ISSN 2754-1118 (Online)
ISSN 2753-6599 (Print)

Safety Assessment of Point Merge Operations in Terminal Airspace

An IEC 61508 Viewpoint

Derek Fowler[1] and Octavian Nicolas Fota[2]

1. Independent Safety Engineering Consultant, Reading, UK
2. EUROCONTROL Innovation Hub, Brétigny, France

Abstract

An article entitled "An IEC 61508 Viewpoint on System Safety in the Transport Sector", in Volume 1, Issue 2, of the Safety-Critical Systems Club eJournal, proposed a way of thinking about the safety assessment of transportation systems that is based on the fundamental principles of international functional-safety standard IEC 61508. Now, in this article, the example of Point Merge — a systemised method for sequencing arrival flows developed by the then EUROCONTROL Experimental Centre and first deployed in Oslo in 2011 — is used to outline how an IEC 61508 approach to safety assessment could be applied to the Air Traffic Management sector in general.

1 Introduction

IEC 61508 (IEC 2010) is probably the most widely-accepted, international generic standard on functional safety. Although its ancestry can be traced back to process industries, the intention behind the standard has always been to provide a solid, comprehensive basis for adaptation, as necessary, to meet the needs of a wide range of industry sectors.

Fowler (2022), proposed 'a way of thinking' about the assessment of the various safety-related systems deployed in the Transport sector — especially commercial-aviation and rail applications — based on the key principles and safety lifecycle set out in IEC 61508-1 and IEC 61508-4.

This article now takes an example application, from the Air Traffic Management (ATM) sector, of an operational concept for sequencing arrival flows in Terminal airspace, known as Point Merge, and uses it to outline how an IEC 61508 approach to safety assessment could be applied effectively to the ATM sector, and what the results thereof might look like, starting from the viewpoint of the traffic in the airspace being "virtual Equipment Under Control".

It is important to note that it is *not* the intention herein to prescribe IEC 61508-compliant processes for ATM applications — rather, it is to use the IEC 61508-1 lifecycle cycle model to shape thinking about system safety assessments away from a mindset that "*focussed too much on system reliability and not enough on system functionality, contrary to, inter alia, the most basic principles of the international functional-safety standard IEC*

© Derek Fowler and Octavian Nicolas Fota 2023.

61508" (Fowler 2022). *Nor* is it the intention to carry out a detailed compliance assessment of any existing ATM safety standards against IEC 61508 — the latter is left to readers with a sector-specific interest, and for whom the findings of Fowler (2015) might be relevant.

Like Fowler (2022), the scope of this article is limited to the following, initial phases of the IEC 61508 safety lifecycle, which result in the specification of detailed *functional safety requirements*[1] and *safety integrity requirements* necessary and sufficient for the subject safety-related systems to achieve a tolerable level of risk:

- Concept (Phase 1);
- Overall scope definition (Phase 2);
- Hazard and risk analysis (Phase 3);
- Overall safety requirements (Phase 4);
- Overall safety requirements allocation (Phase 5);
- Safety -related System (SRS) Safety Requirements Specification (Phase 9)[2];
- Other Risk-reduction Measures (ORRM) Safety Requirements Specification (Phase 10).

As we work herein through these lifecycle phases for Point Merge, it might appear that some of the steps could be simplified by, for example, subsuming them into other steps. Indeed, IEC 61508 allows for this to be done, where applicable, but, for the purposes of this paper, we decided to adhere exactly to the lifecycle detailed in Fowler (2022), except where indicated otherwise below.

2 Operational Context

Arrival procedures in Terminal airspace have historically involved open-loop vectoring of aircraft by Air Traffic Controllers. However, since the 1990s, Area Navigation (RNAV) procedures have gradually been introduced to systematise operations in most areas. A major drawback of both of these techniques, however, is that, under conditions of high traffic flows, their use tends to favour capacity at the cost of low flight efficiency and high environmental impact.

Therefore, the then EUROCONTROL Experimental Centre[3], Brétigny, France developed Point Merge operations (EUROCONTROL 2021) as a new method for integrating arrival flows, safely and efficiently, by combining the systematic use of lateral guidance by the aircraft's flight management system (FMS), with continuous descent approaches (CDAs), even at high traffic throughput.

Point Merge operations make use of Precision RNAV (P-RNAV)[4] procedures in terms of airspace design and functionality in the aircraft, but applied in a very specific way for arrival traffic in Approach airspace. The main difference between radar-vectoring (or

[1] The term *functional safety requirements* was coined in Fowler (2022) in preference to the (arguably ambiguous) IEC 61508 term of *safety functions requirements*; it covers safety requirements for both functionality (what has to be done) and performance (how well it has to been done).

[2] IEC 61508 phases 6 to 8 are concerned only with the planning of subsequent lifecycle phases and so are outside the scope of this paper

[3] Now called the EUROCONTROL Innovation Hub.

[4] Or equivalent

conventional P-RNAV) operations[5] and Point Merge operations is that in the former, arrivals are typically merged on to a line, whereas in the latter, they follow predefined routes until they are merged on to a point, known as a Merge Point.

Point Merge was first deployed in Oslo in 2011 and now operational at 37 or more airports across 4 continents, where it has been shown to provide significant potential benefits in terms of flight efficiency and the environment.

The question for the remainder of this paper is, however, would its introduction to a hypothetical airport be safe, and how would we demonstrate this, if we were to follow the IEC 61508 safety lifecycle?

3 Safety Assessment

3.1 Concept (IEC 61508-1 Phase 1)

3.1.1 Aim

The aim of this phase is to gather as much information about what IEC 61508 calls the *Equipment Under Control* (EUC), its *Environment*, and the *EUC Control System*, as necessary and sufficient to enable the other safety lifecycle activities to be satisfactorily carried out.

It is important to note that, as an enabling activity, this would be a precursor to, but not form part of, the safety assessment *per se* and would require substantial operational and system-engineering specialist input, relevant to each specific application. In practice, such material may be found in a typical Concept of Operations document.

3.1.2 EUC

As with other ATM applications, we can understand the EUC as being, in general, the flow of aircraft through the airspace, during landing or taking off, and/or taxiing on the airport surface — in this case, it is the flow of arrival traffic through Approach airspace, until each aircraft intercepts the Instrument Landing System (ILS) Glidepath beam for its final descent to the runway. This understanding is consistent with the core IEC 61508 principle that the EUC is the main source of hazards, which Safety Related Systems (SRSs) are required to mitigate in order to achieve a tolerable level of risk.

The key inherent properties of the EUC that we will assume for this Point Merge example are as follows:

- traffic is a mix of commercial jets / turbo-props and general aviation;
- arrivals per year: 100,000;
- maximum sustained arrival rate: 28 per hour;
- average arrival flight time in Approach airspace: 12 minutes;

[5] For example in "tromboning", where P-RNAV routes define a complete path from the Initial Approach Fix (IAF) to the final approach fix (FAF), including an extended down-wind leg, base leg, and initial approach path, but aircraft are vectored off the downwind leg to merge on to the runway extended centreline.

- on average, at least 95% of aircraft in the main arrival flow are certified and approved for P-RNAV approaches;
- aircraft wake-turbulence category mix is dependent on time of day; during peak times it averages 1.5% super; 25% heavy; 65% medium; 8.5% light.

3.1.3 Environment

IEC 61508 defines the environment in terms that include its physical, operating, legal and maintenance properties.

The environment properties for Point Merge operations are assumed to be as follows, the list covering most of the key points necessary for the safety assessment:

- Airspace Parameters and Flight Rules:
  - applies to Approach airspace / Approach control phase, corresponding to Approach arrival sectors, typically between the IAF and the FAF or transfer to the Tower;
  - all traffic operates under Instrument Flight Rules.
- Transition Altitude is 18,000 ft, well above the highest part of the Point Merge structure.
- Adjacent Airspace / Operations:
  - adjacent surrounding airspace is En-route;
  - airport served by the Point Merge structure has two, parallel, main runways (26L and 26R), one for landing and one for take-off (interchangeable), with ILS Cat II.
- Climate and Terrain:
  - climate is temperate, liable to dense fog in winter and occasional heavy thunderstorm activity in summer; prevailing winds are westerly;
  - terrain is generally undulating but with high mountains starting at 35 nautical miles South-west of the runway.
- Environmental Constraints: for the purposes of this paper, we will assume that no particular environmental constraints apply to Point Merge operations.

3.1.4 EUC Control System

Given the above interpretation of the EUC itself, we can understand the EUC Control System as being a functional system, encompassing people, procedures and equipment, and comprising, in general:

- The usual Air Traffic Services (ATS) and facilities to be found at a typical busy airport, irrespective of the specific type of Approach operations in place; and
- The Flight Crew actions related to flying the P-RNAV routes and following the ATS procedures and instructions, together with airborne equipment supporting the execution of those actions.

It is important to emphasise that, in the description of the EUC Control System which follows, the focus is on the business / operational *rationale* for Point Merge, and the text

deliberately makes little or no explicit reference to the safety constraints that, of course, must be applied to Point Merge operations — these will be addressed in Phase 3 *et seq*.[6]

The Point Merge configuration applicable to this safety assessment is a single structure, as shown in Figure 1.

The Point Merge structure comprises two continuous P-RNAV routes, linking two IAFs (IAF1 and 2) to the FAF[7] and the start of final descent into a single arrival runway (RWY 26L), with waypoints signified by the star symbols. It includes the following key stages:

- Two Sequencing Legs, which are centred on the Merge Points; the inner Leg (i.e. the one closer to the Merge Point) is, wherever practicable, higher than the outer Leg;
- Two Run-off Legs, each one of which connects the end of a Sequencing Leg to the Merge Point;
- The FAF, by which time the aircraft will have acquired the ILS Glidepath for final approach and landing.

A holding point is provided prior to each Point Merge entry point, for use as required.

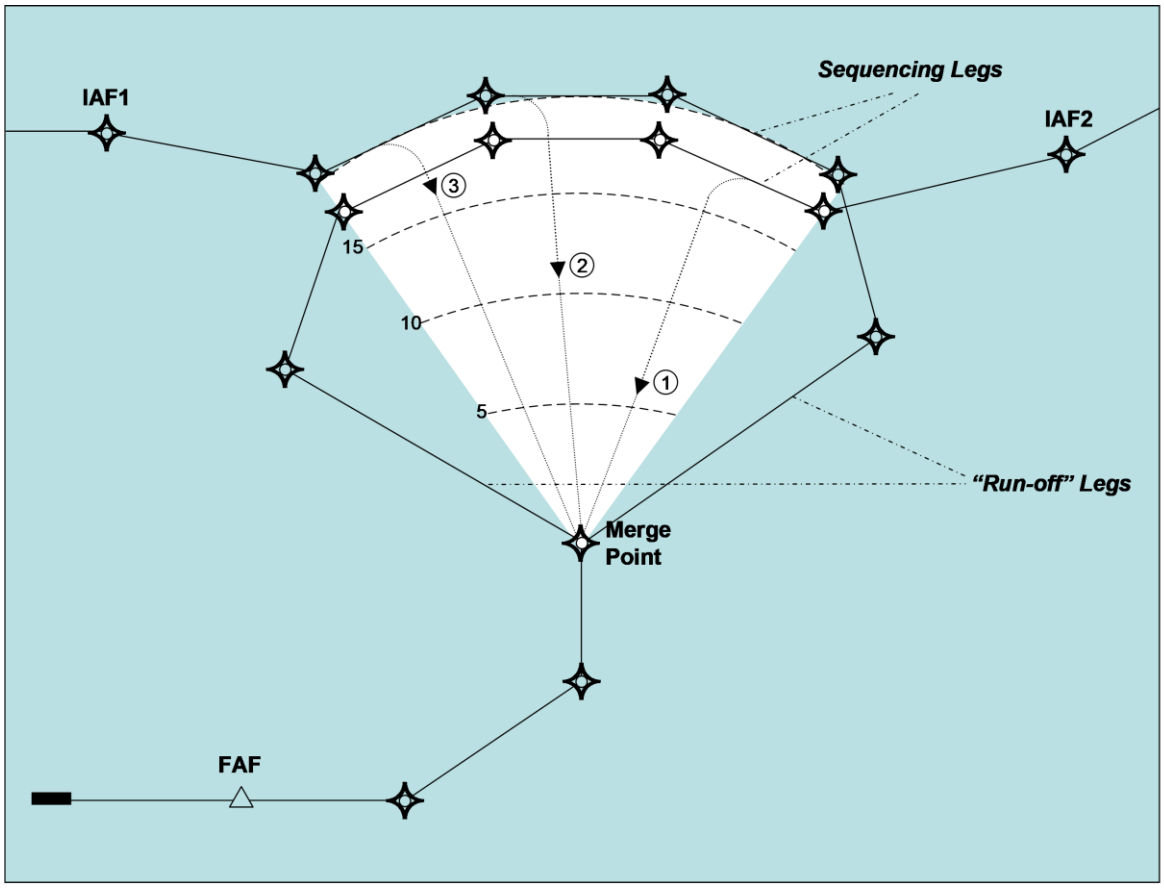


Figure 1 ~ Point Merge Route Layout

The boundary between Approach airspace and adjacent En-route / Terminal airspace sectors occurs before the IAF in each case.

[6] It is acknowledged that this distinction might seem somewhat artificial; however, it serves to emphasise the point made, at Sub-section 3.1.1 herein, that this phase is a necessary precursor to, rather than a part of, the safety assessment *per se*.

[7] A dual configuration is also possible, based on an additional, mirror-image structure to the south of the runway centreline, with the two Merge Points linked to a Common Point, which itself has a single route linking it to the FAF.

What we have identified as the "EUC Control System", is required, under *normal* operating conditions[8], to establish and maintain the arrival sequence, within this structure, i.e. to order the arrivals, and *space* them in accordance with the runway metering requirements, so as to maximize runway throughput while taking account of the safety and other needs of individual flights[9]. This is achieved as follows:

- non-arrival traffic in the area is handled as follows:
  - departing traffic (usually from RWY26R) follows standard instrument departure (SID) routes, above the Point Merge structure, to the top of climb;
  - overflying traffic follows conventional Airways route structure;
  - low-level transits of traffic operating under Instrument Flight Rules, and Arrivals to proximate aerodromes, are radar-vectored though Approach airspace, whilst avoiding the Point Merge structure;
- the required aircraft-arrival rate is derived in Approach airspace and fed upstream to adjacent En-route / Terminal airspace sectors as "metering" requirements based on runway capacity and the limited ability of Approach airspace to absorb momentary traffic overloads;
- sequencing and spacing of traffic are established initially in En-route/ Terminal airspace according to the metering requirements, and to an initial estimation of the order of aircraft in the final landing sequence, that would achieve the maximum runway throughput commensurate with the need to maintain adequate spacing between aircraft in the same flow;
- arriving traffic is cleared initially, by ATC[10], to follow standard P-RNAV Terminal airspace arrival routes (STARs) from the top of descent to the IAF;
- prior to reaching its IAF, ATC clears each P-RNAV-capable arrival to continue to follow the remainder of the appropriate P-RNAV route, i.e. down to the FAF but subject to contrary instructions from ATC as necessary;
- aircraft that are not P-RNAV capable (i.e. not equipped or suffering from P-RNAV equipment failure) are vectored along the appropriate Point Merge route, to emulate P-RNAV-capable aircraft, as per the rest of the sequence;
- ATC issues a Direct-to instruction (or a vector, in the case of a non-P-RNAV aircraft) to each aircraft to leave its Sequencing Leg, and head to the Merge Point, once sufficient spacing has been established behind the aircraft immediately preceding it in the overall landing sequence — note that the preceding aircraft might not be on the same Sequencing Leg;
- if the spacing requirements cannot be met before the aircraft reaches the end of the Sequencing Leg[11], the aircraft will, by default, continue on its P-RNAV route (and / or vectors) to the Merge Point — i.e. following the associated Run-off Leg;
- once ATC clears the aircraft to start its descent towards the Merge Point (having ensured safe separation from traffic on the parallel sequencing leg), it will converge vertically (and laterally) with the other aircraft in the flow;
- finally, from the Merge Point to the FAF, there is now only one horizontally-merged flow in which all the aircraft are spaced longitudinally. Along this segment, each

[8] i.e. what we want, and expect, to happen in day-to-day operations (Fowler 2022).

[9] The use of the term "space" here includes *implicitly* the need to also apply the required longitudinal separation minima, wherever other separation *modes* are not available. The way in which the various separation modes are applied throughout the Approach airspace is addressed explicitly in Phase 3 *et seq*.

[10] ATC = Air Traffic Control

[11] Or, for example, and aircraft is unable to respond to a Direct-to instruction

aircraft is cleared to continue its descent until it eventually acquires the final-approach path to the runway.

3.2 Overall Scope Definition (IEC 61508-1 Phase 2)

3.2.1 Aim and Objectives

The aim of this phase is to define the scope of the Hazard and Risk Analysis, for Phase 3.

It seeks to achieve that aim through determining the boundary of the EUC / EUC Control System and its Operational Environment and, within those constraints, specifying the scope of the Hazard and Risk Analysis.

This would be particularly important when assessing the safety of a change to an existing operation and/or system so as to identify, and exclude, the unnecessary safety assessment of those elements that are not affected by the change. It should be noted, however, that we can do this only in general terms herein because of the necessarily generic nature of the operational context for which this example safety assessment is being carried out.

3.2.2 Boundary Constraints

For the purposes of the safety assessment of Point Merge operations, the flow of arrival traffic, which constitutes the EUC, is that which lies between the IAF and the FAF, though it might be necessary to consider the conditions for handover from the adjacent En-route airspace and to final approach and landing. The functioning of the EUC Control System and the properties of the Operational Environment are similarly limited spatially.

3.2.3 Scope of the Hazard and Risk Analysis

Within the above constraints, it is *not* intended to address:

- any hazardous event or situation that does not involve at least one arriving aircraft; nor
- hazards associated with failure onboard an aircraft that leads to a loss of control, other than the effects that such events might have on other aircraft in the vicinity.

3.3 Hazard and Risk Analysis (IEC 61508-1 Phase 3)

3.3.1 Aim

The aim of this phase is to determine, and characterise, all the hazards and risks associated with the EUC[12], in the stated Environment, and within the scope already identified in Phase 2.

Note: it is acknowledged that these EUC hazards (and some of the detail that follows, up to and including Sub-section 3.4.3 below), which are not specific to Point Merge operations, might have already been identified and documented adequately in, say, a safety

[12] Strictly speaking, IEC 61508 includes "EUC Control System Hazards" here as well. We have taken the view that, for ATM, failures with the EUC Control System are among the *causes* of EUC hazards.

case for the airspace concerned. For the purposes of this paper, however, we do not assume this to be the case.

3.3.2 EUC Hazard Identification

The objective here is to determine the hazards relating to the EUC, within the scope defined in Sub-section 3.2 above.

From the IEC 61508 definition of a hazard, which can be paraphrased as "*a potential **source** of death, physical injury or damage to the health of people or damage to property or the environment*" (Fowler 2022), it follows that we must first identify the types of harmful **outcome,** i.e. accident, that fall within ATM's general sphere of responsibility and specifically within the above scope of Point Merge operations.

Table 1 shows accident types relevant to ATM, in Approach airspace, and has been adapted from ICAO (2011)[13] and, in each case, involves death or serious injury to one or more of those on board.

Table 1 ~ Accident Types Relevant to ATM in Approach Airspace

Accident Type	Description
Mid-air collision (MAC)	All collisions between aircraft (or between an aircraft and an unmanned aerial vehicle or missile), while both are airborne
Controlled Flight into Terrain (CFIT)	Inflight collision with terrain, water, or obstacle without loss of control
Uncontrolled Flight into Terrain (UFIT)	Inflight collision with terrain, water, or obstacle following loss of control, *except* where such loss is caused by failure(s) internal to the aircraft
Abrupt, Violent Manoeuvre (AVM)	Sudden, large, intentional or unintentional departure from the intended flightpath and/or attitude, *except* where such departure is caused by failure(s) internal to the aircraft

The EUC hazards derived from the above, and in relation to what are seen to be credible accident outcomes, are shown in Table **2**. The hazards are (by definition) those that are inherent in aviation, in the stated Operational Environment. It is crucial to note that these hazards apply directly to the EUC (the flow of arrivals through Approach airspace) and exist *before* any form of EUC-hazard mitigation has been applied (Fowler 2022).

The numbers in parentheses in Table **2** refer to the notes that follow the table.

Table 2 ~ EUC Hazards and Precursor States

ID	EUC Hazard Title (1)	Immediate Precursor State (2)	Related Accident(s)
Hp#1	Conflicts between pairs of aircraft 4-D flight trajectories	The trajectories concerned intersect, at the approximately same altitude, and the two aircraft would arrive at the crossing point at approximately the same time	MAC or AVM (3)

[13] ICAO (2011) Categories are intended for use in *a posteriori* categorisation of actual occurrences, rather than *a priori* safety assessment — hence the need for some adaptation

ID	EUC Hazard Title (1)	Immediate Precursor State (2)	Related Accident(s)
Hp#2	Aircraft in conflict with terrain or obstacle	Aircraft, under the control of the flight crew (or autopilot), is on a downward trajectory that would bring it in contact with the ground or fixed obstacle, *other* than at a suitable runway touchdown point at an appropriate speed and in an appropriate configuration	CFIT or AVM (3)
Hp#3	Aircraft in conflict with unauthorized areas	Aircraft is on a trajectory that would pass through active restricted airspace without authority	MAC (4)
Hp#4	Aircraft in conflict with severe weather conditions	Aircraft is on a trajectory that would pass through an area of weather conditions that are severe enough for its ability to continue its flight safely to be significantly impaired	AVM or UFIT (5)
Hp#5	Aircraft in conflict with wake turbulence	Aircraft is on a trajectory that would put it in an area of wake turbulence that is severe enough for its ability to continue its flight safely to be significantly impaired	AVM or UFIT (5)

Notes:

1. "Conflict" is used here in its broadest sense – see column 3.
2. IEC 61508 requires that the sequence of events be described for each EUC hazard, but it would be impracticable for ATM, at this stage in the process, because of the number of causal factors involved. What we can usefully do *here* is to describe the immediate precursor to each hazardous event, and leave it to the modelling approach described in Sub-section 3.4.2 below, which does capture how such states are arrived at in the first place, and thus satisfy this IEC 61508 requirement.
3. AVM here is the result of *onboard* actions to avoid an imminent collision
4. Incudes collision with another airborne vehicle and from being hit by some form of munitions.
5. AVM would be the more likely outcome except when the aircraft is closer to the ground and timely recovery from the departure is more difficult.

What we have not said thus far is anything about the probability that each EUC hazardous event would lead to the related accident except, that the probability would, by definition, be finite. That is addressed next, in Sub-section 3.3.3.

3.3.3 EUC Risks

Severity of a hazard could, in general be deduced from the probability that the hazard would lead to the associated accident(s)[14], and the seriousness of the accident in term of the number of fatalities and/or degree and extent of serious injury involved; in ATM, however, the latter has traditionally *not* been considered in *a priori* safety assessments.

In theory, we could then determine either:

[14] Otherwise known as the probabilistic "distance" to the accident

- the EUC risks: i.e. by *estimating* the frequency of occurrence of each EUC hazard and combining it with an assessment of the hazard's severity; or
- the tolerable frequency of occurrence for each hazard: i.e. by setting a *target* tolerable level of EUC risk for each hazard and dividing it by the assessed hazard severity.

Fowler (2022) discussed the potential problems of identifying EUC risk, and Sub-section 3.4 below explains why its determination is actually not necessary under IEC 61508, though it is clear that a method of determining hazard severity is needed in *either* case. Unfortunately, in ATM, predicting the outcome of any hazard is not that simple because:

- as shown in Table 2, each EUC hazard has more than one potential, credible accident outcome;
- any given probability of such an outcome would vary according to, *inter alia*, phase of flight, traffic patterns and density;
- the probability and harmful effects would vary between accident types, e.g. between MAC and AVM, notwithstanding the fact that, traditionally, most ATM harmful events are treated as being of the same severity, irrespective of the number of people affected.

Concerns about hazard-severity / risk-classification schemes, in general, are not new; indeed, as long ago as 2006, the then EUROCONTROL Safety Case Development Manual (EUROCONTROL 2018), expressed concerns about the potential misuse of such schemes unless the user understands:

- at what level in the system hierarchy the values are intended to be applied;
- where the probability/frequency values used in the scheme came from and whether they are (still) valid;
- to what operational environment the values apply, eg type of airspace, traffic patterns, traffic density, spatial dimension, phase of flight, etc;
- how the aggregate risk, as specified in ESARR 4[15] for example, can be deduced from analysis of individual hazards, in restricted segments of the total system.

With all of the above issues in mind, Sub-section 3.4 below introduces a more rigorous approach to hazard and risk assessment, which has been developed by the EUROCONTROL Innovation Hub (EIH) for the Single European Sky ATM Research (SESAR) programme (SESAR 2021). It is based on a set of Accident Incident Models (AIMs), one per accident type, from each of which an RCS can be derived. More information on AIMs is provided in SESAR (2018a) and SESAR (2018b) but, essentially, they model the contributions that the ATM functional system makes to aviation safety, both when working as specified, and in the event of failure. The RCSs derived from the AIMs have four key advantages over the more traditional schemes referred to above:

- they are based on real, historical accident and incident data;
- they more accurately capture the progression of a hazardous event through to an accident;
- they provide safety criteria at many levels in the ATM functional-system hierarchy and for specific phases of flight;
- they provide safety criteria that take account of future changes to the ATM functional system and/or operational environment.

[15] ESARR 4 was the EUROCONTROL Safety Regulatory Requirement "Risk Assessment and Mitigation in ATM", which has since been overtaken by Single European Sky legislation.

3.4 Overall Safety Requirements (IEC 61508-1 Phase 4)

3.4.1 Aim

The aim of this phase is to produce a specification of the Overall Safety Requirements for each Overall Safety Function in order to achieve the required level of functional safety. These requirements cover both functional-safety and safety-integrity properties.

3.4.2 Introduction

According to IEC 61508, an Overall Safety Function is the highest-level abstraction of the "*Means of achieving, or maintaining, a safe state for the EUC, in respect of a* specific *hazardous event*", and therein lies a problem — the relationships between accidents and hazards (as explained above) is "many-to many" and so is the relationship between EUC hazards and the safety functions that are intended to mitigate them.

This can be illustrated by expressing the three layers of ATM, described in the ICAO Global ATM Concept (ICAO 2005), in the form of a generic Barrier Model[16], as shown in Figure 2 (Fowler et al 2009).

The inputs to the model are the relevant EUC hazards and the barriers, acting in rough sequence from left to right, effectively "filter out" a proportion of the EUC hazards. The final barrier reflects the point that, even when all three layers of ATM have been unable to remove a hazard, there is still a relatively high probability that an actual accident will not result, as indicated by the Providence barrier. This probability depends on a number of factors, including the type of the resulting accident, the volume of the available airspace, the density of traffic therein, and the geometry of the encounter.

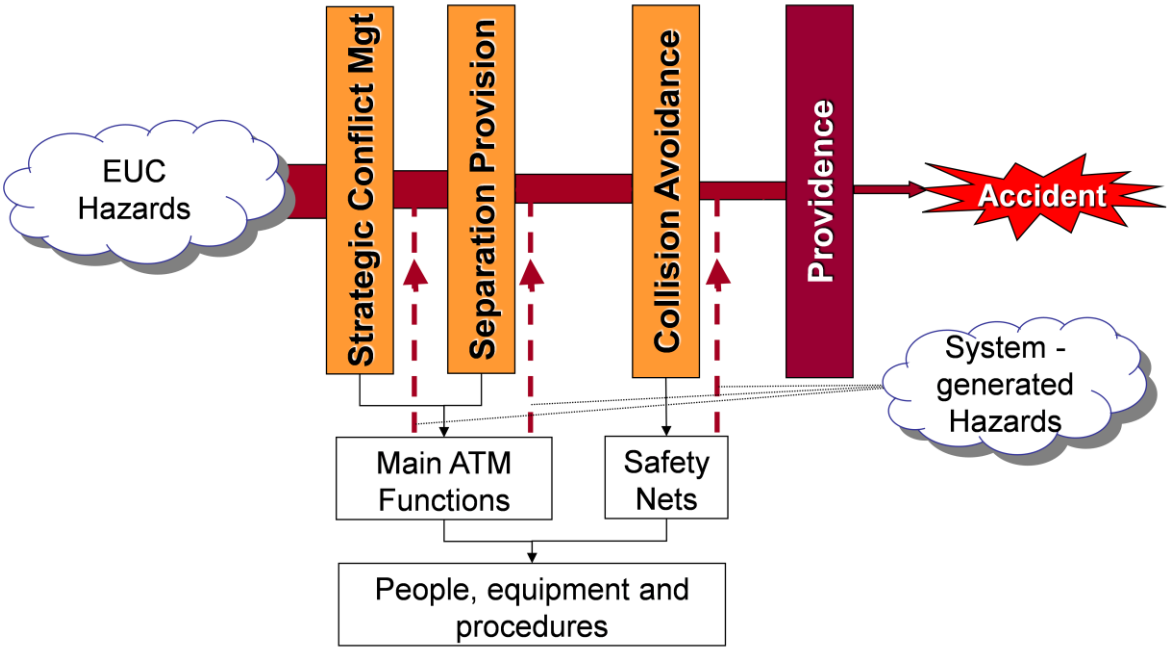


Figure 2 ~ ATM Barrier Model

[16] Derived from James Reason's "Swiss Cheese" model (Reason 2000)

The main three barriers are provided by the primary ATM safety functions and ground-based / airborne safety nets, implemented in the elements of the end-to-end ATM system. Of course, these elements can fail to operate, effectively reducing the probability of success of the barrier, or operate incorrectly, giving rise to new, *system-generated* hazards.

Fowler (2022) presented a simple fault tree model of a generic safety function and showed how its safety properties govern its ability to prevent, i.e. to act as single a barrier to, the progression of an EUC hazard through to an accident. That idea, based on a low-demand situation, is extended, in Figure 3 to represent the multi- barrier model of Figure 2.

Apart from its slightly unconventional layout, this model has one very important feature that distinguishes it from most other Fault Trees — i.e. it has an external input (EUC hazards)[17], which enables the computation of the risk of an accident (R_A) from:

- the EUC hazards (those hazards inherent in aviation) and their frequencies (F_U);
- the net probability of success ($P_S n$) of each barrier in mitigating those risks, taking account of its functionality and performance, and of the probability that it might occasionally fail to operate at all; and
- the frequency ($F_F n$) with which corrupt-operation failure of each of the main barrier introduces new, system-generated hazards / risks.

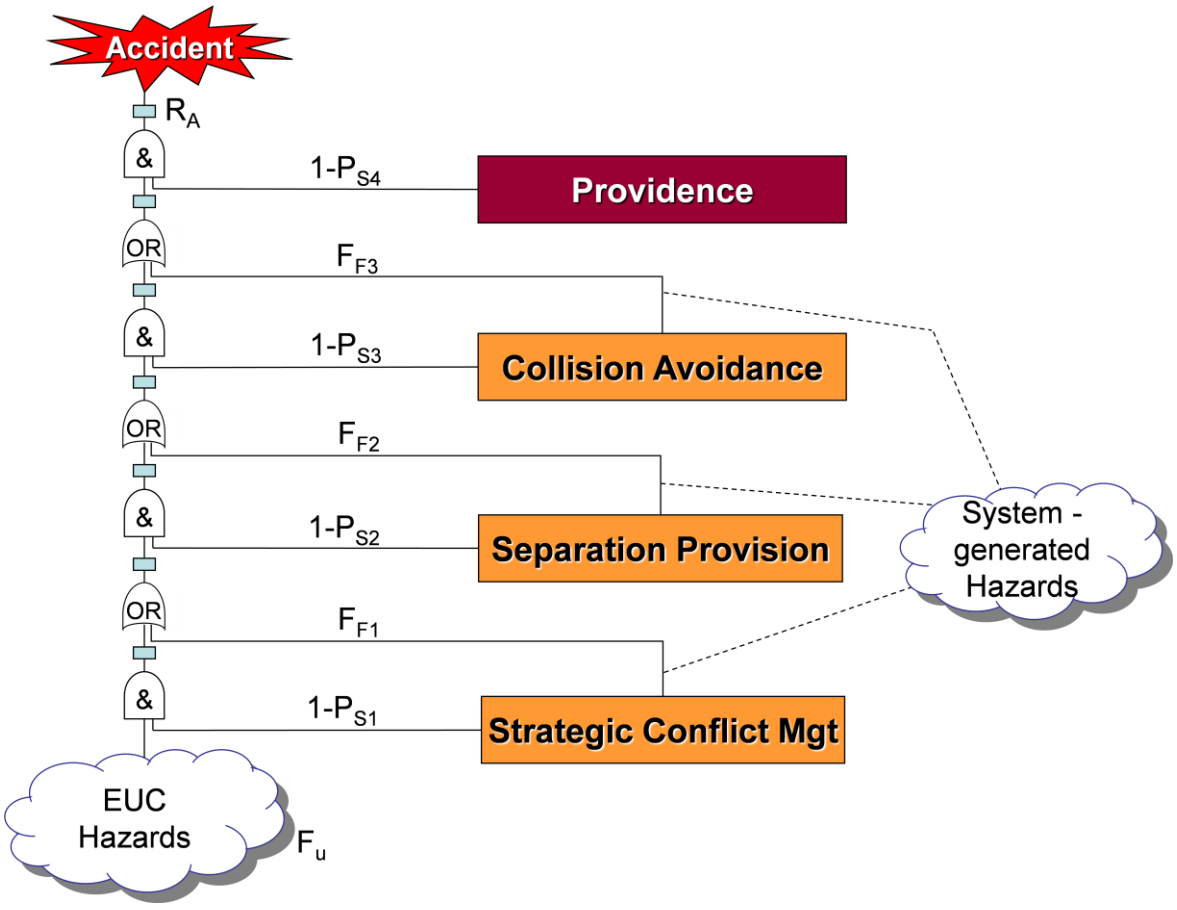


Figure 3 ~ Fault Tree Version of the ATM Barrier Model

[17] Without this input, a Fault Tree could model only *failures internal* to the system on which the Fault Tree is based – i.e. it could model only *negative* effects on safety

Alternatively, of course, if we make the top-level risk our target (R_T) then, given F_P and access to historical accident and incident data, we can make informed judgements about what $P_S n$ and frequency $F_F n$ are required to be in order to satisfy R_T.

Thus the model captures the net positive, as well as the negative, contributions of ATM to aviation safety, and it is this form of risk model on which the SESAR Accident Incident (AIM) models (SESAR 2018a) are based.

Of course, the model, as presented here, is purely illustrative and very high-level. In reality, each AIM model is very much more comprehensive, and actually represents the Barrier model as an Event Tree which integrates the Fault Trees dedicated to each Barrier.

In seeking to overcome many of the shortcomings of traditional hazard-severity / risk-classification schemes, discussed in Sub-section 3.3.3 above, the SESAR approach:

- has, at a detailed level, separate models for each phase of flight and accident type;
- uses real accident and incident data to populate the model with the required probability and frequency values; and
- is capable of modelling the interdependencies between barriers, including lower-level common-cause and common-mode failures, that are implied in Figure 2.

The remainder of this sub-section follows the above principles embedded in the AIM.

3.4.3 Overall Safety Function Identification

The objective here is to identify a set of Overall Safety Functions, based on the EUC hazardous events derived from the hazard and risk analysis of Phase 3. Notwithstanding the minor problem that the IEC 61508 view, of a one-to-one relationship between EUC hazards and Overall Safety Functions, does not work for ATM, the three ATM barriers (or "layers" (ICAO 2005)) fit the role of Overall Safety Functions quite nicely, and are shown in Table **3**.

Table 3 ~ Overall Safety Functions

ID	Overall Safety Function Title	Related EUC Hazards
OSF#1	Strategic Conflict Management (SCM)	Hp#1, Hp#2, Hp#3, Hp#4, Hp#5
OSF#2	Separation Provision (SP)	Hp#1, Hp#2, Hp#3, Hp#4, Hp#5
OSF#3	Collision Avoidance (CA)	Hp#1, Hp#2

3.4.4 Overall Safety Function Required Functional Properties

This step involves the determination of the required functional properties of each of the above Overall Safety Functions. The resulting Overall Safety Requirements (OSRs) are based on the *reference* operational scenario described in Sub-section 3.1.4 above and cover those items that are necessary and sufficient to ensure the safety of Point Merge operations.

In order to avoid, and / or mitigate the consequences of, the hazards shown in Table 1, the functional properties shown in Table 4 are required of the respective Overall Safety Functions. It should be noted that these requirements are objective based — i.e. they express what the OSF have to achieve rather than what they have to do.

Table 4 ~ Overall Functional Safety Requirements for Normal Operations

Reqt. ID	Requirement Description	Related EUC Hazard
OSF#1	**Strategic Conflict Management**	
OSR1.1	Arrival rates into Point Merge airspace shall not exceed the capacity of the P-RNAV routes or runway	Hp#1, Hp#5
OSR1.2	Crossing traffic and departures shall be segregated strategically from the Point Merge structure	Hp#1
OSR1.3	The Point Merge structure shall be segregated strategically from all restricted airspace	Hp#3
OSF#2	**Separation Provision**	
OSR2.1	All aircraft in Approach airspace shall be separated from each other, by either: the greater of the radar-separation minima and the wake-turbulence minima, horizontally; or by 1000ft vertically	Hp#1, Hp#5
OSR2.2	At all points along each route, from IAF to FAF, aircraft shall remain above the altitude of all close terrain/obstacles and/or be adequately separated laterally from such terrain/obstacles	Hp#2
OSR2.3	Point Merge operations shall cease in the event of severe weather posing a threat to the safety of arriving traffic flow in the Point Merge structure	Hp#4
OSF#3	**Collision Avoidance**	
OSR3.1	When the associated *separation mode* has been compromised, *mid-air* collision-avoidance action shall be taken in accordance with current operational procedures	Hp#1
OSR3.2	When the associated *separation mode* has been compromised, *terrain/obstacle* collision-avoidance action shall be taken in accordance with current operational procedures	Hp#2

3.4.5 Determine the Safety Integrity Requirements for each Overall Safety Function

This step involves the determination of the SIRs required of each of the above Overall Safety Functions, to achieve a tolerable level of risk overall. Two points are stressed in Fowler (2022):

- IEC 61508 states that the SIRs, at this level, must be specified in terms of either:
  - the risk reduction required to achieve the tolerable level of risk; or
  - the tolerable [EUC] hazardous event rate to achieve the tolerable level of risk; and
- according to IEC 61508, SIRs at this "overall" level are *not*, despite their name, properties of the OSF to which they relate — they actually specify a *target* amount of EUC risk reduction that the OSF has to meet, and could be seen to correspond to the more appropriately termed *safety criteria* in ATM.

Here, the SESAR AIM approach has two big advantages over IEC 61508 Phase 4, as follows:

- it derives SIRs that *are* properties of the OSFs themselves; and
- those properties accord directly, and fully, with the concept of Safety Integrity as defined in IEC 61508 — viz:

> *"the probability of a … safety-related system satisfactorily performing the specified safety functions under all the stated conditions, within a stated period of time"*

There is not the space in the context of this paper to provide a worked example for Point Merge but, in principle, we can see from Figure 3 above how, given sufficient relevant real-world accident data, a realistic value of EUC hazard rate and a risk tolerability level for, say, a MAC accident, the following three SIRs could be derived for each ATM barrier:

- probability of successful mitigation of the input hazard, in the absence of failure internal to the barrier;
- frequency or probability of failure internal to the barrier[18]; and
- frequency of corrupt operation of the barrier.

3.5 Overall Safety Requirements Allocation (IEC 61508-1 Phase 5)

3.5.1 Aim

The aim of this phase is to allocate to SRS(s) and/or ORRM(s), the functional safety requirements and safety integrity requirements, which were derived for the corresponding overall safety function in Phase 4.

3.5.2 Discussion

IEC 61508 gives prominence to the distinction between SRSs and ORRMs — partly, it would seem because, once identified, the latter measures fall outside the scope of the Standard.

For ATM in general, ORRMs could include non-functional, safety-related items such as airspace /route structure and runway / taxiway layout, for which specific design & development standards exist in most cases. However, given the close interaction between ATC and, say, P-RNAV route structures in the SP barrier for Point Merge, it was decided that there was little additional value in the distinction, in this case[19]. Therefore, Table 5 shows the allocation of the OSFs from Table 4 on to what might be interpreted generically as SRSs[20], within an ATM "system of systems".

Table 5 ~ Allocation of Overall Safety Functions for Point Merge

OSF/OSR ID	**Safety-related System**
OSF#1	**Strategic Conflict Management**
OSR1.1	Demand & Capacity Balancing (DCB)

[18] Depending on whether the barrier operates continuously, i.e. at a high demand rate, or at a low demand rate, respectively.

[19] We considered whether ORS1.2 should be allocated to ORRMs since the segregation of transits / overflights and departures depends on risk-reduction measures which fall mainly outside of the scope of Point Merge. Whereas this would have merit as a way of managing such measures, it would have added non-essential complexity to this paper, which we chose to avoid.

[20] These are based on what ICAO (2005) terms "*ATM operational concept components*".

OSF/OSR ID	Safety-related System
OSR1.1	Departure Synchronisation (DS)
OSR1.1	Arrival Sequencing & Spacing (ASS)
OSR1.1	Airspace Organisation & Management (AOM)
OSR1.2	
OSR1.3	
OSF#2	**Separation Provision**
OSR2.1	ATC Pre-tactical Conflict Management ~ air-to-air (ATC-PTCM-AA)
OSR2.2	ATC Pre-tactical Conflict Management ~ air-to-ground (ATC-PTCM-AG)
OSR2.1 OSR2.3	ATC Tactical Conflict Management ~ air-to-air (ATC-TCM-AA)
OSR2.2	ATC Tactical Conflict Management ~ air-to-ground (ATC-TCM-AG)
OSR2.2	Airborne Tactical Conflict Management ~ air-ground (AB-TCM-AG)
OSF#3	**Collision Avoidance**
OSR3.1	ATC mid-air collision-avoidance (ATC-MACA)
OSR3.2	Airborne mid-air collision-avoidance (AB-MACA)
OSR3.2	ATC terrain collision-avoidance (ATC-TCA)
OSR3.3	Airborne terrain collision-avoidance (AB-TCA)

The ICAO Global ATM Concept (ICAO 2005) uses the term "strategic" to mean "in advance of tactical" whilst recognising that "a continuum exists from the earliest planning of the user activity through to the latest avoidance of the hazard". In respect of the use of P-RNAV routes, with various altitude constraints, to effect separation, it is debatable whether that is strategic or tactical, or lies on the continuum somewhere between the two; we concluded that the latter was the case and coined the term "pre-tactical", within Separation Provision, to capture this in Table **5**.

Furthermore, where pre-tactical separation is provided, by the P-RNAV route structures of Point Merge, we envisage that ATC monitoring of aircraft compliance with the P-RNAV route parameters would be provided within the two (ATC-TCM) barriers, in advance of Collision Avoidance.

3.6 Safety Requirements Specification (IEC 61508-1 Phases 9 and 10)

3.6.1 Aim

In IEC 61508, the respective aims of Phases 9 and 10 is to develop safety requirements for the "SRSs" and "ORRMs" identified in Phase 5, in terms of their Functional Safety Requirements (FSRs) and the SIRs, in order to achieve the required functional safety under all *normal*, *abnormal* and *failure* conditions.

Given that, in the case of Point Merge above, we have viewed the distinction between SRSs and ORRMs as being of limited value, we have thus combined Phases 9 and 10 together in this sub-section.

3.6.2 Overview

It is important to note here that IEC 61508-1 places great emphasis on the need for a description of the workings of the SRS at this level, including:

- a description of all the safety functions, how they work together to achieve the required functional safety and whether they operate in low-demand, high-demand or continuous modes of operation;
- the required performance attributes of each safety function — e.g. timing properties and, for more data-intensive applications than possibly envisaged by IEC 61508, data accuracy, latency, refresh rate, and overload tolerance;
- all interfaces that are necessary to achieve the required functional safety;
- all relevant modes of operation of the EUC;
- response of the SRSs to abnormal conditions that might arise in the EUC or its environment;
- all required modes of behaviour of the SRSs — in particular, its failure behaviour and the required response in the event of such failure (Fowler 2022).

In the particular case of Point Merge operations, there are no new SRSs /safety functions; rather, the operational concept is based on existing Approach airspace functions / infrastructure, most of which are elements of the ATM system, i.e. what IEC 61508 terms the "EUC Control System" (see Sub-section 3.1.4 above), and which must be considered to be SRSs in their own right by virtue of their safety significance in Point Merge operations.

The questions that we need to address at this stage, therefore, are *where and when* those safety functions are deployed for Point Merge and would that be safe. To that end, this sub-section comprises four stages, as follows.

Firstly, the development of FSRs using operational scenarios, covering *normal* operations. This will be done initially at two levels (see Sub-section 3.6.3 below):

1. initially, at a relatively abstract level, without reference to explicit elements within the end-to-end ATM system, and
2. then, the lower level of a "*logical*-architecture" representation of the ATM system (i.e. the "EUC Control System")[21].

The former level is focused on *what* needs to be done and uses narrative scenarios to represent a (basic) form of behavioural model of Point Merge, which captures the initial FSRs, for the operational processes involved in a typical flight through the airspace. The latter, however, focusses on *how* this is achieved by the logical elements of the ATM system[22].

[21] Whereas IEC 61508 does not distinguish between these two levels, the approach described here has been found by the authors to be a useful approach to the safety assessment of a number of ATM applications

[22] As noted in Sub-section 3.7.2 of Fowler (2022), the IEC 61508 objective here is to "*describe, in terms not specific to the equipment, the required safety properties of the SRS(s)*". Both of these levels of requirements expression respect that objective since neither makes any assumptions about the technology involved in the realisation of the requirements.

Secondly, to show that the FSRs specified for the SRSs would be adequate to meet the risk-reduction required of the barriers / SRSs, in the absence of failure (see Sub-section 3.6.4).

Thirdly, to analyse, in a similar manner, scenarios covering *abnormal* events in order to identify any additional FSRs necessary to maintain a tolerable level of safety during such events (see Sub-section 3.6.5 below).

Fourthly, to analyse scenarios relating to potential failures of the ATM system in order to identify SIRs, and any additional FSRs, necessary to maintain a tolerable level of safety during such failure events (see Sub-section 3.6.6 below).

3.6.3 FSRs for Normal Operations

3.6.3.1 Derivation of FSRs for the "Reference" Operational Scenario

In order to derive the initial set of FSRs, the analysis first considers a typical flight through Approach airspace, as a continuum, looking in particular at transitions in the *separation mode* and in the merging of traffic, for the Point Merge structure shown in Figure 1.

For the purpose of analysis, the *subject* aircraft is assumed to be P-RNAV capable and enters the Point Merge structure, in a westerly direction, at IAF1[23]. It is termed the *reference* scenario (designated N0) since it is based on the most likely set of operational and environmental conditions[24].

For each stage in the flight at which something has to be achieved in relation to one or more of the OSRs shown in Table **4** above, the need for an FSR is identified, as shown thus "{FSR#n}" in the text below, and then the corresponding FSRs are detailed (and traced back to the related SRS(s), at Table 10 in Appendix A.

General Conditions: the following conditions apply generally throughout flight in Approach airspace:

- vertical separation at intersections of Point Merge routes with SIDs is provided achieved through aircraft conforming to appropriate published altitude restrictions {FSR#1};
- all other traffic is kept away from the Point Merge structure strategically, or by ATC tactical intervention as and when appropriate {FSR#2};
- the whole Point Merge structure is segregated spatially from Restricted Airspace {FSR#3};
- entire P-RNAV routes (i.e. from IAF to FAF) are designed in accordance with ICAO Doc 8168 Vol II (ICAO 2014) {FSR#4}.

Pre-conditions: the following conditions apply prior to aircraft entering the Point Merge structure at the designated IAF:

- required aircraft-arrival rate is derived in Approach airspace and fed upstream to adjacent En-route / Terminal airspace sectors as "metering" requirements based on runway capacity (arrivals and departures) and the limited ability of Approach airspace to absorb momentary traffic overloads {FSR#5 and FSR#6};

[23] The choice here is entirely arbitrary, and the analysis would apply equally to any P-RNAV-capable aircraft entering at the other IAF.

[24] Other scenarios will cover other *normal* conditions, e.g. the cases of aircraft that are not P-RNAV capable, as well as, later in this sub-section, *abnormal* and *failure* conditions.

- sequencing and spacing of traffic are established initially in En-route/ Terminal sectors according to the metering requirements, and to an initial estimation of the order of aircraft in the final landing sequence, that would achieve the optimum runway throughput commensurate with the need to maintain separation minima/wake turbulence criteria and maintain the required departure flow {FSR#7, FSR#8};
- ATC monitoring of aircraft conformance with all clearances and instructions is carried out throughout each flight, including when aircraft are following the predefined P-RNAV routes that make up most of the Point Merge structure {FSR#9}.

***Flight in Approach Airspace*:** the aircraft proceeds as follows:

- entry into Approach airspace is coordinated with the adjacent upstream sector(s) according to the agreed entry conditions, including the aircraft being stable at the defined altitude prior to Sequencing Leg entry {FSR#10} — this is to reduce the chances of unnecessary ACAS / STCA alerts with opposite-direction aircraft that are approaching the end of the adjacent Sequencing Leg;
- on entry to, and along, the Sequencing Leg (SL1), the aircraft remains in level flight and is vertically separated from each eastbound aircraft on the adjacent, opposite-direction Sequencing Leg (SL2) by all aircraft complying with height restrictions published for the P-RNAV route applicable to its Sequencing Leg {FSR#11};
- spacing from preceding and succeeding aircraft on the same Sequencing Leg is provided tactically by ATC such that the 3 nautical mile longitudinal-separation minimum and wake-vortex criteria are maintained {FSR#12};
- vertical clearance from terrain/obstacles is provided by the minimum altitude specified for each Sequencing Leg's P-RNAV route section {FSR#13};
- once sufficient spacing has been established behind the aircraft immediately preceding it in the overall landing sequence, the subject aircraft is instructed by ATC to leave its Sequencing Leg, on a *Direct-to* towards the Merge Point (MP) {FSR#14} — its position in the final sequence order is thus established;

  Notes:

  1. If the spacing requirements cannot be met before the aircraft reaches the end of the Sequencing Leg, the aircraft will continue on its P-RNAV route to the Merge Point – see scenario N1 below.
  2. The handling of aircraft that are not P-RNAV-capable is discussed in scenario N2 below.

- during the Direct-to section of the flight, the following separation rules apply:
  - in this case, the subject aircraft is on the higher, i.e. inner, Sequencing Leg, and as the aircraft starts to follow the Direct-to, vertical separation from traffic on the *adjacent*, i.e. lower, Sequencing Leg is maintained by ATC instructing the subject aircraft to maintain its altitude until longitudinal separation from the aircraft still on the adjacent Sequencing Leg has been achieved {FSR#15};
  - once the subject aircraft is clear of the adjacent Sequencing Leg *and* longitudinal separation from other aircraft also heading to the MP has been established (see {FSR#15 above}), it can be cleared to descend to the MP;
  - terrain/obstacle clearance is enabled by the minimum altitude of the MP being such that there is no terrain/obstacle that is higher than the MP anywhere in the sector of the circle defined by the MP and its outermost Sequencing Leg {FSR#16};

  - unless instructed otherwise by ATC, the aircraft flight crew is responsible for maintaining safe altitude from the start of descent on the "Direct-to" leg until acquiring the ILS glidepath {FSR#17}.

- finally, from the MP to the FAF, there is now only one horizontally-merged flow; along this segment, the aircraft continues its descent, and eventually acquires the Final Approach path.

Table 10 in Appendix A specifies each of the FSRs identified above.

3.6.3.2 Derivation of Additional FSRs for other Normal Scenarios

Other scenarios describing *normal* operations, are usually variations on scenario N0, two examples of which are as follows.

Firstly, scenario N1 in which a non-P-RNAV aircraft requires to join the landing sequence. In this case, all the ATC-related FSRs for operational scenario N0 apply, with the following addition:

> *FSR#18 All non-P-RNAV aircraft shall be vectored along the Point Merge routes to emulate P-RNAV aircraft, whilst being provided with obstacle / terrain clearance by ATC.*

Secondly, scenario N2 in which an aircraft reaches the end of its Sequencing Leg before it had been possible to find a slot for it in the landing sequence[25]. The FSRs for scenario N0 apply, with the following addition:

> *FSR#19 Each Point Merge route shall include a Sequencing Leg Run-off procedure (P-RNAV segments and / or ATC manual procedure) to ensure that an aircraft will automatically continue to the Merge Point, on a predefined vertical profile, in the event that no Direct-to instruction is received before reaching the end of the Sequencing Leg.*

Other *normal* scenarios might include the following:

- planned transitions into, and out of, Point Merge operations;
- planned change of runway (same direction);
- planned change of runway direction;
- onset of strong winds.

In analysing such scenarios, any additional FSRs would need to be identified and specified.

3.6.3.3 Logical FSRs for Normal Operations

Thus far, we have specified, at a conceptual level, *individual* FSRs for the management of conflicts and avoidance of collision for Point Merge operations under normal and abnormal conditions.

What needs to be done next is to describe *how* these FSRs map on to the ATM system and how the system itself needs to behave in order to achieve the desired result.

It was decided to carry out such analyses (and the subsequent failure analysis) at the level of the system *logical* design, which describes the main human roles / tasks and machine-based functions of the system but in a manner that is entirely independent of the eventual *physical* implementation of that design — to this extent it conforms to the associated provisions of Phase 9 of the IEC 61508.

[25] Could also be a mitigation of an ATM system failure – e.g. lost comms

A typical set of elements of the Logical Model that would be appropriate to Point Merge is shown in Table 6. The list is not exhaustive in that elements not specifically affected by Point Merge, e.g. are required to simply perform their normal functions, are excluded at this stage. The type of element is also shown, and is designated as MF (machine function), HR (human role) or a set of Data.

Table 6 ~ Logical Elements

ID	Description	Type
ACAS	Airborne Collision Avoidance System	MF
AD	Airspace Design	Data
AP/FD	Autopilot/Flight Director	MF
AMAN	Arrival Manager (tools)	MF
EXEC	Executive (Tactical) Controller	HR
FCRW	Flight Crew	HR
FDP	Flight Data Processing	MF
FMS	Flight Management System	MF
MSAW	Minimum Safe Altitude Warning	MF
PLNR	Planner Controller	HR
P-RNAV	P-RNAV Procedure	Data
STCA	Short-term Conflict Alert	MF
TAWS	Terrain Awareness Warning System	MF

Examples of how FSRs then map on to the relevant Logical Elements is shown in Table 7.

Table 7 ~ Example Mapping of FSRs to Logical Model

ID	Safety Requirement	Maps to:
FSR#3	Point Merge structures shall be segregated from restricted airspace	AD
FSR#7	Sequencing and spacing of traffic shall be established initially in adjacent En-route/ Terminal airspace sectors according to the metering requirements, and to an initial estimation of the order of aircraft in the final landing sequence, that would achieve the optimum runway throughput commensurate with the need to maintain separation minima/wake turbulence criteria and maintain the required departure flow	AMAN, PLNR
FSR#10	Vertical separation, of at least 1,000 ft, between adjacent Sequencing Legs shall be provided, by appropriate published altitude restrictions along the entire length of the Sequencing Legs	P-RNAV
FSR#11	Aircraft on the same Sequencing Leg shall be separated longitudinally, by ATC, by a 3nautical mile radar -separation minimum, or the appropriate wake-turbulence separation minimum, whichever is the greater	EXEC

ID	Safety Requirement	Maps to:
FSR#16	Except where instructed otherwise by ATC, the aircraft shall assume responsibility for maintaining safe altitude from the start of descent on the "Direct-to" leg until acquiring the ILS glidepath	FCRW, TAWS

The mapping process would then be completed by deriving appropriate (lower-level, Logical) FSRs, for each Logical Model element, in response to the higher-level FSRs assigned to it.[26]

Given then a complete Logical Model, a technique that can be used very effectively in modelling the *behaviour* of transactional system such as ATM is some form of Use Case analysis. A suitable notation for this purpose would be a sequence diagram (SD), straightforward guidance on which can be found at Sparx Systems (2022).

For many ATM applications, SDs have proved to be a very useful design-analysis technique in that they:

- provide a means of cross-checking the completeness, correctness and consistency of the lower-level FSRs which are mapped on to the SD;
- tell us more about the intended operation of the ATM system than could the FSRs individually;
- are an effective way of highlighting transitions between, inter alia, separation modes at various points in the flight;
- provide very useful, scenario-based information for real-time operational simulations and the development of operator training material; and
- provide, for the subsequent failure analysis, a valuable insight into sources of potential system failures.

Furthermore, since it also defines the required behaviour of the ATC system), it is designated as a functional safety requirement in its own right.

In a full safety assessment, other normal scenarios might also need to be similarly analysed, including scenarios N1 and N2.

3.6.4 Adequacy of the Functional Safety Requirements

In the barrier-model approach outlined in Sub-section 3.4 above, it was noted that it is the functional properties of a barrier that determines the probability of successful mitigation of the input hazard, in the absence of failure internal to the barrier. It was also noted that, in case of the SESAR AIMs, the required probability of success, and the maximum rates of occurrence of failure and corrupt operation, of each barrier is, as far possible, based on actual historic data.

In practice, establishing a *direct* relationship between the required functional properties (FSRs) of a barrier, and the required probability of its successful mitigation of input hazards, can be far from straightforward, depending on the circumstances. This is illustrated by considering two general cases, as follows:

- when ATM operations, albeit conducted in a different way from previous operations in the subject environment, remain fully compliant with established ICAO Standards and Recommended Practices (SARPs);

[26] Not done herein in order to avoid unnecessary detail…

- when ATM operations deviate from those SARPs in some way.

The first case applies to Point Merge for which, in the various normal and abnormal scenarios, the FSRs are specified so as to ensure compliance with, for example, ICAO separation minima throughout each step/portion of arrival flight in Approach airspace.

The (qualitative) safety argument would then be relative — i.e. that, given previous (ICAO complaint) arrival operations in the airspace were deemed to be tolerably safe, Point Merge operations would themselves be safe in the absence of failure. Such an argument should be reinforced by demonstrating the viability of the FSRs, as a whole, through real-time simulations, from an ATC and/or aircraft perspective, as appropriate.

The second case would apply, for example, whenever separation was applied below the associated ICAO minima and would require a more direct approach. In the specific case of reduced vertical separation minima (RVSM) in European En-route airspace, data from real-time monitoring of aircraft height-keeping accuracy was used to compute (in effect) the probability of successful vertical separation between two aircraft separated nominally by 1,000 ft, in the absence of failure. Equivalent approaches have been applied in the safety assessment of reduced wake-turbulence separation, using real-time, LIDAR measurement of wave-vortex phenomena.

3.6.5 Point Merge Operations under Abnormal Environmental Conditions

The following are examples of what were identified as abnormal conditions relevant to Point Merge operations:

- Aircraft Emergency — medical, technical, etc.
- Aircraft experiences ACAS Resolution Advisory (RA)
- Unplanned runway change, e.g. unplanned change of direction
- Unforeseen runway closure, e.g. blocked runway
- Missed Approach
- Very strong winds, e.g. > 30 knots

Table 8 contains two examples and shows, for each abnormal condition concerned, the immediate operational effect, the possible mitigations of the safety consequence of that effect and the related FSR(s).

Table 8 ~ Example Mitigation for Abnormal Operations

Ref.	Abnormal Event	Operational Effect	Mitigation of Effects	FSR
1	Aircraft Emergency	Aircraft in the landing sequence needs priority over preceding aircraft	Move the affected aircraft up the sequence order, if necessary, creating a gap by vectoring a preceding aircraft out of the sequence	FSR#20
2	Aircraft experiences an ACAS RA	Aircraft in the landing sequence needs to follow the RA	If necessary to maintain separation, and once the RA has been resolved, remove the aircraft from the landing sequence	FSR#21

It is also possible to quantify the residual risk associated with each of the abnormal events; however, this is beyond the scope of this article. What is more important at this stage is that the above analysis identified the abnormal conditions that might be encountered in the Point Merge Operational Environment and specified potential mitigations of the consequences thereof.

3.6.6 Point Merge Operations under Internal-failure Conditions

Finally, for Phases 9 and 10, is the analysis of potential failures internal to the overall Point Merge ATM system.

IEC 61508 suggests a Risk Classification Scheme (RCS) as a possible method for deriving SIRs at this level but, having already cast doubt on the validity of RCSs used traditionally in ATM, we will now outline a scheme based on that used on the SESAR Programme, which resolves most, if not all, of those doubts. The approach has one RCS dedicated to each type of accident and a hazard-severity scheme based on the success or failure of the individual stages of the Barrier Model outlined above.

The illustration shown in Table **9** is for the MAC accident type, in Terminal airspace, for which the tolerable level of risk of an accident is 1E-9 per flight hour.

Table 9 ~ Illustrative Risk Classification Scheme

Severity Class	**Hazardous Situation**	**Operational Effect**	**MTFoO**[27]
MAC-SC1	An aircraft comes into physical contact with another aircraft	Accident — Mid-air collision	1E-9
MAC-SC2a	An imminent collision was not mitigated by an airborne collision avoidance but for which geometry has prevented physical contact	Near Mid-air Collision	1E-6
MAC-SC2b	Airborne collision avoidance prevents near collision	Imminent Collision	1E-5
MAC-SC3	An imminent collision was prevented by ATC Collision prevention	Imminent Infringement	1E-4
MAC-SC4a	An imminent separation infringement coming from a crew/aircraft-induced conflict was prevented by tactical conflict management	Tactical Conflict (crew/aircraft induced)	1E-3
MAC-SC4b	An imminent separation infringement coming from a planned conflict was prevented by tactical conflict management	Tactical Conflict (planned)	1E-2

The tolerable level of risk for each for each hazardous situation (except for the ultimate occurrence, of an accident) is expressed in terms of the Maximum Tolerable Frequency of occurrence of the Operational Effect (MTFoO), the values for which were obtained from the corresponding AIM model. In allocating the risk budget to each hazard in a given

[27] MTFoO is the Maximum Tolerable Frequency of Occurrence per flight hour.

severity class, a pre-defined number of operational hazards was assumed for each severity class, e.g. a factor of 10 for each operational effect.

The use of the scheme then follows standard ATM safety practices, in deriving SIRs for lower-level elements of the ATM system — in this case, at the *logical* level of system design as introduced in Sub-section 3.6.2 above.

In assessing such outcomes of system failures, account must be taken of:

- any mitigations of effect that might be available and FSRs specified for any new mitigating measures. For example, "*FSR#22, Aircraft shall report loss of P-RNAV capability to ATC immediately*" could be a mitigation against an onboard failure affecting P-RNAV performance;
- the existence of possible common-cause failures that could undermine the (thus far) assumed independence of barriers, OSFs, SRSs or safety functions.

Finally, in assessing the effect of Point Merge operations on overall risk, from a system-failure perspective, this could be done one of two ways:

- *absolutely*, by considering *every* failure and calculating its risk contribution from the consequences and expected failure rate; or
- *relatively*, by comparing the risk between Point Merge and existing operations but only for any new system failures or existing failures for which the consequences had changed.

The latter approach would usually be preferred whenever the risk of *existing* operations had already been shown to be tolerable but, in either case, the overriding need is to comply with, *inter alia*, the following requirement of IEC 61508, Sub-section 7.5.2.5:

> *"If, in assessing the EUC Risk, the average frequency of dangerous failures of a single EUC control system function is claimed as being lower than 1e-5 dangerous failures per hour then the EUC Control System shall [itself also] be considered to be a safety-related control system [and] subject to the requirements of this Standard".*

4 Conclusions

This paper is the second in a series of three parts, which sets out to show what functional safety assessments for transport applications might look like if they followed the safety principles and lifecycle steps set out in IEC 61508-1 and IEC 61508-4. The first part (Fowler 2022) gave an overview of those principles and lifecycle steps, together with some transport-orientated guidance, illuminated by applying them to a simple, hypothetical example of the assessment of a proposed means of enabling pedestrians to cross a busy road safely.

The scope of that exercise was limited to the seven IEC 61508 lifecycle phases relating to the specification of safety requirements. This was because most of the key principles underpinning IEC 61508 — i.e. the universal principles set out in Parts 1 and 4 of the Standard, which govern the determination of the required risk-reducing properties of safety-related systems — take effect during these earlier phases, whereas the subsequent realisation and operating phases are less specific to the Standard.

The application, herein, of those principles to the ATM example of Point Merge operations has found that applying the subject IEC 61508 lifecycle phases directly to a typical project in the ATM sector was reasonably straightforward, and the results fitted well with the

forward-looking IACO Global ATM Concept and SESAR approach to ATM safety assessment. In particular:

- treating the flow of traffic through the airspace as being the "EUC" worked very well and rightly focussed the initial stages of the safety assessment where it should always be, i.e. on the hazards that exist in the airspace, which are inherent in aviation and which the ATM system has to be shown to be able to mitigate sufficiently, in order to achieve a tolerable level of risk;
- treating the overall ATM system as the "EUC Control System" followed naturally from our interpretation of the EUC and also worked well; it provided clarity on what was, and what was not, new in relation to Point Merge, and also between safety and non-safety issues;
- above all, the early IEC 61508 lifecycle steps, followed herein, demanded that the safety functionality and performance of the ATM system in the Point Merge context be specified so as to reduce EUC risk to better than a tolerable level, when operating correctly, *before* considering what happens to EUC risk in the event of system failure.

Hence, following the principles of the specific phases of IEC 61508 provides a considerable overall benefit of ensuring a better balance in the approach to functional-safety assessment than might otherwise be the case — for which see Fowler (2015).

Acknowledgments

The authors wish to acknowledge the considerable help, support and understanding of many colleagues from EUROCONTROL and beyond, over many years, without which this paper would not have come to fruition.

The copyright holder of the quotations from published standards used for illustration in this paper is the International Electrotechnical Commission, Geneva.

References

EUROCONTROL. (2018). *Safety Assessment Methodology — Safety Case Development Manual*. EUROCONTROL, The European Organisation for the Safety of Air Navigation. Available at https://www.eurocontrol.int/tool/safety-assessment-methodology, Accessed 8th September 2022.

EUROCONTROL. (2021). *Point Merge — Improving and harmonising arrival operations*. EUROCONTROL, The European Organisation for the Safety of Air Navigation. Available at https://www.eurocontrol.int/concept/point-merge, Accessed 19th November 2022.

Fowler D, Perrin E and Pierce R. (2009). *2020 Foresight — A systems-engineering approach to assessing the safety of the SESAR Operational Concept*. Paper 446 in Proceedings of the Eighth USA/Europe Air Traffic Management Research and Development Seminar (ATM 2009), Napa, California, USA. Available at https://drive.google.com/file/d/1Tq7Qs7Reuuk9Y_4dtoV-DJNkUVPzB51t/view, Accessed 19th November 2022.

Fowler D. (2015). *Functional Safety by Design — Magic or Logic?* In Proceedings of the 23rd Safety-Critical Systems Symposium, Bristol, UK. Available at https://scsc.uk/r129/7:1. Accessed 19th June 2022.

Fowler D. (2022). *IEC 61508 Viewpoint on System Safety in the Transport Sector: Part 1 — An Overview of IEC 61508*, in Safety-Critical Systems eJournal, Vol. 1, Iss. 2. Available at https://scsc.uk/r176.3:1, Accessed 29th December 2022.

ICAO. (2005). *Global ATM Operational Concept*. The International Civil Aviation Organisation. ICAO Doc 9854, 1st edition, 2005. Available at https://www.icao.int/Meetings/anconf12/Document%20Archive/9854_cons_en[1].pdf, Accessed 19th November 2022.

ICAO. (2011). *Aviation Occurrence Categories — Definitions and Usage Notes*. ICAO, The International Civil Aviation Organization. Version 4.2, Oct 2011. Available at https://www.icao.int/APAC/Meetings/2012_APRAST/OccurrenceCategoryDefinitions.pdf, Accessed 29th December 2022.

ICAO. (2014). *Procedures for Air Navigation (Operations) — Vol II, Construction of Visual and Instrument Flight Procedures*. ICAO, The International Civil Aviation Organization. Doc 8168-2, Edition 6, 2014. Available from https://skybrary.aero/sites/default/files/bookshelf/5801.pdf, Accessed 7th September 2022.

IEC. (2010). *Functional Safety of Electrical/electronic/programmable electronic Safety-related Systems*. IEC 61508, Ed.2. International Electrotechnical Commission. Geneva.

Reason J. (2000). *Human Error: Models and Management*, British Medical Journal, BMJ 2000;320:768. Available at http://www.bmj.com/cgi/content/full/320/7237/768, Accessed 21st September 2022.

SESAR. (2018a). *Safety Reference Material*. SESAR Joint Undertaking. Edition 00.04.01, 14 Dec 2018. Available at https://www.sesarju.eu/sites/default/files/documents/transversal/SESAR2020%20Safety%20Reference%20Material%20Ed%2000_04_01_1%20(1_0).pdf, Accessed 19th November 2022.

SESAR. (2018b). *Guidance to Apply SESAR Safety Reference Material*. SESAR Joint Undertaking. Edition 00.03.01, 14 Dec 2018. Available at https://www.sesarju.eu/sites/default/files/documents/transversal/SESAR%202020%20-%20Guidance%20to%20Apply%20the%20SESAR2020%20Safety%20Reference%20Material.pdf, Accessed 19th November 2022.

SESAR. (2021). *Delivering the Digital European Sky*. SESAR Joint Undertaking. Available at https://www.sesarju.eu/sites/default/files/documents/reports/SESAR%203%20launch%20brochure.pdf, Accessed 19th November 2022.

Sparx Systems. (2022). *UML 2 Tutorial – Sequence Diagram*. Sparx Systems Pty Ltd. Available at https://sparxsystems.com/resources/tutorials/uml2/sequence-diagram.html, Accessed 29th December 2022.

Appendix A. Point Merge Functional Safety Requirements

The following table lists all Point Merge FSRs that have been derived from the analysis at 3.6 above and shows traceability back to the SRSs in Table 5.

Table 10~ Consolidated List of FSRs for SRSs

ID	Safety Requirement	Traceability
FSR#1	Vertical separation at intersections of Point Merge routes with SIDs shall be provided by aircraft conformance to appropriate published altitude restrictions	SCM-AOM
FSR#2	Vertical separation at intersections of Point Merge routes with pre-defined routes for transit flights, overflights and other arrivals shall be provided strategically by aircraft conformance to appropriate published altitude restrictions	SCM-AOM
FSR#3	Point Merge structures shall be segregated from restricted airspace	SCM-AOM
FSR#4	All P-RNAV routes (i.e. from IAF to FAF) shall be designed in accordance with ICAO PANS-OPS, (Doc 8168) Vol II	SCM-AOM
FSR#5	The required aircraft-arrival rate shall be derived in Approach airspace and fed upstream to adjacent En-route / Terminal airspace sectors as “metering” requirements based on runway capacity (arrivals and departures) and the limited ability of Approach airspace to absorb momentary traffic overloads	SCM-DCB
FSR#6	Holding points for arrivals shall be provide in an area between the IAF and Sequencing Leg entry point for use in the event that Approach airspace becomes overloaded or that the arrival flow becomes otherwise disrupted	SCM-AOM
FSR#7	Sequencing and spacing of traffic shall be established initially in En-route/ Terminal airspace sectors according to the metering requirements, and to an initial estimation of the order of aircraft in the final landing sequence, that would achieve the optimum runway throughput commensurate with the need to maintain separation minima/wake turbulence criteria and maintain the required departure flow	SCM-ASS
FSR#8	The required aircraft-departure flow rate shall be derived by airport ATC and fed upstream to adjacent En-route / Terminal sectors for synchronisation with the arrival flow requirements	SCM-DS
FSR#9	ATC shall monitor aircraft conformance with all clearances and instructions, throughout each flight, including when aircraft are following predefined P-RNAV routes and associated altitude constraints	ATC-TCM AA, ATC-TCM AG

ID	Safety Requirement	Traceability
FSR#10	Entry into Approach airspace is coordinated with the adjacent upstream sector(s) according to the agreed entry conditions, including the aircraft being stable at the defined altitude well before Sequencing Leg entry	ATC-PTCM-AA
FSR#11	Vertical separation, of at least 1,000 ft, between adjacent Sequencing Legs shall be provided, by aircraft conformance to appropriate published altitude restrictions along the entire length of the Sequencing Legs	ATC-PTCM-AA
FSR#12	Aircraft on the same Sequencing Leg shall be separated longitudinally, by ATC, by a 3 nautical mile radar-separation minimum, or the appropriate wake-turbulence separation minimum, whichever is the greater	ATC-TCM AA
FSR#13	The minimum altitude of each Sequencing Leg shall be sufficient to provide vertical clearance from terrain/obstacles along its entire length	ATC-PTCM-AG
FSR#14	An aircraft shall not be turned off the Sequencing Leg towards the Merge Point until it is spaced behind the previous aircraft, i.e. the aircraft immediately preceding it in the final sequence, sufficiently to ensure that at least minimum longitudinal separation / wake-vortex criteria will be established well before vertical / lateral separation minima are infringed as a consequence of flow convergence	ATC-TCM AA
FSR#15	As each aircraft turns off the Sequencing Leg towards the Merge Point, vertical separation shall be maintained between it and all aircraft on the adjacent sequencing leg until horizontal separation is established (and can be maintained) between them	ATC-TCM AA
FSR#16	The minimum altitude of the Merge Point shall be set such that there is no terrain/obstacle that is higher than the Merge Point anywhere in the sector of the circle defined by the Merge Point and its outermost Sequencing Leg	ATC-PTCM-AG
FSR#17	Except where instructed otherwise by ATC, the aircraft (flight crew) shall assume responsibility for maintaining safe altitude from the start of descent on the “Direct-to” leg until acquiring the ILS glidepath	AB-TCM AG
FSR#18	All non-P-RNAV aircraft shall be vectored along the Point Merge routes to emulate P-RNAV aircraft, while being provided with sufficient obstacle / terrain clearance by ATC	ATC-TCM
FSR#19	Each Point Merge route shall include a Run-off procedure so that aircraft will automatically continue to the Merge Point, on a predefined vertical profile, if no Direct-to instruction is received before reaching the end of the Sequencing Leg	ATC-PTCM-AG
FSR#20	In the event of an aircraft emergency, ATC shall move the subject aircraft forward in the sequence order, (by an early Direct-to or by radar vectoring, as appropriate) sufficiently to minimise the delay to its landing	ATC-TCM AA

ID	Safety Requirement	Traceability
FSR#21	Where it is necessary to resolve a conflict (or other urgent situation, e.g. an aircraft ACAS RA), ATC shall remove the affected aircraft from the landing sequence and reinsert upstream, i.e. later in the sequence, by radar vectoring.	ATC-TCM AA
FSR#22	Aircraft shall report loss of P-RNAV capability to ATC immediately	ATC-PTCM AA, ATC-PTCM AG