NAVISAT

Certification Study - Phase 2

Initial Requirement Baseline

Written by	***Responsibility*** + handwritten signature if no electronic workflow tool
Jean Pierre Ollivier-Henry	
Matthieu Dabin	
NAVISAT	
Verified by	
Matthieu Dabin	
Approved by	
Charlotte Neyret-Gigot	

Approval evidence is kept within the documentation management system.

CHANGE RECORDS

ISSUE	DATE	§ CHANGE RECORDS	AUTHOR
0.1	25/03/2010	First Draft Version to provide required inputs	JPOH, MD
0.2	23/04/2010	Second Draft Version providing more information on requirements process and RFI content	JPOH, MD
0.3	7/06/2010	Third Draft version updated with actions 1) and 2) defined during the meeting held on the 19/05/2010 in Cairo.	JPOH, MD
1.0	6/07/2010	Version 1.0 updated with NAVISAT comments during the meeting held in Cairo on the 5 & 6/07/2010	JPOH, MD, NAVISAT

TABLE OF CONTENTS

ATTACHMENTS:

1- **ICAO Annex 10 Volume 3, Part 1, Chapter 4. Aeronautical Mobile Satellite (route) Service**
2- **Manual for Aeronautical Mobile Satellite (Route) Service – Draft 1st edition. ICAO**

1. SCOPE OF THIS DOCUMENT

1.1 Context

This document is produced in the context of the NAVISAT frequency coordination, regulatory and certification study – Phase 2.

This deliverable, produced under WP4 "NAVISAT Certification support" is the third issue of the "Initial Certification Requirements baseline" provided to NAVISAT as an helpful basis to define the NAVISAT System certification framework.

1.2 Objective

After recalling NAVISAT services and associated Certification context and need, this document aims at providing an initial Certification requirements baseline to be considered by the different parties (CAAs, Industry, Operator) to initiate the certification process. It can be considered as a "guideline".

Knowledge and implementation of such requirements would also give confidence in the NAVISAT delivered Services to the ANSPs or to the relevant certification Authority.

This initial requirements baseline is defined using the European regulation framework as example and support material. It has then to be adapted by NAVISAT to the local context for finalization and implementation when needed.

Three categories of requirements are proposed in this initial baseline:

- **Category 1: the organizational requirements.** The requirements of this first category are selected and adapted from the **European Regulation context** (mainly [RD02]) related to ANSP certification. The objective is to propose an adapted framework that can be made applicable to NAVISAT organization. Their selection is based on what could be requested by an Authority or an ANSP to NAVISAT in terms of organization for the operation of such safety related system, and what is interesting to implement by NAVISAT to be prepared to this Certification phase.
- **Category 2: The technical requirements** applicable to the Communication System design and that should be the basis for the Technical compliance demonstration:
    - Technical requirements related to the Communication System mission: ICAO Annex 10 requirements (called by regulation).
    - Manual for Aeronautical Mobile Satellite (Route) Service . ICAO std.
    - Safety related technical requirements which need to be considered for the design of such system.
- **Category 3: Inputs for Dependability and Safety Processes** that need to be implemented by Industry in the frame of the design phase for dependability and safety compliance demonstration. This should be part of the Product Assurance process.

1.3 Reference document

[RD01] NAVISAT Certification Study – Phase 1. D4.4 – Recommendations for NAVISAT certification roadmap including elements of Estimated Cost of certification. Issue 1.0. 1/09/2009

[RD02] Commission regulation (EC) No 2096/2005 of 20 December 2005 laying down common requirements for the provision of air navigation services

[RD03] Regulation (EC) No 550/2004 of the European Parliament and of the council of 10 March 2004 on the provision of air navigation services in the single European sky (the service provision Regulation)

[RD04] Regulation (EC) No 552/2004 of the European Parliament and of the council of 10 March 2004 on the interoperability of the European Air Traffic Management network (the interoperability Regulation)

[RD05] ICAO Standard and recommended practices: Annex 10 Volume 3 Part 1 Chapter 4: Aeronautical Mobile-Satellite (Route) Service (AMS(R)S)

[RD06] Manual for Aeronautical Mobile Satellite (Route) Service – Draft 1st edition. ICAO

[RD07] Regulation (EC) N°1315/2007 Safety Oversight Regulation

[RD08] ICAO Standard and recommended practices: Annex 11.

All these reference documents will be attached on a CD-Rom.

1.4 Limitation of the document

This document presents an initial baseline of requirements selected for NAVISAT context and issued from the European Air Navigation Services Regulation framework and from ICAO standards

This referential recalled in the Reference documents (§1.3) is used in Europe for Air Navigation Services Systems and Organisation Certification purpose.

However, it must be clarified that this document, which is an initial requirement baseline, needs to be used as a "guideline" by the different parties involved in the certification process (CAA's, NAVISAT Certification team, industry, operator) to understand what is proposed and be prepared to this certification process.

It also obvious that this document is not exhaustive today and need to be updated in the future with relevant requirements related to the Region context and System performances.

2. NAVISAT SERVICES AND CERTIFICATION CONTEXT

In order to understand which kind of requirements could be proposed in the frame of NAVISAT context, it is necessary to recall the services potentially delivered by NAVISAT and the associated certification constraints.

The information are issued from the study done in phase 1 [RD01].

2.1 The NAVISAT case

NAVISAT is an organisation intending to provide in the African and Middle East regions a set of services in the following domains:

- Mobile safety communication services between aircraft and ATC centres, Companies, etc.

- Fixed communication services between ATC centres or between ATC and meteorological centres.
- Satellite Navigation services.

Generally speaking, the objectives of certification activity is to provide confidence, via evidences and justifications (Certification Review Items) for CAA's and to enable Air Navigation Traffic Service Providers to demonstrate that their communications infrastructure solution based on NAVISAT system fit for purpose to their regulators.

The General principle applied to the NAVISAT services study case is the following one:

- The National or transnational Authority is in charge of defining the regulation referential. It certifies the ANSP and accepts the ANSP Safety case before the System operation and Service Authorisation. The Authority can also certifies other entities when defined by the referential (for example the main subcontractors).
- The Air Navigation Service Providers (ANSP) is in charge of delivering the service to the "End user".
    - It implements an internal "safety organisation" and presents a safety case to the Authority
    - It "qualifies " all its subcontractors contributing to the "safety" mission
    - It collects all the necessary evidences, data, studies, indicators from the subcontractors contributing to the justification of its safety case.
    - Such organisation with subcontractors is managed by contract.
- The subcontractors contributing to "safety or availability tasks":
    - They have an organisation in place consistent with the ANSP certification need (Safe and available Service delivery, operation, data & evidence delivery, change management, etc.)
    - The operated system is qualified for the ANSP service delivery.
    - The qualification is maintained in case of evolution, maintenance, etc.

The following paragraph presents the context of each of the service and identifies in a certification context what could be the position and actions to be done by NAVISAT. This service description is recalled from [RD01].

2.1.1 Fixed services

The fixed communication service could be provided either to VSAT network operators or in some cases directly to end users. In this last case the mission of NAVISAT should also encompass the provision of Hub and earth stations and management of the ground network necessary services.

The first case is likely the most probable for this service. It will be the only one addressed in the scope of this document.

The fixed service function provided by NAVISAT will be used by VSAT network operator/service provider that will sell their service to several types of end users. Technically speaking the NAVISAT mission will be to provide a transparent transceiving capability in the appropriate frequency band.

The certification of this satellite capability itself has no meaning due to the fact that this function is not capable to provide a service to end users. The fixed service capability is only an enabler to provide the VSAT service to end users.

It is clearly the VSAT network operator/service provider that will build the certification file to be presented to the relevant authority.

NAVISAT position:

In that case, NAVISAT is a subcontractor. NAVISAT should design and operate fixed services installation qualified to respect the Customer objectives.

NAVISAT should have an organisation and provide justifications and evidences to support the VSAT network operator/service provider certification case.

The last part of this document gives input to help NAVISAT to be prepared to this role.

The technical evidences to be provided by NAVISAT and necessary to support the ANSP Service provider safety case (design justification, service and/or safety indicators, service availability measurement, etc.) need to be defined between the different parties in a contractual frame.

2.1.2 SBAS Services

The navigation payload provided by NAVISAT will be used by an SBAS operator/service provider. Technically speaking the NAVISAT mission will be to provide a transparent transmitting capability in a given frequency band.

The certification of the payload itself is a non sense due to the fact that the payload itself is not providing any service usable by end users. The payload is only an enabler to provide the SBAS service.

If we take the EGNOS case, several payloads are provided by Inmarsat and tomorrow by ASTRA. Those payloads are linked to NLESs (Navigation Land Earth Station) that generate the signal to be broadcasted, the payload does not provide other function than broadcasting without any change the signal uploaded by the NLES.

It is clearly the SBAS operator/service provider that will build the certification file to be presented to the relevant authority. The only link with the payload provider will be the organisational or technical requirements formulated in the form of an ICD (Interface Control Document) and the associated SLA (Service Level Agreement) specifying the quality of service (availability, time to restore in case of failure, financial incentive or penalties, …).

NAVISAT will have to set up such contractual arrangements with future SBAS providers (e.g. ESSP in Europe or Regional providers for Africa and Middle East).

Due to the fact that those future SBAS operators does not exist at that stage it is recommended to use the ICD and SLA elaborated within the EGNOS development as the basic input for this service, thus facilitating the "certification" aspects by direct similarity with the EGNOS/ESSP case.

NAVISAT position:

This case is quite similar to the one described in §2.1.1. In that case, NAVISAT is also a subcontractor. NAVISAT should design and operate a navigation payload qualified to respect the Customer objectives.

NAVISAT should have an organisation and should be able to provide justifications and evidences to support the SBAS Operator/Service provider certification case.

The last part of this document gives input to help NAVISAT to be prepared to this role.

The technical evidences necessary to support the Service provider safety case (design justification, service and/or safety indicators, service availability measurement, etc.) need to be defined between the different parties in a contractual frame.

2.1.3 Mobile Air/Ground Communication Service

The mobile air/ground communication service is intended to be provided to the end users through two possible solutions:

- In the short term, the air/ground communication service is intended to be provided mainly through recognised Communication Service Providers (CSP) like SITA or ARINC.
- In the medium term, it will be provided certainly through direct contractual arrangements between NAVISAT and end users.

In the first context, NAVISAT will be a provider of link capacity to CSP and mainly SITA that is the main CSP for the two regions (Africa and Middle East).

This current situation does not impose to SITA, for example, to be certified by national or regional authorities (e.g. in Europe SITA is not certified but is considered as a sub-contractor of ANSP as far as ATS communications are concerned). Therefore there is no clear certification obligation resulting from this level of service.

However, it is clearly SITA or other CSPs that have to develop a certification file to be presented to the relevant authority if required in a near future (it is very unlikely that such situation occurs). The link with the CSPs will be the organisational and the technical requirements formulated in the form of an ICD (Interface Control Document) and the associated SLA (Service Level Agreement) specifying the quality of service (availability, time to restore in case of failure, financial incentive or penalties, …).

In medium terms, the migration of ATM data-link communications from ACARS (corresponding to Inmarsat Classic Aero SDM data 2 service) toward ATN (corresponding to Inmarsat Classic Aéro SDM Data 3 service) that will be motivated, in Europe and the USA, by 2015, by mandatory carriage of ATN routers (mainly associated with VDL mode 2 radio link) applicable to aircraft flying in their upper airspace.

In this new context, as it seems to be the case in Europe, the provision of “Data3” Inmarsat like service could be required in other regions (Middle East and Africa) simply due to the proportion of the fleet fitted with this new capability.

It could then be possible that NAVISAT as potential Data 3 service provider has direct links with ANSPs and with airspace users thus changing its responsibilities and duties in the service provision. In such situation NAVISAT could be requested to provide more detailed compliance demonstration and be subjected to a new level of certification.

NAVISAT position:

In the short term, NAVISAT is a provider of a link capacity to a ANSP subcontractor. Its role is to be able to design and operate a link ensuring the delivery of the data to the ANSP subcontractor (CSP). NAVISAT should be able to demonstrate that the data are delivered according to the relevant Standard or Customer specification.

In the mid term, NAVISAT is again a direct subcontractor of the ANSP. The principle is there the same as in the other cases. The only point to highlight is perhaps the importance of the task to be done and the responsibility level

NAVISAT should have an organisation and should be able to provide justifications and evidences to support the Operator/Service provider certification case.

The last part of this document gives input to help NAVISAT to be prepared to this role.

The technical evidences necessary to support the Service provider safety case (design justification, service and/or safety indicators, service availability measurement, etc.) need to be defined between the different parties in a contractual frame.

2.2 Link with Certification

The analysis done in the three business cases before shows that, in most of the cases studied, NAVISAT is not considered as an ANSP. It means that normally NAVISAT does not need to be formally certified by an Authority as an ANSP.

However, NAVISAT can contributes to a “safety of life” service delivery or to an “Safety related Communication/Navigation” service delivery which is provided to the end users by a “Certified ANSP”.

In an usual Certification Referential, NAVISAT is considered in a position to provide, what is called, an “External Service” to ANSP and can contributes directly to the end user “safety”.

It means that the ANSP shall ensure that NAVISAT controls its design and operation (including maintenance) in order to be compliant to the allocated safety related requirements.

NAVISAT shall be able to demonstrate this compliance. This means that NAVISAT should be able to ensure confidence to the ANSP wrt its own mission:

- NAVISAT Operational organisation is in place and is able to provide the ANSP (or N-1 Subcontractor) with the necessary indicators, feedback and justification wrt the need of the ANSP safety case or Safety Management System records in the frame of operation.
- NAVISAT Technical system design respect the “safety”, “Dependability” requirements wrt the overall mission objective. Evidences exist and can be provided to the ANSP and Authority when necessary (technical files) to support the ANSP safety case.
- NAVISAT Design team is in place in order to assess and document the impact of the System evolutions and maintain its qualification.

3. CATEGORY N°1: REGULATION CONTEXT AND ASSOCIATED REQUIREMENTS

3.1 Introduction for requirements selection

The previous part has shown that NAVISAT activity can contribute to Safety Of Life Services even if NAVISAT is not directly considered as ANSP. In this context, NAVISAT should implement an organization able to answer to an Authority or to ANSPs and demonstrate its compliance to the referential (regulation and/or specification).

Usually such organizational framework is proposed by the States regulation. As a working support, the main texts of European regulation related to ANSP certification are taken into account to propose a selection of appropriate requirements to the NAVISAT context.

But only the most appropriate regulation texts for the present work is considered in the selection of the requirements.

These EC texts are the following ones:

- **Regulation (EC) 1315/2007** – Safety oversight regulation [RD07]. This regulation concern the Safety oversight to be done by the Authority and is considered not relevant for the present work.
- **Regulation (EC) No 550/2004** - the service provision Regulation- [RD03]. This regulation also concerns the authority and is considered not relevant for the present work.
- **Regulation (EC) No 552/2004** – Interoperability regulation [RD04]. This regulation defines the Declaration of Verification to be done by ANSP and to be presented to the Authority with a Technical File. As the aim of this document is focused on the project preparation and development phase, the way to do a "declaration of verification" is not developed.

  However, such process can concern NAVISAT if the CAA decide to request a Declaration of Verification to deliver the Certificate to the ANSP.
- **Regulation (EC) No 2096/2005** (Common Requirements for the provision of air navigation services) - [RD02]. This regulation is the most relevant for the present work. It gives inputs for the organization to put in place in such certification process and call for the technical ICAO standard of the domain. It is the reason why this regulation is selected as the basis if this Category 1 of requirements.

3.2 Requirements selection

This paragraph is then a proposition of a regulatory context based on the European Regulation (EC) n° 2096/2005 of 20 December 2005 laying down common requirements for the provision of Air Navigation Services [RD02].

This European regulation text is tailored as an example in order to highlight applicable requirements to NAVISAT.

The selection criteria for the requirements is based on the NAVISAT position and aims at keeping the spirit of the certification process but without introducing too heavy constraints which are useless. Mainly the topics related to organization and technical area are kept and derived. Financial and business requirements are not considered.

Basically, three parts of the initial text are kept:

- Part 1: Article 1 to 8 are related to the regulation context and the role of NAVISAT. The following topics considered in the scope of NAVISAT interest are derived:
  - Risk methodology, Safety management system, Qualification & training of people involved in safety tasks
  - Be able to provide evidence of compliance to general and specific requirements
  - Notification of change and keep compliance
  - Case of Loss of qualification/certification
  - Compliance monitoring by ANSP or Authority

- Part 2: Annex 1 of the regulation. Presents general requirements related to organization (Safety management System)
- Part 3: Annex 5 of the regulation presents the specific requirements for the provision of communication, navigation or surveillance services. Be able to ensure safety and availability performance. Working methods and operating procedures refer to ICAO std.

 # Part 1: Regulation context

Definition:

- **Safety assurance:** shall mean all planned and systematic actions necessary to afford adequate confidence that a product, a service, an organization, or a functional system achieves acceptable or tolerable safety.
- **Safety objective**: shall mean a qualitative or quantitative statement that defines the maximum frequency or probability at which a hazard can be expected to occur.
- **Safety requirement:** shall mean a risk-mitigation means, defined from the risk mitigation strategy that achieves a particular safety objective, including organizational ; operational, procedural, functional, performance and interoperability requirements or environment characteristic.

Article 1: Subject-matter and scope

This Regulation identifies and adopts the mandatory provisions of the following Safety Regulatory Requirements which are relevant for the certification of air navigation service providers and qualification of ANSP External provider Subcontractors like NAVISAT:

- Implementation of a Risk assessment methodology for design and changes assessment wrt System safety objectives
- Implementation of a Safety Management System including safety performance monitoring and incident recording wrt NAVISAT service and contribution to ANSP safety related mission.
- Qualification and training of people involved in “critical tasks” for operation and maintenance

Article 2: Granting of certificates or Qualification

1. In order to obtain the Certificate/Qualification necessary to provide the relevant External Services, External Service providers shall comply with the general following common requirements set in annex I as well as with the specific requirements set out in annex II to V.
2. A national supervisory authority (/ANSP) shall verify an External Service Provider's compliance with the common requirements before issuing a Certificate/Qualification to that provider.
3. An External Service provider shall comply with the common requirements no later than [TBD].

Article 3: Demonstration of compliance

Compliance to the following common requirements to be demonstrated by the External Service Provider to ANSP (or Authority):

1. External Service Provider shall contribute, on ANSP request, to provide evidences to the common requirements as far as activities are concerned.

2. An External Service Provider (subcontractor) shall notify the ANSP (Authority) of planned changes to its provision of services which may affect its compliance with the applicable common requirements or with the conditions attached to its qualification/certification.

3. An External Service Provider shall notify the ANSP (Authority) of planned safety related changes to the provision of its services.

4. Where a Qualified External Service Provider does not comply any longer with the applicable common requirements or with the conditions attached to the qualification, the competent ANSP supported by the National Supervisory Authority shall take a decision within a time period not exceeding one month [TBC]. By this decision, the ANSP supported by the National Supervisory Authority shall require the External Service Provider to take corrective action. The decision shall immediately be notified to the relevant External Service Provider.
5. The ANSP shall check that the corrective action has been implemented before notifying its approval to the relevant External service provider.

Article 4 & 5: removed for NAVISAT context

Article 6: Facilitation of compliance monitoring

External service providers shall facilitate inspections and surveys by the ANSP or by a recognised organisation acting on the latter's behalf, including site visits *(and visits without prior notice?)*

The authorised persons shall be empowered to perform the following acts:

(a) to examine the relevant records, data, procedures and any other material relevant to the provision of safety related service services;

(b) to take copies of or extracts from such records, data, procedures and other material;

(c) to ask for an oral explanation on site;

(d) to enter relevant premises, lands or means of transport.

Such inspections and surveys shall be carried out in compliance with the legal provisions of the Member State in which they are to be undertaken.

Article 7: On-going compliance

The ANSP (or Authority) shall, on the basis of the evidence at its disposal, monitor annually the ongoing compliance of the External Service Providers which it has qualified.

This can be done through an inspection programme covering all the external providers. The programme shall indicate the envisaged interval of the inspections of the different sites.

Article 8: Entry into force

This Regulation shall enter into force on the third day following its publication in the Official Journal of the XXX

 # Part 2:

Annex I: General Requirements for the provision of External Service

1. Organisational Structure & management

1.1. Organisational structure

An External Service provider shall set up and manage its organisation according to a structure that supports the safe, efficient and continuous provision of services.

The organisational structure shall define:

(a) the authority, duties and responsibilities of the nominated post holders, in particular of the management personnel in charge of safety, quality, security, finance and human resources related functions;

(b) the relationship and reporting lines between different parts and processes of the organisation.

 # 2. Safety and Quality Management

 # 2.1. Safety Management

An External Service provider shall manage the safety of all its services. In doing so, it shall establish formal interfaces with all stakeholders which may influence directly the safety of its services.

 # 2.2. Quality management system

An External Service provider shall have in place at the latest two years after entry into force of this Regulation a quality management system which covers all Communication/navigation services it provides

 # 2.3. Operations manuals

An External Service provider shall provide and keep up-to-date operations manuals relating to the provision of its services for the use and guidance of operations personnel. It shall ensure that:

(a) Operations manuals contain instructions and information required by the operations personnel to perform their duties;

(b) relevant parts of the operations manuals are accessible to the personnel concerned;

(c) the operations personnel are expeditiously informed of the amendments to the operations manual applying to their duties as well as of their entry into force.

 # 3. Security (TBC]

An External Service provider shall establish a security management system to ensure:

(a) the security of its facilities and personnel so as to prevent unlawful interference with the provision of services;

(b) the security of operational data it receives or produces or otherwise employs, so that access to it is restricted only to those authorised.

The security management system shall define:

(a) the procedures relating to security risk assessment and mitigation, security monitoring and improvement, security reviews and lesson dissemination;

(b) the means designed to detect security breaches and to alert personnel with appropriate security warnings;

(c) the means of containing the effects of security breaches and to identify recovery action and mitigation procedures to prevent re-occurrence.

An External Service provider shall ensure the security clearance of its personnel, if appropriate, and coordinate with the relevant civil and military authorities to ensure the security of its facilities, personnel and data.

 # 4. Human Resources

An External service provider shall employ appropriately skilled personnel to ensure the provision of its services in a safe, efficient, continuous and sustainable manner. In this context, it shall establish policies for the recruitment and training of personnel.

 # PART 3:

 # ANNEX V: SPECIFIC REQUIREMENTS FOR THE PROVISION OF COMMUNICATION, NAVIGATION OR SURVEILLANCE SERVICES

 # 1. TECHNICAL AND OPERATIONAL COMPETENCE AND CAPABILITY

A provider of communication, navigation or surveillance services shall ensure the availability, continuity, accuracy and integrity of its services.

A provider of communication, navigation or surveillance services shall confirm the quality level of the services it is providing and shall demonstrate that its equipment is regularly maintained and where required calibrated.

 # 2. SAFETY OF SERVICES

A provider of communication, navigation or surveillance services shall comply with the requirements of Annex II, part 3 on the safety of services (See below)

 # 2.1 Safety Management System

 # 2.1.1. General Safety requirements

A provider of External Services shall, as an integral part of the management of its services, **have in place a Safety Management System (SMS)** which:

- **ensures a formalised, explicit and proactive approach to systematic safety management** in meeting its safety responsibilities within the provision of its services; operates in respect of all its services and the supporting arrangements under its managerial control; and includes, as its foundation, a statement of **safety policy defining the organisation's fundamental approach to managing safety** (safety management),

- ensures that **everyone** involved in the safety aspects of the provision of the services **has an individual safety responsibility for their own actions**, that the **top management of the provider carries an overall safety responsibility** (safety responsibility),
- ensures that the **achievement of satisfactory safety** in services shall be afforded the **highest priority** (safety priority),
- ensures that while providing safety related services, the principal safety objective is to **minimise its contribution to the risk** of an aircraft accident as far as reasonably practicable (safety objective).

 # 2.1.2 Requirements for safety achievement

Within the operation of the SMS, a provider of External services shall:

- ensure that **personnel are adequately trained and competent for the job they are required to do**, in addition to being properly licensed if so required and satisfying applicable medical fitness requirements (competency),
- ensure that a **safety management function is identified with organisational responsibility for development and maintenance of the safety management system**; ensure that this point of responsibility is independent of line management, and accountable directly to the highest organisational level. However, in the case of small organisations where combination of responsibilities may prevent sufficient independence in this regard, the arrangements for safety assurance shall be supplemented by additional independent means; and ensure that the top management of the service provider organisation is actively involved in ensuring safety management (safety management responsibility),
- ensure that, wherever practicable, **quantitative safety levels are derived and are maintained for all functional systems** (quantitative safety levels),[TBC]
- ensure that the **SMS is systematically documented** in a manner, which provides a clear linkage to the organisation's safety policy (SMS documentation),
- ensure **adequate justification of the safety of the externally provided services and supplies**, having regard to their safety significance within the provision of its services (external services and supplies),
- ensure that **risk assessment and mitigation is conducted to an appropriate level** to ensure that due consideration is given to all aspects of the provision of the External delivered Service (risk assessment and mitigation). As far as changes to the External service functional system are concerned, the provisions of part 1.2 of this Annex shall apply,
- ensure that **External Service operational or technical occurrences which are considered to have significant safety implications are investigated immediately**, and any necessary corrective action is taken (safety occurrences). It shall also demonstrate that it has implemented the requirements on the reporting and assessment of safety occurrences in accordance with applicable national and Community law.

 # 2.1.3 Requirements for safety assurance

Within the operation of the SMS, a provider of External safety related services shall ensure that:

- **safety surveys are carried out as a matter of routine**, to recommend improvements where needed, to provide assurance to managers of the safety of activities within their areas and to confirm compliance with the relevant parts of the SMS (safety surveys),

- **methods are in place to detect changes in functional systems or operations** which may suggest any element is approaching a point at which acceptable standards of safety can no longer be met, and that corrective action is taken (safety monitoring),
- **safety records are maintained throughout the SMS operation** as a basis for providing safety assurance to all associated with, responsible for or dependent upon the services provided, and to the ANSP/National Supervisory Authority (safety records).

 # 2.1.4 Requirements for safety promotion

Within the operation of the SMS, a provider of External safety related services shall ensure that:

- **all personnel are aware of the potential safety hazards connected with their duties** (safety awareness),
- the **lessons arising from safety occurrence investigations** and other safety activities **are disseminated** within the organisation at management and operational levels (lesson dissemination),
- **all personnel are actively encouraged to propose solutions to identified hazards, and changes** are made to improve safety where they appear needed (safety improvement).

 # 2.2. Safety requirements for risk assessment and mitigation with regard to changes

 # 2.2.1. Section 1 [TBC]

Within the operation of the SMS, a provider of External safety related services shall ensure that hazard identification as well as **risk assessment and mitigation are systematically conducted for a new System of for any changes** to those parts of the Navigation/Communication functional system in a manner which addresses:

- the complete life cycle of the constituent part of the Navigation/Communication functional system under consideration, from initial planning and definition to post-implementation operations, maintenance and de-commissioning;
- the airborne, ground and, if appropriate, spatial components of the Navigation/Communication functional system, through cooperation with responsible parties,
- the equipment, procedures and human resources of the Navigation/Communication functional system, the interactions between these elements and the interactions between the constituent part under consideration and the remainder of the Navigation/Communication functional System. [TBC]

 # 2.2.2. Section 2

The **hazard identification**, risk assessment and mitigation processes shall include:

(a) a determination of the scope, boundaries and interfaces of the constituent part being considered, as well as the identification of the functions that the constituent part is to perform and the environment of operations in which it is intended to operate;

(b) **a determination of the safety objectives** to be placed on the constituent part, incorporating:

- an identification of External safety related services credible hazards and failure conditions, together with their combined effects,

- an assessment of the effects they may have on the safety of aircraft, as well as an assessment of the severity of those effects, using the severity classification scheme dedicated to such assessment (see proposition in §4)
- a determination of their tolerability, in terms of the hazard's maximum probability of occurrence, derived from the severity and the maximum probability of the hazard's effects, in a manner consistent with Section 4;

(c) **the derivation, as appropriate, of a risk mitigation strategy** which:

- specifies the defences to be implemented to protect against the risk-bearing hazards,
- includes, as necessary, the development of safety requirements potentially bearing on the constituent part under consideration, or other parts of the ATM functional system, or environment of operations, and
- presents an assurance of its feasibility and effectiveness;

(d) **verification that all identified safety objectives and safety requirements have been met**:

- prior to its implementation of the change,
- during any transition phase into operational service,
- during its operational life, and
- during any transition phase until decommissioning.

 # 2.2.3. Section 3

The results, associated rationales and evidence of the risk assessment and mitigation processes, including hazard identification, shall be collated and documented in a manner which ensures that:

- complete arguments are established to demonstrate that the constituent part under consideration, as well as the overall Communication/Navigation functional system are, and will remain tolerably safe by meeting allocated safety objectives and requirements. This shall include, as appropriate, specifications of any predictive, monitoring or survey techniques being used,
- all safety requirements related to the implementation of a change are traceable to the intended operations/-functions

 # 2.2.4. Section 4

Hazard identification and severity assessment

A systematic identification of the hazards shall be conducted. The severity of the effects of hazards in a given environment of operations shall be determined using the classification scheme proposed in section 4 and based on the following scale:

1 – Catastrophic

2 – Hazardous

3 – Major

4 – Minor

5 – Negligible

Risk classification scheme

Safety objectives based on risk shall be established in terms of the hazards maximum probability of occurrence, derived both from the severity of its effect, and from the maximum probability of the hazard's effect.

The demonstration shall establish that quantitative objectives are met.

 # 2.2.5 Section 5

Software safety assurance system

Within the operation of the safety management system, a provider of air traffic services shall implement a software safety assurance process in accordance with International SW Development Standards (for instance DO 178B).

 # 2.3. Safety requirements for engineering and technical personnel undertaking operational safety related tasks

A provider of External safety related services shall ensure that technical and engineering personnel including personnel of subcontracted operating organisations who operate and maintain ATM equipment approved for its operational use have and maintain sufficient knowledge and understanding of the services they are supporting, of the actual and potential effects of their work on the safety of those services, and of the appropriate working limits to be applied.

With regard to the personnel involved in safety related tasks including personnel of subcontracted operating organisations, the provider of External safety related services shall document the adequacy of the competence of the personnel; the rostering arrangements in place to ensure sufficient capacity and continuity of service; the personnel qualification schemes and policy, the personnel training policy, training plans and records as well as arrangements for the supervision of non-qualified personnel.

A provider of External safety related services shall maintain a register of information on the numbers, status and deployment of the personnel involved in safety related tasks. The register shall:

(a) identify the accountable managers for safety related functions;

(b) record the relevant qualifications of technical and operational personnel, against required skills and competence requirements;

(c) specify the locations and duties to which technical and operational personnel are assigned, including any rostering methodology.

 # 3. WORKING METHODS AND OPERATING PROCEDURES

A provider of communication, navigation or surveillance services shall be able to demonstrate that its working methods and operating procedures are compliant with the standards of **Annex 10 on aeronautical telecommunications to the Convention on International Civil Aviation** (Volume I: 5th edition, July 1996; Volume II: 6th edition, October 2001; Volume III: 1st edition, July 1995; Volume IV: 3rd edition, July 2002; Volume V: 2nd edition, July 2001 including all amendments up to No 79) as far as they are relevant for the provision of communication, navigation or surveillance services in the airspace concerned.

In the present case the Annex 10, volume III, part 1, Chapter four is the relevant technical referential (see § 4 of this report – [RD05]).

4. CATEGORY N°2: TECHNICAL REQUIREMENTS

The technical requirements described in this part constitutes the baseline applicable for the design and the performances of the NAVISAT Communication System. The compliance to these requirements needs to be demonstrated by the suppliers as well as by the operator (as far as they are concerned). The associated documentation will constitute the technical evidences usable for certification argumentation if it is requested by ANSPs or Authority.

The technical requirements proposed have the following origin:

- ICAO standards. Annex 10 on the convention of Civil aviation [RD05]
- Aeronautical Mobile Satellite (Route) services – Notice to user [RD06]
- Safety related requirements

4.1 ICAO Annex 10 related to Technical requirements for AMS(R)S

The technical requirements applicable to NAVISAT System are presented in the ICAO Standard and recommended Practices (SARPS) and more particularly in the Annex 10 to the convention on International Civil Aviation, Volume III, Part I, Chapter 4.

We can here confirm that this part of annex 10 of the ICAO standard is called by the European regulation 2096/2005 (annex 5) as the technical standard to apply to the design of such communication system.

As this document is considered as a direct “applicable document”, and is not too heavy, the requirements are directly put in annex of this baseline.

Compliance demonstration to these ICAO requirements is of course part of the System Qualification document and part of the certification documentation support.

4.2 Manual for Aeronautical Mobile satellite (Route) Service

This manual is to be considered in conjunction with ICAO Standards and Recommended Practices (SARPs) as contained in Annex 10, Volume III, Part I, Chapter 4. This manual provides implementation guidance for specific satellite systems operating in the AMS(R)S.

This document is today a draft but needs also to be considered as a technical requirement baseline called by the regulation compliance demonstration.

This document [RD06] is considered as an applicable document and is not copied in this report.

4.3 Safety Technical Requirements for design & Operation

4.3.1 System Safety objective assumption

The System designed and operated by NAVISAT aims at delivering Communication/Navigation information to End users (aircrafts). This information is delivered either "directly" or "indirectly" by NAVISAT to the Aircrafts pilots. This depends on NAVISAT mission in the value chain.

This means that such information, used together with the other pilots means, might contribute to the safety of the aircraft flights (Aircraft separation).

The assumption is done in this study that this safety related contribution exists. This means that design and operation constraints need to be specified and implemented in the NAVISAT System design.

These constraints are defined in the following paragraph.

4.3.2 System Safety related feared events and severity scheme

The aim of the system is to deliver Navigation/Communication information aiming at ensuring the separation of the aircrafts or providing them with clearance for some operation.

The associated feared events usually defined for such system and usable for NAVISAT system could be the following ones:

- Loss of message integrity
- Loss of message/transaction continuity
- Unavailability of the communication links (for one aircraft or for all the aircrafts)

They are then classified into a severity scheme in order to be able to define the design/operational constraints associated to the function leading to such feared events.

Sev.	Severity	NAVISAT Feared Event	Potential Consequence at Aircraft level – (Transcription of ESARR 4)
1	Catastrophic	-	- One or more Catastrophic Accidents
2	Hazardous	Loss of integrity [TBC]	- Large reduction in separation (e.g., a separation of less than half the separation minima), without crew or ATC fully controlling the situation or able to recover from the situation. - One or more aircraft deviating from their intended clearance, so that abrupt manoeuvre is required to avoid collision with another aircraft or with terrain (or when an avoidance action would be appropriate).
3	Major	Loss of continuity for Service provision [TBC] Service provision unavailability [TBC]	- Large reduction (e.g., a separation of less than half the separation minima) in separation with crew or ATC controlling the situation and able to recover from the situation. - Minor reduction (e.g., a separation of more than half the separation minima) in separation without crew or ATC fully controlling the situation, hence jeopardising the ability to recover from the situation (without the use of collision or terrain avoidance manoeuvres).
4	Minor	Single User unavailability [TBC] Single user loss of continuity [TBC]	- Increasing workload of the air traffic controller or aircraft flight crew, or slightly degrading the functional capability of the enabling CNS system. - Minor reduction (e.g., a separation of more than half the separation minima) in separation with crew or ATC controlling the situation and fully able to recover from the situation.
5	Negligible		- No Hazardous conditions

Table 1 : Feared event classification

4.3.3 Technical safety requirements

The following list of requirements is proposed to give Guideline for the NAVISAT System design wrt the potential hazardous situations that could occur and based on the severity scheme defined previously.

Regulation

[Xxx]: The System design shall be compliant with the safety regulations both for:

- Navigation/Communication domain (See § 1.3)
- Personal safety domain

Severity classification:

[Xxx]: As a part of hazard evaluation, hazards shall be classified according to the following consequence severity categories:

- I Catastrophic
- II. Hazardous
- III. Major
- IV. Minor
- V. Negligible

[Xxx]: Segments hazardous events shall be specified within the Segment requirements, together with:

- the assigned consequence severity
- the required probability of occurrence

Consequence Severity:

[Xxx]: See Table 1

Required probability of occurrence

[Xxx]: The probability that the NAVISAT system causes a “Loss of Integrity” shall be less than YYY (TBC)

[Xxx]: The probability that the NAVISAT system causes a “Loss of continuity for the Navigation//communication Service provision” shall be less than XXX (TBC)

[Xxx]: Availability of the NAVISAT Navigation/Communication Service provision for all user in visibility the shall be better than XXX (TBC)

[Xxx]: Availability of the NAVISAT Navigation/Communication Service of a single user the shall be better than XXX (TBC)

Failure tolerance:

[Xxx]: No single failure or operator error shall have a critical or catastrophic consequence.

[Xxx]: No combination of: two failures or two operator errors or one failure and one operator error shall have catastrophic consequences.

[Xxx]: No single operator error shall have major consequences

[Xxx]: Multiple failures which result from common cause or common mode failure mechanisms shall be identified and shall be considered as single failures for the purpose of determining failure tolerance.

[Xxx]: The design shall comply with the failure tolerance requirements during operations and maintenance.

Redundancy separation

[Xxx]: Safety critical redundant subsystems shall be physically and functionally separated, or protected in such a way that any event which causes the loss of one path shall not result in the loss of alternative, or redundant path.

Safe without service:

[Xxx]: When the safe operation of the System depends on externally provided services (e.g. power, external data/files), the design shall be such that critical or catastrophic consequences are not induced (for a period of time to be mutually agreed between ESA and the Contractor) after the loss or upon the sudden restoration of those services.

[Xxx]: The Ground Segment and its parts shall be designed in a such way that failures bring the Segment into a state that does not lead to critical or catastrophic consequences.

Control of hazardous Functions

[XXX] Ground Segment functions that, if lost or degraded or that, through incorrect or inadvertent operation, would result in a catastrophic or critical hazardous consequence, shall be identified as safety critical functions.

[XXX] For safety critical functions the system shall include:

- Real time failure detection
- Announcement of loss of operational redundancy
- Notification of redundancy switch-over
- Change of inhibit status

Software DAL allocation:

[Xxx]: The results of Safety analysis done at System, Segment or lower level shall enable the specification of safety requirement for safety related Software as well as the SW DAL allocation according to the dedicated process.

[Xxx]: The SW DAL assignment shall follow the following rules:

- Level A: Software whose anomalous behaviour would cause or contribute to a failure resulting in a Catastrophic event.
- Level B: Software whose anomalous behaviour would cause or contribute to a failure resulting in a Hazardous event.
- Level C: Software whose anomalous behaviour would cause or contribute to a failure resulting in a Major event.
- Level D: Software whose anomalous behaviour would cause or contribute to a failure resulting in a Minor event.
- Level E: Software whose anomalous behaviour would cause or contribute to a failure resulting in a Negligible event.

Architecture requirements:

[Xxx]: The System architecture and design shall be such that service performance does not degrade during maintenance of one of its elements.

Operational requirements:

[Xxx]: The System shall support handovers within the System or with external Systems in a seamless manner without service interruption or performance reduction.

[Xxx]: In case of redundant satellites, switch from nominal to redundant satellite shall be seamless and shall not lead to performance reduction.

[Xxx]: The System shall operate in all weather conditions

[Xxx]: The System shall have a maximum outage time of TBD sec.

[Xxx]: The System shall have a maximum time to restore of TBD sec.

[Xxx]: The System shall be designed to allow preventive and corrective maintenance over 30 years without any degradation of service performance.

Maintenance design

[Xxx]: The System shall be designed to allow preventive and corrective maintenance over 30 years without any degradation of service performance.

[Xxx]: The System Maintenance and upgrade activities/processes shall be designed to eliminate or minimise the potential for hazardous events occurring in the user domain resulting from human error during the maintenance/repair procedure(s).

Communication Standard:

[Xxx]: The satellite communication standard shall support operational safety requirements in order to ensure the specified:

- Data integrity

- Continuity of operation
- Availability of service

Network requirements:
[Xxx]: A partial or complete failure of the Network shall not prevent the continued operation of the system

[Xxx]: A partial or complete failure of the Network shall not reduce the availability of the service

Space Segment

[Xxx]: The Space Segment design shall be such that the service remains available with the specified performance during Space Segment orbit maintenance manoeuvres

5. CATEGORY N°3: DEPENDABILITY AND SAFETY REQUIREMENTS RELATED TO PROCESS AND ANALYSIS

The following requirements are proposed to give a frame for the Dependability and Safety assessment process. It relies on the regulation framework described in section 3

Dependability programme:

[XXX] The Contractor shall assign a Dependability manager who shall be a member of the project Product Assurance organization.

[XXX] The Dependability program shall envisage the following activities:

- The issue of several Dependability analyses according to Statement Of Work.
- The collaboration with the Engineering Department on the following issues:
    - Segment performance requirements allocation into Dependability related requirements for Segment sub-assemblies
    - Assessment of Dependability qualitative/quantitative requirements and identification of suitable barriers for risk mitigation
    - Validation, through iterative process, of Dependability related requirements for Segment sub-assemblies
    - Verification of Ground Segment performance requirements
    - Review of Program Plans, Test Plans, Drawings, Layouts, Technical Specifications, to ensure compliance to the relevant applicable Dependability requirements, and to verify the implementation of any change that has been required by the Dependability analyses
    - Definition of Contingency and Operation Requirements (at Subsystem/Segment level) to ensure that Operators are able to diagnose and successfully react to the fault conditions resulting as failures or unacceptable degradations of Segment performances.

[XXX] Dependability analyses shall be implemented, providing a timely feedback to the design engineers, in order to:

- Ensure that Dependability targets, specified in the Segment Technical Specifications, are met.

- Identify all potential failure modes and technical risks with respect to functional needs which can lead to no achievement of Dependability targets, provide risk assessment and risk reduction and control measures in line with the risk management process implemented on the project.
- cover all lifecycle phases: design, operations and maintenance

[XXX] All proposed design changes shall be evaluated and considered against Dependability aspects, in particular no new potential Dependability Critical Item shall be introduced by the implementation of a proposed design change.

[XXX] The Dependability manager shall maintain a tracking list of all Dependability-related non conformances and waivers reviewed and shall submit them to Prime/Customer.

[XXX] The Dependability manager shall attend those reviews/meetings concerned with Dependability critical functions and items.

[XXX] The Dependability documentation shall be provided at each main step in the Program development (according to SOW).

[XXX] The results of the Dependability Analyses shall be incorporated into the Design and Performance Justification documents.

FMECA

[XXX] A systematic analysis of Equipment/Assembly/Subsystem/Segment failure modes and effects leading to the assessment of their criticality to mission success (ref. section 0) shall be carried out and documented.

[XXX] The FMECA shall be performed on both functional and physical design. Initially, it shall be performed at the level of functions; as the design evolves, the FMECA shall be repeated, updated and refined to reflect the increased design maturity.

FTA

[XXX] The FTA shall be used to verify that the design complies with the failure tolerance requirements for combinations of failures.

Common Cause analysis

[XXX] Common Mode and Common Cause Analyses shall be performed on reliability and safety critical

items to identify the root cause of failures that have the potential to negate failure tolerance levels.

SW DAL Allocation

[XXX] SW components Development Assurance Levels (DALs) determination shall be performed by all Ground Segment levels of responsibility: Ground Segment, subsystem/Assembly/Equipment (in generic terms these are called “upper level”) and component.

Maintainability analysis

[XXX] The object of the Maintainability shall be to ensure that the Equipment / Assembly / Subsystem /Segment design shall meet the maintainability requirements and allow maintenance at all levels with a minimum of resources.

Availability analysis

[XXX] The object of the Availability is to ensure that the Equipment / Assembly / Subsystem / Segment design shall meet the availability requirements during the defined operating period and in the specified environmental conditions, integrating reliability and maintainability results.

[XXX] The results of the Availability shall be used to:

- Optimise the design, operations and maintenance
- Provide inputs to verify the cost of operation.

[XXX] The results of all the following availability analyses, shall be used to identify critical items risking mission success. All these items shall be listed in the PA Critical Items List (CIL).

Safety Programme:

[XXX] the contractor shall assign a Safety manager who will be member of the project assurance organization.

[XXX] The Safety manager shall have sufficient organizational authority and independence to ensure that the safety programme is properly implemented

[XXX] the safety manager shall assure the implementation of the safety programme in close cooperation with Design engineering and other disciplines (Dependability, SW PA, Integration and verification team, etc.

Safety activities

[XXX] The safety manager shall be responsible for assuring that the design and the operations of System/Segments comply with the applicable safety requirements, with any additional safety requirements coming from previous projects lessons learned and from the safety analyses performed during the project.

[XXX] The Safety manager shall provide and maintain a Safety and Dependability plan in close cooperation with the Dependability manager.

[XXX] The Safety & Dependability plan shall describe methods, tools, approach and organization for safety activities for the different project milestones in relation with the development plan. The plan shall also specify the relation of safety analyses and activities with the engineering activities.

[XXX] The Safety & Dependability plan shall be updated at each main milestone.

[XXX] The Equipment/Assembly/Subsystem/Segment safety manager shall prepare and submit to the higher level of responsibility the safety analyses done in the frame of the safety programme, in accordance with the Statement of Work agreements.

[XXX] The Safety program shall envisage the following activities:

a) the issue of several Safety analyses according to Statement Of Work

b) the collaboration with the Engineering Department on the following issues:

- System/Segments performance requirements allocation into Safety related requirements for Segment sub-assemblies
- Assessment of Safety qualitative/quantitative requirements and identification of suitable barriers for risk mitigation
- Validation, through iterative process, of Safety related requirements for Segment sub-assemblies
- Verification of System performance requirements
- Review of plans, technical specifications, operation and test procedures to ensure that:

  o compliance with the applicable safety requirements is met

  o safety provisions are incorporated into design, manufacturing and in order to meet the applicable safety requirements, safety verification activities are performed in order to demonstrate compliance with such requirements.

  o changes which may be necessary as a result of safety analyses and safety recommendations are adequately implemented
- review and approval of hazardous and safety critical operational procedures
- definition of FDIR, Contingency and Operation Requirements (at Subsystem / Segment level) to ensure that Operators are able to diagnose and successfully react to the fault conditions resulting as failures or unacceptable degradations of the Ground Segment performances.

c) the management of safety risks by performing the following activities: allocation of safety requirements, hazard identification, hazard evaluation, hazard prevention, reduction and control, hazard close-out including residual risk acceptance. The output of the risk management process shall provide inputs to the project reviews.

[XXX] The Safety Program shall envisage the development of a Safety Assurance File, consisting of a report and associated database, to present the results of safety activities undertaken in accordance with the NAVISAT Safety program.

The report shall provide the justifications of the baseline architecture from the viewpoint of safety of the end user, addressing the system level hazards as defined in the safety requirements.

[XXX] All proposed design changes shall be evaluated and considered against safety aspects. In particular no new potential hazards shall be introduced by the implementation of a proposed design change.

[XXX] The safety manager shall review all non-conformances and waivers to determine their effect on the applicable project safety requirements or safety-critical functions and items.

[XXX] The safety manager shall maintain a tracking list of all safety-related non-conformances, failures, deviations, waivers, accident or incident reports that shall be formally accepted and closed, through submittal to Authority.

[XXX] The safety manager shall be present at those reviews/meetings concerned with safety-critical functions, procedures and items.

Safety Analysis

[XXX] The contractor shall prepare or update the relevant Safety analyses.

[XXX] The primary objectives of the safety analyses process is to ensure that the applicable Safety Requirements are met and to obtain concurrence with the safety assurance process conducted by the relevant safety authority. Safety analyses shall cover all lifecycle phases: design, operations and maintenance

[XXX] The contractor shall perform a functional analysis at segment level. As a result of this functional analysis the contractor shall identify safety requirements and transfer them into the technical specifications.

[XXX] The contractor shall perform probabilistic safety risk assessments at segment level in order to demonstrate that the design meet the quantitative safety performances.

[XXX] The safety analyses are based on the results obtained from the following supporting analyses:

- Functional Analysis
- Hazard Analysis (HA)
- Failure Mode, Effects and Criticality Analysis (FMECA)
- Common Cause and Common Mode Failure Analysis (CCCMA)
- Fault Tree Analysis (FTA)
- Reliability, Availability and Maintainability (RAM) Analysis
- Contingency Analysis
- Outage Analysis
- Human Dependability Analysis

[XXX] The results of safety analyses at segment or lower level shall enable the specification of safety requirements for safety critical software.

[XXX] The contractor shall establish a safety verification status logbook to ensure that:

- the safety requirements are verified;
- the corresponding procedures are validated;
- the safety verification reports are analysed;
- the tests results are validated;
- the verified items configuration is representative and under control;
- the safety critical functions are validated by end to end testing;
- all open verifications are monitored.

[XXX] The contractor shall establish and maintain a Safety and Dependability Recommendations status logbook to monitor and track all safety and dependability related recommendations. This logbook shall be controlled by the Safety manager

[XXX] To allow the safety manager to fulfil this job, the Contractors of safety-critical equipment shall supply him with safety analyses at equipment level to demonstrate that their project is safety addressed, controlled and achieved.

Safety documentation

[XXX] The safety documentation shall be provided at each main step in the program development.

- Safety and Dependability analysis relevant for the milestones
- Safety Assurance File
- Dependability and Safety Recommendation Status Log

[XXX] The safety documentation shall support the safety review process according to the relevant safety authority.

ANNEX

ICAO Annex 10 Volume 3 Part 1

CHAPTER 4. AERONAUTICAL MOBILE-SATELLITE (ROUTE) SERVICE (AMS(R)S)

Note 1.— This chapter contains Standards and Recommended Practices applicable to the use of Aeronautical Mobile-Satellite (R) Service communications technologies. The Standards and Recommended Practices in this chapter are service and performance-oriented and are not tied to a specific technology or technique.

Note 2.— Detailed Technical Specifications of AMS(R)S Systems are contained in the manual on AMS(R)S. This document also provides a detailed description of the AMS(R)S, including details on the Standards and Recommended Practices below.

4.1 DEFINITIONS

Connection establishment delay. Connection establishment delay, as defined in ISO 8348, includes a component, attributable to the called subnetwork (SN) service user, which is the time between the SN-CONNECT indication and the SN-CONNECT response. This user component is due to actions outside the boundaries of the satellite subnetwork and is therefore excluded from the AMS(R)S specifications.

Data transfer delay (95th percentile). The 95th percentile of the statistical distribution of delays for which transit delay is the average.

Data transit delay. In accordance with ISO 8348, the average value of the statistical distribution of data delays. This delay represents the subnetwork delay and does not include the connection establishment delay.

Network (N). The word "network" and its abbreviation "N" in ISO 8348 are replaced by the word "subnetwork" and its abbreviation "SN", respectively, wherever they appear in relation to the subnetwork layer packet data performance.

Residual error rate. The ratio of incorrect, lost and duplicate subnetwork service data units (SNSDUs) to the total number of SNSDUs that were sent.

Spot beam. Satellite antenna directivity whose main lobe encompasses significantly less than the earth's surface that is within line-of-sight view of the satellite. May be designed so as to improve system resource efficiency with respect to geographical distribution of user earth stations.

Subnetwork (SN). See ***Network (N).***

Subnetwork service data unit (SNSDU). An amount of subnetwork user data, the identity of which is preserved from one end of a subnetwork connection to the other.

Total voice transfer delay. The elapsed time commencing at the instant that speech is presented to the AES or GES and concluding at the instant that the speech enters the interconnecting network of the counterpart GES or AES. This delay includes vocoder processing time, physical layer delay, RF propagation delay and any other delays within an AMS(R)S subnetwork.

Note.— The following terms used in this chapter are defined in Annex 10 as follows:

• *Aeronautical telecommunication network (ATN): Volume III, Chapter 1.*

• *Aeronautical mobile-satellite (route) service (AMS(R)S): Volume II, Chapter 1.1.*

• *Aircraft earth station (AES): Volume III, Chapter 1.*

• *Ground earth station (GES): Volume III, Chapter 1.*

• *Subnetwork layer: Volume III, Chapter 6.1.*

4.2 GENERAL

4.2.1 Any mobile-satellite system intended to provide AMS(R)S shall conform to the requirements of this chapter.

4.2.1.1 An AMS(R)S system shall support packet data service, or voice service, or both.

4.2.2 Requirements for mandatory carriage of AMS(R)S system equipment including the level of system capability shall be made on the basis of regional air navigation agreements which specify the airspace of operation and the implementation timescales for the carriage of equipment. A level of system capability shall include the performance of the AES, the satellite and the GES.

4.2.3 The agreements indicated in 4.2.2 shall provide at least two years' notice of mandatory carriage of airborne systems.

4.2.4 **Recommendation.—** *Civil aviation authorities should coordinate with national authorities and service providers those implementation aspects of an AMS(R)S system that will permit its worldwide interoperability and optimum use, as appropriate.*

4.3 RF CHARACTERISTICS

4.3.1 Frequency bands

Note.— ITU Radio Regulations permit systems providing mobile-satellite service to use the same spectrum as AMS(R)S without requiring such systems to offer safety services. This situation has the potential to reduce the spectrum available for AMS(R)S. It is critical that States consider this issue in frequency planning and in the establishment of national or regional spectrum requirements.

4.3.1.1 When providing AMS(R)S communications, an AMS(R)S system shall operate only in frequency bands which are appropriately allocated to AMS(R)S and protected by the ITU Radio Regulations.

4.3.2 Emissions

4.3.2.1 The total emissions of the AES necessary to meet designed system performance shall be controlled to avoid harmful interference to other systems necessary to support safety and regularity of air navigation, installed on the same or other aircraft.

Note 1.— Harmful interference can result from radiated and/or conducted emissions that include harmonics, discrete spurious, intermodulation product and noise emissions, and are not necessarily limited to the "transmitter on" state.

Note 2.— Protection requirements for GNSS are contained in Annex 10, Volume I.

4.3.2.2 INTERFERENCE TO OTHER AMS(R)S EQUIPMENT

4.3.2.2.1 Emissions from an AMS(R)S system AES shall not cause harmful interference to an AES providing AMS(R)S on a different aircraft.

Note.— One method of complying with 4.3.2.2.1 is by limiting emissions in the operating band of other AMS(R)S equipment to a level consistent with the intersystem interference requirements such as contained in RTCA document DO-215.

RTCA and EUROCAE may establish new performance standards for future AMS(R)S which may describe methods of compliance with this requirement.

4.3.3 Susceptibility

4.3.3.1 The AES equipment shall operate properly in an interference environment causing a cumulative relative change in its receiver noise temperature ($\Delta T/T$) of 25 per cent.

4.4 PRIORITY AND PRE-EMPTIVE ACCESS

4.4.1 Every aircraft earth station and ground earth station shall be designed to ensure that messages transmitted in accordance with Annex 10, Volume II, 5.1.8, including their order of priority, are not delayed by the transmission and/or reception of other types of messages. If necessary, as a means to comply with the above requirement, message types not defined in Annex 10, Volume II, 5.1.8 shall be terminated even without warning, to allow Annex 10, Volume II, 5.1.8 type messages to be transmitted and received.

4.4.2 All AMS(R)S data packets and all AMS(R)S voice calls shall be identified as to their associated priority.

4.4.3 Within the same message category, the system shall provide voice communications priority over data communications.

4.5 SIGNAL ACQUISITION AND TRACKING

4.5.1 The AES, GES and satellites shall properly acquire and track service link signals when the aircraft is moving at aground speed of up to 1 500 km/h (800 knots) along any heading.

4.5.1.1 **Recommendation.—** *The AES, GES and satellites should properly acquire and track service link signals when the aircraft is moving at a ground speed of up to 2 800 km/h (1 500 knots) along any heading.*

4.5.2 The AES, GES and satellites shall properly acquire and track service link signals when the component of the aircraft acceleration vector in the plane of the satellite orbit is up to 0.6 g.

4.5.2.1 **Recommendation.—** *The AES, GES and satellites should properly acquire and track service link signals when the component of the aircraft acceleration vector in the plane of the satellite orbit is up to 1.2 g.*

4.6 PERFORMANCE REQUIREMENTS

4.6.1 Designated operational coverage

4.6.1.1 An AMS(R)S system shall provide AMS(R)S throughout its designated operational coverage (DOC).

4.6.2 Failure notification

4.6.2.1 In the event of a service failure, an AMS(R)S system shall provide timely predictions of the time, location and duration of any resultant outages until full service is restored.

Note.— Service outages may, for example, be caused by the failure of a satellite, satellite spot beam, or GES. The geographic areas affected by such outages may be a function of the satellite orbit and system design, and may vary with time.

4.6.2.2 The system shall annunciate a loss of communications capability within 30 seconds of the time when it detects such a loss.

4.6.3 AES requirements

4.6.3.1 The AES shall meet the relevant performance requirements contained in 4.6.4 and 4.6.5 for aircraft in straight and level flight throughout the designated operational coverage of the satellite system.

4.6.3.1.1 **Recommendation.—** *The AES should meet the relevant performance requirements contained in 4.6.4 and 4.6.5 for aircraft attitudes of +20/-5 degrees of pitch and +/-25 degrees of roll throughout the DOC of the satellite system.*

4.6.4 Packet data service performance

4.6.4.1 If the system provides AMS(R)S packet data service, it shall meet the standards of the following subparagraphs.

Note.— System performance standards for packet data service may also be found in RTCA Document DO-270.

4.6.4.1.1 An AMS(R)S system providing a packet data service shall be capable of operating as a constituent mobile subnetwork of the ATN.

Note.— In addition, an AMS(R)S may provide non-ATN data functions.

4.6.4.1.2 *DELAY PARAMETERS*

Note.— The term "highest priority service" denotes the priority which is reserved for distress, urgency and certain infrequent network system management messages. The term "lowest priority service" denotes the priority used for regularity of flight messages. All delay parameters are under peak-hour traffic loading conditions.

4.6.4.1.2.1 *Connection establishment delay*. Connection establishment delay shall not be greater than 70 seconds.

4.6.4.1.2.1.1 **Recommendation.—** *Connection establishment delay should not be greater than 50 seconds.*

4.6.4.1.2.2 In accordance with ISO 8348, data transit delay values shall be based on a fixed subnetwork service data unit (SNSDU) length of 128 octets. Data transit delays shall be defined as average values.

4.6.4.1.2.3 *Data transit delay, from-aircraft, highest priority*. From-aircraft data transit delay shall not be greater than 40 seconds for the highest priority data service.

4.6.4.1.2.3.1 **Recommendation.—** *Data transit delay, from-aircraft, highest priority. From-aircraft data transit delay should not be greater than 23 seconds for the highest priority data service.*

4.6.4.1.2.3.2 **Recommendation.—** *Data transit delay, from-aircraft, lowest priority. From-aircraft data transit delay should not be greater than 28 seconds for the lowest priority data service.*

4.6.4.1.2.4 *Data transit delay, to-aircraft, highest priority*. To-aircraft data transit delay shall not be greater than 12 seconds for the highest priority data service.

4.6.4.1.2.4.1 **Recommendation.**— *Data transit delay, to-aircraft, lowest priority. To-aircraft data transit delay should not be greater than 28 seconds for the lowest priority data service.*

4.6.4.1.2.5 *Data transfer delay (95th percentile), from-aircraft, highest priority*. From-aircraft data transfer delay (95th percentile), shall not be greater than 80 seconds for the highest priority data service.

4.6.4.1.2.5.1 **Recommendation.**— *Data transfer delay (95th percentile), from-aircraft, highest priority. From-aircraft data transfer delay (95th percentile), should not be greater than 40 seconds for the highest priority data service.*

4.6.4.1.2.5.2 **Recommendation.**— *Data transfer delay (95th percentile), from-aircraft, lowest priority. From-aircraft data transfer delay (95th percentile), should not be greater than 60 seconds for the lowest priority data service.*

4.6.4.1.2.6 *Data transfer delay (95th percentile), to-aircraft, highest priority*. To-aircraft data transfer delay (95th percentile), shall not be greater than 15 seconds for the highest priority data service.

4.6.4.1.2.6.1 **Recommendation.**— *Data transfer delay (95th percentile), to-aircraft, lowest priority. To-aircraft data transfer delay (95th percentile), should not be greater than 30 seconds for the lowest priority data service.*

4.6.4.1.2.7 *Connection release delay (95th percentile).* The connection release delay (95th percentile) shall not be greater than 30 seconds in either direction.

4.6.4.1.2.7.1 **Recommendation.**— *The connection release delay (95th percentile) should not be greater than 25 seconds in either direction.*

4.6.4.1.3 *INTEGRITY*

4.6.4.1.3.1 *Residual error rate, from-aircraft*. The residual error rate in the from-aircraft direction shall not be greater than 10-4 per SNSDU.

4.6.4.1.3.1.1 **Recommendation.**— *The residual error rate in the from-aircraft direction should not be greater than 10-6 per SNSDU.*

4.6.4.1.3.2 *Residual error rate, to-aircraft*. The residual error rate in the to-aircraft direction shall not be greater than 10-6 per SNSDU.

4.6.4.1.3.3 *Connection resilience*. The probability of a subnetwork connection (SNC) provider-invoked SNC release shall not be greater than 10-4 over any one-hour interval.

Note.— Connection releases resulting from GES-to-GES handover, AES log-off or virtual circuit pre-emption are excluded from this specification.

4.6.4.1.3.4 The probability of an SNC provider-invoked reset shall not be greater than 10-1 over any one-hour interval.

4.6.5 Voice service performance

4.6.5.1 If the system provides AMS(R)S voice service, it shall meet the requirements of the following subparagraphs.

Note.— ICAO is currently considering these provisions in the light of the introduction of new technologies.

4.6.5.1.1 *CALL PROCESSING DELAY*

4.6.5.1.1.1 *AES origination.* The 95th percentile of the time delay for a GES to present a call origination event to the terrestrial network interworking interface after a call origination event has arrived at the AES interface shall not be greater than 20 seconds.

4.6.5.1.1.2 *GES origination.* The 95th percentile of the time delay for an AES to present a call origination event at its aircraft interface after a call origination event has arrived at the terrestrial network interworking interface shall not be greater than 20 seconds.

4.6.5.1.2 *VOICE QUALITY*

4.6.5.1.2.1 The voice transmission shall provide overall intelligibility performance suitable for the intended operational and ambient noise environment.

4.6.5.1.2.2 The total allowable transfer delay within an AMS(R)S subnetwork shall not be greater than 0.485 seconds.

4.6.5.1.2.3 **Recommendation.—** *Due account should be taken of the effects of tandem vocoders and/or other analog/digital conversions.*

4.6.5.1.3 *VOICE CAPACITY*

4.6.5.1.3.1 The system shall have sufficient available voice traffic channel resources such that an AES- or GESoriginated AMS(R)S voice call presented to the system shall experience a probability of blockage of no more than 10-2.

Note.— Available voice traffic channel resources include all pre-emptable resources, including those in use by non- AMS(R)S communications.

4.6.6 Security

4.6.6.1 The system shall provide features for the protection of messages in transit from tampering.

4.6.6.2 The system shall provide features for protection against denial of service, degraded performance characteristics, or reduction of system capacity when subjected to external attacks.

Note.— Possible methods of such attack include intentional flooding with spurious messages, intentional corruption of system software or databases, or physical destruction of the support infrastructure.

4.6.6.3 The system shall provide features for protection against unauthorized entry.

Note.— These features are intended to provide protection against spoofing and "phantom controllers".

4.7 SYSTEM INTERFACES

4.7.1 An AMS(R)S system shall allow subnetwork users to address AMS(R)S communications to specific aircraft by means of the ICAO 24-bit aircraft address.

Note.— Provisions on the allocation and assignment of ICAO 24-bit addresses are contained in the Appendix to Chapter 9.

4.7.2 Packet data service interfaces

4.7.2.1 If the system provides AMS(R)S packet data service, it shall provide an interface to the ATN.

Note.— The detailed technical specifications related to provisions of the ATN-compliant subnetwork service are contained in Section 5.2.5 and Section 5.7.2 of Doc 9880 — Manual on Detailed Technical Specifications for the Aeronautical Telecommunication Network (ATN) *(in preparation).*

4.7.2.2 If the system provides AMS(R)S packet data service, it shall provide a connectivity notification (CN) function.

END OF DOCUMENT