

# SESAR 3 ER 1 Green-GEAR D4.3 – RVSM 2 Safety Case

<b>Deliverable ID:</b>	<b>D4.3</b>
<b>Project acronym:</b>	<b>Green-GEAR</b>
<b>Grant:</b>	<b>101114789</b>
<b>Call:</b>	<b>HORIZON-SESAR-2022-DES-ER-01</b>
<b>Topic:</b>	<b>WA 2.7 ATM application-oriented Research for Aviation Green Deal</b>
<b>Consortium coordinator:</b>	<b>DLR e.V.</b>
<b>Edition date:</b>	<b>28 February 2025</b>
<b>Edition:</b>	<b>01.00</b>
<b>Status:</b>	<b>Official</b>
<b>Classification:</b>	<b>PU</b>

## Abstract

---

The “Separation Minima” Solution assesses the feasibility of reducing the vertical separation minima to 500 ft in upwards-extended Reduced Vertical Separation Minima (RVSM) airspace with the use of improved altitude keeping expected with GNSS altimetry, also named the RVSM 2 concept. The work in this report is part of a larger safety case (or safety assessment) and focuses on the risk due to non-nominal causes. The approach was to adopt the Target Level of Safety (TLS) of 1000 ft RVSM, to describe the RVSM 2 concepts on a functional level, and by deriving safety specifications through a Functional Hazard Analysis (FHA). The most important insights are the need for a procedure in case GNSS altimetry is lost by all airspace users, which is only very rarely allowed to happen, and the need for a re-designed Airborne Collision Avoidance System (ACAS). The result of this study can serve as further guidance in the design of the RVSM 2 concept.

## Authoring & approval

### Author(s) of the document

Author	Organisation	Date
Patrick Jonk	Royal NLR	28-02-2025
Bart Klein Obbink	Royal NLR	28-02-2025
Job Smeltink	Royal NLR	28-02-2025
	Royal NLR	28-02-2025

### Reviewed by

Organisation name	Date
Tobias Bauer	DLR 25-02-2025

### Approved for submission to the SESAR 3 JU by<sup>1</sup>

Organisation name	Date
Patrick Jonk, Solution Leader 0407 and Work Package Manager WP4, Royal NLR	28-02-2025
Tobias Bauer, Project Manager, DLR	28-02-2025

### Rejected by<sup>1</sup>

Organisation name	Date
-------------------	------

## Document history

Edition	Date	Status	Organisation / Author	Justification
00.01		initial draft	Royal NLR / Patrick Jonk	
00.02		draft	Royal NLR / Patrick Jonk	
00.03	21-02-2025	final draft	Royal NLR / Patrick Jonk	for review
00.04	28-02-2024	release candidate	Royal NLR / Patrick Jonk	comments included
01.00	28-02-2025	release	DLR / Tobias Bauer	submitted to SJU

The beneficiaries/consortium confirm(s) the correct application of the Grant Agreement, which includes data protection provisions, and compliance with GDPR or the applicable legal framework with an equivalent level of protection, in the frame of the Action. In particular, beneficiaries/consortium confirm(s) to be up to date with their consent management system.

<sup>1</sup> Representatives of the participants to the project

**Copyright statement** © 2025 – Green-GEAR Consortium. All rights reserved. Licensed to SESAR 3 Joint Undertaking under conditions.

### Disclaimer

The opinions expressed herein reflect the author’s view only. Under no circumstances shall the SESAR 3 Joint Undertaking be responsible for any use that may be made of the information contained herein.

# Green-GEAR

GREEN OPERATIONS WITH GEOMETRIC ALTITUDE, ADVANCED  
SEPARATION & ROUTE CHARGING SOLUTIONS

# Green-GEAR

This document is part of a project that has received funding from the SESAR 3 Joint Undertaking under grant agreement No 101114789 under European Union’s Horizon Europe research and innovation programme. UK participants in Green-GEAR have received funding from UK Research and Innovation (UKRI) under the UK government’s Horizon Europe funding guarantee [grant numbers 10087714 (NATS) and 10091330 (University of Westminster)].



## Table of contents

Abstract .....	1
<b>1 Introduction.....</b>	<b>6</b>
<b>2 Safety of a System.....</b>	<b>8</b>
<b>3 System definition (RVSM 2).....</b>	<b>10</b>
<b>3.1 General concept .....</b>	<b>10</b>
<b>3.2 Domains.....</b>	<b>11</b>
3.2.1 Altitude information domain .....	12
3.2.2 Airborne domain .....	12
3.2.3 Ground domain .....	13
<b>3.3 Functions of the RVSM2 system .....</b>	<b>14</b>
3.3.1 Primary functions .....	14
3.3.2 Secondary functions.....	15
<b>3.4 Contingency procedures .....</b>	<b>16</b>
<b>4 Risk due to non-nominal behaviour .....</b>	<b>18</b>
<b>4.1 Introduction .....</b>	<b>18</b>
<b>4.2 Functional Hazard Assessment method .....</b>	<b>18</b>
<b>5 Hazard analysis.....</b>	<b>23</b>
<b>5.1 Identified hazards.....</b>	<b>23</b>
<b>5.2 Causal analysis H1 .....</b>	<b>23</b>
5.2.1 Causes .....	23
5.2.2 Consequences .....	24
<b>5.3 Causal analysis H2 .....</b>	<b>24</b>
5.3.1 Causes .....	25
5.3.2 Consequences .....	25
<b>5.4 Causal analysis H3 .....</b>	<b>25</b>
5.4.1 Causes .....	25
5.4.2 Consequences .....	25
<b>5.5 Causal analysis H4 .....</b>	<b>26</b>
5.5.1 Causes .....	26
5.5.2 Consequences .....	26
<b>6 Safety Specification.....</b>	<b>27</b>
<b>6.1 Approach .....</b>	<b>27</b>
<b>6.2 Safety specifications for H1.....</b>	<b>28</b>
<b>6.3 Safety specifications for H2, H3 and H4 .....</b>	<b>30</b>
6.3.1 ATC collision prevention.....	33
6.3.2 Visual- and ACAS-based avoidance .....	33

<b>7</b>	<b>Conclusion .....</b>	<b>35</b>
<b>8</b>	<b>References .....</b>	<b>37</b>
<b>9</b>	<b>List of acronyms .....</b>	<b>38</b>

## List of figures

Figure 1: In order to define the functions within RVSM2, three domains are relevant: ground, airborne and altitude information domain.....	11
Figure 2: There are four primary functions required for RVMS 2 operations.....	14
Figure 3: There are seven potential secondary functions for RVMS2 operations. ....	16
Figure 4: The integration of the system specification and the safety analysis .....	19
Figure 5: The main steps in the execution of the FHA .....	20
Figure 6: Mid Air Collision (MAC) en route (ER) Accident Incident Model (AIM) adapted to the 1000 ft RVSM operation .....	32
Figure 7: Mid Air Collision (MAC) en route (ER) Accident Incident Model (AIM) adapted to the RVSM 2 concept.....	34

## List of tables

Table 1: list of acronyms .....	38
---------------------------------	----

# 1 Introduction

---

Green-GEAR Work Package (WP) 4 assesses the feasibility of reducing the vertical separation minima to 500 ft in upwards-extended Reduced Vertical Separation Minima (RVSM) airspace with the use of improved altitude keeping expected with Global Navigation Satellite System (GNSS) altimetry, also named the RVSM 2 concept, in the “Separation Minima” Solution. The main focus here is on the safety aspects of the concept, and the work is structured by considering the technical (nominal) risk and the operational (non-nominal) risk separately, which add up to the total, or overall risk. In short, iD4.1 Collision Risk Analysis (CRA) [1] focuses on the nominal collision risk, iD4.2 Wake Turbulence Risk Analysis (WTRA) [2] focuses on the nominal wake turbulence risk, and this deliverable, D4.3 RVSM 2 Safety Case focuses on a Functional Hazard Assessment (FHA) that considers the non-nominal risk, and in addition provides an over-arching perspective on the risk of the three parts as a whole.

First some words of caution are spent on the term Safety Case. A Safety Case is typically defined as *“the documented assurance, including argument and supporting evidence, of the achievement and maintenance of safety”* [3]. It represents a structured logical reasoning and provides evidence for the different parts, which in total prove that a system is safe. This implies that the system is ready for implementation from a safety perspective and is something that is typically carried out at high Technology Readiness Level (TRL). As an alternative, a Preliminary Safety Case reports on the safety of a new concept and depends on strict conditions on the implementation. The concept that is studied in Green-GEAR WP4 is at such an early stage that many of the details are not yet determined. This document should therefore not be interpreted as a strict Safety Case, but rather more loosely a preliminary study that gives a first estimate of the feasibility of the concept.

GNSS is nowadays used by most aircraft for horizontal positioning, at least in commercial air transport. GNSS is also used for altimetry but only occasionally in specific flight procedures, such as LPV, GBAS and RNP AR approach procedures. The Green-GEAR project researches the possibility to use GNSS for vertical navigation in aviation more broadly, as this potentially offers several benefits. In Green-GEAR WP3 for example, the feasibility of GNSS altimetry in a Terminal Manoeuvring Area (TMA) environment is studied, which would allow for the removal of the barometric transition layer. This would require the introduction of a geometric altimetry system including agreements and coordination about the definition of the altitude coordinate in a geodetic reference (that is, so to speak: a vertical coordinate geometrically attached to the earth, such as in WGS 84, as used by GPS).

If aircraft use GNSS for vertical navigation and if such a geometric altimetry system is introduced, it might be feasible to reduce the currently applied vertical separation minima. A reduction of the vertical separation minima would increase capacity and would allow aircraft to fly closer to their preferred altitude, thereby possibly offering efficiency, cost and environmental benefits. The possibility to operate with reduced vertical separation minima is the main topic of Green-GEAR WP4. There are basically two reasons why this might indeed be feasible. The main reason is that GNSS altimetry is supposed to be more accurate than barometric altimetry, and the related margins in spacing might therefore be reduced. The second reason is that the accuracy of GNSS altimetry is not sensitive with respect to altitude while barometric altimetry is. The currently applied vertical separation minima of 2000 ft above FL410 could then be reduced, even if GNSS altimetry is only as accurate as barometric altimetry at lower altitudes.

The RVSM 2 concept thus focuses on an upwards-extended RVSM airspace, from FL290 to FL600 (inclusive). Altitude estimates of the airspace users are to be provided through one or multiple GNSSs and aircraft are separated through a geodetic reference. The vertical separation minimum will be reduced to 500 ft from 1000 ft and 2000 ft minimal separation below and above FL410 respectively. All airspace users are assumed to be only navigating on geometric altimetry. Considering the European focus of this project, the European RVSM airspace will serve as a test case. The concept is further described in the initial Operational Service and Environment Definition (OSED) [4] and will be further updated in the final OSED.

The first chapter describes how to determine if a system is safe and how this is set up for the subsequent parts of WP4. Next, the RVSM 2 concept is defined on a conceptual level by considering an altitude information-, airborne-, and ground domain, and defining primary and secondary functions that act within and between the different domains. Hazards are defined by considering the failure of primary functions, and the hazards are analysed to provide estimates of the severity and maximally allowable likelihood, which serve as a safety specification. These results will serve as guidance on the further development of the concept.

## 2 Safety of a System

---

The safety of a system depends on a number of characteristics of the airspace, including the airspace (route) structure, the communication capabilities, the (independent) surveillance capability, the aircraft navigation performance; and the effectiveness of safety barriers like Short-Term Conflict Alert (STCA) and Airborne Collision Avoidance System (ACAS).

When the relevant characteristics of a proposed system have been identified and quantified, there are two basic methods for determining whether the system is acceptably safe [5]:

- a) comparison with a reference system;
- b) evaluation of system risk against a threshold.

Comparison with a reference system is a “relative” method, i.e. all the relevant characteristics of the proposed system are compared with the corresponding characteristics of a reference system which has been judged to be safe. Provided that the proposed system can be demonstrated to be similar to or better than the reference system in all safety-related aspects and provided that the reference system is considered safe, then the proposed system also may be assumed to be safe. Clearly, the most important aspect of this approach lies in the identification of a suitable reference airspace which, for minor changes, may include the current system and the demonstration that the proposed system is sufficiently similar to justify the approach.

The evaluation of system risk against a threshold is an absolute method where, after identification and quantification of all the safety-related characteristics of the system, an explicit relation between these characteristics and accident risk is determined and used to estimate system safety. This estimate is then compared against a maximum tolerable risk - for example, a Target Level of Safety (TLS). The estimation of risk for any airspace is a complex procedure and may require extensive data on all aspects of the performance of the system. Another important element is the choice of a suitable value for the maximum level of risk.

So, a proposed system can be judged to be safe if either:

- a) it has been shown to be at least as safe as a reference system which has already been judged to be safe;
- b) the quantitative estimate of risk of the proposed system is no greater than a predetermined acceptable level of risk.

In the introduction of RVSM the method of evaluation against a threshold was used. A TLS of  $5.0 \cdot 10^{-9}$  was set for fatal accidents per aircraft flight hour for vertical accidents independent of the causes. Subsequently the nominal, or technical risk was evaluated separately for which the TLS was set to  $2.5 \cdot 10^{-9}$ . This implicitly left a minimal risk budget of  $2.5 \cdot 10^{-9}$  fatal accidents per flight hour due to non-nominal causes. The technical risk refers to accidents due to vertical navigation errors between correctly separated aircraft. Non-nominal causes refer to risks related to weather, turbulence, responses to airborne collision avoidance system alerts, emergency descents and operational errors in the issuance of, or compliance with, Air Traffic Control (ATC) instructions.

Risks due to wake turbulence encounters were not explicitly considered in the safety case of RVSM. For wake turbulence risk, it is common practice to use a comparative approach where the current

operational system is taken as the reference. If a proposed system change would lead to an increase in wake turbulence risk, the change would only be permitted if mitigating procedures are included. Additionally, the risk associated with wake turbulence encounters is typically not quantified through the likelihood of a major top-event such as a mid-air collision or a loss-of-control. Wake turbulence risks are quantified by the frequency and the severity of occurrences, which are often only quantified by the subjective acceptability of the roll moment applied by a wake vortex on an aircraft by the pilot in command. Relating this wake turbulence risk to a TLS would constitute a considerable exercise on its own.

For RVSM 2, the technical and the total risk, excluding the wake turbulence risk, are studied through the evaluation against a threshold, similar to RVSM. This is done for a number of reasons. First of all, whether the TLS for the nominal risk will be met is dependent on the balance between the positively contributing, increasing altimetry system accuracy and the negatively contributing, decreasing separation minima. The overall technical risk may very well increase. Secondly, RVSM 2 relies on GNSS altimetry which has a vulnerability, the outage or distortion of the satellite signals effecting all aircraft users in a large part of the airspace, that has no analogue in the reference system, based on barometric altimetry. Thirdly, the introduction of RVSM took many years of assessments and deliberations. Assuming a similar approach allows building on that foundation of work. Finally, the system safety is highly dependent on parameters such as altimetry system errors (ASE) and the amount of traffic, which have been shown to have evolved to a great extent throughout the years in RVSM collision risk assessments. Using a comparative approach may simply mean that from year to year the amount of traffic may not be allowed to increase.

The RVSM 2 concept will be assessed against the same TLS for the technical and total risk as RVSM, which are  $2.5 \cdot 10^{-9}$  and  $5 \cdot 10^{-9}$  fatal accidents per flight hour respectively. In RVSM, if the technical risk of the system turns out to be well below the  $2.5 \cdot 10^{-9}$  threshold, the remaining 'risk budget' for non-nominal causes is higher, as the TLS for the total risk is constant. In the assessment of the technical risk the fully available budget of  $2.5 \cdot 10^{-9}$  is used in setting specifications for the altimetry and height-keeping performance. The assessment of the technical risk is described at length in the Collision Risk Assessment [1]. This document will focus on the risk due to non-nominal causes. Finally, the wake turbulence risk is assessed separately [2] using a comparative approach.

## 3 System definition (RVSM 2)

---

### 3.1 General concept

The precise RVSM 2 system, that is: the system delivering minimal vertical separation of 500 ft, is not yet entirely defined. The vertical separation could in principle be provided by the existing, current means by which for example 1000 ft minimal separation is provided. These means consist, among other elements, of barometric altimetry in each aircraft, a uniform specification of altitudes in terms of barometric pressure and a general agent, air traffic control, that dynamically assigns such altitudes to individual aircraft. There is however evidence that the accuracy of currently used barometers is not sufficient to apply 500 ft minimal vertical separation safely, especially at high altitudes, see also the collision risk assessment [1].

Therefore, the system should include GNSS based altimetry, which may provide an accuracy that is sufficient. This would in turn imply geometric altimetry with a specification of altitudes in terms of the geometry of the globe. As considered in other Green-GEAR work packages, especially WP3, this geometric nature brings benefits as aviation gets rid of the transition layer and as approach procedures become more flight efficient and less demanding. This and the benefits of a stepwise introduction are reasons to expect that geometric altimetry is introduced first, after which, possibly, the minimal vertical separation is reduced to 500 ft in a later phase. Hence, the safety assessment of 500 ft minimal vertical separation is not to be confused by the safety assessment of geometric altimetry; and the functional hazard assessment of 500 ft minimal vertical separation is not the functional hazard assessment of geometric altimetry.

In line with the previous chapter, the approach adopted here is however to assess the RVSM 2 concept as a whole, including both GNSS based altimetry and a reduction of vertical separation, against a given TLS, namely  $2.5 \cdot 10^{-9}$  fatal accidents per flight hour. This RVSM 2 concept, including the environment it is supposed to operate in, is described in [4]. Anticipating the Functional Hazard Analysis method, as described in section 4.2, it makes however sense to decompose the functions within the RVSM 2 concept. Before this decomposition is presented in section 3.3, the meaning of some terms used in the remainder of this report is clarified below and a distinction of domains is presented in section 3.2.

The airspace under consideration is a block of RVSM 2 airspace with well demarcated horizontal and vertical boundaries, in which nominally only geometric altimetry and only 500 ft vertical separation are applied.

When referring to aircraft in the following, the aircraft in the RVSM 2 airspace at any moment are meant. When it is stated that aircraft are separated, this refers to the spacing of their physical hulls, or actually to the spacing of the reference points within these hulls. When it is stated that aircraft have certain functions, this refers to the aircraft including controls, avionics and sometimes even implicitly the crew controlling them. Aircraft can only enter this airspace under certain rules, including that the aircraft have the capabilities required to apply 500 ft minimal vertical separation, see also the analysis

of the technical risk [1]. An important assumption is that all aircraft in the airspace comply to the airspace access rules<sup>2</sup>.

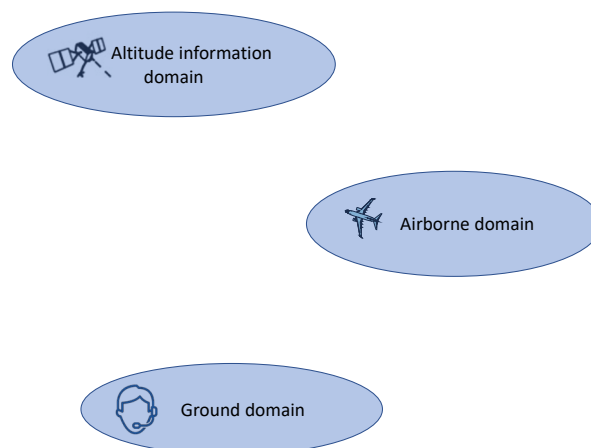
An altitude in this context is a reference level defined by a geodesic coordinate system around the globe, or at least in the airspace. In this context, it might be assumed that WGS 84 serves as this coordinate system, although this is not necessary in the derivation of requirements. The important point here is that all parties involved apply the same coordinate system, without any unclarities or reference errors. This is however an assumption that might also be challenged later on, which could then lead to hazards in which altitude reference errors are considered. That is however also considered out of the scope of this assessment.

The term in a continuous way is used to indicate that something happens all the time or happens in a fast, repetitive way and then typically with a constant, high frequency.

## 3.2 Domains

For RVSM2 the following three domains are distinguished, as shown in Figure 1:

- Altitude information domain;
- Airborne domain;
- Ground domain.



**Figure 1: In order to define the functions within RVSM2, three domains are relevant: ground, airborne and altitude information domain.**

---

<sup>2</sup> This assumption might be challenged later on in the Preliminary System Safety Assessment (PSSA), which could lead to hazards in which non-conformance to the access rules is considered. That is however out of the scope of this Functional Hazard Assessment.

One might think of the three domains in terms of space, aircraft and ATM respectively. It is however emphasized that these terms do not strictly point at the location where a function is executed. It is for example possible that a subfunction within the altitude information or airborne domain is executed on a location on the ground.

Two types of descriptions of each of these domains are provided in the subsections 3.2.1, 3.2.2 and 3.2.3 below. The first description is on an abstract, conceptual level, not considering sub-domains or physical elements executing functions, as if vertical separation is to be provided in a logical way. The second description is on an operational, material level, assuming recognizable designs that correspond to current or future ways of operations, as if vertical separation is to be provided in an instrumental way.

### **3.2.1 Altitude information domain**

The altitude information domain provides information from which sensors can derive an estimate of their altitude. This information, referred to as altitude information, is nominally provided in the whole airspace in a continuous way. In addition to this information, the altitude information domain may provide other information, including: information from which a longitude and latitude can be derived, information from which the local time can be derived and information about the expected accuracy and integrity of this navigation information.

The primary candidate for the altitude information domain in the context of 500 ft minimal vertical separation is GNSS, with possible enhancements. GNSS is the term to indicate a satellite navigation system providing autonomous geopositioning with global coverage, such as GPS, Galileo, BeiDou and GLONASS. The satellites in these systems send out electromagnetic time signals from which the altitude, longitude and latitude with respect to some coordinate system can be derived by means of receivers, together with the local time. In addition to that, a Satellite Based Augmentation System (SBAS) might be used to improve the accuracy of GNSS position information and to indicate the expected accuracy and integrity of the navigation signals. It is noted that the altitude information domain is not necessarily one GNSS with or without an SBAS, it might also be a combination of systems or even sub-systems.

Another candidate for the position information domain is the atmospheric pressure as applied today for the barometric altimetry in aviation. Its nature is completely different as it is not man-made like GNSS. It is noted that if the atmospheric pressure is somehow to be combined with GNSS data to derive an altitude estimate, different reference systems need to be combined. This might for example be done in the airborne domain after receiving data about the local atmospheric pressure from a meteorological service, such that the geometric altitude, in terms of the geodesic coordinates, is derived from a barometric altitude. The provisioning of data about the local atmospheric pressure would then also be in the altitude information domain.

### **3.2.2 Airborne domain**

The airborne domain lets aircraft fly assigned altitudes. The assigned altitudes are the altitudes as instructed by the ground domain, see the section 3.2.3 below. In order to fly these altitudes, the airborne domain needs to receive these instructions. Moreover, it is needed that the airborne domain

provides estimates of the altitudes of the aircraft in a continuous way. Since the assignment of altitudes is dynamic, the airborne domain also includes functions such that each aircraft can change its altitude if so instructed. It is therefore also stated that aircraft fly *according* to their assigned altitudes, implying that they might be descending or ascending between the previously and the newly assigned altitude but not below the lowest or above the highest. In addition to this, the airborne domain may provide information about the altitude of aircraft<sup>3</sup>. This information is nominally an accurate estimate provided in a continuous way. Moreover, the airborne domain may execute several other functions including the following ones: notifications are provided if an aircraft cannot fly an assigned altitude and alerts are provided if an aircraft has lost the capability of flying assigned altitudes.

The primary candidate for the airborne domain is a distribution of functions over several individual aircraft, consisting of the aircraft bodies and the avionics and aircrew within. There seems however no reason in this context to exclude for example that the aircraft is flying completely autonomous by means of systems, that the human operators flying the aircraft are not in the aircraft themselves or that such humans operate several aircraft. The distribution of subtasks over avionics and aircrew is also not fixed. The primary candidate for this distribution would typically be as follows. The sensors receive the altitude information and the airborne navigation system processes this into an actual altitude estimate. This actual altitude estimate is broadcast by ADS-B. If the aircraft is flying level, the autopilot handles the controls to make slight corrections if assigned and actual altitude deviate from each other. If the assigned altitude is changed, the information is received by the aircrew via Radio Telephony (RT) or Controller Pilot Data Link Communications (CPDLC). The aircrew confirms receipt and execution of this instruction, again via RT or CPDLC, and then manually inputs the newly assigned information into the autopilot to change altitude. The autopilot handles the controls to let the aircraft fly to the assigned altitude. As indicated, this is the primary way of operations but other ways are possible as well, for example in which the pilot flying handles the controls directly or in which the Flight Management System (FMS) instructs the autopilot to descend or ascend according to a certain profile.

### 3.2.3 Ground domain

The ground domain assigns altitudes to individual aircraft such that vertical separation is provided if necessary. Vertical separation is provided if the vertical distance between any two aircraft is 500 ft or more. Vertical separation is necessary if there is no other separation, such as horizontal separation or self-separation<sup>4</sup>. As vertical separation is applied for all aircraft all the time, if necessary, also when one or several aircraft ascend or descend to newly assigned altitudes, it is often stated that the ground domain *maintains* vertical separation. In addition, the ground domain may execute several other functions including the following ones: monitor whether the altitude information has sufficient availability, accuracy and integrity and take action if not, monitor whether individual aircraft fly

---

<sup>3</sup> Actually, aircraft currently do broadcast their altitude, for example via Mode C, Mode S and ADS-B. However, there might be no reason to exclude the possibility of 500 ft vertical separation in an airspace without full coverage by secondary radar surveillance or ADS-B. In that case, there is no need to require that information about the altitude of aircraft which is provided by the airborne domain in this context.

<sup>4</sup> In case of self-separation, advanced aircraft systems, such as ASAS, and aircrew provide separation, without a ground domain being involved. It cannot be excluded that this kind of separation also applies a minimal vertical separation of 500 ft, but this possibility is not considered in this FHA.

according to their assigned altitudes and take action if not, monitor whether vertical separation is indeed provided if necessary and take action if not.

The primary candidate for the ground domain is a set of ATC units that cover the whole airspace. Each ATC unit contains a set of systems, procedures and air traffic controllers. Altitudes are assigned to the airborne domain by means of RT or CPDLC. Altitudes might be assigned for certain flight segments if there is no full surveillance or communication coverage, that is: in a procedural way, but might also be assigned till further notice. In practice, there is often communication between the ground and airborne domain about altitude assignments; that is: the aircrew can indicate preferences, requests and infeasibilities to the controller. If an aircraft is handed over from one ATC unit to another, the assigned altitude is taken over.

### 3.3 Functions of the RVSM2 system

#### 3.3.1 Primary functions

Primary functions are the functions necessary for applying geometric altimetry and the provisioning of minimal vertical separation. The following four primary functions (also shown in Figure 2) are distinguished:

- The altitude information domain provides altitude information in the entire airspace in a continuous way.
- The airborne domain receives the altitude information and provides estimates of the altitude of each individual aircraft in a continuous way.
- The ground domain assigns an altitude to each individual aircraft such that it is vertically separated if necessary.
- The airborne domain receives the assigned altitudes and let each individual aircraft fly according to the assigned altitude.

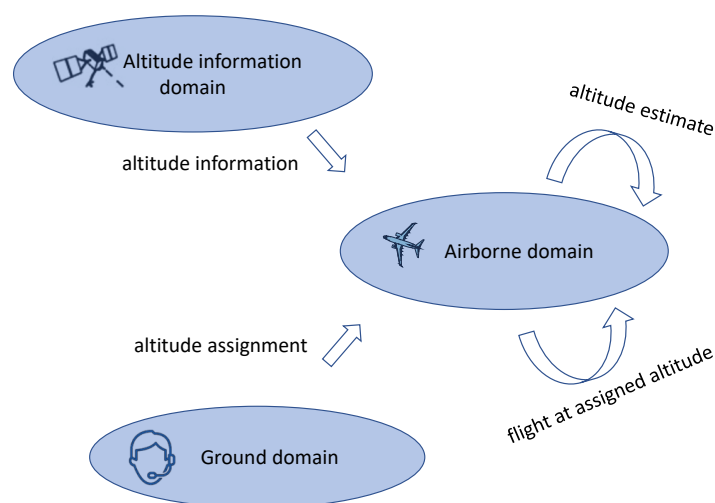


Figure 2: There are four primary functions required for RVMS 2 operations.

### 3.3.2 Secondary functions

Secondary functions are the functions that might be necessary for the safe provisioning of 500 ft minimal vertical separation in case any of the primary functions are jeopardized. A non-exhaustive list of secondary functions is given below. It is not yet specified whether these functions are indeed necessary; that is to be derived in the Functional Hazard Assessment. Some of the functions imply sending out messages or signals. It is also not yet specified which parties should receive these messages and signals; that is also to be derived in the functional hazard assessment.

The following seven secondary functions may be distinguished:

- The altitude information domain provides a *lack of altimetry integrity* message if there is uncertainty about the accuracy of the altitude estimate that can be derived from the altitude information in a part of the airspace.
  - The *lack of altimetry integrity* messages are received by the ground domain, at least by the ATC units providing service in or close to the part of the airspace where it applies.
  - The *lack of altimetry integrity* messages are received by the airborne domain, at least by the aircraft flying in or close to the part of the airspace where it applies.
- The airborne domain monitors the availability, accuracy and integrity of the altitude estimate of each individual aircraft in the airspace. This is done by means of internal consistency checks, using the received *lack of altimetry integrity* message from the altimeter information domain.
- The airborne domain sends out *own altitude* signals for each individual aircraft in a continuous way. These signals include the altitude estimate, together with some kind of identification of the aircraft sending the signals out.
  - The *own altitude* signals are received by the ground domain, at least by the ATC units providing services in the part of the airspace in which the aircraft that sends out the signals fly.
  - The *own altitude* signals are received by the airborne domain, at least by the aircraft flying in the vicinity of the aircraft that sends out the signals<sup>5</sup>.
- The airborne domain sends out an *unable altimetry* message if a lack of availability, accuracy or integrity of the altitude estimate of an aircraft is detected<sup>6</sup>.
  - The *unable altimetry* messages are received by the ground domain, at least by the ATC units providing service in the part of the airspace in which the aircraft fly.
  - The *unable altimetry* messages are received by the airborne domain, at least by the aircraft flying in the vicinity of the aircraft that sends out the message.
- The airborne domain sends out an *unable height keeping* message if an aircraft is not able to maintain assigned altitudes in a proper way for other reasons than a lack of availability, accuracy and integrity of the altitude estimate<sup>7</sup>.
  - The *unable height keeping* messages are received by the ground domain, at least by the ATC units providing service in the part of the airspace in which the aircraft fly.

---

<sup>5</sup> This function currently exists. The relevant question here is whether this information is required for the safe provisioning of 500 ft minimal vertical separation.

<sup>6</sup> This message might be implicit in the current *unable RNP* message. It is understood that this message is sent out some limited time after the actual detection, to give the systems the opportunity to recover quickly.

<sup>7</sup> This message might be implicit in the current messages sent out after cabin depressurisation, engine failures, hydraulic malfunctions, etc.

- The *unable height keeping* messages are received by the airborne domain, at least by the aircraft flying in the vicinity of the aircraft that sends out the message.
- The ground domain receives the *own altitude* signals of each individual aircraft in a continuous way and verifies if it deviates significantly (in magnitude and in time) from the altitude assigned to that aircraft. If a significant deviation is detected, the ground domain communicates with that individual aircraft to reassure conformance.
- The ground domain detects inadequacy of the altitude information in a part of the airspace. This can be done by processing one or a combination of the following information items: a) receipt of a *lack of altimetry integrity* message from the altitude information domain, b) receipts of *lack of unable altimetry* messages from several aircraft, c) the detection of several aircraft deviating from their assigned altitude and d) other information items, such as an indication of jamming or spoofing.

A subset of the secondary functions is shown in Figure 3.

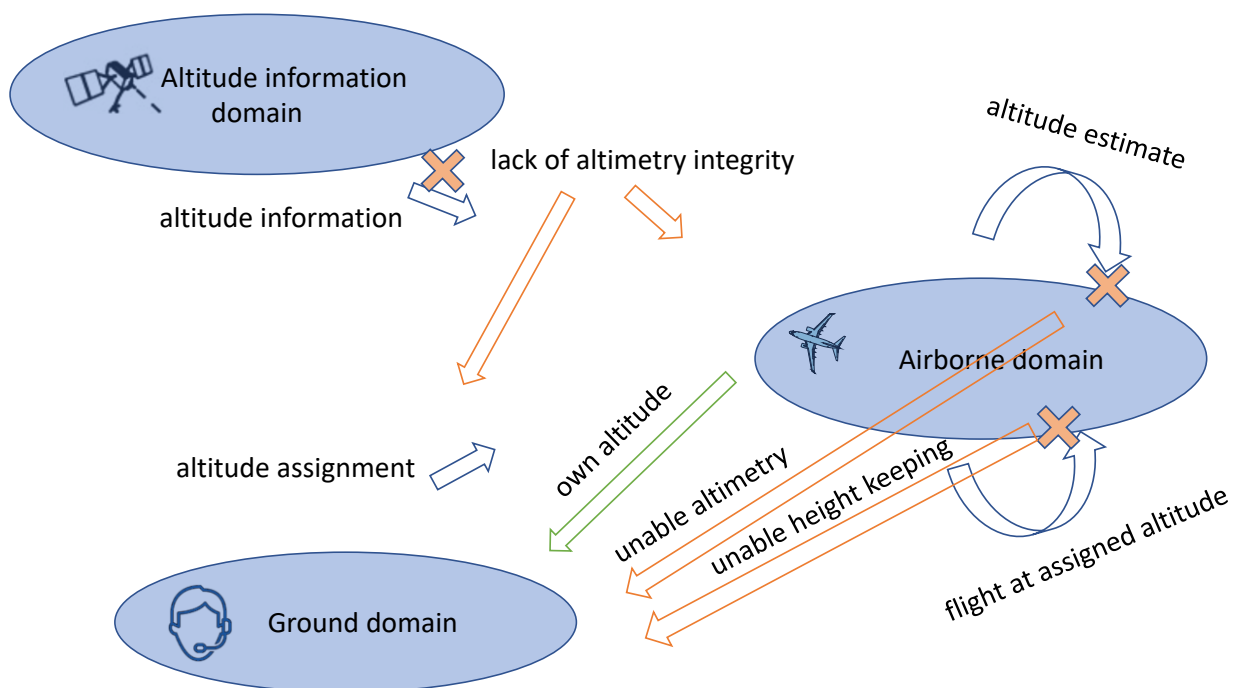


Figure 3: There are seven potential secondary functions for RVSM2 operations. The ones not indicated in this figure in order to keep it readable are the following: the monitoring of the availability, accuracy and integrity of the altitude estimates in the airborne domain, the verification by the ground domain whether the *own altitude* signals correspond to the assigned altitudes and the possible detection by the ground domain of inadequacies of the altitude information.

### 3.4 Contingency procedures

There are two contingency procedures relevant in the context of this assessment:

1. The first contingency procedure, referred to as *Procedure Single Unable Altimetry* (PSUA) is applied if it is detected that one aircraft is not able to derive an altitude estimate with sufficient accuracy in a continuous way or if it is detected that one aircraft has not sufficient capabilities to maintain assigned altitudes. The procedure aims to maintain sufficient spacing between this aircraft and all other aircraft. The procedure is not designed yet, as it should first be derived from this functional hazard assessment how safe it should be. Basically, there are two options:
  - Option 1, typically applied if the ground domain does not actively control the air traffic (i.e.; there is procedural control, without full surveillance and communication coverage, and the ground domain is for example not receiving the *own altitude* signals for each individual aircraft and neither the *unable altimetry* messages). The PSUA is then executed by the aircraft that is not able to derive an altitude estimate or is not able to keep its assigned altitude. The aircraft might then need leave the RVSM 2 airspace.
  - Option 2, typically applied if the ground domain is actively controlling the air traffic with full surveillance and communication coverage, receiving the *own altitude* signals from each individual aircraft and receiving *unable altimetry* messages. The PSUA then possibly involves standardized communication between ground and airborne domain and might involve dedicated communication between aircrew and controller, for example about the cause of the lack of altimetry capabilities. This ground domain might then maintain horizontal separation or provide vertical spacing with respect to other aircraft with large margins.
  
2. The second contingency procedure, referred to as *Procedure Multiple Unable Altimetry* (PMUA) is applied if it is detected that the provided altitude information is not adequate in the entire airspace, or in a part of it. *Not adequate* in this context is not yet precisely defined but includes situations such as: the information is not available for some period, the estimates derived from it are rather inaccurate for some period and the estimates derived from it are incorrect for some period. The procedure aims to maintain sufficient spacing between all aircraft in the relevant part of the airspace. The procedure is not designed yet, as it should first be derived from this assessment how safe it should be.

## 4 Risk due to non-nominal behaviour

---

### 4.1 Introduction

In the CRA on the risks of mid-air collisions [1] and the WTRA wake turbulence accidents [2], the main assumption is that the RVSM 2 operations are nominal; that is: all systems and people act as intended and no operational errors are made. In this report, the risks of non-nominal behaviour are considered, basically assuming that the nominal operation is sufficiently safe (although this is not yet shown).

Besides risks associated with nominal behaviour, there may be risks from other sources, such as height deviations due to weather/turbulence, responses to airborne collision avoidance system alerts, emergency descents and operational errors in the issuance of, or compliance with, air traffic control (ATC) instructions. Risk from other sources is referred to a non-nominal behaviour.

The following broad categories of potential causes of total vertical accident risk have been distinguished:

- A. ATC error;
- B. Pilot error;
- C. ACAS events;
- D. Non-approved (military or civil) aircraft;
- E. Equipment failure;
- F. Weather/turbulence<sup>8</sup>; and
- G. Aircraft contingency events.

In order to develop RVSM 2 operations that are also sufficiently safe in case of non-nominal behaviour, there is a need to iterate system specification and safety analysis. At this point of the life cycle of the RVSM 2 development, the precise operations are not yet completely specified although high level functions can be defined and non-nominal behaviour can be identified (see Chapter 3). Therefore, in line with the Expanded Safety Reference Material (E-SRM), an FHA is executed. The general idea of an FHA is to derive how safe a system needs to be to achieve an acceptable risk. This assessment is carried out in the RVSM 2 system definition phase, to assist the system design in the next phase.

### 4.2 Functional Hazard Assessment method

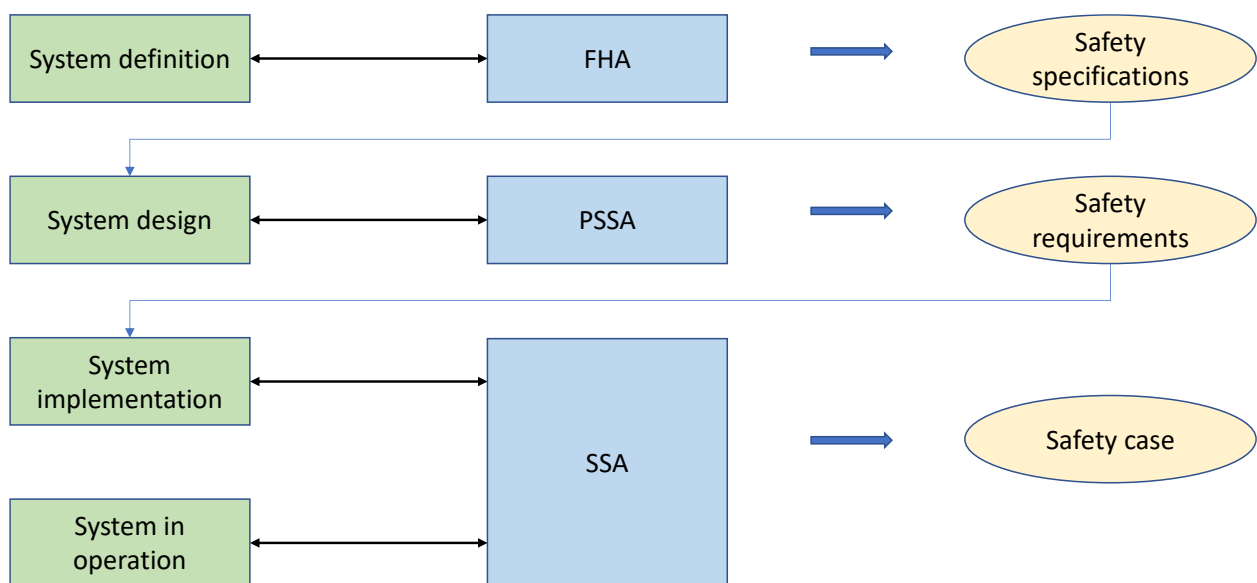
The aim of a functional hazard assessment is to deduce safety objectives for the system, or in terms of E-SRM, safety specifications. As also indicated in the previous section, the system is not yet completely designed; the design should be based on the outcome of the Functional Hazard Assessment. Therefore, so-called primary functions are defined on a conceptual level (see Chapter 2). The collection of primary

---

<sup>8</sup> excluding wake vortex turbulence

functions is a kind of minimal set of utilities by which geometric altimetry and vertical separation can be delivered. It is assumed that if these functions are working well, 500 ft minimal vertical separation is acceptably safe, as considered in the collision risk analysis [1].

How safe the system needs to be is expressed in terms of safety objectives, or safety specifications in the E-SRM terminology. These safety specifications are derived by identifying hazards, identifying the potential safety consequences of those hazards, determining the severities of those consequences and then applying safety criteria. The safety specification can subsequently be used in the next phase, in which the system is designed and a preliminary system safety assessment (PSSA) is carried out. Figure 4 shows an overview of the safety analysis, from system definition to full safety case.

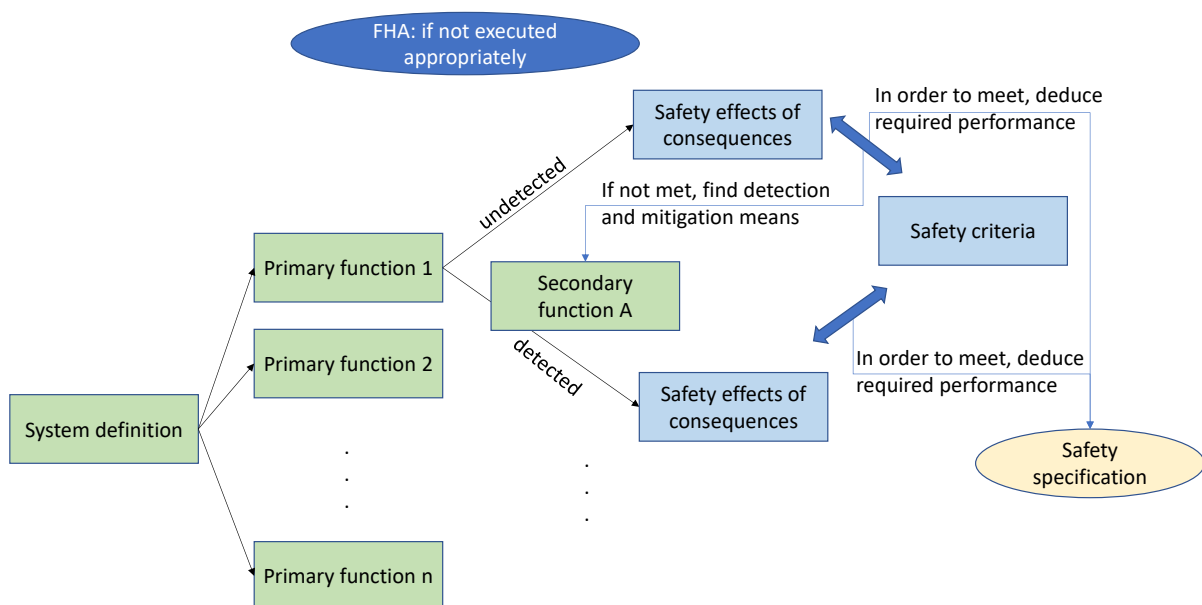


**Figure 4: The integration of the system specification and the safety analysis. FHA, PSSA and SSA stand for Functional Hazard Assessment, Preliminary System Safety Assessment and System Safety Assessment. For the RVSM 2 system, a distinction can be made to nominal operations (considering technical risks, see the collision risk analysis and the wake turbulence risk analysis) and non-nominal operations (operational risks, see the FHA). In Green-GEAR WP4, only the first iteration loop is executed, in which safety specifications are derived.**

The functional hazard assessment in this report focusses on the risks of providing separation in combination with geometric altimetry, in the context of reduced minimal vertical spacing as described in the Operational Service and Environment Definition [4], by means of the primary functions described in section 3.3.1. As will turn out, the only new main risk is a global failure of the altimetry, that is: one affecting multiple aircraft which are to be separated. Such global altimetry failure was not considered when assessing for example RVSM, as this would imply unconceivable behaviour of the earth’s atmosphere. Other risks of providing vertical separation by geometric altimetry are comparable to the risks of providing separation by barometric altimetry, but might increase as the minimal spacing is reduced.

The functional hazard assessment is executed as follows (as shown in Figure 5):

1. Formulate a hazard for the situation that a primary function is not executed properly.
2. For each hazard, identify the potential safety effects of its consequences if not detected.
3. For each hazard, identify the secondary functions to detect it and identify contingency procedures that can mitigate the potential severe safety effects of the consequences and then identify the potential safety effects in case the hazard is detected and mitigated.
4. Deduce safety specifications from the severity of the consequences of detected and undetected hazards how often each hazard might occur undetected and how often each hazard might occur detected.



**Figure 5: The main steps in the execution of the FHA. The primary functions follow from the system definition. The first set of questions to be answered is: what are the consequences if a primary function is not appropriately executed, what is the severity of these consequences, is the risk of those consequences acceptable? This might lead to conditions on the quality of the primary function and to a need to introduce secondary functions that intend to mitigate those risks if considered unacceptable. The second set of question to be answered is: what are the consequences if a primary function is not appropriately executed but a secondary function mitigates the consequences, what is the severity of these consequences, is the risk of those consequences acceptable? This might lead to conditions on the quality of the secondary function.**

Step 1 starts with the four primary functions that were introduced in Chapter 3. Abbreviated, they read:

1. Altitude information is provided;
2. Aircraft's altitudes are estimated;
3. Altitudes are assigned to aircraft such that vertical separation is provided;
4. Aircraft fly according to the assigned altitudes.

These functions are elementary and already implemented in today's aviation, with several relations to all kinds of other operations.

Given these primary functions and the domains executing them, a functional hazard assessment would start by considering: what happens if these functions are not or are not appropriately executed? Possible follow-up events include that this is detected, communicated and counteracted. Although, as stated, the system design is not completely described in detail yet, it is possible to define functions for such detection, communication and counteracts. These are the secondary functions and contingency procedures as introduced in Chapter 3. The descriptions provided are on a conceptual level, as the secondary functions are to be designed in detail later on.

In Step 4 safety specifications are deduced from the assessment of the risk of these hazards. There is some arbitrariness in deducing the safety specifications, as is in any allocation of safety objectives, for the following reason. It might be required that a hazard would virtually never occur, such that secondary functions are not required. It may also be required that a hazard might occur undetected with a certain limited probability, leading to safety specifications for the secondary functions and the contingency procedures. It is tried to make reasonable choices in this respect, in line with what is currently applied in aviation. Moreover, certain arbitrariness might be kept since it depends on the situation whether all secondary functions are available. There is for example a difference between an airspace with full surveillance and air-ground communication coverage and an airspace without such coverage. As it may not seem appropriate to declare *a priori* that such coverage is essential<sup>9</sup>, the functional hazard assessment leaves these options open to a certain extent.

Since this research is exploratory, since the RVSM 2 system is not completely described yet, and since it is beneficial to keep some matters open for more in-depth analysis later on, it is decided to execute this functional hazard assessment in a semi-quantitative way.

In the guidance on E-SRM, several tasks are indicated that might assist in in preparation of executing an FHA. These tasks correspond to questions such as: who are the users of the services, what is the baseline reference, is the role of the human is consistent with human capabilities, etc.? Given the exploratory character of this research, these tasks are executed on a high level, and the basic answers to these questions are as follows:

- The relevant users of RVSM 2 are all airspace users entering the RVSM 2 airspace. As a starting point of this FHA, it is assumed that these airspace users comply to the rules and conditions for entering RVSM2 airspace. These rules and conditions are to be derived from the results of the FHA. In a later stage, in the preliminary safety assessment, the risks of entering the airspace without complying to the rules and conditions are to be analysed.
- The benefits of RVMS 2 for its users are the increase in airspace capacity and the possibility to fly closer to the preferred altitude, thus reducing fuel consumption. RVSM 2 does not intend to deliver a safety benefit.
- The baseline (reference scenario) is the current operation for delivering vertical separation in en route airspace.

---

<sup>9</sup> From a pure European perspective, this might not be a relevant issue but as 500 ft minimal vertical separation might also be introduced in airspaces with procedural control, it globally is. It is anyway beneficial to determine to which extent certain ATC functions are critical for 500 ft minimal vertical separation.

- As indicated implicitly in the OSED [4], there are no significant concerns about whether the role of the human (i.e., pilots and air traffic controllers) are consistent with human capabilities, whether the technical systems support the human actors in performing their tasks, if the team structure (i.e., aircrew and combination of executive and planning controller) and team communication support the human actors in performing their tasks, with the argument that there is no qualitative change of the human tasks to be performed when vertical separation minima are reduced from 1000 ft to 500 ft.

## 5 Hazard analysis

---

### 5.1 Identified hazards

As indicated in Chapter 4, a hazard is formulated for the situation that a primary function is not executed properly. This leads to the following four hazards:

- H1: The altitude information is not provided properly in a part of the airspace.
- H2: The estimate of the altitude of an aircraft is not provided properly.
- H3: An aircraft has not an altitude assigned to it such that it is vertically separated.
- H4: An aircraft does not fly according to its assigned altitude.

### 5.2 Causal analysis H1

The hazard H1 occurs when the altitude information domain does not provide altitude information at all, does not provide altitude information in a continuous way or does not provide proper, accurate altitude information in at least a part of the airspace.

#### 5.2.1 Causes

There are several events that might cause H1. These can occur at satellite level, in space and on Earth as well.

Satellites are prone to failures. If one satellite fails somehow and does not send out proper signals, this is not a direct cause for H1 in itself as there is redundancy in the receivers covered by multiple satellite fields of views. However, in case a poor Position Dilution of Precision (PDOP) applies, see also [1], a malfunctioning satellite may lead to the situation that the combination of remaining satellites signals is insufficient to obtain a sufficiently accurate estimate of the vertical position. Also, errors in the control segment of GNSS [1] may lead to the occurrence of hazard H1. For example, the GNSS error is dependent on the Age Of Data (AOD). This data concerns satellite's clock and ephemeris, which becomes less accurate if it is not updated often [6]. In a situation where many satellites in the field of view have a high AOD, the GNSS position determination is not accurate anymore.

GNSS signals are prone to atmospheric (mainly ionospheric) distortion. The magnitude of the ionospheric effects depends on time-of-day, season, location and solar conditions [7]. Moreover, cosmic rays interact with Earth's ionosphere, possibly distorting GNSS signals [8]. The local distortion might be such that this leads the occurrence of hazard H1.

GNSS signals are also prone to interference. This interference can be intentional or unintentional. Unintentional interference may occur when a radio-frequency signal in the GNSS band is transmitted that has a different purpose in itself or is the unintended result of poor system design or operational malfunctions. This could potentially overpower GNSS signals and degrade reception and accuracy [9]. Widespread intentional interference of GNSS signals usually occurs for military purposes and could potentially affect all aircraft in a certain airspace.

Two types of intentional interference can be distinguished: jamming and spoofing. In case of jamming, the GNSS signals are overpowered by other signals in the same radio frequency band, rendering the

GNSS locally ineffective. Incidents of intentional, large-scale jamming have among others occurred in Eastern Europe in relation to the conflict in Ukraine, in the USA and in the Middle East [10]. But also the use of personal privacy devices to prevent tracking has been known to locally jam GNSS signals. In case of spoofing, counterfeit GNSS signals are broadcast, causing receivers to compute incorrect position estimates. By contrast to jamming, the *production* of signals able to spoof GNSS receivers cannot occur as an unintended side effect because of the complexity of the signal, but incidents of unintentional spoofing are known: e.g. when the replay of recorded GNSS signals for test purposes has unintentionally been received by operational users [11]. It appears that even after an aircraft has flown out of an area with spoofing, its navigation might be disturbed for some time as the navigation filters may have been incorrectly tuned with the counterfeit position and/or velocity input.

### 5.2.2 Consequences

If there are no secondary functions, the consequence of an occurrence of H1 is that, depending on its cause, aircraft in a part of the airspace cannot derive altitude estimates in a continuous way or derive incorrect altitude estimates. In both cases, aircraft might deviate from their assigned altitudes. This might in turn lead to an increase of the mid-air collision probability as vertical separation is not maintained.

If the cause of the hazard H1 occurrence is inside the altitude information domain, a *lack of altimetry integrity* message might be provided, if that secondary function as described in section 3.3.2 is available. The airborne domain then becomes aware of the occurrence and individual aircraft might then apply the *Procedure Single Unable Altimetry* (PSUA). Moreover, the ground domain then also becomes aware and might apply the *Procedure Multiple Unable Altimetry* (PMUA). The latter is preferred as multiple aircraft might be affected and coordination in precautionary actions might be more effective.

If the cause of the hazard occurrence is outside the altitude information domain, there are other secondary functions that might detect the hazard occurrence. The most relevant one is that the ground domain detects the occurrence by processing one or a combination of the following information items: receipts of *lack of unable altimetry* messages from several aircraft (if that secondary function is available), the detection of several aircraft deviating from their assigned altitude (if the following secondary functions are available: aircraft send out *own altitude* signals and the ground domain verifies if these signals correspond to the altitudes assigned) and other information items, such as an indication of jamming or spoofing. After the ground domain has detected the occurrence, it might apply the *Procedure Multiple Unable Altimetry* (PMUA). The consequences of the PSUA application are likely a significant disruption of the air traffic flow and an at least temporary increase of the mid-air collision probability.

## 5.3 Causal analysis H2

Hazard H2 occurs when the estimate of the altitude of an aircraft is not provided properly. H1 taking precedence over H2 implies that the altitude information domain is providing adequate altitude information, and that the cause is therefore internal to the aviation domain. The causes for H2 are different when using geometric altimetry, but the consequences are similar as they would be when using barometric altimetry. The failure of the GNSS altimetry system in the airborne domain is only described here on a high level.

### 5.3.1 Causes

Even though sufficient GNSS signals are provided, the airspace user's systems are not able to produce a proper altitude estimate. When using geometric altimetry, the most important cause for this would be a technical failure of the hard- or software of the geometric altimetry system. Hardware components that could fail are for example the GNSS receiver, antennas, connectors and cabling, data networks, the cockpit display, or for example the power supply. A software failure would occur for example when Receiver Autonomous Integrity Monitoring (RAIM) fails and the operators are not notified of possible errors.

### 5.3.2 Consequences

When there are no secondary functions the consequence of an occurrence of H2 would be that a single aircraft cannot derive altitude estimates in a continuous way or derives incorrect altitude estimates. Since the causes are internal to the airborne domain, or a single aircraft, it is extremely unlikely that a large number of aircraft would be affected by this hazard at the same time. If H2 occurs an aircraft might deviate from its assigned altitude, possibly leading to vertical separation not being maintained, ultimately leading to a mid-air collision.

When an aircraft is subject to H2 and it is detected by the aircraft itself, it might emit an *unable altimetry* message, which is to be received by the other airspace users in the vicinity, and by the ATC unit where this aircraft is under control. The *own altitude* secondary function would be compromised since the aircraft would no longer be able to provide an estimate of its own altitude. In this case the PSUA would have to be initiated in order to ensure sufficient separation from other airspace users.

## 5.4 Causal analysis H3

Hazard H3 occurs if an aircraft does not have an altitude assigned to it such that it is vertically separated. This is a direct failure of the primary function that the ground domain assigns an altitude to each individual aircraft such that it is vertically separated. Note that this function and hazard are also present in current RVSM operations and are not different in RVSM 2 to any significant degree.

### 5.4.1 Causes

A number of causes can be named for an aircraft not to have an altitude assigned to it such that it is vertically separated. First, the message was not sent, which could happen due to some technical malfunction. Second, the message was not received, which could also happen due to technical circumstances. Third, an altitude was assigned that will not guarantee vertical separation, which could be both due to technical and human error. All of these causes are already at play today at 1000 ft separation and barometric altimetry, and will stay the same when reducing the separation minima and transitioning to GNSS altimetry.

### 5.4.2 Consequences

H3 would lead to aircraft not having altitudes assigned such that they are sufficiently separated, or that aircraft do not have an altitude assigned to it at all. If no secondary functions are present this could lead to a mid-air collision as different airspace users could be traveling on conflicting trajectories.

In current RVSM operations STCA and ACAS form important barriers to mitigate these risks, and they likewise would have to do so in RVSM 2.

## 5.5 Causal analysis H4

H4 occurs when an aircraft does not fly according to its assigned altitude. Again, note that this is hazard is also present in barometric RVSM. In RVSM 2 a geometric target altitude would be followed, instead of a barometric altitude, but the hazard is otherwise not appreciatively different.

### 5.5.1 Causes

Pilots typically enter the commands issued by ATC in the FMS. With input from the FMS the autopilot then actuates the control surfaces such that the aircraft navigates as close as possible according to the intended altitude. Any technical issue in any of these sub-systems could cause the Flight Technical Error (FTE) (see [1]) to be unacceptably large, which are out of scope for this FHA, except for a number of operational errors listed in section 4.1. For example, atmospheric disturbances such as turbulence may lead to large height deviations for which the aircraft's flight control system cannot sufficiently correct.

Entering the commands issued by ATC into the aircraft's technical systems leaves room for human operators to make errors. For example, a pilot may wrongfully think to hear a different altitude than what is communicated through RT by the ATC unit. Or the pilot may hear the cleared altitude correctly, but enters the wrong altitude into the FMS.

### 5.5.2 Consequences

When an aircraft does not fly according to its assigned altitude ATC cannot ensure that the aircraft are sufficiently separated, which could ultimately lead to a mid-air collision. In the case the inability to maintain a certain flight level is detected an *unable height-keeping* message can be issued to other airspace users and to the relevant ATC unit. ATC can then provide sufficient separation from other airspace users, or airspace users can take corrective actions themselves, which could be issued by for example ACAS.

Another secondary function that could act as a barrier here is conformance monitoring, where the ATC unit receives *own altitude* signals from all aircraft and check if these deviate from the assigned altitude. If this deviation were to exceed a certain duration or magnitude ATC could provide corrective actions.

## 6 Safety Specification

---

### 6.1 Approach

As explained in chapter 5, the next step in the FHA approach is to deduce safety specifications from the likelihood and severity of the consequences of detected and undetected hazards, in terms of primary and secondary functions. As indicated, this is done not purely quantitatively as this is not yet possible. Instead, a qualitative and semi-quantitative approach is adopted.

The approach to the safety specification within the FHA for RVSM 2 is based on the following observation. The hazard H1 does not apply in the reference situation (the current operations) while the hazards H2, H3 and H4 do. This is first explained in some detail below, after which it is explained what this implies for the safety specification approach.

The hazard H1 roughly corresponds to the situation in which altitude information is not provided properly in a certain block of airspace. It is considered a global hazard as it may affect multiple aircraft. It might occur in RVSM 2 operations as GNSS is dependent on man-made systems and vulnerable transmissions of electromagnetic signals. When these systems fail or when the transmissions are distorted, all aircraft in a part of the airspace suffer consequences. The hazard H1 does not occur in the reference situation: there is no common cause for failures affecting multiple aircraft navigating vertically by means of barometric altimetry (apart from very unlikely events in the earth's atmosphere which would severely endanger aircraft anyway, like volcanic eruptions). The hazards H2, H3 and H4 roughly correspond respectively to situations in which aircraft do not obtain proper altitude estimates, in which no vertical separation is provided by assigning altitudes and in which aircraft deviate from their assigned altitudes. All these hazards may occur in the RVSM 2 operations as well as in the reference situation.

Their frequency or severity in the RVSM 2 operations might however not be the same as in the current operations, as the vertical separation minima are reduced. For example, the frequency of failure of an aircraft to obtain an altitude estimate may be higher or lower when using GNSS altimetry as opposed to barometric altimetry. Also, the severity of H2, H3 and H4 may be higher as there is less spacing and time for corrective actions through secondary functions. Even though H2, H3 and H4 are present in both RVSM and RVSM 2, simply copying the safety specifications from RVSM may not suffice.

Due to this observation that H1 is novel while H2, H3 and H4 are not, the derivation of safety specifications for H1 is different from the derivation of safety specifications for H2, H3 and H4. For the latter ones, the Accident Incident Models (AIM) of E-SRM can be used. This model describes the relevant risks in the reference situation, that is: the accident distance-based classes and associated frequency of occurrences for Mid-Air Collision (MAC) in controlled airspace for the current en route operations [12]. For each of the causes and barriers in the model, the probabilities are roughly reassessed considering the differences between current and RVSM 2 operations. Applying the safety criteria, safety specifications are deduced. Due to the novel and global nature of hazard H1, this approach cannot be adopted. Instead, an absolute approach is adopted, without reference to the current operations, deducing safety specifications on more general risk considerations.

## 6.2 Safety specifications for H1

The probability of a hazard H1 occurrence is difficult to estimate, mainly as the development of jamming and spoofing events in the future is uncertain. However, due to the variety of potential causes of H1, the probability is not negligible. As the consequence of an undetected or not-mitigated occurrence of hazard H1 is an increase of the mid-air collision probability, this leads to the conclusion that there is a need for mitigation, independent of which precise safety criteria are applied.

Some causes, such as the unintended interference, can be mitigated by the use of Dual Frequency receivers. As the prevention of a hazard H1 occurrence is preferred over the mitigation of its consequences, this leads to the following safety specification:

- *Aircraft in RVSM 2 airspace should use Dual Frequency receivers.*

Some causes, such as in the GNSS control segment or due to a low VDOP related to the dynamic GNSS constellation, can be mitigated by the use of multiple GNSSs. This might lead to a safety specification prescribing that but this might also have other drawbacks. A more detailed analysis about the pros and cons of such specification is therefore postponed to the PSSA.

There are basically two types of counteractions against a hazard H1 occurrence: with and without coordination of the aircraft involved. The main candidate for the coordinating actor is the ground domain. As indicated before, there is not however a priori need for a ground domain that can communicate in a continuous way with all aircraft in RVSM 2 operations; just like RVSM operations are applied in airspaces without ATC surveillance and communication. Therefore, first the situation without such ground domain is considered.

If there is no coordination to counteract the consequences of a hazard H1 occurrence, it might be possible that aircraft coordinate their actions among them. This is however a way of operating without a solid analogue in the current operations and therefore disregarded in this report. If there is no coordination, individual aircrew might apply the *Procedure Single Unable Altimetry*, as described in section 3.4, being aware that their altitude estimate is not proper but possibly not being aware that aircraft in the vicinity suffer the same problem. This likely imposes severe conditions on the PSUA design in order to maintain safe operations. This leads to the following safety specification:

- *If there is no ground domain that takes coordinated actions in case altitude information is not provided properly in a part of the airspace, the PSUA should be designed such that it is safe when applied simultaneously by several aircraft in each other's vicinity.*

If there is however a ground domain that might coordinate actions in case of a hazard H1 occurrence, this is preferred above uncoordinated action as such precautionary actions are more effective. Moreover, in case the RVSM 2 airspace is controlled tactically, the ATC units involved have means for secondary surveillance and two-way air-ground communications, easing not only the detection of a hazard H1 occurrence but the implementation of subsequent actions. A coordinated action by the ground domain requires the last secondary function described in section 3.3.2: the ground domain detects inadequacy of the altitude information in a part of the airspace. This can be done by processing one or a combination of the following information items: a) receipt of a *lack of altimetry integrity* message from the altitude information domain, b) receipts of *unable altimetry* messages from several aircraft, c) the deduction of several aircraft deviating from their assigned altitude and d) other

information items, such as an indication of jamming or spoofing. If the ground domain has detected the inadequacy of the altitude information, it might initiate the *Procedure Multiple Unable Altimetry*.

However, an individual crew that has detected that the altitude estimate is not proper might initiate the PSUA before the PMUA is initiated. This is not preferred, as coordination might be lost, when some aircraft execute the PSUA and others do not. In order to prevent this, the ground domain should detect a potential inadequacy of the altitude information in a part of the airspace fast and first inform aircraft even before aircraft are instructed to manoeuvre to regain separation. These considerations lead to the following set of safety specifications.

- *The altitude information domain should provide a lack of altimetry integrity message if there is uncertainty about the accuracy of the altitude estimate that can be derived from the altitude information. These messages should be received by the ground domain, at least by the ATC units providing services in and close to the part of the airspace where it applies. These messages should be received by the airborne domain, at least by the aircraft flying in and close to the part of the airspace where it applies.*
- *Each individual aircraft should send out own altitude signals in a continuous way. These signals include the altitude estimate, together with some kind of identification of the aircraft sending the signals out. These signals should be received by the ATC units providing services in or close to the part of the airspace in which that aircraft flies.*
- *The ATC units should receive the own altitude signals of each individual aircraft in a continuous way and verify if there are significant deviations from the assigned altitudes.*
- *Each aircraft should send out an unable altimetry message if a lack of availability, accuracy or integrity of the altitude estimate is detected. These messages should be received by the ground domain, at least by the ATC units providing service in and close to the part of the airspace in which the aircraft flies.*
- *The ATC units should detect inadequacy of the altitude information in a part of the airspace by processing the following information items: a) receipt of lack of altimetry integrity messages from the altitude information domain, b) receipts of lack of unable altimetry messages from several aircraft, c) detection of several aircraft deviating from their assigned altitude in a part of the airspace and d) other information items, such as indications of jamming or spoofing.*
- *If an ATC unit detects that there is a possibility that altitude information in a part of the airspace is inadequate, it should first inform all aircraft about this possibility. The aircrew having received this information should not initiate a PSUA.*
- *If an ATC unit has confirmation that altitude information in a part of the airspace is inadequate, it should coordinate with other ATC units and it should initiate a PMUA.*

The PMUA is not designed yet. Despite of that, one can imagine a procedure in which the ATC units start separating aircraft horizontally if possible. In case this is not possible and there are only concerns about the limited accuracy of the altitude estimates, aircraft might be separated vertically by 1000 ft or 2000 ft. As this is not possible in each situation, the use of barometric altimetry might be required, possibly in combination with declaring a reference barometric pressure to avoid large height adaptation when aircraft change from a geometric altitude to a corresponding barometric altitude. These considerations show that the operational consequences of a PMUA implementation are likely

critical, especially if several ATC units are involved. These considerations also show that there might be a need for a flexible procedure, that depends on the circumstances (e.g. the potential conflicts, the local air traffic density, the possibilities to divert horizontally) and leaves options for the air traffic controller. This might however make the procedure also complex. It seems to be required that the PMUA is only applied rarely, in the order of once in ten years for an airspace as the ICAO EU Region, although this is not deduced from solid grounds. In order to have a reference, this is however formulated as a safety specification.

- *The frequency of occurrence of altitude information being inadequate in a significant part of the airspace should be less than once in ten years.*

### 6.3 Safety specifications for H2, H3 and H4

The RVSM 2 concept focuses on the European RVSM airspace. This area is a tactically controlled airspace that has complete surveillance and communication coverage. The causes and likelihoods for H2, H3 and H4 are therefore the same as in current operations (with possibly an exception for H2, but the likelihood of failure can be specified to not be lower than barometric systems), but the consequences are likely to change due to the reduced separation.

This would lead to the following three specifications related to the latter three hazards:

- *GNSS altimetry systems should have a similar maximally allowed rate of failure as current barometric altimetry systems.*
- *An aircraft not having an altitude assigned to it such that separation is maintained will have the same maximally allowed occurrence rate as in current operations.*
- *In RVSM 2 an aircraft not flying to its assigned altitude should have a similar maximally allowed rate as in current RVSM operations.*

In accordance with the E-SRM, the EUROCONTROL Accident Incident Model (AIM) is used to evaluate the total risk with regard to hazards H2, H3 and H4 by considering that the frequency of occurrence of these hazards may not change, but that due to the reduced separation the margin for corrective actions through barriers is reduced. The AIMs are a series of barrier-based trees describing risk propagation in ATM operations and have been developed in a number of SESAR projects [12]. The AIM model that is applicable to the RVSM 2 concept is the one for Mid-Air-Collision risk in the en-route (MAC ENR) part of the flight. As noted in the accompanying documentation, this model is designed to be generic and flexible, and can be used as a starting point and adapted to specific operational environments.

As such the MAC ENR AIM will be adapted to the current operations (by only considering risk due to vertical deviations and conflicts, which will serve as a reference) and to RVSM 2 concept with the following steps:

- A selection will be made among the precursors by considering only those that are relevant for providing vertical separation, considering vertical deviations. Precursors that are not relevant are removed.
- The effectiveness of each barrier is evaluated.

- The risk for a mid-air collision is evaluated by re-calculating the propagated risk. When considering accidents and precursors, moving up the tree, risk propagates by addition when branches merge. For the barriers the risk propagates upwards by multiplying with the barrier failure probability. The top accident-element in the risk tree is the risk of a mid-air collision.
- This top mid-air collision risk is assessed against the TLS of  $2.5 \cdot 10^{-9}$  for the risk due to non-nominal causes.

The adapted MAC ENR AIM for RVSM is shown in Figure 6, the original can be found in [12]. In the context of RVSM the focus is only on the collision risk due to vertical deviations. Consequently, any lateral deviations, indicated as *Aircraft Lateral Deviation* and *Aircraft Speed Deviation*, are out of scope. Also, *Aircraft Vertical Rate Deviation* is out of scope as these are not expected to lead to more conflicts when the separation minima are reduced. Pre-tactical conflicts are related to a failed management of the density of airspace users in a certain section of airspace. The added flight levels will increase the capacity however and as such pre-tactical conflicts are perhaps less likely to occur. Pre-tactical conflicts can therefore conservatively be left out of the analysis.

Airspace infringements could lead to aircraft not being vertically separated, as the involved aircraft are not under the control of the same unit. With increased capacity this risk may in fact decrease, so this factor can also be conservatively left out. That leaves the adapted AIMs to focus on, as shown in Figure 6 and Figure 7, *Aircraft Vertical Deviation*, *Unit/Sector Induced Tactical Conflict* and *Other sectors/units Induced Tactical Conflict*.

One may notice the barrier failure probability of the first barrier B61 of 100%. This stems from the assumption in the original ENR AIM that there is no ATC monitoring tool for deviation and warning.

The resulting AIM is representative for the risk of current operations in the en-route part of the flight, of which RVSM is a part. The risk of a mid-air collision can be calculated in this system by propagating the risk (i.e. add when branches merge, multiply with the barrier failure probabilities). *The Aircraft Vertical Deviation* leads via *Trajectory Vertical deviation not timely detected and corrected by ATC*, *Conflict due to Vertical Deviation* and *Conflict due to Crew/ac Deviation* to *Crew/Aircraft Induced conflict*. Similarly, *Unit/Sector Induced Tactical Conflict* and *Other sectors/units Induced Tactical Conflict* lead to *ATC Induced conflict*.

Now these *Crew/Aircraft Induced conflict* and *ATC Induced conflict* both lead to the same precursor: *Imminent Separation Infringement*. In short, through a number of events, among which the *ATC collision prevention* barrier, the *Imminent Collision* precursor, and the *Combined Visual- and ACAS-based avoidance* barrier this leads to a MAC probability of  $2.5 \cdot 10^{-10}$  per flight hour, which is a factor of 10 below the maximally permissible TLS.

Now it should be recognized that the RVSM 2 adapted MAC ENR AIM is the same as the one just described for the reference scenario, except for two important factors: *ATC collision prevention* and *ACAS-based avoidance* (which itself is part of the *Combined Visual- and ACAS-based avoidance*), as (i) the time available for solving conflicts will be reduced and (ii) the availability of ACAS in RVSM 2 is not self-evident. This will be further explained in the coming two sections, but the RVSM 2 adapted can already be seen in Figure 7.

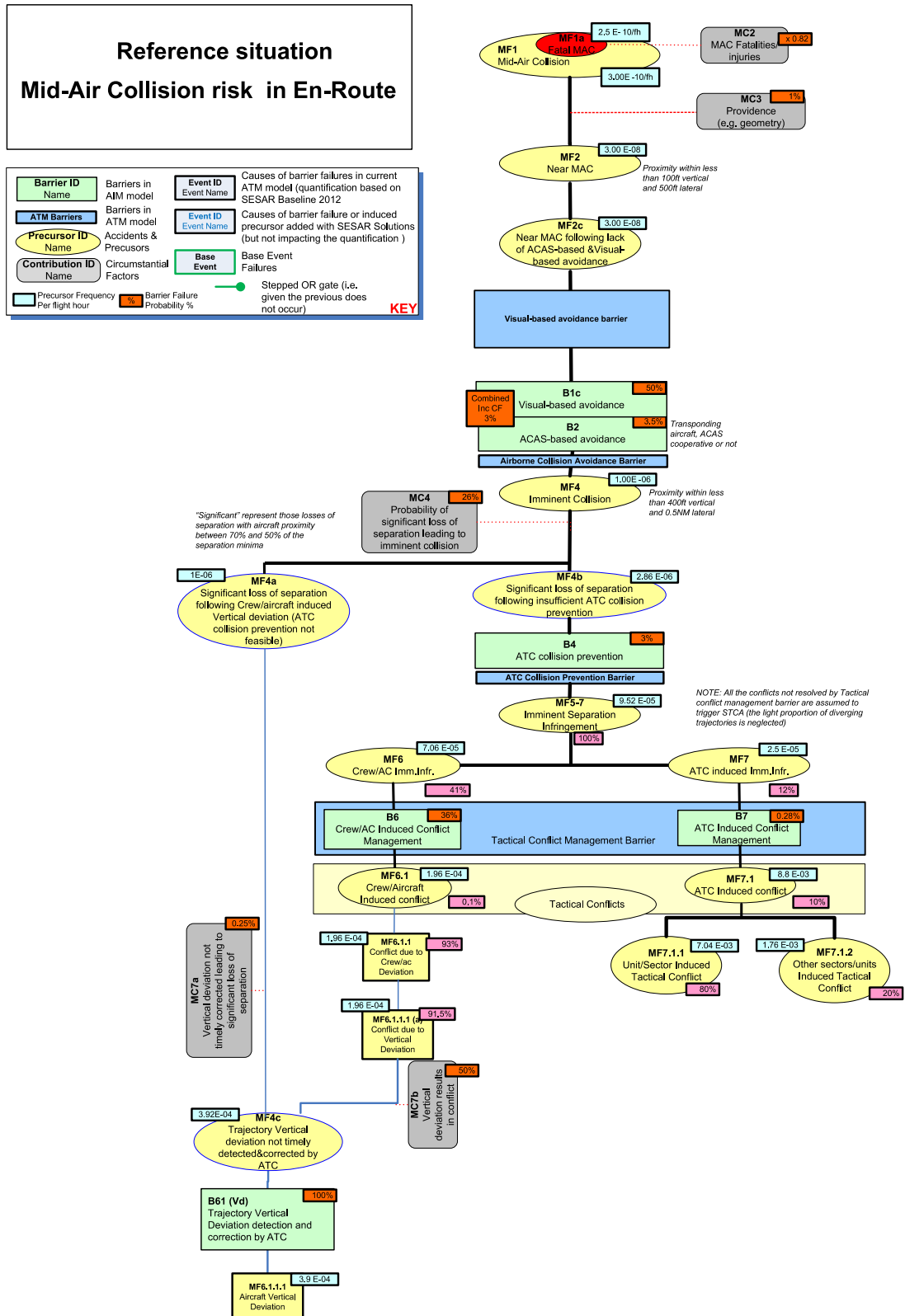


Figure 6: Mid Air Collision (MAC) en route (ER) Accident Incident Model (AIM) adapted to the 1000 ft RVSM operation. Note that with this approach the probability of a MAC top event is  $2.5 \cdot 10^{-10}$  per flight hour.

### 6.3.1 ATC collision prevention

Because the time for resolving conflicts is effectively halved when transitioning to RVSM 2, the effectiveness of the ATC collision prevention barrier is reduced. This can be understood by considering two aircraft that are vertically separated at the minimum distance for a conflict. Since the causes in RVSM 2 are similar to the reference situation and only the separation minimum is reduced, the amount of time available to solve vertical conflicts is halved when halving the minimal vertical separation distance, which would be the case when transitioning from 1000 ft separation to 500 ft separation. Therefore, if the time available to solve a conflict at traditional RVSM was  $t_{collision}$ , the time available to solve a similar conflict will be  $t_{collision}/2$ . The new barrier failure probability is estimated by assuming that the time to solve a conflict for ATC can be modelled with an exponential distribution, the Cumulative Density Function (CDF) of which is given by  $F(t) = 1 - e^{-\lambda t}$  for  $t \geq 0$ , where  $F(t)$  is the fraction of problems solved at time  $t$  and  $\lambda$  is the problem-solving rate.

According to Figure 6 the barrier failure probability is 3% in classical RVSM, in other words, 97% of conflicts are resolved within the time that is available. This can also be written as  $F(t_{collision}) = 1 - e^{-\lambda t_{collision}} = 0.97$ . For RVSM, the same expression is  $F(t_{collision}/2) = 1 - e^{-\lambda t_{collision}/2}$ . When combining both these equations, it can be shown that  $F(t_{collision}/2) \approx 0.83$ , which results in a barrier failure probability of 17%.

### 6.3.2 Visual- and ACAS-based avoidance

Issues regarding ACAS have previously been described in the Collision Risk Analysis [1]. In current ACAS systems resolution advisories will be issued when aircraft would be vertically separated at the proposed 500 ft separation. ACAS was therefore not listed in chapter 3 as one of the functions. However, recalculating the risk in Figure 5 showed that without the ACAS barrier, meeting the TLS would not be possible. As such, it was determined that the ACAS barrier will have to be present in order for the RVSM 2 concept to be feasible. Beyond the issue of unwanted advisories, the effectiveness is also likely to lower because of the reduced time for solving conflicts. ACAS will therefore likely have to be adapted both to fit the 500 ft separation minimum requirement, and to provide sufficient effectiveness to meet the TLS.

The way the ACAS-based avoidance barrier is incorporated in the AIM is somewhat more complex than the ATC collision prevention barrier, and how this is done in the original model cannot be easily determined. This is likely due to the fact that the ACAS-based avoidance barrier and the visual based avoidance barriers are highly interdependent, leading to a reduced effectiveness when they're combined. By assuming a maximally allowable top mid-air collision risk of  $2.5 \cdot 10^{-9}$ , a target effectiveness of the combined visual and ACAS barrier can be derived. Combining the  $2.5 \cdot 10^{-9}$  TLS and the increased ATC collision prevention barrier failure probability of 17% and recalculating the risk leads to a maximally allowable probability of failure for the combined visual- and ACAS-based avoidance barrier of 6.7%, or a barrier effectiveness of 93%.

Thus, the AIM-analysis leads to two additional safety specifications:

- *The combined visual- and ACAS-based avoidance barrier is to have an effectiveness of at least 93%.*
- *Controlled airspace-based operations are required in order to provide the ATC collision prevention barrier.*

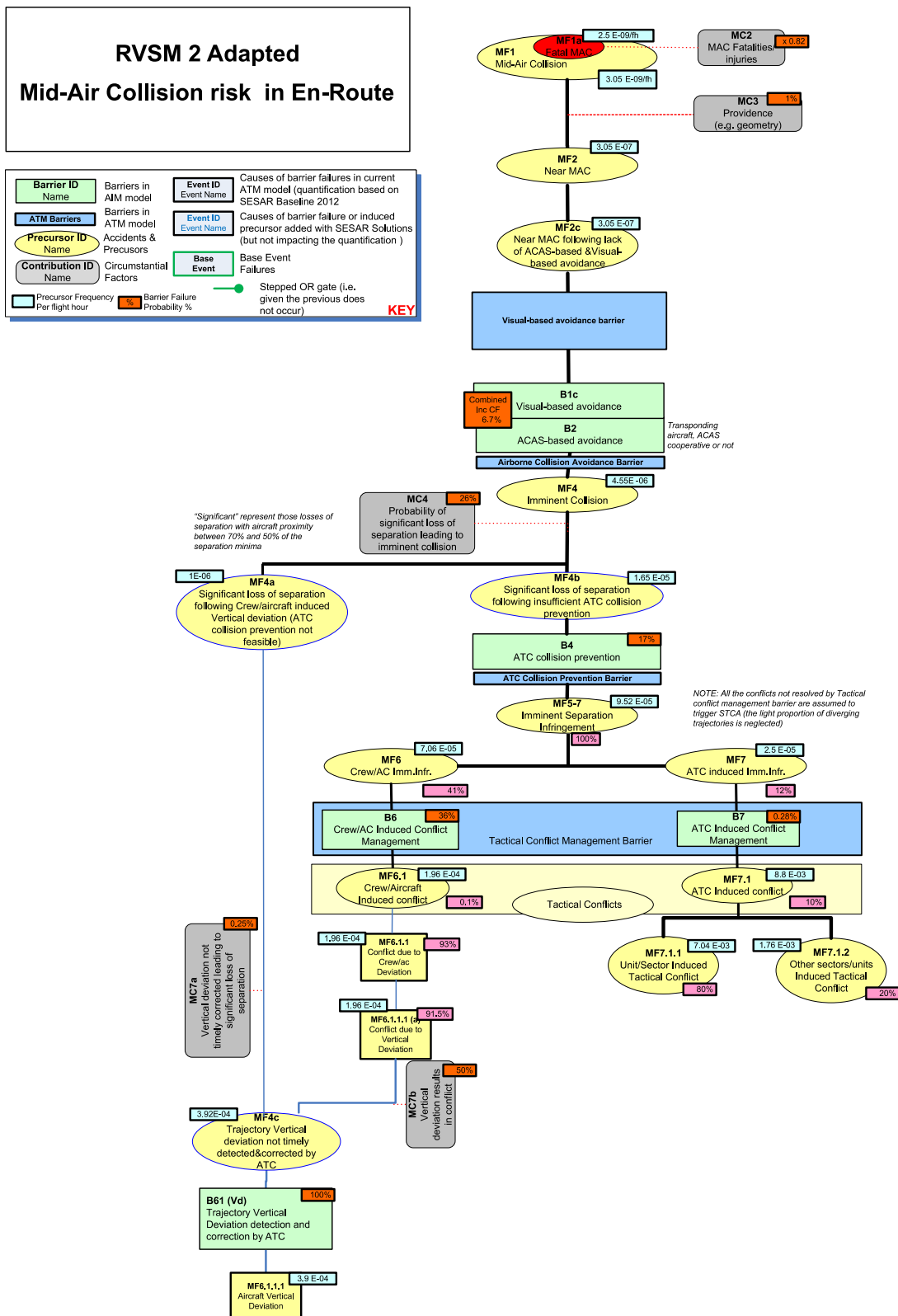


Figure 7: Mid Air Collision (MAC) en route (ER) Accident Incident Model (AIM) adapted to the RVSM 2 concept. Note that with this approach the probability of a mid-air collision top event is set to  $2.5 \cdot 10^{-9}$  per flight hour.

## 7 Conclusion

---

This study focused on the non-nominal risk associated with reducing the vertical separation minima to 500 ft in a GNSS based altimetry scenario in RVSM airspace. A top-down approach was used where the system risk was evaluated against a threshold of  $2.5 \cdot 10^{-9}$  collisions per flight hour, similar to traditional 1000 ft RVSM. Considering the low maturity of the concept not all details are known yet, and a combination of qualitative and quantitative safety specifications were derived.

A total of four primary functions were derived, in short: altitude information is provided, aircraft's altitudes are estimated, altitudes are assigned to aircraft such that vertical separation is provided and that aircraft fly according to the assigned altitudes. The four hazards corresponding to the failure of primary functions were respectively defined as (H1) the altitude information is not provided properly in a part of the airspace, (H2) the estimate of the altitude of an aircraft is not provided properly, (H3) an aircraft has not an altitude assigned to it such that it is vertically separated and (H4) an aircraft does not fly according to its assigned altitude.

It was recognised that only the first hazard was significantly different from current RVSM operations. In GNSSs the altitude information provided through the electromagnetic systems can be disrupted, for example through intended or unintended interference, which would affect all airspace users in a given region. For this no analogue exists in barometric altimetry operations where air pressure is the medium that provides the altitude information. Solutions such as Dual Frequency GNSS receivers will likely be necessary to reduce the likelihood of H1, but it can still not be considered as negligible. If there is no ground domain that can take coordinative actions, a Procedure Single Unable Altimetry (PSUA) should be in place that multiple aircraft safely execute individually.

Having a ground domain that coordinates a contingency procedure, Procedure Multiple Unable Altimetry (PMUA), when multiple aircraft lose the ability to determine altitude, would likely be preferable. This would likely also require a function for the ground domain to detect inadequacy of the altitude domain, which could be provided through different means, such as *lack of altimetry integrity* messages from the altitude information domain, or *unable altimetry* messages from the airborne domain. Because such a procedure would constitute a serious disruption of the air traffic operations, it is rather loosely concluded that it should not be required to be enacted more than once every ten years.

The likelihood and severity of the latter three hazards may be different if not effectively mitigated with secondary functions, but the required functions and procedures are not very different from current operations. As such the frequency of occurrence of the latter three hazards were assumed to stay the same when transitioning to RVSM 2. Further effects from transitioning to RVSM 2 were studied by the use of the Mid-Air Collision En-Route Accident Incident Model (MAC ENR AIM) from the E-SRM. The AIM was first adapted to 1000 ft operations, showing that according to this model the current risk due to non-nominal deviations is a factor 10 below the maximally allowed TLS.

Due to the reduced separation, it was recognised that a number of barriers would become less effective when transitioning to 500 ft separation, and that ACAS would require a complete reconsideration due to incompatibility of the systems that are currently in use with 500 ft minimal separation. Assuming a recalculated effectiveness of the ATC collision prevention barrier and a maximally allowable risk of a mid-air collision of  $2.5 \cdot 10^{-9}$  led to a minimal effectiveness requirement

of the combined visual- and ACAS based avoidance of at least 93%, as opposed to the 97% effectiveness at 1000 ft in traditional RVSM.

Even though a less effective ACAS is permissible in RVSM 2, achieving such a system is no trivial task. First of all, ACAS would have to be redesigned not to issue warnings at 500 ft vertical separation. In addition, the parameters of ACAS, such as the look-ahead time would likely have to be updated to accommodate the reduced available time for conflict resolution, but this is not allowed to result in unacceptable levels of nuisance resolution advisories. In addition, the 93% allowed effectiveness is based on the availability of ATC collision prevention. This was not a requirement in traditional RVSM, and would result in the requirement of RVSM 2 only being allowed in controlled airspace.

Since the exact details of RVSM 2 are not yet known this FHA only serves as an initial estimate of the system requirements, and can serve as a setup for further design of the RVSM 2 concept. The most important technical challenges identified in this study that would have to be solved in order for RVSM 2 to be feasible are the re-design of an effective ACAS, and the need for a contingency procedure in case a large number of the airspace users is unable to obtain adequate altitude measurements, which would only be allowed to be rarely needed. The latter may be especially challenging since disruption of the altitude information domain is currently of daily occurrence at the borders of the European airspace in the form of jamming and spoofing.

## 8 References

---

- [1] P. Jonk, B. Klein Obbink, J. Smeltink and I. Boshuizen, “Green-GEAR – iD4.1 – Separation Minima – Collision Risk Analysis,” SESAR , 2025.
- [2] T. Bauer and A. Koloschin, “SESAR 3 ER 1 Green-GEAR iD4.2 – Wake Turbulence Risk Analysis,” SESAR, 2025.
- [3] SKYbrary, “Safety Case | SKYbrary Aviation Safety,” [Online]. Available: <https://skybrary.aero/articles/safety-case>. [Accessed 24 02 2025].
- [4] P. Jonk, I. Boshuizen, A. Koloschin, B. Klein Obbink and J. Smeltink, “SESAR 3 ER 1 Green-GEAR,” SESAR Joint Undertaking, 2024.
- [5] ICAO, “Doc 9689-AN/953, MANUAL ON AIRSPACE PLANNING METHODOLOGY FOR THE DETERMINATION OF SEPARATION MINIMA,” icao, 1998.
- [6] United States Department of Defense, “Global Positioning System Standard Positioning System Performance Standard,” 2020.
- [7] Y. Béniguel, M. Angling and E. Banfi, “Ionospheric Effects on GNSS Performance,” 2012.
- [8] P. Velinov, S. Asenovski and K. Kudela, “Impact of cosmic rays and solar energetic particles on the Earth’s ionosphere and atmosphere,” *EDP Sciences*, 2013.
- [9] E. Ghizzo, E. Djelloul and J. Lesouple, “Assessing jamming and spoofing impacts on GNSS receivers: Automatic gain control (AGC),” 2024.
- [10] M. Felux, P. Fol and B. Figuet, “Impacts of Global Navigation Satellite System Jamming on Aviation,” *Institute of Navigation*, 2024.
- [11] K. Alexander and D. Lawrence, “GNSS Intentional Interference and Spoofing,” FAA, 2015.
- [12] D. S. a. R. (DSR), “Integrated Risk Model for MAC En Route,” EUROCONTROL, 2023.
- [13] ICAO, “Manual on Implementation of a 300 m (1000 ft) Vertical Separation Minimum Between FL 290 and FL 410 Inclusive,” International Civil Aviation Organization, 2002.
- [14] J. Brown, “What is GPS Spoofing? ...And How to Avoid It,” 2024.

## 9 List of acronyms

Acronym	Description
ACAS	Airborne Collision Avoidance System
AOD	Age Of Data
ATC	Air Traffic Control
CPDLC	Controller Pilot Data Link Communications
CRA	Collision Risk Analysis
FHA	Functional Hazard Assessment
FL	Flight Level
FMS	Flight Management System
FTE	Flight Technical Error
GBAS	Ground Based Augmentation System
GLONASS	GLObal'naya NAVigatsionnaya Sputnikovaya Sistema
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
LPV	Localiser Performance with Vertical Guidance
OSED	Operational Service and Environment Definition
PDOP	Position Dilution Of Precision
PMUA	Procedure Multiple Unable Altimetry
PSSA	Preliminary System Safety Assessment
PSUA	Procedure Single Unable Altimetry
RAIM	Receiver Autonomous Integrity Monitoring
RNP AR	Required Navigation Performance Authorisation Required
RT	Radio Telephony
RVSM	Reduced Vertical Separation Minima
STCA	Short-Term Conflict Alert
TLS	Target Level of Safety
TMA	Terminal Manoeuvring Area
TRL	Technology Readiness Level
WP	Work Package
WTRA	Wake Turbulence Risk Analysis

Table 1: list of acronyms

**AIRBUS**



**NATS**



**UNIVERSITY OF  
WESTMINSTER**



**UNIVERSITÀ  
DEGLI STUDI  
DI TRIESTE**

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or SESAR 3 JU. Neither the European Union nor the SESAR 3 JU can be held responsible for them.