International Civil Aviation Organization

THE NINTH MEETING OF AUTOMATIC DEPENDENT SURVEILLANCE – BROADCAST (ADS-B) STUDY AND IMPLEMENTATION TASK FORCE (ADS-B SITF/9)

Jakarta, Indonesia, 18 -19 August 2010

Agenda Item 4: **Review the Terms of Reference and Subject/Task Lists**
Task No 14: Guidance Material on building a safety case for delivery of separation services

GUIDANCE MATERIAL ON PREPARATION OF A SAFETY CASE FOR DELIVERY OF SEPARATION SERVICES

(Presented by Australia)

SUMMARY

Task No 14 requires Australia to prepare draft guidance material on building a Safety Case for delivery of separation services.

The Attachment to this WP is a Draft for consideration by the ADS-B SITF/9 Meeting.
The Draft document makes reference to and takes extracts from two highly relevant existing ICAO documents, as well as some other guidance material derived from a previously prepared Safety Case covering an ADS-B separation service in Australia.

1. INTRODUCTION

1.1 ADS-B SITF Task No 14 is for the preparation of guidance material on the building of a Safety Case for the delivery of ADS-B based separation services. This WP and its DRAFT attachment titled '**Guidance Material on Building a Safety Case for Delivery of a Separation Service'** are provided for consideration by the ADS-B SITF.

1.2 **What is a Safety Case:** A Safety Case is a documented record of the steps and processes taken and followed by the change proponent to ensure the change has been designed and implemented and operated as safely as reasonably practicable. A basic component of the Safety Case is a structured, comprehensive statement of the hazards, their operational consequences, their safety risks and the means of control of the risks, surrounding the provision of an operational service. The basic steps in the preparation of a Safety Case are:

a) The definition of the system, its operational purpose, its boundaries and its interfaces;

b) The identification of the possible hazards in the operation of the system, as well as the operational consequences of the occurrence of each hazard;

c) The assessment of the risk to the safety of persons and property of the operational consequences of the hazards. Each risk is assessed in terms of the likelihood of occurrence and the potential severity of the impact on safety;

d) The categorization of the tolerability of each risk based on a standard risk classification scheme; and

e) The means to manage or control each risk that is assessed as intolerable or requiring mitigation.

1.3 For ADS-B surveillance, the systemic hazards and the safety risks and the means of their control have generally been identified at forums such as ADS-B SITF. More particularly, in the opinion of Australia, three documents that have already been prepared and formally published by ICAO and by RTCA/Eurocae provide comprehensive guidance material for the purpose. These documents are referenced and summarized in the Draft attached.

1.4 The Draft also includes guidance material on structuring the contents of a Safety Case for an ADS-B enroute service. That material has not generally been covered in the ICAO documentation. The information has been extracted from a Safety Case prepared in Australia for the approval of the ADS-B Upper Airspace Program in that State.

2. GENERIC GUIDANCE MATERIAL

2.1 **ICAO Doc 9859 AN/474 'Safety Management Manual (SMM)' Second Edition 2009** provides States with guidance to develop material for service providers to implement a Safety Management System (SMS). The SMM follows a building block approach. It presents basic safety concepts in Chapter 2. Chapter 3 introduces the basics of safety management in aviation. Chapters 4 and 5 are highly relevant to Safety Case preparation in that they introduce the framework underlying safety risk assessment and management and explain the two basic concepts – safety hazards and safety risks. These two Chapters provide generic guidance for preparation of any aviation Safety Case. The remaining Chapters 6 through 11 are mainly relevant to the implementation of an SMS and therefore are not of specific relevance in the preparation of a Safety Case.

2.2 **CASA CAAP:** The Civil Aviation Safety Authority Australia has previously produced a Civil Aviation Advisory Publication (CAAP) on the topic of Safety Case preparation. It also provides generic guidance material. The CAAP is titled **'Guidelines for the Preparation of Safety Cases covering Airways Systems'**. It can be accessed on the CASA website at the following internet link: http://casa.gov.au/wcmswr/_assets/main/download/caaps/airways/airway_1.pdf

3. GUIDANCE MATERIAL SPECIFIC TO ADS-B SURVEILLANCE SERVICE

3.1 In May 2006, ICAO published (as draft material) Circular 311 that described the comparative assessment undertaken by the ICAO Separation and Airspace Safety Panel (SASP) on the use of ADS-B surveillance by the Air Traffic Services. That assessment concluded that ADS-B can be used to provide a five (5) nautical mile separation minimum, subject to certain conditions being satisfied. (Subsequently, the ICAO SASP has updated Circular 311 to include Multilateration (MLAT) based services that also can be used to provide ATS surveillance, subject to certain conditions. It also includes assessment of the use of ADS-B and MLAT for 3NM terminal area separation. At the time of preparation of this WP, ICAO had not published the updated Circular.)

3.2 Circular 311 provides the references and technical evidence to show that ADS-B is as good as or better than an MSSR when used for an enroute 5NM separation service by ATC. Subject to certain qualifications, it is therefore unnecessary to demonstrate that in a Safety Case covering a State

or local surveillance service. All that is necessary is for a State to simply make reference to that finding in Circular 311. However, it should be noted that the Circular clearly points out that the analysis by the SASP makes assumptions on airspace situations which may not be totally relevant to the airspace situation in any particular State, and that State and/or local level assessments should be undertaken where there is any difference between the Sate's conditions and those in the assumptions made in the Circular.

3.3 The further significant value of Circular 311 as guidance material for ADS-B Safety Case preparation is that it provides a Compendium of Hazards and Mitigation Measures which has been extracted from several site-specific ADS-B Safety Cases of ADS-B trials and implementation undertaken in two States. This Hazard Compendium will be of assistance to those States embarking on their own program, as guidance in specific HazId and risk mitigation for that separation service.

3.4 **Contents of the Safety Case**. The draft material in the Attachment also provides guidance on the **contents** (i.e. the topic headings, with a brief description of each topic that may be included under each heading) for inclusion in an ADS-B Design and Implementation Safety Case. This topic content listing has been derived by reference to the Safety Case for the ADS-B Upper Airspace Program (UAP) prepared in Australia by the ANSP. (That particular Safety Case was the basis of the regulatory approval by CASA of the now implemented ADS-B UAP of Airservices Australia.)

4. ACTION BY THE MEETING

4.1 The Meeting is invited to consider the draft reference material in the Attachment and decide whether it provides sufficient and satisfactory guidance for the preparation of ADS-B related Safety Cases. Any comments for improvement would be welcomed.

– – – – – – – – – – – –

INTERNATIONAL CIVIL AVIATION ORGANIZATION
ASIA AND PACIFIC OFFICE

DRAFT

GUIDANCE MATERIAL ON

BUILDING A SAFETY CASE FOR

DELIVERY OF AN ADS-B SEPARATION SERVICE

Version xx

June 2010

CONTENTS

GUIDANCE MATERIAL ON BUILDING A SAFETY CASE FOR DELIVERY OF AN ADS-B SEPARATION SERVICE

PRIMARY REFERENCES

This guidance material relies heavily on references to the following three reference documents. Much of the information needed for the preparation of a Design Safety Case for an ADS-B surveillance service can be derived from this documentation. The aspects that need to be separately covered by a proponent are those arising from any differences in the specific airspace for the surveillance system, and the system engineering of the surveillance services if they differ from the reference systems.

1. ICAO Doc 9859 AN/474 Safety Management Manual (SMM), Second Edition 2009 – in particular Chapter 4 'Hazards', and Chapter 5 'Safety Risks'

2. ICAO Circular 311 AN/177 'Assessment of ADS-B to Support Air Traffic services and Guidelines for Implementation, First Edition 2006'

3. RTCA DO-303/EUROCAE ED-126 December 13, 2006 'Safety, Performance and Interoperability Requirements Document for the Non-Radar Airspace Application'

INTRODUCTION

This document provides basic guidance on the building of a Safety Case for delivery of an ADS-B separation service. It relies on referencing existing guidance material in the two ICAO publications listed above, as well as some existing Safety Cases covering early ADS-B services.

A number of discrete 'steps' in the building of a Safety Case are described to progress to a completed document.

The first steps cover the generic requirements for the preparation of a Safety Case for any airways system, including any surveillance systems used for separation by ATC. The primary reference is Chapters 4 and 5 of ICAO Doc 9859.

The remaining steps cover the elements of a Safety Case specific to a new ADS-B surveillance service. The basic references are ICAO Circular 311 and RTCA DO-303/Eurocae ED-126. These documents contain a significant amount of information on hazard identification and risk assessment of an enroute ADS-B service in Non-Radar Airspace (NRA). The final steps are provided as guidance to the actual content headings of a Safety Case for an ADS-B service.

Definitions

Accuracy: A measure of the difference between the aircraft position reported by the surveillance system, as compared to the true position

ALARP: As Low as Reasonably Practicable (in risk mitigation)

Availability The probability that a system will be able to perform its intended function when required for use

Continuity The probability of a system to perform its required function without unscheduled interruption, assuming the system is available when the procedure is initiated (Circ 311)

Failure: Inability of the system to perform its intended service or function

Fault: Degradation in the performance of a system

Hazard: A condition or set of conditions of a system, or an object, with the potential to cause injury to personnel, damage to equipment or structures, loss of material, or reduction of ability to perform a prescribed function.

Hazard identification: The process of recognising that a hazard exists and defining its characteristics

Integrity: The ability of a system to provide timely warnings to users when the system should not be used for navigation (and, in the case of ADS-B for surveillance).

Maintainability: The ability of a system to be retained in, or restored to service

NRA: Non-Radar Airspace

Operational requirement: The stated purpose of the (surveillance) system

Reliability: The probability that, during a certain period of time, a system performs its prescribed functions (usually expressed in MTBF)

Risk: The probability of occurrence, together with the severity of the consequence(s), of a hazardous event

Risk assessment: The process of determining the risk involved in the occurrence of a hazardous event, and the tolerability of that risk

Risk management: The systematic application of management policies, procedures and practices to the tasks of identifying hazards and assessing and controlling risks

Safety: The state in which the possibility of harm to persons or of property damage is reduced to, and maintained at or below, an acceptable level through a continuing process of hazard identification and safety risk management. (Doc 9859)

Safety Case: A document which provides substantial evidence that the system to which it pertains meets its safety objectives

PART A: GENERIC GUIDANCE FOR SAFETY CASE PREPARATION

1 What is a Safety Case?

1.1 One of the primary purposes of a Safety Management System is to predict what accidents or incidents may occur, how they may happen, and how they may be prevented. The processes for safety assurance may differ in details; however they all prescribe the systematic undertaking of safety risk assessment and the presentation of evidence that the particular system is safe.

One way of presenting such evidence is by preparing a Safety Case. A Safety Case is an explicit documentation of a safety critical system, its corresponding safety objectives, and the associated safety risk assessment and risk management of the system, at appropriate milestones in the life of the system.

2 Generic contents of a Safety Case

2.1 A Safety Case is a documented record of the steps or processes undertaken by the system proponent to ensure that the system has been designed, tested and implemented as safely as reasonably practicable. Its basic component is a structured, comprehensive statement of the hazards and the corresponding safety risks of the occurrence of the hazards surrounding the provision of an operational service. This should include the significance of the hazards in terms of their likelihood of occurrence and potential effects on aviation safety, and the means whereby they are to be managed. The essential features of a Safety Case are that it should:

a) fully describe the surveillance system including the operational role and functions which it covers (i.e. the configuration and the boundaries of the system);
b) define or reference the performance standards and specifications of the system;
c) establish the safety objectives and the safety requirements for the system;
d) identify the hazards and the operational consequences of the hazards. Identification of hazards and consequences must ensure that all possible failure and fault modes have been identified under all normal and abnormal modes of operation;
e) assess the associated risks (in terms of frequency of occurrence and severity) of each identified operational consequence;
f) categorize each of the risks within a recognised risk tolerability classification scheme;
g) establish the controls necessary to ensure the risks are tolerable.

3 Safety planning

3.1 It is expected that safety will be built into any new surveillance system from its early inception and that the management of safety related activities will be undertaken in a planned manner over the lifecycle of the system.

3.2 The safety plan may be a discrete element of a project management plan, if applicable, or it may stand-alone. The Safety Plan is an important basic document that sets out the safety objectives and requirements and the actions and processes to be followed in the development of the system.

3.3 The safety plan should provide the basis for the development of the several parts of the Safety Case at defined milestones as the development, design and implementation of the surveillance system progresses to commissioning and normal day-to-day operation.

4 A Safety Case may have several discrete parts over the system lifecycle

4.1 ATC surveillance systems have a lifecycle consisting of several distinct phases. The safety hazards and associated risks may differ in type and degree in each phase, and their identification and control treatment will be more appropriately undertaken at a particular phase in the lifecycle. Accordingly, Safety Cases need to be developed to separately consider the safety situation in each of the lifecycle phases. This may require several parts of the Safety Case, with each part building on the previous part as the system is developed.

4.2 The distinct phases of a surveillance system's life which may be covered by a Safety Case, are normally:

a) **the operational requirements phase**, when the role and broad functionality of the new system is determined. This phase should identify the safety objectives of the system and its applicable system safety requirements, (these may be based on ICAO SARPS, the State's regulatory requirements, and the service provider's internal safety standards);

b) **the design and procurement phase**, when the system is designed and developed to meet the specified operational and/or engineering requirements. In this phase, the system configuration and operation is defined, incorporating the safety objectives and requirements within the evolving design. A full hazard and risk assessment is usually undertaken at this time;

c) **the implementation phase,** when the system is subject to procedural and/or engineering readiness testing against the design specifications, followed by operational trials, such as ghosting or mimicking. At this phase, the risk assessment is tested and validated by actual trials and testing of the installed system, and specific safety related operational, engineering and/or management procedures are developed to obviate or control the identified risks; and

d) **the routine operations phase,** when the safety of the system continues to be monitored and improved as any hazards are identified as they arise, and the risks are mitigated during actual operations.

4.3 The Safety Case should describe the historical and current safety status of the system or service as it develops throughout its entire lifecycle.

5 STEP 1 – State the purpose and scope of the safety case

5.1 The purpose and scope of the Safety Case should be clearly stated in its introductory paragraphs, and should include:

a) A statement of the purpose and role of the surveillance system under consideration, i.e. its Operational Requirement.

b) A description of the system and its location; its configuration including the sub-system

elements; the system boundaries; the elements of the system which have been considered within the scope of the document, i.e., whether it covers equipment, procedures, airspace, personnel, etc.; and the interfaces with other external systems.

c) A statement of the assumptions upon which the Safety Case is based. This should include the defined or known levels of safety, or integrity, of each of the interfacing or support systems/services, and those other services externally provided by third parties, such as those provided by telecommunications service providers, electrical power service providers, etc.

5.2 The relevant lifecycle phase of the system, covered by the particular part/s of the Safety Case should also be defined.

6 STEP 2 – Develop and document the safety objectives and system safety requirements

6.1 The overall safety objectives and related system safety and safety related performance requirements supporting the objectives for the system should be defined as far as possible, particularly at the design stage. Safety objectives and system safety/performance can be derived by reference to the Operational Requirement and the type of service involved – for example an enroute surveillance service may have a lower level of criticality of availability and continuity than a terminal surveillance service. The safety requirements of a particular service may be established by assessing the effect of possible functional failure or fault modes as the source of safety hazards and the associated effect on the operation of the system.

6.2 The fault modes analysis should cover conceivable faults or eventualities affecting system performance including the possibility of human errors, common mode failures, simultaneous occurrences of more than one fault, and external eventualities which cause or result in the loss of, or affect the integrity of, external data, services, security, power supply, or environmental conditions.

6.3 The assessment of the safety objectives may then result in an iterative process of revision and further development of the system design, the adoption of modified operational procedures, or the establishment of contingency arrangements. For this reason, as far as possible the safety objectives should be expressed in a form that is clear and unambiguous so that they can be tested against, and the compliance of the system determined.

6.4 The selection of an appropriate way of expressing the safety objectives is important. Traditional measures include the specification of ***reliability, availability, continuity, maintainability, recoverability, accuracy,*** *etc.,* which have some interdependence. In the case of surveillance systems, specifying only availability, without also specifying a limit on the rate of occurrence of failures and faults, and the recoverability of the system following failure, could be insufficient to adequately define the safety requirements. For instance, a very infrequent occurrence of a fairly long down-time may be less hazardous than more frequent failures with shorter down-times, particularly for an ADS-B service in NRA where reversion to procedural separation is the contingency for system failure.

6.5 Quantitative statements of safety objectives and system performance requirements should be used where possible, however, in many areas (e.g.; where people and procedures are involved) it may not be feasible to define quantitative values. For these, qualitative values can be established. Where possible, these should be equated to or assigned corresponding quantitative values.

For a surveillance system, it is obviously important for safety that the voice or data communications service between pilot and ATC has a level of reliability (i.e. availability and continuity) at least of the same levels of performance as that assigned to the surveillance system itself. Obviously the two systems should be designed so that no single point of failure can result in both systems simultaneously failing at remote stations where single power source may only be available. Bearer links back to the ATC Centre will normally need to be duplicated on separate bearer circuits in order to achieve the reliability required for surveillance services.

6.6 In the development of the Australian ADS-B surveillance service in low density enroute airspace, the following basic safety and performance requirement for both the ADS-B service and the related voice communication service were established:

Table 1 – Basic Performance Parameters for ADS-B ground system (aircraft component not included)

SERVICE	SERVICE CATEGORY	GROUND SYSTEM OPERATIONAL AVAILABILITY	GROUND SYSTEM RELIABILITY per sector. MTBF (95%confidence level)
Enroute surveillance and voice comms (low density airspace)	Essential	.999	5000 hours
Terminal surveillance and voice comms (high density airspace)	Critical	.99999	10000 hours

Source: Airservices Australia Ops Requirements Doc v2.0

7 STEP 3 – Develop a Safety Risk management methodology

7.1 An appropriate, recognised methodology for safety risk management, i.e. for hazard identification; risk assessment; risk management, control, and mitigation, of a surveillance system, is required. The methodology may vary depending upon the type and safety implications of the proposed surveillance system, and the use of different methods, or combinations thereof, may be appropriate for the different elements and lifecycle phases included in the safety case.

7.2 Chapters 3 and 4 of the ICAO SMM are recommended as an appropriate methodology for States to adopt. Persons preparing Safety Cases are encouraged to familiarise themselves with the concepts in those two Chapters. The following Steps 4 – are based on and derived from those Chapters.

8 STEP 4 – Process for Hazard Identification and Analysis

8.1 Surveillance systems for aircraft separation services provide significant safety enhancement compared with procedural systems. However, there are safety consequences that predominantly arise during abnormal conditions or in fault or failure situations. Potential risks arise if related systems for air ground communication fail, or aircraft navigation or transponder avionics lose integrity or fail. Lesser impacts on safety might occur where the integrity of a system is degraded or lost but where there are alternative back-up systems, or contingency arrangements, that can be reverted to in order to maintain separation.

8.2 The process for hazard identification and analysis is set out in section 4.5 of the ICAO SMM, from which some of the information in this section is extracted and summarised.
It is essentially a 3 step process:

a) First: Identify the generic hazard (also known as top level hazard, or TLH). Generic hazard is used as a term that intends to provide focus and perspective on a safety issue, while also helping to simplify the tracking and classification of many individual hazards flowing from the generic hazard.
b) Second: Break down the generic hazard into specific hazards components of the generic hazard. Each specific hazard will likely have a different and unique set of causal factors, thus making each specific hazard different and unique in nature.
c) Third: Link specific hazards to potentially specific operational consequences, i.e. specific events or outcomes of the occurrence of the hazard.
d) Fourth: Document the hazards and its consequence.

8.3 Techniques for hazard identification and analysis for a new surveillance system may include:

a) the use of data or experience with similar systems/changes undertaken by overseas or other
b) respected providers of ATC surveillance services;
c) quantitative modelling based on sufficient data, a validated model of the change, and analyzed assumptions; e.g. RAM modelling.
d) the application and documentation of expert knowledge, experience and objective judgement by specialist staff;
e) trial implementation of a proposed change in an “off-line” system, or under a pre-existing surveillance service, and with sufficient backup facility to revert to the existing system before the change, if risks cannot be mitigated;
f) event tree analysis (ETA);
g) failure modes and effects analysis (FMEA);
h) human factors analysis (HFA);
i) hazard identification workshop with expert personnel (HAZID).

9 STEP 5 – Establish the Safety Risk of each Hazard

9.1 The reference for this process is section 5.4 and 5.5 of the ICAO SMM, and Tables 30 and 31 of RTCA DO-303/Eurocae ED-126.

9.2 For each of the identified operational consequences of the identified hazards, the safety risk should be established by assessing the probability of occurrence, and the severity of the consequence or outcome.

9.3 Safety risk probability is defined in the SMM as the likelihood that an unsafe event or condition might occur. Safety risk severity is defined as the possible consequences of an unsafe event or condition.

9.4 The following tables have been extracted from the SMM as the criteria for the risk assessment process.

9.5 Particular attention should be given to hazards that have operational consequences of common mode failure. For example, for an ADS-B surveillance service, failure or drop-out or short term loss of integrity of the GNSS may lead to total or partial loss of ATC surveillance and aircraft navigation. The risk control avenues open to a service provider may identify that a safety requirement is to ensure a means of backup to provide continuity of navigation and surveillance during the loss of GNSS, particularly for a terminal are service. Alternatively procedural mitigation may be implemented. Service providers should identify the most appropriate means or combination of risk controls based on local infrastructure and operational circumstances.

Table 2: Safety Risk Probability Table (source ICAO SMM)

Probability	Meaning	Value
Frequent	Likely to occur many times	5
Occasional	Likely to occur sometimes	4
Remote	Unlikely to occur, but possible	3
Improbable	Very unlikely to occur	2
Extremely improbable	Almost inconceivable that the event will occur	1

Table 3: Safety Risk Severity Table (source ICAO SMM)

Severity of Occurrence	Meaning	Value
Catastrophic	Equipment destroyed Multiple deaths	A
Hazardous		B
Major	A significant reduction in safety margins, physical distress or a workload	C
Minor	Nuisance Operating limitations Use of emergency procedures Minor incident	D
Negligible	Little consequences	E

10 STEP 6 – Establish the Safety Risk Assessment Criteria

10.1 In order to ensure that the range of possible safety risks are appropriately classified and controlled, it is necessary for service providers to establish standard, stand-alone, criteria for safety risk assessment and classification. Such a safety risk classification scheme provides a structure for deriving the safety requirements for any airways system, as well as the criteria for risk control decisions. Typically, such schemes provide a standard relationship between the probability of

occurrence of each risk and the categorised severity of the risk in terms of its potential impact on safety.

10.2 A Safety Case document must include or reference the risk assessment criteria (also termed a Risk Tolerability Classification scheme) adopted by the service provider for system safety management.

10.3 The following two Tables (Table 4 and Table 5) have been extracted from the ICAO SMM for Safety Risk Assessment criteria and Safety Risk Tolerability criteria:

Table 4: Safety Risk Assessment Matrix (source ICAO SMM)

Risk Probability	Risk Severity				
	Catastrophic A	**Hazardous B**	**Major C**	**Minor D**	**Negligible E**
Frequent 5	5A	5B	5C	5D	5E
Occasional 4	4A	4B	4C	4D	4E
Remote 3	3A	3B	3C	3D	3E
Improbable 2		2B	2C	2D	2E
Extremely Improbable 1	1A	1B	1C	1D	1E

Table 5: Safety Risk Tolerability Matrix (source ICAO SMM)

Suggested criteria	Assessment risk index	Suggested criteria
INTOLERABLE	5A, 5B,5C, 4A, 4B, 3A	Unacceptable
TOLERABLE/MITIGATE	5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C	Acceptable based on risk mitigation. May require management decision
ACCEPTABLE	3E, 2D, 2E, 1A, 1B, 1C, 1D, 1E	Acceptable

10.4 A further reference, specifically for a surveillance service is shown in. Table 30 of that document presents a qualitative Hazard Classification Matrix derived from ED-78A/DO-264 with 5 grades of risk severity. However, the Risk Classification Scheme (RCS) actually used in the Operational Safety Analysis presented in RTCA DO-303/EUROCAE ED-126 at Table 31 is derived from Table 30 and is based on 5 grades of Safety Targets with the Risk Classification per flight hour of each expressed quantitatively. The scheme is repeated in Table 6 below for reference:

Table 6: DO-303 OSA - Risk Classification Scheme for ADS-B Surveillance Service

Safety Targets	Risk per flight-hour	Risk per flight
ST1 Accident	**1e-08**	**1e-08**
ST2 Serious Incident	**1e-05**	**1e-05**
ST3 Major Incident	**1e-04**	**1e-04**
ST4 Significant Incident	**1e-02**	**1e-02**
ST5 No immediate effect on safety	**Not rated**	**Not rated**

11 STEP 7 – Process for Risk Control and Mitigation

11.1 A risk control process to eliminate, control or mitigate all risks categorised as intolerable or unacceptable, to at least to a tolerable or acceptable level, must also be defined. Risk controls may vary considerably, and employ any one, or a combination of, the following:

a) system redesign, modification or replacement;
b) process or procedures redesign, particularly procedures by operational personnel;
c) reliability improvement schemes;
d) personnel education and/or training;
e) various management controls on personnel, operational procedures and equipment; and
f) regulatory controls; including aircraft equipage mandates, limitations on entry to airspace by unequipped aircraft; equipage requirements in accordance with ICAO SARPs, etc..

11.2 Any identified risks which cannot be controlled to a tolerable level shall be explicitly included in a section of the Safety Case which includes a full discussion on all relevant aspects of the risk. The rationale for any decision to proceed with the development or operation of the system while the risk prevails is to be stated and justified.

11.3 **Precedence of Risk Controls.** In the application of the above or other risk control processes, a safety precedence sequence should be adopted and applied. For instance, control of identified hazards should normally be sought first through improved system design or equipment changes, followed then by specific operational procedures or training. For some risks, only one type of mitigation process will be feasible, others may need several means of risk control to bring the overall risk into tolerability. Whichever means of control is implemented the control process should demonstrate how the risks are being brought within the acceptable or tolerable areas of the criteria.

12 STEP 8 – Document and track the Hazards and their Risks

12.1 A standard method of documenting and tracking Hazards and Risks should be established.

12.2 Figure 4.2 of Chapter 4 of the ICAO SMM indicates the process involved in hazard/risk documentation.

12.3 The proformae used for the purpose of documenting/tracking Hazards relevant to ADS-B service as used by two States are shown in ICAO Circular 311 at Attachments E-1/E-2 (Australia) and Attachment E-3 (USA).

13 STEP 9 – Safety Case coverage over the lifecycle of the surveillance system

13.1 As previously discussed, Safety Cases should be developed in separate parts to define the safety situation of the system over the discrete stages of its lifecycle. A four part Safety Case has been adopted by some service providers to define the safety situation at the Operational Requirements stage, at the completion of the Design and Procurement phase, at the Implementation stage, and for the routine Operational phase.

13.2 The contents of the Safety Case will differ for each part. For some systems, it may be appropriate to have more or fewer parts of the Safety Case. For all parts, the level of description and detail included should be sufficient to provide a reasonably informed reader with an understanding of the safety situation, without the need to refer extensively to supporting references.

13.3 A guide to the coverage of each part of a four part Safety Case is included in Attachment A ‘Safety Case Coverage for a Four Part Safety Case’.

14 STEP 10 – Authority for issue and change of the Safety Case

14.1 Safety Cases should be placed under a documentation control process. The Safety Case should be authorised by competent authority designated by the service provider. An authority or authorities covering System Requirements, System Design, System Operation, and System Maintenance should be appointed, and the issue of the parts of the Safety Case should be made under the authorization of one or more of these designated bodies, as appropriate to the content of each part.

PART B: SPECIFIC ELEMENTS FOR INCLUSION IN SAFETY CASE COVERING ADS-B BASED SURVEILLANCE SYSTEMS

Primary references:

ICAO Circular 311, in particular:

Chapter 2: ATC Surveillance
Chapter 3: Assessment of ADS-B surveillance
Chapter 4: State Implementation Roadmap
Attachment A: General Description of the Reference SSR
Attachment B: Technical Comparison between Reference SSR and ADS-B
Attachment C: Key ADS-B Performance Requirements to Support the Claim that ADS-B Surveillance "Is As Good As the Reference SSR"
Attachments E1,E2: HAZID and Mitigation (Australia)
Attachment E3: Hazard Analysis Report (US Capstone Program)

RTCA DO-303/EUROCAE ED-126 December 13, 2006 Safety, Performance and Interoperability Requirements Document for the ADS-B Non-Radar Airspace Application
Note: This document is also included in ICAO Circ 311 as Attachment N)

Secondary reference:

ICAO Doc 9689 AN/953 Manual on Airspace Planning Methodology for the Determination of Separation Minima First Edition 1998

Introduction

This Part itemises the topics that should specifically be included in a Design and Implementation Safety Case for the introduction of an ADS-B based surveillance system in non-radar airspace. The information herein is derived from two sources; ICAO Circular 311, and the actual Design Safety Case that was produced by the Australian ANSP to gain the approval of the aviation regulator for the commissioning of the Upper Airspace ADS-B surveillance system. That Safety Case was essentially based on a comparative assessment showing that ADS-B was as good as or better than a Monopulse SSR system when used for the same surveillance purposes in the same airspace by ATC. This comparative assessment approach has been documented by the ICAO SASP in Circular 311 as an appropriate means of assessing the safety of an ADS-B separation service in non-radar enroute airspace.

1 STEP 11 – State Implementation Roadmap

1.1 For this STEP, readers should first acquaint themselves with Chapters 3 and 4 of ICAO Circular 311.

1.2 In Chapter 3 of ICAO Circular 311, the ICAO SASP describes the assessment it undertook of the use of ADS-B to support ATS. The assessment methodology compared

ADS-B to a Reference SSR which the SASP defined in terms of its technical performance. The assessment demonstrated that ADS-B surveillance is better or at least no worse than the

Reference SSR and therefore no less safe than Radar. The SASP concluded that, if a number of ADS-B performance requirements relating to the integrity and accuracy of the received ADS-B transmissions from aircraft and the overall latency and update rates of the system are met, then ADS-B can be used as a means of supporting the provision of a 5NM separation minima similar to that used with radar.

1.3 However, in making that conclusion, the SASP noted that its assessment was undertaken based on global assumptions and was for low complexity airspace and for the defined reference radar. In its Conclusion to Chapter 3, for reasons it explains in the Chapter, it noted that there remained the requirement for a region or State to undertake a State or local assessment that demonstrates the intended safety level will be met using ADS-B surveillance. To this end, a 'State implementation roadmap' was provided for the guidance of States.

1.4 Circular 311 provides the references and technical evidence to show that ADS-B is as good as or better than an MSSR when used for an enroute 5NM separation service by ATC. It is therefore unnecessary to demonstrate that in a Safety Case covering a State or local surveillance service. A State can make reference to that finding in Circular 311 rather than prove that in a Safety Case. However, it should be noted that the Circular clearly points out that the analysis by the SASP makes assumptions on a generic airspace situation which may not be totally relevant to the airspace situation in any particular State, and that State and/or local level assessments should be undertaken where there is any difference between the Sate's conditions and those in the assumptions made in the Circular. (Refer to Sections 4.5.1 and 4.5.2 of Circular 311.) Further, there always remains the requirement to undertake State or local level hazard identification and risk analysis of all hazards. For that purpose, the further value of Circular 311 as guidance material for ADS-B Safety Case preparation is that it provides a Compendium of Hazards and Mitigation Measures which has been extracted from several site-specific ADS-B Safety Cases of ADS-B trials and implementation undertaken in two States (USA and Australia), as well as those identified by EUROCAE in the Annexes to ED-126 also attached to Circular 311. This Hazard Compendium will be of value as a reference to those States embarking on safety assessment of their own ADS-B programs.

1.5 The State Implementation Roadmap in Circular 311 comprises four distinct Processes. Process C is the Safety Assessment (Initial, Implementation and Operational), implying that a three part Safety Case is required for those three phases of system development. General guidance on the undertaking of all four Processes is given in Section 4.6 of Circular 311. It is recommended that authors of Safety Case documents for ADS-B surveillance should familiarize themselves with that Section.

1.6 **ADS-B System Design - Performance standards**. In Attachment C to Circular 311 the ICAO SASP identified the key ADS-B performance requirements for an ADS-B system to enable

use of a 3NM or 5NM separation minimum in the provision of ATC. Subsequently, at its WG/WHL/13 Meeting in May 2008, the ICAO SASP agreed to update its Circular 311 including Attachment C to the effect that ADS-B 3NM and 5 NM separation services could be delivered when ADS-B data quality indicators met the following requirements:

Table 6: SASP Comparative Assessment – ADS-B Performance Characteristics (extracted from ICAO Circ 311).

	Characteristic	Minimum Requirement 3NM separation service	Minimum Requirement 5NM separation service
1	Position: Accuracy	NACp = 6 or better; corresponds to HFOM < 0.3NM	NACp = 4 or better; corresponds to HFOM < 0.5NM
2	Position: Integrity	NUC = 5 or better; OR NIC = 5 or better ; corresponds to HPL containment radius < 1NM SIL = 2 or better	NUC = 4 or better; OR NIC = 4 or better; corresponds to HPL containment radius < 2NM SIL = 2 or better
3	Position: Latency	4 seconds	4 seconds
4	Position: Update Rate	12 seconds	12 seconds

Note 1: These values in Table 6 differ from those presently included in Attachment C to Circular 311. It is recommended that these performance parameters in Table 6 can be used by States for ADS-B system design pending the publication of the amendments to Attachment C to Circular 311 by ICAO.

2 STEP 12 – Safety Case for ADS-B NRA

2.1 **RTCA DO-303/EUROCAE ED-126**. Extensive guidance material to assist in preparation of a Design Safety Case on the ADS-B NRA Application is contained in RTCA DO-303/EUROCAE ED-126. That document is a virtual Safety Case and the publication can be used as a reference alongside ICAO Circular 311. The complete document is relevant although the **Operational Safety Assessment** at Annex C has most relevance. Annex C contains the following Steps:

a) Hazard Classification Matrix as per DO-264/ED-78A (Table 30)
b) Safety Targets and Risk Classification Scheme (Table 31)
c) Operational Hazards Identification by Expert Analysis (Table 33)
d) Allocation of Safety Objectives (the maximum frequency or probability at which an operational hazard can be tolerated to occur) and the Safety Requirements for Operational Hazard mitigation.

3 STEP 13 – Safety Case Contents

3.1 **Contents of the Safety Case**. Guidance material on the **contents** (i.e. the topic headings, with a brief description of each topic that may be included under each heading) for inclusion in an ADS-B Design Implementation Safety Case is at Attachment B . This topic listing has been derived by reference to the Safety Case for the ADS-B Upper Airspace Program (UAP) prepared in Australia by the ANSP. (That particular Safety Case was the basis of the regulatory approval by CASA of the now implemented ADS-B UAP of Airservices Australia.)

ATTACHMENT A

Safety Case Coverage for a Four Part Safety Case

The following is a guide to the structure of a four part Safety Case over the life of an airways system.

Safety Case Part 1 - Operational Requirements Phase
A Safety Case Part 1 contains the Safety Objectives and the corresponding Safety Requirements for the proposed system, and will normally be the initial document provided to advise the proposed project's existence and its safety significance. The Safety Case at this stage should be an evaluation of the proposed system, perhaps most appropriately carried out by means of a Preliminary System Safety Assessment (PSSA), supplemented as necessary by overseas or previous experience, and in-house expertise and knowledge of deficiencies in existing systems which the new system is to replace.

Safety Case Part 2 - Design and Procurement Phase
Part 2 of the Safety Case is essentially to assure that the design of the system supports and provides for the safety requirements. Arguments to support the design rationale and the proposed technology of the system, and to verify and validate that such satisfies the safety requirements will be provided. The human factors aspects of the design, and the safety implications of the design of the procedures, and the ability of personnel to safely operate to the design procedures, should also be considered. Here, a full hazard and risk evaluation of the detailed design, including hardware, software, man/machine interface, human factors, equipment and administrative interfaces and external factors, should be undertaken.

Safety Case Part 3 – Implementation Phase
Part 3 of the Safety Case will provide an analysis of the safety situation following its installation and integration. The functional testing to be carried out for installation and pre-commissioning evaluation of the safety situation is detailed in this part. A testing regime aimed at validating the risk assessment made in Part 2 of the Safety Case, and identifying safety hazards not previously identified at Part 2 which arise during testing and integration and related activities, should be defined , with the strategy for assessing and managing these hazards and the safety issues which arise from such testing also specified.

Safety Case Part 4 - Normal Operations Phase
Part 4 of the Safety Case will provide the evidence that the system is safe in operational service. It will address all relevant operational and management issues, and will take account of the safety findings from the preceding three parts of the Safety Case. This part of the Safety Case is maintained as a living document for the life of the system, to define and document any further hazards, identified at post-commissioning or during routine operations, and the risk control actions taken to maintain compliance with safety objectives, in the light of actual day-to-day knowledge and experience with the system.

Note in respect to all Parts
It is important that all parts of the Safety Case be retained and maintained as necessary over the life of the system, reflecting the safety situation for any approved modifications or changes to the system.

ATTACHMENT B

Sample Headings and Content for an ADS-B System Implementation Safety Case

No.	Heading	Brief Description of Content
1	Title	State the Title of the Safety Case. E.G. ADS-B Upper Airspace Program – Implementation Phase Safety Case
2	Purpose/Background/Operational Requirement	State the background to the development of the system. State the previous trials leading up to the implementation of the surveillance system. State the operational requirement of the system; the scope of the system and the scope of the safety case.
3	Scope	Define the scope of the system covered by the Safety Case. Operational staff impact. Technical staff impact. Changes to voice comms system. System coverage, engineering and operational standards adopted. Include coverage and location of ground station infrastructure, ground station design, bearer link network design, changes to ATM facilities at Area Centres. System transition management. Relativity to other programs. Existing system upgrade requirements. Development of new ATC procedures. Regulatory approval requirements/plans.
4	System Overview and Description	Overall system description/diagram. Ground Stations locations. Site Monitor. Terrestrial and satellite bearer links to ATC Centres. ATC System Processors. ATC Display. Remote Control and Monitoring System. RAIM prediction system. Power supply system(s). Provide schematic diagram of overall system including third party provided services and data-links
5	VHF Communication System	Overall voice comms system description/performance standards/overview/ bearers/third party provided services.
6	New ATC Procedures and Staff Training plan	Define existing separation standards and the intended new separation standard(s). Define ATC staff training required for ‘radar-like service’.
7	Logistics support	Define all aspects of the ILS plan including hardware and software maintenance, spares support plan,
8	Safety Requirements	Establish the safety standards and requirements in terms of system performance parameters (RAM).
9	Assumptions, Constraints and Dependencies	Comparison with radar for 5NM separation service. Proposed aircraft operational accuracy (NAC) and integrity (HPL) standards. State dependencies with related projects (voice, data bearers, aircraft equipage requirements, ATC system upgrades, etc)
10	Responsibilities	Establish the relevant staff responsibilities for the project implementation and safety management. Include all specialist and management personnel and responsibilities
11	Consultation and Communication	State the external consultation undertaken with stakeholders including any issues in relation to safety

No.	Heading	Brief Description of Content
		considerations. Provide references to documentation of consultation outcomes.
12	Design Process	Define the design process undertaken in system development. Define the design test plan/procedures and the outcome of design reviews.
13	Design Safety Risk Management	Describe the processes undertaken for Safety Risk Management at the design phase. Include reference to design HAZID and HAZLOG reviews undertaken. Establish the current status of all hazards identified in the design phase
14	Design Limitations and Shortcomings	Itemize all design phase deficiencies remaining (major and minor) and their safety status and impact
15	Implementation Process	Establish engineering transition plan. Establish operational transition plan. Establish contingency plan for reversion to existing system.
16	Status of Safety Controls and Safety Requirements	State the status of all safety controls and requirements. All outstanding Hazards and all safety requirements not satisfied to be subject to individual documentation
17	Engineering Support and Engineering System Maintenance	Describe the means of future engineering support – internally and externally to the organisation as applicable. Provide references to documented system maintenance procedures.
18	Criteria for Maintenance Technician certification	Establish the technician competency requirements for system monitoring, operation and maintenance.
19	Safety Performance Monitoring	Describe or reference the process for monitoring and management of safety performance after implementation of the system.
20	ATC Staff Training and Education Plan	Establish the ATC staff training plan and comprehensive training package.
21	Pilot Information Package	Provide reference to the Pilot Information and the dissemination of the package.
22	SystemTransition Plan	
23	RAM End-to-End System Analysis	Undertake Reliability, Availability, Maintainability analysis of the end-to-end system. (Use manufacturer provided RAM data or field data if available.) Compare results with established design standards/requirements.
24	System Test Procedure	Describe generally and provide reference to the detailed System Test Plan.
25	System Test Results	State the outcome of the system tests undertaken
26	**Define the System Safety Risk Management plan**	**Provide documentation of the safety risk management plan**
27	**Define Risk Management Process used for the Safety Case**	**Risk Management Process to be defined or referenced. Include process for Hazard Identification, Risk Assessment, Risk Classification, and Risk Control processes.**
28	**HAZID**	**Provide the record of all HAZID activities undertaken**
29	**Status of Hazards (HAZLOG)**	**Provide documentation of the status of all Hazards.**
30	**List all Hazards not controlled to tolerable level**	**List all Hazards not controlled to tolerable level, the reasons and justification.**
31	Post implementation review plan	Establish the plan, timing and procedures for post

No.	Heading	Brief Description of Content
		implementation review of the performance and safety of the system.
32	Related documentation	Include listing of references to all related or referenced documents

ICAO APAC SITF/9 WP/7

presented by Australia

DRAFT ICAO APAC Guidance Material

Building a Safety Case for a Surveillance Service

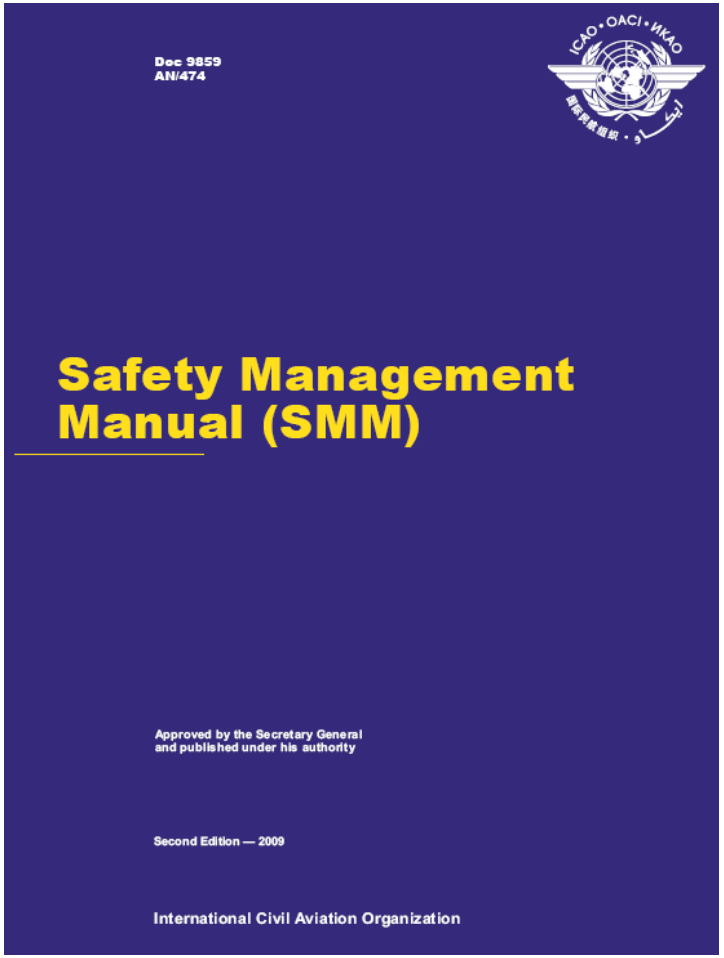
for consideration by SITF/9

Guidance Material for Building a Safety Case for a Surveillance Service

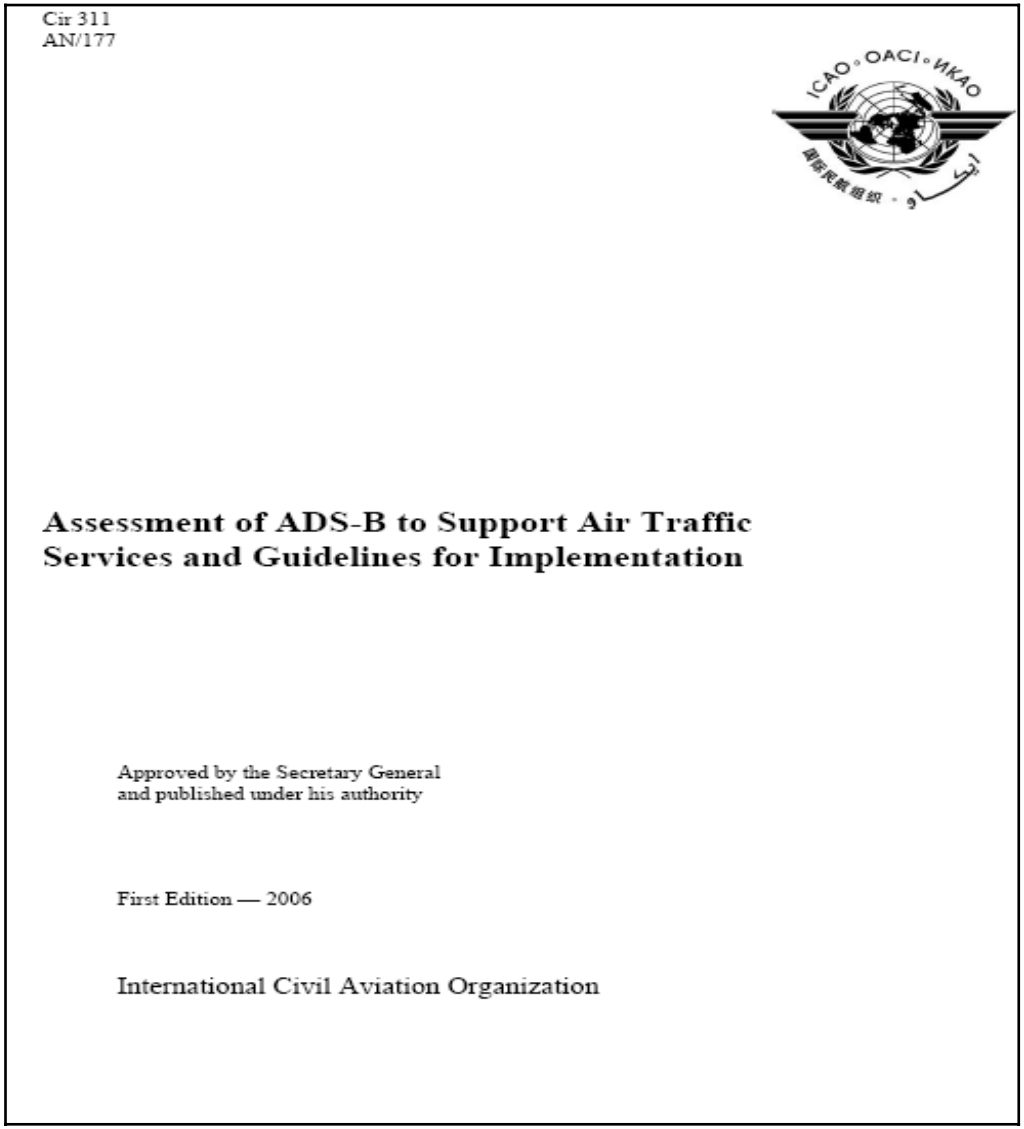
- Guidance material does not try to reinvent anything – relies heavily on references to 2 existing ICAO Docs and one RTCA/Eurocae doc.
- Two Parts:
- Part A: Generic aspects of developing a safety case for any airways system or service
- Part B: Specific elements of a safety case for an ADS-B based surveillance service

Generic reference - HazID and Risk Management
ICAO DOC 9859 Safety Management Manual
Chapters 4 and 5

www.icao.int/icaonet/



Specific reference for ADS-B service (and MULTILAT to be included in next update issue) : ICAO Circular 311
www.icao.int/icaonet/



Cir 311
AN/177

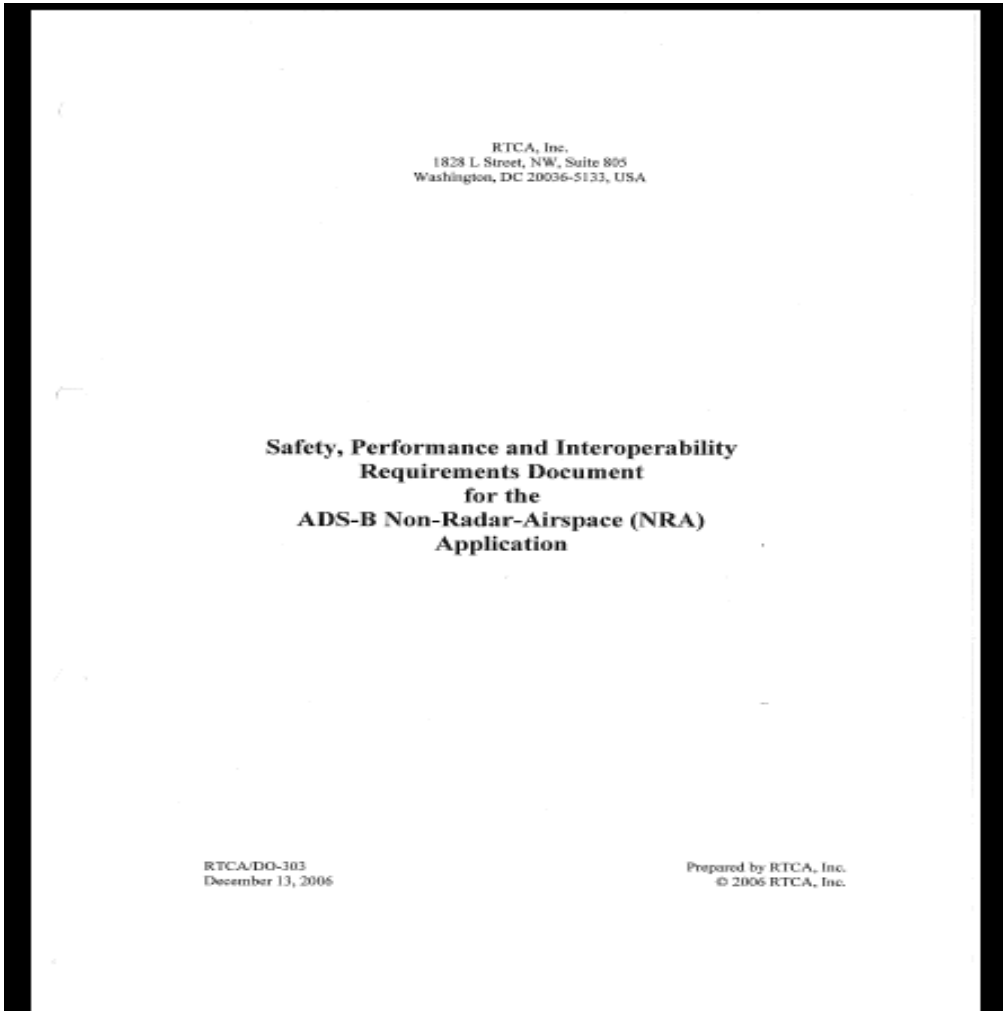
Assessment of ADS-B to Support Air Traffic Services and Guidelines for Implementation

Approved by the Secretary General
and published under his authority

First Edition — 2006

International Civil Aviation Organization

Specific reference for ADS-B safety case preparation:
RTCA DO-303/EUROCAE ED-126 - Dec 2006
Safety, Performance and Interoperability Requirements Document for the NRA Application



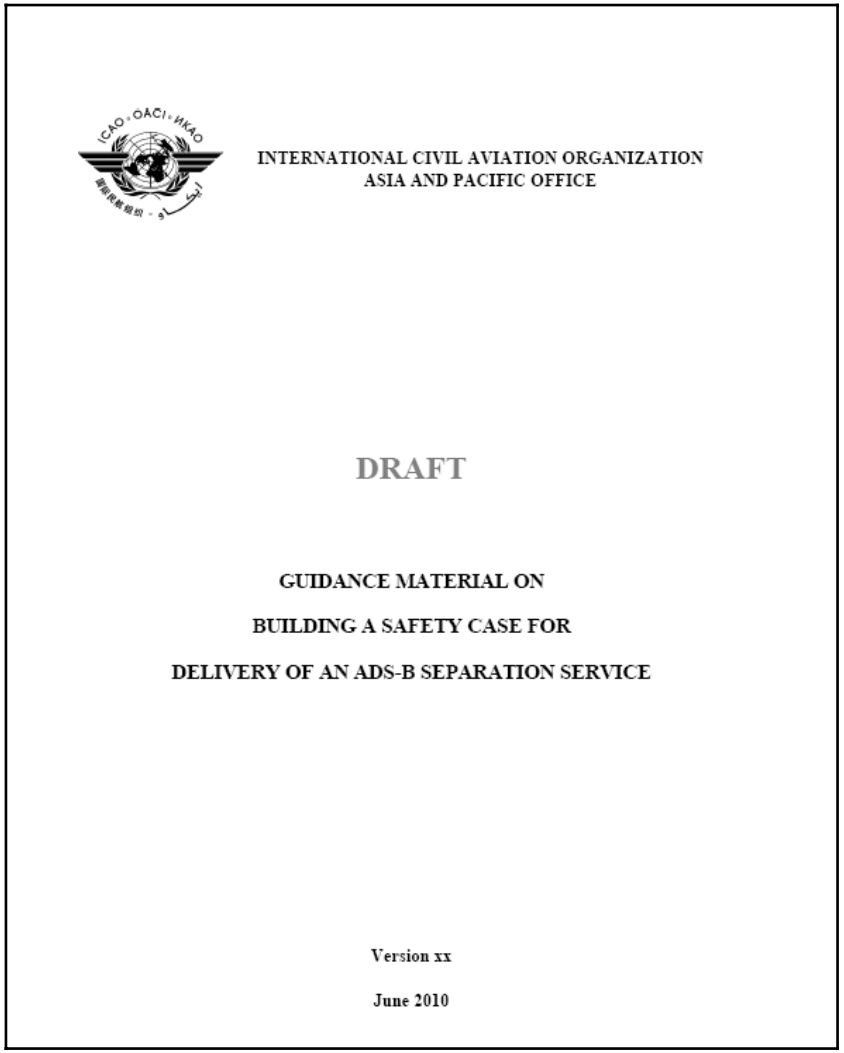
RTCA, Inc.
1828 L Street, NW, Suite 805
Washington, DC 20036-5133, USA

Safety, Performance and Interoperability Requirements Document for the ADS-B Non-Radar-Airspace (NRA) Application

RTCA/DO-303
December 13, 2006

Prepared by RTCA, Inc.

Draft Guidance Material on Building a Safety Case for Delivery of an ADS-B Service essentially derived from those 3 docs



INTERNATIONAL CIVIL AVIATION ORGANIZATION
ASIA AND PACIFIC OFFICE

DRAFT

GUIDANCE MATERIAL ON

BUILDING A SAFETY CASE FOR

DELIVERY OF AN ADS-B SEPARATION SERVICE

Version xx

June 2010

Guidance Material – Contents

- **Primary References – the 3 docs in the previous slides**
- **Introduction**
- **Definitions**

- **PART A Generic Guidance on Safety Case Preparation – ICAO Doc 9859 + CASA Australia CAAP**

- **PART B Specific Elements For Inclusion in Safety Case Covering ADS-B Based Surveillance System**

  ICAO Circ 311 + RTCA Do-303/Eurocae ED-126

- **Attachments**

Part A: **Generic Guidance on Safety Case Preparation**

- What is a Safety Case
- Generic contents of a Safety Case
- Safety Planning
- A Safety Case may have several discrete parts over the system lifecycle
- STEP 1 – State the Purpose and Scope of the Safety Case
- STEP 2 – Develop and document the safety objectives and safety requirements
- STEP 3 – Develop a Safety Risk management methodology
- STEP 4 – Process for Hazard Identification and Analysis
- STEP 5 – Establish the Safety Risk of each Hazard
- STEP 6 – Establish the Safety Risk Assessment Criteria
- STEP 7 – Process for Risk Control and Mitigation
- STEP 8 – Document and Track the Hazards and the Risks
- STEP 9 – Safety case coverage over the lifecycle of the surveillance system
- STEP 10 – Authority for issue and change of the safety case

Part B: **Specific Elements for Inclusion in a Safety Case Covering ADS-B Surveillance System**

- **Primary references:**
- STEP 11 –State Implementation Roadmap (ICAO Circ 311)
- STEP 12 – Example of Safety Case for ADS-B NRA
- STEP 13 – Safety Case Contents
- Attachment A – Safety Case Coverage for a Four Part Safety Case
- Attachment B – Sample Headings and Content for an ADS-B System Design and Implementation Safety Case

Part B: **Specific Elements for Inclusion in a Safety Case Covering ADS-B Surveillance System**

Primary references:

- **ICAO Circular 311, in particular:**
  - **Chapter 2: ATC Surveillance**
  - **Chapter 3: Assessment of ADS-B surveillance**
  - **Chapter 4: State Implementation Roadmap**
  - **Attachment A: General Description of the Reference SSR**
  - **Attachment B: Technical Comparison between Reference SSR and ADS-B**
  - **Attachment C: Key ADS-B Performance Requirements to Support the Claim that ADS-B Surveillance "Is As Good as the Reference SSR"**
  - **Attachments E1,E2: HAZID and Mitigation (Australia)**
  - **Attachment E3: Hazard Analysis Report (US Capstone Program)**

- **RTCA DO-303/Eurocae ED-126 December 2006: Safety, Performance and Interoperability Requirements Document for the ADS-B Non-Radar Airspace Application**
  - **Note: also reproduced in ICAO Circ 311 at Attachment N**

Four Part Safety Case to cover airways system lifecycle

- Part 1: **Operational Requirements Phase**
  - contains safety objectives and corresponding safety requirements of the surveillance system
- Part 2: **Design and Procurement Phase**
  - Parts 1 and 2 might be combined
  - Contains evidence that system design meets safety requirements
- Part 3: **Implementation Phase**
  - Safety analysis following installation and integration
  - Testing plan and results
- Part 4: **Normal Operations Phase**
  - Includes additional hazards arising during routine operations