AFI RVSM PRE-IMPLEMENTATION SAFETY CASE CORE DOCUMENT

FINAL VERSION

FEBRUARY 2008

READERS NOTES

DOCUMENT RELEASE APPROVAL

The AFI RVSM Pre-Implementation Safety Case is approved for release by the AFI Regional Program Office (ARPO) located at the ICAO ESAF office

Apolo Kharuga
ARPO

Page intentionally left blank.

Document change record

Version	Issue date	Author	Change Description
0.1	▸02/06/06◂	ALTRAN Technologies ▸ Julien Lapie, Richard Beaulieu National Aerospace Laboratory (NLR) ▸ Geert Moek, Job Smeltink	Initial working draft for ARMA review
0.2	▸09/06/06◂	ALTRAN Technologies ▸ Julien Lapie, Richard Beaulieu National Aerospace Laboratory (NLR) ▸ Geert Moek, Job Smeltink	Working draft for initial AFI RVSM Project Management Team (PMT) review
0.3	▸23/06/06◂	ALTRAN Technologies ▸ Julien Lapie, Richard Beaulieu National Aerospace Laboratory (NLR) ▸ Geert Moek, Job Smeltink	Second working draft for initial AFI RVSM Project Management Team (PMT) review
0.4	▸08/11/06◂	ALTRAN Technologies ▸ Julien Lapie, Richard Beaulieu National Aerospace Laboratory (NLR) ▸ Geert Moek, Job Smeltink	Third working draft for initial AFI RVSM Project Management Team (PMT) review. Includes amendments following Core Team response to open issues
0.5	▸15/12/06◂	ALTRAN Technologies ▸ Julien Lapie, Richard Beaulieu National Aerospace Laboratory (NLR) ▸ Geert Moek, Job Smeltink	Fourth working draft following AFI RVSM Task Force 11
0.6	▸08/11/06◂	ALTRAN Technologies ▸ Julien Lapie, Richard Beaulieu National Aerospace Laboratory (NLR) ▸ Geert Moek, Job Smeltink	Fifth working draft for AFI RVSM Task Force 12
0.7	▸30/07/07◂	ALTRAN Technologies ▸ Julien Lapie, Richard Beaulieu National Aerospace Laboratory (NLR) ▸ Geert Moek, Job Smeltink	Fifth working draft following AFI RVSM Task Force 13
Final	27/02/08	AFI RVSM Project Management Team	Final copy following AFI RVSM PMT Johannesburg 25 – 27 Feb 2008

Summary

The justification for the implementation of RVSM in AFI airspace is the requirement to provide additional airspace system capacity to meet the ever-rising number of aircraft movements as well as accessibility to more fuel efficient levels. In conjunction with this the benefits of RVSM will be available to the aviation community. Traffic forecasts have indicated that the number of movements will continue to increase, and implementation of RVSM is considered to be the most cost effective means of meeting this challenge through the provision of six additional flight levels for use in the airspace from FL290 to FL410 inclusive.

As required in other regions AFI is also required to conduct safety assessments to periodically establish the vertical collision risk measured against the overall Target Level of Safety (TLS), as determined by ICAO. This requirement alone is not sufficient to demonstrate that RVSM will be safe in AFI airspace. A Safety Policy was approved laying out the processes that are required. The three main deliverables of the RVSM Safety activities are Functional Hazard Assessment (FHA), Collision Risk Assessment (CRA) and National Safety Plans. These three deliverables form the major input to the development of the AFI RVSM Pre-Implementation Safety Case (PISC). In addition, the PISC contains those elements of the AFI RVSM Programme to be taken into account when addressing the safe introduction of RVSM in AFI RVSM airspace.

Twenty eight (28) hazards for the core airspace and twenty (20) hazards for the switch-over period were identified, assessed and classified during the process. All the risks identified for the Core Airspace and Switchover period were assessed as tolerable, except for one, provided that the proposed mitigation is implemented. The hazard in question is identified as a deviation from a clearance in airspace without surveillance. This is an inherent hazard in any airspace without surveillance and is thus extremely difficult to mitigate against.

The PISC sets out the safety requirements broken down to the level of system elements. It establishes all the arguments and evidence necessary to demonstrate that the ICAO RVSM Concept as applied to the AFI RVSM Airspace, and the Implementation of RVSM by the participating States, will be tolerably safe when assessed against the requirements of the AFI RVSM Safety Policy.

The PISC demonstrates that this aim has been achieved, by means of the following principal safety arguments:

(a) That a set of Safety Requirements have been specified for RVSM that fully address all the functionalities, performances and integrity requirements necessary to ensure that the safety risks under RVSM will be tolerable.
(b) That RVSM for the AFI region has the potential to satisfy the RVSM Safety Requirements.
(c) That Implementation of the RVSM Concept by individual participating States will satisfy the RVSM Safety Requirements.
(d) That the Switch-Over from CVSM, 2000 ft (600m), to RVSM, 1000 ft (300m), will not adversely affect the safety of the on-going air traffic operations. Each of the above arguments is developed in the relevant section of the PISC, evidence is shown that all the arguments are valid and detailed conclusions are drawn.

A sufficient set of safety requirements have been specified for AFI RVSM, including those generated by the Functional Hazard Assessments (FHA). Identified hazards are sufficiently mitigated. The RVSM Concept satisfies the safety requirements for each RVSM system element. States within the RVSM programme have made steady progress towards safe implementation and are ready. The identification, and implementation of measures to control and/or mitigate, hazards and risks associated with Switch-over were identified through the

FHA. The mitigating factors were identified and incorporated into a RVSM Countdown and Switchover Plan produced by AFI. Based on the conclusion drawn in each of the above arguments and subject to the conditions mentioned, the application of the ICAO RVSM Concept in the AFI Region, and the Implementation of RVSM by the participating States can be considered as tolerably safe and satisfying the criteria defined in the AFI RVSM Safety Policy.

Page intentionally left blank.

Page intentionally left blank.

Table of contents

Page intentionally left blank.

Table of figures

Page intentionally left blank.

Table of tables

Page intentionally left blank.

1. Introduction

1.1 Aim and purpose

This document constitutes the AFI RVSM Pre-Implementation Safety Case (PISC).

It aims to show by means of argument and supporting evidence that AFI RVSM will be safe in operational service, i.e. to provide assurance that the operations of the AFI RVSM System[1] (cf. **Appendix A**) will be safe. In the context of the AFI RVSM programme, what is safe is defined by the Safety Objectives from the AFI RVSM Safety Policy **[2]**.

The PISC has been produced for the AFI RVSM Programme in response to the AFI RVSM Safety Policy **[2].** Its completion is a key element of the Go/Delay decision on the implementation of RVSM in the AFI Region

The PISC has been developed by ALTRAN - ATM Division and the National Aerospace Laboratory NLR in co-operation with the AFI RVSM Project Management Team **[66]**.

This version constitutes the final document. This final document has been reviewed by the AFI RVSM Project Management Team (PMT), amended where required and submitted.

In particular, a major objective that constantly needs to be assessed is the total vertical collision risk estimate which needs to be measured against the total vertical Target Level of Safety (TLS) of 5×10^{-9} fatal accidents per flight hour **[68]**. Nonetheless, it has been deemed useful to present the currently available information for evaluation. Moreover, States have agreed at APIRG/15/16 and relevant ARTF, to take the necessary steps to significantly reduce the rate of vertical incidents. Consequently, the vertical collision risk assessment is currently being updated with the third result expected prior to implementation.

The completed PISC will be then submitted to ICAO Montreal to be placed on the agenda for review and approval by the ICAO Air Navigation Commission (ANC).

[1] In the ATM meaning

1.2 Background

The Reduced Vertical Separation Minimum (RVSM) is planned to be introduced into AFI (Africa Indian Ocean) airspace on 25 September 2008. As a result, the vertical separation between RVSM-approved aircraft operating between Flight Levels 290 and 410 inclusive will be reduced from 600 m (2000 ft) to 300m (1000ft).

The AFI RVSM Programme was developed by the AFI RVSM Task Force (ARTF) based on its mandate as assigned by APIRG/14 **[14]** following the endorsement by APIRG/13 **[15]** of the objectives of capacity and potential economy benefits associated with RVSM.

The 52 States that are participating in the AFI RVSM Programme are listed in the following table:

Algeria *	Angola	Benin	Botswana
Burkina Faso	Burundi	Cameroon	Cabo Verde *
Central African Republic	Chad	Comores	Congo
Côte d'Ivoire	Djibouti	Democratic Republic of Congo	Egypt *
Equatorial Guinea	Eritrea	Ethiopia	Gabon
Ghana	Guinea Bissau	Guinea	Kenya
Lesotho	Liberia	Libyan Arab Jamahiriya	Madagascar
Malawi	Mali	Mauritania	Mauritius
Mozambique	Namibia	Niger	Nigeria
Reunion	Rwanda	Sao Tome	Senegal *
Seychelles	Sierra Leone	Somalia	South Africa
Sudan	Swaziland	Tanzania	The Gambia
Togo	Uganda	Zambia	Zimbabwe

Table **1** : States participating in the AFI RVSM Programme

States marked with "*" have already fully implemented RVSM or are part of an RVSM transition area. Nevertheless, they are participating in the RVSM Programme as part of the AFI region and should address issues related to full RVSM airspace implementation and/or coordination with neighbouring FIRs.

The AFI RVSM Programme consists of five sub-programmes including a Safety sub-Programme. The objective of the Safety sub-Programme is to ensure, and to provide evidence on, the compliance of the AFI RVSM Programme with the AFI RVSM Safety Objectives stated in the AFI RVSM Safety Policy **[2]**. It requires five deliverable documents as follows:

- Functional Hazard Assessment (FHA) report;
- Collision Risk Assessment (CRA) report;
- National Safety Plans (NSPs);
- Pre Implementation Safety Case (PISC); and
- Post Implementation Safety Case (POSC).

This document constitutes the Pre Implementation Safety Case (PISC).

1.3 Scope

The AFI RVSM PISC is the documented assurance (argument and evidence) of the achievement and maintenance of the safety of AFI RVSM operations. It is a System (Project) Safety Case documenting the demonstration of the safety of the **change** that constitutes the introduction of the AFI RVSM System.

It has been developed on the basis of the experience taken from the EUR RVSM PISC **[80]** and of the guidance provided by the EUROCONTROL Safety Case Development Manual **[88]**.

The PISC scope is determined by the AFI RVSM Safety Policy **[2]**. Like its European counterpart **[78]**, the AFI RVSM Safety Policy covers two main elements. Firstly, it is fully compliant with the safety objective for the vertical collision risk and the Target Level of Safety (TLS) from the ICAO RVSM Guidance Material **[1]**. Secondly, it takes a broader perspective in that, additionally to the Collision Risk Assessment, a full Functional Hazard Assessment looking at the whole AFI RVSM system, including air and ground segments and the proposed operational concept, must be conducted; and that States must ensure a safe implementation of RVSM through National Safety Plans to be developed with the support of the AFI RVSM Programme.

In line with the above, the AFI RVSM Safety sub-Programme deliverables, CRA Report, FHA Report and NSPs, constitute the main inputs to the AFI RVSM PISC. In addition, other elements of the AFI RVSM Programme that are relevant to the safety of RVSM in the AFI Region are also taken into account. The PISC, then, combines the various inputs to show that the Safety Objectives from the AFI RVSM Safety Policy are being met.

As a Pre-Implementation Safety Case, the four main, continuous stages of the lifecycle of the change (the AFI RVSM System) are to be addressed, namely:

- (i) The application of the ICAO RVSM Concept in the AFI Region (pre-change);
- (ii) The implementation of the resulting concept by the AFI States (pre-change);
- (iii) The migration (switch-over) from CVSM operations to RVSM operations (change); and,
- (iv) The on-going AFI RVSM operations (post-change)[2].

In this lifecycle, two operational situations are considered, namely a stabilised situation of mature RVSM operations (stages (i), (ii) and (iv)) and the specific switch-over operations on a specific date and time (stage (iii)).

It should be noted that the provision of a business justification for AFI RVSM has been agreed to be beyond the scope of this document however, the ongoing RVSM operations in Europe, South America and other regions provide sufficient justification for the implementation of RVSM in the AFI Region to the benefit of the aviation community as a whole.

[2] As a post-change stage, only monitoring is addressed in this PISC in order to show that the associated operations will be shown to be safe.

1.4 Structure of the document

Section 2 of the document provides important background information on the safety management of AFI RVSM through the description of the AFI RVSM Safety Policy and its main elements (safety statements, objectives, deliverables and responsibilities). It presents also how the PISC aim is developed using Goal Structuring Notation (GSN) and how the overall safety claim is decomposed into four principal safety arguments.

Sections 3 to **6** address each of the four principal safety arguments by further decomposition into lower-arguments and provision of the supporting evidence. They are structured similarly:

- Objective related directly to the principal safety argument
- Strategy (breakdown of the principal safety argument into lower-level arguments) and its rationale
- Lower-level arguments and supporting evidence

The evidences are provided either in terms of text or discussion in the sub-section, or in terms of reference to a relevant appendix or an external document.

Section 7 and **section 8** provides the caveats: the assumptions on which the PISC depends and the outstanding issues (that must be resolved before the PISC overall safety claim to be considered to be valid), if any, respectively.

Section 9 provides the conclusion of the PISC.

Annex 1 provides the references and **Annex 2** presents a list of abbreviations and explanation of terms.

Annex 3 outlines the GSN principles for the purpose of the PISC and **Annex 4** provides a synthesis of the whole PISC argument and evidence structure.

Appendices A to H are provided in a separate document.

Appendix A provides an overview of the AFI RVSM System, subject of the Pre Implementation Safety Case.

Appendix B presents a summary of the AFI RVSM Functional Hazard Assessment.

Appendix C provides the set of AFI RVSM System Elements Requirements (SER's).

Appendix D provides the approach for and resulting evidence of the realisation of the SER's at Concept and Implementation levels, i.e. in the design and in the implementation of the AFI RVSM System.

Appendix E contains details related to airspace design issues.

Appendix F provides background material on ARMA's activities with respect to Readiness Assessment and height monitoring.

Appendix G presents a summary of the results of the Collision Risk Assessment (CRA).

Appendix H provides detailed material on the development of National Safety Plans and on the review of States' safety readiness.

Page intentionally left blank.

2. AFI RVSM Safety Management

2.1 Introduction

This section describes two important elements of AFI RVSM Safety Management, namely the AFI RVSM Safety Policy and the overall safety argument used to demonstrate that the AFI RVSM Safety Objectives are being met. The AFI RVSM Safety Policy successively describes the definition of the AFI RVSM Safety Policy, the AFI RVSM Safety Objectives, the Safety Deliverables and the Safety Responsibilities (section 2.2). The overall Safety Argument and its decomposition into four principal arguments are described in section 2.3.

2.2 AFI RVSM Safety Policy Document

2.2.1 Introduction

The starting point for the AFI RVSM Safety Policy has been the RVSM Guidance Material **[1]**. The latter begins with a statement that the implementation of RVSM should be based on a safety assessment, demonstrating that RVSM safety objectives have been satisfied (meaning that AFI RVSM will be safe in operational service). The safety assessment should include a Collision Risk Model (CRM) for the airspace under consideration in accordance with the RVSM Guidance Material. The RVSM Safety Objective for technical risk stated in the RVSM Guidance Material is a TLS of 2.5×10^{-9} fatal accidents per flight hour. The RVSM Guidance Material also states that the RVSM Safety Objective for overall risk should be set by regional agreement, taking due account of existing ICAO guidance on safety objectives and of safety objectives applied in other ICAO Regions.

Based on the above, the AFI RVSM Task Force has developed the AFI RVSM Safety Policy **[2]** for which, in particular, use has been made of the safety assessment work for the implementation of RVSM in the European Region (which benefited again from the first implementation of RVSM in the NAT Region).

2.2.2 AFI RVSM Safety Policy

The Safety Policy for RVSM implementation in the AFI Region has been established to meet the requirements of ICAO Standards and Recommended Practices and guidance material on managing collision risk consequent on the implementation of RVSM.

The following statements define the Safety Policy of the AFI RVSM Programme **[2]**:

(a) The AFI RVSM Programme uses an explicit, pro-active approach to safety management in the development, implementation and continued operation of RVSM;

(b) The responsibility of management for the safety performance of the RVSM Programme is recognised. The RVSM programme manager is responsible for the overall management of the Programme. The RVSM safety programme manager is responsible to the RVSM programme manager for ensuring the compliance of the Programme with AFI Safety Policy and appropriate <u>international standards and requirements</u>. The RVSM safety programme manager is also responsible for liaison with the Regulation Authorities;

(c) The implementation of RVSM shall be conducted in accordance with <u>ICAO requirements</u> and requires <u>ninety percent RVSM approved aircraft</u> operating within AFI;

(d) The safety of air navigation has been given the highest priority in the development of the RVSM operational concept and the Implementation Programme; and

(e) The RVSM Programme shall minimise the program's contribution to the serious or risk bearing incidents or aircraft accidents as far as is reasonably practicable.

2.2.3 AFI RVSM Safety Objectives

The AFI RVSM Safety Objectives have been established to meet the AFI RVSM Safety Policy statements. These safety objectives will be complemented by safety requirements resulting from the Functional Hazard Assessment.

The following statements define the AFI RVSM Safety Objectives **[2]**:

(i) The RVSM Programme shall conduct a full Functional Hazard Analysis looking at the whole system including air and ground segments and the proposed operational concept. This analysis shall adopt a total aviation system perspective and a risk based approach to the classification of hazards. The analysis shall include, but not be restricted to, those risks already identified by ICAO for RVSM implementation;

(ii) The RVSM programme shall, as its principal safety objective, minimise the program's contribution to the risk of an aircraft accident. The RVSM Programme recognises the AFI safety objectives and strategy, in particular the general objective to improve safety levels by ensuring that the number of ATM induced accidents and serious or risk bearing incidents do not increase and, where possible, decrease. Therefore, the implementation of RVSM shall not adversely affect the risk of en-route mid-air collision;

(iii) The RVSM Programme shall establish an explicit Safety sub-Programme to ensure that Programme's contribution to the risk of an aircraft accident is minimised in accordance with the principal safety objective;

(iv) In accordance with ICAO Guidance Material the management of vertical collision risk within RVSM airspace shall meet the Target Level of Safety of 5×10^{-9} fatal accidents per flight hour;

(v) In accordance with ICAO Guidance Material, the risk of mid-air collision in the vertical dimension within RVSM airspace, due to technical height-keeping performance, shall meet a Target Level of Safety of 2.5×10^{-9} fatal accidents per flight hour;

(vi) Guidance shall be given to the States to explain the necessary activities to provide evidence about the safe implementation of RVSM on the national level and subsequently assure the preparedness of the States.

The Safety Objective for overall vertical risk has been set by regional agreement as a TLS of 5×10^{-9} fatal accidents per flight hour. The same TLS has been in use in e.g. the NAT and EUR Regions for several years. It is also remarked that it was agreed that the overall TLS would not be partitioned into individual budgets, for the risk due to different causes. This does not preclude, however, the assessment of the technical risk against a smaller TLS of 2.5×10^{-9} fatal accidents per flight hour.

As stated above, the safety objectives have been established to meet the AFI RVSM Safety Policy statements. Although it is beyond the scope of the PISC to demonstrate the consistency between the safety objectives and the safety policy statements, Table 2 shows that each statement is covered by several safety objectives. The Safety Policy statements (a), (d) and the larger part of (b) are formulated in fairly general terms whereas otherwise specific statements like international standards, ICAO requirements and minimise the program's contribution to an incident or accident are used. The fact that e.g. an FHA and a CRA have been conducted can be taken as evidence of the safety policy statements being met by the safety objectives. In the Table, the more direct relationships are represented by the symbol * whereas the less direct relationships are represented by the symbol (*). The only safety policy statement that is not clearly represented by the six safety objectives is the second part of statement (c), viz. "requires ninety percent RVSM approved aircraft within the Region". This statement, however, is more related to operational efficiency than to safety. It is addressed in **Appendix F**.

AFI RVSM Safety Policy statement	Safety objective					
	(i)	(ii)	(iii)	(iv)	(v)	(vi)
(a)	(*)	(*)	(*)	(*)	(*)	(*)
(b)	(*)	(*)	(*)	*	*	(*)
(c)	*		(*)	*	*	(*)
(d)	(*)	(*)	(*)	(*)	(*)	(*)
(e)	(*)	*	(*)	(*)	(*)	(*)

Table 2 : Relationship between AFI RVSM Safety Policy statements and safety objectives

2.2.4 AFI RVSM Safety Deliverables

The AFI RVSM Safety Policy has defined five deliverables in support of the provision of the assurance that the objectives stated in the AFI RVSM Safety Policy are met. The first three deliverables are:

- AFI RVSM Functional Hazard Assessment (FHA) report;
- AFI RVSM Collision Risk Assessment (CRA) report; and
- AFI RVSM National Safety Plans (NSPs).

These three deliverables are used as main inputs to the other two deliverables, the PISC and the POSC. All five deliverables are briefly discussed below.

2.2.4.1 Functional Hazard Assessment report

A full Functional Hazard Assessment (FHA) has been conducted by ALTRAN - ATM Division and has been endorsed by the AFI RVSM Task Force 6 in May 2005 **[22]**. It is documented in **[71]**.

This deliverable consists of an FHA and of the first steps of a PSSA (Preliminary System Safety Assessment), according to the EUROCONTROL Safety Assessment Methodology **[87]**. It provides assurance that all hazards and risks associated with RVSM in the AFI Region have been identified and classified, and that risk mitigation measures have been identified to ensure the achievement of tolerable safety levels.

The scope of the assessment addressed the following:

- The "AFI RVSM Core Airspace": RVSM operations in a mature situation, one year after implementation; and
- The "AFI RVSM Switch-Over Period": the change-over on the day of RVSM Implementation

As the surveillance capabilities and level of ATM services differ from FIR to FIR within the AFI Region, four different environmental types have been considered when identifying and assessing the hazards.

Due to the implementation of RVSM in the CAR and SAM Regions in January 2005, it was agreed that it was not necessary to address any transition airspace between RVSM and non-RVSM airspace in this FHA.

On implementation of AFI RVSM there will be no non-RVSM airspace surrounding AFI as AFI will be the last region to implement thus doing away with transition areas which is consequent with the AFI safety policy

2.2.4.2 Collision Risk Assessment report

Two Collision Risk Assessments have been conducted by the National Aerospace Laboratory NLR and are documented in **[68]** and **[69]**. A third is under development. The scope of the assessment addressed the following:

- Assessment of the technical vertical collision risk against a technical vertical TLS of 2.5 x 10^{-9} fatal accidents per flight hour; and
- Assessment of the total vertical collision risk against a total vertical TLS of 5 x 10^{-9} fatal accidents per flight hour.

2.2.4.3 National Safety Plans

Each State participating in the AFI RVSM Programme has developed its own National Safety Plan (NSP) for the implementation of RVSM in its local airspace. The development of these plans has been supported by a NSP template **[47]** and two RVSM NSP workshops on NSP **[35]** and **[36]**. The plans have been submitted to ICAO for validation/review (through an NSP Validation Panel - NSPVP) and to the appropriate national regulator for approval.

2.2.4.4 Overall Safety Case: PISC and POSC

In addition to the previous three deliverables, the AFI RVSM Safety Policy document has defined an overall RVSM Safety Case based on a Pre Implementation Safety Case (PISC) and a Post Implementation Safety Case (POSC) as deliverable.

The current document constitutes the Pre Implementation Safety Case (cf. sections 1.1 and 1.3).

The Post-Implementation Safety Case essentially aims to confirm post implementation the estimates, assumptions and efficiency of risk mitigation measures made prior to the actual RVSM implementation in the AFI Region. The POSC will be produced in three stages: 6, 12 and 18 months after implementation.

2.2.5 AFI RVSM Safety Responsibilities

With regard to the AFI RVSM safety responsibilities, a distinction is made between responsibility for the application of the RVSM Concept in the AFI Region and the actual implementation of this concept by the participating States (cf. section 2.3.7).

2.2.5.1 Application of the RVSM concept

The AFI RVSM Programme Office (ARPO) is responsible for the application of the RVSM concept being tolerably safe and, where possible, the risk being as low as is reasonably practicable. ARPO is therefore responsible for the following elements of the AFI RVSM Programme:

- Overall RVSM Programme management;
- Support to aircraft operators and air traffic service providers;
- Development and validation of ATS procedures;
- Development of ATS training guidance material;
- Facilitation of air traffic services readiness for RVSM operations;
- Facilitation of operator readiness for RVSM operations;
- Institution of a Regional Monitoring Agency (ARMA);
- Together with the ARMA, provision of monitoring infrastructure for aircraft height-keeping performance;
- Together with the ARMA, analysis of aircraft height-keeping performance data; and
- Overall Safety Case development.

2.2.5.2 Implementation of the RVSM concept

Each State participating in the AFI RVSM Programme is ultimately responsible for the safe implementation of the RVSM concept in its airspace, even if that airspace has been delegated to an ATM provider.

The national RVSM programme managers are responsible for ensuring that all requirements concerning the safe implementation of RVSM in their States have been met. The means of providing this assurance include the National Safety Plans.

The AFI RVSM Programme Office (ARPO) has a secondary responsibility for the implementation of the RVSM concept in the provision of:

- Guidance to States on the safe implementation of the RVSM concept;
- AFI RVSM FHA results for local adaptation; and
- Review of National Safety Plans and States' readiness for RVSM operations.

2.3 AFI RVSM Overall Safety Argument

2.3.1 Introduction

As noted in section 1.1, the aim of the AFI RVSM PISC is to show by means of argument and supporting evidence (assurance) that AFI RVSM will be safe in operational service, meaning that the operations of the AFI RVSM System[3] will be safe.

To achieve this, a safety argument and evidence structure is developed using a recognised good practice, i.e. Goal Structuring Notation (GSN). An outline of the GSN principles is presented in **Annex 3**.

2.3.2 Overall Claim

The PISC aim is considered to be achieved by demonstrating the overall **Safety Claim A0**:

A0: "AFI RVSM will be safe in operational service"

2.3.3 Context

An overview of the AFI RVSM System is provided in **Appendix 1**.

2.3.4 Safety criteria

In the context of the overall claim **A0,** what is safe is defined by safety criteria **Cr01** based on the AFI RVSM Safety Objectives (refer to section 2.2.3), as follows:

Cr01: "Achieve AFI RVSM Safety Objectives"

Cr01 encloses sub-criteria defining absolute safety levels required by the AFI RVSM Safety Policy **[2]**:

- a) ***TLS of 5x10^{-9} fatal accidents per flight hour for total vertical collision risk***
- ***b) TLS of 2.5x10^{-9} fatal accidents per flight hour for technical vertical collision risk***
- ***c) Risk Classification Scheme (RCS) for the risks associated with FHA hazards***

The items (a) and (b) define the safety targets for the collision risks. They are derived from the AFI RVSM Safety Objectives **(v)** and **(iv)** respectively. The item (c) defines the tolerable risk levels for the hazards identified during the FHA process **[71]**. It is derived from the AFI RVSM Safety Objective **(i)**.

Cr01 is completed by the AFI RVSM Safety Objectives **(ii)**, **(iii)** and **(vi)** not directly related to absolute safety levels, but required by the Safety Policy **[2]** to be demonstrated as achieved.

[3] In the ATM meaning

2.3.5 Principal safety arguments

The strategy (***St00***) consists in the decomposition of the overall **Safety Claim A0** into four principal arguments which relate to:

- (a) the specification of how the AFI RVSM System (change) shall be safe *"in principle"*, on the basis of the safety criteria (**Cr01**)
- (b) the four main, continuous stages of the lifecycle of the AFI RVSM System:
    - (i) The application of the ICAO RVSM Concept in the AFI Region (pre-change);
    - (ii) The implementation of the resulting concept by the AFI States (pre-change);
    - (iii) The migration (switch-over) from CVSM operations to RVSM operations (change); and,
    - (iv) The on-going AFI RVSM operations (post-change).

Noting that item (a) addresses the four stages of item (b), and that the monitoring of on-going operations is part of the concept and of its implementation, the strategy ***St00*** consists in arguing that each stage corresponding to the items (i) and (ii) and (iii) are safe on the basis of item (a), while considering item (iv) embedded in the items (i) and (ii)[4]. The resulting four principal safety arguments are:

- **A1** asserts that AFI RVSM is safe "***in principle"***, i.e. subject to subsequent and correct implementation of the safety requirements. The strategy (***St01***) consists in the demonstration that a set of <u>necessary</u> safety requirements which fully address all the functionality, capacity, performances and integrity has been specified for each stage of the AFI RVSM System lifecycle, including the changeover and the monitoring of on-going operations. Necessary in this context means necessary to achieve the safety criteria **Cr01** (the AFI RVSM Safety Objectives);
- **A2** asserts that the AFI RVSM Concept, as developed by AFI RVSM Programme Office (ARPO), is safe through the satisfaction, initially in the AFI RVSM System design, of the safety requirements. The strategy (***St02***) consists in the demonstration that the safety requirements have been properly addressed in the design of the constituent elements of the AFI RVSM System, including the System Monitoring element;
- **A3** asserts that the implementation of the AFI RVSM Concept is safe. The strategy (***St03***) consists in the demonstration that the safety requirements have been properly addressed in the implementation of the AFI RVSM System as designed, including its System Monitoring element, by the individual participating States and the ARMA; and
- **A4** asserts that the migration (switch-over) from the CVSM to RVSM will not adversely affect the safety of the on-going air traffic operations. The strategy (***St04***) consists in the demonstration that the switch-over safety requirements will be fully satisfied in the design and the implementation of the switch- over concept.

[4] Note that the lifecycle phase "on going operations" could have been addressed in a separate principal argument asserting that the on-going operations will be shown to be safe. However for historical reasons, this lifecycle phase has been addressed as part of the concept and of its implementation, considering the system monitoring as a constituent element of the AFI RVSM System.

Figure **1** illustrates this argument structure graphically using GSN:

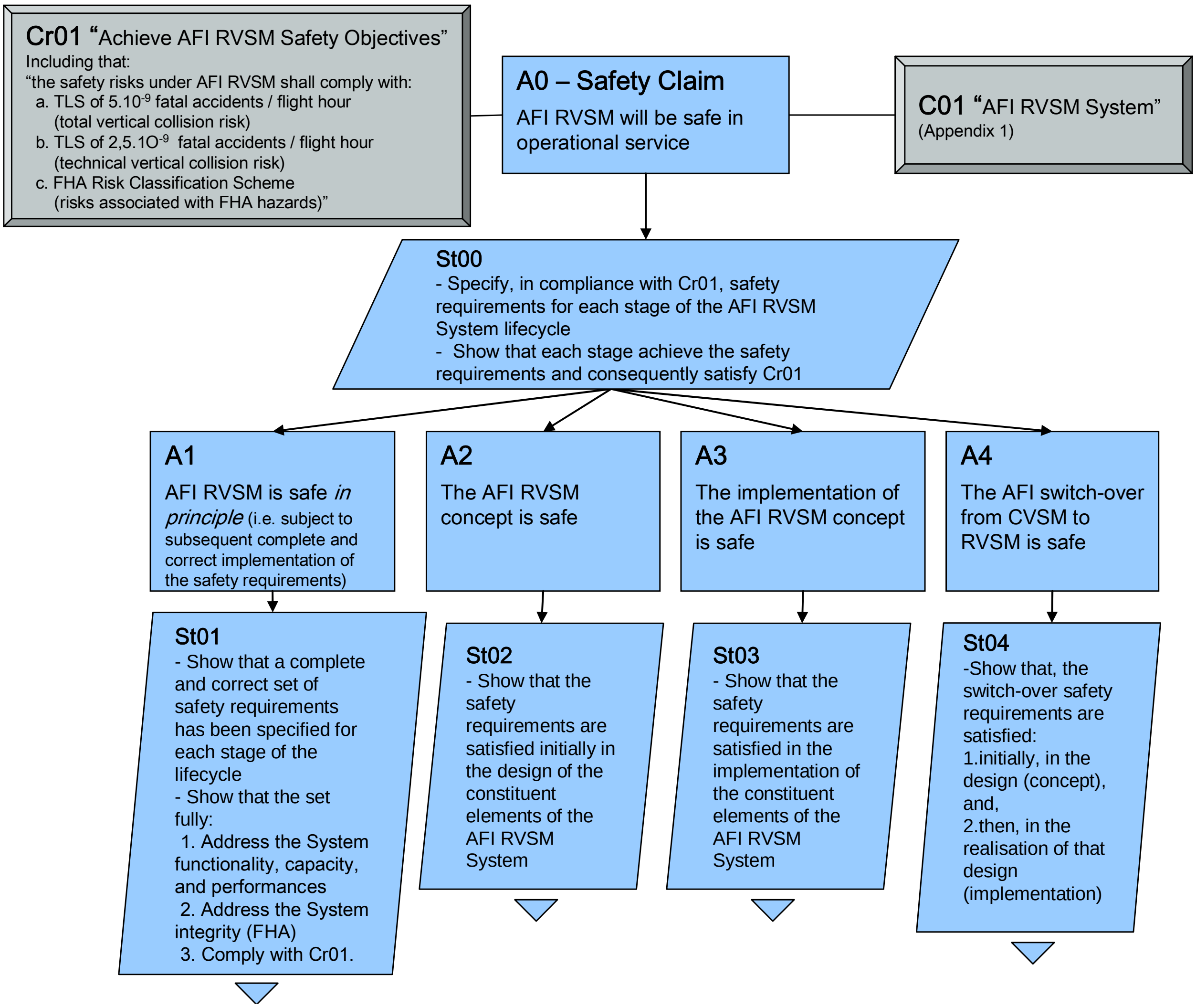

Figure **1** : PISC overall Safety Argument

The principal safety arguments **A1 – A4** are considered to be necessary and sufficient to demonstrate **A0**, since:

- The AFI RVSM Safety Objectives (**Cr01**) are achieved under **A1**, through the set of safety requirements which address the whole System lifecycle; and,
- The AFI RVSM Safety Objectives are subsequently disseminated in **A2**, **A3**, and **A4** (corresponding to the lifecycle phases), since the corresponding System lifecycle phases are demonstrated as safe with reference to the set of safety requirements addressed in **A1**.

In addition to **A1**, the decomposition formally addresses two “directions”:

- the concept (design) and the implementation (realisation of the design) levels; and,
- the three main stages of the AFI RVSM System, namely the mature and switch-over RVSM operations, and the monitoring of the on-going RVSM operations.

The decomposition along these “two directions” is discussed in some more detail in sections 2.3.6 and 2.3.7 respectively.

Due to the special nature of the switch-over, its concept and implementation are addressed jointly under the single argument **A4**.

The applicability of the safety criteria depends on the phases of the AFI RVSM System lifecycle (e.g. TLS are only applicable for mature RVSM operations and in concept, i.e. in the design). This applicability will be reflected in the applicability of the safety requirements which are resulting from. The traceability will be kept until the end of the process (presentation of evidence). Compliance of the safety requirements to the AFI RVSM Safety Objectives will be discussed in details under **A1** in section 3.

The four principal safety arguments reflect the way the safety of AFI RVSM has been addressed. In particular, they may be associated with the following questions:

- **A1:** How will the AFI RVSM System be safe?
- **A2:** How can this be done in the design of the System and has it been done (and how)?
- **A3:** How can this be done in the implementation of the System, and has it been done (and how?)
- **A4:** How can this be done in the design and implementation of the switch-over, and has it been done (and how?)
- **A5:** How can this be done in the design and implementation of the operational service monitoring, and has it been done (and how?)

The question “how can this be done” can also be described as what is the approach of satisfaction of the safety requirements **[58]**.

Each of the four principal safety arguments **A1 – A4** is further developed in the relevant section of this document (sections 3 to 6, respectively), together with the lower-level arguments and supporting direct and backing evidence.

A synthesis of the overall safety assurance (i.e. argument and evidence) structure is presented in **Annex 4**.

2.3.6 Different stages of RVSM operations

The following two stages of RVSM operations are distinguished:

Stage a) A 24 hour period of time around the actual switch-over from CVSM to RVSM operations

Stage b) A stabilised situation of mature RVSM operations.

Each of the stages may be further subdivided into stages of normal or abnormal operating conditions (see e.g. section 4.2.3 of the AFI RVSM FHA **[71]**).

Stage a) corresponds to the specific period of 24 hours around the time of RVSM introduction, i.e. the “AFI RVSM switch-over period” considered by the FHA.

Stage b) corresponds to the situation whereby RVSM has been fully operational for some time with all introductory problems having been solved, i.e. it corresponds to the “AFI RVSM core airspace” considered by the FHA. It is expected that this stage will be reached fairly quickly after the switch-over. A Quick Response Team (QRT) has been established to deal with any introductory or transition problems during the intermediate period of time. It is described in the addendum to the AFI RVSM Switch-over Plan forwarded to States for attachment in their national switch-over plan.

The stages a) and b), therefore, are deemed to be fully representative of the state of AFI RVSM operations with time.

It should be noted that it takes some time to collect the data necessary to confirm the safety of AFI RVSM operations after implementation. To be able to make such assessments with an increased level of confidence, an AFI RVSM POSC will be compiled after 6, 12 and 18 months.

2.3.7 AFI RVSM Concept and Implementation of the Concept

The AFI RVSM Concept and its implementation are related to the AFI RVSM System, which (in the ATM meaning) is defined by the elements of the AFI Air Navigation System (ANS) involved in RVSM operations. The AFI RVSM System is composed of a ground based ATM component and an airborne ATM component providing RVSM services. As an ATM system (refer to **Annex 2** for definitions), it includes three high-level constituent elements, namely a human element, procedures and equipment (hardware and software). It assumes the existence of a supporting CNS system. A more detailed description of the System and of its constituent elements is provided in **Appendix A**.

The application of the ICAO RVSM Concept in the AFI Region corresponds to the **Design** of the different elements of the AFI RVSM System (e.g. design of procedures, design of training programmes, design of required ATS equipment changes…) in accordance with the RVSM operational concept described in the ATC operations manual for implementation of RVSM in the AFI Region **[43]**

The implementation of the Concept by the participating AFI States corresponds to the **Implementation** (or realisation) of the different elements of the AFI RVSM System into their national airspace (e.g. inclusion of RVSM procedures into ACC operations manual, delivery of ATS training, changes to ATS equipment as required…).

States shall ensure that the local RVSM system they implement is compliant with the AFI RVSM System, and with any additional requirements that may prevail.

Thus, in order to address the full implementation from end-to-end, the assessment includes thus two different levels:

- Assessment of the Safety of the Concept; and,
- Assessment of the Safety of the Implementation.

2.3.8 Conclusion

The overall AFI RVSM safety claim **A0** has been decomposed into four principal safety arguments.

Argument 1 results from the need to define how the AFI RVSM System shall be safe, through a necessary set of safety requirements that fully address the functionality, capacity, performances and integrity of the AFI RVSM System along its whole lifecycle, including changeover and the monitoring of on-going operations, Necessary in this context means necessary to achieve the safety criteria **Cr01** (the AFI RVSM Safety Objectives).

Arguments 2, 3 and 4 result from addressing the different stages of RVSM operations in the AFI Region from two different perspectives (Concept and Implementation) as follows:

- **A2** addresses the safety of the Concept for mature RVSM Operations, including monitoring operations;
- **A3** addresses the safety of the Implementation for mature RVSM operations, including monitoring operations; and
- **A4** addresses simultaneously the safety of the switch-over concept and implementation.

3. Argument 1: AFI RVSM Safety Requirements

3.1 Introduction

Argument A1 asserts the safety "in principle" of AFI RVSM. It addresses, through the strategy ***(St01)*,** the completeness and correctness of the necessary safety requirements for each stage of the AFI RVSM System lifecycle. Necessary in this context means necessary to ensure that the safety criteria **(Cr01)** (the AFI RVSM safety objectives) will be met, and especially that the safety risks meets the safety targets embedded in **Cr01**.

Thus, this section describes the detailed arguments, strategies and evidence that:

> *A1:*
>
> *"AFI RVSM is safe "in principle", i.e. subject to subsequent complete and correct implementation of the safety requirements"*

3.2 Strategy

The strategy ***(St01)*** to show that Argument **A1** is valid consists in:

- Showing that a complete and correct set of safety requirements, fully addressing the System functionality, performances, capacity and integrity has been identified for each stage of the lifecycle:
    - The AFI RVSM Concept and its implementation;
    - The AFI switch-over from CVSM to RVSM; and
    - The monitoring of AFI RVSM in operational service.
- Showing that the set of safety requirements meets **Cr01**, i.e. the AFI RVSM Safety Objectives.

In this context, the role of the set of safety requirements for AFI RVSM is to specify the necessary means by which the AFI RVSM Safety Objectives are met. This set can be decomposed in two types of safety requirements:

- a set of **High-level of Safety Requirements** directly resulting from the AFI RVSM Safety Objectives,
- a set of **Integrity Safety Requirements** indirectly resulting from the Safety Objective **(i)** through the FHA process.

Indeed, the safety of the AFI RVSM System is not only dependent on its integrity, but also on its desired functionality, performance, and capacity. Either reduction in the System functionality, performance and capacity, or failure within the System, can cause risk to increase and to exceed the safety targets of **Cr01**.

It results in the need to distinguish the safety requirements in terms of resulting from a "success approach" or from a "failure approach" **[87]**. The High-level Safety Requirements specify the desired functional, performance and capacity properties of the System, whereas the Integrity Safety Requirements formally specify the necessary risk reduction measures identified in the hazard and risk analysis (FHA).

In order to be successfully addressed and realised both in the design (concept) and implementation of the AFI RVSM System, as explained in section 2.3, these two sets of safety requirements have been translated into system element requirements (SER) by detailing and allocating them to the various constituent elements of the AFI RVSM System described in **Appendix 1**. The objective of the allocation is to define which element(s) of the AFI RVSM System is (are) responsible for addressing a requirement, in order to provide further evidence of its successful realisation.

The process of specification and allocation of the safety requirements can be illustrated as follows:

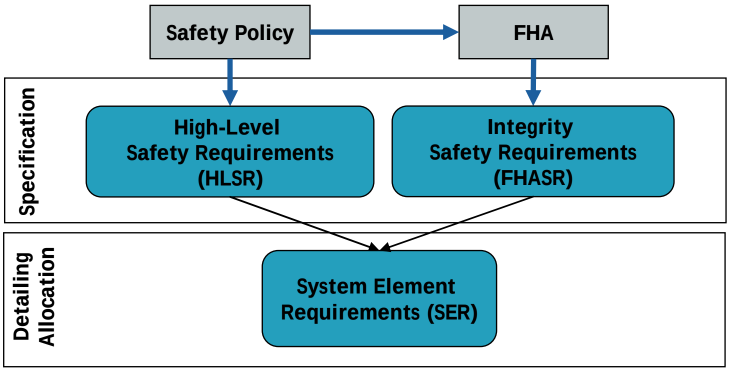

Figure **2** : Safety requirements specification and allocation process

Completeness and correctness of the System Element Requirements (SER) follows from:

- the completeness and correctness of the specified high-level and integrity safety requirements; and,
- the completeness and correctness of the process of detailing and allocation to the System Elements.

In this context, completeness means that all aspects of the safety of AFI RVSM operations have been addressed, and correctness means that they have been addressed in a manner that complies with the AFI RVSM Safety Objectives **(Cr01)**.

The safety assurance (lower-level argument and evidence) supporting **A1** consists of two parts:

- **Argument and direct evidence** that A1 is true; and
- **Argument and backing (supporting) evidence** that the direct evidence itself is trustworthy.

Figure 3 shows the argument and direct evidence structure for **Argument A1**. The direct evidence is presented in detail in section 3.3 below.

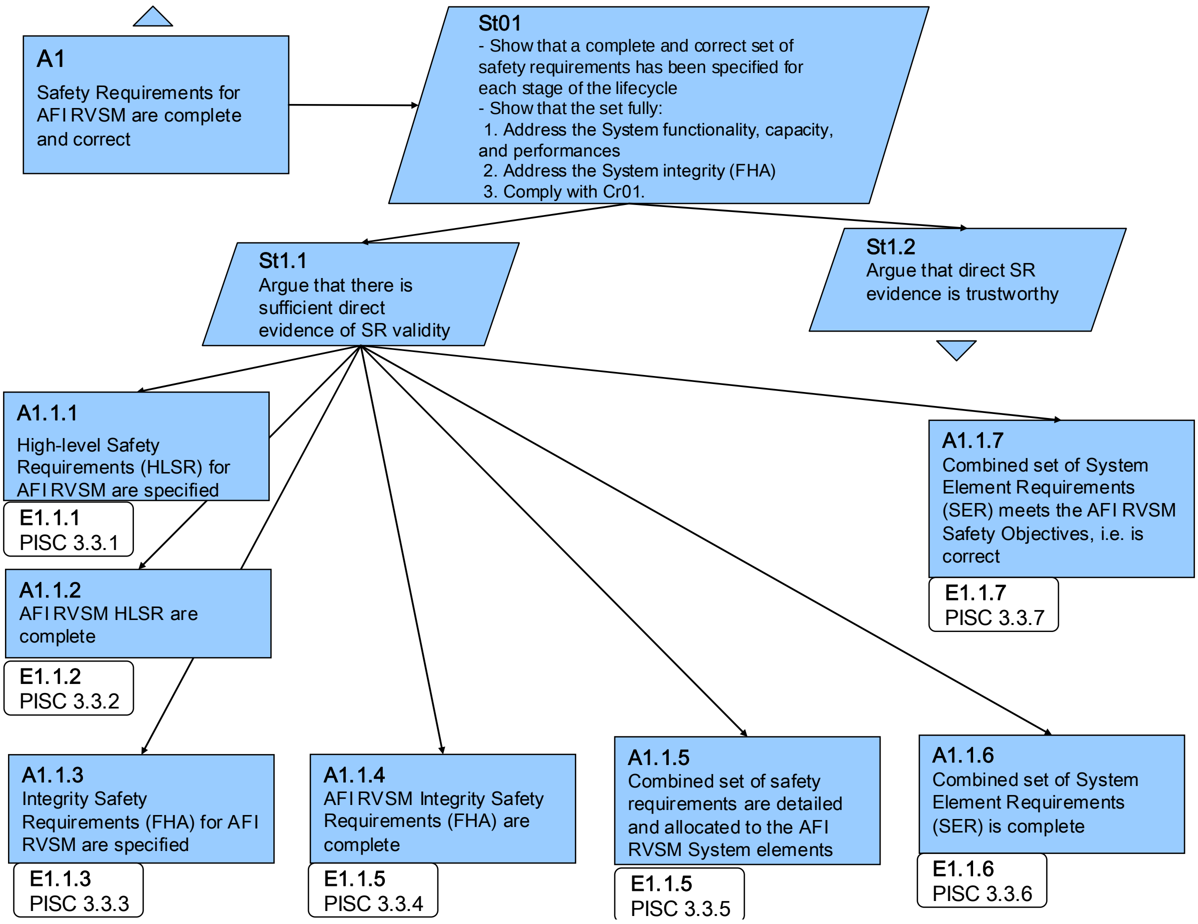

Figure 3 : Argument 1 – Argument and direct evidence structure

Figure 4 shows the argument and backing evidence structure for the **Argument A1**. Backing evidence is provided in support of the trustworthiness of the direct evidence. In this context, the complete and correct set of System Element Requirements (SER) is considered to be trustworthy on the basis that:

- The concept of operations for AFI RVSM is known and has been derived in a competent manner;
- The ICAO Target Levels of Safety (TLSs) and their application are appropriate for AFI RVSM;
- The derivation of the safety requirements (both high-level and FHA-based) has been conducted by competent staff, supported by competent and representative operational experts from the AFI Region, and
- The FHA and CRA techniques have, within reason, been validated.

The Backing Evidence supporting **Argument A1** is presented in detail in section 3.4 below.

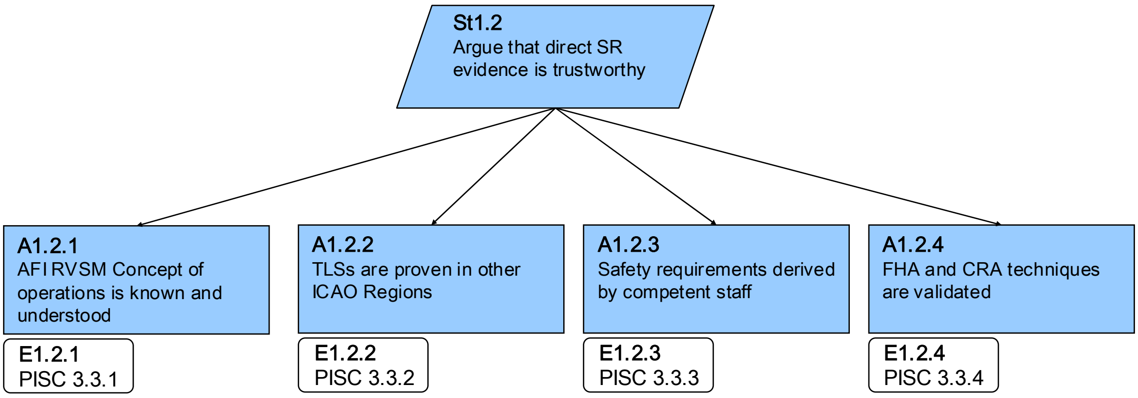

Figure 4 : Argument 1 –Argument and backing evidence structure

3.3 Direct evidence

3.3.1 Specification of High-level Safety Requirements

A1.1.1:

"High-level Safety Requirements for AFI RVSM are specified"

The complete set of high-level safety requirements is to account for all aspects of AFI RVSM operations, i.e. the AFI RVSM safety objectives and the desired functional, performance and capacity properties of the operational concept of the AFI RVSM System.

The hazard and risk analysis (FHA) has produced, through a "failure approach", a set of integrity safety requirements by examining the potential hazards for various operational scenarios and operating conditions. It is beyond the scope of an FHA, however, to look specifically at the TLSs for technical and total vertical risk in the AFI RVSM safety objectives **(iv)** and **(v)**, and to address the desired properties of the System. Hence, in addition to the integrity, safety requirements from the FHA, additional safety requirements are needed to and these are referred to as high-level safety requirements.

Section 2.2.3 listed five Safety Objectives for AFI RVSM. However, these objectives as such do not explicitly depend on the AFI RVSM concept. They could equally well be formulated for a completely different operational concept. Thus, the Safety Objectives need to be translated into the High-level Safety Requirements specifically on the basis of the AFI RVSM operational concept. Such a translation into a complete set of safety requirements is generally not a straightforward exercise. Therefore, the method developed for the EUR RVSM PISC **[80]** has been used. As described in section 4.3 of **[80]**, this method combines elements from the International Safety Management Standard IEC 61508, Part 1 **[100]** and CAP 670 – ATS Safety Requirements **[101]**. The starting point for the method is to characterise the process of the provision of vertical separation, i.e. the AFI RVSM operational concept, in terms of a number of so-called behavioural attributes and to use these as inspiration to identify all the threats to the safety of AFI RVSM operations. Reference **[80]** utilised the following attributes:

- Function;
- Accuracy;
- Capacity;
- Overload tolerance;
- Robustness;
- Reliability; and
- Maintainability.

Based on the method of reference **[80]**, the resulting high-level safety requirements for the AFI RVSM operational concept are shown in Table 3. The first three requirements are directly related to the AFI RVSM concept described in section 2.2.3. The next three requirements are a straightforward translation of the pertinent safety objectives. Requirement AFI RVSM 7 is related to one specific type of operating conditions, namely contingencies and emergencies. Finally, requirement AFI RVSM 8 is based on the fact that AFI RVSM operations should not only be safe upon implementation, but should continue to be safe with time. Notice that no high level safety requirements have been inferred from the capacity and overload tolerance attributes.

The above shows that there is sufficient evidence that **Argument A1.1.1 is true**.

Attribute	High-level Safety Requirement		Rationale
Function	AFI RVSM 1	Only RVSM approved aircraft and State aircraft shall be cleared into AFI RVSM airspace.	Fundamental requirement of AFIRVSM concept
	AFI RVSM 2	Safe vertical separation of aircraft in AFI RVSM airspace shall be provided by assigning aircraft to different flight levels using the following vertical separation minima: (i) 300m (1000ft) between RVSM approved aircraft; (ii) 600m (2000ft) between non-RVSM approved State aircraft and any other aircraft; and (iii) 600m (2000ft) between all military formation flights and any other aircraft.	Fundamental requirement of AFI RVSM concept
	AFI RVSM 3	Non-RVSM approved aircraft shall be allowed to climb/descend uninterrupted through AFI RVSM airspace without intermediate level stops only.	Fundamental requirement of AFI RVSM concept
Accuracy	AFI RVSM 4	The accuracy of the RVSM approved aircraft height-keeping performance shall be sufficiently high for the risk of a mid-air collision in the vertical dimension in the AFI RVSM airspace to meet a TLS of 2.5×10^{-9} fatal accidents per flight hour.	AFI RVSM safety objective (v)
Reliability	AFI RVSM 5	The probability of any system failure leading to a mid-air collision shall be sufficiently low for the risk of mid-air collision due to the loss of vertical separation from all causes in AFI RVSM airspace to meet a TLS of 5×10^{-9} fatal accidents per flight hour.	AFI RVSM safety objective (iv)
	AFI RVSM 6	The system shall be sufficiently reliable for the number of ATM-induced accidents and serious or risk-bearing incidents in AFI RVSM airspace not to increase from current CVSM levels and, where, possible to decrease.	AFI RVSM safety objective (ii)
Robustness	AFI RVSM 7	Facilities shall be provided for safe operation under abnormal conditions, e.g. aircraft on-board emergencies.	AFI RVSM shall remain safe under emergency and contingency conditions
Maintainability	AFI RVSM 8	The performance and reliability of the system shall not deteriorate over time.	AFI RVSM shall be safe upon implementation and beyond
Capacity		No specific safety requirements	-
Overload tolerance		No specific safety requirements	-

Table 3 : AFI RVSM High-level Safety Requirements

3.3.2 Completeness of High-level Safety Requirements

A1.1.2:

"AFI RVSM High-level Safety Requirements are complete"

As regards the completeness of the high-level safety requirements, recall that the method used was an extension of a well-known safety standard **[100]**. It provides the best assurance that the set of high-level safety requirements is complete and correct by examining a broad set of behavioural attributes associated with the operation of AFI RVSM. The requirements cover in particular the AFI RVSM operational concept, the quantitative safety objectives **(iv)** and **(v)**, and operation under emergency and contingency situations. Since the FHA will be shown to have taken care of the potential hazards under normal and adverse operating conditions (section 3.3.4), it is concluded that the set of high-level safety requirements is complete.

Based on these considerations, there is sufficient evidence that **Argument A1.1.2 is true**.

3.3.3 Specification of Integrity Safety Requirements

A1.1.3:

"Integrity Safety Requirements (FHA) for AFI RVSM are specified"

Following the Safety Objective **(i)** (refer to section 2.2.3), a full Functional Hazard Assessment (FHA) has been conducted with the aim to address "the whole RVSM Concept", i.e. to address two stages of operations of AFI RVSM (see section 2.3.6):

- A stabilised situation whereby RVSM has been fully operational for some time (taken here as one year) with all introductory problems having been resolved; so-called "AFI RVSM Core Airspace"; and
- A 24 hour period of time around the actual change-over from CVSM to RVSM, so-called "AFI RVSM Switch-over period".

The objectives of the FHA were:

- To identify and classify all hazards and risks associated with RVSM;
- To specify the safety objectives associated with the hazards identified and to assess their achievement by expert judgment;
- To determine the integrity safety requirements formally specifying the necessary[5] risk reduction measures and to be met by the AFI RVSM System and.
- To allocate the integrity safety requirements to the constituent elements of the generic AFI RVSM System.

In addition, as the ATM/CNS context (route network, traffic complexity, ATM services, CNS capabilities…) differ from FIR to FIR within the AFI Region, four different environmental types, namely controlled airspace with and without surveillance capabilities (radar or ADS) and uncontrolled airspace

[5] In this context, necessary means necessary to achieve the tolerable risk levels defined in the Risk Classification Scheme.

with and without surveillance capabilities (radar or ADS), have been distinguished when identifying and assessing the hazards.

The AFI RVSM FHA is documented in **[71]** and a summary is provided in **Appendix B**. The methodology applied is detailed in Annex C of **[71]**.

The classification of the hazards, in compliance with the applicable Severity Classification Scheme, is presented in the hazard classification tables of Appendix D of **[71]**. The hazards of severity 1 to 4 have been assigned a safety objective, in compliance with the applicable Risk Classification Scheme.

The hazards have been classified into two categories: safety critical and not safety critical. Safety critical hazards correspond to hazards for which the safety objective (maximum tolerable likelihood), has been assessed, by expert judgment, as not to be met and require the identification of supplemental mitigations in addition to the ones[6] already taken into consideration in the initial assessment.

The risk mitigation strategy has then been formally determined for each hazard for which a safety objective has been specified. This strategy consists of identifying all the mitigations that will ensure the tolerability of risks associated to the hazards, based on the following approaches:

- Risk elimination (elimination of the hazard);
- Risk reduction or prevention (reduction of the hazard likelihood); and
- Risk control or protection (reduction of the hazard severity).

The mitigation strategy for each hazard is presented in Appendix E of **[71]**.

The identified mitigations have been expressed in the form of explicit requirements, so-called integrity safety requirements, which have been allocated to the constituent elements of the generic AFI RVSM System. These requirements therefore formally specify the necessary risk reduction measures. Their realisation by the System Elements aims to ensure the proper implementation of these necessary reduction measures, and consequently the achievement of tolerable risk levels.

The integrity safety requirements and their allocation to the System Elements are presented in Appendix F of **[71]**. It should be noted that the purpose of the FHA was to determine the allocation approach but not to provide the results of that allocation, i.e. the system element requirements.

Based on these considerations, there is sufficient evidence that **Argument A1.1.3 is true**.

[6] CVSM mitigations already operated and RVSM mitigations already specified and planned

3.3.4 Completeness of Integrity Safety Requirements

A1.1.4:
"AFI RVSM Integrity Safety Requirements (FHA) are complete"

The following elements provide evidence of the completeness of the integrity safety requirements (FHA-based):

- **Evidence 1:** The hazard and risk analysis process (FHA) has ensured that, within reason, all significant hazards and sufficient mitigations are identified; and
- **Evidence 2:** The assessment of the hazards identified and the derivation of the risk mitigation strategy is representative of the AFI operational environment and of the pilot's and controller's workload that will be encountered in the AFI RVSM airspace.

Evidence 1:

As detailed in Annex C of **[71]**, the hazard identification, carried out during dedicated and structured brainstorming sessions, has been based on operational scenarios and on their associated operating method. These scenarios, detailed in Appendix C of **[71],** have addressed both normal and adverse operating conditions for both AFI RVSM Core Airspace and Switch-over Period as follows:

- AFI RVSM Core Airspace:
    - Normal RVSM operations:
        - Flying according to assigned flight level in RVSM airspace
        - Change of flight level (descent/climb) inside RVSM airspace
        - Change of ACC/UAC
        - Entrance into RVSM airspace
        - Exit RVSM airspace
        - Climbing/descending through RVSM airspace without intermediate stops
    - Abnormal RVSM operations:
        - Deviation from assigned flight level due to local weather phenomena
        - Deviation from assigned flight level due to adverse traffic conditions
        - Emergency descent
- AFI RVSM Switch-over Period:
    - Normal and abnormal RVSM operations:
        - State or RVSM civil aircraft flying at T0
        - Non RVSM Civil aircraft flying at T0
        - State or RVSM civil aircraft taking off after T0
        - Non RVSM Civil aircraft taking off after T0

The set of operational scenarios has been considered by the AFI RVSM FHA Brainstorming Group to be complete as covering all the different aspects of the concept of RVSM operations within the AFI Region.

Due to the structure and techniques of the brainstorming sessions, detailed in Appendix A of **[71]**, the following is considered:

- The set of hazards identified with the support of the pertinent set of operational scenarios is considered to be complete for the AFI RVSM System; and
- The associated set of the mitigations is considered to be sufficient to achieve tolerable risk levels according to the applicable Risk Classification Scheme, and is thus complete.

Furthermore, the hazards identified by EUROCONTROL for EUR RVSM Implementation **[84]** have been used as a starting point while benefiting from the experience gained since in the application of the EUROCONTROL Safety Assessment Methodology **[87]**. This provides additional assurance of AFI RVSM hazards completeness.

Evidence 2:

The assessment of the identified hazards and the derivation of the risk mitigation strategy by the AFI RVSM Brainstorming Group are considered to be representative of the AFI operational environment within which the AFI RVSM System is to be implemented. The assurance of this is provided by the attendance of the brainstorming sessions by experts representing the various AFI operational environments and the various groups of people (controllers, pilot, national RVSM Program Managers etc…) who will design as well as work with the future AFI RVSM System. The composition of the AFI RVSM Brainstorming Group is detailed in Appendices A and B of Reference **[71]**, and is graphically illustrated in **Appendix B**.

Nevertheless, it should be noted that a number of assumptions have had to be made in the FHA, and that they are essential to the completeness of the FHA results, especially og the integrity safety requirements, completeness. These assumptions are recalled and discussed in section 7.

As a conclusion, on the basis of the above considerations, and <u>provided that the FHA assumptions are valid</u>, there is sufficient evidence that **Argument A1.1.4 is true**.

3.3.5 Detailing and allocation of Safety Requirements

A1.1.5:
"Combined set of Safety Requirements are detailed and allocated to the AFI RVSM System Elements"

To be able to show that the combined set of high-level and integrity safety requirements is fully realised at both Concept and Implementation levels, as explained in section 2.3, it is necessary, as a preliminary step, to detail and allocate them to specific elements of the AFI RVSM System, to provide then evidence that the particular elements have successfully addressed the requirement(s) allocated to them.

A description of the AFI RVSM System and of its constituent elements is provided in **Appendix A**.

The detailing and allocation is carried out in two stages: firstly, the determination of the allocation approach by identifying which element(s) have to address each safety requirement, and secondly the specification of the System Element Requirement (SER) resulting from that allocation.

The allocation approach for the integrity safety requirements and the high-level Safety Requirements are respectively provided in Appendix F of **[71]** and in Table 4 below. It should be noted that the AFI RVSM 5 and AFI RVSM 6 have been retained as high-level requirements and allocated to the overall System (RVSM).

The set of System Element Requirements (SER), resulting from the detailing and allocation, as well as the associated mapping with the previous requirements, is provided in **Appendix C**.

On the basis of the above considerations, **Argument A1.1.5 is considered as true**.

High-level Safety Requirement	Allocated to	Reference	Comments
<u>AFI RVSM 1</u> Only RVSM approved aircraft and State aircraft shall be cleared into AFI RVSM airspace.	Airspace design System monitoring Aircraft equipment Flight crew procedures Flight crew training ATS equipment ATS procedures ATS training	 SM1 FCOP2 FCOT1 ATSE1 ATSP1a ATST1a	 Measures to exclude non-RVSM a/c Revised flight planning procedures Training in revised flight planning proc Mean to identify non-RVSM a/c Revised clearance procedures Training in revised clearance proc
<u>AFI RVSM 2</u> Safe vertical separation of aircraft in AFI RVSM airspace shall be provided by assigning aircraft to different flight levels using the following vertical separation minima: (iv) 300m (1000ft) between RVSM approved aircraft; (v) 600m (2000ft) between non RVSM approved State aircraft and any other aircraft; and (vi) 600m (2000ft) between all military formation flights and any other aircraft.	Airspace design System monitoring Aircraft equipment Flight crew procedures Flight crew training ATS equipment ATS procedures ATS training	AD1 FCOP1 FCOT2 ATSE2 ATSP1b ATST1b	New Flight Level Orientation Scheme Use of new flight levels and flows Training in new procedures New vertical separation parameter values for conflict detection/alerting Use of new flight levels and flows Training in new procedures

High-level Safety Requirement	Allocated to	Reference	Comments
<u>AFI RVSM 3</u> Non-RVSM approved aircraft shall be allowed to climb straight through AFI RVSM airspace without intermediate level stops only.	Airspace design System monitoring Aircraft equipment Flight crew procedures Flight crew training ATS equipment ATS procedures ATS training	 FCOP4 ATSP3 ATST3	 Note: not relevant to FC training New procedure Training in new procedure
<u>AFI RVSM 4</u> The accuracy of the RVSM approved aircraft height-keeping performance shall be sufficiently high for the risk of a mid-air collision in the vertical dimension in the AFI RVSM airspace to meet a TLS of 2.5×10^{-9} fatal accidents per flight hour.	Airspace design System monitoring Aircraft equipment Flight crew procedures Flight crew training ATS equipment ATS procedures ATS training	 AC1	 Allocated in entirety to aircraft altimetry and autopilot systems[7]
<u>AFI RVSM 5</u> The probability of any system failure leading to a mid-air collision shall be sufficiently low for the risk of mid-air collision due to the loss of vertical separation from all causes in AFI RVSM airspace to meet a TLS of 5×10^{-9} fatal accidents per flight hour.	 Airspace design System monitoring Aircraft equipment Flight crew procedures Flight crew training ATS equipment ATS procedures ATS training	RVSM5	
<u>AFI RVSM 6</u> The system shall be sufficiently reliable for the number of ATM-induced accidents and serious or risk-bearing incidents in AFI RVSM airspace not to increase from current CVSM levels and, where, possible to decrease.	 Airspace design System monitoring Aircraft equipment Flight crew procedures Flight crew training ATS equipment ATS procedures ATS training	RVSM6	

[7] Dependent on risk exposure (traffic density, navigation performance), an airspace design requirement may be required.

High-level Safety Requirement	Allocated to	Reference	Comments
<u>AFI RVSM 7</u> Facilities shall be provided for safe operation under abnormal conditions, e.g. aircraft on-board emergencies.	Airspace design System monitoring Aircraft equipment Flight crew procedures Flight crew training ATS equipment ATS procedures ATS training	AD2 FCOP3 FCOT3 ATSP2 ATST2	Provision of emergency levels Revised contingency procedures Training in revised procedures Revised contingency procedures Training in revised contingency procedures
<u>AFI RVSM 8</u> The performance and reliability of the system shall not deteriorate over time.	Airspace design System monitoring Aircraft equipment Flight crew procedures Flight crew training ATS equipment ATS procedures ATS training	 SM2 SM3 SM4 SM5 AC2	 Monitor effectiveness of ongoing maintenance programmes in MASPS Collect and analyse data on operational errors for collision risk assessment Monitor risk exposure (traffic flows, navigation performance) for collision risk assessment Monitor rates of ACAS/TCAS traffic alerts and resolution advisories Provide ongoing monitoring programmes for MASPS approved aircraft

Table 4 : Allocation of High-level Safety Requirements

3.3.6 Completeness of System Element Requirements

A1.1.6:
"Combined set of System Element Requirements (SER) is complete"

The completeness of the set of System Elements Requirements (SERs) stems from the completeness of the high-level safety requirements and of the integrity safety requirements (FHA) from which they have been inferred, and from the completeness of the detailing and allocation process.

Evidence of completeness of the sets of high-level and integrity safety requirements were presented in sections 3.3.2 and 3.3.4 respectively.

Examination of the tables in **Appendix C** shows the complete traceability from the combined set of high-level and integrity safety requirements through to the SERs. No requirement has been missed out and no spurious ones have been introduced either. In addition, it shows that all the hazards identified in the FHA **[71]** are traceable to their mitigating safety requirements placed on the System Elements.

This complete traceability from the high-level and FHA-based safety requirements through to the SERs provides assurance of the completeness of the detailing and allocation and apportionment process.

As a conclusion, the combined set of SER is complete and **Argument A1.1.6 is true**.

3.3.7 Compliance of SER with AFI RVSM Safety Objectives

A1.1.6
"Combined set of System Element Requirements (SER) meets the AFI RVSM Safety Objectives, i.e. is correct"

Sections 3.3.1 - 3.3.6 developed the argument and evidence on the completeness of the System Element Requirements (SER) for AFI RVSM. The AFI RVSM Safety Objectives formed one of the inputs to this development, the other inputs being the operational scenarios, the operating conditions and the generic AFI RVSM System. Following this, it is necessary to look back and verify that the SERs do indeed cover the AFI RVSM Safety Objectives, in order to provide assurance of their correctness.

The AFI RVSM Safety Objectives specified in section 2.2.3 may be summarised as follows:

(i) Conduct a full FHA;

(ii) Show that RVSM will not adversely affect the risk of en-route mid-air collision;

(iii) Establish an explicit safety sub-Programme;

(iv) Show that the RVSM-approved aircraft height-keeping accuracy is consistent with a TLS of 2.5×10^{-9} fatal accidents per flight hour;

(v) Show that the total vertical risk meets a TLS of 5×10^{-9} fatal accidents per flight hour; and

(vi) Provide guidance to States

3.3.7.1 Safety Objectives (i), (iii) and (vi): FHA, Safety sub-Programme and guidance to States

Safety objective **(i)** has been covered by the AFI RVSM FHA **[71]** which provides the basis for the specification of the set of integrity safety requirements. The FHA has also been conducted as a part of the AFI RVSM Strategic Action Plan **[31]** developed by the AFI RVSM Task Force 2 following the Safety Objective **(iii)**. This strategic action plan covers all the necessary activities to be undertaken prior to the implementation of RVSM, including the Safety activities. This plan is updated at each meeting of the AFI RVSM Task Force **(**refer to **[17]**, **[18]**, **[19]**, **[20]**, **[22]**, **[23]**, **[24]**, **[25]** and **[26]** and is lodged with the ARPO. In addition reference **[2] [66] [68] [69] [70]** and **[71]** show that the safety of planned RVSM operations has been explicitly addressed by the RVSM Safety sub-Programme. Safety Objective **(vi)** has been covered by the dissemination of the FHA results to the AFI States for review and inclusion in their National Safety Plan **[35] [36]**. Section 5 provides further details on how these requirements have been realised by the Implementation of the AFI RVSM Concept at State level.

3.3.7.2 Safety Objective (iv): Accuracy of RVSM-approved aircraft height-keeping

Safety objective **(iv)** for the accuracy of RVSM-approved aircraft height-keeping was directly translated into the high-level safety requirement AFI RVSM 4 and this was subsequently allocated to the AFI RVSM System element "Aircraft Equipment" as System Element Requirement AC1 (see Table 3 and Table 4 respectively in sections 3.3.1 and 3.3.5).

This is a correct representation on the understanding that the risk exposure, i.e. the combined effect of all the other factors (traffic flows, relative speeds, aircraft dimensions) affecting the technical vertical risk, is taken into account in the requirement AC1. In this context, it should be noted that it follows from the RVSM guidance material **[1]** that the link between the TLS, risk exposure and aircraft height-keeping accuracy is to be provided by an appropriate collision risk model.

3.3.7.3 Safety Objective (v): Total vertical collision risk

Safety objective **(v)** concerning the total vertical collision risk due to all causes was directly translated into the High-level Safety Requirement AFI RVSM 5 (see Table 3 and Table 4 respectively in sections 3.3.1 and 3.3.5). As this requirement concerns the total vertical collision risk, it was not divided any further into requirements at system element level. Thus, AFI RVSM 5 as a requirement is a correct representation of safety objective **(v)**. It will be shown in section 4.4 how it has been addressed through collision risk modelling.

As set out in **[80]**, there could be a consistency issue with regard to this quantitative safety objective/requirement in relation to the qualitative risk assessment of the FHA. Recall that the FHA, through its risk-classification matrix (see **Appendix B**), puts safety objectives and, where necessary, safety requirements on <u>individual hazards</u>. It does not, however, put a quantitative limit on the <u>combined risk effect</u> of the hazards. For the EUR PISC, this issue was addressed in two ways. Firstly, it was addressed by examining the total number of hazards and risks per severity class. Secondly, it was addressed by looking at the hazards as potential causes of atypical technical and operational errors. On the assumption of an appropriate monitoring system being in place, cf. System Element Requirement SM3, the frequency and effect of these hazards may be estimated from incident reports and included in the assessment of the total vertical risk. Sections 4.3.9 and 4.4 provide further details on how this has been addressed for the AFI RVSM concept.

3.3.7.4 Safety Objective (ii): Risk of en-route mid-air collision

Safety objective **(ii)** was translated directly into the high- level safety requirement AFI RVSM 6 (see Table 3 and Table 4 respectively in sections 3.3.1 and 3.3.5). Thus, this safety objective is correctly represented by the safety requirement. It will be shown in section 4.5 how it has been addressed for the AFI RVSM concept.

Reference **[80]** identified a number of potential safety benefits associated with the European RVSM Programme. Many of these are equally valid for The AFI RVSM Programme, such as:

- The six additional flight levels will reduce controller workload and, hence potential for errors;
- The six additional flight levels will reduce the exposure to the loss of vertical separation;
- Improved communication failure procedures will enhance operational efficiency;
- The RVSM-approval process will lead to improved height-keeping equipment and maintenance standards; and
- RVSM flight crew training will result in an increased awareness of safety issues concerning level busts, wake vortices and causes of operational errors.

Another potential safety benefit of the implementation of RVSM in the AFI Region will be the removal of RVSM transition airspace.

3.3.7.5 Conclusion

Based on the considerations in sections 3.3.7.1 - 3.3.7.4 above, it is concluded that the set of System Element Requirements is a correct representation of the AFI RVSM Safety Objectives. Thus, **Argument A1.1.7** is considered as true.

3.4 Backing evidence

3.4.1 Introduction

This sub-section provides backing evidence in support of the trustworthiness of the direct evidence presented in section 3.3. The backing evidence consists of the following elements:

- The concept of operations for AFI RVSM has been derived in a competent manner and is known and understood;
- The ICAO Target Levels of Safety (TLS) and their application are appropriate for AFI RVSM;
- The derivation of the safety requirements (both high-level and FHA-based) has been conducted by competent staff, supported by competent and representative operational experts from the AFI Region, and
- The FHA and CRA techniques have, within reason, been validated.

3.4.2 AFI RVSM Concept of operations

A1.2.1:

"AFI RVSM Concept of operations is known and understood"

The ICAO RVSM concept of operations has been developed for the operational environment of the AFI Region under the direction of the RVSM Programme Office (ARPO). The programme was supported by the AFI RVSM Task Force (ARTF) made up of representatives of various African countries and international organisations. Extensive use has been made from experience gained in Europe with the implementation of RVSM in the EUR region.

As is well known, the RVSM concept concerns the use of a 1000 ft vertical separation minimum between RVSM-approved aircraft between FL290 and FL 410 inclusive instead of 2000 ft. It provides six additional cruising levels for the benefit of the airspace users as well as the Air Traffic Service Providers.

All aircraft other than State aircraft wanting to operate in AFI RVSM airspace must have received appropriate RVSM approval/certification from the State of Registry or from the State of the operator and must indicate their RVSM status on Filed Flight Plans.

RVSM will be applied between RVSM approved aircraft within the designated AFI RVSM airspace identified in **Appendix A**. Note in particular the new Flight Level Orientation Scheme reflecting the change in airspace design as a result of the implementation of RVSM in the AFI Region.

Non-RVSM approved aircraft other than State aircraft will not be allowed to operate in AFI RVSM airspace. Non-RVSM approved aircraft will be allowed to traverse from below to above AFI RVSM airspace, and vice-versa, without intermediate level stops.

With the surrounding airspaces already being RVSM airspace, no RVSM transition airspace or procedures are required.

RVSM requires specific training of ATS staff and flight crew prior to the start of RVSM operations. RVSM may also require modification of ATS equipment and procedures based on specific Programme requirements prior to the start of the operations.

This AFI RVSM concept has been disseminated to the AFI States through two RVSM seminars **[32]** and **[33]** and has been used as a basis for the hazard and risk analysis.

On the basis of the above considerations, it is concluded that the AFI RVSM Concept has been derived in a competent manner and is known and understood, and consequently that **Argument A1.2.1 is true.**

3.4.3 Target Levels of Safety

A1.2.2:

"TLSs are proven in other ICAO Region"

In the ICAO Regions where RVSM has been implemented, the ICAO TLSs have been successfully applied to RVSM as a means for quantitative risk management. The technical TLS as the basis for the global RVSM MASPS is globally applicable. The total TLS of 5×10^{-9} fatal accidents per flight hour for the total vertical risk due to all causes has been successfully applied to RVSM in e.g. the ICAO NAT, EUR and CAR/SAM Regions. There are currently no indications why a different total TLS should be applied for AFI RVSM.

Based on these considerations, **Argument A1.2.2 is considered as true.**

3.4.4 Safety requirements derived by competent staff

A1.2.3:

"Safety requirement derived by competent staff"

As described in section 3.3.5, the set of system element safety requirements was derived from the high-level safety requirements and integrity (FHA-based) safety requirements.

The competence of the staff who conducted the Functional Hazard Assessment is justified in **[71]**. The work was conducted in close cooperation with the AFI Regional Monitoring Agency (ARMA) and with the support during the FHA brainstorming sessions of operational experts having great experience of operations in the AFI Region and being acquainted to RVSM operations. The composition of the brainstorming group provided in **Appendix B** reflects a representative selection of operational experts who will design or develop as well as work with the future AFI RVSM system, ensuring the representative outcome of the sessions and subsequently of the FHA. In addition, the great involvement from that group of experts and the maturity reached in a very short time should be mentioned, giving further confidence in the relevance and completeness of the results.

Based on the above, the FHA staff has been demonstrated to be competent and to have been supported by competent and representative operational experts from the AFI Region.

The competence of the staff that derived the high-level safety requirements is justified in **Appendix G**, see also **[68]**. Like the FHA, the work has been conducted in close cooperation with the AFI Regional Monitoring Agency (ARMA).

Consequently, **Argument A1.2.3 is true**.

3.4.5 Validation of FHA and CRA techniques

A1.2.4:
"FHA and CRA techniques are validated"

As detailed in **Appendix B**, the FHA was conducted in a way consistent with the EUROCONTROL EATMP Air Navigation System Safety Assessment Methodology **[87]**, within the regulatory framework supported by the Risk Classification Scheme (RCS) and Severity Classification Scheme (SCS) applicable for AFI RVSM. That process conducted, as well as the RCS and SCS, has been validated by the AFI RVSM Task Force 5 **[20]**.

The AFI RVSM CRA was conducted in a similar way as other RVSM collision risk assessments, see e.g. section 6 of reference **[90]** and **[92] [95]**.

Following these considerations, **Argument A1.2.4 is considered as true.**

3.5 Conclusion

It has been shown in this section that:

- A complete and correct set of safety requirements, fully addressing the System functionality, performance, capacity and integrity has been specified for each stage of the lifecycle:
    - The AFI RVSM Concept and its implementation;
    - The AFI switch-over from CVSM to RVSM; and
    - The monitoring of AFI RVSM in operational service.
- The set of safety requirements meets **Cr01**, i.e. the AFI RVSM Safety Objectives.

on the basis that:

- There is sufficient direct evidence of Safety Requirements validity **(St1.1)**; and
- The direct Safety Requirements validity evidence is trustworthy **(St1.2)**.

All the safety requirements have been allocated to the appropriate AFI RVSM System Elements except for two high-level safety requirements retained at System level. The resulting System Element Requirements constitute the basis for demonstrating in the following sections the safety of each stage of the lifecycle, at both concept and implementation levels.

As a conclusion, **Argument A1 is considered as true**.

Page intentionally left blank.

4. Argument 2: Safety of the AFI RVSM Concept

4.1 Introduction

Argument A2 asserts the safety of the AFI RVSM concept. It addresses, through the strategy (St02), the realisation of the AFI RVSM safety requirements initially in the design of the constituent elements of the AFI RVSM System.

Thus, this section describes the detailed arguments, strategies and evidence that:

A2:
"The AFI RVSM concept is safe"

4.2 Strategy

The strategy ***(St02)*** to show that **Argument A2** is valid consists in:

- Showing that the safety requirements are satisfied initially in the design of the constituent elements of the AFI RVSM system

As discussed in section 2.3.7, the AFI RVSM Concept results from the application of the ICAO RVSM Concept in the AFI Region. It corresponds to the design of the different elements of the AFI RVSM System. The realisation of the safety requirements by the concept thus corresponds to the design of the AFI RVSM System elements in compliance with these requirements.

As detailed in section 3, the set of AFI RVSM safety requirements is composed of System Element Requirements (SERs) and of two high-level safety requirements not allocated to a particular element and maintained at System level. The set of SERs results partially from the explicit derivation of the mitigations identified in the FHA **[71]** that ensure the achievement of tolerable risk levels. The hazard mitigations are thus an integral part of the AFI RVSM System. Theoretically, in the absence of any hazards, RVSM operations would be absolutely safe. However, because of the possible presence of some hazards, certain levels of risk are tolerated and are achieved as such through these mitigations.

Based on the above, in order to show that **Argument A2** is true, the design of each element of the AFI RVSM System (described in **Appendix A**) is to be demonstrated as addressing successfully the set of System Element Requirements (SER) allocated to it; and the AFI RVSM System is to be demonstrated as designed in compliance with RVSM5 and RVSM6.

In addition, in order to pick up any issues that may not have been resolved under the previous arguments, **Argument A2** is further supported by evidence that:

- Safety constraints, if any, are satisfied; and
- Residual risks, if any, are tolerable.

Consequently, **Argument A2** is decomposed within the following argument and evidence structure:

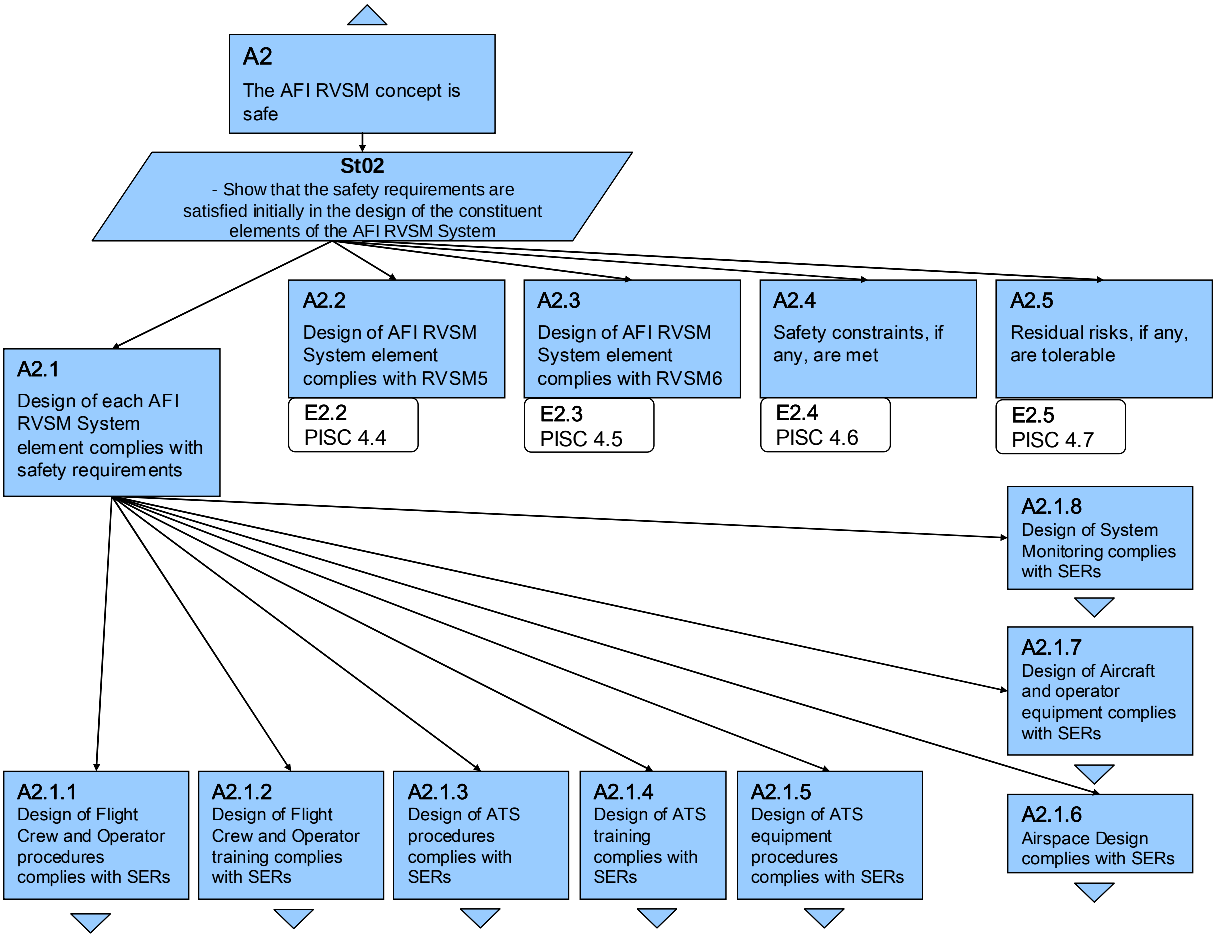

Figure 5 : Argument 2 – Argument and evidence structure

4.3 Design of AFI RVSM System elements

4.3.1 Introduction

This section presents the strategy, detailed argument and evidence that Arguments 2.1.1 – 2.1.8, and consequently Argument A2.1, are true.

A2.1:
"Design of each AFI RVSM System element complies with SERs"

As mentioned in Annex 3, each of these arguments is decomposed along the two following directions:

- Direct Argument and Evidence that the argument is true; and,
- Backing (Supporting) Argument and Evidence that the Direct Evidence itself is trustworthy.

For each System element, the direct evidence of the System Element Requirements realisation is addressed in two steps. Firstly, it is shown how the considered element of the System has to address each individual requirement, i.e. what shall be designed in this aim. This is so-called "Approach of satisfaction". Secondly, evidence of requirements satisfaction following this approach is provided.

The approach of satisfaction of the SERs resulting from the High-level Safety Requirements is captured within the lower argument and evidence structure and is discussed in the following sections as such.

The realisation the SERs resulting from the FHA-based Safety Requirements is addressed within the lower-argument "Hazards and risks mitigated". The realisation of these requirements at a Concept level corresponds to the design of the FHA mitigations within the System elements[8].

Based on the above, the discussion by System element is made up of the following parts:

(i) Purpose and description of System Element Requirements

(ii) Approach of realisation and safety argument and evidence sub-structure

(iii) Direct evidence

(iv) Backing evidence

(v) Conclusion concerning design of System element

[8] It should be recall that the hazards have been identified in the FHA at an ATM level and are not related to a particular element of the System. It is the mitigations that are allocated and apportioned to the System elements.

4.3.2 Flight Crew and Operator procedures

A2.1.1:
"Design of Flight Crew and Operator procedures complies with SERs"

This section sets out the argument and evidence that Flight Crew and Operator procedures (FCOP) have been designed in compliance with the System Element Requirements.

4.3.2.1 System Element Requirements

In order to support safe operations in AFI RVSM Airspace, appropriate Flight Crew and Operator procedures shall be developed. It includes normal, contingency and transiting[9] procedures for flight crew and flight planning procedures for operator, as per its constituent sub-element:

- Normal Procedures (FCOP_1)
- Planning Procedures (FCOP_2)
- Contingency Procedures (FCOP_3)
- Transiting Procedures (FCOP_4)

The set of SERs applicable to that element is firstly composed of requirements resulting from the High-level Safety Requirements. They are intended to ensure that the appropriate procedures are available during operation in the AFI RVSM airspace, as follows:

- **FCOP1** (AFI RVSM 2): "Flight Crew procedures shall be specified for RVSM operations (including use of new FLAS/FLOS)"
- **FCOP2** (AFI RVSM 1): "Flight planning procedures shall be revised and reinforced for RVSM "
- **FCOP3** (AFI RVSM 7); "Flight Crew in-flight contingencies shall be specified"
- **FCOP4** (AFI RVSM 3): "Non-RVSM-approved civil aircraft transiting procedures (including contingencies) shall be defined"

The set of SERs is completed by requirements resulting from the FHA (integrity safety requirements). They are intended to ensure that the hazard mitigations provided by Flight Crew and Operator Procedures are available during RVSM operations. These requirements are presented in **Appendix C**.

[9] Procedure facilitating the transit of non RVSM-civil aircraft through the RVSM airspace, as part of the AFI RVSM operational concept (refer to section 3.4.2 and **Appendix A**)

4.3.2.2 Approach

The System Element Requirements **FCOP1** to **FCOP4** are considered to be realised by the Concept if:

(i) Procedures are produced in the material promulgated by ICAO and the JAA

(ii) States are required to institute these procedures

(iii) Extension of existing RVSM approval ensures inclusion of AFI procedures for flight crew and operator

As stated in section 4.3, this approach of satisfaction is captured in the argument and evidence structure supporting Argument A2.1.1.

Regarding the integrity safety requirements resulting from the FHA, this approach is addressed under the lower argument "Hazards and risks mitigated".

Based on that, the direct argument and evidence structure support Argument 2.1 is as follows:

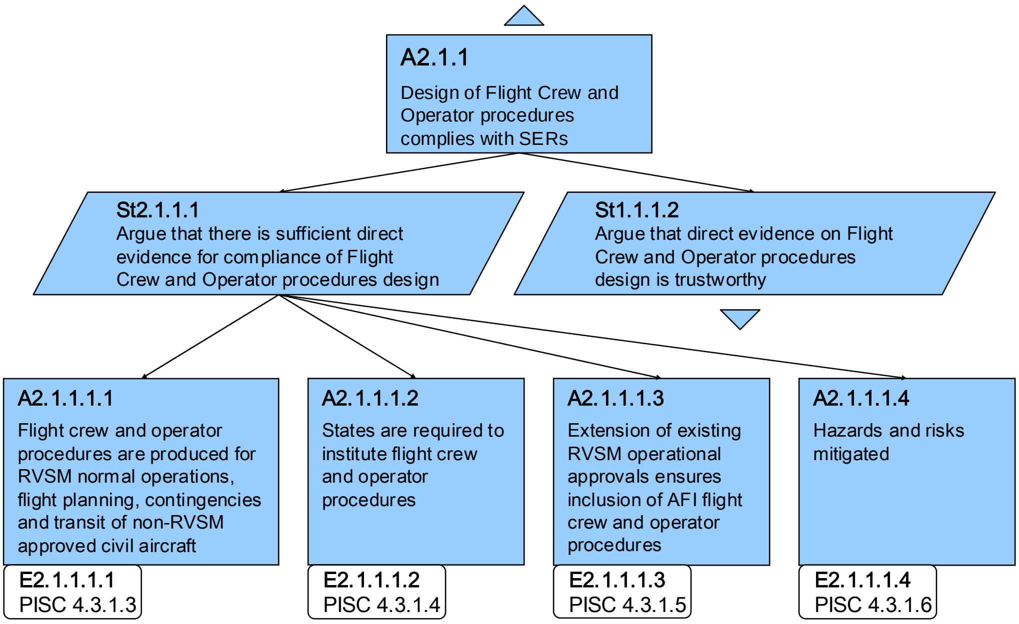

Figure 6 : Argument 2.1.1 – Direct argument and evidence structure

The direct evidence supporting the **Argument 2.1.1** is presented in the sections 4.3.2.3 to 4.3.2.6.

The approach used to provide backing evidence is the following:

- the procedures are not significantly different from or additional to those used and proven in other ICAO Regions; and
- the AFI Region is benefiting from the experience gained in their successful application since the previous RVSM implementations.

Indeed, the main difference between the AFI RVSM Concept and the RVSM concept applied in the other ICAO Regions concern the transit through RVSM airspace of non RVSM-approved civil aircraft. It is part of the CAR/SAM RVSM operational concept **[96]** but this is not allowed in the EUR RVSM airspace (except in transition airspace, if any) **[80]**.

Based on these considerations, the direct evidence is considered to be trustworthy on the basis that:

- Flight crew procedures for normal RVSM operations are proven in the EUR RVSM airspace,
- RVSM flight planning procedures for operators are proven in the EUR RVSM airspace,
- RVSM contingency procedures are proven in the EUR RVSM airspace,
- Procedures related to the transit of non RVSM-approved civil aircraft are proven in normal operations .

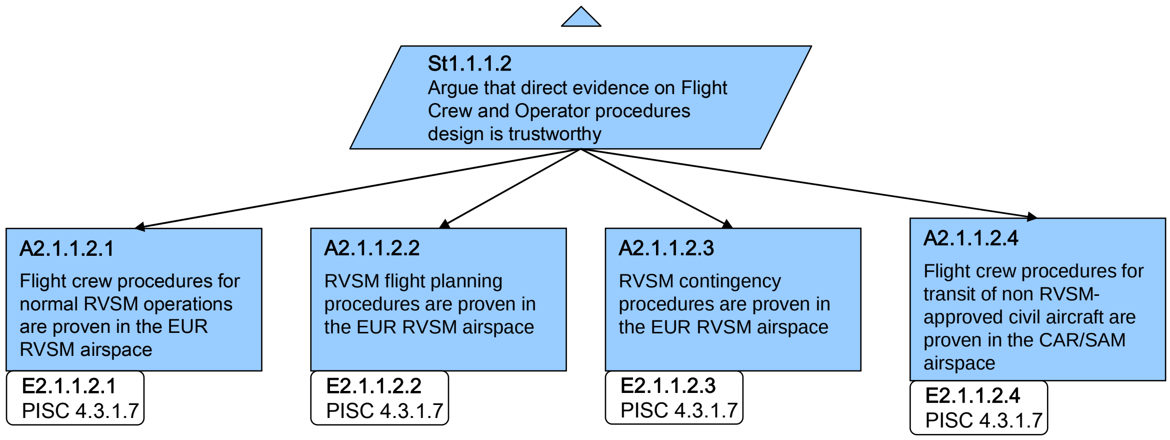

Figure 7 : Argument 2.1.1 – Backing argument and evidence structure

The backing evidence supporting the **Argument A2.1.1** is presented in section 4.3.2.7.

4.3.2.3 Provision of flight crew and operator procedures

A2.1.1.1.1:

"Flight crew and operator procedures are produced for normal RVSM operations, flight planning, contingencies and transit of non RVSM-approved civil aircraft "

Flight crew and operator procedures are provided/notified in the *ICAO Doc. 7030/4 Regional Supplementary Procedures (amendment 212)* **[44]** - *AFI Supps – Part 1 - Rules of the Air, Air Traffic Services and Search and Rescue*:

- Section 6 provides procedures for normal RVSM operations,
- Section 2 provides flight planning procedures,
- Section 6 provides contingency procedures, and
- Section 6 provides procedures for transit of non-RVSM civil aircraft.

These procedures address RVSM operations in both ATC and FIS environments.

Additional information on the procedures required for operations in any RVSM airspace is provided in *JAA Temporary Guidance Leaflet n°6* **[40]** – *Appendix 4 – Training programmes and operating practises and procedures*. This material addresses standard normal, contingency and flight planning procedures and cross-refers to the AFI 7030 Supps for the specific regional procedures.

Consequently, it is concluded that **Argument A.2.1.1.1** is true.

4.3.2.4 Institution of flight crew and operator procedures

A2.1.1.1.2:
"States are required to institute flight crew and operator procedures"

Flight crew and operator procedures are instituted by States through the operational approval of operator that is required besides the RVSM approval of the operated aircraft (refer to TGL 6 Rev 1 of **[44])**.

As stated in *JAA Temporary Guidance Leaflet n°6* **[40]** – *Section 11 – Operational Approval*, operator should submit to the responsible authority their operating practises and procedures related to AFI RVSM operations in order to ensure that flight crew and operator staff are aware of, and trained regarding AFI RVSM procedures. *Appendix 4 – Training Programmes and operating practises and procedures* of the same reference **[40]** provides information on the procedures required in any RVSM airspace and refers to the *ICAO Doc. 7030/4 Regional Supplementary Procedures (amendment 212)* **[44]** for the publication of the specific AFI regional operational procedures.

Based on the above, **Argument A2.1.1.2 is considered as true**.

4.3.2.5 Applicability of existing RVSM operational approvals

A2.1.1.1.3:
"Extension of existing RVSM operational approval ensures the inclusion of AFI flight crew and operator procedures"

State RVSM Operational Approvals issued outside of AFI are accepted within AFI for operations by other regions aircraft. This is consequent with ICAO Document 9574. RMAs on a monthly basis exchange State RVSM Operational Approvals consequent with the RMA manual. This dataset provides each RMA with an updated version of which operators and aircraft are current for RVSM operations.

Based on the above, **Argument A2.1.1.3 is considered as true**.

4.3.2.6 Mitigation of hazards and risks

A2.1.1.1.4:

"Hazards and risks are mitigated"

The set of SERs resulting from the integrity safety requirements (FHA) are presented in **Appendix C**. They are intended to ensure that the hazard mitigations related to flight crew and operator procedures are available during RVSM operations.

The global approach for realising these SER is similar to the one used above for FCOP1, FCOP2, FCOP3 and FCOP4 and is based on:

(i) Procedures are produced in the material promulgated by ICAO and the JAA

(ii) States are required to institute these procedures

(iii) Extension of existing RVSM approval ensures inclusion of AFI procedures for flight crew and operator

Item (iii) has been discussed for <u>all</u> the procedures under argument A2.1.1.3 in section 4.3.2.5. Regarding items (i) and (ii), the approach for each SER is detailed in **Appendix D** which also provides the evidence of their realisation through this approach.

On the basis of the results presented in this **Appendix D,** it can be concluded that the hazard mitigation related to flight crew and operator procedures have been properly addressed by the AFI RVSM Programme, and consequently that **Argument A2.1.1.1.4 is considered as true**.

4.3.2.7 Backing evidence

The above direct evidence is considered to be trustworthy on the basis that the following arguments are true:

A2.1.1.2.1:

"Flight Crew procedures for normal RVSM operations are proven in the EUR RVSM airspace"

The correctness of flight crew procedures for normal operations has been demonstrated by 6 years of continuous and successful application in the EUR RVSM airspace. These procedures had previously been proven by 3 years of application in the NAT Region; except for minor modifications validated by EUROCONTROL by means of ATC simulations (refer to Appendix D of reference **[80]**).

Based on this consideration, **Argument A2.1.1.2.1 is considered as true**.

A2.1.1.2.2:

"RVSM flight planning procedures are proven in the EUR RVSM airspace"

The correctness of RVSM flight planning procedures has been demonstrated by 6 years of continuous and successful application in the EUR RVSM airspace. These procedures had previously been proven by 3 years of application in the NAT Region and the use and effectiveness of the letter W (to indicate that the aircraft is RVSM approved) have been evaluated by EUROCONTROL (refer to section 5.8 of **[80]**).

Based on this consideration, **Argument A2.1.1.2.2 is considered as true**.

A2.1.1.2.3:

“RVSM contingency procedures are proven in the EUR RVSM airspace”

The correctness of RVSM contingency procedures has been demonstrated by 6 years of continuous and successful application in the EUR RVSM airspace. As indicated in section 5.3 of **[80]**, these contingency procedures had been independently validated by EUROCONTROL by means of ATC simulations (refer to Appendix D of **[80]**) carried out by staff independent from the procedure design work.

Based on this consideration, **Argument A2.1.1.2.3 is considered as true**.

A2.1.1.2.4

“Flight crew procedures for transit of non RVSM-approved civil aircraft are proven in the CAR/SAM RVSM airspace”

The correctness of flight crew procedures for transit of non RVSM-approved civil aircraft though the RVSM airspace has been demonstrated by a period of 24 months of continuous application in the CAR/SAM RVSM airspace, that has been considered as sufficient to reach mature RVSM operations.

Based on this consideration, **Argument A2.1.1.2.4 is considered as true**.

4.3.2.8 Conclusion regarding flight crew and operator procedures

The arguments direct- and backing-evidence, presented sections 4.3.2.3 - 4.3.2.7 above, show that the system element requirements **FCOP1**, **FCOP2**, **FCOP3** and **FCOP4** allocated to Flight Crew and Operator Procedures have been properly addressed by the AFI RVSM programme. It has also been shown that <u>all</u> the other system element requirements (resulting from the FHA) allocated to that element have been realised in Concept, meaning that <u>all</u> the associated mitigations have been properly designed. It will ensure the validity of design of flight crew and operator procedures and the provision of the associated mitigations. It can be concluded that **Argument A2.1.1 is true**.

4.3.3 Flight Crew and Operator training

A2.1.2:
“Design of Flight Crew and Operator training complies with SERs ”

This section sets out the argument and evidence that Flight Crew and Operator training (FCOT) has been designed in compliance with the System Element Requirements.

4.3.3.1 System Element Requirement

The purpose of the Flight Crew and Operator Training (FCOT) element is to provide appropriate training in order to support safe operations in AFI RVSM Airspace. It is composed of:

- Training for Normal Procedures (FCOT_1)
- Training for Planning Procedures (FCOT_2)
- Training for Contingency Procedures (FCOT_3)

The set of SERs applicable to FCOT is firstly composed of requirements resulting from the High-level Safety Requirements. They are intended to ensure that a suitable provision is made for training, as follows:

- **FCOT1** (AFI RVSM 2): “Flight crew shall be trained regarding AFI RVSM procedures”
- **FCOT2** (AFI RVSM 1): “Operator and flight crew shall be appropriately trained with regards to flight planning procedures revised for RVSM operations”
- **FCOT3** (AFI RVSM 7): “Flight crew shall be trained appropriately with regards to in-flight contingencies”

The set of SERs is completed by requirements resulting from the integrity safety requirements (FHA), that are intended to ensure that the hazard mitigations provided by flight crew and operator training are available during RVSM operations. They are presented in **Appendix C**.

4.3.3.2 Approach

The System Element Requirements **FCOP1** to **FCOP3** are considered respectively to be realised by the Concept on the basis that flight crew and operator training material is specified and instituted, as shown in Figure 8. Regarding the requirements resulting from the FHA, the approach is addressed under the lower argument “Hazards and risks mitigated”.

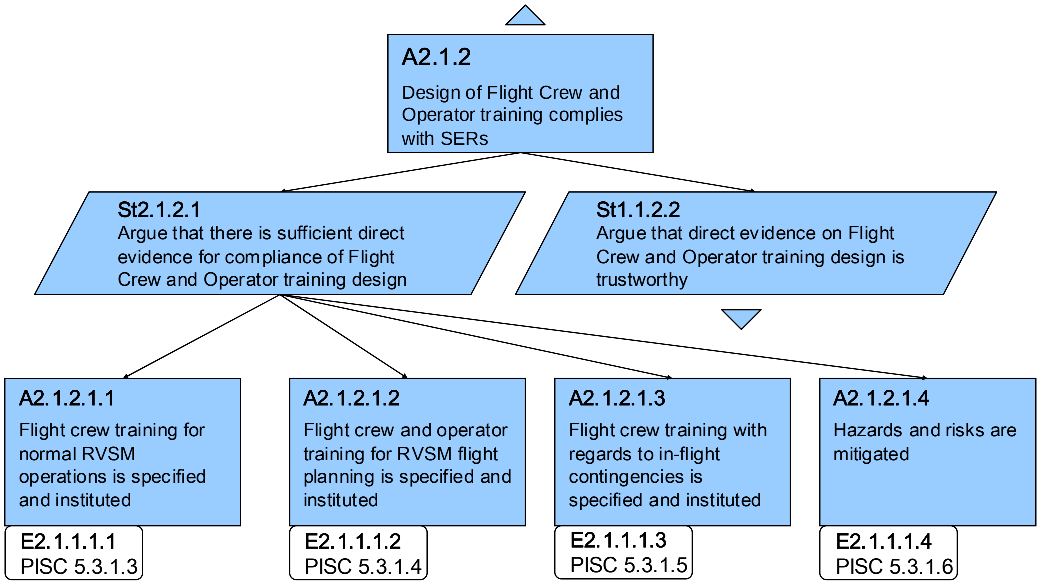

Figure 8 : Argument 2.1.2 – Direct argument and evidence structure

The direct evidence supporting the **Argument 2.1.1** is presented in the sections 4.3.3.3 to 4.3.3.6.

The approach used to provide backing evidence is similar to the one used for flight crew and operator procedures in section 4.3.2. The direct evidence is considered to be trustworthy on the basis that the flight and operator training as designed is correct by demonstrating that:

- Flight crew training for normal RVSM operations and in-flight contingencies have been validated in EUR, and,
- Flight crew and operator training for RVSM flight planning has been validated in EUR.

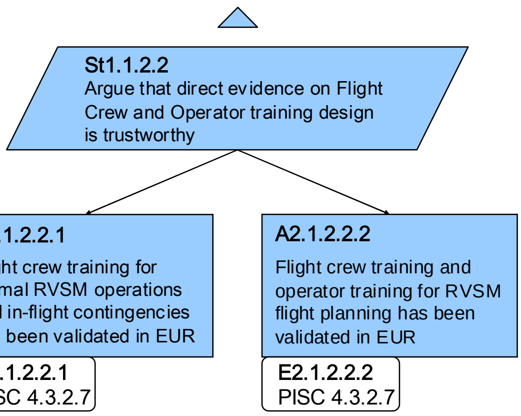

Figure 9 : Argument 2.1.2 – Backing argument and evidence structure

The backing evidence supporting **Argument A2.1.1** is provided in section 4.3.3.7.

4.3.3.3 Provision of training for normal RVSM operations

A2.1.2.1.1:

"Flight crew training for normal RVSM operations is specified and instituted "

An initial guidance on the training necessary for flight crews for operations in any RVSM airspace is provided in the ICAO *Guidance Material on the Implementation of RVSM* **[1]**. This material is completed for operations in the AFI Region through the requirement placed on operator to obtain RVSM approval.

Indeed, in order to ensure that flight crews are trained to the procedures for normal operations in the AFI RVSM airspace (that are instituted by States, see section 4.3.2.4), requirements are placed upon operators that operating practises and training programmes for AFI RVSM operations should in line with AFI regional procedures contained in *ICAO 7030/4 AFI* **[44]**, be stated in the operations manual or appropriate crew guidance, and submitted to the approval authority. These requirements are stated in the section 11 and Appendix 4 of JAA TGL6 revision 1 **[40]** that is the AFI standard for conducting RVSM approvals **[17]**. Reference **[40]** provides also special emphasis special items related to training to be standardised and incorporated into training programmes and operating practises.

In addition, in a similar way as discussed in section 4.3.2.5, extension of existing RVSM operational approval ensures the inclusion of specific training with regards to RVSM operations in the AFI Region.

The ultimate responsibility for ensuring that flight crews are appropriately trained to operate in the AFI RVSM airspace rests with the States that issue the RVSM approval to the operators. This will be discussed in section 5.

A revised pilots training syllabus was accepted at Task Force 13 as prepared by IFALPA.

Based on the above, **Argument A2.1.2.1.1** is considered as true.

4.3.3.4 Provision of training for in-flight contingencies

A2.1.2.1.2:

"Flight crew and operator training for RVSM flight planning is specified and instituted "

The requirement placed on operator to obtain RVSM approval and to submit training programmes to the approval authority includes also training for flight crew and operator with regards to RVSM flight planning, as indicated in section 2 of Appendix 4 of reference **[40]**.

A pilots training syllabus was accepted at Task Force 13 as prepared by IFALPA.

Consequently, following the same approach as for Argument A2.1.2.1.1, **Argument A2.1.2.1.2** is considered as true.

4.3.3.5 Provision of training for RVSM flight planning

A2.1.2.1.3:
"Flight crew training for in-flight contingencies is specified and instituted "

The requirement placed on operator to obtain RVSM approval and to submit training programmes to the approval authority includes also training for flight crew with regards to in-flight contingencies, as indicated in section 5 of Appendix 4 of reference **[40]**.

A pilots training syllabus was accepted at Task Force 13 as prepared by IFALPA.

Consequently, following the same approach than for Argument A2.1.2.1.1, **Argument A2.1.2.1.3** is considered as true.

4.3.3.6 Mitigation of hazards and risks

A2.1.2.1.4:
"Hazards and risks are mitigated "

The set of SERs resulting from the integrity safety requirements (FHA) are presented in **Appendix C**. They are intended to ensure that the hazard mitigations provided by flight crew and operator training are available during RVSM operations.

The global approach for realising these SER is similar to the one used above for FCOT1 to FCOT3, except that the mitigations related to flight crew and operator training, as resulting from the Functional Hazard Assessment, are considered to be specific to the AFI Region and are assumed[10] not to be included in the *Guidance Material on the Implementation of RVSM* **[1]**. Consequently, the approach used is only based on the requirement placed upon operators to obtain RVSM operational approval.

Appendix D provides the individual approach for each SER as well as the evidence collected to meet these approaches.

On the basis of the results presented in this **Appendix D,** it can be concluded that the hazard mitigations related to flight crew and operator training have been properly addressed by the AFI RVSM Programme, and consequently that **Argument A2.1.1.1.6** is true.

[10] It could be possible that reference**[1]** addresses certain SER but it has not been considered as this material is intended to be applicable to any RVSM airspace and as it has been issued before the launch of the AFI RVSM Programme.

4.3.3.7 Backing evidence

A2.1.2.2.1:

"Flight crew training for normal RVSM operations and in-flight contingencies has been validated in EUR "

The correctness of the design of flight crew training with regards to normal RVSM operations and in-flight contingencies has been demonstrated by 6 years of continuous and successful application in the EUR RVSM. This training had previously been proven by 3 years of application in the CAR/SAM and NAT Region.

Based on this consideration, **Argument A2.1.2.2.1 is considered as true**.

A2.1.2.2.2:

"Flight crew and operator training for RVSM flight planning has been validated in EUR "

The correctness of the design of flight crew and operator training with regards RVSM flight planning has been demonstrated by 6 years of continuous and successful application in the EUR RVSM. This training had previously been proven by 3 years of application in the CAR/SAM and NAT Region.

Based on this consideration, **Argument A2.1.2.2.2 is considered as true**.

4.3.3.8 Conclusion concerning flight crew and operator training

The arguments direct- and backing-evidence, presented sections 4.3.3.3 - 4.3.3.7 above, show that the system element requirements **FCOT1**, **FCOT2** and **FCOT3** allocated to Flight Crew and Operator Training have been properly addressed by the AFI RVSM programme. It has also been shown that all the other system element requirements (resulting from the FHA) allocated to that element have been realised in Concept, meaning that all the associated mitigations have been properly designed. It will ensure the validity of design of flight crew and operator training and the provision of the associated mitigations. It can be concluded that **Argument A2.1.2 is true**.

4.3.4 ATS procedures

A2.1.3:

"Design of ATS procedures complies with SERs "

This section sets out the argument and evidence that ATS procedures (ATSP) have been designed in compliance with the System Element Requirements.

4.3.4.1 System Element Requirement

Application of RVSM in the AFI airspace is a fundamental change to vertical separation that needs to be supported by appropriate ATS procedures covering all possible operational scenarios encountered by ATS staff (civil and military controllers, and maintenance staff). Following that, the ATS Procedures element is composed of:

- Normal Procedures (ATSP_1)
- Contingency Procedures (ATSP_2)
- Transiting Procedures (ATSP_3)

The set of SERs applicable to ATSP element is firstly composed of requirements resulting from the high-level safety requirements. They are intended to ensure that the procedures cover precisely and clearly the description of the new vertical separation minimum, the requirements for its use, and enable the safe and expeditious flow of traffic throughout the AFI RVSM airspace, as follows:

- **ATSP1a** (AFI RVSM1): "Clearance procedures shall be revised to clear only RVSM civil aircraft and State aircraft into the RVSM airspace";
- **ATSP1b** (AFI RVSM2): "ATS Procedures shall be specified for RVSM operations (including use of new FLAS/FLOS)";
- **ATSP2** (AFI RVSM 7): "Revised contingency procedures shall be defined";
- **ATSP3** (AFI RVSM 3): "Procedures facilitating the transit of non-RVSM civil aircraft through the RVSM airspace without intermediate stops shall be defined";

ATSP1a and **ATSP1b** address the provision of appropriate procedures for controllers with regards to normal RVSM operations, and **ATSP2** with regards to all non-normal situations within the AFI RVSM airspace. **ATSP3** addresses the specific procedures for handling non RVSM-civil aircraft transiting through the RVSM airspace.

The set of SERs is completed by requirements resulting from the integrity safety requirements (FHA). They are intended to ensure that the hazard mitigations provided by the ATS procedures are available during RVSM operations. These requirements are presented in **Appendix C**.

4.3.4.2 Approach

The system element requirements **ATSP1a**, **ATSP1b**, **ATSP2** and **ATSP3** are considered to be realised in Concept if the procedures for RVSM normal operations, contingencies and for handling the transit of non RVSM civil aircraft:

(i) concerning both flight crew and controllers are produced in the *ICAO AFI 7030 Regional Supps* **[44]**; and

(ii) Concerning only controllers are produced in the *AFI RVSM ATS manual* **[43].**

This approach is rationalised by the requirement placed:

- upon Operators to develop operating procedures in compliance with the ICAO 7030 (cf. section 4.3.2), and;
- upon States to develop ACC ATS Operations Manual in compliance with the ICAO 7030 Document and the AFI RVSM ATS manual. This latter requirement is an Implementation requirement and is discussed as such in section 5.

Regarding the integrity safety requirements resulting from the FHA, this approach is addressed under the lower argument “Hazards and risks mitigated”.

The above direct evidence structure is supported by the following backing approach:

- the procedures are not significantly different from or additional to those used and proven in other ICAO Regions; and
- the AFI Region is benefiting from the experience gained in their successful application since the previous RVSM implementations.

Indeed, the main difference between the AFI RVSM Concept and the RVSM concept applied in the other ICAO Regions concern the transit through RVSM airspace of non RVSM-approved civil aircraft. It is part of the CAR/SAM RVSM operational concept **[96]** but this is not allowed in the EUR RVSM airspace (except in transition airspace, if any) **[80]**.

Based on these considerations, the direct evidence is considered to be trustworthy on the basis that:

- ATS procedures for normal RVSM operations and contingencies are proven in the EUR RVSM airspace,
- ATS procedures for handling the transit of non RVSM-approved civil aircraft are proven as normal operations.

Following that, Figure 10 shows the direct argument and evidence structure supporting **Argument A2.1.3**. The direct and backing evidence are provided in sections 4.3.4.3 - 4.3.4.4 and section 4.3.4.5 respectively.

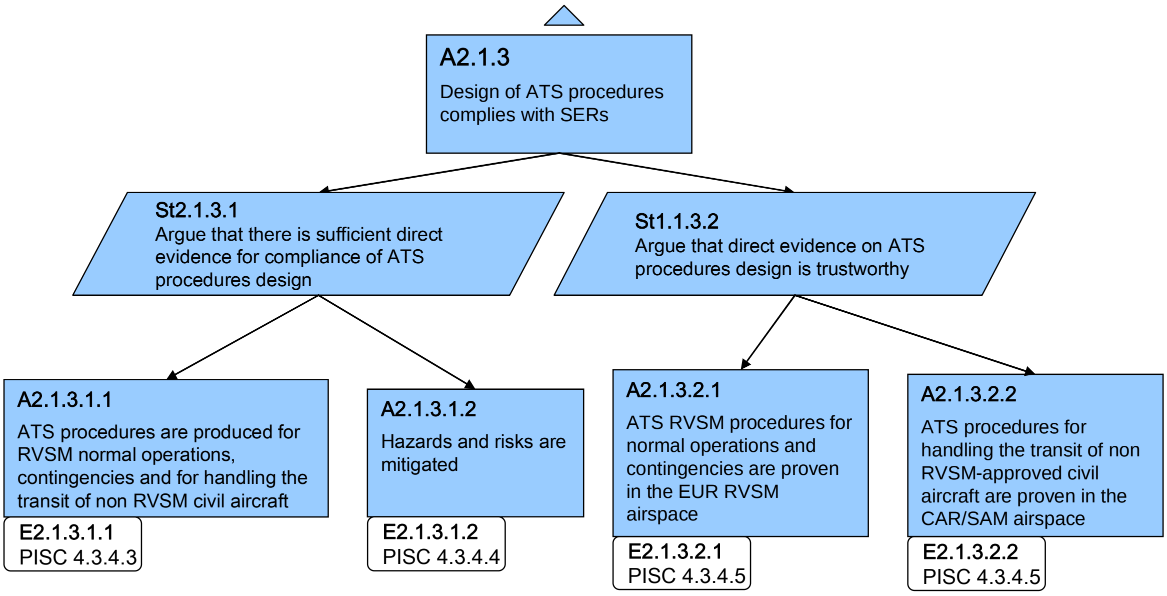

Figure 10 : Argument 2.1.3 – Argument and evidence structure

4.3.4.3 Production of procedures

A2.1.3.1.1:

"ATS procedures are produced for normal RVSM operations, contingencies and for handling the transit of non RVSM civil aircraft"

The ATS procedures for use in the AFI RVSM airspace are provided in the *AFI 7030 Regional Supps* **[44]**, *AFI RVSM ATS manual* **[43]** and *AFI RVSM LoA/P template* **[45]**, promulgated by ICAO, as following:

(i) References **[44]** provides ATS procedures concerning both flight crew and controllers:

- Section 6 provides procedures for normal RVSM operations,
- Section 6 provides RVSM contingency procedures, and
- Section 6 provides procedures for handling the transit of non-RVSM civil aircraft.

(ii) References **[43]** and **[45]** provide ATS procedures concerning only controllers:

- Section 6 of **[43]** provides ATS specific procedures for normal RVSM operations,
- Section 6 of **[45]** provides ATS RVSM coordination procedures,
- Section 6 of **[43]** provides ATS specific contingency procedures, and
- Section 6 of **[43]** provides ATS specific procedures for handling the transit of non-RVSM civil aircraft.

These procedures address RVSM operations in both ATC and FIS environments.

Reference **[43]** and **[44]** show that the requirements **ATSP1a**, **ATSP1b**, **ATSP2** and **ATSP3** have been properly addressed in the provision of the ATS procedures.

Consequently, it can be concluded that a complete ATS RVSM training guidance has been developed and that this material is applicable for the AFI Region. **Argument A2.1.3.1.1 is considered as true.**

4.3.4.4 Mitigation of hazards and risks

A2.1.3.1.2:

"Hazards and risks are mitigated "

The set of SERs resulting from the integrity safety requirements (FHA) are presented in **Appendix C**. They are intended to ensure that the hazard mitigations provided by ATS procedures are available during RVSM operations.

The global approach for realising these SER is based on the provision of ATS procedures in the material promulgated by ICAO, with the following distinctions:

(i) ATS RVSM procedures concerning both flight crew and controllers are produced in the *ICAO AFI 7030 Regional Supps* **[44]**;

(ii) ATS RVSM procedures concerning only controllers are provided in the *AFI RVSM ATS manual* **[43]** and in the *AFI RVSM LoA Template* **[45]**; and

(iii) ATS procedures not specific to RVSM normal operations but providing mitigations for those operations, are provided in other ICAO material such as ICAO Doc. 9426 **[5]**.

Appendix D provides the individual approach for each SER as well as the evidence collected to meet these approaches. [open issue 4.22]

On the basis of the results presented in this **Appendix D,** it can be concluded that the hazard mitigations related to ATS procedures have been properly addressed by the AFI RVSM Programme, and consequently that **Argument A2.1.3.1.2** is true.

4.3.4.5 Backing evidence

The above direct evidence is considered to be trustworthy on the basis that the following arguments are true:

A2.1.3.2.1:

"ATS procedures for normal RVSM operations and contingencies are proven in the EUR RVSM airspace"

The correctness of ATS procedures for normal RVSM operations and of RVSM contingencies has been demonstrated by 6 years of continuous and successful application in the EUR RVSM airspace. These procedures had previously been proven by 3 years of application in the NAT Region; except for minor modifications validated by EUROCONTROL by means of ATC simulations (refer to Appendix D of reference **[80]**).

Based on this consideration, **Argument A2.1.3.2.1 is considered as true**.

A2.1.3.2.2
"ATS procedures for handling the transit of non RVSM-approved civil aircraft are proven in the CAR/SAM RVSM airspace"

The correctness of ATS procedures, for handling the transit of non RVSM-approved civil aircraft though the RVSM airspace, has been demonstrated by a period of 24 months of continuous application in the CAR/SAM RVSM airspace. This period has been considered as sufficient to reach mature RVSM operations.

Based on this consideration, **Argument A2.1.3.2.2 is considered as true**.

4.3.4.6 Conclusion concerning ATS procedures

The arguments direct- and backing-evidence, presented sections 4.3.4.3 - 4.3.4.5 above, show that the system element requirements **ATSP1a**, **ATSP1b**, **ATSP2** and **ATSP3** allocated to ATS procedures have been properly addressed by the AFI RVSM programme. It has also been shown that all the other system element requirements (resulting from the FHA) allocated to that element have been realised in Concept, meaning that all the associated mitigations have been properly designed. It will ensure the validity of the design of ATS procedures and the provision of the associated mitigations. It can be concluded that **Argument A2.1.2 is true**.

4.3.5 ATS training

A2.1.4:

"Design of ATS training complies with SERs "

This section sets out the argument and evidence that ATS training (ATST) has been designed in compliance with the System Element Requirements.

4.3.5.1 System Element Requirement

The purpose of the ATS Training (ATST) element is to provide appropriate training for both civil and military controllers as well as for maintenance staff, in order to support safe operations in AFI RVSM Airspace. It is composed of:

- Training for Normal Procedures (ATST_1);
- Training for Contingency Procedures (ATST_2); and
- Training for Transiting[11] Procedures (ATST_3).

The set of SERs applicable to ATST sub-elements is firstly composed of requirements resulting from the high-level safety requirements. They are intended to ensure that a suitable provision is made for training in order to prepare ATS staff to the new RVSM environment and operations, as follows:

- **ATST1a** (AFI RVSM1): "Controllers shall be trained appropriately regarding revised clearance procedures";
- **ATST1b** (AFI RVSM2): "Controllers shall be trained appropriately regarding ATS procedures for RVSM operations";
- **ATST2** (AFI RVSM 7): "Controllers shall be trained appropriately with regards to RVSM contingencies";
- **ATST3** (AFI RVSM 3): "Controllers shall be trained appropriately with regards to Non-RVSM civil aircraft transiting procedures (including contingencies)"

ATST1a and **ATST1b** address the provision of appropriate training for controllers with regards to normal RVSM operations, and **ATST2** the provision of training covering all non-normal situations within the AFI RVSM airspace. **ATST3** addresses the training related to the specific situation of the transit of non-RVSM civil aircraft. These four requirements covers training with regards to the whole set of new/revised procedures for RVSM.

The set of SERs is completed by requirements resulting from the integrity safety requirements (FHA). They are intended to ensure that the hazard mitigations provided by ATS training are available during RVSM operations. These requirements are presented in **Appendix C**.

[11] Procedure facilitating the transit of non RVSM-civil aircraft through the RVSM airspace, as part of the AFI RVSM operational concept (refer to **Appendix A**)

4.3.5.2 Approach

The system element requirements **ATST1a**, **ATST1b**, **ATST2** and **ATST3** are considered to be realised in Concept if:

(i) an appropriate training guidance material applicable for the AFI Region has been developed;

(ii) the States' ATC instructors/trainers have been properly briefed on the content of this material;

This approach is based on the requirement placed upon States to develop national RVSM training material in compliance to the AFI training guidance material. This latter requirement is an Implementation requirement and is discussed as such in **section 5**.

The above direct evidence structure is supported by the following backing approach:

- the RVSM training guidance material applicable to the AFI Region has been proven in other ICAO Regions; and
- Its applicability for the AFI Region has been validated.

Following that, Figure 11 shows the direct argument and evidence structure supporting **Argument A2.1.4**. The direct and backing evidence are provided in sections 4.3.5.3 - 4.3.5.5 and section 4.3.5.6 respectively.

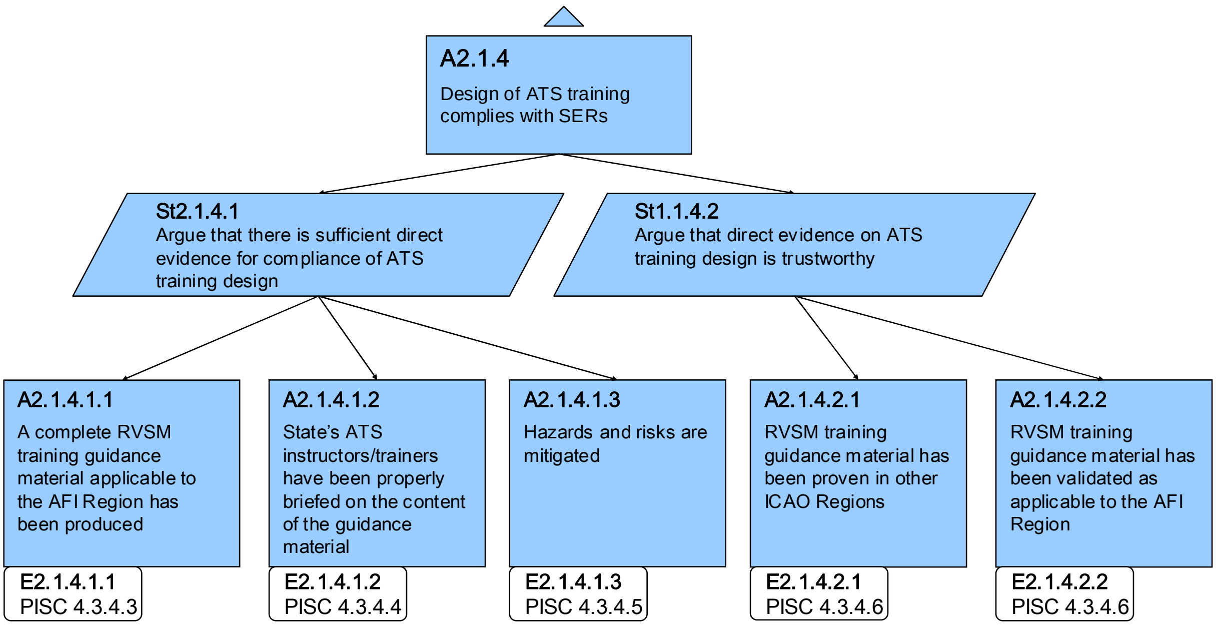

Figure 11 : Argument 2.1.4 – Argument and evidence structure

4.3.5.3 Provision of AFI RVSM training guidance material

A2.1.4.1.1:

"A complete ATS RVSM training guidance material applicable to the AFI Region has been produced"

A training guidance material has been produced by the ARTF/TF2 and is documented in the *AFI ATS RVSM Training Guidance Material* **[48]**. This material constitutes the applicable standard for the AFI Region [ref TF 2].

Reference **[48]** provides guidance on the RVSM training requirements of controllers at a State level in the form of a training syllabus. That syllabus is divided into different modules that cover not only the provision of air traffic services in RVSM airspace[12], but also the various aspects of RVSM in order to provide awareness on the whole RVSM concept of operations, as follows:

- **Historical background of RVSM**: awareness on historical development of RVSM in ICAO and an overview of RVSM implementation in the NAT and EUR Regions;
- **Aircraft requirements and approval**: awareness on the requirements and processes for the operator and aircraft approvals to operate in the AFI RVSM airspace;
- **Safety monitoring**: awareness on the safety monitoring of RVSM;
- **Flight planning**: awareness of the flight planning elements of RVSM;
- **Operational procedures:** explanation of RVSM procedures for operations within the AFI RVSM airspace including general procedures and contingencies;
- **Phraseology**: explanation correct RVSM phraseologies for use between controller/pilot and inter/intra ATS Unit; and
- **Simulated practical exercises:** practical demonstration of competence in the above various aspects of RVSM.

For each of these modules, the training requirements are stated in the form of objectives, content and duration, with additional details when necessary. In addition, assessment criteria are provided.

Reference **[48]** and the above considerations show that the requirements **ATST1a**, **ATST1b** and **ATST2** have been properly addressed in the development of the training guidance material.

The requirement **ATST3** is addressed successfully in the syllabus.

Consequently, it can be concluded that a complete ATS RVSM training guidance material has been developed and that this material is applicable for the AFI Region. **Argument A2.1.4.1.1 is considered as true.**

[12] Note that the material addresses also transition airspaces for historical reasons, as it was part of the initial AFI RVSM concept

4.3.5.4 Briefing of State's instructors

A2.1.4.1.2:

"State's ATS instructors/trainers have been properly briefed on the content of the guidance material"

The State's ATS instructors have been properly briefed on the training guidance material on the basis that:

- As per ARTF conclusions on the training of ATS personnel **[16] [18] [19] [20] [22] [23] [24] [25] [26]**, ATS training seminars have been organised between ATNS (Air Traffic Navigation Services) and ASECNA (Agence pour la Sécurité de la Navigation Aérienne en Afrique et Madagascar) and their clients.
- <u>At least one</u> ATS instructor of each State participating in RVSM (except those that have already implemented in RVSM as indicated in section 1.2) has attended seminar and has been briefed on the training material.

Based on the above, **Argument A2.1.4.1.2** is considered as true.

4.3.5.5 Mitigation of hazards and risks

A2.1.4.1.3:

"Hazards and risks are mitigated"

The set of SERs resulting from the integrity safety requirements (FHA) are presented in **Appendix C**. They are intended to ensure that the hazard mitigations provided by ATS training are available during RVSM operations.

The global approach, for realising these SER, is similar to the one used above (for **ATST1a**, **ATST1b**, **ATST2,** and **ATST3)**. **Appendix D** provides the individual approach for each SER as well as the evidence collected to meet these approaches.

On the basis of the results presented in this **Appendix D,** it can be concluded that the hazard mitigations related to ATS been have been properly addressed by the AFI RVSM Programme, and consequently that **Argument A2.1.4.1.3** is true.

4.3.5.6 Backing evidence

A2.1.4.2.1:

"RVSM training guidance material has been proven in other ICAO Regions "

The AFI ATS RVSM training guidance material has been developed on the basis of material developed by EUROCONTROL for EUR RVSM with the appropriate adaptation to the specific AFI aspects. It has thus been proven by the successful implementation of the EUR RVSM airspace.

Based on this consideration, **Argument A2.1.4.2.1** is considered as true.

A2.1.2.4.2:

"RVSM training guidance material has been prepared by competent staff and validated as applicable to the AFI Region"

The AFI ATS RVSM training guidance material has been prepared and validated as applicable by the AFI RVSM Task Force / 2 made up of specialist representatives of States participating in the AFI RVSM programme and international organisations, having the pre-requisite background, experience and expertise. See ARTF 2 for further details.

Based on this consideration, **Argument A2.1.4.2.2** is considered as true.

4.3.5.7 Conclusion concerning ATS training

The arguments direct- and backing-evidence, presented sections 4.3.5.3 to 4.3.5.6 above, show that the system element requirements **ATST1a**, **ATST1b**, **ATST2** and **ATST3** allocated to ATS Training have been properly addressed by the AFI RVSM programme. It has also been shown that <u>all</u> the other system element requirements (resulting from the FHA) allocated to that element have been realised in Concept, meaning that <u>all</u> the associated mitigations have been properly designed. It will ensure the validity of the design of ATS training and the provision of the associated mitigations. It can be concluded that **Argument A2.1.2 is true**.

4.3.6 ATS equipment

A2.1.5:
"Design of ATS equipment complies with SERs "

This section sets out the argument and evidence that ATS Equipment (ATSE) has been designed in compliance with the System Element Requirements.

4.3.6.1 System Element Requirements

In order to support safe operations in the AFI RVSM airspace, ATS equipment needs to be modified. This need for modifications stems from the application of different vertical separation minima due to the composite population of aircraft that are intended to operate in the AFI RVSM airspace. This population consists of RVSM-approved aircraft and of non RVSM-approved State aircraft for which 1000 and 2000 feet of separation shall be applied respectively, and of non RVSM-approved civil aircraft transiting through the AFI RVSM airspace as part of the operational concept of AFI RVSM (refer to **Appendix A**).

The first system element requirement **ATSE1** is intended to ensure that aircraft are correctly separated and coordinated (internally or externally) and that the associated risks are mitigated through the provision for indication to controllers and ATS equipments of the RVSM status[13] of all aircraft operating in, or planning to enter, the AFI RVSM airspace, as follows:

- **ATSE1** (AFI RVSM 1): "ATS equipment shall be modified to indicate and display RVSM status"

The second system element requirement addresses the conflict detection/alerting capabilities. It is a fundamental aspect of the AFI RVSM safety assessment that the AFI RVSM Safety Objectives are demonstrated as achieved without these capabilities that are to be considered as additional safety nets. Indeed, they have not been considered as mitigation means to control the identified risks in the FHA **[71]** as reported from the FHA brainstorming sessions **[72] [73] [74]**. However, as for ACAS/TCAS capabilities, they can introduce additional risks through nuisance alerts that shall be minimised through an appropriate update to be consistent with RVSM operations and associated separation minima. To this end, **ATSE2** has been formulated:

- **ATSE2** (AFI RVSM 2); "Existing conflict detection/alerting capabilities shall be updated to be consistent with RVSM operations"

The set of system element requirements, applicable to ATS equipment, is completed by requirements resulting from the integrity safety requirements (FHA). As detailed in section 3.3.3, they show how the ATS Equipment element shall contribute to the mitigation of the hazards and risks associated with AFI RVSM. They are presented in **Appendix C**.

[13] Status of RVSM-approved aircraft, State aircraft etc… as per AFI RVSM flight planning detailed in **[44]**

4.3.6.2 Approach

The system element requirements **ATSE1** and **ATST2** are considered to be realised respectively in concept on the basis that:

(i) **ATSE1**: necessary ATS equipment changes to indicate and display RVSM status have been specified; and

(ii) **ATSE2:** necessary update of conflict detection/alerting capabilities to be consistent with RVSM operations has been specified.

The need for such ATS equipments modifications is to be addressed through requirements to be detailed in the *ATC Operations Manual for Implementation of RVSM in the AFI Region* **[43]**.

The above direct evidence structure is demonstrated to be trustworthy on the basis that the necessary ATS equipment changes have been proven in EUR RVSM airspace.

Following that, Figure 12 shows the direct argument and evidence structure supporting **Argument A2.1.5**. The direct and backing evidence are provided in sections 4.3.6.3 - 4.3.6.5 and section 4.3.6.6 respectively.

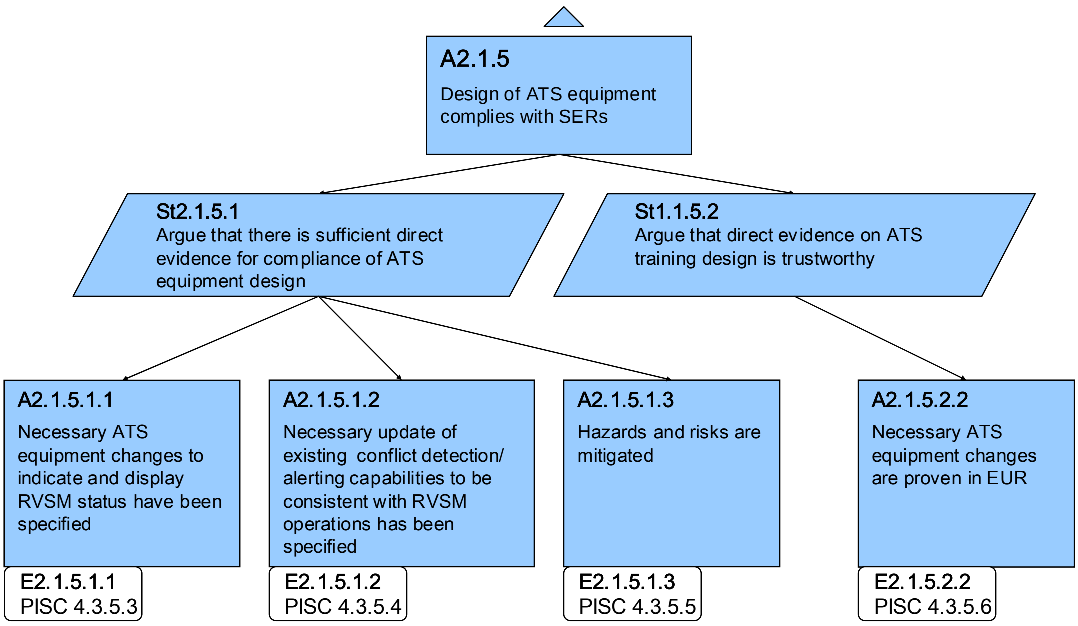

Figure 12 : Argument 2.1.5 – Argument and evidence structure

4.3.6.3 Indication of RVSM status

A2.1.5.1.1:

"Necessary ATS equipment changes to indicate and display RVSM status have been specified"

The necessary changes to provide controllers with a distinguishable feature that identifies RVSM status[14] of aircraft operating in, or planning to enter, the AFI RVSM airspace includes:

- Modification of radar/ADS data processing and display systems including back-up systems to display aircraft RVSM status on position HMI (ENV1 and ENV3[15] only); and
- Modifications of flight data processing systems (FDPS) including back-up systems to display aircraft RVSM status, as filed by operator, on all flight strips (all ENV).

These necessary modifications differs thus from environmental types as it depends if surveillance capabilities are provided at ACC level. In addition, they address both primary and back-up systems, the latter being used in the event of failure of the former one. It is indeed essential to ensure that the back-up systems are also modified to provide the same functionalities than the equivalent primary systems, in order to maintain their effectiveness.

Radar/ADS data processing and display systems (ENV1 and ENV3)

The modifications to radar and/or ADS data processing and display systems are to provide controllers with a clear and unambiguous indication of the current RVSM status (non RVSM approved aircraft, State aircraft…) of all flights under their responsibility. Such modifications include:

- Clear, unambiguous and automatic indication of RVSM status on the radar/ADS position symbols and labels associated with aircraft operating in the RVSM airspace, and where radar or ADS is used as primary mean for applying separation, with aircraft operating within such level bands above and below the RVSM airspace; and
- Functionality for manual manipulation of the radar/ADS position symbols and/or labels associated with aircraft

The *ATC Operations Manual for Implementation of RVSM in the AFI Region* **[43]** provides operational specifications of these equipment changes and the requirements placed upon States to implement such changes. Radar data processing and display is addressed in section 9.2 of reference **[43]**.

FDPS and flight strips (all ENV)

The modifications to FDPS are to provide controllers with a clear indication of RVSM status, as filed by the operator in respect of AFI RVSM flight planning **[44]**, in all flight strips (paper, electronic or, in the absence of either, extended label). Such functionalities, as well as the requirements placed upon States to implement them, are presented in section 9.3 of *ATC Operations Manual for Implementation of RVSM in the AFI Region* **[43]**.

[14] Status of RVSM-approved aircraft, State aircraft etc… as per AFI RVSM flight planning detailed in **[44]**
[15] Environmental types as part of the AFI RVSM concept described in **Appendix A**

Consequently, on the basis of the above evidence, it can be concluded that **ATSE1** has been properly addressed in concept and so that **Argument A2.1.5.1.1 is true**.

4.3.6.4 Modifications of vertical separation parameters

A2.1.5.1.2:

"Necessary update of existing conflict detection/alerting capabilities to be consistent with RVSM operations has been specified"

The necessary update of conflict detection/alerting capabilities to be consistent with RVSM operations includes modifications to existing Short Term Conflict Alert (STCA) and Medium Term Conflict Detection (MTCD) capabilities, and to other alerting capabilities if provided in ACC. The modifications aim to ensure that such capabilities are consistent with RVSM operations, and especially with the different separation minima to be applied. They are only applicable in ENV1 and ENV3 and must be conducted with respect of the constraint of minimising nuisance alerts and operational disruptions.

Short Term Conflict Alert (ENV 1 and ENV3)

The parameters for vertical separation of current STCA systems, where provided, must be modified to selectively apply a 1000 feet- or 2000 feet-VSM as determined by the RVSM approval status of aircraft, as required by the *ATC Operations Manual for Implementation of RVSM in the AFI Region* **[43]** in its section 9.5.

Medium Term Conflict Detection (ENV1 and ENV3)

The MTCD capabilities is quite different from STCA in that sense it concerns medium term conflicts and constitutes an important planning tool for controllers. However, the requirement to selectively apply 1000 ft- or 2000 feet-VSM is also applicable to MTCD, as the operational concept remains the same. This requirement is addressed in section 9.5 of the *ATC Operations Manual for Implementation of RVSM in the AFI Region* **[43]**

Others alerting capabilities

Other alerting capabilities, when provided, shall be modified in the same way.

The above shows that the necessary modifications to conflict detection/alerting capabilities for RVSM operations have been specified. Consequently it can be concluded that **Argument A2.1.5.1.2 is true**.

4.3.6.5 Mitigation of hazards and risks

A2.1.5.1.3:

"Hazards and risks are mitigated"

The set of SERs resulting from the integrity safety requirements are presented in **Appendix C**. They are intended to ensure that the hazard mitigations provided by ATS equipment are available during RVSM operations.

The global approach for realising that set of SERs in concept is based on the placement of requirements upon States, through the *ATC Operations Manual for Implementation of RVSM in the AFI Region*, to appropriately modify ATS equipment to meet these SERs.

Appendix D provides the individual approach for each SER as well as the evidence collected to meet these approaches.

On the basis of the results presented in this **Appendix D,** it can be concluded that all the hazard mitigations related to ATS equipment been have been properly addressed by the AFI RVSM Programme, and consequently that **Argument A2.1.5.1.3** is true.

4.3.6.6 Backing evidence

A2.1.5.2.1:

"Necessary ATS equipment changes are proven in EUR"

The *ATC Operations Manual for Implementation of RVSM in the AFI Region* has been developed on the basis of material developed by EUROCONTROL for EUR RVSM with the appropriate adaptation to the specific AFI aspects. As discussed above, this manual provides a description of the required ATS changes. The correctness of these changes is thus proven by 6 years of continuous RVSM operations in EUR. In addition, these changes had been previously subjected to real-time simulations by EUROCONTROL (refer to Appendix B of **[80]**) and it was confirmed that the clear and unambiguous indication of RVSM status facilitated controllers tasks and improve coordination, and constitutes an efficient mitigation against the risk of applying wrong VSM between aircraft irrespective of their RVSM status.

Based on these considerations, **Argument A2.1.5.2.1 is considered as true**.

4.3.6.7 Conclusion concerning ATS equipment

The arguments direct- and backing-evidence presented above show that the system element requirements **ATSE1** and **ATSE2** allocated to ATS Equipment have been properly addressed by the AFI RVSM programme. It has also been shown that all the other system element requirements (resulting from the FHA) allocated to that element have been realised in Concept, meaning that all the associated mitigations have been properly designed. It will ensure the validity of design of ATS equipment and the provision of the associated appropriate mitigations. It can be concluded that **Argument A2.1.5 is true**.

4.3.7 Airspace Design

A2.1.6:
"Airspace Design complies with SERs "

This section sets out the argument and evidence that Airspace Design (AD) complies with the System Element Requirements.

4.3.7.1 System Element Requirements

The objective of Airspace Design is to provide an airspace structure (FIRs, sectors, routes, FLs) that meets all of the operational requirements, including safety, from both an Air Traffic Management point of view and a Flight Operations viewpoint. A key element of airspace design under AFI RVSM concerns the six additional flight levels as compared to the conventional situation. Another characteristic element is that, due to the presence of RVSM in the surrounding ICAO Regions, no transition airspace is required.

As the required changes to the Airspace Design need to cover all operating conditions, the following two formal system element requirements, **AD1** and **AD2**, have been formulated:

- **AD1** (AFI RVSM 2) : "An appropriate Flight Level Orientation Scheme shall be developed"
- **AD2** (AFI RVSM 5) : "Airspace facilities for emergency situations shall be provided"

AD1 addresses the provision for implementation and use of the six additional Flight Levels available under RVSM; and **AD2** the provision of any changes necessary to accommodate contingency procedures and/or measures arising from abnormal conditions or emergencies. **AD1** covers the normal operational situation, whereas **AD2** is to cover <u>all</u> non-normal situations.

It should be noted that no FHA-based safety requirements have been allocated to the Airspace Design element.

4.3.7.2 Approach

The two Airspace Design system element requirements **AD1** and **AD2** are considered to be met if:

- A new Flight Level Orientation Scheme, including the six additional flight Levels, has been designed and validated; and
- The airspace structure changes necessary with regard to contingencies, abnormal conditions or emergencies have been designed and validated.

As stated in section 4.3, this approach of satisfaction is captured in the argument and evidence structure supporting **Argument A2.1.6**:

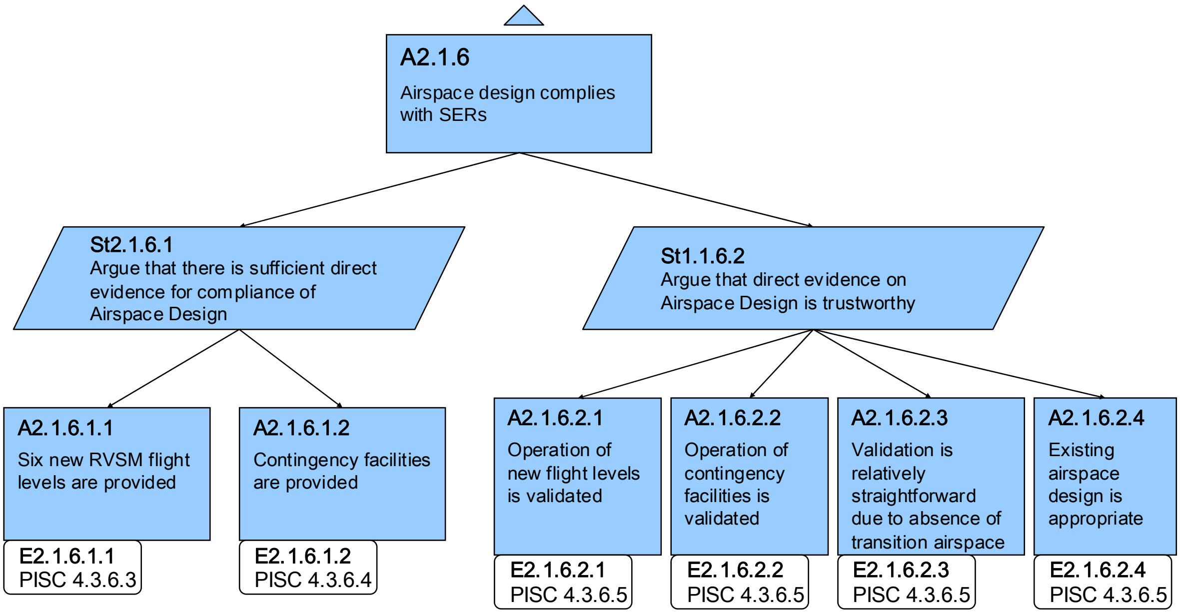

Figure 13 : Argument 2.1.6 – Argument and evidence structure

The direct evidence supporting the **Argument 2.1.6** is presented in sections 4.3.7.3 - 4.3.7.4. The backing evidence is presented in section 4.3.7.5.

4.3.7.3 Provision for new flight levels

A2.1.6.1.1:
"Six new RVSM flight levels are provided "

The discussion of the Airspace Design under the AFI RVSM concept may conveniently be subdivided into two parts, namely the flight levels and all other parts like route structure and sectorisation.

Flight Level Allocation Scheme

Appendix 3 to ICAO Annex 2 **[3]** specifies the Table of Cruising Flight Levels to be used when RVSM is applied. The AFI RVSM Task Force reviewed the suitability of this scheme for AFI RVSM operations in the AFI Region **[51]**. The report concluded that the Appendix 3 scheme was suitable for AFI RVSM operations. Potential problems with this scheme in the transition between RVSM and CVSM airspace became irrelevant due to there being no need for such transition airspace. The connection with the surrounding RVSM airspaces in the EUR, NAT, CAR, SAM and MID Regions was also examined. No problem areas were identified. It was also noted that the AFI RVSM procedure facilitating for non-RVSM approved aircraft a straight climb/descent through AFI RVSM airspace (cf. **Appendix A**) did not affect the suitability of the scheme.

It is known that currently there exist a few routes within the AFI Region where routes with different flight level usages are joining. States have reviewed with regard to the implementation of the new RVSM flight levels and States have updated their procedures and where applicable the LOPs. This system currently works without any problems thus with the adjustment of flight levels the same will apply.

Route network and sectorisation

RVSM operations as such do not require any changes to the route network. Safe operations in transition airspace might require some changes but as no transition airspace for AFI RVSM is needed, this potential reason can be left out as well. Like in other ICAO Regions, changes to the existing route network take place on a more or less regular basis to improve airspace capacity and/or flight operations efficiency. The AFI RVSM Task Force reviewed the existing route network within the AFI Region, including the latest proposed changes and concluded that these would be fully supportive of RVSM on the assumption that the corresponding risk exposure would be consistent with the technical vertical TLS and total vertical TLS **[52]**.

Summary and conclusion

All elements related to the AFI RVSM system element safety requirement **AD1** have been examined. The FLOS as per ICAO Annex 2 Appendix 3 has been adopted for AFI RVSM. The pre- and post-RVSM cruising levels and traffic flows for the AFI Region have been documented in the *Air Traffic Control Operations Manual for Implementation of RVSM in the AFI Region* **[43]**

4.3.7.4 Provisions for contingency facilities

A2.1.6.1.2

"Contingency facilities are provided"

The AFI RVSM Task force has reviewed the airspace structure in the AFI Region with respect to any changes that might be required with respect to the safe operation of RVSM under any non-normal operating conditions. Due account was given to the RVSM contingency procedures, including the possible discontinuation of RVSM under extreme circumstances, provided in the *ATC Operations Manual for Implementation of RVSM in the AFI Region* **[43]**. It has been concluded that no specific changes to the Airspace Design were required with respect to the AFI RVSM system element requirement **AD2**.

Based on this consideration, **Argument 2.1.6.1.2 is considered as true.**

4.3.7.5 Backing evidence

The evidence concerning AFI RVSM Airspace Design is considered to be trustworthy because:

(i) The Airspace Design with respect to the safety requirements **AD1** and **AD2** has been reviewed by the AFI RVSM Task Force, comprised of competent staff familiar with aircraft operations in the AFI Region;

(ii) AFI RVSM is relatively straightforward with regard to Airspace Design since no transition airspace is needed; and

(iii) The existing Airspace Design is assumed to be appropriate with respect to operations under both normal and non-normal circumstances.

4.3.7.6 Conclusion concerning Airspace Design

The arguments and direct- and backing-evidence presented in sections 4.3.7.3 - 4.3.7.5 show that the system element requirements **AD1** and **AD2** allocated to Airspace Design have been properly addressed by the AFI RVSM Programme. The pre- and post-RVSM cruising levels and traffic flows for the AFI Region have been documented in the ARTF meetings and associated documentation. In addition, no SER resulting from the FHA were allocated to Airspace Design.

Consequently, **Argument A2.1.6 is considered as true**.

4.3.8 Aircraft and operator equipment

A2.1.7:
"Design of aircraft and operator equipment complies with SERs "

This section sets out the argument and evidence that Aircraft and Operator equipment (ACOE) have been designed in compliance with the System Element Requirements.

4.3.8.1 System Element Requirements

Aircraft height-keeping performance is the key parameter for the collision risk due to the loss of correctly established vertical separation. Therefore, as stated in section 3.3.5, the high-level safety requirement AFI RVSM 4 concerning the technical vertical collision risk has been allocated in its entirety to the Aircraft Equipment element of the ATM system. As, in principle, equipment performance may vary over time, it is important to ensure that initial performance will not deteriorate over time. Thus, the following two formal Safety Requirements, **AC1** and **AC2**, have been formulated:

- **AC1** (AFI RVSM 4) "RVSM-approved aircraft height-keeping shall be consistent with a TLS of 2.5×10^{-9} fatal accidents per flight hour"; and
- **AC2** (AFI RVSM 4) RVSM-approved aircraft height-keeping shall <u>continue</u> to be consistent with a TLS of 2.5×10^{-9} fatal accidents per flight hour".

The set of SERs is completed by requirements resulting from the integrity safety requirements. They are intended to ensure that the hazard mitigations, related to flight crew and operator training, are available during RVSM operations. These requirements are presented in **Appendix C**.

4.3.8.2 Approach

The two safety requirements **AC1** and **AC2** have been addressed by the development of an aircraft specification, the MASPS, Minimum Aircraft System Performance Specification (References **[40] [41]**). The MASPS comprises two elements, namely the performance specification proper and on-going maintenance requirements. Thus, the Aircraft Equipment system element requirements **AC1** and **AC2** will be met if:

(i) All aircraft operating in AFI RVSM airspace meet the height-keeping performance specification of the MASPS; and

(ii) All aircraft operating in AFI RVSM airspace meet the maintenance requirements of the MASPS.

It is important to recognise that the technical vertical TLS and the MASPS are global entities, equally applicable to any ICAO Region (cf. reference **[1]**).

Figure 14 shows the arguments and evidence that the Aircraft Equipment safety requirements have been met in the AFI RVSM Concept. Note that as for the other System elements, SERs resulting from the integrity safety requirements (FHA) are addressed under the lower argument "Hazards and risks are mitigated".

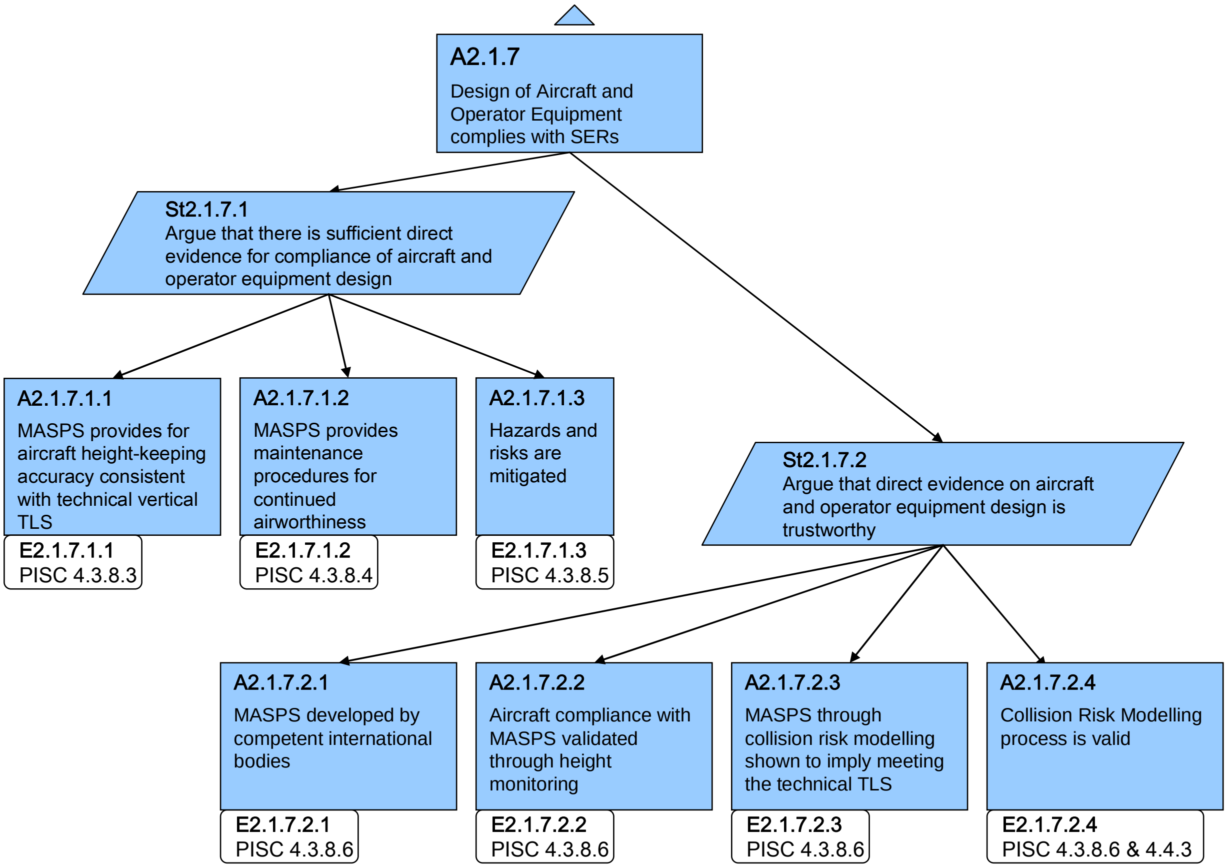

Figure 14 : Argument 2.1.7 – Argument and evidence structure

These are discussed in more detail in the following subsections. Because of the global nature of the pertinent requirements **AC1** and **AC2**, the reasoning for will be seen to be very similar to that utilised in reference **[80]**. Concerning the SERs resulting from the FHA (mitigation of hazards and risks), the approach is similar for each System element.

4.3.8.3 Aircraft height-keeping performance in the MASPS

A2.1.7.1.1:

"MASPS provides for aircraft height-keeping accuracy consistent with technical vertical TLS"

As stated before, aircraft height-keeping performance is the key parameter for the collision risk due to the loss of correctly established vertical separation. The technical vertical TLS of 2.5×10^{-9} fatal accidents per flight hour specifies an upper bound for this type of risk. This upper bound on the risk has been translated into MASPS limits for aircraft height-keeping in a number of steps based on the work presented at RGCSP/6 and RGCSP/7 **[7] [8]**. These steps are summarised below. The credibility of the work performed on the MASPS will be addressed in section 4.3.8.6.

The first step towards the MASPS has been the derivation of the global system performance specification (Refs. **[1]** and **[7]**). This specification sets limits to the probability of vertical overlap for aircraft on adjacent flight levels separated by 1000 ft and to the frequency of exposure to the risk of the loss of vertical separation. As risk exposure varies from airspace to airspace dependent on route structure and navigation accuracy, RGCSP/6 specified a conservative upper limit for the level of risk exposure, namely the equivalent of 2.5 opposite direction aircraft passing per flight hour. This value was subsequently used in an appropriate collision risk model to derive a globally applicable upper limit for the probability of vertical overlap that is consistent with the technical vertical TLS of 2.5×10^{-9} fatal accidents per flight hour. The resulting upper limit for the probability of vertical overlap was found to be 1.7×10^{-8}.

The upper limit on the probability of vertical overlap was then used as the basis for the derivation of a global height-keeping performance specification which sets limits on the proportions of Total Vertical Error (TVE) in a number of ranges, namely beyond 300 ft, 500 ft, 650 ft, and between 950 ft and 1050 ft in magnitude.

Finally, the global height-keeping performance specification was translated by international technical bodies into performance specifications for Altimetry System Error (ASE) and altitude control systems, the RVSM MASPS. The MASPS sets limits on the ASE of individual airframes as well as on the mean ASE and the mean ASE plus three standard deviations for groups of aircraft. It also requires an automatic altitude control system capable of controlling altitude within a certain width about the selected altitude. The detailed specifications of the MASPS are included in references **[40]** and **[41]**.

In order to ensure that each aircraft wanting to operate in RVSM airspace meets the MASPS, it needs to be formally RVSM approved by the responsible certifying authority as set out in references **[40]** and **[41]**.

Based on these considerations, **Argument A2.1.7.1.1 is considered as true**.

4.3.8.4 Maintenance requirements in the MASPS

A2.1.7.1.2:

“MASPS provides maintenance procedures for continued airworthiness ”

As described in reference **[1]**, it is imperative that all aircraft continue, during their service life, to satisfy the requirements of the MASPS. Therefore, maintenance procedures related to continued airworthiness have been developed as a part of the MASPS. Details of these procedures may be found in section 10 of references **[40]** or **[41]**.

Argument A2.1.7.1.2 is considered as true.

4.3.8.5 Mitigation of hazards and risks

A2.1.7.1.3:

“Hazards and risks are mitigated ”

The set of SERs resulting from the integrity safety requirements (FHA) are presented in **Appendix C**. They are intended to ensure that the hazard mitigations, related to aircraft and operator equipment, are available during RVSM operations.

The approach for realising these SER is detailed in **Appendix D** which also provides the evidence of their realisation through this approach.

On the basis of the results presented in this **Appendix D**, it can be concluded that the hazard mitigations related to aircraft and operator equipment have been properly addressed by the AFI RVSM Programme. Consequently, **Argument A2.1.7.3 is considered as true.**

4.3.8.6 Backing evidence

This section sets out why the MASPS are a credible solution to meeting the high-level safety requirement AFI RVSM 4 for the technical vertical collision risk. Two elements have to be distinguished, namely the development of the MASPS as such and the relationship between the MASPS and technical vertical collision risk, taking into account that the latter is also dependent on other airspace parameters.

The MASPS has been developed by competent international groups like RTCA and EUROCAE based on the prior work performed by the ICAO RGCSP. The key of the MASPS are requirements on ASE and altitude control that all aircraft have to meet. How to precisely meet these requirements is dependent on the aircraft under consideration. Aircraft manufacturers have used the MASPS to develop height-keeping system designs (new aircraft) and design changes (service bulletins, existing aircraft) to make their aircraft MASPS compliant.

One way of demonstrating actual compliance with the MASPS is the collection and statistical analysis of height monitoring data. Guidance on this has been provided by ICAO in the *Manual on Implementation of a 300m (1000ft) Vertical Separation Minimum between FL 290 and FL410 inclusive* **[1]**. Ground-based and GPS-based monitoring systems have been developed and utilised for the benefit of the implementation of RVSM, e.g. in the NAT and Europe. Subsequent analysis of height monitoring data has shown the efficacy of the MASPS (Refs. **[82]** and **[91]**). See **Appendix F** for further details.

Consider now the relationship between the MASPS, the technical vertical collision risk and the pertinent TLS of 2.5×10^{-9} fatal accidents per flight hour. The claim behind the MASPS is that meeting it provides confidence that the global height keeping performance specification for RVSM **[1]** is met, which, in turn, provides confidence that the probability of vertical overlap for aircraft at adjacent flight levels will meet the global system performance specification, which finally provides confidence that the technical vertical collision risk will meet the technical vertical TLS.

To prove the validity of this claim, an assessment of the technical vertical collision risk (CRA) has been made using data obtained from the AFI region. The CRA is fully documented in section 3 of **[68]** and has been summarized in **Appendix G**. The CRA has shown that the technical vertical collision risk in AFI RVSM airspace does meet the technical vertical TLS of 2.5×10^{-9} fatal accidents per flight hour.

It may thus be concluded that the (global) MASPS do ensure that the technical vertical collision risk meets the technical vertical TLS, i.e. the validity of the AFI system element safety requirement **AC1**.

As far as the MASPS maintenance requirements **AC2** are concerned, these can only be validated for the AFI Region after a certain period of time of AFI RVSM operations. However, experience in the NAT and Europe has shown the effectiveness of these requirements, despite a slight trend in ASE performance. The causes of this trend are under investigation. Height monitoring for the AFI Region is further discussed as a part of system performance monitoring in section 4.3.9.

4.3.8.7 Conclusion concerning aircraft and operator equipment

The arguments direct- and backing-evidence presented in sections 4.3.8.3 to 4.3.8.6 show that the safety requirements **AC1** and **AC2,** as well as the applicable integrity safety requirements, allocated to Aircraft and Operator Equipment have been properly addressed by the AFI RVSM programme.

Consequently, **Argument A2.1.7 is considered as true**.

4.3.9 System Monitoring

A2.1.8:
"Design of System Monitoring complies with SERs "

This section sets out the argument and evidence that System Monitoring (SM) has been designed in compliance with the System Element Requirements.

4.3.9.1 System Element Requirement

The objective of System Monitoring is to observe/measure with appropriate means the proper and safe operation of AFI RVSM. One critical element of this operation concerns the exclusion from AFI RVSM airspace of non-RVSM approved aircraft and another concerns the collection of data on all airspace parameters related to vertical collision risk, i.e. technical height-keeping deviations, operational errors, traffic flows, navigation accuracy. System Monitoring is, in principle, an on-going process (see **[1]**). To achieve the system monitoring objective, the following five formal Safety Requirements, **SM1 – SM5**, have been formulated (cf. section 3.3.5 and **Appendix C**):

- **SM1** (AFI RVSM 1): "The exclusion of non-RVSM approved non-State aircraft from AFI RVSM airspace shall be monitored" :
- **SM2** (AFI RVSM 8): "The height-keeping performance of RVSM-approved aircraft shall be monitored"
- **SM3** (AFIRVSM 8): "Data on operational errors shall be collected for collision risk estimation"
- **SM4** (AFI RVSM 8): "Data on risk exposure shall be collected for collision risk estimation"
- **SM5** (AFI RVSM 8): "Data on ACAS/TCAS events shall be collected and evaluated"

SM1 addresses the provision for support measures to exclude non-RVSM approved aircraft from AFI RVSM airspace.

SM2 and **SM5** address the provision for measures to monitor respectively the effectiveness of the MASPS, including on-going maintenance programs, with respect to technical height-keeping deviations (SM_2), and ACAS/TCAS traffic alerts (TAs) and Resolution Advisories (RAs) (SM_5).

SM3 and **SM4** address the provision for measures to collect and analyse data respectively on operational errors to assess their contribution to the total vertical TLS (SM_3) and on risk exposure (traffic flows, navigation accuracy) for use in the collision risks models for technical and total vertical risk (SM_4).

It should be noted that no FHA-based safety requirements have been allocated to System Monitoring as it was not the purpose of the FHA **[71]** to address the monitoring of operational errors and ATS performance.

4.3.9.2 Approach

The five safety requirements **SM1 – SM5** have been addressed by the development of appropriate systems and/or arrangements. A key role is played by the Regional Monitoring Agency (RMA) for the AFI Region, ARMA, in conformity with ICAO guidance material **[39]**. Due account has been taken from the experience gained in other ICAO Regions where RVSM was implemented previously.

Figure 15 and Figure 16 show the arguments and evidence that the System Monitoring safety requirements have been met in the AFI RVSM concept. These are discussed in more detail in the subsequent sections 4.3.9.3- 4.3.9.8.

It should be noted that there is a strong link between System Monitoring and the collision risk assessment, the latter using the data resulting from the former. Some elements related to the modelling of technical vertical collision risk were already discussed in section 4.3.8, Aircraft and Operator Equipment. Collision risk modelling elements pertaining to total vertical risk due to the remaining causes will be dealt with in section 4.4 for the safety requirement RVSM5.

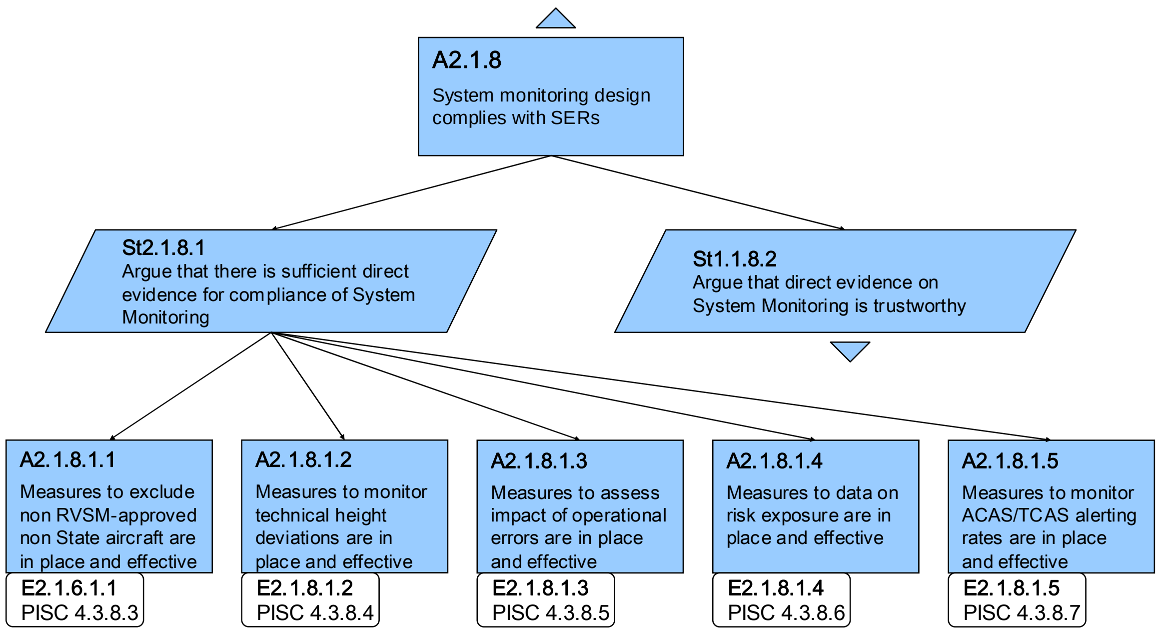

Figure 15 : Argument 2.1.8 – Direct argument and evidence structure

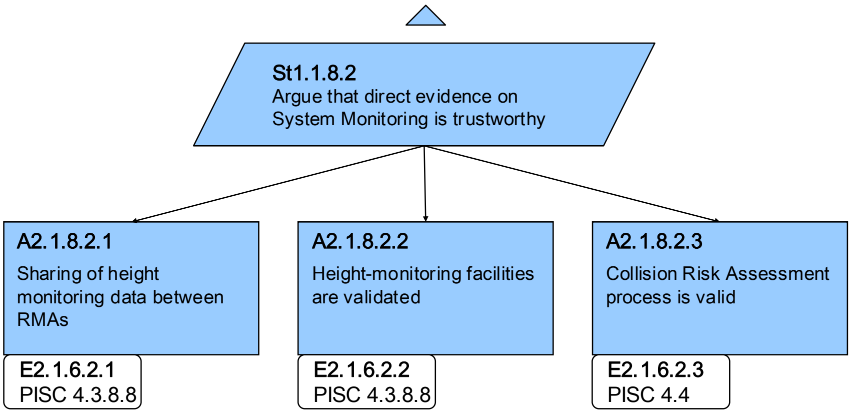

Figure 16 : Argument 2.1.8 – Backing argument and evidence structure

4.3.9.3 Measures to exclude non RVSM-approved non-state aircraft

A2.1.8.1.1

"Measures to exclude non RVSM-approved non-State aircraft are in place and effective"

A database on RVSM approvals relevant to AFI RVSM is held by ARMA. Data has been obtained from the following sources:

- Airworthiness Authority of State of aircraft registration;
- Airworthiness Authority of State of operator registration;
- Operator; and
- EUROCONTROL, APARMO, SATMA and MAAR RVSM database.

The data will be used for cross-checking against flight plan data where the letter "W" in field 10 of a flight plan indicates that the aircraft/operator have received RVSM approval from the responsible State Authority(s). Unlike in e.g. Europe, there is no central flight planning facility for the AFI Region. ARMA has and will continue to retrospectively process sample flight plan data to verify the validity of the RVSM approval status as filed by the operators. Operators will be queried in cases where discrepancies have been found in order to minimise the likelihood of non-RVSM approved aircraft entering into AFI RVSM airspace. See also sections 4.3.2 and 4.3.4 and concerning Flight Crew/Operator and ATS procedures with respect to flight planning for AFI RVSM airspace.

ARMA has made an inventory of the potentially RVSM capable aircraft fleet registered in the African States. It was concluded that, as of October 2005, a large percentage of this fleet, 46% had not yet been RVSM approved **[60]**. A second inventory in April 2006 showed that this percentage had increased to 49%.

Based on the above, **Argument 2.1.8.1.1 is considered as true**.

4.3.9.4 Measures to monitor technical height-keeping performance

A2.1.8.1.2

"Measures to monitor technical height deviations are in place and effective"

Measures to monitor technical height-keeping deviations can be broadly subdivided into ground-based systems (HMU/TMU) or GPS-based systems (GMU). Although no ground-based height monitoring system has been developed for the AFI Region, ARMA, as responsible, amongst other things, for height monitoring, has co-ordinated with EUROCONTROL in its capacity of RMA for the EUR Region, with regards to the exchange of height monitoring data collected in Europe for those aircraft types operating in the AFI Region. This data has been used for the assessment of the technical vertical collision risk under AFI RVSM as documented in reference **[68]** and as summarised in **Appendix G** to the underlying safety case (See also section 4.3.7).

In addition, ARMA has entered into a contract with ARINC for GMU-based height monitoring of those aircraft types for which no other data was available. **Appendix F** provides a summary of the initial results obtained from this monitoring.

The above fits within the AFI RVSM Monitoring Policy developed by ARMA in conjunction with the AFI RVSM Task force **[42]**. Monitoring targets form an important part of the monitoring policy. A summary of the achievement of these targets is included in **Appendix F**.

Another use of height monitoring data is to provide follow-up in case of a measurement showing poor height-keeping performance, with a view to assessing and remedying the causes **[1]**. This follow-up is performed by ARMA in close co-operation with State Authorities, operators, manufacturers and other RMAs **[39]**. The same process has been proven to be effective in e.g. the NAT and EUR Regions.

Based on these considerations, **Argument 2.1.8.1.2 is considered as true**.

4.3.9.5 Measures to assess the impact of operational errors

A2.1.8.1.3

"Measures to assess impact of operational errors are in place and effective"

Conclusion 5 of the first meeting of the AFI RVSM Task Force initiated all States to institute procedures for reporting of data, incidents and conditions relevant to pre-implementation collision risk assessment. A reporting format as in Appendix B to the meeting report was to be used **[16]**. The topic was subsequently discussed at several Task Force meetings. States have been formally requested by ICAO State Letter to comply with this conclusion **[56] [57] [58] [59]**. Consequently, each State has instituted a national data collection programme for the benefit of the implementation of RVSM in the AFI Region (See also section 5). Different States have started submitting different quantities of operational error data from November 2004 onwards.

In addition to direct reports from States, ARMA has co-ordinated with IATA, specifically the AIAG, on the use of operational error data available at the aircraft operators' side.

A summary of the pertinent operational error data is provided in **Appendix I**.

Like the monitoring data on technical height-keeping deviations, the operational error data have been used in an appropriate collision risk model to assess their contribution to the total vertical collision risk. In fact, two assessments have been performed. The first assessment used operational error data provided by the AFI

States for the period of time from September 2004 to May 2005 and provided by the AIAG for the year 2003. It was found that the estimate of the total vertical collision risk did not meet the total vertical TLS of 5×10^{-9} fatal accidents per flight hour **[68]**. This result was presented to the APIRG 15 meeting in Nairobi, Kenya, in September 2005, together with recommendations on how to reduce the occurrence rate of vertical incidents **[69]**. A new set of operational error data pertaining to the period of time 1 January 2006 to 31 December 2006 was subsequently acquired and used in a second assessment showing that there was an improvement **[70]**. A summary of the pre-implementation assessment of the total vertical collision risk in AFI RVSM airspace will be provided in **Appendix G**. Data from the on-going system performance monitoring will be used for a post-implementation collision risk assessment to confirm certain assumptions and approximations that necessarily had to be made prior to implementation. Recall that a Post Implementation Safety Case will be produced in due course as another deliverable of the AFI RVSM safety sub-programme.

Based on these considerations, **Argument A2.1.8.1.3 is considered as true**.

4.3.9.6 Measures to collect data on risk exposure

A2.1.8.1.4

"Measures to collect data on risk exposure are in place and effective"

As follows from section 3 in Appendix A to reference **[1]**, two methods exist for estimating risk exposure, namely the use of flight progress information or radar data. The flight progress information method has been used for AFI RVSM. Appropriate data collection forms have been developed in the same way as for the collection of operational error data described in section 4.3.9.5 The core of the data to be collected consists of the flight level and the time of passing a reporting point, for all the reporting points on all the routes in each State's airspace between FL290 and FL410 inclusive. It should be noted that for a pre-implementation assessment this data is collected in a CVSM environment and needs to be translated to an RVSM environment.

Like the other monitoring data, traffic flow data on risk exposure has been used in the assessments of technical and total vertical collision risk as summarised in **Appendix G**.

Based on the above, **Argument 2.1.8.1.4 is considered as true**.

4.3.9.7 Measures to monitor ACAS/TCAS alerting rates

A2.1.8.1.5

"Measures to monitor ACAS/TCAS alerting rates are in place and effective"

The ACAS events are duly recorded by the IATA AIAG database and supplied to ARMA for the assessments. This is further recorded on the ARMA F3 forms which are returned on a monthly basis to ARMA. The events where applicable have been worked into the CRA 2 and are satisfactory.

4.3.9.8 Backing evidence

The trustworthiness of the evidence with regard to System Monitoring presented in the sections 4.3.9.3 - 4.3.9.7 is based on that related to the monitoring infrastructure together with that related to the use of the monitoring data for collision risk assessment. The latter part will be dealt with in section 4.4 as part of the treatment of high-level safety requirement RVSM5 for the total vertical risk.

For the majority of the aircraft types that will be operating in AFI RVSM airspace, technical height-keeping data collected by means of the ground-based height monitoring infrastructure in the EUR Region has been used. The validity of the latter has been established in **[80]**.

Monitoring of the remaining aircraft types by means of GMUs started in the middle of the year 2006. This type of monitoring has also taken place and has been validated for EUR RVSM. The contractor performing this type of monitoring for the AFI Region under the leadership of ARMA has been involved with the development of the GMU-based monitoring system from the very beginning and is, therefore, quite competent in this field.

Sharing of monitoring data between RMAs and use of common procedures and practices has been stimulated by ICAO as reflected, for instance, in the *Handbook for RMAs* **[39]**.

Another important part of the monitoring infrastructure concerns the collection of data on operational errors and risk exposure. The process put in place builds on experience gained in other ICAO Regions, particularly the European and NAT Regions. Its trustworthiness ultimately depends on the co-operation of the States and the other stakeholders. States have fully committed themselves to the process through their National Safety Plans (cf. section 5). Based on the initial CRA and the subsequent urge at the APIRG/15 meeting **[13]** to both address the causes of vertical incidents and to improve upon the incident reporting rate, significant improvements have been observed, see **Appendix G** and reference **[70]**.

4.3.9.9 Conclusion concerning System Monitoring

The arguments and direct- and backing-evidence presented in sections 4.3.9.3 - 4.3.9.8 show that the safety requirements **SM1 – SM5** allocated to System Monitoring have been properly addressed by the AFI RVSM Programme. In addition, no SER resulting from the FHA were allocated to System Monitoring.

4.3.10 Conclusion concerning design of System elements

The arguments and direct- and backing-evidence presented in sections 4.3.2 to 4.3.9 show that the safety requirements allocated to the elements of the AFI RVSM system have been properly addressed by the AFI RVSM Programme. Consequently, **Argument A2.1.8 is considered as true**.

4.4 Total vertical risk to meet the TLS

This section sets out the argument and evidence that:

A2.2: "Design of AFI RVSM System complies with RVSM5 "

4.4.1 Introduction

An overall measure of the safety of AFI RVSM operations is the total vertical collision risk, i.e. the risk due to all causes leading to the loss of vertical separation. Based on the ICAO guidance material **[1]** and the AFI RVSM Safety Policy **[2]**, this has resulted in the following high-level safety requirement:

- **RVSM5** (AFI RVSM 5): "The probability of any system failure leading to a mid-air collision shall be sufficiently low for the risk of mid-air collision due to the loss of vertical separation from all causes in AFI RVSM airspace to meet a TLS of 5×10^{-9} fatal accidents per flight hour."

Notice that system failure refers to equipment, people as well as to procedures.

Figure 17 and Figure 18 show the arguments and evidence with respect to the work performed by the AFI RVSM Programme on **RVSM5**:

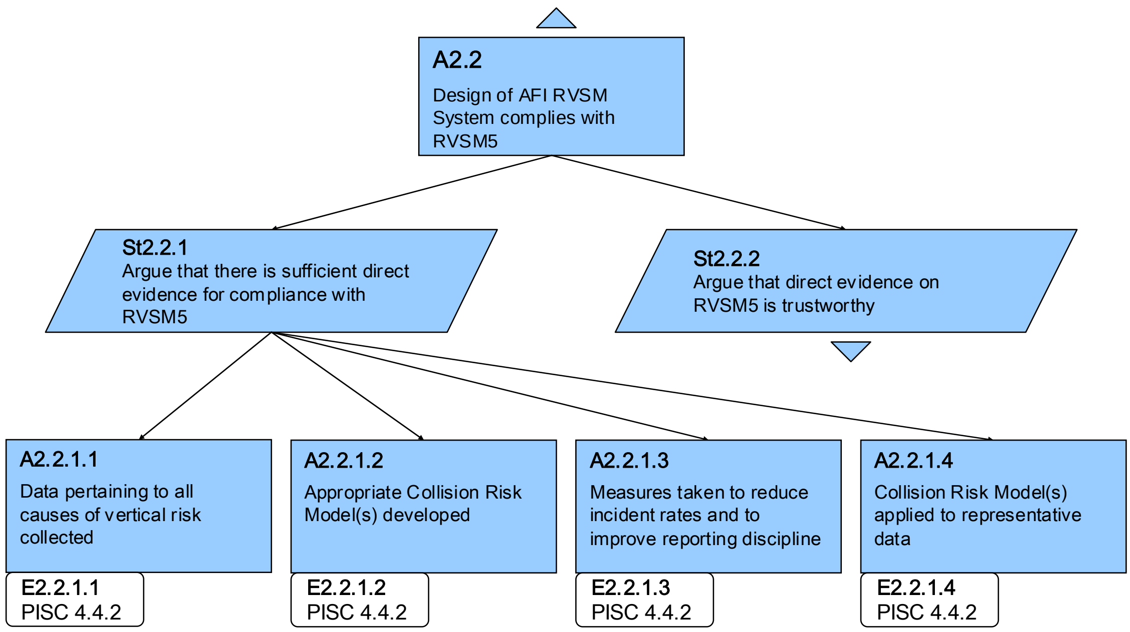

Figure 17 : Argument 2.2 – Direct argument and evidence structure

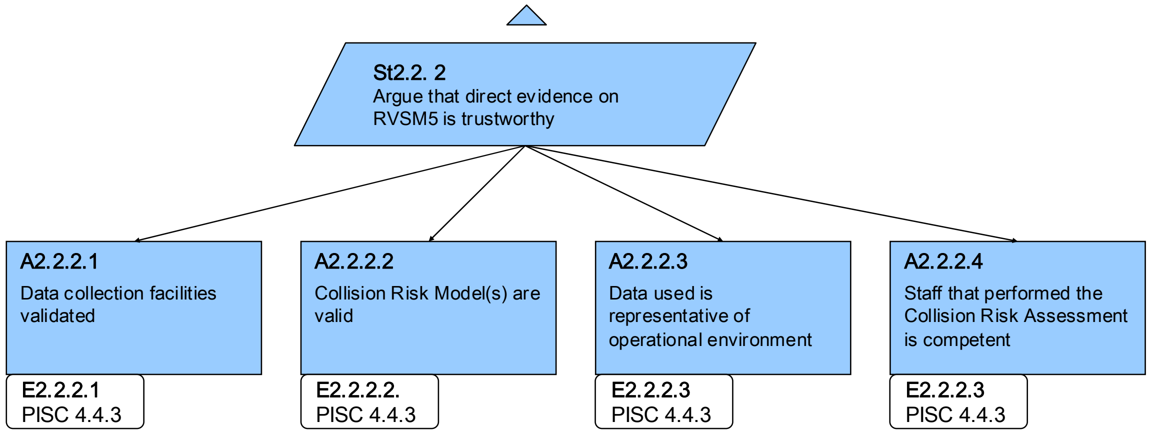

Figure 18 : Argument 2.2 – Backing argument and evidence structure

4.4.2 Direct evidence

The direct evidence is that, under the auspices of ARMA, a collision risk assessment has been conducted as reported in detail in references **[68]** and **[70]**. The assessment comprised three steps:

(i) Collection of data pertaining to all causes of vertical collision risk;

(ii) Development of an appropriate collision risk model (CRM); and

(iii) Application of the model to the data collected.

Data on technical height-keeping deviations, operational errors, aircraft population and traffic flows have been collected by ARMA through system performance monitoring as described in section 4.3.9.

Since the assessment is to cover the vertical collision risk due to all causes, different collision risk models have been developed for different causes, taking into account the specificities of how each cause of the loss of vertical separation could lead to a collision between two aircraft. The models may be broadly classified on the basis of the following:

(i) Collision risk due to normal technical height-keeping deviations of aircraft assigned to adjacent flight levels separated by 1000 ft;

(ii) Collision risk due to an aircraft traversing through a flight level without a proper clearance;

(iii) Collision risk due to an aircraft levelling off at an incorrect flight level; and

(iv) Collision risk due to other large a-typical height-keeping deviations.

The first type of risk is usually referred to as technical vertical collision risk and was assessed <u>individually</u> against the technical TLS of 2.5×10^{-9} fatal accidents per flight hour on the basis of the high-level safety requirement AFI RVSM 4 or, equivalently, the Aircraft Equipment system element requirement AC1 (cf section 4.3.8). <u>Together</u> with the other three types of collision risk, it is also to be assessed against the total vertical TLS of 5×10^{-9} fatal accidents per flight hour. The second and third types of risk are usually referred to as operational risk. It should be noted that there are <u>no individual</u> TLSs for these two risk components. They need to be assessed jointly and in combination with the technical risk and the risk due to other large height deviations against the total TLS.

The collision risk models have been developed on the basis of previous collision risk modelling work performed by RGCSP **[7] [8]**, the EUROCONTROL Mathematics Drafting Group (MDG) **[79] [80]** and the NAT **[90]**. Full details of the model can be found in references **[68]** and **[70]**.

The various collision risk models have been applied to data collected over two different time periods. The first application was to data from the period of time November 2004 to 31 December 2005. It was found that the estimate of the technical vertical risk met the technical vertical TLS with a fair margin. This was anticipated since the MASPS apply globally and traffic flows are not excessive in the AFI Region. However, the estimate of the total vertical collision risk was found to exceed the total vertical TLS by a considerable factor. See reference **[68]** for a detailed description of the initial assessment.

The results of the first assessment were presented to APIRG/15 in September 2005, together with some recommendations for the way ahead **[13]**. APIRG Conclusion 15/51, amongst other things, required states to pursue stringent incident reporting measures and to intensify their efforts in reducing the incident rates to support positive collision risk assessment.

Following APIRG 15, ARMA, has closely monitored the course of the rate of incidents based on the information provided by the States, IATA AIAG and concluded that a second collision risk assessment should be performed on the basis of an 8 – 12 month period of time starting on 1 January 2006. The previously developed collision risk models have then been applied to the new data and showed that there has been a significant decline. The second collision risk assessment is summarised in **Appendix G**. Full details are provided in **[70]**.

4.4.3 Backing evidence

The backing evidence comprises four parts as indicated in Figure 18. The first part, validation of the data collection facilities, has been discussed in section 4.3.9.

Any collision risk model needs to be fed with <u>data</u> that is <u>representative</u> of the operational environment under consideration. This concerns many variables, particularly the aircraft population, traffic flows and operational errors. The role of ARMA has been instrumental in ensuring this representation. Detailed evidence on this is provided in section 2, Airspace description, of references **[68]** and **[70]**.

The collision risk models developed for the different causes of vertical risk under AFI RVSM are based on suitable extensions and modifications of models in use elsewhere for determining safe vertical or (horizontal) separation minima **[7] [9] [79] [90] [92] [94] [98]** The mathematical correctness of the models, therefore, rests partly on the correctness of those other models. Internal peer review has confirmed the correctness of the extensions and modifications developed. Some software has been developed for the estimation of the amount of exposure to the risk of the loss of vertical separation, given the route network and traffic flows in the AFI Region. The software has been carefully tested, partly by means of 2-version programming. As explained in e.g. **[80]**, validation of collision risk models against empirical data is not feasible due to, fortunately, the rareness of the occurrence of collisions.

Finally, evidence on the competence of the staff who conducted the assessment of the total vertical collision risk is included in **Appendix G**.

4.4.4 Conclusion regarding the assessment of the total vertical risk

The result of the CRA 2 clearly demonstrated that there has been a significant improvement since the first assessment. The total vertical risk was assessed to be $15x10^{-9}$. In compliance with APIRG conclusion 16/43 the following additional measures will be applied in order to drive the level of safety towards the ICAO TLS.

- SMS application
- Reduction of operational errors
- Seminars
- Refresher training
- Media exposure

The total vertical risk will be assessed at least on an annual basis to monitor the trend.

4.5 Number of ATM-induced accidents and incidents not to increase

This section set outs the argument and evidence that:

A2.3: "Design of AFI RVSM System complies with requirement AFI RVSM6 "

4.5.1 Introduction

The main purpose of Air Traffic Management (ATM) is to ensure the safe separation of aircraft whilst expediting and maintaining an orderly flow of traffic. Since the number of ATM-induced accidents and incidents with regard to the provision of safe vertical separation could be different in an RVSM environment as compared to a conventional environment, the AFI RVSM Safety Policy includes a safety objective to account for this (cf. section 2.2.3). The objective was translated directly into the following high-level safety requirement (section 3.3.1):

- **RVSM6** (AFI RVSM 6): "The system shall be sufficiently reliable for the number of ATM-induced accidents and serious or risk-bearing incidents in AFI RVSM airspace not to increase from current levels and, where possible, to decrease".

Figure 4.6 shows the arguments and evidence concerning the work performed by the AFI RVSM Programme on this high-level safety requirement. Notice that the direct evidence distinguishes between pre- and post-implementation measures.

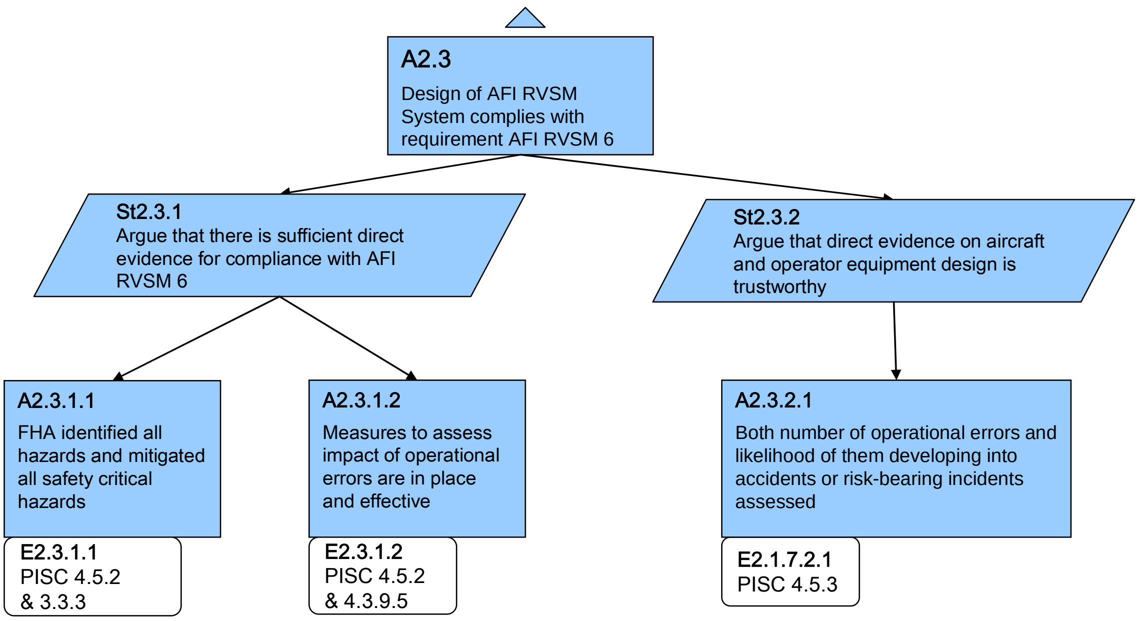

Figure 19 : Argument 2.2 – Backing argument and evidence structure

4.5.2 Direct evidence

The number of ATM-induced, more specifically, ATS-induced, accidents and risk-bearing incidents might be different between an RVSM environment and a CVSM environment due to two factors. The first factor concerns the actual number of ATS errors and the second factor concerns the consequences of an error, given that one has occurred. There is no prior reason why the number of ATS errors in an RVSM environment would be higher than in a CVSM environment. In fact, as it has been argued , the number of ATS errors might well be lower because of ATS having more flexibility to provide safe separation between aircraft. On the other hand, there might also be some increase in ATS workload, e.g. due to an increase in nuisance wake vortex encounters. As regards the second factor, the consequences of an ATS error might be different in an RVSM environment in that there may generally be less time for resolution after an ATS error has been committed. Hence, there may be a higher likelihood of an error actually developing into an accident or risk-bearing incident.

If follows from the above that the key with respect to the risk due to ATM-induced accidents and incidents are the hazards related to ATS Procedures, Training and Equipment. As set out in section 3.3.3 and summarised in **Appendix B**, the AFI RVSM Programme has conducted a full Functional Hazard Assessment, the first step of which was hazard identification through brainstorm sessions with participation of experts from the AFI Region **[71]**. All hazards have been assessed with regard to their severity and occurrence frequency. Subsequently, risk mitigation and safety requirements have been developed. This should ensure that, upon implementation of AFI RVSM, the ATM-induced risk has been reduced as far as is reasonably practicable.

Following the implementation of AFI RVSM, the number of ATM-induced accidents and risk-bearing incidents shall continue not to increase and, preferably, to decrease. This may be achieved through the ongoing assessment of the impact of operational errors as described in section 4.3.9 under System Monitoring.

4.5.3 Backing evidence

The number of ATM-induced accidents and incidents depends on the number of ATM errors and their consequences in the sense of the likelihood of such errors actually developing into accidents or incidents. The direct evidence concerning **RVSM6** is considered trustworthy because both factors (number of errors and consequences) have been addressed. Additional evidence follows from the trustworthiness of the FHA process and the measures to assess the impact of operational errors.

4.5.4 Conclusion regarding ATM-induced accidents and incidents

The arguments and direct- and backing-evidence presented in sections 4.5.2 and 4.5.3 show that the system element requirement **RVSM6** has been properly addressed by the AFI RVSM Programme.

4.6 Safety constraints

A2.4: "Safety constraints, if any, are met "

Aircraft collision risk increases with the number of flights in a given airspace. There are no explicit criteria for the number of flights that the AFI ATM system must be able to handle for the next 10 years, say. Nonetheless, it is clear that the results of the collision risk assessment with respect to meeting the technical TLS and the total vertical TLS need to remain valid over an appropriate planning horizon.

The current collision risk assessment as summarised in **Appendix G** was based on 2004/2005 traffic levels. The effect of traffic growth in the AFI Region has also been examined and summarised in **Appendix G**.

4.7 Residual risks

A2.5: "Residual risks, if any, are tolerable "

4.7.1 Introduction

This section discusses in some further detail four aspects of AFI RVSM operations that have a special relationship with safety, namely level busts, ACAS/TCAS issues, wake vortices, and mountain waves. Formally, only level busts in "environment 2" should be considered as residual, since the pertinent hazard remained safety critical after mitigation **[71]**. The discussion of other three aspects may be considered as additional backing evidence concerning the safety of the AFI RVSM concept.

4.7.2 Level Busts, Large Height Deviations

The FHA assessed one hazard in one "environment" (cf. reference **[71]**) as safety critical after mitigation, viz. **AH $_{\text{core}}$_11**, pilot deviates from clearance. This hazard was assessed as safety critical for environment 2, i.e. controlled airspace without radar or ADS surveillance capability (procedural airspace).

The cause of the hazard is human error, such as misreading of clearance, call sign confusion or incorrect level input into the flight control unit. It was recognised that although elimination of the hazard was not possible, several risk reduction and control factors existed. One safety requirement for Procedures, **Req $_{\text{Core}}$_29**, and two safety requirements for Training, **Req $_{\text{Core}}$_25** and **Req $_{\text{Core}}$_35**, were formulated, together with a safety recommendation, **RCo $_{\text{Core}}$_7**. These have been reflected in the *RVSM Guidance Material to States*, in the Flight Crew procedures in *JAA Administrative & Guidance Material Leaflet No. 6 Revision 1* **[40]**, and in the *Flight Crew Awareness Video* provided to AFI from the European program

It should also be noted that level busts or Large Height Deviations are taken into account as operational errors in the assessment of the total vertical collision risk. In this context, two points should be made. Although the initial assessment of the total vertical risk in reference 2 was found to exceed the total vertical TLS of 5×10^{-9} fatal accidents per flight hour, 7 of the 31 incidents had been classified as a level bust or Large Height Deviation. As described in section 4.4, based on the results of the initial CRA, APIRG/15 has required States to intensify their efforts in reducing incidents and this should also have a positive effect on the occurrence of level busts or Large Height Deviation.

Three more points are worth mentioning. Firstly, a large proportion, about 50%, of the flights in the AFI Region consists of flights into and out of Europe and the Middle East where flight crew are quite familiar with RVSM operations and the potential risk associated with level busts. Secondly, due to the availability of the six additional flight levels, it is likely that the number of requests for en-route level changes will be reduced and hence the potential for the occurrence of level busts. Thirdly, experience has shown that a considerable proportion of level busts is caused by over- and undershoots when an aircraft levels off at the assigned flight level **[80]**. This proportion is expected to go down for two reasons. One of the causes of over- and undershooting of the assigned flight level is the lack of an automatic flight level capture capability on older aircraft (types). Many of these are likely not to apply for RVSM approval. The risk of over- or undershooting is also related to the climb or descent rate applied by an aircraft and, as described in section 6, awareness/procedures have been taken with respect to ACAS/TCAS nuisance alerts to lower the vertical speed in the final stage of a flight level change.

Taking the above five factors into account, it is concluded that the FHA may have overestimated the likelihood of the **AH_{core}_11**, pilot deviates from clearance, hazard. Consequently, all the measures described above are assumed to be sufficient to ensure the safety of RVSM operations in the AFI Region. System Monitoring as described in section 4.3.9 should provide further evidence concerning this conclusion in the future.

It should also be noticed that level busts have been recognised in a broader context than RVSM to be a hazard in aviation and that ways are being pursued to reduce their occurrence .

4.7.3 ACAS/TCAS issues

ACAS/TCAS is generally considered an effective safety net, however not taken into consideration as an AFI RVSM mitigation both in the 1000 ft environment below FL290 and in the airspace at and above FL290. For the AFI Region, for example, the analysis of the operational error data from the airspace between FL290 and FL410 inclusive showed that ACAS/TCAS played a major role in preventing the incidents to develop into collisions between two aircraft. Based on current ICAO policy with regard to safety nets **[10]**, this risk mitigating effect was not included in the collision risk assessment.

The FHA identified one hazard, **AH_{core}_25**, ACAS RA (nuisance), with respect to the use of ACAS[16]. This hazard was assessed as safety critical before mitigation and as non-safety critical after mitigation . Nuisance RAs may occur with the latest version, ACAS II/TCAS 7.0, as well as with the older version TCAS 6.04a. In fact, it is well-known that TCAS 6.04a is not compatible with any 1000 ft environment because its logic is based on a 2000 ft VSM rather than a 1000 ft VSM **[11]**. Hence, use of TCAS 6.04a could lead to a high rate of nuisance RAs. Following a nuisance RA by the flight crew could result in a relatively large deviation from assigned flight level. Based on the TCAS logic, however, this is assumed not to pose any risk to third party aircraft. Nonetheless, following the practice developed for the annual RVSM collision risk assessment for the EUR Region (see reference **[80]**, Appendix F), such deviations are accounted for in the assessment of total vertical risk of AFI RVSM (Refs. **[68]** and **[70]**). The same is done with respect to height deviations resulting from genuine ACAS/TCAS RAs.

The carriage of ACAS II/TCAS 7.0 has been mandated in the AFI Region as per Annex 6 . As a result, an acceptable rate of nuisance RAs may be assumed. In fact, the AFI RVSM Programme has examined the carriage of this version of ACAS/TCAS by the candidate AFI RVSM aircraft population and concluded that all RVSM aircraft are equipped. Based on the assumption that all aircraft in AFI RVSM airspace would indeed be carrying ACAS II/TCAS 7.0, the FHA assessed the **AH_{core}_25**, ACAS RA (nuisance), hazard as non-safety critical after mitigation.

[16] Note that hazard AH_{core}_24 (ACAS TA) was assessed to have no impact on the RVSM operation.

It is recognised that some risk might be associated with ACAS/TCAS when a flight crew decides not to comply with an RA. Based on reference **[80]**, this may be concluded to lead to additional ATS workload. However, reference **[80]** (section 5.12.2) also concluded that this was workable. Not following up on an ACAS/TCAS RA by the flight crew was not identified as a hazard by the AFI RVSM FHA. However, any (large) height deviation of the aircraft causing the RA will be included in the collision risk assessment. Following in particular the Lake Constance mid-air collision in 2002, the procedures with respect to the response to ACAS/TCAS RAs by both flight crew and ATS have been scrutinised and tightened up by ICAO **[12]** As a result, all aircraft flying in the RVSM band will conform to the same procedures.

4.7.4 Wake vortices

As described in section 4. hazard **AH $_{\mathbf{core}}$_21**, unexpected severe vortices, was assessed as non-safety critical before mitigation. This hazard was also briefly discussed in section 4.2.6 in relation to Airspace Design. It was noted that although no independent wake vortex study similar to reference 20 had been performed as a part of the AFI RVSM Programme, pilots and air traffic control would be informed that nuisance encounters would increase.

It should also be mentioned that subsequent study of wake vortex encounters after the implementation of EUR RVSM did indeed confirm the initial thesis of wake vortices in RVSM airspace being non-safety critical.

Although no <u>special</u> reporting procedure for wake vortex encounters has been developed, the reporting of any large height deviations due to wake vortex encounters is an integral part of AFI RVSM System Monitoring. See reference RMA Manual for the incident reporting form currently in use.

Pending the availability of any actual data from AFI RVSM operations, it is concluded that hazard **AH $_{\mathbf{core}}$_21** has been sufficiently addressed.

4.7.5 Mountain waves

Mountain waves can have a very similar effect on the vertical motion of an aircraft as wake turbulence. The FHA did not identify mountain waves as a hazard to AFI RVSM operations.

The issue of mountain wave activity in the AFI Region's airspace was investigated by the AFI RVSM Task Force in a paper at its 11-th meeting. The paper concluded that mountain waves were rare in AFI however they should not be excluded.

Nonetheless, there is specific phraseology in the ICAO Doc 4444 for pilots to indicate an inability to maintain RVSM operations due to weather-related phenomena, including mountain wave activity. In addition, the *ATC Operations Manual for Implementation of RVSM in the AFI Region* **[43]** provides procedures for individual as well as multiple aircraft that are reporting height-keeping problems due to adverse weather conditions.

4.7.6 Conclusion

Based on the above, residual risks are considered to be tolerable and **Argument A2.5 as true**.

4.8 Conclusion

Based on the argument and evidence detailed above, it has been shown in this section 4 that **Argument A2 is true**.

5. Argument 3: Safety of the AFI RVSM Implementation

5.1 Introduction

Argument A3 asserts the safety of the AFI RVSM implementation. It addresses, through the strategy (St03), the realisation of the AFI RVSM safety requirements in the implementation of the constituent elements of the AFI RVSM System.

Thus, this section describes the detailed arguments, strategies and evidence that:

A3:
"The implementation of the AFI RVSM concept is safe"

5.2 Approach

As stated in section 2.2.5, each State participating in the AFI RVSM Programme is ultimately responsible for the safe implementation of the RVSM concept in its airspace, even if that airspace has been delegated to an ATM provider. The national RVSM programme managers are responsible for ensuring that all requirements concerning the safe implementation of RVSM in their national airspace have been met. In addition, the AFI RVSM Programme Office (ARPO) responsibilities are:

- to provide guidance, coordination and support to States in their preparation for the implementation of the AFI RVSM concept;
- to review States' readiness for RVSM implementation; and
- to provide independent verification and validation of implementation of RVSM through the monitoring of AFI RVSM System performance by the AFI Regional Monitoring Agency (ARMA)

As seen in section 1.2, among the AFI States participating in the AFI RVSM programme, a distinction should be made between:

- States working today in a CVSM environment in which shall implement the AFI RVSM concept in their respective national ATM system; and
- States already working in a RVSM environment, following the implementation of RVSM in neighbouring ICAO regions, and which shall modify their national RVSM systems to be consistent with the AFI RVSM Concept.

With regard to the first category of States, the implementation of the AFI RVSM concept is considered to be safe if all the system element requirements are met. The approach consists in the development of National Safety Plans by States to show how the respective State responsibility is discharged and what activities they are undertaking to achieve the safety requirements. Approval of such safety plans provides a commitment to make endeavours to implement those plans. However, in order to ultimately ensure the implementation of system element requirements, the approach is completed by the formal certification by the Directors General of national Civil Aviation Authorities (CAAs) of States safety readiness.

Based on that, and according to the respective responsibilities of States and ICAO/ARPO, the safety of implementation is considered to be demonstrated if:

- Implementation requirements ensuring that all the system element requirements are achieved have been produced by ARPO and incorporated into guidance material on the development of National Safety Plans;
- Safety guidance on the development of National Safety Plans has been provided by ARPO through dedicated workshops;
- Each State has produced a National Safety Plan to achieve the implementation requirements;
- National Safety Plans have been reviewed by a dedicated panel of experts, so-called National Safety Plan Validation Panel (NSPVP), chaired by ICAO Montreal, ATM Bureau;
- Each State has certified compliance with its national safety plan and readiness for safe implementation of RVSM; and,
- System monitoring mechanisms have been implemented by the ARMA

Thus, Figure 20 summarises the direct argument and evidence structure supporting **Argument A3**. Direct evidence supporting Argument A3.1 is provided in sections 5.3.1 - 5.3.5.

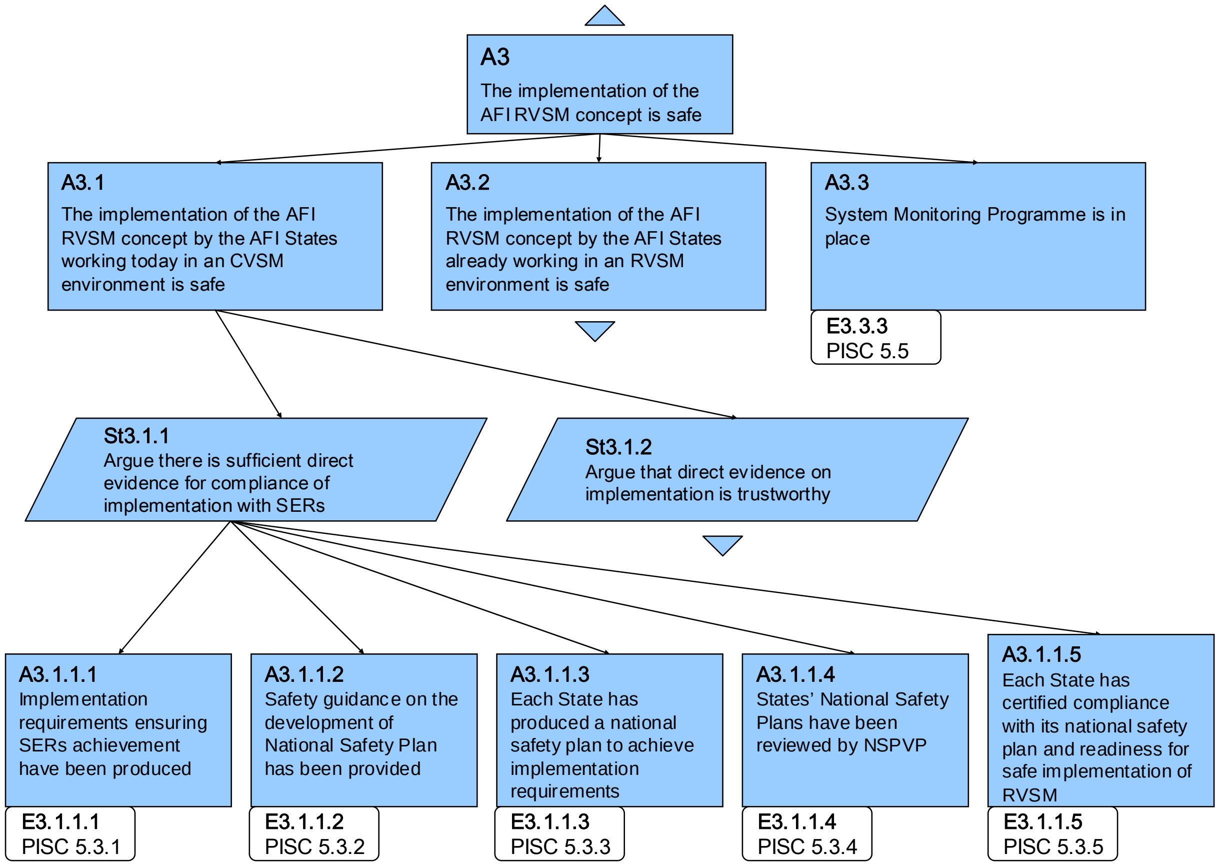

Figure 20 : Argument 3.1 – Direct argument and evidence structure

The backing evidence for Argument A. 3.1 is based on the wide dissemination of the material published by the AFI RVSM Programme and on the correctness of the implementation requirements. The latter have been developed on the basis that the implementation requirement have been proven in EUR RVSM implementation, and that appropriate adaptation to the AFI Region has been made by competent staff.

Figure 21 shows the backing argument and evidence structure supporting **Argument A3.1**. Backing evidence is provided in section 5.3.6.

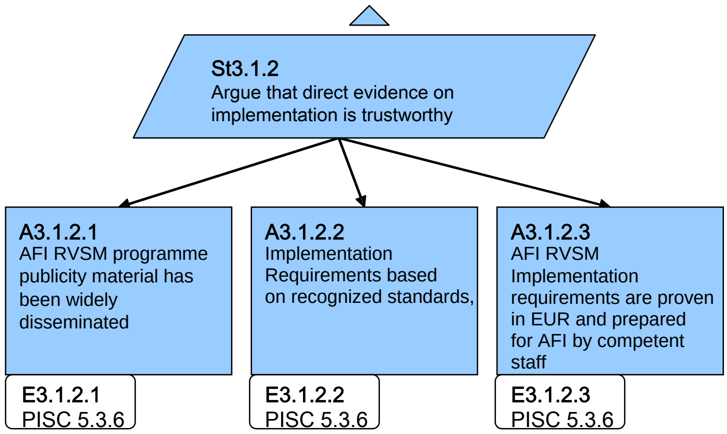

Figure 21 : Argument 3.1 – Backing argument and evidence structure

As far as the States that have already implemented RVSM are concerned, the implementation of the AFI RVSM concept is considered to be safe if changes to the States RVSM systems have been implemented to be consistent with the AFI RVSM concept. Indeed, the safety of RVSM operations has been demonstrated as part of other ICAO RVSM programmes and the approach used is thus relative as only consisting in assessing the changes. The impact of the application of the AFI RVSM concept is twofold[17]:

- Changes to be consistent with the AFI RVSM operational concept; and
- Changes to provide mitigations against the hazards and risks introduced by the application of that concept.

[17] Such distinction has not been made concerning the first category of States because hazard mitigations are an integral part of SERs and thus of the generic AFI RVSM system to be implemented as a whole.

Following that, the safety of implementation of the AFI RVSM concept is considered to be demonstrated if:

- Implementation requirements on the necessary changes to the national RVSM systems have been produced by ARPO;
- States have confirmed that they will implement the necessary changes; and
- States have conducted local hazard and risk analysis.

Figure 22 shows the argument and evidence structure supporting **Argument A3.2**. The direct and backing evidence are provided in sections 5.4.1 - 5.4.3 and sections 5.4.4 respectively.

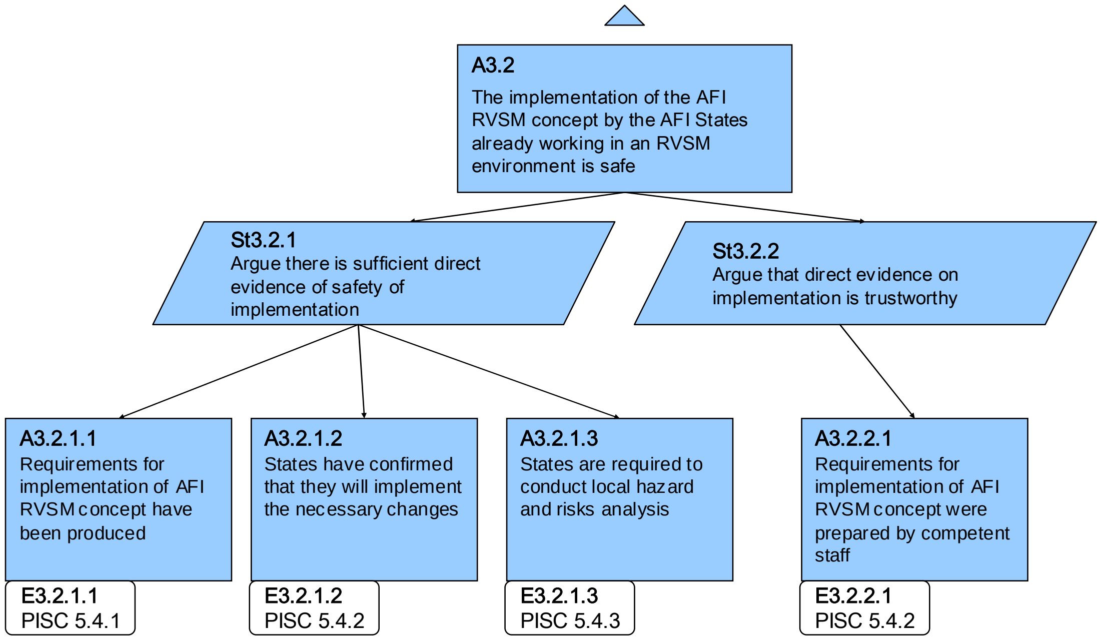

Figure 22 : Argument 3.2 – Argument and evidence structure

Finally, evidence supporting Argument A 3.3 is provided in 5.5

5.3 Implementation by States working CVSM today

5.3.1 Specification of implementation requirements

A3.1.1.1:
"Implementation requirements ensuring SERs achievement have been produced"

5.3.1.1 Introduction

The implementation requirements address the necessary activities to permit safe implementation of RVSM at the national level. To this end, they shall ensure system elements requirements (SERs) achievement by reflecting the approach to satisfy them in implementation.

The implementation requirements have been incorporated into a National Safety Plan (NSP) template **[47]** that is the framework used for providing guidance to States. This template has been developed by ARPO on the basis of the guidance produced for the EUR RVSM implementation with substantial adaptation for the AFI Region. To this end, the following was considered:

- States are sovereign and responsible for meeting those established obligations within ICAO. They should be able to provide evidence of acceptance of the associated responsibilities;
- States that have delegated the responsibility for upper airspace to an ATM provider are ultimately responsible for provision of air traffic services and consequently shall produce and submit for review their own NSP, with the appropriate support of the ATM provider. States approval authorities are the ultimate signatories of the States' NSP's; and
- State authorities that have established comprehensive regulatory systems may identify additional requirements to those specified in ICAO Annexes and should also address these in their NSP.

5.3.1.2 Approach

Following the above, the framework used for specifying implementation requirements is based on the States' obligations within ICAO, namely, in the context of AFI RVSM implementation, that States have aircraft and operator approval processes (coming from ICAO Annex 2 **[3]**) and are responsible for the provision of appropriate air traffic services (coming from ICAO Annex 11 **[4]**). This is the key assertion around which the template of NSP has been built.

Consequently, the implementation requirements are twofold:

- Implementation requirements asking for the evidence that a State has aircraft and operator approval processes; and
- Implementation requirements asking for the evidence that an appropriate air traffic service is provided in the airspace for which a State has jurisdiction.

The framework used for ATS aspects ask for evidence that:

(i) Necessary changes to their national ATM system have been identified and implemented;

(ii) Changes have been approved by appropriate authorities within the State;

(iii) Appropriate quality in the implementation of changes has been achieved; and

(iv) The mitigations against the identified RVSM risks have been properly implemented, ensuring the level of risks to be tolerable and as low as practicable.

The necessary changes to the national ATM system (i) result from the implementation of the generic AFI RVSM system into the airspace for which a State has jurisdiction. These changes concern ATS procedures, ATS training, ATS equipment, airspace design and RVSM operational safety monitoring. The associated implementation requirements are derived from the set of SERs resulting from the high-level safety requirements. They ask for evidence of realisation of these SERs in implementation. As far as the management of RVSM risks are concerned (iv), States are required to review and to adapt to their airspace the results of the AFI RVSM FHA **[71]**. The review process, detailed below, ensures that the SERs resulting from the FHA have been properly addressed in implementation. Finally, the approach is completed by evidence on approval of changes (ii) and on quality assurance (iii).

A similar framework has been used for aircraft and operator approval aspects.

Following that, the NSP template is structured as follows:

- Section 1: Introduction
- Section 2: Aircraft and operator approvals
- Section 3: ATS training
- Section 4: ATS equipment
- Section 5: ATS procedures
- Section 6: Airspace Design
- Section 7: RVSM switch-over[18]
- Section 8: Operational monitoring of RVSM
- State hazard log (iv)

Section 2 related to RVSM approval and sections 3 to 8 for ATS aspects are structured according to the following approach:

- Introduction
- Safety Requirement
- Standard applied
- Activities (i)
- Approval of activities (ii)
- Quality assurance of activities (iii)
- Risk management (iv)

Risk management is addressed in every section from 2 to 8 as well as in Appendix.

[18] Switch-over from CVSM to RVSM is not the purpose of Argument A3 and is addressed in section 4 under Argument A4

5.3.1.3 Implementation requirements

This section discusses the implementation requirements related to the items (i) and (iv) of the above approaches and aims to show that they ensure SERs realisation in implementation. As explained above, the set of SER's resulting from the high-level safety requirements is addressed under item (i) and the associated SER resulting from the FHA are addressed under item (iv). Item (iv) is common to all sections but is addressed below in a separate paragraph.

Implementation requirements related to the items (ii) and (iii), which are thus not directly related to the SERs, as well as those related to the items (i) and (iv), are provided in the AFI RVSM NSP template **[47]**.

Aircraft and operator approval

The system element requirements (resulting from the high-level safety requirements) applicable to flight crew, operator and aircraft elements (FCOP, FCOT, AC) have been realised in concept through the promulgation of appropriate material and the institution by States of aircraft and operator approval processes. The JAA TGL6 revision 1 **[40]** constitutes the applicable standard for States to conduct such approval of aircraft and operators for RVSM operations.

The SERs realisation in implementation is achieved through the States' CAA responsibility to describe their regulatory activities that will lead to documentary proof of the States' diligence with respect to these approvals. The implementation requirement is thus to show that all operators based in the State are aware of the RVSM implementation and have obtained RVSM approval for themselves and their aircraft as appropriate.

More details can be found in section 2 of reference **[47]**.

ATS training

The applicable system element requirements (resulting from the high-level safety requirements) **ATST1a**, **ATST1b**, **ATST2** and **ATST3** address the appropriate training of controllers with regards to RVSM procedures, contingencies, flight plans and non-RVSM civil aircraft transiting through the AFI RVSM airspace. Following their realisation in concept (refer to section 4.3.5) resulting in the design of ATS training, the applicable standard is the *AFI ATS RVSM training guidance material* **[48]**, approved by the AFI RVSM Task Force for application within the AFI Region. It is to be used for the development of States' training material.

Realisation in implementation of requirements **ATST1a**, **ATST1b**, **ATST2** and **ATST3** results in the implementation requirement to show that all relevant staff have been appropriately trained in RVSM procedures and are competent to operate within an RVSM environment through:

- The development of States' training material in compliance with the applicable standard;
- The training of all controllers licensed in RVSM airspace sectors prior to the RVSM implementation date; and
- The provision of refresher training as needed.

More details can be found in section 3 of reference **[47]**.

ATS equipment

The applicable system element requirements **ATSE1** and **ATSE2** address the necessary changes to ATS equipment for RVSM operations. Following their realisation in concept (refer to section 4.3.6), the *ATC Operations Manual for Implementation of RVSM in the AFI Region* **[43]** constitutes the basis for the changes to ATS equipment required for the AFI Region. It is consistent with *ICAO Document 7030/4* **[44]** and provides further information.

Realisation in implementation of **ATSE1** and **ATSE2** results in the implementation requirement to show that the changes to ATS equipment have been made successfully and have been approved for operational use, through the provision of the detailed program for these changes.

More details can be found in section 4 of reference **[47]**.

ATS procedures

The applicable system element requirements ATSPxx address the changes required to existing ATS procedures and the implementation of new ATS procedures within each ACC. Following their realisation in concept (refer to section 4.3.4) the *ICAO Document 7030/4* **[44]** constitutes the standards for ATS procedures. In addition, ARPO has developed the *ATC Operations Manual for Implementation of RVSM in the AFI Region* **[43]** that is consistent with *ICAO 703/4* and provides further amplification of its implementation in the AFI Region

The resulting implementation requirements are to show that the changes to the ATS procedures have been implemented and approved for use, through the changes to ACC operations manual and Letter of Procedures (LoP) and the coordination with State aircraft authorities.

More details can be found in section 5 of reference **[47]**.

Airspace Design

The applicable system element requirements **AD1** and **AD2** addresses the implementation and use of the six additional Flight Levels available under RVSM, and of any changes necessary to accommodate contingency procedures and/or measures arising from abnormal conditions or emergencies respectively. Following their realisation in concept (refer to section 4.3.7), it is best practice to simulate such changes to show both the impact on traffic flows and controller workload, since there are no standards applicable to Airspace Design changes.

Realisation in implementation of **AD1** and **AD2** result in the implementation requirement to show that the changes are appropriate and are consistent with the safe operation of RVSM in the airspace for which a State has jurisdiction, through the provision of the detailed program for these changes.

More details can be found in section 6 of reference **[47]**.

System monitoring

The applicable system element requirements **SM1** to **SM5** address the appropriate means to observe/measure the proper and safe operation of AFI RVSM. One critical element of this operation concerns the exclusion from AFI RVSM airspace of non-RVSM approved aircraft and another concerns the collection of data on all airspace parameters related to vertical collision risk, i.e. technical height-keeping deviations, operational errors, traffic flows, navigation accuracy.

The resulting implementation requirement applicable to each State is to show that appropriate monitoring of the operational safety performance of the ATS in the application of RVSM is provided through two key activities:

- ATS performance safety monitoring; and
- Operational error reporting.

The latter activity asks for State commitment to provide ARMA with operational error data reported by controllers in their ACCs and or flight crew in order to continue contributing to the AFI RVSM Safety Case. Realisation in implementation of **SM1** to **SM5** is indeed shared between the ARMA and the State, the latter providing data to the former.

More details can be found in section 8 of reference **[47]**.

RVSM risk management

The implementation requirement is to show that a State has carried out local hazard and risk assessment. The approach consists of States showing that they have identified and assessed the hazards associated with RVSM operations in their airspace and presenting the activities undertaken to properly implement mitigations, ensuring the risks to be tolerable. This requirement is achieved through:

- The States' commitment to review and adapt the results of the AFI RVSM FHA **[71]** as follows:

(i) Review of FHA operational scenarios and appropriate adaptation as needed;

(ii) Review of FHA hazards per operational scenarios and appropriate adaptation as needed: on the other hand, a State may identify additional hazards that are specific to the local airspace, whereas on the other hand, a State may discard FHA hazards that are considered as not relevant to the local airspace. In the latter case, a rationale is to be provided;

(iii) Review of FHA mitigations and appropriate adaptation as needed States shall review and adapt accordingly the set of mitigations in compliance with their own risk tolerable criteria (that may differ to those used in the FHA); and as a result identify additional mitigations or discard FHA ones as appropriate, and

(iv) Review of allocation of FHA mitigations to the elements of their own RVSM system.

The review of the FHA results is to be captured in the State hazard log table (for AFI RVSM core airspace, purpose of Argument A3) to be included in the NSP appendix (the FHA hazards have been identified at an ATM level and are not associated to a particular element of the RVSM system). This table aims to describe the State RVSM hazards and to provide the set of associated mitigations. The intermediate steps with regard to the assessment of hazard severity, the determination of safety objectives, as well as the rationale for the mitigation strategy, are at States' discretion and are not to be included. Additional details can be found in the Appendix to reference **[47]**.

- The States commitment to provide details on activities undertaken to implement the mitigations against the RVSM risks.

The program of activities for the implementation of the individual mitigations is captured in tables to be provided in each risk management section. Indeed, the risk mitigation strategy for each individual hazard is shared between the system elements and consequently the individual mitigations are specific to a given system element. Addition details can be found in sub-sections n.7 of reference **[47]**.

This process ensures that all SERs resulting from the FHA are successfully addressed at the implementation level. Detailed approach and associated evidence for each individual SER is provided in **Appendix D**.

Conclusion

The above shows that a complete set of implementation requirements have been specified for the RVSM implementation by States and that those requirements ensure the achievement of the whole set of system element requirements. Consequently, **Argument A3.1.1.1 is considered as true**.

5.3.2 Safety guidance on National Safety Plan development

A3.1.1.2:

“Safety guidance on the development of National Safety Plan has been provided”

Introduction

Safety guidance on the development of National Safety Plan has been provided to the States through two dedicated ICAO workshops. The workshops were prepared and facilitated, on behalf of ICAO, by an ATM Safety expert from the ALTRAN Technologies Company, as follows:

- From July 18 to July 23, 2005, in Nairobi (Kenya), under ICAO ESAF office responsibility, facilitated in the English language
- From July 25 to July 29 July, 2005, in Dakar (Senegal), under ICAO WACAF office responsibility, facilitated in the English and French languages

Objectives and contents

The two workshops were similarly structured and composed of two main modules:

- Module 1: Presentation of, and training on, necessary safety concepts to develop NSP (1 day)
- Module 2: Development of their NSP by the States (4 days)

Module 1

The objective of the module 1 was to provide safety background information and to present how the NSP shall be completed. The agenda was the following:

- Risk assessment principles
- Risk Assessment and mitigation in the Air Traffic Management domain
- AFI RVSM Safety Assessment: safety sub-programme, safety policy, process and deliverables
- The RVSM NSP: objectives and structure
- Processing of AFI RVSM FHA results for local adaptation and complements

Module 2

The objective of the module 2 was for States to complete their NSP, with the individual guidance and support provided by the facilitators, on the basis of:

- the AFI RVSM NSP template **[47]**, that provides the AFI RVSM Implementation requirements (cf. section 5.3.1), and of,
- The results of the AFI RVSM FHA **[71]** to adapted and completed to the airspace for which individual States have jurisdiction, as part of the State local hazard and risk assessment, as detailed in section 5.3.1.

To this end, different working groups were created on the basis of the States operational environment and ATM system characteristics.

Outcome

The Nairobi workshop was attended by 71 participants from 21 States and 3 international organizations, namely AFRAA, IFALPA and IFATCA. The Dakar workshop was presented to participating States and International Organizations in West Africa.

The workshops proved to be successful in providing the guidance that States required to complete NSP for ICAO review. Seminar delegates were able to return home with definite guidelines and examples.

Additional details can be found in references **[35]** and **[36]**.

Follow-up

After the two workshops, the safety guidance has been completed and provided by ARPO and ARMA through ICAO AFI RVSM Task Force meetings. In addition, ARMA has continuously provided additional guidance on individual request of the States.

Conclusion

On the basis of the above considerations, **Argument A3.1.1.3 is considered as true**.

5.3.3 States' safety plans

A3.1.1.3:

"Each State has produced a national safety plan to achieve implementation requirements"

As stated in section 2.2.5, each State participating in the AFI RVSM Programme is ultimately responsible for the safe implementation of the RVSM concept in the airspace for which it has jurisdiction, even if that airspace has been delegated to an ATM provider.

In application of the above, each State has produced a unique national safety plan. In the case the airspace for which a State has jurisdiction has been delegated to one or several ATM provider, the NSP has been completed as follows: sections 1 and 2 completed by the State, and sections 3 to 8 completed by the ATM provider(s). Nevertheless the ultimate approval authorities of the NSP are the State ones, which have the responsibility to submit the NSP to ICAO.

The status of the States in their development of national safety plans is provided in **Appendix H**. In summary, there has been a complete response from States: all States have produced and submitted to ICAO an approved National Safety Plan. Those plans are lodged with the ARMA.

As a conclusion, **Argument A3.1.1.3** is considered as true.

5.3.4 Review of States safety plans

A3.1.1.4:

"States' National Safety Plans has been reviewed by NSPVP"

Establishment of the National Safety Plan Validation Panel

As stated in section 2.2.5, the AFI RVSM Programme Office (ARPO) has a secondary responsibility for the implementation of the RVSM concept, in particular, in the provision of review of the National Safety Plans submitted by the States.

In application of the above, the AFI RVSM Task Force has identified the need to establish a dedicated National Safety Plan Validation Panel to carry out the ICAO task of conducting review of the NSP produced by the States. The purpose of the NSPVP was to examine NSPs and to provide feedback to States in the form of individual comments. The panel was composed of Mr. Kevin Ewels, Manager of the African Regional Monitoring Authority (ARMA), Mr. Martin Sacramento Safety Assessment Manager, ASECNA Directorate of Operations, Mr. Harry Roberts, Manager Operational Planning Services, Air Traffic and Navigation Services (ATNS), Mr. Apolo Kharuga, Regional Officer/ATM, ICAO Regional Office, Nairobi, Mr. Ibrahim U. Auyo, Regional/ATM Officer, ICAO Regional Office, Dakar, and of Mr. Craig Partridge, Manager S.O. & I. IATA. The panel was chaired by Mr. Drazen Gardilcic, Technical Officer/ATM, Air Navigation Bureau, ICAO Montreal. Technical support was provided by two ATM Safety experts from the ALTRAN Technologies Company.

The NSPVP held two meetings, convened in Johannesburg (Republic of South Africa), under the auspices of ICAO and support from IATA:

- From September 12 to September 23, 2005, at the IATA office
- From March 21 to March 24, 2006, at the ARMA office

NSPVP review process

The purpose of the review was to seek to establish that each State has produced a National Safety Plan in compliance with the provided guidance, providing as a result, assurance that they will undertake the necessary activities to achieve the implementation requirements.

To this end, the Panel developed an evaluative template that was applied to all submitted safety Plans by the various States in order to assess their validity. This common measuring tool allowed the NSPVP to accurately conclude fair comparative assessments among all the NSPs. With this process the Panel was able to provide a quantifiable assessment of the level of completion of each Plan in terms of percentage of completion of each Plan. In addition to the comparative assessment, the NSPVP undertook a limited review of NSPs compliance with selected items from the FHA tables. The evaluative framework was divided into seven criteria family to compare with each NSP. The seven criteria families were:

- **Editorial:** aimed to seek to establish that the NSP has been produced in conformance with the structure of the NSP template, except for those States for which existing Safety Management Systems require a different structure, due to the additional implementation requirements that may prevail.
- **Overall approval/regulatory process**: aimed to seek to establish that the State has an overall approval/regulatory process for the implementation of RVSM and the State approval of the NSP
- **Operator and aircraft RVSM approval process**: aimed to seek to establish that the State has an effective regulatory process for approval of operator and aircraft for RVSM operations

- **Necessary ATS activities for RVSM operations**: aimed to seek to establish that the State has undertaken, or will undertake (with the associated planning and deadlines), the necessary activities to ensure that appropriate Air Traffic Services will be provided for RVSM operations.
- **Necessary ATS changes/activities approval process**: aimed to seek to establish that the State has accepted responsibility for the provided ATS and has provided the staff positions and names of the persons, in the organisation, with the responsibility for the approval of the different ATS activities.
- **ATS Quality achievement process**: aimed to seek to establish that the State has provided assurance that the ATS activities will meet the relevant ICAO standard, through the provision of details of the State quality achievement activities.
- **RVSM Risk management**: aimed to seek to establish that the State has undertaken the necessary activities to manage the identified RVSM risks, as the result of its local hazard and risk assessment, based on the AFI RVSM FHA, as detailed in section 5.3.1.

Using this evaluative framework and the Functional Hazard Assessment tables for details, the Panel was able to determine, with some limitations, the level of State's compliance of the various NSPs submitted. The limitations in the depth to which the NSPVP was able to analyze the Plans were brought upon by a combination of:

- the large number of NSP submitted,
- the large number of pages and items in the FHA tables (122 pages), and,
- the limited time the Panel had to conduct its evaluation.

Consequently, it is critical to recall that the Panel was able to review only certain items from the tables that it deemed were of higher importance.

In addition to the limitations mentioned above, the Panel wished to clarify that this assessment was based strictly on the contents of the National Safety Plans as presented to the Panel. The Panel had no means to check and was neither qualified nor empowered to independently verify, that the Plans as presented are in fact being carried out in each State. Therefore, the feedback that the Panel will be sending to States is a set of individual comments based solely on a comparison between the submitted NSPs and the NSP template and selected sections of the AFI RVSM Functional Hazard Assessment tables.

NSPVP outcome

After its two meetings, the Panel has provided individual feedback to States in the form of line by line comments on each of the criteria for which they were rated. Those comments have then been incorporated by States in an updated edition of their NSP document that has been approved by the States authorities before submission to ICAO.

The details of the Plans reviewed by the NSPVP I and II are given in **Appendix H**.

Conclusion

The feedback provided to States was necessarily limited in:

- in the evaluation of the compliance with the FHA hazard identification and mitigation tables
- in the fact that the Panel was not able to verify if the comments that has been issued from the NSPVP II are incorporated in the updated edition of the Plans, as the Panel did not meet a third time
- in the fact that the Panel was not able to independently verify that the activities that are described in the Plans are in fact backed by concrete actions.

The latter limitation, which is the most critical, will be recalled in the PISC conclusion (section 9).

Nevertheless, on the basis of the above considerations and of the information contained in Appendix H, **Argument A3.1.4 is considered as true**.

5.3.5 State confirmation of readiness for safe implementation of RVSM

A3.1.1.5:

"Each State has certified compliance with its national safety plan and readiness for safe implementation of RVSM"

The production of the National Safety Plans and more especially their approval by the States' authorities give a commitment that States make their best endeavours to implement the activities contained in those plans.

On the basis of the information provided above this, **Argument A3.1.5 is considered as true**.

5.3.6 Backing evidence

A3.1.2.1:

"AFI RVSM Programme publicity material has been widely disseminated"

The AFI RVSM awareness material has been disseminated to all States via the National Program Manager at all the ARTF meetings. Further to this various media articles have been prepared and published. Selected items are available on the ICAO ESAF website. Initially all States were supplied with an RVSM starter pack which was to be used for their own domestic program.

Consequently, **Argument A3.1.2.1 is considered as true**.

A3.1.2.2:
“Implementation requirements are based on recognised standards”

As stated in section 5.3.1, ICAO Annexes 2 **[3]** and 11 **[4]** has been used as sources for the implementation requirements contained in the AFI RVSM National Safety Plan template **[47]**.

Consequently, **Argument A3.1.2.2 is considered as true**.

A3.1.2.3:
“Implementation requirements are proven in EUR and prepared for AFI by competent staff”

The implementation requirements contained in the AFI RVSM National Safety Plan template **[47]** have been specified on the basis of the EUR implementation requirements which have been proven over 6 years of successful RVSM operations. Nevertheless, a strong adaptation has been made for the AFI Region, in order to take into account the benefits gained in the mean time in the use of the risk assessment methodology. Indeed, the main adaptation addresses the RVSM risk management requirements which have been modified because of the identification of the RVSM hazards at an ATM level in the AFI Region (instead of being identified at system element level, which is considered to be no longer relevant). This adaptation has been made by competent staff, with the pre-requisite background, experience and expertise in the use of the risk assessment methodology. Evidence of this can be found in the FHA document **[71]**, as the staff that produced the FHA was also responsible for preparing the AFI RVSM NSP template.

Consequently, **Argument A3.1.3.2 is considered as true**.

5.3.7 Conclusion

On the basis of the above direct and backing evidence, **Argument A.3 is considered as true**.

5.4 Implementation by States already working RVSM

Introduction: concerned States are Cabo Verde, Egypt, Algeria, Morocco, Tunisia and Dakar Oceanic

5.4.1 Specification of implementation requirements

A3.1.1.1:

"Requirements for implementation of AFI RVSM Concept have been produced"

Description of requirements as discussed during NSPVP II:

AFI States: Dedicated State letter (by ARPO): provision of evidence/reference of:

- Changes to LOP (evidence = State's readiness assessment
- Changes to FLAS evidence = publication of FLAS
- Changes to ACC Operations Manual evidence = State's readiness assessment
- Switchover plan evidence = State's readiness assessment
- Training/Awareness on Non RVSM civil aircraft transiting evidence: acknowledgment of ICAO 7030

5.4.2 Confirmation of changes implementation

A3.1.1.2:

"States have confirmed that they will implement the necessary changes"

Description of required evidence in order to prove the confirmation. Confirmation is mainly based on the acknowledgment of State letters as discussed during NSPVPII requirements:

AFI States: Dedicated State letter (by ARPO): provision of evidence/reference of:

- Changes to LOP State's readiness assessment
- Changes to FLAS evidence = publication of FLAS
- Changes to ACC Operations Manual= State's readiness assessment
- Switchover plan = State's readiness assessment
- Training/Awareness on Non RVSM civil aircraft transiting (evidence: acknowledgment of ICAO 7030)

5.4.3 State hazard and risk analysis

A3.1.1.3:

"States are required to conduct local hazard and risk analysis"

States are required to conduct local hazard and risk analysis, in application of the §2.26 "ATS Safety Management" of the ICAO Annex 11 **[4]** and especially of the following:

"Any significant safety-related change to the ATC system, including the implementation of a reduced separation minimum or a new procedure, shall only be effected after a safety assessment has demonstrated that an acceptable level of safety will be met and users have been consulted. When appropriate, the responsible authority shall ensure that adequate provision is made for post-implementation monitoring to verify that the defined level of safety continues to be met."

The ICAO requirement applied to any significant safety-related change to the ATM system, and a fortiori to the implementation of the AFI RVSM System that constitutes a safety-related change.

Consequently, **Argument A3.1.1.3 is considered as true**.

5.4.4 Backing evidence

A3.1.1.3:

"Requirements for implementation of AFI RVSM Concept were prepared by competent staff"

Process of requirements specification: starting point is the difference between the RVSM operational concepts that differ from one neighbouring region to another. The main impacts of the application of the RVSM concept is the removal of transition airspaces and the possibility offered to the non RVSM civil aircraft to transit through the RVSM airspace based on this assessment, the Core Team has developed specific implementation requirements for those States (Egypt, Morocco etc.) during NSPVP II

5.4.5 Conclusion

On the basis of the above direct and backing evidence, **Argument A.3 is considered as true**.

5.5 System monitoring programme

A3.3:

"System monitoring programme is in place"

The infrastructure for the AFI RVSM system monitoring is in place and can be described as follows:

The ARMA is applying all the tasks as detailed in ICAO Doc 9574 applicable to RMAs. Further to this all the duties as described in the AFI RMA Manual are being carried out.

On a monthly basis the AF State returns are submitted to ARMA for collation and inclusion into the annual safety assessment. Vertical incidents are also collected from IATA after they have been submitted by member airlines.

Height Monitoring is in place and data from other regions is also taken into consideration as per ICAO.

Although it might be suggested that there is an under reporting of incidents the culture of reporting is improving. It can therefore be said that there is a well managed AFI RVSM system monitoring programme in place.

On the basis of the above backing evidence, **Argument A.3.3 is considered as true**.

5.6 Conclusion

Based on the argument and evidence detailed above, it has been shown in this section 5 that **Argument A3 is true**.

6. Argument 4: Safety of Switch-over from CVSM to RVSM

6.1 Introduction

Argument A4 asserts the safety of the switch-over from CVSM to RVSM. It only addresses the Safety of the specific period of 24 hours around the actual Time of Switch-over (ToS) and does not address the actions and timelines required prior to RVSM implementation, which are reflected in the AFI RVSM strategic/action plan **[31]**. It corresponds to the stage a) of the RVSM operations considered in section 2.3.6, i.e. the "AFI RVSM switch-over period" considered by the FHA **[71]**.

Argument A2 addresses, through the strategy (St04), the realisation of the AFI RVSM switch-over integrity safety requirements (cf. **Appendix C**), initially in the design of the switch-over concept and then in the implementation of that concept.

Thus, this section describes the detailed arguments, strategies and evidence that:

A4: *"The AFI switch-over from CVSM to RVSM is safe "*

6.2 Approach

As detailed in section 2.3, **Argument A4** addresses simultaneously the safety of the Concept <u>and</u> of its Implementation for the switch-over operations. The strategy ***(St02)*** to show that **Argument A2** is valid consists in:

- Showing that the switch-over system element requirements are satisfied initially in the design of the switch-over concept and then in the implementation of that concept

Section 3 shows that a complete and correct set of safety requirements has been specified for switch-over operations, as part of the AFI RVSM Concept. Following the same approach as for **Argument A2** in section 4, the switch-over concept is considered to be safe if all the safety requirements have been realised through the successful design of specific elements (procedures, training/awareness, flight planning, etc…) for switch-over operations. That set of system element requirements is only composed of integrity safety requirements and corresponds to the explicit derivation of the specific mitigations identified in the FHA **[71]** that ensure the achievement of tolerable risk levels.

Based on the above, the switch-over safety requirements are considered to be realised in Concept on the basis that:

- A detailed switch-over plan for AFI RVSM has been produced, addressing the principle concerns of the Aviation Community and providing guidance for the development of States' switch-over plans;
- Switch-over hazards and risks are mitigated, meaning that the SERs are realised in Concept; and
- Residual risks related to switch-over, if any, are tolerable, in order to pick up any issues that may not have been resolved under the previous sub-arguments.

The backing evidence is based on the correctness of the switch-over plan for AFI RVSM. As it has been developed on the basis of the switch-over planning used for the EUR RVSM implementation, that appropriate adaptation to the AFI Region has been made, and that switch-over mitigations for AFI RVSM have been appropriately included (cf. section 6.3.1.2 below), it is considered to be correct on the basis that:

- Switch-over planning has been proven in EUR RVSM implementation;

- The AFI RVSM switch-over plan was prepared by competent staff; and,
- After the Go Decision, the AFI RVSM switch-over plan will be continuously reviewed and checked prior to the commencement of RVSM operations.

Figure 23 shows the direct argument and evidence structure for the safety of switch-over concept. The direct- and backing-evidence are provided below in sections 6.3.1 and 6.3.2 respectively.

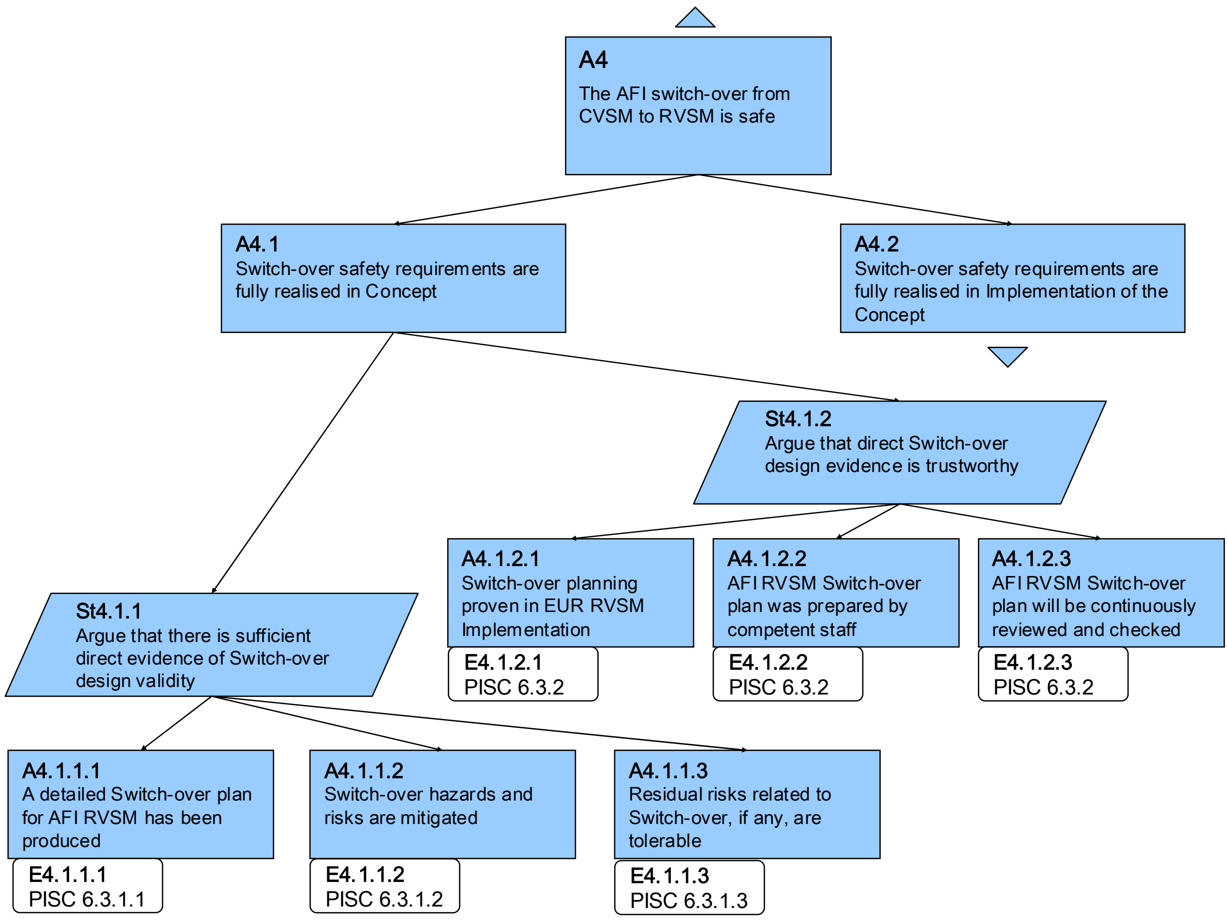

Figure 23 : Argument 4 – Argument and evidence structure (1)

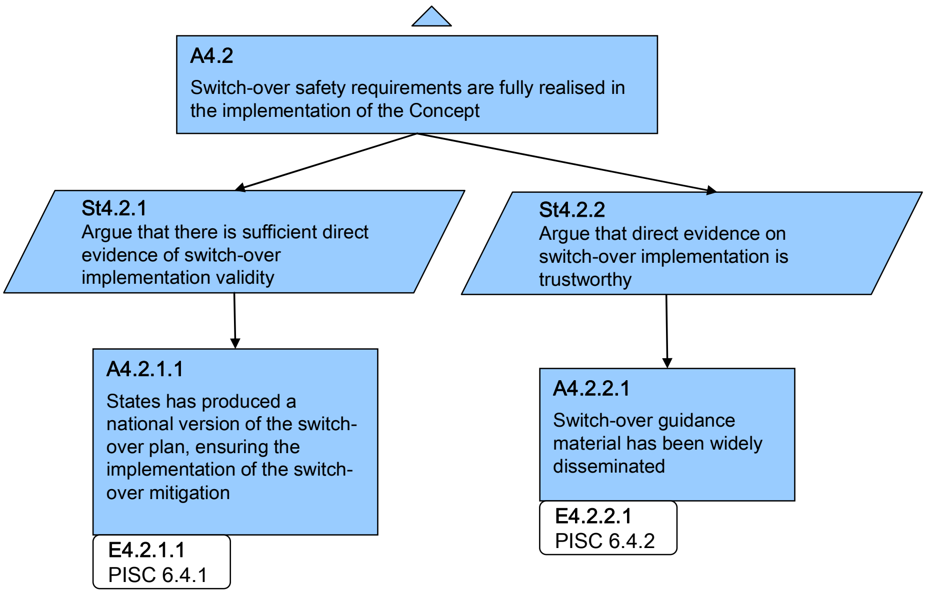

Figure 24 : Argument 4 – Argument and evidence structure (2)

6.3 Safety of Switch-over concept

6.3.1 Direct evidence

6.3.1.1 AFI RVSM Switch-over plan

A4.1.1.1:
"A detailed switch-over plan for AFI RVSM has been produced "

A detailed switch-over plan for AFI RVSM has been issued by the AFI RVSM Task Force / 9 **[25]** and is documented in reference **[61]**. An amendment has been then produced and is documented in reference **[62]**

It aims to provide guidance for the development of States Switch-over Plans so that they are applicable to their own local RVSM System. It addresses the principal concerns of the Aviation Community with regards to the operations during the switch-over period and provides mitigations related to switch-over hazards.

The AFI RVSM switch-over plan has been developed on the assumption that the Go Decision will only be made if the fundamental processes required prior to RVSM implementation, as part of the AFI RVSM strategic/action plan **[31]**, are in place, especially the Safety Case, with special reference to the total vertical risk.

The AFI Regional Monitoring Agency (ARMA) will serve as a focal point of contact during the switch-over period and States are required to report all significant operations/events/problems relating to the switch-over to the ARMA.

The concept of AFI RVSM switch-over is decomposed into three different phases:

- Immediate pre-implementation phase: ToS - 24h to ToS

- Implementation phase: ToS; and
- Immediate post-implementation phase: ToS to ToS + 24h

Immediate pre-implementation phase: ToS – 24h to ToS

During this period, National Programme Managers (NPM) will continue reporting implementation readiness to ARMA. The actions to be undertaken address airspace configuration, flight planning, civil/military coordination, ground communications, Letters of Agreement/Procedures LoAs/LoPs, and the awareness campaign to operators with regards to RVSM operator/aircraft approval and RVSM flight planning. Details are provided in section 2 of **[61]**.

Implementation phase: ToS

The implementation phase starts in intermediate period prior to ToS and ends when all aircraft are reported at their new RVSM flight levels. During this phase, the whole airspace will be in transition for controllers and flight crews.

The actual ToS will be published in aeronautical documentation for 25 September 2008.

In the immediate period prior to ToS, the prime activity will consist of assigning non RVSM approved civil flights to their new flight levels below FL290 (operations above FL410 will not be permitted) and of broadcasting periodically the pending switch-over.

At ToS, the sequence of events will consist of the reassignment of RVSM-approved and State aircraft to their new RVSM flight levels, the application of appropriate RVSM separation standards, and the on-going verification of operator/aircraft approval status.

Section 3 of **[61]** emphasises special items as flow management, staffing levels, contingency planning and weather phenomena.

Immediate post-implementation phase: ToS to ToS + 24h

FIR's experiencing or envisaging problems are required to report these to ARMA such that remedial action can be taken. The report shall include any large height deviations, wake-vortex encounters and any other reportable events brought about by the implementation of RVSM. During this phase, the nature of RVSM operations will be similar to that of the mature operations considered in sections 4 and 5 except for those specifically related to the switch-over (suspension of flight levels, etc)

Based on the above considerations, **Argument A4.1.1.2 is considered as true**.

6.3.1.2 Mitigation of hazards and risks related to Switch-over

A4.1.1.2:

"Switch-over hazards and risks are mitigated"

The set of System Element Requirements (SERs) resulting from the FHA-based Safety Requirements are presented in **Appendix C**. They are intended to ensure that the mitigations related to the switch-over hazards, as identified in the FHA **[71]**, are provided during switch-over operations. The set of SERs is composed of SERs allocated to particular System elements and of SERs allocated to the overall AFI RVSM System.

SERs allocated to particular System Elements

The global approach for realising the first sub-set of requirements is based on the development of the AFI RVSM switch-over plan **[61]** to be disseminated to States (for ATS procedures, training and equipment), and to Operators (for Flight Crew and operator procedures and training) through State Integrated Aeronautical Information Package (IAIP) channels. The global approach is completed by the development of pilot and controller bulletins in order to keep the AFI RVSM switch-over plan as simple as possible.

With regard to the flight crew and operator allocated SERs (**S_FCOP** and **S_FCOT)**, the completion consists of the development of a flight crew switch-over bulletin to be disseminated by IFALPA and the development of guidance material by ARPO on awareness workshops for operators and of the requirement placed on States to organise such workshops. The SERs that are only related to operator (or related ATS elements) are to be addressed within the AFI RVSM switch-over plan, whereas the others (only related to flight crew) are to be addressed in the flight crew information bulletin.

With regard to the ATS related SERs (**S_ATSP**, **S_ATST** and **S_ATSE**), the approach is completed by the development of a controller switch-over bulletin. The SERs that are also related to the flight crew and operators elements or only related to ATS maintenance staff are to be addressed in the AFI RVSM switch-over plan (SERs reflecting switch-over mitigations judged as major by the ARTF are to be addressed within the AFI RVSM switch-over plan and the others are to addressed through a formal requirement on their inclusion in States switch-over plans). The SERs that are only related to the controller and are judged as minor by the ARTF are to be addressed under the controller switch-over bulletin. **Appendix D** provides in the form of tables additional details on the individual approach for each SER as well as the evidence collected to meet this approach.

As it can be seen in **Appendix D**, the tables provide evidence that the switch-over safety requirements allocated to particular system elements have been successfully addressed in the relevant switch-over concept documentation (cf. **[61]** **[62] [63] [64]** and **0**). [open issue 6.4];

SERs allocated to the overall AFI RVSM System

Regarding the SERs allocated to the overall system, the approach of satisfaction is based on the design of the ToS and its inclusion in the AFI RVSM switch-over plan. As shown in reference **[61]**, the date of ToS is 25 September 2008. This has been determined on the basis of a traffic analysis demonstrating the low frequency and stability of operations at that time (as per **S_RVSM1** and **S_RVSM5**). As regards **S_RVSM3**, the analysis has shown that no limitation of traffic density is needed. The Switch-over period will thus be outside of Hadj period (as per **S_RVSM2**). Finally, **S_RVSM6** is to be addressed at State level due to the nature of this requirement. As switch-over mitigation, States are required to review and implement it, as shown in section 4.8 of reference **[61]**.

Based on the above, it can be concluded that the switch-over system element requirements have been properly addressed by the AFI RVSM Programme and consequently that **Argument A4.1.1.2** is true.

6.3.1.3 Residual risks

A4.1.1.3:

“Residual risks related to switch-over, if any, are tolerable”

As a conclusion of the FHA (cf. **[71]** and **Appendix B**), all the switch-over hazards are considered as tolerable provided that the identified mitigations are in place. That means that no risks related to the switch-over are residual.

Thus, **Argument A4.1.1.3 is considered as true**.

6.3.2 Backing evidence

The above direct evidence is considered to be trustworthy on the basis that the following arguments are true:

A4.1.2.1:

"Switch-over planning proven in EUR RVSM implementation"

The switch-over planning has been proven by the successful implementation of EUR RVSM.

Argument A4.1.2.1 is considered as true.

A4.1.2.2:

"AFI RVSM switch-over plan was prepared by competent staff"

The AFI RVSM switch-over plan was prepared by the AFI RVSM Task Force / 9 made up of specialist representatives of States participating in the AFI RVSM programme and international organisations, having the pre-requisite background, experience and expertise. Refer to ARTF/9 reports.

Thus, **Argument A4.1.2.2 is considered as true**.

A4.1. 2.3:

"AFI RVSM switch-over plan will be continuously reviewed and checked"

The continuous review and check of the AFI RVSM switch-over plan, after the Go Decision, is demonstrated as part of:

- The plan own aim, as stated in section 1.3 of reference **[61]**.
- The AFI RVSM strategic action plan **[31]**

Thus, **Argument A4.1.2.3 is considered as true**.

6.3.3 Conclusion

It has been shown in sections 6.3.1 and 6.3.2 that the AFI RVSM switch-over concept is safe and consequently that **Argument A4.1** is true.

6.4 Safety of Switch-over implementation

6.4.1 Direct evidence

AFI has developed a SWOP and disseminated it to all States. The SWOP is continually reviewed for applicability and if amendments are made an updated version is sent to States

6.4.2 Backing evidence

The implementation of RVSM from CVSM has been proved in all other regions that are currently operating RVSM. Similar SWOP have been used in these regions and they proved to be successful.

6.4.3 Conclusion

On the basis of the above considerations, **Argument A4.2 is considered as true.**

6.5 Conclusion regarding switch-over from CVSM to RVSM

It has been showed in this section 6 that the concept and implementation of the switch-over from CVSM to RVSM is safe. Consequently, **Argument A4 is considered as true**

7. Assumptions

7.1 Introduction

This section summarises all the assumptions on which the Pre-Implementation Safety Case depends. It includes the assumptions that have had to be made in the present PISC document, as well as in its principal contributions, i.e. the Functional Hazard Assessment **[71]** and in the Collision Risk Assessment **[68]**.

These assumptions are essential to the completeness and correctness of the present safety case.

7.2 Assumptions made in the PISC

No specific assumptions have been made in this PISC.

7.3 Assumptions made in the FHA

A number of assumptions have been made in the FHA and have served as a basis for the hazard and risk analysis. They are essentials to the completeness of the integrity safety requirements (refer to section 3.3.4).

Some of them are applicable to the overall AFI RVSM System (refer to section 2 of **[71]**), whereas others are specific to mature and switch RVSM operations (refer to section 4.2.1 and 5.2.1 respectively of **[71]**). In addition, some of them were specific to RVSM, whereas others are not.

As the FHA was conducted in 2004/05, the assumptions specific to RVSM have been verified in the mean time (assumptions b – c – g – i – k – 1 – 2 – 3 – 4 – 5) and can be considered today as part of the AFI RVSM system, subject of the present safety case.

The remaining assumptions are thus not specific to RVSM, but remain essential for the completeness and correctness of the safety case, and therefore for the safety of RVSM operations within the AFI Air Navigation System. They are:

- FHA assumption (d): all Letters of Agreements are in place and all coordination procedures with adjacent sectors are in place and commonly used by the air traffic controllers;
- FHA assumption (e): the co-ordination procedures between MIL and CIV units are in place and commonly used by the civil and military air traffic controllers;
- FHA assumption (h): AFI RVSM airspace is covered at least by one air/ground communication means;
- FHA assumption (f): the Radio Communication Failure (RCF) procedures are in place and commonly used by flight crews and air traffic controllers
- FHA assumption (j): ground-ground communications (AFTN and ATS/DS) are available between adjacent ACCs/sectors, as required by the AFI AFTN and ATS/DS rationalised plans

7.4 Assumptions made in the CRA

A number of assumptions have been made which has lead to the development of the two Collision Risk Assessments and it is assumed that they will continue to be contributing assumptions to all future assessments. It is assumed that:

- 50% of the flying time is GNSS navigation flying time
- 50% of the flying time is conventional navigation flying time
- Traffic samples are representative of AFI traffic
- There is an under reporting of operational errors
- The total flying hours for AFI are correct

This section must be read in conjunction with the revised Pre-Implementation Collision Risk Assessment for RVSM in the Africa Indian Ocean Region considered as CRA 2

8. Outstanding safety issues

There are no outstanding safety issues.

9. Conclusions

The AFI RVSM Pre-Implementation Safety Case (PISC) aims to show by means of argument and supporting evidence that AFI RVSM will be safe in operational service, i.e. it aims to provide assurance that the operations of the AFI RVSM System will be safe. In this context what is safe is defined by the Safety Objectives from the AFI RVSM Safety Policy **[2]**.

On the basis on the information developed in the present document, the following is concluded:

GENERAL CONCLUSION:

It has been shown, in compliance with the AFI RVSM Safety Objectives, that

"AFI RVSM will be safe in operational service",

Provided that:

a) The commitments contained within the National Safety Plans are completely, correctly and successfully implemented by the Participating States, which have the ultimate responsibility of RVSM implementation in the airspace for which they have jurisdiction.

CAVEATS

a) The safety case applies to the AFI RVSM System and does not cover the AFI States not participating to the AFI RVSM Programme, in particular the AFI neighbouring States with which implementation shall be coordinated

b) The safety case applies to the operational concept described in Appendix A

c) Some important assumptions, not directly related to RVSM, have had to be made (section 7)

Annex 1: References

Applicable documents

[1] Manual on Implementation of a 300 m (1000 ft) Vertical separation Minimum Between FL290 and FL410 inclusive, Doc 9574 AN/934, Second edition - 2002, International Civil Aviation Organisation.
[2] AFI Reduced Vertical Separation Minimum (RVSM) RVSM Safety Policy, ARPO/ICAO, 30 July 2004

Reference documents

ICAO documents:

[3] ICAO Annex 2, Rules of the Air, Ninth edition – July 1990, including all amendments and corrigenda up to applicability date
[4] ICAO Annex 11, Air Traffic Services, Thirteenth Edition, July 2001
[5] ICAO Doc 9426, Air Traffic Services Planning Manual, 1984;
[6] ICAO Doc 4444, Procedures for Air Navigation Services
[7] ICAO Doc 9536, Review of the General Concept of Separation Panel, 6th Meeting, report, RGCSP/6 Volumes 1 et 2, 1988;
[8] ICAO Doc 9572, Review of the General Concept of Separation Panel, 7th Meeting, report, RGCSP/7, 1990;
[9] ICAO Doc 9689-AN/953, Manual on airspace planning methodology for the determination of separation minima, First edition, 1998.
[10] ICAO Safety net policy
[11] TCAS logic V6.04a and 2000ft
[12] ICAO on TCAS RA follow up

AFI RVSM Programme:

[13] Report of the 15th meeting of the AFI Planning and Implementation Regional Group (APIRG), Nairobi, Kenya, 26-30 September 2005
[14] Report of the 14th meeting of the AFI Planning and Implementation Regional Group (APIRG), Yaoundé, Cameroon, 23-27 June 2003
[15] Report of the 13th meeting of the AFI Planning and Implementation Regional Group (APIRG), Sal, Capo Verde, June 2001
[16] AFI RVSM Task Force 1 report, Dakar, Senegal, 17-18 June 2002
[17] AFI RVSM Task Force 2 report, Dakar, Senegal, 19-21 November 2003
[18] AFI RVSM Task Force 3 report, Nairobi, Kenya, 22-23 April 2004
[19] AFI RVSM Task Force 4 report, Lagos, Nigeria, 29-30 July 2004
[20] AFI RVSM Task Force 5 report, Dakar, Senegal, 16-17 November 2004
[21] AFI RVSM Go/Delay Coordination meeting, Dakar, Senegal, 18-19 November 2004
[22] AFI RVSM Task Force 6 report, Nairobi, Kenya, 25-27 May 2005
[23] AFI RVSM Task Force 7 report, Dakar, Senegal, 8-9 August 2005
[24] AFI RVSM Task Force 8 report, Lagos, Nigeria, 11-13 October 2005
[25] AFI RVSM Task Force 9 report, Nairobi, Kenya, 19-20 April 2006
[26] AFI RVSM Task Force 10 report, Dakar, Senegal, 27-28 June 2006
[27] AFI RVSM Go/Delay Coordination meeting report, Dakar, Senegal, 29-30 June 2005
[28] AFI RVSM Task Force 11 report, Nairobi, Kenya, 13 November 2006
[29] AFI RVSM Task Force 12 report, Dakar, Senegal, 23 - 24 April 2007
[30] AFI RVSM Task Force 13 report, Nairobi, Kenya, 13 September 2007

[31] Strategic/Action for Implementation of Reduced Vertical Separation Minima in the AFI Region, ICAO/ARPO
[32] RVSM seminar summary, Lagos, Nigeria, 26-28 July 2004, ICAO/ARPO
[33] RVSM seminar summary, Nairobi, Kenya, 19-21 April 2004, ICAO/ARPO
[34] RVSM seminar summary, Nairobi, Kenya, 13 November 2006, ICAO/ARPO
[35] AFI RVSM National Safety Plan (NSP) workshop summary, Nairobi, Kenya, 18-22 July 2005, ICAO ESAF Office
[36] AFI RVSM National Safety Plan (NSP) workshop summary, Dakar, Senegal, 25-29 July 2005, ICAO WACAF Office
[37] AFI RVSM National Safety Plans Validation Panel (NSPVP) report I, Johannesburg, South Africa, 12-23 September 2005, ICAO Montreal ATM Bureau
[38] AFI RVSM National Safety Plans Validation Panel (NSPVP) report II, Johannesburg, South Africa, 21-24 March 2005, ICAO Montreal ATM Bureau
[39] Handbook for AFI RMA supporting implementation and continued safe use of RVSM, February 2006;
[40] JAA Temporary Guidance Leaflet No.6 (TGL 6) Guidance Material on the approval of aircraft and operators for flight in airspace above F290 where a 300m (1,000ft) vertical separation minima is applied, revision 1, October 99
[41] Guidance material on the Approval of Operators/Aircraft for RVSM Operations, Federal Aviation Administration, FAA 91-RVSM, 2/10/04.
[42] AFI RVSM Safety Monitoring policy
[43] Air Traffic Control Operations Manual for Implementation of RVSM in the AFI Region, ICAO/ARPO, April 2006
[44] Proposal for amendment to the Regional Supplementary Procedures – Doc.7030/4 – Africa Indian Ocean (AFI) Region, ICAO/ESAF, ESAF-S 06/2 – AFI/RAC/1 – April 2006
[45] AFI RVSM Letter of Agreement/Procedure Template –, ICAO/ARPO
[46] Specimen of National Plan for Implementation of RVSM, ICAO/ARPO
[47] Template of National Safety Plan for Implementation of RVSM, July 2005, ICAO/ARPO
[48] AFI ATS RVSM Training Guidance Material, ICAO/ARPO
[49] Specimen AIC on RVSM
[50] Specimen NOTAM on RVSM;
[51] Review of FLAS/FLOS for AFI RVSM, ARTF/
[52] Review of route structure for AFI RVSM, ARTF/11
[53] Review of sectorisation for AFI RVSM, ARTF
[54] Review of contingency facilities for AFI RVSM, ARTF
[55] Mountain waves activity, WP/2, ARTF/11
[56] ICAO State Letter ES AN 4/44 – 0607, 10 August 2004.
[57] ICAO State Letter ES AN 4/44 – 0764, 29 September 2004.
[58] ICAO State Letter ES AN 4/44 – 0030, 13 January 2005.
[59] ICAO State Letter ES AN 4/44 – 0406, 14 June 2005.
[60] AFI RVSM safety and Consolidated Readiness assessment, ICAO, APIRG 15, WP 17, Nairobi Kenya, 26 – 30 September 2005
[61] AFI RVSM Switch-Over Plan, ICAO/ARPO, edition 0.03, April 2006
[62] Amendment to the AFI RVSM Switch-Over Plan, ICAO/ARPO, Task Force 13
[63] AFI RVSM Flight Crew Switch-over bulletin.
[64] AFI RVSM Controllers Switch-over bulletin.
[65] ICAO Guidance Material on the organisation of RVSM workshops for operators.

AFI RVSM PISC Project:

[65] Pre-Implementation Safety Case for the AFI RVSM programme contract, AT/SDI/PC05-022C/05-009
[66] AFI RVSM Pre-Implementation Safety Case Project Management Plan, ALTRAN Technologies CNS/ATM Division, Ref AT/SDI/DT05-045B/05-009, edition 1.0, 18/01/06
[67] AFI RVSM PISC System Elements Requirements specification and approach of satisfaction, ALTRAN Technologies CNS/ATM Division in conjunction with National Aerospace Laboratory (NLR), Ref AT/SDI/DT06-001A/05-009, edition 1.0, 23/01/06

AFI RVSM CRA Project:

[68] Pre-Implementation Collision Risk Assessment for RVSM in the Africa Indian Ocean Region, National Aerospace Laboratory (NLR) NLR-CR-2005-443, July 2005
[69] Pre-Implementation Collision Risk Assessment for RVSM in the Africa Indian Ocean Region, ICAO, APIRG/15, WP16, Nairobi, Kenya, 26-30 September 2005
[70] Update of the Pre-Implementation Collision Risk Assessment for RVSM in the Africa Indian Ocean, National Aerospace Laboratory (NLR), NLR-CR-2006

AFI RVSM FHA Project:

[71] AFI RVSM Functional Hazard Assessment, 25 May 2005, ALTRAN Technologies, AT/SDI/05-024.A/05-003, edition 0.1, 22/05/05
[72] Report on the initial AFI RVSM FHA Brainstorming Session – Edition 0.1 – 14 December 2004, ALTRAN Technologies – CNS/ATM Division
[73] Report on the second AFI RVSM FHA Brainstorming Session – Edition 0.1 – 14 February 2005, ALTRAN Technologies – CNS/ATM Division
[74] Report on the third brainstorming session AFI RVSM FHA Brainstorming Session – Edition 0.1 – 12 April 2005, ALTRAN Technologies – CNS/ATM Division
[75] Guidelines for Initial Brainstorming Session – AFI RVSM Functional Hazard Analysis (FHA), Edition 0.1 – 27 October 2005, ALTRAN Technologies – CNS/ATM Division
[76] Guidelines for the second Brainstorming Session – AFI RVSM Functional Hazard Analysis (FHA), Edition 0.1 – 26 January 2005, ALTRAN Technologies – CNS/ATM Division
[77] Guidelines for the third Brainstorming Session – AFI RVSM Functional Hazard Analysis (FHA), Edition 0.1 – 28 March 2005, ALTRAN Technologies – CNS/ATM Division

EUR RVSM:

[78] Reduced Vertical Separation Minimum (RVSM) Safety Policy, Edition 1.0, 18 September 2000, EUROCONTROL
[79] The EUR RVSM Mathematical Supplement, RVSM 830, Version 1.0, EUROCONTROL, Brussels, August 2001, Proposed issue
[80] EUROCONTROL. RVSM 691. The EUR RVSM Pre-Implementation Safety Case. Version 2.0 14 August 2001;
[81] EUROCONTROL. RVSM A1190. The EUR RVSM Post-Implementation Safety Case. Version 1.0, 27 January 2003;
[82] The EUR RVSM Safety Monitoring Report 2004, EUROCONTROL, Edition 0.2, 2004
[83] EUROCONTROL, ATC Manual for RVSM Implementation in Europe, version 2.0, 1st February 2001;
[84] EUR RVSM Functional Hazard Assessment, Version 1.0, 12 February 2001, RVSM 697, EUROCONTROL;
[85] En-route encounters with wake vortices and the implications of Reduced Vertical Separation Minimum (RVSM), Woodsfield Aviation Report N° 9901, March 1999
[86] ESARR 4, Risk Assessment and Mitigation Methodology in ATM, version 1.0, 5 April 2001.

[87] EUROCONTROL EATMP Air Navigation System Safety Assessment Methodology, version 2.0, 20 April 2004
[88] EUROCONTROL Safety Case Development Manual, edition 2.0, 28 September 2005

NAT RVSM:
[89] ICAO NAT Doc.002 – Guidance Material on Implementation of a 300M (1000 FT) Vertical Separation Minimum in the Minimum Navigation Performance Specification Airspace of the NAT Region
[90] Risk assessment and system monitoring for the verification and operation of a 300 m (1000 ft) vertical separation minimum in the Minimum Navigation Performance Specification airspace of the North Atlantic Region, Supplement to NAT Doc 002, Draft Version 2.0, March 1996.
[91] Summary of ASE results, North Atlantic Systems Planning Group (NAT SPG), 36th meeting, Mathematicians Working Group (MWG), NAT SPG/36 MWG IP/5, ICAO Paris, May 2000

PAC RVSM:
[92] RVSM Safety assessment - Final Report, RVSM safety assessment for the Australian FIRs, Air services Australia, September 1999.
[93] Guidance Material on the Implementation of a 1 000 ft Vertical Separation Minimum for application in the airspace of the Pacific Region;
[94] Preliminary analysis for Pre-Implementation Safety Assessment for Japanese Domestic RVSM, ICAO SASP/WG/WHL-WP/14, Montreal, May 2005.

SAT RVSM:
[95] Risk assessment of RNP10 and RVSM in the South Atlantic Flight Identification Regions Including an Assessment for Limited Application of RVSM on RN741, ARINC, 21054, Rev. A, August 2001, NLR-CR-2002-015, January 2002.

CAR/SAM:
[96] CAR/SAM RVSM Concept of Operations – CONOPS – CAR/SAM RVSM TF – August 2003
[97] Safety Bulletin on CAR/SAM implementation – IFALPA – January 2005
[98] RVSM Post Implementation Safety Assessment in CAR/SAM regions, SAT/12-TF/1-WP/07, Rio de Janeiro, Brazil, September 2006.

Others:
[99] Link2000+ Programme Pre-Implementation Safety Case, EUROCONTROL, edition 1.0, 10 June 2004
[100] International Safety Management Standard IEC 61508, First Edition 1998-12, Part 1, General requirements, IEC 61508-1:1998(E)
[101] CAP670, ATS Safety Requirements, First Issue, UK Civil Aviation Authority, April 1998

Annex 2: Abbreviations and definitions

Abbreviations

As per ICAO documentation

Definitions / Explanation of terms

The following definitions are taken from:

- ESARR4 [86]
- EUROCONTROL Safety Case Development Manual [88]

A		
Air Navigation System		
Argument	A statement asserting a fact that can be shown to be true or false.	[88]
Assessment	An evaluation based on engineering, operational judgment and/or analysis methods	[86]
Assumption	Statement, principle and/or premises offered without proof	[86]
ATM	The aggregation of ground based (comprising variously ATS, ASM and ATFM) and airborne functions required to ensure the safe and efficient movement of aircraft during all appropriate phases of operations.	[86]
ATM Service	A service for the purpose of ATM	[86]
ATM Service Provider	An organisation responsible and authorised to provide ATM service(s)	[86]
ATM System	ATM System is a part of ANS system composed of a Ground Based ATM component and of an airborne ATM component. The ATM System includes the three constituent elements: human, procedures and equipment (hardware and software). The ATM System assumes the existence of a supporting CNS system.	[86]
B		
Backing <entity>	Arguments, strategies or evidence that help to support and validate Direct evidence of the satisfaction of a goal/argument/claim. For example, competence, methodology, following a process, etc.	[88]
C		
CNS System	All the hardware and software that make up a function, tool or application that is used to one or more ATM services. The CNS System is an enabler to the provision of ATM services.	[86]
D		
Direct <entity>	Arguments, strategies or evidence that directly support the satisfaction of a goal/argument/claim. For example, test results, FHA results, etc.	[88]
G		
Good Practice	A practise that is sufficiently recognised by various people/organisations to allow it to be used as an informal standard.	[88]

	The concept of Good Practice is derived from our responsibilities as professional operators, engineers and managers. We set ourselves a duty of care for all the people who use, operate, maintain and come into contact with the Air Traffic Service domain. Our objective is to ensure that we only make claims relating to safety that are supportable by the use of within current good practice.	
H		
Hazard	Any condition, event, circumstance or circumstance which could induce an accident.	[86]
I		
Integrity	The assurance that all functions of a system perform within operational performance limits.	[88]
M		
Mitigation	Steps taken to control or prevent a hazard from causing harm and reduce risk to a tolerable or acceptable level.	[86]
R		
Reliability	The probability of performing a specified function without a failure under given conditions for a specific period of time.	[88]
Risk	The combination of the overall probability, or frequency of occurrence of a harmful effect induced by a hazard and the severity of that effect.	[86]
Risk assessment	Assessment to establish the achieved or perceived risk is acceptable or tolerable.	[86]
S		
Safety	Freedom from unacceptable risk of harm.	[86]
Safety Argument	A statement (or a set of statements) that is used tu assert that the service or system concerned is safe.	[88]
Safety Assurance	All planned and systematic actions necessary to provide adequate confidence that a product, a service, an organisation or a system achieves acceptable or tolerable safety.	[86]
Safety Case	The documented assurance (i.e. argument and supporting evidence) of the achievement and maintenance of safety. In the context of ATM, the safety case documents the demonstration of safety of ATM applications, including ongoing service provision and changes to service provision (including new ATM systems or components and modifications to current systems)	[88]
Safety Criterion	A specification of what is acceptable and/or tolerable in terms of risk	[88]
Safety Evidence	Information, based on established fact or expert judgment, which is presented to show that the Safety Argument to which it relates is valid (true).	[88]

Safety Monitoring	A systematic action conducted to detect changes to the ATM System with the specific objective of identifying that acceptable or tolerable safety can be met.	[86]
Safety objective	A safety objective is a planned safety goal, a qualitative or quantitative statement that defines the maximum frequency or probability at which a hazard can be expected to occur.	[86]
Safety requirement	Means by which a risk mitigation measure, defined from a risk mitigation strategy, necessary to achieve a particular safety objective, is formally specified. Safety requirements may take various forms, including organisational, operational, procedural, functional, performance, and interoperability requirements or environment characteristics.	[86]
Severity	Level of effect/consequences of hazards on the safety of flight operations (i.e. combining level of loss of separation and degree of ability to recover from the hazardous situation).	[86]
Severity Class	Gradation from, ranging from 1 (most severe) to 5 (least severe), as an expression of the magnitude of the effects of hazards on flight operations.	[86]
System	A set of interconnected, independent parts, forming an identifiable, organised complex and dynamic whole. In the context of ATM, it includes airspace, equipment, people and procedures	[88]
T		
Target Level of Safety	A level of how far safety is to be achieved in a given context, assessed with reference to an acceptable or tolerable risk	[88]
V		
Validation		
Verification		

Annex 3: Goal Structuring Notation

Introduction

The Goal Structuring Notation (GSN) is a good practice, recognised by EUROCONTROL **[88]** that is commonly used for developing and presenting the Safety Argument, forming the framework of a Safety Case, in a rigorous, hierarchical and easily-understood manner.

GSN provides graphical means of:

- setting out hierarchical safety arguments, with textural annotations and references to supporting evidence; and of,
- capturing essential explanatory and contextual information including assumptions, context and justification, within the argument framework

GSN provides thus a logical approach to capture the process used for the safety arguments derivation (explanatory and contextual information) and the solutions produced as a result of carrying out that process (arguments and evidence).

This section presents the essentials of the GSN solution, that are more commonly used on ATM Safety Cases.

More details can be found in the *EUROCONTROL Safety Case Development Manual* **[88]** and examples of application by EUROCONTROL can be found in **[80] [99]**.

The direct application of GSN for the purpose of the AFI RVSM PISC is detailed in section 2.3.2.

Overview of GSN

Symbology

The symbology can be illustrated using the following specimen of Argument and Evidence structure:

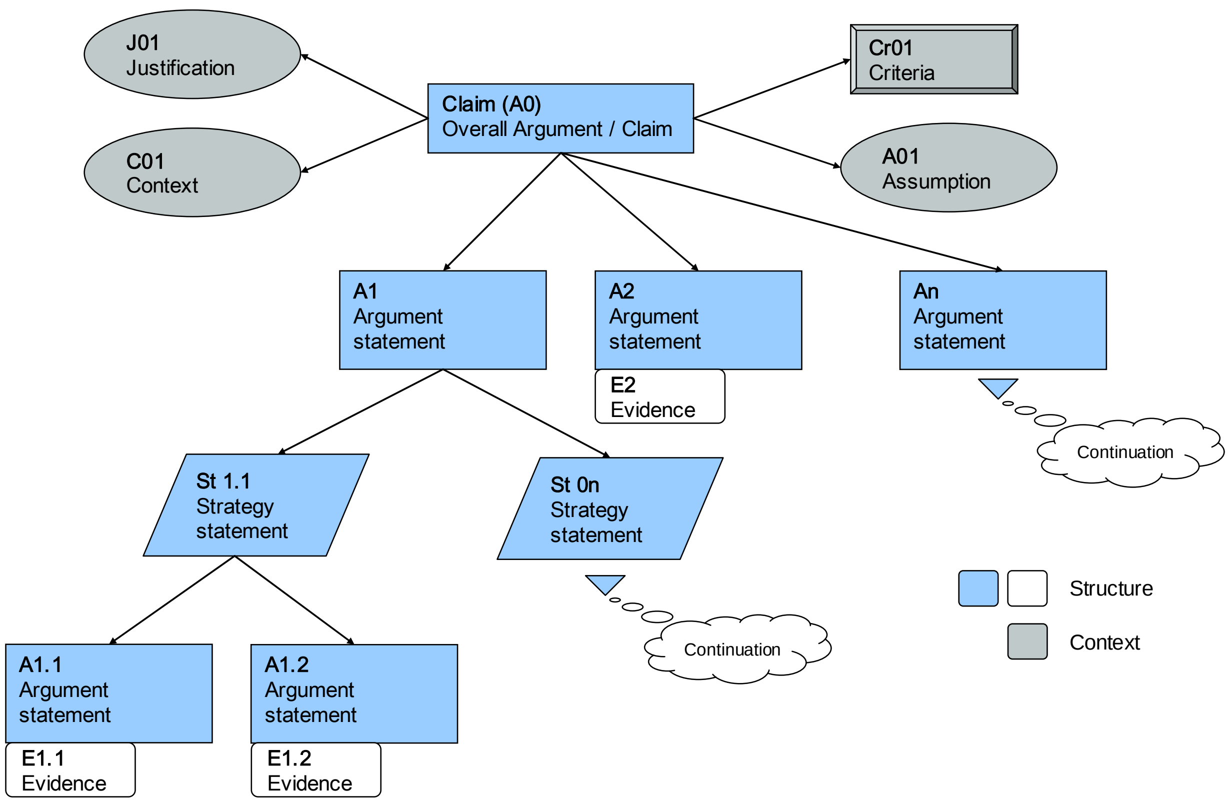

Figure 25 : GSN Symbology

The GSN elements can be grouped in two classes:

- Elements from the structural construction: mainly *Arguments*, *Strategies*, and *Evidence*;
- Elements used as contextual information: mainly *Context*, *Criteria*, *Assumptions* and *Justification*.

Structural elements

Structural elements are used to form the Argument and Evidence structure resulting from logical decomposition of the safety arguments into lower-level arguments.

They are mainly:

- **Argument (A):** Statement claiming about the safety properties of the considered system, or some target to be met. An argument should be formulated as a predicate, i.e a simple predicate which can be shown to be only TRUE or FALSE.
- **Strategy (St):** Element of explanation introduced into the argument structure. It helps to show how the safety arguments are constructed and broken down into sub-arguments. A strategy is not a predicate; rather it is there purely for explanation of the argument decomposition;
- **Evidence (E):** Evidence of direct satisfaction of an argument. Evidence always appear at the bottom level of the GSN decomposition and are attached to the argument they support.

Contextual elements

Contextual information elements are connected to the structure of the GSN decomposition, providing additional understanding and clarity. They do not form part of, however are attached to, the logical argument and evidence structure.

They capture important items such as:

- **Assumption (A):** Statement, principle and/or premises offered without proof, whose validity has to be relied upon;
- **Criteria (Cr):** Means by which the satisfaction of an Argument can be checked;
- **Justification (J):** Rationale given for the use or satisfaction of a particular Argument or Strategy. It is generally used to justify the change that is the subject of the Safety Case; and,
- **Context (C):** Information necessary for an Argument to be understood and amplified.

GSN principles

In the GSN approach for, a safety argument structure is built starting from the **top-level claim (or argument)** of the safety case, i.e. what the safety case is trying to show. This should be directly related to the claim that the subject of the safety case is safe.

Further more arguments and evidence are attached to this top-level claim. Indeed, demonstration that this **top-level argument** has been met is achieved by further decomposition into **sub-arguments**. Logically, an argument is true (has been satisfied) if, and only if (necessary and sufficient condition), its all sub-arguments are true.

For a safety argument structure to be sufficient, it is essential to ensure that, at each level of the decomposition:

- The set of arguments covers everything that is needed in order to show that the parent argument is true; and,
- There is no valid (counter) arguments that could undermine the parent argument.

Following these principles, it is necessary to show only that each argument at the very bottom of the structure is satisfied, in order to assert that the top-level claim has been satisfied.

Satisfaction of the lowest-level arguments is the purpose of **Evidence**. To this end, an argument is decomposed to a level at which clear **Evidence** of the validity of the sub-arguments can be identified.

For a safety argument structure to be considered complete, every branch must be terminated in an item of **Evidence** that supports the argument to which it is attached.

For the structure to be sufficient, it is essential to ensure that, at every branch of structure:

- Evidence is appropriate to, and necessary to support, the related argument; and,
- Evidence is sufficient to support the related argument

Having established that, the adequacy of the safety case is dependent only on the quality of the Evidences supporting the Arguments.

Strategies are mainly used to highlight a clear distinction between, and correct use of:

- **Direct (product-based) arguments** and related **evidence**; and,
- **Backing**, or **supporting (process-based) arguments** and related **evidence**.

Direct argument and evidence are used to show that a particular objective has been achieved (i.e. that the higher level argument has been shown to be true). **Direct** evidence is obtained from the observable properties of a **product** (i.e. the output of a process), supporting a logical argument as to how the product satisfies its safety objectives and requirements, as appropriate.

Backing argument and evidence are used to show that the **Direct** evidence is trustworthy (i.e. that it can be relied upon). **Backing** evidence is obtained from the properties of the **processes** by which the direct evidence was obtained. It aims to show that those processes (tools, techniques, human resources etc) were appropriate, adequate and properly deployed.

Traceability and numbering

For the purpose of the AFI RVSM PISC:

- **Arguments (A)** are numbered hierarchically (e.g. A1, A1.1 etc…) to reflect their logical structure,
- **Evidence (E)** are numbered according to the higher-level argument they support / are attached to (e.g. E1.1 supports Arg1.1). They are referenced by the appropriate section of the document (e.g. PISC 1.1.1) in which they can be found in the form of a text or a reference to a relevant appendix or an external document.
- **Strategies (St)**, **Assumptions (A)**, **Criteria (Cr)** etc… are numbered sequentially (e.g. St1.1, St 1.2) on the basis of the argument they are connected to.

Annex 4: Argument and evidence structure

This annex provides the whole breakdown of the PISC argument and evidence structure.

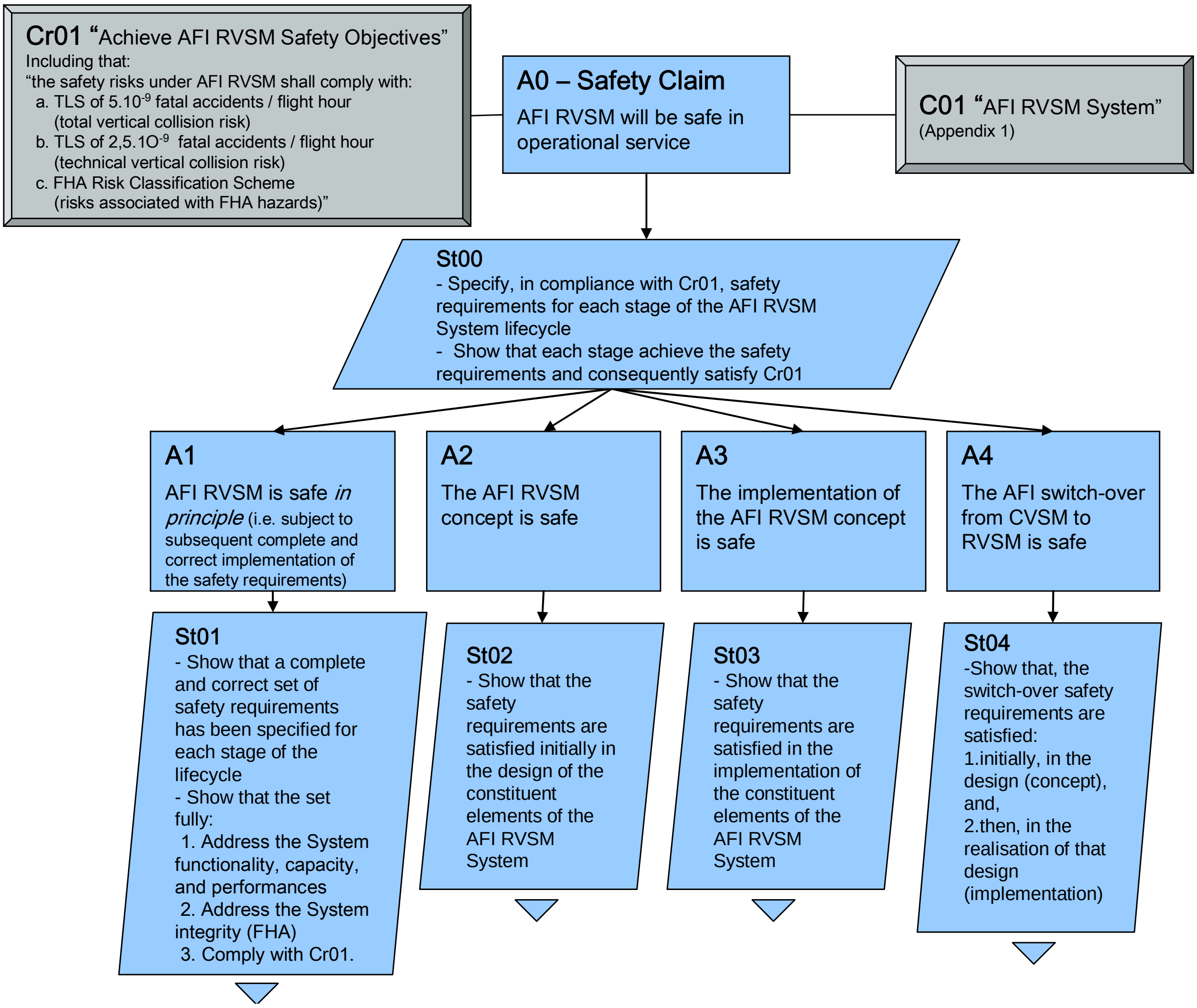

Figure **26** : PISC overall Safety Argument

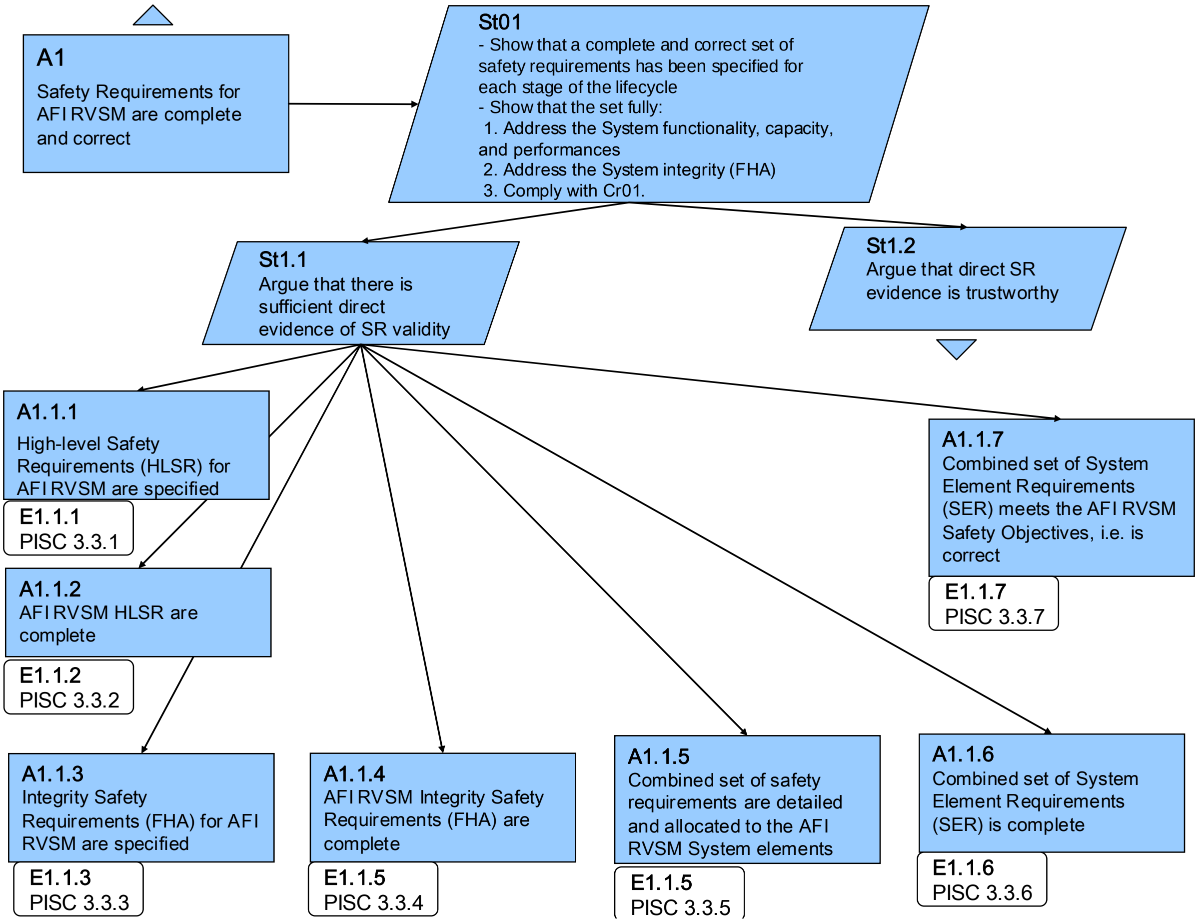

Figure 27 : Argument 1 – Argument and direct evidence structure

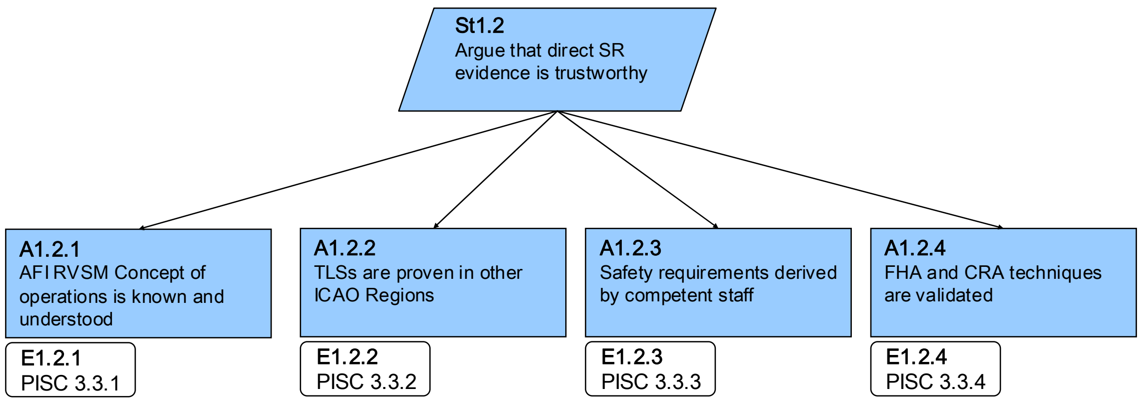

Figure 28 : Argument 1 –Argument and backing evidence structure

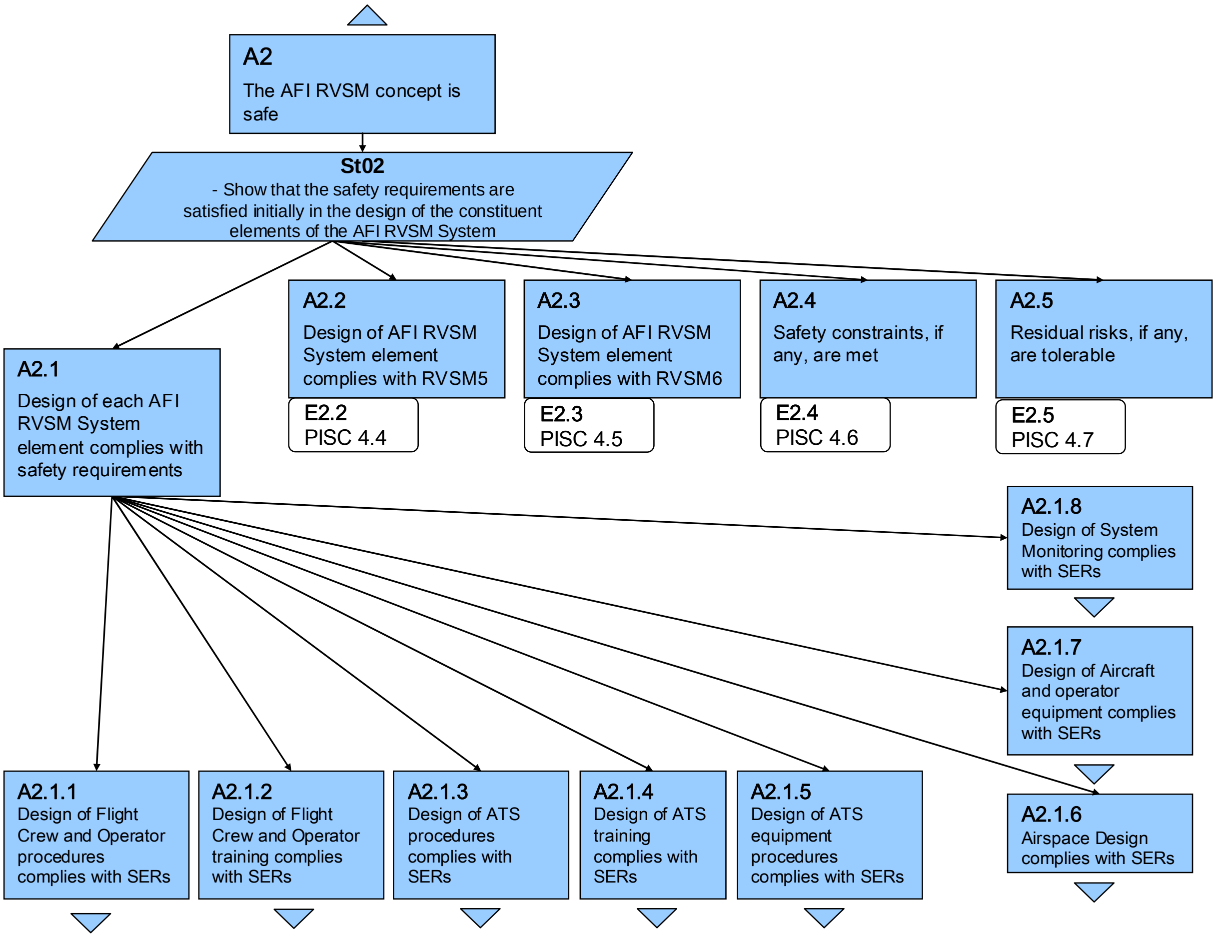

Figure 29 : Argument 2 – Argument and evidence structure

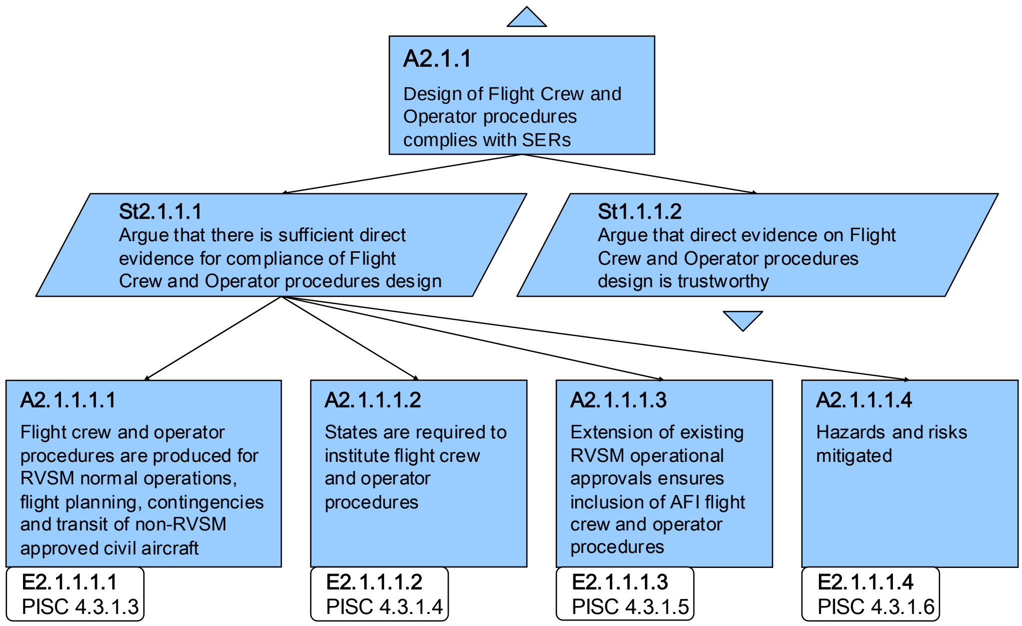

Figure 30 : Argument 2.1.1 – Direct argument and evidence structure

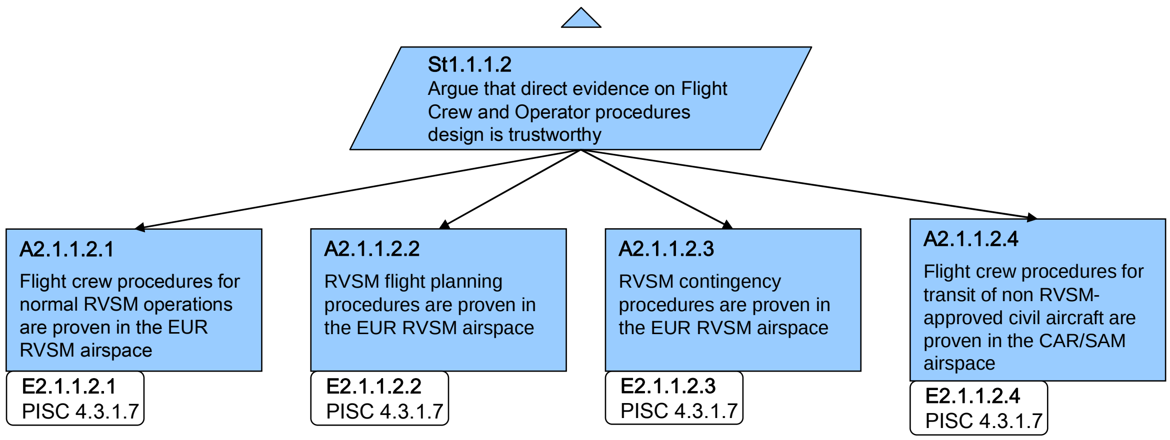

Figure 31 : Argument 2.1.1 – Backing argument and evidence structure

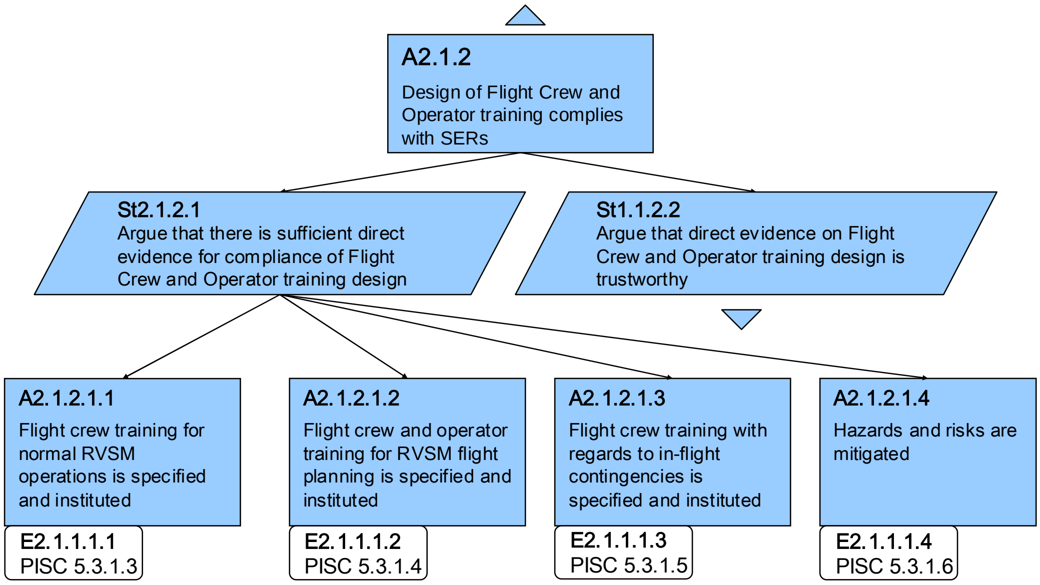

Figure 32 : Argument 2.1.2 – Direct argument and evidence structure

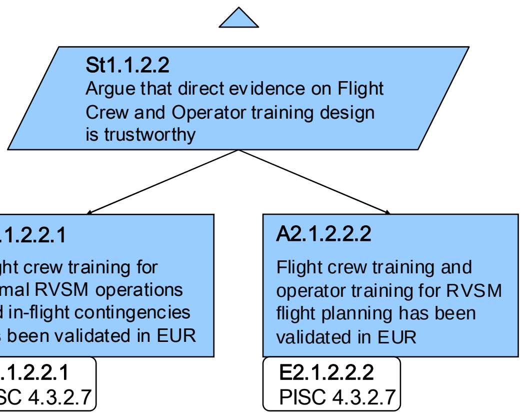

Figure 33 : Argument 2.1.2 – Backing argument and evidence structure

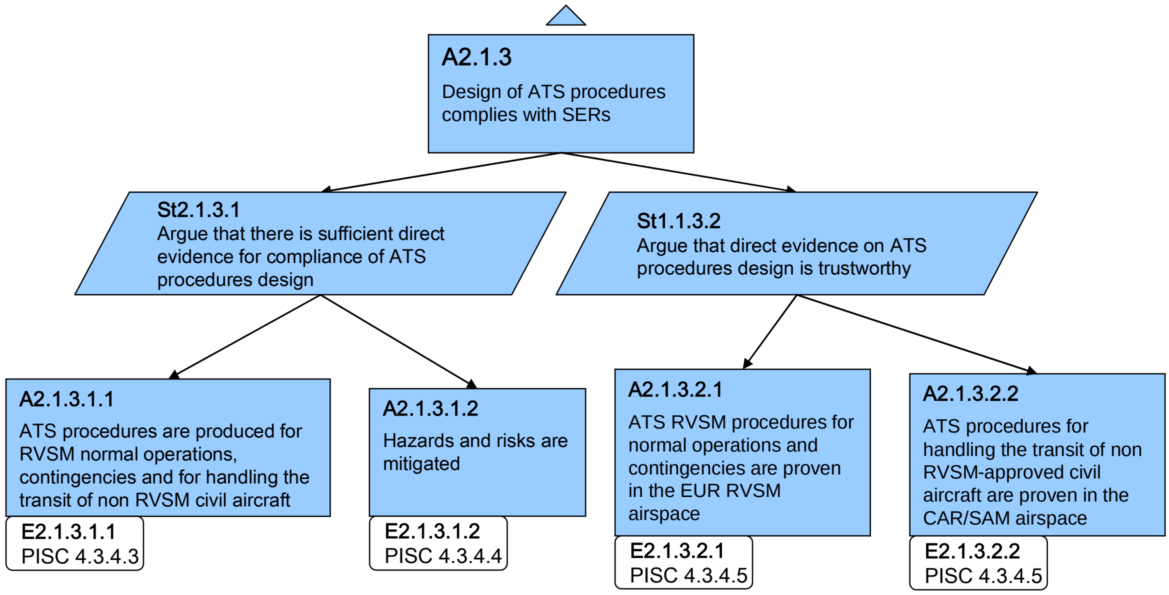

Figure 34 : Argument 2.1.3 – Argument and evidence structure

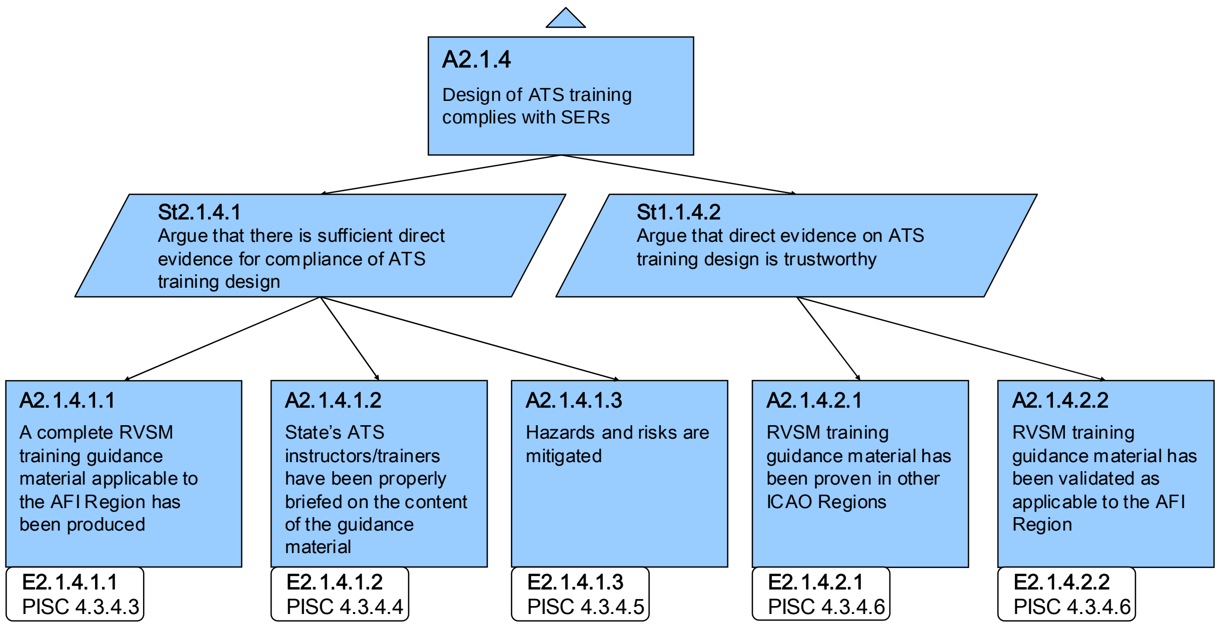

Figure 35 : Argument 2.1.4 – Argument and evidence structure

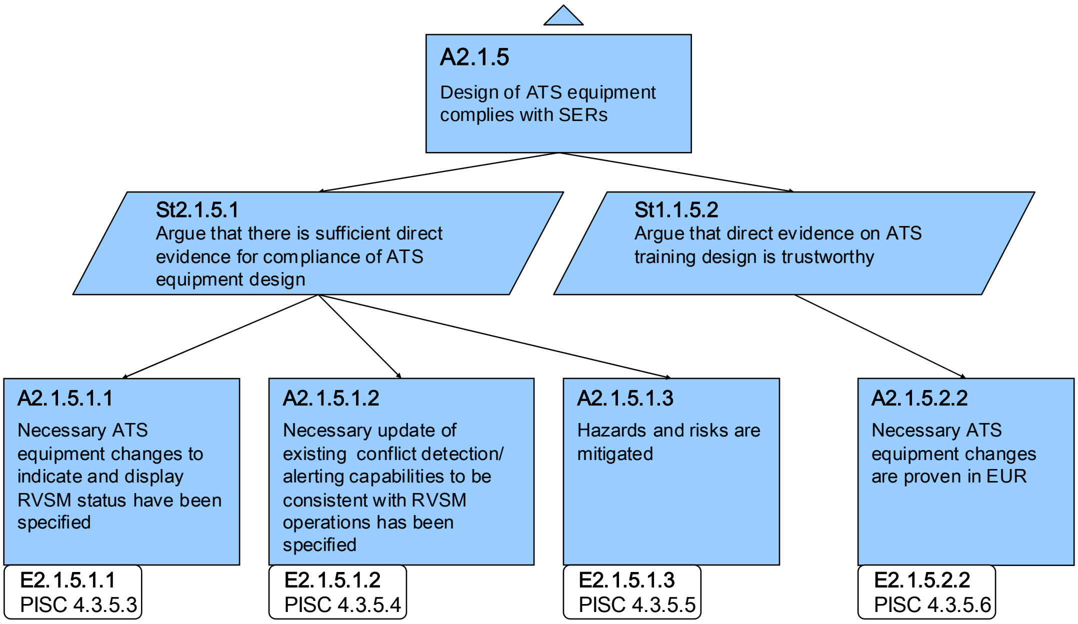

Figure 36 : Argument 2.1.5 – Argument and evidence structure

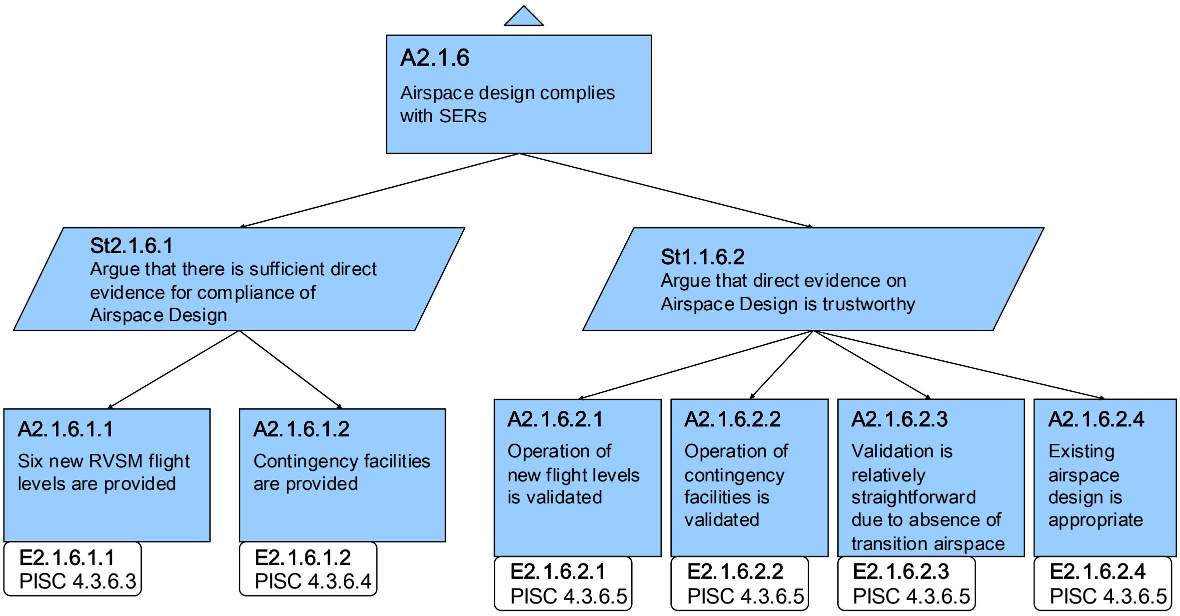

Figure 37 : Argument 2.1.6 – Argument and evidence structure

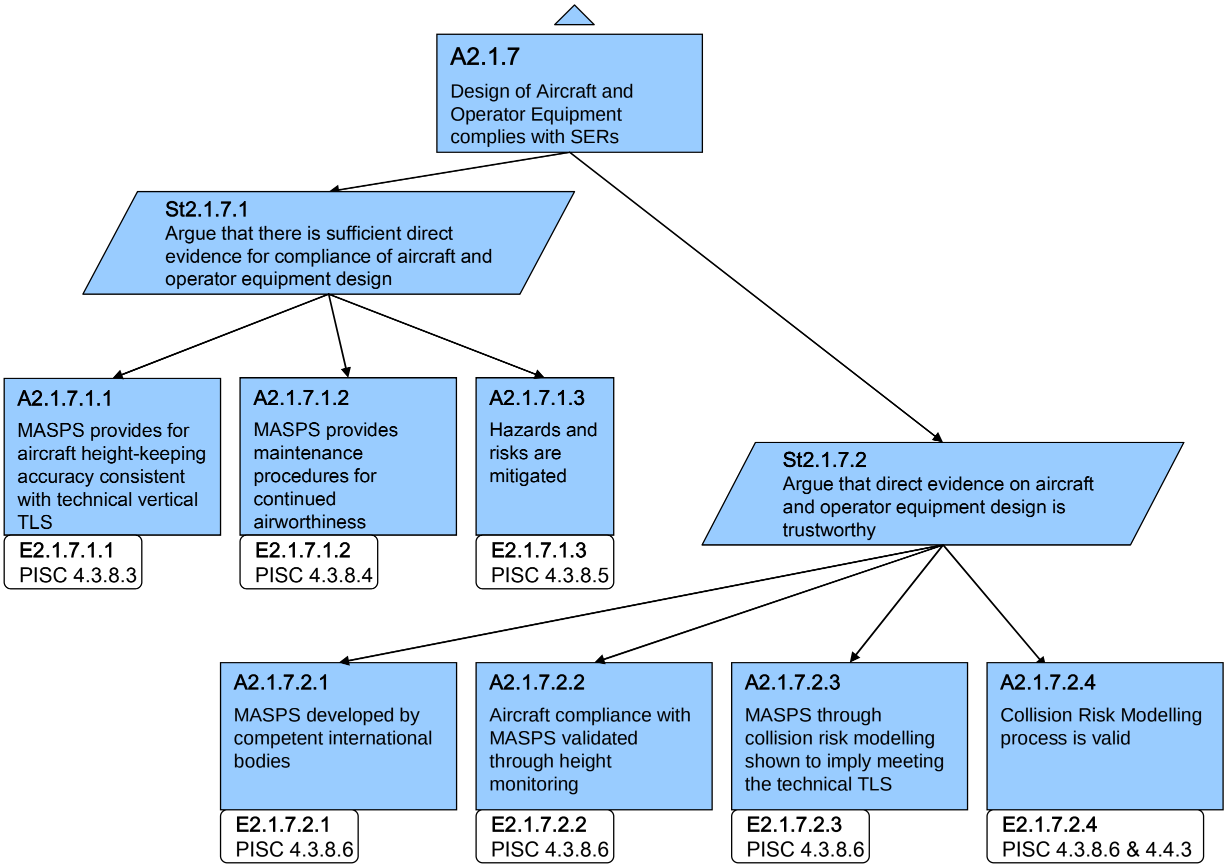

Figure 38 : Argument 2.1.7 – Argument and evidence structure

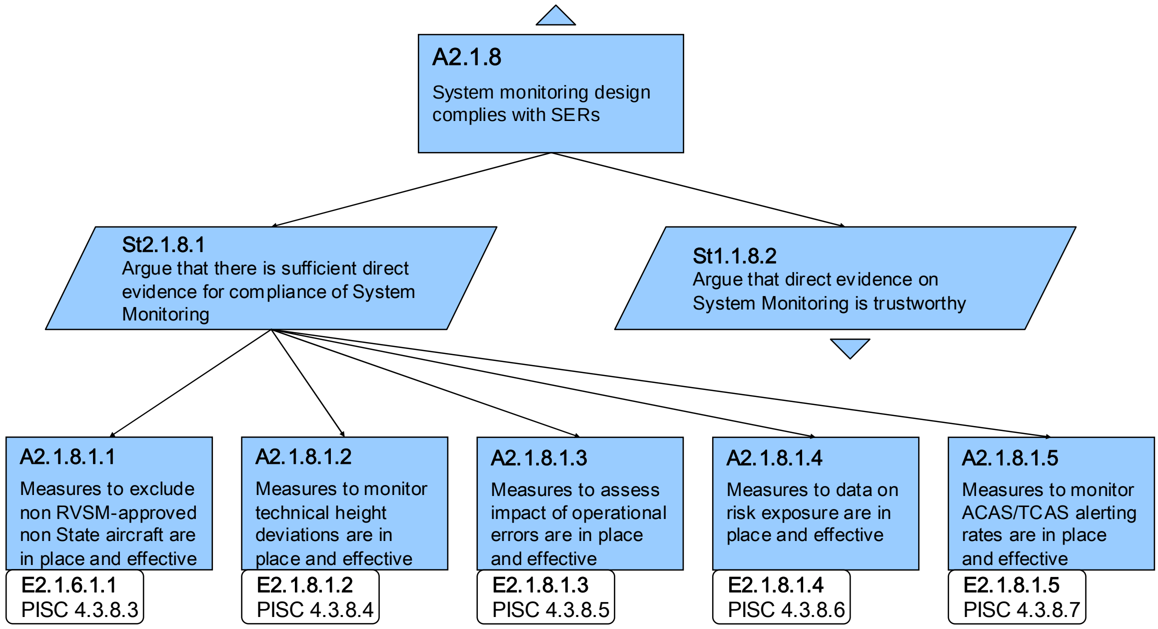

Figure 39 : Argument 2.1.8 – Direct argument and evidence structure

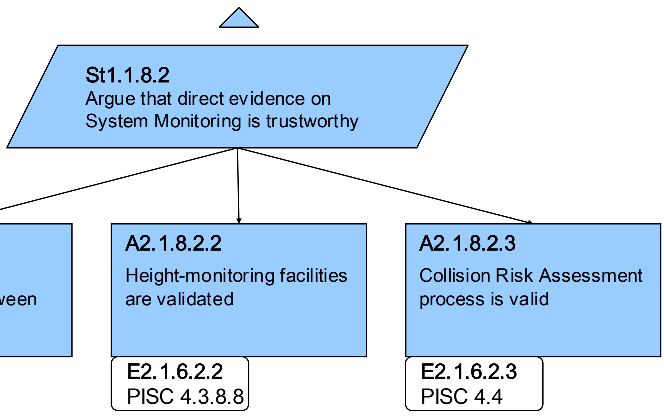

Figure 40 : Argument 2.1.8 – Backing argument and evidence structure

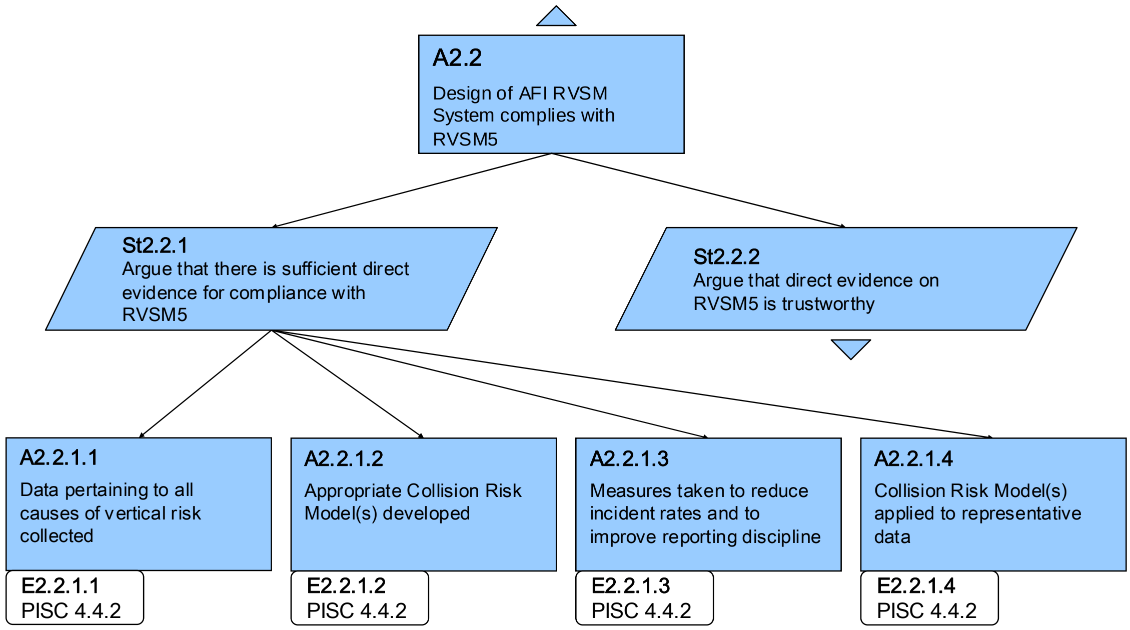

Figure 41 : Argument 2.2 – Direct argument and evidence structure

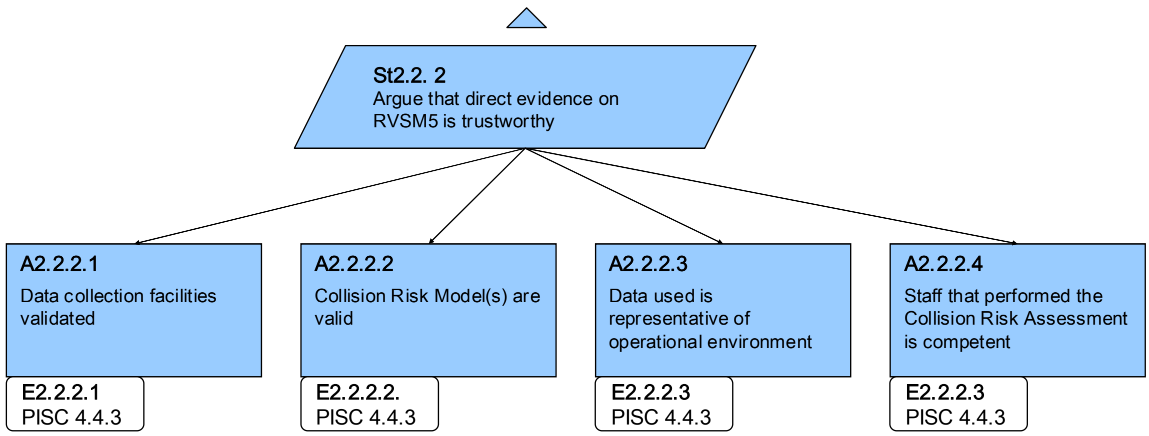

Figure 42 : Argument 2.2 – Backing argument and evidence structure

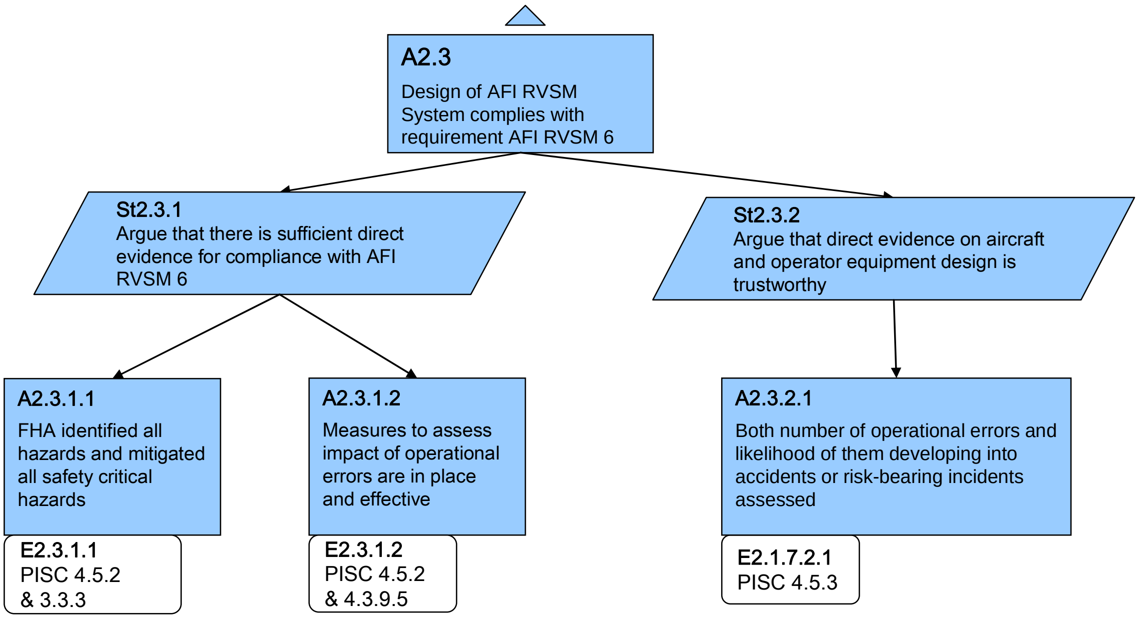

Figure 43 : Argument 2.2 – Backing argument and evidence structure

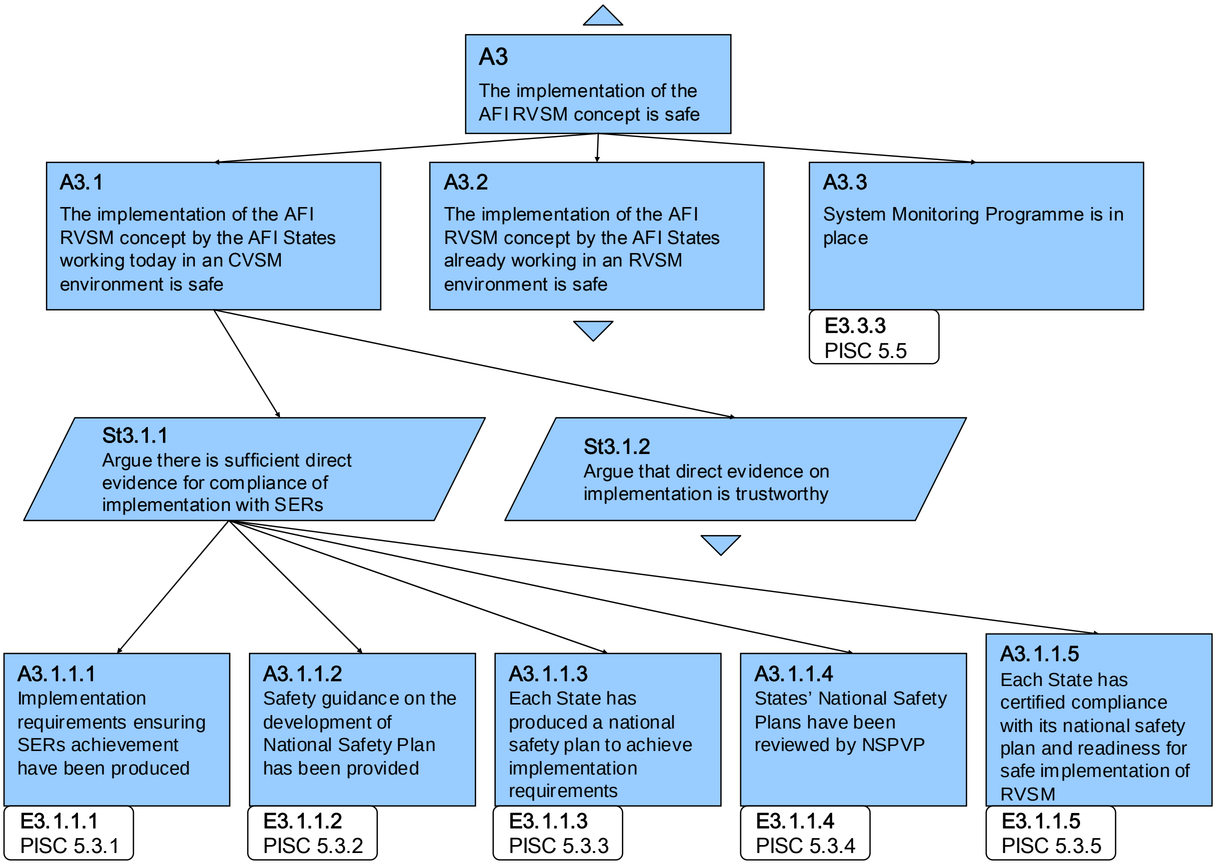

Figure 44 : Argument 3.1 – Direct argument and evidence structure

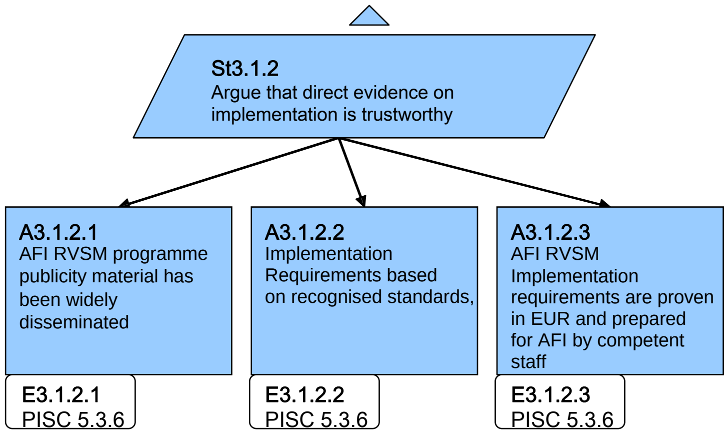

Figure 45 : Argument 3.1 – Backing argument and evidence structure

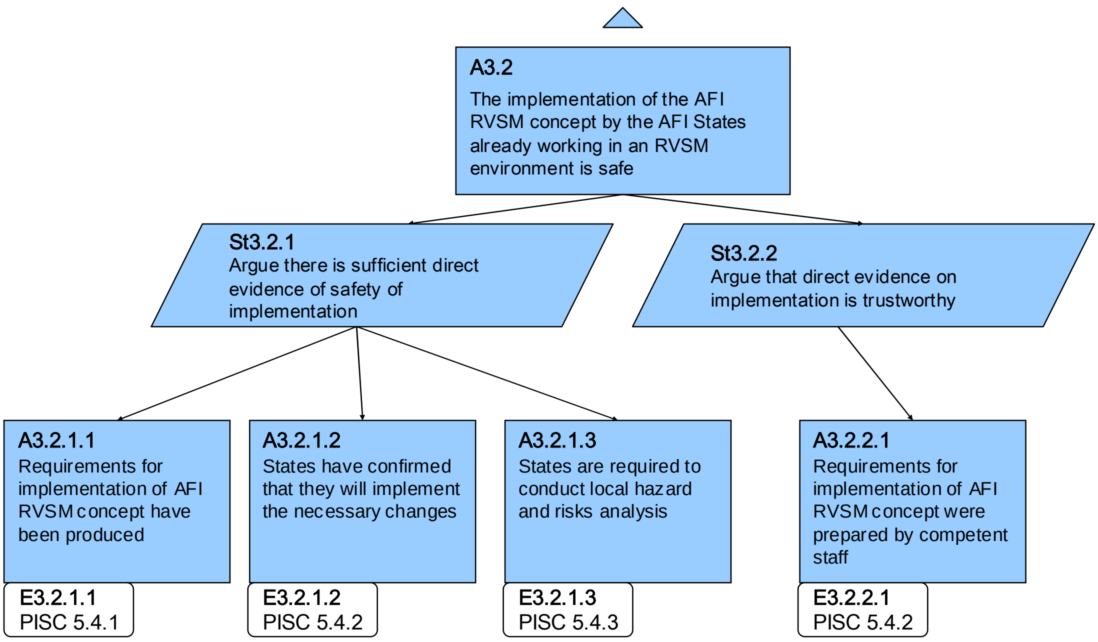

Figure 46 : Argument 3.2 – Argument and evidence structure

END OF THE DOCUMENT