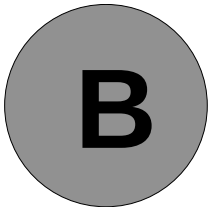

APPENDIX:

EXAMPLE OF TLS APPORTIONMENT METHOD:

EN-ROUTE AIRSPACE

Contents

1 Introduction

1.1 Purpose

This document presents a worked example of the application of the TLS Apportionment Method [1] to a typical block of EUR en-route airspace. It has been produced to illustrate the use of the Method.

This page is intentionally left blank.

2 Stage 1: ATM Safety Targets

2.1 Context

Phase of Flight: Typical en-route airspace between FL290 and FL410. This is defined to consist entirely of RVSM airspace but does not include any (RVSM - to - non-RVSM) Transition Areas.

Scope: It was decided to consider the horizontal dimensions and the vertical dimension separately, because:

1 An additional ICAO TLS exists specifically for vertical collision risk in RVSM airspace (ie for the selected phase of flight), and,

2 Some characteristics are different between the vertical and horizontal dimensions (though some are also shared between the two).

In order that the horizontal dimensions and the vertical dimension can be addressed separately from each other, it was necessary to record the following existing ATM rule, as **operational domain knowledge**:

ODK1: Safe separation between aircraft shall be maintained at all times, in at least one dimension – ie horizontal or vertical.

Finally, In order to keep this example (relatively) simple, only the vertical separation function is developed fully herein, and it is assumed that the airspace concerned contains no Danger or Prohibited Areas.

2.2 Stage 1.1: Safety Target Determination

2.2.1 Introduction

The starting point was the ESARR 4 service-level TLS of 1.55×10^{-8} SC1 outcomes per flight hour (pfh), as specified in ESARR 4. [1]

It was decided that it would not be appropriate to weight the TLS for the selected phase of flight in this case because the hypothetical Upper Area Centre (UAC) being considered is responsible only for en-route control.

2.2.2 Apportioning the ESARR 4 TLS

In general, apportioning the ESARR 4 TLS between the horizontal dimension and vertical dimension would normally be done from a mix of historical data (on say Airproxes), operational experience, and assessment of the relative complexity of the system from the Vertical Separation and Horizontal Separation perspectives.

However, for the case under consideration – ie RVSM airspace - a further ICAO RVSM TLS of a probability 2.5×10^{-9} SC1 events[2] per flight hour. This TLS uses the term "due to *all* causes" to define its

[1] A conversion to other units – eg per operating hour or per flight – could have been made at this point but it was decided not to, thus avoiding the need to consider issues such as sectorisation at this stage.

scope of application, compared with the term "ATM direct contributions" used in ESARR 4. However, taking account of the guidance given in [1], and the interpretation of "all causes" made on the EUR RVSM Programme (ie all ATM-related causes), it was concluded that, in this Example, there is no significant difference in scope between ESARR 4 and the ICAO RVSM TLS[3].

Therefore it was decided that it would be sensible at this stage to apportion to **vertical separation** an amount of the ESARR 4 TLS equal to the RVSM TLS – ie 2.5×10^{-9} SC1 events pfh.[4]

From this the following safety target was derived:

ST1: The likelihood of an ATM-related SC1 event[5] arising from loss of vertical separation shall not exceed 2.5×10^{-9} per flight hour, for all current and forecast traffic levels. [6].

2.3 Stage 1.2: Safety Target Validation

It is beyond the scope of this worked example to carry out a formal validation of the safety targets. However, the following notes highlight the key issues that would normally be addressed.

Validation of ST1 would require it to be shown that the balance of the ESARR 4 TLS (ie 1.3×10^{-8}) could be satisfied in the horizontal dimension. Normally, both the horizontal and vertical dimensions would be analysed at the same time – it is an artificiality of this example that they are not in this case. On the other hand, if it was necessary in practice to consider the vertical dimension in isolation, then a qualitative argument, based on historical evidence, could be used for the horizontal dimension.

[2] The RVSM TLS is actually specified as 5×10^{-9} accidents pfh. However, in the context of ICAO RVSM requirements, an SC1 event (collision) counts as two accidents

[3] It was noted at this point that if subsequent analysis showed this interpretation to be wrong then the TLS apportionment would be adjusted accordingly – in the event, that adjustment did not prove to be necessary.

[4] This leaves 1.3×10^{-8} pfh for the horizontal dimensions. In a full analysis (ie including horizontal dimensions), account would have to be taken as to whether the target for the horizontal dimensions was achievable. However, on the basis that as much as 84% of the ESARR 4 TLS has been allocated to the horizontal dimensions, it is unlikely that a significantly better apportionment could be arrived at

[5] Includes not only those SC1 events which ATM causes but also those which ATM should prevent but fails to do so.

[6] In practice these levels should be quantified in terms of annual totals, and normal and peak flow rates for the airspace concerned

Intentionally Blank

3 Stage 2: Specification of Safety Functions and Objectives

3.1 Stage 2.1: Functional Design

A functional service-level model of ATM for the airspace under consideration was developed, based upon the generic model defined in Appendix A of the Method.

The model, presented in Figure 1, shows a Vertical Separation (VS) function in a path parallel to Tactical Conflict Resolution (TCR) and Strategic Conflict Resolution (SCR) but sharing the outputs from Tactical Conflict Detection (TCD) and Strategic Conflict Detection (SCD). The rationale for this is that VS is effectively one of two possible ways of resolving (or avoiding) a conflict in the horizontal dimension (the other being TCR or SCR as appropriate).

The following points should be noted in respect of the model:

- Vertical Separation is in fact both strategic and tactical [7]
- None of the Traffic Management functions is applicable to the vertical dimension. Airspace management is not applicable because airspace design is taken into account later under the heading of domain knowledge (it is a one-off - or infrequently recurring - activity rather than an ongoing process). Flow management is applicable only to prevailing direction of flight – ie the horizontal dimension.
- Flight Progress Monitoring was not included at this stage, as it did not seem to apply in the vertical dimension. [8]

In a full exercise, it would be necessary to specify the whole ATC service at this stage of the process. **For the purpose of this example**, only the **Vertical Separation** and Aircraft-based functions are refined, as shown in Figure 2, below.

[7] In effect, it is used by both the planner and executive (radar) controller, though the distinction between these roles is not made herein.

[8] Flight Progress Monitoring would have merged emerged later in the process, in a specific form, as a mitigation against aircraft deviating from assigned FL, had that particular hazard (see H3 in paragraph 3.5.1) been analysed in full.

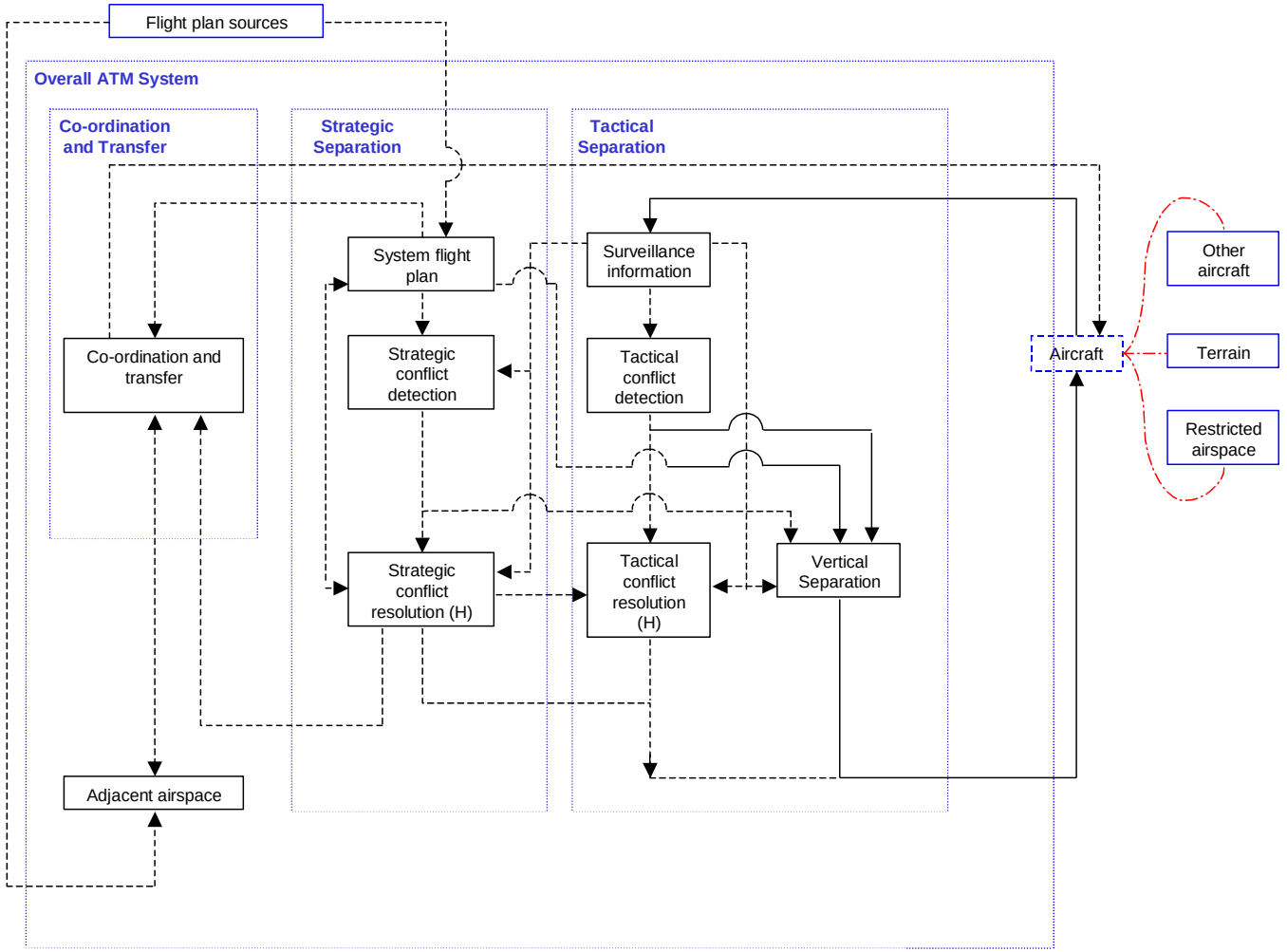

Figure 1: Overall Service-Level Functional Model

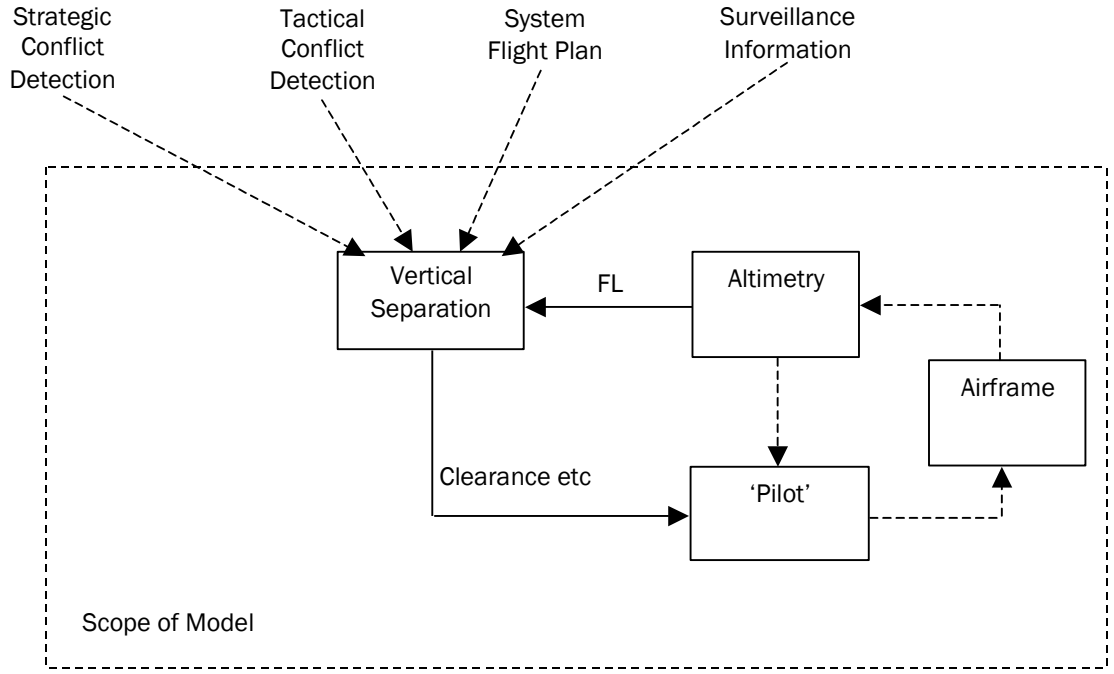

Figure 2: Expanded Model - Vertical Separation Functional

Vertical Separation is a double closed-loop system which, as noted above, is triggered by detection of a conflict (TCR or SCR) in the horizontal dimension and may be used either tactically or strategically, using Surveillance and / or Flight Plan information and current aircraft Altimetry information.

The resolution, in the form of a (vertical) clearance is sent to the 'Pilot' function, which sends a climb / descend / maintain command to the Airframe. Current Altimetry information is fed back to the 'Pilot', forming an inner closed loop (shown by the dotted arrows) that places the aircraft on the required vertical trajectory / at the required flight level, as appropriate.

3.2 Stage 2.2: Safety Functions

The initial ATM safety function **Vertical Separation** (SF1) was then specified as follows:

1 Functionality

SF1.1: **Vertical Separation** shall provide safe vertical separation of aircraft by assigning them vertical trajectories that ensure that the minimum separation criteria are maintained according to the RVSM status of the aircraft involved. For aircraft in cruise, this is done by assigning them to different, pre-determined fixed flight levels, according to the RVSM status of the aircraft involved and the direction of flight.

2 Accuracy

SF1.2: Under normal operating circumstances, **Vertical Separation** shall assign an aircraft precisely to the appropriate fixed flight level (ie zero error tolerance).

3 Timing

SF1.3: When used to resolve a horizontal conflict, a safe **Vertical Separation** solution shall be generated and delivered to the **Pilot**[9], within a total elapsed time of *20 seconds*.[10]

4 Capacity

SF1.4: The capacity of **Vertical Separation** shall be sufficient to handle 15 aircraft per sector safely at any given time under normal operating conditions[11].

5 Overload tolerance:

SF1.5: The capacity of **Vertical Separation** shall be sufficient to handle 20 aircraft per sector safely at any given time under peak traffic conditions.

6 Robustness:

SF1.6: Safe[12] vertical separation shall be maintained under abnormal (as well as normal) operating conditions – eg aircraft on-board emergencies and loss of R/T communications.

7 Maintainability:

SF1.7: The system shall maintain the specified level of performance and reliability[13] throughout its operational life.

3.3 Domain Knowledge

In drawing up the above models and safety functions, the following items of operational **domain knowledge** were identified:

ODK2: Fixed flight levels are defined from FL290 to FL410 at intervals of 1000 feet.

ODK3: Permitted directional use of the fixed flight levels is defined in the Flight Level Orientation Scheme for EUR RVSM airspace as modified in specific areas by Letters of Agreement (LoAs) between ACCs[14].

ODK4: All adjacent airspace, above and below, is non-RVSM airspace [15] All adjacent airspace, horizontally, is RVSM airspace.

---

[9] Note that 'Pilot' is used generically and may take the form of Flight Crew or autopilot

[10] Required for tactical control. Less critical for strategic control.

[11] The capacity dimensions for SF1.4 and SF1.5 are purely arbitrary values chosen for the purpose of this example.

[12] "Safe" means meeting the TLS. However, this does not mean that the service has to achieve the same level of performance under abnormal conditions as it does under normal conditions - the time at risk should be very much lower for the former compared with the latter.

[13] As stated in the methodology, reliability requirements cannot be defined until the functional risk assessment stage.

[14] To be detailed

[15] See paragraph 2.1

ODK5: RVSM airspace rules[16] specify the following vertical separation minima:

1 1000 ft between RVSM-approved aircraft.

2 2000 ft between:

- non-RVSM-approved State aircraft and any other aircraft operating within the EUR RVSM airspace.
- all formation flights of State aircraft and any other aircraft operating within the EUR RVSM airspace.

ODK6: It is assumed that aircraft technical height keeping performance will be within ICAO MASPS requirements [3]

ODK7: Operational procedures require flight crew to maintain the assigned flight level under normal operating conditions.[17].

Additional domain knowledge is identified at various subsequent stages of the process below.

This concludes Stage 2.2 for this example – ie the initial safety functions related to **Vertical Separation** have been defined.

3.4 Stage 2.3: Performance Risk Assessment

At this point, and before safety objectives can be specified for the above ATM safety functions, it is necessary to know how much of each TLS needs to be allocated to the performance aspects of safety function SF1, in the absence of failure.

Were it not for the fact that RVSM had recently been introduced into the airspace under consideration, it could have been argued from a historical perspective that the separation minima are set such that the principal performance risk associated with Vertical Separation - ie aircraft technical height keeping error - is negligible. However, given that the separation minima were halved in 2002, a historical argument is not possible and, therefore, a mathematical model of vertical collision risk is required, as used on the RVSM Height Monitoring Programme. The results obtained on this Programme show in [2] that, in the absence of failure, the risk of collision is no more than 1% of the total TLS (ie is negligible in the context of the analysis herein). Therefore, in this case it is reasonable to carry the whole TLS of 2.5×10^{-9} pfh forward to Stage 2.6, to cover system failures.[18]

[16] As defined in [3]

[17] An exception to normal operating conditions here would be, for example, acting on a TCAS resolution advisory.

[18] Had the risk from aircraft technical height keeping error been significant only the appropriate portion of the TLS would have been carried forward to Stage 2.6.

3.5 Stage 2.4: Functional Hazard Assessment

3.5.1 Hazard Identification

Although there is only one overall hazard (**H0** – *aircraft at wrong flight level*), it is appropriate to consider the hazards that exist at the boundary of each of the functions / sub-functions shown in Figure 2.[19] [20] Where applicable, two types of failure mode – loss and corruption, are considered for each function [21].

1 Vertical Separation

H1: Loss of **Vertical Separation** function.

H2: **Vertical Separation** function assigns an inappropriate flight level to an aircraft. [22].

2 Pilot

H3: **Pilot** deviates from cleared level [23]

3 Airframe[24]

H4: **Airframe** is unable to maintain cleared level

4 Aircraft[25]

H5: Non-RVSM approved aircraft is indicated as RVSM approved

H6: Detectable loss of aircraft RVSM capability

5 Altimetry System

H7: Undetectable altimetry system error

---

[19] The decision at which level to carry out hazard identification is a matter of judgement – see[1]

[20] As noted in the TLS Methodology, it is not sufficient to consider only hazard associated with the failure of the ATM aspects of the system, otherwise a whole set of vital ATM safety functions / objectives – ie those related to the mitigation of hazards in the non-ATM functions / application domain – would be missed.

[21] The list is illustrative for the purposes of this example and not necessarily exhaustive - in real applications of the Guidance, other failure modes (eg lateness in performing the function) may also need to be considered.

[22] "Inappropriate" here means either that the FL to which the aircraft is assigned (or through which it needs to pass in order to comply with its clearance) is occupied by another aircraft such that the relevant horizontal separation minimum is (or could be) substantially infringed.

[23] This hazard assumes that the Pilot function is given correct information but produces incorrect outputs to the Airframe function causing the aircraft to deviate from the level cleared by ATC

[24] The term airframe is used here to denote the aircraft less the pilot / autopilot, and altimetry systems.

[25] The term aircraft includes pilot / autopilot, and altimetry systems since the properties of these determine whether the aircraft is RVSM approved / capable.

Figure 3 shows these hazards in the context of the system functional model.

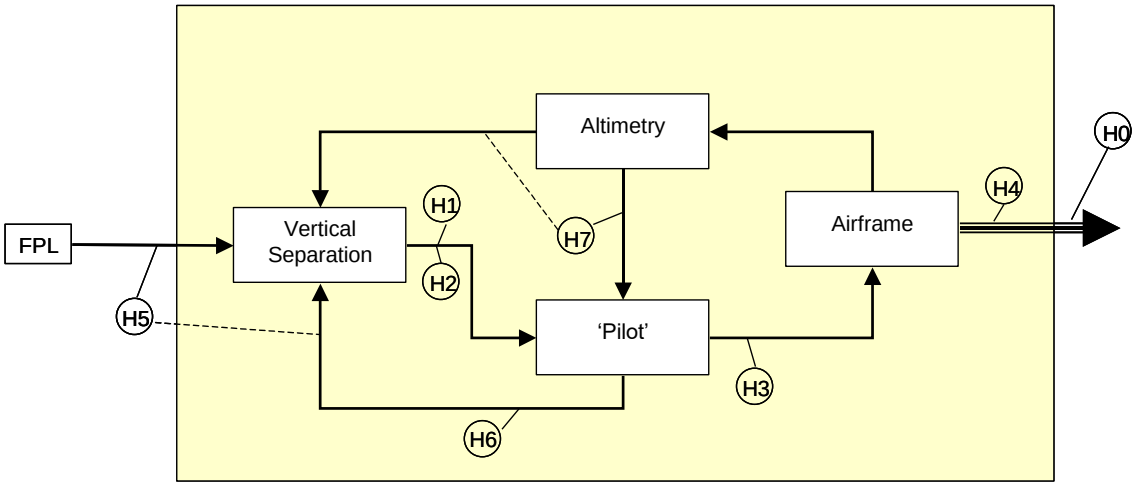

Figure 3: System Functional Hazard Model

3.5.2 Hazard Consequence Analysis – General

Hazard Consequence Analysis was carried out using an Event Tree approach. The potential mitigations (deliberate and circumstantial) and related outcomes were identified in each case. The probability of success or failure of each mitigation was then estimated and the rationale for the estimates recorded.

Two examples of the analysis, Hazard 1 and Hazard 5, are discussed respectively in paragraphs 3.5.3 and 3.5.4 below. Hazard 5 was chosen as an example of a hazard that lies outside of the function (Vertical Separation) for which safety objectives are to be determined; Hazard 1 stems directly from failure of the Vertical Separation function itself.

3.5.3 Hazard 1 – Consequence Analysis

H1: Loss of Vertical Separation function.

3.5.3.1 Mitigation Identification

The two main means of mitigating the consequences of Hazard 1 identified in the assessment are shown below, together with an assessment of the expected probability that the mitigation would not be successful:

1 Horizontal Separation is Possible

Probability that mitigation will NOT work = 0.2

Of course Vertical Separation is only one way of separating aircraft. This mitigation allows for the possible use of Horizontal Separation, assuming that it hasn't failed as well. Until the possible **causes** of loss of Vertical Separation are determined, the **estimated** probability of failure of the mitigation cannot be ascertained. The value **assumed** at this stage is 20% and implies an independence safety objective for Vertical Separation (see **Error! Reference source not found.** below)

2 No other aircraft in horizontal overlap

Probability that mitigation will NOT work = 10^{-3}

This mitigation is circumstantial – ie it is a matter of pure chance that even if an aircraft is at the wrong altitude there will not be another aircraft in the same horizontal proximity at the same time. The value used was obtained from the *horizontal overlap frequency* derived in the EUR RVSM Post-implementation Safety Case [2].

3.5.3.2 Event Tree Analysis

The Event Tree for Hazard 1 is shown at Figure A.1 of Appendix A. At this stage, the frequency (w) of occurrence is set to unity in order to show the probability of the various outcomes (consequences) given that the hazard had already occurred. Each of the Q values represents the probability of failure of the mitigation (see paragraph 3.5.3.1 above) at the head of each of the next two columns.

The Event Tree shows that the probability of an SC1 event resulting from Hazard 1[26] is 2x 10^{-4}. This figure is carried forward to the risk analysis in paragraph 3.6 below.[27]

3.5.4 Hazard 5 – Consequence Analysis

H5 - Non-RVSM approved aircraft is indicated as RVSM approved

3.5.4.1 Further Domain Knowledge

A key rule, of relevance to this hazard, applies in RVSM airspace:

ODK8: In order to reduce the risk from mixed-mode operations, non-approved civil aircraft are not permitted to enter RVSM airspace.

Both ODK6 and ODK8 require ATC to have the correct indication of RVSM approval status especially, from a safety perspective, for non-approved aircraft. The result of Hazard 5, if undetected, would therefore be that an unapproved aircraft would be given inadequate (ie 1000 ft) separation.

3.5.4.2 Mitigation Identification

The main means of mitigating the consequences of Hazard 5 identified in the assessment are shown below, together with an assessment of the expected probability that the mitigation would not be successful:

1 Flight crew recognises and notifies ATC of aircraft non RVSM status

Probability that mitigation will NOT work = 10^{-1}

[26] Ie given that given that H1 has occurred

[27] It is recognised that **safety nets** might be available to prevent an accident resulting from this hazard. However, the benefits of neither STCA nor TCAS are counted in the analysis because STCA is not in universal use (and may well suffer a common-cause failure with Vertical Separation) and current ICAO / EUROCONTROL policy is not to include TCAS as a mitigation in risk analysis.

It was felt that in most cases the Flight Crew would be aware of the true RVSM status of their aircraft even though, say, the FPL filed by the AOC might be in error – indeed Flight Crew are required to confirm that status before entering RVSM airspace from non-RVSM airspace. Therefore where a mistake had been made, leading to ATC giving a non-RVSM aircraft clearance into RVSM airspace, the Flight Crew would normally recognise that and advise ATC, for the appropriated re-clearance action to be taken.

2 No other aircraft in horizontal overlap

Probability that mitigation will NOT work = 10^{-3}

This is the same as Mitigation 2 for Hazard 1.

3 Other aircraft is RVSM approved

Probability that mitigation will NOT work = 1.5×10^{-4}

This mitigation is intended to account for the fact that, should the aircraft in question be in horizontal overlap with another aircraft, the probability that the two aircraft will be in vertical overlap will depend on, inter alia, whether the second aircraft is also non RVSM approved (but indicating that it is approved).

The probability that the mitigation will not work was obtained from the probability that the second aircraft would be not approved (ie 0.15%, as per [2]) multiplied by the probability that the error would not be detected by the Flight Crew for that aircraft (ie mitigation #2 above).

4 No vertical overlap with other aircraft

Probability that mitigation will NOT work = 10^{-3}

It is assumed (pessimistically) that whenever two non-approved aircraft are nominally separated by 1000 ft in RVSM airspace then vertical overlap will occur – therefore the mitigation is ineffective. However, if one of those two aircraft is RVSM approved the probability of vertical overlap is three orders of magnitude lower – see EUR RVSM Post-implementation Safety Case [2] – hence the (relative) mitigation of 10^{-3}.

3.5.4.3 Event Tree Analysis

The above process was then followed for Hazard 1 to produce the Event Tree at Figure A.2 of Appendix A.

The Event Tree shows that two paths lead to a SC1 event [28], and that the combined probability of an SC1 event resulting from Hazard 5 [29] is 1.15×10^{-7}. This figure is carried forward to the risk analysis in paragraph 3.6 below.

[28] An attempt was made to assess the severity of the hazard using the EATMP ANS Safety Assessment Methodology. The initial conclusion was SC 2/3 on the basis that the hazard represented a 50% reduction in the applied separation (2000 ft to 1000 ft). However, further consideration identified two problems with this approach – ie the severity of the hazard should depend on the size of the aircraft's altimetry error and on whether the aircraft comes into proximity with other aircraft and whether or not they are RVSM approved. It was concluded therefore that the classification scheme could not be applied satisfactorily to hazards and further attempts to do so were abandoned. However, it was found to be useful to categorise the outcomes as shown on the Event Trees

It should be noted that NO safety nets are available to prevent an accident resulting from this hazard; both STCA and TCAS use pressure altitude and rely on correct RVSM status, and would therefore be unaware of the existence of the hazard.

3.5.5 Other Hazards – Consequence Analysis

[Repeating the above process for the other hazards would complete Stage 2.4, identifying in each case the possible mitigations and the probability that the hazard (having occurred) would lead to an SC1 event]

3.6 Stage 2.5: Functional Risk Assessment

3.6.1 Risk Tolerability Scheme

A preliminary risk assessment was done in order to determine the tolerable frequency of occurrence of each hazard and hence derive the safety objectives for each safety function. Recognising that the safety objectives could not be confirmed until a full causal analysis is carried out – ie when the safety functions / objectives are allocated to the relevant subsystem, as in paragraph 4.2.1 below - a Risk Tolerability Scheme (RTS) was devised for ST1, in Table 1.

	Prob (SC1 / Hazard)					
No of Hazards	**1.00E-02**	**1.00E-03**	**1.00E-04**	**1.00E-05**	**1.00E-06**	**1.00E-07**
1	*2.5E-07*	*2.5E-06*	*2.5E-05*	*2.5E-04*	*2.5E-03*	*2.5E-02*
2	*1.3E-07*	*1.3E-06*	*1.3E-05*	*1.3E-04*	*1.3E-03*	*1.3E-02*
5	*5.0E-08*	*5.0E-07*	*5.0E-06*	*5.0E-05*	*5.0E-04*	*5.0E-03*
7	*3.6E-08*	*3.6E-07*	*3.6E-06*	*3.6E-05*	*3.6E-04*	*3.6E-03*
10	*2.5E-08*	*2.5E-07*	*2.5E-06*	*2.5E-05*	*2.5E-04*	*2.5E-03*

Table 1: Risk Tolerability Scheme for Satisfaction of ST1

The table specifies the maximum frequency of occurrence for a particular hazard, for the ST to be met, depending on:

- The total number of hazards in the system, and
- The value of *Prob (SC1 / Hazard)* - ie the probability that an SC1 event will occur given that the hazard has already occurred.

such that the product *Number of hazards* **x** *Prob (SC1 / Hazard)* **x** *Maximum frequency of occurrence* = the risk specified in the safety target.

For example:

[29] Ie given that given that H5 has occurred

- If a total of 5 hazards contribute to ST1, then any hazard that has a probability of $1x10^{-4}$ of leading to an SC1 event can occur at a frequency of not greater than $5.0 x10^{-6}$ pfh.

- If a total of 7 hazards contribute to ST1, then any hazard that has a probability of $1x10^{-6}$ of leading to an SC1 event can occur at a frequency of not greater than $3.6x10^{-4}$ pfh

3.6.2 Risk Analysis against ST1

In assessing risk against the ST1, all seven hazards associated with the vertical dimension (see paragraph 3.5.1 above) need to be included since each hazard either

1 Lies within the ATM system loop – irrespective as to whether the problem is in the ground, air or space segment of that loop.

2 Or lies outside of the ATM loop but ATM could reasonably have been expected to mitigate the initiation or consequence of the causal event.

Therefore, for **Hazard 1**, as analysed in paragraph 3.5.3.2 above, we have:

- Total no of hazards contributing to risk: 7

- Prob (SC1 / Hazard 1): $2.0 x 10^{-4}$

It should be noted that the Event Tree for Hazard 1 contains an outcome "ATCO applies horizontal separation" which has been allocated SC4 in recognition of the fact that it might involve a significant increase in ATCO workload while the hazard is being dealt with. In this sense the outcome is "undeveloped" – ie it could in itself lead (through a mistake on the part of the ATCO) to an SC1 event. For the purpose of this analysis it is assumed that the probability of this SC4 event leading to an SC1 event is not more than 10^{-6}. and therefore its contribution to the overall risk of an SC1 event is relatively negligible at $8x10^{-7}$.

Given the total probability of $2.0x10^{-4}$ for an SC1 event, the following can be interpolated from Table 1:

The occurrence rate for Hazard 1 must be not greater than $1.8 x 10^{-6}$ pfh

Similarly, in for **Hazard 5** we have:

- Total no of hazards contributing to risk: 7

- Prob (SC1 / Hazard 5): $1.15 x 10^{-7}$ (see paragraph 3.5.4.3 above)

It should be noted that the Event Tree for Hazard 5 contains an outcome "ATC applies 2000ft separation ....." which has been allocated SC4 (increase in ATCO workload). Again, assuming that the probability of this SC4 event leading to an SC1 event is not more than 10^{-6}, its contribution to the overall risk of an SC1 event is a further $9x10^{-7}$ – ie greater than the more direct SC1 outcomes!

Given the total probability of $1.015x10^{-6}$ for an SC1 event, the following can be interpolated from Table 1:

The occurrence rate for Hazard 5 must be not greater than $3.5 x 10^{-4}$ pfh

3.6.3 Stage 2.5 Conclusion

The above maximum occurrence rates for each hazard, are used in Stage 2.6 to derive the associated safety objectives. [30]

3.7 Stage 2.6: Derived Safety Properties

3.7.1 Safety Objectives

The maximum frequency of occurrence for Hazards 1 and 5 above, are now expressed as initial [31] safety objectives, as follows:

> **SO1**: Loss of the Vertical Separation function shall not occur at a frequency greater than 1.8×10^{-6} pfh.[32]
>
> **SO2**: The frequency with which a non-RVSM-approved aircraft is indicated to the ATCO as being RVSM approved shall not be greater than 3.5×10^{-4} pfh.[33]

3.7.2 Additional Safety Functions

Additional safety functions are required to implement any deliberate mitigations for other hazards. In this limited example, the following procedure safety functions may be deduced from Hazard 1, in order to provide the mitigation "Horizontal separation possible":

> **SF2**: In the event of failure of the Vertical Separation function, Horizontal Separation shall be applied to all aircraft in the affected airspace.[34]

The following three procedure safety functions may be deduced from Hazard 5, in order to provide the mitigation " Flight Crew recognises [error] and notifies ATC of aircraft non-RVSM status":

> **SF3**: ATC shall confirm with the Flight Crew the RVSM status of each aircraft before the aircraft is cleared into RVSM airspace.
>
> **SF4**: In the event that a non-RVSM (non-State) aircraft is found to be in RVSM airspace, the ATCO shall apply 2000 ft separation to that aircraft and shall expedite clearance of the aircraft out of RVSM airspace. [35]

---

[30] In a full analysis the same process would be followed for the other five hazards, leading to maximum occurrence rates for each

[31] Ie subject to subsequent causal analysis

[32] A safety objective would be created for **corruption** of Vertical Separation (from Hazard 2)

[33] Similar safety objectives would be created for all of the other system functions, in order to limit the frequency of occurrence of each associated hazard.

[34] This is a safety function / objective for Horizontal Separation – it also has training implications, for which safety functions should be derived.

SF5: The Flight Crew shall check the RVSM status of the aircraft from the aircraft manual, before departure, and shall report the status to ATC on first entering RVSM airspace

3.7.3 Independence Safety Objectives

The mitigation "Horizontal Separation possible" for Hazard 1 has an assumed success rate of 80%, hence implying the following safety objective:

SO3: The probability that **Horizontal Separation** fails, Vertical Separation having already failed, shall not be greater than 0.2.

No independence safety objectives emerged from analysis of Hazard 5.

3.7.4 More Domain Knowledge

The circumstantial mitigations identified in the above Event Trees were explicitly captured as Domain Knowledge, as follows:

ODK9: It is assumed that the instantaneous probability of two aircraft being in horizontal overlap, is not greater than 10^{-3}.

ODK10: It is assumed that the probability of a non-RVSM approved aircraft in RVSM airspace being in close proximity with another non-RVSM approved aircraft is not greater than 1.5×10^{-4}.

ODK11: It is assumed that whenever two non-approved aircraft are nominally separated by 1000 ft in RVSM airspace then vertical overlap will occur. However, if one of those two aircraft is RVSM approved the probability of vertical overlap is three orders of magnitude lower.

3.7.5 Stage 2.6 Conclusion

System-level safety functions (SF1 to 5) and safety objectives (SO1-3) have now been defined, as listed in Table B.1 of Appendix B.

In Stage 3, these will be allocated and apportioned to the subsystems identified in the high-level architectural design of the system.

3.7.6 Stage 2.7: Validation of Safety Functions / Objectives

It is beyond the scope of this worked example to carry out a formal validation of the above safety functions and objectives. However, this paragraph highlights the key issues that would normally be addressed.

The satisfaction argument should demonstrate that:

1 Given the accuracy of aircraft height keeping assumed in ODK6, and the other domain knowledge set out in ODK2 to 5, the ATM safety functions are sufficient to ensure that the probability of an SC1 event in the absence of failure is negligible.

[35] For some complex or equipment-based mitigations it may be appropriate to formally specify a maximum probability of failure (on demand) as a safety objective. That was judged to be unnecessary in this case

2 Given the domain knowledge set out in ODK6 to 11, the safety objectives are sufficient to ensure that the probability of an SC1 event due to failure Is not greater than 2.5×10^{-9} per flight hour.

In relation to item 1, there is no historical basis for arguing that risk associated with 1000ft separation for RVSM-approved aircraft is negligible – that inevitably requires mathematical modelling of the relationship between aircraft technical height-keeping errors and collision risk, for the stated separation minima and traffic conditions. Such a collision-risk analysis (CRA) was carried out on the EUR RVSM Programme and [2] provides sufficient evidence to show that the risk of collision in the absence of failure is no more than 1% of the TLS.

In addressing item 2, techniques such as Fault Tree and Event Tree analysis can be used to model static properties of the system in support of the satisfaction argument. However, it is also very important that the dynamic aspects of the ATM safety functions, included interactions between functions as outlined in Figure 2, are modelled in order to ensure that the safety functions are complete and correct.

Intentionally Blank

4 Stage 3: Subsystem Safety Requirements

4.1 Stage 3.1: High-level Architectural Design

Figure 4 shows a high-level architectural design of the system to implement the safety functions determined above. The allocation of those safety functions (and corresponding safety objectives) to the main elements of the design is shown at Appendix B.

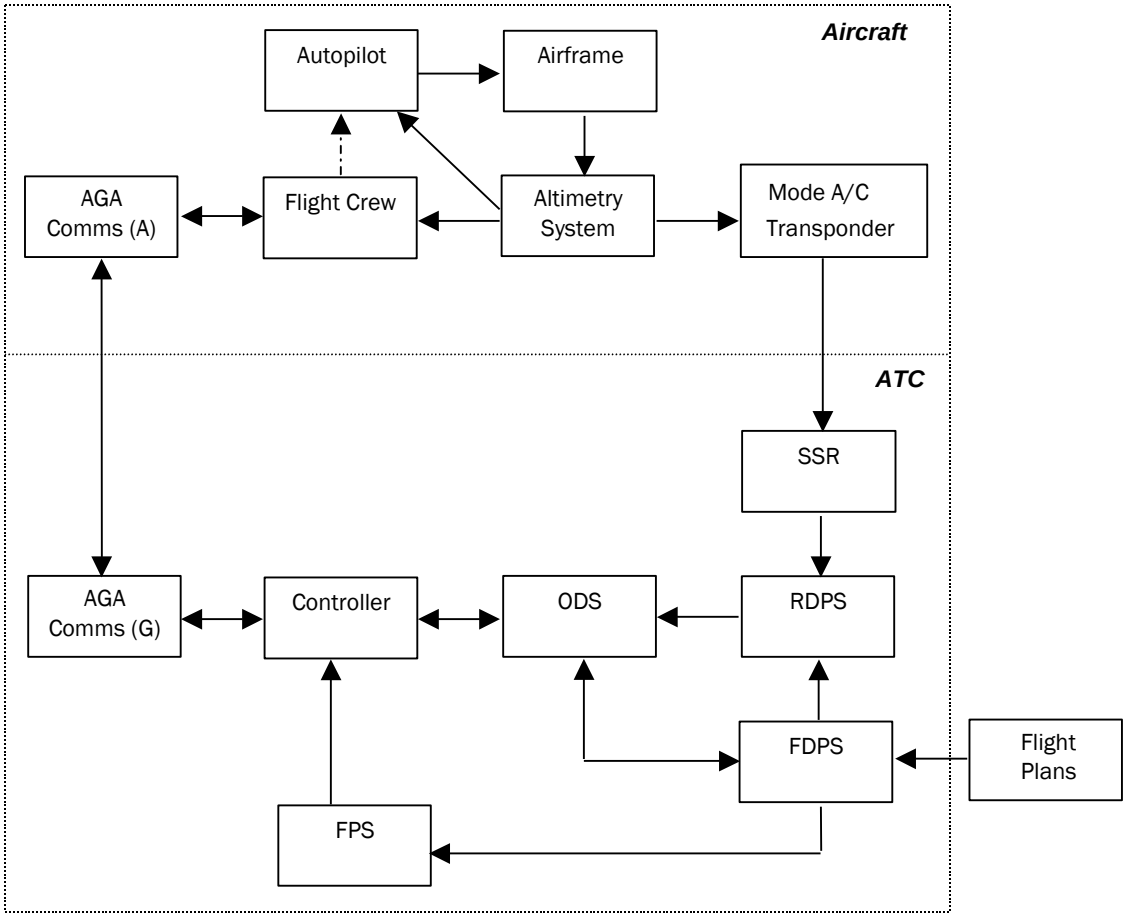

Figure 4: High-level Architectural Design

Each functional block is described below. Note that these descriptions are restricted to functions which are relevant to Vertical Separation. In reality, some of the functional blocks will perform other additional functions not identified here.

4.1.1.1 Functional Description: Controller

The *Controller* receives the air situation display presented by the *ODS*, and, based upon this information, issues clearances and other instructions to *Flight Crew* via *AGA Comms (G & A)* as necessary to maintain the required separation minima between aircraft. The *Controller* also receives flight progress strips (*FPS*) from *FDPS* for each aircraft under his control, and maintains the flight data to record clearances issued and progress achieved.

4.1.1.2 Functional Description: ODS

The *ODS* presents a continually updated air situation display to the *Controller*, taking input from the *RDPS* and *FDPS*. ODS also provides an input facility for the *Controller* to selectively modify the flight data, feeding the data (unmodified) to the *FDPS*. The *ODS* shows a considerable amount of data – in the context of this analysis it is important to note that it provides the aircraft's current FL (pressure altitude), Assigned Flight Level, vertical transition data and RVSM status.

4.1.1.3 Functional Description: FDPS

The *FDPS* receives system flight plans from external sources. It passes relevant sub-sets of the flight plan data to *FPS* (for flight strip printing), to *RDPS* (for code-callsign correlation) and to *ODS* (to allow for editing by the *Controller*). It updates system flight plan status in response to changes made by the *Controller* via the *ODS*. In particular, the FDPS provides RVSM status and the aircraft's Requested FL.

4.1.1.4 Functional Description: RDPS

The *RDPS* receives secondary radar information - ie aircraft position, code (mode A) and flight level (mode C) from *SSR* - correlates this information with the callsign matching the mode A code using system flight plan information received from *FDPS*, and sends the resulting track information to the *ODS* for presentation.

4.1.1.5 Functional Description: FPS

The *FPS* receives system flight plan information from the *FDPS*, and prints this information on paper strips which are then used by the *Controller*. The FPS data is replicated on, and maintained through, the ODS.

4.1.1.6 Functional Description: SSR

SSR interrogates all *SSR Transponders* within its area of coverage, and receives mode A and mode C SSR data (when available) in return. The interrogation process is repeated at intervals of 7 seconds. It encodes the data and sends it to *RDPS* for further processing.

4.1.1.7 Functional Description: AGA Comms (Ground)

AGA Comms (Ground) provides a transmit and receive facility for the *Controller* to communicate by voice radio with the *Flight Crew* via *AGA Comms (Air).*

4.1.1.8 Functional Description: AGA Comms (Air)

AGA Comms (Air) provides a transmit and receive facility for the *Flight Crew* to communicate by voice with the *Controller* via *AGA Comms (Ground)*.

4.1.1.9 Functional Description: Altimetry System

The *Altimetry System* measures the pressure altitude[36] of the *Airframe*, and presents this information to the *Flight Crew*, the *Autopilot* and the *SSR Transponder*.

[36] ie relative to the standard pressure setting of 1013.2 mb.

4.1.1.10 Functional Description: Flight Crew

The *Flight Crew*:

- receives and acknowledge instructions from the *Controller*, via *AGA Comms (Air* and *Ground***)**, to maintain a specific flight level;
- controls the *Airframe* via the *Autopilot* (or, exceptionally, manually, by reference to the pressure altitude displayed by the *Altimetry System*) so as to climb to/descend to/maintain the flight level requested by the *Controller*;
- monitors the performance of the *Airframe,* by reference to the pressure altitude displayed by the *Altimetry System*, to ensure that its vertical performance is as selected via the *Autopilot*, and intervene if necessary.

4.1.1.11 Functional Description: Autopilot

The *Autopilot* controls the *Airframe* so as to climb to/descend to/maintain the flight level selected by the *Flight Crew*.

4.1.1.12 Functional Description: Airframe

The *Airframe* responds to height-keeping control inputs received from the *Autopilot*, or, exceptionally, from the *Flight Crew*.

4.1.1.13 Functional Description: SSR Transponder

The *SSR Transponder*:

- receives pressure altitude (flight level) information from the *Altimetry System*;
- when interrogated by *SSR*, sends a reply which contains both the Mode A transponder code and the latest flight level information (Mode C).

4.2 Stage 3.2: Subsystem Functional Safety Requirements

4.2.1 ATM Safety Function Allocation

The ATM safety functions identified earlier (see paragraphs 3.2 and 3.7.2 above) were allocated to the subsystems identified above – see Appendix B, table B.1.

4.2.2 Specification of Subsystem Safety Functions

Subsystem requirements were then developed so as to satisfy the allocation of the system safety functions (see paragraph 4.2.1, above). In a complete example, this would be done for all subsystems; in the current example it has been developed for the Controller (safety requirements ATCO 1 to 10) and ODS (ODS 1 to 5) only – see Appendix B, table B.2.[37]

[37] In practice, safety requirements for pre-existing non-ATM subsystem may be declared as assumptions, as far as ESARR4 is concerned, as domain knowledge, for the ICAO RVSM TLS case.

4.3 Stage 3.3: Subsystem Risk Analysis

4.3.1 Approach

The safety integrity requirements and additional functional safety requirements for each subsystem were derived using Hazard Causal Analysis (ie "top down") techniques:

4.3.2 Hazard Causal Analysis

4.3.2.1 General[38]

Hazard Causal Analysis was carried using Fault Tree Analysis (FTA) where the top event in each Fault Tree corresponded with the initiating event for the associated Event Tree, thus forming a set of "Bow Tie" models – ie one for each hazard[39].

In most cases, the Fault Tree was decomposed only as far as necessary to identify the contribution of the relevant subsystems; the subsystem failures were recorded as "undeveloped" causal events, for further decomposition at a later (ie PSSA) stage. A frequency of failure (per flight hour) was than ascribed to each causal event, such that the frequency of occurrence of the top-level event (ie the hazard in question) was close to the maximum specified in the related safety target.

4.3.2.2 Fault Tree Analysis - Hazard #1

A Fault Tree for Hazard #1 is shown at Appendix C, Figure C.1.

The failure frequencies assigned to the individual subsystems were then carried forward as safety integrity requirements; see paragraph 4.4.1 below. Within the scope of this example, only the integrity requirements relevant to the controller (ATC012) and ODS (ODS7) were identified; again, in a complete example, similar integrity requirements would need to be associated with each basic or undeveloped event.

4.3.2.3 Fault Tree Analysis - Hazard #5

A Fault Tree for Hazard #5 is shown at Appendix C, Figure C.2.

Note that the fault tree includes both ATM causes and apparently non-ATM causes. For example, corruption of the RVSM status by ODS is an obvious ATM-related cause while the aircraft manual incorrectly presenting the RVSM status as being RVSM-approved is outside the normal scope of ATM. However, the whole concept of RVSM status was made a part of the ATM system in order to reduce a risk caused solely by the introduction of RVSM.

As above, the failure frequencies assigned to the individual subsystems were then carried forward as safety integrity requirements; see paragraph 4.4.1 below. Within the scope of this example, only the integrity requirements relevant to the controller (ATC011) and ODS (ODS6) were identified; in a

[38] In this example only Hazards #1 and #5 are considered – in reality all hazards would have to be analysed.

[39] Although it did not arise in this example, the linking between Event Tree and Fault Tree may sometimes be made at a level below the hazard itself in order, for example, to account for the applicability of consequence mitigations in the Event Tree being dependent on specific causes in the Fault Tree.

complete example, similar integrity requirements would need to be associated with each basic or undeveloped event.[40]

4.4 Stage 3.4: Derived Subsystem Safety Requirements

4.4.1 Safety Integrity Requirements

Safety integrity requirements were deduced from the base events from the Fault Trees as follows[41].

4.4.1.1 Controller

ATC011: The probability that the Controller manually enters the wrong RVSM status into the ATC system shall not exceed $5x10^{-5}$ per flight hour[42].

ATC012: The probability that the Controller fails to separate aircraft vertically (when required) shall not exceed $6x10^{-7}$ per flight hour[42].

4.4.1.2 ODS

ODS6: The probability that the ODS corrupts the displayed RVSM status shall not exceed 10^{-5} per flight hour.

ODS7: The probability that the ODS fails to display aircraft height[43] shall not exceed $5x10^{-7}$ per flight hour.

4.4.2 Additional Functional Safety Requirements

No additional functional safety requirements emerged from the subsystems risk analysis.

4.4.3 Independence Safety Requirements

No independence safety requirements emerged from the subsystems risk analysis.

---

[40] It would normally be important to explore the sensitivity of the probability of success / failure of the mitigations here – particularly those about which there was some uncertainty – otherwise the conclusions from the FTA could be incorrect.

[41] The Safety integrity requirements are based only on the two Fault Trees developed in the example – in reality all the Fault Trees would have to be developed and safety integrity requirements deduced from them in order to ensure that the all the ATM-safety objectives are satisfied.

[42] This is probably an unrealistically high safety objective for an unaided human operator, and would either need (causal) mitigation to be provided at the design stage, or, if this were not possible, it would be necessary to reallocate risk budget within the fault tree.

[43] It is acknowledged that this failure mode – ODS fails to display any aircraft FL but continues to display other aircraft parameters (position, track etc) - is somewhat contrived for the purposes of this simple example. In reality, failure of an ODS is likely to involve the whole display and (assuming a back-up was not immediately available) would render both vertical and horizontal separation impracticable, at that controller position.

4.4.4 System-level Domain Knowledge

SDK1: It is assumed that the probability of a second aircraft suffering a complete loss of SSR Transponder, RT Comms or Altimeter system, given that an aircraft under control of the same ATCO has is already suffering from the same failure, shall not exceed 0.1[44].

4.5 Stage 3.5: Validation of Subsystem Safety Requirements

It is beyond the scope of this worked example to carry out a formal validation of the above safety requirements. However, this paragraph highlights the key issues that would normally be addressed.

The satisfaction argument should demonstrate, inter alia, that:

1 The subsystem safety functional safety requirements are sufficient to implement the ATM service-level safety functions completely and correctly

2 There are no dysfunctional interactions or data inconsistencies in the system.

3 The safety integrity requirements satisfy the ATM service-level safety objectives.

Items 1 and 2 would be addressed typically by (static) design analysis techniques, with ATC operational simulations used to validate the dynamic aspects of the system behaviour.

Item 3 would be addressed typical using subsystem failure consequence analysis (ie “bottom up”) techniques, to complement the top-down causal approach used to derive the safety integrity requirements in the first place (see paragraph 4.3.2 above.

4.6 Stage 3 Conclusion

In Stage 3, the system-level safety functions and safety objectives, produced in Stage 2, were allocated and apportioned to the subsystems identified in the high-level architectural design of the system, to form a (validated) set of functional safety requirements and safety integrity requirements for each subsystem.

[44] See causal mitigation in Figure C.2

Intentionally Blank

5 Safety Monitoring Requirements

5.1 Introduction

The aim of safety monitoring is to measure the achievement of safety against the TLS. However, as the ESARR4 target of 1.55x10-8 SC1 events pfh (ie only about one event every 10 years for the whole of ECAC airspace) then using the frequency of occurrence of SC1 events as a measure of safety would be not only unacceptably retrospective but also statistically inadequate.

In principle therefore, monitoring should use safety indicators that are based on events of lesser severity than SC1 and which, therefore, are likely to occur more frequently. The advantage of such an approach is that much more data are available; however, in using data from lower-level events to predict the frequency of SC1 events requires a correct model of the relationship between the lower-level and SC1 events.

Fault Trees and Event Trees of course provide such a model. The Event Trees at Appendix A, Figure A.3 and A.4 are linked to the Fault Trees at Appendix C, Figure C.1 and C.2 respectively, such that the initiating event in the Event Tree is the same as the top-level event in the corresponding Fault Tree. Therefore the ***w*** value in the first column of the Event Tree shows the frequency of occurrence of the hazard and the penultimate column shows the frequency of occurrence of each possible outcome.

5.2 Safety Monitoring – Hazard 1

The appropriate safety indicators (SIs) for Hazard 1 are as follows:

1 Occurrence of the Hazard itself, against the expected value of 1.76×10^{-6} pfh.

2 Occurrence of the SC2 outcome, against the expected value of 3.5×10^{-7} pfh – TCAS (and possibly) STCA) would be capable of detecting such occurrences. If SI# 1 is within target but SI#2 is high, that would suggest that either the *No other aircraft in horizontal overlap* mitigation is **more** effective than assumed in the model and/or the *Horizontal separation possible* mitigation is **less** effective than assumed in the model.

3 In order to resolve which of the above mitigation conclusions is correct, the occurrence of the SC4 outcome should also be monitored and the appropriate mitigation should be adjusted accordingly. This is most important since it might have significant implications for the frequency of the SC1 outcome .

5.3 Safety Monitoring – Hazard 5

Monitoring for Hazard 5 is more difficult since neither the Hazard itself nor the two SC2/3 outcomes are observable, and also neither STCA nor TCAS would be capable of monitoring any of the outcomes. In this case, it is necessary to select safety indicators from the Event Tree and Fault Tree, as follows:

1 Occurrence of the SC4 outcome, against the expected value of 3.16×10^{-4} pfh. This would give an indication of the frequency of the Hazard, if the assumed effectiveness of the Flight Crew mitigation is correct.

2 Occurrence of the Fault Tree causal events *Incorrect RVSM status from IFPS, ATCO Planner manually enters wrong RVSM status* and *ATC equipment corrupts RVSM approval status*, against

the relevant expected values. These account for about 75% of the expected sources of RVSM status error, and when compared with #1 should provide a reasonable validation of the Flight Crew mitigation.

A Appendix: Event Trees

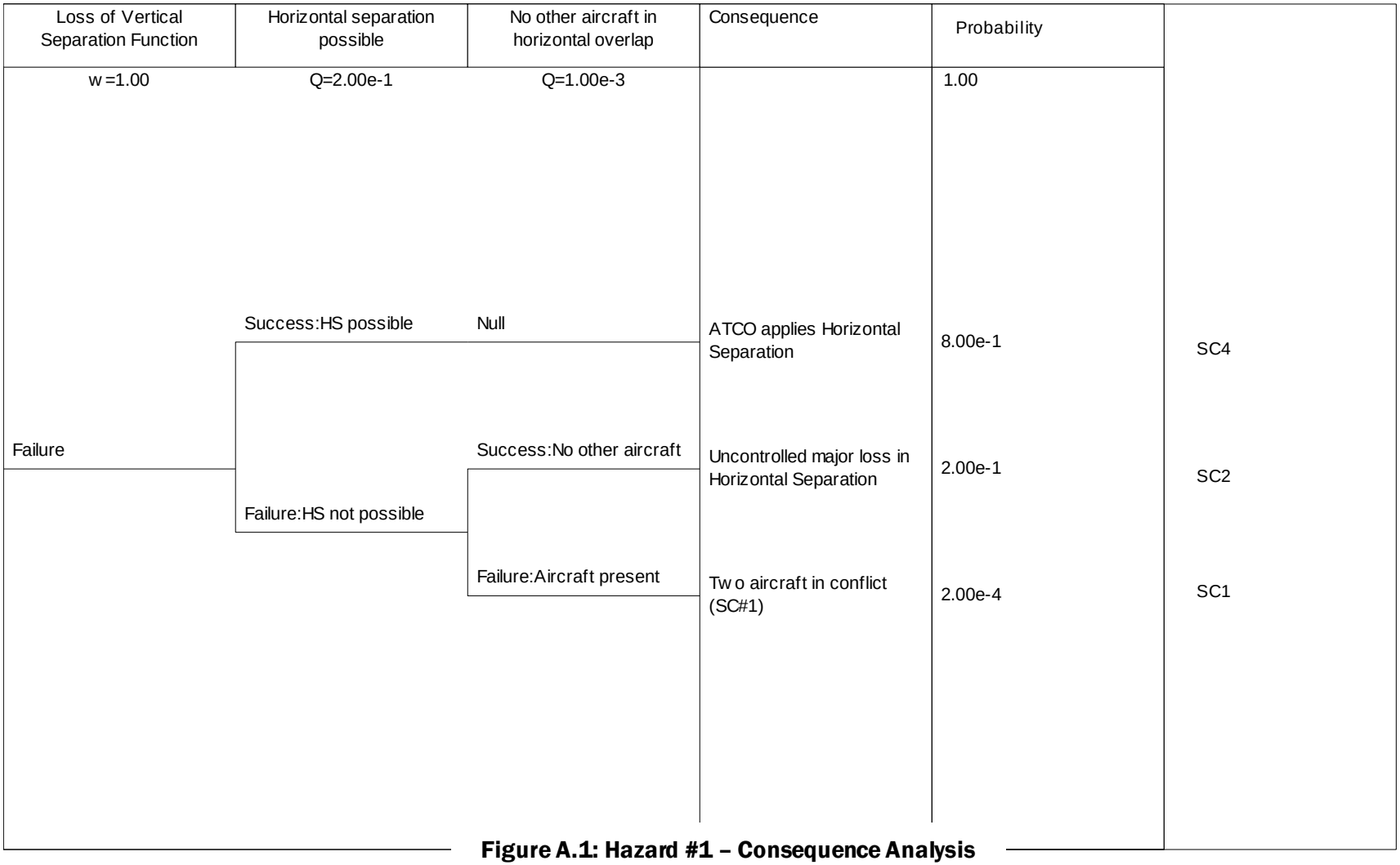

Figure A.1: Hazard #1 – Consequence Analysis

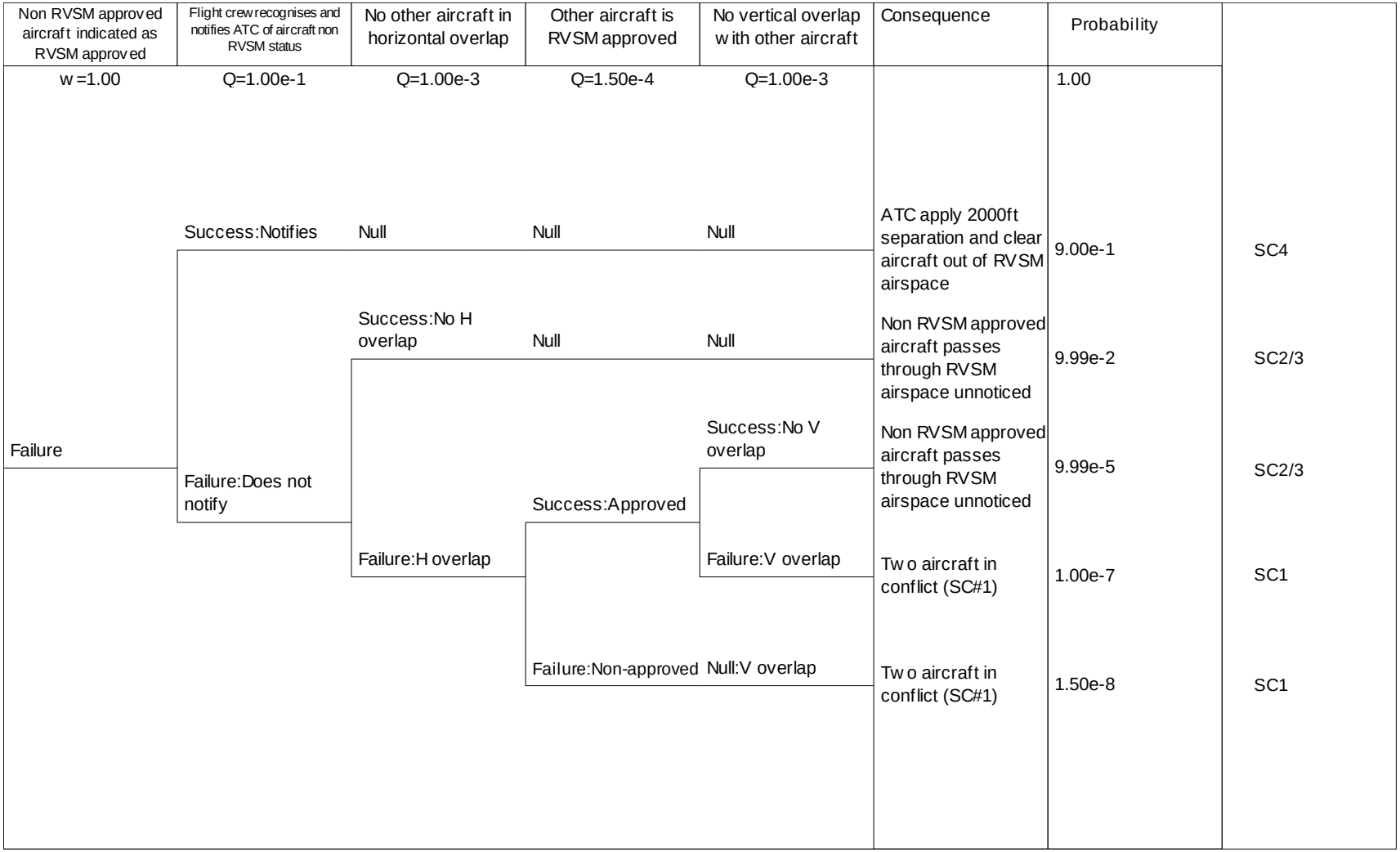

Figure A.2: Hazard #5 – Consequence Analysis

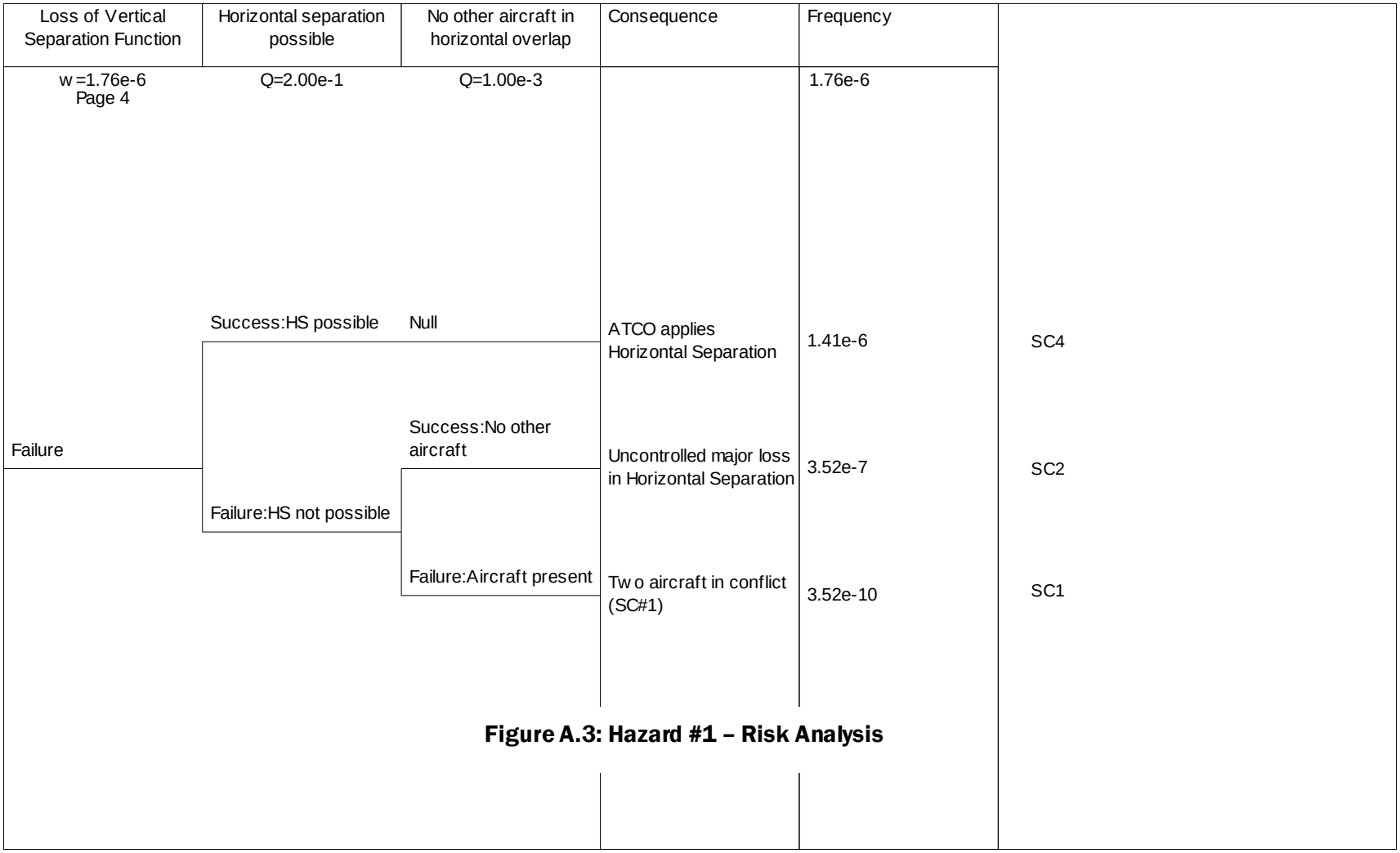

Figure A.3: Hazard #1 – Risk Analysis

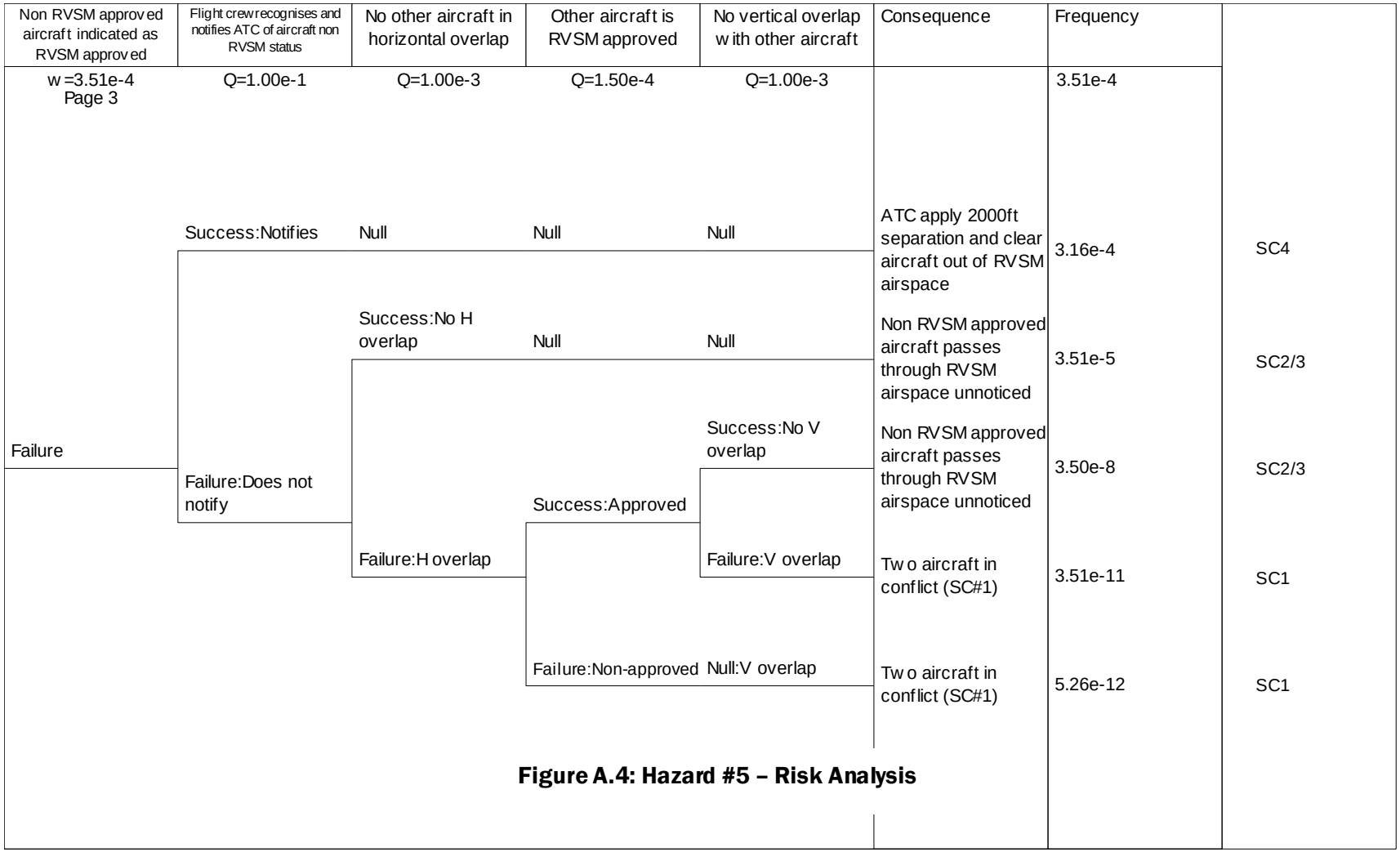

Figure A.4: Hazard #5 – Risk Analysis

Intentionally blank

B Appendix: Safety Functions and Objectives

Table B.1 Safety Function and Safety Objective Allocation

No:	Safety Function / Objective	Attribute	Allocation	Reference
SF1.1	**Vertical Separation** shall provide safe vertical separation of aircraft by assigning them to different, pre-determined fixed flight levels according to the RVSM status of the aircraft involved and the direction of flight.	Function	Controller ODS RDPS FDPS FPS SSR(G) SSR Transponder Altimetry System AGA Comms (G) AGA Comms (A) Flight Crew	ATCO1 ODS1 RDPS1 FDPS1 FPS1 SSRG1 SSRT1 AS1 AGAG1 AGAA1 FC1
SF1.2	Under normal operating circumstances, **Vertical Separation** shall assign an aircraft precisely to the appropriate fixed flight level	Accuracy	Controller ODS RDPS FDPS FPS SSR(G) SSR Transponder Altimetry System	ATCO1 ODS2 RDPS2 FDPS2 FPS2 SSRG2 SSRT2 AS2

No:	Safety Function / Objective	Attribute	Allocation	Reference
SF1.3	When used to resolve a horizontal conflict, a safe **Vertical Separation** solution shall be generated and delivered to the **Pilot**, within a total elapsed time of *20 seconds*	Timing	Controller ODS RDPS FDPS SSR(G) AGA Comms (G) SSR Transponder Altimetry System AGA Comms (A) Flight Crew	ATCO3 ODS3 RDPS3 FDPS3 SSRG3 AGAG3 SSRT3 AS3 AGAA3 FC2
SF1.4	The capacity of **Vertical Separation** shall be sufficient to handle 15 aircraft per sector safely at any given time under normal operating conditions	Capacity	Controller ODS RDPS FDPS FPS SSR(G) AGA Comms (G)	ATCO4 ODS4 RDPS4 FDPS4 FPS3 SSRG4 AGAG3

No:	Safety Function / Objective	Attribute	Allocation	Reference
SF1.5	The capacity of **Vertical Separation** shall be sufficient to handle 20 aircraft per sector safely at any given time under peak traffic conditions	Overload tolerance	Controller ODS RDPS FDPS FPS SSR(G) AGA Comms (G)	ATCO5 ODS4 RDPS4 FDPS4 FPS3 SSRG4 AGAG3
SF1.6	Facilities shall be provided for safe operation under emergency and contingency conditions	Robustness	Controller Flight Crew	ATCO6 FC3
SF1.7	The system shall maintain the specified level of performance and reliability throughout its operational life	Maintainability	Controller ODS RDPS FDPS FPS SSR(G) AGA Comms (G) Altimetry System SSR Transponder AGA Comms (A) Flight Crew	ATCO7,8 ODS5 RDPS5 FDPS5 FPS4 SSRG5 AGAG4 AS3 SSRT4 AGAA3 FC4
SF2	In the event of failure of the **Vertical Separation** function, Horizontal Separation shall be applied to all aircraft in the affected airspace	Function (mitigation)	[Horizontal Separation]	
SF3	ATC shall confirm with the Flight Crew the RVSM status of each aircraft before the aircraft is cleared into RVSM airspace	Function (mitigation)	Controller	ATCO9 FDPS6 FC5
SF4	In the event that a non-RVSM (non-State) aircraft is found to be in RVSM airspace, the ATCO shall apply 2000 ft separation to that aircraft and expedite	Function (mitigation)	Controller	ATCO10

No:	Safety Function / Objective	Attribute	Allocation	Reference
	clearance of the aircraft out of RVSM airspace		FDPS	FDPS7
SF5	The Flight Crew shall check the RVSM status of the aircraft from the aircraft manual, before departure, and shall report the status to ATC on first entering RVSM airspace	Function (mitigation)	Flight Crew	FC6

No:	Safety Function / Objective	Attribute	Allocation	Reference
SO1	Loss of the **Vertical Separation** function shall not occur at a frequency greater than 1.8×10^{-6} pfh	Reliability	[see hazard & risk analysis]	
SO2	The frequency with which a non-RVSM-approved aircraft is indicated to the ATCO as being RVSM approved shall not be greater than 3.5×10^{-4} pfh	Reliability	[see hazard & risk analysis]	
SO3	The probability that **Horizontal Separation** fails, Vertical Separation having already failed, shall not be greater than 0.2	Reliability (mitigation)	[Horizontal Separation]	

Table B.2: Subsystem Safety Requirements

No:	Source	Safety Requirements
Controller		
ATCO1	SF1.1, SF1.2	ATC procedures shall be developed for the provision of safe vertical separation of aircraft by assigning them to different, pre-determined fixed flight levels, according to the RVSM status of the aircraft involved
ATCO2	SF1.1	RT procedures shall be developed for the Controller to pass FL clearances and other instructions to the aircraft, and for acknowledgement of them by the Flight Crew
ATCO3	SF1.3	Given the necessary display and communication facilities, the Controller shall be able to generate, transmit and check acknowledgement of a FL change, in order to resolve a Horizontal conflict, within a total elapsed time of 20 seconds
ATCO4	SF1.4	Given the necessary display and communication facilities, the Controller shall be able to provide Vertical Separation for up to 15 aircraft per sector continually, under normal operating conditions
ATCO5	SF1.5	Given the necessary display and communication facilities, the Controller shall be able to provide Vertical Separation for up to 15 aircraft per sector continually, under peak traffic conditions
ATCO6	SF1.6	ATC procedures shall be developed for the provision of safe Vertical Separation under aircraft emergency and contingency conditions
ATCO7	SF1.7	A process shall be put in place for the monitoring, investigation and correction of Controller errors in relation to Vertical Separation
ATCO8	SF1.7	Continuation training shall be provided for Controllers as necessary to maintain the safe of the Vertical Separation service.

ATC09	SF3	ATC procedures shall be developed to require the Controller to confirm with the Flight Crew the RVSM status of each aircraft before the aircraft is cleared into RVSM airspace
ATC010	SF4	ATC procedures shall be developed to ensure that, in the event that a non-RVSM (non-State) aircraft is found to be in RVSM airspace, the ATCO applies 2000 ft separation to that aircraft and expedites clearance of the aircraft out of RVSM airspace
ATC011	Fault Tree – Hazard 5	The probability that the Planner Controller manually enters the wrong RVSM status into the ATC system shall not exceed $5x10^{-5}$ per flight hour
ATC012	Fault Tree – Hazard 1	The probability that the Controller fails to separate aircraft vertically (when required) shall not exceed $6x10^{-7}$ per flight hour
ODS		
ODS1	SF1.1	The ODS shall provide a display of the FL and RVSM status of each aircraft within the appropriate area of coverage
ODS2	SF1.2	Aircraft FL shall be displayed on the ODS with a resolution of 100 ft, and to an accuracy of 10 ft of the corresponding input data
ODS3	SF1.3	The ODS display of the FL and RVSM status of each aircraft shall be refreshed at intervals of less than 2 seconds.
ODS4	SF1.4, SF1.5	The ODS shall be able to maintain display of at least 100 aircraft within the required area of coverage
ODS5	SF1.7	Maintenance facilities shall be provided to ensure that the specified level of performance and reliability of continue to be met throughout the operational life of the ODS
ODS6	Fault Tree – Hazard 5	The probability that the ODS corrupts the displayed RVSM status shall not exceed 10^{-5} per flight hour.
ODS7	Fault Tree – Hazard 1	The probability that the ODS fails to display aircraft height shall not exceed $5x10^{-7}$ per flight hour

C Appendix: Fault Trees

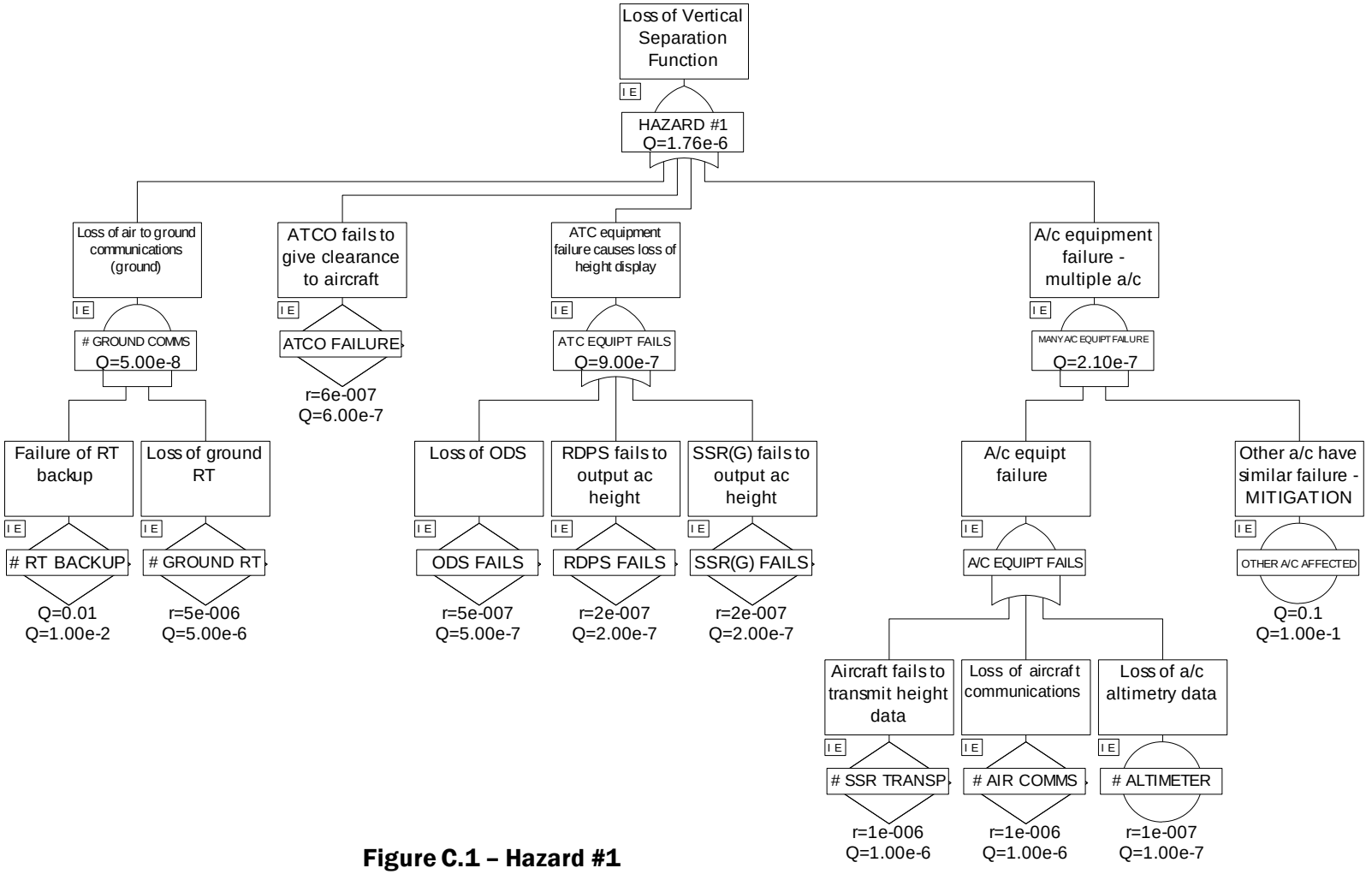

Figure C.1 – Hazard #1

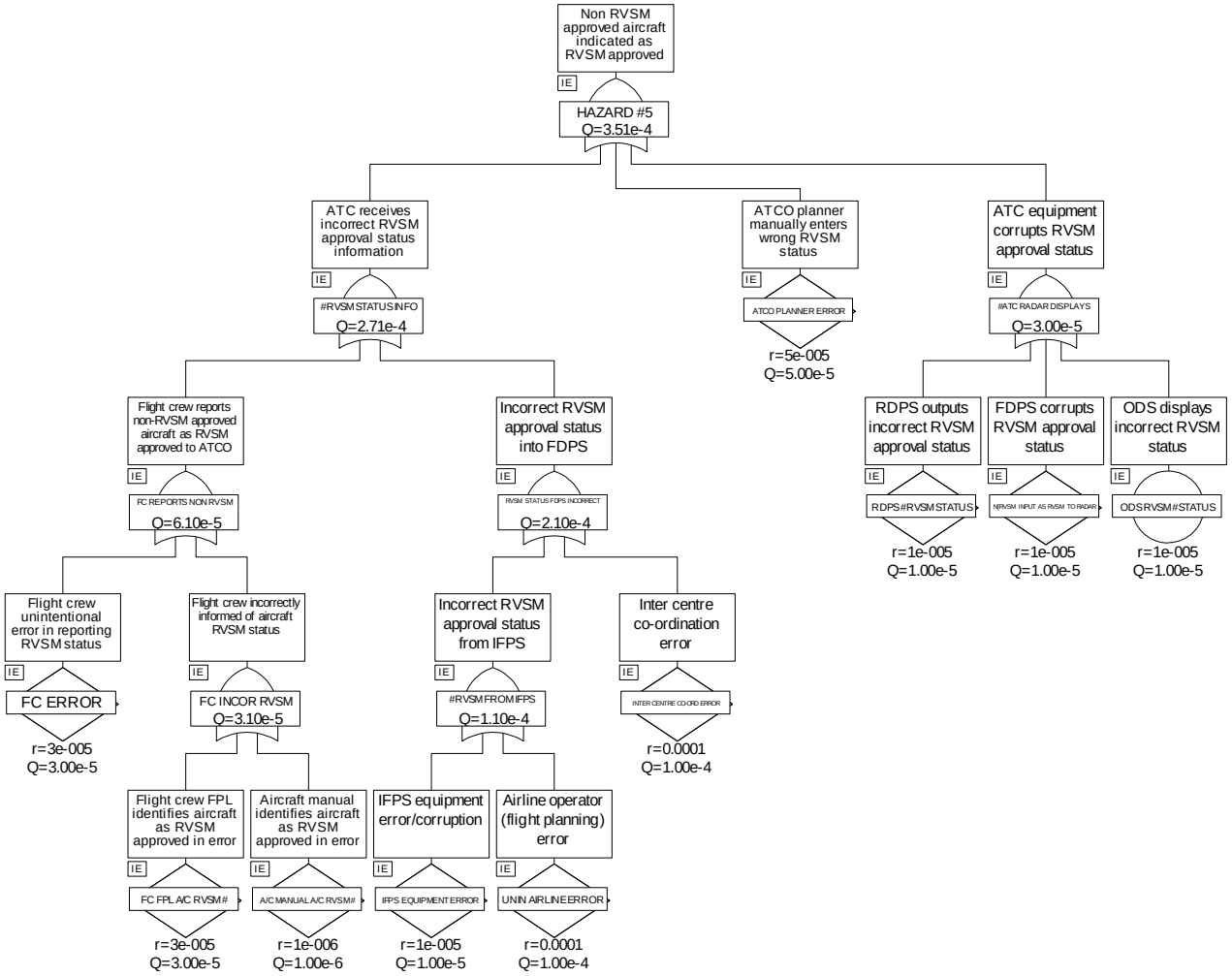

Figure C.2 – Hazard #5

Intentionally blank

D Appendix: Abbreviations

Abbreviation	Description
FPS	Flight Progress Strip(s)
MASPS	Minimum Aircraft System Performance Specification
ODS	Operational Display System
RVSM	Reduced Vertical Separation Minima
pfh	Per Flight Hour

Table 2 Abbreviations

Document references

1 TLS Apportionment Method, SAM-FHA Chapter 3 Guidance Material J

2 EUR RVSM Post-Implementation Safety Case (tbd)

3 JAA Administrative and Guidance Material, Section One: General Part 3: Temporary Guidance Leaflet No. 6, Revision 1 – Guidance Material on the Approval of Aircraft and Operators for Flight in Airspace above Flight Level 290 where a 300M (1000 ft) Vertical Separation Minimum is applied (October 1999)

4 EUR RVSM Pre-Implementation Safety Case, RVSM 691, Version 2.0, 14 August 2001.