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)	30/11/17
Checked by:	M Dumville (NSL)	30/11/17
Authorised by:	M Dumville (NSL)	30/11/17

Pages: 99

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

Table of Contents

1 Introduction 12
1.1 Purpose of Document 12
1.2 STRIKE3 Overview 12
1.3 Document Overview 12
1.4 References 13
1.4.1 Applicable Documents 13
1.4.2 Reference Documents 14
1.5 Acronyms 14
1.6 Terminology 15
2 Overview of Threat Monitoring and Reporting System 17
2.1 Rationale for Threat Monitoring and Reporting Standards 17
2.2 Description of Proposed System 17
2.2.1 High Level Concept 17
2.2.2 Justification of Proposed Approach 19
2.2.2.1 Definition of standard event criteria 20
2.2.2.2 Minimum set of information in reporting standard 21
2.2.2.3 Contributor and user registration 21
3 Proposed Reporting Message 23
3.1 Overview of Approach 23
3.2 Event Message Definition 23
3.3 System Information Message Definition 25
3.4 Event Definition 27
4 Analysis and User Access 30
4.1 Introduction 30
4.2 Baseline Analysis 30
4.3 Extended Analysis and Data Requests 31
5 Reporting System Requirements 32
5.1 Introduction 32
5.2 High Level Requirements 32
6 Demonstration Reporting System Design 40
6.1 Introduction 40

6.2 High Level Design of STRIKE3 Centralised Server 40
6.2.1 Overview 40
6.2.2 Description of STRIKE3 Gateway 41
6.2.3 Description of the SQL Database Server 42
6.3 Description of Interfaces 43
6.3.1 Overview 43
6.3.2 Account Management Services Interface 45
6.3.3 Report Upload Service Interface 46
6.3.4 Data Mining Service Interface 47
6.3.5 Advanced Data Request Service Interface 48
6.4 Implementation 48
7 Demonstration Web Service Definition 50
7.1 Introduction 50
7.1.1 Data Integrity 51
7.1.2 Message Structure 51
7.1.2.1 Message Digest Node 51
7.2 Account Management Services (Monitoring Network) 52
7.2.1 Add_IMN Request Message 52
7.2.1.1 Header Node 52
7.2.1.2 Body Node 52
7.2.2 Add_IMN Response Message 55
7.2.2.1 Header Node 55
7.2.2.2 Body Node 55
7.2.2.3 Negative Response Node 56
7.2.3 View_IMN Request Message 57
7.2.3.1 Header Node 57
7.2.3.2 Body Node 57
7.2.4 View_IMN Response Message 58
7.2.4.1 Header Node 58
7.2.4.2 Body Node 58
7.2.4.3 Negative Response Node 60
7.2.5 Edit_IMN Request Message 61
7.2.5.1 Header Node 61

7.2.5.2 Body Node 62
7.2.6 Edit_IMN Response Message 64
7.2.6.1 Header Node 64
7.2.6.2 Body Node 64
7.2.7 Delete_IMN Request Message 65
7.2.7.1 Header Node 65
7.2.7.2 Body Node 65
7.2.8 Delete_IMN Response Message 66
7.2.8.1 Header Node 66
7.2.8.2 Body Node 66
7.3 Report Upload Service 67
7.3.1 Push_IR Request Message 67
7.3.1.1 Header Node 67
7.3.1.2 Body Node 68
7.3.2 Push_IR Response Message 70
7.3.2.1 Header Node 70
7.3.2.2 Body Node 71
7.4 Account Management Services (End Users) 72
7.4.1 Add_IMU Request Message 72
7.4.1.1 Header Node 72
7.4.1.2 Body Node 72
7.4.2 Add_IMU Response Message 73
7.4.2.1 Header Node 74
7.4.2.2 Body Node 74
7.4.2.3 Negative Response Node 75
7.4.3 View_IMU Request Message 75
7.4.3.1 Header Node 75
7.4.3.2 Body Node 76
7.4.4 View_IMU Response Message 76
7.4.4.1 Header Node 76
7.4.4.2 Body Node 77
7.4.4.3 Negative Response Node 78
7.4.5 Edit_IMU Request Message 78

7.4.5.1 Header Node 79
7.4.5.2 Body Node 79
7.4.6 Edit_IMN Response Message 80
7.4.6.1 Header Node 80
7.4.6.2 Body Node 81
7.4.7 Delete_IMU Request Message 81
7.4.7.1 Header Node 81
7.4.7.2 Body Node 82
7.4.8 Delete_IMU Response Message 82
7.4.8.1 Header Node 82
7.4.8.2 Body Node 83
7.5 Data Mining Service 84
7.5.1 Get_IMD Request Message 84
7.5.1.1 Header Node 84
7.5.1.2 Body Node 85
7.5.2 Get_IMD Response Message 86
7.5.2.1 Header Node 86
7.5.2.2 Body Node 87
7.5.2.3 Negative Response Node 90
7.6 Advanced Data Request 92
7.6.1 Get_Adv_IMD Request Message 92
7.6.1.1 Header Node 92
7.6.1.2 Body Node 92
7.6.2 Get_Adv_IMD Response Message 93
7.6.2.1 Header Node 93
7.6.2.2 Body Node 93
7.6.2.3 Negative Response Node 95
8 Future Considerations 96
Annex 98

List of Tables

Table 1-1: Applicable Documents 13
Table 1-2: Reference Documents 14
Table 1-3: Acronyms and Abbreviations 15
Table 3-1: Description of the information shared for each detected event. 25
Table 3-2: Description of Type of Detection Equipment that is used 26
Table 3-3: Description of an interference monitoring network. 27
Table 3-4: Different types of event definitions. 28
Table 5-1: High Level Reporting System Requirements – STRIKE Centralised Server 33
Table 5-2: High Level Reporting System Requirements – STRIKE3 Monitoring systems 38
Table 6-1: Technical Interface definitions 44
Table 6-2: ITF001 description 45
Table 6-3: ITF002 description 46
Table 6-4: ITF003 description 47
Table 6-5: ITF004 description 48
Table 7-1: Message Digest Node 51
Table 7-2: Add_IMN – Request Header Node 52
Table 7-3: Add_IMN – Request Body Node 53
Table 7-4: Add_IMN – Response Header Node 55
Table 7-5: Add_IMN – Response Body Node 55
Table 7-6: Add_IMN – Negative Response Node 56
Table 7-7: View_IMN – Request Header Node 57
Table 7-8: View_IMN – Request Body Node 57
Table 7-9: View_IMN – Response Header Node 58
Table 7-10: View_IMN – Response Body Node 58
Table 7-11: View_IMN – Negative Response Node 61
Table 7-12: Edit_IMN – Request Header Node 61
Table 7-13: Edit_IMN – Request Body Node 62
Table 7-14: Edit_IMN – Response Header Node 64
Table 7-15: Edit_IMN – Response Body Node 64
Table 7-16: Delete_IMN – Request Header Node 65
Table 7-17: Delete_IMN – Request Body Node 65
Table 7-18: Delete_IMN – Response Header Node 66

Table 7-19: Delete_IMN – Response Body Node 66
Table 7-20: Push_IR – Request Header Node 67
Table 7-21: Push_IR – Request Body Node 68
Table 7-22: Push_IR – Response Header Node 71
Table 7-23: Push_IR – Response Body Node 71
Table 7-24: Add_IMU – Request Header Node 72
Table 7-25: Add_IMU – Request Body Node 72
Table 7-26: Add_IMU – Response Header Node 74
Table 7-27: Add_IMU – Response Body Node 74
Table 7-28: Add_IMU – Negative Response Node 75
Table 7-29: View_IMU – Request Header Node 75
Table 7-30: View_IMU – Request Body Node 76
Table 7-31: View_IMU – Response Header Node 76
Table 7-32: View_IMU – Response Body Node 77
Table 7-33: View_IMU – Negative Response Node 78
Table 7-34: Edit_IMU – Request Header Node 79
Table 7-35: Edit_IMU – Request Body Node 79
Table 7-36: Edit_IMU – Response Header Node 80
Table 7-37: Edit_IMU – Response Body Node 81
Table 7-38: Delete_IMU – Request Header Node 81
Table 7-39: Delete_IMU – Request Body Node 82
Table 7-40: Delete_IMU – Response Header Node 83
Table 7-41: Delete_IMU – Response Body Node 83
Table 7-42: Get_IMD – Request Header Node 84
Table 7-43: Get_IMD – Request Body Node 85
Table 44: Get_IMD Request - Query rule options 85
Table 7-45: Get_IMD – Response Header Node 86
Table 7-46: Get_IMD – Response Body Node 87
Table 7-47: Get_IMD – Negative Response Node 90
Table 7-48: Get_Adv_IMD – Request Header Node 92
Table 7-49: Get_Adv_IMD – Request Body Node 93
Table 7-50: Get_Adv_IMD – Response Header Node 93
Table 7-51: Get_Adv_IMD – Response Body Node 94

Table 7-52: Get_Adv_IMD – Negative Response Node 95

List of Figures

Figure 2-1: Overview of Threat Monitoring and Reporting System Concept 18
Figure 6-1: STRIKE3 Centralised Server Architecture 41
Figure 6-2: STRIKE3 Centralised Server Interfaces 43
Figure 6-3: Account Management Service Interface 45
Figure 6-4: Report Upload Service Interface... 46
Figure 6-5: Data Mining Service Interface 47
Figure 6-6: Adv. Data Request Service Interface.. 48

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.

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.

The second half of the document contains specific information related to the design of the demonstration threat reporting system within STRIKE3, and is provided as supporting information to those who wish to contribute to or access data from the STRIKE3 demonstration server:

- **Section 5** contains requirements for the system to support threat monitoring and reporting;
- **Section 6** presents the preliminary system design;
- **Section 7** contains the preliminary web service definition;
- **Section 8** contains a section on future considerations;
- **Annexes** contain the WSDL files for the web services.

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

Acronym	Definition
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.

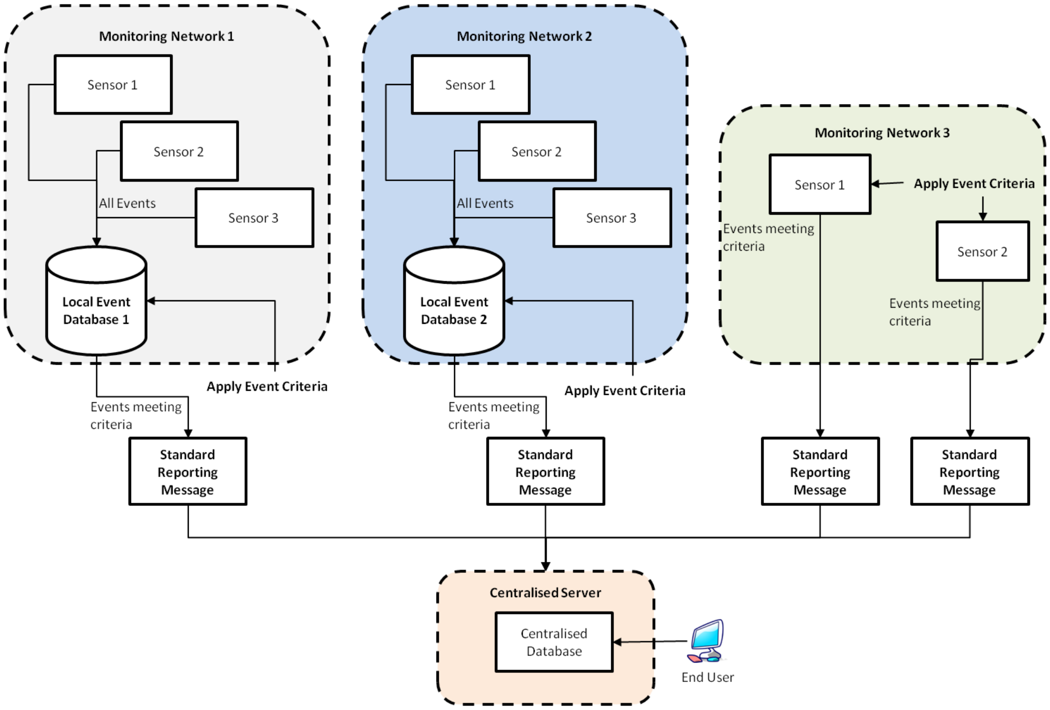

Figure 2-1: Overview of Threat Monitoring and Reporting System Concept

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 3-4 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
Date	The date (relative UTC) of when this event was detected.	No
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*

Field	Description	Optional
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

For an interference monitoring network the information shown in Table 3-3 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
Equipment types	A list of used types of detection equipment within the network. Individual sensors are described according to Table 3-2	No

Field	Description	Optional
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 3-3: 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 3-4 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 3-4: 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.

5 Reporting System Requirements

5.1 Introduction

In order to support the threat reporting standards and the system concept proposed in sections 2 and 3, it is necessary to design and implement a reporting system architecture to demonstrate the approach. The development will be in the context of the STRIKE3 project and so will be a demonstration system rather than an operational system. Nevertheless, the design and implementation must be practical and be representative enough to demonstrate how such a system could work in practice.

The high level requirements for this demonstration reporting system within the STRIKE3 project are defined in the following section.

5.2 High Level Requirements

The following tables detail the high level requirements for the demonstration STRIKE3 reporting system to be developed within the STRIKE3 project. There are separate tables for the centralised server and for the monitoring systems that will contribute to the STRIKE3 centralised server.

These are the key requirements that will influence the design and will be validated during the project in order to demonstrate the threat reporting standards and overall concept.

For the verification method, the possible methods are:

- Review: requirement will be verified through review of design documents
- Test: requirement will be verified through a defined test case with set pass/fail criteria
- Demonstration: requirement will be verified through demonstration of system operation

Table 5-1: High Level Reporting System Requirements – STRIKE Centralised Server

Category	Req Id	Req Title	Description	Verification Method	Comments
Interface - input	STRIKE3-CS-INT-001	Server Input Event Format	The STRIKE3 centralised server shall take as input interference event reports in the defined format	Test	Format and contents according to section 3
	STRIKE3-CS-INT-002	Server Input Reporting Networks	The STRIKE3 centralised server shall accept interference event reports from different monitoring networks	Test	
	STRIKE3-CS-INT-003	Server Input Detection Equipment	The STRIKE3 centralised server shall accept interference event reports from detection equipment produced by different manufacturers	Test	
	STRIKE3-CS-INT-004	Event Upload Security	The upload of interference event reports to the STRIKE3 centralised server shall use a secure connection	Review, demonstration	Secure connection means that all communication traffic is encrypted between the two points by using either the SSL or TLS security protocol. For STRIKE3 the priority for this is data integrity and confidentiality.
	STRIKE3-CS-INT-005	Event Upload Initiation	The sending of interference event reports to the STRIKE3 centralised server shall be initiated by the contributing party	Test	i.e. Reports are pushed to database by contributor - database does not send a request
	STRIKE3-CS-INT-006	Contributor Registration	Interference event reports shall only be accepted from registered parties	Test	Want to have some control over who is uploading reports
	STRIKE3-CS-INT-007	Server Acknowledgement of Upload	The STRIKE3 centralised server shall acknowledge successful transfer / upload of interference event reports	Test	

Category	Req Id	Req Title	Description	Verification Method	Comments
	STRIKE3-CS-INT-008	Event Upload Latency	Interference event reports can be sent at any time after the occurrence of the event	Review, Test	i.e. Don't necessarily need real time, or to receive reports within a certain time e.g. 1 day of occurrence
	STRIKE3-CS-INT-009	Event Upload	The STRIKE3 centralised server interface shall allow upload of a single event per message	Test	Although each message contains just a single event, the choice of when to upload is controlled at the monitoring system side. Contributors can choose to upload events as they happen (near real-time) or do a batch assessment and upload once a week, once or month, etc.
	STRIKE3-CS-INT-010	Server Interface Expandability - Formats	The STRIKE3 centralised server interface shall be easily expandable to allow additional parameters to be included in the future.	Review	Format needs to be flexible / expandable.
	STRIKE3-CS-INT-011	Server Interface Expandability – Number of Contributors	The STRIKE3 centralised server interface shall be expandable to allow a large number of organizations to contribute interference event reports in the future	Review	Protocols and data transfer needs to be expandable and allow multiple people to contribute and send reports
	STRIKE3-CS-INT-012	Centralised Server Response Time for Upload	The STRIKE3 centralised server level for response is 99% within 10 seconds for a single event upload.	Test	
Database	STRIKE3-CS-DB-001	Database Parameters Storage	The STRIKE3 centralised database shall store all parameters included in the interference event report messages	Test	

Category	Req Id	Req Title	Description	Verification Method	Comments
	STRIKE3-CS-DB-002	Database Expandability - Parameters	The STRIKE3 centralised database shall be designed to be expandable to allow adding of new parameters	Review	
	STRIKE3-CS-DB-003	Database Expandability - Number of Contributors	The STRIKE3 centralised database shall be designed to be expandable to allow information to be contributed by a large number of contributors	Review	
	STRIKE3-CS-DB-004	Authorized Database Access	The STRIKE3 centralised database shall only allow authorized access through defined interfaces	Review, Test	
	STRIKE3-CS-DB-005	Database Robustness	The STRIKE3 centralised database shall be robust and protect against loss of data	Review	
	STRIKE3-CS-DB-006	Database Storage of Sensitive Information	The STRIKE3 centralised database shall not store sensitive information about events (e.g. Precise location information, I/Q data)	Review	
	STRIKE3-CS-DB-007	Database Storage Capacity	The STRIKE3 centralised server shall be able to store events covering 1-year of monitoring from up to 20 networks with up to 50 sensors in each network.	Review	This is a requirement for the hardware of the demonstration system in STRIKE3. The capacity could easily be expanded for an operational system by using different hardware and storage.
User access	STRIKE3-CS-USER-001	User Access	The STRIKE3 centralised server shall allow users to access the information in the centralised database through a defined interface	Test	

Category	Req Id	Req Title	Description	Verification Method	Comments
	STRIKE3-CS-USER-002	User Registration	Access to the information in the centralised database shall be controlled to registered users	Test	
	STRIKE3-CS-USER-003	Standard User Application	There shall be a standard demonstration application to allow users to view results and generate statistics about events from the information in the STRIKE3 centralised database	Demonstration	Something simple for the project to showcase the potential
	STRIKE3-CS-USER-004	Standard User Application – Event Information	The standard demonstration application shall provide controls to enable users to enter information about events such as date, type, affected frequency band and country when requesting events from the server.	Test	
	STRIKE3-CS-USER-005	Standard User Application – Total Event Analysis	The standard demonstration application shall provide an option to allow the request of the total number of events in a defined period.	Test	
	STRIKE3-CS-USER-006	Standard User Application – Event Date Analysis	The standard demonstration application shall provide an option to allow the request of the total number of events in a daily and weekly manner in a defined period.	Test	
	STRIKE3-CS-USER-007	Standard User Application – Event Filtering	The standard demonstration application shall provide a filter option on all event requests. The available filters would be: location, event type (power or SNR) and affected frequency band.	Test	

Category	Req Id	Req Title	Description	Verification Method	Comments
	STRIKE3-CS-USER-008	User Interface Flexibility	The user interface to the STRIKE3 centralised server shall allow for end users to develop their own analysis and visualization applications.	Review	
	STRIKE3-CS-USER-009	Detailed Information Request	The STRIKE3 centralised server shall provide a mechanism for users to request and/or access additional event information from organizations that have contributed to the STRIKE3 centralised database	Test	
	STRIKE3-CS-USER-010	User Interface Expandability – Number of Users	The user interface for the STRIKE3 centralised server shall be expandable to allow a large number of users to simultaneously access the data	Review	
	STRIKE3-CS-USER-010	Centralised Server Response Time – User Requests	The STRIKE3 centralised server level for response is 99% within 20 seconds for all the service requests.	Test	
	STRIKE3-CS-USER-011	Centralised Server Handling Large Requests	The STRIKE3 centralised server shall be able to handle requests covering large numbers of events (i.e. >10000).	Review, Test	This is to protect against requests for very large numbers of events that may cause problems with data transfer. The mechanism to handle large queries may include returning a negative response and instructions to users to change their search criteria.

Table 5-2: High Level Reporting System Requirements – STRIKE3 Monitoring systems

Category	Req Id	Req Title	Description	Verification Method	Comments
Functional	STRIKE3-MON-FUN-001	Monitoring Band	The STRIKE3 monitoring systems shall detect interference in at least GPS L1 band	Review, Test	
	STRIKE3-MON-FUN-002	Event ID	The STRIKE3 monitoring systems shall allocate a unique ID to each event	Review, Test	This is required so it is possible to trace back from the events at the centralised server to the original event and information
	STRIKE3-MON-FUN-003	Monitoring Event Filtering	The STRIKE3 monitoring systems shall filter the detected interference events using either power- or AGC-based criteria, or C/N0 criteria.	Test	
	STRIKE3-MON-FUN-004	Monitoring Event Criteria	The STRIKE3 monitoring systems shall only report to the centralised server those events that meet the defined event criteria.	Test	
	STRIKE3-MON-FUN-005	Monitoring Upload Initiation	The STRIKE3 monitoring systems shall initiate the upload of events to the centralised server.	Demonstration	Could be automatic or a manual process by the operator. The important thing is that the data provider initiates the upload – it is not the centralised server that makes a request for information.

Category	Req Id	Req Title	Description	Verification Method	Comments
	STRIKE3-MON-FUN-006	Monitoring System Event Upload	The STRIKE3 monitoring systems shall upload a single event per message	Test	Although each message contains just a single event, the choice of when to upload is controlled at the monitoring system side. Contributors can choose to upload events as they happen (near real-time) or do a batch assessment and upload once a week, once or month, etc.
Interface	STRIKE3-MON-INT-001	Monitoring Upload Format	The STRIKE3 monitoring systems shall send interference event reports to the centralised server in the defined format	Test	Format and contents according to section 3
	STRIKE3-MON-INT-002	Monitoring Upload Minimum Information	The STRIKE3 monitoring systems shall send at least the minimum set of information requested in the event reports (i.e. event ID, equipment type, event definition, frequency band, region and date).	Test	
	STRIKE3-MON-INT-003	Monitoring Upload Security	The STRIKE3 monitoring systems shall upload interference event reports to the STRIKE3 centralised server using a secure connection	Review, demonstration	Secure connection means that all communication traffic is encrypted between the two points by using either the SSL or TLS security protocol. For STRIKE3 the priority for this is data integrity and confidentiality.
	STRIKE3-MON-INT-004	Monitoring System Registration	The STRIKE3 monitoring systems and equipment shall be registered before uploading interference event reports to the STRIKE3 centralised server	Demonstration	

6 Demonstration Reporting System Design

6.1 Introduction

This section aims to describe the architecture of the demonstration STRIKE3 centralised server subsystem as well as the interfaces and web services provided by this subsystem.

The STRIKE3 centralised server will consist of a gateway with a series of SOAP based web services available to clients as well as an open source database server module that will run on a server rack under the Windows Server operating system.

The purpose of breaking up the operations of the STRIKE3 centralised server into web services is to create a system that will be scalable and flexible to meet future needs. Also it will be easier to maintain and debug during testing and live operations.

6.2 High Level Design of STRIKE3 Centralised Server

6.2.1 Overview

The STRIKE3 centralised server consists mainly of a series of SOAP-Based web services that handle GNSS interference report uploads from contributor's central hub (and/or from their equipment itself) as well as external end user interference data requests. A database server module is also part of the system and facilitates data storage of all the incoming and outgoing messages. The initial group of web services compiled under the STRIKE3 gateway is:

- Account Management Services.
- Interference Monitoring Data Management Services.

The diagram below shows how the web services and the rest of the modules are linked together on the server and how the flow of data is running between them. Contributors of interference reports and end users exchange data with the server using the SOAP protocol.

The firewall component showing in the diagram below is not a separate subsystem that provides dedicated firewall capabilities (e.g. hardware firewall). It is instead a software firewall component offered by the Centralised Server in order to allow or block incoming connections to the server.

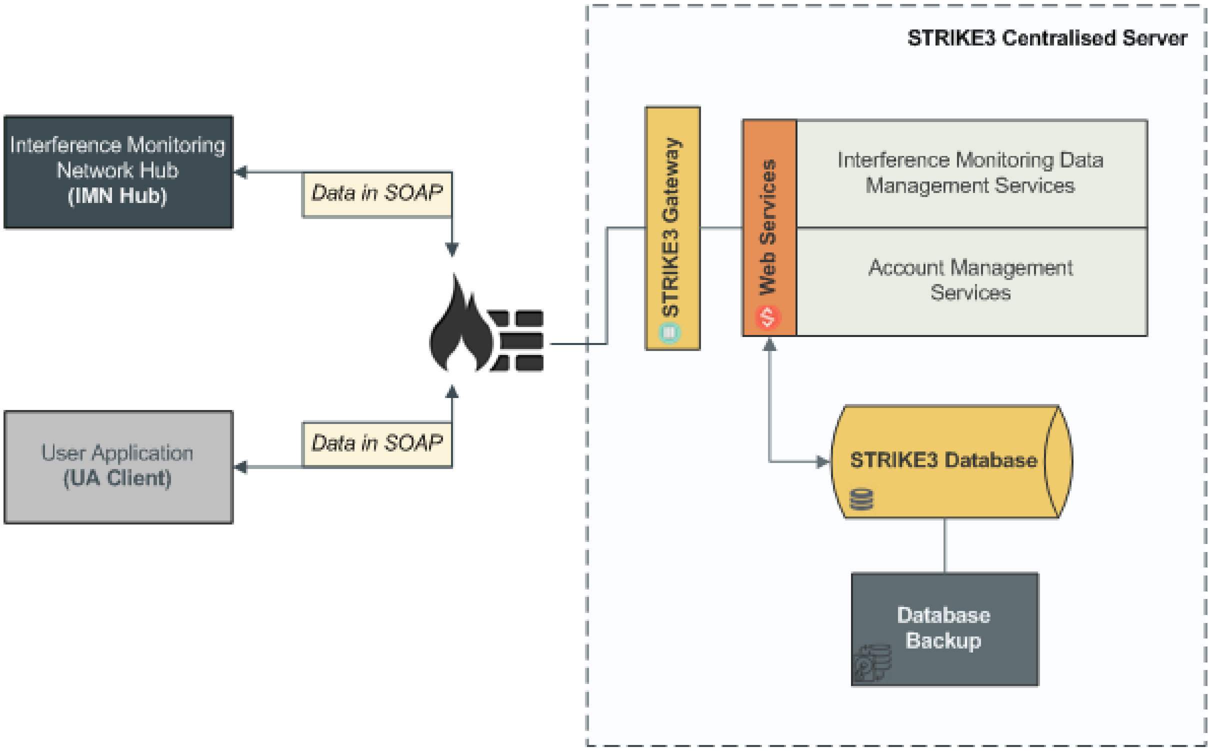
STRIKE3 Centralised Server
Interference Monitoring Network Hub (IMN Hub)
Data in SOAP
User Application (UA Client)
Data in SOAP
STRIKE3 Gateway
Web Services
Interference Monitoring Data Management Services
Account Management Services
STRIKE3 Database
Database Backup

Figure 6-1: STRIKE3 Centralised Server Architecture

Description of each web service group and system modules is explained in the paragraphs below.

6.2.2 Description of STRIKE3 Gateway

The STRIKE3 Gateway is a secure HTTP web server (with SSL) that hosts the SOAP-Based Web Services that will be used to handle GNSS interference report requests from either contributors or end user clients. The purpose of each web service group is described in the following paragraphs.

1. **Account Management Services:** This group of services is available to both contributors and end users. The list of services included in this group are:

   a. **Add Network Service:** The purpose of this service is to register a monitoring network of sensors to the system. After successful addition to the system the service returns back a **KEY** and a **CLIENTID** which will allow them to access the rest of the web services provided by the system. Authentication and licensing models for each user group will also be linked to this unique **KEY/CLIENTID** pair.

b. **View Network Service:** The purpose of this service is to load the profile of a registered monitoring network.
c. **Edit Network Service:** The purpose of this service is to allow modification of registered monitoring networks.
d. **Remove Network Service:** The purpose of this service is to delete a registered monitoring network from the system.
e. **Add User Service:** The purpose of this service is to register an end user to the system. After successful addition to the system the service returns back a **KEY** and a **CLIENTID** which will allow them to access the rest of the web services provided by the system. Authentication and licensing models for each user group will also be linked to this unique **KEY/CLIENTID** pair.
f. **View User Service:** The purpose of this service is to load the profile of a registered end user.
g. **Edit User Service:** The purpose of this service is to allow modification of registered end user profiles.
h. **Remove User Service:** The purpose of this service is to delete a registered end user from the system.

2. **Interference Monitoring Data Management Services:** The list of services included in this group are:

a. **Report Upload Service:** This service is available to data providers (contributors) only. Its purpose is to allow data providers to upload detection reports to the system. The service will store the reports to the STRIKE3 centralised database and send a negative or positive response back to the client.
b. **Data Mining Service:** This service is available to end users only. Its main purpose is to interrogate the SQL database on request and provide analysis and statistics of the interference reports uploaded by the data providers. Data pattern discoveries and data relationships are also features provided by this service.
c. **Advanced Data Request Service:** This service is available to end users only. Its purpose is to make available extra/advanced information about a report to a user such as RF data, spectrum or spectrogram values, etc, by proving the necessary communication information required to retrieve these extra data (e.g. ftp accounts, email addresses etc).

6.2.3 Description of the SQL Database Server

The database server is the open source object-relational database, PostgreSQL. The database will consist of one scheme, **STRIKE3**. Under this scheme there will be a series of tables that will hold the interference report messages and the user accounts.

6.3 Description of Interfaces

6.3.1 Overview

The interfaces between the STRIKE3 centralised server modules and the other subsystems are shown in the figure below.

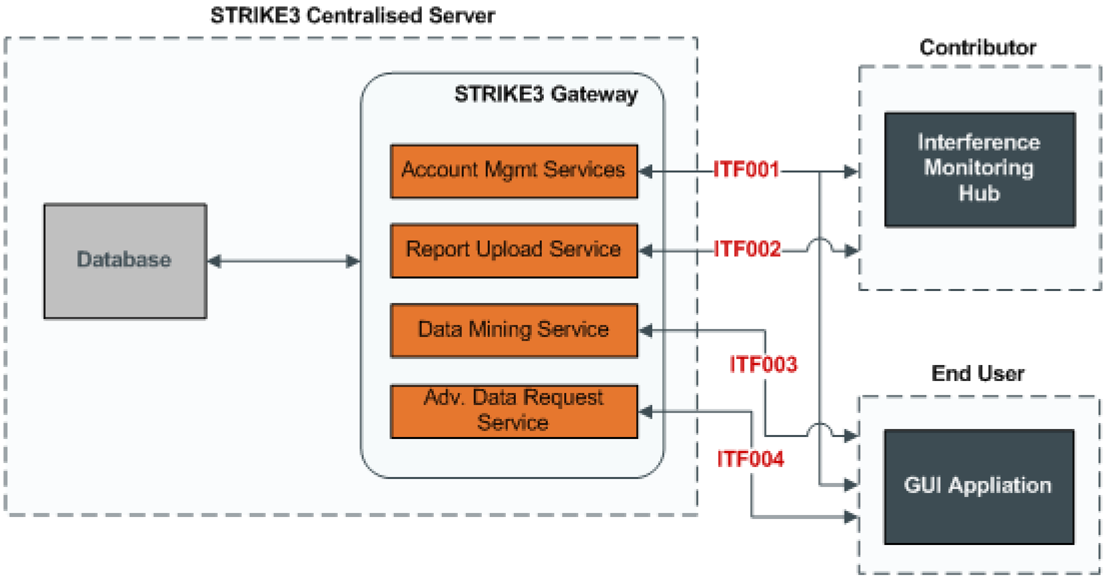

Figure 6-2: STRIKE3 Centralised Server Interfaces

The business interface between STRIKE3_CS and Contributor consists of two technical interfaces, **ITF001** and **ITF002**. Similarly, the interfaces, **ITF001**, **ITF003** and **ITF004** are also technical interfaces between the business interface STRIKE3_CS and End User.

All interfaces provided by STRIKE3_CS are web services. The protocol used to communicate between the STRIKE_CS and the End User or Contributor is based on the SOAP 1.2 protocol over HTTPS.

The Web Service Definition Language (WSDL) files used to describe web services as well as the actual address of the services will be provided on request to End users and contributors.

An abstract description of all the technical interfaces is shown in the table below.

Table 6-1: Technical Interface definitions

Interface Id	Description
ITF001	Account management services
ITF002	Report upload service
ITF003	Data mining service
ITF004	Advanced data request service

6.3.2 Account Management Services Interface

The technical interface between this service group and the contributor's or end user's subsystem is shown below.

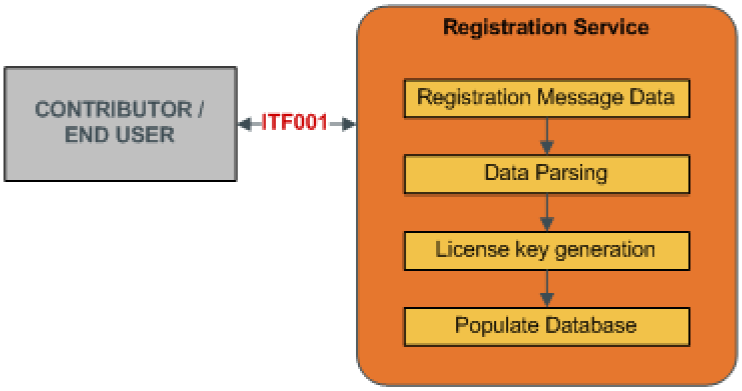

Figure 6-3: Account Management Service Interface

A description of the ITF001 interface is shown in the table below.

Table 6-2: ITF001 description

#	Interface	Technology	Network	From	To	Frequency
ITF001	Account Management Services	SOAP Based Request [*Gateway listening on port **6588***]	WAN	Contributor or end user.	STRIKE3 Gateway	On Request

The web services that will be available to the Contributors through this interface are:

- Add Interference Monitoring Network [*Add_IMN*[
- View Interference Monitoring Network [*View_IMN*[
- Edit Interference Monitoring Network [*Edit_IMN*]
- Delete Interference Monitoring Network [*Delete_IMN*]

Similarly the web services that are available to the End user through this interface are:

- Add Interference Monitoring User [*Add_IMU*]
- View Interference Monitoring User [*View_IMU*]
- Edit Interference Monitoring User [*Edit_IMU*]
- Remove Interference Monitoring User [*Delete_IMU*]

Both Contributors and End users will call these web services with the required parameters as described in sections 7.2 and 7.4 accordingly. The result will be synchronously returned back in the form of a XML string.

6.3.3 Report Upload Service Interface

The technical interface between the Report Upload Service and the contributor's subsystem is shown below.

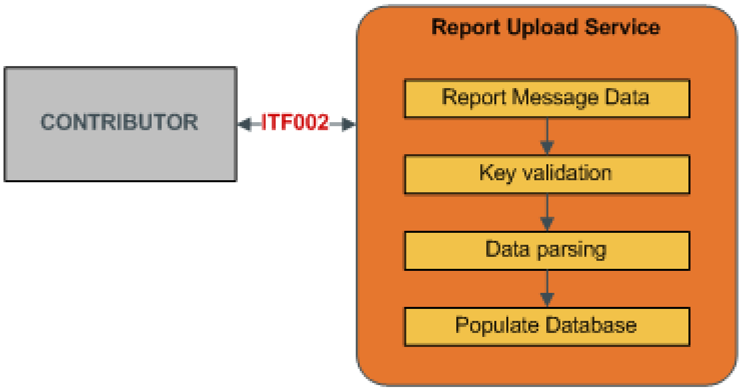

Figure 6-4: Report Upload Service Interface

A description of the ITF002 interface is shown in the table below.

Table 6-3: ITF002 description

#	Interface	Technology	Network	From	To	Frequency
ITF002	Report Upload Service	SOAP Based Request *[Gateway listening on port **6588]***	WAN	Contributor's Subsystem	STRIKE3 Gateway	On Request

The web service that will be available to the Contributor through this interface is:

- Push Interference Report [*Push_IR*].

The Contributor will call this web service with the required parameters as described in section 7.3. The result will be synchronously returned back in the form of a XML string.

6.3.4 Data Mining Service Interface

The technical interface between the Data Mining Service and the end user's subsystem is shown below.

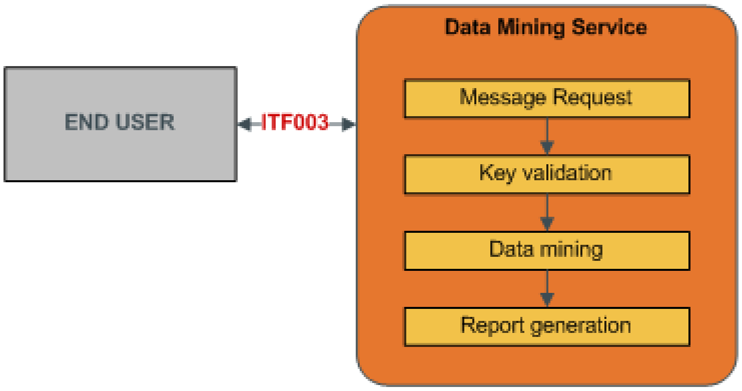

Figure 6-5: Data Mining Service Interface

A description of the ITF003 interface is shown in the table below.

Table 6-4: ITF003 description

#	Interface	Technology	Network	From	To	Frequency
ITF003	Data Mining Service	SOAP Based Request [*Gateway listening on port* ***6588]***	WAN	End user's Subsystem	STRIKE3 Gateway	On Request

The web service that will be available through this interface to the End user is:

- Get Interference Monitoring Data [*Get_IMD*]

The End user will call this web service with the required parameters as described in section 7.5. The result will be synchronously returned back in the form of a XML string.

6.3.5 Advanced Data Request Service Interface

The technical interface between the Advance Data Request Service and the end user's subsystem is shown below.

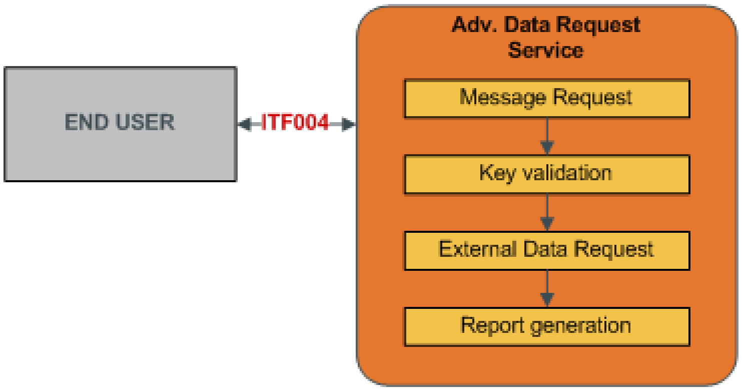

Figure 6-6: Adv. Data Request Service Interface

A description of the ITF004 interface is shown in the table below.

Table 6-5: ITF004 description

#	Interface	Technology	Network	From	To	Frequency
ITF003	Advanced Data Request Service	SOAP Based Request [*Gateway listening on port* ***6588]***	WAN	End user's Subsystem	STRIKE3 Gateway	On Request

The web service that will be available through this interface to the End user is:

- Get Advanced Interference Monitoring Data [*Get_Adv_IMD*]

The End user will call this web service with the required parameters as described in section 7.6. The result will be synchronously returned back in the form of a XML string.

6.4 Implementation

During the development of the demonstration platform within the STRIKE3 project, the following process is foreseen:

- In coordination with other project partners, NSL will define the detailed interfaces and protocols for each of the web services. This includes the account management, interference report upload, data mining, and advanced data request services;
- NSL will develop the STRIKE3 centralized database and web services according to this detailed interface definitions;
- The detailed interface definitions will be made available via the project website, along with standard application software for registration (data provider / contributor and end user), and for data mining and advanced data requests;
  - The standard application software for registration allows data providers / contributors to register in order to be able to add interference events to the STRIKE3 centralised database;
  - The standard application software for registration allows end users to register in order to be able to view information and statistics about events;
  - The standard application software for data mining allows end users to view standard results and statistics about detections from all monitoring networks that report to the STRIKE3 centralised server and stored in the centralised database. The software will allow end users to filter events based on parameters such as date range, country, affected frequency band, etc. and display the results;
  - The standard application software for advanced data requests allows end users to request additional detailed information about specific events from data providers that is held at the local event database of the data provider.
- Monitoring network operators (including STRIKE3 project partners) can use the detailed interface definition in order to create their own application to upload event information to the STRIKE3 centralised database;
- End users can use the standard application for viewing results and information, or they can use the detailed interface definition to create their own application with different visualization and data analysis to interact with the STRIKE3 centralised server and request event data from the centralised database for analysis.

7 Demonstration Web Service Definition

7.1 Introduction

It is the intention of this section to outline the basic web services (WS) and message formats that would provide STRIKE3 Gateway with the data needed to satisfy the requirements of the reporting messages and overall architecture as defined in this document. As such, this section can be regarded as the basis for further elaboration in to workable WSDL (Web Services Description Language) files which would need to be provided to potential contributors and end users in order to populate the database and retrieve event information. The web services compiled under the STRIKE3 Gateway are grouped between end users and providers as follows:

Group A: Provider Related Web Services

- Add Interference Monitoring Network [*Add_IMN*]
- View Interference Monitoring Network [*View_IMN*]
- Edit Interference Monitoring Network [*Edit_IMN*]
- Delete Interference Monitoring Network [*Delete_IMN*]
- Push Interference Report [*Push_IR*]

Group B: End User Related Web Services

- Add Interference Monitoring User [*Add_IMU*]
- View Interference Monitoring User [*View_IMU*]
- Edit Interference Monitoring User [*Edit_IMU*]
- Remove Interference Monitoring User [*Delete_IMU*]
- Get Interference Monitoring Data [*Get_IMD*]
- Get Advanced Interference Monitoring Data [*Get_Adv_IMD*]

The above services are synchronous WS. The syntax for invocation of an interface method will follow the SOAP v1.2 standard. As the owner of the WS, NSL shall define Web Service Description Language files (WSDL, Version 1.1). GNSS Interference Detection Providers will prepare messages that conform to the WSDL provided by NSL.

In common with other web interfaces within the programme, Transport Layer Security (TLS) 1.2 with AES encryption is used to secure the communications between the interface endpoints. X.509 certificates will be installed on each endpoint device. In line with other interfaces within the project as a whole the authentication used should be SSL with Certificate based client authentication.

Hashed message digests (using SHA256 encryption) will be used to assure message integrity, with the hash value being included within the message. The message hash will be comprised of the hash of the message Header and the message Body.

7.1.1 Data Integrity

The integrity of the message interface will be assured by:

- The conformance to the defined message structure.
- The checking of the hash of the message Header and message Body against the value stored in the HashValue element.
- The use of the HTTPS protocol.

7.1.2 Message Structure

For consistency with other messages within the solution, messages between NSL (as the developer and operator of the demonstration centralised database) and external parties (contributors and users) users shall follow the general structure of:

- Header node.
- Body node.
- Message Digest node.

It is noted that all fields in the messages are mandatory, i.e. every field must be included in the message with a value. However, for those fields where the information to be provided by the monitoring network operator is optional (as defined in the tables in section 3), it is allowable to provide a default value of ‘NA’ if the contributor is not providing that information – either because it is not available from the system or there are security or confidentiality concerns that limit the distribution of such information. The table sin the following sections clearly indicate which fields allow the use of default NA values for optional information.

7.1.2.1 Message Digest Node

The message digest node is common across all the messages and shall be formatted as follows:

Table 7-1: Message Digest Node

Element	Purpose	Type	Inclusion
<MessageDigest>			
<MsgDigest/>	The hash calculated from the message	String	Mandatory

	header and body. This should be done by taking the string value of the XML representations of the header and body sections of the message, concatenating. Used by receiving service to confirm message has not been tampered with in transit.		
</MessageDigest>			

7.2 Account Management Services (Monitoring Network)

These messages relate to the account management services included within interface ITF001 (see section 6.3.2) for the monitoring network operators who will contribute information to the STRIKE3 centralised server.

7.2.1 Add_IMN Request Message

This section describes the input parameters contained within the <header> and <body> nodes of the registration request message.

7.2.1.1 Header Node

For consistency with other messages in the solution, the header node should follow this format:

Table 7-2: Add_IMN – Request Header Node

Element	Purpose	Type	Inclusion
<Header>			
<Version/>	May be required in future to allow backward compatibility in the event that message format definitions change over time.	String	Mandatory
<MsgDateTime/>	Date/time the message was originated, to millisecond precision.	DateTime	Mandatory
</Header>			

7.2.1.2 Body Node

The following table describes the input parameters required by the Add_IMN WS:

Table 7-3: Add_IMN – Request Body Node

Element	Purpose	Type	Inclusion
<Body>			
<AddIMNRequest>			
<Name/>	Descriptive name of the monitoring network, used to identify their reported events.	String	Mandatory
<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 (NSL for STRIKE3).	String	Mandatory
<NumOfEquipTypes/>	The number of different types of detection equipment that make up this network.	Integer	Mandatory
<EquipTypes>	Container node for all network detection equipment types.		
<EquipType>	Container node for a single type of detection equipment.		
<Name/>	Descriptive name of the detection equipment	String	Mandatory
<Manufacturer/>	Manufacturer of the interference detection equipment	String	Mandatory
<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.	String	Mandatory
<FreqBand/>	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.	String	Mandatory
<SwVersion/>	Version of the detection equipment software	String	Mandatory (default value = **NA** if the information is not provided)

<HdwVersion/>	Version of the detection equipment hardware.	String	Mandatory (default value = **NA** if the information is not provided)
</EquipType>			
</EquipTypes>			

<DetailedInfo/>	A detailed list of other type of information that is available in the system for authorized personnel only, plus details of how to access this detailed information (e.g. email contact details for request, ftp site details, etc.). The text format of this parameter shall be in **JSON.** An example of available data (e.g. RF and logs) via an FTP connection is shown below:
	{
	"info": "RF,logs",
	"conntype": "ftp",
	"host": "provider001",
	"user": "username",
	"password": "password",
	"port": "22",
	"remote_path": "/net001/sensors/",
	"file_permissions": "664",
	"dir_permissions": "775",
	"connect_timeout": 30,
	"keepalive": 120,
	"ftp_passive_mode": true,
	"remote_encoding": "utf-8",
	}
		String	Mandatory
			(default value = **NA** if the information is not provided)

</AddIMNRequest>			
</Body>			

7.2.2 Add_IMN Response Message

The STRIKE3 Gateway processes the Add_IMN request synchronously and responds with the appropriate data (or suitable error/status messages). This means the body node of this response will consist of an either positive or negative node.

7.2.2.1 Header Node

For consistency with other messages in the solution, the header node should follow this format:

Table 7-4: Add_IMN – Response Header Node

Element	Purpose	Type	Inclusion
<Header>			
<Version/>	May be required in future to allow backward compatibility in the event that message format definitions change over time.	String	Mandatory
<MsgDateTime/>	Date/time the message was originated, to millisecond precision.	DateTime	Mandatory
</Header>			

7.2.2.2 Body Node

The body node of the Add_IMN response message should be formatted as follows:

Table 7-5: Add_IMN – Response Body Node

Element	Purpose	Type	Inclusion
<Body>			
<AddIMNResponse>			
<AddIMNPosResponse>	This node is used by the WS if it has successfully interpreted the parameters and has registration data to return to user/provider.		Optional
<Key/>	The license key will be used to authenticate requests to the system by users and providers.	String	Mandatory

	Length = 256Bit		
<ClientID/>	To be used to identify requests to the system by users and providers. Length =128Bit	String	Mandatory
</AddIMNPosResponse>			
</AddIMNResponse>			
</Body>			

7.2.2.3 Negative Response Node

The purpose of the negative response node is to allow the WS to communicate to users the reasons for rejecting the request or to describe an error condition that prevents the WS satisfying the request. The <AddIMNNegResponse> node is populated and returned in the response to user and should be formatted as follows:

Table 7-6: Add_IMN – Negative Response Node

Element	Purpose	Type	Inclusion
<AddIMNNegResponse>	This node is used by the WS if it has failed to interpret the parameters or cannot return registration data to user/provider.		Optional
<ErrorMsg/>	Description of error from the WS.	String	Mandatory
</AddIMNNegResponse>			

7.2.3 View_IMN Request Message

This section describes the input parameters contained within the <header> and <body> nodes of the registration request message.

7.2.3.1 Header Node

For consistency with other messages in the solution, the header node should follow this format:

Table 7-7: View_IMN – Request Header Node

Element	Purpose	Type	Inclusion
<Header>			
<Version/>	May be required in future to allow backward compatibility in the event that message format definitions change over time.	String	Mandatory
<MsgDateTime/>	Date/time the message was originated, to millisecond precision.	DateTime	Mandatory
<Key/>	The license key provided during registration.	String	Mandatory
<ClientID/>	The client id provided during registration.	String	Mandatory
</Header>			

7.2.3.2 Body Node

The following table describes the input parameters required by the View_IMN WS:

Table 7-8: View_IMN – Request Body Node

Element	Purpose	Type	Inclusion
<Body>			
<ViewIMNRequest>			
<Reason/>	A free text to describe the reason of this request.	String	Mandatory
</ViewIMNRequest>			
</Body>			

7.2.4 View_IMN Response Message

The STRIKE3 Gateway processes the View_IMN request synchronously and responds with the appropriate data (or suitable error/status messages). This means the body node of this response will consist of an either positive or negative node.

7.2.4.1 Header Node

For consistency with other messages in the solution, the header node should follow this format:

Table 7-9: View_IMN – Response Header Node

Element	Purpose	Type	Inclusion
<Header>			
<Version/>	May be required in future to allow backward compatibility in the event that message format definitions change over time.	String	Mandatory
<MsgDateTime/>	Date/time the message was originated, to millisecond precision.	DateTime	Mandatory
</Header>			

7.2.4.2 Body Node

The following table describes the input parameters required by the View_IMN WS:

Table 7-10: View_IMN – Response Body Node

Element	Purpose	Type	Inclusion
<Body>			
<ViewIMNPosResponse>			
<Name/>	Descriptive name of the monitoring network, used to identify their reported events.	String	Mandatory
<Contact/>	Contact information to the organization that has provided information to the database. To be used for managing the registration	String	Mandatory

	and interface between the organization and the central database operator (NSL for STRIKE3).		
<NumOfEquipTypes/>	The number of different types of detection equipment that make up this network.	Integer	Mandatory
<EquipTypes>	Container node for all network detection equipment types.		
<EquipType>	Container node for a single type of detection equipment.		
<Name/>	Descriptive name of the detection equipment	String	Mandatory
<Manufacturer/>	Manufacturer of the interference detection equipment	String	Mandatory
<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.	String	Mandatory
<FreqBand/>	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.	String	Mandatory
<SwVersion/>	Version of the detection equipment software	String	Mandatory (default value = **NA** if the information is not provided)
<HdwVersion/>	Version of the detection equipment hardware.	String	Mandatory (default value = **NA** if the information is not provided)
</EquipType>			
</EquipTypes>			
<DetailedInfo/>	A detailed list of other type of information that is available in the system for authorized personnel only, plus details of how to access this detailed information (e.g. email contact details for request, ftp site details, etc.). The text format of this	String	Mandatory (default value = **NA** if the information is not provided)

	parameter shall be in **JSON.** An example of available data (e.g. RF and logs) via an FTP connection is shown below:
	{
	"info": "RF,logs",
	"conntype": "ftp",
	"host": "provider001",
	"user": "username",
	"password": "password",
	"port": "22",
	"remote_path": "/net001/sensors/",
	"file_permissions": "664",
	"dir_permissions": "775",
	"connect_timeout": 30,
	"keepalive": 120,
	"ftp_passive_mode": true,
	"remote_encoding": "utf-8",
	}

</ViewIMNPosResponse>	
</Body>	

7.2.4.3 Negative Response Node

The purpose of the negative response node is to allow the WS to communicate to users the reasons for rejecting the request or to describe an error condition that prevents the WS satisfying the request. The <ViewIMNNegResponse> node is populated and returned in the response to user and should be formatted as follows:

Table 7-11: View_IMN – Negative Response Node

Element	Purpose	Type	Inclusion
<ViewIMNNegResponse>	This node is used by the WS if it has failed to interpret the parameters or cannot return registration data to user/provider.		Optional
<ErrorMsg/>	Description of error from the WS.	String	Mandatory
</ViewIMNNegResponse>			

7.2.5 Edit_IMN Request Message

This section describes the input parameters contained within the <header> and <body> nodes of the registration request message.

7.2.5.1 Header Node

For consistency with other messages in the solution, the header node should follow this format:

Table 7-12: Edit_IMN – Request Header Node

Element	Purpose	Type	Inclusion
<Header>			
<Version/>	May be required in future to allow backward compatibility in the event that message format definitions change over time.	String	Mandatory
<MsgDateTime/>	Date/time the message was originated, to millisecond precision.	DateTime	Mandatory
<Key/>	The license key provided during registration.	String	Mandatory
<ClientID/>	The client id provided during registration.	String	Mandatory
</Header>			

7.2.5.2 Body Node

The following table describes the input parameters required by the Edit_IMN WS:

Table 7-13: Edit_IMN – Request Body Node

Element	Purpose	Type	Inclusion
<Body>			
<EditIMNRequest>			
<Name/>	Descriptive name of the monitoring network, used to identify their reported events.	String	Mandatory
<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 (NSL for STRIKE3).	String	Mandatory
<NumOfEquipTypes/>	The number of different types of detection equipment that make up this network.	Integer	Mandatory
<EquipTypes>	Container node for all network detection equipment types.		
<EquipType>	Container node for a single type of detection equipment.		
<Name/>	Descriptive name of the detection equipment	String	Mandatory
<Manufacturer/>	Manufacturer of the interference detection equipment	String	Mandatory
<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.	String	Mandatory
<FreqBand/>	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.	String	Mandatory
<SwVersion/>	Version of the detection equipment	String	Mandatory

	software		(default value = **NA** if the information is not provided)
<HdwVersion/>	Version of the detection equipment hardware.	String	Mandatory (default value = **NA** if the information is not provided)
</EquipType>			
</EquipTypes>			

<DetailedInfo/>	A detailed list of other type of information that is available in the system for authorized personnel only, plus details of how to access this detailed information (e.g. email contact details for request, ftp site details, etc.). The text format of this parameter shall be in **JSON.** An example of available data (RF and logs) via an FTP connection is shown below:
	{
	"info": "RF,logs",
	"conntype": "ftp",
	"host": "provider001",
	"user": "username",
	"password": "password",
	"port": "22",
	"remote_path": "/net001/sensors/",
	"file_permissions": "664",
	"dir_permissions": "775",
	"connect_timeout": 30,
	"keepalive": 120,
	"ftp_passive_mode": true,
	"remote_encoding": "utf-8",
	}
		String	Mandatory

</EditIMNRequest>			
</Body>			

7.2.6 Edit_IMN Response Message

The STRIKE3 Gateway processes the Edit_IMN request synchronously and responds with a suitable error/status message.

7.2.6.1 Header Node

For consistency with other messages in the solution, the header node should follow this format:

Table 7-14: Edit_IMN – Response Header Node

Element	Purpose	Type	Inclusion
<Header>			
<Version/>	May be required in future to allow backward compatibility in the event that message format definitions change over time.	String	Mandatory
<MsgDateTime/>	Date/time the message was originated, to millisecond precision.	DateTime	Mandatory
</Header>			

7.2.6.2 Body Node

The body node of the Edit_IMN response message should be formatted as follows:

Table 7-15: Edit_IMN – Response Body Node

Element	Purpose	Type	Inclusion
<Body>			
<EditIMNResponse>			
<Msg/>	A response message from the WS.	String	Mandatory
</EditIMNResponse>			
</Body>			

7.2.7 Delete_IMN Request Message

This section describes the input parameters contained within the <header> and <body> nodes of the registration request message.

7.2.7.1 Header Node

For consistency with other messages in the solution, the header node should follow this format:

Table 7-16: Delete_IMN – Request Header Node

Element	Purpose	Type	Inclusion
<Header>			
<Version/>	May be required in future to allow backward compatibility in the event that message format definitions change over time.	String	Mandatory
<MsgDateTime/>	Date/time the message was originated, to millisecond precision.	DateTime	Mandatory
<Key/>	The license key provided during registration.	String	Mandatory
<ClientID/>	The client id provided during registration.	String	Mandatory
</Header>			

7.2.7.2 Body Node

The following table describes the input parameters required by the Delete_IMN WS:

Table 7-17: Delete_IMN – Request Body Node

Element	Purpose	Type	Inclusion
<Body>			
<DeleteIMNRequest>			
<Name/>	Descriptive name of the system used to identify their reported events.	String	Mandatory
</DeleteIMNRequest>			
</Body>			

7.2.8 Delete_IMN Response Message

The STRIKE3 Gateway processes the Delete_IMN request synchronously and responds with a suitable error/status message.

7.2.8.1 Header Node

For consistency with other messages in the solution, the header node should follow this format:

Table 7-18: Delete_IMN – Response Header Node

Element	Purpose	Type	Inclusion
<Header>			
<Version/>	May be required in future to allow backward compatibility in the event that message format definitions change over time.	String	Mandatory
<MsgDateTime/>	Date/time the message was originated, to millisecond precision.	DateTime	Mandatory
</Header>			

7.2.8.2 Body Node

The body node of the Delete_IMN response message should be formatted as follows:

Table 7-19: Delete_IMN – Response Body Node

Element	Purpose	Type	Inclusion
<Body>			
<DelIMNResponse>			
<Msg/>	A response message from the WS.	String	Mandatory
</DelIMNResponse>			
</Body>			

7.3 Report Upload Service

These messages relate to the report upload service included within interface ITF002 (see section 6.3.3). This is the interface by which contributors will send event reports to the STRIKE3 centralised server for adding to the centralised database.

7.3.1 Push_IR Request Message

This section describes the input parameters contained within the <header> and <body> nodes of the report upload request message.

7.3.1.1 Header Node

For consistency with other messages in the solution, the header node should follow this format:

Table 7-20: Push_IR – Request Header Node

Element	Purpose	Type	Inclusion
<Header>			
<Version/>	May be required in future to allow backward compatibility in the event that message format definitions change over time.	String	Mandatory
<MsgDateTime/>	Date/time the message was originated, to millisecond precision.	DateTime	Mandatory
<Key/>	The license key provided during registration.	String	Mandatory
<ClientID/>	The client id provided during registration.	String	Mandatory
</Header>			

7.3.1.2 Body Node

The body node of the Push_IR response message should be formatted as follows:

Table 7-21: Push_IR – Request Body Node

Element	Purpose	Type	Inclusion
<Body>			
<PushIRRequest>			
<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, to obtain more detailed information. The link back to the originating systems is only available to users authorized by that system.	String	Mandatory
<EquipType/>	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.	String	Mandatory
<EventDef/>	One of the two provided event definitions must be selected and followed. Selection of type a) or b).	String	Mandatory
<FreqBand/>	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 band that are not supported at this moment.	String	Mandatory
<Location>	The node that includes details 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.		
<Country/>	The ISO Alpha-3 code country code where this interference event was detected.	String	Mandatory

<City/>	The name of the city of town where this interference event was detected.	String	Mandatory (default value = **NA** if the information is not provided)
<Coord/>	The latitude and longitude of the location where this interference event was detected, in decimal degrees. E.g. 52.934888, -1.164876	String	Mandatory (default value = **NA** if the information is not provided)
</Location>			
<Date/>	The date (relative UTC) of when this event was detected.	DateTime	Mandatory
<StartTime/>	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.	DateTime	Mandatory (default value = **NA** if the information is not provided)
<Duration/>	The duration of this event, when the selected event definition is true, in seconds.	String	Mandatory (default value = **NA** if the information is not provided)
<GNSSFixLost/>	A GNSS-receiver, at the location of the detection system, lost their position fix during this event; Yes or No.	Boolean	Mandatory (default value = **NA** if the information is not provided)
<EventSpectrum/>	A frequency spectrum of the detected event. A frequency and power vector (with equal length) shall be reported.	String	Mandatory (default value = **NA** if the information is not provided)
<RawData/>	A flag that indicates whether or not raw data (I/Q data) is available at the local event database.	Boolean	Mandatory (default value = **NA** if the information is not provided)
<AntennaType/>	The used antenna type.	String	Mandatory (default value = **NA** if the information is

			not provided)
<NoiseFigure/>	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.	String	Mandatory (default value = **NA** if the information is not provided)
<DeltaPow/>	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.	String	Mandatory (default value = **NA** if the information is not provided)
<BaseLineCN0/>	The average C/N0 (dB-Hz), for used satellites in the positioning solution, 1 minute before the interference was detected. 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.	String	Mandatory (default value = **NA** if the information is not provided)
<DeltaCN0/>	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.	String	Mandatory (default value = **NA** if the information is not provided)
</PushIRRequest>			
</Body>			

7.3.2 Push_IR Response Message

The STRIKE3 Gateway processes the Push_IR request synchronously and responds with a positive acknowledgment or suitable error/status message.

7.3.2.1 Header Node

For consistency with other messages in the solution, the header node should follow this format:

Table 7-22: Push_IR – Response Header Node

Element	Purpose	Type	Inclusion
<Header>			
<Version/>	May be required in future to allow backward compatibility in the event that message format definitions change over time.	String	Mandatory
<MsgDateTime/>	Date/time the message was originated, to millisecond precision.	DateTime	Mandatory
</Header>			

7.3.2.2 Body Node

The body node of the Push_IR response message should be formatted as follows:

Table 7-23: Push_IR – Response Body Node

Element	Purpose	Type	Inclusion
<Body>			
<PushIRResponse>			
<AckStatusFlag/>	0 – Upload process was successful, 1 – Upload process failed.	Integer	Mandatory
<AckMsg/>	Description of error from the WS	String	Mandatory
</PushIRResponse>			
</Body>			

7.4 Account Management Services (End Users)

These messages relate to the account management services included within interface ITF001 (see section 6.3.2) for the end users who wish to view results and analysis of events.

7.4.1 Add_IMU Request Message

This section describes the input parameters contained within the <header> and <body> nodes of the registration request message.

7.4.1.1 Header Node

For consistency with other messages in the solution, the header node should follow this format:

Table 7-24: Add_IMU – Request Header Node

Element	Purpose	Type	Inclusion
<Header>			
<Version/>	May be required in future to allow backward compatibility in the event that message format definitions change over time.	String	Mandatory
<MsgDateTime/>	Date/time the message was originated, to millisecond precision.	DateTime	Mandatory
</Header>			

7.4.1.2 Body Node

The following table describes the input parameters required by the Add_IMU WS:

Table 7-25: Add_IMU – Request Body Node

Element	Purpose	Type	Inclusion
<Body>			
<AddIMURequest>			
<Email/>	A valid corporate email address that will used to register the user to the	String	Mandatory

	system.		
<Forename/>	The first name of the user.	String	Mandatory
<Surname/>	The surname of the user.	String	Mandatory
<CompanyName/>	The full company name of the user.	String	Mandatory
<CompanySector/>	The sector/industry the company operates in.	String	Mandatory (default value = **NA** if the information is not provided)
<AddressLine/>	The address details of the company.	String	Mandatory (default value = **NA** if the information is not provided)
<TownCity/>	The town or city the company is registered to.	String	Mandatory (default value = **NA** if the information is not provided)
<PostCode/>	The post code address.	String	Mandatory (default value = **NA** if the information is not provided)
<Country>	The country name	String	Mandatory (default value = **NA** if the information is not provided)
<PhoneNum/>	A contact phone number.	String	Mandatory (default value = **NA** if the information is not provided)
</AddIMURequest>			
</Body>			

7.4.2 Add_IMU Response Message

The STRIKE3 Gateway processes the Add_IMU request synchronously and responds with the appropriate data (or suitable error/status messages). This means the body node of this response will consist of an either positive or negative node.

7.4.2.1 Header Node

For consistency with other messages in the solution, the header node should follow this format:

Table 7-26: Add_IMU – Response Header Node

Element	Purpose	Type	Inclusion
<Header>			
<Version/>	May be required in future to allow backward compatibility in the event that message format definitions change over time.	String	Mandatory
<MsgDateTime/>	Date/time the message was originated, to millisecond precision.	DateTime	Mandatory
</Header>			

7.4.2.2 Body Node

The body node of the Add_IMU response message should be formatted as follows:

Table 7-27: Add_IMU – Response Body Node

Element	Purpose	Type	Inclusion
<Body>			
<AddIMUResponse>			
<AddIMUPosResponse>	This node is used by the WS if it has successfully interpreted the parameters and has registration data to return to user/provider.		Optional
<Key/>	The license key will be used to authenticate requests to the system by users and providers. Length = 256Bit	String	Mandatory
<ClientID/>	To be used to identify requests to the system by users and providers. Length =128Bit	String	Mandatory
</AddIMUPosResponse>			
</AddIMUResponse>			
</Body>			

7.4.2.3 Negative Response Node

The purpose of the negative response node is to allow the WS to communicate to users the reasons for rejecting the request or to describe an error condition that prevents the WS satisfying the request. The <AddIMUNegResponse> node is populated and returned in the response to user and should be formatted as follows:

Table 7-28: Add_IMU – Negative Response Node

Element	Purpose	Type	Inclusion
<AddIMUNegResponse>	This node is used by the WS if it has failed to interpret the parameters or cannot return registration data to user/provider.		Optional
<ErrorMsg/>	Description of error from the WS.	String	Mandatory
</AddIMUNegResponse>			

7.4.3 View_IMU Request Message

This section describes the input parameters contained within the <header> and <body> nodes of the registration request message.

7.4.3.1 Header Node

For consistency with other messages in the solution, the header node should follow this format:

Table 7-29: View_IMU – Request Header Node

Element	Purpose	Type	Inclusion
<Header>			
<Version/>	May be required in future to allow backward compatibility in the event that message format definitions change over time.	String	Mandatory
<MsgDateTime/>	Date/time the message was originated, to millisecond precision.	DateTime	Mandatory
<Key/>	The license key provided during registration.	String	Mandatory
<ClientID/>	The client id provided during registration.	String	Mandatory

</Header>			

7.4.3.2 Body Node

The following table describes the input parameters required by the View_IMU WS:

Table 7-30: View_IMU – Request Body Node

Element	Purpose	Type	Inclusion
<Body>			
<ViewIMURequest>			
<Reason/>	A free text to describe the reason of this request.	String	Mandatory
</ViewIMURequest>			
</Body>			

7.4.4 View_IMU Response Message

The STRIKE3 Gateway processes the View_IMU request synchronously and responds with the appropriate data (or suitable error/status messages). This means the body node of this response will consist of an either positive or negative node.

7.4.4.1 Header Node

For consistency with other messages in the solution, the header node should follow this format:

Table 7-31: View_IMU – Response Header Node

Element	Purpose	Type	Inclusion
<Header>			
<Version/>	May be required in future to allow backward compatibility in the event that message format definitions change over time.	String	Mandatory
<MsgDateTime/>	Date/time the message was originated, to millisecond precision.	DateTime	Mandatory
</Header>			

7.4.4.2 Body Node

The body node of the View_IMU response message should be formatted as follows:

Table 7-32: View_IMU – Response Body Node

Element	Purpose	Type	Inclusion
<Body>			
<ViewIMUResponse>			
<ViewIMUPosResponse>	This node is used by the WS if it has successfully interpreted the parameters and has registration data to return to user/provider.		Optional
<Email/>	A valid corporate email address that will used to register the user to the system.	String	Mandatory
<Forename/>	The first name of the user.	String	Mandatory
<Surname/>	The surname of the user.	String	Mandatory
<CompanyName/>	The full company name of the user.	String	Mandatory
<CompanySector/>	The sector/industry the company operates in.	String	Mandatory (default value = **NA** if the information is not provided)
<AddressLine/>	The address details of the company.	String	Mandatory (default value = **NA** if the information is not provided)
<TownCity/>	The town or city the company is registered to.	String	Mandatory (default value = **NA** if the information is not provided)
<PostCode/>	The post code address.	String	Mandatory (default value = **NA** if the information is not provided)
<Country>	The country name	String	Mandatory (default value =

			NA if the information is not provided)
<PhoneNum/>	A contact phone number.	String	Mandatory (default value = **NA** if the information is not provided)
</ViewIMUPosResponse>			
</ViewIMUResponse>			
</Body>			

7.4.4.3 Negative Response Node

The purpose of the negative response node is to allow the WS to communicate to users the reasons for rejecting the request or to describe an error condition that prevents the WS satisfying the request. The <ViewIMUNegResponse> node is populated and returned in the response to user and should be formatted as follows:

Table 7-33: View_IMU – Negative Response Node

Element	Purpose	Type	Inclusion
<ViewIMUNegResponse>	This node is used by the WS if it has failed to interpret the parameters or cannot return registration data to user/provider.		Optional
<ErrorMsg/>	Description of error from the WS.	String	Mandatory
</ViewIMUNegResponse>			

7.4.5 Edit_IMU Request Message

This section describes the input parameters contained within the <header> and <body> nodes of the registration request message.

7.4.5.1 Header Node

For consistency with other messages in the solution, the header node should follow this format:

Table 7-34: Edit_IMU – Request Header Node

Element	Purpose	Type	Inclusion
<Header>			
<Version/>	May be required in future to allow backward compatibility in the event that message format definitions change over time.	String	Mandatory
<MsgDateTime/>	Date/time the message was originated, to millisecond precision.	DateTime	Mandatory
<Key/>	The license key provided during registration.	String	Mandatory
<ClientID/>	The client id provided during registration.	String	Mandatory
</Header>			

7.4.5.2 Body Node

The following table describes the input parameters required by the Edit_IMU WS:

Table 7-35: Edit_IMU – Request Body Node

Element	Purpose	Type	Inclusion
<Body>			
<AddIMURequest>			
<Email/>	A valid corporate email address that will used to register the user to the system.	String	Mandatory
<Forename/>	The first name of the user.	String	Mandatory
<Surname/>	The surname of the user.	String	Mandatory
<CompanyName/>	The full company name of the user.	String	Mandatory
<CompanySector/>	The sector/industry the company operates in.	String	Mandatory (default value = **NA** if the information is

			not provided)
<AddressLine/>	The address details of the company.	String	Mandatory (default value = **NA** if the information is not provided)
<TownCity/>	The town or city the company is registered to.	String	Mandatory (default value = **NA** if the information is not provided)
<PostCode/>	The post code address.	String	Mandatory (default value = **NA** if the information is not provided)
<Country>	The country name	String	Mandatory (default value = **NA** if the information is not provided)
<PhoneNum/>	A contact phone number.	String	Mandatory (default value = **NA** if the information is not provided)
</AddIMURequest>			
</Body>			

7.4.6 Edit_IMN Response Message

The STRIKE3 Gateway processes the Edit_IMU request synchronously and responds with a suitable error/status message.

7.4.6.1 Header Node

For consistency with other messages in the solution, the header node should follow this format:

Table 7-36: Edit_IMU – Response Header Node

Element	**Purpose**	**Type**	**Inclusion**

<Header>			
<Version/>	May be required in future to allow backward compatibility in the event that message format definitions change over time.	String	Mandatory
<MsgDateTime/>	Date/time the message was originated, to millisecond precision.	DateTime	Mandatory
</Header>			

7.4.6.2 Body Node

The body node of the Edit_IMU response message should be formatted as follows:

Table 7-37: Edit_IMU – Response Body Node

Element	Purpose	Type	Inclusion
<Body>			
<EditIMUResponse>			
<Msg/>	A response message from the WS.	String	Mandatory
</EditIMUResponse>			
</Body>			

7.4.7 Delete_IMU Request Message

This section describes the input parameters contained within the <header> and <body> nodes of the registration request message.

7.4.7.1 Header Node

For consistency with other messages in the solution, the header node should follow this format:

Table 7-38: Delete_IMU – Request Header Node

Element	Purpose	Type	Inclusion
<Header>			

<Version/>	May be required in future to allow backward compatibility in the event that message format definitions change over time.	String	Mandatory
<MsgDateTime/>	Date/time the message was originated, to millisecond precision.	DateTime	Mandatory
<Key/>	The license key provided during registration.	String	Mandatory
<ClientID/>	The client id provided during registration.	String	Mandatory
</Header>			

7.4.7.2 Body Node

The following table describes the input parameters required by the Delete_IMU WS:

Table 7-39: Delete_IMU – Request Body Node

Element	Purpose	Type	Inclusion
<Body>			
<DeleteIMURequest>			
<Email/>	The unique email address of the user.	String	Mandatory
</DeleteIMURequest>			
</Body>			

7.4.8 Delete_IMU Response Message

The STRIKE3 Gateway processes the Delete_IMU request synchronously and responds with a suitable error/status message.

7.4.8.1 Header Node

For consistency with other messages in the solution, the header node should follow this format:

Table 7-40: Delete_IMU – Response Header Node

Element	Purpose	Type	Inclusion
<Header>			
<Version/>	May be required in future to allow backward compatibility in the event that message format definitions change over time.	String	Mandatory
<MsgDateTime/>	Date/time the message was originated, to millisecond precision.	DateTime	Mandatory
</Header>			

7.4.8.2 Body Node

The body node of the Delete_IMU response message should be formatted as follows:

Table 7-41: Delete_IMU – Response Body Node

Element	Purpose	Type	Inclusion
<Body>			
<DelIMUResponse>			
<Msg/>	A response message from the WS.	String	Mandatory
</DelIMUResponse>			
</Body>			

7.5 Data Mining Service

These messages relate to the data mining service included within interface ITF003 (see section 6.3.2 and 6.3.4) for end users, and details how request for data are made and responses received.

7.5.1 Get_IMD Request Message

This section describes the input parameters contained within the <header> and <body> nodes of the report upload request message.

7.5.1.1 Header Node

For consistency with other messages in the solution, the header node should follow this format:

Table 7-42: Get_IMD – Request Header Node

Element	Purpose	Type	Inclusion
<Header>			
<Version/>	May be required in future to allow backward compatibility in the event that message format definitions change over time.	String	Mandatory
<MsgDateTime/>	Date/time the message was originated, to millisecond precision.	DateTime	Mandatory
<Key/>	The license key provided during registration.	String	Mandatory
<ClientID/>	The client id provided during registration.	String	Mandatory
</Header>			

7.5.1.2 Body Node

The body node of the Get_IMD response message should be formatted as follows:

Table 7-43: Get_IMD – Request Body Node

Element	Purpose	Type	Inclusion
<Body>			
<GetIMDRequest>			
<MatchRules/>	This flag indicates how to match the rules below. The value can be either ANY or ALL.	String	Mandatory
<NumOfRules/>	The number of rules in this request.	Integer	Mandatory
<Rules>	Container node for all rules in the request.		
<Rule/>	A comma separated text that describes a single query in the following format: ***REPORT_FIELD,COND,VALUE***. REPORT_FIELD could be any field from the table below. COND is either: >,<,=,<=,>=, LIKENOT LIKE VALUE is a numerical or text value	String	Mandatory
<\Rules>			
</GetIMDRequest>			
</Body>			

Table 44: Get_IMD Request - Query rule options

Report Field	Description	Rule Example
EQUIP_TYPE	The name of the type of detection equipment that has detected events.	*EQUIP_TYPE,=,GSS100D* *EQUIP_TYPE,LIKE,%GSS%*
EVENT_DEF	One of the two provided event definitions, either **a** or **b**.	*EVENT_DEF,=,a* *EVENT_DEF,LIKE,a*
FREQ_BAND	The frequency band where interference has been detected, current value supported 1575.42	*FREQ_BAND,=,1575.42*
REGION	The ISO Alpha-3 code of a country or the city/town name where	*REGION,LIKE,CZE*

	interference events have been detected.	
DATTIME	The date and time (relative UTC) of when an event was detected, in ISO8601 format (YYYY-MM-DDThh:mm:ss.sssZ).	*DATETIME,>,2017-09-10T00:00:00.000Z*
DURATION	The duration of an event, in seconds.	*DURATION,>=,10*
FIX_LOST	A GNSS-receiver, at the location of the detection system, lost their position fix during an event, true or false.	*GNSS_FIX_LOST,=,true*
RAW_DATA	A flag that indicates whether or not raw data (I/Q data) is available at the local event database, true or false.	*RAW_DATA,=,true*
DELTA_POW	Maximum delta power in decibel (dB).	*DELTA_POW,>,5*
DELTA_CN0	Maximum decrease in C/N0 in decibel (dB).	*DELTA_CN0,<=,6*

7.5.2 Get_IMD Response Message

The STRIKE3 Gateway processes the Get_IMD request synchronously and responds with the appropriate data (or suitable error/status messages). This means the body node of this response will consist of an either positive or negative node.

7.5.2.1 Header Node

For consistency with other messages in the solution, the header node should follow this format:

Table 7-45: Get_IMD – Response Header Node

Element	Purpose	Type	Inclusion
<Header>			

<Version/>	May be required in future to allow backward compatibility in the event that message format definitions change over time.	String	Mandatory
<MsgDateTime/>	Date/time the message was originated, to millisecond precision.	DateTime	Mandatory
</Header>			

7.5.2.2 Body Node

The body node of the Get_IMD response message should be formatted as follows:

Table 7-46: Get_IMD – Response Body Node

Element	Purpose	Type	Inclusion
<Body>			
<GetIMDResponse>			
<GetIMDPosResponse>	This node is used by the WS if it has successfully interpreted the parameters and has registration data to return to user/provider.		Optional
<NumOfData>	The number of data records returned in this request.		
<IMDataSet>	A container node for list of .IM data.		
<IMData>			
<S3ID>	A unique identifier of the event within the Strike3 database. Use this ID when requesting specific event information from the Strike3 server, ie Advanced data request service.	String	Mandatory
<EventID/>	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, to obtain more detailed information. The link back to the originating systems is only available to users authorized by that	String	Mandatory

	system.		
<EquipType/>	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.	String	Mandatory
<EventDef/>	One of the two provided event definitions must be selected and followed. Selection of type a) or b).	String	Mandatory
<FreqBand/>	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 band that are not supported at this moment.	String	Mandatory
<Location>	The node that includes details 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.		
<Country/>	The ISO country code where this interference event was detected.	String	Mandatory
<City/>	The name of the city or town where this interference event was detected.	String	Mandatory (default value = **NA** if the information is not provided)
<Coord/>	The latitude and longitude of the location where this interference event was detected, in decimal degrees. E.g. 52.934888, -1.164876	String	Mandatory (default value = **NA** if the information is

			not provided)
</Location>			
<Date/>	The date (relative UTC) of when this event was detected.	DateTime	Mandatory
<StartTime/>	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.	DateTime	Mandatory (default value = **NA** if the information is not provided)
<Duration/>	The duration of this event, when the selected event definition is true, in seconds.	String	Mandatory (default value = **NA** if the information is not provided)
<GNSSFixLost/>	A GNSS-receiver, at the location of the detection system, lost their position fix during this event; Yes or No.	Boolean	Mandatory (default value = **NA** if the information is not provided)
<RawData/>	A flag that indicates whether or not raw data (I/Q data) is available at the local event database.	Boolean	Mandatory (default value = **NA** if the information is not provided)
<AntennaType/>	The used antenna type.	String	Mandatory (default value = **NA** if the information is not provided)
<NoiseFigure/>	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.	String	Mandatory (default value = **NA** if the information is not provided)
<DeltaPow/>	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.	String	Mandatory (default value = **NA** if the information is not provided)

<BaseLineCN0/>	The average C/N0 (dB-Hz), for used satellites in the positioning solution, 1 minute before the interference was detected. 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.	String	Mandatory (default value = **NA** if the information is not provided)
<DeltaCN0/>	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.	String	Mandatory (default value = **NA** if the information is not provided)
</IMData>			
</IMDataSet>			
</GetIMDPosResponse>			
</GetIMDResponse>			
</Body>			

7.5.2.3 Negative Response Node

The purpose of the negative response node is to allow the WS to communicate to users the reasons for rejecting the request or to describe an error condition that prevents the WS satisfying the request. The <GetIMDNegResponse> node is populated and returned in the response to user and should be formatted as follows:

Table 7-47: Get_IMD – Negative Response Node

Element	Purpose	Type	Inclusion
<GetIMDNegResponse>	This node is used by the WS if it has failed to interpret the parameters or cannot return registration data to user/provider.		Optional
<ErrorMsg/>	Description of error from the WS.	String	Mandatory
</GetIMDNegResponse>			

7.6 Advanced Data Request

These messages relate to the advanced data request service included within interface ITF004 (see section 6.3.26.3.5) for end users, and details how requests for advanced data are made.

7.6.1 Get_Adv_IMD Request Message

This section describes the input parameters contained within the <header> and <body> nodes of the report upload request message.

7.6.1.1 Header Node

For consistency with other messages in the solution, the header node should follow this format:

Table 7-48: Get_Adv_IMD – Request Header Node

Element	Purpose	Type	Inclusion
<Header>			
<Version/>	May be required in future to allow backward compatibility in the event that message format definitions change over time.	String	Mandatory
<MsgDateTime/>	Date/time the message was originated, to millisecond precision.	DateTime	Mandatory
<Key/>	The license key provided during registration.	String	Mandatory
<ClientID/>	The client id provided during registration.	String	Mandatory
</Header>			

7.6.1.2 Body Node

The body node of the Get_Adv_IMD response message should be formatted as follows:

Table 7-49: Get_Adv_IMD – Request Body Node

Element	Purpose	Type	Inclusion
<Body>			
<GetAdvIMDRequest>			
<S3ID/>	A unique identifier of the event within the Strike3 database.	String	Mandatory
</GetAdvIMDRequest>			
</Body>			

7.6.2 Get_Adv_IMD Response Message

The STRIKE3 Gateway processes the Get_Adv_IMD request synchronously and responds with the appropriate data (or suitable error/status messages). This means the body node of this response will consist of an either positive or negative node.

7.6.2.1 Header Node

For consistency with other messages in the solution, the header node should follow this format:

Table 7-50: Get_Adv_IMD – Response Header Node

Element	Purpose	Type	Inclusion
<Header>			
<Version/>	May be required in future to allow backward compatibility in the event that message format definitions change over time.	String	Mandatory
<MsgDateTime/>	Date/time the message was originated, to millisecond precision.	DateTime	Mandatory
</Header>			

7.6.2.2 Body Node

The body node of the Get_Adv_IMD response message should be formatted as follows:

Table 7-51: Get_Adv_IMD – Response Body Node

Element	Purpose	Type	Inclusion
<Body>			
<GetAdvIMDResponse>			
<GetAdvIMDPosResponse>	This node is used by the WS if it has successfully interpreted the parameters and has registration data to return to user/provider.		Optional

<DetailedInfo/>	A detailed list of other type of information that is available in the system for authorized personnel only, plus details of how to access this detailed information (e.g. email contact details for request, ftp site details, etc.). The text format of this parameter shall be in **JSON.** An example of available data (e.g. RF and logs) via an FTP connection is shown below:
	{
	"info": "RF,logs",
	"conntype": "ftp",
	"host": "provider001",
	"user": "username",
	"password": "password",
	"port": "22",
	"remote_path": "/net001/sensors/",
	"file_permissions": "664",
	"dir_permissions": "775",
	"connect_timeout": 30,
	"keepalive": 120,
	"ftp_passive_mode": true,
	"remote_encoding": "utf-8",
	}
		JSON String	Mandatory
			(default value = **NA** if the information is not provided)

<EventSpectrum/>	A frequency spectrum of the detected event. A frequency and power vector (with equal length) shall be reported.	String	Mandatory (default value = **NA** if the information is not provided)

</GetAdvIMDPosResponse>
</GetAdvIMDResponse>
</Body>

7.6.2.3 Negative Response Node

The purpose of the negative response node is to allow the WS to communicate to users the reasons for rejecting the request or to describe an error condition that prevents the WS satisfying the request. The <GetAdvIMDNegResponse> node is populated and returned in the response to user and should be formatted as follows:

Table 7-52: Get_Adv_IMD – Negative Response Node

Element	Purpose	Type	Inclusion
<GetAdvIMDNegResponse>	This node is used by the WS if it has failed to interpret the parameters or cannot return registration data to user/provider.		Optional
<ErrorMsg/>	Description of error from the WS.	String	Mandatory
</ GetAdvIMDNegResponse >			

8 Future Considerations

Within STRIKE3, the centralised server is developed as a demonstration platform in order to showcase the use of the reporting standards to gather information from multiple networks and type of sensor. The purpose is to show what can be done and to arouse interest from potential users and stakeholders and not necessarily to represent a final operational system. Nevertheless, there are additional points to consider for the future if such a system were to be turned operational.

One is the question of who are the potential end-users of the aggregated data within the centralized database, and whether it can support revenue generation in some way. Some examples of end users of the system could be frequency regulators (to see level of activity in their Country), organisations that rely on GNSS for operations (e.g. aviation, road charging, timing community) or governments who implement GNSS based schemes (e.g. for road-charging) to see any impact of policy on the interference environment. The intention is to provide them with a high level view of activity and the change over time. Having the link back to the monitoring network operator to potentially get more detailed data allows the possibility of more in depth analysis. In terms of revenue generation, it depends on who runs the database but options to subsidize the running cost of STRIKE3 server platform could be a fixed member fee charged to each contributor, and maybe users, together with a per successful transaction or click for a user to take the services or special data of a contributor (similar to quidco cash-back model).

Another question is who will own the centralized database and the data therein. In part this depends on who shows interest in such a system and standardisation approach and who is willing to take on the operation of it. It could be a body like the GSA with a wide remit to promote GNSS. It could be a frequency regulator for a particular country, or a wider international body such as ITU. It could even be an industry led platform (e.g. NSL or another company who wish to provide this service). Part of the reason of limiting the data in the centralised database is so there is not anything very sensitive or confidential in the database - that is kept by the original monitoring network operators - so in the end this is just a platform for showing high level results and then to enable links between end users and monitoring network operators.

Linked to this is the question of whether a distributed database architecture could be used instead of a single centralized one. For example, it may be easier to convince a European entity to maintain a database for Europe, and a North American entity for NA, rather than convincing someone to maintain a single world-wide database. Certainly this is possible but to the end user there is probably more benefit if the central database spans multiple networks from many different countries in order to get a comparison of the level of interference from different places, but you could potentially see the case where a single country maintains a database including a lot of the optional information, and then have a database combining results from multiple countries than includes only the minimum set of information. The reporting standards do not preclude this and are there to make comparing data from different monitoring networks easier at region, country or global level.

In terms of the reporting system itself there is a question over whether there should be any performance guarantees to end-users, e.g. availability, reliability, response time, etc. of the database. However, at this stage there is no intention for that – this type of reporting system is not meant to be for real-time alerts or enforcement, for example. If such requirements are required by end users then it is expected these will apply to the monitoring networks themselves that are deployed for specific purposes.

Finally there is the issue of data quality and how can it be guaranteed that the event information provided by contributors is authentic/realistic. This may be difficult to achieve completely without more stringent checks on the contributing organisations and their detection equipment, but there are certain things that can be done to help in this regard. Having registration for providers and the standard event definition to follow hopefully goes some way to ensuring results are consistent, but it does rely on the provider using the event definition in the correct way and not (intentionally or unintentionally) providing erroneous data. One thing that could be considered for an operational system is having some sort of feedback mechanism from end users - like ratings for sellers on ebay - so if people request additional data and get poor responses or the data is wrong this is reported to the system and can be flagged. Another option may be to provide example event information to a contributor when they register and use this as a check that they are checking events against the standard event definition criteria correctly.

Annex

WSDL files for data provider web services and end user web services are provided separately as attachements.

END OF DOCUMENT