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

STRIKE3

D4.1: Draft Standards for Threat Monitoring and Reporting

Prepared by:	M Pattinson (NSL), D Fryganiotis (NSL), P Eliardsson (FOI)	25/01/19
Checked by:	M Dumville (NSL)	25/01/19
Authorised by:	M Dumville (NSL)	25/01/19

Pages: 27

Document Classification: Public

Change Record

Issue Rev	Date	§: Change Record	Author(s)
1.0	30.01.2017	First version of document delivered for Requirements Review	MP / DF/ PE
1.1	16.03.2017	Updated version following external review and changes agreed at Requirements Baseline Review meeting: • DRS Id. 3: Added new requirements on STRIKE3 centralised server performance to table 5-1, and added new table for STRIKE3 monitoring system requirements • DRS Id. 4: Format of requirements table modified to include Req Id, title, description, verification and comments • DRS Id. 6: Added note in section 6.2.1 that firewall in the diagram is a software utility to block incoming connections rather than a hardware component • DRS Id. 10: Text added to section 6.3.1 to add some more detail. In addition, names of interfaces and web services have been modified to be consistent in section 6 and section 7. • DRS Id. 11: Label in figure 6-6 corrected to 'Adv. Data Request Service' • DRS Id. 12: Corrected typo in tables 6-2 to 6-5 from SAOP to SOAP. • DRS Id. 13: Clarified in section 7.1 that group A and B refer to web services, and modified earlier section 6.3 so that there is consistency in naming.	MP / DF / PE
2.0	10.11.17	Updated version delivered for Deployment Readiness Review at end of WP5: Threat Reporting Validation Platforms: • Updated description of events 'a' and 'b' in section 3.4 according to new work and removed TBCs (RBR DRS Id 2) • Modified web services definitions as necessary in section 7 following work during implementation	MP / DF

Issue Rev	Date	§: Change Record	Author(s)
2.1	30/11/17	Minor updates following Deployment Readiness Review to include WSDL files in Annex and correct formatting	MP
3.0	25/01/19	Final version updated for end of project following validation process: • Added site ID to information for event • Added list of sites (with Site ID) to registration info for networks	MP, PE

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Purpose of Document

This document is the Draft Standards for Threat Monitoring and Reporting. The main objectives of this document are to:

- Develop draft standards for threat monitoring and reporting, to include rationale and justification of the proposed approach
- Identify minimum specifications and identify potential scope for extension and enhancement

It should be noted that the focus of the STRIKE3 project is on interference for the GPS L1 band and this is reflected in the threat reporting standards. Nevertheless, possible extensions to allow reporting of threats in different frequency bands are highlighted in the draft standards.

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

The lead partner for WP4 is SAC. This document has been prepared by NSL and FOI with contributions from NLS and review and comment by SAC, AGIT, ETRI and GNSS labs.

The current version of the document is the final version from the project and includes modifications to previous versions based on experience from validation of the standards through long-term monitoring, and comments from external review of the document by other interested parties.

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

The first sections of the document are the generic sections related to proposed draft standards for threat reporting:

- **Section 1** the current section, is an introduction which describes the purpose, scope and structure of the document.
- **Section 2** provides an overview of the proposed threat monitoring and reporting system;
- **Section 3** contains the definition of the proposed reporting message standard;
- **Section 4** details the user side, in terms of standard analysis and data access.

1.4 References

1.4.1 Applicable Documents

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

Table 1-1: Applicable Documents

1.4.2 Reference Documents

No.	Reference
RD1	

Table 1-2: Reference Documents

1.5 Acronyms

Acronym	Definition
AGC	Automatic Gain Control
C/N0	Carrier to Noise density ratio
CORS	Continuously Operating Reference Station
dB	Decibel
FTP	File Transfer Protocol
GPS	Global Positioning System
GNSS	Global Navigation Satellite System
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
RF	Radio Frequency
SNR	Signal to Noise Ratio
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
SSL	Secure Sockets Layer
TBC	To Be Confirmed
TLS	Transport Layer Security
UTC	Universal Time Coordinated
WAN	Wide Area Network
WP	Work Package
WS	Web Service
WSDL	Web Service Definition Language
XML	Extensible Markup Language

Table 1-3: Acronyms and Abbreviations

1.6 Terminology

Detection Equipment

This is equipment that is used to detect GNSS interference. Different types of detection equipment may function in different ways, e.g. through power- or AGC-monitoring, or through monitoring of post-correlation values such as C/N0.

Sensor

This is a generic term for deployed equipment that is used for GNSS interference monitoring and reporting. A sensor will consist of some **Detection Equipment** plus other necessary components such as GNSS antenna, communications, etc.

Monitoring Site

This is a physical location that hosts one or more **sensors**.

Local Event Database

This is a database that stores all interference event information reported by one or more **sensors**. The information that is stored in a local event database will depend on the capabilities and configuration of the **sensors**, but may include additional information such as I/Q data, signal type classification, etc., as well as the times of detected events and power levels.

Monitoring Network

This is a collection of multiple **monitoring sites** that are somehow connected, for example being operated by a single **monitoring network operator** or reporting to a common **Local Event Database**.

Monitoring Network Operator

A monitoring network operator is someone who operates a **monitoring network** in the sense that they are responsible for the data that is produced by the network, including interference events.

Data Provider

A data provider is someone who provides interference information to the **centralised server** using the reporting standards defined in this document. The data provider is also sometimes known as a **Contributor**.

Centralised Server

This is a function for collecting interference event reports (according to the reporting standard format and contents) from multiple **data providers** (**contributors**) for storage in a **centralised database**. The centralised server also providers an interface for **end users** to access information and view analysis and statistics about reported interference events.

Centralised Database

This is used to store the information from the interference event reports provided to the **centralised server** by the **data providers**.

End User

This is someone who wishes to view information (including analysis and statistics) about the combined set of interference events stored in the **centralised database**.

2 Overview of Threat Monitoring and Reporting System

2.1 Rationale for Threat Monitoring and Reporting Standards

Dependence on GNSS is increasing as GNSS is used for an ever expanding range of safety, security, business and policy critical applications. However, increasing dependence on GNSS brings a risk that such services can be affected by interference on GNSS – either unintentional or intentional. In order to understand the level of threat, and to develop effective countermeasures against interference, it is highly desirable to monitor for interference in a systematic way and to share the results with interested stakeholders. There are a number of different types of detection equipment that can be used to detect GNSS interference, and there are previous and existing projects and monitoring campaigns to try to detect interference. However, although these types of local monitoring efforts can be effective at monitoring and protecting a specific site or local area, the ability to combine results from different detection equipment and monitoring networks and gain a wider understanding of the level of threat is limited for several reasons. Firstly, different detection equipment and monitoring networks report different values and statistics about interference events and so it is not always easy to combine results. Secondly, different types of detection equipment have different detection algorithms and thresholds as they are designed for different purposes, and so different types of detection equipment installed at the same site may report completely different numbers of events.

The goal of this document therefore is to propose a system architecture and draft reporting standard that can enable the results from different types of detection equipment and monitoring networks to be reported in a common format and combined in common analysis. Such a system could be very valuable in monitoring the level of threat posed by GNSS interference over large areas and to see how the threat changes over time by combining data from many different types of monitoring network.

2.2 Description of Proposed System

2.2.1 High Level Concept

The proposed threat monitoring and reporting system consists of two main elements:

- Sensors (for detecting interference and reporting events)
- Centralised server (for collating reports from the different sensors in a centralised database and providing access to the results for end users).

In this concept, the sensors are operated independently of the centralised server, i.e. there is no need to deploy specific monitoring networks or a single specified type of detection equipment to support the centralised database of events. It is the intention to allow different types of detection equipment from different manufacturers to be used for interference monitoring, and to enable already deployed sensors and monitoring networks to contribute to the centralised database, as well as new installations.

The centralised server will act as a central hub to collect results from different sensors deployed in a variety of monitoring networks, and allow end users to view information about the events and generate statistics.

The purpose of the threat reporting standards defined in this document is therefore to ensure that the information about interference events from different monitoring networks and types of detection equipment is reported in a standard way so that meaningful analysis and statistics can be generated at the centralised server. This overall architecture is illustrated in the following figure.

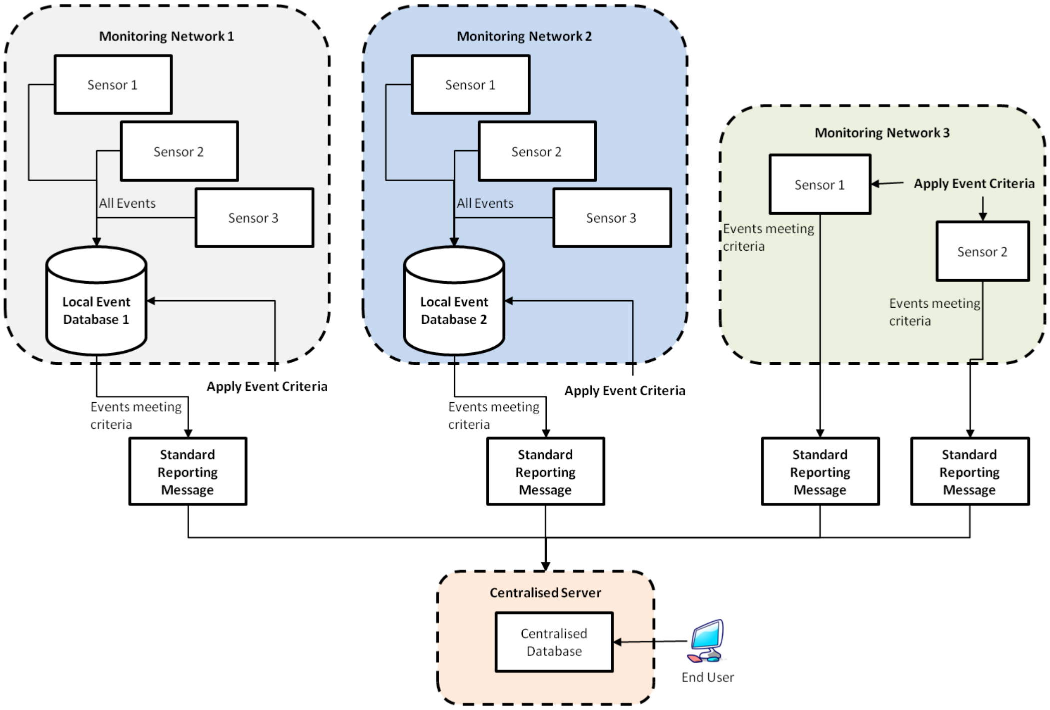

Figure 2-1: Overview of Threat Monitoring and Reporting System Concept

The proposed reporting message contents are defined in section 3. The philosophy behind the proposed messages is to have a minimum required set of information about events that will allow analysis of event occurrence and evolution over time without compromising site anonymity, whilst also providing a mechanism for those authorities that wish to do so to provide additional information about events.

The logic of this approach is as follows:

- Sensors (using different types of detection equipment) will be used to detect interference events. The sensors may be deployed in a monitoring network where they report to their own local event database or the sensors may store data locally at the sensor;

- Interference events that are detected by the sensors will be provided to the centralised server for storage in the centralised database following the proposed standards:
    - The events detected by the detection equipment at the sensors must be checked against the standard event criteria (defined in section 3) as a pre-filtering step. Only those that meet the event definition criteria should be provided to the centralised server. This pre-filtering can be done either at a local network database (as in ‘other monitoring network 1’ in Figure 2-1) or at the sensor itself (as in ‘other monitoring network 2’ in Figure 2-1);
    - Those events that meet the event definition criteria must be formatted according to the reporting standard and provided to the centralized server;
        - A minimum set of mandatory information is defined for all events;
        - Optional fields are also available to allow organizations to provide additional information that is interesting for more detailed analysis if so desired;
    - It is foreseen that contributing organizations will need to register before they can contribute to the centralized database.
- The centralised server will store all the events received from the different sensors in a centralised database
    - Only the information received in the standard reports will be stored. This is purposely kept high-level to avoid having sensitive information (e.g. I/Q data) at the centralised database;
- An interface will be available to allow end users to access the information in the centralized database in order to view the information about events and perform some simple analysis.
    - As the information stored in the centralized server is only high-level, the sort of analysis and results that can be viewed will be quite basic but will allow a widescale analysis of level of threat activity and change of threat level over time;
    - It is envisaged that this interface will also allow correspondence between the end users and monitoring network operators who contribute information about events to the centralised server. This provides a mechanism for end users to obtain additional detailed information about certain events from the organisation that owns the data (e.g. event time, precise location, raw data sample, etc.), and also allows monitoring network operators to provide additional data and services to interested end users.

2.2.2 Justification of Proposed Approach

When defining the proposed reporting standards and system architecture there were a number of elements to consider, many of which are conflicting. For example, adding more detailed information about events to the test standards increases the level of analysis that is available at the centralised server and makes this more attractive to end users, but on the other hand having more detailed information in the event messages may raise sensitivity and security issues in terms of the data, which may increase the requirements on the centralised server and may also discourage monitoring network operators from wanting to contribute data in the first place. Similarly, imposing more constraints on the detection equipment at the sensors can help to ensure that events reported by different sensors and monitoring networks are compatible, but if too proscriptive may reduce the available pool of sensors and networks that are able (and willing) to report according to the standards. The draft standards proposed in this document reflect a compromise of all these different aspects to try to maximise the number of sensors and monitoring networks that will be able (and willing) to report, whilst still ensuring that the core results are useful to end users. Some of the key points and their justification are described below.

2.2.2.1 Definition of standard event criteria

Any analysis of the level of threat and changing nature of the threat requires a large amount of data from a large number of sites in order to be meaningful. This is best achieved through allowing results from different types of detection equipment from different monitoring networks to be combined, as this means that any monitoring site can potentially contribute data and there is no need for a dedicated (costly) deployment activity tied to a single supplier. However, different types of interference detection equipment will perform detections in different ways using different types of check and different thresholds. The result is that two different types of detection equipment deployed at a single site may not report the same number of interference events, which means that it is difficult to combine the raw figures from different systems.

One way to overcome this would be to define a standard detection algorithm and thresholds that all types of detection equipment need to adhere to. However, that would necessitate changes to the detection equipment itself. Under this approach it would take some time before compliant equipment was available (even after standards were agreed), and may not be attractive to suppliers of detection equipment anyway – depending on the purpose of the monitoring activity it may be entirely justified that different algorithms and different thresholds are used in different situations depending on whether the purpose of the monitoring is for protection of an area against interference, for enforcement, or for research purposes.

The approach proposed in these standards attempts to overcome some of these difficulties whilst still ensuring that reports from different systems are compatible. In section 3 two event definitions are provided - one based on the power of detected interference signal and one based on signal to noise ratio (SNR) of the GPS signals. The idea is that any individual sensor or monitoring network operator that wishes to contribute to the centralized server and database will first check their detected events against the threat definition, and only those that meet the criteria are reported. This has the following benefits:

- Having this pre-filtering step allows very low level events that will not impact GPS to be filtered out, hence ensuring that only those events that may be of significance to be reported;

- Having this common event definition ensures that there is consistency in the types of event that are reported by different types of monitoring equipment and different;
- Having multiple types of event definition allows different types of detection system to contribute to the centralized server, hence increasing the potential number of sensors that can contribute to the results;
- Applying these event criteria as a pre-filtering stage to events before they are submitted to the centralised server rather than at the initial detection stage means that there is no need to change the detection algorithms or thresholds within the detection equipment at the sensors. This means that existing sensors and monitoring networks can continue to operate according to their designed purpose (for enforcement, research, etc.) without any modification.

2.2.2.2 Minimum set of information in reporting standard

The more information that is available about events, the more a user can know about the event and the more detailed analysis can be performed. For example, with detailed information about timing, location, type of signal, etc, it becomes possible to make some assessment of the likely causes of events. However, providing very detailed information about events raises issues of sensitivity and security. Certain organizations may not wish to provide such detailed information, and even if they do the data security and integrity requirements for the centralized server will increase.

Therefore the approach taken in these draft standards is to define a minimum required set of information about events that all data providers must contribute. This minimum set is designed to provide useful information to allow analysis and the level of threat and change in threat over time, but does not include sensitive information. This should help to avoid discouraging organizations from providing event information.

If more detailed information about events is available then data providers may choose to provide this as optional information. Alternatively, they may simply store the additional information at their local event database over which they have control and which could potentially be provided via another means to authorized end users for detailed analysis and assessment.

2.2.2.3 Contributor and user registration

One question when considering the standards and the centralised server is how open to make the data and the results. Should the server be open for anyone to contribute to and for any user to access, or should it be restricted in some way?

With the proposed architecture it is envisaged that there will be a registration process both for potential data providers and for end users who want to view the information. This is not necessarily to restrict who can have access but more to have some control of the data that is provided to the centralized server, and to encourage the use of the standards and centralized server through opening up the possibility of additional services.

For example, if an end user wants to see further details about an event or all events from one or more monitoring sites, this proposed architecture provides the capability for them to make contact with the applicable data provider to arrange access to more detailed data that is available from the local event database. In this way, the centralized server acts not only as somewhere to view useful analysis of the general level of threat over a wide area, but also as a platform to link end users and data providers and allow the exchange of more detailed data for additional services. Having such a function potentially offers a further incentive to monitoring network operators to provide information to the centralised server.

3 Proposed Reporting Message

3.1 Overview of Approach

The purpose of the proposed reporting message is to share information about detected jamming events, within an interference monitoring network, to a centralised server. Information about detected events can be distributed to the server in near-real time or in periodic batches, e.g. once every month.

For a detected interference event some estimated metrics or some information about the interference event might be sensitive for an organization to share within a big community. Therefore, privacy and security aspects have been considered when the proposed reporting message was developed. The reporting message consists of two types of data; mandatory information and optional information. The intention behind the mandatory information is that this should only be non-sensitive information that could be shared by everyone to a big community. Information that potentially could be sensitive for someone to share is left in the optional part of the reporting message.

Many different interference monitoring networks will potentially use this reporting message for sharing of data about detection events to a centralised server. These monitoring networks will most likely have their own technology for how they detect jamming events which will lead to many different definitions of what an interference event is. Therefore, two different types of interference event definition is provided herein. Without a common basis of what an interference event is, it would be very difficult to do reliable statistics and trend analysis at the centralized server.

In the following sections the contents of the proposed reporting messages will be described. The exact format of the transferred messages between the interference monitoring network and the centralized server is not described here, but will be further developed and distributed at a later date.

3.2 Event Message Definition

The contents of the event message are described in Table 3-1. 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). *Note: See event definition section Table 3-5 for a definition of the different types.*	No
Frequency band	The frequency band where this interference event was detected. The current options are; 1575.42 MHz *Note: This could be extended in the future to cover other frequency bands that are not supported at this moment.*	No
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
Site ID	An anonymous, but unique, ID for the site where the event was detected. The site id should be specific for a physical location. It should not be possible to determine the actual position of the site from this ID. If the detection equipment is installed at a platform that moves around, for example a boat, this should be treated as one site and not multiple sites as the platform moves around.	No
Date	The date (relative UTC) of when this event was detected.	No

Field	**Description**	**Optional**
Start time	The UTC timestamp of when this event was detected. *Note: Start time is not required as mandatory, but it is highly recommended that the start time is reported for the event.*	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. *Note: The user interface will render the spectrum figure in the same format for all different types of interference detection systems.*	*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). *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.*	*Yes*
Delta power	Maximum delta power in decibel (dB) above systems noise floor at the specific monitoring site. *Note: This is only applicable when event definition type a) is used.*	*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 *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.*	*Yes*
Delta C/N0	Maximum decrease in C/N0 in decibel (dB) relative the C/N0 without interference of the receiver at the specific monitoring site. *Note: This is only applicable when event definition type b) is used.*	*Yes*

Table 3-1: Description of the information shared for each detected event.

3.3 System Information Message Definition

It can be foreseen that potentially many different types of GNSS interference monitoring networks are going to send regular reports to the centralised server. The different monitoring networks will most likely consist of different sensors with different types of detection equipment, or a combination of detection equipment from different manufactures. Different sensors are, most likely, going to have different technical specification and thus different capabilities in, for example, which frequency band they will be able to detect interference, their detection performance etc. Therefore, the centralized server will build up a table of all available types of detection equipment that are used in the different monitoring networks. For each type of detection equipment, the information shown in Table 3-2 will be stored at the centralised server. Detection equipment can, potentially, cover multiple frequency bands with various bandwidths. Such equipment should report their frequency bands as a vector of individual frequency band together with a vector of corresponding bandwidths.

Field	**Description**	**Optional**
Name	Descriptive name of the type of Detection Equipment	No
Manufacturer	Manufacturer of the interference detection equipment	No
Bandwidth	Monitoring bandwidth in MHz. *Note: For a multiband system this is reported as a vector of multiple bandwidths. The length should be equal to the frequency band vector.*	No
Frequency band	Centre frequency, of the monitoring frequency bands, in MHz. *Note: For a multiband system this is reported as a vector of multiple frequency bands. The length should be equal to the bandwidth vector.*	No
Software version	Version of the Detection Equipment software.	*Yes*
Hardware version	Version of the Detection Equipment hardware.	*Yes*

Table 3-2: Description of Type of Detection Equipment that is used

Field	**Description**	**Optional**
Site ID	An anonymous, but unique, ID for the site. The site id should be specific for a physical location. It should not be possible to determine the actual position of the site from this ID. If the detection equipment is installed at a platform that moves around, for example a boat, this should be treated as one site and not multiple sites.	No

Field	Description	Optional
Equipment type	Equipment type for detection equipment at this site. Individual sensors are described according to Table 3-2	No

Table 3-3: Description of Sites in the Network

For an interference monitoring network the information shown in Table 3-4 is needed at the registration phase of the network. The mandatory part is very basic, just a name of the network and contact details to a person, which is responsible for the monitoring network. A list of one or multiple types of detection equipment are also mandatory, as discussed above.

Field	Description	Optional
Name	Descriptive name of the monitoring network, used to identify their reported events.	No
Contact	Contact information to the organization that has provided information to the database. To be used for managing the registration and interface between the organization and the central database operator.	No
Sites	A list of sites operating within the network.	No
Detailed information	A detailed list of other types of information that is available at the local event database for authorized personnel only, plus details of how to access this detailed information (e.g. email contact details for request, ftp site details, etc.).	*Yes*

Table 3-4: Description of an interference monitoring network.

3.4 Event Definition

To be able to compare results and statistics from different interference monitoring networks is important to have a common definition of what an interference event is. Without a common definition it will be impossible to do a comparison. However, even if the criteria for an event is well defined, it is in the end the sensitivity of the detection system that defines when the event is detected.

In Table 3-5 two types of events are defined. Event type a) is intended for interference detection equipment that is capable of measuring received power or GNSS-receivers that provide AGC (Automatic Gain Control) information. Type b) is intended to be used by detection equipment that is based on GNSS-receivers only, for example CORS networks.

Type	Description
a	This event definition is intended for interference detection equipment that base the detection function on either power- or AGC-monitoring. If the received power is 5 dB stronger than the expected noise power and if the event duration is greater than 5 seconds, then an interference event should be reported. Where: • the expected noise power is the measured received power 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 received power first exceeds the 5 dB threshold for increase • 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 *Note: For AGC-monitoring systems this means a decrease of 5 dB in the AGC value and it should last at least for 5 seconds.*
b	This event definition is intended for interference based on GNSS-receivers without AGC enabled, where measured C/N0 is compared against expected C/N0 to detect events. 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

Table 3-5: Different types of event definitions.

The threshold for event type a) and b) are selected so that the reported event most likely will affect the performance of a GNSS receiver negatively. There could however be many detections made that do not fulfil these event requirements. One reason could be that the distance to the interference source is too large so that the energy that reaches the detection system is less the than the threshold stated in the event definition. The basic problem is the geometry between the interference source, detection system and the victim receiver. It is when the victim receiver and the detection systems is not co-located the problem arises.

In both of the event definitions a) and b) the thresholds are relative to an expected level, for example noise power or C/N0. These levels will be different from site to site. Therefore, sites with low expected noise power are more sensitive or have better detection distance compared to sites with higher expected noise power. This means for a GNSS receiver that is installed at a site with higher expected noise power that the C/N0 will be a few dB less compared with a GNSS receiver at a site with low expected noise power. The detected interference event according to for example definition b) can therefore be more severe for the GNSS receiver with lower expected C/N0.

The decrease in C/N0 can also be very dependent on the GNSS receiver type. Different manufactures can have implemented various interference mitigation techniques, which will affect how the C/N0 response to different interference signals. Therefore, might one GNSS receiver mark an interference source as an interference event while another receiver will not, according to definition b).

Event definition type a) and b) both have the drawback that they are relative to the noise power at the corresponding site. However, they are quite straightforward to implement in many types of detection equipment. A more sophisticated definition could in the future be based on correlation of received signals to a threat database. With that definition, the received waveform characteristics are correlated with characteristics of known interference source in the database. Some of this interference source could be so well known so that the output power of the source is known. Then it will be more realistic to predict the impact of the interference source for a GNSS receiver in the surrounding of the interference detection equipment. As the capabilities and performance of detection equipment evolve in the future, additional event definitions could be added to the reporting standards.

4 Analysis and User Access

4.1 Introduction

The previous sections have described the overall concept of the reporting system and have detailed the threat reporting messages and event definition. Together these explain what information about interference events is reported to the centralised server.

On the other hand, the information that is reported in the event messages is only useful if it is made available for end users to view and analyse. At a high level, it is proposed that any potential end user will register in order to gain access to the information. Once registered, end users will be able to access the data and results through a defined interface. This section therefore provides some further description of the envisaged user access for the reporting system.

4.2 Baseline Analysis

The minimum set of information defined in the proposed reporting message includes the following information:

- Event date
- Event type (power or SNR based detection)
- Affected frequency band (nominally GPS L1 but potentially others in the future)
- Country

With this information the following basic analysis can easily be provided:

- Total number of events in a defined period
    - Filtered on location information (e.g. all sites, per country)
    - Filtered on event type (e.g. power or SNR)
    - Filtered on affected frequency band (e.g. all events or GPS L1 only)
- Time variation of number of events in a defined period (e.g. daily, weekly or monthly number of events)
    - Filtered on location information (e.g. all sites, per country)
    - Filtered on event type (e.g. power or SNR)
    - Filtered on affected frequency band (e.g. all events or GPS L1 only)

In combination with figures for how many monitoring sites are in each country, such analysis (although simplistic) allows end users to assess relative levels of detected events between countries and between different sites, and also allows the changing level of threat over time to be assessed.

4.3 Extended Analysis and Data Requests

The proposed reporting standards also make provision for the inclusion of additional data above the minimum set.

If data providers wish to include this additional information (e.g. start time, duration, frequency spectrum, etc.) as part of the information they provide to the centralised database they can do so. End users can then retrieve this information from the database for those events and can perform extended analysis.

In addition, data providers may store additional information about events in their own local event database, but for security or confidentiality reasons may not wish to provide it openly to the centralised database without restrictions. In these circumstances the proposed message formats allow for contact details and/or data access information to be provided to end users on request for particular events. In that way, authorized end users can gain access to additional data to perform more detailed analysis, but this remains under the control of the original data providers.

END OF DOCUMENT