EUROCONTROL

ACAS RA Downlink

Safety Summary Report

Edition Number	:	1.3
Edition Date	:	31 May 2007
Status	:	Released Issue
Intended for	:	General Public

DOCUMENT CHARACTERISTICS

TITLE

ACAS RA Downlink
Safety Summary Report

	ALDA Reference:	07/06/01-31
Document Identifier	**Edition Number:**	1.3
	Edition Date:	31/05/2007

Abstract

The report documents safety assessment of RA Downlink. It addresses the safety of RA Downlink based on the selected operational concept. It does not cover safety issues resulting from the implementation phase or transfer to operation of RA Downlink.

Keywords

RA	RA Downlink	TCAS	ACAS
FARADS	Safety Case	Safety Study	

Contact Person(s)	**Tel**	**Unit**
Stanislaw Drozdowski	+32.2.729.3760	DAP/ATS

STATUS, AUDIENCE AND ACCESSIBILITY

Status		**Intended for**		**Accessible via**	
Working Draft	□	General Public	☑	Intranet	□
Draft	□	EATMP Stakeholders	□	Extranet	□
Proposed Issue	□	Restricted Audience	□	Internet (www.eurocontrol.int)	☑
Released Issue	☑				

ELECTRONIC SOURCE

Host System	Software	Size
Windows_NT	Microsoft Word	Kb

EUROCONTROL Agency, Library Documentation and Archives (ALDA)
EUROCONTROL Headquarters (50.703)
96 Rue de la Fusée
B-1130 BRUSSELS

Tel: +32 (0)2 729 11 52
E-mail: publications@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
Originator	HVR Ltd.	12/10/06
Safety Expert	Derek Fowler	12/10/06
Project Manager	Stanislaw Drozdowski	12/10/06

DOCUMENT CHANGE RECORD

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

EDITION NUMBER	EDITION DATE	REASON FOR CHANGE	PAGES AFFECTED
1.0	09/10/06	First released issue	All
1.1	12/10/06	EUROCONTROL review	All
1.2	27/03/07	Review by ESL as part of ACAS II safety review	All
1.3	31/05/07	Formatting changes	All

CONTENTS

EXECUTIVE SUMMARY

This document is the Safety Summary[1] Report for RA Downlink. It has been produced as part of the Feasibility of ACAS RA Downlink Study (FARADS).

The aim of the report is to assess whether RA Downlink can provide a substantial net safety benefit compared to the current scenario. In order to do this, a structured Safety Argument was developed and then Evidence, gathered throughout the FARAD Study, was collated and presented to satisfy each strand of the Argument structure.

The Safety Summary Report addresses the intrinsic safety of RA Downlink Operational Concept 7 (OC7) within ECAC member states. It does not cover safety issues resulting from the implementation phase or transfer to operation of RA Downlink.

Hazards and risks associated with the current (pre-RA Downlink) and RA Downlink situations were captured during an FHA/PSSA workshop, attended by ATM operational, technical and safety experts, by representatives from the commercial pilot community, and by experts in human interaction within the ATM system – ie Cognitive Task Analysis and Human Reliability Assessment. Possible hazards and risks were elicited through brainstorming, the evaluation of functional / operational models of the ATM system including RA Downlink and the construction of an Event Tree to compare the probabilities of possible outcomes between the current and RA Downlink situations.

On the safety benefits side, the evidence gathered from the FHA/PSSA, CTA, HRA, Simulations and FARADS Latency Study shows that RA Downlink could, overall:

- improve Controller general situational awareness regarding the RA and other aircraft;
- increase the Controller's awareness of RA completion, thereby increasing the likelihood that the Controller would resume responsibility for separation at the appropriate time;
- help prevent interruption to the execution of RAs due to a combination of Controllers inadvertently issuing instructions to RA incident aircraft and Pilots failing to comply with ICAO requirements to ignore ATC instructions when involved in an RA;
- lead to a reduction in RT, during RAs, to the benefit of both Controller and Pilot.

It was noted in the safety assessment that the current evidence for the third of these benefits is marginal, and the estimated increase in the likelihood of a successful RA outcome is not necessarily statistically significant in relation to the uncertainty in the data used.

A number of potential disbenefits were also identified. Safety Requirements were derived in the FHA/PSSA process to mitigate most of these, although the following two possible disadvantages of RA Downlink could not be entirely resolved:

- in some areas of the airspace, 'unnecessary' RAs (those not requiring deviation from ATC clearance) might cause an excess of information on the screen – reducing the number of RAs caused by high vertical speed would help alleviate this problem;
- Controllers would no longer be able to issue clearances to aircraft involved in an RA, even when such clearances would not conflict with the RA – this is, however, probably more of an operational, rather than safety, issue.

The conclusion from the largely qualitative evidence gathered so far is that, on balance, there would be a net safety benefit from RA Downlink if all of the Safety Requirements,

[1] The term "Safety Summary Report" is used in recognition of the fact that the document is neither complete, nor conclusive, enough to be called a Preliminary Safety Case. Nevertheless , it has been produced in accordance with the EUROCONTROL Safety Case Development Manual and could be developed into a full Safety Case if appropriate in the future

specified herein, were satisfied in the implementation of RA Downlink.

However, whether the net safety benefits of RA Downlink are substantial or not is subjective, and will remain until sufficient data is available to carry out a quantified risk assessment.

It is recommended that further assessments be carried out:

1. into the reasons for non-compliance by flight crew with current requirements for RT reporting of RAs to ATC.
2. to validate the provisional 20-second interval after the RA Downlink annotation has been removed from the Controller’s display before the Controller can resume responsibility for providing clearances to affected aircraft if no ‘Clear of Conflict’ voice report is received.
3. to investigate the possible inconsistency between not being able to filter out RAs that do not require a deviation from clearance and the proposed revision to ICAO Doc. 4444 that will allow pilots not to report RAs that do not require a deviation from clearance.
4. into the operation of RA Downlink in specific types of airspace / sectors be conducted to determine suitability for implementation in those areas.
5. to recommend (for incorporation in ATC Procedures) what Controllers should do in the event of conflicting RA reports, between pilot voice report and RA Downlink; and of reports received through one channel only - pilot voice report or RA Downlink.
6. into the effect of an overall increase in the number of reported RAs on Controller confidence / turnover during a shift.
7. of Controller reaction to an RA being reported by the downlink for the situation where they still believe they are responsible for separation (no deviation from clearance), including the scenario where separation had been provided by ATC (ie ‘unnecessary’ RAs).
8. to recommend (for incorporation in ATC Procedures) what Controllers should do in the event of an RA being displayed for an aircraft when there does not appear to be an intruder aircraft present, for two scenarios: the pilot reports the RA; and the pilot does not report the RA.
9. to recommend (for incorporation in ATC Procedures) what Controllers should do in the event of an aircraft manoeuvring in a manner different to that displayed to the Controller by RA Downlink.
10. to review the regulations in paragraph 15.6.3.2 of ICAO Doc 4444, governing the provision of traffic information to aircraft involved in an RA, on the basis that the practice might distract the pilot from following the RA.
11. to validate the provisional figure of 10^{-5} per operating hour for the maximum frequency of a false display of an RA to the Controller.
12. to review current ICAO regulations (PANS-OPS and PANS-ATM) for internal and mutual -consistency, regardless of whether RA Downlink is implemented or not.
13. in order to come to a quantitative conclusion regarding the safety benefits of RA Downlink.
14. into the reasons for non-compliance by flight crew with the PANS-OPS requirements to follow an RA despite contradictory ATC intervention, regardless of whether RA Downlink is implemented or not.
15. Whether it is necessary, or desirable, for Controllers to be able to issue clearances to aircraft, even if the RA does not require a deviation from clearance / manoeuvre and there is no conflict between ATC and the RA, should be investigated

Finally.

16. If, as a result of the further assessments recommended in this report, it is decided to implement RA Downlink then guidance material for implementers should be developed by EUROCONTROL.

This page intentionally blank

1. INTRODUCTION

This document is the Safety Summary Report for RA Downlink, as part of the wider Feasibility of ACAS RA Downlink Study (FARADS).

This report presents an argument, using Goal Structuring Notation (GSN), that the System proposed for consideration (RA Downlink operations within ATM) would deliver a substantial net safety benefit and weighs the available evidence that might support (or undermine) that argument.

1.1 Background

The safe, orderly and expeditious flow of air traffic is dependant on effective communication between flight crews and air traffic controllers.

High-risk scenarios such as the loss, or imminent loss, of separation between aircraft may be stressful events for both pilots and controllers, which can lead to break down of communications.

From 1 January 2005, all turbine-engined aeroplanes of a maximum certificated take-off mass in excess of 5700 kg or authorized to carry more than 19 passengers must be equipped with an Airborne Collision Avoidance System, ACAS, to aid pilots in avoiding collisions by providing Traffic Advisories (TAs) and Resolution Advisories (RAs).

Currently controllers can only become aware of an ACAS RA if the incident pilots provide a voice report[2], after which the controller should not attempt to manoeuvre that aircraft until it is 'Clear of Conflict'[3].

If a voice report is not provided by the flight crew the controller will be unaware of the ACAS instruction and hence could issue a clearance in a sense opposite to that advised by ACAS.

Although regulated to always adhere to ACAS Resolution Advisories[4], pilots may in some circumstances consider accepting, or actually accept, an ATC clearance which could severely degrade separation.

RA Downlink has been proposed as a possible method of improving controller awareness of ACAS events, thereby reducing the probability of the controller intervening during an ACAS RA.

1.2 Aim

The aim of this report is to assess whether RA Downlink can deliver a substantial net safety benefit compared with the current pre-downlink scenario.

1.3 Purpose

To allow EATMP stakeholders to evaluate the concept and determine whether there is justification for further effort toward the implementation of the RA Downlink concept as proposed.

[2] Requirement of PANS-OPS (Doc 8168)[5], Part VIII, Chap3, para 3.2c)4)

[3] Requirement of PANS-ATM (Doc 4444) [6] para 15.6.3.2 & .3

[4] Requirement of PANS-OPS (Doc 8168)[5], Part VIII, Chap3, para 3.2c) 1) & 2)

1.4 Scope

This Safety Summary Report addresses the conceptual operation of RA Downlink Operational Concept 7 [2] within ECAC member states.

The report does not review the safety issues of the implementation phase or transfer to operation of RA Downlink. These would need to be addressed in local implementation safety cases, if the RA Downlink concept is approved for use within ECAC airspace.

1.5 Structure of this Document

Sections 1 and 2 provide background, operational / system descriptions and the methodology employed.

Section 3 states the Overall Safety Argument.

Section 4 gives the lower level safety arguments with supporting evidence.

Sections 5 – 9 list the assumptions, issues, limitations, conclusions and recommendations of the Preliminary Safety Assessment.

A glossary and references complete the document.

2. SYSTEM DESCRIPTION

2.1 ACAS

ACAS operates by interrogating Secondary Surveillance Radar (SSR) transponders on nearby aircraft, in Modes A/C or Mode S if available, and monitoring the replies. Each reply provides the data to calculate the intruder's range, bearing, and, if the intruder is suitably equipped, its altitude. Using a series of replies from other aircraft the closure rate between those aircraft and the subject can be deduced, as well as the vertical speed for altitude-reporting aircraft.

The system will give a Traffic Advisory to alert the flight crew of the presence of another aircraft that might become the subject of a Resolution Advisory.

If the system calculates a risk of collision with an intruder aircraft, it will provide avoidance manoeuvres or manoeuvre restrictions in the vertical plane by generating an RA. The RA may be preventive or corrective:

- **Preventive RA:** A Resolution Advisory giving a manoeuvre restriction intended to maintain existing separation
- **Corrective RA:** A Resolution Advisory instructing a manoeuvre intended to provide separation from all threats

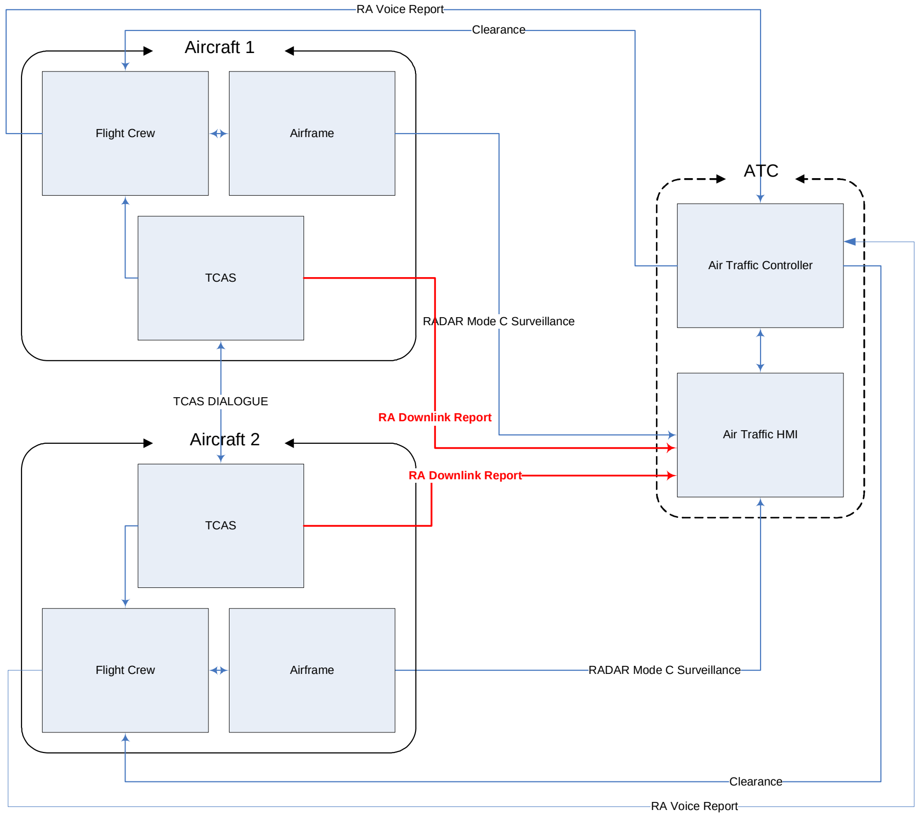
2.2 RA Downlink Operational Concept 7

Whenever an RA is generated, the aircraft's transponder provides information about the RA, which could be downlinked to ATC for display on Controller Working Positions (CWP). In the proposed operational concept, the following information will be displayed on the controllers HMI:

- An indication of all initial RAs (preventative and corrective) including the identity of the aircraft generating the RA and the intruder aircraft;
- Weakening RAs will not be indicated,
- All follow-up strengthening RAs will be indicated,
- All follow-up reversal RAs will be indicated,
- The climb/descend, increase climb/increase descend, crossing climb/descend, reversal climb/reversal descend RA information will be displayed in a graphical form representing the vertical movement,
- For all other RAs, information is presented in a graphical form indicating that a vertical speed limit RA has been issue,
- There is no indication of 'Clear of Conflict'.

2.3 Operation Context Model

Figure 1 below shows the context model of two ACAS equipped aircraft under the control of one air traffic controller. This model shows the difference between pre and post implementation of the RA Downlink. Additional models were used during the FHA / PSSA workshop; Two ACAS equipped aircraft controlled by two independent air traffic controllers; and One ACAS equipped aircraft and one non-equipped aircraft, controlled by one air traffic controller.



Notes:

The diagram displays the post RAD implementation model.

To achieve the pre RAD implementation model the red 'RA Report' lines are removed.

Figure 1. Operational Model

2.4 Pre RA Downlink Implementation

Under the current operational scenario, without RA downlink, the functions of the Controller and Flight Crew have been identified as:

2.4.1 Flight Crew Functions

a. Manoeuvre the aircraft in accordance with the RA

b. Report RA to ATC by RT

c. Return to cleared flight level once 'Clear of Conflict'

d. Report 'Clear of Conflict' to ATC by RT

2.4.2 Controller Functions

a. Receive and acknowledge Pilot report

b. Identify which aircraft are involved in the RA event

c. Identify whether they are responsible for separation

d. Cease further instructions to incident aircraft

e. Give essential-traffic information, as required

f. Detect and resolve third party conflicts

g. Reassume responsibility for separation when 'Clear of Conflict' received and acknowledged

h. Continue to provide a separation service to all non-incident aircraft in the sector

2.5 Post RA Downlink Implementation

With the introduction of the RA Downlink the functions of both the flight crew and the controller are unchanged. The purpose of the downlink is not to alter ACAS procedures, but rather to provide the controller with a timely and reliable indication of an RA so that situational awareness is maintained.

This page intentionally blank

3. OVERALL SAFETY ARGUMENT

This section presents the overall safety argument for the safety of RA Downlink.

A high-level view of the safety argument structure is provided, in the form of Goal Structuring Notation (GSN), in Figure 2 below.

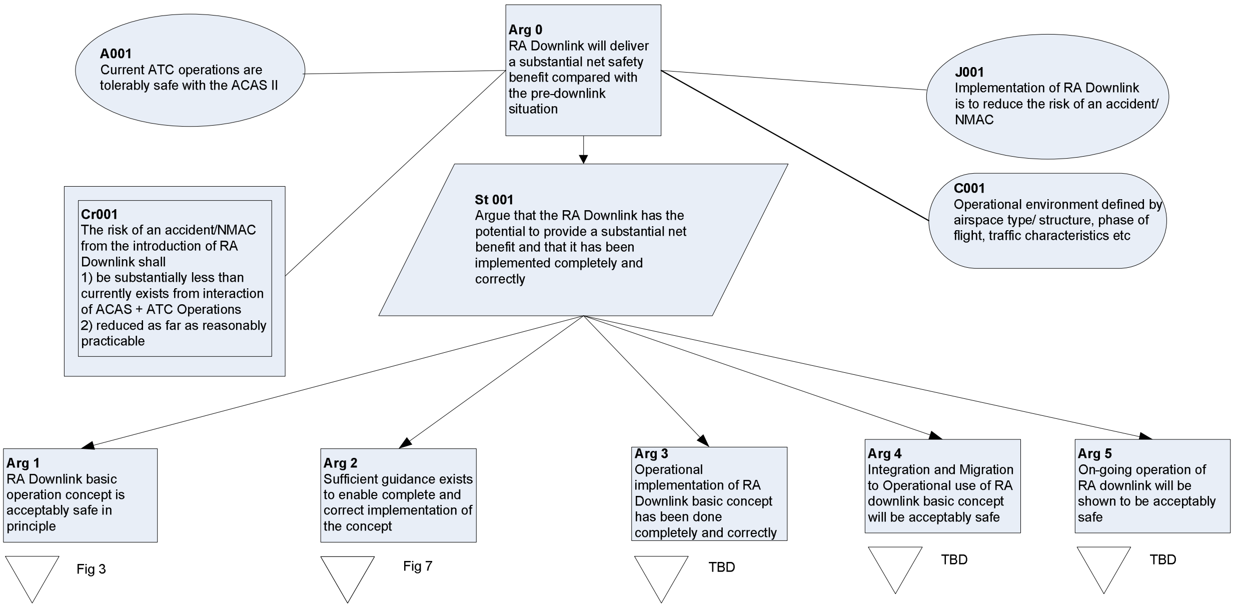

A001
Current ATC operations are tolerably safe with the ACAS II
Arg 0
RA Downlink will deliver a substantial net safety benefit compared with the pre-downlink situation
J001
Implementation of RA Downlink is to reduce the risk of an accident/ NMAC
C001
Operational environment defined by airspace type/ structure, phase of flight, traffic characteristics etc
Cr001
The risk of an accident/NMAC from the introduction of RA Downlink shall
1) be substantially less than currently exists from interaction of ACAS + ATC Operations
2) reduced as far as reasonably practicable
St 001
Argue that the RA Downlink has the potential to provide a substantial net benefit and that it has been implemented completely and correctly
Arg 1
RA Downlink basic operation concept is acceptably safe in principle
Fig 3
Arg 2
Sufficient guidance exists to enable complete and correct implementation of the concept
Fig 7
Arg 3
Operational implementation of RA Downlink basic concept has been done completely and correctly
TBD
Arg 4
Integration and Migration to Operational use of RA downlink basic concept will be acceptably safe
TBD
Arg 5
On-going operation of RA downlink will be shown to be acceptably safe
TBD

Figure 2. Overall Safety Argument

3.1 Claim

Arg 0: RA Downlink will deliver a substantial net safety benefit compared with the pre-downlink situation – this is the single justification for introducing RA Downlink in the first place.

In order for a net safety benefit to be realised, the risk-reduction associated with the normal operation of RA Downlink must be significantly greater than any increase in risk that might arise during abnormal operation, including human error and failure of the Downlink itself.

3.2 Criteria

Cr001: The criteria for the satisfaction of **Arg 0** are that the risk of an Accident / Near Mid-air Collision (NMAC) from the introduction of RA Downlink shall be:

1) substantially less than currently exists, from interaction of ACAS and ATC operations; and
2) reduced as far as reasonably practicable.

3.3 Context

The environment in which RA Downlink is intended to operate is defined by a number of factors, including airspace type / structure, the phase of flight and traffic density. Potentially, this could include all ECAC En-route and Terminal Airspace where traffic is under ATC radar control.

3.4 Justification

The purpose of ACAS is to alert flight crews to a potential conflict and give resolution advice if required; RA Downlink is intended to reduce the risk of inadvertent ATC intervention in an RA, as well as help prevent consequential conflicts, through improvements in Controller situational awareness.

3.5 Strategy

The strategy (**St001**) for decomposing the top-level Claim (**Arg 0**) is to argue that RA Downlink Concept has the potential to provide a substantial net safety benefit and (eventually) that the Concept has been implemented completely and correctly.

This is reflected in the five principal safety arguments (**Arg 1** to **Arg 5**), as follows:

Arg 1: RA Downlink basic operation concept is acceptably safe in principle;

Arg 2: Sufficient guidance exists to enable complete and correct implementation of the concept;

Arg 3: Operational implementation of RA Downlink has been done completely and correctly;

Arg 4: Integration and migration to operational use of RA Downlink basic concept will be acceptably safe;

Arg 5: On-going operation of RA Downlink will be shown to be acceptably safe.

This Safety Summary Report seeks to demonstrate that RA Downlink Concept is acceptably safe (as defined by the safety criteria in **Cr001**) *in principle* – ie subject to its subsequent complete and correct implementation; therefore this document will support Arguments 1 and 2.

If the RA Downlink concept is given stakeholder approval for implementation, the report should be developed into a full safety case, completed through to **Arg 5** and regularly updated to ensure that it remains applicable and current – this will be reflected in the guidance material to be developed in support of **Arg 2**.

3.6 High-Level Assumptions

It is assumed (**A001**) that current ATC operations are tolerably[5] safe with ACAS II. This establishes a baseline for RA Downlink, which seeks to improve on the tolerable level of safety.

[5] Tolerable in this sense means meeting at least the minimum regulatory requirements. For the avoidance of doubt, A001 means that ATC operations are tolerably safe without taking account of any benefits from ACAS II but taking full account of any negative safety effects that ACAS II might have on ATC.

4. SAFETY OF THE RA DOWNLINK CONCEPT

This section presents the Argument that the RA Downlink Concept is acceptably safe in principle (**Arg 1**), and assesses the available Evidence to support that Argument.

Where sufficient Evidence to validate the Argument is not available, further recommendations are made (in section 8 below) to ensure that implementation of RA Downlink is safe.

4.1 Argument Structure

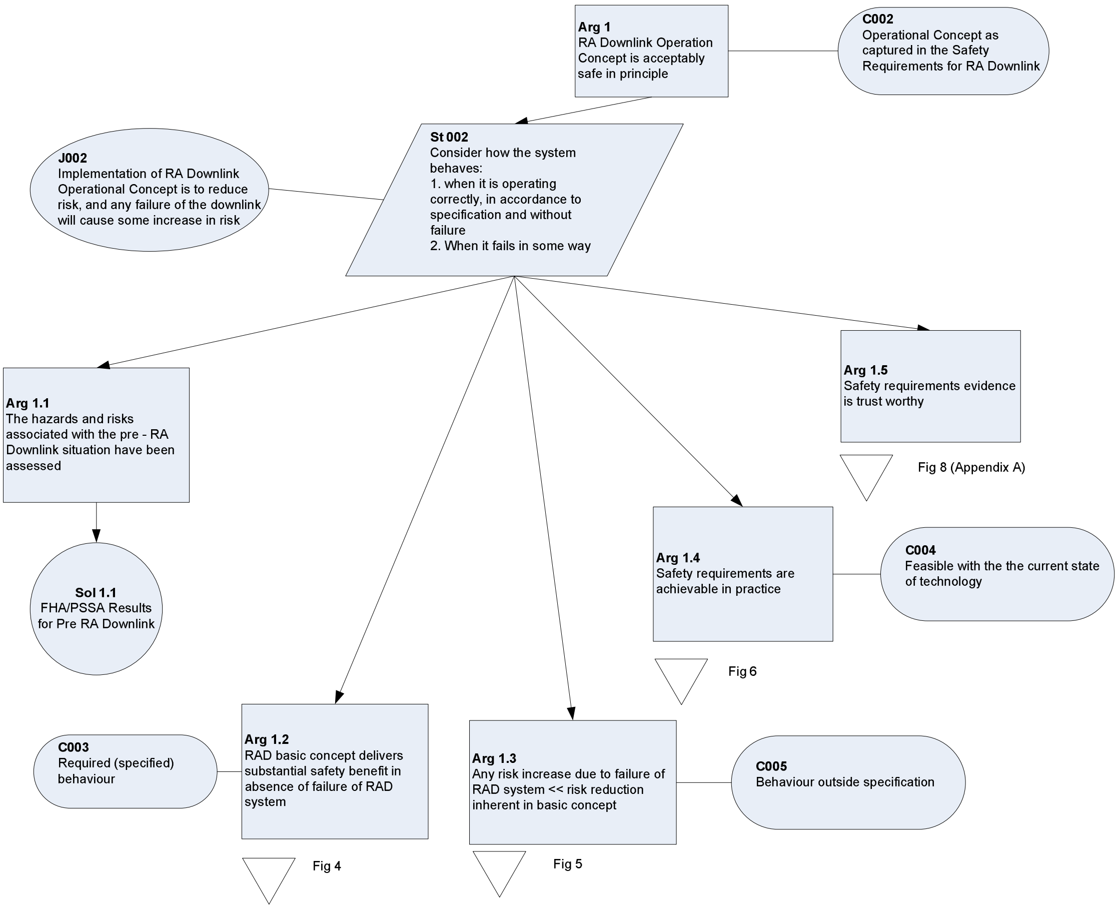

Arg 1
RA Downlink Operation Concept is acceptably safe in principle
C002
Operational Concept as captured in the Safety Requirements for RA Downlink
J002
Implementation of RA Downlink Operational Concept is to reduce risk, and any failure of the downlink will cause some increase in risk
St 002
Consider how the system behaves:
1. when it is operating correctly, in accordance to specification and without failure
2. When it fails in some way
Arg 1.1
The hazards and risks associated with the pre - RA Downlink situation have been assessed
Sol 1.1
FHA/PSSA Results for Pre RA Downlink
Arg 1.5
Safety requirements evidence is trust worthy
Fig 8 (Appendix A)
Arg 1.4
Safety requirements are achievable in practice
C004
Feasible with the the current state of technology
Fig 6
C003
Required (specified) behaviour
Arg 1.2
RAD basic concept delivers substantial safety benefit in absence of failure of RAD system
Fig 4
Arg 1.3
Any risk increase due to failure of RAD system << risk reduction inherent in basic concept
Fig 5
C005
Behaviour outside specification

Figure 3. Strategy 002

4.2 Context

The context for **Arg 1** is the Operational Concept [2].

4.3 Strategy

The decomposition of **Arg 1** is shown in Figure 3 above.

The strategy is to show that:

a. when the RA Downlink is operating correctly - ie in accordance with specification, and without failure – it would deliver a substantial reduction in the risk of an accident, compared with the pre-Downlink situation; and

b. failures of the RA Downlink would not significantly undermine its risk-reduction potential.

The rationale for this approach (**J002**) is that the objective of RA Downlink is to reduce risk from adverse interaction of ACAS and normal ATC operations.

The strategy is achieved through **Arg 1.1** to **Arg 1.4**, as discussed in paragraphs 4.4 to 4.7 below.

4.4 Pre-Downlink Hazard and Risk Assessment (Arg 1.1)

4.4.1 Supporting Evidence for Arg 1.1

Detailed Evidence to show that the hazards and risks associated with the pre-RA Downlink situation have been assessed (**Arg 1.1**) is given in the RA Downlink FHA/PSSA Report [11].

In summary, the hazards and risks associated with the pre-RA Downlink situation were captured during an FHA/PSSA workshop attended by ATM experts. Possible hazards and risks were elicited through brainstorming and the evaluation of functional / operational models of the current ATM system.

The hazards associated with the pre-RA Downlink situation were agreed to be:

- Two aircraft encounter a genuine RA
- Multiple aircraft encounter a genuine RA
- Aircraft encounters an ‘unnecessary’ RA
- Aircraft encounters a false RA
- Aircraft does not react to an RA

The accident sequence (scenario) associated with the first of these hazards was used as the initial basis of the *success viewpoint* (see section 4.5 below) to show that RA Downlink could, under normal operating conditions, provide a substantial safety benefit. The other hazardous scenarios were used mainly to “test” the *success viewpoint* for fundamental weaknesses (see *failure viewpoint,* in section 4.6 below – specifically Arg 1.3.1)

Considering the hazardous scenarios presented, the participants of the FHA/PSSA workshop identified the following occurrences which might prevent the effective mitigation of the hazard consequences identified for the pre-RA-Downlink situation:

- Pilot voice report is missing
- Pilot voice report is late
- Controller may attempt to issue clearances if unaware of RA
- Pilot voice report is incorrect
- Extended RT resulting from controller confusion due to incorrect report blocks the frequency
- Threat aircraft is not identified

- Non-structured voice reports block the frequency and could cause confusion
- Clear of Conflict report may be missing
- Clear of Conflict report may be late

4.4.2 Other Issues related to the Pre-RA Downlink Situation

The safety study of RA Downlink has also highlighted inconsistencies in the current regulations between ICAO Doc 4444 (PANS-ATM) [6] and Doc 8168 (PANS-OPS) [5] [6].

Currently, PANS-OPS Chapter 3, paragraph 3.2, c), 4, states that the flight crew should 'as soon as possible, as permitted by aircrew workload, notify the appropriate ATC unit of the RA, including the direction of any deviation from the current air traffic control instruction or clearance' [5]. However, the experience of the participants at the FHA/PSSA workshop was that only RAs which required a deviation from clearance or a manoeuvre were reported to ATC.

It is understood that the ICAO regulations may be changed to reflect current practice, at which time RA Downlink, unless modified, will be in contravention of the regulations as it is currently not possible to filter RAs according to whether a deviation is required – see Recommendation #3, in section 8 below.

Furthermore, PANS-ATM, 15.6.3.2 states 'When a Pilot reports a manoeuvre induced by an ACAS resolution advisory (RA), the Controller shall not attempt to modify the aircraft flight path until the Pilot reports returning to the terms of the current air traffic control instruction or clearance but shall provide traffic information as appropriate.

15.6.3.3 states 'Once an aircraft departs from its clearance in compliance with a resolution advisory, 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 resolution advisory.

However a manoeuvre does not always result in a deviation from clearance and conversely a deviation from clearance does not necessarily require a manoeuvre. Ambiguity regarding responsibility for separation could arise, although PANS-OPS requires the pilot to follow an RA irrespective of the circumstances – so, during the period of the RA the responsibility for separation appears to be irrelevant.

Recommendation: Current ICAO regulations (PANS-OPS and PANS-ATM) be reviewed for internal and mutual -consistency, regardless of whether RA Downlink is implemented or not.

4.4.3 Conclusion – Arg 1.1

The hazards and risks associated with the pre-RA Downlink scenario have been qualitatively assessed; however quantification of the results would require reliable occurrence data of all of the aspects of ACAS RA events, which is not currently available. **Arg 1.1** has been partially satisfied (ie qualitatively), although further analysis of RA cause, location and rate data is required to quantify the ability of

[6] ICAO State Letter AN 1312.5-06155 [14] proposes amendment to clarify the role of air traffic controllers and flight crew in operation of ACAS and in responding to its associated advisories.

RA Downlink to provide a net safety benefit specifically in terms of reduced risk of an accident.

Recommendation: Further work be carried out in order to come to a quantitative conclusion regarding the safety benefits of RA Downlink.

4.5 Success Viewpoint - RA Downlink Risk-reduction Potential (Arg 1.2)

The decomposition of Arg 1.2 is shown in Figure 4 below.

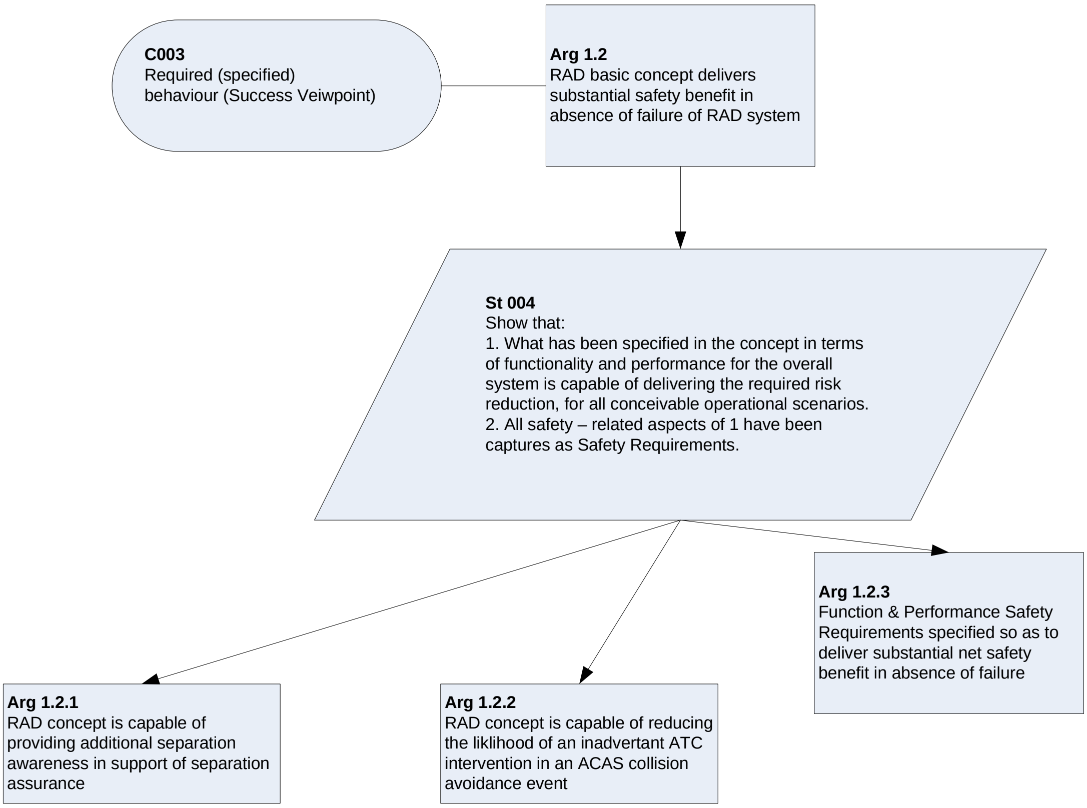

C003
Required (specified) behaviour (Success Veiwpoint)
Arg 1.2
RAD basic concept delivers substantial safety benefit in absence of failure of RAD system
St 004
Show that:
1. What has been specified in the concept in terms of functionality and performance for the overall system is capable of delivering the required risk reduction, for all conceivable operational scenarios.
2. All safety – related aspects of 1 have been captures as Safety Requirements.
Arg 1.2.3
Function & Performance Safety Requirements specified so as to deliver substantial net safety benefit in absence of failure
Arg 1.2.1
RAD concept is capable of providing additional separation awareness in support of separation assurance
Arg 1.2.2
RAD concept is capable of reducing the liklihood of an inadvertant ATC intervention in an ACAS collision avoidance event

Figure 4. Decomposition of Argument 1.2

4.5.1 Context

The Argument that the RA Downlink basic concept delivers substantial safety benefit in absence of failure of RA Downlink system (Arg 1.2) is made in the context of the "success viewpoint", and is related to the required behaviour of RA Downlink, as captured in the RA Downlink Functional Safety Requirements.

4.5.2 Strategy

The strategy is to show that:

1) What has been specified in the concept in terms of functionality and performance for the overall system is capable of delivering the required, substantial risk reduction, for all conceivable operational scenarios;

2) All safety-related aspects of 1) have been captured as Functional Safety Requirements for RA Downlink.

In order to achieve the strategy, **Arg 1.2** has been divided into three lower-level arguments (Arg 1.2.1 to Arg 1.2.3), which are discussed in paragraphs 4.5.3 to 4.5.5 below.

4.5.3 Supporting Evidence for Argument 1.2.1

Evidence that RA Downlink concept is capable of providing additional situational awareness in support of ATC Separation Provision is presented in detail in section 5 of the RA Downlink FHA/PSSA Report [11], the CTA Report [7] and the report on the EEC RA Downlink Simulations [13].

Under the RA Downlink Concept, the following facilities are provided to the Controller, in respect of aircraft involved in an RA:

- RA Downlink provides a structured RA report showing the aircraft involved and the type and direction of manoeuvre (if any) generated by the RA.
- All RA incident aircraft are identified on the Controller's display.
- RA is visible to the Controller for the duration of the RA.
- RA revisions (except 'weakening' RAs) are displayed to the Controller.
- 'Clear of Conflict' may be inferred from removal of the RA from the Controller's display.

The FHA / PSSA workshop concluded that the downlink could improve Controller situational awareness such that the Controller would be better able to direct non-incident aircraft away from the RA event as they would be aware of the deviations from clearance, if any, of the RA aircraft from their clearances.

The subsequent CTA [7] identified the following further safety benefits in support of the Arg 1.2.1:

- RA Downlink allows ATC to anticipate changes by preparing the Controller to expect an RA voice report from the Pilot.
- The RA Downlink visual "pop-out" effect transforms the current-day task of locating aircraft (remembering call sign, scanning screen, identifying aircraft calling) to a largely perceptual one, and can benefit all three phases (before, during, after) of the RA encounter.
- Under OC7, ATC has the means to verify a patently false RA (e.g. by verifying that no conflict situation exists), albeit at the cost of time.

The general conclusion regarding improved situational awareness was confirmed by the conclusions of the FARADS simulations at EEC [13], but only in respect of RAs caused by Controller or Pilot error – for so-called "unnecessary RAs (ie those, commonly caused by high vertical speed, that do not require deviation from clearance) there was no observable difference in situational awareness between the non-RA Downlink and RA Downlink scenarios.

4.5.4 Supporting Evidence for Argument 1.2.2

Evidence that RA Downlink concept is capable of reducing the likelihood of an inadvertent ATC intervention in an ACAS collision avoidance event is presented in detail in section 5 of the RA Downlink FHA/PSSA Report [11] and in the report [4] on a FARADS Latency Study carried out for EUROCONTROL by QinetiQ.

The FHA / PSSA workshop (see section 5 of [11]) concluded that the main cause of Controller intervention in RA events was lack of knowledge that an RA was in progress at the time. It is clear from PANS-OPS [5], Part VIII, Chap3, paragraph 3.2c)4) which states:

> *"as soon as possible, as permitted by aircrew workload, notify the appropriate ATC unit of the RA, including the direction of any deviation from the current air traffic control instruction or clearance"*

that reporting of an RA to ATC is not the Pilot's first priority in ensuring the safety of the aircraft.

It was noted also that even if a Controller did try to intervene in an RA this should not be a major problem if the Pilot complied with the following provisions of PANS-OPS [5], Part VIII, Chap3, paragraph 3.2c):

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;*
>
> *2) follow the RA even if there is a conflict between the RA and an air traffic control (ATC) instruction to manoeuvre;*

Nevertheless, there was some evidence[7] that, even post Überlingen, some pilots chose to follow contrary ATC instructions rather than adhere to the RA[8].

Recommendation: Assessment be conducted into the reasons for non-compliance by flight crew with the PANS-OPS requirements to follow an RA despite contradictory ATC intervention, <u>regardless</u> of whether RA Downlink is implemented or not.

Thus it was concluded that RA Downlink could reduce the likelihood of an inadvertent ATC intervention in an ACAS collision avoidance event by providing timely and reliable RA reports to the Controller.

However, the effectiveness of RA Downlink in this respect would be <u>limited</u> by two factors: inherent latency in the Mode S system on which RA Downlink depended; and likelihood that Pilots would ignore ATC intervention in an RA.

Inherent latency in the Mode S based system would leave a window of opportunity, immediately following the onset of the RA, for inadvertent ATC intervention in the period between the initiation of an RA and the event being displayed to the Controller.

The FARADS Latency Study [4] concluded that the proportion of "uninformed" Controller involvement in RAs that could be avoided by RA Downlink is:

- 80-90% for RAs that carry a high risk of collision;
- around 35% for RAs for which there is little or no risk of collision (ie nuisance RAs).

[7] One such occurrence was reported by DSNA and reproduced in the EUROCONTROL Hindsight magazine, edition 2, January 2006.

[8] The reason for this behaviour was not obvious and is the subject of Recommendation #**Error! Reference source not found.Error! Reference source not found.**, in section 8 below

The report also points out that preventing uninformed controller involvement is most important in the former scenario.

The Latency Study [4] also concluded that the downlink of RA information would be sufficiently timely to allow a significant increase of the situational awareness of Controllers in ACAS encounters, as follows

- Currently (ie pre-RA Downlink) a controller may be totally unaware of up to 15% of ACAS RAs and of the remainder he will typically become aware of the RA in a **mean** time of **30s** after the RA has occurred;
- For the best RA Downlink configuration considered (Extended Squitter), the downlink of RA information could make the controller aware of RAs in a **mean** time of **6.5s** and of **95%** of RAs within **8s**, of their occurrence;
- For a Mode S configuration, the downlink of RA information could make the controller aware of RAs in a **mean** time of 8s and of **95%** of RAs within **11.5s**, of their occurrence.

Overall, and taking account of the likelihood that Pilots would ignore ATC attempts to intervene in an RA, the FHA/PSSA analysis showed a decrease in the likelihood that inadvertent ATC intervention would adversely affect the outcome of an RA; however, that decrease was marginal and not necessarily statistically significant in the context of the uncertainty in accuracy of the data used in the analysis.

The FHA/PSSA Workshop also concluded that RA Downlink could result in a beneficial reduction in RT resulting from the Controller not having to clarify non-structured voice reports; therefore flight crew would be less likely to be distracted from following the RA.

4.5.5 Supporting Evidence for Argument 1.2.3

Section 5 of the RA Downlink FHA/PSSA Report [11] shows how the following Functional Safety Requirements were derived from the analysis of the results of the FHA/PSSA workshop, in accordance with EUROCONTROL SAM Methodology, as appropriate to a comparative risk assessment.

These safety requirements capture the features of the RA Downlink that are essential to provide the safety benefits discussed above.

Ref	Functional Safety Requirement
SR_01	RAs shall be downlinked and displayed to the Controller.
SR_02	The RA Downlink display shall show the direction of the RA, as displayed by TCAS to the Pilot.
SR_03	Training shall reinforce that Controllers shall not issue clearances to aircraft involved in an RA.
SR_04	The downlinked RA shall be displayed to the Controller within 10 seconds of the RA being activated in the Cockpit.
SR_05	RA Downlink shall provide identity data for the subject aircraft, and intruder aircraft where a Mode S address is available, as well as details of

	the subject aircraft's RA instruction
SR_06	The RA Downlink display shall be intuitive for Controller comprehension
SR_07	The RA Downlink tag with vertical rate symbology shall only be associated with the aircraft reporting the RA.
SR_08	Where a non-ACAS equipped aircraft is involved in an RA event, the Mode S address, where available, shall be downlinked by the ACAS equipped aircraft and that aircraft identified to the Controller
SR_09	Where the Mode S address of a non-ACAS aircraft is unavailable, the ATM system shall perform a correlation to indicate the intruder to the Controller
SR_10	The RA Downlink display shall remain active on the Controllers HMI until the aircraft is 'Clear of Conflict'
SR_11	In the absence of a voice "Clear of Conflict" report from the Pilot(s) of aircraft that had been involved in an ACAS RA, the Controller shall, if appropriate, resume responsibility for providing clearances to those aircraft 20 seconds[9] after the RA annotation has been removed from the RA Downlink Display.

4.5.6 Argument 1.2 Conclusions

It has been shown that:

- RA Downlink can provide additional situational awareness in support of Separation Provision;
- RA Downlink is capable of reducing the likelihood of an inadvertent ATC intervention during an RA event, though its effectiveness in this respect is reduced somewhat by the inherent latency of the technology proposed for the RA Downlink system;
- RA Downlink can reduce the level of RT traffic during an RA;
- The features that are necessary for RA Downlink to deliver a substantial safety benefit in absence of failure have been captured as an initial set of Functional Safety Requirements for implementation of the RA Downlink Concept.

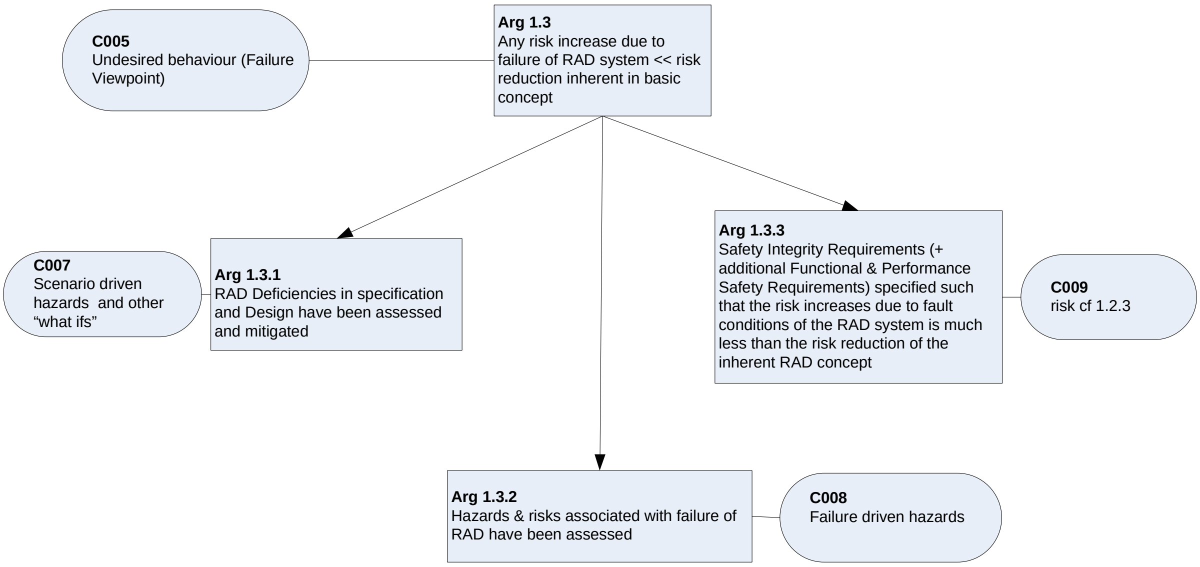
However, whether the RA Downlink basic concept delivers substantial safety benefit in absence of failure of RA Downlink system (**Arg 1.2**) has not (yet) been demonstrated conclusively, either way. In particular, the safety benefit of preventing ATC interference in an RA, depends not only on the inherent latency of the RA Downlink system, but also on whether a pilot would in any event (and in accordance with PANS-OPS) chose to ignore such intervention.

Furthermore, before any overall conclusions can be drawn regarding the net benefits of RA Downlink, the effects of potential failure of the system must be considered, as in section 4.6 below.

[9] But see Recommendation #2, regarding the 20second time interval

4.6 Failure Viewpoint - RA Downlink Risk Increase (Arg 1.3)

The decomposition of **Arg 1.3** is shown in Figure 5 below.



C005
Undesired behaviour (Failure Viewpoint)
Arg 1.3
Any risk increase due to failure of RAD system << risk reduction inherent in basic concept
C007
Scenario driven hazards and other "what ifs"
Arg 1.3.1
RAD Deficiencies in specification and Design have been assessed and mitigated
Arg 1.3.3
Safety Integrity Requirements (+ additional Functional & Performance Safety Requirements) specified such that the risk increases due to fault conditions of the RAD system is much less than the risk reduction of the inherent RAD concept
C009
risk cf 1.2.3
Arg 1.3.2
Hazards & risks associated with failure of RAD have been assessed
C008
Failure driven hazards

Figure 5. Argument 1.3

4.6.1 Context

The claim that any risk increase due to implementation of the RA Downlink system, whether due to failure or inherent, is much less than the risk reduction potential of the basic concept is made in the context of the "failure viewpoint", which is related to any undesired behaviour of RA Downlink – due either to deficiencies (weaknesses, omissions or dissonances) inherent in the concept / system design or to component failures in the physical system (including human errors).

To demonstrate that deficiencies and failure hazards have been assessed, **Arg 1.3** has been decomposed into three lower-level arguments, which are presented, together with supporting evidence, in paragraphs 4.6.2 to 4.6.5 below.

4.6.2 Supporting Evidence for Argument 1.3.1

Evidence that RA Downlink deficiencies in specification and design have been assessed and mitigated was derived from scenario-driven hazards and other 'what ifs', analysed by experts at the FHA/PSSA workshop, and is presented in detail in section 6 of the RA Downlink FHA/PSSA report [11] and within the CTA report [7].

The deficiencies in specification and design identified by the FHA/PSSA workshop are shown in the following table, along with (where applicable) the associated Safety Requirement, which provides mitigation of the deficiency:

Ref	Deficiency	Mitigation
1.	Possible misinterpretation of RA Downlink symbols because, for example, 'climb' (or 'descend') is similar to maintain vertical speed[10]	SR_14
2.	Screen blocking caused by the RA Downlink tags[11]	SR_17
3.	RA Downlink data sharing between ATC Units is not specified, though it would be required to ensure that Controllers of different sectors are both able to see the Downlink in the case of one aircraft being non-ACAS enabled	SR_19
4.	Non-universal implementation of RA Downlink must not lead to a requirement for Flight Deck procedures to change dependent on whether the sector being flown is RA Downlink enabled[12]	SR_20
5.	Under the current regulations, responsibility for separation will be ambiguous at the end of the event when the RA Downlink has cleared but there is no 'Clear of Conflict' report from the flight crew	SR_11, SR_12, SR_13
6.	Procedures concerning RAs that do not require a deviation from clearance must be defined; because RA Downlink cannot distinguish between those RAs that require a deviation from clearance and those that do not, it will not be immediately clear to the Controller whether he/she remains responsible for separation	SR_12
7.	Controllers would not be able to issue clearances that do not conflict with ACAS to aircraft subject to an RA that does not require a deviation from clearance / manoeuvre	Not mitigated
8.	With RA Downlink, there would be two methods for reporting RAs - ie voice and RA Downlink. There may be problems caused by conflicting reports, or confusion caused reports received through one channel only. [13]	SR_15, SR_12
9.	The RA Downlink might distract the Controller from maintaining awareness or performing other tasks in the sector of control[14]	SR_06, SR_14

[10] Concerns about the interpretation of certain RA symbols were also raised in the RA Downlink Simulations [13]

[11] Concerns about screen clutter were also raised in the RA Downlink Simulations [13]

[12] The implied requirement for Pilots to continue to provide verbal reports of RAs to ATC was endorsed by Controllers in the RA Downlink Simulations [13]

[13] An additional, specific point was raised during in the RA Downlink Simulations [13] concerning the need to be precise about which event should signal the suspension of the Controller's separation-provision responsibility during, and for the aircraft involved in, an RA – ie receipt of an RA Downlink or the corresponding Pilot report

[14] The issue of possible distraction of the Controller by RA Downlink was also addressed in the RA Downlink Simulations [13]. An observed marginal increase in the number of late Transfers following

10.	RA Downlink creates the Controller task of detecting an early warning, as well as introducing the task of seeking confirmatory evidence for the RA (if voice report is late / missing)	SR_14
11.	Delay in presenting the RA to the Controller reduces the effectiveness of RA Downlink in preventing ATC intervention during the critical initial period of the event	SR_04
12.	Controllers might be exposed to an excess of information on the screen as all RAs, whether or not they require a deviation from clearance, will be reported; SR_28 seeks to reduce number of 'unnecessary' RAs but the effect of an increase in the number of reported RAs on Controller confidence / turnover has not been established	Partly mitigated by SR_28
13.	RA Downlink does not indicate the flight crews intent, therefore it may be misleading[15]	SR_16
14.	RA Downlink might prime ATC to hear what they expect to hear, and as a result mishear the subsequent pilot report	SR_15
15.	'Unnecessary' RAs may distract the Controller and need to be reduced in frequency	SR_28
16.	False downlink / display of RA could undermine Controller's trust in RA Downlink	SR_26
17.	False RAs might cause the Controller to believe they are not responsible for separation and may prevent them from contacting the flight crew until after a proposed time-out period (see also SR_11) or until the fault clears.	SR_21, SR_26
18.	The provision of traffic information during an RA was questioned on the basis that visual acquisitions of threat aircraft may be misleading and the information would not aid (indeed might distract) the flight crew in following the RA	Not mitigated [16]

The safety requirements referred to in the table are presented in Section 4.6.4

4.6.3 Supporting Evidence for Argument 1.3.2

Detailed evidence to support the argument that the hazards and risks associated with failure of RA Downlink have been assessed can be found at Section 6 of the RA Downlink FHA/PSSA report.

an RA, for the RA Downlink scenarios, might have been indicative of "cognitive tunnelling". However, there was no other_evidence of such perceptual narrowing – in particular, there was no observed increase in the number of post-RA STCA alerts or in post-RA separation infringement in general.

[15] Fears were expressed by Controllers during the RA Downlink Simulations [13] that they might be held responsible in situations that a pilot failed to follow an RA and the Controller, being aware of the RA through RA Downlink, took no action to prompt the Pilot to follow the RA.

[16] But see Recommendation #**Error! Reference source not found.**, in section 8

The failure driven hazards and risks associated with the RA Downlink concept were also identified by ATM experts at the FHA/PSSA workshop through evaluation of functional / operational models, the completion of a Failure Mode and Effect Analysis table, and the discussion of a number of 'what if' scenarios. The following failure driven hazards were identified:

- Complete loss of RA Downlink
- Loss of a single aircraft's RA Downlink
- Continuous false RA reporting
- Spurious RA reporting
- Downlink ends before RA ends
- Every aircraft appears to have an RA
- The direction of RA displayed is corrupted
- The display of the identity of the aircraft involved in an RA is corrupted

The loss or corruption of RA Downlink is mitigated by the requirement (SR_20) for Pilots to continue reporting RAs by voice, although it was concluded that conflicting reports or unusual situations are likely to distract the Controller and cause confusion.

Safety requirements derived from the analysis of RA Downlink failure modes to mitigate the other failure driven hazards are presented in Section 4.6.4 of this document.

4.6.4 Supporting Evidence for Argument 1.3.3

Detailed evidence of the process undertaken to derive the additional Functional and Performance Safety Requirements, specified such that the risk increase due to the failure of the RA Downlink system is much less than the risk reduction of the inherent RA Downlink concept, can be found in Section 6 of the RA Downlink FHA/PSSA report [11].

The safety requirements described below supplement those identified in paragraph 4.5.5 above. These safety requirements should be addressed to mitigate issues identified, in section 4.6 above, from the 'failure viewpoint' analysis of the RA Downlink concept.

Ref	Functional Safety Requirement / Safety Integrity Requirement
SR_12	Responsibility for separation upon activation and de-activation of an RA Downlink alert must be defined.
SR_13	Once an RA is displayed to the Controller via RA Downlink they should not attempt to issue clearances to any aircraft involved in the event until either: • the display is cleared from the radar screen and the Pilot has reported 'Clear of Conflict' or; • the RA has been cleared from the radar display for a minimum of 20 seconds[20] and it is clear that the aircraft involved are diverging.
SR_14	Recurring Controller training shall be provided to ensure that the RA display

	is familiar and that procedures associated with the RA display are applied rigorously.
SR_15	ATC Procedures shall make it clear to Controllers what they should do in the event of: • conflicting RA reports, between Pilot voice report and RA Downlink; • reports received through one channel only – Pilot voice report or RA Downlink.
SR_16	ATC Procedures shall make it clear to Controllers what they should do in the event of an aircraft manoeuvring in a manner different to that displayed to the Controller by RA Downlink.
SR_17	Controllers shall have the ability to move the RA Downlink tag around the screen as necessary.
SR_18	RA Downlink should break through radar screen filters so that appropriate controllers are aware of any threat to the aircraft they are controlling. At Clear of Conflict, when the RA cursor disappears, the threat aircraft should remain visible for a short period to assure controllers that there was no collision.
SR_19	An RA Downlink data-sharing network shall be implemented between all RA Downlink enabled ATC centres to ensure that RA events are visible to all appropriate controllers in the case of ACAS conflicts involving non-ACAS operational aircraft and two or more controllers operating in separate ATC centres.
SR_20	There shall be no change in procedures imposed on flight crews with respect to actions during or immediately after an RA encounter. Pilots must continue to provide RA voice reports as soon as possible as permitted by flight crew workload and provide a clear of conflict report when resuming, or having resumed, the ATC clearance.
SR_21	ATC Procedures shall make it clear to Controllers what they should do in the event of an RA being displayed for an aircraft when there does not appear to be an intruder present, for two scenarios: • the pilot reports the RA; • the pilot does not report the RA.
SR_22	RA Downlink shall have operational availability of at least 95%.
SR_23	Pilot training shall reinforce the requirement to report RAs that require a deviation from clearance as soon as is practical / possible.
SR_24	Controllers shall be permitted to communicate with RA incident Pilots if the RA Downlink display has not cleared and no Clear of Conflict report has been issued within 1 minute of the RA initialisation. The Controller's HMI shall provide a signal to the controller when an RA has been active for the specified time.
SR_25	Controllers shall have the ability to disable RA Downlink for selected aircraft. Where RA Downlink has been disabled for a particular aircraft there shall be an indication to the Controller that the downlink is not active for that aircraft. Procedures for analysing / fixing the RA Downlink fault and re-enabling the downlink shall be drafted before RAD implementation.

SR_26	The frequency of a false display of an RA to the Controller (ie an RA that does not exist, or annotation of an RA to the wrong aircraft) shall not exceed 10^{-5} per operating hour[17]
SR_27	RA Downlink enabled ATC units shall have the ability to disable RA Downlink for all aircraft. Where RA Downlink has been disabled or is out of operation there shall be an indication to the Controller that the downlink is not active.
SR_28	Flight crew operating procedures and training shall require Pilots to reduce their rate of climb / descent to less than 1500ft/min when in RVSM airspace or within the last 1000ft before cleared level.

4.6.5 Argument 1.3 Conclusion

The safety integrity, functional and performance safety requirements specified above mitigate the risk due to failure and design deficiency. Whereas it seems likely that any residual risk increase due to failure of RA Downlink would be less than the risk reduction potential of the concept, that has yet to be verified quantitatively – see also the conclusions regarding Arg1.2, in paragraph 4.5.6 above.

However the following two safety issues cannot be mitigated fully:

- Controllers would not be able to issue clearances to aircraft, even if the RA does not require a deviation from clearance / manoeuvre and there is no conflict between ATC and the RA. Whether this point, raised by one participant in the FHA/PSSA Workshop, would be a problem (or even be permitted!) has yet to be addressed – see Recommendations 15 below.
- Controllers might be exposed to an excess of information on the screen as all RAs, whether or not they require a deviation from clearance, will be reported. SR_28 seeks to reduce number of 'unnecessary' RAs but the effect of an overall increase in the number of reported RAs the effect on Controller confidence / turnover has not been established – see Recommendations #6 and 11, in section 8 below.

The degree to which the two unmitigated issues might reduce the safety benefits identified in Argument 1.2.1 (Section 4.5.3 above) has not yet been assessed. RA Downlink could provide a net safety benefit, although whether it is substantial is dependent on the importance placed upon these two issues.

There were concerns expressed in the FHA/PSSA Workshop that RA Downlink may not be suitable for those types of airspace, or in particular sectors, where it is important for ATC to maintain control during RAs that do not require a deviation-from-clearance manoeuvre[18] or where there is a high occurrence of 'unnecessary' RAs. Associated with these points are the inconclusive findings of the FARADS simulations at EEC [13] concerning the benefits / disbenefits of RA Downlink in

[17] This is a very provisional figure and needs to be validated

[18] A deviation from clearance does not necessarily require a manoeuvre, and conversely an RA-induced manoeuvre does not always result in a deviation from clearance.

Terminal Airspace[19]. Further work is required on all three issues – see Recommendation #4, in section 8 below

Overall, however, it is concluded that RA Downlink can provide a net safety benefit if all of the safety requirements can be achieved, although that benefit might not be a substantial in all sectors / types of airspace.

4.7 Safety Requirements are Achievable (Arg 1.4)

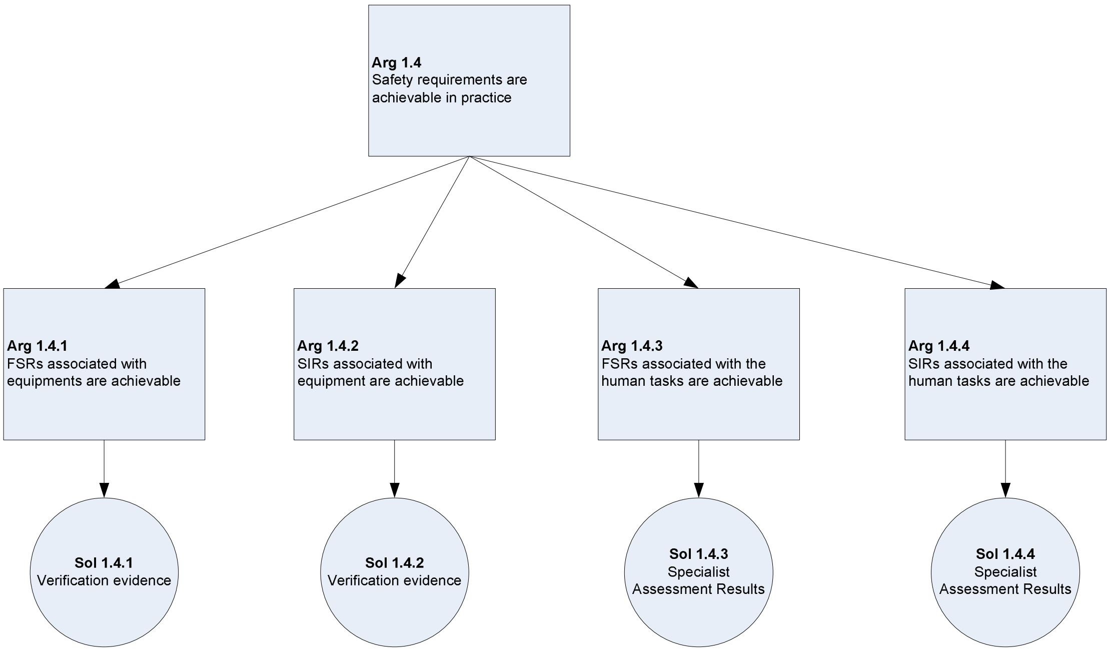

Arg 1.4
Safety requirements are achievable in practice
Arg 1.4.1
FSRs associated with equipments are achievable
Arg 1.4.2
SIRs associated with equipment are achievable
Arg 1.4.3
FSRs associated with the human tasks are achievable
Arg 1.4.4
SIRs associated with the human tasks are achievable
Sol 1.4.1
Verification evidence
Sol 1.4.2
Verification evidence
Sol 1.4.3
Specialist Assessment Results
Sol 1.4.4
Specialist Assessment Results

Figure 6. Argument 1.4

4.7.1 Evidence to Support Argument 1.4.1

The Functional Safety Requirements (FSRs) associated with the equipment have been reviewed by SMEs and have all been deemed technically feasible. The safety requirements which define the concept have been proven through RA Downlink development studies [1] [2] [4] and simulation [13].

Arg 1.4.1 is therefore satisfied.

4.7.2 Evidence to Support Argument 1.4.2

The Safety Integrity Requirements (SIRs) specified for the RA Downlink equipment have also been reviewed by SMEs and have been deemed feasible.

The requirements are approximately equal to a Safety Integrity Level (SIL) 1, which is the lowest level. However, the SIRs would have to be reviewed if quantification is done (in response to Recommendation #13, in section 8 below) and / or SR_26 is changed (as a result of see Recommendation #11, in section 8 below).

[19] It is acknowledged in the RA Downlink Simulations report [13] that, because of limitations in the way the simulations were conducted, the results for Terminal Airspace should not be taken as Evidence for or against the benefits of RA Downlink.

Arg 1.4.2 is therefore satisfied provisionally.

4.7.3 Evidence to Support Argument 1.4.3

The FSRs associated with human tasks have been derived through Cognitive Task Analysis [7] and Human Reliability Assessment [12].

Through analysis of human tasks the studies undertaken are intended to highlight functions that could introduce risk due to human error, or would not be feasible for a human to complete accurately and/or reliably. No such issues were identified in the CTA or HRA, or during the RA Downlink Simulations [13].

One matter that was raised in the CTA / HRA is the time period in which some of the equipment-based functionality could be utilised by the Controller. For example, SR_17 states that the 'Controller shall have the ability to move the RA Downlink tag around the screen as necessary'; however, due to the short duration of RAs (15 to 45 seconds before CPA), the requirement would not be satisfied if the Controller had to navigate through a number of option menus to achieve the action. However, no such problems were observed during the RA Downlink Simulations [13].

Arg 1.4.3 is therefore satisfied, subject to a full evaluation of the final HMI implementation - see Issue #3 in section 6.2 below.

4.7.4 Evidence to Support Argument 1.4.4

No SIRs associated with human tasks have been derived.

4.7.5 Argument 1.4 Conclusion

There have been no issues identified with the proposed equipment functions or human tasks which would result in the requirements being unachievable. All proposals have been reviewed by SMEs and are deemed acceptable. It is therefore concluded that **Arg 1.4** has been satisfied.

4.8 Trustworthiness of Safety Requirements Evidence (Arg 1.5)

The backing evidence to support the statements and evidence provided in the FHA/PSSA, CTA, HRA and this Safety Summary Report can be found at Appendix A of this document.

This shows that the Safety Requirements were derived by following a sound safety assessment process, consistent with the EUROCONTROL SAM methodology, and using people with appropriate and sufficient skills and experience.

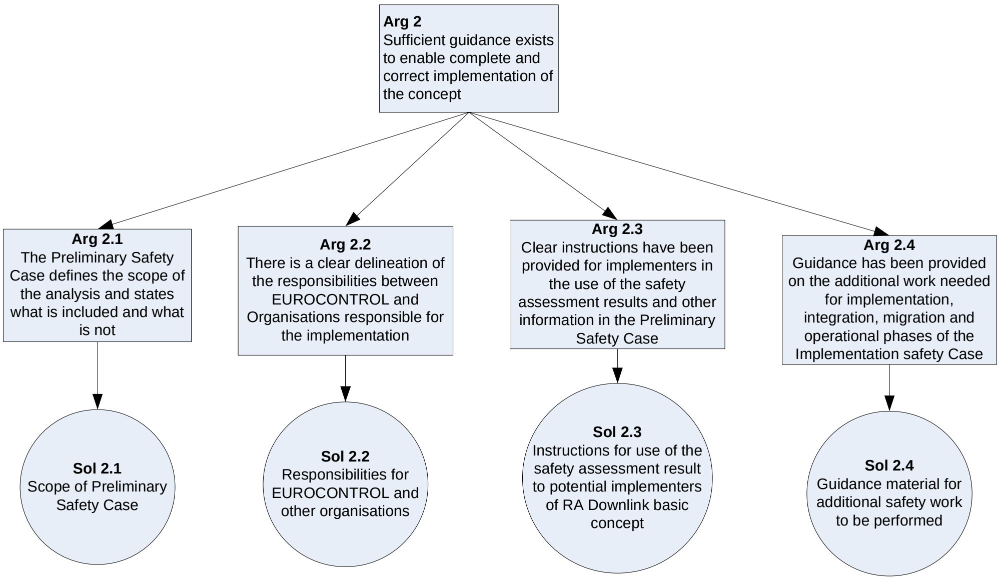
4.9 Overall Conclusions - Argument 1

The overall conclusions regarding the safety of the RA Downlink Concept are presented in section 7 below.

This page intentionally blank

5. GUIDANCE MATERIAL FOR IMPLEMENTATION

This section presents the Argument that sufficient Guidance Material exists to enable complete and correct implementation of the concept, and assesses the available Evidence to support that Argument.



Arg 2
Sufficient guidance exists to enable complete and correct implementation of the concept
Arg 2.1
The Preliminary Safety Case defines the scope of the analysis and states what is included and what is not
Arg 2.2
There is a clear delineation of the responsibilities between EUROCONTROL and Organisations responsible for the implementation
Arg 2.3
Clear instructions have been provided for implementers in the use of the safety assessment results and other information in the Preliminary Safety Case
Arg 2.4
Guidance has been provided on the additional work needed for implementation, integration, migration and operational phases of the Implementation safety Case
Sol 2.1
Scope of Preliminary Safety Case
Sol 2.2
Responsibilities for EUROCONTROL and other organisations
Sol 2.3
Instructions for use of the safety assessment result to potential implementers of RA Downlink basic concept
Sol 2.4
Guidance material for additional safety work to be performed

Figure 7. Argument 2

A proposed decomposition of **Arg 2** is shown in Figure 7 above.

At this stage, sufficient guidance material to enable complete and correct implementation of the concept has not been produced. If, as a result of the further work recommended in this report, it is decided to implement RA Downlink then guidance material for implementers, to satisfy Arguments 2.1 to 2.4, should be developed by EUROCONTROL – see Recommendation #16 in section 10 below.

The guidance should include the need to carry out a full evaluation of the implemented HMI.

This page intentionally blank

6. ASSUMPTIONS, ISSUES AND LIMITATIONS

6.1 Assumptions

The only assumption that was made when analysing the RA Downlink concept is as follows:

- It is assumed that current (pre-RA Downlink) operations are tolerably[20] safe with ACAS II.

6.2 Issues

The following outstanding safety issues must be resolved before it can be shown that RA Downlink can provide a significant net safety benefit in all types of airspace.

1	As discussed in section 4.6.5 above, Controllers would not be able to issue clearances to aircraft, even if the RA does not require a deviation from clearance / manoeuvre and there is no conflict between ATC and the RA – this is the subject of Recommendation #15, in section 8 below.
2	As discussed in section 4.6.5 above, Controllers might be exposed to an excess of information on the screen as all RAs, whether or not they require a deviation from clearance, will be reported. SR_28 seeks to reduce number of 'unnecessary' RAs but the effect of an overall increase in the number of reported RAs on Controller confidence / turnover has not been established – see Recommendation #6, in section 8 below.
3	Guidance to implementers should include the need to carry out a full evaluation of the implemented HMI.

6.3 Limitations

There might be a need to limit RA Downlink to use in specified types of airspace / sectors – see Issues #.1 and 2 above.

[20] Tolerable in this sense means meeting the minimum regulatory requirements. This establishes a baseline for RA Downlink, which seeks to improve on the tolerable level of safety. For the avoidance of doubt, A001 means that ATC operations are tolerably safe without taking account of any benefits from ACAS II but taking full account of any negative safety effects that ACAS II might have on ATC

This page intentionally blank

7. CONCLUSIONS

With regard to the overall claim that RA Downlink will deliver a substantial net safety benefit compared with the pre-downlink (today's) situation, this report has provided sufficient evidence to show qualitatively that a net safety benefit could be achieved.

On the positive side it has been shown - based on a (EUROCONTROL SAM-compliant) Safety Assessment process, ATC Simulation at EEC, and an RA Downlink Latency Study - that RA Downlink could:

- improve Controller general situational awareness regarding the aircraft involved in an RA and other aircraft in vicinity;
- increase the Controller's awareness of RA completion, thereby increasing the likelihood that the Controller would correctly resume responsibility for separation at that time;
- help prevent interruption to RAs due to a combination of Controllers inadvertently issuing clearances to RA incident aircraft and Pilots failing to comply with ICAO requirements to ignore ATC instructions when involved in an RA;
- lead to a reduction in RT, during RAs, to the benefit of both Controller and Pilot during what can be a stressful event.

It was noted in the safety assessment that the current evidence for the third of these benefits is marginal, and the estimated increase in the likelihood of a successful RA outcome is not necessarily statistically significant in relation to the uncertainty in the data used.

Realisation of these benefits depends on the associated Safety Requirements being satisfied in the implementation of the RA Downlink concept. It has been shown that these Safety Requirements are capable of being satisfied by the available technology / trained Controllers, as appropriate.

On the other hand there may be busy areas of ECAC airspace where 'unnecessary' RAs are so prevalent that RA Downlink could be distractive and may prevent Controller's from issuing clearances which would not have conflicted with ACAS.

However, whether the net benefit would actually be substantial in terms of reduction in the risk of an accident would require a more quantitative risk assessment to be carried out when the necessary data becomes available.

Also, in carrying out the FARADS safety assessment, some inconsistencies have been found in, and between, ICAO PANS-OPS and PANS-ATM requirements relating to ACAS operations. These need to be addressed whether or not the RA Downlink is implemented, since they could impact also on current operations.

This page intentionally blank

8. RECOMMENDATIONS

It is recommended that further assessments be carried out:

1. into the reasons for non-compliance by flight crew with current requirements for RT reporting of RAs to ATC.
2. to validate the provisional 20-second interval after the RA Downlink annotation has been removed from the Controller's display before the Controller can resume responsibility for providing clearances to affected aircraft if no 'Clear of Conflict' voice report is received.
3. to investigate the possible inconsistency between not being able to filter out RAs that do not require a deviation from clearance and the proposed revision to ICAO Doc. 4444 that will allow pilots not to report RAs that do not require a deviation from clearance.
4. into the operation of RA Downlink in specific types of airspace / sectors be conducted to determine suitability for implementation in those areas.
5. to recommend (for incorporation in ATC Procedures) what Controllers should do in the event of conflicting RA reports, between pilot voice report and RA Downlink; and of reports received through one channel only - pilot voice report or RA Downlink.
6. into the effect of an overall increase in the number of reported RAs on Controller confidence / shift turnover.
7. of Controller reaction to an RA being reported by the downlink for the situation where hey still believe they are responsible for separation (no deviation from clearance), including the scenario where separation had been provided by ATC (ie 'unnecessary' RAs).
8. to recommend (for incorporation in ATC Procedures) what Controllers should do in the event of an RA being displayed for an aircraft when there does not appear to be an intruder aircraft present, for two scenarios: the pilot reports the RA; and the pilot does not report the RA.
9. to recommend (for incorporation in ATC Procedures) what Controllers should do in the event of an aircraft manoeuvring in a manner different to that displayed to the Controller.
10. to review the regulations in paragraph 15.6.3.2 of ICAO Doc 4444, governing the provision of traffic information to aircraft involved in an RA, on the basis that the practice might distract the pilot from following the RA.
11. to validate the provisional figure of 10^{-5} per operating hour for the maximum frequency of a false display of an RA to the Controller.
12. to review current ICAO regulations (PANS-OPS and PANS-ATM) for internal and mutual -consistency, regardless of whether RA Downlink is implemented or not.
13. in order to come to a quantitative conclusion regarding the safety benefits of RA Downlink.
14. into the reasons for non-compliance by flight crew with the PANS-OPS requirements to follow an RA despite contradictory ATC intervention, regardless of whether RA Downlink is implemented or not.
15. Whether it is necessary, or desirable, for Controllers to be able to issue clearances to aircraft, even if the RA does not require a deviation from

clearance / manoeuvre and there is no conflict between ATC and the RA, should be investigated.

Finally.

16. If, as a result of the further assessments recommended in this report, it is decided to implement RA Downlink then guidance material for implementers should be developed by EUROCONTROL.

APPENDIX A. GLOSSARY AND DEFINITION OF TERMS

A/C	Aircraft
ACAS	Airborne Collision Avoidance System - ACAS II provides resolution advisories in the vertical plane advising the Pilot how to regulate or adjust his vertical speed so as to avoid a collision.
ADS-B	Automatic Dependant Surveillance Broadcast - a technology where aircraft avionics broadcast a variety of parameters completely autonomously
ATC	Air Traffic Control
ATM	Air Traffic Management
Clear of Conflict	The indication given by ACAS to inform the flight crew that an RA has ended.
Continuous RA Downlink	An RA Downlink display which is continuously displayed on the Controller’s HMI after the associated RA has ended.
Corrective RA	A Resolution Advisory requiring a vertical manoeuvre (a change in vertical speed)
CPA	Closest Point of Approach - the instant in an encounter at which the slant range between the two aircraft is at a minimum.
CTA	Cognitive Task Analysis
EATM(P)	European Air Traffic Management (Programme)
ECAC	European Civil Aviation Conference
ESL	Entity Systems Ltd.
False RA	An RA that results from an ACAS equipment fault as there is no credible threat to the subject aircraft
FARADS	Feasibility of ACAS RA Downlink Study
FHA	Functional Hazard Assessment
FSR	Functional Safety Requirement
HMI	Human Machine Interface
HRA	Human Reliability Assessment
HVR-CSL	HVR Consulting Services Ltd
IVSI	Instantaneous Vertical Speed Indicator – the instrument which indicates vertical speed and also displays the vertical rate limits of an RA to the flight crew

Nuisance RA ICAO Annex 10, Vol IV, defines this as follows:

> An RA shall be considered a “nuisance” … unless, at some point in the encounter, in the absence of ACAS, the horizontal separation and the vertical separation [would have been] simultaneously less than the following values:

	Horizontal separation	*Vertical separation*
above FL100	2.0 NM	750 ft
below FL100	1.2 NM	750 ft

Preventive RA A Resolution Advisory that does not require a change from the current vertical speed. It gives a vertical manoeuvre restriction.

PSSA Preliminary System Safety Assessment

RA Resolution Advisory: 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.

RT Radio Telephony - Voice communications between ATC and flight crews

SAM Safety Assessment Methodology (EUROCONTROL document)

SME Subject Matter Expert

SIR Safety Integrity Requirements

Spurious RA Downlink An RA Downlink alert that activates and clears randomly with no association to the actual on-board ACAS state.

STCA Short Term Conflict Alert - a ground based system alerting controllers to potential conflicts.

Strengthening RA Following an initial RA, a strengthening RA requires an increase in vertical rate

TA Traffic Advisory - an ACAS alert warning the Pilot of the presence of another aircraft that might become the subject of an RA.

TCAS Traffic Alert and Collision Avoidance System – a commercial term given to ACAS and also the official phraseology specified by ICAO for identifying ACAS advisories.

Unnecessary RA An RA issued although sufficient separation had been provided by ATC (providing all aircraft adhere to their respective clearances). May be thought of as a special case of a Nuisance RA (qv)

Weakening RA Following an initial RA, a weakening RA allows for a reduction in vertical rate

APPENDIX B. REFERENCES

[1] FARADS - Technical Study of RA Downlink Methods, Version 1.2, 5th January 2005

[2] ACAS RA Downlink: Operational Concepts for FARADS Study, Version 5.0, 30th January 2006

[3] FARADS Hazard Identification Attendee Briefing Notice, Version 1.0, 20th January 2006

[4] FARADS - Study of Latency of RA Downlink, Released Issue, Version 1.4, 15th April 2006

[5] ICAO Doc 8168 (PANS-OPS), ICAO rules pertaining to TCAS Operational use, 1 June 2005

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

[7] ACAS RA Downlink, Cognitive Task Analysis (CTA) of Potential RA Downlink Scenarios, V1.1, 12 October 2006

[8] Kirwan, B. and Ainsworth, L.K. (1992) A guide to task analysis. Taylor and Francis, London

[9] Air Navigation System Safety Assessment Methodology, SAM, SAF.ET1.ST03.1000-MAN-01, Edition 2.0., 30th April 2004

[10] Safety Case Development Manual, DAP/SAF/091, Proposed Issue, 28th Sep 2005

[11] ACAS RA Downlink Combined FHA/PSSA Report, Released Issue 1.0, 9 October 2006

[12] ACAS RA Downlink Human Reliability Assessment (HRA), Version 1.0 (Project Internal), 2 October 2006

[13] ACAS Resolution Advisory Downlink Experiments (RADE), Edition 0.7, 18 September 2006

[14] ICAO State Letter AN 1312.5-06155. ICAO Montreal 28 August 2006.

APPENDIX C. BACKING EVIDENCE FOR ARGUMENT 1

Strategy

St003: Show that the Safety Requirement evidence is trustworthy

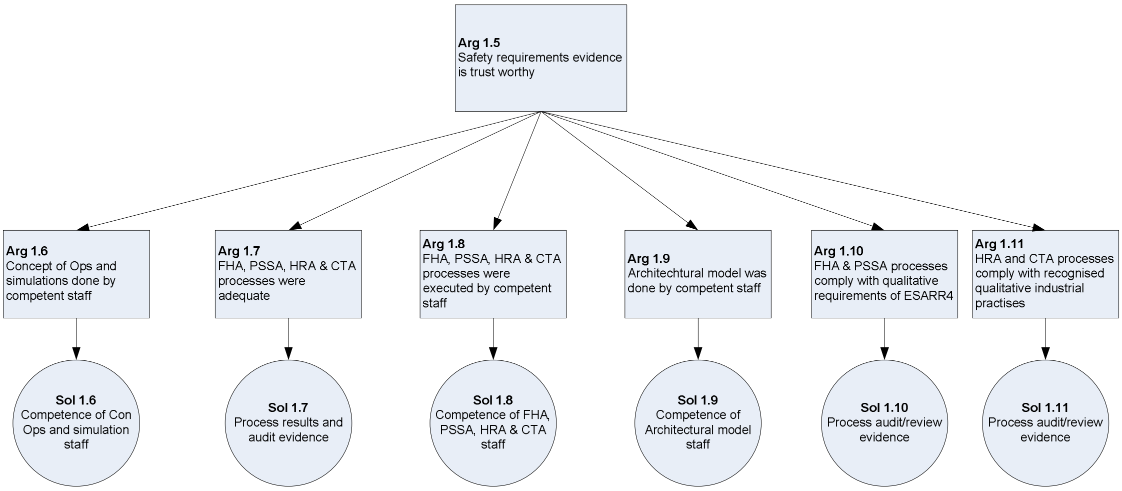

Arg 1.5
Safety requirements evidence is trust worthy
Arg 1.6
Concept of Ops and simulations done by competent staff
Arg 1.7
FHA, PSSA, HRA & CTA processes were adequate
Arg 1.8
FHA, PSSA, HRA & CTA processes were executed by competent staff
Arg 1.9
Architechtural model was done by competent staff
Arg 1.10
FHA & PSSA processes comply with qualitative requirements of ESARR4
Arg 1.11
HRA and CTA processes comply with recognised qualitative industrial practises
Sol 1.6
Competence of Con Ops and simulation staff
Sol 1.7
Process results and audit evidence
Sol 1.8
Competence of FHA, PSSA, HRA & CTA staff
Sol 1.9
Competence of Architectural model staff
Sol 1.10
Process audit/review evidence
Sol 1.11
Process audit/review evidence

Figure 8. Strategy 003

Argument 1.6

Concept of Operations and simulations done by competent staff

Argument 1.6 Evidence

The RA Downlink concept of operations and any simulations based upon that concept have been completed in accordance with standard EUROCONTROL practices and procedures.

Argument 1.6 Conclusion

Argument 1.6 has been satisfied.

Argument 1.7

FHA, PSSA, HRA and CTA processes were adequate

Argument 1.7 Evidence

RA Downlink hazards and risks were identified at a three day FHA / PSSA workshop, held at EUROCONTROL Headquarters, Brussels, from 30th January to 1st February 2006. The workshop was also the basis for the CTA and HRA although further analysis was required

The workshop was attended by a variety of experts in the ATM field to ensure that all derived hazards were applicable and credible. The attendees, with associated roles / expertise, were as follows:

Ben Bakker	ATC Systems
Cay Boquist	ICAO Regulations

Garfield Dean	Technical
Doris Dehn	Human Factors
David De-Smedt	Pilot
Stanislaw Drozdowski	FARADS PM / Controller
Alex Fisher	Pilot
David Fisher	Chairman / Task Manager
Derek Fowler	Safety
Keith Harrison	Facilitator / Safety
Hlin Holm	Controller / Safety
Brian Hilburn	Human Factors
Gavin Jones	Recorder / Safety
Richard Kennedy	Human Factors
Martin Pellegrine	Controller
Mike Wildin	ATC Technical / Procedures

Biographies of the FHA/PSSA workshop attendees are presented in Appendix A of the ACAS RA Downlink Combined FHA/PSSA Report [11].

A complete list of hazards and risks were identified for both pre and post RA Downlink operations by considering four scenarios, namely;

- Operational Scenario A: Two ACAS Equipped Aircraft in Communication with One Controller
- Operational Scenario B: Two ACAS Equipped Aircraft in Communication with Two Controllers
- Operational Scenario C: One ACAS Equipped and One Non-ACAS Equipped / Operational Aircraft in Communication with One Controller
- Operational Scenario D: One ACAS Equipped and One Non-ACAS Equipped / Operational Aircraft in Communication with Two Controllers

Safety requirements were than derived, in accordance with SAM methodology appropriate to comparative studies, to mitigate the hazards and risks that will result from RA Downlink implementation

The general approach for the CTA was to define a functional task description, identify the steps involved in each task, and to systematically evaluate each task with respect to the associated cognitive elements, and potential error mechanisms [7].

The aim of the HRA was to identify the human elements underlying performance in the RA scenarios, and to identify what errors can occur and qualitatively assess how probable it is for the error to occur. The CTA provides the basic psychological knowledge and principles underpinning how, in the event of an RA situation, the ATC, and to a limited extent the Pilot, would perform their tasks with and without an RA Downlink. From the information in the CTA, the 'Human Factors' influencing Human Reliability (e.g. controller and pilot reactions, types of detection failures, interpretation errors, potential ‘workload issues’) could be identified [12].

Argument 1.7 Conclusion

The FHA, PSSA, HRA and CTA processes were adequate.

Argument 1.8

FHA, PSSA, HRA and CTA were executed by competent staff.

Argument 1.8 Evidence

The biographies of the staff that completed the FHA / PSSA are presented below:

David Fisher HVR-CSL Role – Task Manager

David has over 30 years experience in CNS/ATM, both military and civil. For the past 15 years he has been responsible for developing CNS/ATM implementation policies for the world's airlines with the International Air Transport Association in Montreal, (including review and approval of IATA ACAS input to ICAO SICASP Panel, RTCA and EUROCAE); additionally he has worked as Senior Director for ARINC, which included the operational implementation of airline/ATC air ground data link services and as a Technical Consultant for STASYS. David was a member of the EUROCONTROL ATM 2000+ Committee, COM Team and has worked on numerous EUROCONTROL CNS/ATM consultancy projects.

Keith Harrison HVR-CSL Role - Safety Consultant

Keith is a software and systems Safety Engineer with many years consultancy experience working in the defence and aerospace sectors. He has experience in project management, safety programme management and safety team leadership. Keith is recognised as a leading practitioner of GSN having followed, and helped in its development for a number of years. During his time with Praxis, Keith was part of a team that reviewed initial drafts of EUROCONTROL's Safety Assessment methodology. Keith is currently working on a number of EUROCONTROL Safety Case projects.

Gavin Jones HVR-CSL Role - Safety Analyst

Gavin is a graduate Aerospace Systems Engineer working within the Air System Safety team at HVR. In the past he has successfully set-up a number of reliability management tools whilst working with Britannia Airways (now ThomsonFly), including the initialisation of an Early Removals monitoring programme which aimed to reduce the number of rogue components in the airline's stock. In his early role at HVR Gavin provided technical support to the users of the Safety management software tool Cassandra and the Risk Evaluation Management Information System REMIS, whilst also administering the product and user databases. He is now working for the Air System Safety team where he has been involved in FHA/PSSA studies, and subsequent analysis of the output to derive requirements for a safety case.

The CTA was conducted by Brian Hilburn:

Brian Hilburn HVR-CSL Role - Human Factors

Brian has been actively involved in Human Factors research for over 20 years. His particular expertise is in the areas of ATM and human-machine interaction. Until recently he was the Head of NLR Amsterdam's Human Factors department, as well as project leader for several ATM human factors projects. His particular area of expertise is ATM Automation, Visual Performance and Decision Making, Monitoring and Attention. His work for EUROCONTROL has included studies into: ATC Cognitive Complexity Factors and the Impact of Head Up Head Down Time for Air Traffic controllers. He has lectured widely on the area of ATM human factors, and was contracted by the EUROCONTROL IANS Luxembourg training academy to develop and provide training in ATM Human Factors, as part of EUROCONTROL's AADP course. As an active private Pilot, he can also be counted on to provide both a theoretical and practical appreciation of ATM human factors.

The HRA was conducted by Dr Richard Kennedy:

Richard Kennedy HVR-CSL Role - Human Factors/Safety

Dr Richard Kennedy is the Manager of the New Programs Group and a Technical Specialist in Safety and Human Factors at Boeing Research & Technology Europe (BR&TE), based at their Centre in Madrid Spain. He has more than 14 years experience of managing and performing safety and human factors projects in several commercial sectors including Nuclear, Railway, Air Traffic Management and Aviation. During this time he has carried out work for many companies including EUROCONTROL, NATS, Railtrack, London Underground Limited, British Energy and BNFL and also been involved in various European Framework Programme Projects. .He holds a Bachelors Degree in Psychology, a Masters Degree in Human Factors and a PhD in Manufacturing and Mechanical Engineering. He is also Chartered Engineer (CEng) with the UK Institution of Electrical Engineers (IEE). He is an invited Member of various International Engineering R&D Groups and has had his work published in Books, Journals and International Conferences.

Argument 1.8 Conclusion

The FHA, PSSA, HRA and CTA were completed by competent staff.

Argument 1.9

Architectural model was done by competent staff

Argument 1.9 Evidence

All models studied in the safety assessment were presented to and approved by the experts in attendance at the FHA/PSSA workshop.

Argument 1.9 Conclusion

Argument 1.9 has been satisfied

Argument 1.10

FHA and PSSA processes comply with qualitative requirements of ESARR4

Argument 1.10 Evidence

The FHA and PSSA processes have addressed the three different types of ATM elements (human, procedures and equipment) and the interactions between these elements with regard to RA Downlink. This has been achieved by performing an FHA / PSSA to cover procedures and equipment, and undertaking a CTA and HRA to address human factors.

The scope, boundaries and interfaces of the RA Downlink concept were pre-determined by the operational concept. The functions that the downlink is intended to perform were identified at the FHA/PSSA workshop, as was the environment that the downlink is intended to operate within.

Safety requirements have been derived as part of a risk mitigation strategy; although compliance with the requirements does not imply that a substantial safety benefit will be achieved.

Argument 1.10 Conclusion

The qualitative requirements of ESARR4 have been met.

Argument 1.11

CTA and HRA processes comply with recognised qualitative industrial processes

Argument 1.11 Evidence

Task analysis refers to a family of techniques used to describe and analyse operator performance within a human-machine system. All task analysis techniques aim to decompose complex system tasks, to elaborate a description of the system, and to identify information and action flows within the system. *CTA* refers to a group of techniques used to capture and represent the cognitive elements underlying performance of a given task.

The method for the CTA was a hybrid, combining elements of the Applied Cognitive Task Analysis (ACTA) technique (1), with modifications for the system development phase. That is, ACTA typically relies on the Critical Incident Technique (2), which uses open-ended questions to elicit information on particularly challenging past incidents. CIT depends on past experience, and seems less applicable to new systems or operational concepts, however.

References:

(1) Militello, L.G. & Hutton, J.B. (2000). Applied cognitive task analysis: A practitioner's toolkit for understanding cognitive task demands. In J. Annett & N.S. Stanton [eds.] Task Analysis, pp 90-113. London: Taylor & Francis.

(2) Flannagan, J.C. (1954). The critical incident technique. Psychological Bulletin, 51, 327-358.

A full list of the references used in the CTA can be found in Section 5 of the CTA document [7].

Human Reliability Assessment, also synonymously referred to as Human Reliability Analysis, is an approach that provides methods for analysing, assessing and reducing risks caused by human errors and consequently assessing how to reduce the impact of such errors on the system.

To complement the Event Tree Analysis (ETA) performed in the PSSA which is largely deterministic in nature, a Petri Net Analysis was performed to identify some of the basic event sequence and combination possibilities. In the HRA study, the main purpose of the Petri Net analysis was to model an ATM system which is considered to be parallel or concurrent, asynchronous, distributed or stochastic in nature. In other words, although useful and essential in any safety analysis, deterministic approaches such as Fault and Event Tree Analysis (FTA/ETA) are not able to fully cope with the characteristics of ATM in the analysis approach they adopt.

References:

Murata, T. (1989) Petri Nets: Properties, analysis and applications. Proceedings of the IEEE, 77(4):541-580, April.

A full list of the references used in the HRA can be found in Section 7 of the HRA document [11].

Argument 1.11 Conclusion

The CTA and HRA comply with recognised qualitative industrial processes; therefore the argument has been satisfied.