EUROCONTROL

ACAS RA Downlink

Combined FHA & PSSA Report

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

EUROCONTROL

DOCUMENT CHARACTERISTICS

TITLE		
ACAS RA Downlink Combined FHA & PSSA Report		
	ALDA Reference:	07/06/01-30
Document Identifier	**Edition Number:**	1.3
	Edition Date:	31/05/07

Abstract

The document is the combined FHA/PSSA report of RA Downlink. It reports on the findings of FHA/PSSA workshop and subsequent analysis.

Keywords

RA	RA Downlink	TCAS	ACAS
FARADS	FHA	PSSA	Safety

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-CSL	9/10/06
DAP/SAF	Derek Fowler	9/10/06
Project Manager	Stanislaw Drozdowski	9/10/06

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	For final EUROCONTROL review	All
1.1	12/10/06	First released issue	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 FHA/PSSA is a study of the potential effects on safety of an ACAS RA Downlink concept. It has been produced on behalf of EUROCONTROL as part of the Feasibility of ACAS RA Downlink Study (FARADS). If found to be beneficial, this concept is planned to be introduced in all classes of ECAC airspace (ie en-route, terminal and oceanic).

The objective of this study is to consider the ATM operation currently taking place, and it will identify any inherent design or specification weaknesses and possibly hazardous fault conditions of RA Downlink as proposed. Where necessary, safety requirements are defined to ensure that introduction of RA Downlink is acceptably safe (ie that the net safety benefit will be substantially positive) should a decision be taken to proceed to full implementation.

It should be noted that this document does not fully identify human factors issues in respect of possible operational implementation of the RA Downlink concept. The human factors issues are addressed further in the associated RA Downlink Cognitive Task Analysis [7] and Human Reliability Assessment [13]. All of these studies will then form the basis of the RA Downlink Safety Summary.

In order to assess the aspects of the RA Downlink concept, an FHA/PSSA workshop was held at EUROCONTROL Headquarters, Brussels, attended by a selection of Subject Matter Experts (SMEs), including controllers, pilots and safety practitioners.

The analysis of the RA Downlink concept was based on two distinct approaches, namely:

- a *Success Viewpoint,* which assessed the opportunities for RA Downlink functionality and performance to reduce the current risk arising from adverse interactions between ATM separation provision and ACAS-induced collision-avoidance manoeuvres; and
- a *Failure Viewpoint*, which assessed the robustness and integrity of the system in order to ensure that the above risk-reduction potential of the RA Downlink would not be significantly undermined by either deficiencies in the specification / design of the Concept or by fault conditions in the physical RA Downlink system.

These two viewpoints were considered in the context of the following scenarios:

- 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

The analysis of the results of the Workshop resulted in a set of Safety Requirements, covering functionality, performance and integrity, for the equipment, people and procedure elements of the RA Downlink system.

The report concludes that the safety requirements set out herein, if satisfied in the implementation of RA Downlink[1], should result in a substantial net reduction in the current

[1] Achievability of the Safety Requirements will be considered in the subsequent Preliminary Safety Case, taking account of, inter alia, the results of the separate, but related Cognitive Task Analysis (CTA) and Human Reliability Assessment (HRA) studies.

risk of adverse interactions between ATM separation provision and ACAS-induced collision-avoidance manoeuvres. Whether or not that would result in a significant safety benefit over the current scenario will be addressed in the RA Downlink Preliminary Safety Case.

It is recommended that:

Further work be carried out to:

1. investigate the reasons for non-compliance by flight crew with current requirements for RT reporting of RAs to ATC.
2. 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. 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. assess the effectiveness of RA Downlink in specific types of airspace / sectors in order to determine suitability for implementation in those areas.
5. recommend (for incorporation in ATC Procedures if implemented) 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. assess the effect of an overall increase in the number of reported RAs on Controller confidence / turnover.
7. analyse 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. recommend (for incorporation in ATC Procedures if implemented) 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. 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. 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 and visual acquisitions could be misleading.
11. validate the provisional figure of 10^{-5} per operating hour for the maximum frequency of a false display of an RA to the Controller.

1. INTRODUCTION

1.1 Background

This report describes a combined Functional Hazard Assessment (FHA), and Preliminary System Safety Assessment (PSSA)[2] for the possible implementation of an ACAS RA Downlink. The work described within has been prepared by HVR-CSL Ltd for EUROCONTROL under Contract C/1.313/HQ/NB/05, dated 3rd November 2005, to satisfy the EUROCONTROL requirements under PE/1.041/HQ/NB/05, dated 29th August 2005.

The work described in this report forms the first of a series of tasks, including CTA and HRA, leading to the development of a Preliminary Safety Case for the possible future implementation of ACAS RA Downlink.

1.2 Objectives and Scope of this Report

The objective of the study is three fold:

- Investigate the potential safety benefits of the RA Downlink compared with the current situation;
- Investigate the inherent design and specification of the RA Downlink for possible weaknesses;
- Identify hazardous fault conditions associated with the RA Downlink;

In all cases Safety Requirements will be derived so as to provide a substantial[3] safety benefit from RA Downlink.

This document contains no Cost Benefit Analysis, although it is considered that such an analysis would be required to determine whether any perceived benefits could be achieved at a justifiable cost.

1.3 Structure of this Document

This document contains 4 main areas; Sections 1 – 4 provides background, operational / system descriptions and the methodology employed; Sections 5 – 6 provide details of the success and failure cases; Section 7 gives the conclusions and recommendations; the remainder of the document provides reference material and supporting information in Section 8 to 10 and Appendices A – D.

1.4 Operational Context

The RA Downlink concept is intended to apply in ECAC airspace, wherever ACAS is operational;

It is assumed that current rules and procedures will change only to the extent described in the RA Downlink Concept and/or herein.

[2] Separate, related reports will be produced for the subsequent CTA and HRA tasks.
[3] In the terms of this document, substantial is defined as a large reduction in risk.

Page intentionally left blank

2. SYSTEM DESCRIPTION

2.1 Background

The expeditious and orderly flow of air traffic requires close cooperation between flight crew and controllers. This cooperation ensures that thousands of flights reach their destination safely each day, although occasionally there are failures in the system that cause the prescribed separation minima between aircraft to be infringed, which if left unresolved could lead to a collision.

Many aircraft have an Airborne Collision Avoidance System (ACAS)[4] which acts as a 'last-resort' method of preventing mid-air collisions, or near collisions, between aircraft. ACAS produces vertical collision-avoidance advice in Resolution Advisory (RA) messages and displays it to the flight crew 15 to 35 seconds in advance of potential collisions. ACAS RAs are automatically coordinated between the aircraft involved if both are suitably equipped.

The Feasibility of an ACAS RA Downlink Study (FARADS) is an investigation into the downlink of RA information to ATC via a data link. This would mean that all RAs generated for the flight crew would, following a transmission delay, be apparent to ATC.

2.2 ACAS System Description

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, it’s altitude. Using a series of replies from surrounding traffic the closure rate between those aircraft and the subject aircraft can be deduced, as well as the vertical speed for altitude reporting aircraft.

The size of the ACAS surveillance envelope is directly related to the aircraft’s airspeed, therefore in terminal airspace where the aircraft are limited to 250kn (below FL100 as regulated by ICAO) the surveillance envelope will be short, although the traffic is likely to be dense. In en-route airspace the ACAS surveillance expands, although separation between aircraft is also increased.

The system will, if an aircraft enters the ACAS surveillance envelope, give a Traffic Advisory (TA) to alert the flight crew of the presence of another aircraft that might become the subject of an RA.

If the system calculates a risk of collision with an intruder aircraft, it will provide avoidance manoeuvres or manoeuvre restrictions, in the vertical plane only, by generating an RA. The RA is solely intended for collision avoidance (not separation assurance). The RA might be preventive or corrective:

- **Preventive RA:** A Resolution Advisory that does not require a change from the current vertical speed. It gives a vertical manoeuvre restriction.
- **Corrective RA:** A Resolution Advisory requiring a vertical manoeuvre (a change in vertical speed)

[4] The implementation of ACAS is commonly referred to as TCAS – Traffic Alert and Collision Avoidance System.

The use of the terms preventive and corrective RA are dependant on the aircraft's trajectory at the time the RA is issued. Whether the RA is preventive or corrective has no bearing on whether the RA requires a deviation from clearance, therefore the terms cannot be used in relation to Air Traffic Control

Not all RAs are generated by conflicts that would lead to a collision. RAs generated when standard separation would have been maintained, are called *unnecessary* RAs. Often, in airspace where aircraft are climbing or descending rapidly, ACAS might calculate that an aircraft's vertical rate will lead to a collision and issue an RA, even though the intruding aircraft's intentions are to level off with standard separation above or below the subject aircraft. RAs generated when there are large horizontal miss distances are also *unnecessary* RAs.

False RAs are those that are generated although there is no possible collision. These are triggered by equipment faults or surveillance errors, for example, erroneous altitude reporting transponders.

If the intruder aircraft is not transmitting altitude data only a TA can be generated. Aircraft without an operating transponder are not detected by ACAS.

2.3 Current Operations

When an RA is activated, the flight crew should respond by following the RA in order to avoid the potential collision. Currently the Pilot is required to inform ATC of an RA, including any deviation from the cleared flight path[5], as soon as practical [4], so that the Controller is made aware of the RA and that his/her responsibility for separation provision to the aircraft involved in the RA has been, in effect, suspended for the duration of the RA; however, this information might be delayed, incoherent or not transmitted due to the increased pilot workload and pressure of avoiding the possible collision.

The Controller must be informed of any deviation caused through an RA so as not to continue to believe that they remain responsible for separation and continue to issue instructions.

Currently the ATC Controller relies on the flight crew to inform them of any deviation from clearance due to an RA and when the aircraft is clear of conflict. If this information is delayed or not received, the Controller would be unaware and might therefore attempt to resolve the conflict by issuing instructions to the incident aircraft, with the risk that the Pilot might choose to follow the Controller's instructions rather than the TCAS RA and hence increase the risk of collision.

The end of the RA is announced to the aircrew by an aural 'Clear of Conflict' message. Responsibility for separation returns to ATC only when the Controller has acknowledged a report from the flight crew that the aircraft is resuming the current clearance or the Controller acknowledges the report but issues an alternative clearance which is acknowledged by the flight crew.

2.4 RA Downlink Concept

Whenever an RA is generated in the Cockpit, the aircraft's transponder provides detailed information about the nature of the RA, which could be down linked to ATC

[5] Current ICAO regulations imply that all RAs should be reported, although in practice it is only RAs that require a deviation from clearance that are reported. It is understood that ICAO regulations will soon be changed to reflect the current practice.

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;
- All follow-up strengthening RAs will be indicated;
- All follow-up reversal RAs will be indicated;
- All follow-up weakening RAs will not 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 Vertical Speed Limit RAs, information is presented in graphical form indicating that a reduction in vertical speed is required (towards a level off);
- For all other RAs, (Monitor vertical speed, or RAs against multiple intruders) information is presented without a graphical vertical direction symbol;
- There is no indication of ‘Clear of Conflict’; however, the RA indication will be removed from the screen once the aircraft is clear of conflict.

For further detail see Table 1

2.5 Latency

RA Downlink latency is the delay between the RA being generated onboard the aircraft and the RA notification being successfully delivered to, and acknowledged by, the Controller. It is an essential characteristic of the RA downlink concept as the delay should be minimised in order for RA Downlink to provide the maximum possible benefit.

2.6 Data Link Methodology

Following a technical study [1] into RA Downlink it has been proposed that, where available, Mode S is the most suitable technology for downlinking RA reports.

Mode S RA Reports meet all of the implementation criteria with the exception of the worst case en-route latency. In terminal areas, the latency will be significantly reduced due to the faster rotation rates of the TMA radars.

However Mode S RA Reports require a suitable rotating beam radar ground infrastructure. At present this is only planned in Western Europe and is expensive to construct elsewhere.

In areas not covered by a Mode S ground infrastructure, 1090 ES (Extended Squitter) has been proposed as the best method for RA downlink assuming it can be economically implemented as part of an ADS-B system.

2.6.1 Mode S

The ability to downlink ACAS RA information is one of the data link protocols built into the Mode S standard. The downlinked message is referred to as an RA Report and is defined in Annex 10 of the ICAO SARPS [6]. It is a requirement of the ACAS II mandate that all ACAS II equipped aircraft shall be able to transmit this message.

The ability to extract an RA Report over Mode S is part of the functionality of the Mode S ground station and a modern ATC system designed for a Mode S environment should be able to transmit this information to the Controller's CWP.

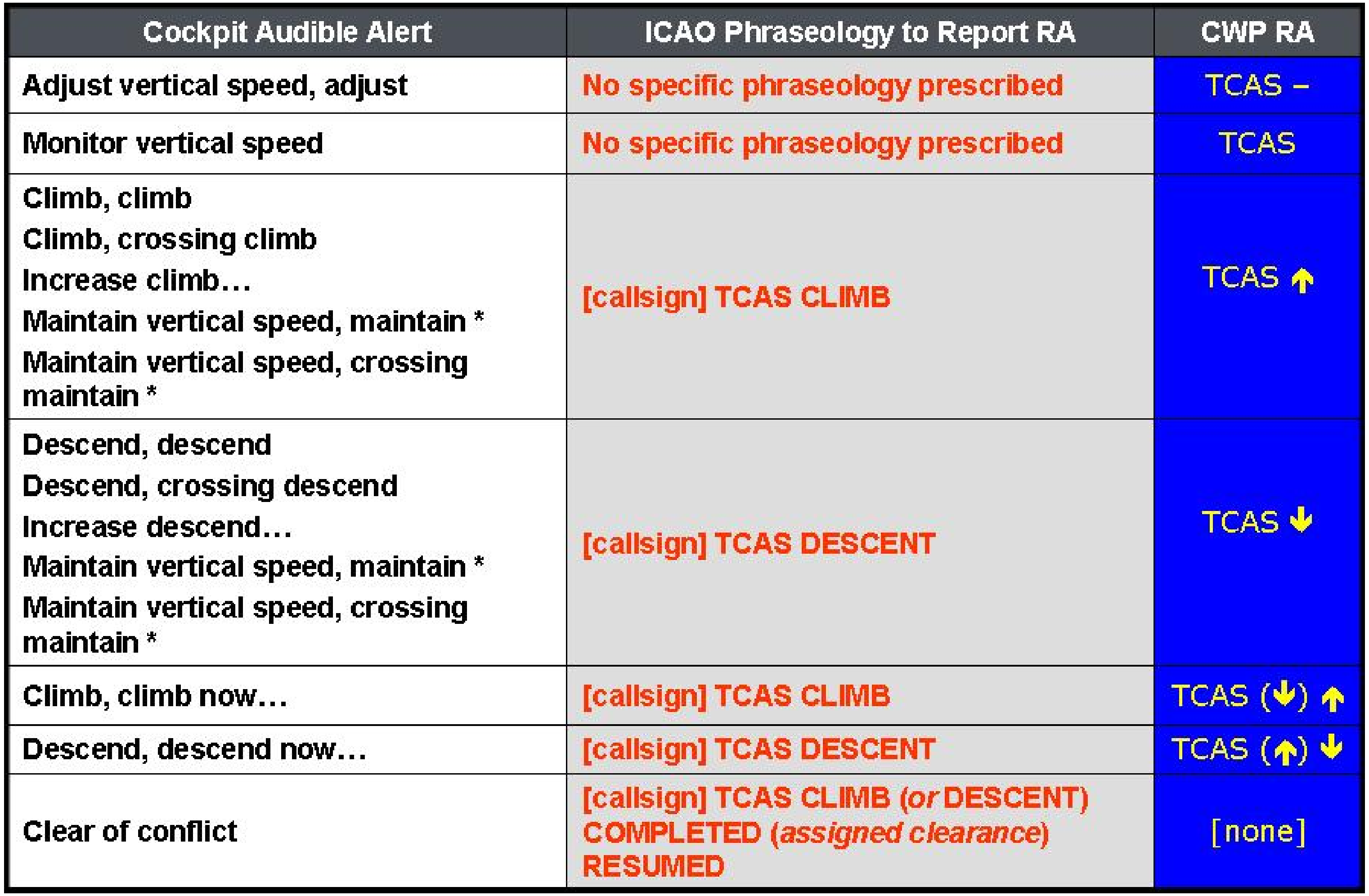
For a number of years RA data has been available for analysis via Mode S, however this is not considered to be a part of the RA Downlink concept as RA data might continue to be collated by this method whether RA Downlink is implemented or not.

2.6.2 1090 ES

1090 Extended Squitter (1090 ES) is an ADS-B technology primarily intended to periodically broadcast aircraft position, velocity and other aircraft parameters. It also has the ability to broadcast event driven data, and it would be using this technique that RAs would be transmitted.

At present, limited ground infrastructure exists for the detection and use of 1090 ES messages. However this is likely to improve with the expected deployment of ADS-B package 1. Hence the equipage of 1090 ES for ADS-B applications might provide an enabler for using 1090 ES to transmit ACAS RAs. In addition, multilateration infrastructure might be suitable to receive RAs transmitted using 1090 ES.

RAs displayed on the CWP have been grouped as follows with the associated phraseology:



Cockpit Audible Alert	ICAO Phraseology to Report RA	CWP RA
Adjust vertical speed, adjust	No specific phraseology prescribed	TCAS –
Monitor vertical speed	No specific phraseology prescribed	TCAS
Climb, climb Climb, crossing climb Increase climb… Maintain vertical speed, maintain * Maintain vertical speed, crossing maintain *	[callsign] TCAS CLIMB	TCAS ↑
Descend, descend Descend, crossing descend Increase descend… Maintain vertical speed, maintain * Maintain vertical speed, crossing maintain *	[callsign] TCAS DESCENT	TCAS ↓
Climb, climb now…	[callsign] TCAS CLIMB	TCAS (↓) ↑
Descend, descend now…	[callsign] TCAS DESCENT	TCAS (↑) ↓
Clear of conflict	[callsign] TCAS CLIMB (*or* DESCENT) COMPLETED (*assigned clearance*) RESUMED	[none]

*This RA can have either upward or downward sense – in real life direction will be shown on the VSI

Table 1 ACAS RAs with Associated Phraseology and Proposed CWP Display

Page intentionally left blank

3. SAFETY MODELS

3.1 Barrier Model

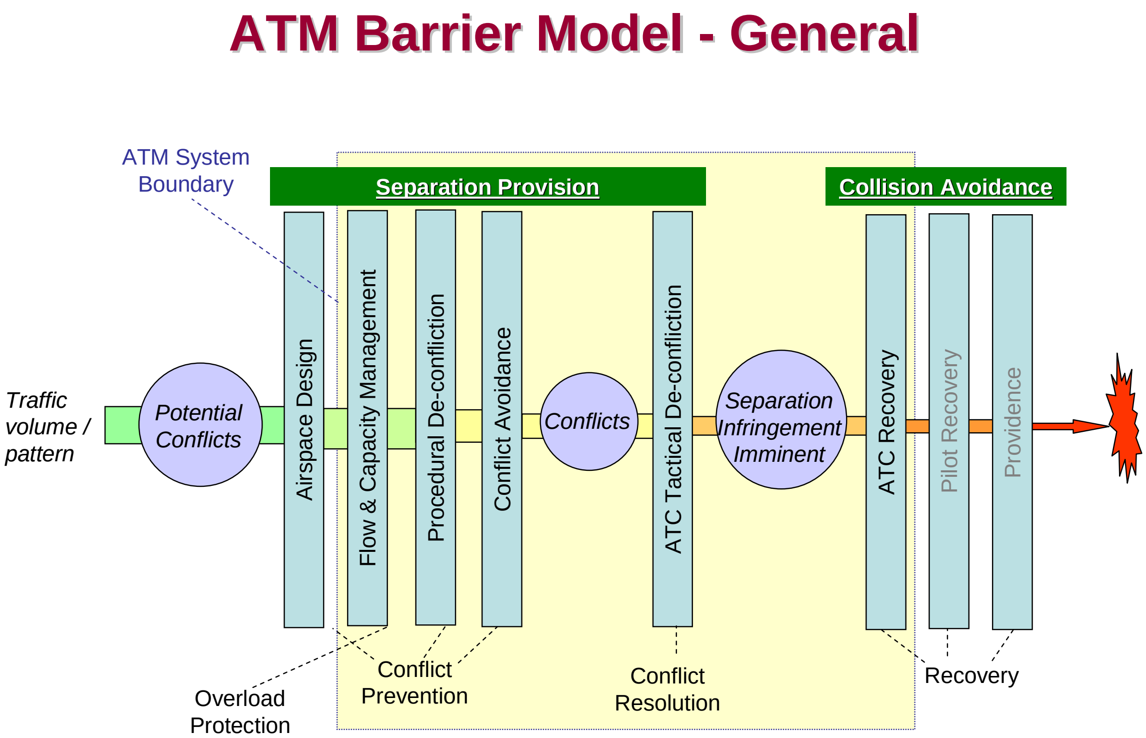


Figure 1. ATM Barrier Model

Figure 1 shows how Air traffic Management (ATM) contributes to the safety of aviation through a series of *barriers*. The barriers operation from left to right in a rough time sequence[6], and each barrier removes a percentage of the potential / actual conflicts; the extent to which they are able to do so depends on the functionality, performance, and integrity of the various elements of the ATM system that underlie each barrier.

Although, for simplicity, it is assumed that the barriers are mutually independent, in reality this is not always the case[7].

The only Separation Assurance barrier of relevance to FARADS, is ATC Tactical De-confliction (representing the role of the Tactical Controller), since it is the only one that operates in real time. The other two barriers that are key to FARADS are related to Collision Avoidance, namely:

- ATC Recovery – this represents “late” intervention by ATC; it uses the same functions as ATC Tactical De-confliction but triggered, typically, by STCA (when implemented as a safety net); and
- Pilot Recovery – intervention by the Pilot triggered, typically, by an ACAS RA.

[6] Under some circumstances, the operation of the barriers can overlap in time.
[7] Such interdependencies are not a problem provided they are captured in subsequent, lower-level analysis.

In the context of FARADS, problems can arise in the current situation when:

- ATC Tactical De-confliction or, more usually ATC Recovery, disrupts the operation of the Pilot Recovery barrier[8]; or
- The (albeit) correct operation of the Pilot Recovery barrier interferes with the provision of Separation to aircraft not directly involved in that recovery.

In simple terms, the aim of the RA Downlink is twofold:

- to facilitate suppression of the ATC Recovery (and ATC Tactical De-confliction) barriers for (and when) aircraft are involved in an ACAS RA manoeuvre; and
- to improve ATC situational awareness in respect of the ATC Tactical De-confliction barrier for those aircraft not involved in the RA situation.

3.2 Functional Model

Figure 2 represents the barriers affected by RA Downlink, in functional terms. The ATC functions shown apply equally to the Tactical De-confliction and ATC Recovery barriers, although in the latter case, the “Tactical Conflict Detection” functions might be supported by STCA.

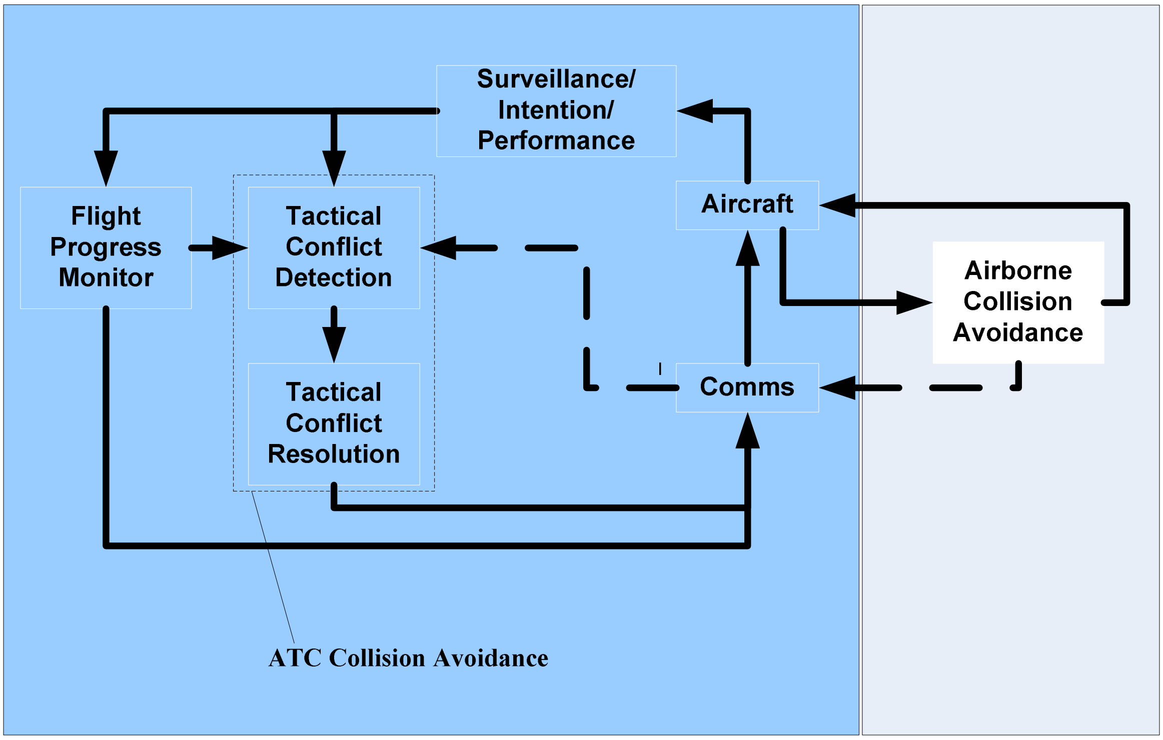

Surveillance/ Intention/ Performance
Flight Progress Monitor
Tactical Conflict Detection
Tactical Conflict Resolution
Aircraft
Comms
Airborne Collision Avoidance
ATC Collision Avoidance

Figure 2. High level Functional Model

The surveillance function of ATC provides controllers with the basic parameters of each flight, including altitude, direction, speed and aircraft type (hence its performance capabilities). By means of flight plan information ATC the Controller will also be aware of each aircraft’s intention in the form of its planned trajectory and destination.

[8] The latter could be considered to have been the case in the Überlingen accident.

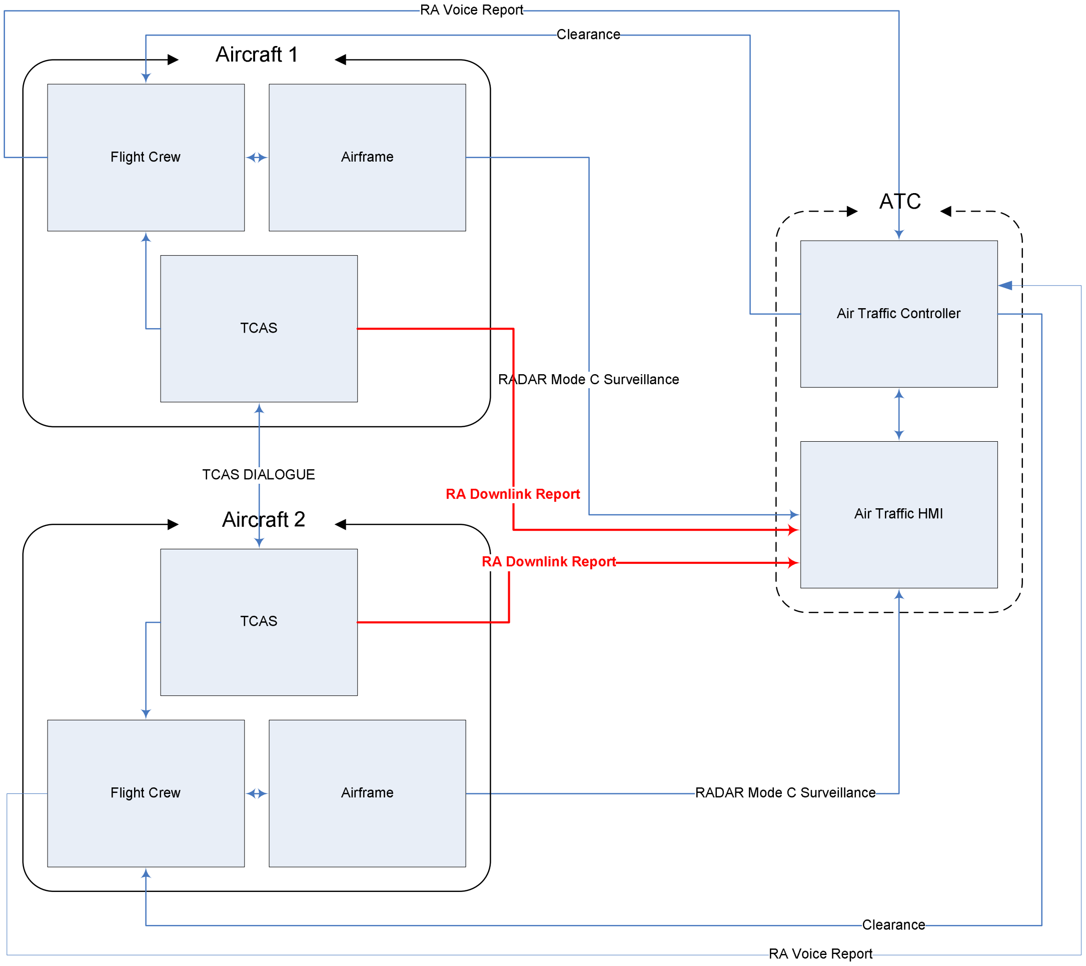
Using this information, flights can be monitored against the clearances they have been given and conflicts detected and resolved (through new clearances, communicated to the Flight Crew) as and when they arise. [9]

Response to a corrective RA by the aircraft immediately and completely overrides any instructions issued by ATC.

The only difference in the functional model for the RA Downlink is the increase in information passing along the dotted line in Figure 2 – ie the likelihood and timeliness of reports, from aircraft to ATC, that aircraft have encountered an RA should be improved, since they would not be dependent on the voice report of the Flight Crew.

3.3 Logical Architecture Model

Figure 3 represents the same situation but in terms of the logical elements of a typical system architecture – in this case, for two TCAS equipped aircraft being controlled by one Controller. This model shows more clearly (in the form of the red lines) the difference between pre- and post- RA Downlink situations and used during the FHA/PSSA workshop to elicit failure modes of the RA Downlink[10].



[9] This summary explanation is considered sufficient to the understanding of RA Downlink.

[10] Similar models were developed and used for the cases of two TCAS equipped aircraft, controlled by two independent air traffic controllers, and one TCAS equipped aircraft and one not, with one Controller.

Figure 3. Logical Architecture Model

3.4 Human Tasks - Pre-RA Downlink

Under the current operational scenario, without RA Downlink, the tasks of the Controller and Flight Crew have been identified (at the highest level) as follows.

3.4.1 Flight Crew Tasks

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

3.4.2 Controller Tasks

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

3.5 Human Tasks - Post-RA Downlink

With the introduction of the RA Downlink the tasks of both the flight crew and the Controller are unchanged, at the high level outlined above[11]. The purpose of the downlink is not to alter RA procedures, but rather to reinforce them by providing the Controller with a timely and reliable indication of an RA to help prevent unintentional intervention in the RA event and to improve the Controller's situational awareness in respect of the aircraft for which he continues to have responsibility for separation.

[11] On a lower level, however, tasks can differ between the pre- and the post-RA downlink situation. For instance, "receive report" refers to the processing of the pilot report in the pre-RA downlink situation, and to the processing of pilot report and/or RA downlink in the post-RA downlink situation. A Cognitive Task Analysis (CTA) was carried out in order to identify the differences in controller tasks between the pre- and the post-RA downlink situation on a detailed level [7].

4. FHA/PSSA WORKSHOP

Following consultation with EUROCONTROL it was agreed that the RA Downlink FHA/PSSA would be a comparative assessment of the risks pre- and post-RA Downlink implementation, aimed at showing the extent and degree to which the risk of an accident could be reduced by the implementation of an adequately specified and implemented RA Downlink.

This approach meant that the FHA/PSSA had in effect to be done for both the current and RA Downlink situations; on the other hand the advantage that the two assessments had to cover only those elements of the ATM / aircraft system that would actually be affected by the introduction of RA Downlink.

4.1 Overview

The development of the RA Downlink Safety Case follows the EUROCONTROL Safety Assessment Methodology (SAM) [11] in principle but adopting a relative safety assessment comprising:

- Risk assessment from *success* and *failure viewpoints*;
- Safety requirements derivation.

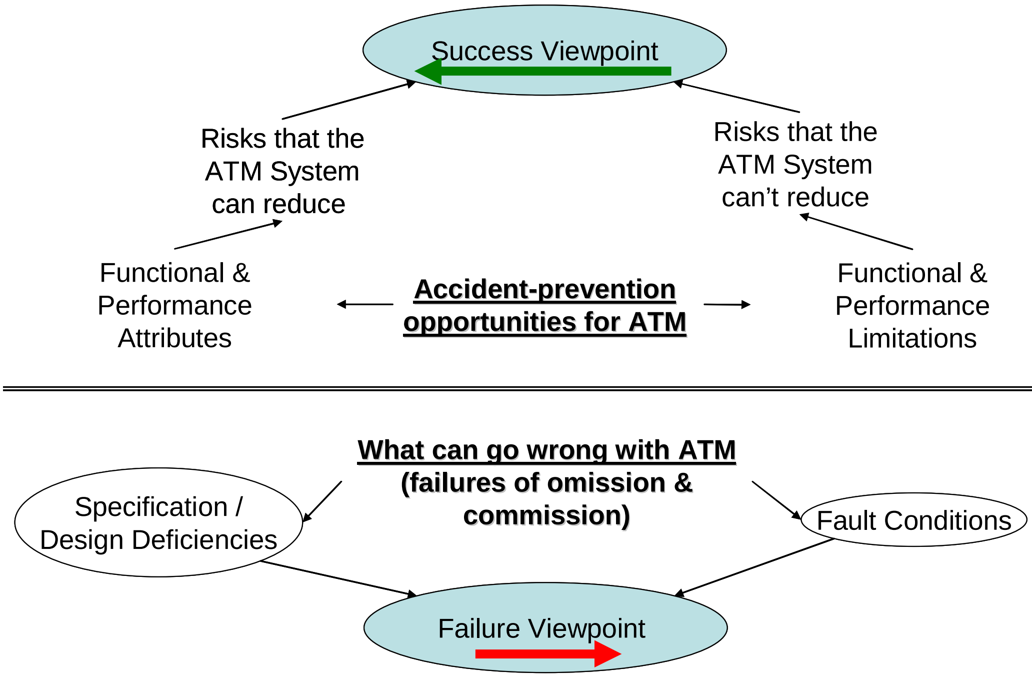

Success Viewpoint
Risks that the ATM System can reduce
Risks that the ATM System can't reduce
Functional & Performance Attributes
Accident-prevention opportunities for ATM
Functional & Performance Limitations
What can go wrong with ATM (failures of omission & commission)
Specification / Design Deficiencies
Fault Conditions
Failure Viewpoint

Figure 4. Success and Failure Viewpoints

4.2 Success and Failure Viewpoints

The Success Viewpoint compares the risks associated with the pre- and post-implementation situations in order to assess the degree and extent to which the ATM system (in this case the RA Downlink) can (and can't) reduce risks, and to identify to the functionality and performance attributes of the RA Downlink that could provide such risk reduction.

The Failure Viewpoint addresses what can go wrong with RA Downlink, and therefore cause some increase in risk, due either to deficiencies in the specification / design or to fault conditions (including human error) occurring during operation of the RA Downlink.

4.3 Safety Requirements Specification

4.3.1 FHA / PSSA

The ultimate aim of the FHA / PSSA is to derive safety requirements for the RA Downlink which, on balance, would result in a substantial net reduction in risk compared with the pre-RA Downlink situation.

Figure 5 shows how the above Success and Failure approach, together with the CTA and HRA, are used to derive and validate the safety requirements.

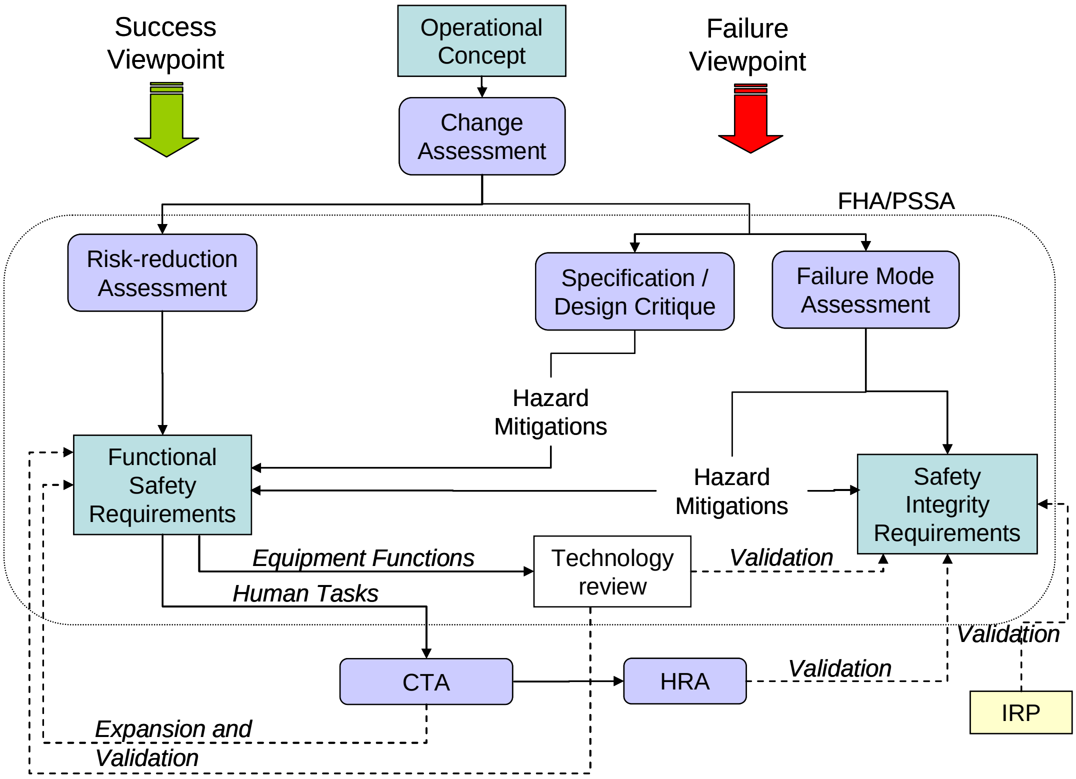


Figure 5. Safety Requirements Specification Process

Note: This document covers the area marked as FHA / PSSA

The Functional Safety Requirements (ie covering functionality and performance, for equipment, people and procedures) are derived from three sources:

- initially, from the need to capture the risk-reduction potential of the RA Downlink (Success Viewpoint);
- further, to correct any deficiencies found in the specification / design of the RA Downlink concept (first stage of the Failure Viewpoint);
- finally, to capture any mitigations of the potential RA Downlink fault conditions, identified in the second stage of the Failure Viewpoint.

The Safety Integrity Requirements (for equipment, people and procedures) are derived from the need to limit the frequency of occurrence of hazardous faults within the RA Downlink system such that the risk associated with these faults is small compared with the risk-reduction of the RA Downlink (as identified in the Success Viewpoint). In general, faults of the form of detected loss of the RA Downlink merely undermine its risk-reducing effectiveness, whereas faults of the form of credible corruption of the RA Downlink could actually introduce new risk (ie risk that was not present before the RA Downlink was implemented).

4.3.2 Cognitive Task Analysis

Cognitive Task Analysis (CTA) is a relatively recent outgrowth of general task analysis methods (a family of techniques used to describe and analyse operator performance within a human-machine system). CTA refers to a group of techniques used to capture and represent the cognitive elements underlying performance of a given task. CTA is particularly suitable for the ATC domain as most controller tasks are cognitive in nature (eg monitoring, interpreting, analysing, planning, diagnosing, deciding, etc).

The aim of the CTA study was to identify the cognitive elements underlying performance in the RA scenarios, and to identify potential error mechanisms. A high-level task description, developed in the FHA / PSSA, served as the basis for the subsequent CTA. Data for the CTA was collected during a half-day session (and follow-up teleconference) between one researcher and a licensed air traffic Controller and then analysed; the results of that analysis was then used to amplify and validate the Functional Safety Requirements and as the basis for the Human Reliability Analysis.

4.3.3 Human Reliability Assessment

Human Reliability Assessment (HRA) 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.

HRA is a hybrid discipline incorporating a technical perspective (engineering aspects of systems) and human factors perspective (psychological basis of human error). The combination of these perspectives provide a foundation for assessing a total risk-picture of a system and to determine which factors impose most risk (human or technical). The three functions of HRA are thus as follows (see Kirwan, 1994 [8]):

- Human error identification: What errors can occur?
- Human error quantification: How probable is it that the errors occur?

- Human error reduction: How can the probability that errors occur be reduced?

Within the FARADS Study, HRA is being used as the means to link the information in the Cognitive Task Analysis (CTA) performed in an earlier report to the safety analysis being performed in the PSSA – in particular, to validate the Safety Integrity Requirements derived for the human elements of the RA Downlink system.

The HRA work will be focused upon the first function of HRA, and will also start to consider the second function, as outlined above. The CTA provides the basic psychological knowledge and principles underpinning how, in the event of an ACAS RA event, the ATCO would perform his/her tasks, with and without the RA Downlink. Therefore, from the information in the CTA, the 'Human Factors' influencing Human Reliability (eg Controller reaction times, types of detection failures, interpretation errors, potential Controller ‘workload issues’) can start to be identified. Subject to sufficient reliable data becoming available, the human factors analyses will be used to validate any integrity requirements placed on the human.

4.4 Operational Context

The above viewpoints were considered in the context of the following scenarios:

- 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

4.5 Assumptions

No high-level Assumptions were necessary in order for the safety analysis to proceed.[12]

[12] The assumption that current (pre-RA Downlink) operations are tolerably safe may be necessary to support the subsequent Safety Argument but is not a pre-cursor for the safey analysis herein.

5. RESULTS: SUCCESS VIEWPOINT

5.1 Introduction

This section presents the results of applying the process in section 4 from a Success Viewpoint, as follows:

- paragraph 5.2 discuses, in a general qualitative sense, the various opportunities for the introduction of RA Downlink to reduce the risk of an accident and/or serious risk-bearing incident due to adverse interactions between ACAS-induced collision-avoidance events and the separation-assurance and recovery functions of ATC.
- paragraph 5.3 uses Event Tree Analysis to put these general risk-reduction opportunities into the context of specific RA scenarios, in order to understand, more quantitatively, how they contribute to risk reduction.
- paragraph 5.4 derives the Functional Safety Requirements arising from the above.

5.2 Opportunities to Reduce Risk

The following positive advantages exist with the implementation of RA Downlink;

5.2.1 Preventing a Controller from Issuing Clearances to RA Incident Aircraft

ICAO Doc 4444 PANS-RAC, paragraph 15.6.3.2, states '*When a Pilot reports a manoeuvre induced by an ACAS RA, the Controller shall not attempt to modify the aircraft flight path*…' However Pilot reports are often late, missing or incorrect / incomplete, and in those circumstances – ie the Controller being unaware of the RA event - he/she might attempt to issue clearances to the aircraft involved, especially if there is an imminent or actual infringement of separation that does not appear to have been resolved.

One of the key aims of RA Downlink is to help to prevent the Controller from inadvertently issuing clearances once an aircraft is involved in an RA. By providing a visual display (SR_06) to the Controller whenever aircraft are involved in an RA (see SR_01, in paragraph 5.4), and reinforcing this aspect of Controller training, it should be clear that, for the duration of the RA, the Controller should not be attempting to modify the flight path of the incident aircraft – ie the aircraft that are directly involved in the RA (SR_03).

As any instructed direction of the RA is also displayed (SR_02) the Controller will have improved situational awareness and it is even less likely that the Controller would, in contravention of ICAO requirements, attempt to give a clearance to the aircraft involved (especially a clearance that was in a contrary sense to that of the RA).

5.2.2 Timely and Reliable RA Report

A recent RA Downlink Latency Study [12] suggests that, in the present situation, a Controller will typically be made aware (by Pilot RT reports) of 85% of RAs about 30seconds after the RA has occurred, and will be completely unaware of the remaining 15% of occurrences.

Recommendation: An investigation be conducted into the reasons for non-compliance by flight crew with current requirements for RT reporting of RAs to ATC.[13]

The Latency Study suggests that, if RA Downlink were implemented, the Controller would be aware of 95% of RAs within 8 seconds. Therefore, as RAs are usually generated between 15 seconds and 35 seconds before the CPA, RA Downlink could provide reliable RA reports in sufficient time (SR_04) to prevent the Controller from issuing instructions that might interfere with the execution of the RA collision-avoidance manoeuvre(s).

5.2.3 Structured RA Report

ICAO Doc. 4444 provides a summary of the phraseology that should be used by pilots to report an RA; however examples were presented at the FHA/PSSA workshop in which pilots had not used the standard terminology. There were also examples of omissions and errors in the voice reports which confused the controllers.

RA Downlink would provide the Controller with a structured display containing only information pertinent to the event, equivalent to that displayed to the Pilot. Automation of the reporting process by RA Downlink should ensure that correct and consistent information is produced (SR_05) and presented to the Controller in an intuitive manner (SR_06).

5.2.4 Reduction in RT

Evidence presented at the FHA/PSSA workshop showed that pilot RT reports are not always structured as prescribed by ICAO, causing ATC confusion and absorbing RT time by seeking clarification, although this should be addressed in training (SR_23).

A structured RA Downlink report (as already captured by SR_05 and SR_06) should negate the need for the Controller to question or clarify Pilot voice reports, thereby eliminating this source of unnecessary RT transmissions.

However, the importance of an early RT report must not be underestimated, as the voice report will alert surrounding traffic on the same frequency of the event and therefore improves situational awareness for all Pilots in the sector as well as the Controller.

5.2.5 Incident Aircraft Identified

Currently the only means of positively alerting controllers to an RA event is via Pilot voice reports once they have deviated, or intend to deviate, from clearance. However this information might be delayed, incoherent / incomplete or not transmitted by the flight crews of one or both aircraft in an RA encounter, due to increased Pilot workload arising from the RA or from frequency congestion.

The implementation of RA Downlink would indicate to the Controller each aircraft that is involved in an RA event (SR_07).

In the event that there is an encounter with a non-ACAS operational / equipped aircraft, the downlink from the equipped aircraft will include the intruder's Mode S address, enabling the non-equipped aircraft to be shown on the Controller's display

[13] The need to address this problem of RA voice reporting becomes even more evident from the discussions in paragraphs 5.2.5 and 6.2.6.

(SR_08). Where the Mode S address is unavailable for the non-ACAS equipped aircraft, some automated ATM systems might be able to perform a correlation to indicate the intruder to the Controller (SR_09).

Simultaneous identification of all aircraft involved in an RA, whether ACAS equipped or not, should reduce Controller workload and could prevent the Controller from issuing clearances to the incident aircraft.

5.2.6 RA Visible for Duration of Event

In the pre-RA-Downlink scenario the Controller must not only correctly identify, from voice reports, all aircraft involved in an RA event, but also remember that clearances must not be given to the affected aircraft until a 'Clear of Conflict' report is received. This task might be complicated by erroneous or incomplete Pilot voice reports, and could increase Controller workload.

With RA Downlink, the Controller will be aware that an RA is active for its whole duration (SR_10). This will reduce the likelihood of a Controller missing the initial RA report or being distracted during the report.

5.2.7 RA Revisions Displayed to the Controller

There are currently no requirements for pilots to report any change to the sense of an RA. It is likely that in practice the increased workload of an RA encounter would prevent the Pilot from being able to provide details of any revisions to the RA.

In this situation RA Downlink would again improve Controller situational awareness as any RA reversals or strengthening of RAs would be displayed (as already captured in SR_02, thereby allowing them to assess the impact of the revision on the traffic for which they retain separation responsibility.

5.2.8 'Clear of Conflict' could be denoted by disappearance of RA Downlink display

Under current ICAO regulations the Controller is prohibited from attempting to modify the flight path of an aircraft subject to an RA *'…until the Pilot reports returning to the terms of the current air traffic control instruction or clearance…'*. As discussed above with regard to the reporting of an RA event, the Clear of Conflict report might be late or missing.

With RA Downlink, the end of an RA event would be denoted by the removal of the RA display from the Controller's HMI (see SR_10). Although this might not be a signal to the Controller to resume issuing clearances immediately, it will make the Controller aware that the aircraft should be returning to the original clearance and that he/she should anticipate a Clear of Conflict report. By anticipating the Clear of Conflict report the Controller will be better prepared to regain responsibility for separation and can prepare a revised clearance, if required, to give once the Clear of Conflict is received.

In the event that a Clear of Conflict voice report is not made by the Pilots involved in the RA the Controller shall assume that he/she might issue clearances a short period - eg 20 seconds, after the RA display is cleared from the radar display (SR_11).

Recommendation: Work be carried out 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.

5.2.9 Summary

The discussions above provide qualitative evidence that the implementation of RA Downlink could provide many advantages over current operations.

5.3 Event Tree Analysis

5.3.1 Context

The following hazards were identified as applicable to RA Downlink by the participants of the FHA/PSSA:

Hazard H1:	Two aircraft encounter a genuine RA
Hazard H2:	Multiple aircraft encounter a genuine RA
Hazard H3:	Aircraft encounters an ‘unnecessary’ RA
Hazard H4:	Aircraft encounters a false RA
Hazard H5:	Aircraft does not react to an RA

It was decided that the most representative basis (and starting point) for analysing the Success Viewpoint would be Hazard H1 for Operational Scenario A – ie two ACAS-equipped aircraft in communication with the same Controller (see paragraph 4.4 above). The analysis would then consider whether the RA Downlink Concept would still deliver a safety benefit for the other (less typical) Hazards / Operational Scenarios.

5.3.2 Method of Analysis

The event trees were elicited through discussion between the various Subject Matter Experts (SMEs) present at the FHA/PSSA workshop. The probabilities that were attributed to each branch of the event tree were estimated by the SMEs for the Pre-RA Downlink case, and then a comparative figure was derived for the Post RA Downlink scenario.

It must therefore be noted that the figures presented have not been validated with operational data, but are rather a representation of specialist opinion regarding the benefit (or disbenefit) of RA Downlink against the current operational scenario.

5.3.3 Hazard 1 / Operational Scenario A

The Event Trees for Hazard 1 / Operational Scenario A, addressing both the pre- and post-implementation of RA Downlink, are presented in Appendix E. They show the possible mitigations, which determine whether the Hazard would lead to a desired outcome or to a state of *degraded collision avoidance*[14].

Clearly, the introduction of RA Downlink can have no influence on frequency with which the Hazard occurs in the first place; therefore, to simplify the comparison between the Event Trees, this value is set to unity for each case.

[14] It was not practicable to develop the Event Trees to the point that an accident actually occurred or was avoided (as the final barrier in the ATM barrier model is providence, which it was not practicable (or necessary) to model for this study) – therefore, it was decided to limit the outcomes to the effect that the Hazard might have on the operation of an ACAS-induced collision-avoidance manoeuvre.

The estimated probability of failure of each mitigation[15], for the pre- and post-implementation of RA Downlink situations, as assessed by the Workshop, shows only one difference, as follows:

- for the pre-implementation situation, it was estimated that the timely and correct reporting of RAs (by voice link) occurs on only 50% of occasions;
- for the post-implementation situation, it was estimated that the timely and correct reporting of RAs (by RA Downlink or voice link) would occur on about 95% of occasions.

However, during the post-workshop analysis[16], it was realised that RA Downlink would also have a positive influence on the success of the final mitigation, provided it is reworded from "Pilot reports resume clearance'" to a more general form of "ATC resumes [responsibility for] separation at the end of the RA". Indeed, one of the qualitative benefits claimed for RA Downlink is that the Controller can see when the RA symbol has disappeared from the screen, from which he could deduce that the RA event is finished. For the purpose of the post-workshop analysis, it was assumed that the success rate for the mitigation would increase from 0.8 (pre-RA Downlink) to 0.95 (with RA Downlink)[17].

The Event Trees, as presented, are a bit coarse in terms of outcome and do not necessarily highlight the full benefits of RA Downlink. Therefore, in the table below, the results are presented in terms of 11 possible outcomes (instead of the three shown in Appendix E) – a "✓"indicates that the mitigation (indicated by the column header[18]) is successful and a "✗"indicates that the mitigation has failed. Where the outcome is not dependent on whether a particular mitigation has succeeded or failed, this is indicated by "[either]"; where a particular mitigation does not apply, this is also shown.

The 11 outcomes are shown generally in descending order of desirability, based on three qualitative criteria:

- the most important consideration is that the RA is executed properly (a "✓" in columns A and D);
- next, ATC should resume responsibility for separation at the end of the RA (a "✓" in column E); and
- thirdly, that ATC is made aware of the existence of the RA, so that the Controller can most effectively continue his/her responsibility for aircraft that are not directly affected by the RA.

[15] The convention used in the Event Trees is that the mitigations are worded such that "success" is always the desired outcome but the probabilities (Q values under each column header) show the probability that the mitigation will NOT be successful.

[16] The post-workshop analysis is not reflected in the Event Tree Analysis at Appendix E – the values used in the latter are those captured at the Workshop itself.

[17] The results were found to be not particularly sensitive to this assumption. For a mitigation success probability of only 0.8 reduces the 58% outcome probability to 49%; and increasing it to the maximum of 1.0 increases the same outcome probability, but only to 62%.

[18] The 5 mitigations shown in the Table are directly equivalent to, but are a clarification of, those in the Event Trees

	Mitigations						
	A	B	C	D	E		
Outcome	Pilot reacts correctly to original RA	ATC is aware of RA	ATC does not attempt to intervene in RA	Pilot continues to follow RA	ATC resumes separation at end of RA	Pre-RA Downlink Probability	Post-RA Downlink Probability
1	✓	✓	✓	✓	✓	26%	58%
2	✓	✓	✗	✓	✓	2%	5%
3	✓	✗	✓	✓	✓	7%	1%
4	✓	✗	✗	✓	✓	17%	2%
5	✓	✓	✓	✓	✗	6%	3%
6	✓	✓	✗	✓	✗	1%	0%
7	✓	✗	✓	✓	✗	2%	0%
8	✓	✗	✗	✓	✗	4%	0%
9	✓	✓	[either]	✗	[N/a]	15%	10%
10	✗	✓	[either]	✗	[N/a]	10%	19%
11	✗	✗	[either]	✗	[N/a]	10%	1%
						100%	100%

The final two columns of the table compare the probability of each of the 11 outcomes (given that Hazard 1 has occurred) for the current, pre-RA Downlink situation with the hypothetical situation post RA Downlink implementation.

Overall, the results show that:

1. RA Downlink provides a substantial improvement (from 28% to 63%) in the aggregate probability of the two most desired outcomes.
2. The aggregate probability of the next six, less desirable (but still probably acceptable outcomes) is actually reduced by RA Downlink – this, of course, is a consequence of the improvement noted in point #1.
3. The aggregate probability of the three unacceptable outcomes – ie those for which the pilot does not continue to follow the RA – is reduced from 35% to 30%.

It appears, therefore, that the main benefit of RA Downlink comes from improved Controller situational awareness – ie the Controller is aware of the RA - not from improved collision avoidance.

Furthermore, if we ignore the situational awareness benefit, by aggregating the probabilities for outcomes 1 to 4, then the probability of a desired outcome increases from 52% (pre-RA Downlink) to 69%. This is an indication of the next most significant benefit of RA Downlink – ie improved probability that the controller will know when to resume responsibility for separation after the RA.

Finally, the reduction in the risk of collision-avoidance failure is marginal, and probably within the bound of uncertainty in the input data – ie is not statistically significant.

The Safety Summary Report for FARADS discusses how these findings compare with the results of the FARADS real-time simulations.

5.3.4 Other Hazards and Operational Scenarios

The benefits of RA Downlink that arise from the various operational scenarios and hazards studied have been covered within the analysis of the two aircraft, single Controller scenario in Section 5.2.

5.4 Summary of Safety Requirements arising from Success Viewpoint

The table below brings together the results of the qualitative assessment (paragraph 5.2) and Event Tree Analysis (paragraph 5.3) in the form of the initial set of Functional Safety Requirements for RA Downlink.

Ref	Functional Safety Requirement	Origins
SR_01	RAs shall be downlinked and displayed to the Controller.	Paragraph 5.2.1 herein
SR_02	The RA Downlink display shall show the direction of the RA, including any revisions (except follow-on weakening RAs), as displayed by TCAS to the Pilot.	Paragraph 5.2.1 herein
SR_03	Training shall reinforce that Controllers shall not issue clearances to aircraft involved in an RA.	Paragraph 5.2.1, 6.2.2, 6.2.13, 7.1.5 herein
SR_04	The downlinked RA shall be displayed to the Controller within 10 seconds of the RA being activated in the Cockpit.	Paragraph 5.2.2, 6.2.7 herein
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	Paragraph 5.2.3 herein
SR_06	The RA Downlink display shall be intuitive for Controller comprehension	Paragraph 5.2.1, 5.2.3, 5.2.7, 6.2.4 herein
SR_07	The RA Downlink tag with vertical rate symbology shall only be associated with the aircraft reporting the RA.	Paragraph 5.2.5 herein
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	Paragraph 5.2.5 herein
SR_09	Where the Mode S address of a non-ACAS intruder aircraft is not available, the ATM system shall, if possible, perform a correlation in order to indicate the intruder to the Controller	Paragraph 5.2.5 herein
SR_10	The RA Downlink display shall remain active on the Controllers HMI until the aircraft is 'Clear of Conflict'	Paragraph 5.2.6, 5.2.8 herein

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[19] after the RA annotation has been removed from the RA Downlink Display.	Paragraph 5.2.8 herein

[19] But see Recommendation #1, regarding the 20second time interval

6. RESULTS: FAILURE VIEWPOINT - SPECIFICATION / DESIGN DEFICIENCIES

6.1 Introduction

Having concluded, as shown in the previous section, that RA Downlink has the potential to deliver some safety benefits for the various Hazards and Operational Scenarios, the Workshop then considered what other circumstances (excluding faults within the RA Downlink system[20]) might cause the RA Downlink Concept to fail, by either:

- undermining the safety benefits; or
- introducing new risks that didn't exist prior to RA Downlink.

These issues are addressed in paragraphs 6.2, and the additional Functional Safety Requirements arising from them are collated in paragraph 6.3

6.2 Issues of Concern

6.2.1 Responsibility for Separation

Paragraph 15.6.3.2 of PANS-ATM [5] states that ''*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*

Paragraph 15.6.3.3 of PANS-ATM [5] states that '*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*'.

The implementation of RA Downlink could introduce ambiguity regarding separation responsibility as, under the current regulations, the Controller would remain responsible for separation until a [voice] report is provided by the Pilot, even though the downlink will have alerted the Controller to the activation of the RA (SR_12).

Furthermore, if the appearance of an RA alert does not signify to the Controller that they are (temporarily) not responsible for separation and a voice report is not forthcoming, the Controller might focus on the event and monitor the incident aircraft for evidence of a deviation from clearance. In this way, the introduction of RA Downlink can yield an additional task for the controller[21]. This has the potential to distract the controller from their other separation responsibilities in the sector

It is unclear how the Controller would react to a situation where they know that an aircraft is subject to an RA yet they remain responsible for separation. It could be assumed that the presence of the RA Downlink will act as a signal to the Controller not to attempt to manoeuvre the incident aircraft (to be confirmed by CTA / HRA), even though responsibility for separation legally seems to remain with ATC if there is no deviation from clearance.

[20] Fault conditions are considered in Section 7 herein.

[21] Additional Controller tasks that can arise from the introduction of RA Downlink are discussed in Paragraph 6.2.4 herein.

Similarly, once the RA Downlink display is cleared from the Controller's screen it might be assumed that the aircraft is clear of the conflict; however the responsibility for separation, and hence the ability to issue clearances, can only currently be resumed by the Controller once a 'Clear of Conflict' report is provided by the flight crew, in accordance with paragraph 15.6.3.3 of PANS-ATM [5], as follows:

> *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.*

If a Clear of Conflict report is not received, the Controller might not resume responsibility for separation as soon as is possible. Therefore, if the voice report is not forthcoming, the Controller should have the ability to resume issuing clearances after a short time period so long as it is clear the aircraft are diverging. A delay of 20 seconds after the RA Downlink display has cleared is recommended to ensure that it will be obvious to the Controller that the aircraft have actually diverged and to allow the Pilot sufficient time to provide a Clear of Conflict report. (SR_13)

The temporary suspension of the Controller's responsibility for separation could be indicated by the appearance of the RA downlink, and responsibility resumed once the display is cleared. However this would present an issue regarding responsibility for separation when an RA does not require a deviation from clearance as there is no method of clearly and reliably differentiating between RAs that do and do not require a deviation from clearance.

6.2.2 Procedures Concerning RAs that do not require a Deviation from Clearance

In the present situation it is widely believed that only RAs that require a departure from clearance must be reported to ATC. However the current ICAO regulations state that 'in the event of an RA, pilots shall: 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'.

The statement does not differentiate between RAs that do or do not require a deviation from clearance, but does say that the RA report should include the direction of any deviation from clearance. However, ICAO Doc 4444 provides no phraseology for reporting an RA that does not require a deviation from clearance.

It is understood that ICAO procedures will be changed so that only RAs that require a deviation from clearance must be reported. This will make the RA Downlink contradictory to Doc. 4444 as it is proposed that RA Downlink will present all initial RAs to the Controller. Although corrective and preventive RAs as issued by ACAS might be distinguished by the RA Downlink alert symbol, without the ATM software knowing the aircraft's clearance there can be no method of indicating to the Controller whether the RA requires a deviation from clearance, although the Controllers might be able to determine this for themselves.

Recommendation: Further work be carried out 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.

In the current scenario, if a Pilot does not report an RA, the Controller will believe that they remain responsible for separation. If the Controller subsequently issues an instruction contrary to the RA, the Pilot is required to report ‘Unable TCAS’, although the Pilot might accept clearances that are not prohibited by the RA. This enables controllers in busy airspace (eg terminal) to continue directing the aircraft so long as the instructions do not create a conflict with the RA.

If it is assumed that the RA Downlink display will be a signal to the Controller that they should not be attempting to communicate with the incident aircraft (SR_03), as is the aim of the downlink, the Controller will be unable to issue clearances to the flight crew despite the fact that the RA might not require a deviation from clearance.

The result of this might be that, in areas equipped with RA Downlink, the Controller loses the ability to issue instructions to maintain an orderly traffic flow for the duration of the RA, assuming that pilots are not required to report RAs that do not require a deviation from clearance.

For example, an aircraft in a stack might receive a preventive RA caused by an aircraft descending to a level above the subject a/c at a high rate. It is assumed the Pilot is not required to report the RA.

In areas not equipped with RA Downlink the Controller can issue an instruction to the subject a/c to descend as they would be unaware of the RA. The instruction is not contrary to the RA therefore the Pilot can accept the clearance.

In areas with RA Downlink the Controller will be made aware of the RA by the downlink. If required not to communicate with aircraft annotated with the RA Downlink symbol the Controller loses the ability to issue an instruction to descend, which might also affect the Controller’s overall traffic management plan.

The introduction of RA Downlink could therefore create a situation where ATC capabilities differ depending on whether the area is RA Downlink enabled.

The question arises as to whether it would be preferable for the Controller not to communicate with the flight crews of aircraft involved in any RA, which might reduce the probability of pilots being distracted from flying the RA or becoming confused and responding slowly, or whether it would be more desirable for the Controller to maintain authority in situations where the RA does not require a deviation from clearance, as in the example given above. If it were a preventive RA, how would the status quo be maintained?

Recommendation: A study into the operation of RA Downlink in specific types of airspace / sectors be conducted to determine suitability for implementation in those areas.

6.2.3 System Complexity

The introduction of RA Downlink will increase the ATM system complexity which will increase the number of possible errors. If two methods for reporting RAs are adopted, ie by voice and by RA Downlink, there are likely to be problems caused by conflicting reports, or confusion caused reports received through one channel only (SR_15).

The current system is acceptably safe so long as Flight Crews adhere to the procedures laid down by ICAO. It is understood however that the requirements are not always met.

Recommendation: An investigation should be conducted to determine the reasons for non-compliance of flight crews with ICAO regulations and how the voice reporting of manoeuvres that require a deviation from clearance can be made more reliable.

6.2.4 Controller Distraction

The experience of controllers at the FHA/PSSA workshop was that RAs were a rare event, although experience will differ depending on the type of airspace that is controlled. Due to their rarity, when an RA is downlinked the Controller might be presented with an infrequent display representing a failure of separation provision. To ensure that the Controller can analyse the display and act appropriately the RA symbology should be intuitive (SR_06) and recurrent training should be undertaken so that the RA Downlink tags are familiar (SR_14).

The fact that RAs do not occur often and that a potential collision is a serious event might cause the Controller to focus on the conflict at the expense of maintaining situational awareness throughout the sector, especially if the conflict was not identified by the Controller until activation of the RA. Recurrent controller training should be undertaken to ensure that the RA Downlink is familiar and that the associated procedures are known and practiced. (SR_14)

RA Downlink will distract the Controller by causing them to focus on one part of the screen at the expense of other traffic, thereby breaking the rotational scan that Controllers are trained to perform and possibly distracting them from performing other tasks. RA Downlink might also have an emotional effect on Controllers, especially if they can see that Pilots are not doing as ACAS is instructing. This might cause a loss of trust in ACAS and undermine Controller confidence in the system. These are some of the probable effects which are to be discussed in the HRA, CTA and further studies.

6.2.5 Additional Controller Task: Seeking Confirmatory Evidence for the RA

In the case where the RA Downlink is received before the pilot report, the Controller is likely to seek confirmatory evidence of an RA event, for instance, by monitoring whether the aircraft adheres to the RA as displayed. This task, which is not necessary in the pre-RA Downlink situation, requires attention and thus potentially distracts the controller from monitoring other traffic in the sector. As soon as the pilot report is received, the Controller task in the post-RA Downlink situation is no different from the controller task in the pre-RA Downlink situation (SR_14).

6.2.6 Conflicting Voice and Downlink Reports

An incorrect direction of deviation report from a Pilot in the pre RA downlink scenario will have no immediate effect as the Controller should have no reason to doubt the Pilot report. If the direction of deviation is similar to that reported by the second aircraft, the Controller might be led to believe that ACAS is degrading separation. Cognitive tunnelling might result as the Controller looks for evidence of the two aircraft diverging, or if they think the situation warrants intervention they might, although trained not to, attempt to issue clearances in order to resolve the conflict. The danger is that, without knowing which aircraft is reporting the true direction of deviation, the Controller cannot know if his/her instructions are consistent with the RA - hence Controllers are required to take a “hands-off” approach once an RA is reported.

If RA Downlink is implemented, a direction of deviation voice report that conflicts with the downlink should be obvious to the Controller. Again this could cause cognitive tunnelling as the Controller might then monitor the vertical rates of the aircraft involved to determine whether the Pilot report or the RA Downlink is in error and to ensure that the conflict is successfully resolved.

If the RA Downlink and Voice report are different, ATC might have to assume that the RA Downlink is correct and that the flight crew have made an error but will still manoeuvre the aircraft correctly (SR_15).

However, if the conflicting direction of deviation is due to a reversed RA instruction, the RA Downlink cursor will present this to the Controller who should then be satisfied that the flight crew are complying with the RA and can divert their attention to other tasks. There is no indication what the Controller could do if not satisfied with the situation, although the Controller’s workload will increase and they might be distracted from other events in the sector.

Recommendation: A further study be carried out 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.

Successful RA Downlink operations experienced on the job and through RA Downlink training should improve Controller trust in the downlink, thereby allowing the Controller to become increasingly confident that the RA Downlink is reliably indicating that ACAS is resolving the conflict and to therefore perform other tasks without focusing unduly on the RA event. (SR_14)

6.2.7 RA Downlink Latency

Although RA Downlink should reduce the time taken for the Controller to become aware of an RA, it was questioned by the participants of the FHA/PSSA whether RA Downlink, with an expected latency of 8s for 95% of RA events [12], would have a significant impact on the probability of the Pilot following the RA to completion.

It has been suggested by pilots at the workshop that the period just before the RA is issued to the flight crew is the critical time in which an ATC instruction is most likely to affect the probability of the Pilot following an RA. **RA Downlink could not prevent controllers issuing instructions during this time.**

If a Controller instruction arrives 10 seconds or more after an RA is issued the Pilot is likely to have already begun to manoeuvre the aircraft in accordance with the RA (if a manoeuvre is required) and it might be assumed that they are more likely to report ‘Unable, TCAS’.

The benefit of RA Downlink decreases as the delay between the RA being issued and the RA Downlink display being presented to the Controller increases, therefore for RA Downlink to have the possibility of providing a significant safety benefit there should be a latency of no more than 10 seconds. (SR_04)

6.2.8 Controller Exposure to RAs

In the present situation RAs which do not require a deviation from clearance might not be reported. If RA downlink is implemented every RA will be displayed to the Controller, therefore it can be assumed that controllers will be exposed to more RA events than is currently experienced.

In some ATC centres, Controllers are relieved of their posts after an RA event in order for them to analyse and report the event without jeopardising the safety of other aircraft in the sector. Continuing this practice post RA Downlink implementation would probably result in higher Controller turnover, which could be compounded by events that occur in overlapping sectors or the RA Downlink, as a safety tool, breaking through radar screen filters.

Recommendation: A further study be carried out into the effect of an overall increase in the number of reported RAs on Controller confidence / turnover.

Most ATC units will have a Safety Management System that will cover the eventuality of an ACAS event. However if RA Downlink is implemented, such procedures will have to be reviewed in order to assess whether they are practical and feasible. These are matters that should be addressed by regulators if RA Downlink reaches operational implementation.

6.2.9 RA Downlink does not Indicate Intent

As the RA display includes an arrow indicating the ACAS instructed direction the Controller might infer that the pilot will follow the RA display and might not verify their initial belief by monitoring the vertical rate of the a/c for compliance. Although in most cases the Pilot will manoeuvre in the direction indicated, there could be situations, albeit unlikely, in which they choose not to manoeuvre in the direction displayed by the RA Downlink.

If aware that an RA has not been followed, the Controller might want to know the reason for non-compliance though should not contact the aircraft until it is ‘Clear of Conflict’ (SR_16).

Recommendation: A further study be carried out 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.

6.2.10 Misinterpretation of RA Downlink Symbols

The controller cannot unambiguously conclude from the RA Downlink whether the required manoeuvre (or restriction) yields a deviation from the clearance or not. According to the proposed display of RAs, “maintain vertical speed” is displayed by an arrow. The same symbol is used for a “climb” or “descend” RA, which are likely to require the pilot to deviate from clearance. Although the Controller should be aware of the aircraft’s current clearance and, thus, should be able to predict whether the aircraft will stay within the current clearance, there is potential for confusion.

In these cases the controllers' assumption that the aircraft has deviated from the clearance will falsely lead them to believe that they are no longer responsible for separation. (SR_12)

6.2.11 Screen Blocking

Multiple aircraft RA events will block a larger proportion of the radar screen. The Controller should be able to move the RA tags around the screen (SR_17), though in busy airspace this might still obscure non-incident aircraft.

Although RA tags can be moved, the process increases the workload of the controller and might distract them from other events in the sector.

6.2.12 Radar Screen Filter Break-through

Where aircraft tracks have been filtered there might be benefit in identifying an intruder aircraft's track through the filter for the duration of the RA to support the Controller's understanding of the RA event. This will also provide the controller with a visual indication of when the aircraft are clear of the conflict. However, the loss of the intruder track once the RA has ended and the filter is re-engaged might concern the Controller if they believe it is due to a collision. (SR_18)

6.2.13 RA Downlink Data Sharing between ATC Centres

An RA might occur between two aircraft in overlapping sectors that are under the control of different ATC centres. In this scenario if one of the aircraft is non-ACAS equipped / operational the Controller of that aircraft will remain unaware of the RA and might attempt to issue clearances.

Although it might be feasible for the Controller of the RA Downlink reporting aircraft to communicate the RA to the unaware Controller, there is no clear method for the Controller to know that their counterpart has not received the RA downlink. In the short timescales involved this kind of communication will be unhelpful and might distract both controllers from other events in their sector.

It is therefore a safety requirement that there should be data-sharing between relevant RA Downlink equipped ATC units to ensure that all controllers of RA incident aircraft are aware of the RA, even if the aircraft being vectored is not ACAS equipped. (SR_19)

6.2.14 Universal Implementation

The FARADS study has been conducted with the provision that the results are applicable to ECAC member states only. It is therefore implied that RA Downlink will not be universally implemented.

As pilots will have no method of determining whether they are flying in RA Downlink enabled airspace, any regulations introduced to supplement the implementation of RA Downlink can not affect ACAS operation in non-RA Downlink enabled airspace. Therefore there can be no change in procedures imposed on pilots. (SR_20)

6.2.15 Unnecessary RAs

An *unnecessary* RA is considered to be an RA issued although sufficient separation had been provided by ATC (providing all aircraft adhere to their respective clearances).

SR_28 seeks to reduce the number of *unnecessary* RAs.

Currently, *unnecessary* RAs might be mitigated by the Controller warning flight crews of approaching traffic. This might make the Pilot more likely not to report the RA in order for ATC to retain responsibility for separation, and hence be able to issue clearances.

Recommendation: Assessment should be carried out 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).

If RA Downlink were to be implemented the Pilot could still use their discretion as to whether an RA is reported verbally or not, however all RAs would be alerted to the controller automatically via the Downlink. As unnecessary RAs might become genuine RAs if clearances are not adhered to pilots should follow all RAs to completion as regulated by ICAO and, if RA Downlink is implemented, controllers should not attempt to communicate with any aircraft that is indicated as being involved in an RA. (SR_03)

6.2.16 False RAs

A false RA is considered to be an RA that results from an equipment error as there is no credible threat to the subject aircraft.

It is unclear whether pilots would be aware of RAs being false, however considering the short period between RA generation and the CPA it is not recommended that pilots should attempt to ascertain whether an RA is genuine or false, and should therefore follow all RAs to completion as regulated by ICAO.

With RA Downlink the Controller might be aware of the lack of a credible intruder and is therefore better placed to determine that the RA is false. However, if controllers were given the ability to intervene where an RA is deemed to be false this would reduce the effectiveness of the RA downlink in preventing controllers from communicating with the flight crew.

In the case of an evident false RA, controllers should follow the safety requirements to wait for either a Clear of Conflict report or for 20s to pass after the false RA clears before attempting to communicate with the flight crew. If the false RA does not clear, the procedures to be followed should be as specified for a continuous RA (see Section 7.1.3) (SR_13)

Recommendation: Further assessment be carried out 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.

6.2.17 Provision of Traffic Information

ICAO regulations state that ‘when a Pilot reports a manoeuvre induced by an ACAS RA, the Controller shall… provide traffic information as appropriate’ [5]. Currently

Maastricht controllers are instructed to provide traffic information to all aircraft reporting an RA, although this might not be the case for all ATC centres across Europe.

The validity of such a procedure was questioned by the members of the FHA/PSSA workshop as the traffic information served no purpose other than to aid visual acquisition of the intruder, which in itself was deemed unnecessary due to the lack of time available to react to a visual acquisition and the possibility of pilots misjudging the trajectory of the acquired intruder.

Also, ICAO Doc. 8168 Part VIII 3.2 c) 1) Note 2 states 'visually acquired traffic might not be the same traffic causing an RA. Visual perception of an encounter might be misleading, particularly at night'.

Communicating traffic information whilst the RA is active might distract the flight crew from their task, or if wrong could cause confusion which might slow Pilot response to the RA.

Recommendation: The provisions of paragraph 15.6.3.2 of ICAO Doc 4444, governing the provision of traffic information to aircraft involved in an RA, should be reconsidered, on the basis that the practice might distract the pilot from following the RA and visual acquisitions could be misleading.

6.3 Safety Requirements to Mitigate Specification / Design Deficiencies

SR_12	Responsibility for separation upon activation and de-activation of an RA Downlink alert must be defined.	Paragraph 6.2.1, 6.2.3 herein
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.	Paragraph 6.2.1 herein
SR_14	Recurring Controller training will be required to ensure that the RA display is familiar and that procedures associated with the RA display are applied rigorously.	Paragraph 6.2.4, 6.2.5 herein
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.	Paragraph 6.2.3, 6.2.6 herein

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.	Paragraph 6.2.9, 7.1.7 herein
SR_17	Controllers shall have the ability to move the RA Downlink tag around the screen as necessary.	Paragraph 6.2.11 herein
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.	Paragraph 6.2.12 herein
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.	Paragraph 6.2.13 herein
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.	Paragraph 6.2.14 herein
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.	Paragraph 6.2.16, 7.1.4 herein

7. RESULTS: FAILURE VIEWPOINT - RA DOWNLINK FAULT CONDITIONS

It was stated by members of the FHA/PSSA workshop that the high quality of Mode S communications would render many of the faults discussed below extremely improbable. However without figures based on in-service assessment the true probability of occurrence cannot be known. Therefore the purpose of this report is to identify the possible faults, however unlikely they might be.

The RA Downlink fault conditions were identified at the FHA/PSSA workshop and were recorded in a series of Failure Mode Effect Analysis tables, which are presented in Appendix H. The results are discussed in the subsequent analysis.

7.1 Analysis of Fault Conditions

7.1.1 Complete Loss of RA Downlink

If Pilots report RAs as required the loss of RA Downlink is not an issue, therefore there should be an organised system for Pilot training across Europe to ensure that all Pilots are trained in RA procedures and that RA voice reports are made as soon as practical / possible (SR_23).

Even so, as in the current situation, the voice report might be late, missing or incorrect, therefore the Controller's situational awareness might be degraded as they might not have available all of the data that the RA Downlink would provide. Also, the Controller might suffer cognitive tunnelling due to the lack of expected downlink. To minimise these effects, RA Downlink shall have operational availability of at least 95% (SR_22)

There is a significant negative benefit if the RA Downlink fails and there is no RA Voice backup. Therefore there is a benefit in having both RA Downlink and RA Voice reporting available if RA Downlink were to be implemented – see also section 6.2.14 above. Nevertheless, under current ICAO regulations Pilots are required to follow the RA instructions if ATC commands are contradictory; therefore, even if the controller is not aware of the RA and attempts to manoeuvre the aircraft against the RA the Pilot should continue to follow the RA and report 'Unable, TCAS'.

7.1.2 Loss of a Single Aircraft's RA Downlink

The failure of a single aircraft's RA downlink should have little effect as the single successful downlink should identify both aircraft involved in the RA. However the threat aircraft's RA instructions will not be displayed, therefore there might be a slight degradation in Controller situational awareness.

If the non RA Downlink transmitting aircraft is not Mode S equipped, the Controller might not receive an indication of the aircraft on their screen. In this situation, although the involvement in the RA should be obvious by its proximity to the subject aircraft, responsibility for separation might be unclear until a voice report is provided by the flight crew of the non RA Downlink reporting Pilot as there is no clear signal to the Controller that the aircraft is reacting to the RA.

7.1.3 Continuous RA Reporting

There might be a system fault or display screen fault which causes an RA Downlink to be continuously displayed on the Controller's screen. Initially the Controller would not be aware of the fault as it is likely that such a fault will propagate from an actual RA event. If the continuous RA is not the result of a genuine RA (according to

ACAS logic[22]) the Controller should be able to identify the fault early as there will be a lack of a credible intruder.

The Controller will also be made aware of the fault if the Pilot reports Clear of Conflict although the RA display remains active. If no Clear of Conflict report is made, the Controller will become concerned at the length of the RA and at some point might be obliged to confirm the existence of the RA with the flight crew unless an RA Downlink 'time out' period is specified. As most RAs are resolved within 35s, controllers should be permitted to contact incident aircraft if the RA Downlink has not cleared and no Clear of Conflict report has been received within one minute of the RA initialisation, unless an aircraft's instructed deviation causes a subsequent conflict with other traffic. (SR_24)

Once identified, a solution to the fault might not be known. A continuous RA might become extremely distracting for the Controller and could obscure the tracks of other aircraft. The continuous RA might also be presented on numerous controllers screens if filter breakthrough is active. As the Controller's radar screen is a primary tool for airborne safety, it is recommended that the Controller has the ability to turn off the RA Downlink display for selected aircraft if there is no other method of resolving the fault (SR_25). However, the person who has responsibility for deactivating the downlink must be determined and procedures put in place to ensure that the reason for the deactivation is addressed.

The time required to identify an RA Downlink fault and mitigate the consequences will increase the Controller's workload and might distract them from other events in the sector.

7.1.4 Spurious RA Reporting

Similar to a continuous reporting RA, a spurious RA is likely not to be recognised as a fault initially unless there is an obvious lack of a credible intruder. Until the Controller is aware that the RA is false they are unlikely to attempt to communicate with the flight crews involved. As there is no RA in the cockpit there might be a void of responsibility, although the Controller might question a lack of manoeuvre and voice report.

Transponder errors should be identified soon after departure when ATC verify that the altitude being reported by the pilots and that being transmitted by the aircraft's transponder are within a set tolerance. This should prevent the majority of ACAS initiated spurious RAs, though spurious RA displays might be caused by a fault in the RA downlink software also (SR_26).

Once identified a spurious RA might not be as distracting as a continuous RA, though the fault will reduce the Controller's confidence in the RA Downlink and might lead them to dismiss a real RA. If the fault persists, and depending on the regularity of the false RAs and their effect on the Controller, the RA Downlink might have to be turned off for that particular aircraft. (SR_25)

Again, the time required to identify an RA Downlink fault and mitigate the consequences will increase the Controller's workload and might distract them from other events in the sector.

[22] ACAS logic refers to the algorithms that ACAS uses to identify whether an aircraft intruding the surveillance envelope is a collision threat. An aircraft might be deemed to be a threat by ACAS logic even though the trajectories of the aircraft are such that no threat of collision exists.

7.1.5 Downlink Ends before RA

As discussed, the end of an RA encounter might be signified by the disappearance of the RA display. If there is a fault which causes the display to disappear before the RA has ended the Controller might be aware that the aircraft are not clear of conflict as the tracks of the aircraft might not be diverging, or the Controller might assume that the conflict has ended and that they might resume control for those aircraft.

The RA Downlink concept has been designed to prevent controllers distracting the flight crew during an RA event, even at the expense of possible further distraction to the controller, although if the Pilot follows ACAS procedures correctly there should be no increased risk to safety as the Pilot should report that they are 'Unable, TCAS' and continue to follow the RA to completion.

However it is believed that any communication with the flight crew during an RA event is undesirable, hence the possible safety benefit of RA Downlink implementation (SR_03).

A Pilot report that the aircraft is not clear of conflict should alert the Controller to the downlink error, who can then notify the appropriate personnel to investigate the fault, thereby increasing the Controller workload.

7.1.6 Every Aircraft Appears to Have an RA

This type of fault should be unlikely due to the reliability and quality of the downlink hardware / software, however this scenario was mentioned at the FHA/PSSA and should therefore be considered a possibility.

Such an event is likely to concern the Controller as they will be unaware of which aircraft are actually involved in an RA and might question why every aircraft appears to have an RA. In busy airspace the RA tags might obscure the air picture and create a hazardous state.

This scenario adds weight to the recommendation that responsible persons should have the ability to turn off the RA Downlink if necessary, according to strict guidelines. It might also be beneficial for the ATC centre to have the option to disconnect RA Downlink entirely. Having this ability (SR_27) would mitigate nearly all RA downlink faults once identified, and any negative effect on safety would be reduced by the requirement for pilots to continue to report RAs by voice SR_20.

7.1.7 Corrupted Downlink: Direction of Deviation

The participants of the FHA/PSSA workshop identified an unlikely scenario in which ACAS momentarily issues similar instructions, eg climb, to two aircraft in an encounter. At that precise time the Mode S transponder is interrogated by radar. In this situation it might appear to the Controller, with RA Downlink, that ACAS is actually degrading separation and they might feel obliged to intervene.

The event described was deemed extremely improbable by the attendees of the FHA/PSSA workshop due to the high quality of Mode S communications, the remote probability of ACAS issuing similar instructions and of the radar interrogating the transponder at that precise moment. Even if the event did occur, the next radar sweep should update the RA display with the correct RA instructions, thereby assuring the Controller that the conflict is being resolved[23],

[23] The actual impact on the Controller will vary depending on the rotation rate of the radar.

If the incorrect direction of deviation is a fault of the downlink which does not resolve itself, the Controller will be more likely to believe that ACAS is actually reducing separation for the incident aircraft. The situation might be resolved by a timely and accurate voice report from the two aircraft involved, which should identify the fault and give the true ACAS instructions, or the Controller might seek evidence to support or negate their initial perception, such as a change in vertical rate.

Failing this the Controller might attempt to intervene to resolve the apparent inability of ACAS to resolve the conflict. Controllers should be trained not to attempt to resolve any supposed ACAS failure as the cause of the discrepancy might be an RA Downlink fault and their intervention might actually degrade separation between the incident aircraft.

Any fault of this kind, although it might not have a significant impact on safety, will affect the Controller's confidence in the RA Downlink, which could have a negative impact in any subsequent RA encounter that is displayed via downlink.

7.1.8 Corrupted Downlink: Incident Aircraft Identity

An unlikely event is the confusion of Mode S addresses so that an aircraft that does not have an RA appears to have one, whilst the aircraft actually encountering the RA does not generate an ACAS display on the Controller's screen (SR_26).

The Controller will be confused by such an occurrence as the two aircraft with the apparent RA are unlikely to be in close proximity. Cognitive tunnelling might result, possibly compounded by a voice report that does not confirm the Controller's display.

In this situation the Controller could attempt to confirm the RA with the aircraft that is displayed as being involved, although the Controller might be regulated not to intervene. If the Controller does contact the non-incident aircraft both the Pilot of that aircraft and the Controller could lose confidence in the RA Downlink.

As the aircraft that is causing the Mode S address confusion will not be identified as experiencing an RA the Controller might attempt to manoeuvre it, although the pilots are regulated to ignore ATC and follow the RA to completion.

7.1.9 Summary

The discussions above provide evidence that the implementation of RA Downlink might present some negative safety effects compared with the current operational situation. However, any such effects need to be balanced against the safety benefits of RA Downlink, identified in section 5 above.

7.2 Safety Requirements to Mitigate RA Downlink Fault Conditions

SR_22	RA Downlink shall have operational availability of at least 95%.	Paragraph 7.1.1 herein
SR_23	Pilot training shall reinforce the requirement to report RAs that require a deviation from clearance as soon as is practical / possible.	Paragraph 7.1.1 herein
SR_24	Controllers shall be permitted to communicate with RA incident	Paragraph

	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.	7.1.3 herein
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.	Paragraph 7.1.3, 7.1.4, herein
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[24]	Paragraph 7.1.4 herein
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.	Paragraph 7.1.6 herein
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.	Paragraph 6.2.15 herein

Recommendation: Further work be carried out 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, specified in SR_26 above.

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

Page intentionally left blank

8. CONCLUSIONS AND RECOMMENDATIONS

8.1 Conclusions

The purpose of this report has been to identify opportunities for RA Downlink to reduce risk, as well as design / specification deficiencies and hazardous failure modes of ACAS RA Downlink and propose safety requirements that ensure the implementation is acceptably safe.

This report provides the detailed information collected from the FHA/PSSA workshop. As a result of the analysis the report has identified some recommendations and safety requirements, as per the objective.

All recommendations need to be considered and all safety requirements would need to be complied with to ensure such implementation is acceptably safe.

These recommendations and safety requirements might be extended as a result of further review and also through construction of the Preliminary Safety Case.

8.2 Safety Requirements for Function & Performance

Ref	Functional Safety Requirement	Origins
SR_01	RAs shall be downlinked and displayed to the Controller.	Paragraph 5.2.1 herein
SR_02	The RA Downlink display shall show the direction of the RA, including any revisions (except follow-on weakening RAs), as displayed by TCAS to the Pilot.	Paragraph 5.2.1 herein
SR_03	Training shall reinforce that Controllers shall not issue clearances to aircraft involved in an RA.	Paragraph 5.2.1, 6.2.2, 6.2.13, 7.1.5 herein
SR_04	The downlinked RA shall be displayed to the Controller within 10 seconds of the RA being activated in the Cockpit.	Paragraph 5.2.2, 6.2.7 herein
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	Paragraph 5.2.3 herein
SR_06	The RA Downlink display shall be intuitive for Controller comprehension	Paragraph 5.2.1, 5.2.3, 5.2.7, 6.2.4 herein
SR_07	The RA Downlink tag with vertical rate symbology shall only be associated with the aircraft reporting the RA.	Paragraph 5.2.5 herein
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	Paragraph 5.2.5 herein

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	Paragraph 5.2.5 herein
SR_10	The RA Downlink display shall remain active on the Controllers HMI until the aircraft is 'Clear of Conflict'	Paragraph 5.2.6, 5.2.8 herein
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[25] after the RA annotation has been removed from the RA Downlink Display.	Paragraph 5.2.8 herein
SR_12	Legal responsibility for separation upon activation and de-activation of an RA Downlink alert must be defined.	Paragraph 6.2.1 herein
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.	Paragraph 6.2.1 herein
SR_14	Recurring Controller training will be required to ensure that the RA display is familiar and that procedures associated with the RA display are applied rigorously.	Paragraph 6.2.3, 6.2.4, 6.2.5 herein
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.	Paragraph 6.2.3, 6.2.6 herein
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.	Paragraph 6.2.9, 7.1.7 herein
SR_17	Controllers shall have the ability to move the RA Downlink tag around the screen as necessary.	Paragraph 6.2.11 herein
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.	Paragraph 6.2.12 herein

[25] But see Recommendation #1, regarding the 20second time interval

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.	Paragraph 6.2.13 herein
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.	Paragraph 6.2.14 herein
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.	Paragraph 6.2.16, 7.1.4 herein
SR_23	Pilot training shall reinforce the requirement to report RAs that require a deviation from clearance as soon as is practical / possible.	Paragraph 7.1.1 herein
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.	Paragraph 7.1.3 herein
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.	Paragraph 7.1.3, 7.1.4, herein
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.	Paragraph 7.1.6 herein
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.	Paragraph 6.2.15 herein

8.3 Safety Integrity Requirements

Ref	Safety Integrity Requirement	Origins
SR_22	RA Downlink shall have operational availability of at least 95%.	Paragraph 7.1.1 herein
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[26]	Paragraph 7.1.4 herein

8.4 Safety Recommendations

It is recommended that further work be carried out to:

1. investigate the reasons for non-compliance by flight crew with current requirements for RT reporting of RAs to ATC.
2. 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. 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. assess the effectiveness of RA Downlink in specific types of airspace / sectors in order to determine suitability for implementation in those areas.
5. recommend (for incorporation in ATC Procedures if implemented) 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. assess the effect of an overall increase in the number of reported RAs on Controller confidence / turnover.
7. analyse 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. recommend (for incorporation in ATC Procedures if implemented) 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. 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. 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

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

the practice might distract the pilot from following the RA and visual acquisitions could be misleading.

11. validate the provisional figure of 10^{-5} per operating hour for the maximum frequency of a false display of an RA to the Controller.

Page intentionally left blank

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	Clear of Conflict - the indication given by ACAS 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
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
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)
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)
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 4.0, 10th August 2005

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

[4] DOC 8168, ICAO rules pertaining to TCAS Operational use, 1 June 2005

[5] DOC 4444 ATM/501 Procedures for Air Navigation Services Air Traffic Management, 14th Edition 2001

[6] ICAO SARPS Procedures – Aircraft Operations

[7] Cognitive Task Analysis (CTA) of Potential RA Downlink Scenarios, V1.0, March 2006

[8] Kirwan, B. (1994) A Guide to Human Reliability Assessment. Taylor and Francis, London.

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

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

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

[12] FARADS - Study of Latency of RA Downlink, Proposed Issue Version 1.3, 27th March 2006

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

APPENDIX C. SUMMARY OF CURRENT ICAO REGULATIONS PERTAINING TO ACAS

C1 Annex 2

3.2 Avoidance of collisions

3.2.2 Right-of-way

The aircraft that has the right-of-way shall maintain its heading and speed, but 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.— Operating procedures for use of ACAS are contained in PANS-OPS (Doc 8168), Volume I, Part VIII, Chapter 3.

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

[The remainder of this paragraph does not address the ACAS issues.]

C2 Annex 6

6.18 Aeroplanes required to be equipped with an airborne collision avoidance system (ACAS II)

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 collisions 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 5700 kg or authorized to carry more than 19 passengers shall be equipped with an airborne collisions 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 Aeroplanes required to be equipped with a pressure-altitude reporting transponder

All aeroplanes shall be equipped with a pressure-altitude reporting transponder, which operates in accordance with the relevant provisions of Annex 10, Volume IV.

Note — This provision is intended to improve the effectiveness of air traffic services as well as airborne collision avoidance systems.

C3 Annex 10

Annex 10, vol. IV contains TCAS technical requirements. The following paragraphs are worth noting:

Definitions

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.

3.5.8.10.3 Contrary Pilot response

Manoeuvres opposite to the sense of an RA might 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.

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.

4.3.6.2.1 Air-initiated downlink of ACAS RAs.

When an ACAS RA exists, ACAS shall:

a) transfer to its Mode S transponder an RA report for transmission to the ground in a Comm-B reply (4.3.11.4.1); and

b) transmit periodic RA broadcasts (4.3.7.3.2).

C4 Annex 11

2.25 Establishment of requirements for carriage and operation of pressure-altitude reporting transponders

States shall establish requirements for carriage and operation of pressure-altitude reporting transponders within defined portions of airspace.

Note.— This provision is intended to improve the effectiveness of air traffic services as well as airborne collision avoidance systems.

C5 Doc 4444

The following table summarises the phraseology presented in ICAO Doc 4444 **12.3.1.2.**

Para.	Circumstances	Phraseologies
r	… after modifying vertical speed to comply with an ACAS resolution	**Aircrew:** TCAS CLIMB (or DESCENT) **Controller:** (acknowledgement)
t	… after ACAS "Clear of Conflict" is annunciated	**Aircrew:** RETURNING TO (assigned clearance) **Controller:** (acknowledgement) (or alternative instructions)
v	… after the response to an ACAS resolution advisory is completed	**Aircrew:** TCAS CLIMB (or DESCENT), RETURNING TO (assigned clearance) **Controller:** (acknowledgement) (or alternative instructions)
x	… after returning to clearance after responding to an ACAS resolution advisory	**Aircrew:** TCAS CLIMB (or DESCENT), COMPLETED (assigned clearance) RESUMED **Controller:** (acknowledgement) (or alternative instructions)
z	… when unable to comply with a clearance because of an ACAS resolution advisory	**Aircrew:** UNABLE, TCAS RESOLUTION ADVISORY; **Controller:** (acknowledgement)

15.6.3 Procedures in regard to aircraft equipped with airborne collision avoidance systems (ACAS)

15.6.3.1 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.

15.6.3.2 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 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. 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.

15.6.3.4 ACAS can have a significant effect on ATC. Therefore, the performance of ACAS in the ATC environment should be monitored.

15.6.3.5 Following an RA event, or other significant ACAS event, pilots and controllers should complete an air traffic incident report.

Note 1.— The ACAS capability of an aircraft might 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 VIII, Chapter 3.

Note 3.— The phraseology to be used by controllers and pilots is contained in Chapter 12, 12.3.1.2.

C6 Doc 7030

20.1 Carriage and operation of ACAS II

20.1.1 ACAS II shall be carried and operated in the EUR region (including FIR Canarias) by all aircraft that meet the following criteria:

a) With effect from 1 January 2000, all civil fixed-wing turbine engined aircraft having a maximum take-off mass exceeding 15 000 kg or maximum approved passenger seating configuration of more than 30.

b) With effect from 1 January 2005, all civil fixed-wing turbine engined aircraft having a maximum takeoff mass exceeding 5 700 kg or a maximum approved passenger seating configuration of more than 19.

20.1.2 From 1 July 2001, ACAS II equipment which operates in accordance with the relevant provisions of Annex 10, Volume IV, shall be carried and operated by 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 operating within the Amman, Beirut, Cairo, Damascus and Tel Aviv FIRs except when operating wholly within an FIR for which the State responsible has notified in its AIP or by NOTAM that these requirements do not apply.

C7 Doc 8168

Part VIII. Chapter 3 OPERATION OF 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 aware-ness, and the active search for, and visual acquisition of, conflicting traffic.

3.1.2 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 initial and recurrent training in ACAS procedures.

Note 2.— ACAS II Training Guidelines for Pilots are provided in Attachment A to Part VIII.

3.2 USE OF ACAS INDICATIONS

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 might not be the same traffic causing a TA. Visual perception of an encounter might 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;

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 might not be the same traffic causing an RA. Visual perception of an encounter might 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 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;

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 an RA are contained in the PANS ATM (Doc 4444), Chapters 15 and 12, respectively.

APPENDIX D. FHA/PSSA/HRA WORKSHOP PARTICIPANTS AND BIO DETAILS

Ben Bakker EUROCONTROL Role - ATC

Ben spent the first 15 years of his professional career in industry, working for Hollandse Signaalapparaten BV, (a subsidiary of Thomson CSF). During that time, Ben was involved in the definition and realization of various ATC systems as a system engineer, system architect, senior consultant, project manager and product manager. Ben worked for EUROCONTROL as an independent consultant during 1993 and 1994 in the field of architecture for EATCHIP Phase III and Phase IV. In 1995 he joined EUROCONTROL as an ATC Expert. Architecture and system engineering remained important aspects of his work, including CIP coordination, technical coordination for European Commission projects and project management for EUROCAE projects. Ben is currently thread leader for System Safety Defences in the European Safety Programme and secretary of the Safety Nets: Implementation and eNhancement (SPIN) Task Force.

Cay Boquist EUROCONTROL Role - ATC Procedures

Cay has a long history of ATM experience as an air traffic Controller with the Swedish ANSP, training specialist and ATM adviser to many States through the ICAO Technical Co-operation Bureau. From 1990 to 2002, Cay was employed at ICAO in Montreal, firstly as a Technical Officer ATM and then from 1997, Chief, ATM Section where his duties included the following: the provision of air traffic management (ATM) information and advice to the President of the Council, Secretary General and Director Air Navigation Bureau; the planning, directing and management of Section staff and preparation of the Section work programme; the planning for Regional Air Navigation (RAN) Meetings; the preparation of working papers and studies in the fields of ATM and search and rescue (SAR). His recent appointment in 2005 was as an ATM Procedures Specialist contractor to EUROCONTROL DAS/AFN.

Garfield Dean EUROCONTROL Role - TCAS/ACAS Technical

Garfield Dean has been an engineer and researcher in ATM for 20 years. He has researched a wide range of topics, including the use of Artificial Intelligence in ATM, controller support tools and the potential for automatic conflict resolution. He also produced one of the first electronic flight strips prototypes. Over the past 10 years he has specialised in research into Airborne Collision Avoidance Systems as an expert at the EUROCONTROL Experimental Centre, in particular leading the 5th Framework ACAS Analysis project. He actively participates in ICAO and RTCA meetings associated with developing ACAS/TCAS standards and supporting material. He has been a technical advisor and participant to the FARADS research team throughout the project. He is currently examining the case for automating the response to ACAS RAs.

Doris Dehn EUROCONTROL Role – Human Factors

From 2004 Doris has been a Human Factors Expert at EUROCONTROL HQ DAS/HUM. Over the period 1997 to 2004 she has held a number of appointments including: Human Factors Expert at the National Aerospace Laboratory (NLR), Amsterdam, Netherlands; Project-Coordinator and Researcher at the Institute for Aeronautics and Astronautics of the Berlin University of Technology, Germany; Researcher at the Psychological Institute of the University of the Saarland. Over the last few years Doris has been involved with ATM – related EUROCONTROL projects such as, DMEAN and CASCADE, and she is the Human Factors Expert in the FARADS RA Downlink Project Team. She also participated in the RA Downlink Experiment when working with NLR.

David de Smedt EUROCONTROL Role – Pilot

David works as a consultant for the Navigation Domain of EUROCONTROL HQ, Brussels. He has been involved in projects related to RNAV, future concepts for navigation in terminal airspace, future concepts for air traffic management and avionics systems. He holds an ATPL licence and has 5 years of recent experience as an operational airline Pilot, flying the Airbus A320 for both national and charter carriers in Europe. He has accumulated approximately 2500 flight hours.

Stanislaw Drozdowski EUROCONTROL Role – ATC Controller FARADS PM

Since 2002, Stan has been employed as an ATM Expert at EUROCONTROL HQ Brussels. He is currently the Project Manager for the Feasibility of ACAS RA Downlink Study (FARADS), is participating in the Mode S & ACAS Programme and has also worked on the Human Machine Interface Service. Between 1992 and 2002, Stan was a Principal Engineer with Northrop Grumman where he developed operational and software requirements for human-machine interface of the Radar Controller Workstation and Flight Data Specialist Workstation (Northrop Grumman AMS2000 and AMS2100 systems) for several international customers to match local operational concepts and conditions. He also developed operational and software requirements for ATC Radar Simulators. From 1983 to 1992 he was an air traffic Controller with Airways Corporation of New Zealand and the Polish Airports State Enterprise.

Alex Fisher HVR-CSL Role - Pilot

From 1971 to 2005, Alex was a Pilot with British Airways and held positions including Pilot, Captain, Flight Technical Officer, and Technical Project Manager. In addition to normal line flying duties, Alex was a mainstay of the BA, Flight Technical Department since 1975. For the majority of that time he was concerned with general technical policy, covering subjects such as All Weather Operations (AWO), Fuel Policy and TCAS. He was responsible for developing appropriate operating rules for TCAS, which are now incorporated in JAR OPS; he specified, and then developed in association with a BA colleague, the first TCAS desktop training aid. His interests and responsibilities have also included wake vortex separation rules, runway occupancy optimisation and approach sequencing rules. From 1998 until retirement in 2005, he chaired the JAA Operational Procedures Study Group (OPSG) of the JAA, the chairmanship of this group having been held by an Industry nominee since its formation. He also chaired the AEA Operations committee since 1998.

David Fisher HVR-CSL Role – Chairman

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.

Derek Fowler EUROCONTROL Role - Safety

Derek Fowler has been involved in the application of Safety Management Systems since joining UK NATS Ltd in 1990. From 1998 he was a safety consultant, and for 5 years worked for two leading UK engineering consultancy companies, carrying out numerous safety and risk assessment assignments.

He has played a leading role for EUROCONTROL in the development of the RVSM Pre- and Post-implementation Safety Cases and carried out safety training and a Functional Hazard Assessment (FHA) and Preliminary System Safety Assessment (PSSA) for Maastricht UAC. He led the development of an ESARR 4-compliant TLS apportionment method and applied it to GBAS and developed EUROCONTROL’s safety case for P-RNAV in Terminal Airspace, including carrying out an FHA and PSSA. He also led the FHA / PSSA and safety case development for RNAV in Final Approach. Since March 2004, he has worked full time for EUROCONTROL DAP/SAF, providing safety assessment and safety case development support to EATM Programme and related Domain activities. .He is also the principal author of the revised EUROCONTROL Safety Case Development Manual, and is playing a leading role in the development of methods for integrating Human Factors into Safety Assessment and Safety Case development.

Keith Harrison HVR-CSL Role - Facilitator/Safety

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, it’s 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.

Hlin Holm Iceland CAA Role – ATC Controller/Safety

From 1988 to 2001 Hlin was an air traffic control officer with the Iceland CAA. This included both terminal area and oceanic areas of responsibility. She then spent a period of time as an instructor at the ATS School before taking up her current job responsibilities in 2003,which includes the following: Occurrence and Incident Investigation; Human Factors Training; Team Resource Management Training; Safety Assessments Facilitation/Participation. Also included is part time ATC responsibilities of Substitute supervisor/shift manager of the Reykjavík OACC and ATCO Reykjavík OACC.

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.

Gavin Jones HVR-CSL Role - Recorder/Safety

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.

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.

Martin Pellegrine EUROCONTROL Role - ATC Controller

Martin joined EUROCONTROL in September 1996 as an ab initio air traffic Controller student. He received his first rating at the end of 1998 and was fully "checked out" in Might 1999. He has always worked in the Maastricht ATCC DECO sector (the Netherlands and northern Germany). He now performs some supervisory tasks and he is a competency assessor for his team. Before joining EUROCONTROL he was a Quantity Surveyor for a major civil engineering and road building company (Tarmac)

Mike Wildin HVR-CSL Role - ATC Regulations/Procedures

Mike is a retired, British, Air Traffic Control Officer with an unrivalled background in airspace management and safety. An air traffic Controller for 28 years Mike joined the UK CAA Safety Regulatory Group in 1990. Mike became Manager Terminal Airspace of the Directorate of Airspace Policy in October 1995. He was appointed the UK Project Manager for Airborne Collision Avoidance Systems in 1999 and served as a member of a number of related work groups including: the ACAS Implementation Coordination Group (AICG); the Emotion 7 Steering Group; the ACAS Operations Monitoring Group.

APPENDIX E. EVENT TREES

E1 Pre implementation of RA Downlink

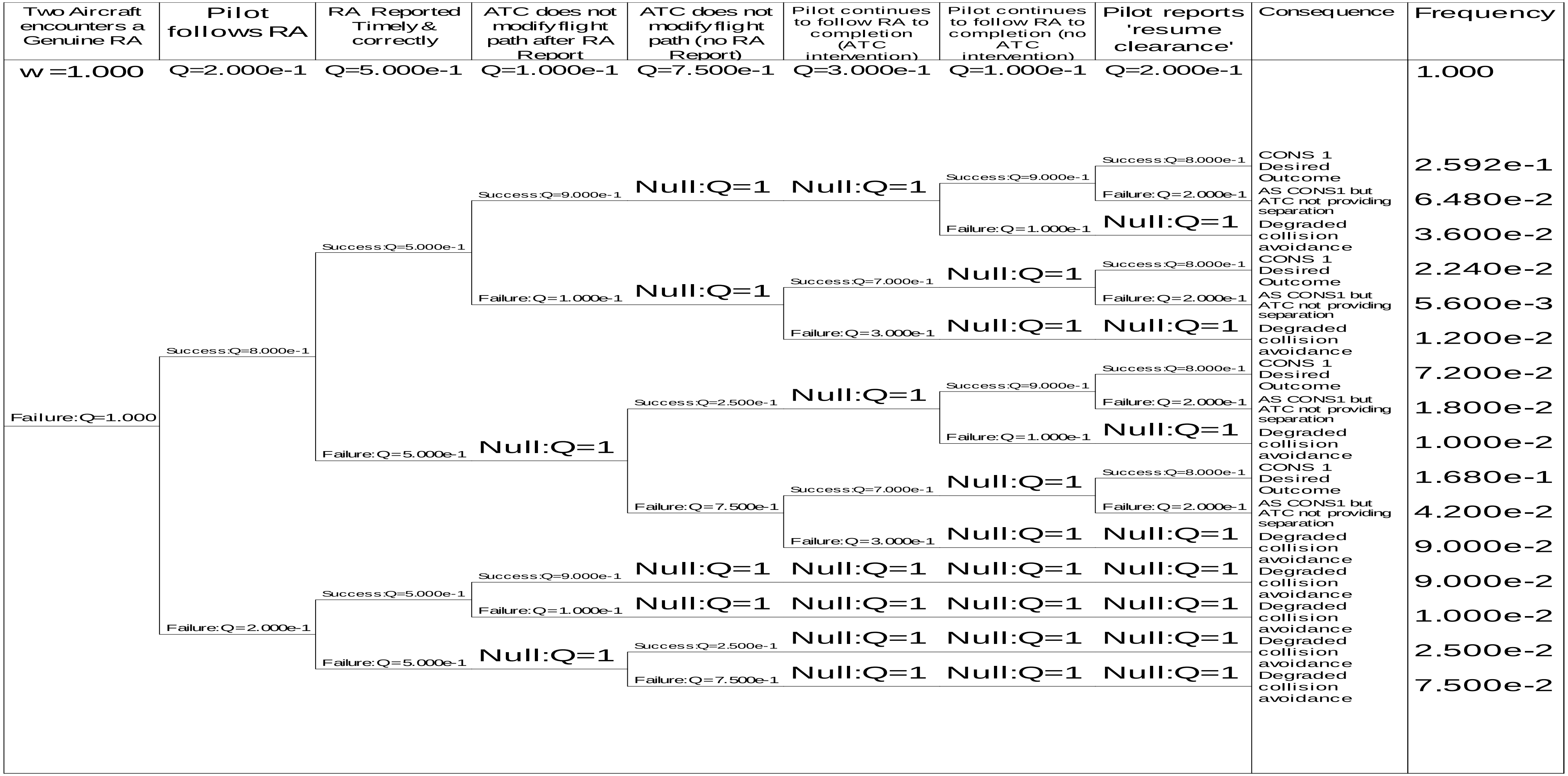

Two Aircraft encounters a Genuine RA
Pilot follows RA
RA Reported Timely & correctly
ATC does not modify flight path after RA Report
ATC does not modify flight path (no RA Report)
Pilot continues to follow RA to completion (ATC intervention)
Pilot continues to follow RA to completion (no ATC intervention)
Pilot reports 'resume clearance'
Consequence
Frequency
w =1.000
Q=2.000e-1
Q=5.000e-1
Q=1.000e-1
Q=7.500e-1
Q=3.000e-1
Q=1.000e-1
Q=2.000e-1
1.000
Failure:Q=1.000
Success:Q=8.000e-1
Failure:Q=2.000e-1
Success:Q=5.000e-1
Failure:Q=5.000e-1
Success:Q=9.000e-1
Failure:Q=1.000e-1
Success:Q=2.500e-1
Failure:Q=7.500e-1
Success:Q=7.000e-1
Failure:Q=3.000e-1
Success:Q=9.000e-1
Failure:Q=1.000e-1
Success:Q=8.000e-1
Failure:Q=2.000e-1
Null:Q=1
CONS 1 Desired Outcome
AS CONS1 but ATC not providing separation
Degraded collision avoidance
CONS 1 Desired Outcome
AS CONS1 but ATC not providing separation
Degraded collision avoidance
CONS 1 Desired Outcome
AS CONS1 but ATC not providing separation
Degraded collision avoidance
CONS 1 Desired Outcome
AS CONS1 but ATC not providing separation
Degraded collision avoidance
Degraded collision avoidance
Degraded collision avoidance
Degraded collision avoidance
Degraded collision avoidance
2.592e-1
6.480e-2
3.600e-2
2.240e-2
5.600e-3
1.200e-2
7.200e-2
1.800e-2
1.000e-2
1.680e-1
4.200e-2
9.000e-2
9.000e-2
1.000e-2
2.500e-2
7.500e-2

Figure 6. Pre Implementation (RA Voice)

a. Consequence Classification

Three consequences have been defined in this Event tree:

- CONS1 Desired Outcome
- CONS2 As CONS1 but ATC not providing separation
- CONS3 Degraded Collision Avoidance

CONS1 and CONS2 are the desired outcome for the accident sequence. CONS3 could lead to an accident that includes collision or two aircraft.

b. Two aircraft encounter a Genuine RA

The Event Tree has been used to model the incident where two TCAS equipped aircraft are in an RA situation. Both aircraft are expected to respond to the RA. The response could be a corrective manoeuvre (climb, descend or level off) or reduce rate of climb or descent. Although there are other incidents where multiple aircraft or non TCAS equipped aircraft could be in similar situations, this is deemed to be the most generic case and has been analysed. Variations to this specific incident will be considered later.

c. Pilot follows RA

The first mitigation in the accident sequence is that the Pilot follows the RA. Pilots are trained to respond to RAs and it is assumed that they will follow the corrective RA 80% of the time (agreed figure from those present at the HAZID workshop). This figure is somewhat arbitrary and is only to be used to compare the RA downlink situation.

d. RA reported timely & correctly

In the current situation (without downlink) the RA is reported by voice from the flight crew to the air traffic Controller. This situation places a reliance on the crew for verbally communicating with ATC during a most critical time of a flight. Since RA voice reporting can be delayed for a number of reasons (workload, frequency blockage, inaccurate message etc) the information might not actually be communicated to ATC till after the incident is over. Timely, means that the RA Voice report has been communicated to ATC as soon as possible. Correctly, means that the report was reported using the correct phraseology and accurately stating the TCAS advice. It is for these reasons that the figure of 50% (agreed figure from those present at the HAZID workshop) was set for successful timely and correctly reporting of the RA. This figure is somewhat arbitrary and is only to be used to compare the RA downlink situation.

e. ATC does not modify flight path after RA Report

The next mitigation in the accident sequence has been spilt into two to reflect the situation where the ATC either receives the RA voice report, timely and correctly or not. This particular mitigation is where the ATC receives the RA voice report timely and correctly and is therefore aware of the aircrafts situation. In this case the ATC will have no legal responsibility for maintaining separation whilst the flight crew are manoeuvring the aircraft. It was agreed that in this situation the ATC would not modify the flight path with knowledge of an RA for 90% of the time (agreed figure from those present at the HAZID workshop). This figure is somewhat arbitrary and is only to be used to compare the RA downlink situation.

In the situation where ATC knows about the RA, however, he/she is still able to provide traffic information to either or both the incident aircraft. The feeling of those present in the workshop was this might distract the flight crew from their immediate problem.

f. ATC does not modify flight path (No RA Report)

The alternate mitigation is where the ATC does not receive an RA voice report prior to or during the aircraft manoeuvre. In this case, ATC would notice a deviation from flight clearance (they are trained to do this) and seek to contact the aircraft flight crew to give additional/further instructions, still believing they have legal responsibility for separation. It was agreed that during this scenario ATC was more likely to give instructions and therefore potentially distract the flight crew from their immediate action. It was agreed that in this situation the ATC would not modify the flight path without knowledge of an RA for 25% of the time (agreed figure from those present at the HAZID workshop). This figure is somewhat arbitrary and is only to be used to compare the RA downlink situation.

g. Pilot continues to follow RA to completion (ATC Intervention)

The ability of the Pilot to continue following the RA might be affected by the involvement of ATC. Therefore there are two mitigation cases to explore during this accident sequence. The first is where the ATC has contacted the flight crew during an RA incident. It was agreed that in this situation the Pilot would continue to follow the RA for 70% of the time (agreed figure from those present at the HAZID workshop). This figure is somewhat arbitrary and is only to be used to compare the RA downlink situation.

h. Pilot continues to follow RA to completion (No ATC Intervention)

If the Pilot had no instruction from ATC then they are more likely to follow the RA to completion. It was agreed that in this situation the Pilot would continue to follow the RA for 90% of the time (agreed figure from those present at the HAZID workshop). This figure is somewhat arbitrary and is only to be used to compare the RA downlink situation.

i. Pilot reports ‘resume clearance’

At the end of an RA incident the aircraft should resume the original clearance. This should be reported to ATC via the voice comms. It was agreed that the Pilot would report the resume to clearance after an RA has finished about 80% of the time (agreed figure from those present at the HAZID workshop). This figure is somewhat arbitrary and is only to be used to compare the RA downlink situation.

j. Discussion of Particular Event Sequences and Probabilities

There are a number of different scenarios represented by this Event Tree. The top of the tree is concerned with the flight crew respond to the RA and the lower part is concerned with the flight crew not responding to the RA. It is not the purpose of this analysis to investigate the reasons why such scenarios might occur.

However, if the flight crew does not follow the original RA then the outcome is going to result in a CONS 3 ‘Degraded collision avoidance’ situation. If the fight crew have not followed the RA then they are unlikely to give a voice report and in this situation there is very little the ATC can do to prevent an accident unless they had prior information their normal screen scan and saw the events leading up to a potential collision. Unfortunately in this situation where TCAS has generated an RA and the aircraft does not manoeuvre then ATC are still responsible for separation; since ICAO regulations state that responsibility for providing separation passes to the Pilot ‘once an aircraft departs from its clearance in compliance with a resolution advisory’ [5].

In the Pre implementation situation using just RA voice reporting it is clear that the major influencing factor to the event tree is the success of ATC obtaining correct and timely information regarding the RA. In the pre implementation this is considered to be very unreliable. ATC would only interrupt the flight crew if they had noticed a variation in the clearance level for either or both aircraft and were able to communicate. It is assumed that if ATC were to interrupt flight crew in this situation they would either be told about the incident or there would be radio silence. It is not clear, if the flight crew are obliged to respond to and ATC call during an RA situation. If the RA Voice report is given timely and correctly then the current legislation is that ATC is only suppose to give traffic information to the flight crew of the incident aircraft. During the HAZID workshop the general consensus was that the giving of traffic information might distract the flight crew from their immediate concern.

If the flight crew follow the original RA and the RA is reported successfully then the outcome probabilities are calculated as follows:

- Probability of successful (CONS1 & CONS2) outcome : 35.20%
- Probability of Degraded collision avoidance (CONS3): 4.80%

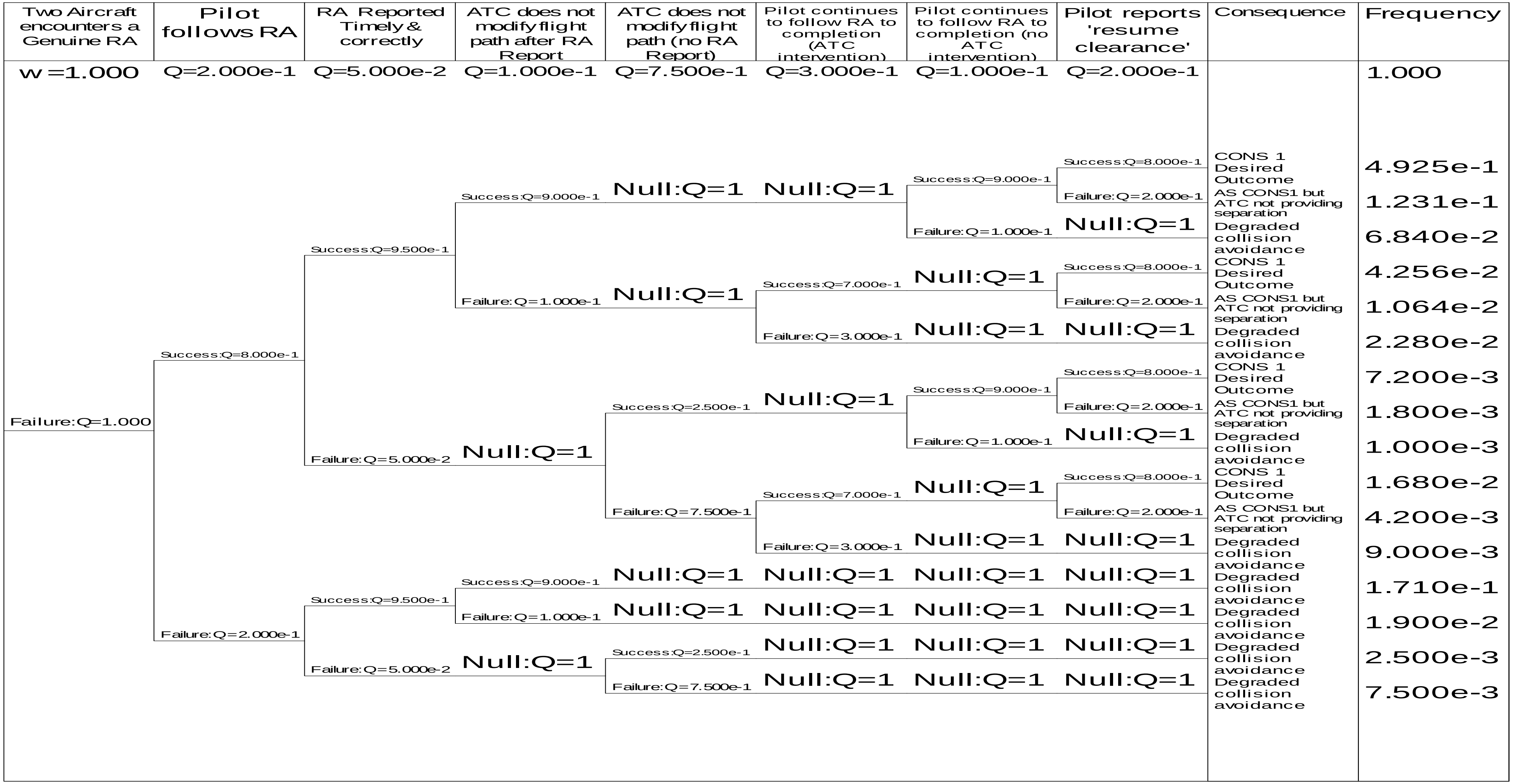
If the flight crew follow the original RA and the RA is no reported successfully then the outcome probabilities are calculated as follows:

- Probability of successful (CONS1 & CONS2) outcome : 30.00%
- Probability of Degraded collision avoidance (CONS3): 10.00%

If the flight crew do not follow the original RA the outcome is always degraded collision avoidance (CONS3) and is calculated as follows:

Probability of Degraded collision avoidance (CONS3): 20.00%

E2 Implementation of RA Downlink



Two Aircraft encounters a Genuine RA
Pilot follows RA
RA Reported Timely & correctly
ATC does not modify flight path after RA Report
ATC does not modify flight path (no RA Report)
Pilot continues to follow RA to completion (ATC intervention)
Pilot continues to follow RA to completion (no ATC intervention)
Pilot reports 'resume clearance'
Consequence
Frequency
w=1.000
Q=2.000e-1
Q=5.000e-2
Q=1.000e-1
Q=7.500e-1
Q=3.000e-1
Q=1.000e-1
Q=2.000e-1
1.000
Failure:Q=1.000
Success:Q=8.000e-1
Failure:Q=2.000e-1
Success:Q=9.500e-1
Failure:Q=5.000e-2
Success:Q=9.000e-1
Failure:Q=1.000e-1
Success:Q=2.500e-1
Failure:Q=7.500e-1
Success:Q=7.000e-1
Failure:Q=3.000e-1
Success:Q=8.000e-1
Failure:Q=2.000e-1
Null:Q=1
CONS 1 Desired Outcome
4.925e-1
AS CONS1 but ATC not providing separation
1.231e-1
Degraded collision avoidance
6.840e-2
CONS 1 Desired Outcome
4.256e-2
AS CONS1 but ATC not providing separation
1.064e-2
Degraded collision avoidance
2.280e-2
CONS 1 Desired Outcome
7.200e-3
AS CONS1 but ATC not providing separation
1.800e-3
Degraded collision avoidance
1.000e-3
CONS 1 Desired Outcome
1.680e-2
AS CONS1 but ATC not providing separation
4.200e-3
Degraded collision avoidance
9.000e-3
Degraded collision avoidance
1.710e-1
Degraded collision avoidance
1.900e-2
Degraded collision avoidance
2.500e-3
Degraded collision avoidance
7.500e-3

Figure 7. Post Implementation (RA Downlink)

k. Consequence Classification

Three consequences have been defined in this Event tree:

- CONS1 Desired Outcome
- CONS2 As CONS1 but ATC not providing separation
- CONS3 Degraded Collision Avoidance

CONS1 and CONS2 are the desired outcome for the accident sequence. CONS3 could lead to an accident that includes collision or two aircraft.

l. Two aircraft encounter a Genuine RA

The Event Tree has been used to model the incident where two TCAS equipped aircraft are in an RA situation. Both aircraft are expected to respond to the RA. The response could be a corrective manoeuvre (climb, descend or level off) or reduce rate of climb or descent. Although there are other incidents where multiple aircraft or non TCAS equipped aircraft could be in similar situations, this is deemed to be the most generic case and has been analysed. Variations to this specific incident will be considered later.

m. Pilot follows RA

The first mitigation in the accident sequence is that the Pilot follows the RA. Pilots are trained to respond to RAs and it is assumed that they will follow the corrective RA 80% of the time (agreed figure from those present at the HAZID workshop). This figure is somewhat arbitrary and is considered to be the same as the pre implementation of RA downlink situation.

n. RA Reported Timely & Correctly

In the RA Downlink situation the RA report will be automatically sent to the air traffic Controller. This situation places no reliance on the crew for verbally communicating with ATC during a most critical time of a flight. Timely means 10 sec after RA has been generated in the Cockpit. Correctly means that the RA Downlink duplicates the meaning of the TCAS warning on the ATC’s display. It is for this reason the figure of 95% (agreed figure from those present at the HAZID workshop) was set for successful timely and correctly reporting of the RA. This figure is somewhat arbitrary but significantly different to the pre implementation of RA downlink situation.

o. ATC does not modify flight path after RA Report

The next mitigation in the accident sequence has been spilt into two to reflect the situation where the ATC either receives the RA voice report, timely and correctly or not. This particular mitigation is where the ATC receives the RA voice report timely and correctly and is therefore aware of the aircrafts situation. In this case the ATC will have no legal responsibility for maintaining separation whilst the flight crew are manoeuvring the aircraft. It was agreed that in this situation the ATC would not modify the flight path with knowledge of an RA for 90% of the time (agreed figure from those present at the HAZID workshop). This figure is somewhat arbitrary and assumed to be no different to the RA downlink situation.

In the situation where ATC knows about the RA, however, he/she is still able to provide traffic information to either or both the incident aircraft. The feeling of those present in the workshop was this might distract the flight crew from their immediate problem.

p. ATC does not modify flight path (No RA Report)

The alternate mitigation is where the ATC does not receive an RA voice report prior to or during the aircraft manoeuvre. In this case, ATC would notice a deviation from flight clearance (they are trained to do this) and seek to contact the aircraft flight crew to give additional/further instructions, still believing they have legal responsibility for separation. It was agreed that during this scenario ATC was more likely to give instructions and therefore potentially distract the flight crew from their immediate action. It was agreed that in this situation the ATC would not modify the flight path without knowledge of an RA for 25% of the time (agreed figure from those present at the HAZID workshop). This figure is somewhat arbitrary and is no different to the pre implementation of RA downlink situation.

q. Pilot continues to follow RA to completion (ATC Intervention)

The ability of the Pilot to continue following the RA might be affected by the involvement of ATC. Therefore there are two mitigation cases to explore during this accident sequence. The first is where the ATC has contacted the flight crew during an RA incident. It was agreed that in this situation the Pilot would continue to follow the RA for 70% of the time (agreed figure from those present at the HAZID workshop). This figure is somewhat arbitrary and is no different to the pre implementation of RA downlink situation.

r. Pilot continues to follow RA to completion (No ATC Intervention)

If the Pilot had no instruction from ATC then they are more likely to follow the RA to completion. It was agreed that in this situation the Pilot would continue to follow the RA for 90% of the time (agreed figure from those present at the HAZID workshop). This figure is somewhat arbitrary and is no different to the pre implementation of RA downlink situation.

s. Pilot reports ‘resume clearance’

At the end of an RA incident the aircraft should resume the original clearance. This should be reported to ATC via the voice comms. It was agreed that the Pilot would report the resume to clearance after an RA has finished about 80% of the time (agreed figure from those present at the HAZID workshop). This figure is somewhat arbitrary and is no different to the pre implementation of RA downlink situation.

t. Discussion of Particular Event Sequences and Probabilities

There are a number of different scenarios represented by this Event Tree. The top of the tree is concerned with the flight crew respond to the RA and the lower part is concerned with the flight crew not responding to the RA. It is not the purpose of this analysis to investigate the reasons why such scenarios might occur.

However, if the flight crew does not follow the original RA then the outcome is going to result in a CONS 3 ‘Degraded collision avoidance’ situation. If the fight crew have not followed the RA then they are unlikely to give a voice report and in this situation there is very little the ATC can do to prevent an accident unless they had prior information their normal screen scan and saw the events leading up to a potential collision. Unfortunately in this situation where TCAS has generated an RA and the aircraft does not manoeuvre then ATC are still responsible for separation; since ICAO regulations state that responsibility for providing separation passes to the Pilot ‘once an aircraft departs from its clearance in compliance with a resolution advisory’ [5].

In the Pre implementation situation using just RA voice reporting it is clear that the major influencing factor to the event tree is the success of ATC obtaining correct and timely information regarding the RA. In the pre implementation this is considered to be very unreliable. ATC would only interrupt the flight crew if they had noticed a variation in the clearance level for either or both aircraft and were able to communicate. It is assumed that if

ATC were to interrupt flight crew in this situation they would either be told about the incident or there would be radio silence. It is not clear, if the flight crew are obliged to respond to and ATC call during an RA situation. If the RA Voice report is given timely and correctly then the current legislation is that ATC is only suppose to give traffic information to the flight crew of the incident aircraft. During the HAZID workshop the general consensus was that the giving of traffic information might distract the flight crew from their immediate concern.

If the flight crew follow the original RA and the RA is reported successfully then the outcome probabilities are calculated as follows:

- Probability of successful (CONS1 & CONS2) outcome : 66.88%
- Probability of Degraded collision avoidance (CONS3): 9.12%

If the flight crew follow the original RA and the RA is no reported successfully then the outcome probabilities are calculated as follows:

- Probability of successful (CONS1 & CONS2) outcome : 3.00%
- Probability of Degraded collision avoidance (CONS3): 1.00%

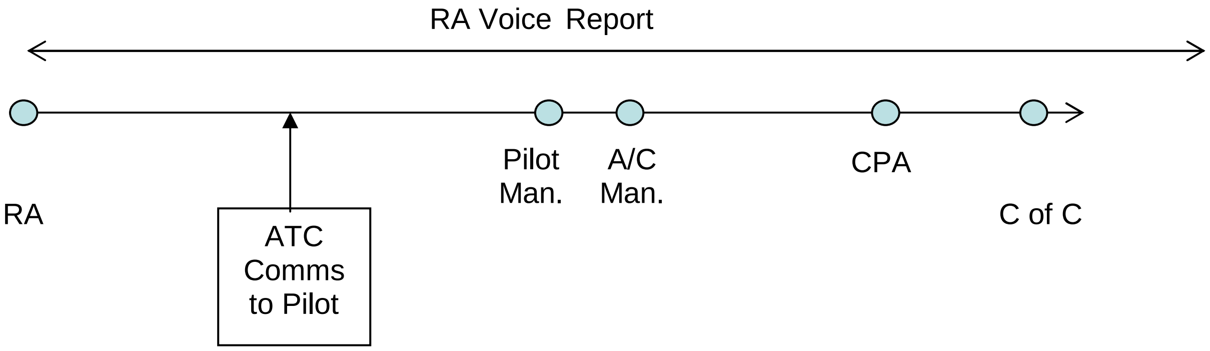
If the flight crew do not follow the original RA the outcome is always degraded collision avoidance (CONS3) and is calculated as follows:

Probability of Degraded collision avoidance (CONS3): 20.00%

APPENDIX F. TIMELINES

During the FHA workshop the pre and post implementation of RA Downlink was investigated through the use of a time line. The discussion focused on ATC contacting the flight crew just prior to receiving the RA notification (either by voice or RA Downlink). The communication from ATC to flight crew was perceived to be the most critical event. Different scenarios were discussed that varied the response of the flight crew. The following text was captured during these discussions and has been used in the discussion for pre and post comparison in failure case section of this report.

F1 Timeline: Pre RA Downlink, 2-Way A/C conflict



Note: Multiple RAs could occur at any time

Scenario 1: Pilot: Ignore ATC Comms
ATC: 1. Try Again
2. (If ignored) Try alternative solution, incl. traffic information

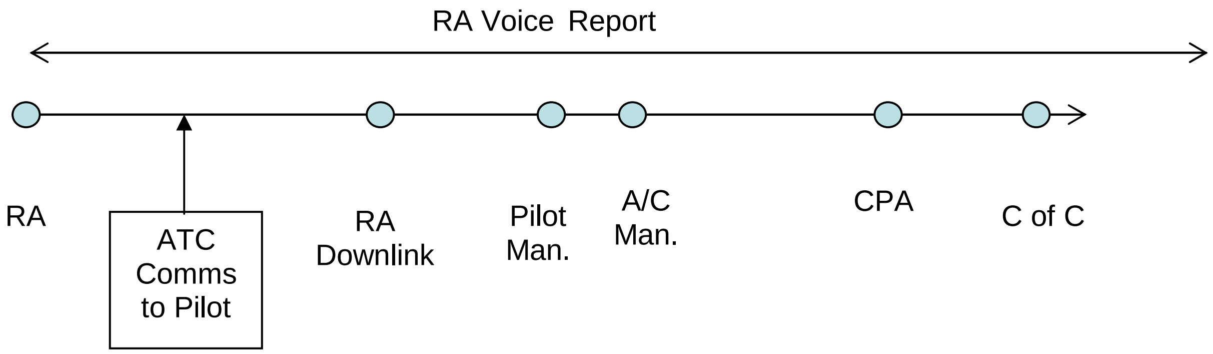
Scenario 2: Pilot: Advise ATC of RA
ATC: 1. Acknowledge
2. Give traffic information
3. Give instruction?

Scenario 3: Pilot: Confused (slower reaction to RA)
ATC: (Depends on Pilot reaction to RA, Scenarios 1,2 or 4)

Scenario 4a: Pilot: Follows ATC instructions, tells ATC of RA
(Unusual but could happen)
ATC: 1. ATC Confusion
2. Maintain control – No break from clearance therefore Controller responsible

Scenario 4b: Pilot: Follows ATC instructions, does not tell ATC of RA
(Expected if RA active)
ATC: Maintain control

F2 Timeline: RA Downlink, 2-Way A/C conflict



Scenario 1: Pilot: Ignore ATC Comms

ATC: 1. Give essential traffic information

2. Maintain separation for other traffic

Note: Downlink positively identifies conflict if ATC are ignored

Scenario 2: Pilot: Advise ATC of RA

ATC: With downlink 1. Give essential traffic information

2. Maintain separation for other traffic

No downlink (fault) As today.

Either Voice or D/L should trigger actions above. Train ATCOs to expect either type of RA notification

Scenario 3: Pilot: Confused

ATC: 1. Confirm TCAS (Action) with Pilot

2. Give essential traffic information

3. Maintain separation for other traffic

Scenario 4: Pilot: Follows ATC Instructions

(Severity dependant on difference between TCAS and ATC instructions)

ATC: 1. Re – evaluate ATC clearance

2. Give essential traffic information

3. Maintain separation for other traffic

2. Confirm TCAS (Action) with Pilot?

(Might make situation worse if reversal is required)

ATC gives instructions - RA downlink is opposite – Pilot apparently following ATC instructions

- Controller is more likely to realise they have given opposite instructions to TCAS

- Could force ATC comms which are undesirable (eg negate one of the points of having RA downlink)

APPENDIX G. FHA/PSSA WORKSHOP

G1 FHA/PSSA Workshop Briefing pack

The HVR-CSL Team prepared a FHA/PSSA briefing pack [3]. Its aim was to set the scope of the workshop, providing an explanation of the RA Downlink concept (as provided by EUROCONTROL –[2]); a description of the hazard identification process for use during the workshop; a set of operational models and the workshop agenda.

G2 Dry Run Workshop

HVR-CSL and EUROCONTROL organised a dry run FHA/PSSA workshop which took place on 9th January 2006. The objective was to dry run the hazard identification process prior to the actual workshop to provide confidence that:

- The process had derived an acceptable set of operational models, which could effectively be used to generate the hazards, their causes and potential accidents;
- In addition to hazard identification the process could identify controls and mitigation as well;
- In addition to hazard identification the process could identify causes of hazards.

Following the dry run HVR-CSL updated the briefing pack and delivered it to EUROCONTROL for wider distribution to the workshop attendees [3].

G3 FHA/PSSA Workshop

The FHA/PSSA workshop held from the 30th January to the 1st February 2006 at EUROCONTROL in Brussels investigated the hazards and mitigations associated with the implementation of an RA Downlink. The following attendees were present.

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

The biographies of the FHA/PSSA workshop attendees are presented at Appendix A.

During the meeting various pre and post RA Downlink scenarios were discussed in order to determine the possible hazards that existed and whether there was a significant advantage or disadvantage post implementation. The workshop followed the agenda:

1. Introductions
2. Feedback on the HAZID Pack
3. Description of the RA Downlink basic concept
4. A Review of the Safety Argument
5. HAZID Study
   - Current situation
   - Post RA Downlink Implementation, including HMI
6. Summary of Findings and Actions
7. The Way Ahead

APPENDIX H. FHA/PSSA FMEA TABLES

Key: Text agreed at the FHA/PSSA/HRA workshop
Text added post workshop for the pre RAD scenario
Text added post workshop for the post RAD scenario

H1 Pre-Implementation Operational Scenario A

Pre RA Downlink Implementation						
Function / Equipment	**HAZOPS Guide Word**	**Effect on System**	**Cause**	**Consequence**	**Hazard / Causal Factors**	**Control / Mitigation**
Pre-Implementation 2a						
RA Voice Report AC1 / AC2	Loss (Both a/c)	Controller unaware of RA	1. RT Failure (One-way) 2. Frequency blocking 3. High pilot workload	Controller might issue a clearance which does not concur with the RA	Pilot does not follow RA	In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller might attempt to communicate and disturb the flight crew	Pilot distracted from flying the RA	In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
	Loss (Single a/c)	Controller confusion over identity of intruder aircraft	1. RT Failure (One-way) 2. Frequency blocking 3. High pilot workload	Controller might attempt to communicate and disturb the flight crew	Pilot distracted from flying the RA	In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller delay in identifying incident aircraft Loss of situational awareness	Controller cognitive tunnelling	Controller should be able to deduce intruder from position and direction of reported incident aircraft
	Incorrect (Call sign confusion)	Controller confusion	1. High pilot workload	Controller might attempt to communicate and disturb the flight crew	Pilot distracted from flying the RA	In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller delay in identifying incident aircraft Loss of situational awareness	Controller cognitive tunnelling	Controller training
	Incorrect (False flight information, i.e. flight level)	Controller confusion	1. High pilot workload	Controller might attempt to communicate and disturb the flight crew	Pilot distracted from flying the RA	In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller delay in identifying incident aircraft Loss of situational awareness	Controller cognitive tunnelling	Controller training
	Incorrect (Not a genuine RA)	Controller believes s/he is no longer responsible for separation	1. Inappropriate pilot response to TA	Controller does not maintain separation for the incident aircraft	Loss of separation	- Pilot response only necessary in the event of an RA - Pilots shall promptly return to the terms of the ATC instruction or clearance when the conflict is resolved, and notify ATC when returning to the current clearance (ICAO - Doc. 8168, part VIII para. 3.2.c) - If there is no timely reaction from the controller to resolve a conflict situation then an ACAS RA will be issued
	Incorrect (Direction of deviation)	Controller confusion	1. High pilot workload 2. Unable to report all instructions in a multiple RA scenario	Controller might be led to believe that TCAS is instructing both aircraft to carry out the same manoeuvre	Controller might attempt to intervene	In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)

Pre RA Downlink Implementation

Function / Equipment	HAZOPS Guide Word	Effect on System	Cause	Consequence	Hazard / Causal Factors	Control / Mitigation
RA Voice Report AC1 / AC2	Delayed	Controller unaware of RA	1. Frequency blocking 2. High pilot workload	Controller might issue a clearance which does not concur with the RA	Pilot does not follow RA	In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)
	Delayed	Controller unaware of RA	1. Frequency blocking 2. High pilot workload	Controller might attempt to communicate and disturb the flight crew	Pilot distracted from flying the RA	In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
	Too Little (No callsign)	Controller confusion	1. High pilot workload	Controller might attempt to communicate and disturb the flight crew	Pilot distracted from flying the RA	In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller delay in identifying incident aircraft Loss of situational awareness	Controller cognitive tunnelling	Controller might request further RA information
	Too Little (No direction of deviation)	Controller unaware of RA direction	1. High pilot workload 2. Pilot reports preventive RA	Controller loses situational awareness Controller unable to direct non-incident aircraft away from those involved in the RA	Loss of controller situational awareness	Controller might request further RA information
	Too Much (Extended Pilot RT)	RT blocks frequency	1. High pilot workload (Stress) 2. Pilot attempts to acquire intruder visually with aid of ATC	Controller attention diverted from other possible incidents	Controller cognitive tunnelling	Controller RT given priority
				Unable to issue instructions to other aircraft	Loss of separation	If there is no timely reaction from the controller to resolve a conflict situation then an ACAS RA will be issued
	Too Much (Unnecessary Pilot RT)	RT blocks frequency	1. Inappropriate pilot response to TA	Controller confusion as to cause of conflict	Controller cognitive tunnelling	Pilot response only necessary in the event of an RA
				Unable to issue instructions to other aircraft	Loss of separation	If there is no timely reaction from the controller to resolve a conflict situation then an ACAS RA will be issued
RA Voice Report AC1 & AC2	Simultaneous (both together)	No clear effect				N/A
	Asymmetry (only 1)	Controller confusion over identity of intruder aircraft	1. RT Failure (One-way) 2. Frequency blocking 3. High pilot workload 4. Report last on RA checklist	Controller might attempt to communicate and disturb the flight crew	Pilot distracted from flying the RA	In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller delay in identifying incident aircraft Loss of situational awareness	Controller cognitive tunnelling	Controller able to deduce intruder from position and track of reported incident aircraft
	One significantly delayed	Controller confusion over identity of intruder aircraft	1. RT Failure (One-way) 2. Frequency blocking 3. High pilot workload 4. Report last on RA checklist	Controller might attempt to communicate and disturb the flight crew	Pilot distracted from flying the RA	In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)

Pre RA Downlink Implementation

Function / Equipment	HAZOPS Guide Word	Effect on System	Cause	Consequence	Hazard / Causal Factors	Control / Mitigation
				Controller delay in identifying incident aircraft Loss of situational awareness	Controller cognitive tunnelling	Controller should be able to deduce intruder from position of reported incident aircraft
Clearance AC1 / AC2	Maintaining	Reduced pilot compliance with RA	1. RA report not received / understood by controller	Pilot less likely to follow RA	Pilot does not follow RA	In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)
	Deviating	Reduced pilot compliance with RA	1. RA report not received / understood by controller	Pilot less likely to follow RA	Pilot does not follow RA	In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)
	Conflicting	Reduced pilot compliance with RA	1. RA report not received / understood by controller	Pilot less likely to follow RA	Pilot does not follow RA	In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)
Traffic Information	Conflicting	Pilot confusion	1. Essential traffic information provided on receipt of a RA report (Maastricht)	Pilot less likely to follow RA	Pilot does not follow RA	Don't give traffic information? Could make situation worse
	Irrelevant	Pilot confusion	1. Essential traffic information provided on receipt of a RA report (Maastricht)	Pilot less likely to follow RA	Pilot does not follow RA	Don't give traffic information? Could make situation worse
RADAR Mode S Surveillance AC1 / AC2	Loss (Aircraft)	No RA	1. Equipment fault	TCAS does not provide conflict resolution	Loss of separation	N/A: No relation to study of RA Downlink
	Loss (Ground)	No effect	N/A	N/A	N/A	N/A
	Incorrect	False RA	1. Equipment fault	TCAS provides false conflict resolution	Pilot unaware of Mode S error	ATC should be aware of a Mode S error
	Delayed	N/A	N/A	N/A	N/A	N/A
TCAS Dialogue	Loss	Independent TCAS resolutions	TCAS might give the same direction to both aircraft (extremely unlikely)	TCAS fails to provide increased separation	Loss of separation	None, Benefit of TCAS outweighs risk
	Incorrect	TCAS gives false information	TCAS might give the same direction to both aircraft (extremely unlikely)	TCAS fails to provide increased separation	Loss of separation	None, Benefit of TCAS outweighs risk

H2 Post-Implementation Operational Scenario A

Post RA Downlink Implementation						
Function / Equipment	**HAZOPS Guide Word**	**Effect on System**	**Cause**	**Consequence**	**Hazard / Causal Factors**	**Control / Mitigation**
Post-Implementation 2a						
RA Voice Report AC1 / AC2	Loss (Both a/c)	Controller aware of RA via downlink	1. RT Failure (One-way) 2. Frequency blocking 3. High pilot workload	Better controller awareness due to RA Downlink therefore controller less likely to issue clearances	Pilot does not follow RA	RA Downlink In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Better controller awareness due to RA Downlink therefore controller less likely to disturb the flight crew	Pilot distracted from flying the RA	RA Downlink In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
	Loss (Single a/c)	Controller can identify intruder aircraft via downlink	1. RT Failure (One-way) 2. Frequency blocking 3. High pilot workload	Better controller awareness due to RA Downlink therefore controller less likely to disturb the flight crew	Pilot distracted from flying the RA	RA Downlink In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller able to identify incident aircraft Loss of situational awareness less likely	Controller cognitive tunnelling	RA Downlink
	Incorrect (Call sign confusion)	Controller aware of call sign error due to downlink	1. High pilot workload	Better controller awareness due to RA Downlink therefore controller less likely to disturb the flight crew	Pilot distracted from flying the RA	RA Downlink In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller able to identify incident aircraft Loss of situational awareness less likely	Controller cognitive tunnelling	RA Downlink
	Incorrect (False flight information, i.e. flight level)	Controller aware of error due to downlink	1. High pilot workload	Better controller awareness due to RA Downlink therefore controller less likely to disturb the flight crew	Pilot distracted from flying the RA	RA Downlink In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller able to identify incident aircraft Loss of situational awareness less likely	Controller cognitive tunnelling	RA Downlink

Post RA Downlink Implementation						
Function / Equipment	**HAZOPS Guide Word**	**Effect on System**	**Cause**	**Consequence**	**Hazard / Causal Factors**	**Control / Mitigation**
	Incorrect (Not a genuine RA)	Controller believes they are no longer responsible for separation	1. Inappropriate pilot response to TA	Controller does not maintain separation for the incident aircraft	Loss of separation	Lack of TCAS alert on HMI might prompt controller to question the RA. Regulations should be clear regarding transfer of responsibility for separation
	Incorrect (Direction of deviation)	Controller aware of RA direction via downlink	1. High pilot workload 2. Unable to report all instructions in a multiple RA scenario	HMI will show instructed deviation of all TCAS incident aircraft. Similar direction instructions extremely improbable	Controller might attempt to intervene	RA Downlink In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)
	Delayed	Controller aware of RA via downlink	1. Frequency blocking 2. High pilot workload	Better controller awareness due to RA Downlink therefore controller less likely to issue clearances	Pilot does not follow RA	RA Downlink In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)
RA Voice Report AC1 / AC2	Delayed	Controller aware of RA via downlink	1. Frequency blocking 2. High pilot workload	Better controller awareness due to RA Downlink therefore controller less likely to disturb the flight crew	Pilot distracted from flying the RA	RA Downlink In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
	Too Little (No callsign)	Controller can identify incident aircraft via downlink	1. High pilot workload	Better controller awareness due to RA Downlink therefore controller less likely to disturb the flight crew	Pilot distracted from flying the RA	RA Downlink In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
	Too Little (No callsign)	Controller can identify incident aircraft via downlink	1. High pilot workload	Controller able to identify incident aircraft Loss of situational awareness less likely	Controller cognitive tunnelling	RA Downlink
	Too Little (No direction of deviation)	Controller aware of RA direction via downlink	1. High pilot workload 2. Pilot reports preventive RA	Controller less likely to lose situational awareness Controller more able to direct non-incident aircraft away from those involved in the RA	Loss of controller situational awareness	RA Downlink
	Too Much (Extended Pilot RT)	RT blocks frequency	1. High pilot workload (Stress) 2. Pilot attempts to acquire intruder visually with aid of ATC	Controller attention diverted from other possible incidents	Controller cognitive tunnelling	Controller RT given priority. Pilots aware of RA Downlink therefore might be less descriptive
				Unable to issue instructions to other aircraft	Loss of separation	If there is no timely reaction from the controller to resolve a conflict situation then an ACAS RA will be issued

Post RA Downlink Implementation						
Function / Equipment	**HAZOPS Guide Word**	**Effect on System**	**Cause**	**Consequence**	**Hazard / Causal Factors**	**Control / Mitigation**
	Too Much (Unnecessary Pilot RT)	RT blocks frequency	1. Inappropriate pilot response to TA	Controller confusion as to cause of conflict	Controller cognitive tunnelling	Pilot response only necessary in the event of an RA. Pilots aware of RA Downlink therefore might be less descriptive
				Unable to issue instructions to other aircraft	Loss of separation	If there is no timely reaction from the controller to resolve a conflict situation then an ACAS RA will be issued
RA Voice Report AC1 & AC2	Simultaneous (both together)	No clear effect	It was agreed at the HAZID that this scenario had no clear effect on the system			N/A
	Asymmetry (only 1)	Controller can identify incident aircraft via downlink	1. RT Failure (One-way) 2. Frequency blocking 3. High pilot workload 4. Report last on RA checklist	Better controller awareness due to RA Downlink therefore controller less likely to disturb the flight crew	Pilot distracted from flying the RA	RA Downlink In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller able to identify incident aircraft Loss of situational awareness less likely	Controller cognitive tunnelling	RA Downlink
	One significantly delayed	Controller can identify incident aircraft via downlink	1. RT Failure (One-way) 2. Frequency blocking 3. High pilot workload 4. Report last on RA checklist	Better controller awareness due to RA Downlink therefore controller less likely to disturb the flight crew	Pilot distracted from flying the RA	RA Downlink In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
RA Voice Report AC1 & AC2	One significantly delayed	Controller can identify incident aircraft via downlink	1. RT Failure (One-way) 2. Frequency blocking 3. High pilot workload 4. Report last on RA checklist	Controller able to identify incident aircraft Loss of situational awareness less likely	Controller cognitive tunnelling	RA Downlink
Clearance AC1 / AC2	Maintaining	Reduced pilot compliance with RA	1. RA report not received / understood by controller	Pilot less likely to follow RA	Pilot does not follow RA	Controller less likely to intervene with RA Downlink In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)
	Deviating	Reduced pilot compliance with RA	1. RA report not received / understood by controller	Pilot less likely to follow RA	Pilot does not follow RA	Controller less likely to intervene with RA Downlink In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)

Post RA Downlink Implementation

Function/ Equipment	HAZOPS Guide Word	Effect on System	Cause	Consequence	Hazard / Causal Factors	Control/Mitigation
	Conflicting	Reduced pilot compliance with RA	1. RA report not received / understood by controller	Pilot less likely to follow RA	Pilot does not follow RA	Controller less likely to intervene with RA Downlink In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)
Traffic Information	Conflicting	Pilot confusion	Traffic information more likely with RA downlink	Pilot less likely to follow RA	Pilot does not follow RA	Don't give traffic information? Could make situation worse
	Irrelevant	Pilot confusion	Traffic information more likely with RA downlink	Pilot less likely to follow RA	Pilot does not follow RA	Don't give traffic information? Could make situation worse
RADAR Mode S Surveillance AC1 / AC2	Loss (Aircraft)	No RA	1. Equipment fault	TCAS does not provide conflict resolution	Loss of separation	N/A: No relation to study of RA Downlink
	Loss (Ground)	No RA Downlink	1. Equipment fault	Similar to pre RA downlink implementation scenarios	Reliance on Downlink	Report by voice Controller training
	Incorrect	Degraded RA	1. Equipment fault	RA Downlink alerts controller to aircraft with Mode S Altitude Error eg Gillham error	Pilot unaware of Mode S error	Condition of Mode S will be known to controller
	Delayed	Delayed downlink report	1. Equipment fault	Controller surprised by degradation of system	Controller cognitive tunnelling	Controller training
TCAS Dialogue	Loss	Independent TCAS resolutions	TCAS might give the same direction to both aircraft (extremely unlikely)	TCAS fails to provide increased separation Controller will be aware via downlink though regulated not to resolve and might not have time to make a difference	Loss of separation	None, Benefit outweighs risk
	Incorrect	TCAS gives false information	TCAS might give the same direction to both aircraft (extremely unlikely)	TCAS fails to provide increased separation Controller will be aware via downlink though regulated not to resolve and might not have time to make a difference	Loss of separation	None, Benefit outweighs risk
RA Downlink	Loss (Both a/c)	Controller unaware of RA until voice report	1. Equipment fault	Downlink expected, loss of confidence in the system. Controller becomes fixated on lack of report?	Controller cognitive tunnelling	Controller trained to expect either form of report
	Loss (Both a/c)	Controller unaware of RA until voice report	1. Equipment fault	Controller might issue a clearance which does not concur with the RA	Pilot does not follow RA	In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre

Post RA Downlink Implementation						
Function / Equipment	**HAZOPS Guide Word**	**Effect on System**	**Cause**	**Consequence**	**Hazard / Causal Factors**	**Control / Mitigation**
RA Downlink						(ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller might disturb the flight crew	Pilot distracted from flying the RA	In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
	Loss (Single a/c)	TCAS alert for one aircraft only	1. Equipment fault	Controller unclear whether they are responsible for the non TCAS highlighted aircraft	Pilot distracted from flying the RA	Report by voice
	Incorrect (Continuous)	Continuous RA	1. Equipment fault	Uncertainty as to whether RA is valid (if there is a credible intruder aircraft)	Controller cognitive tunnelling	Controller procedures must be defined for this situation
			1. Equipment fault	Controller might ignore a real RA	Controller cognitive tunnelling	Controller procedures must be defined for this situation
	Incorrect (Occasional)	Spurious RA	1. Equipment fault	Controller might think that they are not responsible for the aircraft.	Loss of separation	Controller might confirm RA with Pilot
	Delayed	Voice report might come before downlink	1. Equipment fault	Downlink expected, loss of confidence in the system. Controller becomes fixated on lack of report?	Controller cognitive tunnelling	Controller trained to expect either form of report
				Controller might issue a clearance which does not concur with the RA	Pilot does not follow RA	In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)
	Delayed	Voice report might come before downlink	1. Equipment fault	Controller might disturb the flight crew	Pilot distracted from flying the RA	In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
	Too little	Downlink ends before RA	1. Equipment fault	Controller believes they are responsible for separation and issues clearance	Pilot does not follow RA	Clear of conflict report required from pilot, or obvious from RADAR. Regulations should be clear regarding transfer of responsibility for separation
	Too much (changing RA)	Max. Three possible changes to the RA (Original plus two adjustments)	1. Complicated RA scenario	Controller becomes fixated on the TCAS incident	Controller cognitive tunnelling	The CWP display should be designed to minimise confusion. Similar types of RA have been grouped, i.e. weakening RAs will not be shown (HMI)

Post RA Downlink Implementation

Function / Equipment	HAZOPS Guide Word	Effect on System	Cause	Consequence	Hazard / Causal Factors	Control / Mitigation
	Too much (information)	Increased data on screen	1. Equipment fault	Data might block other relevant information	Controller cognitive tunnelling	Emergency data takes precedence
		Controller distraction	1. Equipment fault	Loss of situational awareness	Controller cognitive tunnelling	The CWP display should be designed to minimise confusion. Similar types of RA have been grouped, i.e. weakening RAs will not be shown (HMI)
	Too much (every aircraft appears to have an RA)	Controller confusion	1. Equipment fault	Loss of situational awareness	Controller cognitive tunnelling	Controller training
	Corrupted	Display indicates opposite direction to RA	1. Equipment fault	Controller confusion, increased probability of talking to aircraft	Pilot distracted from flying the RA	High quality of Mode S comms (rare event)
Display	Similar direction	HMI shows TCAS giving similar resolution to incident aircraft	1. Equipment fault	Controller sees two aircraft with descend / climb RA	RADAR sweep catches simultaneous climb / descend instructions to both incident aircraft	Next RADAR update should show resolution of conflict

H3 Pre-Implementation Operational Scenario B

Pre RA Downlink Implementation						
Function / Equipment	**HAZOPS Guide Word**	**Effect on System**	**Cause**	**Consequence**	**Hazard / Causal Factors**	**Control / Mitigation**
Pre-Implementation 2b						
RA Voice Report AC1 / AC2	Loss	Controller unaware of RA	1. RT Failure (One-way) 2. Frequency blocking 3. High pilot workload	Controller might issue a clearance which does not concur with the RA	Pilot does not follow RA	In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller might attempt to communicate and disturb the flight crew	Pilot distracted from flying the RA	In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
	Incorrect (Call sign confusion)	Controller confusion	1. High pilot workload	Controller might attempt to communicate and disturb the flight crew	Pilot distracted from flying the RA	In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller delay in identifying incident aircraft Loss of situational awareness Attention diverted from other possible incidents	Controller cognitive tunnelling	Controller training
	Incorrect (False flight information, i.e. flight level)	Controller confusion	1. High pilot workload	Controller might attempt to communicate and disturb the flight crew	Pilot distracted from flying the RA	In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller delay in identifying incident aircraft Loss of situational awareness Attention diverted from other possible incidents	Controller cognitive tunnelling	Controller training

Pre RA Downlink Implementation

Function / Equipment	HAZOPS Guide Word	Effect on System	Cause	Consequence	Hazard / Causal Factors	Control / Mitigation
RA Voice Report AC1 / AC2	Incorrect (Not a genuine RA)	Controller believes they are no longer responsible for separation	1. Inappropriate pilot response to TA	Controller does not maintain separation for the incident aircraft	Loss of separation	- Pilot response only necessary in the event of an RA - Pilots shall promptly return to the terms of the ATC instruction or clearance when the conflict is resolved, and notify ATC when returning to the current clearance (ICAO - Doc. 8168, part VIII para. 3.2.c) - If there is no timely reaction from the controller to resolve a conflict situation then an ACAS RA will be issued
	Incorrect (Direction of deviation)	None (Controller has no immediate source of conflicting data)	1. High pilot workload 2. Unable to report all instructions in a multiple RA scenario	N/A	N/A	N/A
	Delayed	Controller unaware of RA	1. Frequency blocking 2. High pilot workload	Controller might issue a clearance which does not concur with the RA	Pilot does not follow RA	In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller might attempt to communicate and disturb the flight crew	Pilot distracted from flying the RA	In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
	Too Little (No callsign)	Controller confusion	1. High pilot workload	Controller might attempt to communicate and disturb the flight crew	Pilot distracted from flying the RA	In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller delay in identifying incident aircraft Loss of situational awareness Controller attention diverted from other possible incidents	Controller cognitive tunnelling	Controller might request further RA information
	Too Little (No direction of deviation)	Controller unaware of RA direction	1. High pilot workload 2. Pilot reports preventative RA	Controller loses situational awareness Controller unable to direct non-incident aircraft away from those involved in the RA	Loss of controller situational awareness	Controller might request further RA information
	Too Much (Extended Pilot RT)	RT blocks frequency	1. High pilot workload (Stress) 2. Pilot attempts to acquire intruder visually with aid of ATC	Controller attention diverted from other possible incidents	Controller cognitive tunnelling	Controller RT given priority

Pre RA Downlink Implementation

Function / Equipment	HAZOPS Guide Word	Effect on System	Cause	Consequence	Hazard / Causal Factors	Control / Mitigation
				Unable to issue instructions to other aircraft	Loss of separation	If there is no timely reaction from the controller to resolve a conflict situation then an ACAS RA will be issued
	Too Much (Unnecessary Pilot RT)	RT blocks frequency	1. Inappropriate pilot response to TA	Controller confusion as to cause of conflict	Controller cognitive tunnelling	Pilot response only necessary in the event of an RA
				Unable to issue instructions to other aircraft	Loss of separation	If there is no timely reaction from the controller to resolve a conflict situation then an ACAS RA will be issued
RA Voice Report AC1 & AC2	Simultaneous (both together)	No effect	It was agreed at the HAZID that this scenario had no clear effect on the system			N/A
	Asymmetry (only 1)	N/A	N/A	N/A	N/A	N/A
	One significantly delayed	N/A	N/A	N/A	N/A	N/A
Clearance AC1 / AC2	Maintain	Reduced pilot compliance with RA	1. RA report not received / understood by controller	Pilot less likely to follow RA	Pilot does not follow RA	In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)
	Deviate	Reduced pilot compliance with RA	1. RA report not received / understood by controller	Pilot less likely to follow RA	Pilot does not follow RA	In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)
	Conflicting	Reduced pilot compliance with RA	1. RA report not received / understood by controller	Pilot less likely to follow RA	Pilot does not follow RA	In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)
Traffic Information	Conflicting	Pilot confusion	1. Essential traffic information provided on receipt of a RA report (Maastricht)	Pilot less likely to follow RA	Pilot does not follow RA	Don't give traffic information? Could make situation worse
Traffic Information	Irrelevant	Pilot confusion	1. Essential traffic information provided on receipt of a RA report (Maastricht)	Pilot less likely to follow RA	Pilot does not follow RA	Don't give traffic information? Could make situation worse
RADAR Mode S Surveillance AC1 / AC2	Loss (Aircraft)	No RA	1. Equipment fault	TCAS does not provide conflict resolution	Loss of separation	N/A: No relation to study of RA Downlink
	Loss (Ground)	No effect	N/A	N/A	N/A	N/A

Pre RA Downlink Implementation						
Function / Equipment	**HAZOPS Guide Word**	**Effect on System**	**Cause**	**Consequence**	**Hazard / Causal Factors**	**Control / Mitigation**
	Incorrect	False RA	1. Equipment fault	TCAS provides false conflict resolution	Pilot unaware of Mode S error	
	Delayed	N/A	N/A	N/A	N/A	N/A
TCAS Dialogue	Loss	Independent TCAS resolutions	TCAS might give the same direction to both aircraft (extremely unlikely)	TCAS fails to provide increased separation	Loss of separation	None, Benefit outweighs risk
	Incorrect	TCAS gives false information	TCAS might give the same direction to both aircraft (extremely unlikely)	TCAS fails to provide increased separation	Loss of separation	None, Benefit outweighs risk
Controller to Controller Comms	Loss	No communication between controllers	1. Equipment fault	No coordination of ATC response	Inappropriate ATC response: Pilot distracted from flying the RA	Multiple communication channels, i.e. mobile phones
		Controller confusion	1. Lack of information	Controller confusion as to cause of conflict	Controller cognitive tunnelling	Controller training
	Incorrect (Call sign confusion)	Controller confusion	1. High controller workload 2. Controller mis-informed by pilot	Controller might attempt to communicate and disturb the flight crew	Pilot distracted from flying the RA	In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller delay in identifying incident aircraft Loss of situational awareness Attention diverted from other possible incidents	Controller cognitive tunnelling	Controller training
	Incorrect (False flight information, i.e. flight level)	Controller confusion	1. High controller workload 2. Controller mis-informed by pilot	Controller might attempt to communicate and disturb the flight crew	Pilot distracted from flying the RA	In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller delay in identifying incident aircraft Loss of situational awareness Attention diverted from other possible incidents	Controller cognitive tunnelling	Controller training
	Delayed	Delayed communication between controllers	1. Equipment fault	Delayed coordination of ATC response (significant delay similar to loss of comms due to short RA period)	Inappropriate ATC response: Pilot distracted from flying the RA	Multiple communication channels, i.e. mobile phones

Pre RA Downlink Implementation						
Function / Equipment	HAZOPS Guide Word	Effect on System	Cause	Consequence	Hazard / Causal Factors	Control / Mitigation
		Controller confusion	1. Lack of information	Controller confusion as to cause of conflict	Controller cognitive tunnelling	Controller training

H4 Post-Implementation Operational Scenario B

Post RA Downlink Implementation						
Function / Equipment	**HAZOPS Guide Word**	**Effect on System**	**Cause**	**Consequence**	**Hazard / Causal Factors**	**Control / Mitigation**
Post-Implementation 2b						
RA Voice Report AC1 / AC2	Loss	Controller aware of RA via downlink	1. RT Failure (One-way) 2. Frequency blocking 3. High pilot workload	Better controller awareness due to RA Downlink therefore controller less likely to issue clearances	Pilot does not follow RA	RA Downlink In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Better controller awareness due to RA Downlink therefore controller less likely to disturb the flight crew	Pilot distracted from flying the RA	RA Downlink In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
	Incorrect (Call sign confusion)	Controller aware of call sign error due to downlink	1. High pilot workload	Better controller awareness due to RA Downlink therefore controller less likely to disturb the flight crew	Pilot distracted from flying the RA	RA Downlink In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller able to identify incident aircraft Loss of situational awareness less likely	Controller cognitive tunnelling	RA Downlink
	Incorrect (False flight information, i.e. flight level)	Controller aware of error due to downlink	1. High pilot workload	Better controller awareness due to RA Downlink therefore controller less likely to disturb the flight crew	Pilot distracted from flying the RA	RA Downlink In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller able to identify incident aircraft Loss of situational awareness less likely	Controller cognitive tunnelling	RA Downlink
	Incorrect (Not a genuine RA)	Controller believes they are no longer responsible for separation	1. Inappropriate pilot response to TA	Controller does not maintain separation for the incident aircraft	Loss of separation	Lack of TCAS alert on HMI might prompt controller to question the RA.
	Incorrect (Direction of deviation)	Controller aware of RA direction via downlink	1. High pilot workload 2. Unable to report all instructions in a multiple RA scenario	HMI will show instructed deviation of all TCAS incident aircraft. Similar direction instructions extremely improbable	Controller might attempt to intervene	RA Downlink In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)
	Delayed	Controller aware of RA via downlink	1. Frequency blocking 2. High pilot workload	Better controller awareness due to RA Downlink therefore controller less likely to issue clearances	Pilot does not follow RA	RA Downlink In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Better controller awareness due to RA Downlink therefore controller less likely to disturb the flight crew	Pilot distracted from flying the RA	RA Downlink In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)

Post RA Downlink Implementation						
Function / Equipment	**HAZOPS Guide Word**	**Effect on System**	**Cause**	**Consequence**	**Hazard / Causal Factors**	**Control / Mitigation**
RA Voice Report AC1 / AC2	Too Little (No callsign)	Controller can identify incident aircraft via downlink	1. High pilot workload	Better controller awareness due to RA Downlink therefore controller less likely to disturb the flight crew	Pilot distracted from flying the RA	RA Downlink In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller able to identify incident aircraft Loss of situational awareness less likely	Controller cognitive tunnelling	RA Downlink
	Too Little (No direction of deviation)	Controller aware of RA direction via downlink	1. High pilot workload 2. Pilot reports preventative RA	Controller less likely to lose situational awareness Controller more able to direct non-incident aircraft away from those involved in the RA	Loss of controller situational awareness	RA Downlink
	Too Much (Extended Pilot RT)	RT blocks frequency	1. High pilot workload (Stress) 2. Pilot attempts to acquire intruder visually with aid of ATC	Controller attention diverted from other possible incidents	Controller cognitive tunnelling	Controller RT given priority. Pilots aware of RA Downlink therefore might be less descriptive
				Unable to issue instructions to other aircraft	Loss of separation	If there is no timely reaction from the controller to resolve a conflict situation then an ACAS RA will be issued
	Too Much (Unnecessary Pilot RT)	RT blocks frequency	1. Inappropriate pilot response to TA	Controller confusion as to cause of conflict	Controller cognitive tunnelling	Pilot response only necessary in the event of an RA. Pilots aware of RA Downlink therefore might be less descriptive
				Unable to issue instructions to other aircraft	Loss of separation	If there is no timely reaction from the controller to resolve a conflict situation then an ACAS RA will be issued
RA Voice Report AC1 & AC2	Simultaneous (both together)	N/A	N/A	N/A	N/A	N/A
	Asymmetry (only 1)	N/A	N/A	N/A	N/A	N/A
	One significantly delayed	N/A	N/A	N/A	N/A	N/A
Clearance AC1 / AC2	Maintaining	Reduced pilot compliance with RA	1. RA report not received / understood by controller	Pilot less likely to follow RA	Pilot does not follow RA	Controller less likely to intervene with RA Downlink In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)
	Deviating	Reduced pilot compliance with RA	1. RA report not received / understood by controller	Pilot less likely to follow RA	Pilot does not follow RA	Controller less likely to intervene with RA Downlink In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)

Post RA Downlink Implementation

Function / Equipment	HAZOPS Guide Word	Effect on System	Cause	Consequence	Hazard / Causal Factors	Control / Mitigation
	Conflicting	Reduced pilot compliance with RA	1. RA report not received / understood by controller	Pilot less likely to follow RA	Pilot does not follow RA	Controller less likely to intervene with RA Downlink In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)
Traffic Information	Conflicting	Pilot confusion	Traffic information more likely with RA downlink	Pilot less likely to follow RA	Pilot does not follow RA	Don't give traffic information? Could make situation worse
	Irrelevant	Pilot confusion	Traffic information more likely with RA downlink	Pilot less likely to follow RA	Pilot does not follow RA	Don't give traffic information? Could make situation worse
RADAR Mode S Surveillance AC1 / AC2	Loss (Aircraft)	No RA	1. Equipment fault	TCAS does not provide conflict resolution	Loss of separation	N/A: No relation to study of RA Downlink
	Loss (Ground)	No RA Downlink	1. Equipment fault	Similar to pre RA downlink implementation scenarios	Reliance on Downlink	Report by voice Controller training
	Incorrect	Degraded RA	1. Equipment fault	RA Downlink alerts controller to aircraft with Mode S Altitude Error eg Gillham error	Pilot unaware of Mode S error	Condition of Mode S will be known to controller
	Delayed	Delayed downlink report	1. Equipment fault	Controller surprised by degradation of system	Controller cognitive tunnelling	Controller training
TCAS Dialogue	Loss	Independent TCAS resolutions	TCAS might give the same direction to both aircraft (extremely unlikely)	TCAS fails to provide increased separation Controller will be aware via downlink though regulated not to resolve and might not have time to make a difference	Loss of separation	None, Benefit outweighs risk
TCAS Dialogue	Incorrect	TCAS gives false information	TCAS might give the same direction to both aircraft (extremely unlikely)	TCAS fails to provide increased separation Controller will be aware via downlink though regulated not to resolve and might not have time to make a difference	Loss of separation	None, Benefit outweighs risk
Controller to Controller Comms	Loss	No communication between controllers	1. Equipment fault	RA information provided to both controllers therefore less need for comms	Inappropriate ATC response: Pilot distracted from flying the RA	RA Downlink
		Controller confusion	1. Lack of information	Cause of conflict identified by RA Downlink	Controller cognitive tunnelling	RA Downlink
	Incorrect (Call sign confusion)	Controller confusion	1. High controller workload 2. Controller mis-informed by pilot	Better controller awareness due to RA Downlink therefore controller less likely to disturb the flight crew	Pilot distracted from flying the RA	RA Downlink In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller able to identify incident aircraft Loss of situational awareness less likely	Controller cognitive tunnelling	RA Downlink

Post RA Downlink Implementation						
Function / Equipment	**HAZOPS Guide Word**	**Effect on System**	**Cause**	**Consequence**	**Hazard / Causal Factors**	**Control / Mitigation**
Controller to Controller Comms	Incorrect (False flight information, i.e. flight level)	Controller confusion	1. High controller workload 2. Controller mis-informed by pilot	Better controller awareness due to RA Downlink therefore controller less likely to disturb the flight crew	Pilot distracted from flying the RA	RA Downlink In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller able to identify incident aircraft Loss of situational awareness less likely	Controller cognitive tunnelling	RA Downlink
	Delayed	Delayed communication between controllers	1. Equipment fault	RA information provided to both controllers therefore less need for comms	Inappropriate ATC response: Pilot distracted from flying the RA	RA Downlink In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
		Controller confusion	1. Lack of information	Cause of conflict identified by RA Downlink	Controller cognitive tunnelling	RA Downlink
RA Downlink	Loss (Both a/c)	Controllers unaware of RA until voice report	1. Equipment fault	Downlink expected, loss of confidence in the system. Controller becomes fixated on lack of report?	Controller cognitive tunnelling	Controller trained to expect either form of report
				Controller might issue a clearance which does not concur with the RA	Pilot does not follow RA	In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller might disturb the flight crew	Pilot distracted from flying the RA	In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
	Loss (Single a/c)	One controller unaware of RA	1. Equipment fault	Controller unclear whether they are responsible for the non TCAS highlighted aircraft	Controller cognitive tunnelling	Communication between control centres
				Unaware controller might try to issue clearance to incident aircraft	Pilot does not follow RA	Communication between control centres
				Unaware controller might disturb the flight crew	Pilot distracted from flying the RA	Communication between control centres
	Incorrect (Continuous)	Continuous RA	1. Equipment fault	Uncertainty as to whether RA is valid (if there is a credible intruder aircraft)	Controller cognitive tunnelling	Controller procedures must be defined for this situation
	Incorrect (Continuous)	Continuous RA	1. Equipment fault	Controller might ignore a real RA	Controller cognitive tunnelling	Controller procedures must be defined for this situation
	Incorrect (Occasional)	Spurious RA	1. Equipment fault	Controller might think that they are not responsible for the aircraft.	Loss of separation	Controller might confirm RA with Pilot
	Delayed	Voice report might come before downlink	1. Equipment fault	Downlink expected, loss of confidence in the system. Controller becomes fixated on lack of report?	Controller cognitive tunnelling	Controller trained to expect either form of report
				Controller might issue a clearance which does not concur with the RA	Pilot does not follow RA	In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)

Post RA Downlink Implementation

Function / Equipment	HAZOPS Guide Word	Effect on System	Cause	Consequence	Hazard / Causal Factors	Control / Mitigation
RA Downlink				Controller might disturb the flight crew	Pilot distracted from flying the RA	In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
	Too little	Downlink ends before RA	1. Equipment fault	Controller believes they are responsible for separation and issues clearance	Pilot does not follow RA	Clear of conflict report required from pilot, or obvious from RADAR. Regulations should be clear regarding transfer of responsibility for separation
	Too much (changing RA)	Max. Three possible changes to the RA (Original plus two adjustments)	1. Complicated RA scenario	Controller becomes fixated on the TCAS incident	Controller cognitive tunnelling	The CWP display should be designed to minimise confusion. Similar types of RA have been grouped, i.e. weakening RAs will not be shown (HMI)
	Too much (information)	Increased data on screen	1. Equipment fault	Data might block other relevant information	Controller cognitive tunnelling	Emergency data takes precedence
		Controller distraction	1. Equipment fault	Loss of situational awareness	Controller cognitive tunnelling	The CWP display should be designed to minimise confusion. Similar types of RA have been grouped, i.e. weakening RAs will not be shown (HMI)
	Too much (every aircraft appears to have an RA)	Controller confusion	1. Equipment fault	Loss of situational awareness	Controller cognitive tunnelling	Controller training
	Corrupted	Display indicates opposite direction to RA	1. Equipment fault	Controller confusion, increased probability of talking to aircraft	Pilot distracted from flying the RA	High quality of Mode S comms (rare event)
Display	Similar direction	HMI shows TCAS giving similar resolution to incident aircraft	1. Equipment fault	Controller sees two aircraft with descend / climb RA	RADAR sweep catches simultaneous climb / descend instructions to both incident aircraft	Next RADAR update should show resolution of conflict

H5 Pre-Implementation Operational Scenario C

Pre RA Downlink Implementation						
Function / Equipment	**HAZOPS Guide Word**	**Effect on System**	**Cause**	**Consequence**	**Hazard / Causal Factors**	**Control / Mitigation**
Pre-Implementation 2c						
RA Voice Report AC1	Loss	Controller unaware of RA	1. RT Failure (One-way) 2. Frequency blocking 3. High pilot workload	Controller might issue a clearance which does not concur with the RA	Pilot does not follow RA	In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller might attempt to communicate and disturb the flight crew	Pilot distracted from flying the RA	In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
	Incorrect (Call sign confusion)	Controller confusion	1. High pilot workload	Controller might attempt to communicate and disturb the flight crew	Pilot distracted from flying the RA	In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller delay in identifying incident aircraft Loss of situational awareness Attention diverted from other possible incidents	Controller cognitive tunnelling	Controller training
	Incorrect (False flight information, i.e. flight level)	Controller confusion	1. High pilot workload	Controller might attempt to communicate and disturb the flight crew	Pilot distracted from flying the RA	In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller delay in identifying incident aircraft Loss of situational awareness Attention diverted from other possible incidents	Controller cognitive tunnelling	Controller training
	Incorrect (Not a genuine RA)	Controller believes they are no longer responsible for separation	1. Inappropriate pilot response to TA	Controller does not maintain separation for the incident aircraft	Loss of separation	- Pilot response only necessary in the event of an RA - Pilots shall promptly return to the terms of the ATC instruction or clearance when the conflict is resolved, and notify ATC when returning to the current clearance (ICAO - Doc. 8168, part VIII para. 3.2.c) - If there is no timely reaction from the controller to resolve a conflict situation then an ACAS RA will be issued
	Incorrect (Direction of deviation)	None (Controller has no immediate source of conflicting data)	1. High pilot workload 2. Unable to report all instructions in a multiple RA scenario	N/A	N/A	N/A
	Delayed	Controller unaware of RA	1. Frequency blocking 2. High pilot workload	Controller might issue a clearance which does not concur with the RA	Pilot does not follow RA	In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)

Pre RA Downlink Implementation						
Function / Equipment	HAZOPS Guide Word	Effect on System	Cause	Consequence	Hazard / Causal Factors	Control / Mitigation
RA Voice Report AC1				Controller might attempt to communicate and disturb the flight crew	Pilot distracted from flying the RA	In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
	Too Little (No callsign)	Controller confusion	1. High pilot workload	Controller might attempt to communicate and disturb the flight crew	Pilot distracted from flying the RA	In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller delay in identifying incident aircraft Loss of situational awareness Controller attention diverted from other possible incidents	Controller cognitive tunnelling	Controller requests further RA information
	Too Little (No direction of deviation)	Controller unaware of RA direction	1. High pilot workload 2. Pilot reports preventative RA	Controller loses situational awareness Controller unable to direct non-incident aircraft away from those involved in the RA	Loss of controller situational awareness	Controller requests further RA information
	Too Much (Extended Pilot RT)	RT blocks frequency	1. High pilot workload (Stress) 2. Pilot attempts to acquire intruder visually with aid of ATC	Controller attention diverted from other possible incidents	Controller cognitive tunnelling	Controller RT given priority
				Unable to issue instructions to other aircraft	Loss of separation	If there is no timely reaction from the controller to resolve a conflict situation then an ACAS RA will be issued
	Too Much (Unnecessary Pilot RT)	RT blocks frequency	1. Inappropriate pilot response to TA	Controller confusion as to cause of conflict	Controller cognitive tunnelling	Pilot response only necessary in the event of an RA
				Unable to issue instructions to other aircraft	Loss of separation	If there is no timely reaction from the controller to resolve a conflict situation then an ACAS RA will be issued
Clearance AC1	Maintaining	Reduced pilot compliance with RA	1. RA report not received / understood by controller	Pilot less likely to follow RA	Pilot does not follow RA	In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)
	Deviating	Reduced pilot compliance with RA	1. RA report not received / understood by controller	Pilot less likely to follow RA	Pilot does not follow RA	In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)
	Conflicting	Reduced pilot compliance with RA	1. RA report not received / understood by controller	Pilot less likely to follow RA	Pilot does not follow RA	In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)
Traffic Information AC1	Conflicting	Pilot confusion	1. Essential traffic information provided on receipt of a RA report (Maastricht)	Pilot less likely to follow RA	Pilot does not follow RA	Don't give traffic information? Could make situation worse
	Irrelevant	Pilot confusion	1. Essential traffic information provided on receipt of a RA report (Maastricht)	Pilot less likely to follow RA	Pilot does not follow RA	Don't give traffic information? Could make situation worse

Pre RA Downlink Implementation

Function / Equipment	HAZOPS Guide Word	Effect on System	Cause	Consequence	Hazard / Causal Factors	Control / Mitigation
Clearance AC2	Maintain	New clearance might affect the TCAS resolution	1. Controller assumes responsibility for non-TCAS equipped aircraft 2. RA report not received / understood by controller	Controller interference might aggravate the situation	Loss of separation	Controller should not attempt to modify the flight path of an aircraft involved in a TCAS event. (ICAO?)
Clearance AC2	Deviate	New clearance might affect the TCAS resolution	1. Controller assumes responsibility for non-TCAS equipped aircraft 2. RA report not received / understood by controller	Controller interference might aggravate the situation	Loss of separation	Controller should not attempt to modify the flight path of an aircraft involved in a TCAS event. (ICAO?)
	Unable to communicate	AC2 unaware of loss of separation	1. AC2 not radio equipped (GA) 2. AC2 not in contact with controller of TCAS equipped aircraft	AC2 might manoeuvre or change direction of manoeuvre	Loss of separation	VFR
Traffic Information AC2	Incorrect	Incorrect traffic information might cause pilot to manoeuvre which might affect the TCAS resolution	1. High controller workload 2. Controller mis-informed by TCAS equipped aircraft	Controller interference might aggravate the situation	Loss of separation	Controller should not attempt to modify the flight path of an aircraft involved in a TCAS event. (ICAO?)
RADAR Mode S Surveillance AC1	Loss (Aircraft)	No RA	1. Equipment fault	TCAS does not provide conflict resolution	Loss of separation	N/A: No relation to study of RA Downlink
	Loss (Ground)	No effect	N/A	N/A	N/A	N/A
	Incorrect	False RA	1. Equipment fault	TCAS provides false conflict resolution	Pilot unaware of Mode S error	
	Delayed	N/A	N/A	N/A	N/A	N/A
TCAS Interrogation	Loss	No TCAS resolution	1. Equipment fault	TCAS unable to resolve conflict	Loss of separation	(Legislation to fit transponders to all aircraft)?
	Incorrect	TCAS gives false information	TCAS might give the same direction to both aircraft (extremely unlikely)	TCAS fails to provide increased separation	Loss of separation	None, Benefit outweighs risk

H6 Post-Implementation Operational Scenario C

Post RA Downlink Implementation						
Function / Equipment	**HAZOPS Guide Word**	**Effect on System**	**Cause**	**Consequence**	**Hazard / Causal Factors**	**Control / Mitigation**
Post-Implementation 2c						
RA Voice Report AC1	Loss	Controller aware of RA via downlink	1. RT Failure (One-way) 2. Frequency blocking 3. High pilot workload	Better controller awareness due to RA Downlink therefore controller less likely to issue clearances	Pilot does not follow RA	RA Downlink In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Better controller awareness due to RA Downlink therefore controller less likely to disturb the flight crew	Pilot distracted from flying the RA	RA Downlink In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
	Incorrect (Call sign confusion)	Controller aware of call sign error due to downlink	1. High pilot workload	Better controller awareness due to RA Downlink therefore controller less likely to disturb the flight crew	Pilot distracted from flying the RA	RA Downlink In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller able to identify incident aircraft Loss of situational awareness less likely	Controller cognitive tunnelling	RA Downlink
	Incorrect (False flight information, i.e. flight level)	Controller aware of error due to downlink	1. High pilot workload	Better controller awareness due to RA Downlink therefore controller less likely to disturb the flight crew	Pilot distracted from flying the RA	RA Downlink In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller able to identify incident aircraft Loss of situational awareness less likely	Controller cognitive tunnelling	RA Downlink
	Incorrect (Not a genuine RA)	Controller believes they are no longer responsible for separation	1. Inappropriate pilot response to TA	Controller does not maintain separation for the incident aircraft	Loss of separation	Lack of TCAS alert on HMI might prompt controller to question the RA.
	Incorrect (Direction of deviation)	Controller aware of RA direction via downlink	1. High pilot workload 2. Unable to report all instructions in a multiple RA scenario	HMI will show instructed deviation of all TCAS incident aircraft. Similar direction instructions extremely improbable	Controller might attempt to intervene	RA Downlink In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)
	Delayed	Controller aware of RA via downlink	1. Frequency blocking 2. High pilot workload	Better controller awareness due to RA Downlink therefore controller less likely to issue clearances	Pilot does not follow RA	RA Downlink In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)

Post RA Downlink Implementation						
Function / Equipment	**HAZOPS Guide Word**	**Effect on System**	**Cause**	**Consequence**	**Hazard / Causal Factors**	**Control / Mitigation**
RA Voice Report AC1				Better controller awareness due to RA Downlink therefore controller less likely to disturb the flight crew	Pilot distracted from flying the RA	RA Downlink In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
	Too Little (No callsign)	Controller can identify incident aircraft via downlink	1. High pilot workload	Better controller awareness due to RA Downlink therefore controller less likely to disturb the flight crew	Pilot distracted from flying the RA	RA Downlink In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller able to identify incident aircraft Loss of situational awareness less likely	Controller cognitive tunnelling	RA Downlink
	Too Little (No direction of deviation)	Controller aware of RA direction via downlink	1. High pilot workload 2. Pilot reports preventative RA	Controller less likely to lose situational awareness Controller more able to direct non-incident aircraft away from those involved in the RA	Loss of controller situational awareness	RA Downlink
	Too Much (Extended Pilot RT)	RT blocks frequency	1. High pilot workload (Stress) 2. Pilot attempts to acquire intruder visually with aid of ATC	Controller attention diverted from other possible incidents	Controller cognitive tunnelling	Controller RT given priority. Pilots aware of RA Downlink therefore might be less descriptive
				Unable to issue instructions to other aircraft	Loss of separation	If there is no timely reaction from the controller to resolve a conflict situation then an ACAS RA will be issued
	Too Much (Unnecessary Pilot RT)	RT blocks frequency	1. Inappropriate pilot response to TA	Controller confusion as to cause of conflict	Controller cognitive tunnelling	Pilot response only necessary in the event of an RA. Pilots aware of RA Downlink therefore might be less descriptive
				Unable to issue instructions to other aircraft	Loss of separation	If there is no timely reaction from the controller to resolve a conflict situation then an ACAS RA will be issued
Clearance AC1	Maintaining	Reduced pilot compliance with RA	1. RA report not received / understood by controller	Pilot less likely to follow RA	Pilot does not follow RA	Controller less likely to intervene with RA Downlink In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)
	Deviating	Reduced pilot compliance with RA	1. RA report not received / understood by controller	Pilot less likely to follow RA	Pilot does not follow RA	Controller less likely to intervene with RA Downlink In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)

Post RA Downlink Implementation

Function / Equipment	HAZOPS Guide Word	Effect on System	Cause	Consequence	Hazard / Causal Factors	Control / Mitigation
	Conflicting	Reduced pilot compliance with RA	1. RA report not received / understood by controller	Pilot less likely to follow RA	Pilot does not follow RA	Controller less likely to intervene with RA Downlink In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)
Clearance AC2	Maintain	New clearance might affect the TCAS resolution	1. Controller assumes responsibility for non-TCAS equipped aircraft 2. RA report not received / understood by controller	Controller interference might aggrevate the situation. Better controller awareness due to RA Downlink therefore less likely	Loss of separation	Controller should not attempt to modify the flight path of an aircraft involved in a TCAS event. (ICAO?) Enhanced by RA Downlink
Clearance AC2	Deviate	New clearance might affect the TCAS resolution	1. Controller assumes responsibility for non-TCAS equipped aircraft 2. RA report not received / understood by controller	Controller interference might aggrevate the situation. Better controller awareness due to RA Downlink therefore less likely	Loss of separation	Controller should not attempt to modify the flight path of an aircraft involved in a TCAS event. (ICAO?) Enhanced by RA Downlink
	Unable to communicate	AC2 unaware of loss of separation	1. AC2 not radio equipped (GA) 2. AC2 not in contact with controller of TCAS equipped aircraft	AC2 might manoeuvre or change direction of manoeuvre	Loss of separation	- TCAS will attempt to resolve conflict by instructing AC1, AC2 comms not essential - Airspace design: Flights entering controlled airspace must have a radio (Ref)
RADAR Mode S Surveillance AC1 / AC2	Loss (Aircraft)	No RA	1. Equipment fault	TCAS does not provide conflict resolution	Loss of separation	N/A: No relation to study of RA Downlink
	Loss (Ground)	No RA Downlink	1. Equipment fault	Similar to pre RA downlink implementation scenarios	Reliance on Downlink	Report by voice Controller training
	Incorrect	Degraded RA	1. Equipment fault	RA Downlink alerts controller to aircraft with Mode S Altitude Error eg Gillham error	Pilot unaware of Mode S error	Condition of Mode S will be known to controller
	Delayed	Delayed downlink report	1. Equipment fault	Controller surprised by degradation of system	Controller cognitive tunnelling	Controller training
TCAS Interrogation	Loss	No TCAS resolution	1. Equipment fault	TCAS unable to resolve conflict	Loss of separation	Controller remains responsible for separation
	Incorrect	TCAS gives false information	TCAS might aggravate the situation	TCAS fails to provide increased separation	Loss of separation	None, Benefit outweighs risk
RA Downlink	Loss	Controller unaware of RA until voice report	1. Equipment fault	Downlink expected, loss of confidence in the system. Controller becomes fixated on lack of report?	Controller cognitive tunnelling	Controller trained to expect either form of report
				Controller might issue a clearance which does not concur with the RA	Pilot does not follow RA	In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller might disturb the flight crew	Pilot distracted from flying the RA	In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)

Post RA Downlink Implementation						
Function / Equipment	**HAZOPS Guide Word**	**Effect on System**	**Cause**	**Consequence**	**Hazard / Causal Factors**	**Control / Mitigation**
RA Downlink	Incorrect (Continuous)	Continuous RA	1. Equipment fault	Uncertainty as to whether RA is valid (if there is a credible intruder aircraft)	Controller cognitive tunnelling	Controller procedures must be defined for this situation
			1. Equipment fault	Controller might ignore a real RA	Controller cognitive tunnelling	Controller procedures must be defined for this situation
	Incorrect (Occasional)	Spurious RA	1. Equipment fault	Controller might think that they are not responsible for the aircraft.	Loss of separation	Controller might confirm RA with Pilot
	Delayed	Voice report might come before downlink	1. Equipment fault	Downlink expected, loss of confidence in the system. Controller becomes fixated on lack of report?	Controller cognitive tunnelling	Controller trained to expect either form of report
				Controller might issue a clearance which does not concur with the RA	Pilot does not follow RA	In the event of an RA, pilots shall follow the RA even if there is a conflict between the RA and an ATC instruction to manoeuvre (ICAO - Doc. 8168, part VIII para. 3.2.c)
				Controller might disturb the flight crew	Pilot distracted from flying the RA	In the event of an RA, pilots shall respond by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane (ICAO - Doc. 8168, part VIII para. 3.2.c)
	Too little	Downlink ends before RA	1. Equipment fault	Controller believes they are responsible for separation and issues clearance	Pilot does not follow RA	Clear of conflict report required from pilot, or obvious from RADAR. Regulations should be clear regarding transfer of responsibility for separation
	Too much (changing RA)	Max. Three possible changes to the RA (Original plus two adjustments)	1. Complicated RA scenario	Controller becomes fixated on the TCAS incident	Controller cognitive tunnelling	The CWP display should be designed to minimise confusion. Similar types of RA have been grouped, i.e. weakening RAs will not be shown (HMI)
	Too much (information)	Increased data on screen	1. Equipment fault	Data might block other relevant information	Controller cognitive tunnelling	Emergency data takes precedence
		Controller distraction	1. Equipment fault	Loss of situational awareness	Controller cognitive tunnelling	The CWP display should be designed to minimise confusion. Similar types of RA have been grouped, i.e. weakening RAs will not be shown (HMI)
	Too much (every aircraft appears to have an RA)	Controller confusion	1. Equipment fault	Loss of situational awareness	Controller cognitive tunnelling	Controller training
	Corrupted	Display indicates opposite direction to RA	1. Equipment fault	Controller confusion, increased probability of talking to aircraft	Pilot distracted from flying the RA	High quality of Mode S comms (rare event)
Display	Similar direction	HMI shows TCAS giving similar resolution to incident aircraft	1. Equipment fault	Controller sees two aircraft with descend / climb RA	RADAR sweep catches simultaneous climb / descend instructions to both incident aircraft	Next RADAR update should show resolution of conflict