EUROPEAN ORGANISATION
FOR THE SAFETY OF AIR NAVIGATION

EUROCONTROL

ACAS II Post-implementation Safety Case

Edition Number	:	2.3
Edition Date	:	25/11/2011
Status	:	Released Issue
Intended for	:	ATM Stakeholders

DIRECTORATE NETWORK MANAGEMENT

DOCUMENT CHARACTERISTICS

TITLE

ACAS II Post-implementation Safety Case

	EUROCONTROL ALDA Reference:	11/03/28-15
Document Identifier	Edition Number:	2.3
	Edition Date:	25 November 2011

Abstract

This document contains the Safety Case for ACAS II operations in ECAC airspace following completion of the transition period for implementing Phase 2 of the European ACAS II Policy. The operational context includes the amendments to ICAO ACAS provisions implemented on 20 November 2008.

Keywords

ACAS
Safety Net
Collision Avoidance
Safety Case
TCAS

Contact Person(s)	Tel	Unit
Stanislaw Drozdowski (stanislaw.drozdowski@eurocontrol.int)	+32-2-729-3760	DSR/CMN/ATS

STATUS, AUDIENCE AND ACCESSIBILITY

Status		Intended for		Accessible via	
Working Draft	□	General Public	□	Intranet	□
Draft	□	ATM Stakeholders	☑	Extranet	□
Proposed Issue	☑	Restricted Audience	□	Internet (www.eurocontrol.int)	☑
Released Issue	□	*Printed & electronic copies of the document can be obtained from the EUROCONTROL Infocentre (see page iii)*			

ELECTRONIC SOURCE

Path:	\\HHBRUNA19\sdrozdow$\ACAS Programme\APOSC	
Host System	Software	Size
Windows_NT	Microsoft Word 10.0	3019 Kb

EUROCONTROL Infocentre
EUROCONTROL Headquarters
96 Rue de la Fusée
B-1130 BRUSSELS

Tel: +32 (0)2 729 51 51
Fax: +32 (0)2 729 99 84
E-mail: infocentre@eurocontrol.int
acas@eurocontrol.int

DOCUMENT APPROVAL

The following table identifies all management authorities who have successively approved the present issue of this document.

AUTHORITY	NAME AND SIGNATURE	DATE
Version 2.0 Author/preparer	Ronald H. Pierce	16 November 2010
Version 2.0 Reviewer	Eric Perrin	16 November 2010
APOSC Project Manager	Stanislaw Drozdowski	28 March 2011
Head of Surveillance and Code Coordination Directorate Network Management	John Law	28 March 2011
Head of Safety Directorate Network Management	Antonio Licu	10 May 2011
Head of Deployment Coordination Directorate Network Management	Pascal Dias	10 May 2011
Chief Operating Officer Directorate Network Management	Joe Sultana	3 October 2011

DOCUMENT CHANGE RECORD

The following table records the complete history of the successive editions of the present document.

EDITION NUMBER	EDITION DATE	INFOCENTRE REFERENCE	REASON FOR CHANGE	PAGES AFFECTED
1.0	05/08/05		First draft	All
1.2	05/06/06		Update following independent review by DAP/SAF	
1.3	31/07/07		Completely rewritten to eliminate weaknesses in safety argument	All
1.4	30/09/07		Update incorporating comments from walkthrough review on 02/08/07. Completion of sections 5.9-12.	All
1.5	20/11/07		Update incorporating assessment of revised ICAO ACAS provisions	All
1.6	17/12/07		Update incorporating comments from review meeting on 30/11/07.	All
1.7	18/11/08		Update incorporating formal comments from DAP/SSH and QinetiQ, and residual comments from DAP/SUR	All
1.8	12/03/10		Major changes following review by Safety CoE. Revised structure for main argument, assumptions, safety issues, conclusions and recommendations. Addition of material referring to RA Downlink and Überlingen accident and RA occurrence-rate information. Further safety requirements and issues introduced.	All
1.9	26/04/10		Update following final, independent review on behalf of Safety CoE	All
1.9A	07/10/10		Corrections following EUROCONTROL final review	All
2.0	16/11/10		Released Issue	All
2.1	28/03/11		EUROCONTROL organizational changes; Document reformatted	All
2.2	02/11/11		Addressed PDF conversion problems (mis-formatting). No changes to the text.	All
2.3	25/11/11		Addressed comments received from EASA. Editorial changes.	All

CONTENTS

Page intentionally left blank

EXECUTIVE SUMMARY

This document contains the post-implementation Safety Case for ACAS II operations in ECAC airspace following completion of the transition period for implementing Phase 2 of the European ACAS II requirement. The operational context takes into account the ICAO ACAS provisions as of 20 November 2008[1]. Since all aircraft subject to the requirement are equipped with TCAS II Version 7.0, the Safety Case exclusively addresses ACAS II[2] functionality as defined by the TCAS II specification RTCA DO-185A.

The purpose of the Safety Case is to demonstrate that the safety of aircraft operations is substantially improved by ACAS. It does so by using a structured safety argument, supported by evidence from a safety assessment performed as part of the Safety Case, and from external sources.

The document reflects the regulatory situation on 31 December 2008 and any subsequent changes to European regulations or ICAO provisions are not taken into account.

From the EUROCONTROL viewpoint, the APOSC is considered as an *Air Traffic Management* (*ATM)* Safety Case. In this context, APOSC (and ACAS) need only comply with regulatory requirements and standards applicable to *ATM* Safety Cases and not those applicable to certification/operational approval of avionics systems on civil aircraft. In particular, the APOSC does not seek to demonstrate that ACAS complies with safety targets applicable to aircraft operations in general, or those applicable to avionics equipment.

The APOSC addresses only the functional safety of ACAS operations. By implication, it covers the human and procedural aspects of mid-air collision avoidance using ACAS, as well as the ACAS equipment itself. Airworthiness of equipment (including the associated maintenance aspects) is not considered because it is deemed to be adequately covered by standard avionics design, certification and support practices.

The methodology has necessitated the derivation of key ACAS operating fundamentals, a logical system design, and a set of Safety Requirements covering the equipment, people, and procedural elements of the overall system. These abstract representations of ACAS have hitherto not existed. They form the basis for arguing the safety of ACAS at the current point in its lifecycle, and are crucial for the safety assessment of any significant changes to ACAS operations in the future. The parts of the safety argument which deal with the specification of ACAS have generally concluded that the Safety Requirements represent a system which will substantially increase the safety of aircraft operations <u>if</u> they are correctly implemented. However, further assurance could be gained from the construction of a fully quantified ACAS risk model, and from the procedural mitigation of a number of potential hazard causes arising from permitted operations.

Below the level of the Safety Requirements, ACAS operations are represented by multiple levels of specification for the system and its operation, spanning ICAO provisions down to more-detailed specifications and implementations by all the manufacturers, ANSPs, and aircraft operators who are involved in ACAS operations in ECAC airspace. Some of the direct evidence necessary to support this part of the safety argument is impracticable to assess within the scope of the Safety Case because of its extent, and is not readily available to EUROCONTROL. Consequently, the assurance that ACAS operations conform to the Safety Requirements is limited to a detailed assessment of the ICAO ACAS provisions with which

[1] See Appendix L hereto for a summary of the “ACAS Provisions”

[2] Airborne Collision Avoidance System (ACAS) is the system whose technical characteristics and operation are defined by ICAO. Traffic Alert and Collision Avoidance System (TCAS) II is the system whose technical requirements are defined by RTCA. As TCAS II is the only system commercially available that corresponds to the ACAS II requirements from ICAO, both acronyms are often used when referring informally to the system.

the international aviation community is obliged to comply. This *a priori* assessment has revealed a number of discrepancies within the ICAO documentation, and with its conformity to the Safety Requirements. Whereas these discrepancies are not considered significant enough to undermine the safety claim, they should nevertheless be further investigated.

Despite being an established operational system whose behaviour is routinely monitored, there is no direct, *a posteriori* evidence from real operations that the collision risk reduction achieved by ACAS satisfies the criteria underpinning the Safety Case. Although there are established processes for progressively improving the capabilities of ACAS throughout its operational life, assurance of its overall safety performance is based predominantly upon theoretical *a priori* predictions of risk reduction. This situation is likely to persist throughout its life due to the practical difficulties of measuring collision risk in the airspace.

Based on the evidence contained in this Safety Case, it is concluded that the Safety Claim for current ACAS operations is substantiated. A number of residual safety issues are identified, none of which is sufficiently serious to undermine the Safety Claim, but which if addressed would could provide some further risk reduction, and would provide additional confidence that all steps that are reasonably practicable in risk reduction have been taken.

As well as current ACAS operations, the Safety Case addresses assurance of safety in the future on the basis that the established arrangements for monitoring and rectification of operational problems will continue to be effective. However, these arrangements were changed in 2007 and there remain no formally defined responsibilities or procedures for the overall process. This is listed as one of the outstanding Safety Issues.

Conclusions

Subject to certain Assumptions and the resolution of an outstanding Safety Issues stated herein, ACAS II currently (late 2010) provides a substantial net positive contribution to the risk of a mid-air collision, as demonstrated by analysis of the design and implementation of the total ACAS system. The risk of a mid-air collision with ACAS is believed to be reduced by a factor of about 5 compared with the risk which would exist in the present European ATM and operational environment in the absence of ACAS.

There is little direct statistical evidence from actual experience of ACAS operations, because the absolute risk of a mid-air collision (with or without ACAS) is very low.

ACAS presents a negligible contribution, either positive or negative, to the risk associated with types of aircraft accident other than mid-air collisions or passenger/crew injuries resulting from ACAS-induced manoeuvres or ineffective operation of ACAS. Operational monitoring of ACAS has led to improvements in the net risk reduction provided by the total ACAS system over a period of time (particularly with respect to the people and procedures aspects of the system). Nevertheless, it is acknowledged that some problems still remain to be resolved.

There are other residual Safety Issues which, if addressed, would provide either further risk reduction in accordance with the principle that risk should be reduced As Far as Reasonably Practicable or increased confidence in the achieved contribution of ACAS to risk reduction.

In the short / medium term (until, say, up to 2013), changes in the operational environment are not likely to degrade the effectiveness of ACAS to such an extent that the current safety claim (that it provides a substantial net positive contribution to safety) will cease to be true. Furthermore, as long as ACAS operations remain human centred, they are liable to degrade with time due to increasing inconsistency in human responses to RAs. Therefore, the absence of an ongoing EUROCONTROL monitoring programme means that there will be inevitably an element of uncertainty, which will increase over time, about the degree to which the safety claim for ACAS remains true – this is also raised as a Safety Issue.

In the longer term, some of the changes to European ATM proposed by SESAR could have a significant effect on ACAS operations. Monitoring of the effectiveness of ACAS will inevitably be needed to support the safety cases for such changes and should commence well before the changes are introduced in order to establish a statistically valid data set for comparison with the post-change situation.

Recommendation

The APOSC makes one recommendation concerning the need for explicit regulations to cover the safety assessment[3] of changes affecting ACAS operations.

[3] ie what ESARR 4 refers to as "risk assessment and mitigation"

1 INTRODUCTION

1.1 Background

The Airborne Collision Avoidance System (ACAS) is an airborne safety net which is designed to provide a reduction in the risk of mid-air collision. Based on SSR transponder signals, it operates independently of ground-based equipment to provide advice to the pilot on potential conflicting aircraft that are equipped with compatible transponders. A detailed description of ACAS can be found in [1].

In 1995, the ECAC States agreed a common ACAS II policy and implementation schedule for the mandatory carriage of an ACAS II by certain categories of aircraft when flying in their airspace; hereafter referred to as the European ACAS Policy. This policy was confirmed in 1997 by the ECAC Transport Ministers, and required the mandatory carriage and operation of ACAS II for flight in the airspace of ECAC Member States. The European ACAS II Policy was introduced in two phases which were completed by the end of March 2006. A brief history of ACAS, including its European and worldwide adoption, can be found in [2].

Subsequently, the ACAS II carriage requirement was incorporated into ICAO Annex 6 which requires that from 1 January 2005, all turbine-engined aeroplanes of a maximum certificated take-off mass in excess of 5,700 kg or authorized to carry more than 19 passengers shall be equipped with an airborne collision avoidance system (ACAS II) [3].

EUROCONTROL established a pan-European programme to manage the implementation of ACAS II for ECAC States. Following the completion of the implementation tasks, it was decided that an ACAS II Post-implementation Safety Case should be prepared.

The development and deployment of ACAS has spanned several decades, including its operation in Europe. Many years of successful operational experience with ACAS, complemented by rigorous analysis of its behaviour, had led to the conviction that it provides the expected safety benefit. However, much of its life pre-dates contemporary approaches to ATM safety assessment. Therefore, while its development has involved several safety studies aimed at predicting its collision avoidance effectiveness, it has not benefited from a systematic process of identifying the hazards and risks arising from ACAS operations, and then mitigating the causes of its hazards via the implementation of formal Safety Requirements.

Hereinafter, the term ACAS is used instead of ACAS II, except where important to the context. Furthermore, the term ACAS is generally used when referring to the equipment, whereas ‘ACAS operations’ is used when referring to the overall collision avoidance system comprising people, procedures and equipment.

1.2 Aim

The aim of the ACAS II Post-Implementation Safety Case (APOSC) is to demonstrate that aircraft operations with ACAS II are, and will remain, acceptably safe in ECAC airspace.

1.3 Scope restrictions

The document reflects the regulatory situation on 31 December 2008 and any subsequent changes to European regulations or ICAO provisions are not taken into account.

From the EUROCONTROL viewpoint, the APOSC is considered as an *ATM* Safety Case. In this context, APOSC (and ACAS) need only comply with regulatory requirements and standards applicable to *ATM* Safety Cases and not those applicable to certification/operational approval of avionics systems on civil aircraft. In particular, the APOSC does not seek to demonstrate that ACAS complies with safety targets applicable to aircraft operations in general, or those applicable to avionics equipment.

The APOSC is based upon operations following completion of the transition period for implementing Phase 2 of the European ACAS II Policy. Operational use of ACAS is defined by ICAO provisions[4] [3][5] as superseded by the relevant amendments [6][7][8]. Since all aircraft subject to the Policy are equipped with TCAS II Version 7.0, the Safety Case exclusively[5] addresses ACAS II as defined by the TCAS II specification [9].

The APOSC addresses only the functional safety of ACAS operations. By implication, it covers the human and procedural aspects of mid-air collision avoidance using ACAS, as well as the ACAS equipment itself. Airworthiness of equipment (including the associated maintenance aspects) is not considered because it is deemed to be adequately covered by standard avionics design, certification and support practices.

The APOSC is not limited to the effects of ACAS on mid-air collision avoidance; it addresses the implications of ACAS on all other aspects of aviation safety, as elicited from ACAS-related documentation. However, there is no claimed relationship between the APOSC and any other existing ATM or aviation safety case.

The safety of ACAS operations is dependent upon all levels of specification for the system, as well as the implementation of the equipment, human and procedural elements of the system in accordance with those specifications. However, some of the direct evidence necessary to support all strands of the safety argument is impracticable to assess within the scope of the Safety Case because of its extent, and because it is not readily available to EUROCONTROL. Consequently, the assurance that ACAS operations conform to the Safety Requirements relies partly on a detailed assessment of the ICAO ACAS provisions with which the international aviation community is obliged to comply, although evidence from operational experience is also taken into account.

As well as addressing current ACAS operations, the APOSC aims to provide assurance of safety in the future. However, such assurance would be inadequate if it were based on similarity between future operations and Phase 2 of the European ACAS II Policy. Therefore, the contents of the APOSC need to be reviewed, and updated if necessary, whenever significant changes are made to ACAS or its operational environment.

[4] See Appendix L hereto for a summary of all of the ICAO ACAS Provisions

[5] TCAS II is the only system commercially available that corresponds to the requirements for ACAS II in ICAO Annex 10. In principle, the ACAS II requirements could be satisfied by solutions other than TCAS II. However, such solutions do not yet exist and therefore are automatically excluded from the scope of the Safety Case.

1.4 Purpose

The APOSC is intended for use by all organisations that have an interest in ACAS operations, as follows:

- EUROCONTROL ATC, safety and surveillance activity areas, which need to satisfy themselves that the implementation of the European ACAS II Policy is safe;
- other EUROCONTROL activity areas, which need to assess the implications of new ATM concepts (systems or operational environments) on the safety provided by existing functionality such as ACAS;
- EASA, which is concerned with safety regulation;
- ECAC States' Civil Aviation Authorities, which are concerned with safe aircraft operations in their airspace;
- ECAC ANSPs, which need to take into account any adverse effects of ACAS on their service provision (as part of demonstrating ESARR4 compliance), and conversely, need to determine the effects on ACAS from changes to their service provision;
- ACAS stakeholders[6], which need to be aware of the potential implications on safety of any future changes to ACAS;

1.5 Style of Presentation of Safety Case Material – IMPORTANT

It is very important to note that when an argument is first introduced, as in section 5 and the initial parts of sections 6 to 9, the fact the argument "asserts" something to be true does NOT itself mean that the available evidence shows that it actually is true – for this it is necessary to refer to the presentation of the evidence (and the conclusions) in the remaining parts of sections 6 to 9.

This is not an anomaly. On the contrary, it is a deliberate strategy that the argument should not be limited to, or conditioned by, the available evidence – rather, the arguments in total should represent the ideal conditions for satisfying the top-level Claim and the safety case should then assess the extent to which the available evidence satisfies these conditions. By this means, any weaknesses or gaps in the safety case become more readily apparent.

1.6 Document Structure

Section 2 describes what ACAS is, and how it is represented via different levels of specification.

The applicability to the APOSC of safety regulatory requirements and other standards is explained in section 3.

Section 4 describes where ACAS fits into ATM and explains the risk concepts that form the basis of the safety argument.

Section 5 presents the high-level safety argument for ACAS.

[6] including EUROCONTROL Mode S and ACAS Programme, ICAO, EASA/JAA, FAA, RTCA, EUROCAE, ARINC, ANSPs, Aircraft Operators, and aircraft and equipment manufacturers

Sections 6 to 9 cover the decomposition of, and presentation of evidence for, the four principal safety arguments that address respectively:

- safety **specification**, from an *a priori* safety assessment,
- **implementation** of the specification, through ACAS standards produced by ICAO, RTCA etc,
- experience from the **operational use** of ACAS,
- ensuring the **future** safety of ACAS.

The caveats that have influenced the conclusions of the Safety Case are listed in section 10.

Section 11 presents conclusions about the safety of ACAS operations.

Sections 13 and 14 contain any special abbreviations used by the APOSC, and the bibliographic information for evidence items and other documentation cited within the document.

Appendices B to H, and J, contain the detailed descriptive material and further analyses used to support the safety argument.

Appendix I presents a brief analysis of four accidents in which ACAS was a contributory factor.

2 SYSTEM DESCRIPTION

2.1 ACAS Specification

The definition of ACAS and its operational aspects is formally captured in a number of ICAO documents. Each of the relevant ICAO Annexes and Procedures, however, captures only an individual aspect of ACAS operations in line with the scope of the particular document. Consequently, there exists no conceptual description of ACAS operations which can be used as the starting point for the safety argument.

Moreover, a change to ACAS operations must be introduced via the related ICAO documents by modifying the requirements for the affected elements within the design of the overall system. As there is no overall conceptual description of ACAS operations to provide a means of verifying that such a change is consistent with the rest of the design, it means that a change to an ICAO document could in principle introduce a potentially unsafe inconsistency with the other elements in the design, or could unwittingly depart from an aspect of the established, albeit implicit, concept.

For the two reasons stated above, EUROCONTROL has seen it necessary to produce an overall conceptual description of ACAS as an integral part of its Safety Case. This feature will permit EUROCONTROL to use the APOSC as a means for proposing or assessing changes to ACAS throughout its operational life.

The overall conceptual description comprises two higher level representations of ACAS which sit above the level of the ICAO documents; namely the ACAS Fundamentals and the ACAS Design. The ACAS Fundamentals capture the purpose and the basic principles of ACAS operations without consideration of how they are implemented. The ACAS Design on the other hand represents the established solution to satisfying the Fundamentals using the physical elements of the aviation system. The Design is also used within the Safety Case as the basis for deriving a set of Safety Requirements for ACAS operations.

The Fundamentals and Design have both been created by abstraction of information from ICAO and other existing ACAS documentation. As part of the APOSC, the consistency between the Safety Requirements and the ICAO documents have been assessed as a means of demonstrating herein that the ICAO regulations are internally and mutually coherent. Therefore, the Fundamentals, Design and Safety Requirements provide the essential bases for arguing that there is a coherent definition of ACAS at the ICAO level, even though they have been created by abstraction.

The term *specification*, as used herein, means the definition of ACAS operations via the Fundamentals, Design and its associated Safety Requirements in sections 2.2, 2.3 and Appendix B, respectively. It follows that the APOSC considers any definition of ACAS operations below the level of ACAS Design as being part of the *implementation* of the ACAS specification. Specifically, these levels comprise ICAO regulations, regional regulations and detailed specifications (plus the physical implementation in airborne equipment), and the documentation and creation by individual organisations of those elements in sections 2.3.2 to 2.3.7 which are affected by the introduction of ACAS. The various levels of definition of ACAS are depicted in Figure 1.

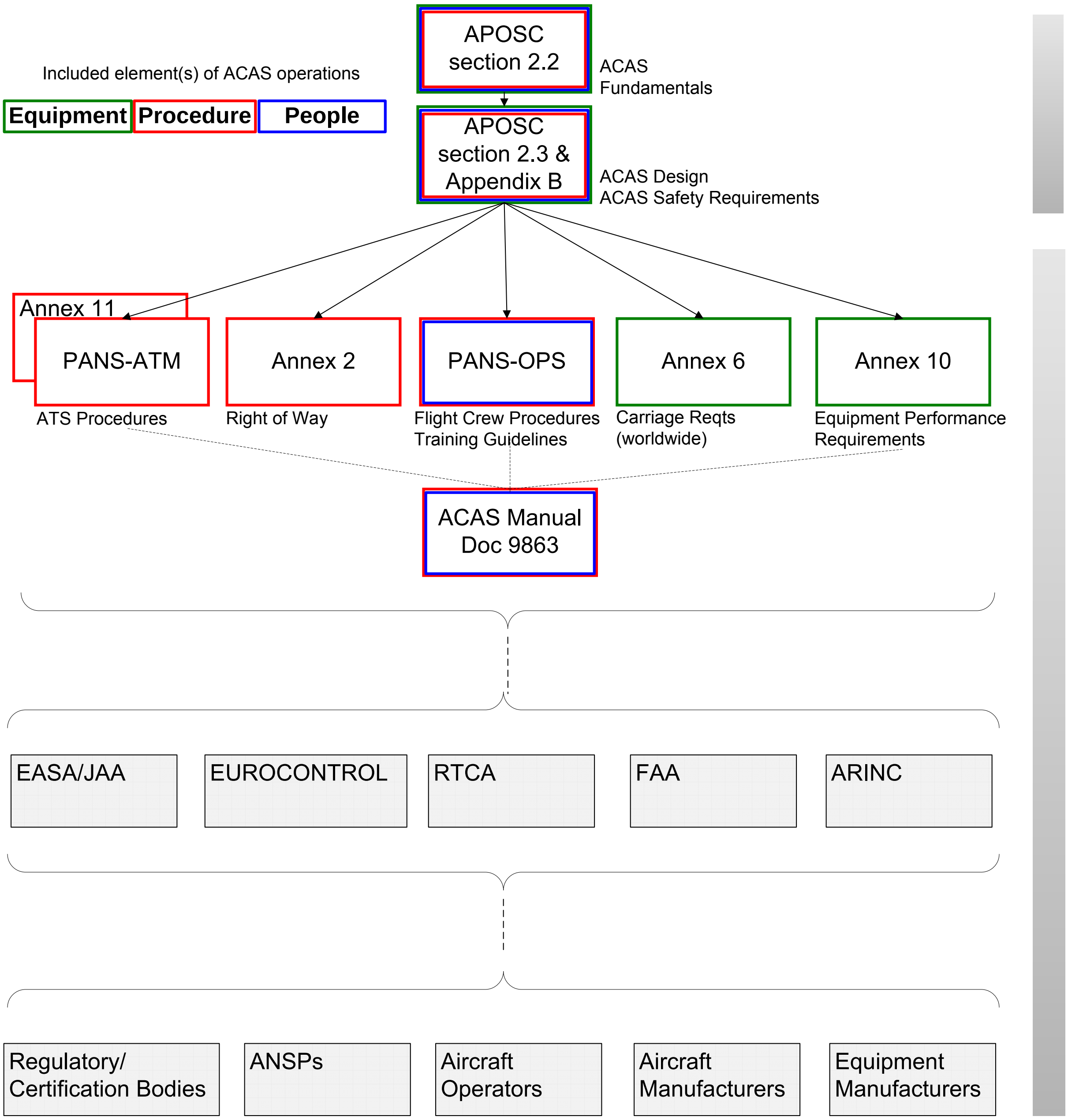


Figure 1 ACAS Levels of Definition

Section 2.2 describes the ACAS Fundamentals. Section 2.3 goes on to describe the ACAS Design, which is an interpretation of the Fundamentals, using a *logical* representation of the collision avoidance architecture and its elements.

At the highest level of implementation, the ICAO documents address those elements in the Design that need to have specific functionality to support ACAS operations, as follows:

- ACAS and transponder performance requirements are defined in ICAO Annex 10 [11].
- Actions by Flight Crew in response to ACAS indications are defined in ICAO Doc 8168 [3] as superseded by Amendments 2 and 3 [6][8]. The relationship between the use of ACAS and other means of collision avoidance by Flight Crew is addressed in ICAO Annex 2 [12].

- Requirements for carriage of ACAS II in the ECAC region (and worldwide) are defined in ICAO Annex 6 [3]. In addition, ICAO Annex 6 [3] and Annex 11 [13] include requirements for carriage and operation of altitude-reporting transponders compatible with ACAS.
- ICAO Doc 4444 [5], as modified by Amendment 5 [7], includes the procedural requirements applicable to air traffic controllers with respect to ACAS and the phraseologies to be used during ACAS-related pilot and controller interchanges.
- ICAO Annex 11 and Doc 4444 both specify that the necessity for an Air Traffic Service, and its supporting procedures, is not to be influenced by the carriage of ACAS[7].

2.2 ACAS Fundamentals

2.2.1 Purpose

The purpose of ACAS is to provide a means of significantly improving the safety of aircraft operations by detecting and resolving potential mid-air collisions by superior means than the existing functions of Separation Recovery by ATC and See & Avoid by Flight Crew.

2.2.2 Environment

ACAS operates in all classes of airspace and during those phases of flight in which it is capable of reliably detecting and safely resolving mid-air collisions. Hence, it does not operate when the aircraft is close to, or on, the ground.

2.2.3 Collision Avoidance

The timing and nature of the ACAS collision-avoidance action is dictated by a compromise between the following objectives:

- to reduce the risk of collision
- to allow time for accurate detection of a potential collision and formulation of resolution guidance
- compatibility with the minimum Flight Crew and airframe capabilities in the environment of use
- to minimise the required deviations in aircraft attitude, body rates and acceleration in order to avoid stress on occupants and airframe
- the need to accommodate unpredictable movement of the other involved aircraft
- to minimise the displacement from flight path in order to avoid consequential loss of separation with third-party aircraft, provided this can be achieved while meeting the other objectives.

To satisfy these objectives, the collision-avoidance principle comprises the following:

- collision avoidance is initiated using a relatively benign control action and, allowing for variability in Flight Crew response, at the latest time

[7] This is in line with the regulatory stance that safety nets must not be used as a reason for relaxing the safety levels provided by other parts of the ATM system.

commensurate with collision-avoidance efficacy and a tolerable level of unnecessary manoeuvres

- the nature of the avoidance action can change during the course of collision avoidance
- the avoidance action is confined to the vertical dimension of motion due to technical limitations in horizontal tracking. The vertical dimension also provides for more effective resumption of separation provision after completion of the action.

2.2.4 Segregation

Since a potential mid-air collision can generally be attributed to a failure of separation provision, ACAS must operate autonomously and independently of the ATM system (which provides *inter alia* the Air Traffic Service) so that it:

- is unaffected by the behaviour of the Air Traffic Service leading up to the potential collision;
- does not rely on any part of the ATM system in order to provide its collision avoidance function;
- is unaffected by interference from the Air Traffic Service while resolving the collision;
- does not interfere with provision of the Air Traffic Service to non-involved aircraft[8].

In the context of the APOSC, the need for a segregation principle is formally demonstrated via the ACAS risk model because ACAS is shown to be a mitigation for hazards produced by (or not removed by) the ATM system[9].

The need for rapid detection/resolution of potential collisions and complete segregation from the ground-based elements of the ATM system leads to a solution which is completely self-contained to the aircraft involved in the potential collision.

2.2.5 Prioritisation

Collision avoidance using ACAS needs to be prioritised with respect to certain other functions on the aircraft. Even though it provides a last resort against a potential mid-air collision, it does not take priority over, and should not interfere with, the need to rectify situations which present an even higher risk of accident to the aircraft.

Similarly, rectifying those situations which have less likelihood than potential mid-air collision to lead to an accident must not take priority over, or interfere with, ACAS.

Although a purpose of ACAS is to provide a superior means of collision avoidance than See & Avoid, there is no explicit prioritisation between the two functions.

In advance of the collision avoidance action, ACAS provides a warning of the presence of traffic in order to alert Flight Crew to the situation. At this stage, there is no ACAS-initiated collision avoidance and therefore no prioritisation aspect to consider.

[8] The ACAS specification contains extensive technical provisions to prevent transponder interrogations by ACAS from disrupting the surveillance service provided by ground-based radars. This feature of ACAS is not discussed further in the APOSC.

[9] and, for certain ACAS hazards, *vice versa*.

2.2.6 Universality

Mid-air collision avoidance depends upon an aircraft having the capability to determine the relative motion of the other aircraft and upon how well it uses relative-motion information to produce an avoidance action. The formulation of collision avoidance guidance arises from algorithms which need to take into account the range of possible movements of the ACAS-equipped aircraft and the other involved aircraft.

Collision-avoidance guidance is produced by equipment, and involves sensors and algorithms on an ACAS-equipped aircraft, and communications between complementary equipment on the other involved aircraft. Due to the fact that ACAS relies upon compatibility and predefined interaction between the equipment on both aircraft, the concept depends on equipment specifications which are applicable worldwide since the involved aircraft might originate anywhere.

For simplicity, the algorithms neither detect, nor adapt their parameters to, aircraft type. Therefore, the efficacy of the algorithms needs to be robust against variability in aircraft-manoeuvring capability and Flight Crew performance. It follows that the collision-avoidance solutions produced by the equipment as a result of its specifications, and the pilot’s ability to react to the resolution guidance, must be compatible with the wide range of airframes and operational environments to which ACAS will be exposed.

2.2.7 Deployment

ACAS deployment has been progressive and over a timescale commensurate with the capabilities of the implementers, users, and certification authorities worldwide.

In order to deal with progressive introduction of ACAS, the system needs to be effective under conditions of partial equipage by aircraft. Therefore, ACAS needs to be effective in providing collision avoidance in the presence of varying levels of relative motion and collision avoidance functionality on the aircraft involved in the potential collision (eg Transponder capability).

2.2.8 Functional Model

At an abstract level, mid-air collision avoidance functionality is represented on the Functional Model given in Figure 2 below.

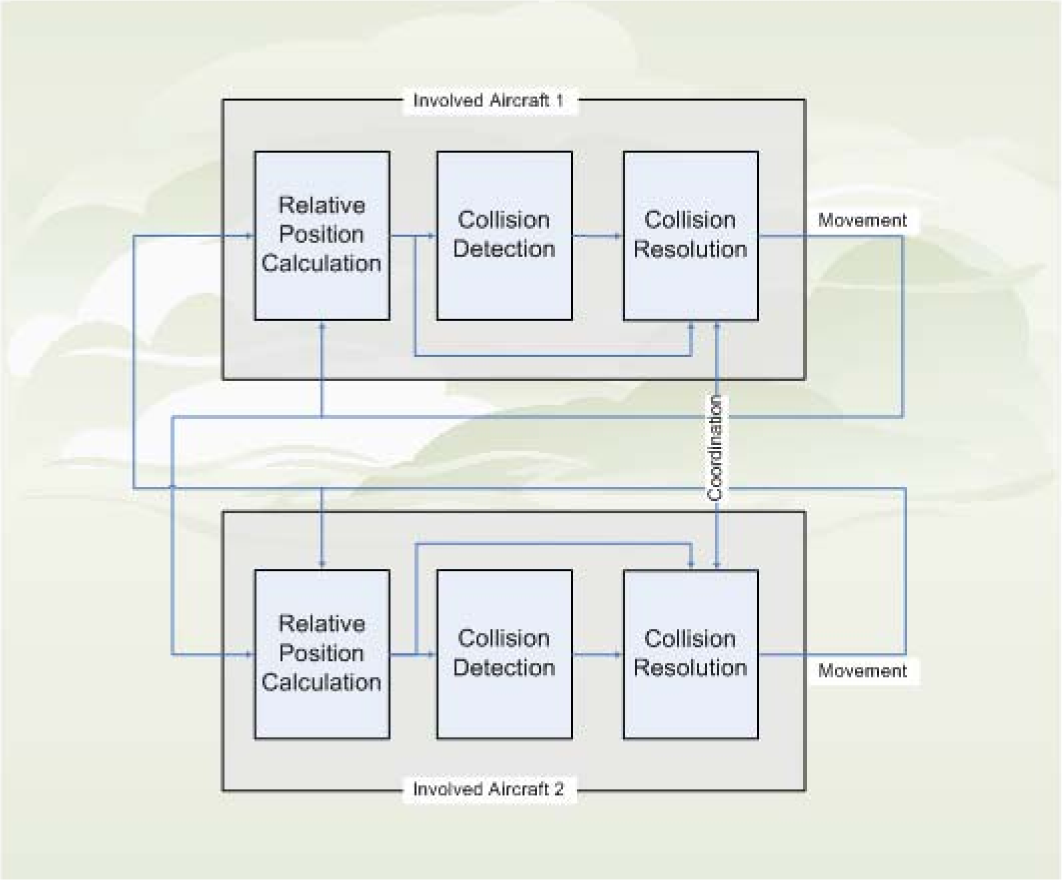


Figure 2 Collision Avoidance Functional Model

This model depicts collision avoidance as being the result of aircraft movement arising from four basic functions on each of the involved aircraft.

Relative position calculation on each aircraft continually computes the relative range and velocity in three dimensions of other aircraft in the surrounding airspace with respect to the involved aircraft (although the model only shows two aircraft for the sake of simplicity and to highlight the Coordination function described below).

Collision detection calculates which other aircraft could potentially collide with the given aircraft by taking into account their projected motions using a tracking algorithm.

Collision resolution is triggered by the collision detection function. Collision resolution calculates the action required to ensure that a collision is avoided between one pair of aircraft. This function takes into account other aircraft to ensure that the resolution will not immediately result in a potential collision with a third aircraft. Collision resolution can be preventative (for example, the resolution may be to continue the rate of climb or descent for one aircraft) or corrective (the resolution is to change the current rate of climb or descent). This function operates according to the principles set out in section 2.2.3 above).

Coordination of the collision resolution action between the two aircraft enhances the effectiveness of collision resolution by ensuring that the movements of the two involved aircraft are in the opposite sense (in the case where the resolution involves both aircraft).Therefore, the functionality involves interdependency between aircraft.

Movement of the aircraft in the vertical dimension results from the output of the collision resolution function such that a potential collision is avoided. Either one or both aircraft involved in a coordinated encounter can move depending on the output of the collision resolution function.

2.3 ACAS Design

2.3.1 Logical Architecture

The total ACAS system depends upon the human element of the system, the Flight Crew, making the final decision on collision-avoidance action. ACAS operations exploit the capability of equipment to rapidly detect conflicts and provide guidance for resolving them, in combination with the capability of humans to correctly prioritise the application of such guidance depending on their perception of the conditions at the time it is provided.

It follows that ACAS does not provide complete collision-avoidance functionality in itself, but does so via the actions of the Flight Crew, and the effect of those actions on movement of the aircraft. An implication of ACAS providing collision avoidance in this way is that the collision-avoidance function is not totally independent of the separation-provision function provided by ATC because it too acts via the Flight Crew.

A logical model, which identifies the elements that provide collision-avoidance functionality, is shown in Figure 3. Interactions between the elements, and between the collision avoidance function and its environment, are also shown.

Within this model, ACAS performs the relative-position calculation and collision detection previously shown in 2.2.8, whereas collision resolution is performed by the combination of ACAS, Flight Crew, and airframe.

Descriptions of the logical elements of the architecture and its environment are provided in sections 2.3.2 to 2.3.8 below. Traceability of the Functional Model to the Logical Model is shown in Appendix J.

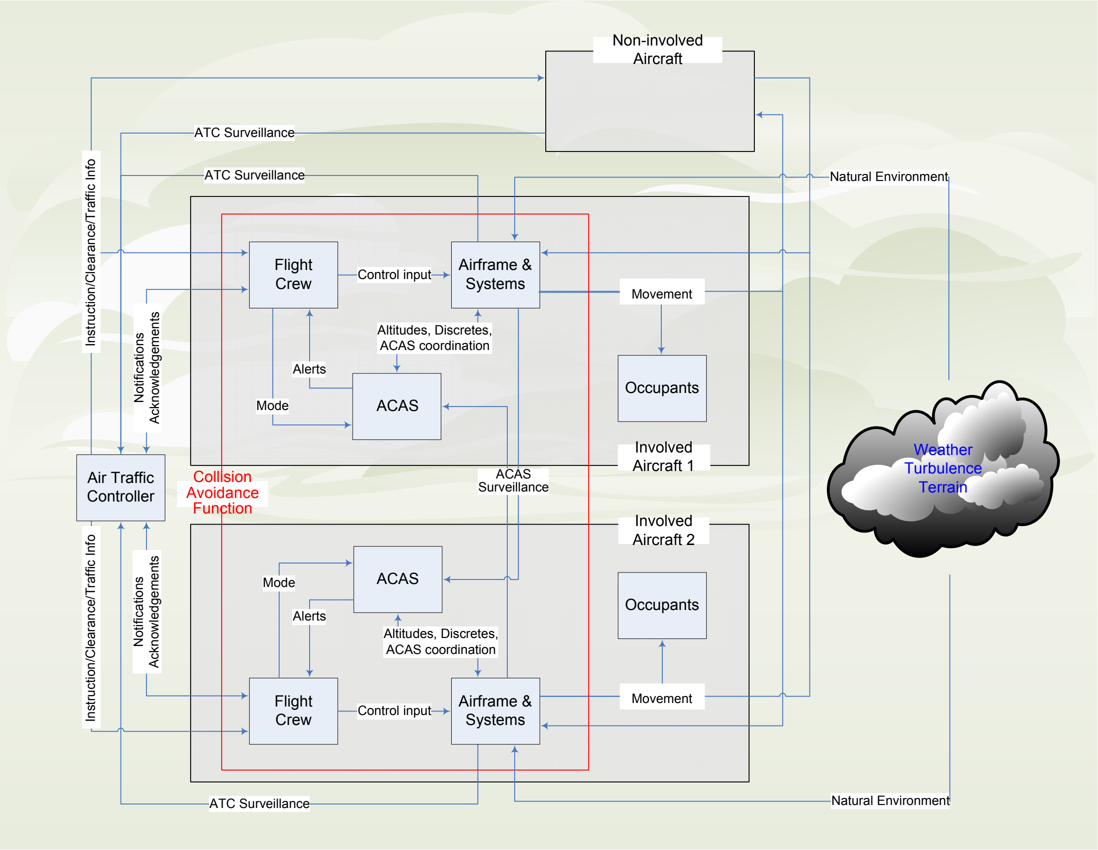


Figure 3 Collision Avoidance Logical Model

2.3.2 ACAS

Note that in this Logical Model diagram, the “ACAS” box means the ACAS equipment on board the aircraft. ACAS alerts pilots to collision threats from other aircraft by interrogating the transponders of all aircraft in the vicinity, and calculating resolution action if it diagnoses that there is potential for collision.

ACAS II [11] represents a type of ACAS functionality which provides vertical Resolution Advisories (RAs) in addition to Traffic Advisories (TAs). It performs the following functions:

- surveillance
- generation of TAs
- threat detection
- generation of RAs
- coordination
- communication with ground stations.[10]

Advisories are triggered when a range test and an altitude test are both satisfied. These tests are performed on each altitude-reporting target every second.

[10] This function is not used as part of ACAS operations in ECAC airspace, although is one possible method of implementing RA Downlink.

Advisories are triggered at a given time before the closest point of approach. The time depends on the flight level of the aircraft, and is a maximum of 35s.[11]

The initial strength of an RA is selected to satisfy an altitude separation goal at closest approach, where this goal varies as a function of flight level. During the course of an encounter, the required advisory strength is continuously evaluated and can be modified either by strengthening, weakening, or reversing the RA.

At the physical level, the ACAS equipment comprises a computer unit, control panel, two antennas, screens and loudspeakers. Collectively, these provide the necessary interfaces with:

- the aircraft's transponder
- the transponders on other aircraft
- the Flight Crew
- the barometric altimeter
- the radar altimeter
- landing gear and flap status, operational performance ceiling, etc.

Currently, ACAS is **not** connected to the autopilot or the FMS[12]. ACAS remains independent and will continue to function in the event of the failure of either of these systems.

ACAS automatically curtails its alerts during aircraft operation close to, or on, the ground. This is because in the associated phases of flight, a *mid-air* collision avoidance action proposed by ACAS is operationally inappropriate (eg during final approach[13]/landing/taxiing), or could even induce an accident (eg a descend RA near the ground). Therefore, ACAS alerts are suppressed according to the following criteria [1]:

- no increase-descent RAs below 1450 ft radio altitude[14] when descending, and 1650 ft radio altitude when climbing
- no descend RAs below 1000 ft radio altitude below when descending, and below 1200 ft radio altitude when climbing
- no RAs below 900 ft radio altitude when descending, and below 1100 ft radio altitude when climbing
- no aural alerts (TAs) below 500 ft radio altitude
- no RAs against aircraft that are determined to be on the ground

For safety reasons, stall warnings, ground-proximity warnings and windshear warnings take precedence over ACAS RAs [1]). When one of these warnings is active, ACAS will automatically switch to a TA-only mode of operation in which the aural annunciations will be inhibited. ACAS will remain in this mode for 10 seconds after cessation of ground-proximity and windshear warnings. The requirement for these inhibitions on ACAS operation originates from certification/operational

[11] The use of time to closest approach is employed to compensate for inaccuracies in relative position calculation and tracking, thus the aircraft do not need to be on a true collision course to cause an RA.

[12] It is understood that coupling of ACAS II to the autopilot (so-called "AP/FD ACAS" function) has been certified for the Airbus A380 – however, this is outside the current scope of the APOSC and should be the subject of a further safety assessment.

[13] Mid-air collision avoidance action on final approach initiated by Flight Crew and possibly involving a horizontal manoeuvre would of course be operationally appropriate.

[14] As determined by the radio altimeter.

approval requirements for avionics systems on civil aircraft and is reflected in the Prioritisation principle, see section 2.2.5.

2.3.3 Flight Crew

Flight Crew manually select the appropriate operating mode of the ACAS equipment during flight, and deactivate ACAS during those situations in which equipment operation is undesirable. In particular, ACAS should be completely deactivated by Flight Crew when the aircraft is on the aerodrome and not occupying the runway [1].

The operating modes are as follows:

STBY places Mode S transponder and ACAS system in standby.

ALT OFF activates transponder without altitude reporting. ACAS system is in standby.

ALT ON activates transponder with altitude reporting. ACAS system is in standby.

TA - Traffic Advisory mode. Presents traffic location on TA display but does not issue Resolution Advisories. TA mode annunciation appears on displays. Activates transponder and altitude reporting.

TA/RA - Traffic Advisory and Resolution Advisory mode. Presents traffic location on displays and issues audio and visual Resolution Advisories for traffic that is determined to be a threat. TA/RA mode annunciation appears on display. Activates transponder and altitude reporting.

On receipt of a TA or an RA in flight, Flight Crew must respond accordingly. On receipt of a TA, pilots are alerted to use all available information to prepare for appropriate action if an RA occurs subsequently. This is intended to include visual acquisition of the threat aircraft prior to the RA. In the event of an RA, the pilot is required to follow the RA, using inputs to the flight controls, unless to do so would jeopardize the safety of the aircraft [3].

2.3.4 Airframe & Systems

The airframe is considered to be part of the Design because it provides the movement necessary to avoid a collision. The capabilities of those airframes which fall within the European ACAS II Policy therefore need to be accommodated within the design of the collision avoidance algorithms. However, aside from equipment carriage aspects, there are no specific airframe requirements (such as functionality, performance or integrity) arising from the introduction of ACAS.

For the purposes of the Safety Case, the airframe is also considered as being part of the environment. This is necessary in order to allow any potentially hazardous effects of ACAS on the airframe to be included in the risk assessment.

As explained in section 2.3.2, ACAS depends upon the presence of a compatible transponder. However, since the technical and carriage requirements for transponders are addressed outside of the ACAS specifications by the relevant sections of [3] [11] [13], consideration of the functionality, performance and integrity of the transponder is deemed to be outside the scope of the Safety Case.

There are no specific requirements on any other aircraft systems, as listed earlier under section 2.3.2, arising from the introduction of ACAS. These systems are considered to be part of the environment.

2.3.5 Operational Environment

The operational environment addressed by the APOSC is ECAC airspace following completion of the transition period for implementing Phase 2 of the European ACAS II Policy. ,

All civil fixed-wing turbine-engined aircraft having a maximum take-off mass exceeding 5,700 kg or a maximum approved seating configuration of more than 19 must carry ACAS II. Any aircraft which is subject to the ACAS II Policy and is not equipped with ACAS II[15] either cannot fly in ECAC airspace, or (exceptionally) must have an exemption. Aircraft not subject to the Policy (ie light aircraft), but equipped with versions of ACAS which are not compliant with the ACAS II requirements, are allowed to fly in ECAC airspace without requiring an exemption.

Due to this deployment strategy, the following equipage scenarios exist for any given encounter[16]:

- both aircraft are ACAS II equipped
- one aircraft is ACAS II equipped and the other aircraft is not ACAS II equipped[17] but has an operational altitude-reporting transponder (or the other aircraft has ACAS but it is selected to TA-only mode)
- one aircraft is ACAS II equipped and the other aircraft is not ACAS II equipped and does not have operational altitude-reporting transponder
- one aircraft is ACAS II equipped - the other is not ACAS II equipped and has a working altitude-reporting transponder but is not providing altitude reports (it is switched to STBY not to ALT) and thus gives only a TA in the ACAS II equipped aircraft
- neither aircraft is ACAS II equipped

It is a characteristic of ACAS that its predicted collision-avoidance performance is very sensitive to the conditions (eg traffic density, encounter geometries and their frequencies) in the airspace in which it is deployed. Therefore, although the ACAS procedures and equipment cited in the APOSC are used worldwide, it should be emphasised that the APOSC is valid only for ACAS operations in the environment and timeframe specified above. It must not be assumed that the results are generally applicable to other airspaces.

[15] ie those which are totally unequipped, or equipped with TCAS II Version 6.04a (which is not compliant with ICAO Annex 10)

[16] See section 2.3.3 for description of the ACAS operating modes

[17] Wherever it is stated that an aircraft is not ACAS equipped, it should be interpreted as also meaning that the aircraft is ACAS equipped but the equipment is not serviceable, as allowed for in the Minimum Equipment List (MEL) provisions, which currently are as follows:

"*Flying with an inoperative ACAS II is permitted, including within RVSM airspace, provided it is done in accordance with the applicable MEL. The MEL for TCAS II throughout Europe is Class C - 10 days (excluding the day of discovery). Operation under the terms of the EASA-OPS 1 TCAS II MEL has been agreed and accepted by the ECAC Member States. JAA TGL 26 (which is still applicable) states that TCAS II "may be inoperative provided the system is deactivated and secured, and repairs or replacements are carried out within 10 calendar days. Note: Local Authorities may impose a more restrictive rectification interval days."* - see http://www.eurocontrol.int/msa/public/standard_page/ACAS_Equipage_Requirements.html

Additional MEL requirements concerning partial failures are also listed in the TGL 26. Note: the actual MEL period applicable to an aircraft is set by the national authority of the aircraft operator: in German airspace the time period during which TCAS II may be inoperative is reduced to 3 days (refer to German AIP GEN 1.5 para. 5). This applies to all aircraft.

Finally, if flying with an unserviceable ACAS II, then the altitude reporting transponder must be serviceable.

2.3.6 Occupants

The aircraft occupants are considered as being part of the environment. This is necessary in order to allow any potentially hazardous effects of ACAS on the occupants to be included in the risk assessment. However, there are no specific requirements on the occupants arising from the introduction of ACAS.

2.3.7 Non-involved Aircraft

Aircraft which are in the vicinity of the encounter, but not subject to an ACAS alert, are considered as being part of the environment. This is necessary in order to allow any potentially hazardous effects of ACAS on these aircraft to be included in the risk assessment. However, aside from equipment carriage aspects, there are no specific requirements on non-involved aircraft arising from the introduction of ACAS.

2.3.8 Air Traffic Controller

The segregation principle [section 2.2.4] requires ACAS to provide collision avoidance independently of the ATM system, and ATS not to interfere with ACAS. Hence, in the functional model of 2.2.8 above, no interaction between ACAS operations and ATM is shown. However, in the logical model, the Air Traffic Controller is shown as an element external to the Design, which can interact with involved and non-involved aircraft as part of ATS delivery. This interaction is addressed as part of the Safety Argument.

A possible extension to the ACAS system which is under consideration is RA Downlink, which would give the Air Traffic Controller automated information on the controller surveillance display that an aircraft had received an RA, and would therefore supplement the voice reporting of RAs. The stated objective of RA Downlink is to enhance the situational awareness of controllers and reduce the likelihood that instructions which conflict with an RA will be issued. The disappearance of the RA indication from the controller's workstation display would also provide alternative "clear of conflict" information. RA Downlink is currently (2010) being implemented by the Czech Republic (Prague ACC/APP), Luxembourg APP, and Hungary (Budapest ACC/APP).

In the logical model of Figure 3, information on RAs in progress could be modelled as part of the ATC Surveillance data flow.

RA Downlink is **not** included in the scope of the APOSC but some footnotes are included to indicate where the addition of RA Downlink might affect hazard causes.

The Feasibility of ACAS RA Downlink Study (FARADS) has produced a safety summary report [52]. The FARADS FHA/PSSA report is referred to elsewhere in the APOSC for hazard analysis results.

3 SAFETY REGULATORY REQUIREMENTS AND STANDARDS

This section describes the applicability to the APOSC of European safety regulatory requirements and standards. It should be noted that, from the EUROCONTROL viewpoint, the APOSC is considered as an *ATM* Safety Case. In this context, APOSC (and ACAS) need only comply with regulatory requirements and standards applicable to ATM Safety Cases and not those applicable to certification/operational approval of avionics systems on civil aircraft. In particular, the APOSC does not seek to demonstrate that ACAS complies with safety targets applicable to aircraft operations in general, or those applicable to avionics equipment.

3.1 ESARR 4

The APOSC is consistent with the intentions of ESARR 4 [14] and the corresponding provisions of Common Requirement CR 2096/2005 [55] as far as practicable and the risk assessment herein satisfies most of the process requirements in ESARR 4 related to risk assessment and mitigation.

3.2 SRC Policy Document 2

The safety argument herein is consistent with the SRC policy [15] that safety nets cannot be used to demonstrate satisfaction of the tolerable safety minima specified in ESARR 4. Moreover, the risk assessment satisfies the policy that risk assessment and mitigation shall be applied to hazards from safety nets which affect Separation Provision, even though there is no attempt to quantify the hazards using Safety Objectives based on the ESARR 4 safety target.

3.3 EUROCONTROL ANS Safety Assessment Methodology

In order that the results of the work reflect ATM safety management best practice, the risk assessment herein conforms to the relevant parts of the EUROCONTROL ANS Safety Assessment Methodology (SAM) [16], and the APOSC as a whole conforms to the ‘essential’ requirements of the Safety Case Development Manual (SCDM) [17].

4 SAFETY CONCEPTS

4.1 Conflict Management

A suitable starting point for explaining how ACAS contributes to aviation safety is ICAO Doc 9854 [20]. This presents the ICAO vision of an integrated, harmonized and globally interoperable ATM system for the period up to 2025 and beyond. It includes a description of Conflict Management, a key component of the 'emerging and future' ATM Operational Concept, which is:

- aimed at reducing, to [at least] a tolerable level, the risk of collision between aircraft and other aircraft, fixed obstacles etc; and
- applied in three layers: Strategic Conflict Management, Separation Provision, and Collision Avoidance.

How this service-level concept works in practice, and relates to the underlying ATM system (ground and airborne components), can be seen from Figure 4 below.

The input to this simple model is the air traffic, the existence of which represents hazards to, *inter alia*, other aircraft within it.

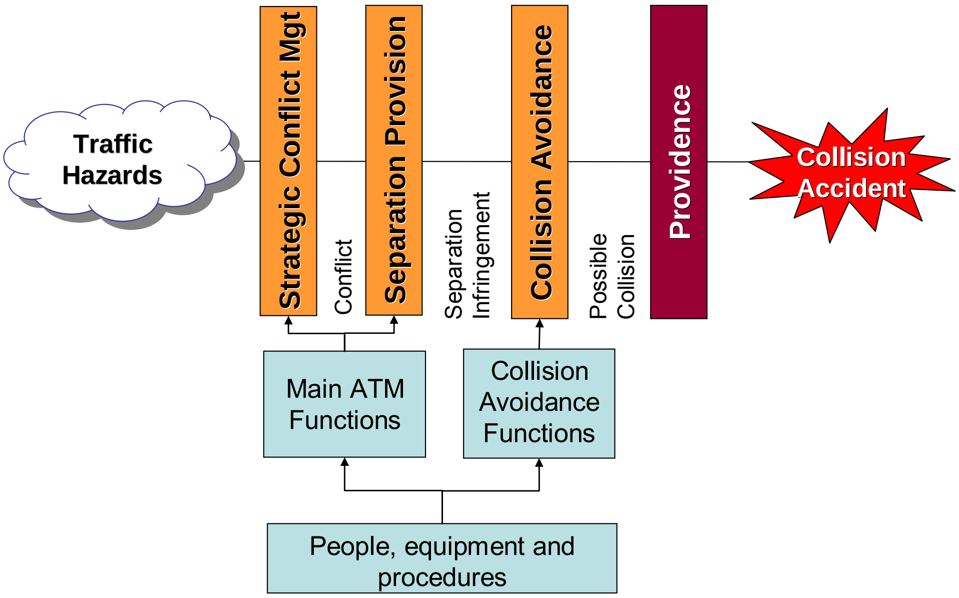


Figure 4 Conflict Management Model

The three layers of Conflict Management identified in Figure 4 can be thought of as barriers which prevent those hazards leading to an accident, and each one has a specific purpose, as follows:

The **Strategic Conflict Management** barrier is provided by the following main ATM functions:

- Airspace design which provides structuring of the airspace so as to keep aircraft apart spatially, in the lateral and/or vertical dimensions

- Flow and Capacity Management which mainly prevents overload of the Separation Provision barrier
- Traffic Synchronisation which involves the tactical establishment and maintenance of a safe, orderly and efficient flow of air traffic.

The **Separation Provision** barrier is the second layer of Conflict Management and is the process of keeping aircraft away from each other, and from fixed obstacles, by at least the appropriate separation minima, by means of tactical intervention. Separation Provision is necessary due to the inherent limitations of Strategic Conflict Management in eliminating all conflicts and may be the responsibility of an ANSP, the airspace user, or a combination of the two.

Collision Avoidance is intended to recover the situation only when the previous two barriers have failed to remove conflicts to the point that there is risk of collision. It can be initiated by either:

- Collision-prevention action by Controllers, often supported by ground-based safety nets such as STCA, or
- Collision-avoidance action by Flight Crew, often supported by airborne safety nets such as ACAS.

The positioning of these collision-avoidance elements with respect to the Conflict Management model is shown in Figure 5. This diagram implies that airborne collision avoidance is independent from (and therefore external to) the ATM system; however this distinction is only important with respect to the applicability of ATM safety regulatory requirements.

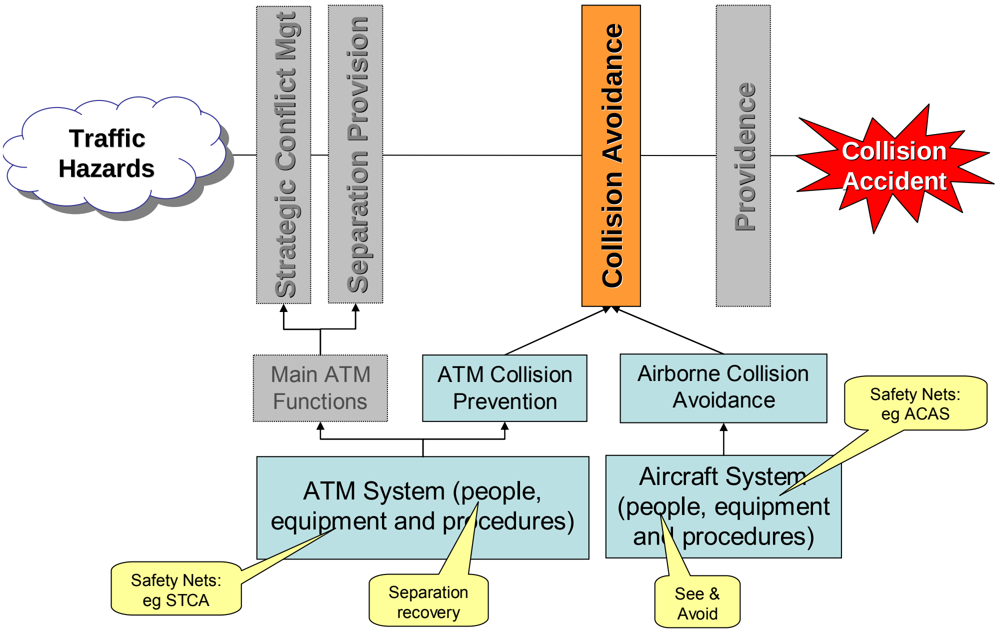


Figure 5 Collision Avoidance Elements

Providence is the final barrier and simply represents the probability that aircraft involved in a given encounter, albeit in close proximity with another aircraft or obstacle, would not actually collide. Although largely a matter of chance, Providence can be affected by such things as airspace design and traffic distribution, and its effectiveness generally decreases as the density of traffic increases with, for example, traffic growth.

4.2 Barrier Risk Contribution

The barriers operate from left to right in a rough time sequence, however one important thing that the barriers have in common is that they are not 100% effective either individually or collectively because of limitations of functionality/performance and/or (occasional) failure. Therefore, each barrier contributes to safety (ie reduces collision risk) by removing *a percentage* of the conflicts[18], which exist in the operational environment. Consequently, a residual risk of collision exists even after the provision of *multiple* barriers. This progressive reduction in collision risk is illustrated in Figure 6.

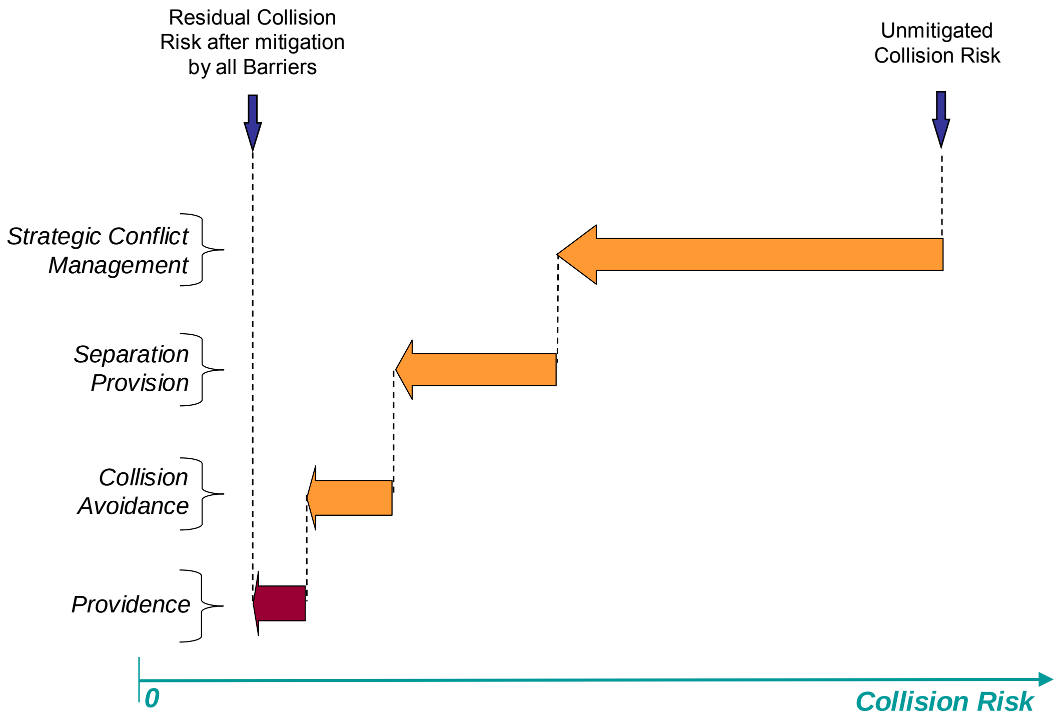

Residual Collision Risk after mitigation by all Barriers
Unmitigated Collision Risk
Strategic Conflict Management
Separation Provision
Collision Avoidance
Providence
0
Collision Risk

Figure 6 Collision Risk Reduction

The ATM system needs to be designed such that the risk reduction from all the barriers is sufficient to achieve a desired level of safety. In ECAC airspace, the desired level of safety is prescribed in ESARR 4[19] [14], however EUROCONTROL policy [15] stipulates that the safety benefit from safety nets cannot be taken into account in demonstrating compliance with the ESARR 4 safety target. It follows that, whereas the aggregate risk reduction from Strategic Conflict Management and Separation Provision is prescribed in regulatory minima (with Providence being implicitly included in the overall safety target set in ESARR 4), no equivalent target

[18] The term Conflict is used herein according to the definition in the ICAO Global ATM Concept [20] – ie “any situation … in which the applicable separation minima may be compromised [infringed]”.

[19] strictly, ESARR 4 prescribes a target for ATM direct contribution to all accidents, not just collisions

exists for the risk reduction afforded by the Collision Avoidance barrier or any of its constituent safety net functions.

4.3 Success & Failure Viewpoints

The degree and extent to which the *man-made* barriers are able to reduce risk (by removing conflicts) depends, in the first place, on the functionality and performance of the various physical elements that underlie each barrier. However, acting against this *intrinsic* risk reduction capability there can be unwanted factors which serve to erode to some extent the safety benefit provided by the barrier. Such factors would certainly include loss of the barrier due to failure of the underlying system components or the external elements on which they rely, but might also include hazards from normal operation of the barrier, and hazards from insidious modes of failure[20]. As a result, the adequacy of the *net* risk reduction afforded by each barrier needs to be argued via both a 'success viewpoint' concerned with intrinsic risk reduction, and a 'failure viewpoint' concerned with the factors that erode it.

The way in which these two components of risk contribute to the effectiveness of the barriers is depicted in Figure 7.

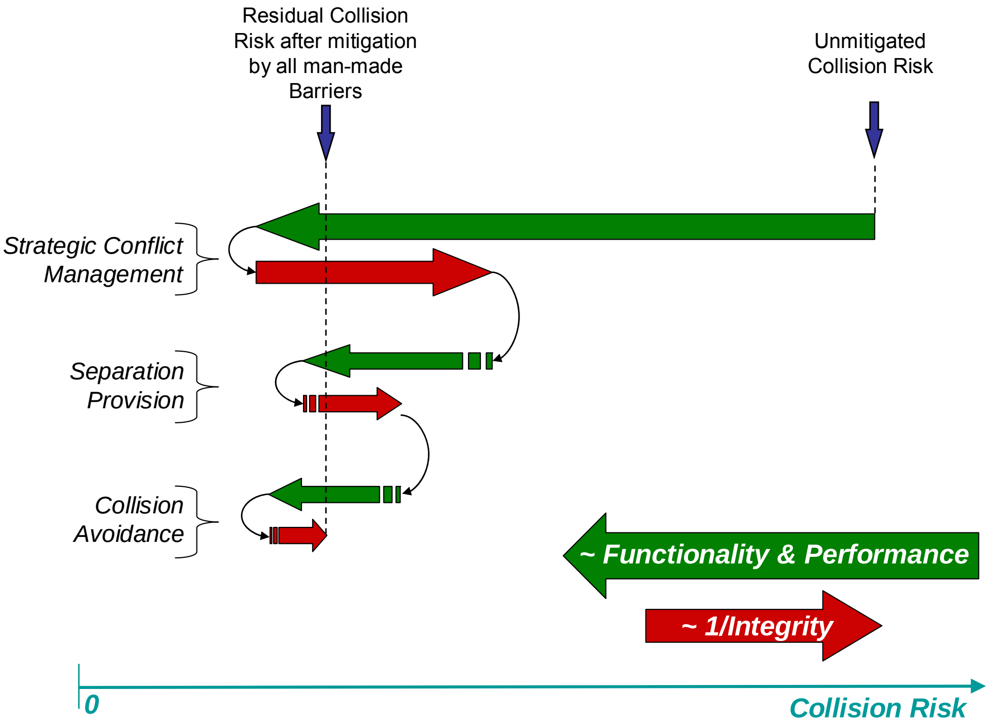

Residual Collision Risk after mitigation by all man-made Barriers
Unmitigated Collision Risk
Strategic Conflict Management
Separation Provision
Collision Avoidance
~ Functionality & Performance
~ 1/Integrity
0
Collision Risk

Figure 7 Barrier Success and Failure Components

4.4 ACAS Safety Concepts

In accordance with the above concepts, it can be seen that ACAS is part of the Collision Avoidance barrier but is implemented entirely within the aircraft system. It could be argued that operations with ACAS are 'safe' if ACAS provides a net safety

[20] Note that the risk increase from Collision Avoidance could in principle exceed the intrinsic risk reduction, thus yielding a negative safety benefit from introducing it as a barrier.

benefit with respect to pre-ACAS operations. Primarily, this means demonstrating that the functionality and performance of ACAS are sufficient to reduce the residual risk of collision[21] that remains as a result of the inherent limitations (or failure) of the preceding barriers *and* the other Collision Avoidance functions. Implicit in this argument is that ACAS should ideally be independent of the operation and physical implementation of the remainder of the ATM system, which supports those preceding barriers; in practice, independence cannot be achieved completely because of the use of the Mode C/Mode S transponder by both the ATM system and ACAS as illustrated by the case of the Brazilian mid-air collision in 2006, summarised in Appendix I, section I.4 below.

However, ACAS also carries with it the possibility of behaviours which have the potential to erode its benefit to aviation safety because they constitute risk-bearing hazards in their own right. These hazards could either diminish the Collision Avoidance capability of ACAS (as part of the ‘failure viewpoint’ discussed in section 4.3) or induce harmful outcomes other than mid-air collision. The latter implies that the safety argument must embrace the effect of ACAS on the risk of *all* types of aircraft accident, not just mid-air collision (MAC).

These principles are illustrated in Figure 8 which shows that mid-air collision is only one contributor to the total risk of an aircraft accident. Other accident types, such as CFIT, are included under Non-MAC Accidents. Therefore, the risk of an accident without ACAS equals the risk of MAC without ACAS plus the risk of Non-ACAS Non-MAC accidents.

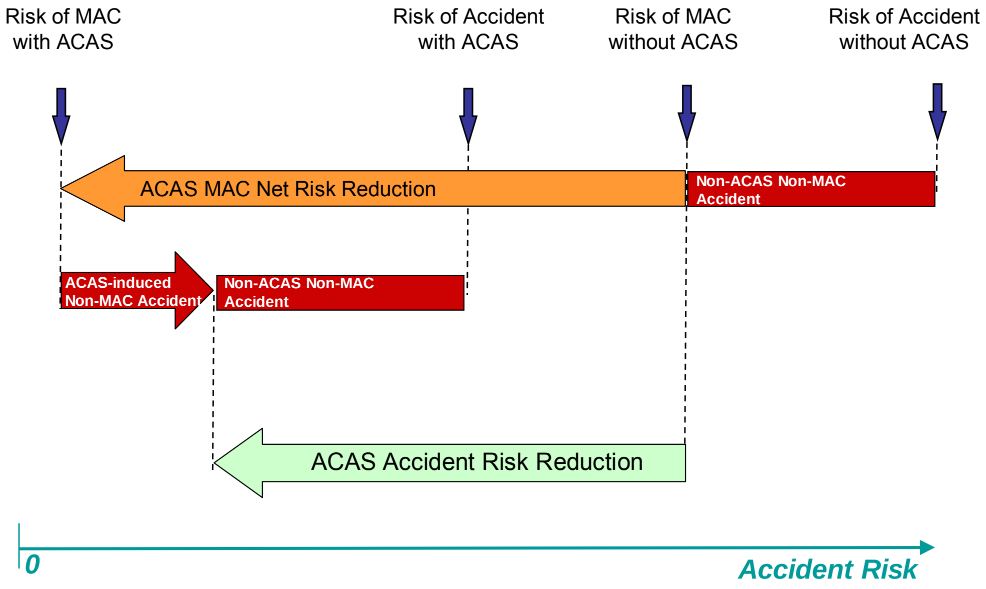

Risk of MAC with ACAS
Risk of Accident with ACAS
Risk of MAC without ACAS
Risk of Accident without ACAS
ACAS MAC Net Risk Reduction
Non-ACAS Non-MAC Accident
ACAS-induced Non-MAC Accident
Non-ACAS Non-MAC Accident
ACAS Accident Risk Reduction
0
Accident Risk

Figure 8 ACAS Accident Risk Reduction

[21] unless otherwise stated, the term ‘collision’ used herein refers only to the mid-air collision component of the Collision Avoidance barrier by default

The introduction of ACAS provides a net reduction in the risk of MAC but might also increase the risk of a non-MAC accident because of its potential to induce these accident types. Therefore, the risk of an accident with ACAS equals the risk of MAC with ACAS plus the risk from (Non-ACAS and ACAS-induced) Non-MAC accidents. Figure 8 shows that the overall accident risk reduction due to ACAS is not dependent on the pre-existing Non-ACAS, Non-MAC accident risk.

Therefore, the Safety Claim for ACAS is based on its ability to provide a net *accident* risk reduction rather than MAC risk reduction alone. Ideally, the accident risk reduction should be *substantial* to have warranted the introduction of ACAS in the first place, and to allow for the uncertainty inherent in quantifying both its intrinsic risk reduction and its risk-bearing hazards.

The propensity for ACAS *in operation* to both reduce risk, but at the same time have potentially hazardous side-effects, originates in its specification. Consequently, the safety argument needs to address the safety properties at each level of definition of ACAS [section 2.1] as well as the observed behaviour of ACAS in service. Since any safety net by definition will be rarely used, it might well be impracticable anyway to argue the achieved risk reduction (and the acceptability of any hazards) based on in-service data due to the vanishingly small event frequencies of interest. Therefore, an *a priori* safety assessment remains essential even for an ACAS *post-implementation* safety case.

5 HIGH-LEVEL SAFETY ARGUMENT

5.1 Safety Claim (Arg0)

The APOSC Safety Claim and high-level argument are presented in Figure 9 below using Goal Structuring Notation (GSN), whose symbology is described in Appendix A. Each evidence reference (circle) identifies the corresponding section in the APOSC where explanatory material, analysis and references to external evidence reports are presented to support the goal. The evidence reference also summarises the nature of the supporting evidence. Interim conclusions are provided at the end of each major argument section (Arg 1.1, 1.2 and so on).

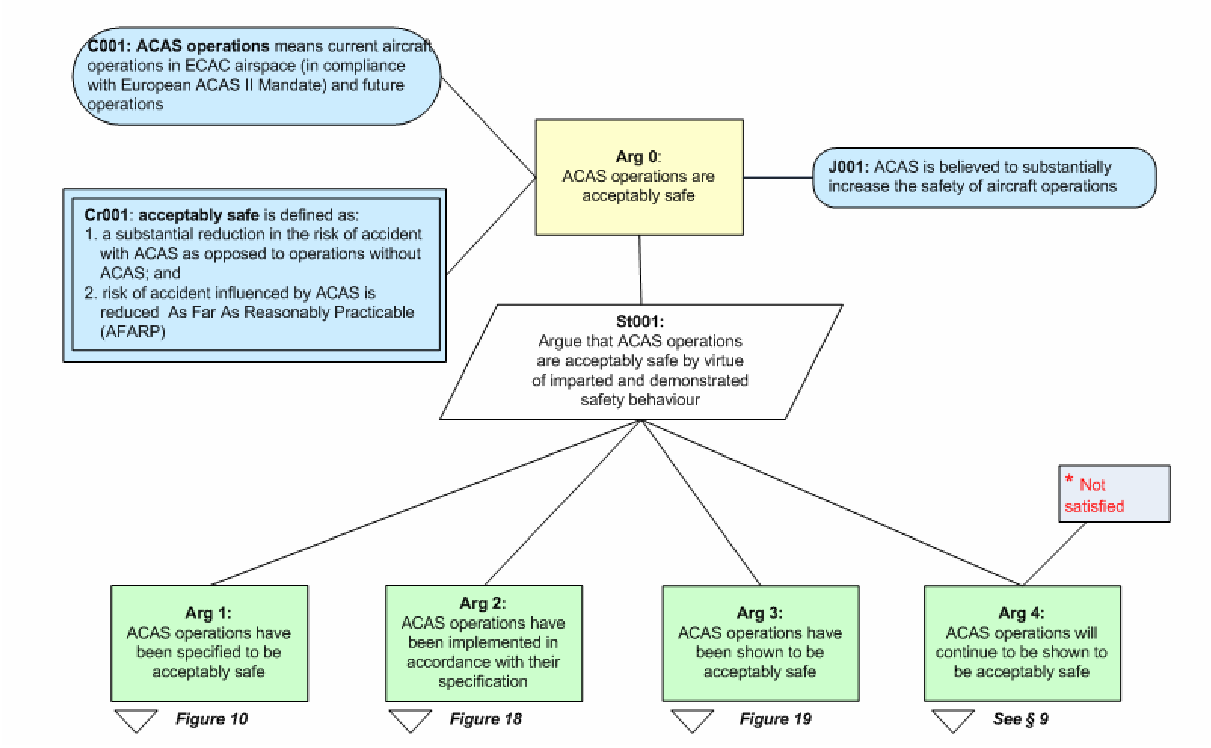

C001: ACAS operations means current aircraft operations in ECAC airspace (in compliance with European ACAS II Mandate) and future operations
Cr001: acceptably safe is defined as:
1. a substantial reduction in the risk of accident with ACAS as opposed to operations without ACAS; and
2. risk of accident influenced by ACAS is reduced As Far As Reasonably Practicable (AFARP)
Arg 0: ACAS operations are acceptably safe
J001: ACAS is believed to substantially increase the safety of aircraft operations
St001: Argue that ACAS operations are acceptably safe by virtue of imparted and demonstrated safety behaviour
* Not satisfied
Arg 1: ACAS operations have been specified to be acceptably safe
Arg 2: ACAS operations have been implemented in accordance with their specification
Arg 3: ACAS operations have been shown to be acceptably safe
Arg 4: ACAS operations will continue to be shown to be acceptably safe
Figure 10
Figure 18
Figure 19
See § 9

Figure 9 High-level Argument

The safety Claim (**Arg0**) is that ACAS operations are *acceptably safe*. Contrary to normal EUROCONTROL practice, this claim has not been extended to read "…and will remain acceptably safe" due to the issues identified in section 9 concerning lack of sufficient evidence to support Arg 4.

The operational context (**C001**) for the Claim is all areas of ECAC airspace in which ACAS functionality[22] is applicable, and equipage reflecting completion of the European ACAS II Policy.

ACAS is intended to reduce the risk of collision independently of the ATM services. Therefore, it can produce a safety benefit regardless of the level of safety being provided by those services[23]. Consequently, the argument does not rely on a supposition of tolerable safety from ATM.

[22] provision of TA or RA alerts
[23] in theory, the less safe are the ATM services, the greater is the scope for ACAS to reduce the risk of collision

5.2 Safety Criteria

What is meant by acceptably safe in Arg0 is defined by the Safety Criteria in **Cr001**.

As described in section 4.2, there is no absolute safety target applicable to the reduction in risk of collision afforded by ACAS operations. ACAS operations can be considered acceptably safe if ACAS provides a reduction in the risk of collision over and above that provided by the ATM services alone, while not adversely affecting the safety of other aspects of aircraft operation. Therefore, the criteria address *accident* risk and not simply the mid-air collision risk. Furthermore, it is important to argue a *substantial* risk reduction because of the uncertainty inherent in quantifying and comparing its safety benefit with any risk-increasing side-effects. That such risk-increasing side effects can and do occur is shown by the analysis given in Appendix I of four accidents where the operation of ACAS was a contributory factor, of which the best known are the Überlingen and Brazil mid-air collisions.

Therefore, the argument uses the following two criteria to define acceptable safety:

1. the risk of an accident with ACAS is substantially lower than without ACAS; and
2. the risk of an accident, as influenced by the operation of ACAS, is reduced as far as reasonably practicable (AFARP).

5.3 Strategy for Supporting the Claim

The Claim is supported by four principal Safety Arguments, using the GSN convention that an Argument can be considered to be true, only if each of its sub-arguments can be shown to be true[24].

Arg 1 asserts that ACAS has been specified to be *acceptably safe*, and is based on a comprehensive, *a priori*, safety assessment[25] which analyses the system in normal operation as well as during failures. The inclusion of such an Argument, despite the fact that ACAS has been in service for a number of years, arises from three main considerations:

- the need to compensate for insufficient documented evidence of the safety performance of ACAS in service
- the need to address the possibility that, despite years of operational experience, there might still be latent problems in the ACAS[26] design
- the need to provide a baseline against which to carry out safety assessment of future developments of ACAS.

Arg 2 asserts that ACAS has been implemented in accordance with the specification. Since APOSC is produced within the scope of EUROCONTROL's safety activities, it is impractical to provide assurance that every responsible body (ie each ANSP, aircraft operator, aircraft manufacturer and equipment manufacturer) has implemented, completely and correctly, the ACAS Safety Requirements that are covered under Arg 1. Therefore, Arg2 is limited to showing that the Safety

[24] At the lowest eventual level of decomposition, of course, an Argument can be considered to be true if there is adequate Evidence to show that it is.

[25] The term *a priori safety assessment* is used in this context to mean an analysis with respect to Success as well as Failure viewpoint

[26] The term *ACAS design* is used in its widest sense herein. It includes not only the aircraft equipment but also the related human and procedural elements, and their interaction with other systems (predominantly, other aircraft systems and ATM).

Requirements are addressed fully by authoritative regulations that the responsible bodies should be aware of and are obliged to comply with (or declare otherwise). This is necessarily supported by an assumption (A003 in section 10.1 below) that the responsible bodies are aware of, and comply with, such regulations.

Arg 3 asserts that ACAS *has been shown* to be acceptably safe in operational service. It is based on two key factors:

- that the overall safety benefit of ACAS has been demonstrated in practice, through safety monitoring
- that measures have been in place (and have been applied effectively) to identify, and eliminate, any safety problems associated with ACAS operations.

Arg 4 asserts that ACAS *will continue to be shown* to be acceptably safe in operational service. This is related to the previous Arguments but is needed in order to show that adequate measures are in place to conduct *a priori* and *a posteriori* assessments of ACAS in the future. Section 9 discusses the reasons for concluding that this argument is not satisfied.

6 SAFETY SPECIFICATION (ARG 1)

6.1 Strategy (St002)

It is the subdivision of Arg 1 which reflects the ‘success’ and ‘failure’ approach to *a priori* safety assessment, as mentioned in section 4.3. This manifests itself through six progressive sub-arguments, as shown in Figure 10, which reflect the different aspects of ACAS success and failure that need to be captured within the ACAS specification **(St002)**.

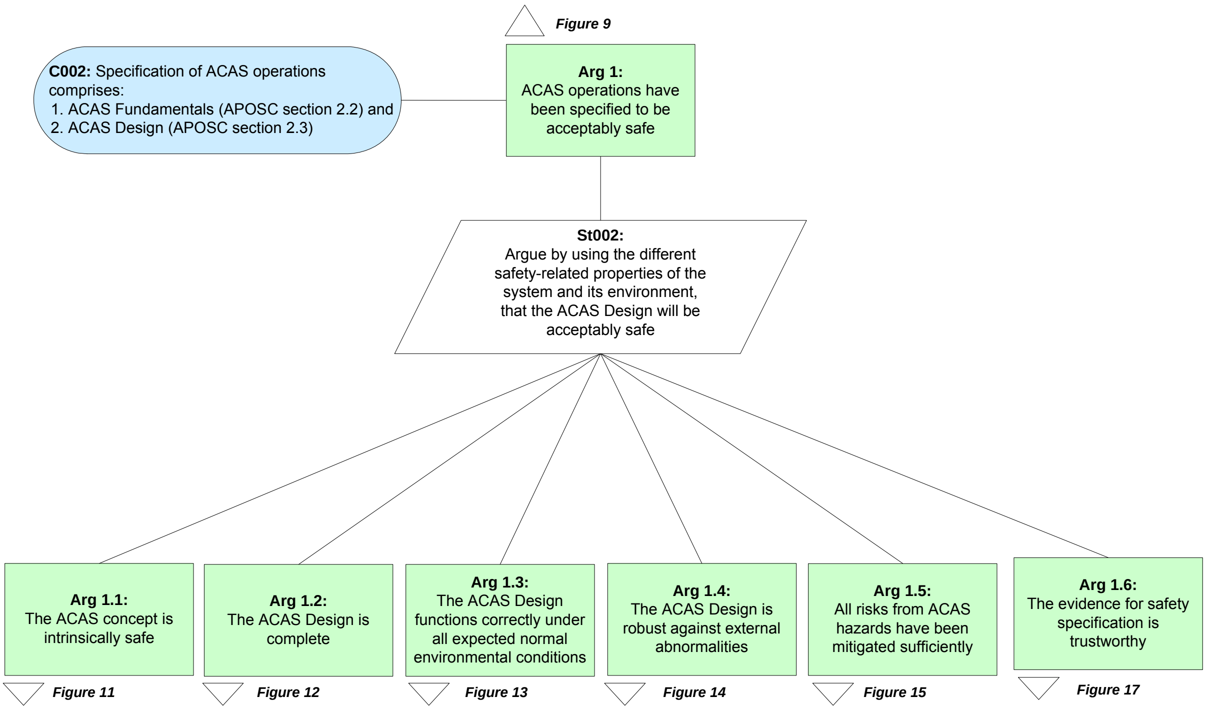


Figure 9
C002: Specification of ACAS operations comprises:
1. ACAS Fundamentals (APOSC section 2.2) and
2. ACAS Design (APOSC section 2.3)
Arg 1: ACAS operations have been specified to be acceptably safe
St002: Argue by using the different safety-related properties of the system and its environment, that the ACAS Design will be acceptably safe
Arg 1.1: The ACAS concept is intrinsically safe
Arg 1.2: The ACAS Design is complete
Arg 1.3: The ACAS Design functions correctly under all expected normal environmental conditions
Arg 1.4: The ACAS Design is robust against external abnormalities
Arg 1.5: All risks from ACAS hazards have been mitigated sufficiently
Arg 1.6: The evidence for safety specification is trustworthy
Figure 11
Figure 12
Figure 13
Figure 14
Figure 15
Figure 17

Figure 10 Safety Specification

The purpose of each sub-argument shown in Figure 10 is as follows:

Arg 1.1 Intrinsic Safety of the Concept

Arg 1.1 asserts that the concept underlying ACAS operations is intrinsically safe; ie that a system design based upon the ACAS Fundamentals has the potential to satisfy the Safety Criteria provided it embodies a set of fundamental parameters. Intrinsic safety is not concerned with the detailed behaviour of the system or its potential for creating hazards.

Arg 1.2 Design Completeness

Arg 1.2 asserts that the ACAS Design is complete. The objective here is to show that the ACAS Design (section 2.3) represents everything that is necessary to fully implement the ACAS Fundamentals (section 2.2). Specifically, it must contain a complete set of Safety Requirements that will permit the implemented system to satisfy the Safety Criteria.

Arg 1.3 Design Correctness

Arg 1.3 asserts that the ACAS Design works correctly under all normal environmental conditions. The objective is to demonstrate that the Design is a correct static and dynamic representation of the ACAS Fundamentals and delivers a substantial degree of collision-risk reduction commensurate with the Safety Criteria when subjected to its normal operational environment.

Arg 1.4 Design Robustness

Arg 1.4 asserts that the ACAS Design is robust against abnormalities in the operational environment, where robustness is the property of safely withstanding those exceptional situations which might cause ACAS behaviour to degrade even though no fault had occurred within the system. The objective is to demonstrate that ACAS operations do not become unsafe under such circumstances because the Design either continues to operate correctly, or its risk-reduction capability is diminished but subsequently recovers. Furthermore, the abnormal conditions would not cause the Design to behave in a way that induces a risk that would otherwise not have arisen.

Arg 1.5 Mitigation of System Hazards

Arg 1.5 asserts that all risks from hazards produced by faults within the system have been mitigated sufficiently within the Design or the environment. Here, the hazardous behaviour of the system is assessed from two perspectives: how loss of functionality could reduce the effectiveness of the system in reducing risk; and how anomalous behaviour of the system could induce a risk that would otherwise not have arisen.

Arg 1.6 Evidence Validity

Arg 1.6 asserts that the Evidence used to support the sub-arguments of Arg 1.1 to 1.5 is trustworthy; ie that it has been produced and checked via reputable processes and personnel.

The breakdown of these six sub-arguments, and the degree and extent to which their supporting Evidence shows them to be true, is described in sections 6.2 to 6.7 below.

6.2 Intrinsic Safety of the Concept (Arg 1.1)

6.2.1 Strategy

In order to argue that ACAS as a concept has the potential to deliver a significant reduction in the risk of mid-air collision, it is necessary to show that, in theory, suitable functionality can be devised which will produce effective collision resolution within many of the scenarios with which ACAS will be faced. The existence of such functionality is argued using the following sub-arguments, as shown in Figure 11:

Arg 1.1.1. The ACAS Fundamentals have been defined.

Arg 1.1.2. The differences from operations before ACAS have been described and reconciled with the Safety Criteria.

Arg 1.1.3. The impact of the concept on the operational environment has been assessed and shown to be consistent with the Safety Criteria.

Arg 1.1.4. The principal functionality and performance parameters associated with the concept have been defined and shown to be consistent with the Safety Criteria.

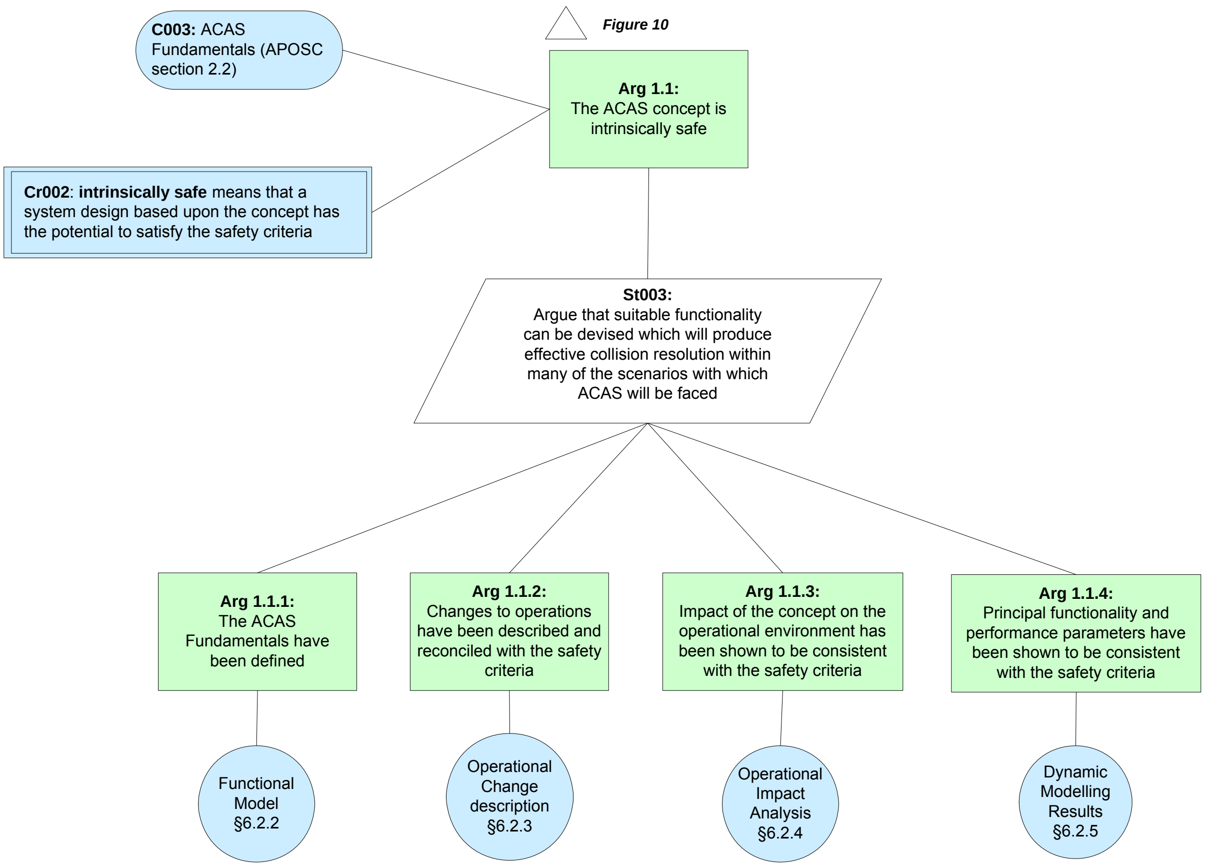

C003: ACAS Fundamentals (APOSC section 2.2)
Figure 10
Arg 1.1: The ACAS concept is intrinsically safe
Cr002: intrinsically safe means that a system design based upon the concept has the potential to satisfy the safety criteria
St003: Argue that suitable functionality can be devised which will produce effective collision resolution within many of the scenarios with which ACAS will be faced
Arg 1.1.1: The ACAS Fundamentals have been defined
Arg 1.1.2: Changes to operations have been described and reconciled with the safety criteria
Arg 1.1.3: Impact of the concept on the operational environment has been shown to be consistent with the safety criteria
Arg 1.1.4: Principal functionality and performance parameters have been shown to be consistent with the safety criteria
Functional Model §6.2.2
Operational Change description §6.2.3
Operational Impact Analysis §6.2.4
Dynamic Modelling Results §6.2.5

Figure 11 Concept Safety

These sub-arguments are addressed in turn, in sections 6.2.2 to 6.2.5 below. Conclusions regarding Arg 1.1 are then drawn in section 6.2.6.

6.2.2 Definition of Fundamentals (Arg 1.1.1)

The ACAS Fundamentals have been defined in section 2.2. The Fundamentals comprise the principles of operation and an abstract Functional Model which together fully describe the ACAS Concept at the service specification level. The evidence that the Fundamentals correctly capture the ACAS Concept is provided by expert review of this document, which is part of the more general Arg 1.6 (section 6.7).

6.2.3 Changes to Operations (Arg 1.1.2)

Prior to the introduction of ACAS, mid-air collision avoidance could be achieved only by See & Avoid action by the Flight Crew and/or intervention from ATC. Due to factors such as the speed and size of the objects involved and the normal workload of a commercial Flight Crew, and the assumption that ATC would provide separation in controlled airspace, it is unlikely that See & Avoid would be performed in the absence of a specific prompt. Moreover, visual perception of an encounter and the Flight Crew's reaction to it were known to be unreliable [18][19], and visual acquisition, even if achieved, would in many cases be in the last few seconds prior to collision and the resulting avoiding action would require high accelerations, possibly causing injuries to occupants. Therefore, it was not effective as a standalone collision-avoidance measure in commercial aircraft operations. Intervention from ATC, either to recover separation by explicit clearances or to prompt the Flight Crew where to visually acquire the conflicting aircraft, would occur due to STCA (if available) or by unaided recognition of the problem by the controller. In both cases, the intervention is performed by the same part of the ATM system that allowed the conflict to develop. It was therefore imperfect as a means of collision avoidance and inevitably relied upon air-ground communications which are inherently subject to delay and/or error (particularly in such high-stress situations).

The introduction of ACAS has dictated a change in aircraft operations because the concept is based upon improved collision avoidance by means of automatic conflict-detection and -resolution guidance to the Flight Crew [section 2.3.1]. Since ACAS is intended as a last resort against mid-air collision, aircraft operations are modified to afford ACAS a higher priority than ATC Separation Recovery. Consequently, Flight Crew are required to respond to ACAS advisories, unless to do so would jeopardize the safety of the aircraft (see Safety Requirement SR_F2 in section 6.3.3 below), in accordance with the Prioritisation principle defined in section 2.2.5. .

The basic collision-avoidance functionality of ACAS [section 2.2.3 above] will be shown in Arg 1.1.4 to produce a substantial reduction in the risk of collision; however this benefit depends upon the correct integration of ACAS operations with pre-existing means of collision avoidance in order to satisfy the prioritisation principle [section 2.2.5]. This is an aspect of the concept that falls outside the scope of Arg 1.1.4 and is covered instead under Arg 1.3.4 later.

Subject to satisfaction of Arg 1.3.4, the differences in operations described above allow the improvement afforded by ACAS to be realised and are therefore reconciled with the Safety Criteria.

6.2.4 Impact on the Operational Environment (Arg 1.1.3)

The general operational environment in which ACAS is used is defined in the Fundamentals [section 2.2.2 above], and the equipage aspects are elaborated in the Design [section 2.3.5]. However, in order to assess the impact of the concept on its operational environment from a safety viewpoint, it is necessary to consider systematically the *elements* in the environment with which ACAS and the Flight Crew interact. These elements can best be identified from the Logical Model in Figure 3 and comprise the following:

- Airframe[27]
- Aircraft Occupants
- Aircraft not involved in the encounter
- Air Traffic Controller

The collision-avoidance part of the Fundamentals [section 2.2.3] recognises that ACAS needs to achieve collision avoidance via the Flight Crew and the airframe dynamics, and the collision-avoidance action is thus constrained by the capabilities of both. In this context, Flight Crew capability also includes their predisposition not to follow ACAS if to do so would involve unacceptable handling of the aircraft. ACAS addresses these factors through conflict-detection and -resolution algorithms which provide a sufficiently effective collision-avoidance action using benign but early action by the Flight Crew.

[27] Airframe is considered to be partly Design and partly environment, as explained in section 2.3.4.

The benign nature of the required action means that ACAS operations do not present a hazard to the environment for the following reasons:

- the action will be within the capabilities of any airframe in the environment, and any position in the flight envelope at which that airframe might be required to respond, because all aircraft subject to the Policy will have been certificated for ACAS carriage;
- the action will not involve airframe movement that could be harmful to aircraft occupants (except in cases of incorrect Flight Crew behaviour) ;
- the excursion in vertical displacement will normally be insufficient to induce a consequential separation infringement with an aircraft not involved in the original encounter. In the event that this does occur, ACAS is designed to provide collision avoidance for the subsequent encounter as necessary.

Since segregation from the ATM system is part of the concept, interaction with the Air Traffic Controller is considered to be outside the scope of Arg 1.1.4 and is deferred until Arg 1.3.4 later.

The concept includes provisions for minimising any adverse safety impact from ACAS operations on each of the elements that make up its airborne environment. These aspects of the concept are therefore qualitatively consistent with the Safety Criteria.

6.2.5 Principal Parameters (Arg 1.1.4)

ACAS detects and resolves conflicts using algorithms[28] applied to aircraft relative-position information. The algorithms and their associated parameters produce the core functionality and performance of ACAS, and their quality largely dictates the safety benefit provided by ACAS over the range of conflict scenarios and operational environments to which it is exposed. Therefore, in order to support the collision-avoidance part of the Fundamentals [section 2.2.3] and to verify Arg 1.1.3, it is necessary to demonstrate that suitable algorithms and parameters do in fact exist. Furthermore, ACAS performs collision avoidance via the Flight Crew which implies the need for fundamental human functionality and performance (ie timely and appropriate response to ACAS) in addition to that provided by equipment, in order to satisfy the concept.

The evidence that the concept can provide a substantial improvement in collision risk using constrained avoidance actions arises from dynamic modelling [21][22][24] of ACAS with algorithms from DO-185A [9], with the supplementary changes [30][31]. Within the modelling studies, the theoretical effectiveness of ACAS in reducing the risk of collision is expressed using a metric known as Logic Risk Ratio (LRR), which is defined as:

$$\text{Risk Ratio} = \frac{\text{Risk of Collision with ACAS}}{\text{Risk of Collision without ACAS}}$$

This parameter is calculated based upon the behaviour of the ACAS algorithms and a pilot-response model in simulated encounters[29]. The most recent study containing

[28] specified in RTCA DO-185A..

[29] these simulations do not take into account factors which might alter the theoretical safety benefit in a practical system design. Simulations to demonstrate the satisfaction of the Safety Criteria by the complete ACAS Design need to take into account all such factors. This is covered under Arg1.3 later.

an estimate for LRR for the whole of ECAC airspace [10] has predicted an LRR of 19.6%, which represents a substantial reduction in the risk of collision[30].

Consequently, the modelling results demonstrate that a fundamental set of algorithms and parameters for the equipment and human elements does exist in support of the concept, and provides collision avoidance performance which is consistent with the Safety Criteria.

6.2.6 Conclusions to Arg 1.1

An assessment of the ACAS Fundamentals and supporting modelling results has demonstrated that ACAS has the potential to deliver a significant reduction in the risk of mid-air collision when exposed to encounters typical of its operational environment. Moreover, it does so without any inherent adverse safety implications elsewhere in its operational environment. The ACAS concept is therefore intrinsically safe and Arg 1.1 is substantiated.

6.3 Design Completeness (Arg 1.2)

6.3.1 Strategy

In order to argue that the ACAS Design is complete it is necessary to show that there exists a complete set of Safety Requirements, referenced to the Design, that satisfy the Fundamentals[31].

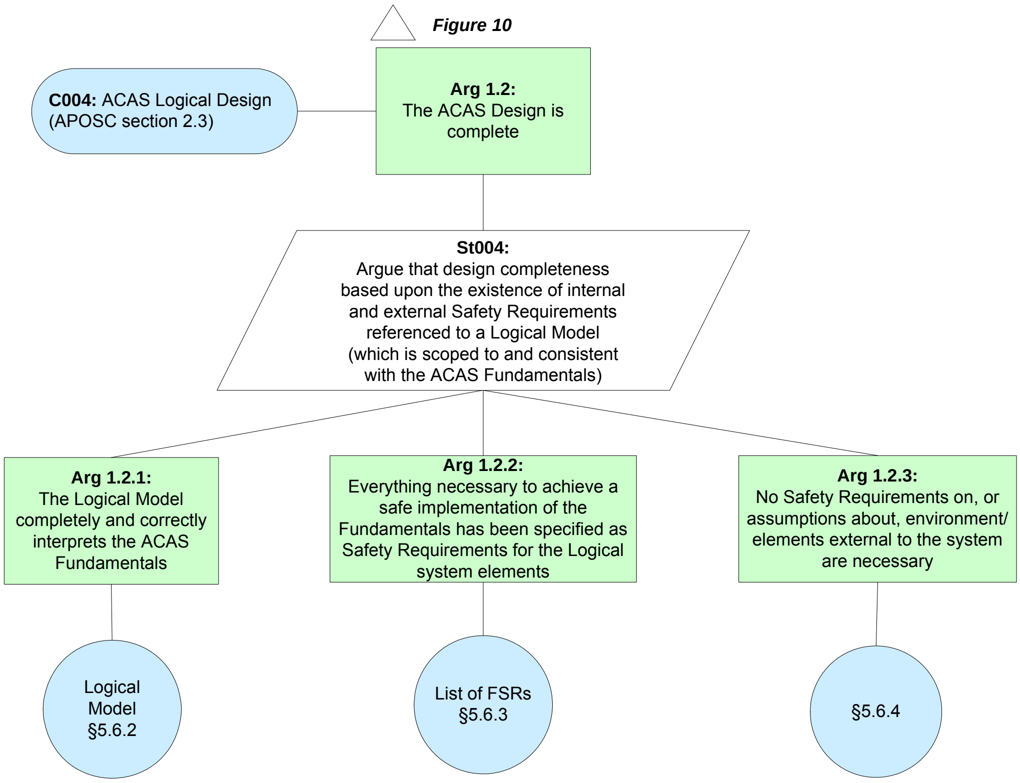


Figure 10
C004: ACAS Logical Design (APOSC section 2.3)
Arg 1.2: The ACAS Design is complete
St004: Argue that design completeness based upon the existence of internal and external Safety Requirements referenced to a Logical Model (which is scoped to and consistent with the ACAS Fundamentals)
Arg 1.2.1: The Logical Model completely and correctly interprets the ACAS Fundamentals
Arg 1.2.2: Everything necessary to achieve a safe implementation of the Fundamentals has been specified as Safety Requirements for the Logical system elements
Arg 1.2.3: No Safety Requirements on, or assumptions about, environment/ elements external to the system are necessary
Logical Model §5.6.2
List of FSRs §5.6.3
§5.6.4

Figure 12 Design Completeness

[30] In RVSM airspace (that is, from Flight Level 290 to 410, inclusive), reference [10] states that the LRR is around ten times better, at 1.7%, because aircraft in this airspace manoeuvre much less than in lower airspace and there is a much higher proportion of ACAS-equipped aircraft.

[31] Further Safety Requirements can arise from Arg 1.3 to Arg 1.5 below

This is argued using the sub-arguments shown in Figure 12.

These sub-arguments are addressed in turn, in sections 6.3.2 to 6.3.4 below. Conclusions regarding Arg 1.2 are then drawn in section 6.3.5.

6.3.2 Logical Definition (Arg 1.2.1)

An ACAS Logical Model and its constituent elements are described in section 2.3. The claim that the Logical Model represents the design solution to the ACAS Fundamentals is supported by the traceability between the ACAS Fundamentals and the Logical Model provided in Appendix J, and by the traceability between Safety Requirements and Fundamentals given in Appendix C

The scope of the ACAS Design is considered to encompass all those elements that collectively produce the required aircraft movement. The Logical Model clearly delineates those elements considered to be part of the ACAS Design from those considered to be part of its environment. The roles played by the elements within the Design, and the environment and elements external to the Design, where they affect, or are affected by, the operation of ACAS are also described in section 2.3. It is argued that these roles are necessary and sufficient to fully implement the Fundamentals.

Evidence that the Logical Model is a correct refinement of the ACAS Fundamentals is also provided by expert review of this APOSC which is subsumed into the more general Argument 1.6 (section 6.7).

6.3.3 Functional Safety Requirements (Arg 1.2.2)

Based upon analysis of the logical model elements described in sections 2.3.2 to 2.3.4, and their relationships to the ACAS Fundamentals, the Functional Safety Requirements following in Table 1 are deemed to be applicable to the elements of the Design:

Ref	Safety Requirement
	ACAS
SR_A1	ACAS shall continuously monitor the aircraft environment for the existence of potential collision
SR_A2	ACAS shall provide a warning (TA) to Flight Crew of the existence of possibly conflicting traffic
SR_A3	ACAS shall provide indications (RA) to Flight Crew on how to act to avoid collision
SR_A4	ACAS collision avoidance indications (RA) shall be produced by algorithms which are equivalent in performance to those specified in DO-185A[32]
SR_A5	ACAS shall coordinate its collision avoidance indications (RA) with those on the intruder aircraft (when ACAS equipped) to ensure that the collision avoidance actions are compatible
SR_A6	ACAS shall provide collision avoidance indications (RA) which are compatible with all types of equipped aircraft in the environment and all points in their flight envelope relevant to the environment
SR_A7	ACAS shall provide collision avoidance indications (RA) which correspond to the minimum manoeuvring necessary to avoid collision

[32] the models used to provide the evidence for Arg1.1.4 contain algorithms conforming to DO-185A

Ref	Safety Requirement
SR_A8	ACAS shall not produce collision avoidance indications (RA) which would cause the aircraft to descend when close to the ground
SR_A9	ACAS shall not produce warnings or collision avoidance indications (TA or RA) during aircraft operation close to, or on, the ground
SR_A15	ACAS shall not produce audible collision avoidance indications (RA) when other onboard warnings (stall, ground proximity, windshear) are being annunciated.
Flight Crew	
SR_F1	Flight Crew shall prepare themselves to act immediately in accordance with any subsequent collision avoidance indications (RA), in response to potential collision warning (TA) from ACAS
SR_F2	Flight Crew shall act immediately in accordance with collision avoidance indications (RA) from ACAS unless doing so would jeopardize the safety of the aircraft due to the existence of a hazardous situation which must be prioritised over collision avoidance
SR_F3	Flight Crew shall act in accordance with collision avoidance indications (RA) from ACAS by using control inputs similar in strength to those used for routine aircraft manoeuvres
SR_F7	Flight Crew shall operate ACAS in TA/RA mode during flight only

Table 1 - Arg 1.2 Functional Safety Requirements

6.3.4 External Safety Requirements (Arg 1.2.3)

Based upon the logical model elements described in section 2.3.5 to 2.3.8, there are no Functional Safety Requirements or assumptions applicable so far to the environment or elements external to the Design. This is because:

- there are no specific requirements on the occupants or non-involved aircraft arising from the introduction of ACAS
- there are no specific requirements on ATC that are necessary for ACAS to operate – however there is a need for ATC not to prevent ACAS from operating and this is captured in a combination of SR_F2 above and SR_C1 in section 6.4.5.2 below.

6.3.5 Conclusions to Arg 1.2

The ACAS Logical model correctly interprets the ACAS Fundamentals. A set of Functional Safety Requirements has been derived for its elements which, if implemented, will enable ACAS to provide the intrinsic safety originating from the concept. At this stage, they constitute a *partial* set because subsequent arguments (Args 1.3 to 1.5) yield additional Functional Safety Requirements. These additional Safety Requirements are combined with those in sections 6.3.3 and 6.3.4 above to produce the final set in Appendix B. The completeness of the final set of Safety Requirements has then been validated by establishing that they address all the Fundamentals, as shown in Appendix C. Arg 1.2 is therefore substantiated.

6.4 Design Correctness (Arg 1.3)

6.4.1 Strategy

In order to argue that the ACAS Design (section 2.3 above) works correctly under all normal environmental conditions, it is necessary to demonstrate that it functions as intended and delivers a degree of collision-risk reduction commensurate with the Safety Criteria when subjected to the environment for which the concept was intended. This is argued using the following sub-arguments, as shown in Figure 13:

Arg 1.3.1. The Design is internally coherent in terms of functionality, data and information flows within and between the elements that make up the Design.

Arg 1.3.2. All reasonably foreseeable normal operational conditions / range of inputs from adjacent systems (such as expected encounter geometries, airframe and Flight Crew capabilities, and intruder equipage) have been identified.

Arg 1.3.3. The Design operates correctly in a dynamic sense, under all reasonably foreseeable normal operational conditions / range of inputs.

Arg 1.3.4. The Design operates in a way that is compatible with the operation of adjacent airspace and external systems with which it interfaces / interacts; in particular its interaction with other on-board accident-avoidance systems and ATM.

Arg 1.3.5. The Design is capable of delivering the desired collision risk reduction under all reasonably foreseeable normal operational conditions / range of inputs.

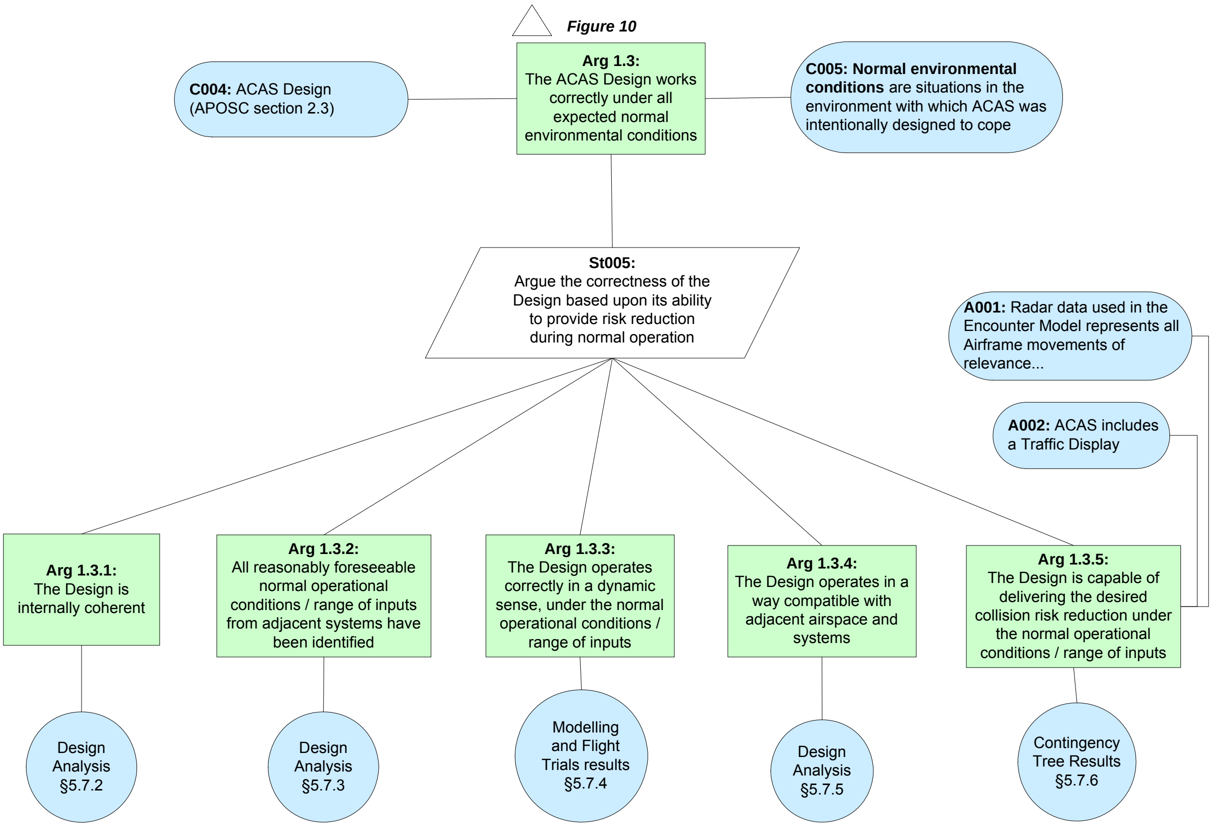


Figure 10
C004: ACAS Design (APOSC section 2.3)
Arg 1.3: The ACAS Design works correctly under all expected normal environmental conditions
C005: Normal environmental conditions are situations in the environment with which ACAS was intentionally designed to cope
St005: Argue the correctness of the Design based upon its ability to provide risk reduction during normal operation
A001: Radar data used in the Encounter Model represents all Airframe movements of relevance...
A002: ACAS includes a Traffic Display
Arg 1.3.1: The Design is internally coherent
Arg 1.3.2: All reasonably foreseeable normal operational conditions / range of inputs from adjacent systems have been identified
Arg 1.3.3: The Design operates correctly in a dynamic sense, under the normal operational conditions / range of inputs
Arg 1.3.4: The Design operates in a way compatible with adjacent airspace and systems
Arg 1.3.5: The Design is capable of delivering the desired collision risk reduction under the normal operational conditions / range of inputs
Design Analysis §5.7.2
Design Analysis §5.7.3
Modelling and Flight Trials results §5.7.4
Design Analysis §5.7.5
Contingency Tree Results §5.7.6

Figure 13 Design Correctness

These sub-arguments are addressed in turn, in sections 6.4.2 to 6.4.6 below. Conclusions regarding Arg 1.3 are then drawn in section 6.4.7.

6.4.2 Design Coherency (Arg 1.3.1)

Internal coherence of the Design is a prerequisite to its possessing correct dynamic behaviour (Arg 1.3.3). Coherency is considered to be the attribute that the elements of the Design are working in concert with each other and the environment due to their functionality, data and information flows being consistent[33].

Since the Functional Safety Requirements derived in section 6.3.3 are a necessary and sufficient description of what each element needs to do to support the Fundamentals, they are used as the basis for demonstrating coherency of the Design. Examination of the Functional Safety Requirements reveals that none of the elements individually possesses contradictory Safety Requirements. This signifies that the functionality of each element is coherent within itself.

Examination of the Functional Safety Requirements also reveals the following set of dependencies between elements:

SR_A2	ACAS shall provide a warning (TA) to Flight Crew of the existence of a potential collision
SR_F1	Flight Crew shall prepare themselves to act immediately in accordance with any subsequent collision avoidance indications (RA), in response to potential collision warning (TA) from ACAS

SR_A3	ACAS shall provide indications (RA) to Flight Crew on how to act to avoid collision
SR_F2	Flight Crew shall act immediately in accordance with collision avoidance indications (RA) from ACAS, unless doing so would jeopardize the safety of the aircraft due to the existence of a hazardous situation which must be prioritised over collision avoidance

SR_A7	ACAS shall provide collision avoidance indications (RA) which correspond to the minimum manoeuvring necessary to avoid collision
SR_F3	Flight Crew shall act in accordance with collision avoidance indications (RA) from ACAS by using control inputs similar in strength to those used for routine aircraft manoeuvres

There is also clearly a necessary dependency between the ACAS equipment in two equipped, conflicting aircraft. Consistency between them is provided by SR_A5.

All dependencies can be seen to be mutually consistent and examination of the Safety Requirements in Table 1 has not revealed any unwanted dependencies / dysfunctional interactions. Therefore the Design is considered to be coherent.

6.4.3 Identification of Normal Environment (Arg 1.3.2)

Identification of the normal conditions in the environment to which ACAS will be exposed is a prerequisite to demonstrating that the Design works correctly and delivers the desired risk reduction under those conditions (Arg 1.3.3 & 1.3.5). This is because these attributes of the Design are assessed in the context of the range of inputs presented to it as a result of conditions in the environment.

[33] For this purpose, ATM is placed outside the boundary of the wider ACAS system and compatibility between ACAS and ATM is, therefore considered under Arg 1.3.4 (see section 6.4.5.2 below

Therefore, in order to support Arg 1.3.2, it is sufficient to identify the aspects of the environment which have an effect on ACAS operations, and not those aspects which receive an effect as a result of ACAS operations[34]. This is equivalent to defining the conditions under which the Functional Safety Requirements must be satisfied.

These conditions comprise the normal range of the parameters that characterise the elements of the environment, as follows:

- normal range of Airframe Movements. This comprises the ranges of each parameter (such as relative bearing, headings, airspeeds, vertical rates) used in ACAS modelling studies to characterise the motion of the two aircraft involved in an encounter
- normal range of Flight Crew capabilities. This comprises their capabilities in terms of response time to an RA and adequacy (strength) of the response to an RA
- normal range of the Natural Environment. This comprises those natural weather conditions/phenomena in whose presence ACAS is expected to provide collision avoidance
- normal range of Airframe Types and their associated flight envelopes. This comprises ranges of each parameter (such as aircraft/engine type, altitude, weight) that characterise the capabilities of those aircraft on board which ACAS is expected to provide collision avoidance
- normal range of equipage by aircraft not subject to the Policy. This comprises the nominal percentage of those aircraft in ECAC airspace whose equipage with ACAS is not mandatory, but nevertheless influences the probabilities of the equipage scenarios described in section 2.3.5.

In accordance with section 2.3, Flight Crew strictly is considered to be an element of the Design rather than the environment. However, SR_F1 to SR_F3 need to be satisfied within the normal range of their capabilities. Therefore, Flight Crew capabilities are included as an environmental condition within the context of Arg 1.3.2 because it is necessary to demonstrate Arg 1.3.3 & 1.3.5 under conditions of varying capability.

The normal range of Airframe Movements during encounters is identified using an Encounter Model which is a component used in ACAS modelling. The Encounter Model creates random artificial encounters based upon the statistics of real encounters observed in radar data. Its objective is to allow demonstration of the theoretical effectiveness of ACAS operations in the specific environment to which the sample of radar data pertains. The normal range of Flight Crew capabilities is also identified in ACAS Safety Studies and has been derived in the latest study [24] from the analysis of airborne recorded data.

The ranges of Natural Environment, Airframe Types and flight envelopes are dealt with at the ACAS Fundamentals level [section 2.2.3 above] by prescribing compatibility of the collision-resolution action with the minimum airframe capabilities, and by the inclusion of safety requirement SR_A6 and SR_A7. This means that the airframe will always be able to respond adequately to Flight Crew control inputs regardless of the combination of aircraft type, airspeed, altitude, weight and weather at the time of the encounter. In practice, this compatibility is achieved by certificating

[34] note that aircraft movement satisfies both aspects

aircraft to carry ACAS. By implication, this means that ACAS-equipped aircraft will by definition be able to perform adequately in response to an RA. Therefore, the certification process in effect ensures that the Design is compatible with the performance range of an equipped aircraft.

With regard to ACAS equipage by aircraft not subject to the Policy, ACAS Safety Studies assumed that they would not be equipped, as this was considered to be the worst case assumption [29].

6.4.4 Dynamic Behaviour (Arg 1.3.3)

Arg 1.3.3 is concerned with demonstrating that the Design is a correct solution to the Fundamentals in terms of dynamic behaviour. As such, it does not seek to demonstrate that the intrinsic safety of the concept has been inherited by the Design; this is covered later in Arg 1.3.5 – rather it seeks to show that the dynamic behaviour of the Design is what was intended.

Correct dynamic behaviour of the Design under normal operational conditions cannot be demonstrated by inspection of the Logical Model, the description of its elements, or the Functional Safety Requirements, because they are parts of a static representation of ACAS operations. Therefore, the evidence comes instead from its implementation [section 2.1], which is addressed in the 6th paragraph of section 7.4.

6.4.5 Design Compatibility (Arg 1.3.4)

Having argued that the Design is internally coherent and dynamically correct, the next aspect to consider is whether its behaviour is compatible with the normal operation of other systems in its environment. The impact of ACAS on aircraft operations and its operational environment has been assessed at the concept level as part of Arg 1.1.2 and Arg 1.1.3. Here it is necessary to show that the Design correctly reflects these aspects of the concept, by capturing these aspects as Functional Safety Requirements.

Based upon Arg 1.1.2 and Arg 1.1.3, the systems with which the ACAS Design must be compatible are as follows:

- other accident avoidance systems
- the ATM system and its provision of ATS
- proximate aircraft (those aircraft that are not directly involved but which could be affected by collision avoidance action taken by the aircraft involved in an ACAS RA).

The compatibility features in the Design, and the existing (or additional) Functional Safety Requirements necessary to support them, are described in sections 6.4.5.1 and 6.4.5.2 below.

6.4.5.1 Compatibility with Other Accident Avoidance Systems

Flight crew do not need to be aware (indeed cannot be aware) of the presence of ACAS on the intruder aircraft, or the way in which that aircraft will respond to ACAS (SR_A1 and SR_A3). Therefore, ACAS operations place no additional perceptual task on the Flight Crew with respect to an intruder aircraft beyond that necessary for operations without ACAS.

ACAS is compatible with other accident-avoidance systems (human and safety nets) because its operation is prioritised (see section 2.2.5) so as not to interfere with systems designed to deal with more immediate threats to aircraft safety than potential mid-air collision. Therefore, it is compatible with on-board accident avoidance systems (viz GPWS, stall warning, windshear warning) to which it gives priority via the ACAS equipment, as described in section 2.3.2 above.

ACAS operation takes precedence over ground-based accident-prevention systems (viz STCA, MSAW, in conjunction with the Controller) because these provide less reliable means of accident avoidance than on-board systems. This prioritisation is effected by the Flight Crew being required to follow an RA (SR_F2).

Mid-air collision avoidance via ACAS is deemed to be compatible [12] with dissimilar parallel means of on-board mid-air collision avoidance (viz See & Avoid) even though the coherence between collision avoidance solutions from independent sources cannot be guaranteed. This is because the Flight Crew have the responsibility to ensure the safety of the aircraft using any means at their disposal.

6.4.5.2 Compatibility with the ATM System

In line with the collision-avoidance principle, ACAS achieves collision avoidance by producing a change in, or maintenance of, vertical speed either when an aircraft is climbing or descending to a new flight level, or when an aircraft is already established at its cleared flight level. The term ‘manoeuvre’ is used below to mean a change in vertical speed.

Due to the principle of minimising the manoeuvring required to achieve adequate collision avoidance, it is feasible for the Flight Crew to follow an RA without violating the current vertical clearance. ACAS therefore has the potential to induce the following effects related to the motion of an RA-incident aircraft:

- produces a manoeuvre or maintenance of vertical speed which violates the aircraft’s ATC clearance by deviating from the cleared flight level and/or vertical speed clearance
- produces a manoeuvre or maintenance of vertical speed which is noticed by a controller even though an ATC clearance is not violated
- produces a manoeuvre or maintenance of vertical speed that does not violate the aircraft’s ATC clearance and goes unnoticed by the controller.

ACAS operations and Separation Provision (or Separation Recovery) provided by ATC are deemed to be mutually compatible *under all circumstances* provided the aircraft does not need to deviate from its current clearance or instruction as a result of an ACAS RA. It follows that:

- A deviation from an existing clearance or instruction, or inability to conform to a new clearance or instruction issued while and RA manoeuvre is in progress, represent the only conceivable incompatibilities between ACAS and ATC
- Separation Provision (or Separation Recovery) can continue to be provided by ATC during an ACAS-initiated collision avoidance action where there is no deviation from clearance

The segregation principle carries with it the adverse implication that if the avoidance action causes a clearance to be violated, the controller will issue further instructions to the aircraft in order to restore separation if the ATM system is unaware of ACAS operation. In other words, the ATM ground-based elements will function normally during collision avoidance presupposing that the ATM system failure which led to the potential collision is transient in nature.

Such continuation of ATC service to an RA-incident aircraft might interfere with the correct performance of collision avoidance by defeating the prioritisation principle [section 2.2.5]. Since prioritisation is performed by humans and collision avoidance is a rare event, it is conceivable that prioritisation might not be performed correctly on every occasion – as was the case in the Yaizu (2001) and Überlingen (2002) accidents described in Appendix I. Therefore, the Design needs to include an interface between Flight Crew and the Air Traffic Controller to actively suppress the issuance of ATC instructions or clearances during any ACAS-initiated collision avoidance action.

However, this simple requirement raises two issues: whether all RAs, or just those involving a deviation from ATC clearance, should be reported; and how soon should the report be made. If all RAs were to be reported, this could possibly produce an unnecessary increase in the workload of the Flight Crew and Air Traffic Controller, including diverting their attention from more urgent tasks. However, since RAs are in fact very infrequent for any given Air Traffic Controller or Flight Crew, concerns over workload increase are, in reality, probably unfounded. Since the existence, nature and duration of an RA are unknown to the Air Traffic Controller, the Flight Crew has the sole responsibility of determining any incompatibility between the RA and instructions/clearances in what is an inherently unfamiliar, stressful situation requiring instant reactions to deal with the RA itself. Therefore, as the Flight Crew cannot always determine at the time of an RA[35] whether the collision avoidance action will ultimately violate a current cleared level[36], notification to the Air Traffic Controller could in certain situations be incorrect, not reported or take place some time after the onset of the RA. Delay can also be caused simply by the fact that the Flight Crew must give priority to responding to the RA over reporting it, and due to limitations of human performance the Flight Crew may simply omit the notification. Equally, the receipt of a new, incompatible instruction/clearance in the presence of an ongoing non-reportable RA would produce a notification by the Flight Crew after the onset of the RA.

A further consideration is that the Air Traffic Controller may issue a horizontal manoeuvring instruction when an RA is in progress in an attempt to resolve the situation (as was the case in the Jeju Island incident discussed in Appendix I, section I.3). Such a manoeuvre may or may not help to avoid a collision, but could cause the flight crew further confusion in an already unfamiliar situation.

Reporting of RAs is covered by SR_F4 below – this requirement has been framed with the intention that an RA would be reported unless it was immediately obvious to the Flight Crew that no deviation from clearance would result – the latter would be the case, for example, where an RA is triggered by high vertical speed when approaching cleared flight level. SR_F4 is not the same as the current requirement in PANS-OPS; this discrepancy is noted as safety issue **ISS-002** in section 10.2.

The problem of the delays to RA reports by Flight Crew could be addressed by RA Downlink, as discussed in section 2.3.8). Since it is more than 9 years since Yaizu and more than 8 years since Überlingen, and RA Downlink has been introduced (ad

[35] including the initial RA and any subsequent RAs in the same encounter

[36] The existence of a manoeuvre in association with the RA is irrelevant to the deviation criterion because a sustained maintain rate RA could produce a 'level bust' deviation from a level clearance.

hoc) by only three ECAC States, the continuing uncertainty concerning the feasibility of RA Downlink has been raised as a Safety Issue (**ISS-001**) in section 10.2 below.

Upon receipt of a notification[37], the Air Traffic Controller ceases to issue instructions / clearances to the notifying aircraft – see SR_C1 below. In addition, it serves to alert the controller of the need to plan for the resumption of Separation Provision to the involved aircraft when the collision avoidance action has been completed.

When a collision avoidance action has terminated, Flight Crew need to notify the controller in order that Separation Provision is resumed[38] - see SR_F10 below. Again, this presupposes that the failure which led to the potential collision was transient in nature. Therefore, satisfactory transition between aircraft control via ATC and ACAS, and back again, is ensured.

The notifications also serve to prompt the controller to assess the impact of the action on separations between the involved aircraft and other traffic, and issue clearances to the latter as necessary. The effect is to minimise any negative safety impact on other air traffic in the sector arising from ACAS operations.

These considerations give rise to the additional Functional Safety Requirements in Table 2 which seek to eliminate the incompatibility between ACAS and ATC:

Ref	**Safety Requirement**
	Flight Crew
SR_F4	As soon as possible, as permitted by workload, Flight Crew shall notify the Air Traffic Controller of the execution of an ACAS-initiated collision avoidance action except when it is believed that the action would not result in a deviation from a clearance or instruction
SR_F8	In the event that the Flight Crew receive an ATC instruction that would result in a contravention of the RA (in strength and / or direction), the Flight Crew shall refuse the instruction and advise ATC as soon as workload permits that the aircraft is involved in an RA
SR_F9	Flight Crew shall notify the Air Traffic Controller as soon as avoidance action is completed and workload permits, and shall resume the vertical clearance that was in effect prior to the RA.
	Air Traffic Controller
SR_C1	Air Traffic Controller shall cease to issue clearances or instructions to an aircraft that has notified its execution of an ACAS-initiated collision-avoidance action

Table 2 – Arg 1.3.4 Functional Safety Requirements

ACAS is effective when the involved aircraft occupy different sectors because the Safety Requirements in Table 2 do not presuppose that both aircraft communicate with a single Air Traffic Controller. Therefore, ACAS operations are compatible with the management of aircraft across airspace boundaries.

Inspection of Table 1 and Table 2 reveals the following new dependencies between elements:

SR_F2	Flight Crew shall act immediately in accordance with collision avoidance indications (RA) from ACAS, unless doing so would jeopardize the safety of the

[37] For the case of RA Downlink, the appearance of an RA indication on a surveillance display, is not necessarily an indication that a deviation from clearance will be required.

[38] RA Downlink could achieve this notification by the removal of the RA indication to the controller, as noted in section 2.3.8.

	aircraft due to the existence of a hazardous situation which must be prioritised over collision avoidance.
SR_F4	Flight Crew shall notify the Air Traffic Controller of the execution of an ACAS-initiated collision avoidance action except when it is believed that the action would not result in a deviation from a clearance or instruction
SR_F8	In the event that the Flight Crew receive an ATC instruction that would result in a contravention of the RA (in strength and / or direction), the Flight Crew shall refuse the instruction and advise ATC as soon as workload permits that the aircraft is involved in an RA
SR_F9	Flight Crew shall notify the Air Traffic Controller as soon as avoidance action is completed and workload permits, and shall resume the vertical clearance that was in effect prior to the RA.
SR_C1	Air Traffic Controller shall cease to issue clearances or instructions to an aircraft that has notified its execution of an ACAS-initiated collision avoidance action, until the Flight Crew have notified the Air Traffic Controller that avoidance action is completed

All new dependencies are mutually consistent and therefore the Design remains coherent in accordance with Arg 1.3.1.

As a result of the analyses in section 6.4.5.1 and above, Arg 1.3.4 is considered to be substantiated provided that the Safety Requirements are satisfied and Safety Issues **ISS-001** and **ISS-002** are resolved satisfactorily.

6.4.6 Risk-Reduction Capability (Arg 1.3.5)

The final property of the Design to be assessed is its ability to provide collision-risk reduction comparable to that of the concept, when subject to its normal environment. As in the case of the concept, the evidence that the Design can provide a substantial reduction in collision risk comes from modelling.

Section 6.2.5 has described the use of ACAS dynamic modelling as a main source of evidence for the intrinsic safety of the concept, as expressed by means of the Logic Risk Ratio (LRR). Results from the dynamic model are also used, in conjunction with a static model known as Contingency Tree [32], to predict the collision risk reduction achievable by ACAS in the presence of influences beyond the mere operation of its algorithms.

The Contingency Tree uses combinatorial logic and contains a number of factors which alter the effectiveness of ACAS compared to the theoretical effectiveness (LRR) of the ACAS algorithms alone. The factors represent the variables within ACAS operations, and the probabilities assigned to the states of each variable (*aka* Contingency Tree Events) influence the overall collision-risk reduction. Since the factors are intended to represent effects in the real world, the result obtained is a metric known as System Risk Ratio (SRR).

Each probability represents the likelihood of occurrence of the Event within the sample of simulated encounters used to calculate the risk reduction. Therefore, it represents the probability of occurrence of the event per encounter during ACAS operations within the real operational environment that the sample of simulated encounters is intended to represent.

Importantly, the Contingency Tree Events are not categorised as either normal or abnormal states; rather this discrimination is implied by the relative event probabilities. Nor does it explicitly represent failures, although failure of the elements of the Design (or the environment) could in principle contribute to some of the Event probabilities.

The risk-reduction capability of the Design is argued on the basis that **if** the Contingency Tree Events capture all reasonably foreseeable external influences on ACAS operations (ie they are a complete representation of the environment), **if** the Events possess valid probabilities, and **if** the collision-risk-reduction computed using Contingency Tree is consistent with the Safety Criteria, then by implication the Design satisfies Arg 1.3.5.

Since the Contingency Tree was not derived from the ACAS Design in section 2.3, the first condition can be partially verified by comparing the Contingency Tree factors with normal conditions and system interactions described in sections 6.4.3 and 6.4.5 above. This comparison is described in section 6.4.6.1 below. The first and second conditions are also addressed by Arg 1.6 later. As these two conditions are substantiated separately, it is then sufficient to support Arg 1.3.5 hereunder using the third condition alone – ie showing that the collision-risk-reduction computed using Contingency Tree is consistent with the Safety Criteria – as discussed in section 6.4.6.2

6.4.6.1 Contingency Tree Events

The Contingency Tree factors and corresponding Events are listed in Appendix D. The factors are as follows:

- Encounter Geometry
- Aircraft Equipage
- ACAS tracking
- Altitude Reporting
- Controller involvement
- Pilot Response
- Traffic Display
- Visual Acquisition
- See-and-Avoid
- ACAS Logic Performance

Comparison of the Contingency Tree factors with the conditions derived in section 6.4.3 reveals the following:

- There is no Contingency Tree factor related to Airframe Movements. This is because in ACAS dynamic modelling, Airframe Movements are synthesised using an Encounter Model, as mentioned in section 6.4.3, and therefore need not be accounted for in the Contingency Tree. It is argued that, since the Encounter Model can provide evidence of ACAS behaviour only on the basis of sampled data, it must be assumed **(A001)** that the data represents all Airframe Movements of relevance, including high rates of climb or descent between cleared flight levels.
- Flight Crew capabilities (viz non-standard responses such as no response, late response, weak or aggressive response, incorrect direction of response) are covered by the Pilot Response model in the dynamic modelling and the

Pilot Response factor in the Contingency Tree which collectively capture all Flight Crew behaviours of relevance.

- There are no Contingency Tree factors related to Natural Environment or Airframe Types. As described in section 6.4.3, Natural Environment, Airframe Types and associated flight envelopes are factors dealt with via compatibility of the collision-avoidance algorithms with the minimum airframe capabilities falling within the scope of the Policy. Consequently, there is no need for the Contingency Tree to model such conditions.
- All the variables associated with ACAS / Transponder equipage and Transponder functionality are covered by Contingency Tree factors. Since the Contingency Tree contains no specific Events for Airframe Type, it cannot explicitly differentiate between aircraft subject to the Policy or not. Therefore, the Event probabilities are used to represent a level of equipage appropriate to the mixture of aircraft subject to the Policy or not expected to be in the airspace at a given point in time. ACAS non-equipage by aircraft outside the Policy is modelled by reducing the relevant equipage Event probability. The abnormality of non-equipage by an aircraft required to carry ACAS II can be modelled in the same way.

Comparison of the Contingency Tree factors with the system interactions described in section 6.4.5 reveals the following:

- The use of See & Avoid in parallel with ACAS is modelled using several Visual Acquisition Events and an Event representing the Flight Crew's reaction to a visually acquired threat.
- Intervention by the Air Traffic Controller during collision avoidance is included in the Contingency Tree using several Controller Involvement and Pilot Response Events which collectively show the likelihood of the Flight Crew following instructions from the Controller rather than ACAS. It is argued that controller intervention falls within the definition of "normal environment" because of the practical difficulty of complying with both SR_F4 and SR_C1 at the instant of the RA.
- Resumption of separation provision to involved aircraft and the controller's capability to adjust separations of traffic in the vicinity of the involved aircraft need not be addressed within the Contingency Tree because they have no bearing on the collision avoidance efficacy of ACAS. Their impact on the overall safety of ACAS operations is, however, addressed under Arg 1.5 later.

In summary, these two sets of comparisons serve to verify that, between them, the dynamic model and the Contingency Tree Events capture all the relevant aspects of the ACAS normal environment.

6.4.6.2 Satisfaction of Safety Criteria

The most recent study containing an estimate for SRR for the whole of ECAC airspace [22] has predicted a SRR of 21.5%, which represents a substantial (5-fold) reduction in the risk of collision (in EUR RVSM airspace, reference [10] states that the SRR is around ten times better, at 1.8%, than for the whole of ECAC airspace). It might be expected that SRR would represent a smaller risk reduction than the LRR result cited in section 6.2.5 because it takes into account factors that have an adverse affect on ACAS theoretical performance. However, when computing LRR, the possibility of visual acquisition is not taken into account [22] because LRR only addresses the performance of the ACAS algorithms. In SRR, the benefit of a TA, in conjunction with the traffic display, prompting a successful See & Avoid action is included, and this contributes significantly to the overall safety benefit from ACAS[39]. Hence, when computed for similar environments, LRR and SRR do not necessarily differ markedly.

Even though the benefit of ACAS traffic display is included in the SRR results used to support the Safety Case, its presence is not subject to a formal ICAO requirement. Therefore, the existence of a traffic display is dealt with as an assumption **(A002)** rather than a Safety Requirement.

6.4.7 Conclusions to Arg 1.3

Assessment of the ACAS Design, results from ACAS modelling, trials and operational use, collectively demonstrate that the ACAS Design works correctly under normal environmental conditions. Furthermore, the Design is shown to be compatible with the operation of other accident avoidance systems and ATM, subject to:

- satisfaction of the specified Functional Safety Requirements
- satisfactory resolution of Safety Issue **ISS-001** concerning the continuing uncertainty about the feasibility of RA Downlink and its potential benefits in mitigating possible adverse interactions between ACAS and ATM caused by Controller's being unaware of the existence of some extant RA event
- satisfactory resolution of Safety Issue **ISS-002** concerning the discrepancy between Safety Requirement SR_F4 and PANS-OPS section 3.2 c) 4)

The collision-risk-reduction capability of the Design is demonstrated by ACAS modelling studies which exploit a Contingency Tree [32] to represent the real-world factors that can influence ACAS operations. These factors are shown to be consistent with those in the ACAS environment defined by the Safety Case, thus providing further assurance that all the reasonably foreseeable normal operational conditions necessary to underpin Arg 1.3 have been identified. The modelling results show that ACAS operations are capable of producing substantial collision-risk reduction (by approximately a factor of 5) commensurate with Safety Criterion #1. Moreover, since the Design represents the culmination of many years of ACAS development (including monitoring and incident investigation), it is also asserted that collision risk has been reduced AFARP in relation to the Design, in line with Safety Criterion #2. Hence, Arg 1.3 is substantiated, subject to resolution of ISS-001 to 003, as above.

6.5 Design Robustness (Arg 1.4)

6.5.1 Strategy

Arg 1.4 is concerned with demonstrating that the ACAS Design can withstand abnormal situations in the environment. Such situations by definition occur infrequently, however, given their existence it is important to demonstrate that ACAS operations do not become *unsafe* due to any resulting perverse operation of the Design.

[39] Although See & Avoid prompted by a TA does not appear as one of the ACAS Fundamentals [section 2.2], the safety benefit provided by TAs warrants their inclusion as a Safety Requirement (SR_A2).

The context of the argument **(C006)** is situations in the environment under which ACAS cannot work correctly because of technical limitations[40].

In order to argue that the Design is robust, it is necessary to show that the following sub-arguments are true, as shown in Figure 14:

Arg 1.4.1. All reasonably foreseeable abnormal operational conditions / range of inputs from adjacent systems have been identified.

Arg 1.4.2. The Design can react safely to all reasonably foreseeable failures in its environment / adjacent systems (that are not covered under Arg 1.5).

Arg 1.4.3. The Design can react safely to all other reasonably foreseeable abnormal conditions in its environment / adjacent systems (that are not covered under Arg 1.3).

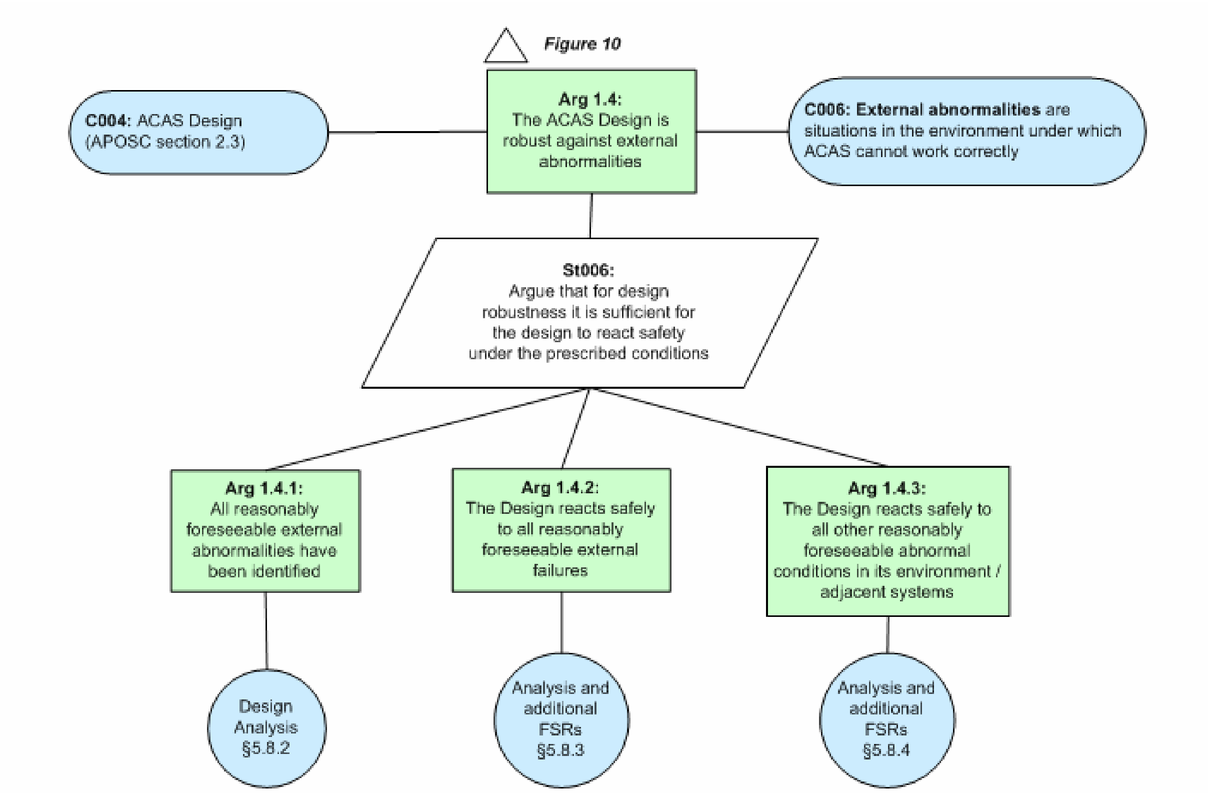


Figure 10
C004: ACAS Design (APOSC section 2.3)
Arg 1.4: The ACAS Design is robust against external abnormalities
C006: External abnormalities are situations in the environment under which ACAS cannot work correctly
St006: Argue that for design robustness it is sufficient for the design to react safety under the prescribed conditions
Arg 1.4.1: All reasonably foreseeable external abnormalities have been identified
Arg 1.4.2: The Design reacts safely to all reasonably foreseeable external failures
Arg 1.4.3: The Design reacts safely to all other reasonably foreseeable abnormal conditions in its environment / adjacent systems
Design Analysis §5.8.2
Analysis and additional FSRs §5.8.3
Analysis and additional FSRs §5.8.4

Figure 14 Design Robustness

It is difficult to demonstrate the behaviour of the Design in the presence of external abnormalities by inspection of the Logical Model, the description of its elements, or the Functional Safety Requirements. Therefore, the evidence presented for Arg 1.4.1 to 1.4.3 in sections 6.5.2 to 6.5.4 below respectively, comes instead from its implementation. This strategy is justified on the basis that the arguments and evidence that the implementation is consistent with the design are established under Arg 2 in section 7 below.

Conclusions regarding Arg 1.4 are drawn in section 6.5.5.

[40] This can create difficulties in differentiating between normal operational conditions and abnormal ones. For example, an encounter is *not* considered to be an abnormal situation in the context of Arg1.4. Similarly, some abnormalities in the environment could be causes of system hazards. The consequence is that certain abnormalities might be justifiably placed under Arg1.3 or 1.5 as an alternative to Arg1.4. However, their precise location is immaterial to the Safety Claim provided each of the abnormalities is addressed under at least one of these arguments.

6.5.2 Identification of External Abnormalities (Arg 1.4.1)

Identification of the external abnormalities is a prerequisite to demonstrating that the Design is robust under abnormal conditions. This is because, as in Arg 1.3 previously, the reaction of the Design is assessed in the context of the range of inputs presented to it as a result of conditions in the environment, including adjacent systems.

The parameters used to specify normal operational conditions in section 6.4.3 clearly can form the basis for categorising abnormal conditions. The abnormal environmental conditions for which there are no corresponding Contingency Tree Events [32] (and therefore are not already dealt with under Arg 1.3) are as follows. Some of these abnormalities can be attributed to failure within the system or its environment, as shown:

- Abnormal Airframe Movements during encounters
- Abnormal Natural Environment
- Abnormal Airframe and associated flight envelope (due to failure)
- Abnormal behaviour of other accident avoidance systems (due to failure)
- Abnormal behaviour of aircraft systems used by ACAS (due to failure)
- Abnormal behaviour of the Air Traffic Controller (due to failure).

These abnormal conditions are discussed in turn below.

ACAS development has revealed limitations in its capability to perform correctly under all encounter scenarios. Since they are situations with which ACAS is unable to cope, they represent *Abnormal* Airframe Movements in the context **(C006)** of Arg 1.4. These conditions are as follows:

- High density of transponder-equipped aircraft in the vicinity [1]
- Intruder aircraft has a vertical speed in excess of 3048 m/min (10000 ft/min) [11]
- Intruder aircraft has high vertical acceleration [1]
- Intruder aircraft has a closing speed in excess of ACAS surveillance capabilities [11]

In addition, a wide range of abnormal conditions can exist with respect to the Natural Environment or Airframe (such as a thunderstorm or engine failure) that could preclude the correct execution of a collision-avoidance manoeuvre even when ACAS is operating correctly. In effect, these conditions can render invalid the compatibility of the collision-avoidance algorithms with the Airframe capabilities, as described in section 6.4.3.

Unlike Airframe Movements and Natural Environment, abnormal behaviour of other accident-avoidance systems, aircraft systems used by ACAS (as identified in section 2.3.4), and the Air Traffic Controller is considered to arise only from failures; ie non-conformity with their requirements. Therefore, the Design needs to be robust against failure of these elements.

6.5.3 Reaction to External Failures (Arg 1.4.2)

Under the failure conditions identified in section 6.5.2 above, ACAS operations need to be modified in accordance with procedural and / or technical provisions to ensure that they do not result in inappropriate collision avoidance action. This ensures that ACAS reacts safely in the presence of external failures.

The reaction of ACAS to the failures identified in section 6.5.2 is identified at the implementation level, as follows:

- The TA-only mode of operation is used in certain *aircraft performance limiting conditions caused by in-flight failures* or as otherwise promulgated by the appropriate authority [3]. This inhibits ACAS on the intruder aircraft from coordinating with ACAS on the impaired aircraft.
- There are no technical provisions to prevent spurious-operation failures of other accident avoidance systems from incorrectly disabling ACAS RAs, which could occur as a consequence of the ACAS inhibits required for certification [section 2.3.2]. The risk presented by such failure modes is considered under Arg 1.5 later.
- ACAS shall continuously perform a monitoring function in order to prevent any further ACAS interrogations if data from external sources indispensable for ACAS operation are not provided, or the data provided are not credible – section 4.3.10 of [11].
- Preventing failure of the Air Traffic Controller from interfering with ACAS operations is addressed inherently by the prioritisation principle [section 2.2.5] as captured explicitly in safety requirements SR_F2 and SR_C1.

These implementation provisions give rise to the following additional Functional Safety Requirements in Table 3:

Ref	Safety Requirement
	ACAS
SR_A10	ACAS shall not produce advisories (TA or RA) if any of the inputs from the aircraft's sensors or transponder are lost or invalid
SR_A13	ACAS shall continuously perform a monitoring function in order to prevent any further ACAS interrogations if data from external sources indispensable for ACAS operation are not provided, or the data provided are not credible
	Flight Crew
SR_F5	Flight Crew shall switch ACAS to TA-only mode when there exists an aircraft-related failure which would preclude an ACAS-initiated manoeuvre should it be necessary

Table 3 – Arg 1.4.2 Functional Safety Requirements

6.5.4 Reaction to Other External Abnormalities (Arg 1.4.3)

In the presence of abnormalities that are not considered to be failure conditions, ACAS operations similarly need to be modified in accordance with procedural and / or technical provisions. This ensures that ACAS will not result in inappropriate collision-avoidance action due to limitations of the system.

The reaction of ACAS to the 'non-failure' abnormalities identified in section 6.5.2 is identified at the implementation level, as follows:

- ACAS might not display all proximate, transponder-equipped aircraft in areas of high-density traffic [1]; the precise choice of which aircraft to display is an equipment-manufacturer decision. It will still display intruder aircraft that are causing alerts.
- ACAS might not display intruders with a vertical speed in excess of 3048 m/min (10000 ft/min) [9][11] and will not give alerts against such intruders [9]. In addition, there might be short-term errors in the tracked vertical speed of an intruder during periods of high vertical acceleration by the intruder [1].
- ACAS will neither display nor give alerts against intruders with a closing speed in excess of its surveillance capabilities [11].
- The TA-only mode of operation is used in certain *aircraft performance limiting conditions* caused by in-flight failures (see SR_F5 and SR_F6) or *as otherwise promulgated by the appropriate authority* [3][41].

These implementation provisions give rise to the additional Functional Safety Requirements in Table 4.

Ref	Safety Requirement
	ACAS
SR_A11	ACAS shall not produce advisories (TA or RA) in situations where there is relative Airframe Movement beyond the capability of its sensors or algorithms
	Flight Crew
SR_F6	Flight Crew shall switch ACAS to TA-only mode when there exists an abnormal environmental situation which would preclude an ACAS-initiated manoeuvre should it be necessary

Table 4 – Arg 1.4.3 Functional Safety Requirements

The inability to alert against intruders with exceptionally high vertical speed / acceleration is not considered to be a significant safety problem because:

- such situations can occur only in an encounter with a military intruder and therefore represents a relatively rare event in the context of all possible encounters
- satisfaction of SR_A11 would ensure that the consequences would be limited to a slight loss in overall effectiveness of ACAS – ie would prevent such an encounter from initiating a <u>new</u> risk-bearing incident due to an inappropriate alert.

6.5.5 Conclusions to Arg 1.4

The robustness of the ACAS Design has been demonstrated by first elaborating those aspects of its environment whose abnormal behaviour either has not already

[41] Due to the large number of abnormal conditions that can exist in the aircraft's environment, and the variable impact each may have on the capability of the Flight Crew to follow an RA, these conditions are not explicitly identified by ICAO. It is left for the Flight Crew to determine whether ACAS-initiated manoeuvring would be precluded by the existence of any given abnormality.

been covered implicitly under Arg 1.3, or is best covered under Arg 1.5 later. In order to prevent inappropriate collision-avoidance action in the presence of such abnormalities, a number of additional Functional Safety Requirements are specified to ensure that ACAS reacts safely by ceasing to provide collision avoidance guidance while an abnormality exists. Arg 1.4 is therefore substantiated.

6.6 Mitigation of System-generated Hazards (Arg 1.5)

6.6.1 Strategy

Whereas Arg 1.4 is concerned with the effect of abnormal environment (ie of external origin) on the safety of ACAS, Arg 1.5 argues from the complementary viewpoint that risks from hazards produced by the system (ie of internal origin) have been mitigated sufficiently within the Design and / or the environment. In the context of ACAS, hazards are considered to be events which have the potential to contribute to an accident **(C007)**; ie they produce a risk increase. This means, for example, that loss of ACAS is considered to be a hazard[42] even though it will not result in a collision by itself.

Therefore, hazardous behaviour of the system could therefore arise from loss of functionality reducing the collision avoidance effectiveness of ACAS, or from anomalous behaviour inducing a risk that would otherwise not have arisen. The anomalous behaviour in turn could arise as a by-product of the normal operation of the system as well as from failure of its elements. In all cases the hazard is considered as belonging to the failure viewpoint because it is risk-increasing, even though some hazards arise from normal operation[43]. Moreover, the risk associated with system hazards need not necessarily be confined to mid-air collision[44]. All behaviours which could contribute to an aircraft accident must be considered in accordance with the scope of the Safety Criteria.

The strategy for subdividing Arg 1.5 is based upon the steps of a conventional ATM risk assessment. It has the objective of identifying causes of system hazards in order to show that all practicable mitigations have been imparted to the Design (or its environment) in accordance with Safety Criterion #2, and to provide assurance that the risk from these hazards is constrained sufficiently to allow ACAS to satisfy Safety Criterion #1. Where this cannot be demonstrated, it serves as a means of identifying where existing mitigations could be strengthened, where existing causes could be eliminated or made less likely, or where additional mitigations could be introduced.

The Safety Case demonstrates adequate mitigation of system hazards using the following sub-arguments, as shown in Figure 15:

Arg 1.5.1. All reasonably foreseeable hazards, at the boundary of the Design, have been identified.

[42] this statement might appear to contradict the rationale behind Arg1.4 in which ACAS is rendered *safe* by disabling it. However, the risk model used by Arg1.5 demonstrates that the consequences of having ineffective ACAS are less severe than having ACAS induce a potential collision because of an inappropriate reaction to external abnormalities.

[43] The rationale is that a risk-increasing “by-product of the normal operation” is an undesired property and would therefore represent a deviation from what is required of the system

[44] As discussed in Appendix I, accidents due to impact of passengers and crew with the aircraft structure or contents are possible consequences of incorrect operation of ACAS.

Arg 1.5.2. The consequences of each hazard have been correctly assessed, taking account of any mitigations that might be available (or could be provided) external to the Design.

Arg 1.5.3. All reasonably foreseeable internal and external causes of each hazard have been identified.

Arg 1.5.4. Safety Requirements have been specified (or Assumptions stated) for the causes of each hazard, taking account of any mitigations that are (or could be made) available internal to the Design, such that the Safety Criteria are satisfied.

Arg 1.5.5. All external and internal mitigations have been captured as either Safety Requirements or Assumptions as appropriate.

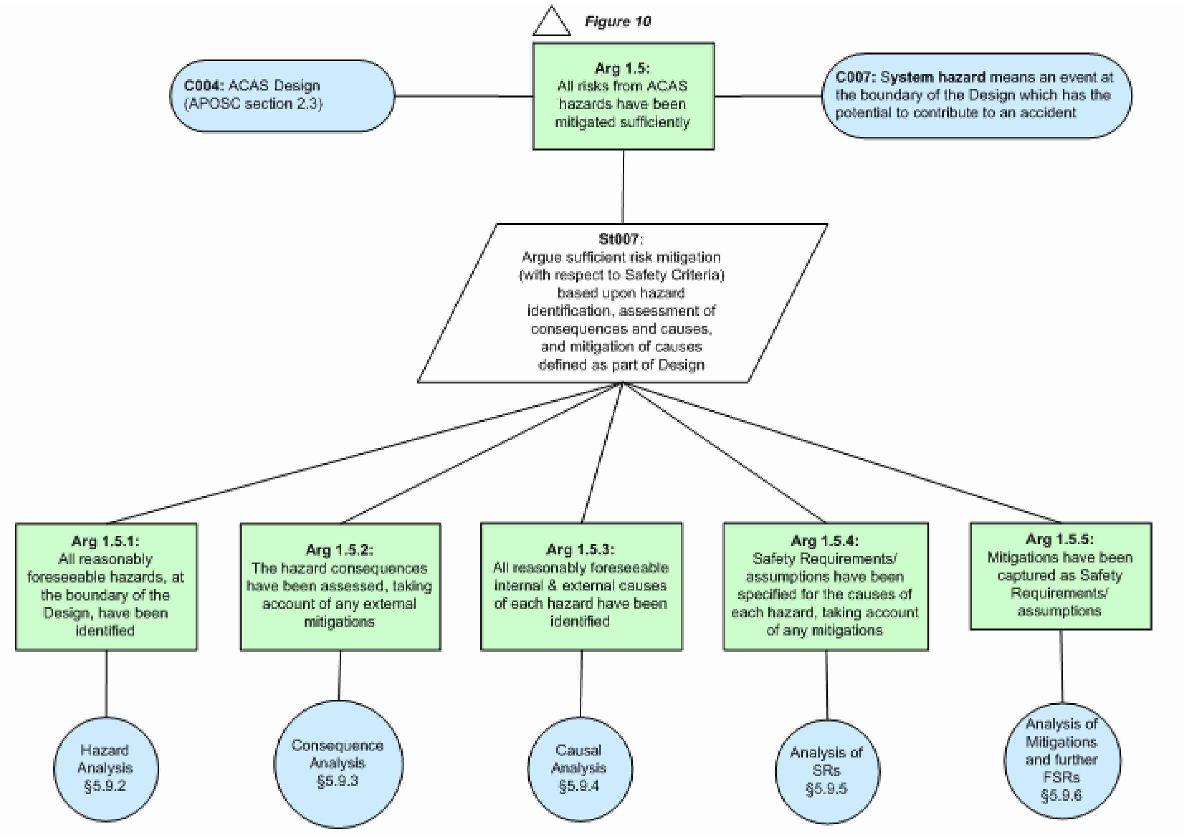


Figure 10
Arg 1.5:
All risks from ACAS hazards have been mitigated sufficiently
C004: ACAS Design (APOSC section 2.3)
C007: System hazard means an event at the boundary of the Design which has the potential to contribute to an accident
St007:
Argue sufficient risk mitigation (with respect to Safety Criteria) based upon hazard identification, assessment of consequences and causes, and mitigation of causes defined as part of Design
Arg 1.5.1:
All reasonably foreseeable hazards, at the boundary of the Design, have been identified
Arg 1.5.2:
The hazard consequences have been assessed, taking account of any external mitigations
Arg 1.5.3:
All reasonably foreseeable internal & external causes of each hazard have been identified
Arg 1.5.4:
Safety Requirements/ assumptions have been specified for the causes of each hazard, taking account of any mitigations
Arg 1.5.5:
Mitigations have been captured as Safety Requirements/ assumptions
Hazard Analysis §5.9.2
Consequence Analysis §5.9.3
Causal Analysis §5.9.4
Analysis of SRs §5.9.5
Analysis of Mitigations and further FSRs §5.9.6

Figure 15 Hazards Mitigation

These sub-arguments are addressed in turn, in sections 6.6.2 to 6.6.6 below. Conclusions regarding Arg 1.5 are then drawn in section 6.6.7.

6.6.2 Hazard Identification (Arg 1.5.1)

The hazards that ACAS presents at the boundary of the system, as expressed in the Design, are all associated with the aircraft movement resulting from collision avoidance. These hazards have been captured as part of a complete accident-causation model for ACAS operations which has been derived to support Arg 1.5.

As explained in section 1.1, the development of ACAS pre-dated contemporary approaches to safety assessment. Therefore, no formal hazard-identification workshops were ever conducted. To circumvent the need to conduct such workshops on a mature operational system, the accident-causation model was instead developed primarily using information that had been produced by the

FHA / PSSA workshops for the EUROCONTROL FARADS project [33]. Those hazards and causes of relevance to ACAS operations were extracted from the workshop records and were blended with a high level aircraft accident-causation model based upon the Integrated Risk Picture developed by EUROCONTROL EEC [34] and the Contingency Tree [32]. The accident-causation model was further refined by making changes to account for ICAO amendments [6][7] that appeared after publication of the FARADS information. Certain *ad hoc* safety issues identified during preparation of the Safety Case were also included.

The resulting accident-causation model uses Fault Tree Analysis (FTA) to represent hierarchically the system hazards, their consequences, their causes, and the relationships between all these events. Basic FTA symbology is described in Appendix E, and the risk model is shown in Appendix F.

The accident-causation model starts by considering the immediate causes of aviation accidents relevant to the ACAS operational environment; namely mid-air collision (MAC) and other accident types relevant to the environment described in section 2.2.2. The latter are termed 'Non-MAC accidents' and comprise the following:

- Controlled Flight into Terrain
- Stall leading to loss of control and Uncontrolled Flight Into Terrain
- Accident due to windshear encounter
- Accident due to other harmful flight conditions such as wake vortex encounter
- Accident due to excessive airframe motions such as velocities, accelerations or rotational rates[45]

The locations of the MAC-related events, barriers, and functions in Appendix F.1 can be identified on Figure 4 and Figure 5. The Collision Avoidance and Strategic Conflict Management barriers do not affect each other adversely, since ACAS operations occur on a tactical timescale whereas Strategic Conflict Management [section 4.1] comprises longer-term traffic management. They are decoupled by virtue of their disparate timeframes of operation. Therefore, the latter barrier does not appear in F.1

As part of the high level breakdown of accident causes, five hazards related to ACAS operations have been identified, as shown in Table 5.

Ref	Hazard
H1	ACAS operations induce non-MAC Accident[46]
H2	ACAS operations induce Possible Collision
H3	Ineffective ACAS collision avoidance
H4	ACAS operations induce ineffective Separation Provision
H5	ACAS operations induce Conflict

Table 5 – ACAS Hazards

[45] While excessive airframe motions can be caused by last-minute avoiding action or excessive control inputs in response to ACAS RAs (see Appendix I), the accidents in this category are regarded as being caused by hazards other than loss of airborne separation.

[46] This hazard is defined at a much higher level in the Fault Tree than the four other hazards in order to avoid having to define a hazard for each non-MAC accident type. This makes the analysis simpler and is justified on the basis that the risks associated with non-MAC are shown to be small compared with those associated with MAC accidents.

6.6.3 Hazard Consequences (Arg 1.5.2)

By definition, the worst possible consequence of a hazard is an accident and this will occur if all of its consequential mitigations are ineffective. Since the top event of the accident-causation model is an accident, it automatically reveals the means by which each hazard can lead to an accident. The *immediate* consequences of each hazard, and the mitigations that prevent the hazard from producing an accident, can be identified from the intermediate layers of F.1. These are summarised in Table 6[47].

Ref	Hazard	Immediate Consequence	Mitigations
H1	ACAS operations induce non-MAC Accident	Non-MAC Accident	None
H2	ACAS operations induce Possible Collision	Possible Collision	Providence
H3	Ineffective ACAS collision avoidance	Possible Collision	Providence
H4	ACAS operations induce ineffective Separation Provision	Separation Infringement	ACAS and Providence
H5	ACAS operations induce Conflict	Conflict	ATC Separation Provision, ACAS and Providence

Table 6 – Hazard Consequences

It should be noted that in some cases the cause of the hazard and one or more of the potential mitigations for the hazard might be not independent – in such cases, the mitigation(s) concerned might be less effective or totally ineffective.

6.6.4 Hazard Causes (Arg 1.5.3)

All reasonably foreseeable internal and external causes of each hazard have been identified in F.2 to F.8. Each cause is phrased in terms of an event with respect to a Design element or the environment, except for the interactions between ACAS operations and non-MAC accident-avoidance functions shown in F.2. This is because in these cases it is unnecessary to analyse ACAS operations in finer detail in order to identify whether the Functional Safety Requirements mitigate any adverse interactions.

Non-equipage by aircraft subject to the European ACAS II Policy is covered by event C_A6 (ACAS not installed) in Appendix F. A quantified risk model could include an estimate of the number of non-compliant aircraft flying in European airspace.

As explained later in section 6.7.2, the causes have been collated from various sources in order to assure completeness, and have then been organised logically to populate the lowest levels of the risk model. As explained in section 6.6.1 above, some of the hazard causes relate to the normal operation of ACAS and its environment rather than failures.

[47] For clarity, the table excludes the effects of ATM Separation Recovery and See & Avoid

Since the causes have been collated independently from the derivation of the Functional Safety Requirements, they provide a means of checking whether these Safety Requirements are complete. This has been done by analysing the relationships between the hazard causes from the accident-causation model and the Functional Safety Requirements, derived previously under Arg 1.2 to Arg 1.4, to determine whether each cause can be equated to non-compliance. Where this cannot be done, it implies that the Safety Requirements incompletely describe all the required functionality of the Design and its environment during normal operation, resulting in the need to derive further Functional Safety Requirements.

The additional Safety Requirement arising from this analysis is shown in Table 7. The justification for SR_A14 does not come from this analysis but is given in section H.1.3.

Ref	Safety Requirement	Related Causes
	ACAS	
SR_A12	ACAS shall provide collision avoidance indications (RA) against a manoeuvring intruder aircraft on board which ACAS collision avoidance is unavailable[48]	C_C1, C_C2, C_F9
SR_A14	When the monitoring function detects a failure, ACAS shall indicate to the flight crew that an abnormal condition exists	H.1.3

Table 7 – Arg 1.5 Functional Safety Requirements

The results from the analysis of hazards, causes, and compliance with the Functional Safety Requirements are shown in Appendix G. Due to the fact that the accident-causation model comprehensively addresses all hazard causes, some of the causes relate to the normal operation of ACAS and its environment rather than failures, as mentioned in section 6.6.1 above. Furthermore, it also captures causes whose occurrence is considered not to be credible, and some causes which have been considered earlier under Arg 1.4.

Those hazard causes which are relevant to Arg 1.5 have therefore been extracted from Appendix G and are summarised in Table 8 below. This table also shows whether or not the causes are included in the Contingency Tree [32] events referred to in section 6.6.5.

Hazard Ref	Hazard Cause	Cause Ref	Non-compliance with SR	Included in Contingency Tree?
H1	ACAS Collision Avoidance is prioritised over CFIT avoidance	C_N1	SR_F2	NO
H1	ACAS Collision Avoidance is prioritised over stall avoidance	C_N2	SR_F2	NO
H1	ACAS Collision Avoidance is prioritised over windshear avoidance	C_N3	SR_F2	NO
H1	ACAS Collision Avoidance is prioritised over resolution of other potentially harmful flight conditions	C_N4	SR_F2	NO

[48] an implication of satisfying the Safety Requirement is that the intruder must be equipped with an operational altitude-reporting transponder, but this detail has been omitted for clarity

Hazard Ref	Hazard Cause	Cause Ref	Non-compliance with SR	Included in Contingency Tree?
H1	ACAS operations induce potential CFIT	C_N5	SR_A8	NO
H1	ACAS operations induce potential stall	C_N6	SR_F2	NO
H2	ACAS incorrectly resolves encounter[49]	C_A1	SR_A4, SR_A5 or SR_A11	NO
H2 & H5	ACAS active failure[50] (ACAS produces false RA)	C_A2	SR_A3	NO
H3	ACAS inadequately resolves encounter[51]	C_A3	SR_A4	✓
H3	ACAS passive failure (ACAS fails to produce RA)	C_A5	SR_A3 or SR_A4	✓
H4	ACAS produces excessive unnecessary RAs	C_A7	SR_A1 or SR_A9	NO
H1	Flight Crew responds excessively to RA	C_F1	SR_F3	✓
H2	Flight Crew misunderstands sense of RA	C_F2	SR_F2	NO
H3	Flight Crew incorrectly operates ACAS	C_F4	SR_F7	NO
H3	Flight Crew prioritises ATC instruction/clearance over RA	C_F5	SR_F2, SR_F8	✓
H3	Flight Crew prioritises reaction to traffic information over RA	C_F6	SR_F2	NO
H3	Flight crew doesn’t notice RA	C_F10	SR_F2	NO
H3	Flight crew performs inadequate manoeuvre	C_F11	SR_F2	✓
H4	Flight Crew doesn’t report ‘Clear of Conflict’	C_F13	SR_F9	NO
H4	Flight Crew doesn’t report RA	C_F14	SR_F4, SR_F8	NO
H4	Flight Crew interprets a TA as being an RA	C_F15	SR_F1	NO
H4	Flight Crew RA report has missing/incorrect callsign	C_F16	SR_F4	✓
H4	Flight Crew reports RA requiring no deviation from instruction/clearance	C_F17	SR_F4	NO
H4	Controller believes it’s an unnecessary RA	C_C4	SR_C1	NO

[49] Incorrect resolution of encounter would occur, for example, if both aircraft were given descend RAs rather than complementary RAs.

[50] A false RA is one which is produced when the ACAS algorithms in DO-185 do not require any RA.

[51] An inadequate RA is one where the strength of the RA would be insufficient to resolve the encounter.

Hazard Ref	Hazard Cause	Cause Ref	Non-compliance with SR	Included in Contingency Tree?
H4	Controller doesn't notice an RA report	C_C6	SR_C1	NO
H4	Controller misunderstands an RA report	C_C7	SR_C1	NO

Table 8 – Hazard Causes

6.6.5 Safety Requirements for Causes (Arg 1.5.4)

Having derived a set of hazard causes related to failures within the system, it is necessary to demonstrate that the risk they represent is commensurate with the Safety Criteria. EUROCONTROL considers this risk to be best captured via a set of valid, assumed probabilities of the causes, rather than formal Safety Integrity Requirements, for the following reasons:

- the probabilities of those Contingency Tree Events (internal or external to the Design) which are equivalent to hazard causes are themselves assumptions. It is not considered practicable to cast these modelling parameters as formal Safety Integrity Requirements at this stage in the operational life of ACAS.
- at the ICAO level, there are no equivalent integrity requirements which would provide a means of demonstrating compliance with APOSC-derived Safety Integrity Requirements, as required by Arg 2.

In order to determine the risk from system-generated hazards, any overlap between the causes identified as part of Arg 1.5.3 and the Contingency Tree Events first needs to be identified because the contribution to risk from the latter is already accounted for as a component of ACAS MAC net risk reduction. This is illustrated in Figure 16.

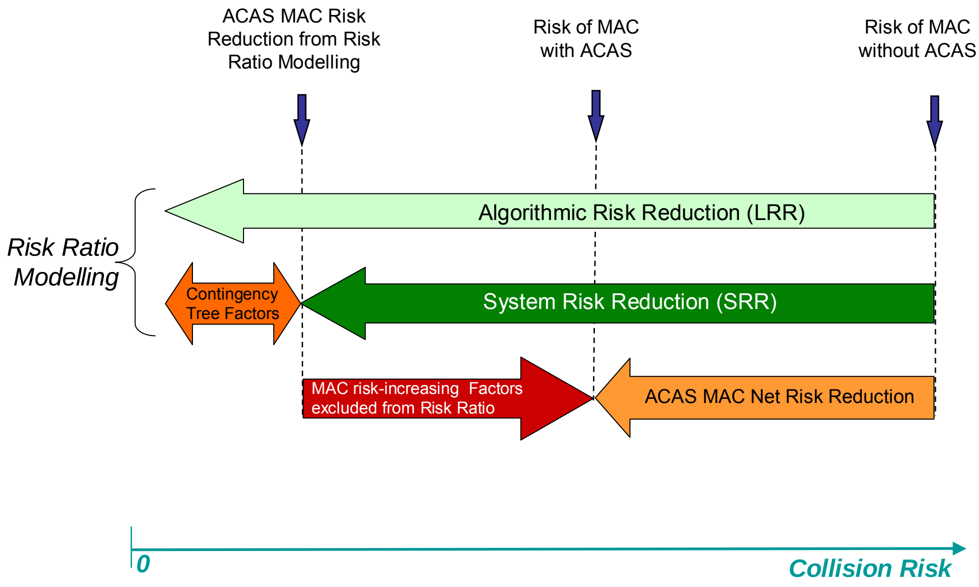

ACAS MAC Risk Reduction from Risk Ratio Modelling
Risk of MAC with ACAS
Risk of MAC without ACAS
Risk Ratio Modelling
Algorithmic Risk Reduction (LRR)
Contingency Tree Factors
System Risk Reduction (SRR)
MAC risk-increasing Factors excluded from Risk Ratio
ACAS MAC Net Risk Reduction
0
Collision Risk

Figure 16 ACAS MAC Risk Reduction Components

It can be seen from Figure 16 that ACAS MAC net risk reduction (depicted originally in Figure 8) comprises the following components:

- algorithmic risk reduction predicted by the dynamic modelling to produce LRR
- the modification of algorithmic risk reduction under the influence of the Contingency Tree factors to produce SRR
- risk increase due to any hazard causes which are not covered by the Contingency Tree factors.

In order to satisfy the Safety Criteria, it is therefore necessary to demonstrate both of the following:

- the risk from MAC hazard causes which are not covered by the Contingency Tree Events is sufficiently small that ACAS MAC net risk reduction remains substantial
- the risk from ACAS-induced non-MAC accident causes is sufficiently small compared to ACAS MAC net risk reduction, thus yielding substantial ACAS accident risk reduction as depicted in Figure 8

This analysis is accomplished using the following steps:

- identifying on the accident-causation model those hazard causes which have an equivalent Contingency Tree Event(s). The relevant causes are shown pictorially in Appendix F and have been designated using the Event Codes in Appendix D. The results are also shown in tabular form in Appendix G.
- determining whether the hazard causes *without* an equivalent Contingency Tree Event have causal mitigations defined as part of the ACAS Design or its

environment (ie via Functional Safety Requirements) by inspection of the accident-causation model and Appendix G.

The results for hazard causes related to failures within the system are summarised in Table 8 in the previous section (indicated by a NO in the column headed "Included in Contingency Tree?"). This shows that all such causes can be equated to non-compliance with the Safety Requirements.

The analysis so far has shown that mitigations for the 'non-Contingency Tree' hazard causes have already been captured via the Functional Safety Requirements. The implication is that the Design includes sufficient functional mitigations, and additional functionality is therefore not required for safety reasons. Hence, it is asserted that the functionality represented by the Design has reduced the risk of an ACAS-induced accident AFARP. However, the analysis has not quantified the risk increase represented by failure to comply with these Safety Requirements due to the finite reliability of the Design elements. Therefore, whereas it might be claimed that Safety Criterion #2 is satisfied with respect to system-generated hazards from 'non-Contingency Tree' causes, the satisfaction of Safety Criterion #1 is not supported by the available evidence.

In order to demonstrate conclusively that the risk increase is sufficiently small for the ACAS accident risk reduction to remain substantial, it would be necessary first to make assumptions about the probabilities of the 'non-Contingency Tree' hazard causes per encounter under the same conditions / assumptions as used for computing SRR. The probabilities would then be incorporated into what would then become a risk model. These causes include the following types of event:

- events related to non-MAC operational occurrences – eg Potential CFIT
- events related to failure modes of avionics equipment; eg ACAS produces false RA, and failure of other on-board accident avoidance systems
- events related to 'failure modes' of the people elements – eg Flight Crew misunderstands sense of RA
- non-equipage by aircraft subject to the European ACAS II Policy,

It is judged by EUROCONTROL that that the probabilities of such events will have been rendered sufficiently low (by means of operational safeguards, and the standard avionics design, certification and support practices mentioned in section 1.3) that the following two risk-increasing components are negligible compared to SRR:

- ACAS-induced non-MAC Accident (Figure 8)
- MAC risk-increasing factors excluded from Risk Ratio (Figure 16)

However, it would be desirable to establish conclusively that this judgement is correct (particularly in view of the non-fatal accident discussed in Appendix I.3). The construction and validation of a fully-quantified accident risk model to demonstrate conclusively that the system-generated hazards satisfy Safety Criterion #1 is, therefore, the subject of a safety issue (**ISS-003**) in section 10.2.

The results in Appendix G show that some hazard causes arise from normal operation. These events are possible because of the way in which ACAS operations have been specified by ICAO. They are as follows:

- Flight Crew initiating (incorrect) See & Avoid in response to TA (C_F12, a cause of H3 and H5)
- Flight Crew requesting guidance from controller in response to TA (C_F7, a cause of H3)
- Controller issuing instruction/clearance to non-ACAS aircraft (that has been (correctly or incorrectly) identified as the threat aircraft causing the RA described in an RA report) (C_C1, a cause of H3)
- Controller issuing traffic information to non-ACAS aircraft (that has been (correctly or incorrectly) identified as the threat aircraft causing the RA described in an RA report) (C_C2, a cause of H3)
- Controller issuing traffic information to RA-incident aircraft (C_C3, a cause of H3)
- Controller has no information about nature of RA (C_C8, a cause of H4)

Even though technical or procedural mitigations exist to deal with each of these events, it would nevertheless be useful to review the operational aspects of ACAS to determine whether change is desirable in order to provide further mitigation of any associated system hazards. The possibility that further mitigation may be necessary / available is captured as Safety Issue **ISS-004** in section 10.2.

6.6.6 Safety Requirements for Mitigations (Arg 1.5.5)

The external mitigations for the hazards are identified in Table 6 and they all correspond to existing functions within the Conflict Management Model of Figure 5. As these functions are established parts of civil aviation, it is not necessary (with the exception of ACAS itself) to capture Functional Safety Requirements or assumptions for these mitigations as part of the Safety Case.

The requirement for independence between ATC and ACAS is part of the ACAS Fundamentals (section 2.2.4). However, independence cannot be complete, since Separation Provision, Separation Recovery and ACAS all rely on aircraft barometric-height measurement and Flight Crew, which can introduce common causes of failure - this is illustrated by the case of the Brazilian mid-air collision in 2006, as explained in Appendix I, section I.4 below.

Similarly, See & Avoid on the part of the Flight Crew as an additional mitigation to ACAS failures is not independent of ACAS since both rely on the Flight Crew and the Flight Crew may use TA information which is itself derived from ACAS to identify an intruder.

6.6.7 Conclusions to Arg 1.5

A risk assessment has identified five hazards at the boundary of the Design, of which four are related to MAC. The consequences of all five hazards have been determined using an accident-causation model. The structure of the MAC part of this model has been based upon the barriers of the Conflict Management model in Figure 4.

The accident-causation model has also been used to elaborate the hazard causes arising from the elements of the Design or the environment. These causes have been used as an aid to completing the set of Functional Safety Requirements derived under Arg 1.2 to Arg 1.4 by revealing causes for which there was no corresponding functionality already defined as part of the Design or its environment.

The causes have then been compared with the Contingency Tree Events in order to identify those causes due to system failure whose accident risk is not already accounted for by the System Risk Ratio. It is concluded that the risk from these causes will be compatible with Safety Criterion #2, ie reduced AFARP, where there is a Functional Safety Requirement specified which acts as a mitigation. However, the assertion that the risk is small enough to satisfy Safety Criterion #1 can only be substantiated by development of a fully quantified version of the accident-causation model, which depends upon aircraft-related evidence. Meanwhile, satisfaction of Safety Criterion #1 relies on the assumption that the currently un-quantified components of risk within the model can be considered negligible due to the influence of normal aircraft operational safeguards, and avionics design, certification and support practices. The development of a fully quantified risk model remains as a Safety Issue (**ISS-003** in section 10.2) so that this assumption can be validated.

A number of potential hazard causes associated with ACAS normal operation were also revealed which, although mitigated elsewhere in the system, might be amenable to further mitigation by modifications to procedures. This is also the subject of a Safety Issue (**ISS-004)**.

The accident-causation model has also facilitated the identification of existing external and internal mitigations to the hazards. Internal mitigations are already satisfied by the Functional Safety Requirements, and additional Safety Requirements covering the independence of well-established external mitigations are also specified.

Overall, Arg 1.5 is considered to be adequately substantiated subject to resolution of Safety Issues **ISS-003** and **ISS-004**, as above.

6.7 Evidence Validity (Arg 1.6)

6.7.1 Strategy

Arg 1.6 is concerned with demonstrating that the Evidence used to support the sub-arguments of Arg 1.1 to 1.5 is trustworthy. Whereas these previous sub-arguments are concerned with using items of Evidence to substantiate their assertions, they do not in themselves provide assurance that each item of Evidence is complete and correct in its own right – ie that it is valid to use the Evidence in the Safety Case. In general, there are no absolute criteria for establishing completeness and correctness of a given piece of evidence, rather the assurance arises from the fact that established processes have been used to create and check it, and have been applied by suitably competent people.

Arg 1.1 to 1.5 make use of two basic forms of Evidence:

- Evidence produced specifically for the purposes of supporting the safety argument and documented within the Safety Case (internal Evidence)
- Pre-existing Evidence originally produced for other purposes, but used to support the safety argument and cited by the Safety Case (external Evidence)

Therefore, in order to argue that the Evidence for safety specification is valid, it is necessary to show that the following sub-arguments are true, as shown in Figure 17:

Arg 1.6.1.1. The internal Evidence has been produced and checked using established processes.

Arg 1.6.1.2. The internal Evidence has been produced and checked by competent people.

Arg 1.6.2.1. The external Evidence has been produced and checked using established processes.

Arg 1.6.2.2. The external Evidence has been produced and checked by competent organizations.

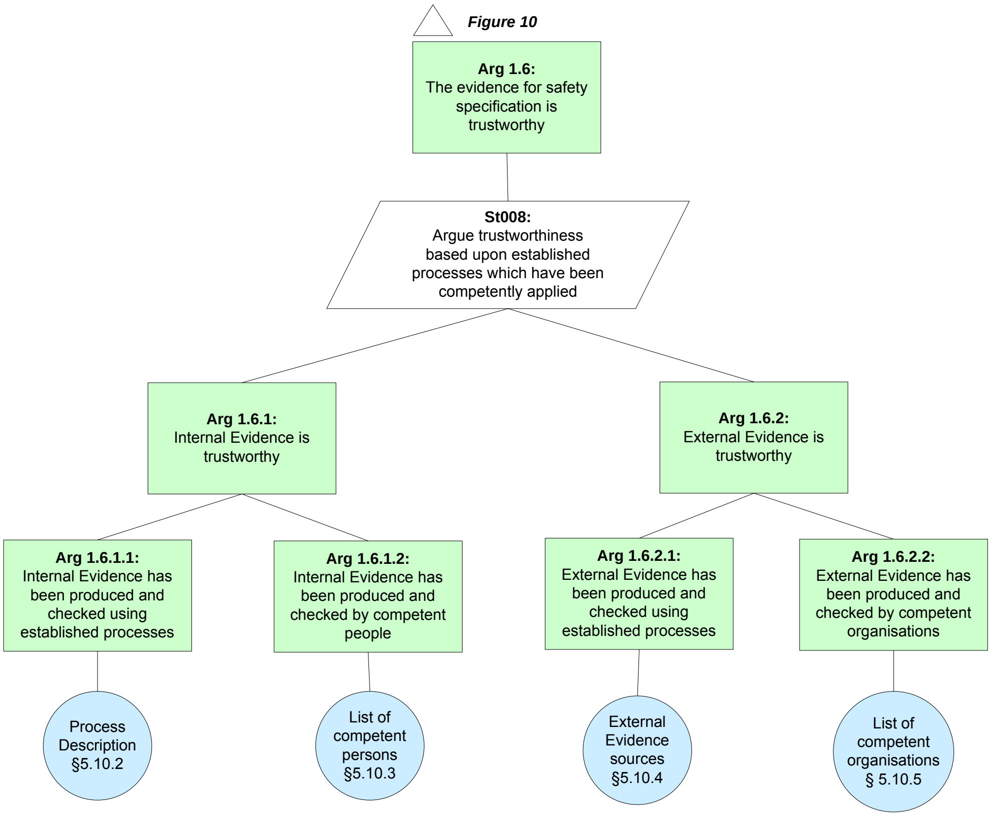


Figure 10
Arg 1.6: The evidence for safety specification is trustworthy
St008: Argue trustworthiness based upon established processes which have been competently applied
Arg 1.6.1: Internal Evidence is trustworthy
Arg 1.6.2: External Evidence is trustworthy
Arg 1.6.1.1: Internal Evidence has been produced and checked using established processes
Arg 1.6.1.2: Internal Evidence has been produced and checked by competent people
Arg 1.6.2.1: External Evidence has been produced and checked using established processes
Arg 1.6.2.2: External Evidence has been produced and checked by competent organisations
Process Description §5.10.2
List of competent persons §5.10.3
External Evidence sources §5.10.4
List of competent organisations § 5.10.5

Figure 17 Evidence Validity

These sub-arguments are addressed in turn, in sections 6.7.2 to 6.7.5 below. Conclusions regarding Arg 1.6 are then drawn in section 6.7.6.

6.7.2 Processes for Internal Evidence (Arg 1.6.1.1)

The internal evidence used by Arg 1.1 to 1.5 comprises the ACAS Fundamentals, ACAS Design, and the accident-causation model.

As discussed in section 2.1, the Fundamentals and Design have both been created by abstraction of information from ICAO and other existing ACAS documentation. No specific documented process was used to perform this abstraction.

Section 6.6.2 goes on to explain that the accident-causation model has been constructed primarily by collating information from the FARADS FHA/PSSA [33]. The FARADS information was produced in accordance with EUROCONTROL SAM using the competent personnel identified in the FHA/PSSA report. The unstructured information has then been used to populate the lower levels of a hierarchical accident-causation model derived from the relevant parts of the Integrated Risk Picture developed by EUROCONTROL EEC [34]. No specific documented process was used to construct the accident-causation model from its various sources.

6.7.3 Personnel for Internal Evidence (Arg 1.6.1.2)

Given that the internal evidence is an integral part of the Safety Case, it has been produced and checked by the Safety Case developers, who are as follows:

Name	Affiliation	Role
John S. Law MA	EUROCONTROL DAP/SUR	Mode S and ACAS Programme Manager
Stanislaw J. Drozdowski MA (Econ)	EUROCONTROL DAP/SUR	APOSC Project Manager
Stephen M. Thomas BSc PhD CEng MIET	Entity Systems Ltd	Safety Expert

In addition, the Safety Case has been independently reviewed by the following experts:

Name	Affiliation	Role
Henry J. Hutchinson BSc	QinetiQ	ACAS Expert
Kenneth M. Carpenter MA PhD FRIN	QinetiQ	ACAS Expert
Ronald H Pierce MSc CEng FBCS	JDF Consultancy LLP	Safety Consultant
Derek Fowler BSc CEng FIET	JDF Consultancy LLP	Safety Consultant

6.7.4 Processes for External Evidence (Arg 1.6.2.1)

The external evidence used by Arg 1.1 to 1.5, and the processes employed to produce and check it, comprise the following:

Evidence Item	Production and Checking Processes
ICAO Annex 2 ICAO ACAS Manual	Standard ICAO processes
RTCA DO-185A	Standard RTCA processes

Evidence Item	Production and Checking Processes
Results from modelling of ACAS operations	Long term development of models derived from DO-185A algorithms, expert judgement informing model structure and parameter values, partial validation of models via peer review, comparison of results between model users, and comparison of models with real encounters
Results from: ACAS Flight trials (UK and USA), TCAS II Certification trials, TCAS II Limited Installation Programme	The documented procedures used by the originators are unknown to EUROCONTROL but are taken to be well-established, since the activities were conducted by reputable and long-standing aviation organisations considered competent to do so by ACAS stakeholders.
ACAS Monitoring Reports	EUROCONTROL processes
Results from simulated reconstruction of individual real encounters	Application of InCAS and OSCAR tools [section 6.4.4]

With the exception of ACAS Monitoring Reports, EUROCONTROL does not have access to any formally documented procedures used by the originators for producing and checking these evidence items.

The Safety Claim depends heavily on the validity of ACAS modelling results used to support Arg 1.1.4 and 1.3.5. According to the model developers, there has been no documented, formal validation exercise on these models [22]. However, they have resulted from long-term development over the life of ACAS, which has included various checks on the validity of different parts of the models and collaboration between the organisations involved in the ACAS modelling studies. The Contingency Tree structure, its Events and probabilities have been developed with the benefit of peer review by ACAS experts.

It is therefore argued that the models have been validated as far as practicable by their developers. They have resulted from long-term development over the life of ACAS, which has included various checks on the validity of different parts of the models and collaboration between the organisations involved in the ACAS modelling studies. The Contingency Tree structure, its Events and probabilities have been developed with the benefit of peer review by ACAS experts.

6.7.5 Organisations for External Evidence (Arg 1.6.2.2)

The external evidence has been produced by the following reputable organisations:

Evidence Item	Originator
ICAO Annex 2 ICAO ACAS Manual	ICAO
RTCA DO-185A	RTCA
Results from modelling of ACAS operations	DSNA, QinetiQ, Sofréavia
Results from: ACAS Flight trials (UK and USA), TCAS II Certification trials, TCAS II Limited Installation Programme	UK CAA, FAA, ICAO, Honeywell, Northwest Airlines, ARINC Research Corporation

ACAS Monitoring Reports	EUROCONTROL
Results from simulated reconstruction of individual real encounters	EUROCONTROL, Egis Avia, *et al*

6.7.6 Conclusions to Arg 1.6

The internal evidence created as an integral part of the Safety Case has in general been derived without use of a formal process. However, it has been produced and checked by a range of suitably competent personnel.

The external evidence, on the other hand, has generally been produced using well-established processes for documenting aviation standards, conducting trials, and performing in-service monitoring. The exception is the modelling of ACAS operations, which as a series of studies, has received some *ad hoc* validation of its component parts but no formal validation of its results as such. However, in all cases, the external evidence has been produced by organisations who are expert in the given field. Therefore, the provision of additional evidence with respect to the validity of ACAS modelling is not seen as essential to the Safety Case. Arg 1.6 is therefore reasonably substantiated.

6.8 Conclusions to Arg 1 – Safety Specification

An assessment of the ACAS Fundamentals and supporting modelling results has demonstrated that ACAS has the potential to deliver a significant reduction in the risk of mid-air collision when exposed to encounters typical of its operational environment. Moreover, it does so without any inherent adverse safety implications elsewhere in its operational environment. The ACAS concept is therefore intrinsically safe and Arg 1.1 is substantiated.

The ACAS Logical model correctly interprets the ACAS Fundamentals. A set of Functional Safety Requirements has been derived for its elements which, if implemented, will enable ACAS to provide the intrinsic safety originating from the concept. Arg 1.2 is therefore substantiated.

Assessment of the ACAS Design, results from ACAS modelling, trials and operational use, collectively demonstrate that the ACAS Design works correctly under normal environmental conditions. Furthermore, the Design is shown to be compatible with the operation of other accident avoidance systems and ATM except for the outstanding Safety Issue (**ISS-001**) concerning the continuing uncertainty about the feasibility of RA Downlink and its potential benefits in mitigating possible adverse interactions between ACAS and ATM caused by Controller's being unaware of the existence of some extant RA events.

The collision-risk-reduction capability of the Design is demonstrated by ACAS modelling studies which exploit a Contingency Tree to represent the real-world factors that can influence ACAS operations. The modelling results show that ACAS operations are capable of producing substantial collision-risk reduction (by approximately a factor of 5) commensurate with Safety Criterion #1. Moreover, since the Design represents the culmination of many years of ACAS development, it is also asserted that collision risk has been reduced AFARP in relation to the Design, in line with Safety Criterion #2. These two conclusions do not take account of the failure risk assessment discussed in the next-but-one paragraph – with that proviso, and subject to resolution of Safety Issues **ISS-001** to **003**, Arg 1.3 is substantiated.

The robustness of the ACAS Design has been demonstrated by first elaborating those aspects of its environment whose abnormal behaviour either has not already been covered implicitly under Arg 1.3, or is best covered under Arg 1.5 later. In order to prevent inappropriate collision-avoidance action in the presence of such abnormalities, a number of additional Functional Safety Requirements are specified to ensure that ACAS reacts safely by ceasing to provide collision avoidance guidance while an abnormality exists. Arg 1.4 is therefore substantiated.

A failure-hazard assessment has identified five hazards at the boundary of the Design, of which four are related to MAC. The consequences of all five hazards have been determined using an accident-causation model, along with their causes. It is concluded that the risk from these causes will be compatible with Safety Criterion #2, ie reduced AFARP, where there is a Functional Safety Requirement specified which acts as a mitigation. However, the possibility that other mitigations may be available has also been identified and, should therefore be investigated in line with the AFARP principle (Safety Issue **ISS-004**).

The assertion that the risk is small enough to satisfy Safety Criterion #1 can only be substantiated by development of a fully quantified version of the accident-causation model although it is likely that will be found to be negligible - the development of a such a model remains as a Safety Issue (**ISS-003**)

Therefore, Arg 1.5 is substantiated subject to resolution of Safety Issues **ISS-003** and **ISS-004**.

The internal evidence created as an integral part of the Safety Case has in general been derived without use of a formal process. However, it has been produced and checked by a range of suitably competent personnel. The external evidence, on the other hand, has generally been produced using well-established processes for documenting aviation standards, conducting trials, and performing in-service monitoring. In all cases, the external evidence has been produced by organisations who are expert in the given field. Arg 1.6 is therefore substantiated.

Since all six of its offspring are otherwise substantiated, Arg 1 is substantiated subject to resolution of Safety Issues **ISS-001**, **ISS-002**, **ISS-003** and **ISS-004**.

7 IMPLEMENTATION OF THE SPECIFICATION (ARG 2)

7.1 Strategy (St009)

Arg 2 is concerned with demonstrating that ACAS operations have been implemented in accordance with the specification.

In the context of this argument, the *specification* means the ACAS Design and its associated Functional Safety Requirements. As discussed in section 2.1, the Safety Case considers any definition of ACAS operations below the level of ACAS Design as being part of the implementation of ACAS. Specifically, these implementation levels comprise ICAO regulations, regional regulations, industry specifications, and the documentation and creation of the Design elements described in section 2.2.7 by individual organisations worldwide. While the position could be taken that it would be sufficient for the Safety Case to demonstrate correct implementation of the ACAS Design at the level of the relevant ICAO regulations, evidence of correct implementation at the airborne equipment level is provided here.

The implementation argument is therefore based upon the following three sub-arguments, as shown in Figure 18:

Arg 2.1. ACAS internationally applicable Operational and System requirements conform to the ACAS Design.

Arg 2.2. ACAS operations conform to internationally applicable ACAS Operational and System requirements.

Arg 2.3 Correct dynamic behaviour of ACAS implementation has been demonstrated.

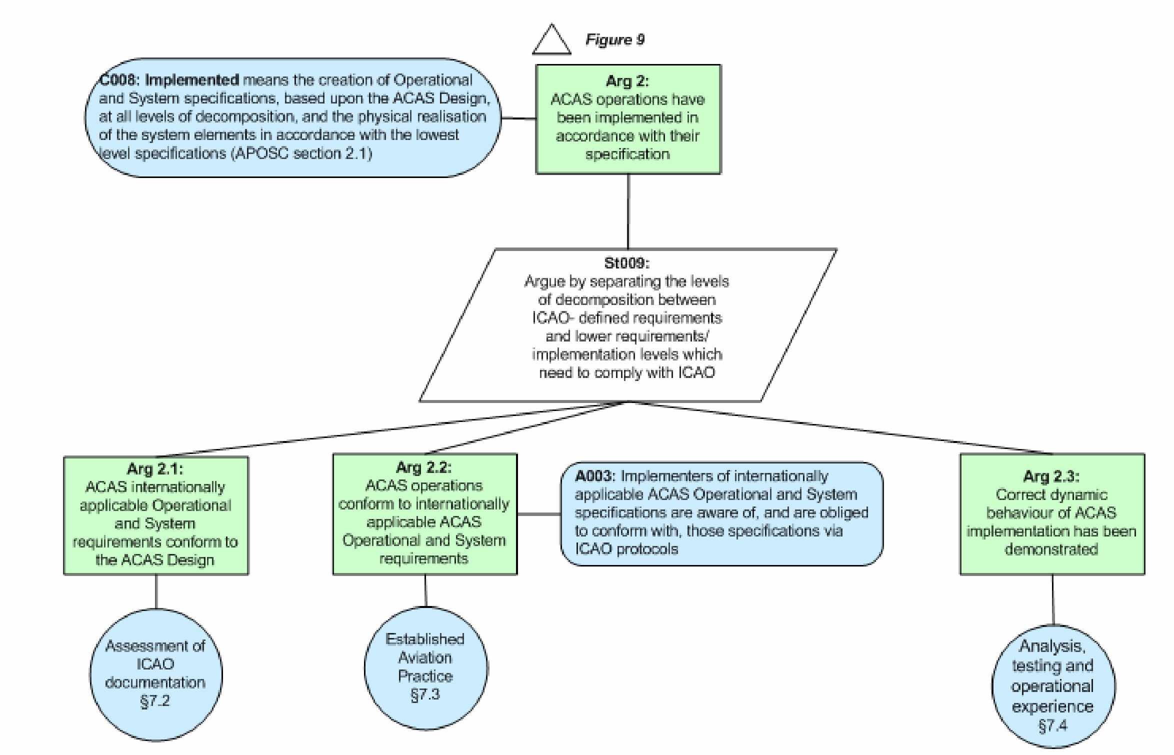


Figure 9
C008: Implemented means the creation of Operational and System specifications, based upon the ACAS Design, at all levels of decomposition, and the physical realisation of the system elements in accordance with the lowest level specifications (APOSC section 2.1)
Arg 2: ACAS operations have been implemented in accordance with their specification
St009: Argue by separating the levels of decomposition between ICAO- defined requirements and lower requirements/ implementation levels which need to comply with ICAO
Arg 2.1: ACAS internationally applicable Operational and System requirements conform to the ACAS Design
Arg 2.2: ACAS operations conform to internationally applicable ACAS Operational and System requirements
A003: Implementers of internationally applicable ACAS Operational and System specifications are aware of, and are obliged to conform with, those specifications via ICAO protocols
Arg 2.3: Correct dynamic behaviour of ACAS implementation has been demonstrated
Assessment of ICAO documentation §7.2
Established Aviation Practice §7.3
Analysis, testing and operational experience §7.4

Figure 18 Implementation

These sub-arguments are addressed in turn, in sections 7.2 to 7.4 below. Conclusions regarding Arg2 are then drawn in section 7.5.

7.2 Implementation of ACAS Design (Arg 2.1)

The argument that internationally applicable Operational and System specifications conform to the ACAS Design is supported by evidence from a systematic assessment of the ICAO documentation cited in section 2.1 against the ACAS Safety Requirements shown in Appendix B. The results of the assessment are shown as Appendix H. This assessment also addresses the degree and extent of the coherency within and between the ICAO ACAS provisions[52].

The results from the assessment reveal the following:

- There is conformity between ICAO equipment provisions and ACAS Safety Requirements;
- There are some ambiguities and inconsistencies within ICAO Flight Crew provisions, some of which have produced non-compliances with the associated ACAS Safety Requirements;
- There are some ambiguities and inconsistencies within ICAO Air Traffic Controller provisions;
- There are no ICAO provisions dealing with the independence between ATM Separation Provision and Separation Recovery, and ACAS.

Any ambiguity in the operational requirements could in principle lead to their potentially hazardous misapplication. However, the ICAO provisions, like the ACAS equipment itself, have arisen from many years of experience with ACAS operations and, **with one exception** (see after the table below), the detected ambiguities are not considered serious enough to undermine the Safety Case. Even the presence of non-conformity with a particular Safety Requirement does not imply that ACAS operations are *unsafe (*ie that the accident risk with ACAS is greater than without it), rather it means that ACAS might not be as fully effective as it would otherwise be.

A summary of the discrepancies between the safety requirements and the ICAO specifications, and the major inconsistencies within the ICAO requirements, are given in the following table. Further details are given in Appendix H.

Summary of Discrepancy	Appendix H reference
PANS-OPS section 3.2c)4) *as soon as possible, as permitted by flight crew workload, notify the appropriate ATC unit of any RA which requires a deviation from the current ATC instruction or clearance* differs from Safety requirement SR_F4. This discrepancy is already raised as ISS-002 in section 6.4.5.	H.2.1
The terminology in PANS-OPS 3.1.2 '*resolve a traffic conflict or avert a potential collision'* is different from the terminology *'best avert collision'* used in the corresponding provision in Annex 2 para 3.2.	H.2.2

[52] See Appendix L hereto for a summary of the ICAO ACAS Provisions

PANS-OPS section 3.1.2 *Nothing in the procedures specified in 3.2, "Use of ACAS indicators", shall prevent pilots-in-command from exercising their best judgement and full authority in the choice of the best course of action to resolve a traffic conflict or avert a potential collision* is contradictory to some of the Flight Crew safety requirements	H.2.3
In ICAO Annex 2 section 3.2, *'collision avoidance manoeuvres'* should be changed to *'actions'* since an RA might not involve a manoeuvre, and *'based on'* should be changed to *'in response to'* to be consistent with PANS-OPS.	H.3.2
ICAO provisions in Annex 2 section 3.2 *Nothing in these rules shall relieve the pilot-in-command of an aircraft from the responsibility of taking such action, including collision avoidance manoeuvres based on resolution advisories provided by ACAS equipment, as will best avert collision* are contradictory to PANS-OPS 3.2.1c) 1)	H.3.3
The conformity assessment has raised numerous comments on PANS-ATM provisions	H.4.2

Although these points may seem to be purely semantic, there is a serious underlying concern in relation to the intent behind the wording of PANS-OPS section 3.1.2 and Annex 2 section 3.2, and the possibility that misinterpretation could lead to inconsistent pilot responses to an RA because these two provisions override what would otherwise be a clear requirement for the Flight Crew to always follow an RA even if given a contrary instruction by ATC. For example, it would not be unreasonable to suggest that the actions of the B747 pilot in the Yaizu incident and the TU154 pilot in the case of the Überlingen accident (for both, see Appendix I below) as falling within what is permitted by PANS-OPS section 3.1.2 rather than contravening PANS-OPS section 3.2[53].

Therefore, this and the other remarks in H.2.2, H.3.2 and H.4.2, and the Conclusions in H.2.3 and H.3.3, are raised as safety issue **ISS-005** in section 10.2.

7.3 Implementation of International Specifications (Arg 2.2)

In accordance with the strategy in section 7.1, the argument that ACAS operations conform to internationally applicable ACAS Operational and System specifications is based on the single assertion that this aspect falls within established aviation practices for introducing changes triggered at the ICAO level. These practices provide for progressive transposition of ICAO requirements down to specification and realisation of ACAS-related equipment, procedures, and training.

The assertion therefore relies upon an assumption that implementers of internationally applicable ACAS Operational and System specifications are aware of, and are obliged to conform with, such specifications via established protocols **(Assumption A003)**.

[53] The use of the Yaizu and Überlingen examples in this discussion are not intended to challenge in any way the findings of the inquiries which followed these accidents – rather they are intended only to illustrate the possible consequences of ambiguity in PANS-OPS leading to an accident serious or incident in the future. In fact Safety Recommendation No. 18/2002 of the Überlingen accident report [51][50] recommends that "*ICAO should change the international requirements in Annex 2, Annex 6 and PANS-OPS (DOC 8168) so that pilots flying are required to obey and follow TCAS resolution advisories (RAs), regardless of whether contrary ATC instruction is given prior to, during, or after the RAs are issued. Unless the situation is too dangerous to comply, the pilot flying should comply with the RA until TCAS indicates the airplane is clear of the conflict*"

7.4 Correct Dynamic Behaviour of ACAS Has Been Demonstrated (Arg 2.3)

The evidence that the implementation of ACAS operations possesses correct dynamic behaviour comes from the reports summarised below. This evidence comprises analysis, testing and operational (field service) experience.

- Modelling of ACAS operations [21][22][24]
- Flight trials of ACAS (UK and USA) [25][26]
- TCAS II Certification Trials [25][27]
- TCAS II Limited Installation Programme [28]
- ACAS Monitoring Reports [35][36][37][38]
- Simulated reconstruction of individual real encounters by *inter alia* EUROCONTROL EEC and Egis Avia, using the InCAS (Interactive Collision Avoidance Simulator) [39] and OSCAR (Off-line Simulator for Collision Avoidance Resolution) [40] tools, respectively

There have been several safety studies [21][22][24] which have used non-real-time dynamic models to predict the reduction in collision risk that ACAS operations will provide. In order to achieve their objective, the models contain the elements in the Design and variables for the range of Airframe Movements during encounters, the range of Flight Crew capabilities, and Equipage. The fault-free behaviour of these models provides evidence that they are dynamically correct. Therefore, if the models and parts of the ACAS implementation are functionally equivalent, the correct behaviour of the models provides assurance that those parts of the implementation are also correct.

The models have used ACAS algorithms which are based upon an internationally used standard for the ACAS equipment [9][8], and a pilot-response model which has been developed via [41][42][43][44][45]. Consequently, each element in the model complies with its associated specification at the implementation level of ACAS thus providing assurance that those parts of the implementation are dynamically correct.

Non-real-time execution of a dynamic model does not, however, conclusively demonstrate that the Design behaves correctly when subject to real-time operation in its natural environment. Evidence to support these aspects of the Design comes from the behaviour of the physical system during flight trials [25][26] and during operational use (limited installation programme [28], monitoring during routine operations [35][36][37][38], and associated encounter reconstructions using simulation tools [39][40]). At each of these stages in its evolution, any deficiencies in the behaviour of ACAS have been corrected via an amendment to the relevant specifications.

7.5 Conclusions to Arg 2

The Safety Case includes a mixture of direct and indirect evidence that ACAS operations have been implemented in accordance with their specification. An assessment of the ICAO ACAS provisions against the ACAS Safety Requirements has shown that, while there is a high degree of conformity overall, there remain some residual weaknesses within the provisions related to the operational aspects which should be investigated and resolved. The general conformity of actual ACAS operations (subject to the fact that human performance and equipment reliability are not perfect) with the ICAO provisions is argued on the basis of established aviation practices; hence relying on an assumption (**A003**) rather than on evidence. However, as pointed out in **ISS-005** in section 10.2, the validity of assumption A003 is undermined by discrepancies in the ICAO provisions themselves. Thus the substantiation of Arg 2 depends on ISS-005 being resolved.

There is sufficient evidence of the correct dynamic behaviour of the implementation of ACAS to support the argument concerning the dynamic behaviour of the ACAS Design, under Arg 1.3.3 – see section 6.4.4 above.

8 OPERATIONAL SERVICE (ARG 3)

8.1 Strategy St010

Arg 3 is concerned with demonstrating that ACAS is acceptably safe in operational service. For a *post-implementation* Safety Case on a mature operational system, due emphasis should be placed on in-service behaviour of the system to vindicate the *a priori* arguments about safety of the specification and implementation.

Inevitably, the argument can only be supported by the results from processes currently applied to ACAS during the operational phase. The safe operations argument is therefore based upon the following three sub-arguments, as shown in Figure 19:

Arg 3.1. The overall safety benefit of ACAS has been demonstrated in service through safety monitoring.

Arg 3.2. There have been effective measures, in place and correctly applied, to identify and eliminate any safety problems associated with ACAS operations.

Arg 3.3. The evidence for safety of operations is trustworthy.

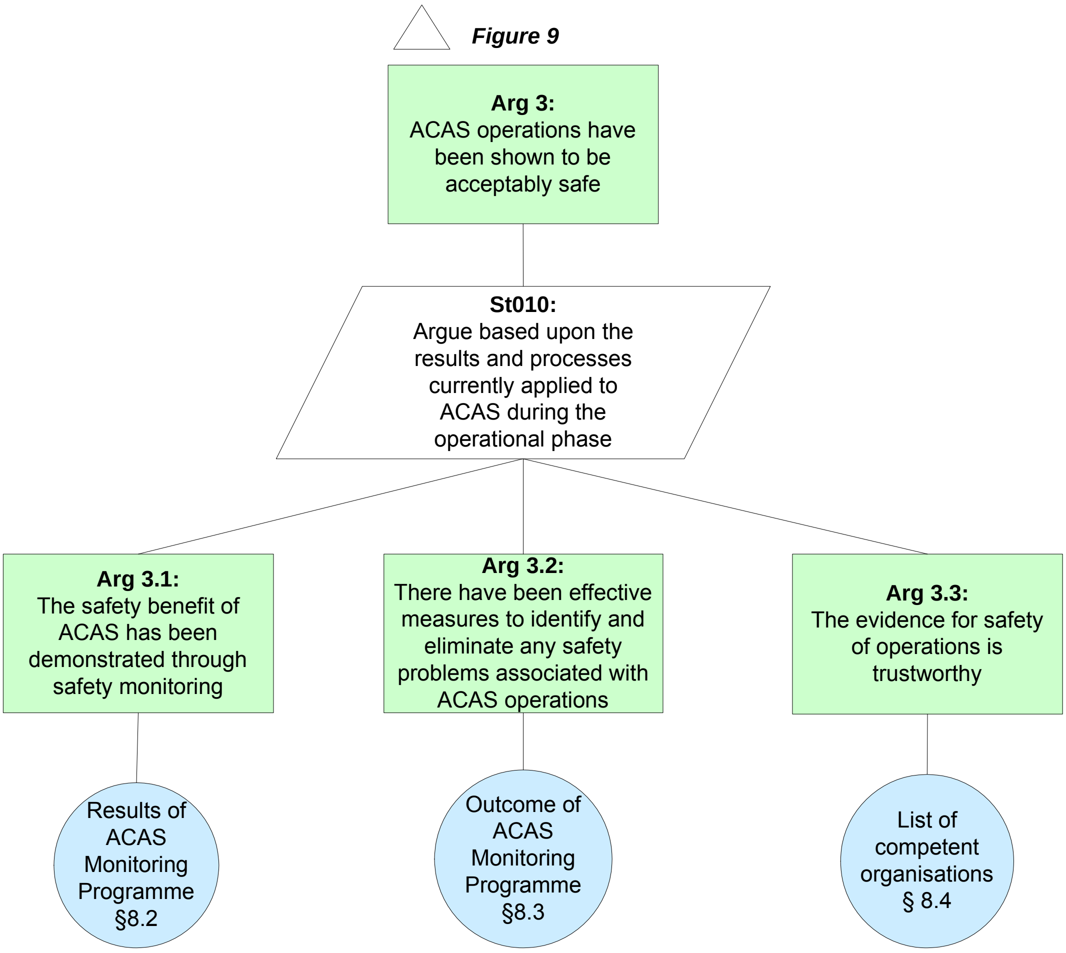


Figure 9
Arg 3:
ACAS operations have been shown to be acceptably safe
St010:
Argue based upon the results and processes currently applied to ACAS during the operational phase
Arg 3.1:
The safety benefit of ACAS has been demonstrated through safety monitoring
Arg 3.2:
There have been effective measures to identify and eliminate any safety problems associated with ACAS operations
Arg 3.3:
The evidence for safety of operations is trustworthy
Results of ACAS Monitoring Programme §8.2
Outcome of ACAS Monitoring Programme §8.3
List of competent organisations § 8.4

Figure 19 Safe Operations

These sub-arguments are addressed in turn, in sections 8.2 to 8.4 below. Conclusions regarding Arg3 are then drawn in section 8.5.

8.2 Safety Monitoring (Arg 3.1)

This section examines the evidence to support the claim that the safety benefits of ACAS are demonstrated through safety monitoring. Much of the evidence to support the argument in this section has already been introduced, in relation to ACAS Implementation, in Arg 2.3.

As intimated in section 4.4 earlier, it can be impracticable to demonstrate achieved risk reduction afforded by safety nets due to the extremely small event frequencies of interest. This is verified by a statement in the ASARP study [24] that radar data[54] used to fit the Encounter model cannot be used to assess the efficacy of ACAS in operation due to the horizontal miss distance associated with most of the observed encounters. This leads to a fundamental difficulty that in-service data cannot be used to determine the System Risk Ratio (SRR) achieved by ACAS in operation.

Individual ACAS occurrences are nevertheless subject to mandatory reporting by Flight Crew and Controllers. The requirements mean that significant ACAS events, including RAs, are reportable [5], whereas TAs are not reportable. This reporting requirement forms the basis for analysis of ACAS operational experience.

As mentioned in section 6.4.4, ACAS has been subject to a European ACAS monitoring programme [35][36][37][38]. Among other things, this collates information about ACAS reported occurrences and presents statistics on the various operational aspects. Analysis of information collected during the PASS project indicates that there are some 18 ACAS RAs generated per day in the ECAC area, or around 6500 per year [53], corresponding to one RA in 2160 flight hours[55].

Regardless of which of the above figures for the number of RAs per flight hour is correct, the collated information does not permit the calculation of ACAS risk-reduction capability and it is therefore not a *safety* monitoring process, strictly speaking, for the following reasons:

1. The majority of RAs are generated by aircraft descending or climbing with high vertical rate, where the aircraft levels off at its cleared, correctly-assigned flight level before close approach actually occurs; and
2. even where the RA is not caused by this situation, there will usually be sufficient horizontal or vertical distance, or both, between the subject aircraft at the point of closest approach, to avoid an accident.

Therefore, only a very small fraction of the total number of encounters leading to recorded RAs would have resulted in an accident, and while it is likely that at least some accidents have been avoided by ACAS, there is insufficient data available to quantify this fraction.

Simulated reconstruction of real encounters has also been used in order to investigate the behaviour of ACAS during specific individual encounters of interest, and was also referred to previously in section 6.4.4. However, whereas these

[54] As used to fit the Encounter model used in ACAS modelling studies

[55] During the development of the APOSC, it was noted that the report on the 2007 Dübendorf workshop on STCA/ACAS Interaction & Interoperability [57] states that "*…in reality, 1 in 10^6 RAs prevents a collision - ie the rate at which RAs are generated is 1 in 300 flying hours while the rate at which collisions occur is 1 in 3 x 10^6 flying hours*". This is a much higher rate of RAs than that stated in reference [53], and the relevant paper in the STCA/ACAS Interaction & Interoperability Workshop [57] as a whole casts some doubt on the risk reduction achieved by ACAS. If it were true that only 1 in 10^6 RAs prevented a collision this would imply that ACAS will prevent only one collision every 150 years (approximately), assuming that the figure of 1 RA in 2160 flight hours is correct, but has already contributed to one collision during its operational life - this was raised as Safety Issue ISS-006 in section 10.2. However, the discrepancy between these figures for the number of RAs per flight hour has now been investigated and the figure stated in [57] has been confirmed to be purely illustrative – see now Appendix K.

reconstructions serve to demonstrate the degree to which ACAS provided a safety benefit in a given encounter, they can give no statistical measure of collision-risk reduction across the airspace.

In-service data and its analysis do not therefore provide direct evidence that ACAS in operation provides a substantial reduction in the risk of an accident (Safety Criterion #1). Whereas they do provide qualitative evidence that ACAS has been effective (or otherwise) in resolving the individual real encounters selected for further analysis, there is no basis for considering this to be a quantitative indication of the safety benefit from ACAS operations in general.

8.3 Rectification of Operational Problems (Arg 3.2)

The ACAS monitoring programme also identifies and analyses operational issues. Any significant issues so identified form the basis for proposing operational or technical modifications. The process was well-established via the EMOTION-7 (European Maintenance of TCAS II version 7.0) project [46] and in the past has resulted in changes being made to ACAS in order to eliminate operational problems.

Any detected operational problems would, by implication, be detrimental to safe ACAS operations. Therefore, their elimination produces a progressive improvement in safety regardless of the collision-risk reduction actually being achieved by ACAS, in line with the AFARP principle (Safety Criterion #2).

An example of safety improvement to the operational requirements for ACAS arising from problem rectification is provided by TCAS II version 7.1. This version introduces two important changes:

i. Change proposal (CP) 112E – improvement of the RA reversal logic in the case where one aircraft fails to obey a climb or descend RA (see Appendix I.2) or one aircraft is unequipped but is manoeuvring in the same vertical sense as the equipped aircraft.

ii. CP 115 – introduction of the RA announcement “Level off, level off” to replace “Adjust vertical speed, adjust” which some flight crew find ambiguous, and requires the TCAS display to be examined to determine the indicated vertical speed to be achieved and whether an increase or decrease is required.

EUROCONTROL proposed that the carriage of TCAS II version 7.1 be mandatory in ECAC airspace (see [56]). However, as the need for CP 112E was demonstrated in the Überlingen accident report more than eight years ago, as one means by which that accident could have been prevented, a mandate for TCAS II version 7.1 should be expedited and the matter should remain an open Safety Issue (**ISS-07**) until the mandate has taken effect.

Therefore, it is asserted that, subject to resolution of Safety Issue **ISS-007** (as well as the other six Safety Issues, at section 10.2) this process has allowed Safety Criterion #2 (ie risk reduced AFARP) to be satisfied by minimising any adverse behaviour of ACAS[56]. However, it order for this assertion to remain true in the future, it is essential to continue to monitor and correct operational problems that

[56] as opposed to satisfying Safety Criterion 2 by maximising ACAS algorithmic risk reduction

might occur as a result of deliberate changes to, and / or insidious degradation in, the operation of ACAS – see section 9.3 and 9.4 below.

Publisher's note (25 November 2011):

European Commission is expected to publish by the end of 2011 a Commission Regulation requiring that all aircraft currently equipped with TCAS II version 7.0 will need to be upgraded to version 7.1 by 1 December 2015 in order to continue to operate in the airspace of European Union. All new aircraft above 5,700 kg Maximum Take-off Mass or passenger seating capacity above 19 will have to be equipped by 1 March 2012.

8.4 Evidence Validity (Arg 3.3)

As for Arg 1.6, the assurance that the evidence for safety of operations is trustworthy arises from the fact that established processes have been used to create and check it, and these processes have been applied by suitably competent people.

The evidence used by Arg 3.1 and 3.2, the originator, and the processes employed to produce and check it, comprise the following:

Evidence Item	Originator of Evidence Item	Production and Checking Processes
ACAS Monitoring Reports	EUROCONTROL	EUROCONTROL processes
Results from rectification of ACAS operational problems	EUROCONTROL	The production of the cited evidence [46] involved multiple ACAS stakeholders. The documented procedures used are unknown to EUROCONTROL but the activities were conducted by reputable and long-standing aviation organisations considered competent to do so by ACAS stakeholders.

8.5 Conclusions to Arg 3

There is no direct evidence from ACAS operations of the actual collision-risk reduction achieved by ACAS. Its ability to deal with specific real encounters can be demonstrated, and this is partial evidence of a safety benefit, but there is no statistical measure of achieved collision-risk reduction to demonstrate satisfaction of Safety Criterion #1, because the risk of collision (even without ACAS) is very small. Therefore, the argument that safety monitoring demonstrates the safety benefit of ACAS can only be substantiated indirectly and that has already been addressed under Arg 1.3.3 and 1.3.5.

The satisfaction of Safety Criterion #2 is however demonstrated by results from established processes for identifying and correcting ACAS operational problems, which have the effect of progressively refining the capabilities of ACAS (and by implication, its safety benefit) in order to improve them As Far as Reasonably Practicable, although the need to expedite the introduction of CP 112E (RA reversal logic) has been raised as Safety Issue **ISS-007**.

9 FUTURE SAFETY OF ACAS (ARG 4)

9.1 Strategy

Having provided assurance via Arg 1 to 3 that ACAS operations are currently safe (subject to the resolution of eight outstanding Safety Issues), it is necessary as part of the Safety Case to provide assurance that they will continue to be shown to be acceptably safe in the future.

Arg 4 is, therefore, anticipating unspecified future changes to ACAS, which can arise principally from the following situations:

- planned changes to the ACAS equipment and / or its operational use
- planned or gradual, incidental changes in the ACAS operational environment
- gradual degradation in the performance of ACAS operations, irrespective of whether the first two situations occur or not.

Since such changes are, by definition, always in the future, the evidence to support Arg 4 is necessarily completely reliant on the processes (ie procedures) which govern the management of such changes.

An appropriate strategy for addressing the future safety of ACAS operations is therefore to show that:

- each planned changes to ACAS, its use or its operational environment (including other elements of the ATM system) will be subject to a formal, *a priori* safety assessment
- on-going safety monitoring and corrective action will carried out indefinitely for all three of the above situations to provide assurance that safety of ACAS is maintained, and where necessary improved, in operational use.

Such a strategy would ideally be based upon the following sub-arguments:

> **Arg 4.1**. adequate processes are in place for the safety management of changes to, or impacting on, ACAS operations
>
> **Arg 4.2**. effective operational monitoring of ACAS safety and related corrective action will continue indefinitely.

However, as explained in sections 9.2 to 9.4 below, there is **insufficient evidence** to support these arguments.

9.2 Safety Management of ACAS-related Changes (Arg 4.1)

Planned changes to ACAS, its use or its environment ought to be the subject of a formal, *a priori* safety assessment – however, the APOSC cannot provide specific assurance that this would be the case and, therefore, such a situation has to be assumed – see **Assumption A004** in section 10.1 below.

Although this seems to be a reasonable assumption as far as the SESAR Programme and EUROCONTROL's own ATM development programmes are concerned, a search of current European ATM safety regulations has failed to find any explicit requirement for carrying out a safety assessment of planned changes to ACAS.

The main two regulations governing changes to ATM (or which, according to the ICAO definition [20], Collision Avoidance is a part) are ESARR 4 [14] and the corresponding provisions of Common Requirement CR 2096/2005 [55]. Neither document mentions ACAS (or TCAS) nor safety nets in general.

In 2003, the EUROCONTROL Safety Regulation Commission issued a policy document (SRC Pol Doc 2 [15]) governing the use of safety nets in [safety] risk assessment and mitigation in ATM, in reaction to ESARR 4. This document gives numerous examples of safety nets but does not include ACAS explicitly – nevertheless it can be interpreted as covering ACAS as well. SRC document 28.06 [58] which may supersede SRC Pol Doc 2 only covers ground-based safety nets and therefore excludes ACAS from its scope.

As noted in section 3.2, the main purpose of SRC Pol Doc 2 is to prevent the benefits of safety nets such as ACAS being counted in the achievement of a tolerable level of risk for the Strategic Conflict Management and Separation Provision layers of ATM (see section 4.1 above). It terms of the safety of safety nets per se, its only provision is as follows:

> *"As safety nets, intended for operation in the Collision Avoidance part of ATM, can themselves induce new hazards to the Separation Provision function of ATM, they shall be subject to specific safety objectives and requirements derived by the application of ESARR 4"*

Thus, from an ACAS perspective, two important aspects of safety assessment are missing:

- firstly, there is no explicit requirement for assurance concerning the positive contribution that ACAS itself makes to the Collision Avoidance layer of ATM
- secondly, there is no explicit requirement for assurance concerning the possible negative affects that the changes within the Separation Provision layer, or within the ACAS operational environment, could have on ACAS operations.

Hence recommendation R-ACAS-1 is made in section 12 below.

9.3 On-going Safety Monitoring (Arg 4.2)

Arg 4.2 is intended to be satisfied through two sub-arguments:

> **Arg 4.2.1**. The future roles and responsibilities for monitoring and effecting corrective actions are defined;
>
> **Arg 4.2.2**. The procedures for monitoring and effecting corrective actions are in place.

And the assumption (see **A005** in section 10.1 below) that the parties responsible for effecting change, monitoring and corrective actions would discharge those responsibilities.

Whereas A005 seems to be a reasonable assumption to make, there is little or no evidence to support Arg 4.2.1 and 4.2.2, as explained in the next two sub-sections.

9.3.1 Monitoring and Rectification Roles & Responsibilities (Arg 4.2.1)

Defined roles and responsibilities for safety monitoring etc formed part of the historical evidence used to support Arg 3. However, they are incapable of providing evidence for future safety assurance – ie for Arg 4.2 – for the following reasons:

- the project charter [48] for the EUROCONTROL ACAS Programme (which managed the implementation of ACAS II in Europe) specified responsibilities for the maintenance of the operational monitoring programme and establishment of a framework for effecting improvements to the ACAS equipment. However, the ACAS Programme was terminated in 2006.
- responsibility for conducting the European ACAS monitoring programme [35][36][37][38] transferred from EUROCONTROL EEC to the EUROCONTROL-managed European Safety Programme (ESP) for ATM [47] at the end of 2006.
- the EMOTION-7 [46] project, whose main objective was to provide the EUROCONTROL ACAS Programme with adequate tools and the adequate structure to minimise the risks associated with the European ACAS implementation, was completed in December 2002.

The status of evidence with respect to future roles and responsibilities for monitoring and effecting corrective actions is as follows:

- the (now completed) EUROCONTROL Mode S and ACAS Programme participated in the activities related to the introduction of TCAS II version 7.1, which is an improvement initiative triggered by operational monitoring of TCAS II version 7.0. However, the Programme had no formal responsibilities with respect to operational monitoring / problem rectification of TCAS 7.0 *per se*.
- responsibilities associated with European ACAS operational monitoring were not formally documented within ESP - furthermore, as of late 2010, ESP no longer exists
- there is no evidence of formally-defined responsibilities for other ACAS stakeholders, in their role as participants in the ACAS improvement framework, with respect to ACAS problem identification, proposing operational or technical amendments, or the ACAS change management process.

There is no evidence, therefore, to support Arg 4.2.1 – the implications of this are discussed in section 9.4 below.

9.3.2 Monitoring and Rectification Procedures Definition (Arg 4.2.2)

The procedures used for the creation of historical evidence used to support Arg 3 are incapable of supporting Arg 4 for the following reasons:

- procedures for European ACAS operational monitoring activities have not been formally documented within ESP. Moreover, the ESP ACAS operational monitoring results and analysis [49] are different in nature and extent to those formerly produced by EUROCONTROL EEC
- there were no formally-defined procedures for the ACAS-related activities of the Mode S and ACAS Programme, and that programme no longer exists

(2010)

- there is no evidence of formally-defined procedures for other ACAS stakeholders, in their role as participants in the ACAS improvement framework, with respect to ACAS problem identification, proposing operational or technical amendments, or the ACAS change management process.

There is no evidence, therefore, to support Arg 4.2.2 either – the implications of this are also discussed in section 9.4 below.

9.4 Implications of the Present Situation

The absence of a continuing, defined EUROCONTROL monitoring programme does not necessarily mean that ACAS will cease to provide the same degree of net collision-risk reduction in the future as it does at present, unless:

- significant changes occur, either in the operational environment or in other parts of the ATM system, that could significantly affect ACAS operations
- changes are made to the ACAS equipment and / or the way that it is used
- the performance of ACAS as a whole degrades insidiously due to human involvement in the system, in the air and / or on the ground.

9.4.1 Changes in the ACAS Operational Environment or ATM system

Three such possible changes can be considered as relevant:

- increase in traffic to the extent that ACAS produces an excessive number of spurious RAs or fails to produce RAs when required (it is noted in earlier in the APOSC (section 2.3.5) that high traffic density can cause problems with ACAS).
- new separation modes and in particular the Airborne Separation Assurance System (ASAS); it has already been identified that ACAS may have to be disabled (for at least one of the aircraft, and possibly both[57]), which are involved in an ASAS manoeuvre to prevent spurious RAs being generated. This would create new system failure modes such as such as incorrect disabling of RAs. An alternative would be to constrain ASAS manoeuvres such that they do not cause unnecessary RAs.
- reduction of vertical separation minima to less than 1000 ft

For the next few years (from 2010) at least, traffic densities are not likely (in the judgement of EUROCONTROL) to rise to such an extent that ACAS will become ineffective, especially as the global recession has reduced traffic by about 10% over 2007 levels.

ASAS will require international effort including effort from ICAO in modifying the ACAS standards, and effectively a new Safety Case for ACAS will have to be created (or the assessment included in the SESAR safety case).

[57] Or at least its alerting parameters adjusted

Similarly, further reduction of vertical separation minima would require a change to all installed TCAS II equipment and a comprehensive safety case which either includes ACAS, or would require a separate ACAS safety case revision.

The main effect of a lack of defined monitoring arrangements would, under this analysis, not be to make ACAS less effective but to introduce an element of uncertainty as to its continuing effectiveness – uncertainty that would increase as traffic levels increase and/or changes are made to the overall ATM system.

The lack of defined monitoring arrangements is identified as safety issue **ISS-008** in section 10.2.

9.4.2 Changes to ACAS Operations

Changes to ACAS operations could include:

- minor changes to current ACAS algorithms – eg improvements in the reversal logic, and introduction of "level off" instead of "adjust vertical speed" which are already proposed for ECAC airspace, see section 8.3
- direct coupling of RA output to the aircraft autopilot
- fundamental changes to ACAS – eg the introduction of horizontal-plane manoeuvres.

The first two examples could be handled by a relatively simple safety assessment and amendment to this APOSC.

The third example would, however, invalidate the APOSC and would require a major safety assessment and completely new safety case.

9.4.3 Insidious Degradation

It has already been noted – not the least in the accounts of the Yaizu, Überlingen and Jeju Island accidents at Appendix I – that inconsistent human behaviour around ACAS RAs can have a major negative effect on the performance of this safety net. Reference [57] stated (in 2007) that:

> *"the weakest element in the ACAS control loop [is that] pilots do not always follow the RA [correctly]; without "human in the loop" the risk ratio would improve by a factor of 10"*

A number of reasons are cited for this, most of which are human related and involve the pilot and the air traffic controller. It is deduced, therefore, that as long as ACAS is dependent on correct and timely human responses ACAS operations will be liable to degradation over time, notwithstanding continuing publicity campaigns to try to prevent this[58]. The ASARP report [32] notes an improvement in human performance between that study and earlier studies, presumably due to the prominence given to the issue following the Überlingen accident, but the concern remains valid.

The implication is that the safety monitoring of ACAS, and related corrective action, is necessary to assure the continuing effectiveness of ACAS in preventing mid-air collisions – reinforcing the validity of safety issue **ISS-008** in section 10.2.

[58] If this was not a valid deduction then the aftermath of the Überlingen collision in 2002 would surely have largely eradicated incorrect pilot responses to, and inappropriate ATC interventions in, ACAS RAs

9.5 Conclusions to Arg 4

It is concluded that Arg 4 is not adequately substantiated by the available evidence.

10 CAVEATS

10.1 Assumptions

A number of assumptions have been made in the Safety Case and are clearly identified in the relevant sections. These assumptions are listed below, together with their origin (in the APOSC) and explanation of why they are justified and therefore reasonable.

No	Assumption	Origin	Justification
A001	Radar data used to fit the Encounter Model represents all Airframe Movements of relevance, including high rates of climb or descent between cleared flight levels	6.4.6	The radar data used as the basis for ACAS modelling studies is from UK and French airspace. The degree to which the data is representative of other airspace within the ECAC region is unknown, however these two airspaces are considered representative of the most demanding environment to which ACAS will be exposed within the region.
A002	ACAS includes a traffic display	6.4.6	Traffic display is not required by ICAO Annex 10 [11], but is part of TCAS II specification [8].
A003	Implementers of internationally applicable ACAS Operational and System specifications are aware of, and are obliged to conform with, those specifications via ICAO protocols	7.3	Standard international and regional aviation practices applicable to any operational or technical change – but see Safety Issue **ISS-005** in section 10.2 below.
A004	Future changes to ACAS, its operational use or its operational environment will be the subject of a formal, *a priori* safety assessment	9.2	Although this is common practice in European ATM, there seems to be no complete, explicit safety regulations in place to address this point – hence recommendation R-ACAS-1 at section 12
A005	Parties responsible for effecting change, monitoring and corrective actions would discharge those responsibilities	9.3	Normal European ATM and aviation practice

10.2 Safety Issues

The following issues are identified in this safety case report. None of the issues is sufficiently serious to invalidate the safety claim for ACAS (that it provides a substantial positive net contribution to the risk of a mid-air collision), as it stands at the moment (2010). However, resolution of the issues could provide some further risk reduction, would provide additional confidence that all steps that are reasonably practicable in risk reduction have been taken, and would provide assurance of the continuing effectiveness of ACAS in the face of increasing traffic levels and the many changes to the overall ATM system planned under SESAR.

No	Issue	Origin
ISS-001	The open matter as to whether or not (and where) RA Downlink should be deployed in ECAC Airspace needs to resolved as soon as possible	6.4.5.2 and 7.2
ISS-002	The discrepancy between Safety Requirement SR_F4 and PANS-OPS section 3.2 c) 4) should be resolved by the appropriate change to the latter	6.4.5.2
ISS-003	A quantified risk model for ACAS based upon the accident-causation model in Appendix F should be created, to provide increased confidence in the achieved contribution of ACAS to risk reduction	6.6.7
ISS-004	The following aspects of ACAS operations should be reviewed to determine whether a change is needed in order to mitigate any associated system hazards: • Flight Crew initiating See & Avoid in response to TA • Flight Crew requesting information or guidance from controller in response to TA • Controller issuing traffic information to RA-incident aircraft • Controller issuing instruction/clearance to non-ACAS aircraft (that has been (correctly or incorrectly) identified as the threat aircraft causing the RA described in an RA report) • Controller issuing traffic information to non-ACAS aircraft (that has been (correctly or incorrectly) identified as the threat aircraft causing the RA described in an RA report) • Controller has no information about the nature of an RA.	6.6.5
ISS-005	Discrepancies (inconsistencies and ambiguities) exist within the ICAO documentation, and with its conformity to the Safety Requirements. This Issue is related to Assumption **A-003** in that the validity of A-003 depends greatly on such discrepancies being removed	7.2
ISS-006	**Resolved** – see Appendix K below	8.2
ISS-007	The introduction of improved reversal logic (CP 112E) as part of TCAS II version 7.1 should be expedited and the matter should remain an open Safety Issue until the mandate for carriage of TCAS II version 7.1 has taken effect **<u>Publisher's note (25 November 2011):</u>** European Commission is expected to publish by the end of 2011 a Commission Regulation requiring that all aircraft currently equipped with TCAS II version 7.0 will need to be upgraded to version 7.1 by 1 December 2015 in order to continue to operate in the airspace of European Community. All new aircraft above 5,700 kg Maximum Take-off Mass or passenger seating capacity above 19 will have to be equipped by 1 March 2012.	8.3
ISS-008	Requirements, responsibilities and procedures for future ACAS operational monitoring and problem rectification within EUROCONTROL need to be formally defined.	9.4

10.3 Limitations

The Safety Case has identified no new limitations of ACAS or its operation, or any restrictions that need to be placed on its use other than those already captured in the ICAO ACAS II material and Safety Requirements herein.

11 CONCLUSIONS

The conclusions of this ACAS II Post-implementation Safety Case are as follows:

C1 Subject to the Assumptions in section 10.1 and resolution of Safety Issue **ISS-003** in section 10.2 concerning additional risk quantification, ACAS II currently (late 2010) provides a substantial net positive contribution to the risk of a mid-air collision, as demonstrated by analysis of the design and implementation of the total ACAS system. The overall risk of a mid-air collision in ECAC airspace with ACAS is believed to be reduced by a factor of between 4 and 5 compared with the risk which would exist in the present European ATM and operational environment in the absence of ACAS.

C2 There is little direct statistical evidence, of ACAS risk reduction, from actual experience of ACAS operations, because the absolute risk of a mid-air collision (with or without ACAS) is very low.

C3 ACAS presents a negligible contribution, either positive or negative, to the risk associated with types of aircraft accident other than mid-air collisions, passenger/crew injuries resulting from ACAS-induced manoeuvres or passenger/crew injuries resulting from ineffective operation of ACAS.

C4 Operational monitoring of ACAS has led to improvements in the net risk reduction provided by the total ACAS system over a period of time (particularly with respect to the people and procedures aspects of the system). Nevertheless, it is acknowledged that some problems still remain to be resolved.

C5 There are some residual Safety Issues (**ISS-001**, **-002**, **-003**, **-004**, **-005** and **-007** in section 10.2) that need to be addressed in order to provide either further risk reduction in accordance with the principle that risk should be reduced As Far as Reasonably Practicable or at least increased confidence in the achieved contribution of ACAS to risk reduction.

C6 In the short / medium term (until, say, up to 2013), changes in the operational environment are not likely to degrade the effectiveness of ACAS to such an extent that the current safety claim (that it provides a substantial net positive contribution to safety) will cease to be true. Furthermore, as long as ACAS operations remain human centred, they are liable to degrade with time due to increasing inconsistency in human responses to RAs. Therefore, the absence of an ongoing EUROCONTROL monitoring programme means that there will be inevitably an element of uncertainty, which will increase over time, about the degree to which the safety claim for ACAS remains true (Safety Issue **ISS-008**).

C7 In the longer term, some of the changes to European ATM expected to be advanced by SESAR could have a significant effect on ACAS operations. Monitoring of the effectiveness of ACAS will inevitably be needed to support the safety cases for such changes and should commence well before the changes are introduced in order to establish a statistically valid data set for comparison with the post-change situation. This reinforces **ISS-008**.

12 RECOMMENDATIONS

It is recommended that:

R-ACAS-1. The EUROCONTROL Safety Regulation Commission considers the need for explicit regulations concerning the safety assessment[59] of changes affecting ACAS operations – see section 9.2 above.

Publisher's note (25 November 2011):

The European Aviation Safety Agency (EASA) is now responsible for regulation of ATM safety. The above recommendation should be considered in the light of this development.

[59] ie what ESARR 4 refers to as "risk assessment and mitigation"

13 ABBREVIATIONS

The following abbreviations are used herein. Some ATM commonly understood abbreviations and names of organisations are excluded for brevity.

ACAS	Airborne Collision Avoidance System
ACC	Area Control Centre
APP	Approach [Control]
ANSP	Air Navigation Service Provider
ASAS	Airborne Separation Assurance System
AFARP	As Far As Reasonably Practicable
AGL	Above Ground Level
APOSC	ACAS II Post-implementation Safety Case
ASARP	ACAS Safety Analysis post-RVSM Project
ATC	Air Traffic Control
CAA	Civil Aviation Administration (generic)
CFIT	Controlled Flight Into Terrain
EASA	European Aviation Safety Agency
EEC	EUROCONTROL Experimental Centre
EMOTION-7	European Maintenance of TCAS II version 7.0
ESP	European Safety Programme (for ATM)
EUROCAE	European Organization for Civil Aviation Equipment
FAA	Federal Aviation Administration (USA)
FARADS	Feasibility of ACAS RA Downlink Study
FHA	Functional Hazard Assessment
FSR	Functional Safety Requirement
FTA	Fault Tree Analysis
GPWS	Ground Proximity Warning System
GSN	Goal Structuring Notation
IMC	Instrument Meteorological Conditions
InCAS	Interactive Collision Avoidance Simulator
JAA	Joint Aviation Authorities
LRR	Logic Risk Ratio
MAC	Mid-air Collision
MSAW	Minimum Safe Altitude Warning
OSCAR	Off-line Simulator for Collision Avoidance Resolution
PSSA	Preliminary System Safety Assessment
RA	Resolution Advisory

RTCA	RTCA Inc. A USA-based non-profit organisation that develops technical standards for regulatory authorities (formerly Radio Technical Commission for Aeronautics)
SAM	Safety Assessment Methodology
SCDM	Safety Case Development Manual
SMS	Safety Management System
SRR	System Risk Ratio
STCA	Short Term Conflict Alert
TA	Traffic Advisory
TCAS	Traffic alert and Collision Avoidance System

14 REFERENCES

[1] ICAO, Collision Avoidance System (ACAS) Manual, Document 9863 AN/461, 1st Edition, 2006

[2] EUROCONTROL, ACASA Project, Work Package 6.1- ACAS Brochure, ACAS/WP6.1/015, Version 2, May 2000

[3] ICAO, Operation of Aircraft, Annex 6 to the Convention on International Civil Aviation, Part 1 – International Commercial Air Transport – Aeroplanes, 8th Edition - November 2001, Amendment 31 – November 2007

[4] ICAO, Aircraft Operations Volume I, Flight Procedures, Doc 8168 OPS/611, 5th Edition, 2006

[5] ICAO, Procedures for Air Navigation Services, Air Traffic Management, PANS-ATM Doc 4444, ATM/501, 14th Edition, 2001

[6] ICAO, Approval of Amendment 2 to PANS-OPS Volume 1, State Letter AN 11/19.1-07/44, 22 June 2007

[7] ICAO, Approval of Amendment 5 to the PANS-ATM, State Letter AN 13/2.1-07/36, 22 June 2007

[8] ICAO, Approval of Amendment 3 to PANS-OPS Volume 1, State Letter AN 11/19-08/71, 31 October 2008

[9] RTCA, Minimum operational performance standards for Traffic alert and Collision Avoidance System II airborne equipment, RTCA DO-185A, 1997

[10] EUROCONTROL, ASARP Project, Work Package 9: Final Report on the Safety of ACAS II in the European RVSM Environment, ASARP/WP9/72/D, Version 1.1, 11 May 2006

[11] ICAO, Aeronautical Telecommunications Volume IV, Surveillance Radar and Collision Avoidance Systems, Annex 10 to the Convention on International Civil Aviation, 3rd Edition, July 2002

[12] ICAO, Rules of the Air, Annex 2 to the Convention on International Civil Aviation, 10th Edition, Amendment 40, November 2007

[13] ICAO, Air Traffic Services, Annex 11 to the Convention on International Civil Aviation, 13th edition, July 2001

[14] EUROCONTROL, ESARR 4, Risk Assessment and Mitigation in ATM, Edition 1.0, 5 April 2001

[15] EUROCONTROL, SRC Policy Document 2, Use of Safety Nets in Risk Assessment & Mitigation in ATM, Edition 1.0, 28 April 2003

[16] EUROCONTROL, Air Navigation System Safety Assessment Methodology, SAF.ET1.ST03.1000-MAN-01-00, Edition 2.1, 3 October 2006

[17] EUROCONTROL, Safety Case Development Manual, DAP/SSH/091, Edition 2.2, 13 November 2006

[18] Limitations of the See-and-Avoid Principle, (Australian) Bureau of Air Safety Investigation, ISBN 0-642-16089-9, April 1991

[19] J. Harris, “Avoid”, the unanalysed partner of “See”, ISASI Forum No. 2, 1983.

[20] ICAO, Global Air Traffic Management Operational Concept, Doc 9854, 1st Edition, 2005

[21] EUROCONTROL, ACAS Programme, ACASA Project, Work Package 1, Final Report on Studies on the Safety of ACAS II in Europe, ACAS/ACASA/ 02-014, Edition 1, March 2002

[22] QinetiQ, QinetiQ's response to Questions about ACAS Risk Ratio Modelling, QQ responses to SMT v1.0.doc, 1 May 2007

[23] EUROCONTROL, ACAS Programme, ACAS Safety Study, Safety Benefit of ACAS II Phase 1 and Phase 2 in the New European Airspace Environment, ACAS/02-022, Edition 1, May 2002

[24] EUROCONTROL, ASARP Project, Work Package 9: Final Report on the Safety of ACAS II in the European RVSM Environment, ASARP/WP9/72/D, Version 1.1, 11 May 2006

[25] D A Howson, TCAS II: Report on UK operational trial, CAA Paper 92011, 1992

[26] The FAA Separation Assurance program: History, Rationale and Status: paper based on an FAA presentation before the House Committee on Science and Technology Subcommittee on Transportation, Aviation and Communications, June and July 1979

[27] R L Ford & D L Powell, Interim report on a series of formal, instrumented trials of TCAS II in the UK, ICAO SICASP/WP2/290, 25 July 1990

[28] Limited Installation Program: Final Report, Honeywell, Northwest Airlines & ARINC Research Corporation, July 1989

[29] EUROCONTROL, ACASA Project, Event tree probabilities, H J Hutchinson, ACASA WP213, November 2001 (and references therein)

[30] Federal Aviation Administration, FAA Technical Standard Order C119b, TCAS II, December 1998

[31] W. J. Hughes FAA Technical Center, TCAS II Requirements Working Group Recommended Modifications 1.0 to TSO C119b, ACT 350, April 1999

[32] EUROCONTROL, ASARP Project, Work Package 6: Final Report on post-RVSM ACAS Full-system Safety Study, ASARP/WP6/58/D, Version 1.0, 10 March 2006

[33] EUROCONTROL, ACAS RA Downlink Combined FHA & PSSA Report, Edition 1.2, 27 March 2007

[34] EUROCONTROL, Main Report For The: 2005/2012 Integrated Risk Picture For Air Traffic Management In Europe, EEC Note No. 05/06, Issued: April 2006

[35] EUROCONTROL, European ACAS Operational Monitoring 2000 Report, EEC Report No. 373, August 2002

[36] EUROCONTROL, European ACAS Operational Monitoring 2001 Report, EEC Report No. 387, December 2003

[37] EUROCONTROL, European ACAS Operational Monitoring 2002 Report, EEC Report No. 393, July 2004

[38] EUROCONTROL, European ACAS Operational Monitoring 2003 Report, EEC Report No. 401, August 2005

[39] Guide to Methods and Tools for Safety Analysis in Air Traffic Management, prepared by: GAIN (Global Aviation Information Network) Working Group B, Analytical Methods and Tools, First Edition, June 2003

[40] CENA, OSCAR test-bench, User's Manual, Version 2.0, October 1996

[41] B Billmann, T Morgan, R Strack, J Windle, Air Traffic Control/Full Beacon Collision Avoidance System Chicago Simulation: Final Report, FAA report FAA-RD-79-16, April 1979

[42] EUROCONTROL, ACASA Project, Human response probabilities, K Carpenter, ACASA WP102, March 2000

[43] EUROCONTROL, ACASA Project, Analysis of pilot reactions based on airborne recorded data, E Vallauri, ACASA WP161, March 2001

[44] EUROCONTROL, ACASA Project, Pilot response models, H Hutchinson, ACASA WP208, August 2001

[45] EUROCONTROL, ASARP Project, Final report on the analysis of airborne recorded data and pilot model specification, ASARP/WP4/19/D, version 1.0, April 2005

[46] EUROCONTROL, ACAS Programme, EMOTION – 7 Final Report, European Maintenance of TCAS II version 7.0, ACAS/03-003, Edition 1, January 2003

[47] EUROCONTROL, European Safety Programme (ESP) for ATM, DAP/SAF 2006-26, Edition 1.0, 16 February 2006

[48] EUROCONTROL, Airborne Collision Avoidance System (ACAS) Programme Charter, Edition 1.0, 14 September 2000

[49] EUROCONTROL, EVAIR Safety Bulletin No 1, Report Period 2007, Issued April 2008[60].

[50] Bundestelle fur Flügunfallundersuchung (German Federal Bureau of Aircraft Accident Investigation), Investigation Report AX001-1-2/02, May 2004.

[51] Aircraft and Railway Accident Investigation Commission of Japan (now Japan Transportation Safety Board), accident report number 02-5-JA9804 (summarised in http://www.asasi.org/papers/2005/Hiroaki%20Tomita%20-%20near%20collision%20in%20Japan.pdf).

[52] EUROCONTROL, ACAS RA Downlink Safety Summary Report, Edition 1.3, 31 May 2007.

[53] Monitoring of TCAS Resolution Advisories in Core European Airspace, Drozdowski, S., Dehn, D. (EUROCONTROL) and Louyot, P (DSNA), Air Traffic Control Quarterly, volume 18, number 3, 2010, published by Air Traffic Control Association Institute, Alexandria, VA.

[54] Aviation Safety Council, Taiwan. Far Eastern Air Transport EF306, Boeing 757-200/Thai Airways (…) Flight TG659, Boeing 757/300. A TCAS Event in Narrow Collision Avoidance at an altitude of 34,000 ft and 99nm south of Jeju Island, Korea on November 16 2006. Final Report, August 2008.

[55] Commission Regulation (EC) No 2096/2005 of 20 December 2005 - Common Requirements for the Provision of Air Navigation Services.

[60] And subsequent reports available from http://www.eurocontrol.int/esp/public/site_preferences/display_library_list_public.html#4

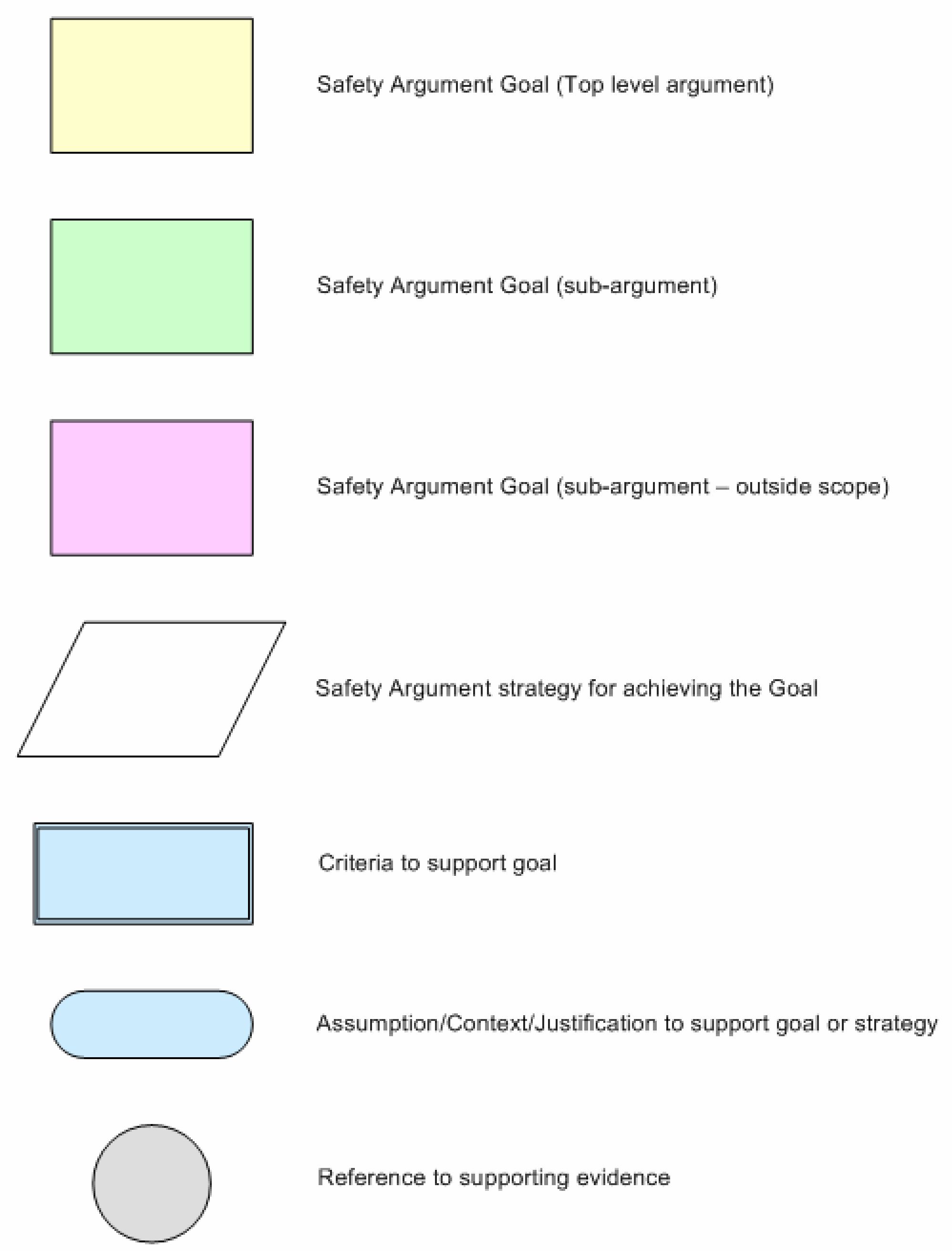
[56] http://www.eurocontrol.int/msa/public/standard_page/ACAS_Upcoming_Changes.html (reference valid in March 2010).

[57] STCA/ACAS Interaction & Interoperability Workshop Report, Dübendorf, 28-29 March 2007, Chapter 2. EUROCONTROL, 14 May 2007.

[58] SRC Action Paper reference 28.06, SRC Policy on Ground-Based Safety Nets, 15 March 2007.

[59] Aeronautical Accident Investigation and Prevention Center, Command of Aeronautics, General Staff of the Aeronautics, Final Report A-00X/CENIPA/2008 on the Mid-air collision between Boeing B-737 8EH and Embraer EMB-135 BJ Legacy aircraft over Brazil on 29 September 2006

APPENDIX A GOAL STRUCTURING NOTATION SYMBOLOGY


Safety Argument Goal (Top level argument)
Safety Argument Goal (sub-argument)
Safety Argument Goal (sub-argument – outside scope)
Safety Argument strategy for achieving the Goal
Criteria to support goal
Assumption/Context/Justification to support goal or strategy
Reference to supporting evidence

APPENDIX B ACAS SAFETY REQUIREMENTS

Ref	Safety Requirement	Origin
	ACAS	
SR_A1	ACAS shall provide a warning (TA) to Flight Crew of the existence of possibly conflicting traffic	6.3.3
SR_A2	ACAS shall provide a warning (TA) to Flight Crew of the existence of a possibly conflicting traffic	6.3.3
SR_A3	ACAS shall provide indications (RA) to Flight Crew on how to act to avoid collision	6.3.3
SR_A4	ACAS collision avoidance indications (RA) shall be produced by algorithms which are equivalent in performance to those specified in DO-185A	6.3.3
SR_A5	ACAS shall coordinate its collision avoidance indications (RA) with those on the intruder aircraft to ensure that the collision avoidance actions are compatible	6.3.3
SR_A6	ACAS shall provide collision avoidance indications (RA) which are compatible with all types of equipped aircraft in the environment and all points in their flight envelope relevant to the environment	6.3.3
SR_A7	ACAS shall provide collision avoidance indications (RA) which correspond to the minimum manoeuvring necessary to avoid collision	6.3.3
SR_A8	ACAS shall not produce collision avoidance indications (RA) which would cause the aircraft to descend when close to the ground	6.3.3
SR_A9	ACAS shall not produce warnings or collision avoidance indications (TA or RA) during aircraft operation close to, or on, the ground	6.3.3
SR_A10	ACAS shall not produce advisories (TA or RA) if any of the inputs from the aircraft's sensors or transponder are lost or invalid	6.5.3
SR_A11	ACAS shall not produce advisories (TA or RA) in situations where there is relative Airframe Movement beyond the capability of its sensors or algorithms	6.5.4
SR_A12	ACAS shall provide collision avoidance indications (RA) against a manoeuvring intruder aircraft on board which ACAS collision avoidance is unavailable	6.6.4
SR_A13	ACAS shall continuously perform a monitoring function in order to prevent any further ACAS interrogations if data from external sources indispensable for ACAS operation are not provided, or the data provided are not credible	6.5.3
SR_A14	When the ACAS monitoring function detects a failure, ACAS shall indicate to the flight crew that an abnormal condition exists	H.1.3
SR_A15	ACAS shall not produce audible collision avoidance indications (RA) when other onboard warnings (stall, ground proximity, windshear) are being annunciated.	6.3.3
	Flight Crew	
SR_F1	Flight Crew shall prepare themselves to act immediately in accordance with any subsequent collision avoidance indications (RA), in response to potential collision warning (TA) from ACAS	6.3.3
SR_F2	Flight Crew shall act immediately in accordance with collision avoidance indications (RA) from ACAS, unless doing so would jeopardize the safety of the aircraft due to the existence of a hazardous situation which must be prioritised over collision avoidance	6.3.3

Ref	Safety Requirement	Origin
SR_F3	Flight Crew shall act in accordance with collision avoidance indications (RA) from ACAS by using control inputs similar in strength to those used for routine aircraft manoeuvres	6.3.3
SR_F4	As soon as possible, as permitted by workload, Flight Crew shall notify the Air Traffic Controller of the execution of an ACAS-initiated collision avoidance action except when it is believed that the action would not result in a deviation from a clearance or instruction	6.4.5.2
SR_F5	Flight Crew shall switch ACAS to TA-only mode when there exists an aircraft-related failure which would preclude an ACAS-initiated manoeuvre should it be necessary	6.5.3
SR_F6	Flight Crew shall switch ACAS to TA-only mode when there exists an abnormal environmental situation which would preclude an ACAS-initiated manoeuvre should it be necessary	6.5.4
SR_F7	Flight Crew shall operate ACAS in TA/RA mode during flight only	6.3.3
SR_F8	In the event that the Flight Crew receive an ATC instruction that would result in a contravention of the RA (in strength and / or direction), the Flight Crew shall refuse the instruction and advise ATC as soon as workload permits that the aircraft is involved in an RA	6.4.5.2
SR_F9	Flight Crew shall notify the Air Traffic Controller as soon as avoidance action is completed and workload permits, and shall resume the vertical clearance that was in effect prior to the RA.	6.4.5.2
Air Traffic Controller		
SR_C1	Air Traffic Controller shall cease to issue clearances or instructions to an aircraft that has notified its execution of an ACAS-initiated collision avoidance action	6.4.5.2

APPENDIX C SAFETY REQUIREMENTS COMPLETENESS

This Appendix contains a mapping between the ACAS Fundamentals in section 2.2 and the ACAS Safety Requirements in Appendix B. A '√' means that the Safety Requirement satisfies the Fundamental or a part thereof. Where a Fundamental is satisfied by multiple Safety Requirements, the coverage of all aspects of the Fundamental has been checked.

Safety Requirement	ACAS Fundamental							
	2.2.1	2.2.2	2.2.3	2.2.4	2.2.5	2.2.6	2.2.7	2.2.8
SR_A1	√		√					√
SR_A2	√		√					
SR_A3	√							√
SR_A4	√		√					
SR_A5	√					√		√
SR_A6	√	√	√					
SR_A7	√		√			√		
SR_A8	√	√						
SR_A9	√	√						
SR_A10	√							√
SR_A11	√							√
SR_A12	√		√				√	
SR_A13								
SR_A14								
SR_A15					√			
SR_F1	√		√					
SR_F2	√	√	√	√	√			√
SR_F3	√		√					
SR_F4	√			√				
SR_F5	√							√
SR_F6	√	√						
SR_F7	√	√						
SR_F8				√				
SR_F9				√				
SR_C1	√		√	√				

The mapping verifies that there are no ACAS Fundamentals that have not been captured as Safety Requirements. Since the Safety Requirements under Args1.3 to 1.5 were derived independently from the Fundamentals, it also provides assurance that the Fundamentals are complete. SR_A13 and SR_A14 are not shown as being derived from the Fundamentals, since they are derived from the need to mitigate ACAS equipment failures.

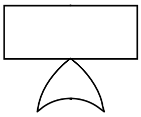
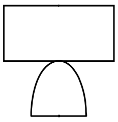
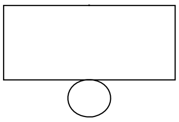
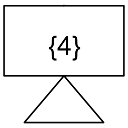
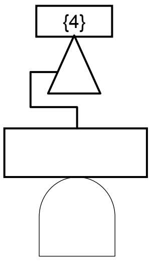
As noted in section 6.4.6, although See & Avoid prompted by a TA does not appear as an explicit ACAS Fundamental, their safety benefit is implicit in the evidence used to support Arg 1.3.5. This warrants its inclusion as SR_A2.

APPENDIX D CONTINGENCY TREE FACTORS AND EVENTS

Factor	Event Description	Event Code
Encounter Geometry	not on an NMAC course	GCCX
Encounter Geometry	on an NMAC course	GCCY
Encounter Geometry	rate of close encounters	GCER
Encounter Geometry	instrument meteorological conditions prevail	GIMC
Aircraft Equipage	aircraft centred risk – own aircraft is unequipped	EAEX_A
Aircraft Equipage	airspace centred risk – first aircraft is unequipped	EAEX_A
Aircraft Equipage	aircraft centred risk – other aircraft is unequipped	EAEX_B
Aircraft Equipage	airspace centred risk – second aircraft is unequipped	EAEX_B
Aircraft Equipage	aircraft centred risk – own aircraft is ACAS equipped	EAEY_A
Aircraft Equipage	airspace centred risk – first aircraft is ACAS equipped	EAEY_A
Aircraft Equipage	aircraft centred risk – other aircraft is ACAS equipped	EAEY_B
Aircraft Equipage	airspace centred risk – second aircraft is ACAS equipped	EAEY_B
Aircraft Equipage	ACAS is operated in TA-only mode	EARX
Aircraft Equipage	ACAS is operated in full TA/RA mode	EARY
Aircraft Equipage	non-ACAS aircraft with transponder is Mode C equipped	EMSX
Aircraft Equipage	non-ACAS aircraft with transponder is Mode S equipped	EMSY
Aircraft Equipage	non-ACAS aircraft is not transponder equipped	ETXX
Aircraft Equipage	non-ACAS aircraft is transponder equipped	ETXY
ACAS Tracking	ACAS fails to track Mode C intruder	ETCX
ACAS Tracking	ACAS tracks Mode C intruder	ETCY
ACAS Tracking	ACAS fails to track Mode S intruder	ETSX
ACAS Tracking	ACAS tracks Mode S intruder	ETSY
Altitude Reporting	Mode C aircraft does not report altitude	EACX
Altitude Reporting	Mode C aircraft reports altitude	EACY
Altitude Reporting	non-ACAS Mode S aircraft does not report altitude	EASX
Altitude Reporting	non-ACAS Mode S aircraft reports altitude	EASY
Controller Involvement	there is a controller	ACEX
Controller Involvement	there is no controller	ACEY
Controller Involvement	controller is not already involved	ACIX
Controller Involvement	controller is already involved	ACIY
Controller Involvement	pilot does not contact controller in response to an ACAS TA	HCCX
Controller Involvement	pilot contacts controller in response to an ACAS TA	HCCY
Controller Involvement	controller instruction counter to RA (not on an NMAC course)	HRXI
Controller Involvement	controller instruction counter to RA (on an NMAC course)	HRXU
Pilot Response	pilot ignores controller instruction	HFCX
Pilot Response	pilot notes/follows controller instruction	HFCY
Pilot Response	pilot ignores RA	HFRX
Pilot Response	pilot notes/responds to RA	HFRY
Pilot Response	pilot prefers controller instruction over an RA	HPRX
Pilot Response	pilot prefers RA over a controller instruction	HPRY
Traffic Display	ACAS has no bearing data on Mode C intruder	EBCX

Factor	Event Description	Event Code
Traffic Display	ACAS has bearing data on Mode C intruder	EBCY
Traffic Display	ACAS has no bearing data on Mode S intruder	EBSX
Traffic Display	ACAS has bearing data on Mode S intruder	EBSY
Traffic Display	ACAS traffic display is not operational	EDOX
Traffic Display	ACAS traffic display is operational	EDOY
Visual Acquisition	visual information is incorrect	GVIX
Visual Acquisition	visual information is correct	GVIY
Visual Acquisition	pilot looks for threat	HPLX
Visual Acquisition	pilot does not look for threat	HPLY
Visual Acquisition	not already visual with ACAS threat	VAAX
Visual Acquisition	already visual with ACAS threat	VAAY
Visual Acquisition	not already visual with unequipped threat	VAUX
Visual Acquisition	already visual with unequipped threat	VAUY
Visual Acquisition	does not acquire unequipped threat (traffic display, no alt.)	VNUX
Visual Acquisition	acquires unequipped threat (traffic display, no altitude)	VNUY
Visual Acquisition	does not acquire ACAS threat (no traffic display)	VXAX
Visual Acquisition	acquires ACAS threat (no traffic display)	VXAY
Visual Acquisition	does not acquire unequipped threat (no traffic display)	VXUX
Visual Acquisition	acquires unequipped threat (no traffic display)	VXUY
Visual Acquisition	does not acquire ACAS threat (full traffic display)	VYAX
Visual Acquisition	acquires ACAS threat (full traffic display)	VYAY
Visual Acquisition	does not acquire unequipped threat (full traffic display)	VYUX
Visual Acquisition	acquires unequipped threat (full traffic display)	VYUY
See-and-Avoid	pilot does not act upon visual acquisition	HPAX
See-and-Avoid	pilot acts upon visual acquisition	HPAY
ACAS Logic Performance	combined manoeuvre does not prevent conflict	LCMI
ACAS Logic Performance	combined manoeuvre does not resolve conflict	LCMU
ACAS Logic Performance	controller instruction fails to resolve NMAC	LCWX
ACAS Logic Performance	controller instruction resolves NMAC	LCWY
ACAS Logic Performance	two evasive manoeuvres induce an NMAC	LRXI
ACAS Logic Performance	two evasive manoeuvres fail to resolve NMAC	LRXU
ACAS Logic Performance	single manoeuvre does not prevent conflict	LSMI
ACAS Logic Performance	single manoeuvre does not resolve conflict	LSMU
ACAS Logic Performance	RA against Mode C threat fails (typical response, not on NC)	LTCI
ACAS Logic Performance	RA against Mode C threat fails (typical response, on NC)	LTCU
ACAS Logic Performance	coordinated RA fails (no response by intruder, not on NC)	LTNI
ACAS Logic Performance	coordinated RA fails (no response by intruder, on NC)	LTNU
ACAS Logic Performance	RA against Mode S threat fails (typical response, not on NC)	LTSI
ACAS Logic Performance	RA against Mode S threat fails (typical response, on NC)	LTSU
ACAS Logic Performance	coordinated RAs fail (typical response, not on NC)	LTTI
ACAS Logic Performance	coordinated RAs fail (typical response, on NC)	LTTU

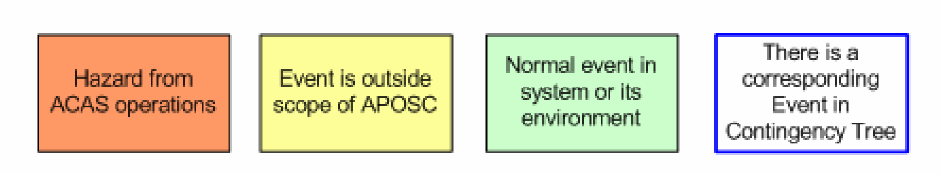
APPENDIX E FAULT TREE SYMBOLOGY

	**OR gate**	Output (event) occurs only if at least one of the input events occurs. A description of the event is provided in the rectangle.
	**AND Gate**	Output (event) occurs only if all input events occur simultaneously. A description of the event is provided in the rectangle.
	**Elementary event**	An event is defined as an elementary occurrence if it does not need further development. A description of the elementary event is provided in the rectangle.
	**Forward**	Event referring to a sub-tree – where the decomposition of this event is presented. The called decomposition (see next line) will have the same reference inside the triangle. A description of the event to which it refers is provided in the rectangle.
	**Forward target:**	Target event that will be used in another tree as a called sub-tree. The calling event (see previous line) has the same reference inside the triangle. A description of this called event (identical to that of the calling event) is provided in the rectangle.

APPENDIX F ACAS ACCIDENT-CAUSATION MODEL

This Appendix contains the accident-causation model for ACAS operations referred to in section 6.6.2. It should be noted that the events in the model include normal and abnormal conditions as well as failures. This model could be converted into an ACAS risk model by inserting quantified event probability or frequency data.

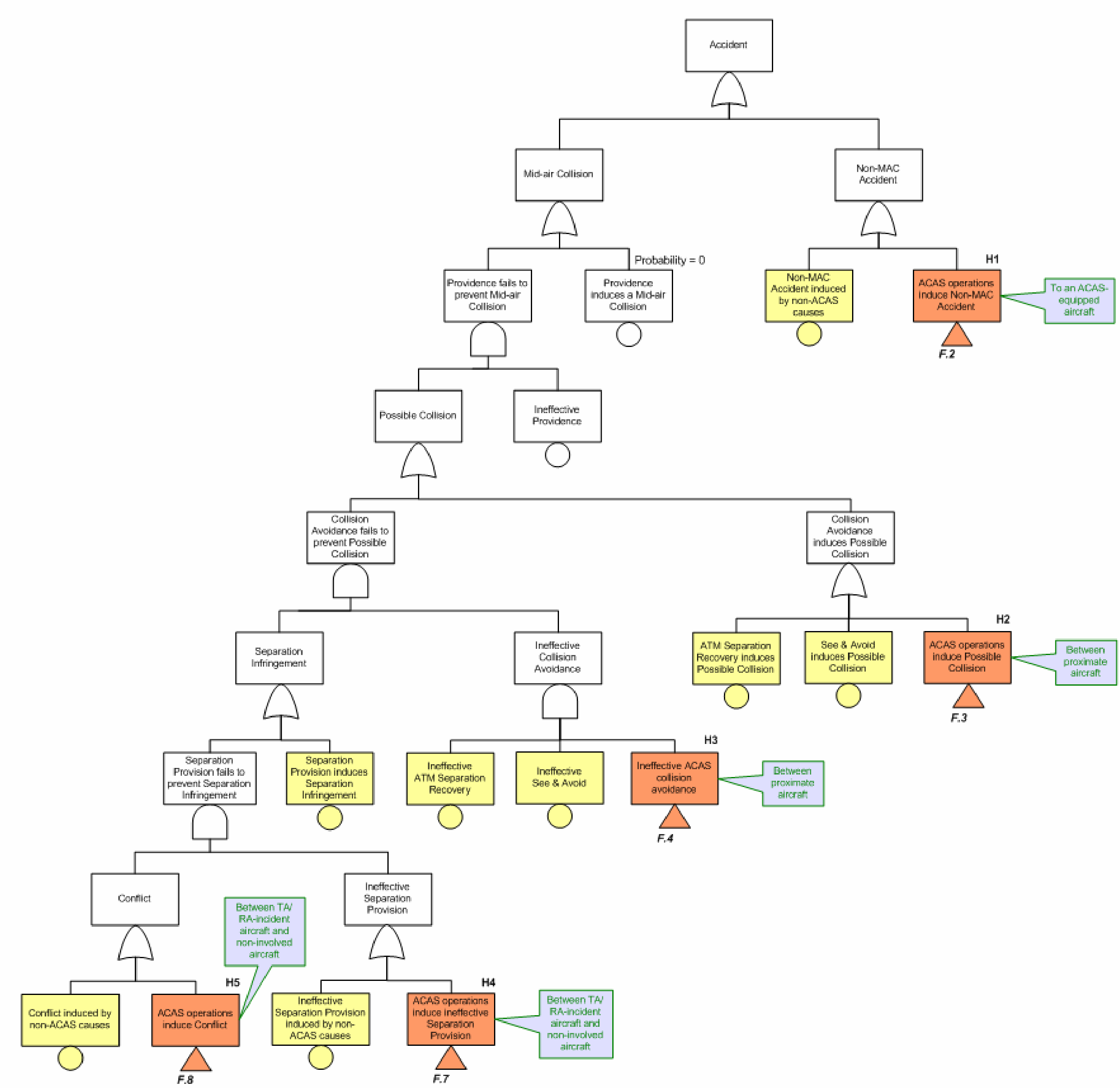
The events are colour coded as follows:


Hazard from ACAS operations
Event is outside scope of APOSC
Normal event in system or its environment
There is a corresponding Event in Contingency Tree

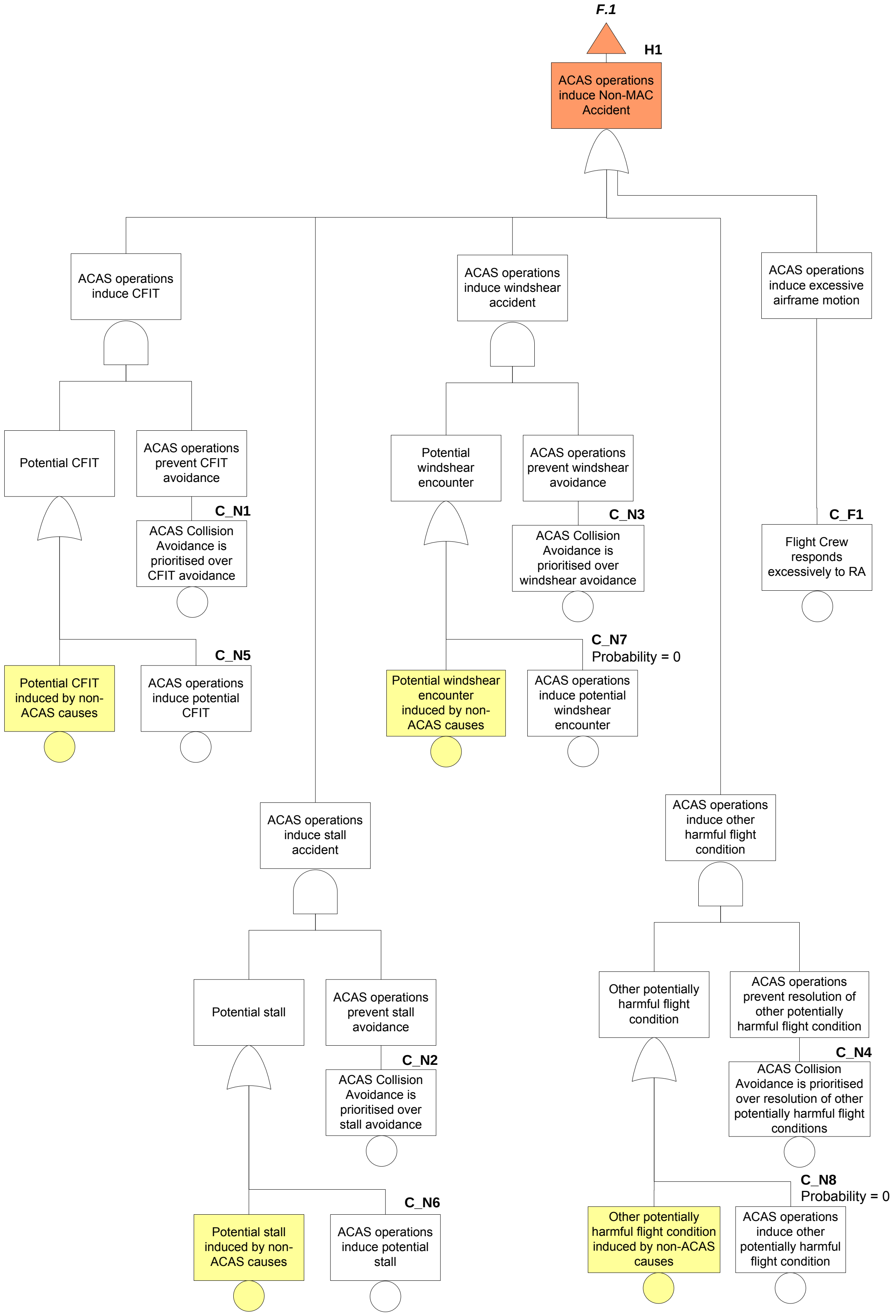
Where an event is shown with a probability of zero, this means that its occurrence is has been assessed as not credible – such events, and their justification, are shown in the following table.

Event	Figure	Justification
ACAS operations inducing a potential windshear encounter	F.2	Windshear encounters necessarily occur at low altitudes. However, in conformity with SR_A8 [H.1.2], ACAS does not issue RAs below 1000ft AGL, and does not issue descend RAs below 1100ft AGL.
ACAS operations inducing a potentially harmful flight condition, other than potential CFIT or stall	F.2	There is no causal relationship between collision avoidance and wake vortex encounter, overspeed, or other harmful situations.
Own Airframe inducing a possible collision, or intruder Airframe rendering own ACAS ineffective	F.3 F.6	Airframe failure or abnormal environment will not by themselves induce a possible collision.

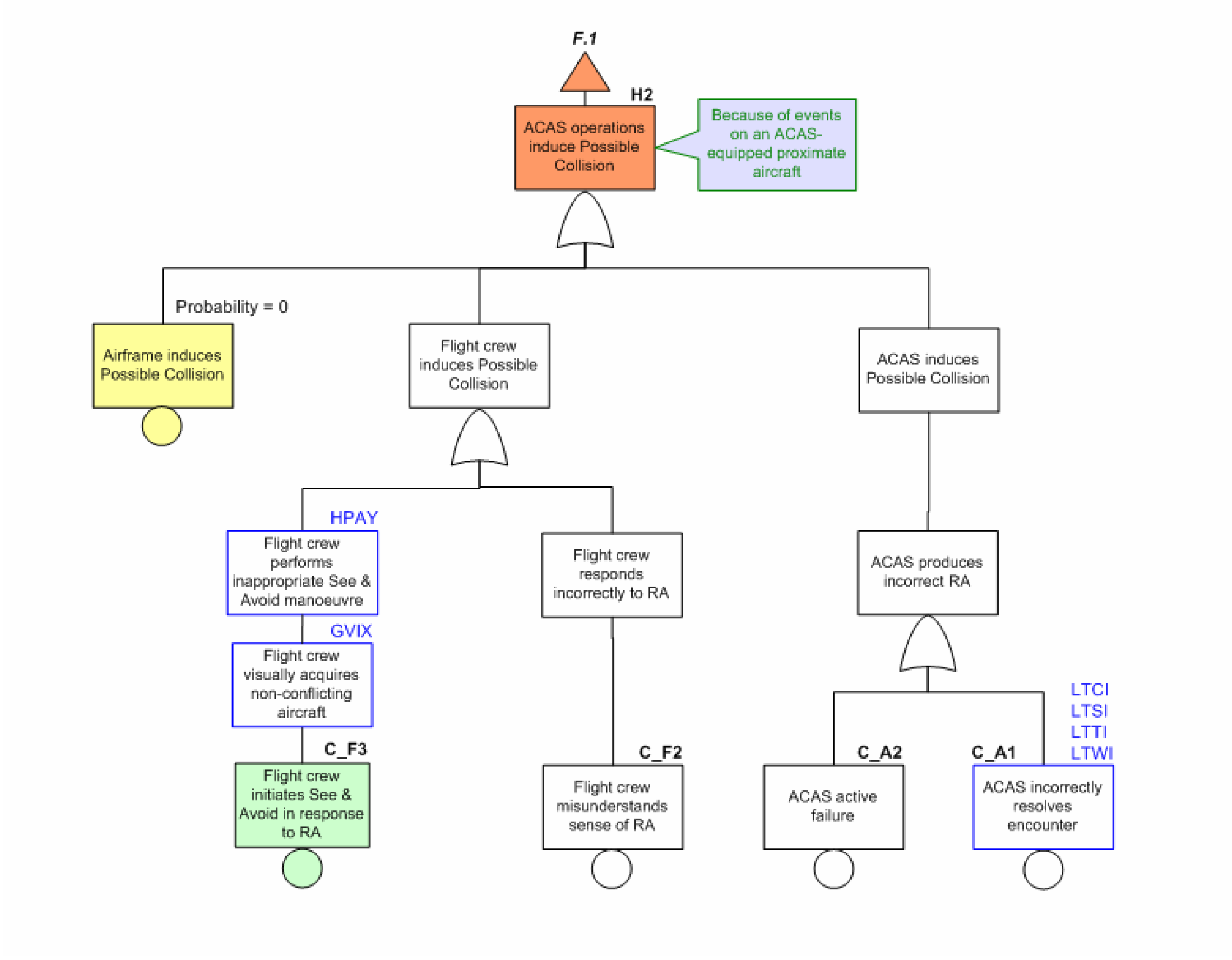
F.1 ACAS Accident Contributors (all Hazards)


Accident
Mid-air Collision
Non-MAC Accident
Probability = 0
Providence fails to prevent Mid-air Collision
Providence induces a Mid-air Collision
Non-MAC Accident induced by non-ACAS causes
H1
ACAS operations induce Non-MAC Accident
To an ACAS-equipped aircraft
F.2
Possible Collision
Ineffective Providence
Collision Avoidance fails to prevent Possible Collision
Collision Avoidance induces Possible Collision
Separation Infringement
Ineffective Collision Avoidance
ATM Separation Recovery induces Possible Collision
See & Avoid induces Possible Collision
H2
ACAS operations induce Possible Collision
Between proximate aircraft
F.3
Separation Provision fails to prevent Separation Infringement
Separation Provision induces Separation Infringement
Ineffective ATM Separation Recovery
Ineffective See & Avoid
H3
Ineffective ACAS collision avoidance
Between proximate aircraft
F.4
Conflict
Ineffective Separation Provision
Between TA/ RA-incident aircraft and non-involved aircraft
Conflict induced by non-ACAS causes
H5
ACAS operations induce Conflict
F.8
Ineffective Separation Provision induced by non-ACAS causes
H4
ACAS operations induce ineffective Separation Provision
Between TA/ RA-incident aircraft and non-involved aircraft
F.7

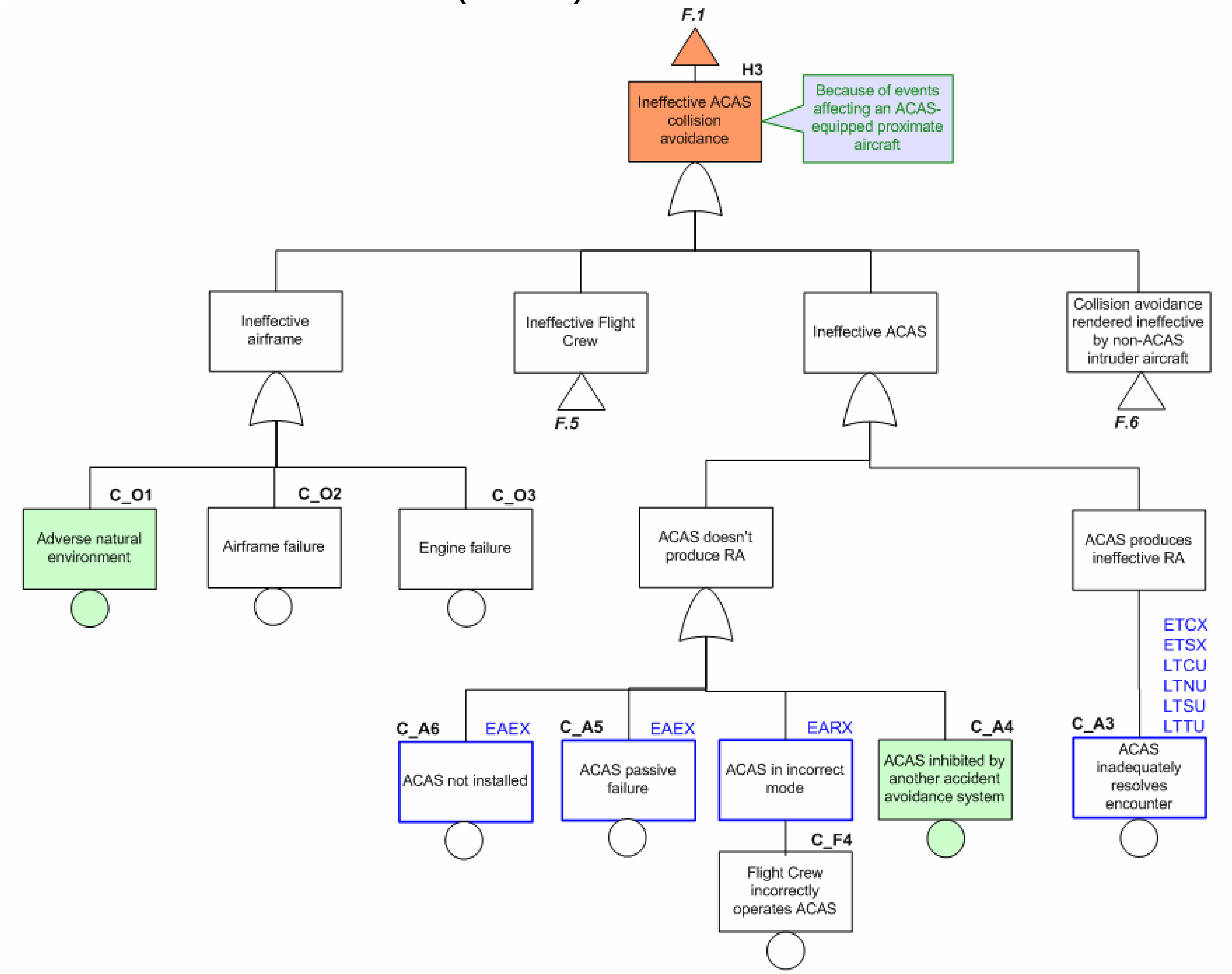
F.2 ACAS Induced Non-MAC Accident (Hazard 1)


F.1
H1
ACAS operations induce Non-MAC Accident
ACAS operations induce CFIT
ACAS operations induce windshear accident
ACAS operations induce excessive airframe motion
Potential CFIT
ACAS operations prevent CFIT avoidance
C_N1
ACAS Collision Avoidance is prioritised over CFIT avoidance
Potential windshear encounter
ACAS operations prevent windshear avoidance
C_N3
ACAS Collision Avoidance is prioritised over windshear avoidance
C_F1
Flight Crew responds excessively to RA
C_N5
Potential CFIT induced by non-ACAS causes
ACAS operations induce potential CFIT
C_N7
Probability = 0
Potential windshear encounter induced by non-ACAS causes
ACAS operations induce potential windshear encounter
ACAS operations induce stall accident
ACAS operations induce other harmful flight condition
Potential stall
ACAS operations prevent stall avoidance
C_N2
ACAS Collision Avoidance is prioritised over stall avoidance
Other potentially harmful flight condition
ACAS operations prevent resolution of other potentially harmful flight condition
C_N4
ACAS Collision Avoidance is prioritised over resolution of other potentially harmful flight conditions
C_N6
Potential stall induced by non-ACAS causes
ACAS operations induce potential stall
C_N8
Probability = 0
Other potentially harmful flight condition induced by non-ACAS causes
ACAS operations induce other potentially harmful flight condition

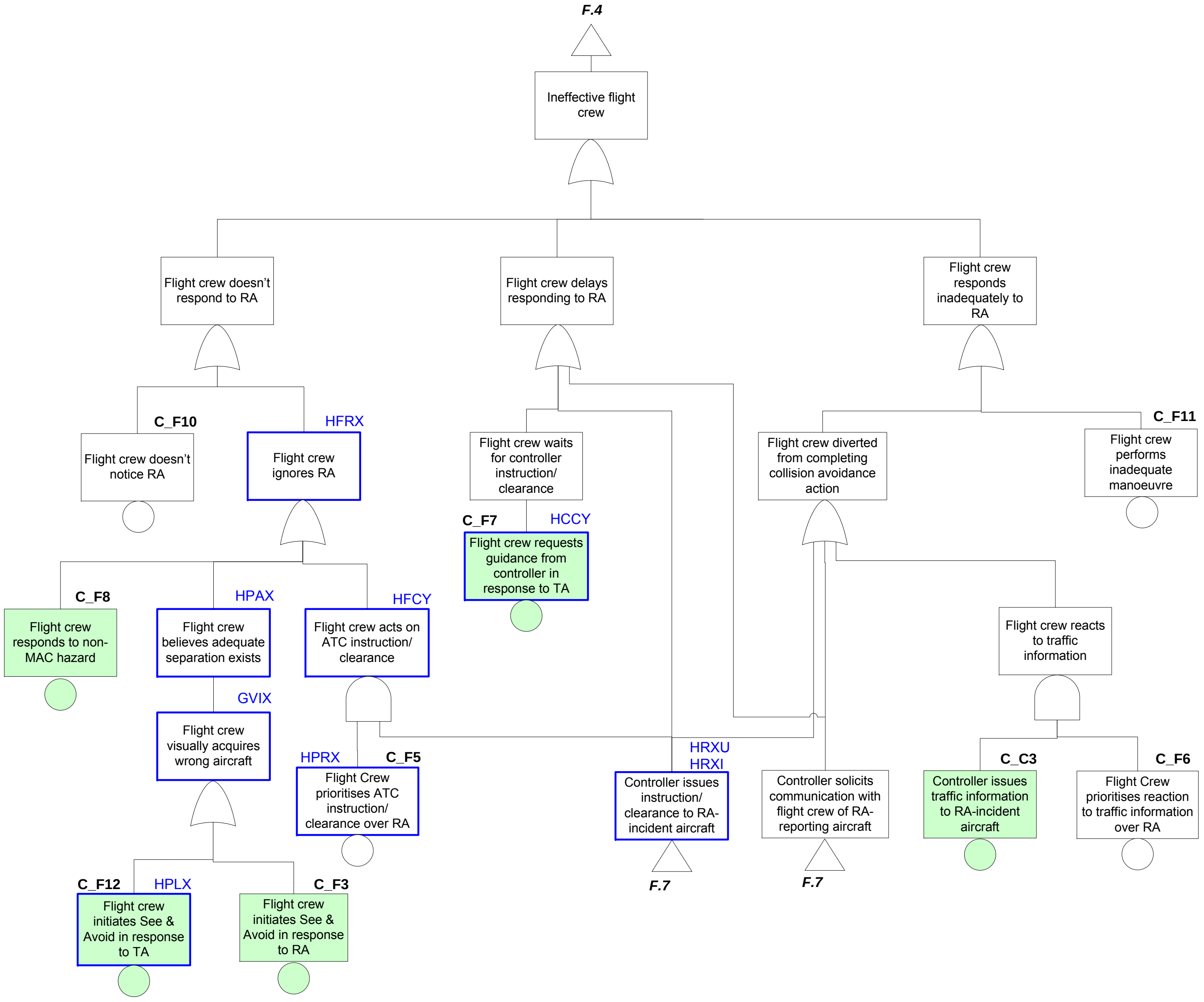
F.3 ACAS Induced Possible Collision (Hazard 2)


F.1
H2
ACAS operations induce Possible Collision
Because of events on an ACAS-equipped proximate aircraft
Probability = 0
Airframe induces Possible Collision
Flight crew induces Possible Collision
ACAS induces Possible Collision
HPAY
Flight crew performs inappropriate See & Avoid manoeuvre
GVIX
Flight crew visually acquires non-conflicting aircraft
C_F3
Flight crew initiates See & Avoid in response to RA
Flight crew responds incorrectly to RA
C_F2
Flight crew misunderstands sense of RA
ACAS produces incorrect RA
C_A2
ACAS active failure
C_A1
LTCI
LTSI
LTTI
LTWI
ACAS incorrectly resolves encounter

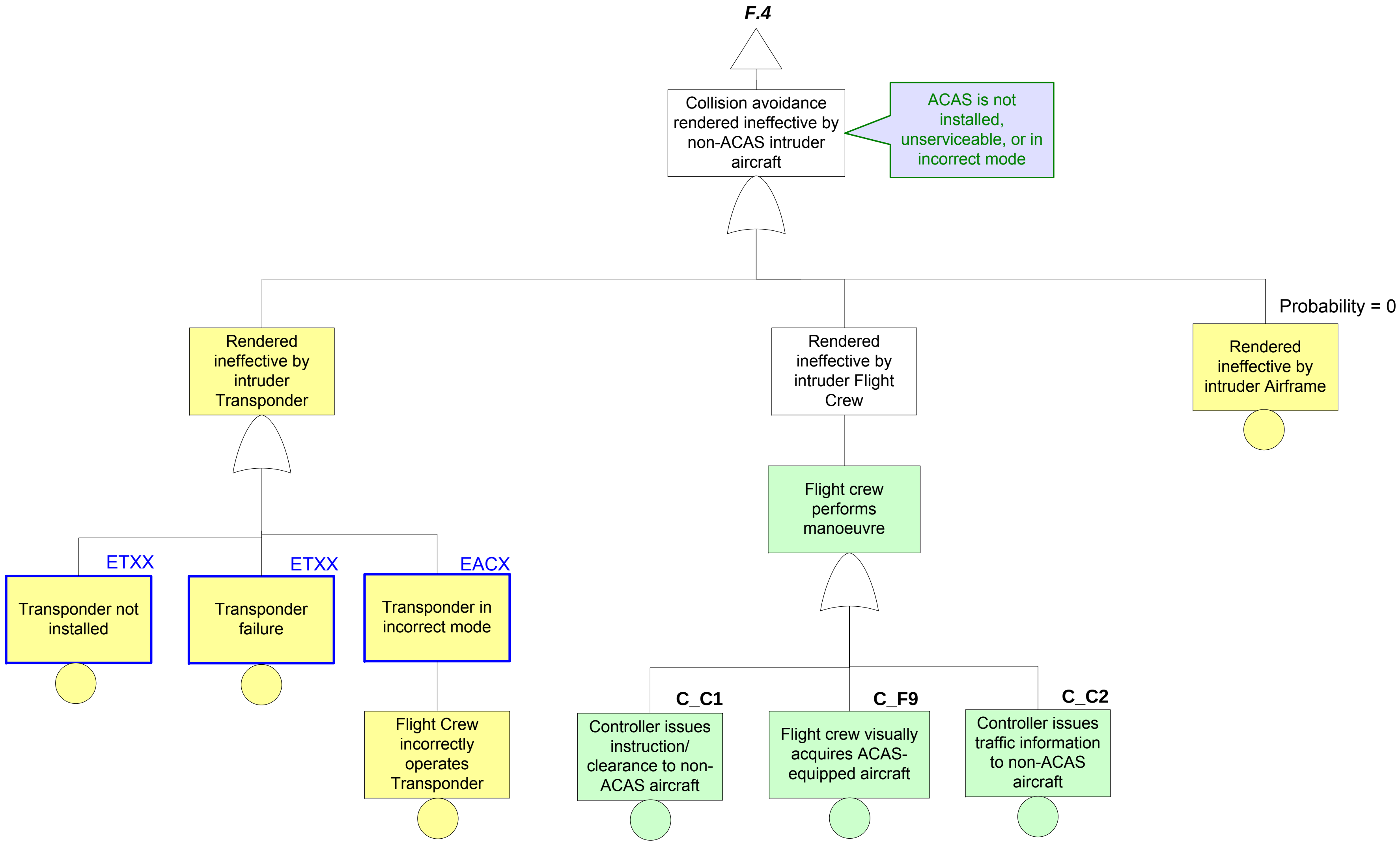
F.4 Ineffective ACAS Collision Avoidance (Hazard 3)


F.1
H3
Ineffective ACAS collision avoidance
Because of events affecting an ACAS-equipped proximate aircraft
Ineffective airframe
Ineffective Flight Crew
F.5
Ineffective ACAS
Collision avoidance rendered ineffective by non-ACAS intruder aircraft
F.6
C_O1
Adverse natural environment
C_O2
Airframe failure
C_O3
Engine failure
ACAS doesn't produce RA
ACAS produces ineffective RA
ETCX
ETSX
LTCU
LTNU
LTSU
LTTU
C_A6
EAEX
ACAS not installed
C_A5
EAEX
ACAS passive failure
EARX
ACAS in incorrect mode
C_F4
Flight Crew incorrectly operates ACAS
C_A4
ACAS inhibited by another accident avoidance system
C_A3
ACAS inadequately resolves encounter

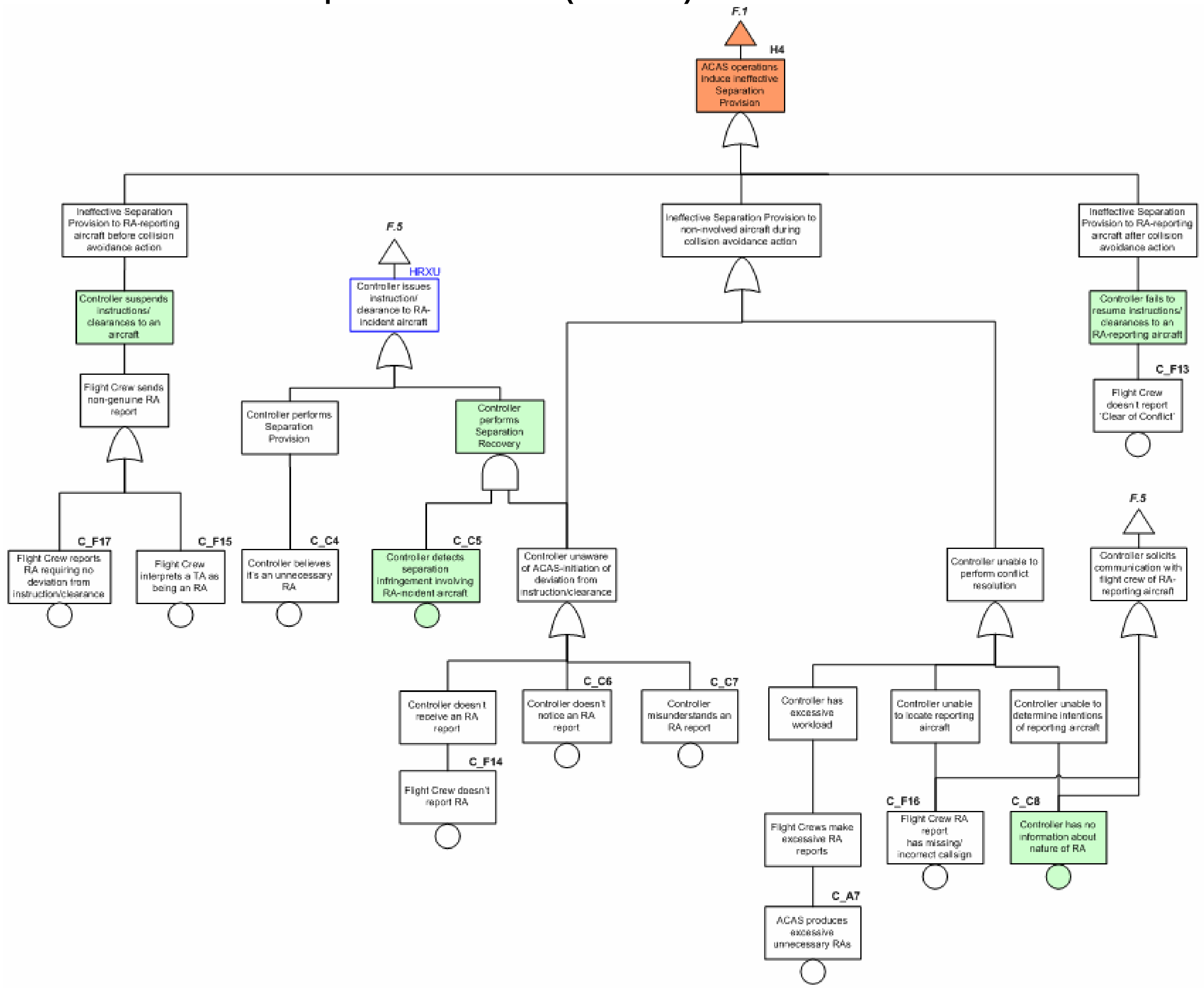
F.5 Ineffective Flight Crew


F.4
Ineffective flight crew
Flight crew doesn't respond to RA
Flight crew delays responding to RA
Flight crew responds inadequately to RA
C_F10
Flight crew doesn't notice RA
HFRX
Flight crew ignores RA
Flight crew waits for controller instruction/ clearance
C_F7
HCCY
Flight crew requests guidance from controller in response to TA
Flight crew diverted from completing collision avoidance action
C_F11
Flight crew performs inadequate manoeuvre
C_F8
Flight crew responds to non-MAC hazard
HPAX
Flight crew believes adequate separation exists
HFCY
Flight crew acts on ATC instruction/ clearance
Flight crew reacts to traffic information
GVIX
Flight crew visually acquires wrong aircraft
HPRX
C_F5
Flight Crew prioritises ATC instruction/ clearance over RA
HRXU
HRXI
Controller issues instruction/ clearance to RA-incident aircraft
Controller solicits communication with flight crew of RA-reporting aircraft
C_C3
Controller issues traffic information to RA-incident aircraft
C_F6
Flight Crew prioritises reaction to traffic information over RA
F.7
F.7
C_F12
HPLX
Flight crew initiates See & Avoid in response to TA
C_F3
Flight crew initiates See & Avoid in response to RA

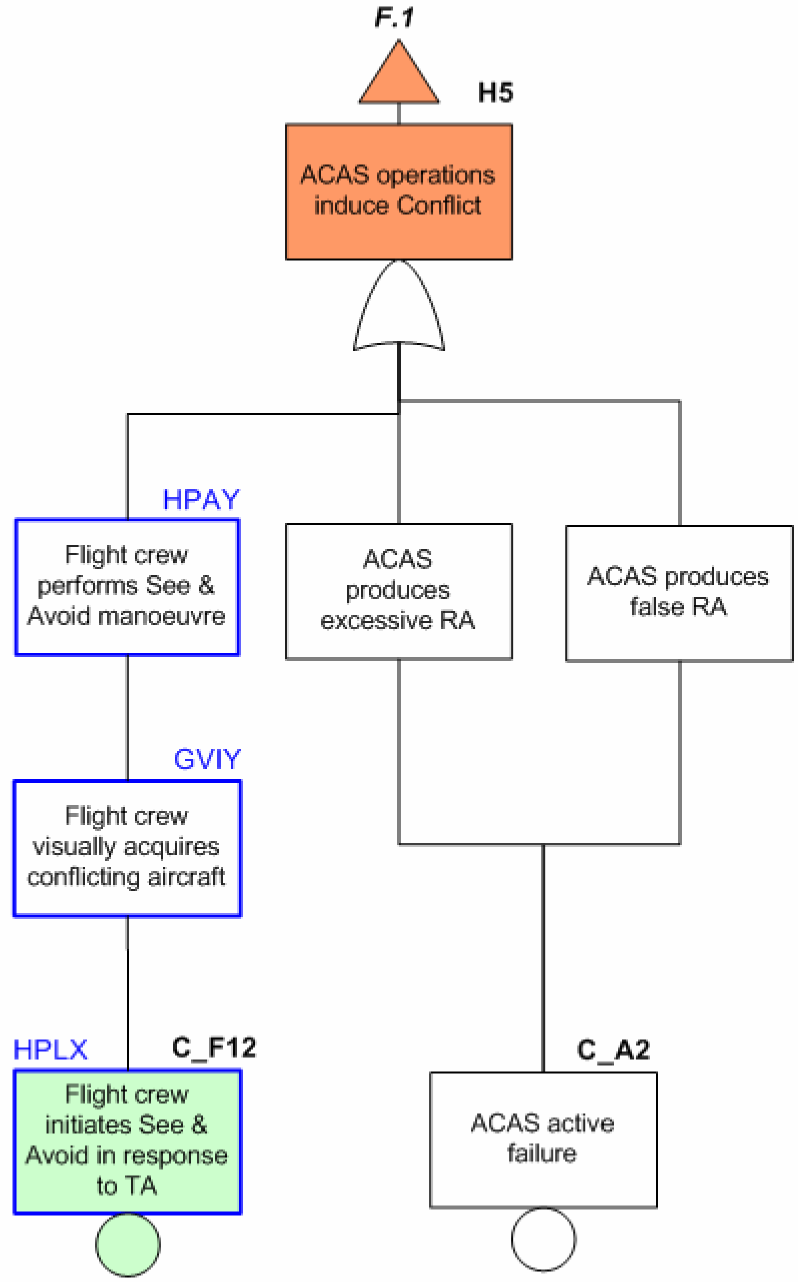
F.6 Intruder Renders Collision Avoidance Ineffective


F.4
Collision avoidance rendered ineffective by non-ACAS intruder aircraft
ACAS is not installed, unserviceable, or in incorrect mode
Rendered ineffective by intruder Transponder
Rendered ineffective by intruder Flight Crew
Probability = 0
Rendered ineffective by intruder Airframe
ETXX
Transponder not installed
ETXX
Transponder failure
EACX
Transponder in incorrect mode
Flight Crew incorrectly operates Transponder
Flight crew performs manoeuvre
C_C1
Controller issues instruction/ clearance to non-ACAS aircraft
C_F9
Flight crew visually acquires ACAS-equipped aircraft
C_C2
Controller issues traffic information to non-ACAS aircraft

F.7 ACAS Induced Ineffective Separation Provision (Hazard 4)


F.1
H4
ACAS operations induce ineffective Separation Provision
Ineffective Separation Provision to RA-reporting aircraft before collision avoidance action
F.5
HRXU
Controller issues instruction/ clearance to RA-incident aircraft
Ineffective Separation Provision to non-involved aircraft during collision avoidance action
Ineffective Separation Provision to RA-reporting aircraft after collision avoidance action
Controller suspends instructions/ clearances to an aircraft
Controller fails to resume instructions/ clearances to an RA-reporting aircraft
C_F13
Flight Crew doesn't report 'Clear of Conflict'
Flight Crew sends non-genuine RA report
Controller performs Separation Provision
Controller performs Separation Recovery
F.5
C_F17
Flight Crew reports RA requiring no deviation from instruction/clearance
C_F15
Flight Crew interprets a TA as being an RA
C_C4
Controller believes it's an unnecessary RA
C_C5
Controller detects separation infringement involving RA-incident aircraft
Controller unaware of ACAS-initiation of deviation from instruction/clearance
Controller unable to perform conflict resolution
Controller solicits communication with flight crew of RA-reporting aircraft
Controller doesn't receive an RA report
C_C6
Controller doesn't notice an RA report
C_C7
Controller misunderstands an RA report
Controller has excessive workload
Controller unable to locate reporting aircraft
Controller unable to determine intentions of reporting aircraft
C_F14
Flight Crew doesn't report RA
C_F16
Flight Crew RA report has missing/ incorrect callsign
C_C8
Controller has no information about nature of RA
Flight Crews make excessive RA reports
C_A7
ACAS produces excessive unnecessary RAs

F.8 ACAS Induced Conflict (Hazard 5)


F.1
H5
ACAS operations induce Conflict
HPAY
Flight crew performs See & Avoid manoeuvre
ACAS produces excessive RA
ACAS produces false RA
GVIY
Flight crew visually acquires conflicting aircraft
HPLX
C_F12
Flight crew initiates See & Avoid in response to TA
C_A2
ACAS active failure

APPENDIX G HAZARD CAUSES

The table below shows the complete set of relationships between hazards and causes extracted from the accident-causation model in Appendix F. These are shown in columns 1-3.

Column 4 shows the relationship between the hazard causes and the ACAS Safety Requirements[61]. Its purpose is to determine whether the hazard cause can be equated to a non-compliance with one or more Safety Requirements. The hazard causes which are attributable to failure of the system elements are used to support Arg 1.5.3 in section 6.6.4.

Column 5 identifies any Contingency Tree Event(s) which are equivalent to the hazard causes. This information is used by the analysis supporting Arg 1.5.4 in section 6.6.5.

Hazard Ref	Hazard Cause	Cause Ref	Non-compliance with SR	Equivalent Contingency Tree Event(s)
Other Accident Avoidance Systems				
H1	ACAS Collision Avoidance is prioritised over CFIT avoidance	C_N1	SR_F2	None
H1	ACAS Collision Avoidance is prioritised over stall avoidance	C_N2	SR_F2	None
H1	ACAS Collision Avoidance is prioritised over windshear avoidance	C_N3	SR_F2	None
H1	ACAS Collision Avoidance is prioritised over resolution of other potentially harmful flight conditions	C_N4	SR_F2	None
H1	ACAS operations induce potential CFIT	C_N5	SR_A8	None
H1	ACAS operations induce potential stall	C_N6	SR_F3	None
H1	ACAS operations induce potential windshear encounter	C_N7	None, but cause not credible	None
H1	ACAS operations induce other potentially harmful flight condition	C_N8	None, but cause not credible	None
Airframe				
H3	Adverse natural environment	C_O1	None, but abnormal environment is addressed by SR_F6	None
H3	Airframe failure	C_O2	None, but aircraft-related failures are addressed by SR_F5	None

[61] the independence Safety Requirements to follow the RA unless to do so would jeopardize the safety of the aircraft are not shown because non-compliance with such Requirements cannot by itself induce a hazard

Hazard Ref	Hazard Cause	Cause Ref	Non-compliance with SR	Equivalent Contingency Tree Event(s)
H3	Engine failure	C_O3	None, but aircraft-related failures are addressed by SR_F5	None
		ACAS Equipment		
H2	ACAS incorrectly resolves encounter[62]	C_A1	SR_A4 SR_A5 or SR_A11	LTCI LTSI LTTI LTWI
H2 H5	ACAS active failure[63] (ACAS produces false RA)	C_A2	SR_A3	None
H3	ACAS inadequately resolves encounter[64]	C_A3	SR_A4	ETCX ETSX LTCU LTNU LTSU LTTU
H3	ACAS inhibited by other accident avoidance system	C_A4	None, required operation in accordance with equipment certification requirements	None
H3	ACAS passive failure (ACAS fails to produce RA)	C_A5	SR_A3 or SR_A4	EAEX
H3	ACAS not installed	C_A6	None, permitted event in normal environment	EAEX
H4	ACAS produces excessive unnecessary RAs	C_A7	SR_A1 or SR_A9	None
		Flight Crew		
H1	Flight Crew responds excessively to RA	C_F1	SR_F3	None, included as part of pilot response model [section 6.2.5]
H2	Flight Crew misunderstands sense of RA	C_F2	SR_F2	None
H2 H3	Flight Crew initiates See & Avoid in response to RA	C_F3	SR_F2	None

[62] Incorrect resolution of encounter would occur if both aircraft were given, for example, descend RAs rather than complementary RAs.
[63] A false RA is one which is produced when the ACAS algorithms in DO-185 do not require any RA.
[64] An inadequate RA is one where the strength of the RA would be insufficient to resolve the encounter.

Hazard Ref	**Hazard Cause**	**Cause Ref**	**Non-compliance with SR**	**Equivalent Contingency Tree Event(s)**
H3	Flight Crew incorrectly operates ACAS	C_F4	SR_F7	None
H3	Flight Crew prioritises ATC instruction/clearance over RA	C_F5	SR_F2	HPRX
H3	Flight Crew prioritises reaction to traffic information over RA	C_F6	SR_F2	None
H3	Flight Crew requests guidance from controller following TA	C_F7	None, permitted aircraft operating procedure	HCCY
H3	Flight Crew responds to non-MAC hazard	C_F8	None, required operation in accordance with SR_F2	None
H3	Flight Crew visually acquires ACAS-equipped aircraft	C_F9	None, normal aircraft operating procedure	None
H3	Flight crew doesn't notice RA	C_F10	SR_F2	None
H3	Flight crew performs inadequate manoeuvre[65]	C_F11	SR_F3	None, included as part of pilot response model [section 6.2.5]
H3 H5	Flight Crew initiates See & Avoid in response to TA	C_F12	None, permitted aircraft operating procedure	HPLX
H4	Flight Crew doesn't report 'Clear of Conflict'	C_F13	SR_F4	None
H4	Flight Crew doesn't report RA	C_F14	SR_F4	None
H4	Flight Crew interprets a TA as being an RA	C_F15	SR_F1	None
H4	Flight Crew RA report has missing/incorrect callsign	C_F16	SR_F4	None
H4	Flight Crew reports RA requiring no deviation from instruction/clearance	C_F17	SR_F4	None
	Air Traffic Controller			
H3	Controller issues instruction/clearance to non-ACAS aircraft	C_C1	None, ATC normal operation	None
H3	Controller issues traffic information to non-ACAS aircraft	C_C2	None, ATS normal operation	None

[65] This cause includes the limiting case, where the flight crew performs no manoeuvre at all in response to an RA, which is perhaps the most common.

Hazard Ref	Hazard Cause	Cause Ref	Non-compliance with SR	Equivalent Contingency Tree Event(s)
H3	Controller issues traffic information to RA-incident aircraft	C_C3	None, ATS permitted operation	None
H4	Controller believes it’s an unnecessary RA	C_C4	SR_C1	None
H4	Controller detects separation infringement involving RA-incident aircraft	C_C5	None, ATC normal operation	None
H4	Controller doesn’t notice an RA report	C_C6	SR_C1	None
H4	Controller misunderstands an RA report	C_C7	SR_C1	None
H4	Controller has no information about nature of RA	C_C8	None, ATC normal operation	None

APPENDIX H CONSISTENCY ASSESSMENT OF ICAO ACAS PROVISIONS

This Appendix contains the results of an assessment of the consistency of ICAO ACAS provisions listed in section 2.1 (and expanded in Appendix L hereto) with the Safety Requirements listed in Appendix B. The assessment also serves to verify the coherency within and between the ICAO provisions themselves. It provides the evidence to support Arg 2.1, as mentioned in section 7.2.

Since the context of the Safety Case is completion of the transition period for implementing Phase 2 of the European ACAS II Policy, there are no Safety Requirements related to ACAS carriage. Therefore, Annex 6 [6] provisions are automatically excluded.

The Annex 11 [13] provision reflects the regulatory stance that the benefit of safety nets such as ACAS shall not be used to influence those ATS normally provided by an ANSP. Since this provision is elaborated in PANS-ATM 15.7.3.1 [H.4.1], Annex 11 is also excluded.

The ACAS Training Guidelines for Pilots in the Attachment to Part III, Section 3, Chapter 3 of PANS-OPS are not considered to be *requirements* on Flight Crew and are therefore excluded.

Finally, the Guidance Material related to ACAS in the Attachment to Volume IV of Annex 10 does not constitute *requirements* on equipment and is excluded.

Notes included in ICAO ACAS provisions are included even though formally they do not constitute a part of ICAO Standards or Recommended Practices.

The notation used in H.1.2, H.2.2, H.3.2 and H.4.2 below is as follows:

C	ICAO Provision is compliant with the Safety Requirement
PC	ICAO Provision is partially compliant with the Safety Requirement
NC	ICAO Provision is non-compliant with the Safety Requirement
N/A	ICAO Provision is unrelated to the Safety Requirement

H.1 Conformity Assessment of Annex 10 [11]

H.1.1 Annex 10 Provisions

Due to the extent of the ACAS provisions in Annex 10 Volume IV, only those functional requirements which can be related to the ACAS Safety Requirements have been reproduced below. Those detailed technical requirements[66] not shown are asserted to be consistent with the related Safety Requirements in those cases where they fall within the scope of the Safety Case. The justification for this assertion is that they all constitute requirements on functionality essential to support implementation of the Safety Requirements, and are therefore consistent with the Safety Requirements. These cases are identified in H.1.2.

4.2 ACAS I GENERAL PROVISIONS AND CHARACTERISTICS

…

4.3 GENERAL PROVISIONS RELATING TO ACAS II AND ACAS III

Note 1.— The acronym ACAS is used in this section to indicate either ACAS II or ACAS III.

Note 2.— Carriage requirements for ACAS equipment are addressed in Annex 6, Part I, Chapter 6.

Note 3.— The term “equipped threat” is used in this section to indicate a threat fitted with ACAS II or ACAS III.

4.3.1 Functional requirements

4.3.1.1 *ACAS functions.* ACAS shall perform the following functions:

a) surveillance;

b) generation of TAs;

c) threat detection;

d) generation of RAs;

e) coordination; and

f) communication with ground stations.

The equipment shall execute functions b) through e) on each cycle of operation.

[66] interference control, protocols, signal formats, *et al*.

Note.— Certain features of these functions must be standardized to ensure that ACAS units cooperate satisfactorily with other ACAS units, with Mode S ground stations and with the ATC system. Each of the features that are standardized is discussed below. Certain other features are given herein as recommendations.

4.3.1.1.1 The duration of a cycle shall not exceed 1.2 s.

4.3.2 Surveillance performance requirements

4.3.2.1 *General surveillance requirements.* ACAS shall interrogate SSR Mode A/C and Mode S transponders in other aircraft and detect the transponder replies. ACAS shall measure the range and relative bearing of responding aircraft. Using these measurements and information conveyed by transponder replies, ACAS shall estimate the relative positions of each responding aircraft. ACAS shall include provisions for achieving such position determination in the presence of ground reflections, interference and variations in signal strength.

4.3.2.1.1 *Track establishment probability.* ACAS shall generate an established track, with at least a 0.90 probability that the track is established 30 s before closest approach, on aircraft equipped with transponders when all of the following conditions are satisfied:

a) the elevation angles of these aircraft are within ±10 degrees relative to the ACAS aircraft pitch plane;

b) the magnitudes of these aircraft's rates of change of altitude are less than or equal to 51 m/s (10000 ft/min);

c) the transponders and antennas of these aircraft meet the Standards of Chapter 3, 3.1.1 and 3.1.2;

d) the closing speeds and directions of these aircraft, the local density of SSR transponder-equipped aircraft and the number of other ACAS interrogators in the vicinity (as determined by monitoring ACAS broadcasts, 4.3.7.1.2.4) satisfy the conditions specified in Table 4-1; and

e) the minimum slant range is equal to or greater than 300 m (1 000 ft).

[Table 4-1]

4.3.2.1.1.1 ACAS shall continue to provide surveillance with no abrupt degradation in track establishment probability as any one of the condition bounds defined in 4.3.2.1.1 is exceeded.

4.3.2.1.1.2 ACAS shall not track Mode S aircraft that report that they are on the ground.

Note.— A Mode S aircraft may report that it is on the ground by coding in the capability (CA) field in a DF = 11 or DF = 17 transmission (Chapter 3, 3.1.2.5.2.2.1) or by coding in the vertical status (VS) field in a DF = 0 transmission (Chapter 3, 3.1.2.8.2.1). Alternatively, if the aircraft is under Mode S ground surveillance, ground status may be determined by monitoring the flight status (FS) field in downlink formats DF = 4, 5, 20 or 21 (Chapter 3, 3.1.2.6.5.1).

4.3.2.1.1.3 **Recommendation.—** *ACAS should achieve the required tracking performance when the average SSR Mode A/C asynchronous reply rate from transponders in the vicinity of the ACAS aircraft is 240 replies per second and when the peak interrogation rate received by the individual transponders under surveillance is 500 per second.*

Note.— The peak interrogation rate mentioned above includes interrogations from all sources.

4.3.2.1.2 *False track probability.* The probability that an established Mode A/C track does not correspond in range and altitude, if reported, to an actual aircraft shall be less than 10–2. For an established Mode S track this probability shall be less than 10–6. These limits shall not be exceeded in any traffic environment.

4.3.2.1.3 *RANGE AND BEARING ACCURACY*

4.3.2.1.3.1 Range shall be measured with a resolution of 14.5 m (1/128 NM) or better.

4.3.2.1.3.2 **Recommendation.—** *The errors in the relative bearings of the estimated positions of intruders should not exceed 10 degrees rms.*

Note.— This accuracy in the relative bearing of intruders is practicable and sufficient as an aid to the visual acquisition of potential threats. In addition, such relative bearing information has been found useful in threat detection, where it can indicate that an intruder is a threat. However, this accuracy is not sufficient as a basis for horizontal RAs, nor is it sufficient for reliable predictions of horizontal miss distance.

4.3.2.2 INTERFERENCE CONTROL

….

4.3.3 Traffic advisories (TAs)

4.3.3.1 *TA function.* ACAS shall provide TAs to alert the flight crew to potential threats. Such TAs shall be accompanied by an indication of the approximate relative position of potential threats.

4.3.3.2 PROXIMATE TRAFFIC DISPLAY

Recommendation.— *While any RA and/or TA are displayed, proximate traffic within 11 km (6 NM) range and, if altitude reporting, ±370 m (1 200 ft) altitude should be displayed. This proximate traffic should be distinguished (e.g. by colour or symbol type) from threats and potential threats, which should be more prominently displayed.*

4.3.3.3 *TAs as RA precursors.* The criteria for TAs shall be such that they are satisfied before those for an RA.

4.3.3.3.1 *TA warning time.* For intruders reporting altitude, the nominal TA warning time shall not be greater than (T+20 s) where T is the nominal warning time for the generation of the resolution advisory.

Note.— Ideally, RAs would always be preceded by a TA but this is not always possible, e.g. the RA criteria might be already satisfied when a track is first established, or a sudden and sharp manoeuvre by the intruder could cause the TA lead time to be less than a cycle.

4.3.4 Threat detection

4.3.4.1 *Declaration of threat.* ACAS shall evaluate appropriate characteristics of each intruder to determine whether or not it is a threat.

4.3.4.1.1 *Intruder characteristics.* As a minimum, the characteristics of an intruder that are used to identify a threat shall include:

a) tracked altitude;

b) tracked rate of change of altitude;

c) tracked slant range;

d) tracked rate of change of slant range; and

e) sensitivity level of intruder's ACAS, *Si*.

For an intruder not equipped with ACAS II or ACAS III, *Si* shall be set to 1.

4.3.4.1.2 *Own aircraft characteristics.* As a minimum, the characteristics of own aircraft that are used to identify a threat shall include:

a) altitude;

b) rate of change of altitude; and

c) sensitivity level of own ACAS (4.3.4.3).

4.3.4.2 *Sensitivity levels.* ACAS shall be capable of operating at any of a number of sensitivity levels. These shall include:

…

4.3.5 Resolution advisories (RAs)

4.3.5.1 *RA generation.* For all threats, ACAS shall generate an RA except where it is not possible to select an RA that can be predicted to provide adequate separation either because of uncertainty in the diagnosis of the intruder's flight path or because there is a high risk that a manoeuvre by the threat will negate the RA.

4.3.5.1.1 *RA cancellation.* Once an RA has been generated against a threat or threats it shall be maintained or modified until tests that are less stringent than those for threat detection indicate on two consecutive cycles that the RA may be cancelled, at which time it shall be cancelled.

4.3.5.2 *RA selection.* ACAS shall generate the RA that is predicted to provide adequate separation from all threats and that has the least effect on the current flight path of the ACAS aircraft consistent with the other provisions in this chapter.

4.3.5.3 *RA effectiveness.* The RA shall not recommend or continue to recommend a manoeuvre or manoeuvre restriction that, considering the range of probable threat trajectories, is more likely to reduce separation than increase it, subject to the provisions in 4.3.5.5.1.1 and 4.3.5.6.

Note.— See also 4.3.5.8.

4.3.5.4 *Aircraft capability.* The RA generated by ACAS shall be consistent with the performance capability of the aircraft.

4.3.5.4.1 *Proximity to the ground.* Descend RAs shall not be generated or maintained when own aircraft is below 300 m (1 000 ft) AGL.

4.3.5.4.2 ACAS shall not operate in sensitivity levels 3-7 when own aircraft is below 300 m (1 000 ft) AGL.

4.3.5.5 *Reversals of sense.* ACAS shall not reverse the sense of an RA from one cycle to the next, except as permitted in 4.3.5.5.1 to ensure coordination or when the predicted separation at closest approach for the existing sense is inadequate.

…

4.3.6 Coordination and communication

4.3.6.1 PROVISIONS FOR COORDINATION WITH ACAS-EQUIPPED THREATS

…

4.3.6.2 PROVISIONS FOR ACAS COMMUNICATION WITH GROUND STATIONS

…

4.3.6.3 PROVISIONS FOR DATA TRANSFER BETWEEN ACAS AND ITS MODE S TRANSPONDER

…

4.3.7 ACAS protocols

4.3.7.1 SURVEILLANCE PROTOCOLS

…

4.3.8 Signal formats

…

4.3.9 ACAS equipment characteristics

4.3.9.1 *Interfaces.* As a minimum, the following input data shall be provided to the ACAS:

a) aircraft address code;

b) air-air and ground-air Mode S transmissions received by the Mode S transponder for use by ACAS (4.3.6.3.2);

c) own aircraft’s maximum cruising true airspeed capability (Chapter 3, 3.1.2.8.2.2);

d) pressure altitude; and

e) radio altitude.

Note.— Specific requirements for additional inputs for ACAS II and III are listed in the appropriate sections below.

4.3.9.2 *Aircraft antenna system.* ACAS shall transmit interrogations and receive replies via two antennas, one mounted on the top of the aircraft and the other on the bottom of the aircraft. The top-mounted antenna shall be directional and capable of being used for direction finding.

…

4.3.9.2.3 *ANTENNA SELECTION*

…

4.3.10 Monitoring

4.3.10.1 *Monitoring function.* ACAS shall continuously perform a monitoring function in order to provide a warning if any of the following conditions at least are satisfied:

a) there is no interrogation power limiting due to interference control (4.3.2.2.2) and the maximum radiated power is reduced to less than that necessary to satisfy the surveillance requirements specified in 4.3.2; or

b) any other failure in the equipment is detected which results in a reduced capability of providing TAs or RAs; or

c) data from external sources indispensable for ACAS operation are not provided, or the data provided are not credible.

4.3.10.2 *Effect on ACAS operation.* The ACAS monitoring function shall not adversely affect other ACAS functions.

4.3.10.3 *Monitoring response.* When the monitoring function detects a failure (4.3.10.1), ACAS shall:

a) indicate to the flight crew that an abnormal condition exists;

b) prevent any further ACAS interrogations; and

c) cause any Mode S transmission containing own aircraft's resolution capability to indicate that ACAS is not operating.

4.3.11 Requirements for a Mode S transponder used in conjunction with ACAS

…

4.3.12 Indications to the flight crew

4.3.12.1 CORRECTIVE AND PREVENTIVE RAS

Recommendation.— *Indications to the flight crew should distinguish between preventive and corrective RAs.*

4.3.12.2 ALTITUDE CROSSING RAS

Recommendation.— *If ACAS generates an altitude crossing RA, a specific indication should be given to the flight crew that it is crossing.*

4.4 PERFORMANCE OF THE ACAS II COLLISION AVOIDANCE LOGIC

Note.— Caution is to be observed when considering potential improvements to the reference ACAS II system described in Section 4 of the guidance material in Attachment A since changes may affect more than one aspect of the system performance. It is essential that alternative designs would not degrade the performances of other designs and that such compatibility is demonstrated with a high degree of confidence.

4.4.1 Definitions relating to the performance of the collision avoidance logic

…

4.4.2 Conditions under which the requirements apply

…

4.4.2.5 STANDARD PILOT MODEL

…

4.4.2.6 STANDARD ENCOUNTER MODEL

…

4.4.2.7 ACAS EQUIPAGE OF THE INTRUDER

…

4.4.2.8 COMPATIBILITY BETWEEN DIFFERENT COLLISION AVOIDANCE LOGIC DESIGNS

…

4.4.3 Reduction in the risk of collision

Under the conditions of 4.4.2, the collision avoidance logic shall be such that the expected number of collisions is reduced to the following proportions of the number expected in the absence of ACAS:

a) when the intruder is not ACAS equipped	0.18;
b) when the intruder is equipped but does not respond	0.32; and
c) when the intruder is equipped and responds	0.04.

4.4.4 Compatibility with air traffic management (ATM)

4.4.4.1 NUISANCE ALERT RATE

…

4.4.4.2 COMPATIBLE SENSE SELECTION

…

4.4.4.3.1 Under the conditions of 4.4.2, the collision avoidance logic shall be such that the number of RAs resulting in “deviations” (4.4.4.3.2) greater than the values indicated shall not exceed the following proportions of the total number of RAs:

[Table]

4.4.4.3.2 For the purposes of 4.4.4.3.1, the “deviation” of the equipped aircraft from the original trajectory shall be measured in the interval from the time at which the RA is first issued until the time at which, following cancellation of the RA, the equipped aircraft has recovered its original altitude rate. The deviation shall be calculated as the largest altitude difference at any time in this interval between the trajectory followed by the equipped aircraft when responding to its RA and its original trajectory.

4.4.5 Relative value of conflicting objectives

Recommendation.— *The collision avoidance logic should be such as to reduce as much as practicable the risk of collision (measured as defined in 4.4.3) and limit as much as practicable the disruption to ATM (measured as defined in 4.4.4).*

4.5 ACAS USE OF EXTENDED SQUITTER REPORTS

…

4.5.1 ACAS hybrid surveillance using extended squitter position data

…

4.5.2 ACAS operation with an improved receiver MTL

…

H.1.2 Conformity Assessment Results

ICAO Provision	Safety Requirement															Remarks
	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	
4.2 - 4.3 Note 3	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Not part of ACAS II requirements.
4.3.1.1 a)	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
4.3.1.1 b)	N/A	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
4.3.1.1 c)	N/A	N/A	C	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
4.3.1.1 d)	N/A	N/A	C	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
4.3.1.1 e)	N/A	N/A	N/A	N/A	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
4.3.1.1 f)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ACAS communications with ground stations are not implemented in ECAC airspace; hence this provision is outside the scope of Safety Case.
4.3.1.1.1	N/A	C	C	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
4.3.2.1	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
4.3.2.1.1 - 4.3.2.1.1.1	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	C	N/A	N/A	N/A	N/A	
4.3.2.1.1.2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	PC	N/A	N/A	N/A	N/A	N/A	N/A	There is no equivalent requirement dealing with Mode A/C aircraft.
4.3.2.1.1.3 - 4.3.2.1.3.2	C	N/A	N/A	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	DO-185A on which ACAS modelling studies are based is assumed to be compliant with the ICAO requirements in accordance with A003.

ICAO Provision	Safety Requirement															Remarks
	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	
4.3.2.2 - 4.3.2.2.2.2.3	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
4.3.3.1	N/A	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	There is no requirement to inhibit aural alerts below 500ft AGL [1].
4.3.3.2 - 4.3.4.1.1e)	N/A	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
4.3.4.1.2 - 4.3.4.1.2c)	N/A	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	C	N/A	N/A	N/A	N/A	N/A	
4.3.4.2 - 4.3.4.5	N/A	N/A	N/A	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	DO-185A on which ACAS modelling studies are based is assumed to be compliant with the ICAO requirements in accordance with A003. SLC commands from the ground are not implemented in ECAC airspace.
4.3.5.1	N/A	N/A	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	C	C	N/A	N/A	N/A	ICAO provision satisfies SR_A12 within the technical limitations of ACAS collision avoidance
4.3.5.1.1 - 4.3.5.3	N/A	N/A	C	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	DO-185A on which ACAS modelling studies are based is assumed to be compliant with the ICAO requirements in accordance with A003.
4.3.5.4	N/A	N/A	N/A	N/A	N/A	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
4.3.5.4.1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	The requirement should say 1100ft instead of 1000ft in order to be consistent with DO-185A. There is no associated requirement to inhibit increase descent RAs below 1450ft AGL [1].

ICAO Provision	Safety Requirement															Remarks
	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	
4.3.5.4.2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	C	N/A	N/A	N/A	N/A	N/A	N/A	
4.3.5.5 - 4.3.5.10	N/A	N/A	C	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	DO-185A on which ACAS modelling studies are based is assumed to be compliant with the ICAO requirements in accordance with A003.
4.3.6.1 - 4.3.6.1.4.3	N/A	N/A	N/A	N/A	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
4.3.6.2 - 4.3.6.2.2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ACAS communications with ground stations are not implemented in ECAC airspace; hence this provision is outside the scope of Safety Case.
4.3.6.3 - 4.3.9.1b)	N/A	N/A	C	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
4.3.9.1c)	N/A	N/A	C	C	N/A	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
4.3.9.1d) - 4.3.9.3.4	N/A	N/A	C	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
4.3.10 - 4.3.10.2)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	C	N/A	N/A	N/A	N/A	N/A	
4.3.10.3a)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	C	N/A	
4.3.10.3b)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	PC	N/A	N/A	C	N/A	N/A	The required effect on any ongoing advisories is not defined.
4.3.10.3c)	N/A	N/A	N/A	N/A	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
4.3.11 - 4.3.11.4.2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Outside scope of Safety Case [section 2.3.4].

ICAO Provision	Safety Requirement															Remarks
	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	
4.3.12 - 4.3.12.2	N/A	N/A	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	There are no *requirements* on what form the indications given to Flight Crew shall take, including visual versus audible means. The implication is that it is unnecessary to standardise ACAS HMI at any level of specification.
4.4 Note	N/A	N/A	N/A	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
4.4.1 - 4.4.2.8b)	C	C	C	C	N/A	C	C	N/A	N/A	N/A	C	C	N/A	N/A	N/A	ACAS modelling studies are assumed to comply with the stated conditions under which ACAS performance requirements shall apply.
4.4.3 - 4.4.4.2c)	N/A	N/A	N/A	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	DO-185A on which ACAS modelling studies are based is assumed to be compliant with the ICAO requirements in accordance with A003.
4.4.4.3.1 - 4.4.4.3.2	N/A	N/A	N/A	N/A	N/A	N/A	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
4.4.5	N/A	N/A	N/A	C	N/A	N/A	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	The recommendation does not address the ‘relative value’ of the two objectives. It therefore implies that they are equally important.
4.5 - 4.5.2.3 b)	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	

H.1.3 Conformity Assessment Conclusions

There are no ACAS equipment Safety Requirements which have no corresponding ICAO provisions.

The following ICAO Provision that falls within the scope of the Safety Case would not strictly be necessary in order for the Design to satisfy the Safety Criteria:

- 4.3.10.3a) When the monitoring function detects a failure, ACAS shall indicate to the flight crew that an abnormal condition exists

The operational status need not be known by Flight Crew because ACAS is a safety net which, by definition, should not affect aircraft operating procedures if it becomes unavailable pursuant to 4.3.10.3b). However, there may be failures which only manifest themselves in flight and therefore should be reported to the Flight Crew for rectification when the aircraft next lands,

Consequently, an additional Safety Requirement SR_A14 has been added corresponding to this ICAO provision.

H.2 Conformity Assessment of PANS-OPS [3][6]

H.2.1 PANS-OPS Provisions

Chapter 3

OPERATION OF AIRBORNE COLLISION AVOIDANCE SYSTEM (ACAS) EQUIPMENT

3.1 GENERAL

3.1.1 Airborne collision avoidance system (ACAS) indications shall be used by pilots in the avoidance of potential collisions, the enhancement of situational awareness, and the active search for, and visual acquisition of, conflicting traffic.

3.1.2 Nothing in the procedures specified in 3.2, “Use of ACAS indicators”, shall prevent pilots-in-command from exercising their best judgement and full authority in the choice of the best course of action to resolve a traffic conflict or avert a potential collision.

Note 1.— The ability of ACAS to fulfil its role of assisting pilots in the avoidance of potential collisions is dependent on the correct and timely response by pilots to ACAS indications. Operational experience has shown that the correct response by pilots is dependent on the effectiveness of the initial and recurrent training in ACAS procedures.

Note 2.— The normal operating mode of ACAS is TA/RA. The TA-only mode of operation is used in certain aircraft performance limiting conditions caused by in-flight failures or as otherwise promulgated by the appropriate authority.

Note 3.— ACAS Training Guidelines for Pilots are provided in the Attachment, “ACAS Training Guidelines for Pilots”.

3.2 USE OF ACAS INDICATORS

The indications generated by ACAS shall be used by pilots in conformity with the following safety considerations:

a) pilots shall not manoeuvre their aircraft in response to traffic advisories (TAs) only;

Note 1.— TAs are intended to alert pilots to the possibility of a resolution advisory (RA), to enhance situational awareness, and to assist in visual acquisition of conflicting traffic. However, visually acquired traffic may not be the same traffic causing a TA. Visual perception of an encounter may be misleading, particularly at night.

Note 2.— The above restriction in the use of TAs is due to the limited bearing accuracy and to the difficulty in interpreting altitude rate from displayed traffic information.

b) on receipt of a TA, pilots shall use all available information to prepare for appropriate action if an RA occurs; and

c) in the event of an RA, pilots shall:

1) respond immediately by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane;

Note 1.— Stall warning, wind shear, and ground proximity warning system alerts have precedence over ACAS.

Note 2.— Visually acquired traffic may not be the same traffic causing an RA. Visual perception of an encounter may be misleading, particularly at night.

2) follow the RA even if there is a conflict between the RA and an air traffic control (ATC) instruction to manoeuvre;

3) not manoeuvre in the opposite sense to an RA;

Note.— In the case of an ACAS-ACAS coordinated encounter, the RAs complement each other in order to reduce the potential for collision. Manoeuvres, or lack of manoeuvres, that result in vertical rates opposite to the sense of an RA could result in a collision with the threat aircraft.

4) as soon as possible, as permitted by flight crew workload, notify the appropriate ATC unit of any RA which requires a deviation from the current ATC instruction or clearance;

Note.— Unless informed by the pilot, ATC does not know when ACAS issues RAs. It is possible for ATC to issue instructions that are unknowingly contrary to ACAS RA indications. Therefore, it is important that ATC be notified when an ATC instruction or clearance is not being followed because it conflicts with an RA.

5) promptly comply with any modified RAs;

6) limit the alterations of the flight path to the minimum extent necessary to comply with the RAs;

7) promptly return to the terms of the ATC instruction or clearance when the conflict is resolved; and

8) notify ATC when returning to the current clearance.

Note.— Procedures in regard to ACAS-equipped aircraft and the phraseology to be used for the notification of manoeuvres in response to a resolution advisory are contained in the PANS-ATM (Doc 4444), Chapters 15 and 12 respectively.

H.2.2 Conformity Assessment Results

ICAO Provision	Safety Requirement									Remarks
	F1	F2	F3	F4	F5	F6	F7	F8	F9	
3.1.1	C	C	C	N/A	N/A	N/A	N/A	N/A	N/A	'shall be used' implies mandatory use of TAs and RAs. This seems to contradict 3.1.2.
3.1.2	NC	C	NC	NC	N/A	N/A	N/A	N/A	N/A	Terminology '*resolve a traffic conflict* or avert a *potential* collision' is different to terminology 'best avert collision' used in the corresponding provision in Annex 2 para 3.2.
3.1.2 Note 1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Reference to training, which is outside scope of conformity assessment.
3.1.2 Note 2	N/A	N/A	N/A	N/A	C	C	PC	N/A	N/A	Should this be a requirement rather than a Note? The statement only applies to the modes of operation in flight but does not say so explicitly. Consequently, it does not reflect the need for ACAS to be manually deactivated on the ground [1].
3.1.2 Note 3	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Reference to Training Guidelines, which are outside scope of conformity assessment.
3.2	C	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	The terminology 'in conformity with the following safety considerations:' is inappropriate because they are *required actions*, not safety considerations. The phrase should be replaced by 'as follows:'
3.2 a)	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	TA can trigger a non-ACAS means of detecting and resolving collision
3.2 a) Note 1	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Given the stated problems with visual acquisition, its utility following a TA is unclear. It could be intended to merely enhance situation awareness and not interfere with the progression from TA to RA, or it could be intended to lead to a Flight Crew-initiated collision avoidance action before the RA if they consider it the best course of action.
3.2 a) Note 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Explanation only.
3.2 b)	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Requirement implies that, for example, visual acquisition and ATC instructions/clearances shall be considered by the Flight Crew before the RA in deciding on how best to react when an RA occurs. Since the validity of the available information is not known and the nature and timing of the RA is also not known, it is unclear how an 'appropriate action', other than following the RA, can be formulated in advance.

ICAO Provision	Safety Requirement									Remarks
	F1	F2	F3	F4	F5	F6	F7	F8	F9	
										Requirement implies that Flight Crew could prepare themselves to ignore the RA.
3.2 c) 1)	N/A	C	C	N/A	N/A	N/A	N/A	N/A	N/A	It is assumed that the caveat can apply either as a consequence of 3.2b), because its 'appropriate action' might be to ignore the RA, or as a result of Flight Crew considering the implications of following the RA once it occurs. It is unclear whether the caveat is intended to encompass the requirement in 3.1.2, or is only dealing with the possibility of non-MAC events. In other words, if the RA is considered by pilot-in-command as not being the *best* course of action to avert collision, does this equate to the RA jeopardizing the safety of the aeroplane?
3.2 c) 1) Note 1	N/A	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	It is unclear whether this is an explanation of the technical prioritisation of multiple alerts from different equipments, or of how Flight Crew is expected to prioritise multiple alerts. If it is the former, and the Note has captured all relevant safety events, then the caveat in 3.2c)1) appears to be redundant because the RA will be automatically suppressed. If it is the latter, the Note should be formalised into a requirement.
3.2 c) 1) Note 2	N/A	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	The Note implies that, in addition to the safety events in 3.2c)1) Note 1, visual acquisition might be used by Flight Crew to determine that following the RA would jeopardize the safety of the aeroplane (or is not the best course of action). Given the stated problems with visual acquisition, and the potential for Flight Crew-initiated collision avoidance contradictory to ACAS, its use following an RA needs to be reconsidered.
3.2 c) 2)	N/A	C	C	N/A	N/A	N/A	N/A	C	N/A	An instruction to manoeuvre in the horizontal plane could never be in direct conflict with the RA since ACAS does not consider horizontal manoeuvres. The PANS-OPS requirement should be clarified to state the action to be taken when a) a horizontal manoeuvre has been initiated before the RA and b) an ATC horizontal manoeuvring instruction is received after the RA. In the latter case the most appropriate action would be to report the RA and inform ATC that the instruction cannot be complied with due to the RA.

ICAO Provision	Safety Requirement									Remarks
	F1	F2	F3	F4	F5	F6	F7	F8	F9	
3.2 c) 3)	N/A	C	C	N/A	N/A	N/A	N/A	C	N/A	Requirement is redundant in the presence of 3.2c)2).
3.2 c) 3) Note	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Explanation only.
3.2 c) 4)	N/A	N/A	N/A	PC	N/A	N/A	N/A	N/A	N/A	This provision differs from safety requirement SR_F4 which reads “As soon as possible, as permitted by workload, Flight Crew shall notify the Air Traffic Controller of the execution of an ACAS-initiated collision avoidance action except when it is believed that the action would not result in a deviation from a clearance or instruction” ‘any RA’ assumed to include modified RA(s) in the same encounter. If RA can modify in the future, is Flight Crew able to determine at the point of a maintain rate RA, whether it will ultimately ‘require’ a deviation from a level clearance? The formulation of SR_F4 deals with this situation better because the flight crew can report the RA by default. Maintain Rate RAs while flying on/to an *incorrect* clearance will not be notified to ATC. As noted under 3.2 c) 2), the current ATC instruction or clearance can include horizontal as well as vertical clearances. If the Flight Crew discontinues a turn manoeuvre in order to better deal with an RA, the requirement could be interpreted as meaning they must report the RA whether or not it produces a deviation from a vertical clearance. Is the requirement intended to address notifications in the reverse situation case in accordance with PANS-ATM 12.3.1.2 x)y)? Does the receipt and rejection of a new clearance or instruction that is contradictory to the current RA considered to be a ‘deviation from the *current* clearance/instruction’?
3.2 c) 4) Note	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Explanation only.
3.2 c) 5)	N/A	C	C	N/A	N/A	N/A	N/A	N/A	N/A	It is unclear whether ‘modified RAs’ are treated differently to ‘an RA’. In accordance with 3.2c), in a given encounter the initial

ICAO Provision	**Safety Requirement**									**Remarks**
	F1	**F2**	**F3**	**F4**	**F5**	**F6**	**F7**	**F8**	**F9**	
										and any subsequent RAs would all be subject to the same requirements.
3.2 c) 6)	N/A	N/A	C	N/A	N/A	N/A	N/A	N/A	N/A	
3.2 c) 7)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	C	Since 3.2 is specifically addressing *Use of ACAS Indications*, 'when the conflict is resolved' should be replaced by 'in response to Clear of Conflict indication'
3.2 c) 8)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	C	'returning to' should be replaced by 'returning to, and upon resumption of,'. 'clearance' should be replaced by 'clearance or instruction'.
3.2 c) 8) Note	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Explanation only. Use of the term 'manoeuvre' is inconsistent with 3.2 c) 4) since a clearance could be violated without manoeuvring. 'manoeuvres' should be replaced by 'actions'.

H.2.3 Conformity Assessment Conclusions

There are no Flight Crew Safety Requirements which have no corresponding ICAO provisions.

There are no ICAO Provisions, other than explanatory Notes, that have no corresponding Flight Crew Safety Requirements.

The following ICAO Provision represents non-compliance with some of the corresponding Flight Crew Safety Requirements:

- 3.1.2 Nothing in the procedures specified in 3.2, “Use of ACAS indicators”, shall prevent pilots-in-command from exercising their best judgement and full authority in the choice of the best course of action to resolve a traffic conflict or avert a potential collision

This non-compliance arises as a result of this mandatory Provision permitting Flight Crew not to comply with SR_F2 and SR_F8 under certain circumstances.

H.3 Conformity Assessment of Annex 2 [12]

H.3.1 Annex 2 Provisions

3.2 Avoidance of collisions

Nothing in these rules shall relieve the pilot-in-command of an aircraft from the responsibility of taking such action, including collision avoidance manoeuvres based on resolution advisories provided by ACAS equipment, as will best avert collision.

Note 1.— It is important that vigilance for the purpose of detecting potential collisions be exercised on board an aircraft, regardless of the type of flight or the class of airspace in which the aircraft is operating, and while operating on the movement area of an aerodrome.

Note 2.— Operating procedures for use of ACAS detailing the responsibilities of the pilot-in-command are contained in PANS-OPS (Doc 8168), Volume I, Part VIII, Chapter 3.

Note 3.— Carriage requirements for ACAS equipment are addressed in Annex 6, Part I, Chapter 6 and Part II, Chapter 6.

ATTACHMENT A. INTERCEPTION OF CIVIL AIRCRAFT

3. Interception manoeuvres

3.2 An aircraft equipped with an airborne collision avoidance system (ACAS), which is being intercepted, may perceive the interceptor as a collision threat and thus initiate an avoidance manoeuvre in response to an ACAS resolution advisory. Such a manoeuvre might be misinterpreted by the interceptor as an indication of unfriendly intentions. It is important, therefore, that pilots of intercepting aircraft equipped with a secondary surveillance radar (SSR) transponder suppress the transmission of pressure-altitude information (in Mode C replies or in the AC field of Mode S replies) within a range of at least 37 km (20 NM) of the aircraft being intercepted. This prevents the ACAS in the intercepted aircraft from using resolution advisories in respect of the interceptor, while the ACAS traffic advisory information will remain available.

H.3.2 Conformity Assessment Results

ICAO Provision	Safety Requirement									Remarks
	F1	F2	F3	F4	F5	F6	F7	F8	F9	
3.2	N/A	NC	N/A	N/A	N/A	N/A	N/A	NC	N/A	'collision avoidance manoeuvres' should be changed to 'actions' since an RA might not involve a manoeuvre. 'based on' should be changed to 'in response to' to be consistent with PANS-OPS. Requirement means that pilot-in-command is: permitted to perform collision avoidance in response to TAs; permitted to respond to RAs which contravene right-of-way rules; and *required* to ignore or fly in contradiction to RAs if other indications of potential collision (MAC or non-MAC) exist.
3.2 Note 1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Note is emphasising an aspect of See & Avoid if 'vigilance' is intended to be mean visual perception only.
3.2 Note 2	See PANS-OPS 3.1.2 in H.2.2	See PANS-OPS 3.1.2 in H.2.2	See PANS-OPS 3.1.2 in H.2.2	See PANS-OPS 3.1.2 in H.2.2	See PANS-OPS 3.1.2 in H.2.2	See PANS-OPS 3.1.2 in H.2.2	See PANS-OPS 3.1.2 in H.2.2	See PANS-OPS 3.1.2 in H.2.2	See PANS-OPS 3.1.2 in H.2.2	'Part VIII' should be replaced by 'Part III'. Only PANS-OPS requirement 3.1.2 refers to the term 'pilot-in-command'.
3.2 Note 3	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Cross-reference to Annex 6, which is outside scope of conformity assessment.
Attch A 3.2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Military interception is outside scope of Safety Case.

H.3.3 Conformity Assessment Conclusions

Most of the Flight Crew Safety Requirements have no corresponding ICAO provisions in Annex 2 because the Annex it is not intended to address ACAS-specific actions.

There are no ICAO Provisions, other than explanatory Notes or matters that fall outside the scope of the conformity assessment, that have no corresponding Flight Crew Safety Requirements.

The following ICAO Provision represents non-compliance with the Flight Crew Safety Requirements SR_F2 and SR_F8:

- 3.2 Nothing in these rules shall relieve the pilot-in-command of an aircraft from the responsibility of taking such action, including collision avoidance manoeuvres based on resolution advisories provided by ACAS equipment, as will best avert collision.

This non-compliance arises as a result of the provision being contradictory to PANS-OPS requirement 3.2c)1) on Flight Crew action in the presence of an RA. This stipulates that Flight Crew shall follow the RA unless to do so would jeopardize the safety of the aircraft. The Annex 2 provision on the other hand implies that if the Flight Crew has access to superior information with respect to collision avoidance than provided by ACAS, this shall be acted upon even if following the RA would *not* jeopardize the safety of the aircraft.

H.4 Conformity Assessment of PANS-ATM [5][7]

H.4.1 PANS-ATM Provisions

12.3.1.2 LEVEL CHANGES, REPORTS AND RATES

… after a flight crew starts to deviate from any ATC clearance or instruction to comply with an ACAS resolution advisory (RA) (Pilot and controller interchange)	*r) TCAS RA;
	s) ROGER;

… after the response to an ACAS RA is completed and a return to the ATC clearance or instruction is initiated (Pilot and controller interchange)	*t) CLEAR OF CONFLICT, RETURNING TO (*assigned clearance*);
	u) ROGER (*or alternative instructions*);

... after the response to an ACAS RA is completed and the assigned ATC clearance or instruction has been resumed (Pilot and controller interchange)	*v) CLEAR OF CONFLICT (*assigned clearance*) RESUMED;
	w) ROGER (*or alternative instructions*);

... after an ATC clearance or instruction contradictory to the ACAS RA is received, the flight crew will follow the RA and inform ATC directly (Pilot and controller interchange)	*x) UNABLE, TCAS RA; y) ROGER. * Denotes pilot transmission.

15.7.3 Procedures in regard to aircraft equipped with airborne collision avoidance systems (ACAS)

15.7.3.1 The procedures to be applied for the provision of air traffic services to aircraft equipped with ACAS shall be identical to those applicable to non-ACAS equipped aircraft. In particular, the prevention of collisions, the establishment of appropriate separation and the information which might be provided in relation to conflicting traffic and to possible avoiding action shall conform with the normal ATS procedures and shall exclude consideration of aircraft capabilities dependent on ACAS equipment.

15.7.3.2 When a pilot reports an ACAS resolution advisory (RA), the controller shall not attempt to modify the aircraft flight path until the pilot reports “Clear of Conflict”.

15.7.3.3 Once an aircraft departs from its ATC clearance or instruction in compliance with an RA, or a pilot reports an RA, the controller ceases to be responsible for providing separation between that aircraft and any other aircraft affected as a direct consequence of the manoeuvre induced by the RA. The controller shall resume responsibility for providing separation for all the affected aircraft when:

a) the controller acknowledges a report from the flight crew that the aircraft has resumed the current clearance; or

b) the controller acknowledges a report from the flight crew that the aircraft is resuming the current clearance and issues an alternative clearance which is acknowledged by the flight crew.

Note.— Pilots are required to report RAs which require a deviation from the current ATC clearance or instruction (see PANS-OPS, Volume I, Part III, Section 3, Chapter 3, 3.2 c) 4)). This report informs the controller that a deviation from clearance or instruction is taking place in response to an ACAS RA.

15.7.3.4 Guidance on training of air traffic controllers in the application of ACAS events is contained in the *ACAS Manual* (Doc 9863).

15.7.3.5 ACAS can have a significant effect on ATC. Therefore, the performance of ACAS in the ATC environment should be monitored.

15.7.3.6 Following a significant ACAS event, pilots and controllers should complete an air traffic incident report.

Note 1.— The ACAS capability of an aircraft may not be known to air traffic controllers.

Note 2.— Operating procedures for use of ACAS are contained in PANS-OPS (Doc 8168), Volume I, Part III, Section 3, Chapter 3.

Note 3.— The phraseology to be used by controllers and pilots is contained in Chapter 12, 12.3.1.2.

H.4.2 Conformity Assessment Results

ICAO Provision	Safety Requirement		Remarks
	F4	C1	
12.3.1.2 r)	C	N/A	Notification doesn't convey intent. 'starts to deviate…to comply with' means that Flight Crew don't need to report an RA that they don't intend to follow. Under these circumstances, the controller maintains responsibility for separation in accordance with 15.7.3.3. If RA can modify in the future, is Flight Crew able to determine at the point of a maintain rate RA, whether it will ultimately 'require' a deviation from a level clearance? In turn, does it imply that the notification can take place sometime after the onset of the RA? The terminology with respect to clearances/instructions is inconsistent throughout 12.3.1.2. 'any ATC' should be changed to 'the assigned ATC'.
12.3.1.2 s)	N/A	C	
12.3.1.2 t)	C	N/A	The terminology with respect to clearances/instructions is inconsistent throughout 12.3.1.2. 'the ATC' should be changed to 'the assigned ATC'. '(assigned clearance)' should be changed to '(assigned clearance or instruction)'.

ICAO Provision	Safety Requirement		Remarks
	F4	C1	
			‘(alternative instructions)’ should be changed to ‘(alternative clearance or instructions)’.
12.3.1.2 u)	N/A	C	
12.3.1.2 v)	C	N/A	The terminology with respect to clearances/instructions is inconsistent throughout 12.3.1.2. ‘(assigned clearance)’ should be changed to ‘(assigned clearance or instruction)’. ‘(alternative instructions)’ should be changed to ‘(alternative clearance or instructions)’. The meaning of assigned clearance/instruction is ambiguous. If an ATC clearance or instruction contradictory to the RA is received (in accordance with 12.3.1.2 x)y), does this supersede the pre-RA clearance/instruction as the assigned clearance/instruction? The phrase ‘assigned …has been *resumed’* could be ambiguous in the case where an alternative clearance issued in accordance with 12.3.1.2 u). In this case, the Flight Crew might report ‘CoC, RESUMED’ even though the requirement 12.3.1.2 v)w) is intended not to apply.
12.3.1.2 w)	N/A	C	
12.3.1.2 x)	C	N/A	Recommend moving this phraseology after 12.3.1.2 r)s) to better reflect the order of events. Procedural requirements should not appear within the circumstances part of phraseology requirements. ‘will follow the RA and inform ATC directly’ should be addressed in PANS-OPS only. If the duration/modification of an RA is unknown as the RA progresses, is Flight Crew able to determine at the point of receiving a new level clearance/instruction whether it will ultimately become contradictory to a maintain rate RA? In turn, does it imply that the notification can take place sometime after the clearance/instruction itself? It’s unclear whether these circumstances equate to 15.7.3.2 or 15.7.3.3. If the ongoing RA has not required a deviation from clearance/instruction, Flight Crew will not have notified ATC and controller retains responsibility for Separation Provision. When a contradictory clearance/instruction is received subsequently, and the Flight Crew notify ATC, it is assumed that this equates to 15.7.3.2 (pilot reports an RA) and the controller must issue no further clearances/instructions. The contradictory clearance/instruction however will not be read-back by the Flight Crew so, unlike 12.3.1.2 r) it is not a deviation from a clearance/instruction in force. Therefore, 15.7.3.3 applies only on the basis that ‘UNABLE, TCAS RA’ equates to the pilot reporting the RA, and not a deviation. At this point, the controller ceases to be responsible for separation. The case of clearance/instruction not contradictory to the RA is not addressed. The implication is that

ICAO Provision	Safety Requirement		Remarks
	F4	C1	
			ATC do not need to be made aware of the RA (this is consistent with PANS-OPS philosophy of only reporting inconsistencies between clearances/instructions and RAs), Flight Crew can and shall acknowledge such clearances/instructions as normal, and ATC retains responsibility for Separation Provision.
12.3.1.2 y)	N/A	C	
15.7.3.1	N/A	N/A	
15.7.3.2	N/A	C	Controller is at liberty to provide traffic (and other) information during a reported collision avoidance action. Controller will continue to provide clearances/instructions during non-reported collision avoidance action.
15.7.3.3	N/A	C	Requirement uses ‘departs from’ whereas 12.3.1.2 uses ‘starts to deviate from’. The terminology should be identical. When there’s an RA that doesn’t induce a deviation from clearance/instruction, the controller retains responsibility for separation but ACAS is concurrently assisting the Flight Crew in collision avoidance. Since the Flight Crew is required to follow the RA *exclusively*, even if it’s consistent with clearance/instruction, what is the purpose of placing such a responsibility on the controller? Controller will be unaware of cessation of responsibility unless the Flight Crew reports the RA. Hence, the responsibility might cease without the controller being aware of it. The controller might subsequently issue clearance/instruction to RA-incident aircraft if it departs from current clearance/instruction, even though responsibility has ceased. Responsibility will then cease upon receiving ‘UNABLE, TCAS RA’. Is the cessation of responsibility irrelevant in light of 15.7.3.2, unless the demarcation is required for legal reasons? Similarly, is the ‘or’ condition redundant because the controller will receive an ‘UNABLE, TCAS RA’ as soon as the RA produces an inconsistency with the clearance/instruction, and this is the point at which separation provision should be suspended? If Flight Crew doesn’t follow the RA, the controller maintains responsibility for separation. For an RA which does not require a deviation from clearance/instruction, the controller is at liberty to issue further clearances/instructions. If these are confined to the horizontal plane, the Flight Crew is required to acknowledge and follow them in parallel with reacting to the vertical RA(s). Is this considered practicable for the Flight Crew? ‘any other aircraft affected as a direct consequence’ is ambiguous. The presence of such a clause

ICAO Provision	Safety Requirement		Remarks
	F4	C1	
			implies that the intruder aircraft could be considered to be affected as a direct consequence of the 'own' aircraft departure from clearance/instruction. It is unclear what the criteria would be for 'affected' since both aircraft are involved in resolving the collision, whether by active or passive means. A further implication is that whereas the controller ceases to be *responsible* for separation provision, 15.7.3.2 does not prohibit the issuance of clearances/instructions to a directly affected non-reporting aircraft, including non-ACAS equipped aircraft, after an RA is reported from the other aircraft. This seems to be inconsistent. 'or a pilot reports an RA' should be replaced by 'or the controller acknowledges an RA notification from the pilot' to be consistent with 15.7.3.3a). The term 'direct consequence' is assumed to imply that consequential effects on 3rd party aircraft are excluded from the requirement. 'manoeuvre' should be replaced by 'departure from clearance or instruction' since a departure might happen without manoeuvring.
15.7.3.3 a)	N/A	C	Recommend reversing the order of 15.7.3.3 a) and b) to align requirements with 12.3.1.2 t)u) and v)w) The requirement is incomplete with respect to 12.3.1.2 v)w) which says the controller can acknowledge *or* issue an alternative clearance/instruction (which would have to be acknowledged by Flight Crew). Requirement uses '*current* clearance' whereas 12.3.1.2 v)w) uses '*assigned* ATC clearance *or instruction*'. The terminology should be identical.
15.7.3.3 b)	N/A	C	Recommend reversing the order of 15.7.3.3 a) and b) to align requirements with 12.3.1.2 t)u) and v)w) The requirement is inconsistent with respect to 12.3.1.2 t)u) which implies that the controller cannot acknowledge *and* issue alternative instructions. 'acknowledges a report' should be replaced by 'receives a report'. Requirement uses '*current* clearance' whereas 12.3.1.2 t)u) uses '*the ATC* clearance *or instruction*'. The terminology should be identical.
15.7.3.3 b) Note	C	N/A	Explanation only. 'which require' means Flight Crew must notify ATC even if they intend **not** to follow RA. Recommend changing to 'are producing'.

ICAO Provision	Safety Requirement		Remarks
	F4	C1	
15.7.3.4	N/A	N/A	Reference to Training guidance, which is outside scope of conformity assessment. This should be a Note rather than a requirement. ‘application’ should be replaced by ‘management’.
15.7.3.5	N/A	N/A	Not an ATS procedure as such, hence outside scope of conformity assessment.
15.7.3.6	N/A	N/A	Not related to ACAS Safety Requirements, hence outside scope of conformity assessment. The term ‘significant’ implies that it’s a reported RA because the controller is required to file an ATIR. In turn, this means that any RA that doesn’t require a deviation from clearance/instruction will not be the reported via an ATIR. How will ACAS performance statistics be compiled and monitored?
15.7.3.6 Note 1	N/A	N/A	Explanation only.
15.7.3.6 Note 2	N/A	N/A	Cross-reference only.
15.7.3.6 Note 3	N/A	N/A	Cross-reference only.

H.4.3 Conformity Assessment Conclusions

The following Controller Safety Requirements have no corresponding ICAO provisions:

- SR_C2 Separation Provision shall be independent from ACAS so far as is reasonably practicable.
- SR_C3 ATM Separation Recovery shall be independent from ACAS so far as is reasonably practicable.

The following ICAO Provision that falls within the scope of the conformity assessment has no corresponding Controller Safety Requirement:

- 15.7.3.1 The procedures to be applied for the provision of air traffic services to aircraft equipped with ACAS shall be identical to those applicable to non-ACAS equipped aircraft. In particular, the prevention of collisions, the establishment of appropriate separation and the information which might be provided in relation to conflicting traffic and to possible avoiding action shall conform with the normal ATS procedures and shall exclude consideration of aircraft capabilities dependent on ACAS equipment.

The context **(C001)** of the Safety Claim is related to aircraft operations in ECAC airspace. The characteristics of this environment of operations are captured by the Encounter Model used in ACAS modelling studies. Hence, the Safety Case is not directly dependent upon the quality of ATS that underpins this environment and no Safety Requirement on the continuation of normal ATS is therefore needed.

APPENDIX I ACCIDENTS WITH ACAS INVOLVEMENT

This appendix discusses four accidents with ACAS involvement, in Japan in 2001, over southern Germany in 2002, in Korean airspace in 2006 and in Brazil in 2006. The second and fourth accidents are well known since they resulted in a mid-air collision with multiple fatalities. The others are less well known; although one resulted in a very close approach between the involved aircraft, with structural damage and serious injuries to persons on board, both aircraft were able to make a safe landing and there were no fatalities.

This appendix presents a short summary of the accident sequences showing how and why ACAS as a "socio-technical system" did not prevent the accidents (despite the fact that the technical functioning of the ACAS *equipment* was correct) and linking the accident to the failure modes/hazards, mitigations and safety issues identified in this Safety Case Report.

I.1 Yaizu Accident, 31 January 2001

On this occasion, a conflict occurred between two Japan Airlines (JAL) aircraft, a Boeing 747 climbing outbound from Tokyo to Okinawa, and a DC-10 inbound to Tokyo from South Korea over Suruga Bay near the city of Yaizu (south-west of Tokyo) [51]. In response to a STCA alert, the air traffic controller instructed the 747 to descend about 3 seconds before TCAS RAs were issued in both aircraft. The TCAS equipment on board functioned in accordance with its specification[67], giving a climb RA to the descending 747, and a descend RA to the DC-10. The DC-10 flight crew obeyed the descend RA but the 747 crew continued the descent in contradiction to the climb RA, an occurrence of either hazard cause **CF_10** (*Flight crew doesn't notice RA*) or **CF_11** (*Flight crew performs no or inadequate manoeuvre*), see Appendix G. Neither flight crew reported the RAs, a failure to conform to **SR_F4**. Two successive heading instructions issued by ATC to the DC-10, presumably for avoidance, were not obeyed. Arguably this was conformance to **SR_F2** which requires the RA to be followed rather than the controller's instruction.

The flight crew of the 747 had been in visual contact with the DC-10 for some time, possibly in response to a TCAS TA at a distance of around 13 nm (in this case, it appears the flight crew of the 747 did not conform to Safety Requirements **SR_F1** and **SR_F2**, in neither preparing themselves for a subsequent RA nor obeying the RA).

The aircraft passed with approximately zero horizontal separation and a vertical separation estimated at about 25m, the 747 passing below the DC-10. Injuries to occupants of the 747 and damage to the cabin interior appear to have resulted from negative G arising from a last-second dive by the 747. Without this violent manoeuvre, a mid-air collision would almost certainly have occurred. The DC-10 also began to reduce its descent rate immediately before the accident.

The precursors to the RAs appear to have been concentration by the controller on other traffic, and callsign confusion between the two JAL aircraft on the part of the controller.

The accident investigation report [51] recommended the introduction of RA Downlink.

[67] Both aircraft were fitted with TCAS V6.04a - however, the incident would have occurred in the same way had they been fitted with V7.0.

I.2 Überlingen Accident, 2 July 2002

A Boeing 757 (B757) cargo aircraft flying north in the cruise at FL 350 requested FL 360, and was incorrectly cleared to climb to this level [50]. This created a crossing conflict with a Tupolev TU154 passenger aircraft flying on an approximately westerly track at the same flight level. For various reasons, the Controller in the Zürich centre did not observe this conflict for some time. When the Controller finally noticed the conflict, he instructed the TU154 aircraft to descend to FL 350 thus "*BTC 2937…descend flight level…350, expedite, I have crossing traffic*". Seven seconds after the start of this instruction, the TCAS systems on both aircraft issued RAs. The B757 received a descend RA and the TU154 a climb RA (ie opposite to the Controller instruction). The B757 flight crew promptly obeyed their RA while the TU154 flight crew, after a short discussion, chose to obey the Controller's instruction. The B757 flight crew reported their RA (badly) 23 seconds after the RA was issued, and 16 seconds after the Controller had issued a second instruction to the TU154 to expedite descent. The TU154 flight crew did not report the RA but did acknowledge the Controller's second descent instruction, in response to which the Controller confirmed that "… *we have traffic at your 2 o'clock position, now at [flight level] 360*". Both aircraft continued to descend and collided. Around 20 seconds before the collision, the B757 TCAS issued a *TCAS increase descent* RA and at 8 seconds the TU154 TCAS issued a *TCAS increase climb* RA. At no stage during the sequence did TCAS generate a reversal command to either aircraft.

During the period between the RA and the collision, the TU154 made a right turn of 10° from 264° to 274° magnetic; this is not discussed in the accident report but followed the disengagement of the autopilot. If the TU154 had maintained its original course it would have passed behind the B757; this illustrates the point made in section 8.2 that the great majority of RAs are issued when a collision will not in fact result from the encounter.

In this case, the TU154 crew failed to conform to Safety Requirement **SR-F2** and thus created hazard cause **C-F5** (*Flight Crew prioritises ATC instruction/clearance over RA*), as listed in Appendix G. This corresponds to event HPRX in the ACAS accident-causation model in Appendix F. In not reporting the RA, they also failed to conform to **SR-F4**. However, this does not mean that they contravened PANS-OPS (Doc 8168), Part VIII, Chapter 3 regarding either reaction to[68], or reporting of[69], the RA since those provisions do not conform exactly to **SR-F2** and **SR-F4** see safety issue Iss-005 in section 10.2.

The Controller did not fail to adhere to safety requirement SR_C1, since he was unaware of the RAs when he issued the two descent instruction to the TU154 aircraft.

In this case, had TCAS not been fitted to the involved aircraft, the accident would not have occurred. The accident report [50] notes that had modification CP 112E (see section 8.3) been fitted to the TCAS II equipment on board, a reversal RA would have been generated for the B757 and, provided that the flight crew had obeyed the reversal, the accident would have been avoided.

[68] Safety Recommendation No. 18/2002 of the Überlingen accident report [51][50] recommends that "ICAO should change the international requirements in Annex 2, Annex 6 and PANS-OPS (DOC 8168) so that pilots flying are required to obey and follow TCAS resolution advisories (RAs), regardless of whether contrary ATC instruction is given prior to, during, or after the RAs are issued. Unless the situation is too dangerous to comply, the pilot flying should comply with the RA until TCAS indicates the airplane is clear of the conflict.

[69] Although it would probably have had no bearing on the accident, it is noted that the reporting requirements in PANS-OPS in 2002 were different than those today (2010) - in 2002 all RAs were reportable whereas today only those resulting in a departure from ATC clearance are reportable.

The EUROCONTROL RA Downlink project was initiated as a result of this accident, with the possibility of providing controllers with automated information about RAs in progress. RA Downlink is discussed in section 2.3.8.

I.3 Jeju Island Korea Accident, 16 November 2006

On this occasion, a conflict occurred between a Boeing 757 and a Boeing 777 aircraft, causing coordinated climb and descend TCAS RAs on board both aircraft [54]. The flight crew of the 757 aircraft reacted to the descend RA with an excessive control input in pitch, causing a maximum acceleration of -1G (negative G) for a few seconds and a maximum descent rate of 12,000 ft/min. This was followed by an opposite stick input, to reduce the excessive descent rate, causing a maxima acceleration of +2.5 G and a pitch change from 4.4 deg nose down to 17.8 deg nose up in just 7 seconds. This corresponds to event C-F1 in the Accident-Causation model and the manoeuvre was therefore in contradiction to safety requirement **SR-F3**. The negative G caused several unsecured passengers in the B757 to collide with the cabin roof and a cabin service trolley to fall upon other passengers. The result of this accident was twenty-one occupants injured (four serious injuries and seventeen light injuries) and minor damage to cabin fittings (including seats). The B757 had to divert to a nearby airport to seek medical assistance for the injured.

The flight crew of the B757 aircraft reported the RA (although with the wrong sense) but no RA report was received from the B777; however both aircraft followed the RA rather than the instructions of the Controller. In this case, the Controller had observed the situation and attempted to increase separation between the aircraft by issuing a heading instruction to one of the involved aircraft – contrary to **SR-C1**. However both flight crews followed the RA rather than the instructions of the Controller.

I.4 Brazil Mid-air Collision, 29 September 2006

On 29 September 2006 a mid-air collision between an Embraer Legacy business jet and a Boeing 737 passenger jet occurred over the Brazilian state of Mato Grosso. All 154 passengers and crew aboard the Boeing 737 were killed when the aircraft broke up in midair, while the Embraer Legacy, despite sustaining serious damage to its left wing and tail, landed safely with its seven occupants uninjured. Both aircraft were equipped with TCAS II version 7.0.

Following several problems related to ATC and air-ground communications, both aircraft were flying on reciprocal tracks at the same flight level (FL370), while ATC expected the Legacy to be at FL360 or FL380.

Moreover, the Legacy's transponder was inadvertently set to "Standby" (ie it was no longer operating), contrary to the rules for RVSM airspace. Consequently:

(1) ATC lost SSR radar contact with the aircraft (including Mode C information), and the current (different from expected) flight level was not seen by the controllers;

(2) the TCAS II system on board the Legacy became inoperative (TCAS II will not operate when own transponder is not functioning);

(3) the Legacy could not be detected by the TCAS II on the Boeing 737.

There appears to have been some disagreement in the conclusions between the official report by the Brazilian authorities [59] and a separate report by the US National Transportation Safety Board (NTSB), concerning allocation of blame. However, what was not in dispute was the fact that, given the situation that the two aircraft were (incorrectly) cleared on reciprocal tracks at the same flight level, the accident would most likely have been avoided if the Legacy’s transponder had been functioning correctly, since either:

- ATC would have been made aware that the two aircraft were at the same FL (and not separated by one flight level as was believed to be the case in the absence of height information prior to the accident) and would have intervened to apply the correct vertical separation; or, failing that
- TCAS would have issued an RA, enabling the pilots to take coordinated action to avoid the collision.

This is a classic common-cause ‘failure’ and illustrates the problem of lack of full independence between ACAS and the rest of the ATM system, as noted in sections 4.4 and 6.6.6 above.

APPENDIX J FUNCTIONAL-TO-LOGICAL MODEL TRACEABILITY

This appendix provides a table summarizing the traceability of the elements of the Functional Model given in section 2.2 to the Logical Model in section 2.3. This table supports the claim that the Logical Model is correctly derived from the Fundamentals. It also comments on the additional elements introduced into the Logical Model. In this table, “ACAS” represents the ACAS equipment on board the aircraft.

Functional Model Element	**Logical Model Element(s)**	**Remarks**
Relative position calculation	ACAS ACAS surveillance (data flow)	
Collision detection	ACAS	
Collision avoidance	ACAS Alerts (data flow) Flight Crew Control inputs (data flow) Airframe and Systems	On one or both involved aircraft, depending on the encounter geometry and ACAS algorithms
Movement	Airframe and Systems Movement	
Coordination	ACAS	
Involved Aircraft 1	Involved Aircraft 1	
Involved Aircraft 2	Involved Aircraft 2	
Non-involved aircraft	Not in FM, but in Fundamentals description	ACAS must be aware of other aircraft to avoid creating new conflict hazards. Algorithms can deal with some cases of multiple aircraft encounters.
Air traffic controller	-	Introduced to support analysis of interactions between ACAS overall system and ATC
Weather, turbulence, terrain	-	Sources of hazards which may have to be prioritized over collision avoidance (see section 2.2.5 in Fundamentals) or may make collision avoidance movement either difficult or impossible
Occupants	-	Included to indicate the subjects at risk

APPENDIX K SAFETY ISSUES THAT HAVE BEEN RESOLVED

This appendix gives details of the Safety Issues that were raised during the development of the APOSC but which were resolved prior to the release of the current version.

Reference	Safety Issue	Resolution	Source
ISS-006	The discrepancy between the number of RAs per flight hour as stated in the STCA/ACAS Interaction Workshop report [57] and the number reported in reference [53] should be resolved	The following response was received by email on 22 July 2010 from Dr Ken Carpenter - the author of the figures in [57]: “I suggest that this [APOSC section 8.2] line of reasoning takes a throw-away remark by [me] too seriously. [My] point was simply that TCAS does not detect a risk of collision at any reasonable level. Rather, it uses the limited amount of information - all that is available - to calculate the time to collision and alerts when it is essential to do so because the warning time is short. In order to make this calculation it assumes that there will be a collision. This being the case, its false alert rate, using that term in the usual engineering sense, is extremely high. (Shorter warning times would increase the probability that the aircraft are on collision course. However, waiting until that probability reaches some threshold closer to normal engineering aspiration would leave insufficient time to take avoiding action.) Furthermore, [I] did not use the PASS figures for the rate of RAs. [I] remarked … that the PASS figures indicate a lower rate of RAs than does other field evidence. [I] would also agree that it is possible that [I] used an overoptimistic figure for the rate of collisions. In summary, using the PASS rate of RAs, [I] would have no difficulty whatsoever accepting 1 in 10^5 in place of 1 in 10^6 as the ratio between RAs and collisions. [I] suggest that the most reliable way to make the calculation [the APOSC is] attempting is to examine the worldwide rate of mid air collisions. It would be best to use the worldwide rate rather than the rate in Europe because the numbers are small making inferences for regions unreliable. Every study that has quantified the efficacy of TCAS has found that it prevents most collisions that would otherwise occur. Precisely what proportion of collisions are prevented depends on many assumptions, but [I] would advise that an assumption that it prevents 70% of the collisions that would otherwise occur is probably conservative (ie TCAS probably prevents more than 70% of the collisions that would otherwise occur). The rate of prevented collisions is then at least 70% of the observed worldwide rate of collisions. However, using the observed rate of actual collisions underestimates the number avoided because it does not include very many collisions that have been prevented by TCAS, many of which probably pass completely unrecorded.	8.2

		Were we to assume that the observed rate of collisions fully reflects the effect of TCAS, then the inferred rate of prevented collisions would be 233% of the observed worldwide rate of collisions. This figure, 233% (=100x70/30), is an underestimate (because 70% is an under-estimate), but the observed rate of collisions almost certainly does not fully reflect the effect of TCAS simply because, for most of the record, it was not fitted."	

APPENDIX L THE ICAO ACAS PROVISIONS - SUMMARY

The following information on the ICAO ACAS Provisions was obtained from the EUROCONTROL website. For further details see:
http://www.eurocontrol.int/msa/public/standard_page/ACAS_ICAO_Provisions.html

The International Civil Aviation Organization (ICAO) is responsible for the global standardisation of ACAS. ACAS Standards and Recommended Practices (SARPs) and procedures are contained in:

- **ICAO Annex 10, Vol. IV**
- **PANS-OPS(Doc. 8168)**
- **PANS-ATM (Doc. 4444)**

This information is supplemented by the **ACAS Manual (Doc. 9863)**, which includes a detailed description of ACAS and associated technical and operational issues in order to facilitate correct operation, operational monitoring as well as training of personnel.

Additionally, the Regional and Supplementary Procedures document (**ICAO Doc. 7030/4**) and **ICAO Annex 6** specify the ACAS II equipage requirements.

Extracts from these documents are provided below.

ICAO Annex 10, Vol. IV - Aeronautical Telecommunications - Surveillance and Collision Avoidance Systems

Definitions:

Airborne collision avoidance system (ACAS)	An aircraft system based on secondary surveillance radar (SSR) transponder signals which operates independently of ground-based equipment to provide advice to the pilot on potential conflicting aircraft that are equipped with SSR transponders. *[Note: SSR transponders referred to above are those operating in Mode C or Mode S}*.
Collision avoidance logic	The sub-system or part of ACAS that analyses data relating to an intruder and own aircraft, decides whether or not advisories are appropriate and, if so, generates the advisories. It includes the following functions: range and altitude tracking, threat detection and RA generation. It excludes surveillance.
Resolution advisory (RA)	An indication given to the flight crew recommending: a) a manoeuvre intended to provide separation from all threats; or b) a manoeuvre restriction intended to maintain existing separation
Corrective RA	A resolution advisory that advises the pilot to deviate from the current flight path.

Preventive RA	A resolution advisory that advises the pilot to avoid certain deviations from the current flight path but does not require any change in the current flight path.
Traffic advisory (TA)	An indication given to the flight crew that a certain intruder is a potential threat.

Contrary Pilot Response

3.5.8.10.3 Manoeuvres opposite to the sense of an RA may result in a reduction in vertical separation with the threat aircraft and therefore must be avoided. This is particularly true in the case of an ACAS-ACAS coordinated encounter.

PANS-OPS (Procedures for Air Navigation Services - Aircraft Operations - Volume I Flight Procedures - ICAO Doc. 8168 OPS/611), Fifth edition – 2006 plus Amendment 3

Chapter 3

3.1 ACAS OVERVIEW

3.1.1 The information provided by an ACAS is intended to assist pilots in the safe operation of aircraft by providing advice on appropriate action to reduce the risk of collision. This is achieved through resolution advisories (RAs), which propose manoeuvres, and through traffic advisories (TAs), which are intended to prompt visual acquisition and to act as a warning that an RA may follow. TAs indicate the approximate positions of intruding aircraft that may later cause resolution advisories. RAs propose vertical manoeuvres that are predicted to increase or maintain separation from threatening aircraft. ACAS I equipment is only capable of providing TAs, while ACAS II is capable of providing both TAs and RAs. In this chapter, reference to ACAS means ACAS II.
3.1.2 ACAS indications shall be used by pilots in the avoidance of potential collisions, the enhancement of situational awareness, and the active search for, and visual acquisition of, conflicting traffic.

3.1.3 Nothing in the procedures specified in 3.2 hereunder shall prevent pilots-in-command from exercising their best judgement and full authority in the choice of the best course of action to resolve a traffic conflict or avert a potential collision.

Note 1 - The ability of ACAS to fulfil its role of assisting pilots in the avoidance of potential collisions is dependent on the correct and timely response by pilots to ACAS indications. Operational experience has shown that the correct response by pilots is dependent on the effectiveness of the initial and recurrent training in ACAS procedures.

Note 2 - The normal operating mode of ACAS is TA/RA. The TA-only mode of operation is used in certain aircraft performance limiting conditions caused by in-flight failures or as otherwise promulgated by the appropriate authority.

Note 3 - ACAS Training Guidelines for Pilots are provided in the Attachment, “ACAS Training Guidelines for Pilots”.

3.2 USE OF ACAS INDICATORS

The indications generated by ACAS shall be used by pilots in conformity with the following safety considerations:

a) pilots shall not manoeuvre their aircraft in response to traffic advisories (TAs) only;

Note 1 - TAs are intended to alert pilots to the possibility of a resolution advisory (RA), to enhance situational awareness, and to assist in visual acquisition of conflicting traffic. However, visually acquired traffic may not be the same traffic causing a TA. Visual perception of an encounter may be misleading, particularly at night.

Note 2 - The above restriction in the use of TAs is due to the limited bearing accuracy and to the difficulty in interpreting altitude rate from displayed traffic information.

b) on receipt of a TA, pilots shall use all available information to prepare for appropriate action if an RA occurs; and

c) in the event of an RA, pilots shall:

1) respond immediately by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane;

Note 1 - Stall warning, wind shear, and ground proximity warning system alerts have precedence over ACAS.

Note 2 - Visually acquired traffic may not be the same traffic causing an RA. Visual perception of an encounter may be misleading, particularly at night.

2) follow the RA even if there is a conflict between the RA and an air traffic control (ATC) instruction to manoeuvre;

3) not manoeuvre in the opposite sense to an RA;

Note - In the case of an ACAS-ACAS coordinated encounter, the RAs complement each other in order to reduce the potential for collision. Manoeuvres, or lack of manoeuvres, that result in vertical rates opposite to the sense of an RA could result in a collision with the threat aircraft.

4) as soon as possible, as permitted by flight crew workload, notify the appropriate ATC unit of any RA which requires a deviation from the current ATC instruction or clearance;

Note - Unless informed by the pilot, ATC does not know when ACAS issues RAs. It is possible for ATC to issue instructions that are unknowingly contrary to ACAS RA indications. Therefore, it is important that ATC be notified when an ATC instruction or clearance is not being followed because it conflicts with an RA.

5) promptly comply with any modified RAs;

6) limit the alterations of the flight path to the minimum extent necessary to comply with the RAs;

7) promptly return to the terms of the ATC instruction or clearance when the conflict is resolved; and

8) notify ATC when returning to the current clearance.

Note - Procedures in regard to ACAS-equipped aircraft and the phraseology to be used for the notification of manoeuvres in response to a resolution advisory are *contained in the PANS-ATM (Doc 4444), Chapters 15 and 12 respectively.*

3.3 HIGH VERTICAL RATE (HVR) ENCOUNTERS

Pilots should use appropriate procedures by which an aeroplane climbing or descending to an assigned altitude or flight level, especially with an autopilot engaged, may do so at a rate less than 8 m/s (or 1 500 ft/min) throughout the last 300 m (or 1 000 ft) of climb or descent to the assigned altitude or flight level when the pilot is made aware of another aircraft at or approaching an adjacent altitude or flight level, unless otherwise instructed by ATC. These procedures are intended to avoid unnecessary airborne collision avoidance system (ACAS II) resolution advisories in aircraft at or approaching adjacent altitudes or flight levels. For commercial operations, these procedures should be specified by the operator. Detailed information on HVR encounters and guidance material concerning the development of appropriate procedures is contained in Attachment B to this Part.

Training guidance is provided in PANS-OPS at:

Attachment A to Part III, Section 3, Chapter 3 - ACAS Training Guidelines for Pilots

Attachment B to Part III, Section 3, Chapter 3 - ACAS Performance During HVR Encounters

PANS-ATM (Procedures for Air Navigation Services - ICAO Doc. 4444 Fifteenth Edition 2007-ATM/501)

15.7.3 PROCEDURES IN REGARD TO AIRCRAFT EQUIPPED WITH AIRBORNE COLLISION AVOIDANCE SYSTEMS (ACAS)

15.7.3.1 The procedures to be applied for the provision of air traffic services to aircraft equipped with ACAS shall be identical to those applicable to non-ACAS equipped aircraft. In particular, the prevention of collisions, the establishment of appropriate separation and the information which might be provided in relation to conflicting traffic and to possible avoiding action shall conform with the normal ATS procedures and shall exclude consideration of aircraft capabilities dependent on ACAS equipment.
15.7.3.2 When a pilot reports an ACAS resolution advisory (RA), the controller shall not attempt to modify the aircraft flight path until the pilot reports “Clear of Conflict”.

15.7.3.3 Once an aircraft departs from its ATC clearance or instruction in compliance with an RA, or a pilot reports an RA, the controller ceases to be responsible for providing separation between that aircraft and any other aircraft affected as a direct consequence of the manoeuvre induced by the RA. The controller shall resume responsibility for providing separation for all the affected aircraft when:

a) the controller acknowledges a report from the flight crew that the aircraft has resumed the current clearance; or

b) the controller acknowledges a report from the flight crew that the aircraft is resuming the current clearance and issues an alternative clearance which is acknowledged by the flight crew.

Note - Pilots are required to report RAs which require a deviation from the current ATC clearance or instruction (see PANS-OPS, Volume I, Part III, Section 3, Chapter 3, 3.2 c) 4)). This report informs the controller that a deviation from clearance or instruction is taking place in response to an ACAS RA.

15.7.3.4 Guidance on training of air traffic controllers in the application of ACAS events is contained in the Airborne Collision Avoidance System (ACAS) Manual (Doc 9863).

15.7.3.5 ACAS can have a significant effect on ATC. Therefore, the performance of ACAS in the ATC environment should be monitored.

15.7.3.6 Following a significant ACAS event, pilots and controllers should complete an air traffic incident report.

Note 1 - The ACAS capability of an aircraft may not be known to air traffic controllers.

Para. 12.3.1.2, items r) to y) – RA Reporting Phraseology

Circumstances:

... after a flight crew starts to deviate from any ATC clearance or instruction to comply with an ACAS resolution advisory (RA) (Pilot and controller interchange):

PILOT: [callsign] TCAS RA;

ATC: [callsign] ROGER;

... after the response to an ACAS RA is completed and a return to the ATC clearance or instruction is initiated (Pilot and controller interchange):

PILOT: [callsign] CLEAR OF CONFLICT, RETURNING TO (assigned clearance);

ATC: [callsign] ROGER (or alternative instructions);

… after the response to an ACAS RA is completed and the assigned ATC clearance or instruction has been resumed (Pilot and controller interchange):

PILOT: [callsign] CLEAR OF CONFLICT (assigned clearance) RESUMED;

ATC: [callsign] ROGER (or alternative instructions);

… after an ATC clearance or instruction contradictory to the ACAS RA is received, the flight crew will follow the RA and inform ATC directly (Pilot and controller interchange):

PILOT: [callsign] UNABLE, TCAS RA;

ATC: [callsign] ROGER;

The correct pronunciation of the phrase "TCAS RA" is "TEE-CAS-AR-AY".

ICAO Doc. 7030/4 (Region Supplementary Procedures), Fifth Edition, 2008

5.3 AIRBORNE COLLISION AVOIDANCE SYSTEMS (ACAS)

5.3.1 Carriage and operation of ACAS II (A10, Vol. IV – Chapter 4; P-OPS, Vol. I)

5.3.1.1 ACAS II shall be carried and operated in the EUR Region (and the Canarias FIR) by all turbine-engined aeroplanes having a maximum certificated take-off mass exceeding 5 700 kg or authorized to carry more than 19 passengers.

ICAO Annex 6: Operation of Aircraft, Part I, International Commercial Air Transport-Aeroplanes, Eighth edition-July 2001, Amendment 31, November 2007

6.18.1 From 1 January 2003, all turbine-engined aeroplanes of a maximum certificated take-off mass in excess of 15 000 kg or authorized to carry more than 30 passengers shall be equipped with an airborne collision avoidance system (ACAS II).

6.18.2 From 1 January 2005, all turbine-engined aeroplanes of a maximum certificated take-off mass in excess of 5 700 kg or authorized to carry more than 19 passengers shall be equipped with an airborne collision avoidance system (ACAS II).

6.18.3 Recommendation.— All aeroplanes should be equipped with an airborne collision avoidance system (ACAS II).

6.18.4 An airborne collision avoidance system shall operate in accordance with the relevant provisions of Annex 10, Volume IV.

6.19.1 All aeroplanes shall be equipped with a pressure altitude reporting transponder which operates in accordance with the relevant provisions of Annex 10, Volume IV.

6.19.2 All aeroplanes for which the individual certificate of airworthiness is first issued after 1 January 2009 shall be equipped with a data source that provides pressure-altitude information with a resolution of 7.62 m (25 ft), or better.

6.19.3 After 1 January 2012, all aeroplanes shall be equipped with a data source that provides pressure-altitude information with a resolution of 7.62 m (25 ft), or better.

6.19.4 Recommendation. The Mode S transponder should be provided with the airborne/on-the-ground status if the aeroplane is equipped with an automatic means of detecting such status.

Note 1 - These provisions will improve the effectiveness of airborne collision avoidance systems as well as air traffic services that employ Mode S radar. In particular, tracking processes are significantly enhanced with a resolution of 7.62 m (25 ft), or better.

Note 2 - Mode C replies of transponders always report pressure altitude in 30.50 m (100 ft) increments irrespective of the resolution of the data source.

Annex 6, Part II - International General Aviation — Aeroplanes, Sixth edition - July 1998, Amendment 26, November 2007

6.14.1 Recommendation.— All turbine-engined aeroplanes of a maximum certificated take-off mass in excess of 15000 kg, or authorized to carry more than 30 passengers, for which the individual airworthiness certificate is first issued after 24 November 2005, should be equipped with an airborne collision avoidance system (ACAS II).

6.14.2 All turbine-engined aeroplanes of a maximum certificated take-off mass in excess of 15000 kg, or authorized to carry more than 30 passengers, for which the individual airworthiness certificate is first issued after 1 January 2007, shall be equipped with an airborne collision avoidance system (ACAS II).

6.14.3 Recommendation.— All turbine-engined aeroplanes of a maximum certificated take-off mass in excess of 5700 kg but not exceeding 15000 kg, or authorized to carry more than 19 passengers, for which the individual airworthiness certificate is first issued after 1 January 2008, should be equipped with an airborne collision avoidance system (ACAS II).

ACAS Manual (ICAO Doc. 9863)

5.2.3. The following ACAS good operating practices have been identified during the use of ACAS throughout the world.

5.2.3.1 To preclude unnecessary transponder interrogations and possible interference with ground radar surveillance systems, ACAS should not be activated (TA-only or TA/RA mode) until taking the active runway for departure and should be deactivated immediately after clearing the runway after landing. To facilitate surveillance of surface movements, it is necessary to select a mode in which the Mode S transponder can nevertheless squitter and respond to discrete interrogations while taxiing to and from the gate. Operators must ensure that procedures exist for pilots and crews to be able to select the operating mode where ACAS is disabled, but the Mode S transponder remains active.

5.2.3.2 During flight, ACAS traffic displays should be used to assist in visual acquisition. Displays that have a range selection capability should be used in an appropriate range setting for the phase of flight. For example, use minimum range settings in the terminal area and longer ranges for climb/descent and cruise, as appropriate.

5.2.3.3 The normal operating mode of ACAS is TA/RA. It may be appropriate to operate ACAS in the TA-only mode only in conditions where States have approved specific procedures permitting aircraft to operate in close proximity or in the event of particular in-flight failures or performance limiting conditions as specified by the Aeroplane Flight Manual or operator. It should be noted that operating in TA-only mode eliminates the major safety benefit of ACAS.

5.2.3.3.1 Operating in TA/RA mode and then not following an RA is potentially dangerous. If an aircraft does not intend to respond to an RA and operates in the TA-only mode, other ACAS-equipped aircraft operating in TA/RA mode will have maximum flexibility in issuing RAs to resolve encounters.

Training guidance is provided in the ACAS Manual at:

Chapter 5 - Operational Use and Pilot Training Guidelines

Chapter 6 - Controller Training Guidelines

End of Document