AFI RVSM
POST-IMPLEMENTATION SAFETY CASE

FHA REVIEW FINAL REPORT

Immeuble SYNAPSE
Parc Centreda
4, Avenue Didier Daurat
31700 Blagnac, France
Tél. : 05 34 610 400
Télécopie : 05 34 610 410

Document à l'attention de :

International Air Transport Association

Mr Gaoussou KONATE
Regional Director, Africa - Indian Ocean
Safety, Operations & Infrastructure,
Sandown Mews, East Block, Ground Floor
88, Stella Street, SANDOWN 2196
PostNet Suite 167, Pvt Bag X9916, SANDTON, 2146
SOUTH AFRICA

Manager ALTRAN SUD-OUEST : Sémou DIOUF, +33 666356505, semou.diouf@altran.com

Page intentionally left blank.

AFI RVSM POST-IMPLEMENTATION SAFETY CASE

FHA REVIEW - FINAL REPORT

FEBRUARY 2010

Page intentionally left blank.

READERS NOTES

Page intentionally left blank.

DOCUMENT CHANGE RECORD

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

Version	Issue Date	Author	Change description
0.1	31/12/2009	Altran Sud-Ouest	Interim report
0.2	12/01/2010	Altran Sud-Ouest	Interim report for FHA participants review
0.3	05/02/2010	Altran Sud-Ouest	Final report following FHA participants review and 29/01 meeting (risk assessment)
0.4	23/02/2010	Altran Sud-Ouest	Final report before formal release
1.0	28/02/2010	Altran Sud-Ouest	Released issue

Page intentionally left blank.

SUMMARY

RVSM was safely and successfully implemented in the AFI airspace on 25 September 2008.

As part of the development of the AFI RVSM Post-Implementation Safety Case (POSC), required by the AFI RVSM Safety Policy, a review of the FHA carried out as part the Pre-Implementation Safety Case (PISC) was conducted in order to further study and update the previous findings in light of the operational experience.

The review aimed to assess the on-going AFI RVSM risks for the time period 25 September 2008 - 30 September 2009, and to update the set of safety requirements developed in the PISC. A new methodology framework, adapted to the post-implementation phase and consistent with the previous FHA and the relevant ICAO guidance material, has been developed to this end.

The review was conducted under the responsibility of ARMA, in close cooperation with IATA, and with the support of competent and representative operational experts of the AFI Tactical Action Group (TAG), through dedicated brainstorming meetings.

On the basis of the principal RVSM functions, 4 individual hazards have been identified:

H1	Non RVSM aircraft is given 1000 feet separation in AFI RVSM airspace *Undetected by ATS (a) or detected by ATS at first contact on frequency (b)*
H2	Non RVSM civil aircraft operates in the AFI RVSM airspace (detected by ATS)
H3	Aircraft is assigned a potentially conflicting flight level
H4	Aircraft deviates from cleared flight level *Unknown by flight crew (a) or known by flight crew (b) and undetected by ATS*

These hazards have been shown to be complete and correct, and to adequately cover the previous FHA hazards. Their causes and the consequences have been modelled using fault and event tree techniques. This modelling has been shown to be complete and correct, and to adequately cover the previous FHA findings thereon. The possible outcomes of the hazards have been assessed in compliance with the same Severity Classification Scheme than used for the PISC. On this basis, the following safety objectives have been specified in compliance with the same Risk Classification Scheme than used for the PISC:

	H1a	**H1b**	**H2**	**H3**	**H4a**	**H4b**
SO per hour	2.0×10^{-2}	2	2.0×10^{-2}	4.0×10^{-6}	4.0×10^{-6}	2.0×10^{-3}

The risk mitigation strategy have been derived for each of the hazards and has resulted into a set of safety requirements that adequately covers the previous FHA mitigations and addresses a number of causes and mitigations that were not explicitly revealed in the previous FHA. No specific requirement on the new issues that have risen since the implementation was found necessary.

The AFI RVSM risks have then been assessed through an estimation of the frequency of occurrence of the hazards, on the basis of the safety occurrences which have been reported, over the time period September 2008 - September 2009, through AIAG, TAG and ARMA mechanisms. This estimation was completed by operational judgment of the FHA review experts as follows:

	H1a	**H1b**	**H2**	**H3**	**H4a**	**H4b**
Est. freq. of occur	4.0×10^{-2}	4.0×10^{-2}	4.0×10^{-2}	3.0×10^{-3}	3.4×10^{-4}	3.0×10^{-3}

As a consequence, the risks arising from the individual hazards have been assessed over the time period September 2008 - September 2009 as follows:

Id.	Risk level	Conclusions
H1a	Tolerable	Risk may increase in the future due to dormant conditions related to the presence of non-RVSM civil aircraft in the AFI RVSM airspace, A/G communications and coordination between ATS units.
H1b	Acceptable	
H2	Tolerable	
H3	Not tolerable	Risk mitigation strategy implementation is not complete/correct Main contributing factors: A/G communications, ATS performance, coordination between ATS units, flight crew discipline Risk may increase in the future due to dormant conditions related to A/G communications, coordination between ATS units and to flight crew discipline
H4a	Not tolerable	Risk mitigation strategy implementation is not complete/correct Main contributing factors undetermined due to incident data limitation.
H4b	Tolerable	Risk may increase in the future due to dormant conditions related to environmental conditions, A/G communications and flight crew discipline

A set of safety recommendations have been issued to improve the level of these risks as well as the reliability of the assessment thereof as part of the next POSC.

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 Background

A Reduced Vertical Separation Minima (RVSM) of 300 m (1000 ft) between FL 290 and 410 inclusive was safely and successfully implemented in the AFI (Africa and Indian Ocean) airspace on 25 September 2008.

As required by the AFI RVSM Safety Policy [1] and in application of the APIRG ATS/AIS/SAR Sub-group Decision 10/02 [2], a first Post-Implementation Safety Case (POSC) shall be produced to ensure that on-going AFI RVSM operations meet safety expectations.

The POSC follows the AFI RVSM Pre-Implementation Safety Case (PISC) [3], endorsed by APIRG prior to RVSM introduction and accepted by the Air Navigation Commission. As an important part of the PISC, a Functional Hazard Assessment (FHA) [5] was conducted between November 2005 and April 2006. The objectives were to identify and mitigate hazards associated with RVSM operations, and to determine a set of integrity safety requirements, whose realisation, by the AFI RVSM concept and its implementation, was addressed in the subsequent parts of the PISC.

As part of the POSC, a review of the FHA is to be conducted in order to further study and update the FHA results, on the basis of the operational experience gained in the AFI Region since 25 September 2008.

1.2 Aim

This document presents and discusses the results of the AFI RVSM FHA review, carried out in December 2009 with the support of the members of the AFI Tactical Action Group (TAG).

It is intended that the findings serve as input to the POSC through:

- an assessment of the on-going AFI RVSM risks for the time period 25 September 2008 - 30 September 2009
- an update of the set of safety requirements developed in the PISC

It provides safety evidence supporting the following POSC safety arguments:

- Argument A1.1.1: “SER related to AFI RVSM system integrity have been reviewed”
- Argument A2.4: “AFI RVSM Concept complies with requirement RVSM6”

Note: RVSM6: “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”

In this context, the results of the FHA review presented hereunder aims to be generic at the AFI Region level and will have to be reviewed, further developed and locally adapted at State level as part of SSP/SMS activities, before subsequent realisation.

1.3 Structure of the Document

The remainder of this document is structured as follows:

Section 2	presents the objectives, scope, methodology, activities and organisation of the AFI RVSM FHA review process.
Section 3	sets out the results of the review of the identification of the AFI RVSM hazards
Section 4	sets out the results of the review of the assessment and mitigation of the AFI RVSM hazards' causes.
Section 5	sets out the results of the review of the assessment and mitigation of the AFI RVSM hazards' consequences.
Section 6	provides a qualitative assessment of the risks associated with the AFI RVSM hazards, for the time period 25 September 2008 - 30 September 2009.
Section 7	sets out the results of the review of the AFI RVSM risk mitigation strategy.
Section 8	provides the conclusions of the FHA review.
Section 9	provides a set of safety recommendations to the attention of ICAO for further consideration at States, ANSPs and operators levels.
Appendix A	describes the methodology framework used for the FHA review, as changed compared to the PISC, to address the limitations of the previous FHA and to serve the purpose of the POSC; and shows the consistence of that framework with the relevant ICAO guidance material.
Appendix B	details the organisation of the FHA review meetings held within the framework of the AFI RVSM Tactical Action Group.
Appendix C	provides the fault trees developed in support of the assessment and mitigation of the hazards' causes (section 4).
Appendix D	provides the event trees developed in support of the assessment and mitigation of the hazards' consequences (section 5).
Appendix E	presents the examination of the reported safety occurrences in support of the assessment of the risks associated with the identified hazards (section 6)
Appendix F	presents the system elements requirements constituting the AFI RVSM risk mitigation strategy (section 7)
Appendix G	provides the traceability between the results of the previous FHA and of the FHA review
Annex 1	provides a list of abbreviations and explanation of terms.
Annex 2	presents the applicable and reference documents.

2. AFI RVSM FHA review process

☞ This section sets out the objectives, scope, methodology, activities and organisation of the FHA review process.

2.1 Previous FHA

The FHA [5] carried out for the Pre-Implementation Safety Case (PISC) went beyond the normal scope of an FHA by addressing, not only the hazards and their consequences and associated protection mitigations, but also their causes and associated prevention mitigations. Therefore, it included activities of a typical Preliminary Safety Assessment (PSSA), referring to the EUROCONTROL Safety Assessment Methodology [9].

The process, mainly based on the model used for the implementation of RVSM in the EUR region [10], comprised 5 main stages:

- Identification of hazards and risks associated with RVSM, on the basis of operational scenarios;
- Categorisation of hazards severity and specification of safety objectives according to the applicable risk acceptance criteria;
- Determination of risk (protection and prevention) mitigation strategies;
- Derivation of the risk mitigation strategies into integrity safety requirements; and,
- Allocation of integrity safety requirements to the components of the AFI RVSM System.

That process was fully successful for AFI RVSM in providing a set of integrity safety requirements fully supporting the related PISC safety arguments.

However, its application for the purpose of the POSC would present some limitations for the assessment of the post-implementation safety. Indeed, it would lead to debatable results in some cases, in particular about the following:

- The risk identification based on operational scenarios would result in hazards of which some would be actually causal events rather than hazards in their own, as they would not be defined at the boundary of the AFI RVSM system.
- Hazards effects would be assessed according to a worst-case scenario not highlighting the efficiency of consequence mitigations and the relationships with the other potential effects in relation to the success and failure cases.
- Safety requirements would only be derived from the identified mitigations: for each hazard, causal events (failures) would not be explicitly identified, as well as all the possible ways the hazard can arise from the failures within the AFI RVSM system.

It has thus been decided to develop a new methodology framework specific to the post-implementation phase, i.e. aiming at developing a hazard model supporting the quantitative assessment (within reason) of the risks associated with the on-going AFI RVSM system.

This model, even if modified compared to the pre-implementation phase, maintains as a basis the same safety concepts and discussions addressed in the previous FHA. Those are just modelled differently, taking also into account, as appropriate, the return of experience on RVSM operations in AFI. The need for that new model has also given the opportunity to take full benefit from the evolution of the safety assessment best-practices (including ICAO provisions, e.g. [8]) that has arisen since.

2.2 Objectives

The review aims to serve as input to the POSC through:

- an assessment of the on-going AFI RVSM risks
- an update of the set of safety requirements contained in the PISC

2.3 Scope

The scope of the FHA review is limited to the post-implementation situation. It addresses the hazards and risks associated with RVSM operations in the “AFI RVSM Core Airspace” (see [3], appendix B). The review does not address the “AFI RVSM switch-over period”.

2.4 Methodology framework

The modified framework, developed for the purpose of the FHA review, is described in Appendix A. It covers typical FHA and PSSA activities (or preliminary safety assessment, referring to the experience in the EUROCONTROL area), as did the previous FHA. It is still based on the severity and risk classification schemes, as approved by the AFI RVSM Task Force and used in the PISC.

It adequately serves the assessment of the on-going RVSM operations, as follows:

- It provides a unique level to describe of hazards: the boundary of the AFI RVSM system
- It allows the explicit identification of all the hazard causes and the modelling of all the ways the hazards can arise from the combinations of those causes
- It allows the modelling of all the potential hazard consequences other than in the worst-case scenario, taking into account of the relative efficiency of the consequences mitigations; it also allows the specification of safety objective for each hazard
- Finally, it allows :
  - the qualitative assessment of the risks associated with the hazards, based on the reported RVSM safety occurrences for the AFI Region, completed by operational expert judgment; and,
  - the derivation of the risk mitigation strategy which serves as a basis for updating the integrity safety requirements.

It is consistent with the previous FHA methodology framework: the validation of the results against the previous FHA is shown all along the next sections.

The framework is also shown to be consistent with the relevant ICAO guidance material [8], see appendix A.6.

2.5 Activities

Taking account of the modified methodology framework, the activities of the FHA review are as follows:

- (1) Hazard identification
- (2) Hazard causes modelling
- (3) Hazard consequences modelling (a) and assessment (b)
- (4) Risk assessment
- (5) Risk mitigation strategy derivation
- (6) Validation of results against the previous FHA
- (7) Demonstration of results' completeness and correctness
- (8) Update of PISC integrity safety requirements

Those activities have been carried in two main stages:

- Activities (1) (2) (3a) (4) through a set of FHA review meetings which aimed to capture the operational expertise in light of the AFI RVSM experience (see Appendix B) and a subsequent processing and consolidation of the captured data.
- Activities (3b) (5) (6) (7) (8) through a post-meetings processing of hazard causes and consequences models, and a further preparation of the outcomes.

2.6 Organisation

The FHA review has been conducted by a team of Altran Sud-Ouest consultants, under the management of ARMA and in close cooperation with IATA. The Altran Sud-Ouest staff involved in that review also developed, in close coordination with ARMA, the AFI RVSM PISC [3] and FHA [5].

This staff has been supported by competent and representative operational experts from the AFI TAG, who brought their expertise during the review meetings and validated their outcomes (see Appendix B).

Page intentionally left blank.

3. Identification of RVSM hazards

☞ This section sets out the results of the review of the AFI RVSM hazards identification. It presents and discusses the AFI RVSM hazards identified according to the modified framework provided in Appendix A. It also addresses their validation against the previous FHA.

3.1 Identification (functional approach)

3.1.1 Generic AFI RVSM hazard

AFI RVSM hazards are the AFI RVSM system states, i.e. the vertical-separation events defined at the boundary of the system, which could lead to an accident. They are considered at the level of a given CTA/UTA.

As defined in the appendix A of the PISC [3], the purpose of the AFI RVSM System is to provide - between FL290 and FL410 inclusive - a 1000 feet vertical separation service to Civil and State RVSM approved aircraft and 2000 feet to State aircraft. Non-RVSM approved civil aircraft are not allowed to operate within the AFI RVSM Airspace but are allowed, subject to traffic levels, to transit through (descent from above FL410 to below FL290 or climb from below FL290 to above FL410), provided the aircraft climbs or descends at no less than standard rate and does not stop at any intermediate flight level in RVSM airspace.

In other words, the AFI RVSM system provides a single principal function:

- Aircraft to operate the AFI RVSM airspace at right flight levels.

In the AFI RVSM context, right flight level means a level in the FL290-410 band:

- operated only by RVSM civil aircraft or State aircraft; and,
- compliant with the applicable Flight Level Allocation Scheme (FLAS); and,
- at which the prescribed vertical and horizontal separation minima are not infringed.

The AFI RVSM principal function leads to a single generic vertical-separation hazard at system level:

H0 - Aircraft operates / ends up a wrong flight level

3.1.2 Specific AFI RVSM hazards

As described in the appendix A of the PISC [3], the AFI RVSM system is composed of 6 basic elements at sub-system levels:

- Flight crew and operator procedures (FCOP)
- Flight crew and operator training (FCOT)
- Aircraft and operator equipment (ACOE)
- ATS procedures (ATSP)
- ATS training (ATST)
- ATS equipment (ATSE)

This decomposition was shown to be very successful from the AFI RVSM system development point of view before the implementation. As AFI RVSM is now in operational service, it is more relevant to consider the AFI RVSM elements from a more functional and operational perspective. In this way, the operator flight planning (equipment, procedures,

training) function provided by the operator can be considered at a lower-level in support to functions provided by ATS and aircraft/flight crew.

Hence, for the purpose of the FHA review, the following AFI RVSM principal sub-systems are considered:

- ATS (equipment, people, procedures) which main function is to assign right flight levels to aircrafts, with the support of following sub-functions:
  - ATCO (people, procedures)
  - Flight data processing
  - Air Traffic Situation Display[1]
  - A/G communications
  - G/G communications
- Aircraft (equipment) and flight crew (people, procedures) which main function is to adhere to the flight level cleared by ATS
  - Flight crew (people, procedures)
  - Autopilot
  - Height keeping
  - Altimetry (height indication)
  - A/G communications

This allows the identification of further 4 hazards at AFI RVSM sub-system levels, as follows:

- ATS sub-system:

H1 - Non RVSM aircraft is given 1000 feet separation in AFI RVSM airspace

And,

H3 - Aircraft is assigned a potentially conflicting flight level

- Aircraft and flight crew sub-system:

H4 - Aircraft deviates from cleared flight level

And,

H2 - Non RVSM civil aircraft operates in the AFI RVSM airspace

Those specific hazards are described at the sub-system level of a given RVSM CTA/UTA. As the elements of the AFI RVSM system are closely interrelated, the hazards can be generated by failures within the associated sub-system but also by failures from the other sub-systems including the operator flight planning supporting element or from the interfaces (e.g. adjacent ATSU RVSM system, weather conditions).

[1] Air Traffic Situation Display (e.g. supported by radar, ADS-B, ADS-C, flight data) function is not implemented in all AFI ATS units and its conditions of use can differ from ATSU to ATSU, as depending on local policy and working methods. However, failures from this function are considered in this review as part of the causes of hazards. When available, such function is also considered as providing mitigations. This point should be addressed locally.

As a conclusion, the AFI RVSM hazards can be modelled as follows:

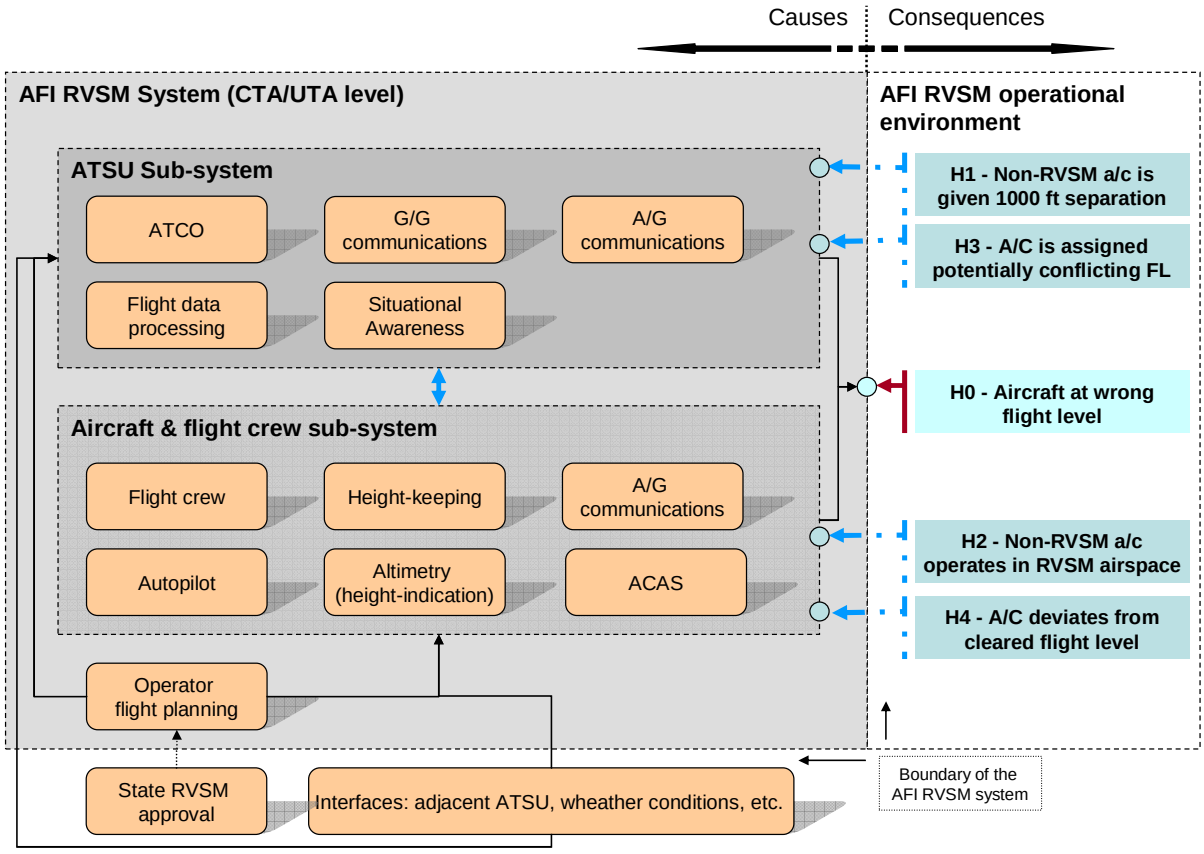

Figure 1 AFI RVSM hazard model

3.2 Hazard H1

H1 - Non RVSM aircraft is given 1000 feet separation in AFI RVSM airspace

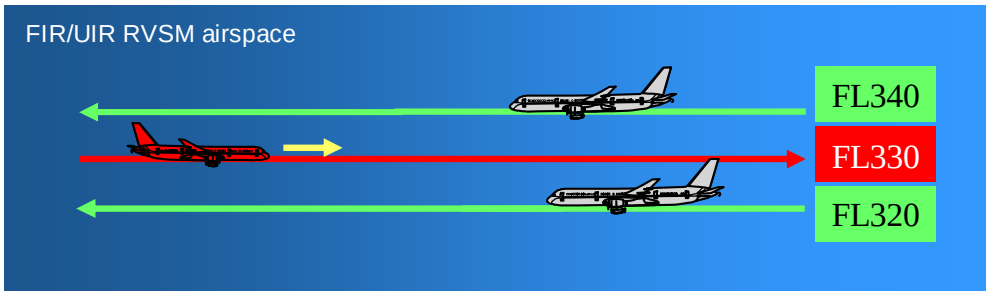

Figure 2 Hazard H1

Hazard H1 addresses the particular situation in which a non-RVSM aircraft is given 1000 feet separation instead of 2000 feet; the aircraft having previously entered into the RVSM airspace from below FL290 or from an adjacent CTA/UTA. The situation can be detected or not, by either ATS or flight crew.

It adequately covers the relevant scenarios of an incorrect application by ATS of the separation minima prescribed in the AFI RVSM airspace (the application of 2000 feet to RVSM aircraft was not considered as relevant from a safety point of view, although potentially reducing the ATM capacity).

Hazard H1 applies to State aircraft cleared into the AFI RVSM airspace ([7], §6.1.1.1) and to civil aircraft exceptionally cleared into the AFI RVSM airspace ([7], §6.1.1.2)

In this context, a non-RVSM aircraft is an aircraft which has not received RVSM State approval (non-RVSM approved aircraft) or an aircraft which has lost its RVSM capability for a specific set of flight (non-RVSM capable aircraft)

The loss of RVSM capability in flight is not considered as part of H1, as the aircraft is assumed to have minimum CVSM navigation performance. It may only deviate from its cleared flight level according to a typical height deviation. Non typical height deviations are addressed within hazard H4. It is also assumed that the flight level assigned by ATS to this aircraft is not conflicting (conflicting flight level assignment is addressed as part of hazard H3).

The incorrectly applied separation minima can be detected or not by either ATS or flight crew (including surrounding flights). If it is detected by flight crew, ATS may be advised or not (for whatever the reason). If the ATCO is not advised, it is equivalent to the situation in which ATS is incorrectly informed by the flight crew at first contact on frequency (for whatever the reason), as he/she will not take appropriate action.

This leads to consider for H1 only two particular situations: detected or not by the ATS. The detection by the ATCO (via flight crew or not) is considered to happen at first contact on frequency. Any later detection is considered as equivalent as the undetected case. Any earlier detection is considered to be solved thanks to coordination with the adjacent ATSU.

As the causes and effects differ from the situation, the two following sub-hazards are considered for H1:

H1a - Non RVSM aircraft is given 1000 feet separation (undetected by ATS)

H1b - Non RVSM aircraft is given 1000 feet separation (detected by ATS at first contact on frequency)

3.3 Hazard H2

H2 - Non RVSM civil aircraft operates in the AFI RVSM airspace

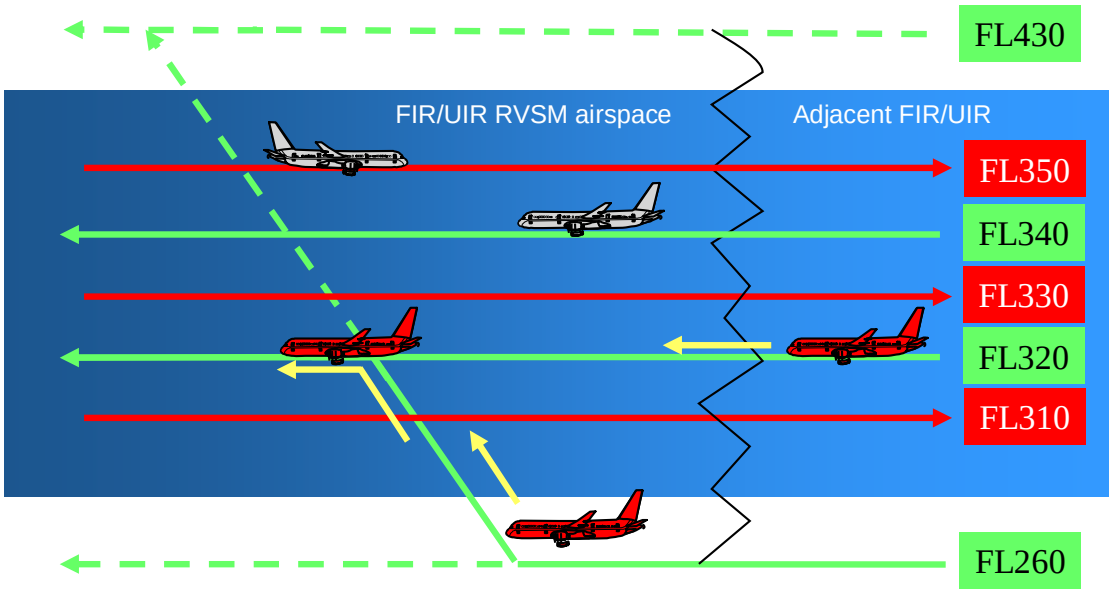

Figure 3 Hazard H2

Hazard H2 addresses the particular situation in which a non-RVSM civil aircraft operates at a flight level between FL290-410 inclusive. Indeed, although only RVSM-approved aircraft, and State aircraft (subject to ATM capacity), shall be cleared into the AFI RVSM airspace ([7], §6.1.1.1), non-RVSM civil aircraft may operate in that airspace according to the following situations[2]:

- A non-RVSM civil aircraft intending to operate above FL410 and which is cleared to transit through the RVSM airspace, subject to traffic levels, and provided that it has the capability to execute an uninterrupted climb and descent ([7], §6.1.1.2), may level-off or may not climb/descent at expected rate.
- A non-RVSM civil aircraft, operating below FL290 and experiencing adverse weather conditions (e.g. severe turbulence, icing) or fuel constraints, may be cleared at a flight level above FL290
- A civil aircraft having lost its RVSM capability may exceptionally be kept in the RVSM airspace by ATS for operational reason

The scenarios covered by hazard H2 consider that ATS is aware of the aircraft non-RVSM status and applies 2000 feet separation (1000 feet separation application is addressed as part of hazard H1). It should be also noted that the case in which ATS is not aware of the presence of the aircraft is considered as out of scope of RVSM.

It is also assumed that the flight level assigned by ATS to this aircraft is not conflicting (conflicting flight level assignment is addressed as part of hazard H3).

[2] Those situations are part of the AFI RVSM concept. Such situations that fall into the scope of hazard H2 should particularly be reviewed at State level (implementation of the concept) as non-RVSM civil aircraft clearance into RVSM airspace may differ from CTA/UTA to CTA/UTA according to State level policy and procedures (cf. [7], §6.4.2.3).

3.4 Hazard H3

H3 - Aircraft is assigned a potentially conflicting flight level

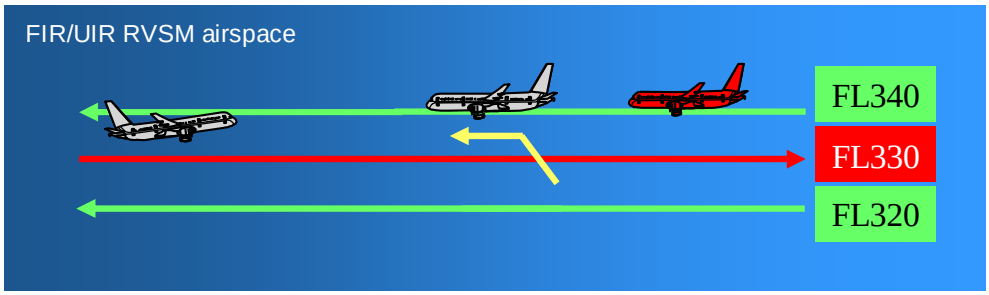

Figure 4 Hazard H3

Hazard H3 addresses the particular situation in which an aircraft is assigned a potentially conflicting flight level. In this context, a potentially conflicting flight level is defined as a flight level operated, reached or traversed by another aircraft being in a horizontal overlap potentially infringing the separation minima. Potentially adverb is used to make the opposition with the situations addressed as part of H1 and H2 and in which the flight level assignment is considered as not conflicting.

Hazard H3 applies to RVSM civil aircraft and to State aircraft (whatever the RVSM status).

It is related to the ATS sub-system and its occurrence mainly arises from failure of the ATS conflict detection and solving functions. Although those functions are not directly bound to AFI RVSM, they may have been impacted by RVSM due to the increased complexity and load of ATCOs' work with a mixed traffic flow to which different separation minima shall be applied.

Hazard H3 can be detected or not by either ATS or flight crew. As the causes do not differ from the situation, H3 is not divided as for H1 and the detection capability is taken into account as mitigation in the assessment of the consequences.

3.5 Hazard H4

H4 - Aircraft deviates from cleared flight level

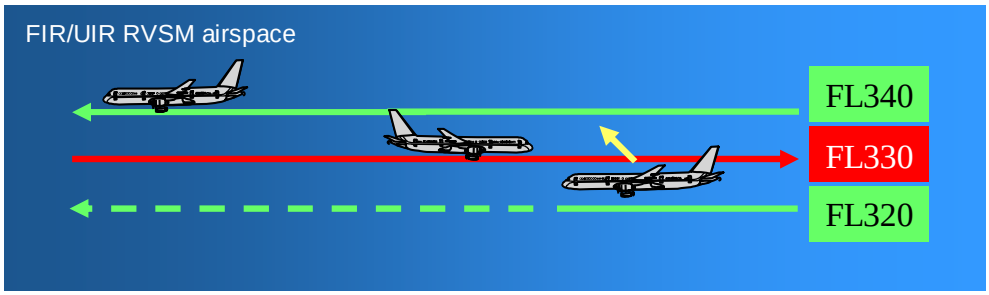

Figure 5 Hazard H4

Hazard H4 addresses the particular situation in which an aircraft deviates from the flight level cleared by ATS. In that situation, the flight level previously assigned by ATS is considered as not conflicting in its own.

Hazard H4 addresses only non typical height deviations. Typical height deviations are considered as part of the assessment of the technical vertical collision risk in the post-implementation CRA[3].

Hazard H4 applies to RVSM civil aircraft and to State aircraft (whatever the RVSM status).

It is related to aircraft and flight crew sub-system and its occurrence arises from failure in maintaining or reaching a cleared flight level.

According to the situation, the flight crew can be aware or not of the non typical height deviation. If aware, the flight crew may not contact and advise ATS (for whatever the reason). The deviation can also be detected by ATS. It should be noted that this capability mainly depends on the surveillance functions (e.g. radar, ADS-C) available at the ATSU level.

The particular case of a deviation detected by ATS requires the availability of surveillance means and is thus limited to airspaces under radar or ADS coverage. It is not further considered in the remainder of the FHA review, as ATS would take appropriate action in time.

This leads to consider for H4 only two particular situations: known or unknown by flight crew, undetected by ATS.

As the causes and effects differ from the situation, the two following sub-hazards are considered for H4:

H4a - Aircraft non-typically deviates from cleared flight level (unknown by flight crew, undetected by ATS)

H4b - Aircraft non-typically deviates from cleared flight level (known by flight crew, undetected by ATS)

[3] It should be noted that typical height deviations for non-RVSM a/c in a situation in which 1000 feet separation is given (instead of 2000 feet) is addressed as part of hazard H1.

3.6 Validation against previous FHA

The validation, against the previous FHA, of the AFI RVSM hazards, identified in the modified methodology framework, is combined with the validation of their causes in section 4.7. That combination is justified by the fact that some of the previous hazards are in reality causal events as they were not described at the boundary of the AFI RVSM system

The combined validation is detailed in Appendix G.1 and shows that the 'reviewed' AFI RVSM hazards adequately cover the previous FHA hazards.

3.7 Completeness and correctness

3.7.1 Completeness

The following elements provide evidence of the completeness of the 'reviewed' AFI RVSM hazards:

- The hazard identification functional approach, described in section 3.1, has ensured that, within reason, all significant hazards are described at the boundary of the AFI RVSM system
- The element of analysis, provided in sections 3.2 to 3.5, shows that all the particular cases of detection or awareness by ATS and flight crew of the hazardous situations have been adequately addressed
- The validation against previous FHA, provided in section 3.6, shows that the reviewed AFI RVSM hazards adequately cover the previous FHA hazards, which were demonstrated in the PISC as complete (see [3], §3.3.4)
- The hazard completeness have been validated by operational judgment of the experts participating to the second meeting of the FHA review (see Appendix B.5)

3.7.2 Correctness

The following elements provide evidence of the correctness of the 'reviewed' AFI RVSM hazards:

- The modified methodology framework of the FHA review is validated: it is based on recognised safety assessment best-practices and consistent with the relevant ICAO guidance material, as shown in appendix A.6
- The reviewed AFI RVSM hazards have been described by a competent staff, as shown in section 2.6 and in Appendix B.2

3.8 Conclusion

The AFI RVSM hazards, as identified in the modified methodology framework, are complete and correct, and adequately cover the previous FHA hazards.

4. Hazards' causes

☞ This section sets out the results of the review of the assessment and mitigation of the AFI RVSM hazards' causes. It presents and discusses the causes and mitigations of the AFI RVSM hazards, according to the modified framework provided in Appendix A. It also addresses their validation against the previous FHA.

4.1 Hazard H1a causes

H1a - Non RVSM aircraft is given 1000 feet separation in AFI RVSM airspace (undetected by ATS)

☞ H1a fault tree is provided in appendix C.2

4.1.1 Primary causes

As described in the previous section, hazard H1a addresses the particular situation, undetected by ATS, in which an aircraft which is not RVSM approved or not RVSM capable for a specific set of flights, is provided a 1000 feet vertical separation.

Hazard H1a is related to the ATS sub-system. Its primary causes are:

- **ATCO applies incorrect separation minima (human error)**

The controller may have the correct information about RVSM status but may not apply the prescribed vertical separation minima for a non-RVSM aircraft (2000 feet). This cause may originate from a cognitive error from the controller (either a mistake, or a lapse or a slip).

This primary cause is not refined at lower-levels of the AFI RVSM system

- **ATCO is incorrectly informed of the flight RVSM status**

The RVSM status information provided to the ATCO may be wrong (flight indicated as RVSM approved/capable whereas it is not). The ATCO uses different sources of information to determine the actual RVSM status of a given flight. These sources are the ATS flight data, the adjacent ATSU during coordination and the flight crew at first contact on frequency.

The ATCO is assumed to have a conservative attitude: if some of the sources indicate the flight as non RVSM approved/capable, and if the other sources are missing[4], then the ATCO will provide 2000 feet separation (except in the case of a human error, covered by the other primary cause). This means that wrong or missing information from the three sources is required for the occurrence of this primary cause.

The primary cause is thus refined through combinations of the following failures:

- (W1) ATS flight data indicates the flight as RVSM-approved or (M1) ATS flight data does not indicated the flight RVSM status; and,
- (W2) Flight RVSM status is incorrectly coordinated or (M2) Flight is not coordinated; and
- (W3) ATS is not informed of non RVSM status by flight crew at first contact on frequency

Note: (W2) and (W3) sub-causes may differ when combined with (M1) and (M2) (e.g the ATCO will query the RVSM status if not available)

[4] For the flight crew case, wrong and missing information are considered under the same notion.

4.1.2 ATS flight data

The ATS flight data are the primary source of information. They provide, under different forms (e.g. paper strip, electronic strips), the RVSM approval status as:

- stated in the flight plan filed by the operator (FPL, RPL);
- received in the current flight plan (CPL) transmitted by departure ATSU through the AFTN network; and as,
- processed by the ATS flight plan system
- updated / entered manually by an ATCO when needed.

Two different situations are considered as causes of H1a:

- **ATS flight data indicates the flight as RVSM-approved (whereas it is not)**

  The RVSM approval status may thus be corrupted at the different levels of the transmission channel (departure ATSU, AFTN network, flight data processing system, manual update/entry by ATCO) or erroneous at the origin (operator). In the last case, the FPL may be filed incorrectly or, in case of RPL, a CHG message is not sent as appropriate (late change of a/c or temporary loss of flight RVSM capability before departure)

- **RVSM approval status is missing for this flight in the ATS flight data**

  It may be generated by either:

  - a missing CPL; or,
  - a CPL not indicating the RVSM approval status in item 10 or item Q, if the FPL or RPL were previously submitted respectively (see [7], §2.1.5.1); or,
  - a failure in the processing of the RVSM approval status by the ATS flight plan processing system

4.1.3 Coordination

During the coordination, the RVSM status may be updated. From the AFI RVSM concept point of view, the transferring ATSU (T-ATSU) is expected to provide the RVSM status to the receiving ATSU (R-ATSU). However it may not be required in the actual applicable Letter of Agreement (LoA)[5].

Two different situations are considered as causes of H1a:

- **Flight RVSM status is incorrectly coordinated**

  The incorrect coordination about the RVSM status is made with the adjacent ATSU (State or civil aircraft) or with a military unit (State aircraft only) when a State aircraft is entering RVSM airspace in GAT from a reserved military airspace adjacent to, or within, the considered CTA/UTA.

  The refinement of the causes is a follows: either a deficient LoA, or the reception (by the R-ATSU) or the provision (by the T-ATSU) of incorrect RVSM status information.

- **Flight is not coordinated**

  The refinement of the causes is as follows: either the adjacent ATCO misses the coordination (human error) or the ATCOs are unable to communicate to each other, either by voice (ATS/DS) or automated systems (OLDI, or AFTN as backup of ATS/DS).

Note: civil/military coordination is assumed to take place systematically. Only the case of incorrect coordination is considered here as part of H1a.

[5] Such procedure was addressed by a specific integrity requirement (Req_{core}_56) as part of the PISC which was not realised by the ICAO concept and the States' implementation and which is an outstanding issue addressed as part of the POSC.

4.1.4 Flight crew report at first contact on frequency

At first contact on the frequency, the RVSM status may be updated.

From the AFI RVSM concept point of view, the flight crew shall report to ATS:

- At the entry into the CTA/UTA, if the flight is not RVSM capable
- At any moment, when a failure occurs that impairs its RVSM capability

At the entry into the CTA/UTA, the RVSM status may also be queried by ATS. The possible causes that could lead to a flight crew not reporting that the flight is not RVSM capable are as follows:

- Flight crew deliberately does not report non-RVSM status or reports a wrong information
- Flight crew intentionally does not report non-RVSM status or reports a wrong information: either the flight crew makes a human error (e.g. due to a lack of training, to inadequate procedure) or the flight crew is provided with incorrect information
- The flight crew is unable to communicate with ATS and the situation is not detected by ATS (otherwise 2000 feet separation would be applied). This encompasses loss of aircraft A/G and ATS A/G communications (deficiency, shortcoming, frequency congestion), including alternative means (if existing), as well as the possibility of a flight crew trying to communicate on an incorrect frequency (e.g. incorrect frequency provided by previous ATSU, flight desk entry error).
- The ATCO controller misunderstands the RVSM status reported correctly by the flight crew.

As set out in section 3.2, the loss of RVSM capability in flight is not considered as part of H1.

4.2 Hazard H1b

H1b - Non RVSM aircraft is given 1000 feet separation in AFI RVSM airspace (detected by ATS)

☞ H1b fault tree is provided in appendix C.3

As described in the previous section, hazard H1b addresses the particular situation, detected by ATS at first contact on frequency, in which an aircraft which is not RVSM approved or not RVSM capable for a specific set of flights, is provided a 1000 feet vertical separation

If the ATCO detects at first contact on frequency (following a query or at flight crew initiative) that the RVSM status is wrong, it means that he/her would have previously been provided with wrong or missing information from the ATS flight data or during the coordination with the adjacent ATS unit.

The primary causes of H1b are thus:

- (W1) ATS flight data indicates the flight as RVSM-approved or (M1) ATS flight data does not indicated the flight RVSM status; and,
- (W2) Flight RVSM status is incorrectly coordinated or (M2) Flight is not coordinated; and
- ATS is informed of non-RVSM status by flight crew at first contact on frequency

The events (W1), (M1), (W2) and (M2) are the same than for H1a.

4.3 Hazard H2 causes

H2 - Non RVSM civil aircraft operates in the AFI RVSM airspace (detected by ATS)

☞ H2 fault tree is provided in appendix C.4

As described in the previous section, hazard H2 addresses the particular situation in which a non-RVSM civil aircraft operates at a flight level between FL290-410 inclusive

Hazard H2 is related to the aircraft/flight crew sub-system. Its primary causes are:

- **Non RVSM civil aircraft levels off or does not climb/descent at expected rate while crossing AFI RVSM airspace**

This primary cause can be refined as follows:

- Unexpected adverse weather conditions (e.g. severe turbulence, icing, convective activity, temperature inversions) that forces the aircraft to stop its vertical progression (climbing and descending situations);
- Insufficient performances that have not been detected prior to entering RVSM airspace: whether the flight crew did not assessed correctly aircraft climbing capability and performances or the controller did not verified it (climbing situation only);
- Unexpected traffic (above or below) due to inadequate traffic management by the ATC (climbing and descending situations);
- Flight crew intentionally levelling off or reducing its vertical speed, which may be due to misunderstanding an ATC instruction, degradation of aircraft operational capability (e.g. emergencies) or the flight crew taking avoidance actions based solely on the TCAS (climbing and descending situations).
- **Non RVSM civil a/c operates below 290 and experiences severe turbulences or icing (or fuel constraints)**
- **A/c loses its RVSM capability and ATC decides to keep it in RVSM airspace**

When ATS is advised by a flight crew of the loss of RVSM capability, the ATCO may exceptionally decide to keep for operational reasons the aircraft in the RVSM airspace. Operational conditions that may lead the ATCO to take such a decision are in particular the ATM capacity and complexity and the fuel constraints experienced by the flight crew.

It should be noted that the particular situation in which the aircraft loses its RVSM capability in flight and the flight crew does not contact ATC (whatever the reason is) is addressed as part of hazard H4.

4.4 Hazard H3 causes

H3 - Aircraft is assigned a potentially conflicting flight level

☞ H3 fault tree is provided in appendix C.5

As set out above, hazard H3 addresses the particular situation in which an aircraft is assigned a potentially conflicting flight level. In this context, a potentially conflicting flight level is defined as a flight level operated, reached or traversed by another aircraft being in a horizontal overlap potentially infringing the separation minima

Hazard H3 is related to the ATS sub-system. Its primary causes are related to the ATS conflict detection and solving functions:

- **ATCO does not identify a conflict in flight level assignment;**

This primary cause may be generated by:

- An ATCO human error in cognitive conflict detection, combined with a failure of the MTCD (when existing)
- An incorrect or missed coordination with the adjacent sector, including due to the loss of G/G communications
- A flight crew not reporting at compulsory reporting point, including due to the loss of A/G communications

- **ATCO creates a conflict when clearing aircraft to execute flight level change**

It may be generated by a human error from the ATCO or by an ATCO provided with incorrect flight progressing data (flight strip or equivalent)

- **ATCO wrongly resolve a conflict identified;**

Wrong conflict resolution may be generated by a human error from ATCO or by an ATCO provided with incorrect flight data (from ATS flight strip or equivalent, or from adjacent ATSU during coordination).

- **ATCO can not resolve a conflict identified**

ATCO may not be able to communicate with the flight crews involved in the conflict. This situation encompasses loss of aircraft A/G and ATS A/G (deficiency, shortcoming, frequency congestion), including alternative means (if existing), as well as the possibility of a flight crew trying to communicate on an incorrect frequency

4.5 Hazard H4a causes

H4a - Aircraft non-typically deviates from cleared flight level (unknown by flight crew, undetected by ATS)

☞ H4a fault tree is provided in appendix C.6

As set out above, hazard H4a addresses the particular situation, unknown by flight crew and undetected by ATS, in which an aircraft non-typically deviates from the flight level cleared by ATS. The flight level previously assigned by ATS is considered as not conflicting in its own.

Hazard H4a is related to the aircraft/flight crew sub-system. Its primary causes are:

- **Aircraft fails to maintain cleared flight level (undetected by flight crew)**

  The adherence to cleared flight level is supported by two main airborne functions: height-keeping and altimetry (height-keeping indication).

  Failures of those functions may not be detected by flight crew. In particular, for the altimetry function, failure may arise from an incorrect altimeter setting (by flight crew).

- **Aircraft fails to reach cleared flight level (undetected level bust)**

  The climbing/descending and adherence to changed flight level is supported by two main airborne functions: autopilot and altimetry.

  Failures of those functions may not be detected by flight crew. In particular, for the altimetry function, failure may arise from an incorrect entry of the level in the flight desk by the flight crew (e.g. human error, clearance misunderstanding and read-back error).

These failures will most probably lead to deviation ranging from 0 to one or two flight levels.

4.6 Hazard H4b causes

H4b - Aircraft non-typically deviates from cleared flight level (known by flight crew, undetected by ATS)

☞ H4b fault tree is provided in appendix C.7

As set out above, hazard H4b addresses the particular situation, undetected by ATS but known by flight crew, in which an aircraft non-typically deviates from the flight level cleared by ATS. The flight level previously assigned by ATS is considered as not conflicting in its own.

Hazard H4b is related to the aircraft/flight crew sub-system.

The flight crew delay in contacting ATC to report the known deviation may arise from intentional delay (e.g. workload, priority management) or un-ability to communicate with ATC (loss of A/G communications, communication initiated on an incorrect frequency).

The other primary causes are:

- **Unexpected adverse weather conditions**

  Severe turbulence, icing or convective activity (and encountered vortex) may force the flight crew to execute a meteorological deviation according to applicable procedures

- **Flight crew intentional deviation**

  As a procedure violation, flight crew may deviate from cleared flight level without any operational justification. It is unlikely but may happen due to a lack of discipline.

- **Aircraft fails to maintain cleared flight level (detected by flight crew)**

  As for H1a, such failure may arise from the height-keeping and altimetry (height indication) functions, at the difference that the errors are detected by the flight crew. This limits to the causes to the technical failures (any error in altimetry setting by flight crew, detected by flight crew, is considered as corrected in time).

- **In flight emergency/contingency or serious aircraft equipment failure**

  This includes any emergency and contingency situation which seriously affects the aircraft capability to maintain the cleared flight level.

- **Flight crew follows an incorrect TCAS RA**
- **Flight crew takes intentional avoidance action based solely on the TCAS**

The majority of the causes presented here above mainly lead to large height deviations. However, in the case of aircraft system failure, it is possible to have detected minor height deviations.

4.7 Validation against previous FHA

As some of the previous FHA hazards are in reality causal events of the 'reviewed' hazards, the validation against the previous FHA is of two types:

- Validation of 'reviewed' FHA hazards against previous FHA, in combination with the section 3.6.
- Validation of 'reviewed' FHA causes against previous FHA

The first type of validation is detailed in Appendix G.1 which shows that the 'reviewed' AFI RVSM hazards adequately cover the previous FHA hazards.

The second type of validation is detailed in Appendix G.2 which shows that the 'reviewed' AFI RVSM causes adequately cover the previous FHA causes. As a result of the FTA technique used in the FHA review, a number of causes and mitigations have emerged that were not explicitly revealed in the previous FHA.

4.8 Completeness and correctness

4.8.1 Completeness

The following elements provide evidence of the completeness of the 'reviewed' AFI RVSM hazards' causes:

- The hazard causes modelling with a structured and logical fault tree technique, described in section C.1, together with the analysis provided in sections 4.1 to 4.6, have ensured that, within reason, all significant failures and mitigations from which the identified hazards may arise are adequately addressed.
- The validation against previous FHA, provided in section 4.7, shows that the reviewed AFI RVSM hazards causes adequately cover the previous FHA hazards causes, which were demonstrated in the PISC as complete (see [3], §3.3.4)
- The hazard causes completeness have been validated by operational judgment of the experts participating to the fourth meeting of the FHA review (see Appendix B.5)

4.8.2 Correctness

The following elements provide evidence of the correctness of the 'reviewed' AFI RVSM hazards:

- The modified methodology framework of the FHA review is validated: it is based on recognised safety assessment best-practices and consistent with the relevant ICAO guidance material, as shown in appendix A.6
- The reviewed hazard causes have been modelled by a competent staff, as shown in section 2.6 and in Appendix B.2

4.9 Conclusion

The causes of the AFI RVSM hazards, as identified in the modified methodology framework, are complete and correct, and adequately cover the causes of the previous FHA hazards.

5. Hazards' consequences

☞ This section sets out the results of the review of the assessment and mitigation of the AFI RVSM hazards' consequences. It presents and discusses the consequences and mitigations of the AFI RVSM hazards, according to the modified framework provided in Appendix A. It also addresses their validation against the previous FHA.

5.1 Hazard H1a consequences

H1a - Non RVSM aircraft is given 1000 feet separation (undetected by ATS)

☞ H1a event tree is provided in appendix D.2

As set out above, hazard H1a addresses the particular situation, undetected by ATS, in which an aircraft, which is not RVSM approved or not RVSM capable for a specific set of flights, is provided a 1000 feet vertical separation. This aircraft may deviate from its cleared flight level according to typical (technical) height-deviation and the flight level assignment is correct on its own.

5.1.1 Mitigations

The main means of mitigating the consequences of hazard H1a are as follows:

- **No horizontal overlap[6] occurs with other a/c on the flight level immediately above/below**

  This mitigation is circumstantial and relies on the operational environment conditions.

  Indeed, it is a matter of pure chance that even if there is a total vertical overlap with another aircraft, the latter will not be at the same horizontal position at the same time.

  Only other aircraft at a flight level immediately above/below are considered here. Indeed, the other aircraft at other flight levels are given 2000 feet separation (out of scope of H1) and it is assumed that there is no other aircraft at the same cleared flight level which could be in the horizontal vicinity (H1 assumes the flight level assignment is correct).

- **No vertical overlap with another aircraft**

  This mitigation relies on the aircraft typical height-keeping capability.

  Indeed, the aircraft, as well as other aircraft in the vicinity at a flight level immediately above/below, may typically deviate from their cleared flight level, leading to a vertical overlap which could be total. Such deviations are assumed as undetected.

  Should the aircraft in question be in horizontal overlap with another aircraft, the probability of the vertical overlap depends also on the typical height-keeping capability of the second aircraft which could be RVSM-approved or not.

- **Other aircraft is RVSM approved/capable**

  This mitigation is intended to take account of the typical height-keeping capability of the second aircraft.

  If the other aircraft is non RVSM approved/capable, it means that the ATCO have not previously been correctly informed of its RVSM status (by ATS flight data, adjacent ATSU or flight crew), as otherwise he/her would have applied 2000 feet separation.

[6] A horizontal overlap occurs when the two aircraft are at the same horizontal position, at the same time. This is considered to be the worst case of horizontal protection volume infringement.

5.1.2 Severity assessment

Taking into account the relative success/failure of the mitigations, the final consequences of hazard H1a are as follows:

	Vertical overlap	No vertical overlap
Horizontal overlap	If there are total vertical and horizontal overlaps with another aircraft, then there will be a total loss of separation leading to an accident. The severity class assigned to those consequences is **SC1**.	If there is another aircraft (whatever its RVSM status) in the horizontal overlap (i.e. at the same position or in the vicinity) and no vertical overlap with that other aircraft, then there will be loss of more than 50% of the separation minima* within a situation considered as controlled (flight level assignment is correct). *: H1 represents in its own a 50% reduction of vertical separation minima, and the horizontal overlap induces total loss of the horizontal separation minima) The severity class assigned to those consequences is **SC3**.
No horizontal overlap	If there are no vertical and horizontal overlaps, then the aircraft in question will continue to operate at a non conflicting flight level and will go unnoticed. The severity class assigned to those consequences is **SC5**.	

Table 1: Hazard H1a final consequences

5.1.3 Safety objective derivation

On the basis on the assessment made as part of the ETA (see section D.2.2), the following safety objective is assigned to hazard H1a:

	Per flight hour	AFI RVSM airspace
H1a	10^{-4} pfh	2.10^{-2} per h (once every 2 days)

Table 2: Hazard H1a safety objective

5.2 Hazard H1b consequences

H1b - Non RVSM aircraft is given 1000 feet separation (detected by ATS at first contact on frequency)

☞ H1a event tree is provided in appendix D.3.1

As set out above, hazard H1b addresses the particular situation, detected by ATS at first contact on frequency, in which an aircraft, which is not RVSM approved or not RVSM capable for a specific set of flights, is provided a 1000 feet vertical separation. The flight level assignment is considered as correct on its own.

5.2.1 Mitigations

The main means of mitigating the consequences of hazard H1b are as follows:

- **ATS takes immediate action**

  This mitigation is deliberate and relies on applicable ATS procedures.

  Indeed, when the ATCO is informed by flight crew at first contact on frequency that the aircraft is non-RVSM approved, he/her will take immediate action consisting in immediately providing 2000 feet to the aircraft in question, and then in clearing it out from the RVSM airspace or exceptionally keeping it in RVSM airspace (as set out in section 3.3)

  This mitigation may not work at 100%, due to potential airspace congestion or ATCO workload or human errors. In the case it does not work, the resulting situation is equivalent to H1a where a non-RVSM aircraft goes unnoticed.

- **No other a/c is in the horizontal overlap on the flight level immediately above/below**

  See section 5.1.1

- **No vertical overlap with another aircraft**

  See section 5.1.1

- **Other aircraft is RVSM approved/capable**

  See section 5.1.1

5.2.2 Severity assessment

Taking into account the relative success/failure of the mitigations, the final consequences of hazard H1b are as follows:

	Immediate action taken by ATS	No immediate action taken by ATS
Horizontal overlap	Whatever if there is another aircraft in the horizontal overlap or not, this situation will result in an increase of ATM complexity and of both ATCO and flight crew workload (to manage air traffic and to provide instructions to restore 2000 feet separation and to clear out/keep aircraft from/in the RVSM airspace, and to execute ATS instructions respectively). The reduction of vertical separation minima, represented by H1b in its own, is considered as fully recovered by ATS and flight crew. The final consequences are thus assigned the severity class **SC4**.	See hazard H1a, section 5.1.2, Table 1: Vertical overlap: Severity class **SC1**. No vertical overlap: Severity class **SC3**.
No horizontal overlap		See hazard H1a, section 5.1.2, Table 1: Severity class **SC5**.

Table 3: Hazard H1b final consequences

5.2.3 Safety objective derivation

On the basis on the assessment made as part of the ETA (see section D.3.2), the following safety objective is assigned to hazard H1b:

	Per flight hour	AFI RVSM airspace
H1b	10^{-2} pfh	2 per h

Table 4: Hazard H1b safety objective

5.3 Hazard H2 consequences

H2 - Non RVSM civil aircraft operates in the AFI RVSM airspace (detected by ATS)

☞ H1a event tree is provided in appendix D.4.1

As set out above, hazard H2 addresses the particular situation in which a non-RVSM civil aircraft operates at a flight level between FL290-410 inclusive

5.3.1 Mitigation

The primary consequence is an increase of ATCO workload to handle the non-RVSM civil aircraft within the other traffic. There only available mitigation of this consequence is circumstantial and obviously relates on the level of complexity of air traffic management at the time the hazard occurs. This level of complexity is modelled as either low or high:

- **Low air traffic management complexity**
  The increase of ATCO workload is considered as having no immediate impact on safety.
- **High air traffic management complexity**
  The increase of ATCO workload is considered to slightly degrade his/her capability.

5.3.2 Severity assessment

Taking into account the above mitigation, the final consequences of hazards H2 are as follows:

- **Low air traffic management complexity**
  No immediate impact on safety; severity class **SC5** is assigned
- **High air traffic management complexity**
  Slight ATS capability degradation; severity class **SC4** is assigned.

5.3.3 Safety objective derivation

On the basis on the assessment made as part of the ETA (see section D.4.2), the following safety objective is assigned to hazard H2:

	Per flight hour	AFI RVSM airspace
H2	10^{-4} pfh	2.10^{-2} per h (once every 2 days)

Table 5: Hazard H2 safety objective

5.4 Hazard H3 consequences

H3 - Aircraft is assigned a potentially conflicting flight level

☞ H1a event tree is provided in appendix D.5.1

As set out above, hazard H3 addresses the particular situation in which an aircraft is assigned a potentially conflicting flight level. In this context, a potentially conflicting flight level is defined as a flight level operated, reached or traversed by another aircraft being in a horizontal overlap potentially infringing the separation minima.

5.4.1 Mitigation

The main means of mitigating the consequences of hazard H3 are as follows:

- **Potentially conflicting flight level detected by ATS**

  This mitigation relies on the ATS capability to detect (potentially) conflicting flight level assignment. This capability may depend on the functions provided by the ATS equipment (e.g. MTCD).

  If this mitigation works, it will result in appropriate actions taken by ATS to restore separation minima in a situation which can be considered as fully controlled and recoverable. If not, the consequences (whatever they are) are considered as not controlled nor recoverable.

- **No horizontal overlap occurs with other a/c at the same flight level**

  This mitigation is circumstantial and relies on the operational environment conditions.

  Indeed, it is a matter of pure chance that even if an aircraft is at wrong flight level, there will not be another aircraft in the same horizontal position at the same time.

5.4.2 Severity assessment

Taking into account the relative success/failure of the mitigations, the final consequences of hazard H3 are as follows:

	Horizontal overlap	No horizontal overlap
Detected by ATS	The presence of another aircraft will result in a reduction in separation which could be large but fully controlled by ATS, due to the awareness of the situation and the appropriate action taken. The final consequences are thus assigned the severity class **SC3**.	The appropriate action taken by ATS will result in a slight increase of both ATCO and flight crew workload (to manage air traffic and to provide instructions to restore separation, and to execute ATS instructions respectively). There is no reduction of separation minima and the final consequences are thus assigned the severity class **SC4**.
Undetected by ATS	The reduction in separation due to the horizontal overlap can be total, as in this case, it is not controlled by either ATS or flight crew. The final consequences are thus assigned the severity class **SC1**.	In this situation the event will go unnoticed. The final consequences are thus assigned the severity class **SC5**.

Table 6: Hazard H3 final consequences

5.4.3 Safety objective derivation

On the basis on the assessment made as part of the ETA (see section D.5.2), the following safety objective is assigned to hazard H3:

	Per flight hour	AFI RVSM airspace
H3	2.10^{-8} pfh	4.10^{-6} per h (once every 30 years)

Table 7: Hazard H3 safety objective

5.5 Hazard H4a consequences

H4a - Aircraft non-typically deviates from cleared flight level (unknown by flight crew, undetected by ATS)

☞ H1a event tree is provided in appendix D.6.1

As set out above, hazard H4a addresses the particular situation, unknown by flight crew and undetected by ATS, in which an aircraft non-typically deviates from the flight level cleared by ATS. The flight level previously assigned by ATS is considered as not conflicting in its own.

5.5.1 Mitigation

The consequences of hazard H4a mainly depend on the magnitude of the non-typical height deviation. This leads to consider:

- large height deviations (> 300 feet)
- minor height deviations (< 300 feet)

Should the height deviation be large or minor, the main mean of mitigating the consequences of hazard H4a is as follows:

- **No horizontal overlap occurs with other a/c at a flight level above/below**

  This mitigation is circumstantial and relies on the operational environment conditions.

  Indeed, it is a matter of pure chance that, even if the aircraft is deviating to a wrong flight level, there will not be another aircraft in the same horizontal position at the same time.

5.5.2 Severity assessment

Taking into account the relative success/failure of the mitigations, the final consequences of hazard H4a are as follows:

	Horizontal overlap	No horizontal overlap
Large height-deviation	Such situation results in a large reduction in separation which can be total, as in this case, it is not controlled by either ATS or flight crew. The final consequences are thus assigned the severity class **SC1**.	In such situation, flight crew does not notice the deviation and the aircraft do not cross any other traffic. The final consequences are thus assigned the severity class **SC5**.
Minor height-deviation	Such situation results in a minor reduction of the separation, without any control and capability to recover from that situation by either ATS or flight crew. The final consequences are thus assigned the severity class **SC3**.	Such situation does not have any immediate impact on the safety of operations. The final consequences are thus assigned the severity class **SC5**.

Table 8: Hazard H4a final consequences

5.5.3 Safety objective derivation

On the basis on the assessment made as part of the ETA (see section D.6.2), the following safety objective is assigned to hazard H4a:

	Per flight hour	AFI RVSM airspace
H4a	2.10^{-8} pfh	4.10^{-6} per h (once every 30 years)

Table 9: Hazard H4a safety objective

5.6 Hazard H4b consequences

H4b - Aircraft non-typically deviates from cleared flight level (known by flight crew, undetected by ATS)

☞ H1a event tree is provided in appendix D.7.1

As set out above, hazard H4b addresses the particular situation, undetected by ATS but known by flight crew, in which an aircraft non-typically deviates from the flight level cleared by ATS. The flight level previously assigned by ATS is considered as not conflicting in its own.

5.6.1 Mitigation

As for hazard H4a, the consequences of H4b mainly depend on the magnitude of the non-typical height deviation. This leads to consider:

- large height deviations (> 300 feet)
- minor height deviations (< 300 feet)

Should the height deviation be large or minor, the main mean of mitigating the consequences of hazard H4b is as follows:

- **No horizontal overlap occurs with other a/c at a flight level above/below**
  See section 5.5.1

5.6.2 Severity assessment

Taking account the relative success/failure of the mitigations, the final consequences of hazard H4b are as follows:

	Horizontal overlap	No horizontal overlap
Large height-deviation	Such situation results in a large reduction of the separation, which is fully controlled by the flight crew, as aware of the height deviation. The final consequences are thus assigned the severity class **SC3**.	The appropriate actions taken by the flight crew as a response of the causal events (e.g. in-flight emergency/contingency, adverse weather conditions, detected failure of height-keeping or altimetry function) induce an important increase of workload to manage the situation. There is no reduction of separation minima (as no other aircraft in the horizontal overlap) and the final consequences are thus assigned the severity class **SC4**.
Minor height-deviation	Such situation results in a minor reduction of the separation, which is fully controlled by the flight crew, as aware of the height-deviation. The final consequences are thus assigned the severity class **SC4**.	Such situation does not have any immediate impact on the safety of operations. The final consequences are thus assigned the severity class **SC5**.

Table 10: Hazard H4b final consequences

5.6.3 Safety objective derivation

On the basis on the assessment made as part of the ETA (see section D.7.2), the following safety objective is assigned to hazard H4b:

	Per flight hour	AFI RVSM airspace
H4b	10^{-5} pfh	2.10^{-3} per h (once very 3 weeks)

Table 11: Hazard H4b safety objective

5.7 Validation against previous FHA

The validation against the previous FHA is limited by essence, as the 'reviewed' hazard consequences are not only modelled according to a worst case scenario but also taking account of the relative efficiency of the mitigations.

As a consequence, for a given 'reviewed' hazard, the validation can be conducted only between its worst credible consequences (subjective approach considering the credibility of success or failure of each of the mitigations) and the consequences of the previous FHA hazards covered by this 'reviewed' hazard (as seen in Appendix G.1). As the worst credible consequences are difficult to determined, it has been decided not to attempt a formal comparison and traceability as did for the 'reviewed' hazards and causes (sections 3.6 and 4.7 respectively), but to assess qualitatively the consistence.

The validation is thus based on expert judgment, conducted through a qualitative examination of the consequences modelled using event trees (and of the severity classes assigned to the final consequences - see Appendix D) and of the severity classes assigned to the previous FHA hazards.

That examination has concluded that the 'reviewed' hazard consequences are consistent with the previous FHA hazard consequences.

5.8 Completeness and correctness

5.8.1 Completeness

The following elements provide evidence of the completeness of the 'reviewed' AFI RVSM hazards' consequences:

- The hazard consequences modelling with a structured and logical event tree technique, described in section D.1, together with the analysis provided in sections 5.1 to 5.6, have ensured that, within reason, all the possible outcomes of the identified hazards, taking account the available mitigations, are adequately addressed.
- The validation against previous FHA, provided in section 4.7, shows that the reviewed AFI RVSM hazards consequences are consistent with the previous FHA hazards consequences.
- The hazard consequences completeness has been validated by operational judgment of the experts participating to the fourth meeting of the FHA review (see Appendix B.5).

5.8.2 Correctness

The following elements provide evidence of the correctness of the 'reviewed' AFI RVSM hazard consequences:

- The modified methodology framework of the FHA review is validated: it is based on recognised safety assessment best-practices and consistent with the relevant ICAO guidance material, as shown in appendix A.6
- The reviewed hazard consequences have been modelled by a competent staff, as shown in section 2.6 and in Appendix B.2.

5.9 Conclusion

The consequences of the AFI RVSM hazards, as identified in the modified methodology framework, are complete and correct, and consistent with the previous FHA.

The specified safety objectives are:

	Per flight hour	AFI RVSM airspace
H1a	10^{-4} pfh	2.10^{-2} per h (once every 2 days)
H1b	10^{-2} pfh	2 per h
H2	10^{-4} pfh	2.10^{-2} per h (once every 2 days)
H3	2.10^{-8} pfh	4.10^{-6} per h (once every 30 years)
H4a	2.10^{-8} pfh	4.10^{-6} per h (once every 30 years)
H4b	10^{-5} pfh	2.10^{-3} per h (once very 3 weeks)

Table 12: Summary of specified safety objectives

Page intentionally left blank.

6. Risk assessment

☞ This section provides a qualitative assessment of the individual risks associated with the AFI RVSM hazards, for the time period 25 September 2008 - 30 September 2009

6.1 Hazard H1a

6.1.1 Estimation of frequency of occurrence

The initial estimation of the H1a frequency of occurrence on the basis of the reported safety occurrences (cf. Appendix E) was not possible. Although it has been shown that non-RVSM aircraft flying in the AFI RVSM airspace were involved in a non negligible number of safety occurrences which can potentially be assigned to H1a (H1b and H2 as well), it was not possible to estimate in which extent H1a has occurred.

Considering:

- that safety occurrences are under-reported in the AFI Region;
- that there is indirect evidence of H1a occurrences;
- the RVSM experience of the FHA review operational experts (cf. Appendix B)

… The frequency of occurrence of hazard H1a is estimated by expert judgment around once a day i.e. 4.10^{-2} / h.

6.1.2 Assessment of the risk

H1a	Safety Objective	Estimated frequency of occurrence
Per Flight Hour	10^{-4} pfh	2.10^{-4} pfh
AFI RVSM airspace	4.10^{-2} / h (once a day)	4.10^{-2} / h (once a day)

Table 13: Safety objective vs. estimated frequency of occurrence (H1a)

H1a safety objective and estimated frequency of occurrence are comparable (i.e. are in the same order of magnitude). H1a safety objective is considered to be met.

As a consequence, it can be concluded that:

The risks arising from **H1a** have been **tolerable** over the time period **September 2008 - September 2009**.

6.2 Hazard H1b

6.2.1 Estimation of frequency of occurrence

H1b analysis is the same than for H1a.

Considering:

- that safety occurrences are under-reported in the AFI Region;
- that there is indirect evidence of H1b occurrences;
- the RVSM experience of the FHA review operational experts (cf. Appendix B)

… The frequency of occurrence of hazard H1b is estimated by expert judgment around once a day i.e. 4.10^{-2} / h.

6.2.2 Assessment of the risk

H1b	Safety Objective	Estimated frequency of occurrence
Per Flight Hour	10^{-2} pfh	2.10^{-4} pfh
AFI RVSM airspace	2 / h	4.10^{-2} / h (once a day)

Table 14: Safety objective vs. estimated frequency of occurrence (H1b)

H1b safety objective is considered to be met by more than one order of magnitude.

As a consequence, it can be concluded that:

The risks arising from **H1b** have been **acceptable** over the time period **September 2008 - September 2009**.

6.3 Hazard H2

6.3.1 Estimation of frequency of occurrence

H2 analysis is the same than for H1a.

Considering:

- that safety occurrences are under-reported in the AFI Region;
- that there is indirect evidence of H1a occurrences;
- the RVSM experience of the FHA review operational experts (cf. Appendix B)

… The frequency of occurrence of hazard H2 is estimated by expert judgment around once a day i.e. 4.10^{-2} / h.

6.3.2 Assessment of the risk

H2	Safety Objective	Estimated frequency of occurrence
Per Flight Hour	10^{-4} pfh	2.10^{-4} pfh
AFI RVSM airspace	2.10^{-2} / h (once every 2 days)	4.10^{-2} / h (once a day)

Table 15: Safety objective vs. estimated frequency of occurrence (H2)

H2 safety objective and estimated frequency of occurrence are comparable (i.e. are in the same order of magnitude). H2 safety objective is considered to be met.

As a consequence, it can be concluded that:

The risks arising from **H2** have been **tolerable** over the time period **September 2008 - September 2009**.

6.4 Hazard H3

6.4.1 Estimation of frequency of occurrence

H3 frequency of occurrence has been initially estimated, on the basis of the reported safety occurrences (cf. Appendix E), as greater than 4,5 x 10^{-4} /h, i.e. more than once occurrence every three months.

Considering:

- that safety occurrences are under-reported in the AFI Region;
- that the 4,5.10^{-4} /h figure is a lower bound, as explained in Appendix E.4
- the RVSM experience of the FHA review operational experts (cf. Appendix B)

… The frequency of occurrence of hazard H3 is estimated by expert judgment around twice a month i.e. 3.10^{-3} / h.

6.4.2 Assessment of the risk

H3	Safety Objective	Estimated frequency of occurrence
Per Flight Hour	4.10^{-8} pfh	1,5.10^{-5} pfh
AFI RVSM airspace	2.10^{-6} / h (once every 50 years)	3.10^{-3} / h (twice a month)

Table 16: Safety objective vs. estimated frequency of occurrence (H3)

H3 safety objective is estimated to be exceeded by more than one order of magnitude.

As a consequence, it can be concluded that:

The risks arising from **H3** have been **not tolerable** over the time period **September 2008 - September 2009**.

6.5 Hazard H4a

6.5.1 Estimation of frequency of occurrence

H4a frequency of occurrence has been initially estimated, on the basis of the reported safety occurrences (cf. Appendix E), as greater than 3,4 x 10^{-4} /h, i.e. more than once occurrence every four months.

This initial estimation has been judged by the FHA review operational experts (cf. Appendix B) as realistic view according to their experience. This estimation is therefore confirmed and rounded to 3,5.10^{-4} /h.

6.5.2 Assessment of the risk

H4a	Safety Objective	Estimated frequency of occurrence
Per Flight Hour	2.10^{-8} pfh	1,7.10^{-6} pfh
AFI RVSM airspace	4.10^{-6} / h (once every 30 years)	3,5.10^{-4} / h (once every 4 months)

Table 17: Assessment of safety objective meeting (H4a)

H4a safety objective is estimated to be exceeded by more than one order of magnitude.

As a consequence, it can be concluded that:

The risks arising from **H4a** have been **not tolerable** over the time period **September 2008 - September 2009**.

6.6 Hazards H4b

6.6.1 Estimation of frequency of occurrence

H4b frequency of occurrence has been initially estimated, on the basis of the reported safety occurrences (cf. Appendix E), as greater than $4{,}5.10^{-4}$ /h, i.e. more than once occurrence every three months.

Considering:

- that safety occurrences are under-reported in the AFI Region;
- that the $4{,}5.10^{-4}$ /h figure is a lower bound, as explained in Appendix E.4
- the RVSM experience of the FHA review operational experts (cf. Appendix B)

… The frequency of occurrence of hazard H4b is estimated by expert judgment around twice a month i.e. 3.10^{-3} / h.

6.6.2 Assessment of the risk

H4b	Safety Objective	Estimated frequency of occurrence
Per Flight Hour	10^{-5} pfh	$1{,}5.10^{-5}$ pfh
AFI RVSM airspace	2.10^{-3} / h (once every 3 weeks)	3.10^{-3} / h (twice a month)

Table 18: Assessment of safety objective meeting (H4b)

H4b safety objective and estimated frequency of occurrence are comparable (i.e. are in the same order of magnitude). H4b safety objective is considered to be met.

As a consequence, it can be concluded that:

The risks arising from **H4b** have been **tolerable** over the time period **September 2008 - September 2009**.

6.7 Validation against previous FHA

As set out in sections 3.6 and 5.7, the 'reviewed' AFI RVSM hazards adequately cover the previous FHA hazards, and their 'reviewed' consequences are consistent with the previous FHA respectively. As a consequence, the previous AFI RVSM risks are considered as adequately addressed in the FHA review.

The previous FHA had concluded that "all the risks identified for the Core RVSM airspace (except AH_{core}_11 in ENV2) have been assessed as tolerable, provided the proposed mitigations are implemented". AH_{core}_11 addressed the situation in which flight crew deviates from ATC clearance, in the following operational environment: "Controlled airspace without radar and ADS surveillance capabilities. Surveillance is procedural and based on communications". AH_{core}_11 is now considered as a cause of hazards H4a and H4b, which assessment has shown their respective unacceptability and tolerability, without being able to determine whether AH_{core}_11 equivalent causes are major contributory factors.

6.8 Completeness and correctness

6.8.1 Completeness

The following elements provide evidence of the completeness of the assessment of the 'reviewed' AFI RVSM risks:

- the 'reviewed' AFI RVSM hazards from which they arise are complete, as set out in section 3.7.1;
- all the possible outcomes of the hazards, taking account the available mitigations, are adequately addressed through the ETA technique, as set out section 4.8.1; and,
- the specified safety objectives, which serve as a basis for the risks level assessment constitute, the more stringent constraints resulting from the severity and possible mitigations of the hazards' outcomes.

6.8.2 Correctness

Although the quantitative estimations used for the assessment are very sensitive to the important assumptions made for the specification of the safety objectives (cf. Appendix D.8) and to the safety occurrences data used as input to initially estimate the frequencies of occurrence (see Appendix E), these are only used to support a qualitative assessment carried out by the AFI RVSM FHA review experts (cf. Appendix A.5.2).

The following elements provide thereby evidence of the correctness of the 'reviewed' AFI RVSM risks:

- The modified methodology framework of the FHA review is validated: it is based on recognised safety assessment best-practices and consistent with the relevant ICAO guidance material, as shown in appendix A.6
- The FHA review experts are a competent staff, as shown in section 2.6 and in Appendix B.2. Their qualitative judgment of the AFI RVSM risks is based on quantitative estimations which, even if limited, are considered as sufficient to draw realistic and representative conclusions about AFI RVSM risks levels.

6.9 Conclusion

The table below summarises the AFI RVSM risks as assessed qualitatively for the period of time 25 September 2008 - 30 September 2009:

	Safety Objective	Est. freq. of occurrence	Risks level
H1a	4.10^{-2} / h	4.10^{-2} / h	Tolerable
H1b	2 / h	4.10^{-2} / h	Acceptable
H2	2.10^{-2} / h	4.10^{-2} / h	Tolerable
H3	2.10^{-6} / h	3.10^{-3} / h	Not tolerable
H4a	4.10^{-6} / h	$3,5.10^{-4}$ / h	Not tolerable
H4b	2.10^{-3} / h	3.10^{-3} / h	Tolerable

Table 19: Summary of the assessment of the AFI RVSM risks

Note: above quantitative values are considered as orders of magnitude.

7. AFI RVSM risk mitigation strategy

☞ This section sets out the update of the AFI RVSM integrity safety requirements as a result of the FHA review

7.1 System Element Requirements

As set out in Appendix A.6, the AFI RVSM risk mitigation strategy is derived in the form of System Element Requirements (SER) allocated to the elements of the AFI RVSM System, which reflects the mitigations which can be used to prevent the occurrence of the AFI RVSM hazards.

The derived set of SER is provided in Appendix F. It includes requirements already developed before implementation (cf. [4], Appendix C) and which are validated in light of the operational experience, as well as new requirements resulting from the FTA technique by which a number of causes and mitigations of hazards have emerged that were not explicitly revealed in the previous FHA. No specific requirement addressing the new issues that had risen since the implementation was found necessary.

7.2 Validation against previous FHA

Appendix G.3 sets out that the previous FHA integrity safety requirements are adequately addressed by the System Element Requirements resulting from the FHA review, except for requirement Req_{Core}_90 which addresses the definition of specific procedures to avoid deviation due to incorrect visual perspective. It shows that all the previous FHA mitigations are validated in light of the operational experience with the above exception which is relevant as flight crew are now familiar with operating 1000 feet separation.

7.3 Completeness and correctness

7.3.1 Completeness

The following elements provide evidence of the completeness of the ‘reviewed’ AFI RVSM risk mitigation strategy:

- the structured and logical approach for specifying the SERs ensures that all the possible mitigations are addressed; the form of SER leads to the allocation of the requirements to the AFI RVSM system elements, ensuring the completeness of the decomposition of the mitigations;
- the ‘reviewed’ AFI RVSM causes which serves as a basis for the specification of the SERs are complete, as set out in section 4.8.1;

7.3.2 Correctness

The following elements provide evidence of the correctness of the ‘reviewed’ AFI RVSM hazards:

- the modified methodology framework of the FHA review is validated: it is based on recognised safety assessment best-practices and consistent with the relevant ICAO guidance material, as shown in appendix A.6;
- the reviewed hazard causes which serves as a basis for the specification of the SERs are correct, as set out in section 4.8.2; and,

7.4 Conclusion

The AFI RVSM risk mitigation strategy, as resulting from the modified methodology framework in the form of System Element Requirements, is complete and correct.

It adequately covers the previous FHA mitigations, with one exception which is relevant in light of the operational experience, and also addresses the new issues that had risen since the implementation.

8. Conclusions

Section 2 showed that the FHA review was based on new methodology framework developed specifically for the post-implementation phase in order to support the assessment the on-going risks arising from the AFI RVSM system. This new framework is consistent with the previous FHA, as well as with the relevant ICAO guidance material on safety management.

Sections 3, 4 and 5 described the results of the assessment of the AFI RVSM hazards and of their causes and consequences, and presented the safety objectives assigned to the AFI RVSM hazards. It showed that the hazards and their causes and consequences as modelled according to the new methodology framework are complete and correct, and adequately address the previous FHA findings thereon.

Section 6 presented the results of the assessment of the AFI RVSM risks and showed that the risks arising from 2 of the 5 identified individual hazards have been not acceptable over the time period 25 September 2008 - 30 September 2009.

Section 7 set out the results of the derivation of the AFI RVSM risk mitigation strategy. In light of the operational experience, it showed that the strategy adequately covers the previous FHA mitigations and includes new requirements resulting from a number of causes and mitigations that were not explicitly revealed in the previous FHA. No specific requirement on the new issues that have risen since the implementation was found necessary.

The situation regarding the individual AFI RVSM hazards is summarised as follows:

Id.	Risk level	Conclusions
H1a	Tolerable	Risk may increase in the future due to dormant conditions related to the presence of non-RVSM civil aircraft in the AFI RVSM airspace, A/G communications and coordination between ATS units.
H1b	Acceptable	
H2	Tolerable	
H3	Not tolerable	Risk mitigation strategy implementation is not complete/correct Main contributing factors: A/G communications, ATS performance, coordination between ATS units, flight crew discipline Risk may increase in the future due to dormant conditions related to A/G communications, coordination between ATS units and to flight crew discipline
H4a	Not tolerable	Risk mitigation strategy implementation is not complete/correct Main contributing factors undetermined due to incident data limitation.
H4b	Tolerable	Risk may increase in the future due to dormant conditions related to environmental conditions, A/G communications and flight crew discipline

Table 20: Summary of the results

Page intentionally left blank.

9. Recommendations

☞ This section provides a set of safety recommendations to the attention of ICAO for further consideration at State, ANSP and operator levels

The following recommendations are issued with the aim to improve the level of the risks arising from the AFI RVSM hazards as well as the reliability of the next assessment thereof.

Id.	Recommendations	Rationale / Comment
1	The reporting and assessment of safety occurrences should be improved to support mapping with the AFI RVSM hazard models and subsequent assessment of risks arising from the individual hazards.	Data limitations, see Appendix E Necessary improvements are further discussed in the POSC.
2	Measures to significantly improve ATS performance (organisation, equipment, procedures, proficiency) should be taken as a matter of highest priority	Main contributory factor (hazard H3, not tolerable)
3	Measures to significantly improve A/G communications performance (e.g. coverage, reliability) should be taken as a matter of highest priority	Main contributory factor (hazards H3 and H4b, not tolerable) Dormant condition (H1a, H3 and H4b)
4	Measures to significantly improve the performance of the coordination between ATS units (G/G communications, procedures, training) should be taken as a matter of highest priority	Main contributory factor (hazard H3, not tolerable) Dormant condition (H1a, H1b and H3)
5	Flight crew discipline should be reinforced	Main contributory factor (hazard H3 and H4b, not tolerable) Dormant condition (H3 and H4b)
6	State-level practises and procedures related to the handling of non-RVSM civil aircraft in RVSM airspace should be surveyed	Dormant condition (H1a, H1b and H2)
7	The implementation of the strategy, for mitigating the risk arising from an aircraft being assigned by ATS a wrong (i.e. potentially conflicting) flight level, should be reinforced as a matter of highest priority	Hazard H3, not tolerable Strategy provided in Appendix F
8	The implementation of the strategy, for mitigating the risk arising from an aircraft deviating from cleared flight level (situation unknown by flight crew),	Hazard H4a, not tolerable

Id.	Recommendations	Rationale / Comment
	should be reinforced as a matter of highest priority	Strategy provided in Appendix F
9	States' capabilities and diligence with regards to operator and aircraft RVSM approval should be reinforced.	Experience reported to ARMA: gap between States' commitments contained in the NSP and the reality. Hazard H1
10	The use of ATS surveillance systems in the provision of area air traffic control service should be reinforced where appropriate	Possible additional mitigation for hazard H4 (cf. Appendix F)
11	The use of CPDLC application in the provision of area air traffic control service should be reinforced where appropriate	Possible additional mitigation for hazards H1, H3 and H4 (cf. Appendix F)
12	Unidirectional and/or parallel tracks should be implemented where appropriate.	Possible additional mitigation for hazard H4 (cf. Appendix F)
13	Strategic Lateral Offset Procedures should be implemented	Possible additional mitigation for hazard H4 (cf. Appendix F)

Table 21: Safety recommendations

These recommendations are further addressed in the POSC.

Page intentionally left blank.

Appendix A Methodology framework for the FHA review

☞ This appendix sets out the methodology framework used for the FHA review and shows its consistence with the relevant ICAO guidance material.

A.1 AFI RVSM generic hazard model

The overall framework is defined by the following generic hazard model:

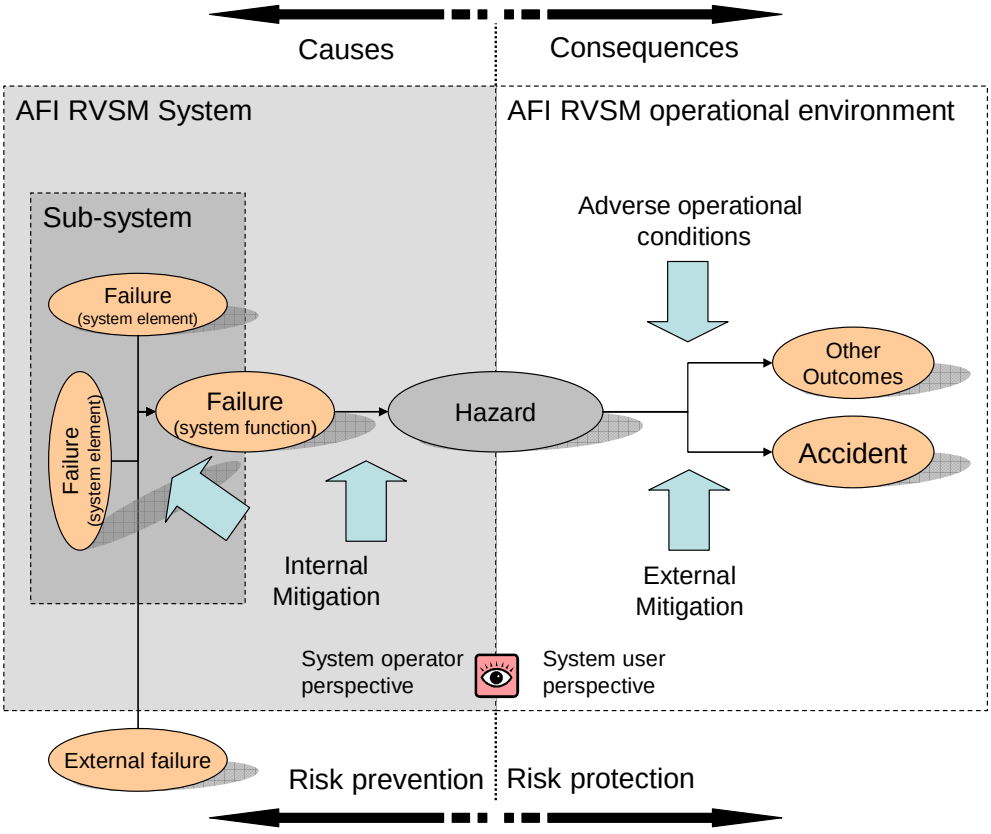

Figure 6 AFI RVSM generic hazard model

This model makes a clear distinction between the AFI RVSM system under assessment and the AFI operational environment in which it is operated, establishing the boundary between causes and consequences spaces.

A.1.1 AFI RVSM hazards

An AFI RVSM hazard:

- is a potential source of threat of safety, i.e. a state of the AFI RVSM system that could lead to an accident;
- is not an incident nor an accident, but a potential source (pre-requisite to the occurrence)
- could lead to an incident or accident when combined with certain adverse operational conditions

Hazards are described at the boundary of the AFI RVSM system under assessment and should be considered at CTA/UTA level. They can be either generic to the AFI RVSM purpose or specific to the AFI RVSM functions.

A.1.2 AFI RVSM hazard consequences

Once a hazard has occurred, the AFI RVSM system has no control over the consequences. The only mean to stop an accident occurring rely on the external mitigations (risk protection).

External mitigations can be either deliberate (e.g. procedure) or a matter of chance (e.g. even if an aircraft operated at wrong flight level, it is unlikely that there would be a second aircraft in the same horizontal position at the same time).

In order to determine the consequences of a given hazard on the safety of AFI RVSM operations, various elements should be considered, such as effects:

- on the AFI RVSM system functional capabilities and ability to provide safe services;
- on the system users and operators working conditions (e.g., workload, ability to perform tasks);
- on the system users and operators ability to cope with adverse operational and environmental conditions; and,
- on the functional capabilities of the user.

The safety of AFI RVSM operations mainly relies on the maintenance of the prescribed separation minima between aircraft.

The severity of a hazard, which is defined as the level of its final consequences on the safety of operations, therefore combines the level of loss of separation and degree of ability to recover from the hazardous situation.

A.1.3 AFI RVSM hazard causes

Hazards are generated by combination of failures within the AFI RVSM system, resulting from combination of faults within the system elements, interactions with other systems and/or external events. As hazards are considered at CTA/UTA level, their causes can relate to the local RVSM system and its operational environnement or from the adjacent CTA/UTA RVSM system.

The causes of a hazard determine its likelihood of occurrence, which can be reduced thanks to internal mitigations (risk prevention).

Internal mitigations are provided by the different elements of the AFI RVSM system and are of various natures, including procedural or technical.

A.2 AFI RVSM hazard identification

AFI RVSM hazards are described at the boundary of the AFI RVSM system at the level of a given CTA/UTA. They are related to the AFI RVSM system purpose and thus to vertical separation.

Their identification is based on the principal functions provided by the AFI RVSM system. Generic and specific AFI RVSM hazards are identified on the basis of a description of those functions at system and sub-systems levels respectively.

A.3 AFI RVSM causes modelling

The potential causes of the AFI RVSM hazards and associated (internal) mitigations are modelled following a fault tree technique, which is a standard safety assessment technique, in particular successfully used for the EUR RVSM POSC. The technique as adapted for the purpose the AFI RVSM FHA review is presented in appendix C.1

A.4 AFI RVSM consequences modelling

The potential consequences of the AFI RVSM hazards and associated (external) mitigations are modelled following an event tree technique, which is a standard safety assessment technique, in particular successfully used for the EUR RVSM POSC. The technique as adapted for the purpose the AFI RVSM FHA review is presented in appendix D.1

The qualitative assessment of the severity of the final consequences is made in consistence with the criteria defined in the following severity classification scheme (SCS):

Severity Class	1 [Most Severe]	2	3	4	5 No safety effect [Least Severe]
Effect on Operations*)	**Accidents**	**Serious incidents**	**Major incidents**	**Significant incidents**	**No immediate effect on safety**
Examples of effects on operations Include*):	❑ one or more catastrophic accidents, ❑ one or more mid-air collisions ❑ one or more collisions on the ground between two aircraft ❑ one or more Controlled Flight Into Terrain ❑ total loss of flight control. No independent source of recovery mechanism, such as surveillance or ATC and/or flight crew procedures can reasonably be expected to prevent the accident(s).	❑ large reduction in separation (e.g., a separation of less than half the separation minima), without crew or ATC fully controlling the situation or able to recover from the situation. ❑ one or more aircraft deviating from their intended clearance, so that abrupt manoeuvre is required to avoid collision with another aircraft or with terrain (or when an avoidance action would be appropriate).	❑ large reduction (e.g., a separation of less than half the separation minima) in separation with crew or ATC controlling the situation and able to recover from the situation. ❑ **minor** reduction (e.g., a separation of more than half the separation minima) in separation without crew or ATC fully controlling the situation, hence jeopardising the ability to recover from the situation (without the use of collision or terrain avoidance manoeuvres).	❑ increasing workload of the air traffic controller or aircraft flight crew, or slightly degrading the functional capability of the enabling CNS system. ❑ **minor** reduction (e.g., a separation of more than half the separation minima) in separation with crew or ATC controlling the situation and fully able to recover from the situation.	No hazardous condition i.e. no immediate direct or indirect impact on the operations.

Figure 7 Severity classification scheme

This SCS was approved for AFI RVSM by the AFI RVSM Task Force and used for the previous FHA (see [5], Annex D).

A.5 Risk assessment

A.5.1 Acceptance/Tolerance criteria

The criteria for acceptance of the risks associated with the AFI RVSM hazards are defined in the following risk classification scheme (RCS):

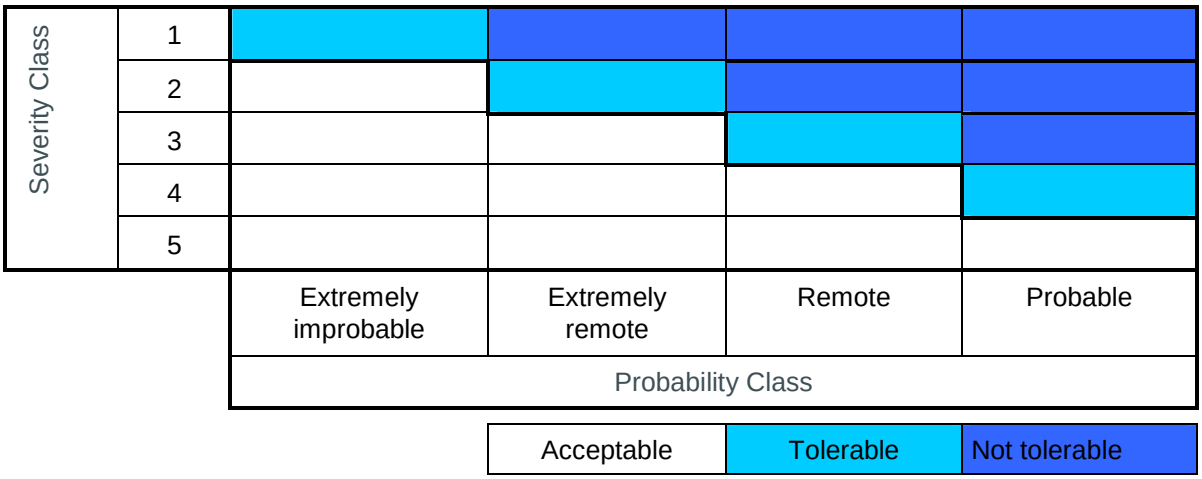

Figure 8 Risk classification scheme

The qualitative probability classes are defined as follows:

Probability Class	Per flight hour / per aircraft	AFI RVSM Airspace
Extremely improbable	**$P \leq 10^{-9}$**	**P≤1/100 years**
Extremely remote	**$10^{-9} < P \leq 10^{-7}$**	**1/100 years < P ≤ 1/year**
Remote	**$10^{-7} < P \leq 10^{-5}$**	**1/year < P ≤ 1/day**
Probable	**$10^{-5} \leq P$**	**1/day ≤ P**

Figure 9 Probability classes

These RCS and associated probability classes were approved for AFI RVSM by the AFI RVSM Task Force and used for the previous FHA (see [5], Annex E).

For the purpose of the FHA review, the application of that RCS for the assignment of target probability (maximum expected frequency of occurrence) to each of the hazard final consequences is as follows:

Severity class	Target Probability (pfh)	Target Probability (AFI RVSM airspace)
SC1	10^{-9} pfh	2.10^{-7} / h
SC2	10^{-7} pfh	2.10^{-5} / h
SC3	10^{-6} pfh	2.10^{-4} / h
SC4	10^{-5} pfh	2.10^{-3} / h

Table 22: Correspondence between severity classes and target probability

Note: The aggregate of the AFI ATS units is assumed to operate 24/24h.

It is estimated that a given hour in the AFI RVSM airspace corresponds to 200 flight hours.

This estimation is mainly based on the traffic data estimated in the CRA (see [3], section 3.4) in the time period 25 September 2010 - 30 September 2009 for the 23 AFI FIRs/UIRs of which the vertical events have been taken into account, as follows:

- 852 000 flight hours are estimated for the considered time period, for 23 FIRs/UIRs
- This number is a lower bound due to the lack of data from 3 FIRs/UIRs
- Traffic data are not available for the other 7 FIRs/UIRs covered by the POSC scope.
- As a consequence, a factor of 2 is assumed between the number of flight hours for the 23 FIRs/UIRs and the entire AFI RVSM airspace
- This factor is acceptable, as values are worked as order of magnitude
- Considering 371 days in the time period and 24 hours per day, the estimated number of flight hours per hour for the entire AFI RVSM airspace is rounded to 200.

A.5.2 Assessment process

The process applied for assessing the AFI RVSM risks comprises four stages:

- Safety objective

  Specification of a maximum frequency of occurrence for each of the AFI RVSM hazards, through ETA technique (cf. section D.1.2)
- “Reported” frequency of occurrence

  Initial estimation for each of the AFI RVSM hazards, based on the examination of the reported safety occurrences in the AFI Region (cf. Appendix E)
- “Estimated” frequency of occurrence

  Final estimation for each of the AFI RVSM hazards, based on the “reported” frequency occurrence which is completed by operational judgment of the FHA review experts, taking account of various factors (cf. section 6.6.1)
- Assessment of the risks

  Assessment, for each of the AFI RVSM hazards, of the “estimated” frequency of occurrence against the specified safety objective

It is important to note that the assessment if the risks is made qualitatively.

Although quantitative figures are handled as part of the process, those figures are only worked as orders of magnitude. This is justified by some uncertainty of the estimations:

- The safety objective values are sensitive to the important assumptions made (cf. Appendix D.8)
- The frequency of occurrence values are sensitive to the input data (see Appendix E)

The quantitative values are thus only used to support a qualitative assessment.

A.6 AFI RVSM risk mitigation strategy

The derivation of the AFI RVSM risk mitigation strategy consists in specifying a set of safety requirements as an expression of the factors mitigating the risks associated with the AFI RVSM hazards. In consistence with the AFI RVSM model (see section 3.1.2), its focuses on the mitigations internal to the AFI RVSM system, i.e. the mitigations which can be used to prevent the occurrence of the AFI RVSM hazards.

The approach is similar to the one used in the previous FHA (see [5], Appendix F), even if it focuses this time only on the causes. The safety requirements are thereby specified, on a cause by cause basis, to reflect the mitigations that could be used to prevent the occurrence of the considered cause. The specification is based on the principle that the realisation of the safety requirements shall ensure the efficiency and implementation of the considered mitigations.

In order to ensure successful use in the POSC document, and in order to benefit from the improvements made in the PISC compared to the previous FHA, the safety requirements of this FHA review are specified in the form of System Elements Requirement - SER (cf. [4], section 3). Indeed, the SERs results from the detail and allocation of the FHA integrity safety requirements (and of the High-Level Safety Requirements as well).

Although the risk mitigation strategy is derived under SER form, the results are then validated against the previous FHA set of integrity safety requirements in order to confirm the mitigations identified in the previous FHA.

This activity is carried out independently from the risk assessment. However, if some risks are assessed as not tolerable, it means that the associated risk mitigation strategy, provided it is complete and correct, is not fully or appropriately implemented as part of the elements of the AFI RVSM system.

Therefore, attention of the States will be particularly drawn to the new safety requirements (not specified at the time of the PISC) and to the ones associated with the risks which are not assessed as tolerable, in order to reinforce awareness as well as subsequent complete and correct implementation.

A.7 Consistency of FHA review methodology with ICAO relevant guidance material

A.7.1 Background

The methodology framework outlined above is mainly based on recognised safety assessment best-practices standardised in the framework of the EUROCONTROL EATMP Safety Assessment Methodology.

As the AFI Region regulatory framework for safety management is based on ICAO provisions, it is necessary to show that the relevant ICAO guidelines are adequately covered by the FHA review framework.

Those ICAO guidelines are enclosed in the ICAO Safety Management Manual Doc.9859 [8]. Regarding hazard and risk assessment, the relevant contents are provided by chapter 4 “Hazards” and chapter 5 “Safety risk”.

A.7.2 Approach

The approach consists in assessing the consistency regarding the following five fundamentals of hazard and risk assessment: Hazard, Risk, Likelihood / Frequency of occurrence, Severity and Risk acceptance criteria

A.7.3 Consistency assessment

Fundamental	ICAO SMM	FHA review	Comment
Hazard			
Hazard definition	§4.2.3 - A condition or an object with the potential of causing injuries to personnel, damage to equipment or structures, loss of material, or reduction or ability to perform a prescribed function	Any condition, event, or circumstance which could induce an accident (i.e. an AFI RVSM system state that could lead to an accident).	Consistent
Hazard are not consequences	§4.2.5 - A consequence is defined as the potential outcomes of a hazard. (A clear differentiation is established between hazards, as sources of potential injury or damage, and their safety consequences described in operational terms - see §5.2.2).	Hazards are not an incident nor an accident, but a potential source (pre-requisite to the occurrence). Hazards could lead to an incident or accident when combined with certain adverse operational conditions. Hazards are described at the boundary of the AFI RVSM system: they are vertical-separation hazards.	Consistent
Generic/specific hazards	§4.5 - Identify generic (A) and specific (B) hazards	Generic hazard at overall system level and specific hazards at principal sub-systems level	Consistent
Risk			
Risk definition	§5.2.8 - Assessment, expressed in terms of predicted probability and severity, of the consequences of a hazard taking as reference the worst foreseeable situation	Combination of the frequency of occurrence of a harmful effect induced by a hazard and the severity of that effect	Consistent, with slight difference: FHA review goes beyond, as AFI RVSM risk covers all the possible consequences of the (vertical-separation) hazard and not only the worst foreseeable situation.
Links with hazards	§5.2.5 - Risks are related to the consequences of hazards.	Risks arise from hazards	Consistent
Likelihood			

Fundamental	ICAO SMM	FHA review	Comment
Likelihood definition	§5.4.2 - Safety risk probability: the likelihood that an unsafe event or condition might occur	Qualitative or quantitative statement that defines the frequency or probability at which a unsafe event can be expected to occur	Consistent
Likelihood classes	Figure 5-2 (example for education purpose: 5 probability classes: 1) Frequent - likely to occur many times 2) Occasional - likely to occur some times 3) Remote - unlikely but possible to occur 4) Improbable - very unlikely to occur 5) Extremely improbable - almost inconceivable that the event will occur	See Figure 9 Probability classes	Consistent, with slight difference, classes for the FHA review includes quantitative definitions. Classes are adapted and commensurate to RVSM risks
Severity			
Severity definition	§5.5.2 Safety risk severity: the possible consequences of an unsafe event or condition, taking as reference the worst foreseeable situation	Level of effect/consequences of hazards on the safety of flight operations (combining level of loss of separation and degree of ability to recover from the hazardous situation)	Consistent, with slight difference: for AFI RVSM, severity is assessed for all the possible consequences of the (vertical-separation) hazard and not only for the worst foreseeable situation.
Severity classes	Figure 5-3: A. Catastrophic B. Hazardous C. Major D. Minor E. Negligible	See Figure 7 Severity classification scheme 1. Accidents 2. Serious incidents 3. Major incidents 4. Significant incidents 5. No immediate effect on safety	Consistent
Severity criteria	Figure 5-3	See Figure 7 Severity classification scheme	Consistent
Risk acceptance			
Acceptance criteria	Figure 5-4	See Figure 8 Risk classification scheme	Consistent

Fundamental	ICAO SMM	FHA review	Comment
Use of RCS	Assessing risk tolerability (reactive)	Assessing risk tolerability (reactive) or setting safety objectives (proactive)	Consistent

Table 23: Assessment of consistency: FHA review framework - ICAO guidelines

A.7.4 Conclusion

The methodology framework used for the FHA review is shown as consistent with the relevant ICAO guidance material contained in Doc. 9859 [8].

Appendix B FHA review meetings

☞ This appendix sets out the organisation of the FHA review meetings held within the framework of the AFI Tactical Action Group.

B.1 Objectives

The FHA review meetings were organised within the framework of the Tactical Action Group, established under the authority of the ICAO Special AFI Regional Air Navigation Meeting of 2008, and operating under the reporting authority of APIRG.

As set out in section 2.5, the FHA review meetings aimed to be a major contributor to the FHA review by brainstorming on the following key areas:

- AFI RVSM hazards identification;
- AFI RVSM hazards' consequences modelling; and,
- AFI RVSM hazards' causes modelling.

B.2 Roles and responsibilities

The key stakeholders involved in the FHA review meetings can be divided in two groups:

- A facilitation team from Altran Sud-Ouest company and managed by ARMA; and,
- AFI RVSM operational experts representing Users, ATS providers and International Organisations

B.2.1 Facilitation team

The facilitation team was responsible for providing all the necessary safety expertise to achieve the meetings' objectives. It is composed as follows:

Organisation	Name	Designation
ARMA	Kevin Ewels	ARMA manager
Altran Sud-Ouest	Julien Lapie	Safety Expert
Altran Sud-Ouest	Christophe Guerber	Safety Expert

Table 24: FHA review meetings - Facilitation Team

Kevin Ewels acted as the chairman and was responsible for leading the meetings, introducing and closing the discussions and ensuring that the sessions' objectives were achieved.

Julien Lapie acted as the facilitator and was responsible for running and guiding the discussions, and eliciting the RVSM operational knowledge and experience from the operational experts.

Christophe Guerber acted as the secretary and was responsible for ensuring that the key findings from the discussions were fully and accurately recorded, using tools based on mind mapping techniques.

B.2.2 Operational experts

The operational experts have great experience of operations in the AFI Region and are acquainted to RVSM operations, as follows:

Organisation	Name	Designation
ICAO Headquarters	Dražen Gardilčić	Air Navigation Bureau, ATM section
ICAO Headquarters	Capt. Miguel A. Marin	Air Navigation Bureau, FLS section
ICAO ESAF	Seboseso Machobane	Regional Officer, ATM
ICAO WACAF	Sadou Marafa	Regional Officer, ATM
ASECNA	Amadou Yoro Diallo	Air Navigation Dpt, Head of ATM programs
South Africa ATNS	Harry Roberts	ATM Specialist and RVSM NPM
East Africa (Kenya)	Patrick Kinuthia	RVSM National Program Manager
IATA	Prosper Zo'o Minto'o	AFI SO&I Assistant Regional Director
IFALPA	Carole Couchman	IFALPA Technical Officer
IFALPA	Capt. Souhail Dallel	IFALPA RVP AFI West
IFALPA	Carl Bollweg	IFALPA RVP AFI South
IFATCA	Keziah Ogutu	Regional Representative ATC

Table 25: FHA review meetings - Operational experts

This team is representative of the AFI RVSM operations and of the various operational environments in which they take place. It is composed of people involved in AFI RVSM operations, as well as in the maintenance of the AFI RVSM system. It appropriately covers the following profiles:

- Flight Crew (Users) operating daily the AFI RVSM airspace
- ATCOs (ANS providers): controllers providing ATS in the AFI RVSM airspace:
  - with the support of radar capability,
  - with the support of ADS/CPDLC capabilities,
  - without the support of any surveillance capability,
- ATM/RVSM experts (ANS providers, International Organisations) involved in the planning, development and maintenance of the AFI RVSM system.

In addition, it should be noted the great involvement from those experts and the maturity reached in a relative short time, giving further confidence in the relevance and completeness of the results.

B.3 Approach

The approach, defined to achieve the objectives set out in section B.1, comprised three main brainstorming sessions as follows:

- Session 1: AFI RVSM hazards identification
- Session 2: AFI RVSM hazards' consequences modelling
- Session 3: AFI RVSM hazards' causes modelling

B.4 Inputs to the meetings

B.4.1 Facilitation team's preliminary work

In order to avoid restarting the work from scratch when reviewing the previous FHA results, a preliminary work was performed by Altran Sud-Ouest, consisting in processing these previous results in the modified methodology framework, presented in Appendix A. The outcomes of this preliminary work kept traceability with the previous FHA results and was presented to the operational experts before each brainstorming session.

In order to ensure the efficiency of the meetings and the achievement of their objectives, the facilitation team also prepared dedicated briefing material [6] for the benefit of the operational experts.

B.4.2 Operational experts' preliminary work

The operational experts have been advised to get acquainted with the briefing material [6] providing general information about the meetings, and guidelines and rules for the brainstorming activities to be conducted.

In order to ensure the quality of the meetings' outcomes, participants have also been advised to prepare, before the first meeting, their preliminary inputs for the brainstorming sessions, on the basis of the operational experience gained within their organisation, and in compliance with the guidelines provided in the briefing material. Then between each meeting, the participants were advised to carry out some home-work (e.g. specific analysis, specific review) according to the previous meeting outcomes.

B.5 Work Plan

According to the approach defined above, the work plan was set-up as follows:

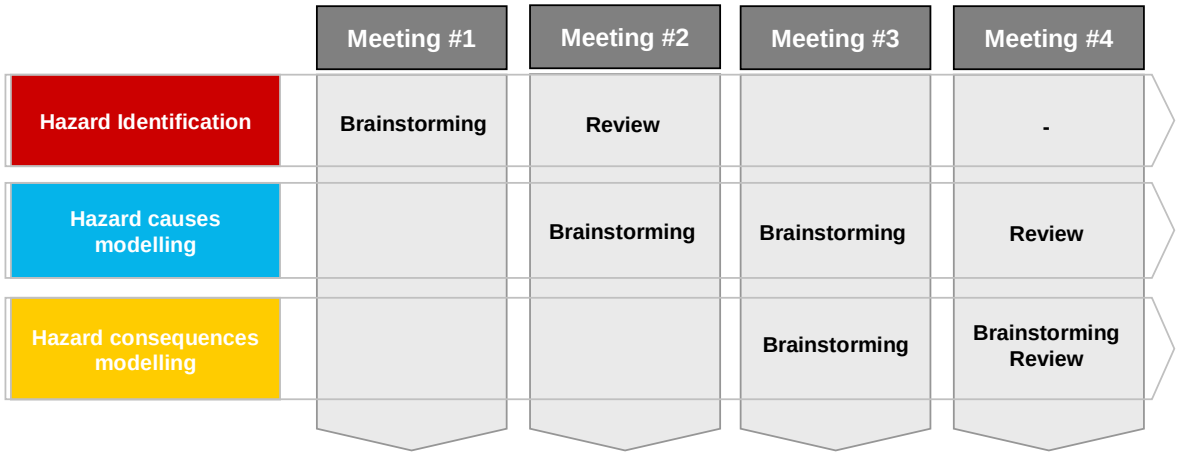

Figure 10 FHA review meetings - Work plan

The schedule was decided and approved during the TAG meeting of 25 November 2009, as follows:

- Meeting #1: 1 December 2009, 13h30 - 16h30 UTC
- Meeting #2: 4 December 2009, 13h30 - 16h30 UTC
- Meeting #3: 9 December 2009, 13h30 - 16h30 UTC
- Meeting #4: 14 December 2009, 13h30 - 16h30 UTC

The teleconferences were hosted by IFALPA.

Note: the assessment of the AFI RVSM risks was addressed during the validation meetings on 20 and 29 January 2010 (see below).

B.6 Meetings management

Before each meeting, the operational experts were provided with:

- the meeting agenda from the facilitation team
- the teleconferences details from IFALPA

The typical agenda was as follows:

- participants welcoming & agenda approval
- introduction
- brainstorming(s) session(s) #n
- debriefing & next steps

The introduction presentation aimed at reminding the context, the progress status and the results obtained so far. It also aimed to introduce the brainstorming sessions to be conducted and to provide the necessary background information to do so.

After each meeting, the operational experts were provided with a 'debriefing and next steps' material comprising:

- a presentation discussing the main 'raw' outcomes and providing guidelines for the 'home-work' expected from the participants before the next meeting,
- the data processed off-line by Altran Sud-Ouest and presented with specific mind-mapping tools.

B.7 Outputs from the FHA review meetings

The main outcomes of the meetings were processed off-line by Altran Sud-Ouest and served as inputs for the next steps of the FHA review (see § 2.4 and § 2.5).

B.8 Validation

The version 0.2 of this report was distributed to the participants for their review prior to the final release. It was presented during the TAG meeting of the 12th January 2010.

Participants were advised to provide their comments, using a dedicated form, before 19 January 2010.

Those comments were reviewed during the FHA review meetings held on 20 and 29 January 2010.

Appendix C Fault trees

☞ This appendix sets out the fault tree technique used as part of the modified methodology framework, and the event trees and the associated assessments made thereof.

C.1 FTA technique

C.1.1 Causes modelling

For each hazard identified, a fault tree is developed to model all the possible ways in which the hazard could arise from failure within the AFI RVSM system.

A fault tree is a graphical and logical model of all the possible causes of the hazard, taking into account the mitigations that could be used to prevent hazard occurrence. It is a top-down deductive technique which allows linking directly the hazard to all the possible causes in a single model.

A fault tree begins at the top with a single hazard and its branches are developed to the bottom. The various paths through the tree model the various parallel and sequential combinations of causes that will result in the occurrence of the top hazard.

The symbology used for the FHA review is described as follows:

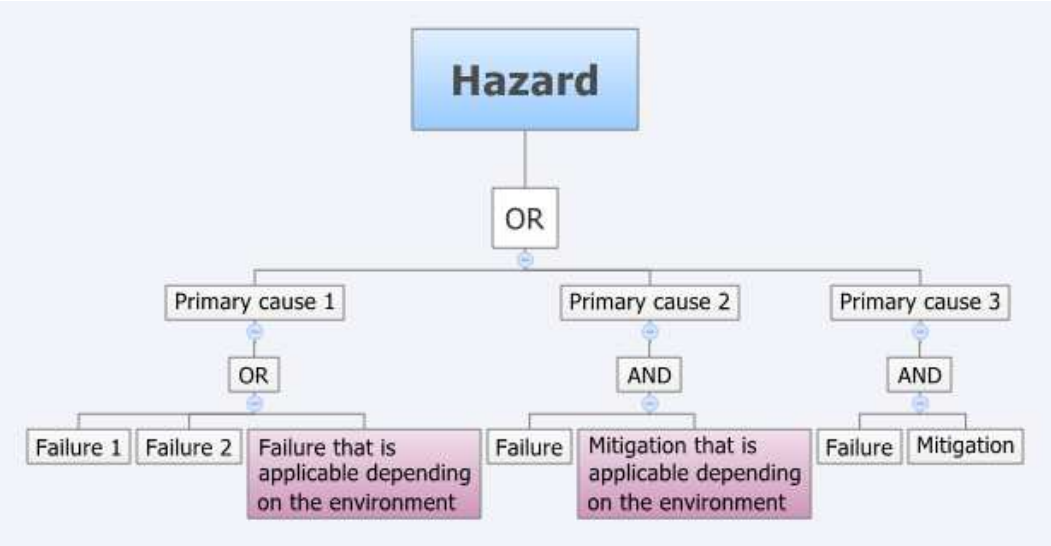

Figure 11 Fault tree symbology

The different levels of the tree shows the relationships, within the AFI RVSM system architecture, of lower events required for the occurrence of the higher events. The graphical nature aids the qualitative identification of the hazard causes.

The relationships are shown with logical gates “AND” and “OR”. The lower and intermediate events/causes can be either a system failure or a mitigation (working or not). The gate “OR” is used when the occurrence of a least of lower-level failure (input to the gate) is required to lead to the higher event (output to the gate). The gate “AND” is used when the occurrence of the lower-level failure and of the success / failure of the mitigation is required to lead to the higher event.

As hazards are considered at CTA/UTA level, the failures can arise from the local RVSM system and its operational environment; or from the adjacent CTA/UTA RVSM system.

As the ATM/CNS capabilities environment in which RVSM is operated is not homogeneous in AFI (see [3], appendix A), some failures or mitigations are only relevant for some particular environmental types.

C.1.2 Assessment

A probability may be assigned to show the relative success / failure of the mitigations. That probability is assessed by operational judgment or engineering technique, or is based on the experience according to the available data.

If all the mitigations are assigned a success / failure probability, the fault tree technique can be used generally:

- to deduce a maximum frequency of occurrence for each of the lower-level causes, if a safety objective (maximum frequency of occurrence) is assigned to the top-level hazard.
- to deduce the frequency at which the intermediate events and the top-level hazard could occur, if a frequency of occurrence is assigned to each of the lower-level causes

These possibilities have not been explored as part of the FHA review, as the frequencies of occurrence of the lower-level causes are not known, as the framework used for safety occurrences reporting and assessment (cf. Appendix E) do not directly provide such data.

As a consequence, it has been found difficult to accurately assess the frequency of occurrence of each hazard on a FTA-basis only. The assessment conducted as part of the FHA review finally consists in examining the reported safety occurrence from a system (hazard) level point of view and in completing the estimations by operational judgment (cf. A.5.2).

C.2 Hazard H1a

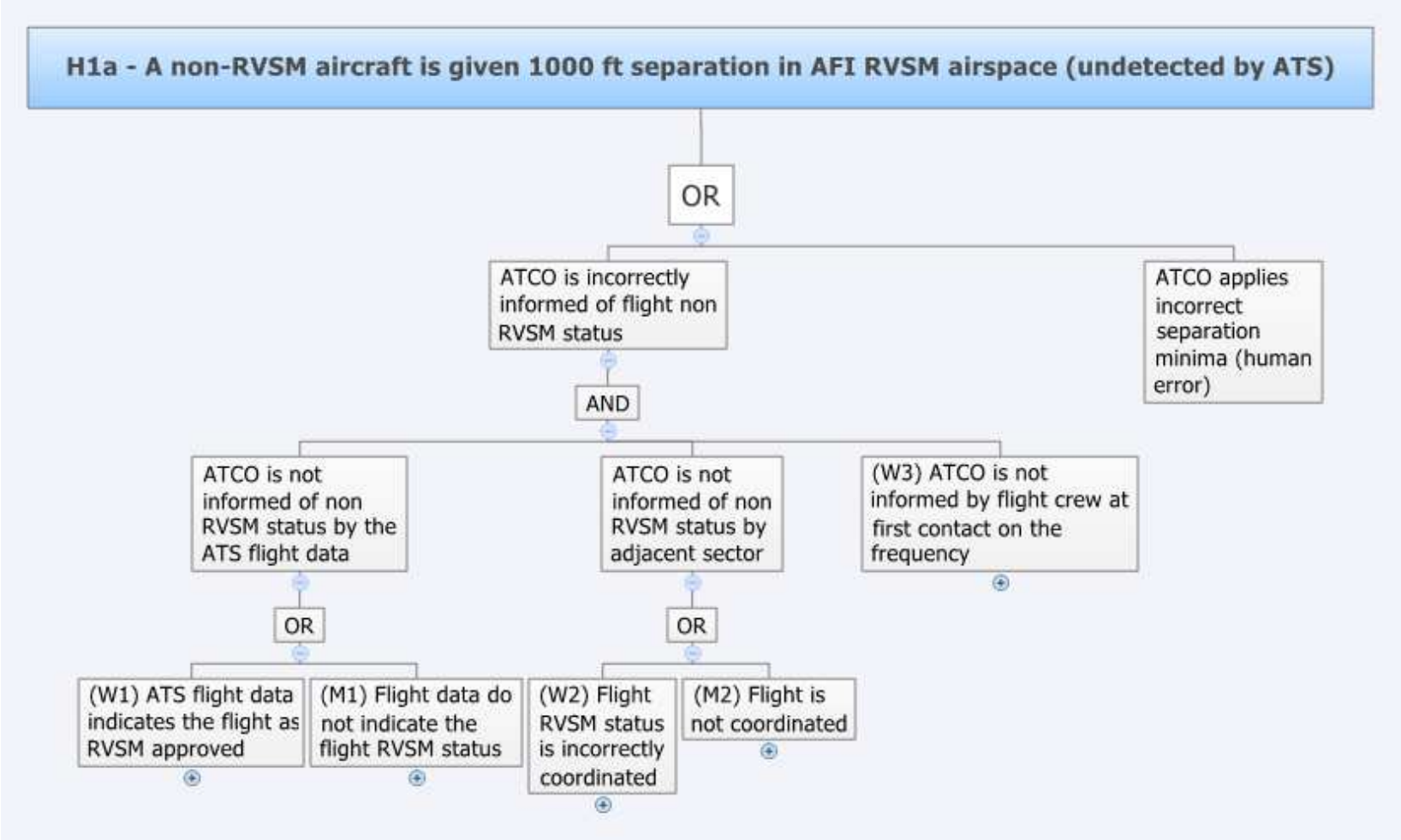

Figure 12 H1a fault tree (1/6)

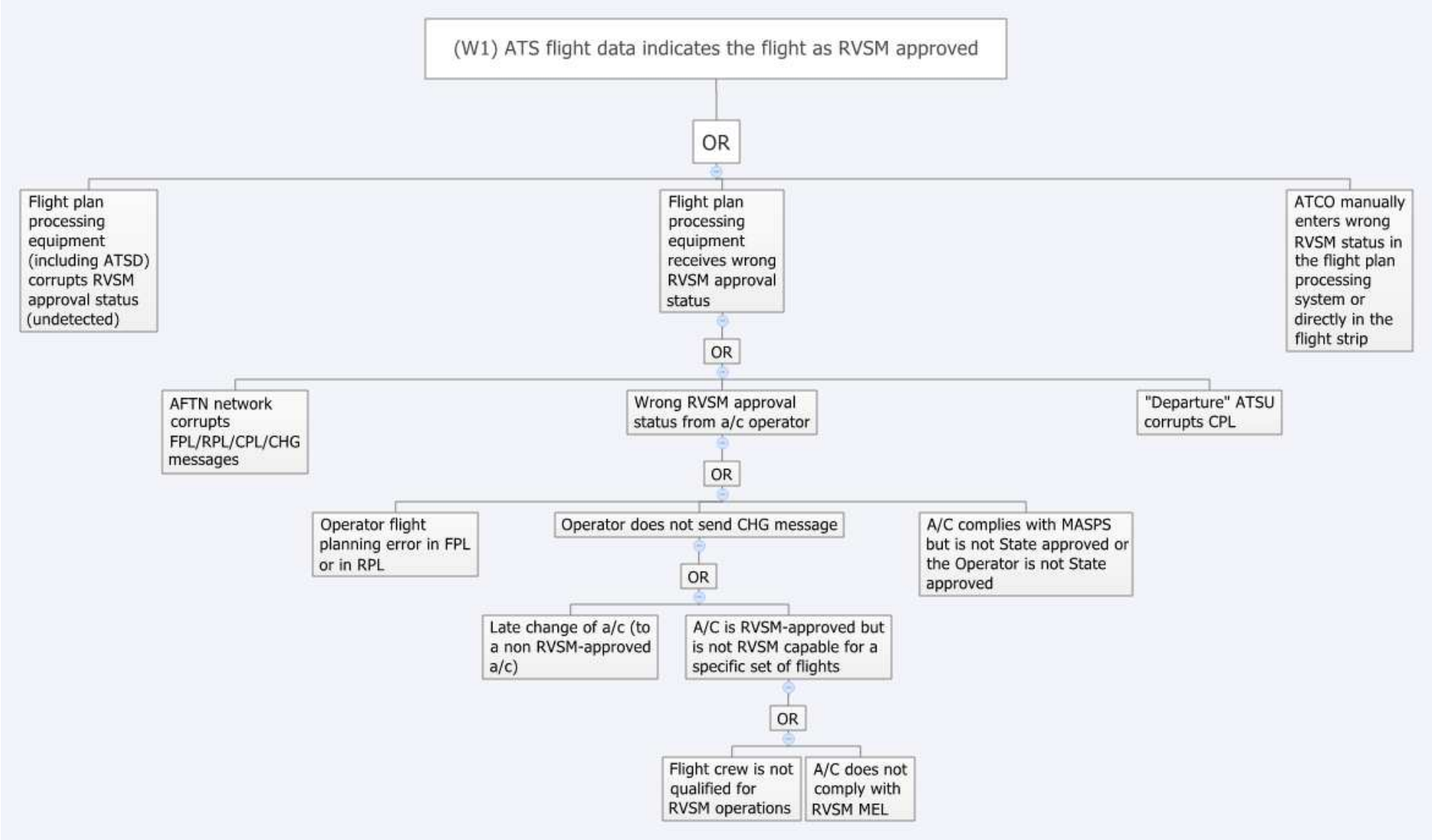

Figure 13 H1a fault tree (2/6)

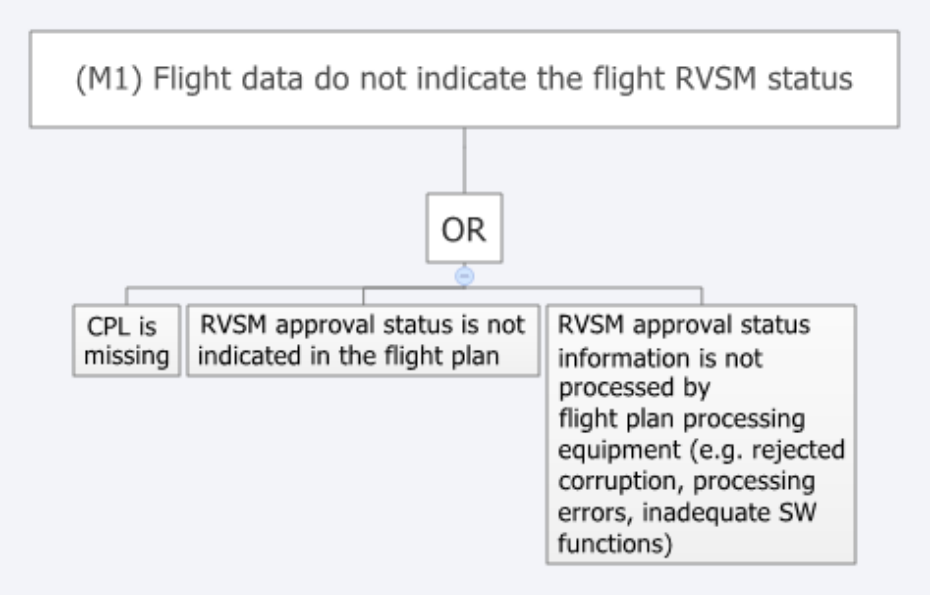

Figure 14 H1a fault tree (3/6)

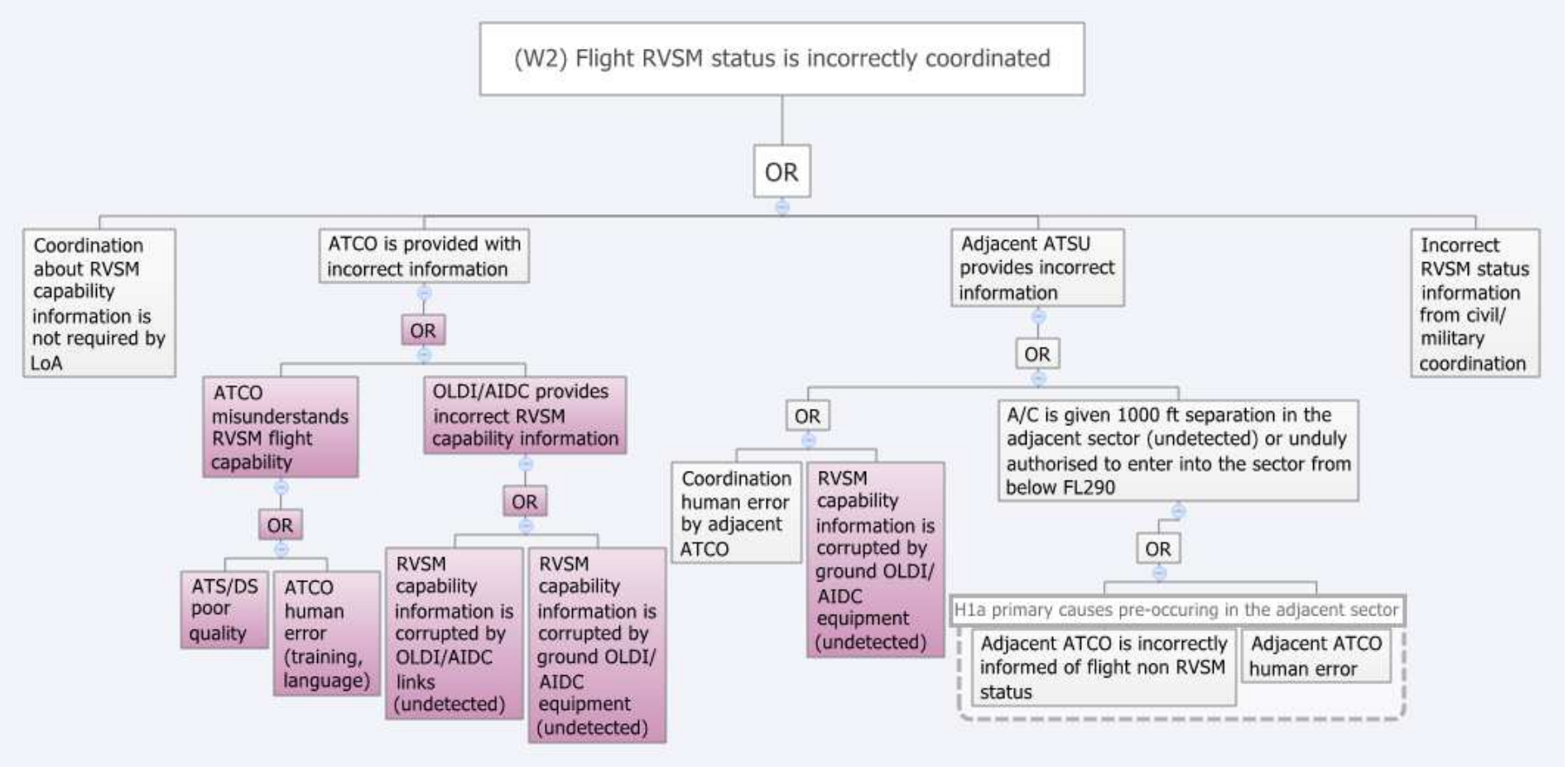

Figure 15 H1a fault tree (4/6)

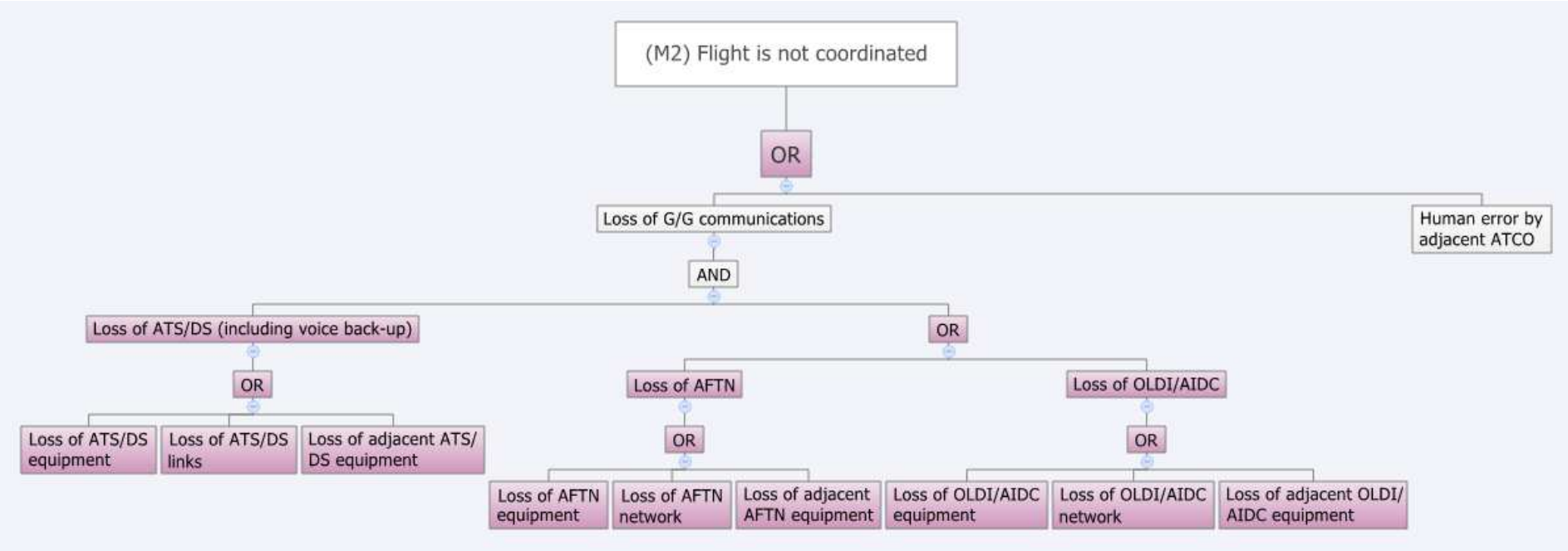

Figure 16 H1a fault tree (5/6)

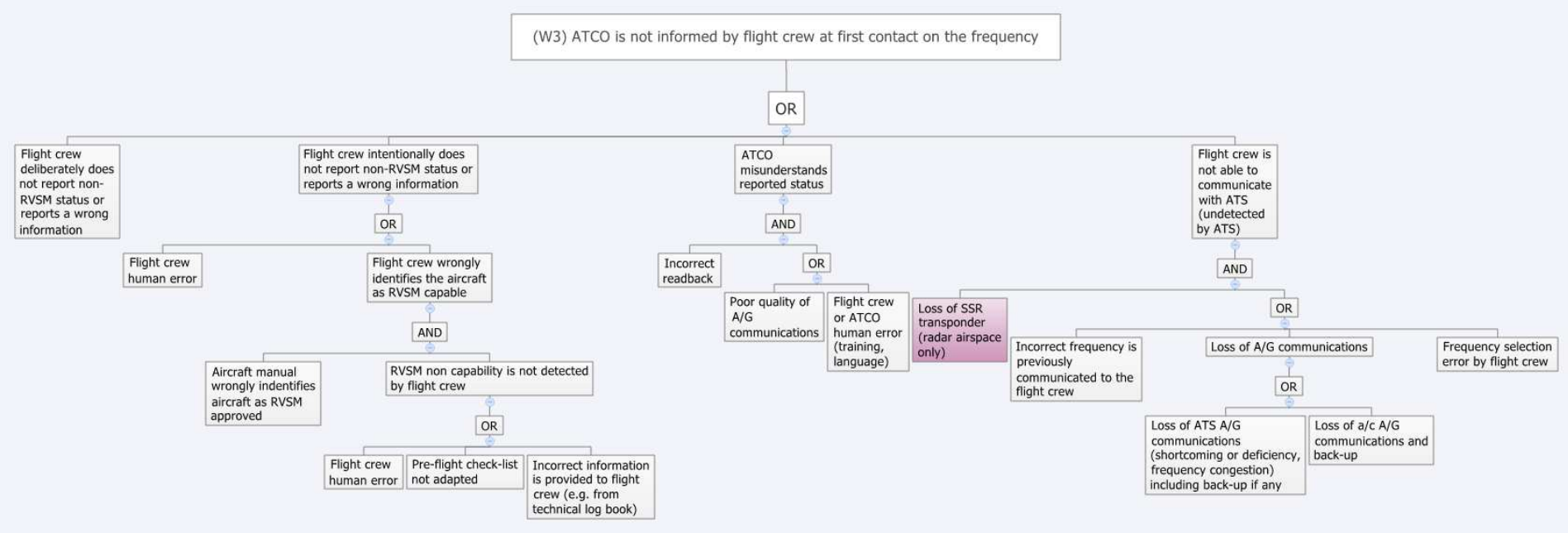

Figure 17 H1a fault tree (6/6)

C.3 Hazard H1b

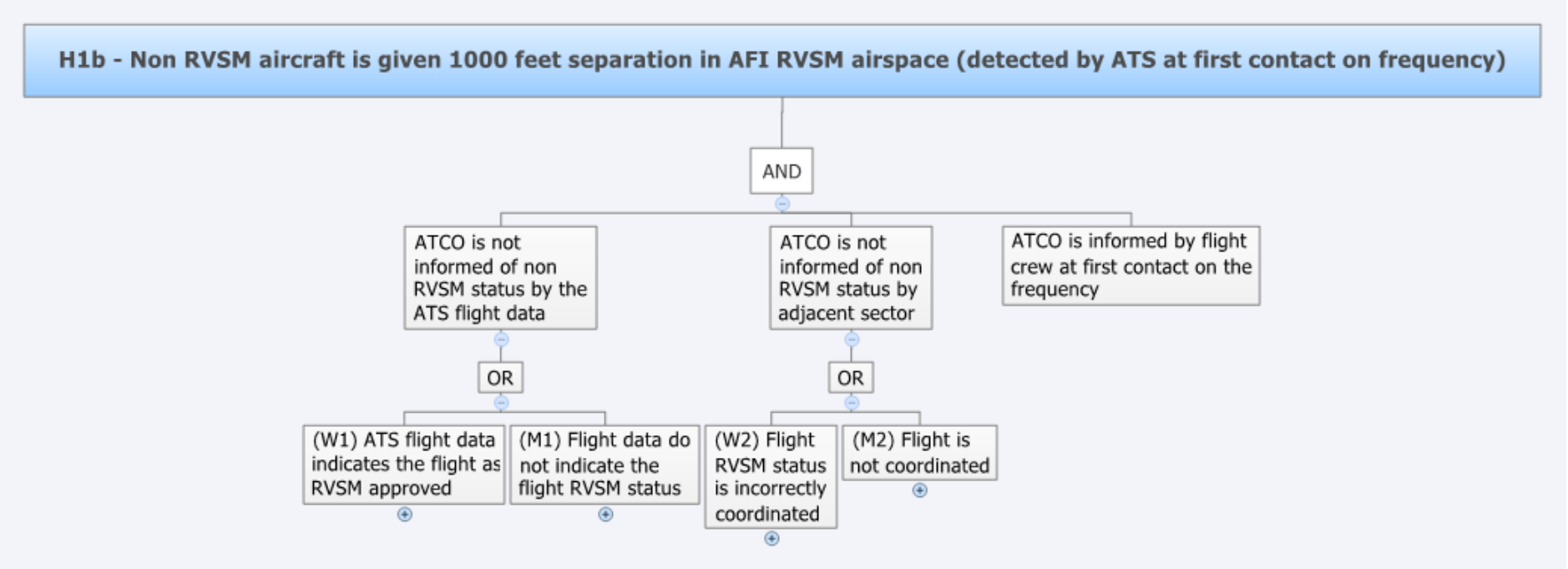

Figure 18 H1b fault tree

The trees for the events (W1), (M1), (W2) and (M2) are the same than for H1a above.

C.4 Hazard H2

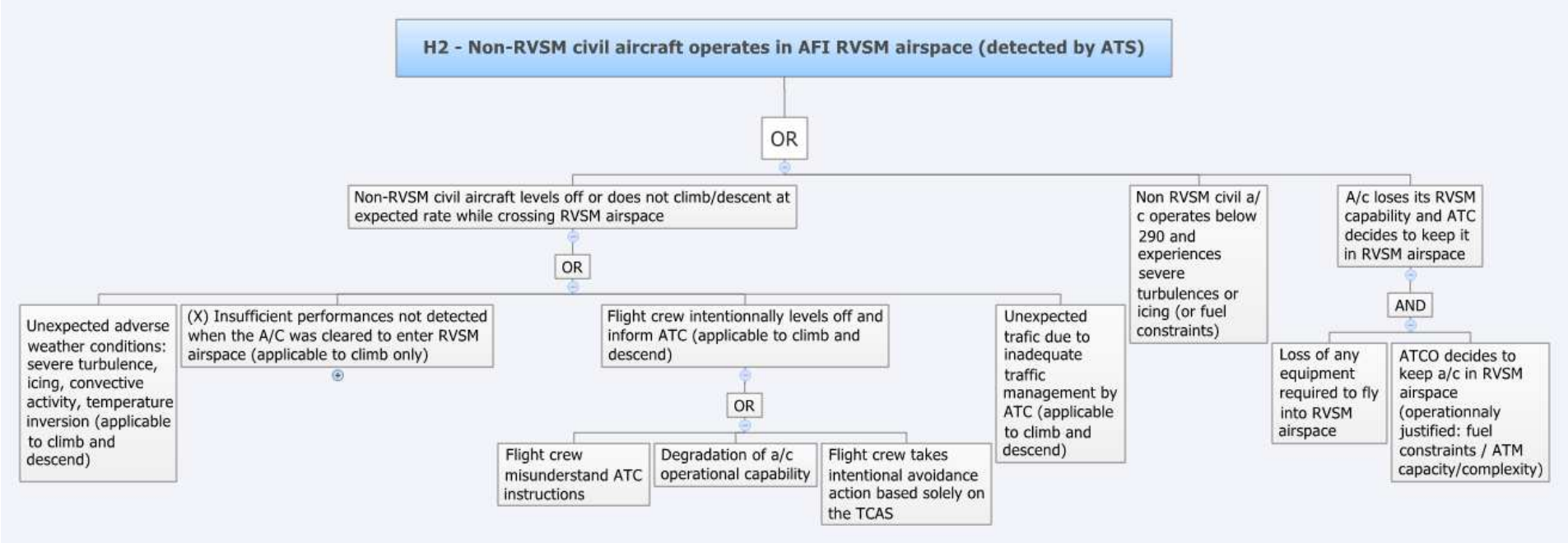

Figure 19 H2 fault tree (1/2)

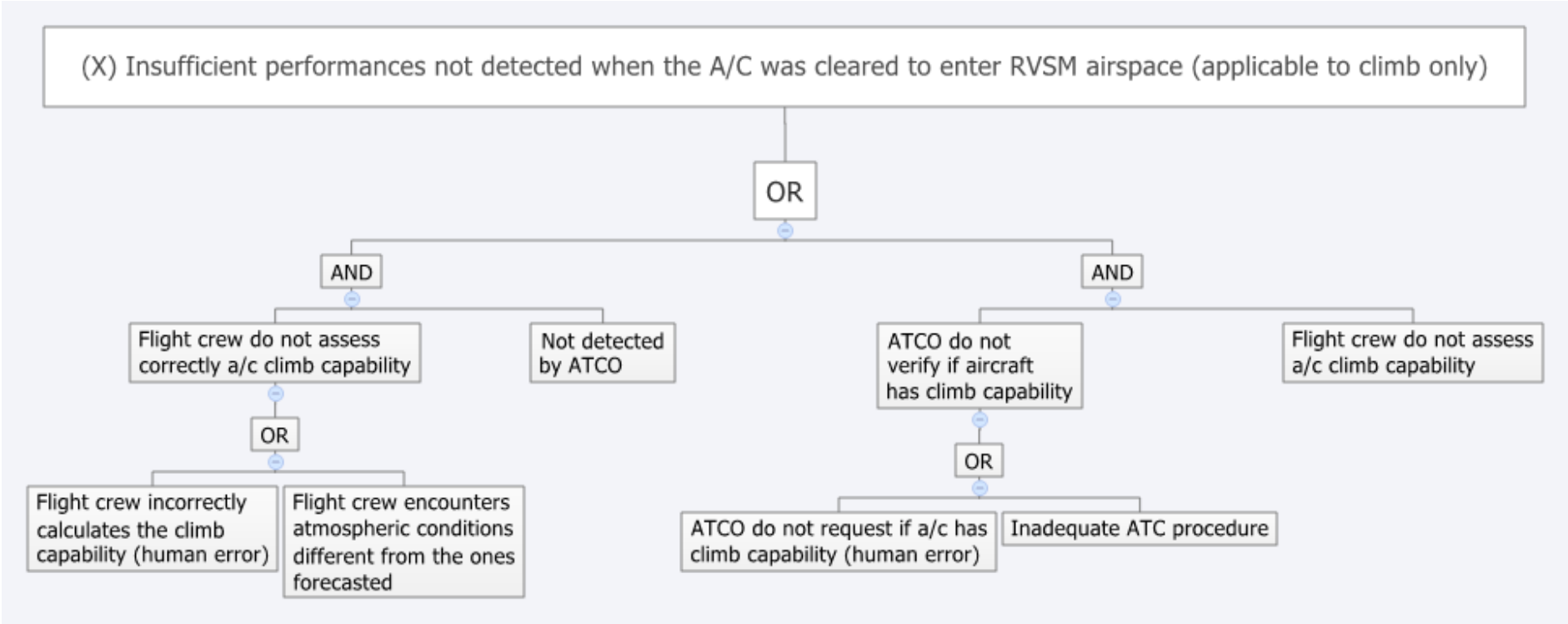

Figure 20 H2 fault tree (2/2)

C.5 Hazard H3

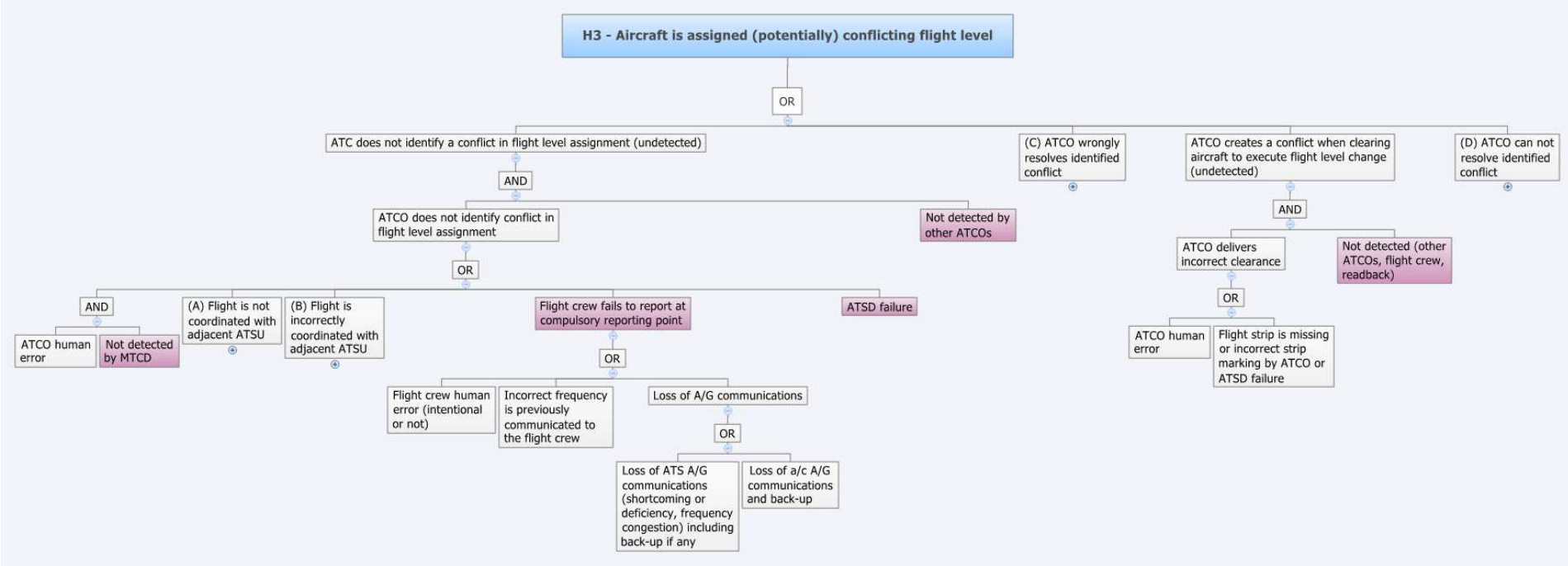

Figure 21 H3 fault tree (1/5)

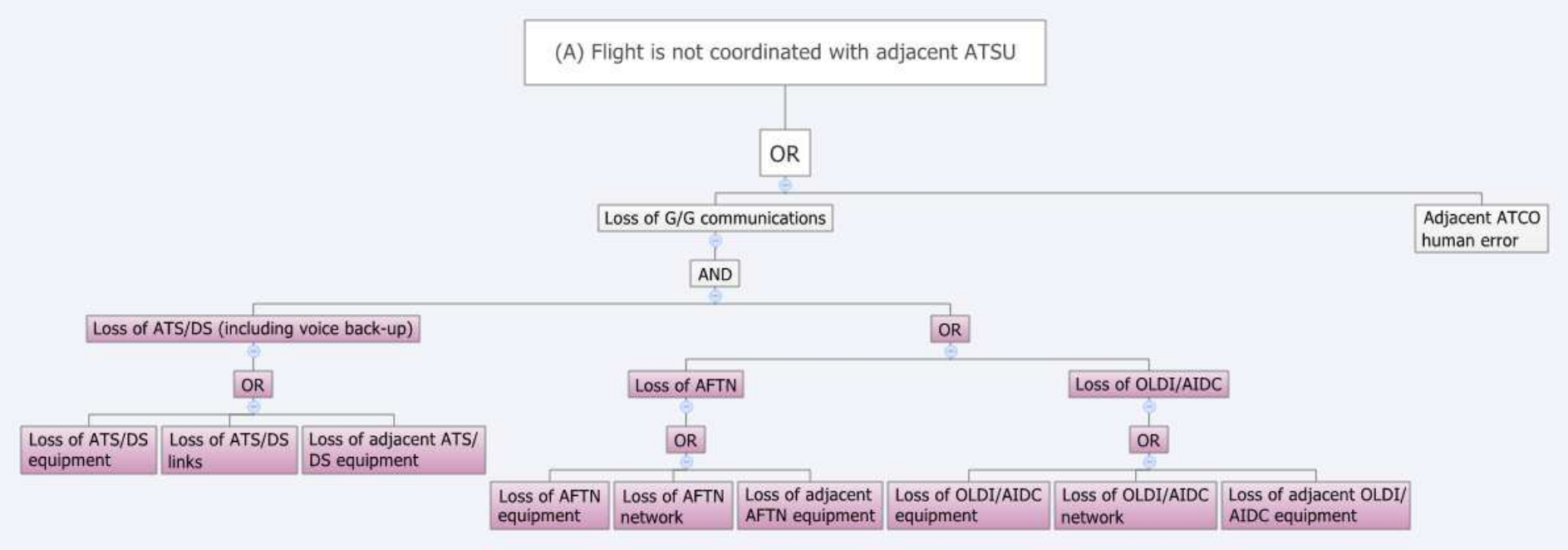

Figure 22 H3 fault tree (2/5)

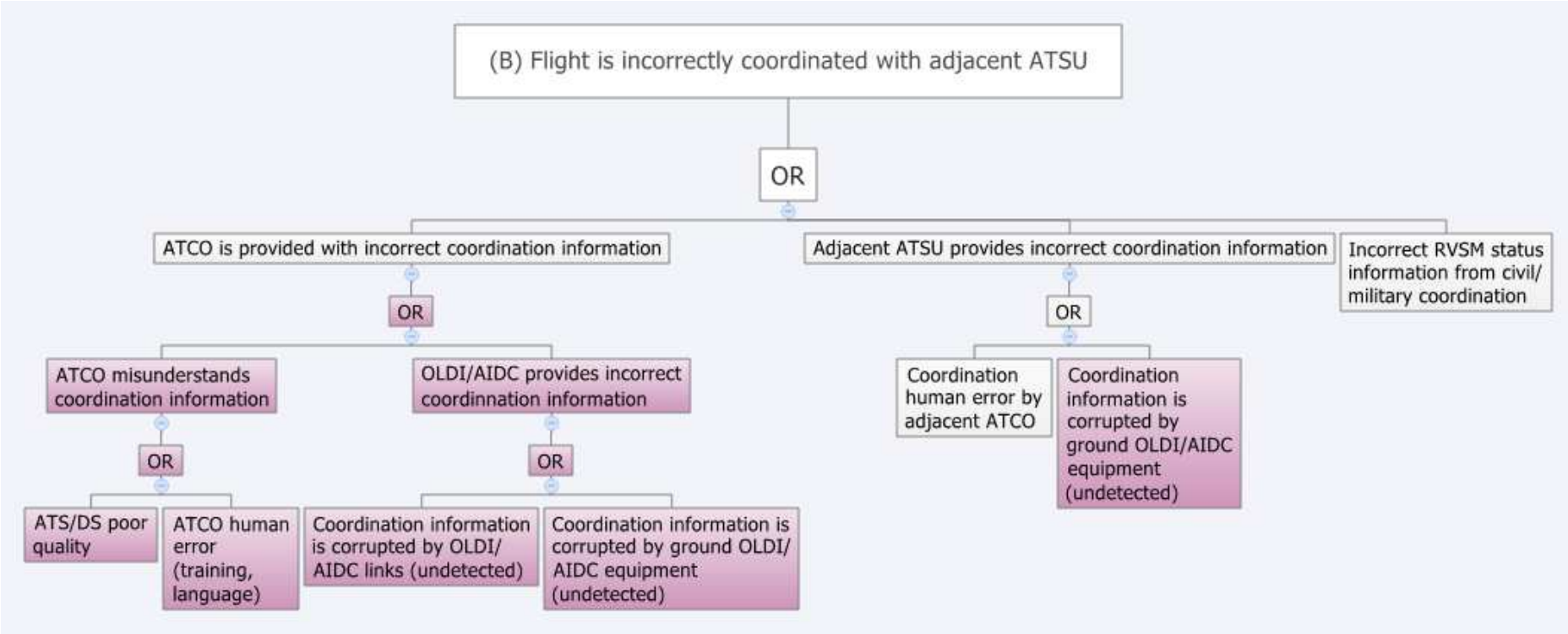

Figure 23 H3 fault tree (3/5)

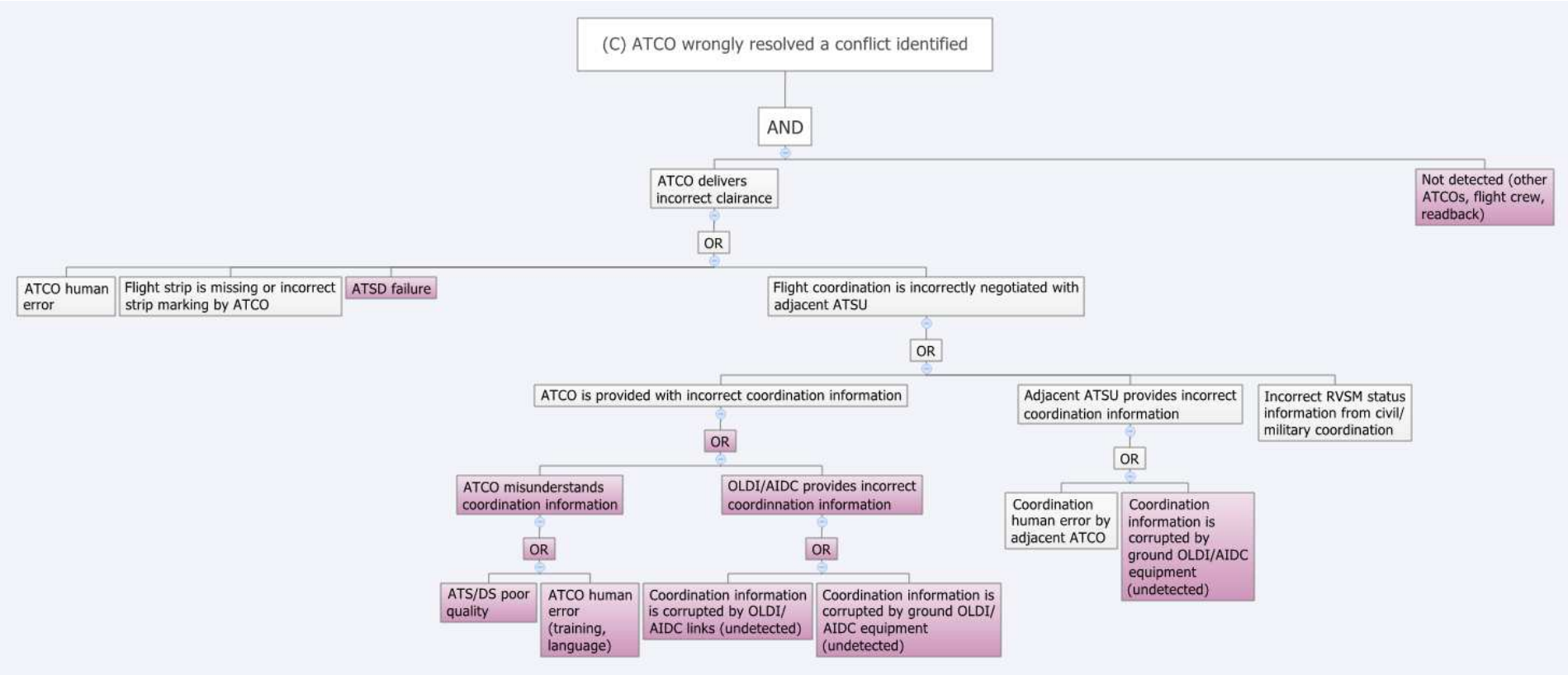

Figure 24 H3 fault tree (4/5)

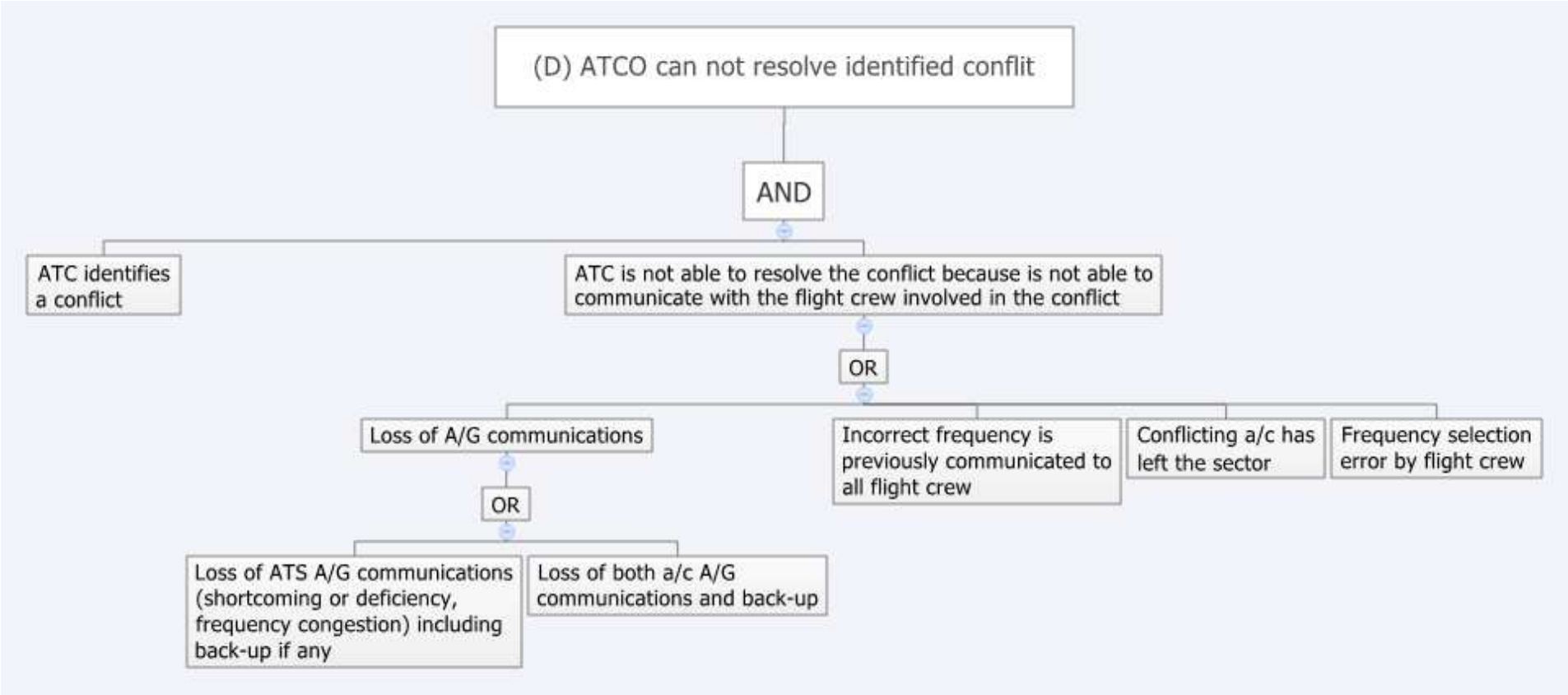

Figure 25 H3 fault tree (5/5)

C.6 Hazard H4a

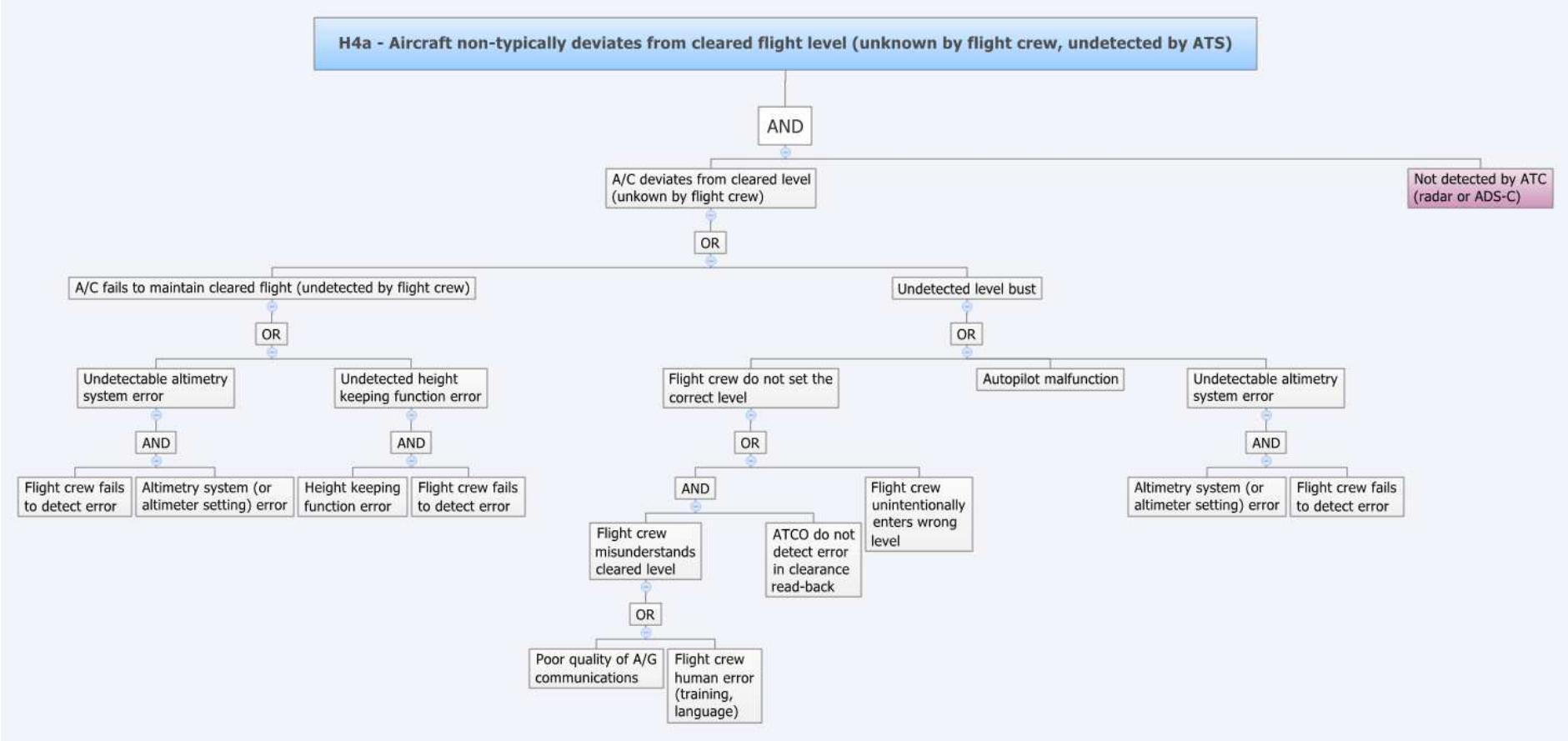

Figure 26 H4a fault tree

C.7 Hazard H4b

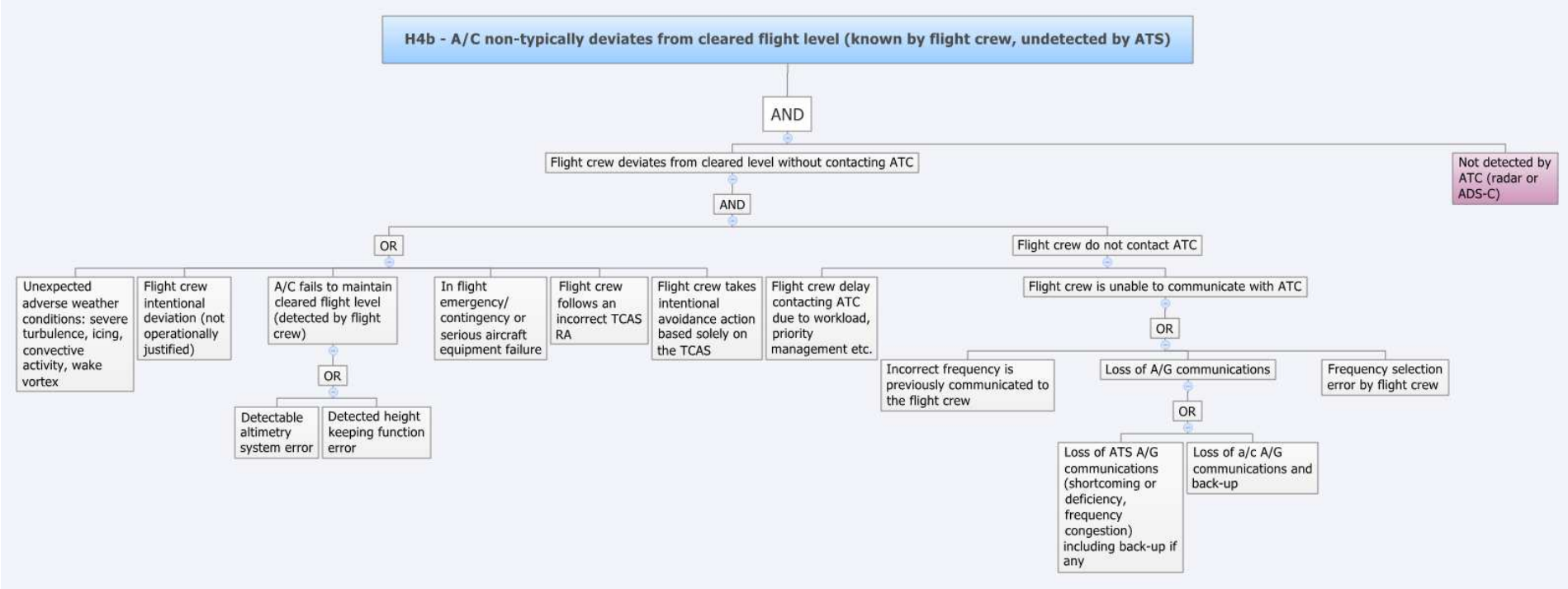

Figure 27 H4b fault tree

Appendix D Events trees

☞ This appendix sets out the event tree technique used as part of the modified methodology framework, and the event trees and the associated assessments made thereof.

D.1 ETA technique

D.1.1 Consequences modelling

For each hazard identified, an event tree is developed to model the possible consequences on the safety of AFI RVSM operations.

An event tree is a graphical and logical model of all the possible outcomes of the hazard, taking into account the available (external) mitigations that may break an accident sequence in the event the hazard occurs. It is a bottom-up deductive technique which allows linking directly the hazard to all the possible consequences in a single model.

An event tree begins at the bottom with a single hazard and its branches are developed to the top. The various paths through the tree:

- reflect whether each mitigation would succeed, fail or not be applicable
- end with the consequence on the safety of operations

The symbology used for the FHA review is described as follows:

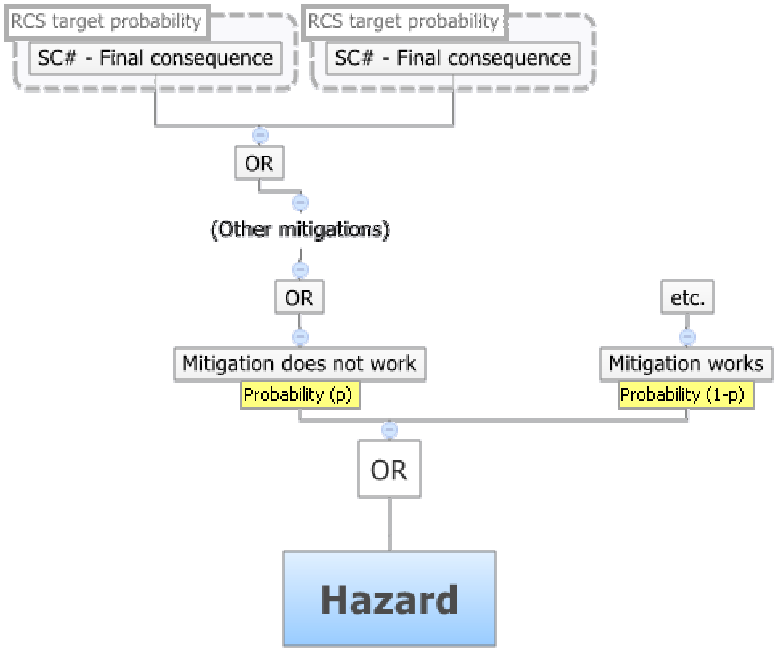

Figure 28 Event tree symbology

The different levels of the tree represent the series of available mitigations and the final consequences at the top on the safety of operations.

The graphical nature aids the qualitative assessment of the final consequences in consistence with the criteria defined in the severity classification scheme (see appendix A.4).

D.1.2 Assessment

A probability may be assigned to show the relative success / failure of the mitigations. That probability is assessed by operational judgment or engineering technique, or is based on the experience according to the available data.

If all the mitigations are assigned a success / failure probability, the event tree technique can be used to specify safety objectives (maximum frequency of occurrence at which hazards are expected to occur). Indeed, if a maximum frequency, at which each of the final consequences is expected to occur, is assigned according to the risk acceptance criteria (see appendix A.5), then a maximum frequency of occurrence can be deduced for the initiating hazard.

Note: In reverse, the event tree technique also allows, if a frequency of occurrence is assigned to the initiating hazard, to deduce the frequency of occurrence of each of the final consequences. This possibility has not been explored as part of the FHA review, as the hazard frequency of occurrence can not be accurately assessed as part of FTA (see C.1.2).

D.2 Hazard H1a

D.2.1 Event tree

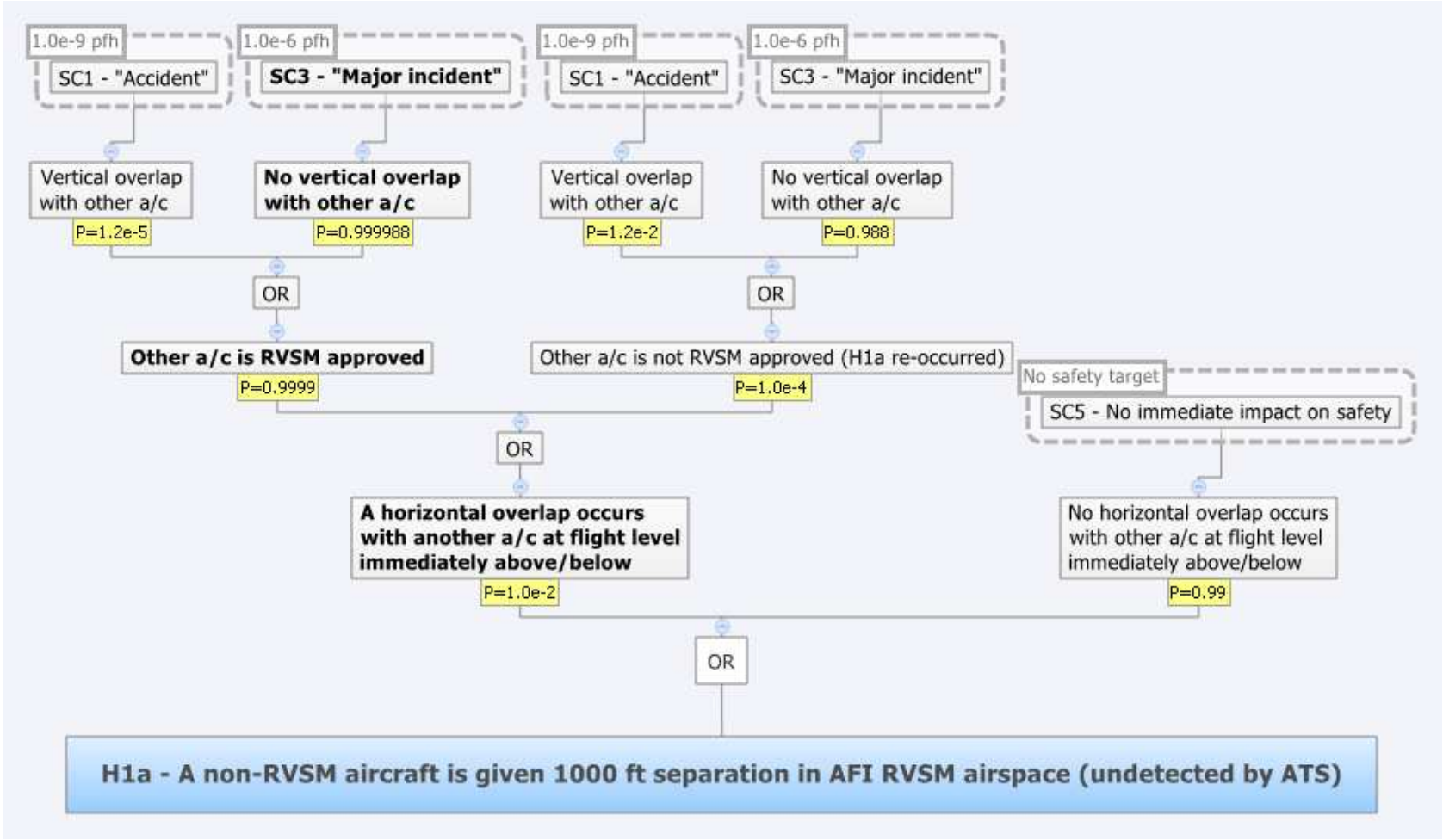

Figure 29 H1a event tree

D.2.2 Assessment

The probabilities assigned to the mitigations presented in section 5.1.1 are as follows:

Mitigation	Failure	Success
No horizontal overlap occurs with other aircraft at flight level immediately above/below.	According to section 2.7 of the CRA (Collision Risk Assessment) [3], the probability of having a horizontal overlap with an aircraft flying at a flight level immediately above or below (total probability taking into account all types of crossing and passing) is approximately $P_y(0)n_x(equiv)=1.0x10^{-2}$.	Probability is one minus the probability of mitigation failure: 0.99
Other aircraft is RVSM	For an a non RVSM aircraft to fly 1000ft below or above another non RVSM aircraft, H1a should occur for both aircraft. Taking as assumption a ratio of 0.1% of non-RVSM flights operating the AFI RVSM airspace and a probability of occurrence of H1a for this second aircraft of $1.0x10^{-1}$, a rough estimation of the probability that this mitigation fails is: $1.0x10^{-4}$.	Probability is one minus the probability of mitigation failure: 0.9999
No vertical overlap between the two aircraft	According to the CRA [3], the probability of vertical overlap for two RVSM aircraft is $1.2x10^{-8}$. Other RVSM safety cases have stated that probability of vertical overlap if only one aircraft is RVSM approved is approximately three orders of magnitude higher than the probability for two approved aircraft: $1.2x10^{-5}$. It is assumed that for two non RVSM aircraft, the same relationship applies: $1.2x10^{-2}$.	Probability is one minus the probability of mitigation failure: 0.999988. Probability is one minus the probability of mitigation failure: 0.988.

Taking into account the probabilities of success or failure of the mitigations, the top-level safety targets (maximum probability assigned to the final consequences according to their assigned severity class) can be derived into maximum expected frequency of occurrence at the hazard level, as follows:

	Safety target	Total Mitigation	Hazard occurrence (pfh)
Horizontal and vertical overlap with RVSM approved aircraft.	SC1: $1.0x10^{-9}$	$1.2x10^{-7}$	$8.3x10^{-3}$
Horizontal overlap only with RVSM approved aircraft.	SC3: $1.0x10^{-6}$	$1.0x10^{-2}$	$1.0x10^{-4}$
Horizontal and vertical overlap with a non-RVSM approved aircraft.	SC1: $1.0x10^{-9}$	$1.2x10^{-8}$	$8.3x10^{-2}$
Horizontal overlap only with non-RVSM approved aircraft	SC3: $1.0x10^{-6}$	$9.9x10^{-7}$	$1.0x10^{0}$

The most stringent constraint is **$1.0x10^{-4}$ occurrence per flight hour per aircraft** or not more than **$2.0x10^{-2}$ occurrence per ATS hour** within the AFI RVSM airspace.

D.3 Hazard H1b

D.3.1 Event tree

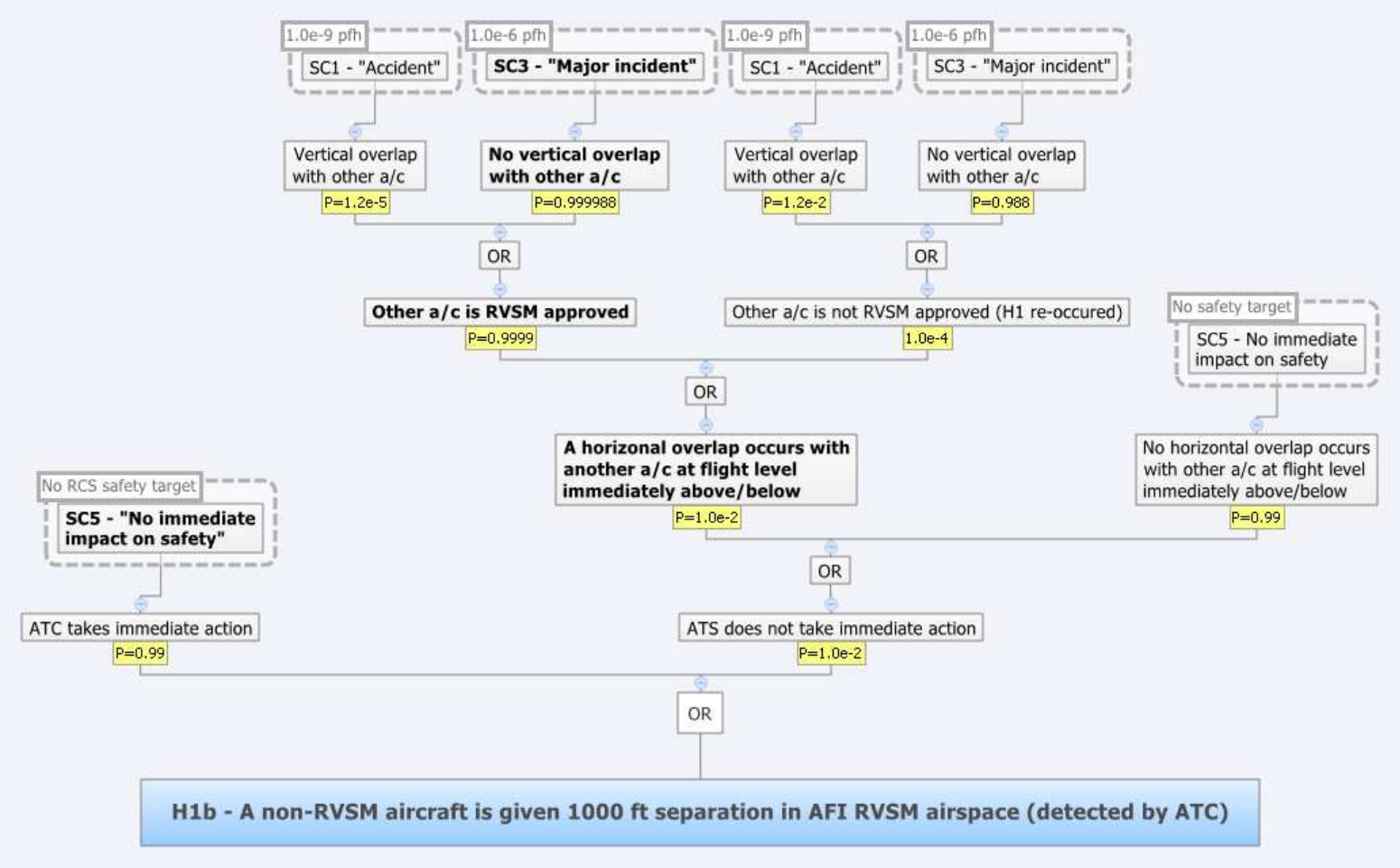

Figure 30 H1b event tree

D.3.2 Assessment

Compared to H1a, one mitigation means is added. This mitigation is assumed to be efficient on a 99% basis, meaning that the probability for this mitigation to fail is $1.00x10^{-2}$.

As a consequence, the derivation of the top-level safety target into the hazards occurrence safety target represents a maximum occurrence probability of **$1.00x10^{-2}$ occurrence per flight hour per aircraft** or **2 occurrences per ATS hour** within the AFI RVSM airspace.

D.4 Hazard H2

D.4.1 Event tree

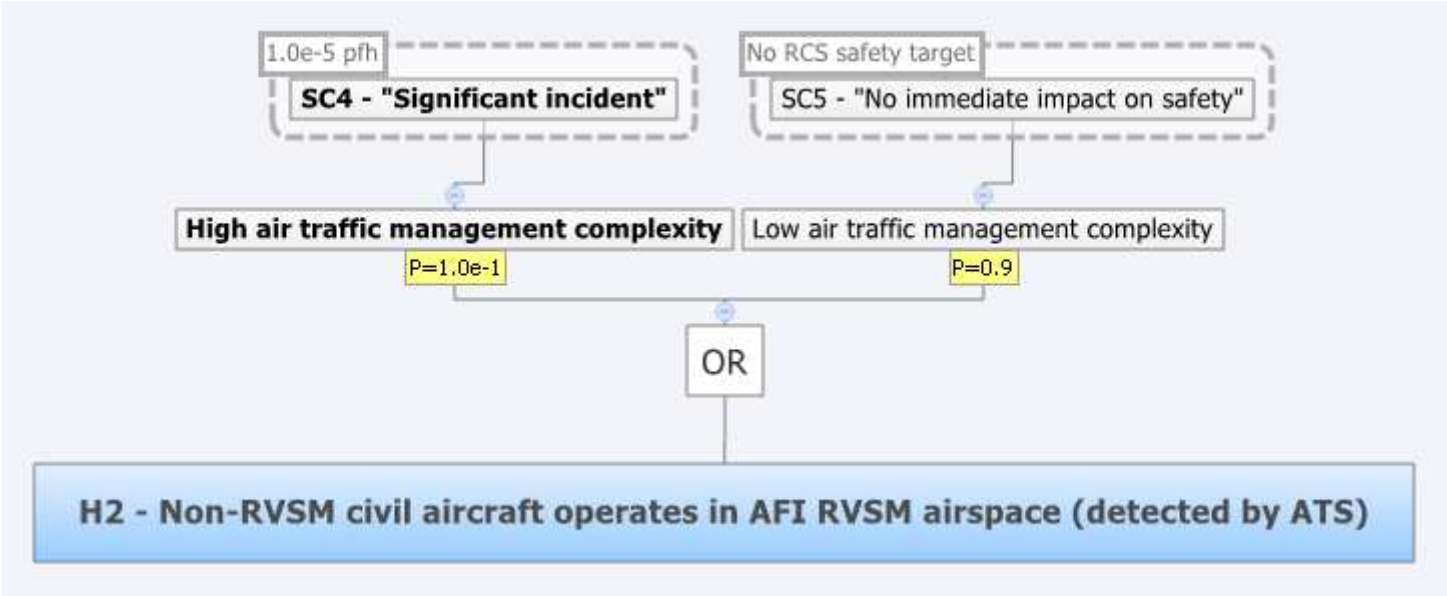

Figure 31 H2 event tree

D.4.2 Assessment

The probabilities assigned to the mitigations presented in section 5.3.1 are as follows:

Mitigation	Failure	Success
The air traffic management complexity is low.	Taking into account the large differences in traffic complexity between the CTA/UTA in the AFI region and the fact that the ATCO will most probably accept non RVSM aircraft only when the air traffic management is not complex, the probability of failure of this mitigation is: $1.0x10^{-1}$.	Probability is one minus the probability of mitigation failure: 0.9

Taking into account the probabilities of success or failure of the mitigations, the top-level safety targets (maximum probability assigned to the final consequences according to their assigned severity class) can be derived into maximum expected frequency of occurrence at the hazard level, as follows:

	Safety target	Total Mitigation	Hazard occurrence (pfh)
High air traffic management complexity.	SC4: $1.0x10^{-5}$	$1.0x10^{-1}$	$1.0x10^{-4}$

Thus the hazard occurrence safety target is equal to the top-level safety target of **$1.0x10^{-4}$ occurrence per flight hour per aircraft** or **$2.0x10^{-2}$ occurrence per ATS hour** within the AFI RVSM airspace.

D.5 Hazard H3

D.5.1 Event tree

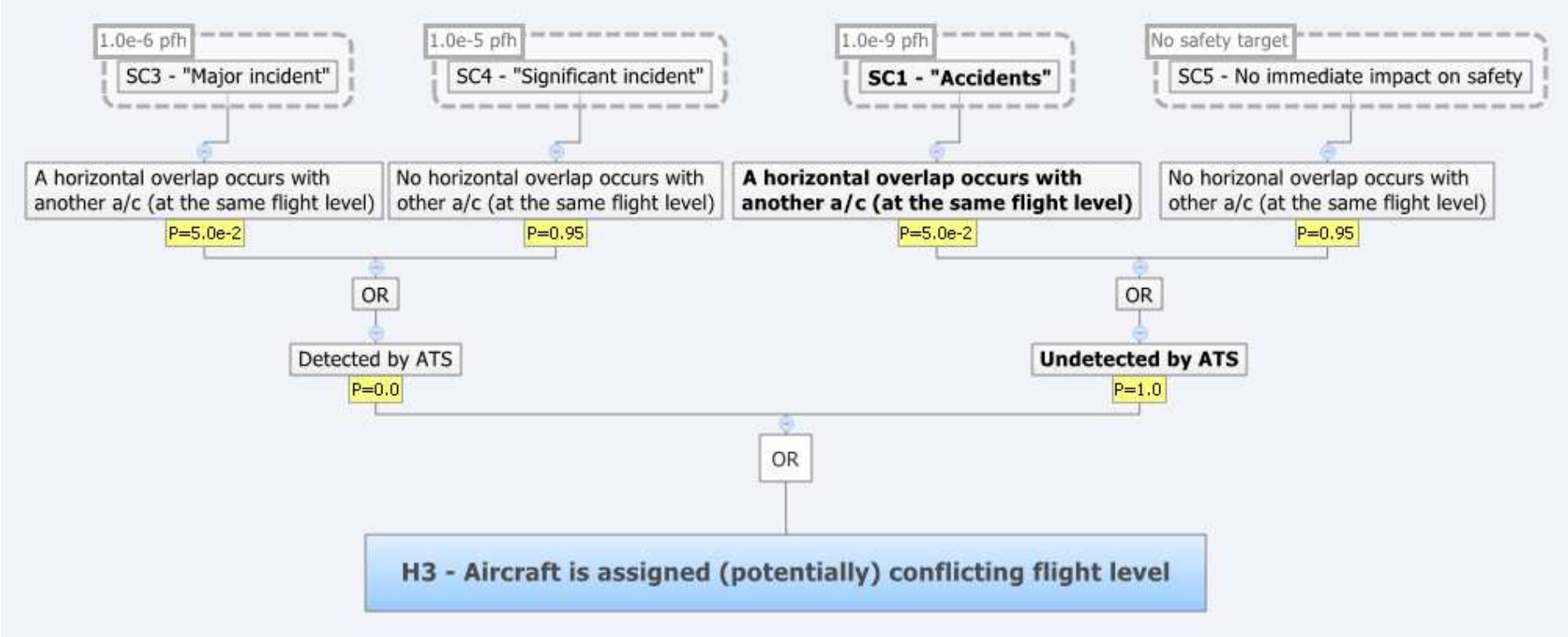

Figure 32 H3 event tree

D.5.2 Assessment

The probabilities assigned to the mitigations presented in section 5.4.1 are as follows:

Mitigation	Failure	Success
No horizontal overlap occurs with other aircraft at the same flight level.	The probability of having a conflicting aircraft on the same flight level can be majored by the probability of having an aircraft at any flight level. It is assumed that the probability of having an aircraft in the horizontal overlap while flying at the same flight level is five times the probability of horizontal overlap for the flight levels immediately above or below: $5.0x10^{-2}$.	Probability is one minus the probability of mitigation failure: 0.95
Detected by ATS	The late detection (of a conflict) is similar to the undetected case as it does not leave sufficient time for the ATCO to react. Moreover, the time to detect is generally very short, as the second aircraft can be immediately above or below. It leaves very few opportunities for all the flight crew and ATCOs to detect the conflict in time. The probability that the ATS does not detect the conflict is thus considered as 0.99.	Probability is one minus the probability of mitigation failure: $1.0x10^{-2}$.

Taking into account the probabilities of success or failure of the mitigations, the top-level safety targets (maximum probability assigned to the final consequences according to their assigned severity class) can be derived into maximum expected frequency of occurrence at the hazard level, as follows:

	Safety target	Total Mitigation	Hazard occurrence (pfh)
Horizontal overlap with undetected	SC1: $1.0x10^{-9}$	$5.0x10^{-2}$	$2.0x10^{-8}$

conflict.			
Horizontal overlap but detected conflict.	SC3: $1.0x10^{-6}$	$5.0x10^{-2}$	$2.0x10^{-5}$
No horizontal overlap but detected.	SC4: $1.0x10^{-5}$	$9.5x10^{-3}$	$1.1x10^{-3}$

The most stringent constraint is **$2.0x10^{-8}$ occurrence per flight hour per aircraft** or **$4.0x10^{-6}$ occurrence per ATS hour** within the AFI RVSM airspace.

D.6 Hazard H4a

D.6.1 Event tree

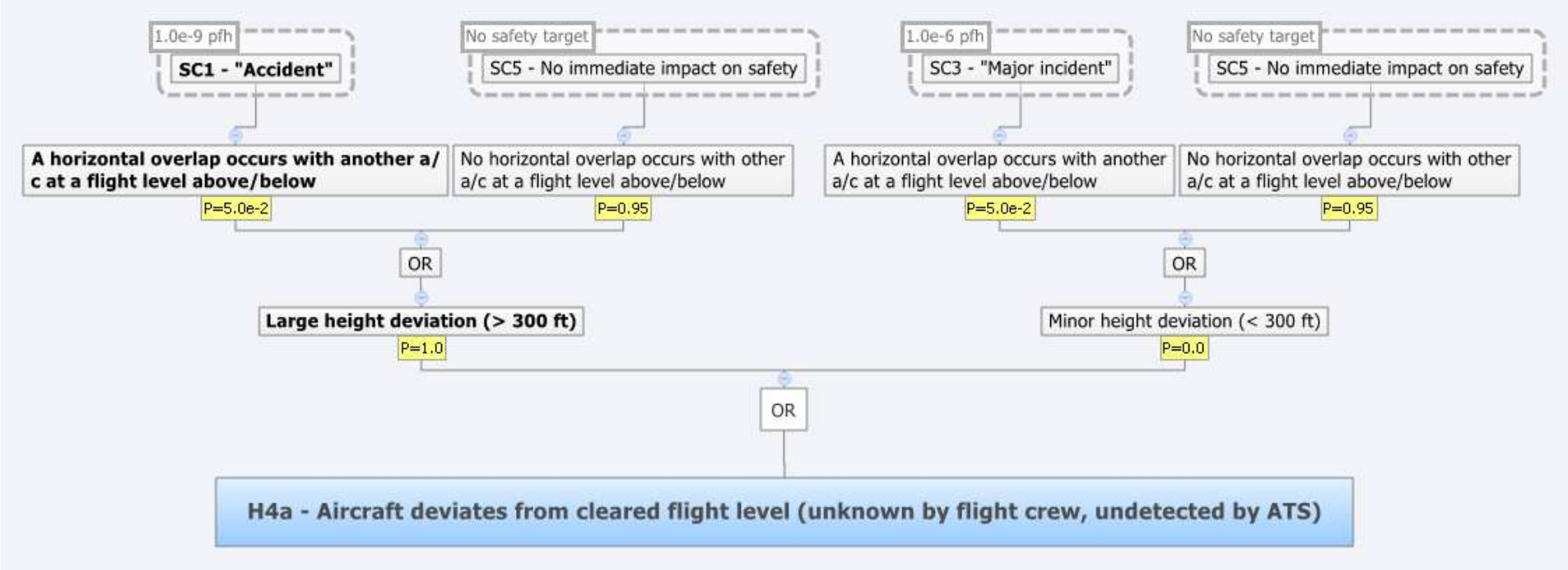

Figure 33 H4a event tree

D.6.2 Assessment

The probabilities assigned to the mitigations presented in section 5.5.1 are as follows:

Mitigation	Failure	Success
No horizontal overlap occurs with other aircraft at the same flight level.	The probability of having a conflicting aircraft on the same flight level can be majored by the probability of having an aircraft at any flight level. It is assumed that the probability of having an aircraft in the horizontal overlap while flying above or below the considered aircraft is five times the probability of horizontal overlap for the flight levels immediately above or below: $5.0x10^{-2}$.	Probability is one minus the probability of mitigation failure: 0.95
Aircraft deviates less than 300 feet.	Considering that the causes leading to less than 300 feet are rare, a conservative assumption is taken: aircraft always deviate more than 300 feet: 1.0.	Probability is one minus the probability of mitigation failure: 0.0.

Taking into account the probabilities of success or failure of the mitigations, the top-level safety targets (maximum probability assigned to the final consequences according to their assigned severity class) can be derived into maximum expected frequency of occurrence at the hazard level, as follows:

	Safety target	Total Mitigation	Hazard occurrence (pfh)
Horizontal overlap with large height deviation.	SC1: $1.0x10^{-9}$	$5.0x10^{-2}$	$2.0x10^{-8}$
Horizontal overlap with minor height deviation.	SC3: $1.0x10^{-6}$	0.0	Not applicable

The most stringent constraint is **2.0×10^{-8} occurrence per flight hour per aircraft** or **4.0×10^{-6} occurrence per ATS hour** within the AFI RVSM airspace.

D.7 Hazard H4b

D.7.1 Event tree

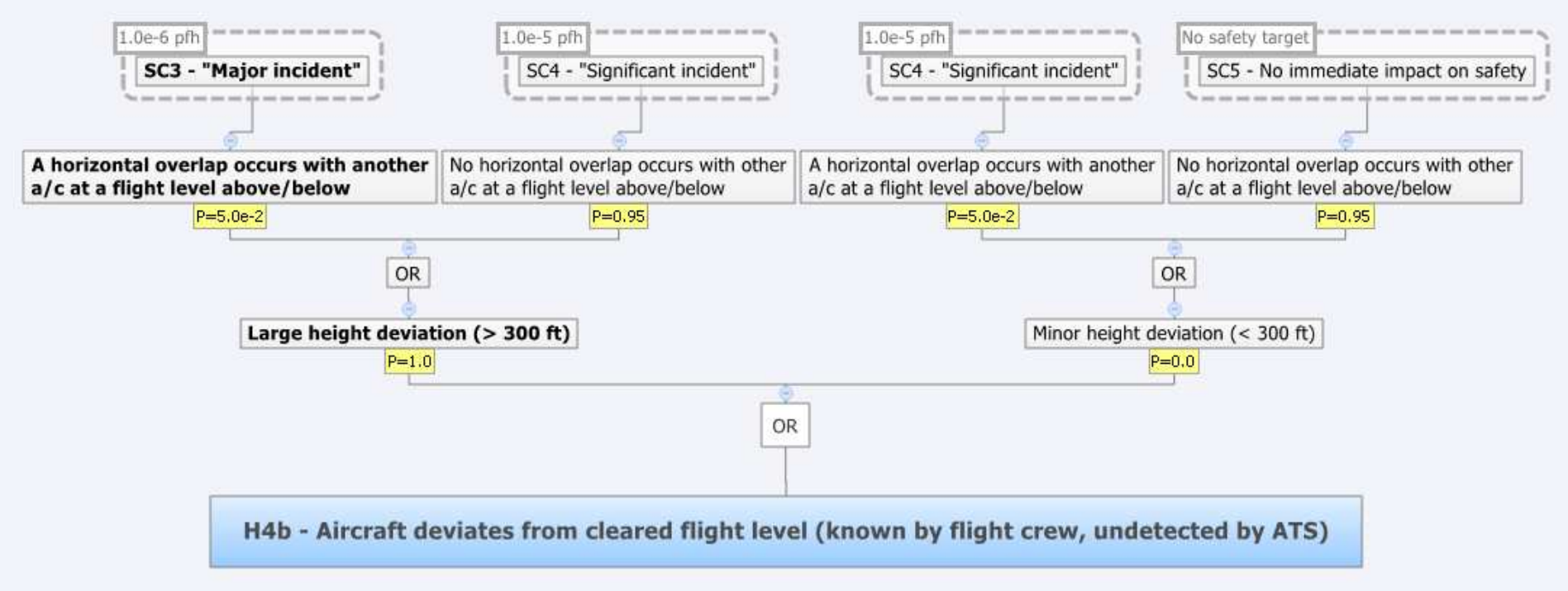

Figure 34 H4b event tree

D.7.2 Assessment

The probabilities assigned to the mitigations presented in section 5.4.1 are as follows:

Mitigation	Failure	Success
No horizontal overlap occurs with other aircraft at the same flight level.	The probability of having a conflicting aircraft on the same flight level can be majored by the probability of having an aircraft at any flight level: $5.0x10^{-2}$.	Probability is one minus the probability of mitigation failure: 0.95
Aircraft deviates less than 300 feet.	Considering that the causes leading to less than 300 feet are rare, a conservative assumption is taken aircraft always deviate more than 300 feet: 1.0.	Probability is one minus the probability of mitigation failure: 0.0.

Taking into account the probabilities of success or failure of the mitigations, the top-level safety targets (maximum probability assigned to the final consequences according to their assigned severity class) can be derived into maximum expected frequency of occurrence at the hazard level, as follows:

	Safety target	Total Mitigation	Hazard occurrence (pfh)
Horizontal overlap with large height deviation.	SC3: $1.0x10^{-6}$	$5.0x10^{-2}$	$2.0x10^{-5}$
No horizontal overlap with large height deviation.	SC4: $1.0x10^{-5}$	$9.5x10^{-1}$	$1.0x10^{-5}$
Horizontal overlap with minor height deviation.	SC4: $1.0x10^{-5}$	0.0	Not applicable

The most stringent constraint is **$1.0x10^{-5}$ occurrence per flight hour per aircraft** or **$2.0x10^{-3}$ occurrence per ATS hour** within the AFI RVSM airspace.

D.8 Assumptions

The assessment made in the previous sections is based on the following assumptions:

Hazard	Assumption
H1	0.1% of the flights operating the AFI RVSM airspace are non-RVSM approved.
H1	The probability of vertical overlap between two non-RVSM aircraft flying at 1000ft vertical separation is three orders of magnitude the same probability for a non-RVSM aircraft and an RVSM aircraft. This is further three orders of magnitude the probability for two RVSM aircraft.
H3	The probability of having an aircraft in the horizontal overlap while flying at the same flight level is five times the probability of horizontal overlap for the flight levels immediately above or below.
H4	The probability of having an aircraft in the horizontal overlap while flying above or below the considered aircraft is five times the probability of horizontal overlap for the flight levels immediately above or below.

It is to be noted that some of the results are very sensitive to these assumptions.

Appendix E Examination of the reported safety occurrences

☞ This appendix provides an examination of the safety occurrences reported in the AFI Region, in support of the assessment of the AFI RVSM risks (section 6), through an initial estimation of the frequency of occurrence of the AFI RVSM hazards (over the time period September 2008 - September 2009), which aims to be completed by operational expert judgment.

E.1 Reported safety occurrences

The reported safety occurrences examined for the purpose of the FHA review have been provided by three mechanisms operated in the AFI Region, namely the AFI ATS Incident Analysis Working Group (AIAG), the AFI Tactical Action Group (TAG) and the AFI Regional Monitoring Agency (ARMA).

E.1.1 AIAG data

The AIAG [13] provides a forum to various aviation organisations of the AFI Region. As a core of the AIAG are IATA, ICAO, IFALPA and IFATCA. Its mandate is to review on an annual basis all the ATS incident reports available to the group, from any source, with a view to identifying causes, trends, and remedial actions that may prevent re-occurrence. IATA SO&I AFI is responsible for updating and maintaining the incident database, compiling the incident reports and for managing the annual meetings.

The AIAG reports examined for this FHA review have been provided by IATA SO&I AFI and include, for the time period 25 September 2008 - 30 June 2009, two types of reports, namely the ATS incident reports (cf.[14] [15] and the ATS irregularity reports [16][17]. Main of them has not yet been investigated according to the AIAG methodology [x] as the next annual meeting is to come in March 2010. As a consequence, those reports only contain the description of the event as perceived by the reporter and, when available, the feedback from the concerned ANSPs. The information is thus sometimes limited. Therefore, some of the reports can not be used to support the pursued initial estimation of the frequency of occurrence.

E.1.2 AFI TAG data

The TAG [13] is a multidisciplinary group established under the authority of the special AFI RAN of 2008 [12] and made up of aviation technical experts from various aviation operational, technical, statistical and other fields as needed. The purpose of the TAG is to improve operational safety in the AFI RVSM airspace by addressing identified problems in the AFI air navigation system on a tactical, short-term basis. This includes the collection, compilation, discussion, classification, and directed action in relation to Unsatisfactory Condition Reports (UCR) that are received from system users, ANSP, pilots, air traffic controllers and or the public. UCRs may be related to unsatisfactory conditions in the areas of communication, navigation and surveillance, as well as in the provision of air traffic control services at or above FL290.

The UCRs examined for this FHA review have been provided by TAG secretariat and include, only for the time period 01 January - 30 September 2009, two types of UCR, namely the “new” UCRs [18] and the “resolved” UCRs [19]. Like the AIAG incidents, these UCR reports include the description the event as perceived by the reporter and, when available, the feedback from the concerned ANSPs. The available information is sometimes limited.

The TAG works in close coordination with the ARMA in the discharge of its duties and TAG members are active in the AIAG to avoid duplication of work between the two groups. Nevertheless, a given safety occurrence can be addressed in the two groups as their mandate are different. This leads to an important part of the provided “new” and “resolved” UCRs which cover safety occurrences also addressed in the AIAG reports.

E.1.3 ARMA form 1

One of the responsibilities of the AFI Regional Monitoring Agency is to monitor aircraft height-keeping performance and the occurrence of large height deviations. All height deviations of 300 ft or more shall be reported using ARMA form 1 as stated in conclusion 3/4 of the RVSM/RNAV/RNP/TF/3 meeting [21]. The reported height deviations are detailed in the UCRs described here above.

The forms examined for this FHA review cover the first year of RVSM operations: from the 25th of September 2008 to the 25th of September 2009 [20].

E.2 Approach

In relation to the main aim of the examination, the approach comprises two stages:

- Mapping the reported safety occurrences with the AFI RVSM hazard model

  This stage consists in analysing the AIAG ATS incident reports and the TAG UCRs to identify those for which the described operational facts correspond to an occurrence of the AFI RVSM hazards, as described in section 3, or at a lesser extent to an occurrence of their primary causes or consequences.

  As a result of that analysis, the safety occurrences are classified according to the following categories:

  - "Not classified"

    Safety occurrences not related to the AFI RVSM airspace or to a vertical separation issue (e.g. horizontal conflicts of aircraft flying at the cleared flight level and not vertically evolving, unidentified traffic).

  - "Undetermined"

    Safety occurrences for which available information, especially about the underlying causes, is not sufficient to conclude which AFI RVSM hazards have occurred.

  - "Mapped"

    Safety occurrences for which available information is sufficient to conclude which AFI RVSM hazards have occurred.

  - "N/A" (specific to H3 related occurrences)

    Safety occurrences related to a conflict detected and resolved in time which are not mapped to H3 for the estimation of the frequency of occurrence, as only the associated safety objective directly related to the undetected case (see Appendix D.5.1)

- Initial estimation of the AFI RVSM hazards' frequency of occurrence

  This stage consists in counting the number of occurrences that can be assigned to the AFI RVSM hazards, and to deduce their "reported" frequency of occurrence (see Appendix A.5)

This approach is limited to the AIAG ATS incident reports and to the TAG 'exclusive'[7] UCRs which do not overlap with the AIAG incidents. Indeed:

- ARMA form 1 data are contained within AIAG and TAG UCR data.
- AIAG ATS irregularities do not correspond to events described at the boundary of the AFI RVSM system and therefore can not be mapped with the AFI RVSM hazards. They refer to lower-level events which can be occurrences of the hazards' causes which were not propagated to the system level thanks to successful internal mitigations or pure chance.

[7] Those which are not also addressed as part of AIAG ATS incidents

However, an examination of the AIAG ATS irregularities is made in order to identify some of the latent failures within the AFI RVSM system that may lead in the future to an increase of the number of occurrences of the AFI RVSM hazards (and consequently of the risks arising from these hazards).

E.3 Mapping with AFI RVSM hazard model

This analysis of the safety occurrences has lead to the following classification:

Type	Not classified	Undetermined	Mapped
AIAG ATS incidents	16	14	8: 4 (H3), 1 (H4a), 3 (H4b)
TAG UCRs[8]	Unknown[9]	Unknown[10]	3: 2 (H4a), 1 (H4b)

Table 26: AIAG ATS incidents and TAG UCRs classification

The analysis carried out for the classified (i.e. undetermined or mapped) AIAG ATS incidents is a follows:

Reference	Description	Classification
1175	The conflict described in this report was detected.	N/A
1183	The conflict described in this report was detected.	N/A
1188	This airprox concern an unidentified traffic and is thus not RVSM specific.	Unclassified
1191	This airprox did not involve a vertically evolving aircraft (causes are Lack of coordination and human error in conflict detection).	Unclassified
1192	There was no vertical risk for this report.	Unclassified
1193	The causes of this airprox are not defined (ATC or Flight crew error) and cannot be accurately mapped to one of the identified hazards.	Undetermined

[8] Only those which are not also addressed in the AIAG ATS incidents
[9] For practical reasons, only well documented UCR reports not already counted in the AIAG incidents concerning AIRPROX and height deviations have been more deeply analysed among the 97 UCRs. Thus, an accurate number of “Not classified” and “Undetermined” UCRs can not be provided.
[10] See note 9.

Reference	Description	Classification
1195	This airprox is due to an aircraft deviating from cleared flight level: the flight crew did not contact the ATC but climbed without clearance.	Mapped with H4b
1196	This airprox is due to an aircraft deviating from cleared flight level: the flight crew did not contact the ATC but climbed without clearance.	Mapped with H4b
1198	This is a report on a TCAS RA due to vertical speed. It is considered a nuisance TCAS alert. No other detail is provided to allow an accurate mapping.	Undetermined
1199	This airprox did not involve a vertically evolving aircraft.	Unclassified
1200	This airprox is due to an aircraft deviating from cleared flight level and not being detected by flight crew.	Mapped with H4a
1201	The causes of this airprox are not defined (ATC or Flight crew error) and cannot be accurately mapped to one of the identified hazards.	Undetermined
1203	This airprox did not involve a vertically evolving aircraft (primary cause is Lack of coordination).	Unclassified
1204	The causes of this airprox are not defined (ATC or Flight crew error) and cannot be accurately mapped to one of the identified hazards.	Undetermined
1212	The causes of this airprox are not defined (ATC or Flight crew error) and cannot be accurately mapped to one of the identified hazards.	Undetermined
1250	This airprox did not involve a vertically evolving aircraft.	Unclassified
1251	The conflict described in this report was detected.	N/A
1252	The conflict described in this report was detected.	N/A
1253	The conflict described in this report was detected.	N/A
1254	This airprox did not involve a vertically evolving aircraft.	Unclassified
1255	This airprox did not involve a vertically evolving aircraft.	Unclassified
1257	This airprox is due to the ATC assigning a potentially conflicting flight level due to ATCO human error.	Mapped with H3
1259	The causes of this airprox are not defined (ATC or Flight crew error) and cannot be accurately mapped to one of the identified hazards.	Undetermined
1260	This airprox did not involve a vertically evolving aircraft.	Unclassified

Reference	Description	Classification
1264	This airprox did not involve a vertically evolving aircraft.	Unclassified
1266	This airprox is due to the ATC assigning a potentially conflicting flight level due to ATCO human error (non standard flight level).	Mapped with H3
1268	The conflict described in this report was detected.	N/A
1269	This is a report on a TCAS RA due to vertical speed. It is considered a nuisance TCAS alert. No other detail is provided to allow an accurate mapping.	Undetermined
1271	This airprox is due to the ATC assigning a potentially conflicting flight level due to ATCO human error.	Mapped with H3
1273	The conflict described in this report was detected.	N/A
1275	This airprox is due to the ATC assigning a potentially conflicting flight level due to Lack of coordination and read back attention.	Mapped with H3
1276	The causes of this airprox are not defined (ATC or Flight crew error) and cannot be accurately mapped to one of the identified hazards.	Undetermined
1277	The conflict described in this report was detected.	N/A
1278	The conflict described in this report was detected.	N/A
1279	This airprox did not involve a vertically evolving aircraft.	Unclassified
1282	This airprox did not involve a vertically evolving aircraft.	Unclassified
1283	The causes of this airprox are not defined (ATC or Flight crew error) and cannot be accurately mapped to one of the identified hazards.	Undetermined
1286	The conflict described in this report was detected.	N/A
1288	The conflict described in this report was detected.	N/A
1289	This is a report on a TCAS RA due to vertical speed. It is considered a nuisance TCAS alert. No other detail is provided to allow an accurate mapping.	Undetermined
1290	The conflict described in this report was detected.	N/A
1292	This airprox did not involve a vertically evolving aircraft.	Unclassified
1296	This is a report on a TCAS RA due to vertical speed. It is considered a nuisance TCAS alert. No other detail is provided to allow an accurate mapping.	Undetermined

Reference	Description	Classification
1297	This airprox did not involve a vertically evolving aircraft.	Unclassified
1298	The causes of this airprox are not defined (ATC or Flight crew error) and cannot be accurately mapped to one of the identified hazards.	Undetermined
1301	This airprox is due to an aircraft deviating from cleared flight level detected by fight crew, due to a high vertical speed and to A/C performance that did not allow compliance with ATC clearance.	Mapped with H4b
1303	The causes of this airprox are not defined (ATC or Flight crew error) and cannot be accurately mapped to one of the identified hazards.	Undetermined
1304	This airprox did not involve a vertically evolving aircraft.	Unclassified
1306	This airprox did not involve a vertically evolving aircraft.	Unclassified
1307	The causes of this airprox are not defined (ATC or Flight crew error) and cannot be accurately mapped to one of the identified hazards.	Undetermined
1312	The conflict described in this report was detected.	N/A

Table 27: Analysis of AIAG ATS incidents

The analysis carried out for the classified (i.e. mapped) TAG UCRs is a follows:

Reference	Description	Classification
78	This airprox is due to an aircraft deviating from cleared flight level and not being detected by flight crew.	Mapped with H4a
90	This airprox is due to an aircraft deviating from cleared flight level. Although there are few information on the reason of the deviation, it seems to be known by the flight crew.	Mapped with H4b
225	This airprox is due to an aircraft deviating from cleared flight level and not being detected by flight crew.	Mapped with H4a

Table 28: Analysis of TAG UCRs

E.4 Initial estimation of frequency of occurrence

On the basis of the safety occurrences mapped with the AFI RVSM hazards, the deduced "reported" frequencies of occurrence are estimated as follows:

Hazard	Nb. of mapped occurrences	"Reported" frequency of occurrence
H1a	No mapped occurrence	Not possible to estimate
H1b	No mapped occurrence	Not possible to estimate
H2	No mapped occurrence	Not possible to estimate
H3	≥ 4 occurrences (AIAG 1257, 1266, 1271, 1275)	≥ 4.5×10^{-4} / h
H4a	≥ 3 occurrences (AIAG 1200 UCR 78, 225)	≥ 3.4×10^{-4} / h
H4b	≥ 4 occurrences (AIAG 1195, 1196, 1301 UCR 90)	≥ 4.5×10^{-4} / h

Table 29: Estimation of "reported" frequency of occurrence

No occurrence was mapped with H1a, H1b and H2, mainly due to limited information. The analysis of the TAG UCRs (including ARMA form 1 related) shows that non-RVSM aircraft flying in the AFI RVSM airspace were involved in safety occurrences. However, due to a lack of information (e.g. the applied separation minima), it was not possible to assign those safety occurrences to any of H1a, H1b and H2. It can be concluded that these hazards occurred in the AFI RVSM airspace but it is not possible to estimate in which extent.

The "reported" frequencies of occurrence estimated for H3, H4a and H4b are lower bounds as:

- Safety occurrences in the AFI region (like in any other region) are underreported as shown by a close examination of the data reported to the ARMA
- Analysed safety occurrences does not cover the entire September 2008 - September 2009 time period
- Analysed safety occurrences classified as undetermined due to limited information can be occurrences of the AFI RVSM hazards

These factors are taken into account when completing the estimated by operational expert judgment (cf. section 6)

E.5 AFI RVSM system latent failures

The examination of the AIAG ATS irregularities has shown the following failures dormant within the AFI RVSM system:

- Loss of A/G communications, mainly due to wave propagation constraints in conjunction with unreliable A/G ATS communication infrastructure (subject of 125 irregularity reports over 217 during the first semester of 2009, leading to a frequency of occurrence greater than once every two days): this can potentially generate occurrences of the hazards H1a, H3 and H4b.
- Incorrect and lack of ATS coordination, either due to human errors, procedures or G/G communications capabilities: this can potentially generate occurrences of the hazards H1a, H1b and H3
- Lack of flight crew discipline: this can potentially generate occurrences of the hazards H3 and H4b
- Presence of non-RVSM aircraft in the AFI RVSM airspace; this can potentially generate occurrences of the hazards H1a, H1b and H2.

Those latent issues shall be appropriately addressed in order to avoid a significant increase of the AFI RVSM risks in the future. They are subject of safety recommendations (cf. section 1).

Appendix F AFI RVSM risk mitigation strategy

☞ This appendix sets out how the AFI RVSM risk mitigation strategy is derived in the form of System Element Requirements (SERs)

The specification of the SER is based on the principle that their realisation shall ensure the implementation and the efficiency of the considered mitigation. The requirements are determined on a cause by cause basis. They address the factors which can be used to prevent the occurrence of the AFI RVSM hazards if the cause occurs.

The table below provides the set of SERs for each of the causes modelled in the fault trees (cf. Appendix C). These requirements can be of two types:

- Requirements already developed before implementation.

  Such requirements were already developed in the PISC (see [4], Appendix C). As a result of the FHA review, they are validated/confirmed in light of the operational experience. In some cases, they can be reworded for clarification or highlight of a particular issue raised during the FHA review, but without modifying the initial meaning.

  These requirements are referenced in the same way than in the PISC. The previous FHA mitigations to which they were derived from are shown in the comment column.

- 'New' requirements resulting from the operational experience.

  Such requirements were not developed in the PISC. As a result of the FHA review, either they address the new issues that had risen since the implementation or they result from the FTA technique by which a number of causes and mitigations of hazards have emerged that were not explicitly revealed in the previous FHA.

  These requirements are referred using the same rule as in the PISC, except that for clarity "new" is indicated as a prefix[11]. The rationale for such requirements, in the light of the operational experience, is provided in the comment column.

It should be noted that some of the causes modelled in the fault trees do not result in a set of requirements. If so, the rationale is provided in the comment column.

[11] Such indication is specific to the present report and will not be used in the subsequent use of the requirements in the POSC document.

Cause	Hazard	System Element Requirements	Comment
RVSM approval related causes			
A/C complies with MASPS but is not State approved or the Operator is not State approved	H1a, H1b	None	Cause addressed through RVSM1 “Only RVSM approved aircraft shall be cleared into AFI RVSM airspace” As set out in the PISC [4], RVSM1 is a high-level safety requirement representing a fundamental requirement of the AFI RVSM Concept and does not directly relate to the system integrity. In the PISC, State RVSM approvals was addressed as an implementation issue (see [4], §5.3.1.3). Evidence of State’s capabilities and diligence with respect to those approvals was provided in the National Safety Plan. The experience reported to ARMA shows a gap between the NSP commitments and the reality. This leads to the need for recommending reinforcement of States’ capabilities and diligence with regards to operator and aircraft RVSM approval.
Operator related causes			
Operator flight planning error in FPL or in RPL	H1a, H1b	FCOP2: Flight planning procedures shall be revised and reinforced for RVSM FCOT2: Operator and flight crew shall be appropriately trained with regards to flight planning procedures revised for RVSM operations ACOE_1-6: Operator flight plan filling capabilities shall be reinforced	These requirements developed in the PISC (from Req_{Core}_58 and Req_{Core}_59 of the previous FHA) are confirmed.
Operator does not send CHG message	H1a, H1b	FCOP_2-3: Operator shall send CHG message when appropriate FCOT_2-1: Operator staff shall be trained to send CHG message when appropriate ACOE_1-5: Operator equipment to send CHG message when appropriate shall be in place	These requirements developed in the PISC (from Req_{Core}_57 of the previous FHA) are confirmed.

Cause	Hazard	System Element Requirements	Comment
Flight crew related causes			
Flight crew misunderstand ATC instructions	H2, H4	FCOP_1-1: Flight Crew procedures for read back shall be reinforced ATSP_1-1: ATS procedures for read back shall be reinforced	Clearance exchange function is not impacted by RVSM, except that errors have more severe effects. Thus, only requirements on the reinforcement of the readback procedure apply (training in that regard is considered as a pre-requisite to RVSM). These requirements developed in the PISC (from Req_{Core}_29 of the previous FHA) are confirmed.
Flight crew wrongly identifies the aircraft as RVSM capable	H1a	FCOP_1-3: New Flight Crew Procedures to check RVSM Status before departure shall be specified FCOT_1-2: Flight crew shall be trained appropriately regarding RVSM Status checking before departure	These requirements developed in the PISC (from Req_{Core}_60 and Req_{Core}_61 of the previous FHA) are confirmed.
Flight crew takes intentional avoidance action based solely on the TCAS	H2	FCOT_1-7: Pilots shall be trained appropriately to TCAS operation (initial and continuous training)	This requirement developed in the PISC (from Req_{Core}_89 of the previous FHA) is confirmed.
Flight crew follows an incorrect TCAS RA	H4a	ACOE_1-2: Aircraft shall be equipped with ACAS II (TCAS version 7.0) FCOP_1-5: Flight Crew procedures to limit Climbing/descent rate during the level change to avoid nuisance RA (e.g.500ft/min to 1000ft/min) shall be defined FCOT_1-6: Flight Crew Training shall include use of procedures for limiting Climbing/descent rate during the level change to avoid nuisance RA (e.g.500ft/min to 1000ft/min) FCOT_1-7: Pilots shall be trained appropriately to TCAS operation (initial and continuous training) ATSP_1-5: Climbing/descent rate shall be limited during the level change to avoid nuisance RA (e.g.500ft/min to 1000ft/min) ATST_1-7: Controllers shall be trained on limitation of Climbing/descent rate during the level change to avoid nuisance RA (e.g.500ft/min to 1000ft/min)	These requirements developed in the PISC (from Req_{Core}_87-88-89 of the previous FHA) are confirmed.

Cause	Hazard	System Element Requirements	Comment
Flight crew incorrectly calculates the climb capability (human error)	H2	FCOT_4-1: Flight crew shall be trained appropriately with regards to Non-RVSM approved civil aircraft transiting procedures (including contingencies) FCOP4: Non RVSM-approved civil aircraft transiting procedures (including contingencies) shall be defined. ATST3: Controllers shall be trained with regards to non RVSM-approved aircraft transiting procedures (including contingencies) ATSP3: Procedures facilitating the transit of non-RVSM civil aircraft through the RVSM airspace without intermediate stops shall be defined (NEW) FCOP_4-1: Flight crew procedures shall be defined to provide ATC with climbing/descending performance before transit clearance is issued. (NEW) ATSP_3-1: Minimum climbing/descending performance shall be requested by ATC before transit clearance is issued.	Theses requirements developed in the PISC are confirmed. New requirements resulting from previous FHA recommendation Rco_{core}_1
Flight crew encounters atmospheric conditions different from the ones forecasted	H2	FCOT_4-1: Flight crew shall be trained appropriately with regards to Non-RVSM approved civil aircraft transiting procedures (including contingencies) FCOP_3-4: Flight Crew Contingency Procedures shall be defined to execute lateral/level deviation from RVSM level for non RVSM civil aircraft FCOP_3-5: Flight Crew Contingency Procedures shall be defined to exit non RVSM civil aircraft from RVSM Airspace (NEW) FCOP4-2: Degradation of climbing/descending performance shall be reported by flight crew to ATC	These requirements developed in the PISC (from Req_{Core}_3, Req_{Core}_4 and Req_{Core}_8 of the previous FHA) are confirmed. New requirements resulting from previous FHA recommendation Rco_{core}_3

Cause	Hazard	System Element Requirements	Comment
Flight crew deliberately does not report non-RVSM status or reports a wrong information	H1	FCOP_1-4: Transferring procedure for flight crew shall be defined (e.g. State Level/RVSM Status before FIR entry) FCOT_1-3: Flight Crew shall be trained to report negative RVSM Status on the initial call on any frequency within the AFI RVSM airspace FCOT_1-8: Flight crew shall be trained appropriately with regards to the transfer procedures ATSP_1-3: ATS Transfer procedures (including read back and RVSM/Non RVSM Status) shall be defined in LoA (NEW) FCOT_1-10: Flight crew discipline with regards to ATC shall be reinforced.	These requirements developed in the PISC (from Req_{Core}_41, 42 and 64 of the previous FHA) are confirmed. New requirement
Flight crew human error providing erroneous RVSM status	H1	FCOP_1-4: Transferring procedure for flight crew shall be defined (e.g. State Level/RVSM Status before FIR entry) FCOT_1-3: Flight Crew shall be trained to report negative RVSM Status on the initial call on any frequency within the AFI RVSM airspace FCOT_1-8: Flight crew shall be trained appropriately with regards to the transfer procedures ATSP_1-3: ATS Transfer procedures (including read back and RVSM/Non RVSM Status) shall be defined in LoA	These requirements developed in the PISC (from Req_{Core}_41, 42 and 64 of the previous FHA) are confirmed.
Flight crew human error (intentional or not) not reporting at compulsory reporting point	H3	FCOT_1-9: Pilots awareness on reporting accuracy shall be reinforced by training	This requirement developed in the PISC (from Req_{Core}_33 of the previous FHA) is confirmed.
Flight crew delay contacting ATC due to workload, priority management etc.	H4b	(NEW) FCOT_3-10: Flight crew awareness with regards to weather deviations procedures (including notification to ATC) shall be reinforced.	This cause is circumstantial and does not relate to any failure from the AFI RVSM system. Appropriate flight crew training and procedures regarding ATS contacting in case of flight level deviation are considered to be provided independently from RVSM operations. However the RVSM operations require reinforcing the flight crew awareness. New requirement.

Cause	Hazard	System Element Requirements	Comment
Frequency selection error by flight crew	H1, H3, H4	FCOT_1-8: Flight crew shall be trained appropriately with regards to the transfer procedures FCOP_1-4: Transferring procedure for flight crew shall be defined (e.g. State Level/RVSM Status before FIR entry)	This cause is not specific to RVSM. Transferring procedures include transfer of communications. These requirements developed in the PISC (from Req_{Core}_41 and 42) of the previous FHA) are confirmed.
Flight crew unintentionally enters wrong level	H4	FCOP_1-1: Flight Crew procedures for read back shall be reinforced FCOT_1-5: Flight Crew shall be trained appropriately with regards to RVSM Procedures (including read back for clearance and leaving/reaching level) ATSP_1-1: ATS Procedures for read back shall be reinforced ATST_1-3: Controllers shall be trained appropriately with regards to RVSM Procedures including read back for clearance ATST_1-3: Controllers shall be trained appropriately with regards to RVSM Procedures including read back for report leaving/reaching level	Requirement developed in the PISC (from Req_{Core}_29, 30, 31, 34 and 35 of the previous FHA).
Flight crew intentional deviation (not operationally justified)	H4	(NEW) FCOT_3-10: Flight crew awareness with regards to weather deviations procedures (including notification to ATC) shall be reinforced. (NEW) FCOT_1-10: Flight crew discipline with regards to ATC shall be reinforced.	New requirements

Cause	Hazard	System Element Requirements	Comment
Onboard systems related causes			
Detected or undetected altimetry system (or altimetry setting) error	H2, H4b	ACOE_1-1: Aircraft shall meet MASPS requirements FCOP_1-2: New operator procedures shall include the checking/assurance that for operation in AFI RVSM airspace, the aircraft equipment meets the RVSM MASPS requirements FCOT_1-1: Flight crew training shall include use of procedures for the checking/assurance that, for operation in AFI RVSM airspace, the aircraft equipment meets the RVSM MASPS Requirement FCOT_3-3: Flight crew shall be trained appropriately with regards to contingency procedures in case of MASPS requirements failure FCOP_3-3: Flight crew contingency procedures shall be defined to provide 2000 feet separation for non RVSM civil aircraft FCOP_3-4: Flight crew contingency procedures shall be defined to execute lateral/level deviation from RVSM level for non RVSM civil aircraft FCOP_3-5: Flight crew contingency procedures shall be defined to exit non-RVSM civil aircraft from RVSM airspace FCOT_3-3: Flight crew shall be trained appropriately with regards to contingency procedures in case of MASPS requirements failure ATSP_2-3: ATS Contingency Procedures shall be defined to provide 2000 feet separation for non RVSM civil aircraft ATST_2-2: Controllers shall be trained appropriately with regards to contingency procedures in case of MASPS requirements failure	These requirements developed in the PISC (from Req_{Core}_1-2-3-4-5-6 of the previous FHA) are confirmed.

Cause	Hazard	System Element Requirements	Comment
Detected or undetected height keeping function error	H2, H4b	ACOE_1-1: Aircraft shall meet MASPS requirements FCOP_1-2: New operator procedures shall include the checking/assurance that for operation in AFI RVSM airspace, the aircraft equipment meets the RVSM MASPS requirements FCOP_3-3: Flight crew contingency procedures shall be defined to provide 2000 feet separation for non RVSM civil aircraft FCOP_3-4: Flight crew contingency procedures shall be defined to execute lateral/level deviation from RVSM level for non RVSM civil aircraft FCOP_3-5: Flight crew contingency procedures shall be defined to exit non-RVSM civil aircraft from RVSM airspace FCOT_1-1: Flight crew training shall include use of procedures for the checking/assurance that, for operation in AFI RVSM airspace, the aircraft equipment meets the RVSM MASPS Requirement FCOT_3-3: Flight crew shall be trained appropriately with regards to contingency procedures in case of MASPS requirements failure ATSP_2-3: ATS Contingency Procedures shall be defined to provide 2000 feet separation for non RVSM civil aircraft ATSP_2-4: ATS Contingency Procedures shall be defined to exit non-RVSM civil aircraft from RVSM airspace ATSP_2-5: ATS Contingency Procedures shall be defined to execute lateral/level deviation from RVSM level for non RVSM civil aircraft ATST_2-2: Controllers shall be trained appropriately with regards to contingency procedures in case of MASPS requirements failure	These requirements developed in the PISC (from Req_{Core}_1-2-3-4-5-6 of the previous FHA) are confirmed.
Autopilot malfunction	H4	ACOE_1-1: Aircraft shall meet MASPS requirements	This cause is not specific to RVSM. This requirement developed in the PISC (from Req_{Core}_1 of the previous FHA) is confirmed.

Cause	Hazard	System Element Requirements	Comment
Loss of a/c A/G communications and back-up	H1a, H3, H4b	FCOP_3-6: Flight crew Radio Communications Failure procedures shall be defined FCOT_3-8: Flight crew shall be trained appropriately with regards to Radio Communications Failure procedures. ATSP_2-6: ATS Radio Communications Failure procedures shall be defined ATST_2-4: Controllers shall be trained appropriately with regards to Radio Communications Failure procedures.	These requirements developed in the PISC (from Req_{Core}_9-10-11 of the previous FHA) are confirmed.
Degradation of a/c operational capability	H2	None.	The cause is circumstantial and does not relate to any failure from the AFI RVSM system.
In flight emergency/ contingency or serious aircraft equipment failure	H4	FCOP_3-11: Flight Crew emergency contingencies shall be specified FCOT_3-7: Flight crew shall be trained appropriately with regards to emergency contingencies ATSP_2-12: Emergency contingencies shall be specified ATST_2-10: Controllers shall be trained appropriately with regards to emergency contingencies	These requirements developed in the PISC (from Req_{Core}_84-85-86 of the previous FHA) are confirmed.

Cause	Hazard	System Element Requirements	Comment
Environmental conditions related causes			
Unexpected adverse weather conditions: severe turbulence, icing, convective activity, temperature inversion /wake vortex	H2, H4b	ACOE_1-3 / 1-4: Weather forecast equipment shall be in place to inform flight crew and operators about areas with severe turbulence / bad weather conditions. FCOP_2-1: Operators Flight planning procedures shall take into account weather forecast FCOP_2-2: Weather forecast shall be in place to inform flight crew and operators about areas with potential severe turbulence and/or bad weather conditions FCOP_3-1: New Flight Crew Procedures to suspend RVSM shall be specified FCOP_3-2: Flight Crew Procedures to report encountered vortices shall be defined FCOP_3-7: Flight Crew Contingency procedures regarding not forecast severe turbulence shall be defined FCOP_3-8: Flight Crew Contingency procedures regarding wake turbulence shall be defined FCOT_2-2: Operator and flight crew shall be appropriately trained with regards to the consideration of turbulence and bad weather forecast when flight planning FCOT_3-1: Flight crew shall be trained to report significant weather encountered en-route FCOT_3-2: Flight Crew shall be trained appropriately regarding suspension of RVSM FCOT_3-4: Flight crew shall be trained appropriately regarding contingency procedures related to not forecast turbulence FCOT_3-5: Flight crew shall be trained appropriately regarding contingency procedures related to wake turbulence ATSE_1-4: Weather forecast equipment shall be in place to inform ATC about areas with severe turbulence ATSE_1-4: Weather forecast equipment shall be in place to inform ATC about bad weather conditions	This cause is circumstantial and does not relate to any failure from the AFI RVSM system. However the AFI RVSM system provides mitigations to handle such situation relating to the operational environment. The mitigation strategy is similar to the one developed in the previous FHA for AH_{core}_19, AH_{core}_20 and AH_{core}_21. These requirements developed in the PISC are confirmed. In addition, the implementation of unidirectional and/or parallel tracks and of Strategic Lateral Offset Procedures is recommended where appropriate.

Cause	Hazard	System Element Requirements	Comment
		ATSP_1-9: Weather forecast procedures shall be in place to inform ATC about areas with potential severe turbulence and/or bad weather conditions ATSP_1-10: Appropriate separation standards shall be specified with regards to wake turbulences ATSP_2-1: ATS Procedures to suspend RVSM shall be defined ATSP_2-2: ATS Procedures to coordinate RVSM suspension with adjacent ACCs shall be defined ATSP_2-9: ATS Contingency procedures regarding not forecast severe turbulence shall be defined ATSP_2-10: ATS Contingency procedures regarding wake turbulence shall be defined ATST_1-10: Controllers shall be trained appropriately regarding Appropriate separation standards related to wake turbulence ATST_2-1: Controllers shall be trained appropriately regarding suspension of RVSM (including coordination with adjacent ACCs) ATST_2-9: Controllers shall be trained appropriately regarding contingency procedures related to not forecast turbulence ATST_2-9: Controllers shall be trained appropriately regarding contingency procedures related to wake turbulence	

Cause	Hazard	System Element Requirements	Comment
Non RVSM civil a/c operates below 290 and experiences severe turbulences or icing (or fuel constraints)	H2	FCOP_3-3: Flight Crew Contingency Procedures shall be defined to provide 2000 feet separation for non RVSM civil aircraft FCOP_3-9: Flight Crew Contingency procedures for Non-RVSM civil aircraft facing severe icing or turbulence shall be defined FCOT_3-6: Flight crew operating Non-RVSM aircraft shall be trained appropriately to contingency procedures related to Non-RVSM aircraft facing severe icing or turbulence ATSP_2-3: ATS Contingency Procedures shall be defined to provide 2000 feet separation for non RVSM civil aircraft ATSP_2-4: ATS Contingency Procedures shall be defined to exit non RVSM civil aircraft from RVSM Airspace ATSP_2-5: ATS Contingency Procedures shall be defined to execute lateral/level deviation from RVSM level for non RVSM civil aircraft ATSP_2-11: ATS Contingency procedures for Non-RVSM aircraft facing severe icing or turbulence shall be defined ATST_2-9: ATC controller shall be trained appropriately regarding contingency procedures related to Non-RVSM aircraft facing severe icing or turbulence	These requirements developed in the PISC (from Req_{Core}_2 to 4, 99 and 100 of the previous FHA) are confirmed.

Cause	Hazard	System Element Requirements	Comment
Civil/military coordination related causes			
Incorrect RVSM status information from civil/military coordination	H1a, H1b, H3	ATSP_1-3: ATS Coordination procedures shall be defined in the Civil – Military LoA ATSP_2-13: Military – Civil coordination Contingency procedures shall be defined in the civil-military LoA ATST_1-5: Controllers shall be trained appropriately with regards to RVSM civil - military Coordination Procedures ATST_1-5: Military controllers shall be trained appropriately with regards to RVSM Coordination Procedures - Controllers shall be trained appropriately with regards to RVSM civil - military Coordination Procedures ATST_2-8: Controllers shall be trained appropriately with regards to coordination Contingency procedures (including Military coordination) - Military Controllers shall be trained appropriately with regards to coordination Contingency procedures ATST_2-8: Military Controllers shall be trained appropriately with regards to coordination Contingency procedures	These requirements developed in the PISC (from Req_{Core}_91-92-93-94-95-96 of the previous FHA) are confirmed.
Others			

Cause	Hazard	System Element Requirements	Comment
CPL is missing	H1a, H1b	FCOP2: Flight planning procedures shall be revised and reinforced for RVSM FCOT2: Operator and flight crew shall be appropriately trained with regards to flight planning procedures revised for RVSM operations ACOE_1-6: Operator flight plan filling capabilities shall be reinforced (NEW) ATSE_1-5: AFTN communications availability/reliability and data rate transmission shall meet the Regional requirements ATSP_2-8: ATS Procedures regarding non-receipt of flight plan shall be defined ATST_2-7: Controllers shall be trained appropriately regarding non-receipt of flight plan ATSP_1-4: ATS Procedures regarding knowledge of RVSM status shall be defined ATST_1-1: Controllers shall be trained appropriately regarding knowledge of RVSM status procedures ATST_2-6: Controllers shall be trained appropriately to operate without FDPS system (blank strip…)	These operator flight planning requirements developed in the PISC (from Req_{Core}_58 and Req_{Core}_59 of the previous FHA) are confirmed. New requirement resulting from previous FHA recommendation Rco_{core}_12 These ATS contingencies requirements developed in the PISC (from Req_{Core}_9-54-55-62-63 of the previous FHA) are confirmed. Note: the loss of CPL by preceding ATSUs is covered otherwise by a similar cause at the considered CTA/UTA level.
RVSM approval status is not indicated in the flight plan	H1a, H1b	FCOP2: Flight planning procedures shall be revised and reinforced for RVSM FCOT2: Operator and flight crew shall be appropriately trained with regards to flight planning procedures revised for RVSM operations ACOE_1-6: Operator flight plan filling capabilities shall be reinforced ATSP_1-4: ATS Procedures regarding knowledge of RVSM status shall be defined (including contingencies) ATST_1-1: Controllers shall be trained appropriately regarding knowledge of RVSM status procedures (including contingencies)	These operator flight planning requirements developed in the PISC (from Req_{Core}_58 and Req_{Core}_59 of the previous FHA) are confirmed. These ATS contingencies requirements developed in the PISC (from Req_{Core}_62-63 of the previous FHA) are confirmed.

Cause	Hazard	System Element Requirements	Comment
Incorrect frequency is previously communicated to the flight crew	H1a, H3, H4b	FCOP_1-1: Flight Crew procedures for read back shall be reinforced ATSP_1-1: ATS procedures for read back shall be reinforced ATSP_2-13: ATS Transfer procedures shall be defined in the LoA (including communications failure contingencies) ATST_1-6: Controllers shall be trained appropriately with regards to transfer procedures	This requirement developed in the PISC (from Req_{Core}_29 of the previous FHA) is confirmed. These requirements developed in the PISC (from Req_{Core}_16-17 of the previous FHA) are confirmed. Transfer procedures include transfer of communications.
Coordination about RVSM capability information is not required by LoA	H1a, H1b	ATSP_1-3: ATS Transfer procedures (including read back and RVSM/Non RVSM Status) shall be defined in LoA	This requirement developed in the PISC (from Req_{Core}_16-37-39-41-56 of the previous FHA) is confirmed. Note: It has not been shown to be realised at the concept level before implementation and constitutes a PISC outstanding issue.
ATCO related causes			
ATCO human error (training, language) when providing RVSM status	H1a, H1b, H3	ATST_1-4: Controllers shall be trained appropriately with regards to RVSM Coordination Procedures	This requirement developed in the PISC (from Req_{Core}_36 of the previous FHA) is confirmed.

Cause	Hazard	System Element Requirements	Comment
Coordination human error by adjacent ATCO	H1, H3	FCOP_1-4: Transferring procedure for flight crew shall be defined (e.g. State Level/RVSM Status before FIR entry) FCOT_1-8: Flight crew shall be trained appropriately with regards to the transfer procedures ATST_1-4: Controllers shall be trained appropriately with regards to RVSM Coordination Procedures ATSE_1-2: RVSM/Non RVSM Status shall be provided by transferring controller (including when status is downgraded) ATSE_1-3: Suitable and reliable ground communications means shall be implemented ATSP_1-3: ATS Transfer procedures (including read back and RVSM/Non RVSM Status) shall be defined in LoA ATST_1-6: Controllers shall be trained appropriately with regards to transfer procedures	These requirements developed in the PISC (from Req_{Core}_36-42 of the previous FHA) are confirmed.
ATCO do not verify/request if aircraft has climb capability	H2	ATST3: Controllers shall be trained appropriately with regards to Non-RVSM civil aircraft transiting procedures (including contingencies) (NEW) ATSP_3-1: Minimum climbing/descending performance shall be requested by ATC before transit clearance is issued.	This requirement developed in the PISC (from Req_{Core}_7 of the previous FHA) is confirmed. New requirements resulting from previous FHA recommendation Rco_{core}_1
ATCO decides to keep non-RVSM a/c in RVSM airspace (operationally justified: fuel constraints / ATM capacity/complexity)	H2	FCOP_3-3: Flight Crew Contingency Procedures shall be defined to provide 2000 feet separation for non RVSM civil aircraft ATSP_2-3: ATS Contingency Procedures shall be defined to provide 2000 feet separation for non RVSM civil aircraft	These requirements developed in the PISC (from Req_{Core}_2 of the previous FHA) are confirmed.

Cause	Hazard	System Element Requirements	Comment
ATCO human error leading to undetected conflict or providing an incorrect clearance (in the vertical dimension)	H3	FCOP_1-1: Flight Crew procedures for read back shall be reinforced	These requirements developed in the PISC (from Req_{Core}_24 to 35 of the previous FHA) are confirmed.
		FCOT_1-4: Flight Crew shall be trained appropriately with regards to RVSM Procedures including correct use of FLAS	
		FCOT_1-5: Flight Crew shall be trained appropriately with regards to RVSM Procedures (including read back for clearance and leaving/reaching level)	
		FCOT_1-9: Pilots awareness on reporting accuracy shall be reinforced by training	
		ATSE1: ATS equipment shall be modified to indicate and display RVSM status	
		ATSE2: Existing conflict detection/alerting capabilities shall be updated to be consistent with RVSM operations	
		ATSP_1-2: Crosscheck between controllers shall be performed	
		ATST_1-2: Controllers shall be trained appropriately with regards to RVSM Procedures including correct use of FLAS	
		ATSP_1-1: ATS Procedures for read back shall be reinforced	
		ATST_1-3: Controllers shall be trained appropriately with regards to RVSM Procedures including read back for clearance	
		ATST_1-3: Controllers shall be trained appropriately with regards to RVSM Procedures including read back for report leaving/reaching level	
		(NEW) ATSE_1-6: STCA capabilities shall be reinforced where appropriate	New requirement resulting from previous FHA recommendation Rco_{core}_6
		(NEW) ATSE_1-10: MTCD capabilities shall be reinforced where appropriate	New requirement

Cause	Hazard	System Element Requirements	Comment
Adjacent ATCO human error not coordinating a flight	H3	ATSE_1-2: RVSM/Non RVSM Status shall be provided by transferring controller (including when status is downgraded) ATSP_1-3: ATS Transfer procedures (including read back and RVSM/Non RVSM Status) shall be defined in LoA ATST_1-4: Controllers shall be trained appropriately with regards to RVSM Coordination Procedures	These requirements developed in the PISC (from Req_{Core}_36, 37 and 39 of the previous FHA) are confirmed.
ATCO manually enters wrong RVSM status in the FDPS or directly in the flight strip	H1a, H1b	(NEW) ATST_1-11: ATCO shall be trained with regards to RVSM status handling into FDPS.	New requirement, as a result of the operational experience.
Preceding ATSU unit corrupts RVSM status	H1a, H1b	None	This cause is considered as an external event as it does not relate to the CTA/UTA level. The similar cause for the CTA/UTA level ATS unit is covered otherwise.
Unexpected traffic due to inadequate traffic management by ATC (applicable to climb and descend)	H2	None	This cause is circumstantial. Causes of inadequate traffic management are covered otherwise.
Flight strip is missing or incorrect strip marking by ATCO	H3	None	This cause is not specific to RVSM.
Ground systems related causes			
RVSM approval status information is not processed by flight plan processing equipment (e.g. rejected corruption, processing errors, inadequate SW functions)	H1a, H1b	ATSE1: ATS equipment shall be modified to indicate and display RVSM status (NEW) ATSE_1-7: ATS equipment shall be developed with a minimum software assurance level to assure acceptable risk of data (e.g. surveillance information, flight plan) corruption	This requirement developed in the PISC (from Req_{Core}_26 of the previous FHA) is confirmed. New requirement.

Cause	Hazard	System Element Requirements	Comment
ATS/DS poor quality	H1, H3	ATSE_1-3: Suitable and reliable ground communications means shall be implemented ATSP_2-13: ATS Transfer procedures shall be defined in the LoA (including communications failure contingencies) ATST_2-3: Controllers shall be trained appropriately with regards to ATS/DS failure contingency procedures FCOT_3-9: Flight crew shall be trained appropriately with regards to ATS/DS failure (awareness training) ATSP_1-7: Ground/Ground Communication system maintenance procedures shall be defined to ensure a communication system recovery in MTTR defined in Service Level Agreement ATST_1-8: Maintenance team shall be trained appropriately with regards to Ground/Ground Communication system maintenance procedures	These requirements developed in the PISC (from Req_{Core}_38 and 18 to 22 of the previous FHA) are confirmed.

Cause	Hazard	System Element Requirements	Comment
Loss of ATS A/G communications (shortcoming or deficiency, frequency congestion) including back-up if any	H1a, H3, H4b	FCOP_3-6: Flight Crew Radio Communications Failure procedures shall be defined FCOT_3-8: Flight crew shall be trained appropriately with regards to Radio Communications Failure procedures ATSE_1-1: Air/Ground Communication system shall be designed to ensure a total coverage of the RVSM airspace with a minimum MTBF defined at CTA/UTA level ATSP_1-6: Air/Ground Communications system maintenance procedures shall be defined to ensure a communication system recovery in MTTR defined in Service Level Agreement ATSP_2-6: ATS Radio Communications Failure procedures shall be defined ATST_1-8: Air/Ground Communications Maintenance team shall be trained appropriately with regards to Air/Ground Communication system maintenance procedures ATST_2-4: Controllers shall be trained appropriately with regards to Radio Communications Failure procedures	The mitigation strategy is similar to the one developed in the previous FHA for AH_{core}_7. The associated PISC requirements are confirmed (ATSE_1-1 has been reworded). To cope with the problems experience in the use of HF communications, the implementation of CPDLC application is recommended.
Poor quality of A/G communications	H4a	-	This cause is not specific to RVSM. To cope with the problems experience in the use of HF communications, the implementation of CPDLC application is recommended.

Cause	Hazard	System Element Requirements	Comment
Loss of G/G communications	H1a, H1b, H3	FCOT_3-9: Flight crew shall be trained appropriately with regards to ATS/DS failure (awareness training) ATSE_1-1: ATS/DS Communication system shall be designed to ensure point-to-point communications between all adjacent ACCs with a minimum MTBF defined at CTA/UTA level. ATSE_1-3: Suitable and reliable ground communications means shall be implemented ATSP_1-3: ATS Transfer procedures (including read back and RVSM/Non RVSM Status) shall be defined in LoA ATSP_1-7: Ground/Ground Communication system maintenance procedures shall be defined to ensure a communication system recovery in MTTR defined in Service Level Agreement ATSP_2-13: ATS Transfer procedures shall be defined in the LoA (including communications failure contingencies) ATST_1-6: Controllers shall be trained appropriately with regards to transfer procedures ATST_1-8: Maintenance team shall be trained appropriately with regards to Ground/Ground Communication system maintenance procedures ATST_2-3: Controllers shall be trained appropriately with regards to ATS/DS failure contingency procedures (NEW) ATSP_2-14: Silent transfer procedures shall be defined in the LoA between ATS units equipped with Radar systems, which are capable of communicating with each other.	The mitigation strategy is similar to the one developed in the previous FHA for AH_{core}_8, even if here the requirements do not only consider ATS/DS. The associated PISC requirements are confirmed (ATSE_1-1 has been reworded). New requirement resulting from previous FHA recommendation Rco_{core}_5.

Cause	Hazard	System Element Requirements	Comment
ATSD failure	H3	ATSP_1-8: FDPS/RDPS/ADS system maintenance procedures shall be defined to ensure a communication system recovery in MTTR defined in Service Level Agreement. ATSP_1-8: FDPS system maintenance procedures shall be defined to ensure a communication system recovery in MTTR defined in Service Level Agreement. ATSP_2-7: ATS Procedures to revert to procedural control shall be specified (due to RDPS/ADS system failure) ATSP_2-7: ATS Procedures to revert to procedural control shall be specified (due FDPS / RDPS/ADS system failure) ATST_1-9: Maintenance team shall be trained appropriately with regards to FDPS/RDPS/ADS systems maintenance procedures ATST_1-9: Maintenance team shall be trained appropriately with regards to FDPS systems maintenance procedures ATST_2-5: Controllers shall be trained appropriately to revert to procedural control in case of FDPS / RDPS/ADS system failure ATST_2-6: Controllers shall be trained appropriately to operate without FDPS system (blank strip…) (NEW) ATSE_1-8: FDPS/RDPS/ADS equipment shall be designed to ensure the achievement of a minimum MTBF defined at CTA/UTA level. (NEW) ATSE_1-7: ATS equipment shall be developed with a minimum software assurance level to assure acceptable risk of data (e.g. surveillance information, flight plan) corruption	These requirements developed in the PISC (from Req_{Core}_43-44-45-46-47-48-49-50-51-52-53 of the previous FHA). New requirement resulting from previous FHA recommendations Rco_{Core}_9, 10 and 11. New requirement
Flight plan processing equipment (including ATSD) corrupts RVSM approval status (undetected)	H1	(NEW) ATSE_1-7: ATS equipment shall be developed with a minimum software assurance level to assure acceptable risk of data (e.g. surveillance information, flight plan) corruption	New requirement
AFTN network corrupts FPL/RPL/CPL/CHG messages	H1a, H1b	(NEW) ATSE_1-5: AFTN communications availability/reliability and data rate transmission shall meet the Regional requirements (NEW) ATSE_1-9: FPDS shall check validity of RVSM status	New requirement resulting from previous FHA recommendations Rco_{Core}_12 and 15

Cause	Hazard	System Element Requirements	Comment
Aircraft deviation is not detected by ATC	H4	(NEW) ATSE_1-8: FDPS/RDPS/ADS equipment shall be designed to ensure the achievement of a minimum MTBF defined at CTA/UTA level. (NEW) ATSE_1-7: ATS equipment shall be developed with a minimum software assurance level to assure acceptable risk of data (e.g. surveillance information, flight plan) corruption	Non detection of aircraft deviation is not considered as an ATC failure if ATS surveillance services are not provided. This leads to the need for recommending the reinforcement of the provision of ATS surveillance services in the AFI Region.

Table 30: AFI RVSM risk mitigation strategy

Appendix G Traceability from FHA to FHA review

☞ This appendix provides the traceability between the results of the previous FHA and of the FHA review

G.1 AFI RVSM hazards

The following table provides the traceability between the previous FHA hazards (see [5], appendix D "hazard classification tables") and the hazards resulting from the FHA review. It shows that the previous FHA hazards are adequately covered by H1, H2, H3, H4a and H4b.

Previous FHA	Description	FHA Review	Comment
AH_{core}_1	Height keeping system failure	H4	AH_{core}_1 is now considered as a cause of H4a and H4b according to the detection or not of the failure by the flight crew.
AH_{core}_2	Loss of at least one of the two main Altitude Indications (display)	H4	AH_{core}_2 is now considered as a cause of H4a and H4b according to the detection or not of the failure by the flight crew.
AH_{core}_3	Loss of transponder capability	H2	AH_{core}_3 is now considered as a cause of H2.
AH_{core}_4	Loss of altitude alerting system	H4	AH_{core}_4 is now considered as a cause of H4a and H4b.
AH_{core}_5	Non RVSM civil Aircraft transiting through RVSM airspace with degraded climb performances	H2	AH_{core}_5 is now considered as a cause of H2.
AH_{core}_6	Loss of aircraft communications capabilities (voice)	H1, H3 & H4b	AH_{core}_6 is now considered as a cause of H1, H3 and H4b according to which procedure is affected by the loss of voice communications (initial contact, vertical clearance delivery or vertical deviation report).
AH_{core}_7	Loss of ground/air (ATC R/T) communications capabilities	H1, H3 & H4b	AH_{core}_7 is now considered as a cause of H1, H3 and H4b according to which procedure is affected by the loss of voice communications (initial contact, vertical clearance delivery or vertical deviation report).
AH_{core}_8	Loss of Point to Point (ATS/DS) communications capabilities	H1 & H3	AH_{core}_8 is now considered as a cause of H1 and H3 according to which coordination is affected by the loss of Point to point communications (entering coordination or outgoing coordination).
AH_{core}_9	Controller issues incorrect clearance	H1 & H3	AH_{core}_9 is now considered as a cause of H1 or H3 according to the underlying cause of the hazard.

Previous FHA	Description	FHA Review	Comment
AH_{core}_10	Controller provides incorrect traffic information	H1 & H3	AH_{core}_10 is the equivalent to AH_{core}_9 applied to specific airspaces and is therefore a cause of H1 or H3.
AH_{core}_11	Pilot deviates from clearance	H4a & H4b	AH_{core}_11 is now considered as a cause of H4a and H4b.
AH_{core}_12	Lack of ATS Coordination	H1 & H3	AH_{core}_12 is now considered as a cause of H1 or H3.
AH_{core}_13	Ground ATC system failure (RDPS/ADS system)	H1 & H3	AH_{core}_13 is now considered as a cause of H1 or H3.
AH_{core}_14	Ground ATC system failure (FDPS)	H1	AH_{core}_14 is now considered as a cause of H1 or H3.
AH_{core}_15	Ground ATC system failure (HMI and/or FDPS+RDSPS/ADS system)	H1 & H3	AH_{core}_15 is now considered as a cause of H1 or H3.
AH_{core}_16	Flight plan not received by accepting ACC	H1	AH_{core}_16 is now considered as a cause of H1.
AH_{core}_17	Incorrect RVSM status on filed and a/c flight plan	H1	AH_{core}_17 is now considered as a cause of H1.
AH_{core}_18	Incorrect RVSM status only on filed ATC flight plan	H1	AH_{core}_18 is now considered as a cause of H1.
AH_{core}_19	Flight level deviation due to not forecast severe turbulence	H4b	AH_{core}_19 is now considered as a cause of H4b.
AH_{core}_20	Flight level / route deviation due to weather conditions	H4b	AH_{core}_20 is now considered as a cause of H4b.
AH_{core}_21	Unexpected severe vortices	H4b	AH_{core}_21 is now considered as a cause of H4b.
AH_{core}_22	Specific situation requires an emergency descent (pressurisation)	H4b	AH_{core}_22 is now considered as a cause of H4b.
AH_{core}_23	Altitude deviation due to degraded aircraft performances	H4b	AH_{core}_23 is now considered as a cause of H4b.
AH_{core}_24	ACAS TA	H4b	AH_{core}_24 is now considered as a cause of H4b.
AH_{core}_25	ACAS RA (nuisance)	H4b	AH_{core}_25 is now considered as a cause of H4b.
AH_{core}_26	Wrong visual perception of other traffic position in relation to vertical separation	None	AH_{core}_26 could be considered as a cause of hazard H4b. However, one year after the implementation of RVSM, pilots are now familiar with operating a 1000ft vertical separation and AH_{core}_26 can be disregarded.
AH_{core}_27	Uncoordinated activation of a military reserved airspace (Temporary segregated area)	None	AH_{core}_27 has been considered outside the scope of RVSM related hazards and causes. However, coordination of RVSM status is a cause of H1.
AH_{core}_28	Non-RVSM civil aircraft which is experiencing severe icing or turbulences requiring a climb into RVSM airspace	H2	AH_{core}_28 is now considered as a cause of H2.

Table 31: FHA to FHA review traceability - Hazard identification

G.2 AFI RVSM hazards causes

The following table provides the traceability between the causes of the previous FHA hazards (see [5], appendix E “hazard mitigation tables”) and the causes as resulting from the FHA review. It shows that the previous FHA causes are adequately covered by the causes of H1, H2, H3, H4a and H4b.

Previous FHA	Description	FHA Review	Comment
AH_{core}_1	Technical failure of Height keeping system	H4	Height keeping system error is a cause of H4a.
AH_{core}_2	Technical failure of Altitude Indication	H4	Altimetry system error (including display and alerting) is a cause of H4a.
AH_{core}_3	Technical failure of transponder	H2	Loss of any equipment required to fly into RVSM airspace is a cause of H2.
AH_{core}_4	Technical failure of Altitude alerting system	H4	Altimetry system error (including display and alerting) is a cause of H4a.
AH_{core}_5	Degradation of climbing performances (operations capabilities reduced) Low climbing performances	H2	Climbing performances issues are causes of H2.
AH_{core}_6	Technical failure of aircraft communication	H1, H3 & H4b	Aircraft communication capabilities failures are causes of hazards H1, H3 and H4b.
AH_{core}_7	Technical failures of air/ground communication Frequency congestions Atmospheric conditions	H1, H3 & H4b	Loss of ATS A/G communications (shortcoming or deficiency, frequency congestion) is a cause of hazards H1, H3 and H4b
AH_{core}_8	Technical failures of ATS/DS communication	H1 & H3	ATS/DS failures are causes of hazards H1 and H3
AH_{core}_9	Application of incorrect separation standards (inadequate knowledge of procedures) Human error Incorrect RVSM status for the a/c	H1 & H3	Human error in applying vertical separation is a cause of H1 (provision of 1000ft separation to non RVSM aircraft) and H3 (wrong clearance). Application of incorrect separation standards should is encompassed by human error cause of H1. Incorrect RVSM status is a cause of H1.
AH_{core}_10	Inadequate knowledge of procedures Human error Wrong RVSM status for the a/c Incorrect pilot reporting	H1 & H3	AH_{core}_10 is the equivalent to AH_{core}_9 applied to specific airspaces. Pilot failing in reporting at compulsory report waypoints is a cause of H3.

Previous FHA	Description	FHA Review	Comment
AH_{core}_11	Human error (misreading of clearance, call sign confusion, incorrect level input into the Flight Control Unit)	H4a & H4b	Errors in level inputs are causes of H4a. Flight crew misunderstanding of cleared flight level is a cause of H4a.
AH_{core}_12	Human error during coordination - From the receiving controller (misreading of information, call sign confusion) - From the transferring controller (incorrect information given, information not transferred)	H1 & H3	Coordination errors during the coordination are causes of a wrong RVSM status and therefore a cause of H1. Lack of coordination is also a cause of undetected conflicts and therefore a cause of H3.
AH_{core}_13	Technical failure of ground ATC system (RDPS/ADS system)	H1 & H3	Errors on the RVSM status indication from the RDPS system is a cause of H1. RDPS/ADS systems failures leading to the inability by the ATCO to detect conflicts are causes of H3.
AH_{core}_14	Technical failure of ground ATC system (FDPS)	H1	Failures of the FDPS to provide flight plans or RVSM status is a cause of H1.
AH_{core}_15	Technical failure of ground ATC system (HMI and/or FDPS+RDPS/ADS system)	H1 & H3	Errors on the RVSM status indication from the RDPS system is a cause of H1. RDPS/ADS systems failures leading to the inability by the ATCO to detect conflicts are causes of H3.
AH_{core}_16	- FPL not sent by flight operator - FPL not sent by point of departure - FPL incorrectly addressed - Late FPL reception - Communications System Failure	H1	FPL not being received is a cause of H1. Its sub-causes have nevertheless not been refined in the FHA review. Communication system failures are causes of H1.
AH_{core}_17	- Late change of a/c or flight crew - Typing error from flight operator - Lack of training for Flight Ops staff	H1	Wrong RVSM status of the flight plan due to late changes or operator's errors is a cause of H1.
AH_{core}_18	- Late change of a/c - Typing error from flight operator - Corruption during transmission	H1	As for AH_{core}_17, late changes or operator's errors are causes of H1. Corruptions during transmissions are causes of H1.

Previous FHA	Description	FHA Review	Comment
AH_{core}_19	- CB Development - Clear Air Turbulence (CAT) - Mountain waves	H4b	Unexpected adverse environmental conditions is a cause of H4b.
AH_{core}_20	- Thunderstorm - Sandstorm - Volcanic activity…	H4b	Unexpected adverse environmental conditions is a cause of H4b.
AH_{core}_21	Severe vortices generated from aircraft flying above or by aircraft crossing at the same level	H4b	Wake vortex crossing is a cause of H4b.
AH_{core}_22	Emergency situation including pressurisation	H4b	In flight emergency/contingency is a cause of H4b.
AH_{core}_23	Degradation of aircraft performances requiring a descent (drift down).	H4b	Serious aircraft equipment failure is a cause of H4b.
AH_{core}_24	Proximity of traffic	H4b	Inappropriate use of TCAS information is a cause of both H2 and H4b.
AH_{core}_25	Close proximity of passing traffic or traffic with high rate of climb or descent	H4b	Incorrect TCAS RA is a cause of H4b.
AH_{core}_26	Human error from flight crew (depending on air traffic complexity)	None	Not applicable (see Table 31:)
AH_{core}_27	Human error (bad coordination or no coordination)	None	Not applicable (see Table 31:)
AH_{core}_28	- Severe icing - Severe turbulences	H2	Unexpected adverse weather conditions (severe turbulence, icing, convective activity, temperature inversion) is a cause of H2

Table 32: FHA to FHA review traceability - Hazard causes

G.3 AFI RVSM safety requirements

The review of the table provided in Appendix F against the integrity safety requirements developed in the PISC FHA shows that all the previous FHA mitigations are validated in light of the operational experience and adequately covered by the System Element Requirements, except for ReqCore_90 “Specific procedures to avoid deviation due to incorrect visual perspective shall be defined” which is no longer considered relevant as flight crew are now familiar with operating 1000 feet separation.

Annex 1 Definitions and Acronyms

1.1 Explanation of terms

A	
Accident	An occurrence associated with the operation of an aircraft which takes place between the time any person boards the aircraft with the intention of flight until such time as all such persons have disembarked, in which: a) a person is fatally or seriously injured as a result of: - being in the aircraft, or - direct contact with any part of the aircraft, including parts which have become detached from the aircraft, or - direct exposure to jet blast, *except* when the injuries are from natural causes, self-inflicted or inflicted by other persons, or when the injuries are to stowaways hiding outside the areas normally available to the passengers and crew; or b) the aircraft sustains damage or structural failure which: - adversely affects the structural strength, performance or flight characteristics of the aircraft, and - would normally require major repair or replacement of the affected component, *except* for engine failure or damage, when the damage is limited to the engine, its cowlings or accessories; or for damage limited to propellers, wing tips, antennas, tires, brakes, fairings, small dents or puncture holes in the aircraft skin; or c) the aircraft is missing or is completely inaccessible.
Aircraft proximity	A situation in which, in the opinion of a pilot or air traffic services personnel, the distance between aircraft as well as their relative positions and speed have been such that the safety of the aircraft involved may have been compromised. An aircraft proximity is classified as follows: - Risk of collision. The risk classification of an aircraft proximity in which serious risk of collision has existed. - Safety not assured. The risk classification of an aircraft proximity in which the safety of the aircraft may have been compromised. - No risk of collision. The risk classification of an aircraft proximity in which no risk of collision has existed. - Risk not determined. The risk classification of an aircraft proximity in which insufficient information was available to determine the risk involved, or inconclusive or conflicting evidence precluded such determination.
Airprox	The code word used in an air traffic incident report to designate aircraft proximity.
Air Traffic Services	A generic term meaning variously, flight information service, alerting service, air traffic advisory service, air traffic control, service (area control service, approach, control service or aerodrome control, service).

Air Traffic Services Unit	A generic term meaning variously, area control centre approach control office or aerodrome control tower. In the AFI RVSM context, only area control centre are considered.
Assessment	An evaluation based on engineering, operational judgment and/or analysis methods.
Assumption	Statement, principle and/or premises offered without proof.
B	
-	
C	
Causes	Actions, omissions, events, conditions, or a combination thereof, which can lead to the accident or incident.
D	
Deviation from cleared flight level	An event in which an aircraft does not reach and maintain flight levels under conditions specified by the ATS unit or other appropriate authority.
E	
-	
F	
Failure	The inability of any element of a system to perform its intended function or to perform it correctly within specified limits.
G	
General Air Traffic	All flights which are conducted in accordance with the rules and procedures of ICAO and/or the national civil aviation regulations and legislation.
H	
Hazard	Any condition, event, or circumstance which could induce an accident.
Horizontal overlap	The probability of having two aircraft at the same position at the same time. We consider two cases of horizontal overlap in this document: • the two aircraft are at the same level (see H3 effect tree analysis), • the two aircraft are at two consecutive flight levels (see H1 effect tree analysis), • the two aircraft are at any flight level (see H4 effect tree analysis).
I	
Incident	An occurrence, other than an accident, associated with the operation of an aircraft, which affects or could affect the safety of operation.
J	

-	
K	
-	
L	
Large height deviation	A vertical deviation of more than 300 feet.
M	
Minor height deviation	A vertical deviation of less than 300 feet.
Mitigation	Steps taken to control or prevent a hazard from causing harm and reduce risk to a tolerable or acceptable level.
N	
-	
O	
-	
P	
-	
Q	
-	
R	
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.
S	
Safety	Safety is the state in which the risk of harm to persons or of damage to property is reduced to, and maintained at or below, an acceptable level trough a continuing process of hazard identification and risk management.
Safety objective	A safety objective is a planned safety goal stated in a safety policy. More specifically in the context of the FHA review, a safety objective is a qualitative or quantitative statement that defines the maximum frequency or probability at which a RVSM hazard can be expected to occur.
Safety occurrence	Accidents, serious incidents and incidents as well as other defects or malfunctioning of an aircraft, its equipment and any element of the Air Navigation System which is used or intended to be used for the purpose or in connection with the operation of an aircraft or with the provision of an air traffic management service or navigational aid to an aircraft
Separation minima infringement	A situation in which prescribed separation minima were not maintained between aircraft (whether or not it led to the submission of an AIRPROX report).

Severity	Level of 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).
Severity class	Gradation, ranging from 1 (most severe) to 5 (least severe), as an expression of the magnitude of the consequences of hazards on flight operations
Short time conflict alert	An automated system that alerts air traffic controllers to potential conflicts between aircraft via an Air Traffic Situation Display.
System	A combination of physical components, procedures and human resources organised to perform a function.
T	
-	
U	
Unsatisfactory Condition Report	(AFI TAG Terminology) Any deficiency, investigation finding or shortcoming related to the TAG Terms of Reference that is brought to the attention of the TAG for action.
V	
Vertical overlap	The probability of having two aircraft being at the same flight level at the same time while still complying with vertical navigation performance requirements.
W	
-	
X	
-	
Y	
-	
Z	
-	

1.2 Acronyms

A/G	Air to Ground
AIAG	AFI ATS Incidents Analysis Group
APIRG	AFI Planning and Implementation Regional Group
ADS	Automatic Dependent Surveillance
AFI	Africa and Indian Ocean Region
ANS	Air Navigation Services
ANSP	Air Navigation Services Provider
ARMA	AFI Regional Monitoring Agency
ARPO	AFI RVSM Programme Office
ASECNA	Agence pour la Sécurité Aérienne en Afrique et à Madagascar
ATC	Air Traffic Control
ATCO	Air Traffic Control Officer
ATM	Air Traffic Management
ATNS	Air Traffic Navigation Services (South Africa)
ATS	Air Traffic Services
ATSU	Air Traffic Services Unit
CHG	Change message
CPL	Current Flight Plan
CRA	Collision Risk Assessment
CTA	Control Area
ETA	Event Tree Analysis
FHA	Functional Hazard Assessment
FIR	Flight Information Region
FLAS	Flight Level Allocation Scheme
FPL	Filed Flight Plan
FTA	Fault Tree Analysis
G/G	Ground to Ground
GAT	General Air Traffic
IATA	International Air Transport Association
IATA SO&I	IATA Safety, Operations and Infrastructure
ICAO	International Civil Aviation Organisation
IFALPA	International Federation of Airline Pilots' Associations
IFATCA	International Federation of Air Traffic Controllers' Associations
LoA	Letter of Agreement
PFH	Per Flight Hour
PISC	Pre-Implementation Safety Case
POSC	Post-Implementation Safety Case
PSSA	Preliminary System Safety Assessment

R-ATSU	Receiving ATS Unit
RAN	Regional Air Navigation meeting
RCS	Risk Classification Scheme
RPL	Repetitive Flight Plan
RVSM	Reduced Vertical Separation Minimum
SC	Severity Class
SCS	Severity Classification Scheme
SER	System Element Requirement
SMS	Safety Management System
SSP	State Safety Program
STCA	Short Term Conflict Alert
T-ATSU	Transferring ATS Unit
TAG	AFI Tactical Action Group
TLS	Target Level of Safety
UCR	Unsatisfactory Condition Report (AFI TAG Terminology)
UTA	Upper Traffic Area

Annex 2 Applicable and reference documents

2.1 Applicable documents

[1] AFI Reduced Vertical Separation Minimum (RVSM) RVSM Safety Policy, ICAO ARPO, 30 July 2004.

[2] Report of the Tenth Meeting of APIRG ATS/AIS/SAR Sub-group, May 2009.

2.2 Reference documents

[3] Post-Implementation Collision Risk Assessment for RVSM in the Africa Indian Ocean Region, NLR Air Transport Safety Institute, NLR-CR-2009-688, February 2010

[4] AFI RVSM Pre-Implementation Safety Case, ICAO ARPO/ARMA, Final Edition, February 2008.

[5] AFI RVSM Functional Hazard Assessment, Altran, AT/SDI/05-024A/05-003, May 2005.

[6] Briefing material - AFI FHA review brainstorming session, ARMA, edition 2.0, 26 November 2009

[7] Regional Supplementary Procedures, ICAO Doc 7030

[8] ICAO Safety Management Manual, ICAO Doc. 9859, second edition, 2009

[9] EUROCONTROL Air Navigation System Safety Assessment Methodology

[10] The EUR RVSM Pre-Implementation Safety Case, EUROCONTROL, RVSM 691, version 2.0, 14 August 2001;

[11] Manual on Implementation of a 300m (1000ft) Vertical Separation minimum Between FL290 and FL410 Inclusive, ICAO Doc 9574

[12] ICAO Special AFI Regional Air Navigation Meeting, SP AFI RAN (2008)

[13] Description of AFI ATS Incidents Analysis Working Group (AIAG) and AFI Tactical Action Group, International Air Transport Association, October 2009

[14] Extract of AIAG incidents reports for the time period 25 September 2008 - 31 December 2009, International Air Transport Association, January 2010

[15] Extract of AIAG incidents reports for the time period 1 January 2009 - 30 June 2009, International Air Transport Association, January 2010

[16] Extract of AIAG irregularity reports for the time period 25 September 2008 - 31 December 2009, International Air Transport Association, January 2010

[17] Extract of AIAG irregularity reports for the time period 1 January 2009 - 30 June 2009, International Air Transport Association, January 2010

[18] Extract of new UCR's detail for the time period 1 January 2009 - 30 September 2009

[19] Extract of resolved UCR's detail for the time period 1 January 2009 - 30 September 2009

[20] Extract of ARMA Form 1 database, AFI Regional Monitoring Agency, January 2010

[21] RVSM/RNAV/RNP TF/3 meeting report, Nairobi, 22-23 April 2004