



SESAR Safety Reference Material

Deliverable ID:	D4.0.060
Dissemination Level:	PU
Project Acronym:	PJ19 CI
Grant:	731765
Call:	H2020-SESAR-2015-2
Topic:	Content Integration
Consortium Coordinator:	EUROCONTROL
Edition date:	14 December 2018
Edition:	00.04.01
Template Edition:	02.00.01

Founding Members



Authoring & Approval

Authors of the document

Name/Beneficiary	Position/Title	Date
Bruno RABILLER/ EUROCONTROL	PJ 19-4 Safety member	14 December 2018
Nicolas FOTA/ EUROCONTROL	PJ 19-4 Safety member	14 December 2018
Laura CARBO/ EUROCONTROL	PJ 19-4 Safety member	14 December 2018

Reviewers internal to the project

Name/Beneficiary	Position/Title	Date
Marta LLOBET LOPEZ/ EUROCONTROL	PJ 19-4 Safety member	14 December 2018

Approved for submission to the SJU By - Representatives of beneficiaries involved in the project

Name/Beneficiary	Position/Title	Date
Jose Manuel CORDERO GARCIA / ENAI	PJ19 WP04 Lead	14 December 2018

Rejected By - Representatives of beneficiaries involved in the project

Name/Beneficiary	Position/Title	Date
------------------	----------------	------

Document History

Edition	Date	Status	Author	Justification
00.04.00	24/03/2016	Final	SESAR 1 Authors	Approved SESAR 1 version (Project 16.06.01 Deliverable D27) used in Wave 1 of SESAR 2020
00.04.01	14/12/2018	Final	See above	SRM update considering feedback from SESAR 2020 Wave 1 and new EASA regulation (EU N° 2017/373)

Copyright Statement This document has been created by EUROCONTROL. © – 2018 – EUROCONTROL

Licensed to use to all SESAR 2020 Partners within the context of SESAR and Licenced to the SESAR Joint Undertaking under conditions.

Table of Contents

Executive Summary.....	5
1 Introduction.....	6
1.1 Purpose of the Document.....	6
1.2 Scope of the document	6
1.3 Coverage and intended readership	7
1.4 Finding your way around	8
1.4.1 Layout	8
1.4.2 Pictograms used to help you	9
1.5 Important messages at this stage... ..	9
2 The need to augment the safety assessment framework in SESAR.....	11
2.1 Why are SESAR Safety Assessments employing a Broader Success-based approach?	11
2.2 Consideration of resilience in design	12
2.3 About the usage of an Accident Incident Model in support of SESAR Safety Assessments	13
2.4 About Human Factors Integration into safe(r) design	15
2.4.1 Introduction	15
2.4.2 Principles of Human Factors Integration into safe(r) design	16
3 SRM: process and lifecycle	18
3.1 Safety Assessments and the SPR-INTEROP/OSD and TS	18
3.2 Safety Assurance Activities & SESAR Deliverables.....	20
3.2.1 Solution Operational Service and Environment Definition (OSD).....	20
3.2.2 Solution Safety, Performance and Interoperability Requirements (SPR/INTEROP)	21
3.2.3 Technical Specification (TS)	21
3.3 V1, V2 & V3 Safety Assessments Example Outputs	21
4 The SRM process in full	27
5 Application of the SRM: Planning the Safety activities for the SESAR Solution	30
6 Application of the SRM: Safety assessment of SESAR Solution at operational level	32
7 Application of the SRM: Safety assessment of SESAR Solution at initial System design level.....	35
8 Application of the SRM: Safety assessment of SESAR Solution at refined System design level.....	37
9 Application of the SRM: Safety Management of VLD	39
9.1 Objectives of a VLD	39

9.2	Scope of VLD safety assurance	40
9.3	VLD Safety assurance	41
10	Document Information.....	43
10.1	References	43
10.2	Acronyms	44
10.3	Definitions	46

List of Tables

No table of figures entries found.

List of Figures

Figure 1: Safety Requirements and the Solution SPR-INTEROP/OSED and TS/IRS	19
Figure 2: Relationship between Safety Assurance Activities and Solution SPR-INTEROP/OSED and TS/IRS.....	26
Figure 3: SAC, SO and SR specification process.....	27
Figure 4: SAC, SO and SR specification process.....	28
Figure 5: Gates and phases of SESAR Solution development life cycle.....	39

Executive Summary

The aim of this document is to present a clear, complete, coherent and integrated approach to safety assessment that meets the needs of the SESAR work programme. It presents the safety tasks to be undertaken by SESAR Solutions in each of the European Operational Concept Validation Methodology (E-OCVM) V1-V4 maturity phases for both:

- The Industrial Research & Validation (IRV) activities (V1-V3 i.e. TRL1-6); as well as
- The Very Large Scale Demonstration (VLD) projects (V4 i.e. from TRL6-7+)

of the SESAR 2020 work programme. For the safety of the VLD, there will be considerable local safety assurance, which needs to be conducted to support the VLD. Both the local safety assurance and approval process are not necessarily within the remit of the SRM, but the material generated by the SRM process and the SRM per se provide practical guidelines as support.

This document has been written for SESAR staff who are involved in:

- SESAR safety assessments
- Derivation of Safety Criteria, Objectives and Requirements
- Development of SPR-INTEROP/OSED, TS/IRS and Validation Plans/ Reports.

In order to properly conduct the safety assessment of SESAR Solutions, the SRM details a broader approach to safety assessment in which ATM/ANS's positive contribution to aviation safety (a success approach), as well as ATM/ANS's negative effect on the risk of an accident (a failure approach), are both addressed. The former is required to show whether the concept is intrinsically safe, in the absence of failure i.e. when working as specified.

SESAR SRM Ed 00.04.01 is based on the SESAR 1 SRM (Project 16.06.01 deliverable D27 Ed 00.04.00) developed within SESAR 1 and used during SESAR 1 and Wave 1 of SESAR 2020. It has been updated considering feedback and comments received during its application in particular with regards to V3 safety assessment where it was clarified that physical design and detailed Safety Requirements have no more to be addressed. Furthermore, this version considers the new EASA regulations on common requirements for ATM/ANS service providers ((EU) N° 2017/373).

Practical guidance to support the safety assessment activities as defined herein can be found in the companion document "Guidance to Apply the SESAR Safety Reference Material".

Safety practitioners could contact the SESAR 2020 Transversal Area project when conducting safety assessments in accordance with this document. The safety Community of Practice (CoP) could be used for any clarification relative to SESAR safety assessment – Visit also the Stellar SJU Extranet.

1 Introduction

1.1 Purpose of the Document

The SESAR Safety Reference Material (SRM) – this document – is a fundamental and critical component of the systematic safety management approach employed in SESAR.

Indeed, the purpose of this document is to provide a detailed practical guide to:

- The safety assessment and assurance of the whole range of SESAR Solutions throughout the typical system development lifecycle being considered in the SESAR Development Phase that is¹:
 - a. V1: Scope Operational Concept and develop validation plans (TRL 1);
 - b. V2: Iteratively develop and evaluate concept and associated technology enablers (TRL 2-3)
 - c. V3: Build, consolidate and Test (TRL 4-6)
- The safety management of the Very Large Demonstrations (VLD) (V4 *i.e.* from TRL6-7+, read also [13]). The SRM does not necessarily scope for the local safety assurance and approval process of VLD; however, material generated by the SRM process and the SRM per se intend to provide practical guidelines to assist with VLD.

The SRM predetermines the safety assurance *objectives* and *activities* throughout the system development lifecycle required to address the *asked questions* in section 1.5 concerning SESAR safety (up to and including a pre-industrialization phase for the R&I activities of the SESAR Programme 2020 and specifically considering the industrialization phase for the VLD). The safety assurance objectives and activities have been developed to mainly address SESAR ATM Operational Solutions as the latter have direct operational consequences with safety implications (*i.e.* accidents and operational incidents perceived by the airspace users).

Practical guidance to apply the Safety Reference Material to the whole range of projects of the SESAR Work Programme is provided in “*Guidance to Apply the SESAR Safety Reference Material*” [1].

The safety part of the SESAR 2020 Project Hand-Book is based on this document and provides:

- a high level introduction to the SRM and the concepts within,
- a guide for project managers wishing to understand the SESAR safety assessments that are required to be undertaken at each of the system development lifecycles V1 to V4.

1.2 Scope of the document

This document addresses the safety aspects of the specification and design stages of SESAR (*i.e.* V1, V2 and V3 phases as explained above) and provides a practical guide to the relevant safety management

¹ See Concept Lifecycle Model as per [7].

aspects of industrialisation and approval that apply to VLD. It does not intend to cover the complete lifecycle of the constituent part of the ATM/ANS functional system² under consideration (Regulation (EC) No 2017/373 -Part ATS.OR.205(a).(1).(iv) [14]).

In order for stakeholders to produce their local safety assessment/safety case for deployment and operation, the local adaptation and further development of the SESAR safety assessment documentation should determine the extent to which the outcomes are applicable and should ensure that related efforts are commensurate and proportionate to the extent of the risk.

The SRM safety assessment process, described here and supplemented by the accompanying Guidance material, is not static or linear, as the safety practitioner may need to undertake iterations of all or part of the process as necessary. The safety assessment process should, however, be fully integrated into the concept development lifecycle, rather than being carried out in isolation. Furthermore, any safety assessment conducted using the SRM should always be proportionate to the extent of the risk being assessed.

When following the SESAR SRM, safety practitioners should be aware that the safety material developed should be suitable for assuring the concept in different operational environments, and not be limited to a local environment.

The rigour and any local tailoring of the analysis should be at a level which supports the meaningful analysis of the safety of the concept, but not to the exclusion of other operational environments. Furthermore, any assumptions or limitations which need to be made to support this analysis should be documented so that future users of the material are fully aware of any restrictions on its applicability.

Similarly, users of the safety material developed according to the SESAR SRM should be aware of the possible generic nature and/or caveats on the applicability of the analysis, which have been used in order to extend the safety assessment. Safety practitioners should consider using SESAR SRM as input to their local safety analysis, e.g. as a reference assessment/argument. The safety material developed in SESAR may be used to support tailored and proportionate safety assessments, consisting of a review of the reference argument and of an assessment of its applicability in the local context, with an accompanying analysis of any gaps or deviations with additional mitigations applied as necessary.

Note: If there are substantial differences between the SESAR reference argument and the local operating environment then it may be cost beneficial to undertake an assessment from scratch rather than to attempt to re-use generic arguments.

1.3 Coverage and intended readership

This document aims mainly at safety practitioners in R&I and VLD projects of SESAR 2020. The intended audience also includes SESAR JU and SJU members, SESAR 2020 Transversal Area and Master Plan

² 'functional system' means a combination of equipment, procedures and human resources organised to perform a function within the context of ATM/ANS

projects, National Supervisory Authorities (NSAs) as well as EASA within the scope of the rulemaking activities in the field of aerodromes, air traffic management and air navigation services.

Safety practitioners could contact the SESAR 2020 Transversal Area project when conducting safety assessments in accordance with this document. The Safety Community of Practice (CoP) could be used for any clarification relative to SESAR Safety Assessment – Visit also the Stellar SJU Extranet.

1.4 Finding your way around

1.4.1 Layout

This document consists of nine further Chapters, as follows.

Section 2 introduces the fundamental aspects of the safety assessment approach defined herein. First, it is explained why a purely failure-based approach to ATM safety assessment is not sufficient to support the new ATM/ANS concepts that are currently being considered in SESAR. It shows how the addition of a success-based approach leads to a more complete specification of an ATM/ANS functional system's safety properties. It anchors the resilience engineering approach to enrich the success-based approach by applying a better understanding of "*work as done*" to provide a more realistic understanding of the total system behaviour through the application of the resilience engineering principles. Then, it introduces how an accident-incident model representing the safety implications of the SESAR Concept is to be used to decompose the ECAC-wide SESAR safety performance ambition into lower level targets for the different elements of the European ATM System³. Finally, it explains how critical it is that the concepts take full account of human strengths and weaknesses in their development by fully addressing the Human components of socio-technical System safety.

Sections 3 and 4 show the relationships between the safety assurance activities and results and the formal SESAR deliverables, i.e. SPR-INTEROP/OSED and TSs.

Sections 5 to 8 address, respectively, the four steps of the safety assessment: (1) planning the safety activities on a Solution; (2) safety assessment of SESAR Solution at operational level; (3) safety assessment of SESAR Solution at initial design level; and (4) safety assessment of SESAR Solution at refined design level.

Section 9 provides an approach to the safety assessment of Very Large Demonstrations (VLD) to the participating providers of air navigation services (Network Manager and Air Navigation Service Providers (ANSPs))

A list of references and a glossary of abbreviations and terms used in the document are given in **Section 10**.

³ The eATM Portal, <https://www.eatmportal.eu/working>, provides an integrated view of the European ATM System.

1.4.2 Pictograms used to help you

The following set of pictograms are used throughout the document; their meaning is represented here:



Guidance



Important information



Tip



For further reading...



Safety Assessment results to be documented



Safety assurance activities mainly aimed at the Operational level



Safety assurance activities mainly aimed at the design level

1.5 Important messages at this stage...



1. Safety Assessments done in accordance with this document must be at **Solution level**.⁴
2. SESAR brings significant changes to ATM/ANS with a much greater use of automation (on the ground and in the air) and a more strategically-based operational service with less tactical interventions by the Controller. It also affords greater delegation of ATM responsibility from the Controller to the Flight Crew. The use of the SRM in safety assessments helps to answer the following fundamental safety questions:
 - Will the ATM/ANS functional system have sufficient safety functionality & performance?
 - Will it work properly, under all normal conditions of the operational environment that it is likely to encounter?

⁴ In most of the cases, SESAR 2020 Solutions present concepts that have an operational effect and it is accepted practices that safety assessments are undertaken at that level. However, it is worth noting that in a number of cases some Solutions are technological/Enabler Solutions. As a consequence, where relevant, it is necessary for safety assessments to be undertaken at a lower level of granularity to support the validation of a SESAR operational Solution within the performance framework set by the Transversal Area project.

	- What happens under abnormal conditions of the operational environment? - What happens in the event of a failure within the ATM/ANS functional system? - Are the Safety Requirements realistic – i.e. could a system be built to deliver them? 3. The properties of the operational environment are crucial to a safety assessment –a safety assessment that is valid for one (reference) operational environment may not be valid for a different operational environment. Therefore, the safety assessment cannot be “<i>generic</i>”. It has to be “<i>specific</i>” to a particular environment and to a “<i>typical</i>” application. E.g. a safety assessment may apply mainly to “typical” high-density, high-complexity TMA Airspace as will apply around years 2020/2030. It is up to the programme management and specifically SESAR Transversal Area project to ensure that the selected specific validation environment is as generic as possible.
	Examples for the above generic questions could be: - Will the automation be as effective – in reducing pre-existing aviation risks – as the humans that it will replace? - When system failures do inevitably occur can they be safely managed by the humans in the chain?⁵

⁵ This includes issues related to operations that are rapidly shifting to engineering-based support systems (incl. maintenance, the engineers themselves and associated Training, Recruitment, staff numbers, etc.)

2 The need to augment the safety assessment framework in SESAR

2.1 Why are SESAR Safety Assessments employing a Broader Success-based approach?

Historically, safety assessments focused on the reliability of ATM/ANS functional system (as a combination of equipments, procedures and human resources organised to perform a function within the context of ATM) to ensure that the system is adequately protected against internal failures. This restricted view of safety was sufficient because ATM/ANS systems gradually evolved and it was adequate to rely on the assumption that ATM/ANS systems are intrinsically safe when no failure occurs. However, this assumption is no longer valid given the nature of SESAR concepts, the development of new technologies and the increasing use of automation. An additional argument is the nature of the ATM/ANS functional system, which is intended to mitigate the aviation risks that pre-exist in the operational environment, like e.g. collision with other aircraft or controlled flight into terrain.

The SESAR safety methodology continues to require that safety assessments examine internal system failures (termed “failure-based approach”); additionally, it also requires the consideration of the “success-based approach”. The “success-based approach” determines the functionality and performance of the design needed to ensure that when the system is working as intended (i.e. as specified) it is able to provide, at the very least, a tolerable level of safety; but it also ensures that the potential safety benefit of the design is maximised. The aggregate of the success and failure contributions needs to be: neutral – to demonstrate that safety will not deteriorate – and substantially positive – for the safety nets. Consequently, not only would the “failure-based approach” be incomplete without the complementary “success-based approach” but it would also depend on it. In other words, we cannot define “failure” until we have fully defined “success”.

Hence, the SESAR Safety Assessments must encompass a “**broader**” approach considering safety from two perspectives:

- Firstly, a **success approach** in which we assess how effective the new concepts and technologies would be when they are working as intended – i.e. how much the pre-existing risks that are inherent to aviation will be reduced by the ATM/ANS changes. This is concerned with the *positive contribution to aviation safety* that the ATM/ANS changes make in the absence of failure.
- Secondly, a **failure approach** in which we assess the ATM/ANS system generated risks – i.e. induced by the ATM/ANS changes failing. This is concerned with the *negative contribution to the risk of an accident* that the ATM/ANS changes might make in the event of failure(s), however caused.

	The SESAR SRM: ▪ puts the SAM [3] into an argument framework to support the failure approach, and ▪ adds a success approach to show whether the concept is intrinsically safe (i.e. mitigates sufficiently the aviation risks), in the absence of failure.
	It is the success approach that is more closely aligned with the SESAR Validation Exercises. This point can be illustrated by considering the KPA/KPI “Capacity”: If Function ‘A’ were intended to increase capacity, we would first assess how successful the Function would be in delivering more capacity, when it was working to specification, including whether that specification was adequate. We would of course then need to consider what would happen if/when the Function failed, since such failure would undermine the capacity benefit. We treat Safety in a similar way. We first assess the contribution that a Function makes to safety (positive, negative or neutral) when it is working to specification, under the full range of normal and abnormal conditions to which the Function may be subjected in its environment. We then consider failure of the Function including the possibility of additional side effects of failure beyond merely undermining an expected safety benefit.

2.2 Consideration of resilience in design

Acknowledging that:

- Due to the high level of safety reached in ATM, relatively little data is available on negative safety outcomes; as a consequence, it is increasingly difficult to deliver further safety benefits using standard approaches to safety (hence the broader approach as per **section 2.1**)
- Performance variability can be the reason why things go right (e.g. it can make the ATM/ANS Functional System more adaptable to varying environmental conditions) as well as why things go wrong – hence the need to manage performance variability, not merely seek to remove it.

The SRM integrates the concept of Resilience to provide a better understanding of the total functional system behaviour.

	The SRM enables, based on the principles of Resilience Engineering, to identify: ▪ small variations in ATM/ANS system performance that may “coincide and combine” to produce variations in safety performance outcomes; ▪ dependencies in the ATM/ANS system that contribute to safety opportunities or increased risk; ▪ the strategies and Solutions used by air traffic controllers, pilots and ATM/ANS functional systems to run operations safely; ▪ recovery/fall back mechanisms that help people to cope with foreseen and unforeseen operations;
---	---

	- the adaptation and flexibility levels needed to handle unpredictable situations; - the different safety features that can interact in a positive way to make for better safety performance.
	Guidance J in [1] describes an approach, based on the principles of Resilience Engineering, which provides a means to investigate everyday operations to improve the resilience of the future ATM/ANS functional system. Based on an analysis of work-as-done, varying conditions and the adaptive capacity in the operation, this guidance supports other safety assurance activities performed, and in particular those safety assurance activities related to both the success case (see section 2.1) and the human factors integration (see section 2.4) of the SRM.
	‘Final Resilience Guidance Material for Safety Assessment (SRM) and Design’ [11], provides wider guidance, including a definition of resilience, its underlying principles and an approach which can assist projects in understanding how the changes introduced affect the performance of the ATM/ANS functional system, including safety performance. This method has been fully integrated into the safety assurance activities summarized in Guidance A1 to A4 in [1]. ‘From Safety-I to Safety-II’ [12], the white paper led by Prof Erik Hollnagel, explains the key differences between, and the implications of, two different ways of thinking about safety. An argument is made that safety management should move from ensuring that ‘as few things as possible go wrong’ to ensuring that ‘as many things as possible go right’ in daily operations.

2.3 About the usage of an Accident Incident Model in support of SESAR Safety Assessments

The main objectives of SESAR are to deliver increased capacity in line with expected demand (an increase of 3-fold by 2035) whilst achieving a 10-fold reduction in the risk per flight, just to maintain the current (very low) annual accident rate.

From a safety perspective, this represents a major challenge.

The SESAR ten times safety performance improvement defines what has to be achieved in terms of safety **at the overall ECAC level** – i.e. it defines what is tolerably safe at this level. However what is required is a set of qualitative and/or quantitative measures that defines **what has to be achieved in terms of safety for specific concepts of operation** in order to satisfy the ECAC-wide safety performance ambition. At the level of the individual concepts, what is tolerably safe is referred to as the **Safety Criteria (SAC)**.

A major problem is the sheer complexity of the SESAR 2020 Concept (number of Solutions and number of Operational Improvements steps (OIs) to be managed), its evolutionary nature (the phased introduction of the distinct operational improvement steps) and the dispersed and disparate nature of the many different organisations contributing to the SESAR Programme. Consequently, the problem arises as to how to derive suitable Safety Criteria while duly considering the many interactions/ interdependencies between the various concepts of operation and while dealing appropriately with

the aggregate safety risk and with the apportionment of the risk budget. Due to the multitude of operational projects involved and to the necessity to be able to predict and assure that the overall x-fold reduction in the risk per flight at the different concept development steps could be met, it is essential that these Safety Criteria are identified and described based on a common framework. In SESAR, this framework is supplied by the Accident Incident Model (AIM), which lies at the heart of this delicate apportionment exercise.⁶ Reference [9] summarises the qualitative and quantitative validation/verification for AIM.

The AIM risk model provides a set of individual models (one for each accident type [8]) that all SESAR Solutions shall use to identify where and how the operational changes brought by a specific Solution will impact the safety of ATM/ANS provision.⁷

AIM is a risk model that shows the risks of aviation accidents⁸ and provides a structured breakdown of the causes, with particular emphasis on ATM/ANS contributions (both positive and negative). The risk picture for SESAR is formed by modifying the baseline AIM risk model to represent the combined effects of the set ATM/ANS changes that are expected to be in place as per the IOC (Initial Operating Capability) and FOC (Final Operating Capability) dates in the ATM Master Plan. Each ATM/ANS change is modelled through adjustments representing its expected impacts on appropriate elements of the risk model. These effects, together with the effects of changes in traffic levels, can then be summed to estimate the total risks and contributory/causal breakdown for the selected years. This approach allows investigation of the improvements that are necessary⁹ to satisfy the ECAC-wide safety performance ambition.

Once the overall SESAR ATM risks meet the overall ECAC-wide performance ambition (i.e. x-fold reduction in the risk per flight at the different concept development steps), the modelled performance of each ATM element can be used as its Safety Criteria. Thus AIM provides a convenient way of apportioning the ECAC-wide target that takes account of actual attainment and interactions with expected future developments as well as the traffic increase (and its effect on safety). The setting of suitable and consistent Safety Criteria is further explained in **Guidance D** of [1]. In addition, AIM includes a set of incidents of different severities, which are precursors of each accident category. These can be used to derive quantitative Safety Objectives for such severities. **Guidance G** of [1] describes

⁶ **Guidance D** in [1] makes clear that Safety Criteria could encapsulate both (i) specific safety performance targets to be met using the Accident Incident Model (AIM); as well as (ii) any operational or technical regulatory requirements and standards (e.g. PANS-ATM, ICAO Annexes, equipment standards, interoperability requirements) that apply to the projects and could have a bearing on the overall safety of the System concerned.

⁷ Outside of the SESAR development phase, when moving towards local implementation, local adaptations to the generic ECAC-wide models might be required to reflect the specific local operational environment, operations, legacy systems and data.

⁸ Models currently exist for MAC En-route, TMA, Oceanic, CFIT, RWY Collision, TWY Collision, and Wake-related accidents for final approach. At the time of the development of this version of the SRM, a RWY Excursion model is being developed. SESAR projects may propose model's modification but only in close cooperation with the SESAR Transversal Area project.

⁹ The Safety Criteria are derived through a series of rationale and informed judgements from Subject Matter Experts (SMEs). Uncertainties related to SAC setting are addressed in **Guidance D** in [1]. Proper safety validation objectives to inform VAL Plan have to be defined to assess in validation exercise the 'achievability' of the SAC (see assurance activities in **Guidance D** in [1]). It is obvious that validation exercises should consider as an input the considered evolutions in airspace and airport traffic for a particular Step of the concept storyboard in order to generate proper evidence to support the safety assessment process.

how to use AIM for the determination of the severity of the effects of operational hazards and associated Safety Objectives.

	Data-based, static models such as AIM, whilst providing the view of how ATM/ANS contribution to safety could look in the future, cannot provide assurance that it will actually look like that in practice. Indeed the latter requires more direct – and for some purposes more dynamic – representations of safety contribution through the specification, modelling and simulation of the safety properties (functionality, performance, and integrity) of the future ATM/ANS system. Consequently the AIM models are <u>not</u> a substitute for the safety assessment. On the other hand, they inform the success and failure-based safety assessment. In this respect they offer a number of advantages as follows: ▪ They are based on real, historical accident and incident data ▪ They provide Safety Criteria at many levels in the ATM/ANS functional system hierarchy (Aggregation of Solutions, and individual Solutions) and for specific phases of flight. ▪ They provide Safety Criteria that take account of future changes to the ATM/ANS functional system and/or operational environment.
	The SESAR Transversal Area project provides all required support to operational and technical Solution projects for the identification of the Safety Criteria. Indeed, in doing so, the Transversal Area project manages the overall risk budget and understands the aggregate risk.

2.4 About Human Factors Integration into safe(r) design

2.4.1 Introduction

The human element remains pivotal to the success of SESAR 2020 and it is foreseen that, for the future, the controller, engineer, assistant, pilot and other operational roles will remain essential in the transition to and the successful implementation of ATM/ANS evolutions. It is therefore critical that the concepts being developed take account of human strengths and weaknesses in their development. By fully addressing the Human components of Functional System safety, this document intends to maximise human performance and minimise human failure in the design of the SESAR 2020 System.

In doing so, and as reflected in both this section as well as in **Guidance A1 to A4** of [1], the SRM has moved towards an integrated approach to performance management with, as a first step, the establishment of a Safety and Human Performance¹⁰ (HP) collaboration to improve the performance

¹⁰ As per [10], Human Performance (HP) is used to denote the human capability to successfully accomplish tasks and meet job requirements. The capability of a human to successfully accomplish tasks depends on a number of variables that are usually investigated within the discipline of "Human Factors (HF)". These are: procedure and task design, design of technical systems and tools, the physical work environment, Founding Members

of the overall Total Aviation System. The Human Performance assessment is performed in SESAR as per the Human Performance Assessment Reference Material [10]. Coordination between both processes is required then, in particular with respect to the items listed in next section. More detail is provided in **Guidance L**.

2.4.2 Principles of Human Factors Integration into safe(r) design

For any change to ATM/ANS functional systems, the following Human Factors (HF) principles shall be adhered to:

- (1) Within the scope of the change, all safety relevant human roles and tasks shall be identified. This shall include both ground and airborne elements.

Justification: Human performance has a significant influence on the safety performance of the ATM/ANS System. Human performance creates safety and it is essential that the contribution (both positive and negative) of human performance and decisions are understood.

- (2) It shall be shown for each safety relevant task that the task is within human capability and limitations. The following shall be considered:

- The variables for each task, and factors that shape performance
- The interactions between the tasks;
- The task conflicts (e.g. creating new conflict(s) by solving one, or efficiency thoroughness trade-offs);
- The extent of variation of the variables themselves.

Justification: The capability of a human to successfully and safely accomplish tasks depends on a number of variables. Understanding these variables and the interplay between them is essential.

- (3) Document and define the environment and assumptions within which the HP and Safety Assessment has been undertaken. Understand the limitations, especially with respect to local factors that might subsequently affect human performance (e.g. local implementation in different environments to those explored in V1 to V3 and V4).

Justification: Human tasks are not independent and it is essential that the context within which decisions are made is understood since it has a significant impact on whether the tasks will be undertaken successfully.

- (4) Demonstrate that (i) the interfaces between humans and (ii) the interfaces between humans and technical equipment have been identified. Understand the variables/factors that influence those interfaces and confirm that those variables remain within the acceptable ranges to ensure safety.

individual competences and training background as well as recruitment and staffing. HP also depends on the way in which Social Factors and issues related to Change & Transition are managed.

Justification: Human tasks are not independent and the impact of performance variability needs to be understood in complex social-technical system design

- (5) show that for tasks which are critical in terms safety impact that an appropriately thorough HF analysis has been undertaken.

3 SRM: process and lifecycle

The safety assurance objectives and activities have been developed to address SESAR ATM Operational Solutions mainly, as they have direct operational consequences with safety implication (i.e. accidents and operational incidents seen by the airspace users). Safety assurance activities dedicated to Technological/Enablers Solutions are proposed in **Guidance O** of [1].

3.1 Safety Assessments and the SPR-INTEROP/OSED and TS

With respect to the formal SESAR deliverables, the SESAR 2020 Solution SPR-INTEROP/OSED and TS formally capture, from a safety perspective, the safety requirement hierarchy¹¹ within a Solution. The **Safety Criteria** define what is considered tolerably safe for the change being introduced by operations within the scope of the Solution. It enables the SESAR Transversal Area project, with the assistance of the Solution operational and technical experts, to determine what proportion of the x10 SESAR safety performance ambition the Solution is expected to deliver.



[4] interprets the x10 SESAR safety performance ambition very precisely and supplies the necessary detail.

However, this SES reference is not practicable in the SESAR programme for the following reasons:

- the 3-fold traffic increase is not solely applicable to SESAR programme but also to some other non-SESAR ATM/ANS improvements;
- SESAR does not provide a consolidated traffic increase indicator, but one for airspace and another one for airport capacity increase;
- the relationship between traffic increase and safety improvement is not systematically to the square. In the case of collisions, this requires the probability of collision per encounter to reduce in proportion to the square of the traffic increase. However in other accident types and with risk metrics directly proportional to the amount of traffic, a reduction equal to the traffic increase would be sufficient.

As a consequence the following Safety High Level Goal has been defined instead: *“there should be no increase in the expected total number of fatal accidents per year with ATM contribution in relation with the airspace capacity and airport capacity KPAs”*.

Safety Criteria (SAC) are derived during V1 through the analysis of AIM and are presented in the V1 Solution Validation Plan – Part II: Safety Plan. As the Solution progresses to V2 and the Solution concept is further refined, the safety assessment at the operational level will establish the **Safety Objectives** to

¹¹ The safety requirement hierarchy is the safety requirement cascade from the Safety Criteria to the Safety Objectives to the safety requirements.

deliver the Safety Criteria, and the safety assessment at initial system design level will establish the **Safety Requirements** to satisfy the Safety Objectives. The Safety Objectives and Safety Requirements are presented in the V2 Solution SPR-INTEROP/OSED and in V2 TS for the technical requirements (if relevant at that stage of the lifecycle).

As the design further develops in V3, safety assessment activities at the refined system design level¹² of the SESAR Solution will refine the Safety Requirements derived at V2 level (e.g. lower level human tasks, technical systems, functional blocks, functions and services etc.). These are presented in the V3 Solution SPR-INTEROP/OSED and in V3 TS. Traceability from the refined requirements to the Safety Criteria must be explicit and presented in SPR-INTEROP/OSED and TS, as appropriate. There needs to be an assessment of the feasibility of satisfying the Safety Requirements as well.

The relationship between the key SESAR formal deliverables and the Safety Requirements is represented in **Figure 1**.

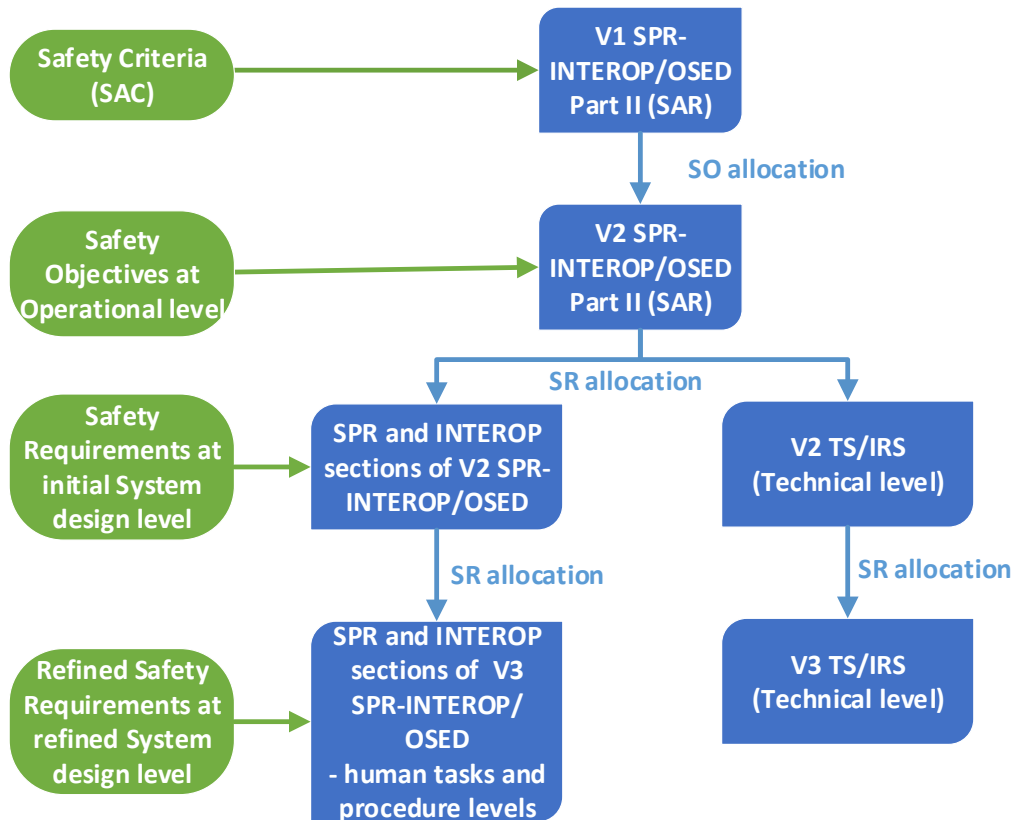


Figure 1: Safety Requirements and the Solution SPR-INTEROP/OSED and TS/IRS

¹² Refined system design level means the lowest system design granularity defined at the SESAR Solution level encompassing technical elements, humans and procedures.

Figure 1 is a top-level view of the System Engineering/development process and how the main outcomes from the SRM safety assessment relate to that process. The development process is iterative in nature. The safety assessment process is an inherent part of this process. As the design evolves, changes are made and the modified design must be reassessed. This reassessment may create new derived safety requirements. These new safety requirements may need further design changes. For the sake of keeping this figure simple, the iterative nature is not explicitly shown.

	The definition of what is meant by safe is described by the Safety Criteria (SAC) which are then allocated to Safety Objectives (SOs), and then Safety Requirements (SRs); both set the minimum positive (success approach), and maximum negative (failure approach), safety contributions of the ATM/ANS system. Provided each system element meets its safety requirements, the functional system will meet its safety criteria. Overall, this is an iterative requirements specification –requirements satisfaction exercise that is completed when it is demonstrated that the System design for the SESAR Solution is realistic, <i>i.e.</i> achievable in terms of the Safety Requirements it places on the human, procedural and technical elements of the System. The Safety Objectives from the success approach are concerned with <u>what</u> the ATM/ANS system has to do in a particular Operational Environment but <u>not how</u> it does it. They specify what needs to happen in the airspace (as opposed to in the ATC ops room or in the cockpit) in order to satisfy the Safety Criteria. The Safety Requirements are concerned with <u>how</u> the design of the ATM/ANS system satisfies the Safety Objectives.
---	---

3.2 Safety Assurance Activities & SESAR Deliverables

As explained above, the Solution SPR-INTEROP/OSED, and Solution TS are key SESAR 2020 deliverables which formally capture, from a safety perspective, the requirement hierarchy between the Solution Safety Criteria, the Safety Objectives and the Safety Requirements. Their relationship is depicted in **Figure 2**. The safety assessment process is interactive and associated with the design definition as per the V1-V3 lifecycle stages. The process is continuous throughout the design cycle. For the sake of readability, feedback loops have not been all represented. This applies to **Figure 3** and **Figure 4** in **section 4** as well.

3.2.1 Solution Operational Service and Environment Definition (OSED)

The OSED section of the SPR-INTEROP/OSED Part I presents the overarching operational concept for the Solution. From a safety perspective, the SPR-INTEROP/OSED Part II (Safety Assessment Report) presents the Safety Criteria for the Solution which will have been established by the V1 Safety Assessment. It is envisaged that the Safety Criteria will then be used to drive the validation activities and will form the safety validation basis of the V1 Validation Plan.

The OSED section of the SPR-INTEROP/OSED Part I is also updated during V2 in order to refine the concept (if needed). From a safety perspective, the SPR-INTEROP/OSED Part II (Safety Assessment Report) presents the Safety Objectives (success and failure approach) derived at the beginning of the V2 safety assessment. The Safety Objectives specify formally the safety properties of the ATM/ANS functional system at the operational service level that are required for the SAC satisfaction. During V2, it is envisaged that the Safety Objectives will be used to drive the safety validation activities within the V2 Validation Plan.

Founding Members

3.2.2 Solution Safety, Performance and Interoperability Requirements (SPR/INTEROP)

The SPR/INTEROP section of the SPR-INTEROP/OSED Part I is produced at the Solution level and is initiated during V2. It consists of requirements (operational, performance, safety, interoperability) reflecting the increased maturity of the intended design Solution. The SPR-INTEROP/OSED Part II (Safety Assessment Report) presents the derivation of the Safety Requirements for the satisfaction of the Safety Objectives, during the V2 safety assessment of the initial System design. The Safety Requirements are presented at a level sufficient to allow the different stakeholders to develop the system elements to enable prototyping in V3 and implementation from V4 onwards (including the VLD – see **section 9** herein). This will ultimately result in requirements that can be addressed through procedural, human, hardware and software solutions during the implementation phase which is outside of the scope of this document. It is envisaged that the Safety Requirements can then be used to support the safety validation activities of the V2 Validation Plan.

The SPR/INTEROP section of the “SPR-INTEROP/OSED Part I” is also updated in V3 to reflect the outcome of the V3 safety assessment of the refined System design for the SESAR Solution. It will refine the Safety Requirements derived at the previous stage.

3.2.3 Technical Specification (TS)

The TS is produced at the Solution level during V2 for the initial System design (if appropriate) and during V3 for the refined System design of the SESAR Solution. Technical Safety Requirements are defined at the level of the technical systems, functional blocks, functions and services and should be traceable to Safety Requirements identified in the SPR-INTEROP/OSED Part I. The TS is written at a level of detail sufficient to allow the technical elements to be designed and implemented by e.g. an industrial partner. It presents the ‘what’ providing flexibility for the e.g. industrial partner to develop the ‘how’. From a safety perspective, the TS includes the Safety Requirements (*functional, performance and integrity properties*) of the relevant technical elements, from the success and failure approaches.

3.3 V1, V2 & V3 Safety Assessments Example Outputs

Safety assessments are performed at the level of the Solution. They are undertaken at E-OCVM phases V1, V2 and V3 at increasing levels of maturity and associated detail. It is essential that the assessments and the subsequent validation activities are undertaken against a specific operational concept, consistent set of assumptions and simulation scenarios valid for the Solution.

V1 Safety Assessment – will derive the Safety Criteria applicable to the relevant operational concept(s). The criteria are developed based on the application of the appropriate accident incident models of AIM as explained in **section 2.3** and expanded in **Guidance D** of [1]. It will establish the safety expectations of the change and dependent on the nature of the change, these may comprise a combination of detrimental or beneficial safety effects for each Solution considered. Care should be taken that some interdependencies might exist between relevant models within AIM.

	1. An example Safety Criterion could read “<i>Solution X shall provide a 5% reduction in the likelihood of ATC Induced Conflicts (per flight hour) despite a x% increase in traffic.</i>” 2. Another example could read: “<i>Solution Y shall provide a 30% reduction in the likelihood of Controlled Flights Towards Terrain (per approach).</i>”
---	---

It is also required that the safety assessment will include a justification that the Safety Criteria (SAC) are appropriate and correct for the environment specified and that any relevant assumptions will be recorded. The SAC must be measurable such that achievement (incl. using proxies, *i.e.* relevant indicators) can be demonstrated in validation exercises.

V2 Safety Assessment – the V2 safety assessment can be considered as consisting of two phases:

Phase One

The phase one V2 safety assessment focuses on a single Solution concept having discarded the alternative concepts having gained an improved level of design maturity during V1. The phase one V2 safety assessment will derive Safety Objectives (both success and failure) in support of the Safety Criteria.

The Safety Objectives (from the success approach) will describe at the **operational level** the functional and performance properties that are required to deliver the Safety Criteria when the system is working as intended. They will establish the safety properties needed to address all normal and abnormal conditions of the operational environment.

	- Examples of Safety Objective (success approach) in normal conditions could read (in that case for Increased Glide Slope (IGS) concept): ▪ “ATC shall apply appropriate spacing between aircraft considering the arrival sequence which is composed of IGS and non-IGS aircraft” ▪ “Aircraft shall be stabilized in speed and thrust level not later than 1000ft above runway threshold in IMC during IGS operations” 2. Examples of abnormal conditions could be: ▪ Sudden reduction in runway capacity - e.g. due to sudden drop in visibility ▪ Unforeseen runway closure ▪ Unexpected tail wind, Very strong winds (e.g. > 50 kts) ▪ Solar storms (ionosphere events) The key message is here that the safety assessments need to consider all foreseeable operating conditions, irrespective of whether they can be defined as “normal” and “abnormal”. An example of Safety Objectives (success approach) in abnormal conditions could read (still in that case for Increased Glide Slope (IGS) concept): ▪ “ATC shall safely handle the situation where an aircraft on the standard approach executes a missed approach which will cross the trajectory of a follower aircraft conducting the IGS approach”
---	--

The Safety Objectives (from the failure approach) will typically describe at the operational level the maximum tolerable frequency of the operational hazards that can be accepted while not failing to meet the Safety Criteria. They are derived from the application of an FHA/OHA against the functional properties of the design (identification of operational hazards, determination of severity(ies) and application of a quantified risk classification scheme to limit the frequencies to a tolerable level).

Founding Members

	To avoid System-generated hazards to be inconsistently defined across the SESAR 2020 work programme, they <u>have to</u> be identified at the level of the Operational services, <i>i.e.</i> a level that is independent of the actual design of the System and is related to the failure of an operational service. The system-generated hazards identified at the operational services level are called Operational Hazards.
	Examples of Operational hazards could read (still in that case for Increased Glide Slope (IGS) concept): ▪ “ATC failure to maintain the separation between aircraft flying IGS and standard approaches for the same runway end” ▪ “Aircraft fail to decelerate to the stabilised approach speed during IGS approach leading to an unstabilised approach”
	Guidance on the identification of Operational hazards and the usage of Risk Classification Schemes to generate Safety Objectives (failure approach) is provided in Guidance G of [1] .

Assurance that the safety objectives are correct, realistic and can be achieved will also have to be included within the phase one V2 safety assessment, by checking whether and how the safety objectives are addressed by the validation exercises.

Phase Two

The phase two V2 safety assessment involves the analysis of the initial System design of the SESAR Solution in order to derive Safety Requirements (success and failure) in support of the Safety Objectives (success and failure) that were derived during the phase one V2 safety assessment. The Safety Requirements (from the failure approach) are derived as a result of the application of the PSSA equivalent activities.

The initial System design of the SESAR Solution is documented and represented in:

- SPR-INTEROP/OSD Part I with the associated EATMA models at operational layer, and in
- initial TS (if already available) with the associated EATMA models at system and service layers

If EATMA models are not available, alternative engineering models can be developed by the safety assessor supported by Project expertise (see **Guidance I of [1]**).

It is expected that Safety Requirements (success and failure) will be documented in V2 SPR-INTEROP/OSD Part I and the safety requirements derivation process (e.g. fault trees, qualitative argumentation for the apportionment or derivation of Safety Requirements) will be described in the Safety Assessment Report *i.e.* V2 SPR-INTEROP/OSD Part II).

	1. Examples of safety requirement (success approach) in normal conditions could read (in that case for Increased Glide Slope (IGS) concept): <i>“Approach Supervisors shall decide when a published IGS approach becomes active/inactive for operations, considering the conditions for application are and remain met:</i> -No operational ATC & weather limitations - Necessary navigation guidance means are serviceable “
---	--

	<i>“The IGS approach chart shall be specific to one final approach path (i.e. angle and touchdown aiming point) and shall highlight the glide path angle in case it is significantly increased (e.g. more than 3.5°)”</i> 2. Examples of safety requirement (success approach) in abnormal conditions could read (still in that case for Increased Glide Slope(IGS) concept): <i>“When the lead aircraft flying on final conventional approach is executing a missed approach and a following traffic is flying on final IGS spaced at or close to the separation minimum, the Approach or Tower Controller shall also instruct the following aircraft flying an IGS to execute a missed approach, either with a "Turn left/right immediately" instruction or ensure that the follower is maintained above the lead traffic (taking into account sufficient climb performance)”</i> <i>“In case of one engine failure, the Flight Crew shall verify that the IGS approach can be continued otherwise he/she will execute a missed approach“</i>
--	---

If applicable at V2 level for the SESAR Solution under assessment, Safety Requirements (success and failure) for the technical elements will be documented in V2 TS document.

V3 Safety Assessment – requires the analysis of the refined System design for the SESAR Solution. The V3 safety assessment is expected to analyse the refined System design in order to derive refined Safety Requirements (success and failure). Resultant requirements that relate to the human task are expected to be documented in the V3 Solution SPR-INTEROP/OSD whereas technical requirements are expected to be documented in the V3 Solution TS document. Traceability from initial Safety Requirements to refined Safety Requirements must be made explicit as well as the detail of the requirements derivation process (in the V3 Solution SPR-INTEROP/OSD Part II).

Assurance that the safety requirements are correct, realistic and can be satisfied in a physical implementation must be provided by checking whether and how the safety requirements are addressed by the validation exercises or, if this is not possible, based on relevant Project operational and technical expertise. This assurance needs to be documented within the safety assessment.

	It should be noted that the initial System design and refined System design of the Solution mentioned herein should already be available as part of the normal operational, project-management and /or systems-engineering processes¹³. Maximum use should be made of such information for safety purposes, provided sufficient confidence is shown in its completeness and correctness. If safety analysis reveals deficiencies in the completeness or correctness of this existing information, suggested corrections of those defects will be fed back to the projects. Proposed corrections could then be validated e.g. during PSSA workshops so that the existing material becomes suitable to support the safety assessment.
---	---

¹³ In particular with the European ATM Architecture (EATMA).

	It is impossible in the SESAR safety assessments to be totally conclusive regarding the safety of the Solution design since many characteristics on which such conclusions depend are determined by the specifics of each implementation of the Solution. Nevertheless, the potential of the Solution to meet the SAC can be proven by describing the safety benefits (if relevant) that are expected to be gained from the Solution, setting Safety Objectives and Safety Requirements, doing a qualitative comparison of the Solution operations with respect to current operations, and using the validation exercises to show both the ability for the Solution to deliver the required operational services and that Safety Requirements and assumptions are capable of being satisfied, etc. Further Guidance are available in Guidance A and M of [1] in particular. It is essential in the safety assessment report to show that Safety Requirements and evidence of achievement/achievability in support of the eventual deployment applies to: • A known Solution System configuration; and • One configuration which is consistent for all phases of the lifecycle. Since projects are liable to changes being introduced at various stages of System development, this requires careful change management and configuration control of the various representations of the Solution System throughout the lifecycle. In addition, the safety assessment requires assumptions about the operational context to be made. Irrespective of the assumption source, assumptions should be managed as thorough as the requirements since they drive the design and validation process. By their nature these assumptions may not be traceable and should have rationale that is visible eventually for the deployment.
	For generic guidance on system engineering models, go to Guidance I of [1].

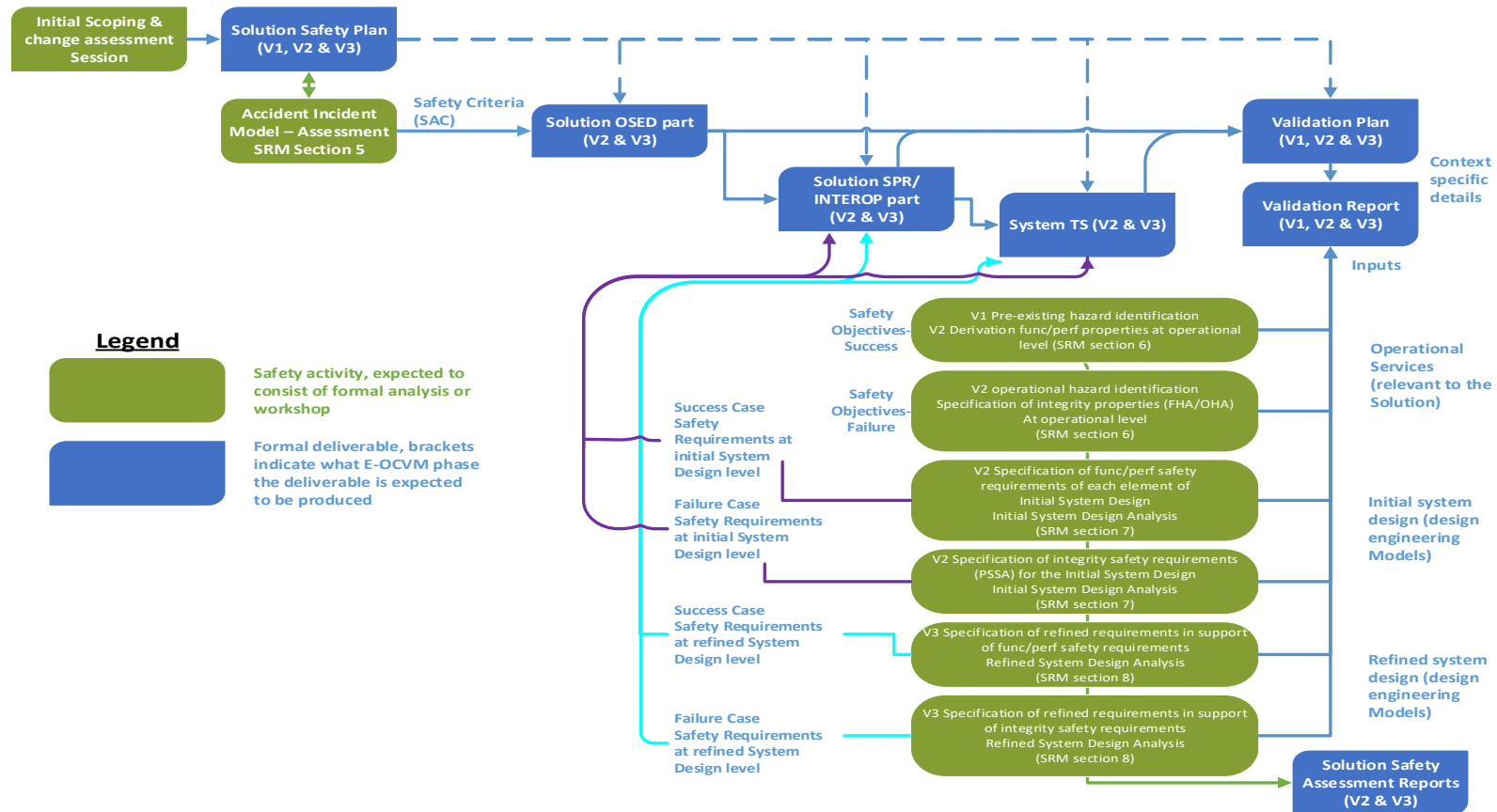


Figure 2: Relationship between Safety Assurance Activities and Solution SPR-INTEROP/OSED and TS/IRS

Founding Members

4 The SRM process in full

The full process for deriving the Safety Criteria (SAC), Safety Objectives (SOs), and Safety Requirements (SRs) as well as relationships with key SESAR deliverables is shown in **Figure 3** and **Figure 4** below. It portrays the overall hierarchy of Safety Requirements described in **section 3** above.

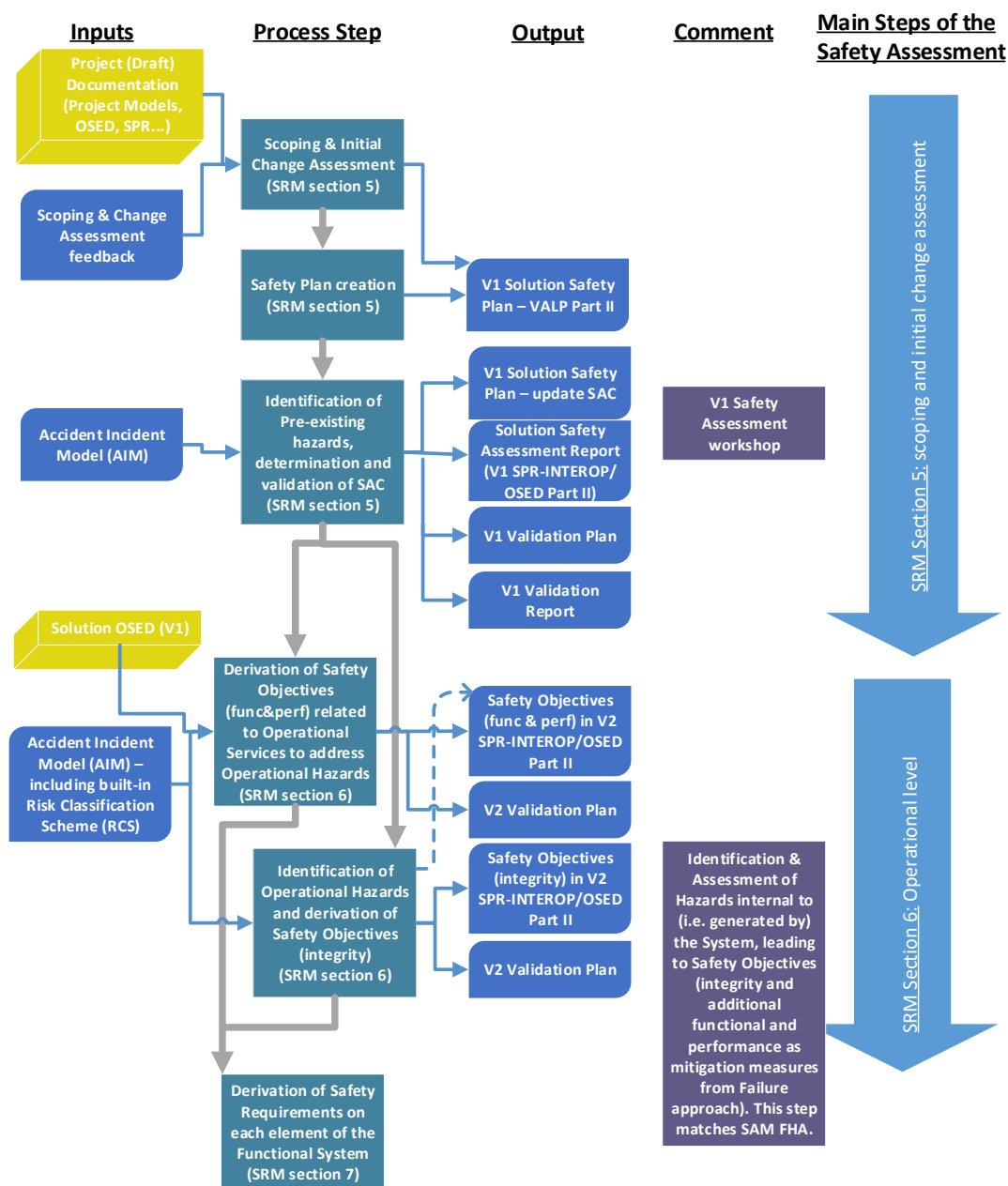


Figure 3: SAC, SO and SR specification process

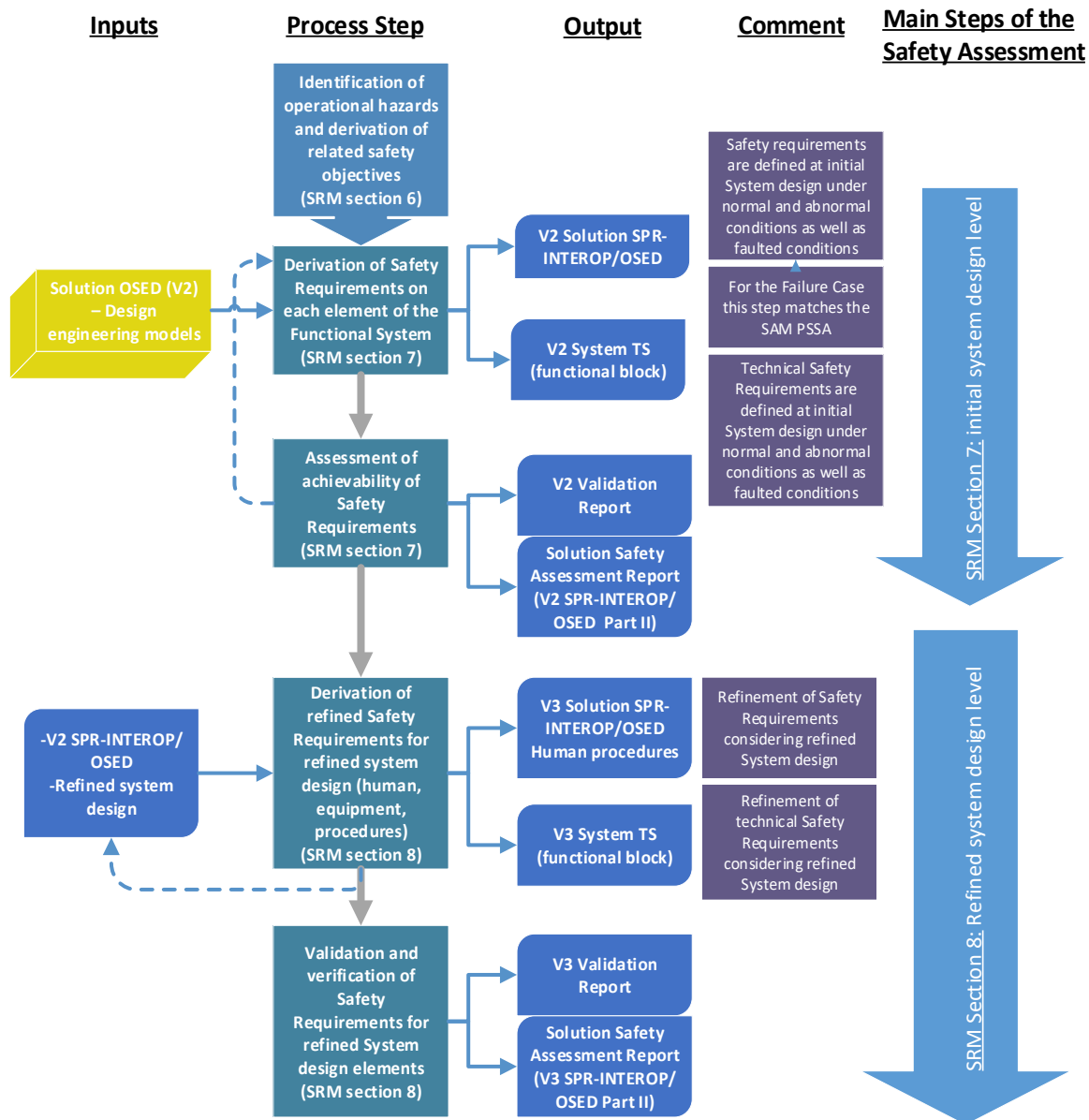
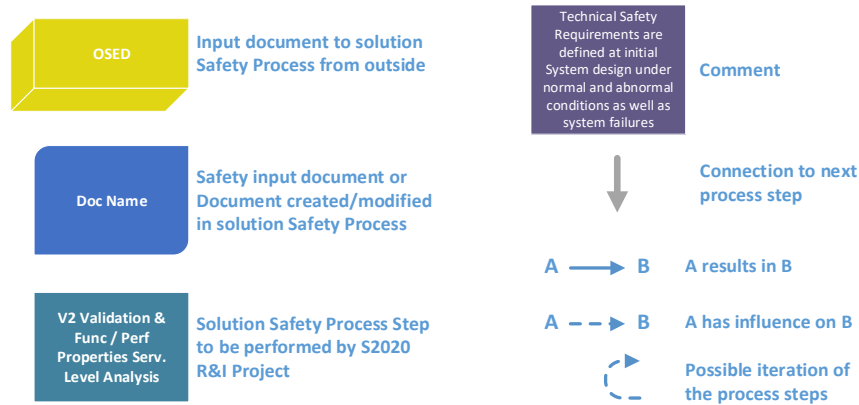


Figure 4: SAC, SO and SR specification process
(cont'd)

The symbols used in **Figure 3** and **Figure 4** are as follows:



5 Application of the SRM: Planning the Safety activities for the SESAR Solution



The safety activities to be conducted for a SESAR Solution are described in the Safety Plan, which is appended to the VALP (VALP Part II). The Safety Plan [5] presents the safety assurance activities to be carried out by a Solution in order to create necessary and sufficient evidence for the production of the Solution Safety Assessment Report (SAR) (encompassing the safety evidence provided by the validation exercises). The Safety Plan also clearly defines the roles and responsibilities amongst the project team.

The Safety Scoping and Change Assessment process aims at specifying the detailed safety assessment activities to be undertaken by the Solution. This preparatory process identifies the main safety issues associated to the Solution as soon as possible after an Operational Concept has been developed and helps in deciding the extent to which the safety assessment has to be conducted.

It provides an initial assessment of the safety implications of the Solution. It should address what the Solution is seeking to achieve (e.g. to deliver benefits in capacity, efficiency and/or safety), the possible impact on safety (in general terms only, since a safety assessment would not have been started at this stage), the criteria for deciding what is “safe” in the context of the Solution (*the Safety Criteria*) and in broad terms the strategy for demonstrating safety.

The following safety assessment activities need to be performed at the safety planning level (details of the planned safety assurance activities are provided in **section A.1** of [1]):

- description of the key properties of the **Operational Environment** that are relevant to the safety assessment
- identification of the **pre-existing hazards** that are inherent in aviation within the scope of the Solution operations
- first determination of the **operational services** relevant to the Solution operations
- derivation of suitable **Safety Criteria** for the Solution operations

	1. The principles, safety assurance objectives and safety assurance activities that are presented in sections 6, 7 and 8 and Guidance A.2 to A.4 of [1] are all generic. The execution of the Safety Scoping and Change assessment process defined in Guidance C of [1] will help identifying what will/will not change and to specify the safety assessment activities applicable to the Solution. 2. The purpose of most safety-related systems is to mitigate the hazards (and associated risks) that are <i>pre-existing</i> in the operational environment of the system concerned. These hazards are not caused by the system – rather, the main purpose of introducing the system is to eliminate those pre-existing hazards or at least maintain the associated risks at a tolerably low level.
---	---

	For an ATM/ANS system the <i>pre-existing hazards</i> and risks are generally those that are inherent in aviation and for which the main purpose of ATM/ANS is to provide as much mitigation as possible. Example of pre-existing hazards: ▪ <i>“a situation in which the intended trajectories of two or more aircraft are in conflict”</i> ▪ <i>“a situation where the intended trajectory of an aircraft is in conflict with terrain or an obstacle”</i>
	1. For guidance on the safety scoping and change assessment process, go to Guidance C of [1] 2. For guidance on describing the Operational Environment, go to Guidance B of [1] 3. For guidance on identifying pre-existing hazards, go to Guidance E of [1] 4. For guidance on setting Safety Criteria, go to Guidance D of [1] 5. A Safety Plan Template was developed [5] to enable the Solution to specify, <i>inter alia</i>, the safety assurance activities that are to be carried out. This Template is available on the Stellar SJU Extranet.

6 Application of the SRM: Safety assessment of SESAR Solution at operational level



The purpose of this section is to derive Safety Objectives under normal and abnormal operational conditions as well as under faulted conditions (case of failures internal to the ATM/ANS functional system in the scope of the Solution). This is the operational level specification of the Change introduced by the SESAR Solution from a safety point of view.

The Safety Objectives are specified at the operational level for three purposes:

- To capture what has to happen in order for the operational services to be delivered, in the defined operational environment, as required by the users – *i.e.* mitigation of the aviation pre-existing risks that are inherent to that operational environment
- To mitigate the consequences of failure / degradation of the operational services however caused
- To limit the frequency with which such failures / degradations of the operational services may occur so as to achieve a tolerable level for the associated system-generated risk, taking account of the above mitigations.

In the first two cases, the Safety Objectives to be achieved address the success approach as they express the *functionality & performance* and, in the third case, the failure approach as they indicate the acceptable level of frequency associated to failure. Taken as a whole, the Safety Objectives cover both the success approach and failure approach and have to be shown to satisfy the Safety Criteria. In all three cases, this includes only what has to be achieved at the operational level, from the service-users' perspective – this helps to ensure the completeness, correctness and consistency of the Safety Objectives without the unnecessary (at this level) detail of how, and by what or whom, the Safety Objectives will be achieved.

Last but not least, the Safety Objectives characterise the Change introduced by the SESAR Solution and as such they specify only what is new or modified.

Consequently, the following activities will be addressed (details in **Guidance A.2** of [1]):

- refined description of the operational services relevant to the Solution operations , and the derivation of Safety Objectives (success approach *i.e.* *functionality and performance*) in order to mitigate the pre-existing risks under normal conditions of the Operational Environment; the impacts of the Solution operations on adjacent airspace or on neighbouring ATM Systems need to be considered as well;
- assessment of the adequacy of the operational services under abnormal conditions of the Operational Environment and derivation of additional Safety Objectives (success approach), if appropriate,

- assessment of the adequacy of the operational services under faulted conditions (case of failures internal to the ATM/ANS functional system in the scope of the Solution) and derivation of Safety Objectives (failure approach)
- verification of Safety Objectives correctness and completeness¹⁴ by reference to the Safety Criteria
- Safety Objectives process verification

	1. <i>Operational Hazards are system-generated hazards defined at the level of the Operational services i.e. a level that is independent of the system design and is related to the failure of an operational service.</i> 2. At the core of the task related to the operational hazards is the FHA/OHA process, carried out on a representation of the system under consideration at the level of the operational service. For each operational hazard, there is a need to: ▪ assess the immediate operational effect(s) ▪ identify the possible mitigations in terms of defences to be implemented to protect against the risk-bearing consequences ▪ assess the severity of the mitigated effect(s), in accordance with the severity scheme in Guidance G of [1] ▪ allocate Safety Objective (failure approach, <i>i.e. integrity safety property</i>) in accordance with Guidance G of [1], in order to limit the frequency with which the operational hazard could be allowed to occur whilst ensuring that the Safety Criteria could be met. 3. To fully address the needs of the broader approach, SAM should be read in conjunction with the following text and section A.2 of [1] hereto
	1. A good starting point for identifying operational hazards is to ‘negate’ (i.e. apply failure modes) to the Safety Objectives derived with the success approach – <i>i.e.</i> asking what if Safety Objective #nn is not or wrongly achieved. 2. The safety assessment at operational level is often called safety assessment at OSED level.
	1. For guidance on the setting of Safety Objectives from the success approach , go to Guidance F of [1]

¹⁴ This would require in particular both the identification of appropriate safety validation objectives for the validation exercises as well as the use of the Severity and Risk Classification Schemes as promulgated by the companion Guidance Material.

	2. For guidance on the relevant Risk Classification Scheme (RCS) and Operational Hazard Severity Classification Scheme to be used to set Safety Objectives (failure approach), go to Guidance G of [1] 3. Further details of the FHA/OHA are given in the SAM [3] 4. A Safety Assessment Report (SAR) Template (SPR-INTEROP/OSED Part II document) was developed [6] to record the results of the safety assessment processes described in sections 6, 7, and 8. This Template is available on the Stellar SJU Extranet.
	As appropriate¹⁵, the Safety Assessment Report (SAR) (SPR-INTEROP/OSED Part II document) shall include: • a list of the key properties of the Operational Environment (or User Domain) that could have an effect on safety (from section 5) • the Safety Criteria and the justification for their selection (from section 5) • a description of the ATM/ANS at the level of the operational services • Safety Objectives, which set both the minimum positive, and maximum negative, safety contributions of the ATM/ANS system, at the level of the operational services and shall present the assurance that these outputs are complete and correct. Where a relative (or comparative) safety assessment is to be carried out, a description of the pre-change (or baseline) situation must also be included and the differences from the pre-change situation reconciled with the Safety Criteria.

¹⁵ What is 'appropriate' is given by the execution of the change assessment as part of the Safety Scoping and Change assessment process described in **section C** of [1].

7 Application of the SRM: Safety assessment of SESAR Solution at initial System design level



The Safety Requirements are design characteristics/items of the functional system to ensure that the system operates as specified. Based on the verification/demonstration of these characteristics/items, it could be concluded that the safety objectives, and consequently the safety criteria, are met.

At the initial System design level, the initial Safety Requirements are the means by which the Safety Objectives are achieved – for this reason they are derived from the proper allocation of the Safety Objectives on the elements of the initial System design. The SESAR SRM also requires the initial Safety Requirements to be shown to fully satisfy the Safety Objectives, it means that the former have the same scope as the latter and thereby necessarily cover the equipment, procedures, human and airspace elements of the functional system under consideration, and both the success and failure approaches.

The safety assurance activities, at the initial system design are listed below (more details in **Guidance A.3 of [1]**):

- description of the initial System design through design engineering representation (e.g. EATMA models, Logical model...) of the Solution system
- derivation of initial Safety Requirements from the Safety Objectives for the initial System design
 - analysis of the operation of the initial System design under normal conditions of the Operational Environment
 - analysis of the operation of the initial System design under abnormal conditions of the Operational Environment
 - assessment of the adequacy of the initial System design under faulted conditions (case of failures internal to the ATM/ANS functional system in the scope of the Solution) and hazard mitigation (i.e. prevent or minimize occurrence of operational hazards)
- verification of initial Safety Requirements correctness and completeness¹⁶ by reference to the Safety Objectives

¹⁶ This would require in particular both the identification of appropriate safety validation objectives, success criteria and associated measuring means in the validation exercises as well as the use of the risk assessment and mitigation as per SAM PSSA.

- Initial Safety Requirements process verification.

	1. At the core of the task related to the initial Safety Requirements from the failure approach is the PSSA process. It intends to demonstrate that the proposed system design can reasonably be expected to deliver the required functionality and performance and achieve the required level of integrity¹⁷ derived in the FHA/OHA. 2. To fully address the needs of the broader approach, SAM [3] should be read in conjunction with the following text and section A.3 of [1] hereto.
	The safety assessment at initial system design is sometimes called safety assessment at SPR level.
	1. For guidance on deriving Safety Requirements from the success approach , go to Guidance H of [1] 2. Details of the PSSA are given in the SAM [3].
	1. As appropriate (see footnote 15), the “SPR-INTEROP/OSED Part II (Safety Assessment Report)” shall include: • The initial Safety Requirements (<i>functionality and performance properties</i> from the success approach) that are necessary to satisfy the operational service-level specification i.e. the Safety Objectives (success approach) • The static and dynamic analysis to show that the initial System design will deliver this functionality and performance under all normal conditions of the operation environment that the system is expected to encounter in day-to-day operations • The static and dynamic analysis to show that the initial System design will deliver this functionality and performance under all abnormal conditions of the operational environment that the system may exceptionally encounter • The evidence that the initial System design is robust against (i.e. work through), or at least resilient to any varying conditions of the operational environment • The initial Safety Requirements (<i>integrity property</i> from the failure approach) that are necessary to satisfy the operational service-level specification i.e. the Safety Objectives (failure approach). and shall present the assurance that these outputs are complete and correct. 2. The SPR-INTEROP/OSED Part I and TS requirement’s sections shall include the applicable initial Safety Requirements derived during the safety assessment of the initial System design.

¹⁷ What is meant here is a Safety Objective (failure-approach) in terms of a hazard maximum tolerable frequency of occurrence (MTFoO) / probability, derived from the severity of its effect.

8 Application of the SRM: Safety assessment of SESAR Solution at refined System design level



The final stage of the SESAR industrial Research and Validation program covers the refined System design for a SESAR Solution addressing the pre-industrial development and integration phase.



1. The refined system design is the design with the lowest granularity for a SESAR Solution.
2. The refined system design encompasses technical elements, humans and procedures but for technical elements it does not aim to specify the physical design of the technical systems, functional blocks, functions and services which remains with industry.
3. Requirements derived at the refined system design level are called refined Safety Requirements compared to those derived at the initial System design level called initial Safety Requirements.

The safety assurance activities, at the refined system design level are listed below (more details in **Guidance A.4** of [1]):

- Refinement of initial Safety Requirements (*functionality and performance* from the success approach) for the refined System design (encompassing the corresponding refined system design representation through adequate design engineering models).
- Refinement of initial Safety Requirements (*integrity* properties from the failure approach) for the refined System design.
- verification of refined Safety Requirements correctness and completeness by reference to the related initial Safety Requirements (it is necessary at this stage to show, not only that the refined Safety Requirements are sufficient to ensure safety but also that these refined Safety Requirements are achievable in terms of timescale, cost, technical development, etc.).
- Refined Safety Requirements process verification.



1. The refined Safety Requirements are obtained by allocating the initial System design Safety Requirements (derived in **section 7**) on to the refined System design of the SESAR Solution (see **section 3.2.2** related to “SPR-INTEROP/OSED Part I” and **3.2.3** related to TS).
2. Similarly to the initial System design level, the derivation of the refined safety requirements from the failure-approach should be driven by the **PSSA process**.

	1. As appropriate (see footnote 15), the “SPR-INTEROP/OSED Part II (Safety Assessment Report)” shall include: • The set of refined Safety Requirements (success approach) for the refined System design that satisfy the initial Safety Requirements (success approach). • The set of refined Safety Requirements (integrity property from the failure approach) for the refined System design that satisfy the initial Safety Requirements (integrity property) • The evidence that refined Safety Requirements are capable of being satisfied in a typical implementation and shall present the assurance that these outputs are complete and correct. 2. The SPR-INTEROP/OSED Part I and TS requirement’s sections shall include the applicable refined Safety Requirements derived during the safety assessment of the refined System design.
---	---

9 Application of the SRM: Safety Management of VLD

9.1 Objectives of a VLD

The Very Large Scale Demonstrations cover the final part of SESAR 2020 Research and Innovation (R&I) Pipeline, as from TRL 6 to TRL7, as shown in **Figure 5** below:

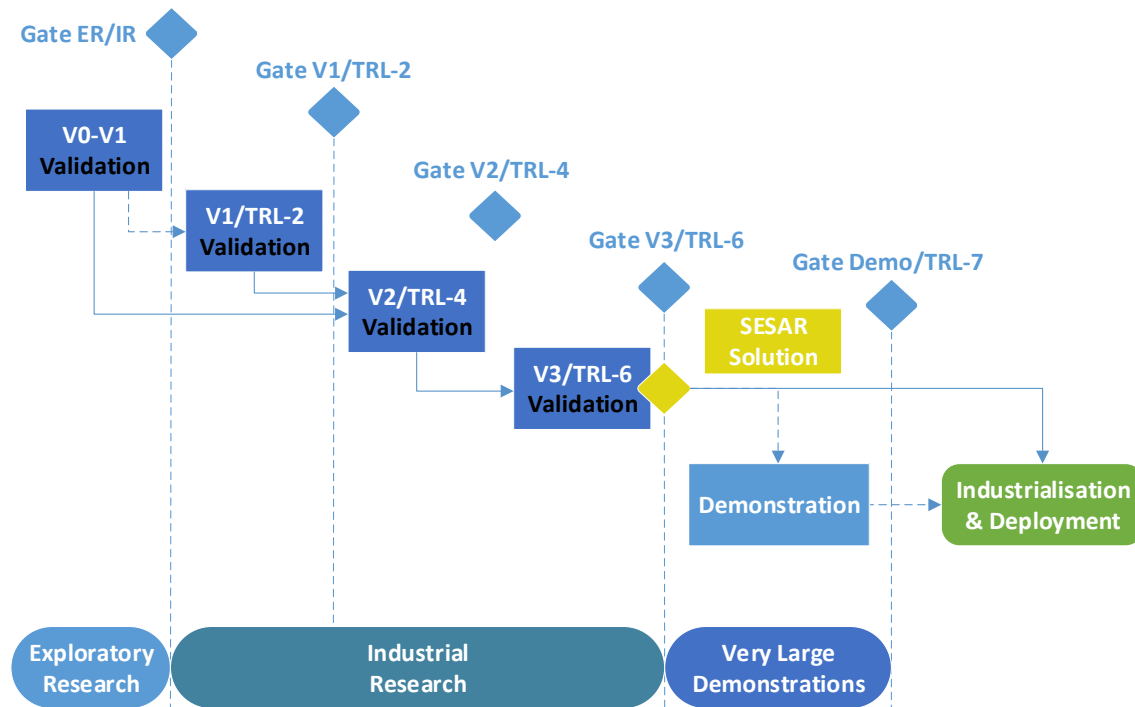


Figure 5: Gates and phases of SESAR Solution development life cycle

The Very Large Scale Demonstrations (VLD) are designed to help to fill the gap between the development and deployment phases and, in particular, to:

- Generate further confidence to support buy-in from main stakeholders including regulators for future deployments.
- Significantly reduce the business risks for both operational stakeholders and industry, in particular for changes included in the Common Projects.
- Provide further inputs to related standardisation activities.
- Raise awareness regarding SESAR activities related to ATM performance issues and their results.
- Accompany SESAR pioneers all the way to pre-deployment.
- To assess full-scale deployment readiness.

The VLDs consist mainly of wide scale live trials where the notion of Proof of Concept is essential. Indeed the Proof of Concept (PoC) to be conducted under a VLD is a confidence building exercise that comes in addition to the traditional validation required prior to certification and implementation of new concepts or new technologies. This has to be distinguished from operational live trials since it brings a new dimension of the validation – that is, early operations with a significant scale environment. In particular, in some occasions a VLD aims at providing inputs and influencing the work at global and regional standardisation level, within ICAO, EUROCAE and/or RTCA.

The PoC consists of an early operation of a SESAR Solution making use of pre-operational or operational products (airborne and ground) in a real operational environment. This includes the preparation and platform availability (ground and on-board) to support the demonstration in the targeted operational environment involving target audience end-users.

Notwithstanding the fact that a VLD is effectively a ‘technology’ demonstration, it still implies that ‘not fully tested’ ‘technology’ will be instantiated into operational – ground based and airside – Systems. The VLD must, therefore, be managed with safety as the primary concern. This includes both that the VLD delivers the required evidence to support the ongoing implementation of the concept being trialled and that the demonstration itself is conducted safely. Consequently local safety assurance which needs to be conducted to support the VLD is an essential part for the VLD safety demonstration. Both the local safety assurance and approval process are not necessarily within the remit of the SRM, but the material generated by the SRM process and the SRM per se (see sections 9.2 and 9.3 below as well as **Guidance N** of [1]) provide practical guidelines as support.

9.2 Scope of VLD safety assurance

The main objective of the safety demonstration is to show that ATS operations during the VLD, which might include participating and non-participating flights, are acceptably safe. The definition of what is acceptably safe must be defined for each VLD but it generally means that the already defined Safety Criteria relative to the SESAR Solution under VLD should be satisfied and that safety level of current ATS operations in the relevant airspace/airport is at least maintained when VLD are conducted.

To support this objective, the VLD safety assurance activities are twofold:

- i. Suitability of the SESAR Solution for the deployment:
 - ✓ The Solution under VLD delivers the foreseen safety performance for the required application/operation; and
- ii. Safety Impact of the VLD on current operations:
 - ✓ The VLD does not degrade to an unacceptable level the safety of the operations (e.g. with other surrounding operations and/or components of the ATM/ANS System)

As a result, the specific activities that must be considered are:

1. Documenting the current safety assurance status in order to make a decision on approval to move a SESAR Solution from a pre-industrialization stage to a ‘ready for VLD’ status. This includes ensuring that the findings of the safety assessment at V3 are fully accounted for and

- any safety issues not adequately addressed in the Solution System design are managed and adequately mitigated in the design of operational procedures, equipment and training before the VLD takes place;
2. Enabling the use of VLDs as a new dimension in the validation approach and providing further evidence as a support to standardisation. This includes, but is not limited to, (i) building and evaluating the VLD physical Solution System (that implements a major part of the design requirements whilst proposing work around solutions for those which are not feasible at this stage) against the refined System design in V3; (ii) the setting of appropriate safety validation objectives; and (iii) as a result preparation and availability of the VLD validation platform (ground and on board) to support the demonstration of the achievement / achievability of the safety validation objectives and Safety Requirements;
 3. Enabling significant levels of engagement and co-ordination of both the end-users (e.g. ANSPs, Network Manager, airports; airspace users, etc.) and appropriate Competent Authorities (National Authorities (NAAs; NSAs) and/or EASA) as fully detailed in [13];
 4. Determining and documenting in a Safety Plan (within the VLD DEMO Plan) the safety assurance to be conducted for the VLD encompassing the suitability of the SESAR Solution for the deployment and the safety impact of the VLD on current operations; and finally;
 5. Documenting the VLD Safety Case (within the VLD DEMO report). The VLD Safety Case is here a means of structuring and documenting a summary of the results of a VLD Safety Assessment addressing the suitability of the SESAR Solution for the deployment and the safety impact of the VLD on current operations

9.3 VLD Safety assurance

Each ANSP has approved safety assurance processes and procedures for the implementation of changes that are in accordance with the common requirements (1034/2011 & 1035/2011 and 2017/373 when applicable) and may have specific additional criteria contained within them to comply with other national legislation beyond just ensuring direct compliance. Each ANSP also has specific approved processes that are to be followed when the Competent Authority advises that they wish to review a planned safety-related change, in that case a VLD.

The ANSP Safety manager should decide, by expert judgement, the safety significance of the change based on the following criteria:

- a) failure consequence: credible worst-case scenario in the event of failure of the functional system under assessment for the VLD, taking into account the existence of safety barriers, such as safety nets or specific procedures, which may be outside the scope of the functional system;
- b) novelty used in implementing the change brought by the VLD: this concerns both what is innovative in the aviation sector, and what is new just for the organisation implementing the change;
- c) complexity of the change: the number of multiple functional systems and interfaces impacted, the number of stakeholders that the change is dependent upon;
- d) ability to monitor the change and take appropriate interventions;
- e) reversibility: what is the opportunity to revert to the previous functional system; and

- f) Inter-relationship with recent changes: assessing the significance of the change taking into account all recent safety-related modifications to the functional system under assessment and which were not judged as significant.

With this in mind, **Guidance N of [1]** has been produced in response to providers of air traffic services' requests for a guidance supporting a formalized, explicit and proactive approach to the systematic safety management of VLD. It is recommended to consider **Guidance N of [1]** in conjunction with **[13]**.

Guidance N of [1] seeks neither to replace local processes nor replicate **[13]**, which focuses on the collaboration and mutual linking between national authorities, providers of air navigation, manufacturers and airspace users involved in the VLD with the aim to support a co-ordinated certification / approval process. Rather it is intended to:

- i. provide a practical guide to safety assessment and assurance to the participant air traffic service providers who have to discharge their safety responsibilities properly; and
- ii. support an adequate level of safety assurance to obtain the necessary regulatory approval for the conduct of a VLD from Competent Authority (NSA and/or EASA).

The material is intended to apply to the full range of VLDs in SESAR 2020. It is, however, not intended to be prescriptive – rather it may be adopted and adapted for particular VLD applications as appropriate and necessary.

10 Document Information

10.1 References

- [1] Guidance to Apply the SESAR Safety Reference Material, Ed 00.03.01 (can be found on the Stellar SJU Extranet)
- [2] SJU, SESAR 2020 Wave 2 Programme Execution Framework - Project Hand-Book (can be found on the SJU Extranet)
- [3] EUROCONTROL, 2007, Air Navigation System Safety Assessment Methodology (SAM), SAF.ET1.ST03.1000-MAN-01, Edition 2.1
- [4] EC, EP3, D2.4.3-01, 2008, White Paper on the SESAR Safety Target, <http://www.episode3.aero/public-documents>
- [5] SESAR 2020 Solution Safety Plan Template (VALP Part II) (can be found on the Stellar SJU Extranet)
- [6] SESAR 2020 Solution Safety Assessment Report Template (can be found on the Stellar SJU Extranet)
- [7] EC/EUROCONTROL, E-OCVM Version 3.0 Volume I, February 2010
- [8] Accident Incident Models Release 2017 -Sept 2017 (can be found on the Stellar SJU Extranet)
- [9] P16.01.01, Validation / Verification of the SESAR Accident Incident Model (AIM), Edition 00.01.00, May 2014
- [10] SESAR Human Performance Assessment process V1 to V3 including VLD, Edition 00.02.00, April 2018 (can be found on the Stellar SJU Extranet)
- [11] P16.01.01b, Final Resilience Guidance Material for Safety Assessment (SRM) and Design, Edition 00.01.00, May 2016
- [12] EUROCONTROL, 2013, White Paper, 'From Safety-I to Safety-II.
- [13] SESAR P16.01.04, Final Guidance Material to Execute Proof of Concept, Ed00.04.00, August 2015
- [14] (EU) No 2017/373 of 01 March 2017 laying down common requirements for providers of air traffic management/air navigation services and other air traffic management network functions and their oversight, repealing Regulation (EC) No 482/2008, Implementing Regulations (EU) No 1034/2011, (EU) No 1035/2011 and (EU) 2016/1377 and amending Regulation (EU) No 677/2011

10.2 Acronyms

AIM	Accident Incident Model
ANS	Air Navigation Services
ANSP	Air Navigation Service Provider
ATC	Air Traffic Control
ATS	Air Traffic Service
ATM	Air Traffic Management
BM	Barrier Model
CFIT	Controlled Flight Into Terrain
CoP	Community of Practice
EASA	European Aviation Safety Agency
EATMA	European Air Traffic Management Architecture
EC	European Commission
ECAC	European Civil Aviation Conference
E-OCVM	European Operational Concept Validation Methodology
FHA	Functional Hazard Assessment
FOC	Final Operating Capability
HF	Human Factors
HP	Human Performance
IGS	Increased Glide Slope
IMC	Instrument Meteorological Condition
INTEROP	Interoperability requirements
IRV	Industrial Research & Validation
JU	Joint Undertaking
KPA	Key Performance Area

KPI	Key Performance Indicator
MAC	Mid Air Collision
NAA	National Aviation Authority
NSA	National Supervisory Authority
OCVM	Operational Concept Validation Methodology
OHA	Operational Hazard Assessment
OI	Operational Improvement
OSD	Operational Service & Environment Description
PoC	Proof of Concept
PSSA	Preliminary System Safety Assessment
RCS	Risk Classification Scheme
RE	Resilience Engineering
R&I	Research and Innovation
RWY	Runway
SAC	Safety Criteria
SAM	Safety Assessment Methodology
SAR	Safety Assessment Report
SAM	Safety Assessment Methodology
SE	System Engineering
SES	Single European Sky
SESAR	Single European Sky ATM Research programme
SJU	SESAR JU
SME	Subject Matters Expert
SO	Safety Objective
SPR	Safety & Performance Requirements

SR	Safety Requirements
SRM	Safety Reference Material
TA	Transversal Area
TMA	Terminal Manoeuvring Area
TRL	Technical Readiness Level
TS	Technical Specification
TWY	Taxiway
VAL	Validation
VALP	Validation Plan
VLD	Very Large Demonstration
WP	Work Package
WX	Weather

10.3 Definitions

The following definitions shall apply:

- a. 'abnormal conditions' are external changes in the operational environment that the ATM/ANS functional system may exceptionally encounter (e.g. severe WX, airport closure, etc.). When encountering such abnormal conditions, the system may be allowed to enter a degraded state provided that it can easily be recovered when the abnormal condition passes and the risk during the period of the degraded state is shown to be tolerable.
- b. 'achievable' shall mean that Safety Requirements are capable of being satisfied in a typical ATM/ANS functional system implementation, *i.e.* they do not impose unrealistic expectations on the design comprising people, procedures, hardware, software and airspace design. This includes feasibility in terms of timescale, cost, and technical development;
- c. 'air navigation services (ANS)' shall mean air traffic services; communication, navigation and surveillance services; meteorological services for air navigation; and aeronautical information services – as defined in Article 2(4) of Regulation (EC) No 549/2004;
- d. 'air traffic management (ATM)' shall mean the aggregation of the airborne and ground-based functions (air traffic services, airspace management and air traffic flow

management) required to ensure the safe and efficient movement of aircraft during all phases of operations – as defined in Article 2(10) of Regulation (EC) No 549/2004

- e. ‘argument’ shall mean statement or set of statements asserting a fact that can be shown to be true or false (by demonstration and evidence);
- f. ‘assurance’ shall mean the results of all planned and systematic actions necessary to afford adequate confidence an air navigation service or ATM/ANS functional system satisfies the Safety Criteria;
- g. ‘ATM/ANS’ shall mean air traffic management and air navigation services and covers all of the following: the air traffic management functions and services as defined in point (10) of Article 2 of Regulation (EC) No 549/2004; the air navigation services as defined in point (4) of Article 2 of that Regulation, including the network management functions and services referred to in Article 6 of Regulation (EC) No 551/2004, as well as services which augment signals emitted by satellites of core constellations of GNSS for the purpose of air navigation; flight procedures design; and services consisting in the origination and processing of data and the formatting and delivering of data to general air traffic for the purpose of air navigation; from Article 3 of Regulation (EU) N° 2018/1139
- h. ‘certification’ shall mean any form of recognition based on an appropriate assessment, that a legal or natural person, product, part, non-installed equipment, equipment to control unmanned aircraft remotely, aerodrome, safety-related aerodrome equipment, ATM/ANS system, ATM/ANS constituent or flight simulation training device complies with the applicable requirements of this Regulation and of the delegated and implementing acts adopted on the basis thereof, through the issuance of a certificate attesting such compliance – as defined in Article 3 of Regulation (EU) No 2018/1139;
- i. ‘degraded mode of operation’ is a reduced level of operational service invoked by abnormal conditions, equipment outage or malfunction, or staff shortage.
- j. ‘design’ shall mean an engineering representation of an air navigation system to be built. The design may be expressed in different ways during the various phases of the development lifecycle;
- k. “design engineering model” shall mean a high-level architectural representation of the ATM/ANS functional system design that is entirely independent of the eventual physical Implementation of that design. This model describes the main human tasks and machine-based functions and explains what each of those “actors” provides in terms of functionality and performance. The model normally does not show elements of the physical design, such as hardware, software, procedures, training etc. – nor does it separately represent human-machine interfaces explicitly, these being implicit in every link between a human and machine actor;
- l. ‘evidence’ shall mean information that establishes the truth (or otherwise) of an argument. Wherever possible, it should consist of proven facts – e.g., the results of a well-established process such as simulations and testing. Only where such objective information is not available should it be based on expert opinion;

- m. 'functional system' shall mean a combination of equipment, procedures and human resources organised to perform a function within the context of ATM/ANS;
- n. 'hazard' shall mean any condition, event, or circumstance which could induce an accident. This covers both pre-existing aviation hazards (not caused by ATM/ANS functional systems) and new hazards resulting from the failure of the ATM/ANS functional systems.

As per the SRM, this definition relates to a broader interpretation of what a hazard is. It addresses two types of hazards: "pre-existing", which the ATM/ANS functional system has to mitigate; and (ii) "system-generated" hazards, resulting from the failure of the ATM/ANS functional system. In SRM the "system-generated" hazards defined at the operational level (level of the operational services i.e. a level that is independent of the system design) are called "operational hazards".

In Regulation (EU) No 2017/373, hazards are relative to (a) new hazards introduced by the change (failure of the functional system and normal operation of the functional system) and (b) already existing hazards that are affected by the change (related to the existing parts of the functional systems or hazards outside the functional system, for example, those inherent to aviation).

- o. 'implementation' shall mean the realisation of design in the form of the built and tested air navigation system prior to its transfer into operational service;
- p. 'integrity' shall mean the ability of a system, under all defined circumstances, to provide all the services (or functions) required by the users, with no unintended or uncommanded services (or functions). It is based on the logical completeness and correctness, and reliability, of the ATM/ANS functional system elements in relation to user / operator requirements. Incorrect (error or omission) specification, design or implementation falls within this definition of (lack of) integrity.
- q. 'normal conditions' are those conditions of the operational environment the ATM/ANS functional system is expected to encounter in day-to-day operations and for which the system must always deliver full functionality and performance.
- r. 'operational hazard' is a "system generated" hazard defined at the operational level (level of the operational services i.e. a level that is independent of the system design) and describing the failure of an operational service
- s. 'operational level' is used herein as the highest level at which the safety properties of the ATM/ANS system are specified – see 'Operational Specification' below.
- t. 'operational service' is what exists at the interface between the ATM/ANS Functional System and the Airspace Users. Operational services are provided by the ATM/ANS Functional System to the User i.e. an aircraft or a group of aircraft.
- u. 'operational specification' shall mean the specification of the operational services i.e. what the ATM/ANS functional system has to provide across the interface between the service provider and service user in order that User Requirements can be satisfied; such a specification takes a "black-box" view of the system, at the operational level (service level).
- v. 'positive contribution to aviation safety' shall mean the contribution of air navigation services to the reduction in pre-existing accident risks that are inherent in aviation;

- w. 'precursors' shall mean the conditions, events, and sequences that precede and lead up to accidents and/or serious incidents. Skybrary provides the following definition: "A *precursor* is an occurrence that remained an incident but that might recur in different conditions and become an accident";
- x. 'pre-existing risks' shall mean the risks that are inherent in aviation. They are not associated with failure of the air navigation services / system - rather it is the primary purpose of air navigation services to reduce these risks wherever possible;
- y. 'process' shall mean a set of interrelated or interacting activities which transform inputs into outputs;
- z. 'rationale' shall mean the explanation of the logical reasons or principles employed in consciously arriving at a conclusion concerning safety. Rationales usually document (1) why a particular choice of argument was made, (2) how the basis of its selection was developed, (3) why and how the particular information or assumptions were relied on, and (4) why the conclusion from the evidence is deemed credible or realistic;
- aa. 'reliability' shall mean the ability of a system/element to perform a given function within a certain period of time without failure.
- bb. 'resilience' shall mean the intrinsic ability of the ATM/ANS functional system to adjust its functioning and performance goals, prior to, during, or following varying conditions.
- cc. 'risk' shall mean the combination of the overall probability, or frequency of occurrence of a harmful effect induced by a hazard and the severity of that effect – as defined in Regulation (EU) No 2017/373;
- dd. 'risk assessment' shall mean a sub-process in the overall safety management process to determine a priori the quantitative or qualitative value of risk related to the provision of air navigation services for a specific operational environment;
- ee. 'safety Assessment' as per the SRM coverage (lifecycle) means an *a priori* risk assessment and mitigation of changes to the ATM/ANS functional system
- ff. 'safety Assurance' means all planned and systematic actions necessary to provide adequate confidence that a product, a service, an organisation or a functional system achieves acceptable or tolerable safety;
- gg. 'safety assurance objective' shall mean a goal (or similar) that has to be achieved in order to satisfy a higher-level safety Argument.
- hh. 'safety Criteria' shall mean explicit and verifiable criteria, the satisfaction of which results in tolerable safety following the change. They may be either qualitative or quantitative and either absolute or relative. They include not just specific risk targets but also safety (and other) regulatory requirements, operational and equipment standards and practices;
- ii. 'safety Objective' shall mean the functional, performance and integrity safety properties of the air navigation system, derived at the operational level. Safety Objectives describe what the air navigation system has to provide across the interface between the service provider and service user in order that the Safety Criteria are

satisfied. They provide mitigation of the pre-existing risks; and limit the risks arising from failures within the air navigation system. As objectives, they should specify what has to be achieved – how it is achieved is covered by Safety Requirements;

This definition relates to a broader interpretation of what a hazard is as per definition n above. As a consequence, the Safety Objectives have to provide mitigation of the pre-existing hazards as well as mitigations of the system-generated hazards derived from the service-level failure analysis.

Safety Objectives as defined in the SRM correspond to the highest layer of Safety Requirements as defined in Regulation (EU) N° 2017/373. The highest layer of Safety Requirements represents the desired safety behaviour of the change at its interface with the operational context.

- jj. 'safety performance' shall mean the performance of relevant and measurable safety indicators whereby the required Safety Criteria will be fully achieved and maintained during the operational lifecycle;
- kk. 'safety requirement' shall mean design characteristics/items of the functional system to ensure that the system operates as specified; - as defined in Regulation (EU) N° 2017/373;
- ll. 'Service Model' shall mean a way of representing an ATM/ANS functional system/operational concept at the level of the operational service. In the SRM, this is being achieved by the Barrier Models used in AIM. AIM models show how the ICAO-defined layers of ATM (and sub-layers thereof) can make a positive and negative contribution to aviation safety;
- mm. 'system-generated hazard' shall mean a hazard which result from failure of the ATM/ANS functional system ;
- nn. 'transition' shall mean the process of changing over the provision of air navigation services from the old (pre-change) functional system to the new functional system. It includes removal of redundant legacy systems;
- oo. 'User Requirements': User(s) in this context are the user(s) of the air navigation service(s) concerned. In general, User Requirements are user's expectations in their domain of operation. From a safety viewpoint, the User Requirements are generally the Safety Criteria;
- pp. 'validation' shall mean an iterative process by which the fitness for purpose of a change to the ATM/ANS functional system or operational concept being developed is established (from E-OCVM 3);
- qq. 'verifiable' shall mean satisfaction of Safety Requirements can be demonstrated by direct means (e.g. testing, simulations, modelling, analysis, etc.), or (where applicable) indirectly through appropriate assurance processes.

-END OF DOCUMENT-