distinguish between the two cases, 'there were no events' and 'the sensor was offline', when there are zero reported events for a time period.
- The event definitions were shown to be reasonably defined, such that the two types of type 'a' event sensors reported similar interference events. Some small variations were seen due to, for example, different bandwidth of the two types of sensor. Overall, both types of sensor report those events that could have an impact on a co-located GNSS receiver in a similar manner.

From the dataset as a whole, considering all sites, the entire project duration, and

additional information in the Detector database, we can make the following conclusions:

- Firstly, there is a lot of interference – far more than we would have expected to see at the start of the project.
- Also, interference – both unintentional and intentional – affects every site that has been monitored. There are no completely ‘clean’ sites.
- However, there is of course a wide variation in activity between sites depending on the type of infrastructure, the local environment, and also the country in which it is located. In general, those sites that are busiest in terms of human activity and traffic (city centres and city motorways) are affected most by intentional interference (from in-vehicle jammers) whereas more remote sites have few jammers.
- The vast majority of interference events were detected with low power and short duration so are really just noise / junk and do not cause any noticeable impact.
- We also see much more unintentional than intentional interference. It is difficult to see a real pattern in these unintentional events, although generally there are more during daytime than night, and more on weekdays, so they still seem to be linked to human activity.
- Although many events have no impact, we still see tens of thousands at a power level that will cause some impact at the monitoring sites and many hundreds that cause a complete loss of GPS positioning at the receiver. However, it should be noted that the COTS receiver in the monitoring equipment through which we measure impact is a particular type and not representative for all users and so impact may be more (or less) for different equipment at the same locations.
- Despite all this interference, reports of real-world impacts are thankfully not common. In general this is good news and shows that receivers (and the applications/operations that make use of them) have some resilience to the sort of low level interference we see going on.
- However, there are a couple of caveats to that though. Firstly, the sort of things that would get reported are major newsworthy events. There could be a lot of lower level impacts (e.g. short losses of positioning, drop in number of satellites tracked) that are occurring but not being reported. Also, the sort of things we have been detecting in STRIKE3, whether unintentional or intentional, are not directed specifically at the infrastructure where the detection equipment is located – it is incidental interference that is being

detected. Therefore in these cases it is perhaps not surprising that the impact is usually low, even if the probability of such interference occurring is high. Some of the highest power events, and certain real world examples, do show the disruption that could be caused if there was a directed attack specifically on a target, in which case the impact would be much higher although the probability of occurrence is very low.

Overall, in terms of the monitoring itself, there are several good outcomes from the process and also some lessons learned that can provide recommendations for future monitoring activities by stakeholders:

- The first main benefit of the monitoring is that doing it on such a wide scale has allowed us to obtain some good evidence for the real-world level of interference that is out there and how widespread jammers are. Previous limited monitoring campaigns and anecdotal evidence had given some idea of the problem, but the sheer number of sites and duration of STRIKE3 monitoring shows the overall picture in a clear way, as well as illustrating differences between sites and changes of activity over time.
- Additionally, the results for specific sites are useful for the hosts to assess specific risks, patterns of activity, etc.
- In terms of the signals, we have also managed to populate a huge database of many different types of signal (both jammers and unintentional events) that are out there in the real-world. This has given a valuable insight into those signals that pose the greatest threat (being the ones that are most widespread and hence will be most commonly encountered by receivers in the real world). Such knowledge has fed into the receiver testing to test receivers against those threats.
- Although we don't know yet which physical jammer (make / model) goes with which signal, we have a lot of jammer families recorded in the database and so potentially in future this could be helpful when jammers are confiscated to test them, match up against database and start to see what jammer matches what signal.
- Having this big database of threats has also allows us to see some emerging trends, such as new types of jammers (e.g. the 'tick' signal), differences in the type of jammers that are common in different cities or countries, and how people's use of jammers could be changing (e.g. use of two separate jammers at the same time).

Going forward, the main recommendation would be that the best way to deploy monitoring equipment depends on what you want to achieve from the monitoring:

- For users and stakeholders that want to assess the level of activity at a high level, gather evidence of the sort of threats that are out there, check changes in activity over time (e.g. in response to legislation) or do things like track and/or locate jammers and interference then the best deployment is to have a network of equipment located in cities and close to major roads where you are likely to see the most activity, and hence capture as many different examples as possible. This approach could be beneficial to governments, frequency/spectrum regulators, etc.
- However, for users that want to protect a particular site or infrastructure then deployments of monitoring equipment are best at the exact location of interest that you want to protect in order to see the exact threats that are affecting it. This is because interference and impact at a particular location is affected by many factors, including type of receiver, distance to interference, blockages / obstructions from buildings, etc. and so even monitoring close-by does not give the same picture. This sort of approach would suit owners and operator of particular sensitive infrastructures (e.g. GBAS, SBAS RIMS, airports in general, etc.)
- A third type of installation could be one to identify vehicles with jammers for enforcement purposes. This has not been specifically looked at within STRIKE3 (the focus was on detection and no attempts at identification have been made) but lessons from certain installations can be helpful to guide this. We can see, for example, that installations in cities with the antenna high on a roof are not good for identification and enforcement because they detect many different signals from nearby and far away vehicles, making identification difficult. However, installations that are set very close to the road, and even have 'natural' barriers and traffic control (such as toll booths and border crossings) could easily be used to detect and identify specific vehicles with jammers.

## D6.2: Threat Database Analysis Report

**Ref:** STRIKE3\_D62\_DatabaseRep

**Issue:** 1.0

**Date:** 25.01.19

---

**END OF DOCUMENT**