SESAR
JOINT UNDERTAKING

Horizon 2020
European Union Funding
for Research & Innovation

SESAR Joint Undertaking (SJU)

Project Execution Guidelines for SESAR 2020 VLD demonstrations awarded under Open Calls

Very Large-Scale Demonstration

Version 1.00.00
6 December 2016

Founding Members
EUROPEAN UNION EUROCONTROL

Authoring & Approval

Authors of the document

Name	Position/Title	Date
Julie Ibalot	Master Planning expert	02/12/2016

Approved By

Name	Position/Title	Date
Benoit Fonck	Chief Development & Delivery	06/12/2016
Alain Siebert	Chief Economist & Master Planning	06/12/2016

Document History

Edition	Date	Status	Author	Justification
00.01.00	02/12/2016	Consolidated draft	J. Ibalot	Initial draft
01.00.00	05/12/2016	Final version	J. Ibalot	

Project Execution Guidelines for SESAR 2020 Very Large Scale Demonstrations

Abstract

This document provides guidance to consortia members on the way they have to fulfil the project management requirements set out by the SESAR Joint Undertaking in the context of the SESAR 2020 VLD activities awarded through open calls.

Table of Contents

1 Introduction

1.1 Purpose of the Document

This document provides guidance to beneficiaries of Grant Agreements that result from SESAR 2020 VLD Open Call for Proposals on the way they are expected to fulfil the project management requirements during project execution.

This is required to allow the SJU to run the Programme and to monitor and control the projects across SESAR 2020 Pillars and will enable the transition of results from Research and Innovation towards the deployment phase.

There are two types of VLD projects inside the SESAR Programme:

- VLD under R&I programme awarded through the industrial partnership conducted by SESAR Members;
- VLD projects awarded through open calls.

This Guidance document applies to the second category, VLD projects awarded through an open call. In this category of VLD projects we can find projects which are linked to other existing projects for which specific procedures and arrangements (cf. §2.3)

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 1.

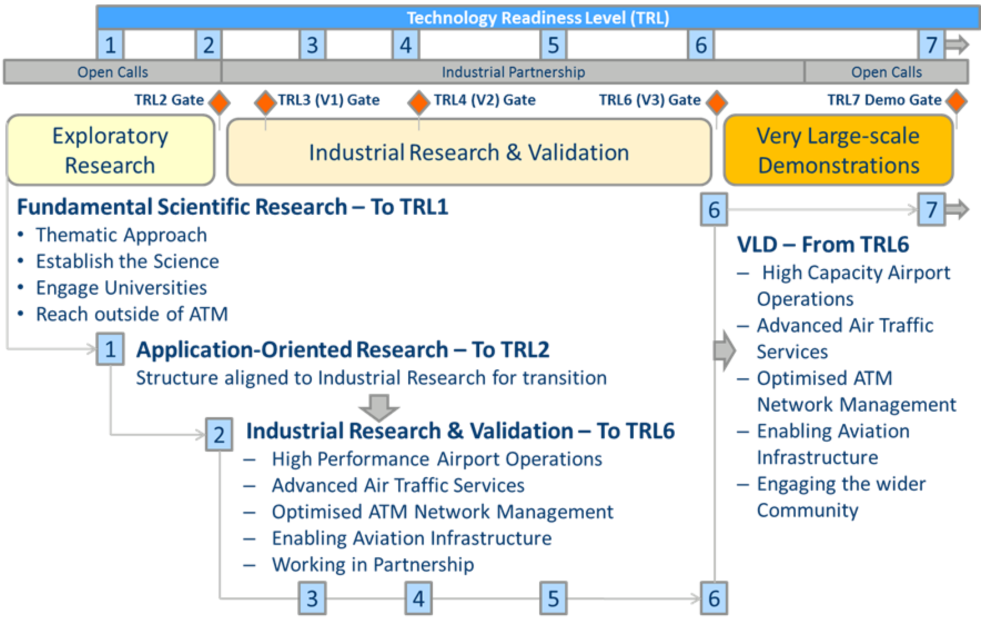

Technology Readiness Level (TRL)
1
2
3
4
5
6
7
Open Calls
Industrial Partnership
Open Calls
TRL2 Gate
TRL3 (V1) Gate
TRL4 (V2) Gate
TRL6 (V3) Gate
TRL7 Demo Gate
Exploratory Research
Industrial Research & Validation
Very Large-scale Demonstrations
Fundamental Scientific Research – To TRL1
• Thematic Approach
• Establish the Science
• Engage Universities
• Reach outside of ATM
1 Application-Oriented Research – To TRL2
Structure aligned to Industrial Research for transition
2 Industrial Research & Validation – To TRL6
– High Performance Airport Operations
– Advanced Air Traffic Services
– Optimised ATM Network Management
– Enabling Aviation Infrastructure
– Working in Partnership
3
4
5
6
6
7
VLD – From TRL6
– High Capacity Airport Operations
– Advanced Air Traffic Services
– Optimised ATM Network Management
– Enabling Aviation Infrastructure
– Engaging the wider Community

Fig. 1: Exploratory Research within SESAR 2020 R&I Pipeline

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.

1.2 Acronyms and terminology

Term	Definition
CAA	Civil Aviation Authority
CFS	Certificate on the financial statement
EASA	European Aviation Safety Agency
EC	European Commission
ER	Exploratory Research
EUROCAE	European Organisation for Civil Aviation Equipment
GA	Grant Agreement
H2020	Horizon 2020
ICAO	International Civil Aviation Organization
MGA	Model Grant Agreement
NAA	National Aviation Authority
NSA	National Supervisory Authority
R&I	Research and Innovation
RIA	Research and Innovation Action
SESAR (2020)	Single European Sky ATM Research Programme (2020)
SJU	SESAR Joint Undertaking
SME	Small and Medium Entreprise
TRL	Technological Readiness Level
VLD	Very Large Scale Demonstrations

2 SESAR 2020 Guidelines adapted to VLD activities

The set of SESAR 2020 project management requirements that are applicable to the VLD projects are those required to comply with the H2020 processes defined in the Annotated Model Grant Agreement (Ref [3]) which derive from best practices in Project Management.

This document focusses on a limited set of H2020 processes that are considered essential for the SESAR 2020 VLD activities, and provides additional SESAR project management guidelines.

It should be noted that the H2020 documentation related to Research and Innovation Actions (RIA) maintained by the EC and published through the H2020 Participants Portal is fully applicable to the VLD projects. Most of the guidelines presented in this document are common to guidelines for VLD projects conducted through the industrial partnership, with some differences specific to VLD awarded through opens calls.

2.1 Key principles applicable to VLD activities

This document provides an overview of the SESAR 2020 Programme Execution Framework applicable to VLD projects awarded through open calls and targets stakeholders participating to SESAR 2020 call for tender.

Safety requirements

As far as safety is concerned, VLD projects should follow the following safety guidance to facilitate approval with the support of EASA:

- SESAR Safety Reference material (Reference [6] SESAR Safety Reference Material, Guidance to Apply the SESAR Safety Reference Material);
- Proof of concept (Reference [5] Final Guidance Material to Execute Proof of Concept).

The Proof of Concept to be conducted under these VLD activities is a dedicated guidance stemming from Safety methodology. It 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.

The Proof of Concept has to be distinguished from operational live trials since it brings a new dimension of the validation: early operations with a significant scale environment.

The proof of concept consists in an early operation of the SESAR Solutions making use of pre-operational or operational products (airborne and ground) in a real operational environment.

To this end, the use of pre-operational products can be envisaged, opening the door for tailored design solutions and tailored certification processes to support the demonstration. But in all cases, full compliance against relevant regulation has to be shown. A revenue flight with pre-operational airborne and/or ground products means that these products are "certified" against the applicable regulations.

Applicable Requirements for Ground part:

The stakeholders participating to VLD shall demonstrate to his National Aviation Authority or Competent Authority that the use and/or failure of this "early" SESAR operational capability will not create unacceptable risk for ATM or airport operation. The results of this risk assessment might lead to necessitate under certain circumstances reversion to the baseline situation (normal operations) and as such this reversion shall be demonstrated to be safe for the ATM or airport operation. A Declaration of Verification/Conformity/Suitability for use for the ground system could be required when ATM operation is impacted by the VLD.

Applicable Requirements for Airborne part:

Any new equipment to be used in the VLD will have to go through a full certification review process to ensure compliance with the applicable certification specification (e.g. CS-25/CS-23/CS-27/CS-29, subpart F). But, assessing this compliance, a more realistic intended use of this equipment will be considered. This might bring some technical challenges that will have to be solved on a case by case basis between the (Supplemental) Type Certificate holder and EASA during the certification review process.

The impact of this reversion at aircraft and ground level will have to be addressed in a timely manner (prior to the execution of demonstration exercises) as it may result in additional design requirements (airborne & ground) specific to the VLD.

For the sake of convenience, EASA can facilitate the coordination of VLD approvals and Authorities involvement with the different Aviation Authorities (NAAs, NSAs CAAs):

- Identifying specific applicable VLD requirements, means of compliance and guidance material
- Facilitating coordination between the relevant Authorities during the different phases of the VLD, in particular during the preparation and the approval.

Link to standardisation and regulatory activities

The airborne and ground systems required to support the platform development for this demonstration should be based on existing standards and regulatory framework where applicable. In the case where an update or amendments are envisaged to the standard or the regulation, the project should coordinate with the relevant standardisation body (e.g. EUROCAE, EASA, ICAO) and provide feedback and any relevant material (e.g. demonstration report) to the involved relevant group. Appropriate participation to the group should be envisaged by the project team.

Performance framework

The results of the projects should include an assessment of the performance benefits following the performance framework applicable within SESAR 2020 programme. As such, the methodology and the performance indicators should be aligned with S2020 performance framework. Further details and supporting documents will be provided by the programme manager at the kick off meeting.

Communication aspects

Each VLD project shall develop and implement a robust communication plan as each SESAR labelled VLD platform should be considered as the global "vitrine" for European leadership in ATM. The key headline to articulate the communication plan is "seeing is believing". To that end the communication plan should acknowledge the need to reach out a broad ATM community. This will help building further confidence on the readiness for larger scale deployment of the targeted SESAR solutions. The communication plan will enable the project to promote its results by providing targeted information to relevant audiences in a strategic and effective manner (cf. section 4).

Ethics requirements

If Ethics requirements have been identified during the proposal evaluation, the project will identify the project's Ethics focal point, provide an overview of the ethics requirements, and make reference to the Ethics deliverables to be produced.

Efforts

In addition to the resources required for the execution of the Projects activities, a need to support relevant coordination activities (e.g. input to standardisation bodies, link with regulatory authorities/EASA) should be identified and planned.

2.2 Deliverables

For each VLD project awarded, the contractual deliverables are as follow:

- a Demonstration Plan which must be transferred to SJU T0+3 months (T0 is the starting date of the Grant);
- quarterly reports;
- a Demonstration Report which must be submitted to SJU at least 2 months before the end of the project/Grant.

All deliverables should follow a SESAR template which will be delivered by the Programme Manager at the project Kick-off Meeting.

Both demonstration plan and demonstration report are publishable.

The main items to consider in the Demo Plan or in the Demo Report are :

1 Executive summary

2 Introduction (Purpose of the document and Scope)

3 Very Large Demonstration (VLD) (Scope ; Purpose; SESAR Solution(s) addressed by VLD)

4 (*Demo Plan*) Project Management (Objectives, Related SESAR Solution(s) reference data pack(s); Content Development and Integration Approach; Project Management and Organisation)

or

(*Demo Report*) Demonstration Results (detailed analysis of the results per demonstration objective; confidence in results)

5 Relations to other projects (Dependencies on other projects)

6 (*Demo Plan*) Demonstration Plan (Demonstration Approach; Stakeholder's expectations; Operating method description; Demonstration Objectives and Assumptions, Exercises Planning; Exercise description and scope; Reference Scenario(s)

Or

(*Demo Report*) Conclusions and Recommendations (considering the industrialisation, standardisation, deployment)

7 Communications and Dissemination (Objectives and Strategy; Project High Level Messages; Target Audience Identification; Schedule of communication and dissemination activities)

8 Reference Documents

Appendix A Safety Plan or Safety Report

Appendix B Security Plan or Security Report

Appendix C Human Performance Assessment Plan or Human Performance Assessment Report

2.3 Specificities applicable to VLD projects linked to existing projects awarded through another call

There are some VLD projects which are linked to existing VLD projects and an appropriate coordination is required to ensure the success of the demonstrations as valuable bridge between development and deployment.

The SESAR JU will set up a dedicated platform to allow these projects to coordinate and share information as necessary.

2.4 Usage of H2020 Participants Portal application

SESAR 2020 VLD projects will have the obligation to use the H2020 Participants Portal application for all project related activities, such as:

- Submission of project deliverables (section 4.1);
- Periodic (once a year) Technical & Financial Reporting (section 4.3);
- Final Periodic Technical & Financial Reporting (section 4.4);
- Quarterly Progress Report (section 4.5)
- Risk & Issues Management (section 4.6);

- Requests for Amendments (Section 4.7);
- Implementation of Ethics Requirements (Section 4.8);
- Submission of Final Project Results Report (Section 4.9).

Further information on how to use the Participants Portal application during the project lifetime can be found in H2020 Participants Portal Online Manual (Ref [2]).

3 Communication and Dissemination Activities

3.1 Communication Plan

Beneficiaries must promote the project and its results, in accordance with Article 38.1 of the SJU Model Grant Agreement (Ref [4]). Therefore, a Communication Plan was already foreseen in the proposal, which may need further elaboration in the Demonstration Plan.

The Communication Plan shall define clear objectives and set out a concrete strategic planning for the communication activities (including a description and timing for each activity throughout the project duration).

3.1.1 Content

The Communication Plan is expected to include the following elements:

- Name and contact details of project communications point of contact;
- Communication objectives;
- Several high-level messages about the project, referring to the benefits that the project is expected to bring (these messages should be updated by the end of the project);
- Short “About” project description (max 15 lines) in language suitable for non-experts;
- A calendar of planned communications activities;
- Metrics (including analytics of press coverage, website and social) used for measuring success of the communication activities.

3.1.2 Key Communication activities per target audience

The Communication Plan is expected to foresee at least activities relating to:

SESAR ATM Community:

- Participation at SESAR demonstrations event (e.g. posters, presentation, demonstrators, reports);
- When required, organisation of dedicated workshops to present the project’s results to the SESAR community and get feedback from domain experts, aiming at incorporating the feedback into the project activities;

General Public:

- Web communication: presence on Corporate Web site of the project partners, presence on the social networks (optional), creation of project website where the abstracts of project deliverables and publications can be made available with a regular update (recommended);
- Other communications on project objectives and results through general press, e-magazines, brochures, news, interview opportunities with the media and dedicated press releases, aimed at raising interest and increasing knowledge to the general public (optional).
- Any communication activity that is expected to have a 'major media impact', i.e. media coverage (online and printed press, broadcast media, social media, etc.), that will go beyond a local impact and which could have the potential for national and international outreach must be first notified to the SJU.

Information given may not include classified or restricted results (cf. Article 37 of the SJU Model Grant Agreement (Ref [4]).

Please note that Communication activities are taken into consideration during the evaluation as part of the criterion "impact".

For further guidance please refer to Article 38.1 of the Annotated Model Grant Agreement (Ref [3]).

3.2 Visibility of EU funding

In accordance with Article 38.2 of the SJU Model Grant Agreement (Ref [4]), beneficiaries shall, during the project and afterwards, ensure the visibility of EU funding for any communication activity related to the project and on any major result (including prototypes) funded by the grant, by:

- displaying the EU and the SJU logos (on the project deliverables, presentations, website, etc..);
- including the reference to EU funding set out in the Grant Agreement;
- including relevant disclaimers.

For further guidance please refer to Article 38.1 of the Annotated Model Grant Agreement (Ref [3]) and to the guidance provided below.

3.3 SESAR 2020 Very Large Scale Demonstration Word Templates

All Project deliverables will comply with a SESAR 2020 VLD Word Template that will be delivered by the Programme Manager at the project Kick-off Meeting.

The following general communication guidelines will apply:

- In the page footer the name of the copyright owner shall be inserted by the beneficiaries based on their legal assessment, in line with their contractual arrangements governing the intellectual property rights (IPR). In case the beneficiaries wish that the copyright disclaimer is used also in the communication activities by the SJU, they shall provide the SJU with their wording.

- The following disclaimer shall be used as a footnote to the introduction: "The opinions expressed herein reflect the author's view only. Under no circumstances shall the SESAR Joint Undertaking be responsible for any use that may be made of the information contained herein."
- The size of the project logo in the page header shall not exceed the size of the SESAR logo.
- If required company logos can be inserted on the last page of the document. As a general rule, when displayed together with another logo, the EU emblem must have appropriate prominence.

3.4 SESAR 2020 Very Large Scale Demonstration Presentation Template

All Project presentations to be provided to the SJU and to an external audience (workshops, conferences, dissemination events in general) will comply with a SESAR 2020 Very Large Scale Demonstration PowerPoint Template that will be delivered by the Programme Manager prior to the project Kick-off Meeting.

The following general communication guidelines will apply:

- If required, the following copyright note can be added to the slide footer: "© – [year] – [name of the copyright owner]. All rights reserved. Licensed to the SESAR Joint Undertaking under conditions."
- The name of the copyright owner shall be inserted by the beneficiaries based on their legal assessment, in line with their contractual arrangements governing the intellectual property rights.
- In case the beneficiaries wish that the copyright disclaimer is used also in the communication activities by the SJU, they shall provide the SJU with their wording.
- The size of the project logo in the slide header shall not exceed the size of the SESAR logo.
- If required company logos can be added on a separate slide.

As a general rule, when displayed together with another logo, the EU emblem must have appropriate prominence.

3.5 SESAR demonstrations event "Seeing is believing"

Demonstrations projects are expected to last approximatively 2 years. Within this timeframe the SESAR JU, supported by its Members expects to organize a communication event to promote the demonstration activities.

All VLD projects are expected to be represented and give a short presentation on the objectives and status of the demonstrations they are conducting.

3.6 Coordination with SJU Communications Sector

To ensure consistency with the SESAR brand, project consortia are requested to contact the SJU Communications Sector when preparing Communication and Dissemination activities.

The following SJU email address will be used: communications@sesarju.eu.

4 Project Execution

4.1 Submission of Project Deliverables

All Project deliverables (quarterly reports as well as Demonstration Plan and Demonstration report) will be handed over for SJU assessment by uploading them (Ref [2]) on the dedicated project page on H2020 Participant Portal.

It should be noted that the Periodic Technical and Financial Reports are not project content related deliverables; therefore they should not be included in the list of project deliverables. However they need to be planned in the Management Work Package.

Based on the fact that the effort spent after the Closure Meeting will not be eligible, all project deliverables and in particular the Demonstration Report will have to be submitted for approval at the latest two months before the Closeout meeting.

4.2 SJU Assessment of Project Deliverables

The SJU assesses the handed-over deliverable with special emphasis on the validity of its content, alignment with commitments, internal consistency and compliance with the relevant contractual provisions set forth in the grant agreement, compatibility with SJU obligatory material (e.g. templates) and other SESAR programme management documents and guidelines as detailed in the present paper.

The SJU aims to evaluate a deliverable within 60 days from the delivery, and may:

- Accept it in writing, in whole or in part, or make acceptance of the deliverable subject to certain conditions;
- Request in writing certain clarifications or additional information, as appropriate. The Consortium shall answer the SJU's request within 15 days from receipt of the SJU's request for clarifications or additional information. If, upon receipt of the clarification or additional information, the SJU does not respond within 30 days, this clarification or additional information shall be deemed accepted.
- Reject it by giving the appropriate justification in writing.

Following the SJU assessment of a project deliverable, the status of acceptance can be:

- Accepted (No Reservation)

  This means that the SJU does not have significant comments and there is no need for the project to produce an improved version of the deliverable. The deliverable will be marked in the Participants Portal as accepted.

- Reservations (Reservations requiring clarifications/revision)

  This means that the SJU has significant comments and there is a need for the project to produce an improved version of the deliverable. The deliverable will be marked as “re-opened” on the Participants Portal, which will allow the project to re-submit this deliverable.

- Rejected (Critically deficient)

  This means that the SJU considers the deliverable of insufficient quality and/or not in line with the deliverables foreseen in the grant. In this case the project is not expected to resubmit an improved version of the deliverable. The deliverable will be marked as ‘Rejected’ in the Participants Portal and the project will not be able to re-submit a new version of this deliverable. There will be implications for the eligible cost of the grant execution.

The status of the deliverable acceptance will be considered in the related Periodic Technical/Financial Report. When relevant, it may lead to suspension of some payments in line with the SJU MGA chapter 6 (Ref [4]).

4.3 Periodic Technical/Financial Reporting

A Periodic Technical and Financial Progress Report shall be submitted via the H2020 Participant Portal (Ref [2]) following each reporting period (every twelve months), at latest within 60 days following the end of the Reporting Period.

The content of the Technical and Financial Progress Reports is detailed in the H2020 User Manual (Ref [2]). Although an overview is provided below, the latest version of the H2020 User Manual remains the reference.

4.3.1 Periodic Technical Report

A Technical Progress Report shall provide a qualitative summary of the work performed according to H2020 guidelines (Ref [2]). It consists of Part A and Part B:

Part A contains:

- the cover page
- a publishable summary, including :
  - ➢ An executive statement on the progress made and key issues;
  - ➢ Achievements made in the last reporting period, i.e. milestones, meetings, and tasks key data;
  - ➢ Main targets and events over the next reporting period.
- Tables covering issues related to the project implementation (e.g. Work Packages, Deliverables, Milestones, etc.) which includes:
  - ➢ Deliverables (indicating the % completion of deliverables)

- ➢ Milestones
- ➢ Ethical Issues (if applicable)
- ➢ Critical implementation risks and mitigation measures
- ➢ Dissemination & exploitation of results
- ➢ Impact on SMEs (if applicable)
- ➢ Open Research Data (if applicable)
- ➢ Gender

- The answers to the questionnaire covering issues related to the project implementation and the economic and social impact, notably in the context of the Horizon 2020 key performance indicators and the Horizon 2020 monitoring requirements.

Part A is generated via the Participant Portal based on the information entered by the participants through the periodic report and continuous reporting modules. The participants can update the information in the continuous reporting module at any time during the life of the project.

Part B contains:

Part B of the periodic technical report provides the narrative part that includes explanations of the work carried out by the beneficiaries during the reporting period. It will include:

- ➢ Explanations of the work carried out by all beneficiaries and linked third parties during the reporting period;
- ➢ An overview of the progress towards the project objectives, justifying the differences between work expected under Annex I and work actually performed, if any;
- ➢ An update on Risks and Issues.

Part B needs to be uploaded as a PDF document. It must be consistent with the template of Part B Periodic Technical report to be provided by the SJU.

4.3.2 Periodic Financial Report

A Financial Progress Report shall be submitted following each reporting period (every twelve months) via the H2020 Participant Portal (Ref [2]) jointly with the Technical Progress Report.

The periodic financial report consists of:

- Individual financial statements (Annex 4 to the GA) for each beneficiary;
- Explanation of the use of resources and the information on subcontracting and in-kind contributions provided by third parties from each beneficiary for the reporting period concerned;
- A periodic summary financial statement including the request for interim payment.

4.4 Final Periodic Technical/Financial Report

The Final Report covers the whole project and is composed of a Final Technical and a Final Financial part. It is delivered as soon as possible, at latest within 60 days from the completion of the Action.

In case not all deliverables have been delivered in time before the completion of the Action, the Project may ask for an extension, as an exception, using the Amendment procedure.

4.4.1 Final Periodic Technical Report

The Final Periodic Technical Report is a publishable summary of the entire project, it provides:

- An overview of the project scope and objectives
- The achieved results and main conclusions, including a self-assessment of the TRL (Technology Readiness Level) achieved at the end of the project.
- The performed communication and dissemination actions
- The Exploitation and follow-up activities proposed for the next stage (deployment).
- The socio-economic impact of the project
- An up-to-date link to the project website
- Project logos, diagrams, photographs and videos illustrating its work (if available).

The final summary must be written in a style understandable for a non-specialist audience. The coordinator must ensure that none of the material submitted for publication includes confidential or 'EU classified' information.

4.4.2 Final Periodic Financial Report

The Final Periodic Financial Report includes:

- The final summary financial statement that is automatically created by the system (consolidating the data from all individual financial statements for all beneficiaries and linked third parties, for all reporting periods) and that constitutes the request for payment of the balance;
- In some cases (and for some beneficiaries/linked third parties) it must be accompanied by a certificate on the financial statements - CFS (one certificate per beneficiary/linked third party).

4.5 Quarterly Progress Report

The objective of Quarterly Progress Reporting process is to allow monitoring in a qualitative and quantitative manner the progress and the forecast of the Projects including the status of their risks and issues. This process has been introduced by the SJU in order to have a more regular view on the programme progress than the Horizon 2020 Reporting would provide.

Quarterly Progress Reports will have to be produced and submitted to Horizon 2020 Participant Portal.

The content of the reporting can be summarised as follows:

- A summary status that gives an executive statement on the progress made since the last report and on key issues;
- Achievements made in the last reporting period and any corrective actions;
- Effort spent in the past quarter per beneficiary and work package.
- Issues that are being handled (including their recovery status);
- Top 5 risks in order of criticality and/or priority;
- Activities and achievements planned in the next Quarter;
- Updated project schedule.

4.6 Risks and Issues Management

Risks are potential events that may affect a project negatively, while issues are actual events. Thus, risks must be managed in order to avoid that they become issues (prevention) or that their initially expected effect becomes actual (protection). Issues must be treated as soon as possible and, where necessary, escalated to the appropriate level in the shortest timeframe. A risk may remain open, while an issue must be solved.

Managing risks and issues is a continuous process to be organized by the project, focussing on:

- Identifying, describing and assessing risks and issues;
- Maintaining risk and issue information regularly, i.e. checking on a regular basis if it is up-to-date, exhaustive and accurate enough;
- Defining actions to mitigate the risks and issues, an expected level of effectiveness of these actions should be assessed;
- Implementing these actions;
- Controlling their effectiveness.

The management of project Risks and Issues will be done through the Periodic Reporting via the H2020 Participant Portal (Ref [2]).

Not all risks and issues are to be reported. Only top Risks and significant issues (if applicable) will be reported in the Technical Progress Reports and in the quarterly report for SJU risk management. The reporting on risks will include impact, likelihood, severity as well as mitigation actions and their status. The reporting on issues will include impact status and corrective actions

All Project risks and issues are reviewed and updated at least once every 3 months, when they are integrated in the quarterly report. Some particular attention could be put on interdependencies with other projects (risks shared with other projects and external risks).

4.7 Request for Amendments

Any contractual change on the Grant Agreement has to be duly justified and has to be requested by initiating an Amendment workflow in the Participants Portal.

In general, the Grant Agreement must be amended if there are any changes required to:

- its terms & conditions (e.g. data or options specific to that agreement);
- its annexes.

Amended provisions become an integral part of the Grant Agreement.

For the H2020 policy on amendments, please refer to the H2020 User Manual (Ref [2]) and to Article 55 of the Annotated Model Grant Agreement (Ref [3]).

4.8 Implementation of Ethics Requirements

When Ethical requirements have been identified during the proposals evaluation, an "Ethics Requirements" Work Package is automatically included in the Grant Agreement. All ethics requirements that are due after project start are automatically included in the grant agreement in the form of deliverables. These deliverables are known as 'ethics deliverables'.

The delivery date of these ethics deliverables is set in the Grant Agreement. When preparing the answers to the various Ethics requirements, the Project can refer to the H2020 guidance on Ethics self-assessment (Ref [1]).

4.9 Final Project Results Report

The project will deliver a publishable Final Project Results Report covering all the research activities performed by the project, based on a template to be provided by the SJU. This report (not to be confused with the H2020 Technical/Financial yearly progress reports) will be used at the Project Closeout meeting to discuss the transition to subsequent development stages including a self-assessment of the TRL (Technology Readiness Level) achieved at the end of the project. The SJU will verify the maturity achieved in order to establish the appropriate transition of the results to subsequent phases.

This report will be delivered to the SJU for approval at latest one month before the project Closeout meeting.

5 Project Meetings

5.1 Kick Off meeting

The project Kick-off meeting is called by the Project Coordinator shortly after contract signature. This meeting will be organised at the SJU.

The Kick-off meeting aims at informing the beneficiary(ies) about the operational and applicable financial provisions in more details, including discussing the project objectives, organisation, deliverables, resources, planning, communication and dissemination activities and other relevant information as outlined in the Description of the Action (Annex I to the Grant Agreement).

It will also allow discussing any practicalities related to the launch of the project and agreeing on the content of the Project Management Plan to be delivered one month after the Kick-off meeting.

5.2 Working Meetings/Workshops/Dissemination events

The project will plan its working meetings, workshops and dissemination events as required. The SJU will be invited to attend. SJU attendance may consist of the SJU Programme Manager and/or a SJU ATM expert and/or SJU Grant Manager. The SJU attendees may however decide not to attend a particular meeting/workshop.

5.3 Project Review and Close out Meeting

The Project Review meeting shall take place on a yearly basis as part of the yearly reporting and payment process in alignment with the related periodic technical and financial reports. This meeting will be held at the SJU and will also aim at steering the project in order to secure the delivery of expected quality and maturity at the project Close-out meeting.

The last project review meeting (also called Close out meeting) shall include a TRL7 maturity assessment to envisage the transfer of the project results for the deployment phase and shall be planned in the last two months before the end of the Grant period.

Guidance on maturity assessment and on the related criteria to apply will be provided at the Kick off Meeting.

If required, ad-hoc review meeting(s) can be organised on SJU request.

6 Referenced Documents

[1] Guidance How to complete your ethics self-assessment
http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf

[2] H2020 Participants Portal Online Manual:
http://ec.europa.eu/research/participants/docs/h2020-funding-guide/index_en.htm

[3] H2020 Annotated Model Grant Agreement. This document summarizes all H2020 contractual requirements applicable during project execution. It can be found on H2020 Participants Portal at:

http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/amga/h2020-amga_en.pdf

[4] SJU Model Grant Agreement:
http://ec.europa.eu/research/participants/data/ref/h2020/other/mga/jtis/h2020-mga-er-sesar-ju_en.pdf

[5] Final Guidance Material to Execute Proof of Concept: In Annex A to this Guidance

Proof of Concept/VLD Template: in Annex B to this Guidance

[6] SESAR Safety Reference Material: in Annex C to this Guidance

Guidance to Apply the SESAR Safety Reference Material: in Annex D to this Guidance

Final Guidance Material to Execute Proof of Concept

Document information	
Project Title	Develop "proof of concept" for aircraft certification when introducing a new concept of operations
Project Number	16.1.4
Project Manager	AIRBUS
Deliverable Name	Final Guidance Material to execute proof of concept V2
Deliverable ID	16.01.04 – D07
Edition	00.03.00
Template Version	03.00.00
Task contributors	
AIRBUS, EUROCONTROL, THALES	

Please complete the advanced properties of the document

Abstract

The aim was to produce a practical guide on how to prepare, seek approval and execute the very large demonstrations for a given SESAR solution involving air – ground integration. Proof of Concept (POC) and very large demonstrations (VLD) have the same meaning within the scope of this document.

Authoring & Approval

Prepared By - *Authors of the document.*		
Name & Company	Position & Title	Date
Joelle Monso / AIRBUS	Project Leader	
Bruno Rabiller / EUROCONTROL	Project Contributor	

Reviewed By - *Reviewers internal to the project.*		
Name & Company	Position & Title	Date
Bruno Rabiller / EUROCONTROL	Project Contributor	
Patrick Lelievre	Contributor Manager	

Reviewed By - *Other SESAR projects, Airspace Users, staff association, military, Industrial Support, other organisations.*		
Name & Company	Position & Title	Date

Approved for submission to the SJU By - *Representatives of the company involved in the project.*		
Name & Company	Position & Title	Date
Joelle Monso / AIRBUS	Project Leader	
Bruno Rabiller / EUROCONTROL	Project Contributor	

Rejected By - *Representatives of the company involved in the project.*		
Name & Company	Position & Title	Date

Rational for rejection
None.

Document History

Edition	Date	Status	Author	Justification
00.00.01	02/10/2014	Draft	Joelle Monso	New Document
00.01.00	09/10/2014	Final	Joelle Monso	Update according to EUROCONTROL comments
00.02.00	30/01/2015	Final	Joelle Monso	Update according to SJU assessment results
00.03.00	28/05/2015	Final	Joelle Monso	Review by EASA and update accordingly

Intellectual Property Rights (foreground)

This deliverable consists of SJU foreground.

Table of Contents

List of figures

Executive summary

The Proof of Concept / Very Large Demonstration is a confidence building exercise that comes in addition to the traditional validation required prior certification and implementation of new concept or new technology.

The Proof of Concept / Very Large Demonstration has to be distinguished from operational live trials since it brings a new dimension of the validation: early operations with a significant scale environment.

A significantly scaled validation for new concept and/or technology is a must for proving early benefits but also gaining all stakeholders' buy-in their early involvement. The proof of concept exercise goes beyond the scope of initial work programme of SESAR, as it may involve new stakeholders through the VLD work arrangement.

The purpose of this guidance material is to provide all stakeholders involved in very large demonstrations with an overview of the activities to be undertaken to bring to a successful implementation of these projects.

The harmonized and consistent process related to the Proof of Concept / Very Large Demonstration is based on a good coordination of all the stakeholders during the following phases: preparation, approval and execution. The objective of this document is to provide details of these phases.

1 Background Information

1.1 Why a Proof of Concept?

The introduction in the ATM of new Concepts & Technologies (C&Ts) will have to be evaluated in terms of their potential benefits to decrease impact on environment and to increase capacity, efficiency and safety. Once the evaluation is complete, the SESAR Members will assess the drift between targeted benefit and finally achieved benefit. If not narrow enough, they will decide re-working to quickly move forward.

The proof of concept / Very Large Demonstration exercise consists in an early operation of the SESAR C&Ts making use of pre-operational or operational products (airborne and ground) in a real operational environment. A sufficient number of aircraft will have to be equipped to assess the actual performance and benefits delivered by the new concept and/or technology.

This project draws on extensive experience of Industrial Partners in concept design, aircraft / product architecture & certification, flight testing and results analysis to help SESAR Members mature the most promising SESAR C&Ts into fielded solutions in the Single European Sky.

1.2 What is a Proof of Concept?

The Proof of Concept / Very Large Demonstration is a confidence building exercise that comes in addition to the traditional validation required prior certification and deployment of new concept or new technology.

The proof of concept relies mainly on a wide scale demonstration aiming to show to the different stakeholders that the foreseen performances (safety, capacity and environment) could be actually met. Without involvement of the airspace users, such demonstration will not be carried out and the validation will rely on traditional validation processes. The large scale trials will bring more credibility. This is a huge difference to one flight live-trials. It is this credibility "jump" which is the key benefit of the Proof of Concept. It validates the assumptions - particularly benefits - generated during the R&D. It also proves that the concept can be done in a real-life environment, thus removing some potential risks in the transition from R&D to full operations.

Proof of Concept might be a real live operation decision making process, e.g. more reflective of the link between V3 and V4 (E-OCVM), It could help to convince the people involved in the financing mechanisms. To name just a few features in favor on proof of concept:

1. Feasilibility in real environment; usually, airspace user Investment Case is based on simulation featuring always ideal scenario with meteo not representative. Proof of Concept is showing real life and makes the concept more robust, in particular regarding unscheduled operations (variable winds and weather).
2. “Safety first”: the only ways of proving safety benefits (particularly protection from or mitigation for unforeseen scenarios) is through large scale trials such as POC/VLD. Anything else has a strong risk of probe bias (i.e. the subject is prepared for the non-nominal event, and does not react in the same way).
3. Benefit of POC/VLD for sensible transition strategy.
4. Collective benefits for the airspace users.

It is therefore the interest of all stakeholders (e.g. the SESAR extended community including SESAR Partners together with airspace users, Authorities, Network Manager and Deployment Manager) to evaluate actual performances for SESAR operational improvements/projects associated to brand new concept/technology before the SESAR deployment.

1.3 Who will decide Proof of Concept?

The decision to conduct a proof of concept / Very Large Demonstration to validate some elements of SESAR proposed solutions is to be taken when the SESAR 2020 activities related to VLD projects are launched.

Therefore as a result, the organizational aspects including governance mechanisms (project organization and project management) will be known at that time.

1.4 What is needed to know about Proof of Concept?

1.4.1 Terminology

The Proof of Concept as considered by this Project P16.1.4 should not be assimilated to the "proof of concept" TLR 3 NASA definition.

Note: If a comparison or correlation is to be made with the Technology Readiness Level Concept defined by NASA, then the TLR 9 is the one closest (but not identical).

The SESAR Proof of Concept (P16.1.4) is seen as addressing an accurate verification of the technical development and as delivering a proven vehicle for accelerating the operational acceptance and the industrialization of the SESAR solutions.

1.4.2 Refined Scope & Context

The initial scope and perimeter of the 16.01.04 Project has been refined to support the very large demonstrations through the Change Request 1953. This supporting activity is reflected within the task 16.01.04 T008 for the production of the POC/VLD template to be used for the very large demonstrations.

1.4.3 V3+ Context

The Proof of Concept live trials were initially planned as V1 to V3 (E-OCVM) activities, which means to be carried out with "pre-operational" products for airborne and ground systems. But now some of the very large demonstrations are planned as V3+ (early industrialization) activities, which mean that in most cases the live trials, will be carried out with the industrial products.

VLDs are at the boundary in terms of maturity transition from the Industrial Research & Validation and the Industrialisation / deployment and this bridging in term of development lifecycle is called V3+. Indeed V3+ is a step beyond V3, implying validation by using end-user systems

The high level requirements of the current regulatory framework are appropriate for the VLD, but, for the VLD conducted with the industrial products, it may be deemed necessary to have an agreement with the relevant authorities on the necessary means of compliance (e.g. industry standards), which should be used as final standards or that should be validated during the VLD.
This would require early involvement of EASA and the National Authorities for scoping and coordinating the necessary approvals addressing the end to end aspects of the ATM operations.

This additional step beyond V3 should facilitate the work of the SESAR Deployment Manager who will have to ensure the synchronisation of the ground and air deployments.

1.5 VLDs versus Proof of Concept

At the inception of the SESAR Programme (in 2009), it was foreseen to execute "proof of concept" trials for any SESAR solution that could reply to the eligibility criteria defined in the POC GM Draft 1 but the necessary managerial functions to conduct such a project for a particular element of the SESAR concept were not addressed.

Now, the managerial aspects are now being addressed project by project, under the leadership of a project leader together with a well-established SESAR framework. That is to say a Very Large Demonstration is the realization of the proof of concept for a dedicated SESAR solution via a SESAR project.

To make it short, the Proof of Concept is a methodological tool to perform the Very Large Demonstration and the POC/VLD Guidance Material is to be used to produce the VLD Plan and Report.

Considering the clarification provided for the VLD and POC meanings, this guidance material is to be applied to Very Large Demonstration Projects as defined by the SESAR framework.

Therefore in the rest of this document POC or VLD are used indifferently.

1.6 SESAR VLDs

Very Large Scale Demonstrations (VLD) as defined by the SESAR framework should help to fill the gap between development and deployment phases and consists of demonstrating key SESAR concepts and technologies to raise awareness regarding SESAR activities related to ATM performance issues and their results as well as assessing full-scale deployment readiness.

VLDs will focus on concepts that provide significant contribution to performance, being sufficiently mature and requiring coordination at European/Global level (in particular with regards to air-ground and/or ground-ground integration).

2 Essential Elements of Proof of Concept

Like SESAR in general, Proof of Concept/ Very Large Demonstration is a collaborative project which investigates new ways of working together to help to change working habits pushing further the concept of coordination and collaboration.

2.1 New type of Trials

The proof of concept has to be distinguished from the operational and live trials since it shows on a larger scale, how the SESAR change could be brought into operations to deliver the required performances and further deployed. It is proposed to differentiate the various types of validation exercises falling under the scope of SESAR as follows:

- **Live trials** are typically trials performed by the aircraft manufacturer with flight test aircraft to test new CNS/ATM aircraft functions and operational procedures in live conditions with coordination with normal traffic.

- **Operational trials** are typically trials performed by the operators during revenue flights using existing aircraft capability to test new ATC procedures.

- **Proof of concept trials** are typically trials performed by the operators during revenue flights using pre-operational or operational products (CNS/ATM airborne & ground, equipment & procedures) to confirm initial ATM operation benefit analysis of new concepts and technologies.

2.2 Full Scale Validation

The full scale validation for SESAR concept and/or technology is a must for proving early benefits but also gaining early involvement of all stakeholders. The proof of concept exercise goes beyond the scope of work of SESAR:

- Within Europe, it involves stakeholders outside the SESAR community like Aircraft Type Certificate holder (not always SESAR partner), aircraft operators and competent authorities.
- But also, outside Europe, It may involve OEM in the US and FAA as such bringing international dimension to SESAR R&D project.
- It may support the activities of the international standardization organizations (ICAO and EUROCAE/RTCA) by reinforcing validation of global standards.

Currently, several projects of ATM modernization of which SESAR in Europe and Next Gen in the US, have been launched to cope with the projection of the airline needs up to 2020 and beyond. Both SESAR and Next Gen, are aimed at enhancing safety and efficiency in their respective region both advancing new concepts and new technology but are they harmonized enough to allow seamless operations and to achieve global aviation safety and efficiency? The proof of concept should provide the answer to the question.

Another dimension to be taken into account with SESAR and the other projects of the modernization of the ATM over the world, normally not covered by the traditional V&V within the certification context, is the~~:~~ global interoperability. The overall objective of the proof of concept is to address global interoperability and safety considerations.

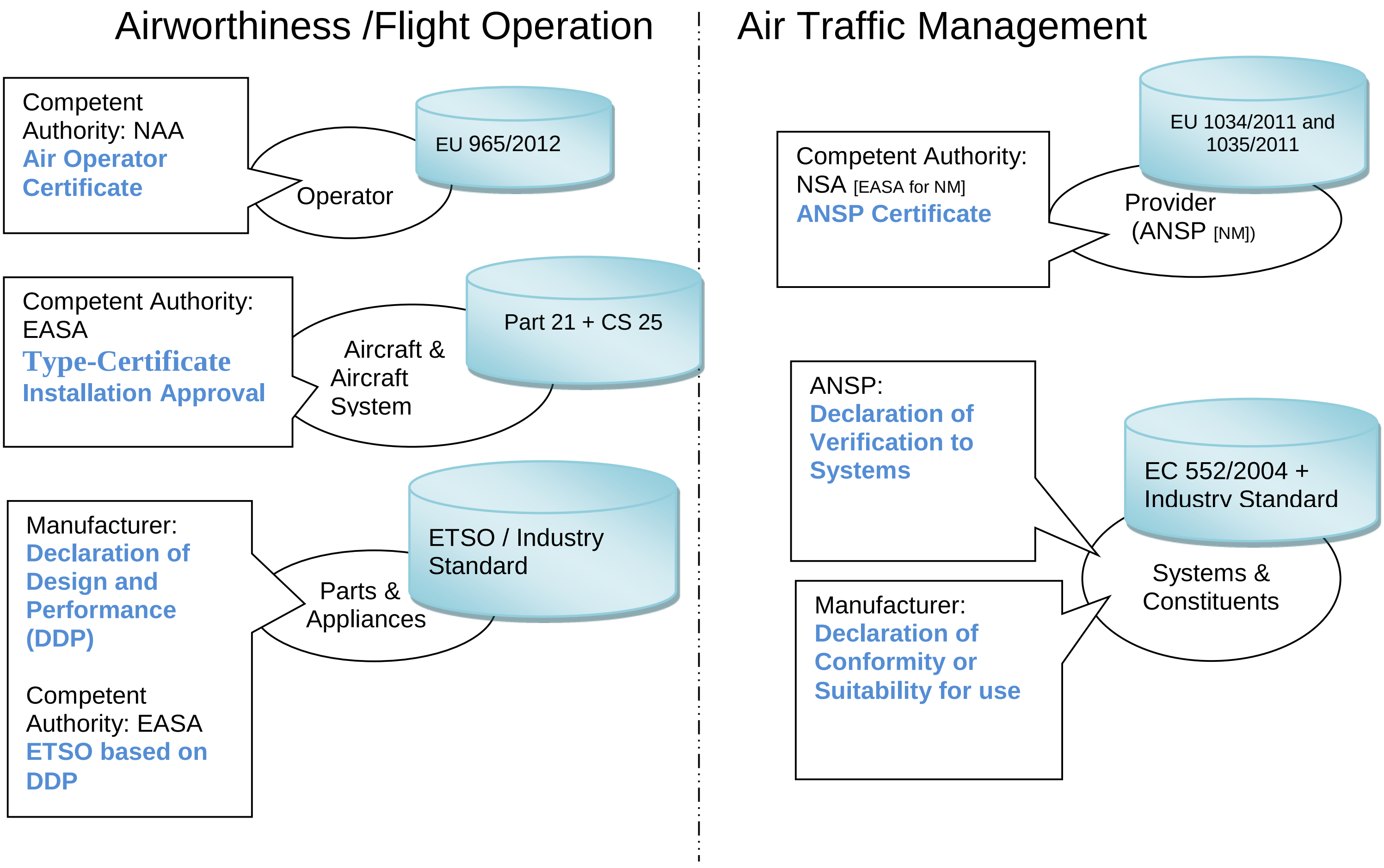
In the light of the above statement, Proof of concept exercise might be conducted in different countries and might address the interoperability considerations when coordinated with the ANSPs, Network Manager (NM), Aerodrome operators and the competent authorities within Europe and outside Europe.

2.3 Tailored Certification Process

When considering a significant change which is introducing a new concept (e.g. 4D trajectory, ASAS...) or a new technology (e.g. GBAS Cat II/III), it might be necessary to evaluate performances of such concept/technology as early as possible in a real operational environment to analyze the achievability of the specified performances before its implementation/industrialization.

To this end, the use of pre-operational product can be envisaged, opening the door for tailored design solutions and tailored certification processes to support the demonstration. A tailored certification process means that the means of compliance (MOC) to show compliance with the applicable regulations are specifically tailored for this installation with the competent authorities and in particular with EASA through a Certification Review Item (CRI) for the airworthiness aspect.

But in all cases, full compliance against relevant regulation has to be shown. A revenue flight with pre-operational airborne and/or ground products means that these products are “certified” against the applicable regulations. The current regulatory context is summarized here below:


Airworthiness /Flight Operation
Air Traffic Management
Competent Authority: NAA
Air Operator Certificate
Operator
EU 965/2012
Competent Authority: EASA
Type-Certificate
Installation Approval
Aircraft & Aircraft System
Part 21 + CS 25
Manufacturer:
Declaration of Design and Performance (DDP)
Competent Authority: EASA
ETSO based on DDP
Parts & Appliances
ETSO / Industry Standard
Competent Authority: NSA [EASA for NM]
ANSP Certificate
Provider (ANSP [NM])
EU 1034/2011 and 1035/2011
ANSP:
Declaration of Verification to Systems
EC 552/2004 + Industry Standard
Systems & Constituents
Manufacturer:
Declaration of Conformity or Suitability for use

2.4 Applicable Requirements for Airborne part

The applicable regulation is the basic regulation (EC) N°216/2008 for airworthiness and aircraft operation.

- EC 965/2012 is applicable for air operations➔ the air operator participating to the Proof of Concept / Very Large Demonstration shall demonstrate to his national authority that flight operation during those trials is acceptably safe.

- (EU) 748/2012 Implementing Rules for Airworthiness (Part 21) and Certification Specification "CS 23 or CS 25" Airworthiness Standard are applicable for the aircraft & aircraft systems→ the TC holder (or STC Holder) participating to the Proof of Concept / Very Large Demonstration shall demonstrate to his airworthiness authority that the aircraft is still airworthy.

The related aircraft design change is approved under part 21 subpart D or E. The on-board new equipment to be used in the Proof of Concept exercise will have to go through a full certification review process to ensure compliance with all applicable CS 25 or 23 requirements.

2.4.1 Operational Product / SESAR Solutions

In case of installation of operational product implementing a new airborne CNS/ATM functions as per SESAR solution, it is recommended to apply, in complement to CS 25, the relevant part of the CS-ACNS to show compliance with the basic regulation for the airborne ATM part, including performance and interoperability requirements (EC 552/204).

Note: only new generation aircraft have the CS-ACNS or some parts of it in their Type Certificate Certification Basis. However as the CS-ACNS contains the certification and interoperability standards for onboard Communications, Navigation and Surveillance systems and the alignment of the existing AMC 20 material*, the applicant may elect to comply with the part of CS-ACNS which is relevant for the installation of the new on-board CNS/ATM system or functionality on a voluntary basis.*

2.4.2 Pre-Operational Product / Preliminary SESAR Solutions

In case of installation of a pre-operational product (not final SESAR solution yet) and provided that it is not a "required" equipment, the principle for a "tailored" certification process may apply. This "tailored" certification may consist in showing "no safety effect" for the loss or erroneous behaviour of this equipment as compliance with the applicable CS25 or 23 requirements. The approach will focus on the "non-interference" demonstration on the aircraft systems and the monitoring of loss or erroneous behaviour by operational procedure specifically tailored for the POC/VLD to revert to baseline situation when needed. This might bring some technical challenges that will have to be solved on a case by case basis between the Type Certificate holder and EASA during the certification review process.

Note: The "required" systems or equipment shall be understood as per CS 25.1309a definition: "*Those required for type certification or by operating rules". This precludes a "tailored" certification for systems performing required functions such as Data link service, BRNAV, etc.*

.

2.5 Applicable Requirements for Ground part

In the field of aerodromes, air traffic management and air navigation services , the applicable regulation is the Basic Regulation (EC) N°216/2008 as amended by (EC) N°1108/2009[1].

- EU 139/2014 proposes a new regulatory framework for aerodromes.
- Regarding the ATM and ANS, the applicable regulation is with a dual legal basis:
    - SES regulations: (EC) N°549/2004, (EC) N°550/2004, (EC) N°551/2004 and (EC) N°552/2004 as amended by (EC) N°1070/2009 (SES 2) for the Air traffic Management and Air Navigation Services, including FAB Regulation: (EU) N°176/2011 for VLD taking place across several countries.
    - Basic Regulation: Under the Basic Regulation (N°216/2008), the common requirements for ANS/ANSP & NM (EU) N°1035/2011 and safety oversight in ATM (EU) N°1034/2011 are applicable.

[1] Extension of the EASA system to safety regulation of air traffic Management and Air Navigation Services.

2.6 Tailored Risk Assessment

Working together as a team for the VLD project, the applicants for a change in the domain of airworthiness, flight operation, aerodrome operation, Network Management and Air Traffic Services, shall identify the hazards caused by the use and failure of this "early" SESAR operational capability on an overall basis; It means potential hazards on all domains.
The results of this overall risk assessment might lead to necessitate, under certain circumstances, reversion to the baseline situation (normal operations) and when this happens, the reversion shall be demonstrated to be safe for all domains (aircraft, aircraft operation, airport operation, Network operation and ATS). The impact of this reversion at aircraft and ground level will have to be addressed in a timely manner as it may result in additional design requirements (airborne & ground) specific to the proof of concept trials. A Declaration of Verification/Conformity for the ground system may be required when ATM operation is impacted by the VLD.

2.7 Tailored Design / Procedural Solution

Airworthiness & Flight Operation Aspects

Innovative solutions have to be found to show compliance with the applicable Certification Specification items. In case of use of pre-operational products for which hardware and software qualification activities have not been completed to show compliance with CS 25.1301, 1302 &1309 for instances, alternate solutions have be considered such as:

- Installation on non-interference basis for non-required equipment (CS 25.1301, 1302),
- Demonstration of "No Safety Effect" for the loss or erroneous behavior of not-required equipment (CS25.1309, 1302),
- Safety nets / mitigation means that allows considering that the "No Safety Effect" assumption is valid for required equipment (CS25.1309, 1302),
- Flight crew procedures (use of back-up and monitoring means), Aircraft Flight Manual limitations (CS 25.1309, 1302) for required equipment.

In any case, these solutions will have to cope with the safety (CS. 25.1309) and security requirements (EU 965/212 Parts ORO & CAT). When compliance with the applicable regulations will not be possible to establish, then there should be no possibility to perform proof of concept with the aircraft type design. A certain number of rules have to be established by the TC/STC Holders & Aircraft operators to address the 'acceptability" of the pre-operational solution when defining the criteria of eligibility for SESAR element to be candidate to a proof of concept.

Examples for the airborne part:

- Use of EFB class 2 to host pre-operational SESAR function **cannot** be envisaged for the "required" airborne equipment as per CS 25.1309 definition unless specific measures are taken to solve the security issues (EU 965/2012).
- Use of not fully qualified equipment (e.g. red label) for equipment "required" by the operational regulation can be envisaged only if it can be monitored and disabled by the cockpit crew to revert to normal equipment.
- Use of not fully qualified equipment (e.g. red label) for equipment not "required" by the operational regulation can be envisaged on a basis of non-interference with other equipment fitted onboard the aircraft.

Examples for the ground part:

- Need of shadowing controllers in order to help recognizing situation necessitating reversion or contingency procedures.
- Use of segregated routes for flights participating to the VLD.

2.8 Coordinated Approval Process

The pre-requisite element for obtaining the “approvals” will be the effectiveness of the proposed operational mitigation measures (ATC [or Network Manager] Procedures and/or Flight Crew Procedures).

The way to ensure the effectiveness and alignment of these risk mitigations during the VLD is to implement an End-to-End approach for a consistent and coordinated safety assessment between each domain (airworthiness, flight operation, airport operation and ATM).

The current process with the three or four independent approvals shall evolve and consider end-to-end system functionalities, seamlessly encompassing airborne and ground constituents.

Consequently, a holistic safety regulatory approach taking into account the particular context of the POC/VLD may be needed to ensure ATM safety consistency.

The proposed coordinated approval process that is discussed later in this document could consist in theses 3 main steps:

- Coordinated risk assessment:
  - A common methodology for the overall risk assessment as defined in section 8.4 “Preparation phase/ Risk Assessment” shall be applied.
  - Coordinated review of the overall risk assessment by the competent authorities,
- Coordinated safety assessments:
  - All the assumptions and safety risk mitigations which have been made at local levels during the various safety cases by ANSP/ADR, NM, TC/STC Holder and the operator based on standard operational procedures & contingency procedures will have to be commonly agreed.
- Coordinated approval from each competent authority.

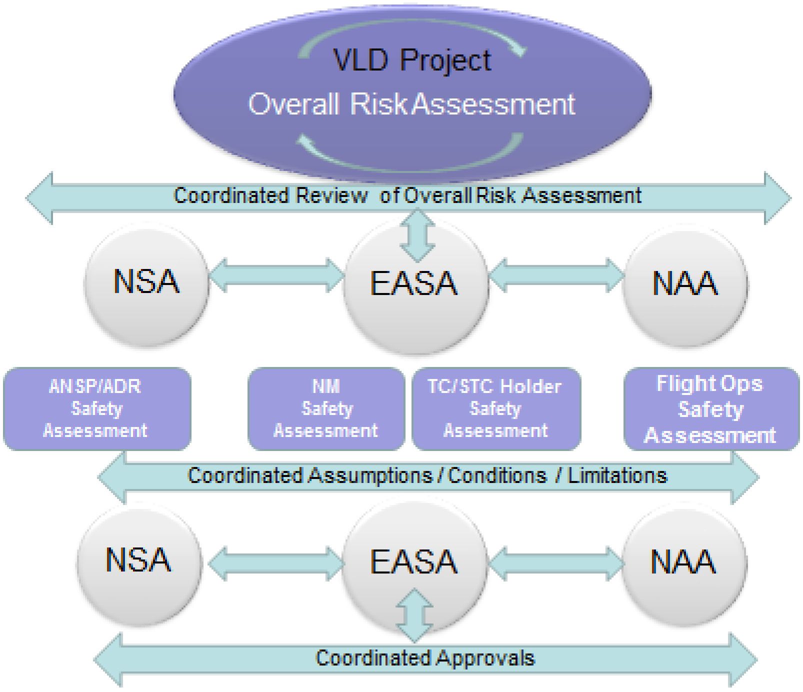

VLD Project
Overall Risk Assessment
Coordinated Review of Overall Risk Assessment
NSA
EASA
NAA
ANSP/ADR Safety Assessment
NM Safety Assessment
TC/STC Holder Safety Assessment
Flight Ops Safety Assessment
Coordinated Assumptions / Conditions / Limitations
NSA
EASA
NAA
Coordinated Approvals

Figure 1: Coordinated Approval Process

EASA will have to play a Key role for the coordination of the involvement of the competent authorities and the review by them of the POC/ VLD risk assessment as well as for the coordination of the different approvals.

This coordination & oversight role of EASA for the VLD will be formalized in an ad-hoc manner in the "Project Interface Document" and "Conditions and Limitations" supporting material attached to the approvals formalizing inter alia:

- The coordination arrangements between the authorities for each phase of each VLD project (preparation, approval and execution) that will be specified in the "Project Interface Document".
- The agreed and aligned assumptions and risks mitigations that will be put in the "conditions & Limitation" supporting material and the relevant operational documentation [AIP, (AFM: limitations, Standard Operational Procedures & Contingency procedures), FCOM, ..]

From a regulatory perspective, this may suggest that the VLD is treated as a 'multi-actor change' and that overall risk assessment is performed during the preparatory phase and prior to the execution of the life trials. This overall risk assessment should then be reviewed by the authorities and the review been coordinated by EASA. This overall risk assessment could very similar to what has been done for the FAB safety cases and the goal is to ensure that all the high level hazards have been identified and the high level risk evaluated and the mitigation is taken by the appropriated actor. The project manager for the VLD could be the facilitator of such overall risk assessment and all actors (TC/STC holders, ANSPs, NM, airport/aircraft operators, military, GA, authorities and EASA) involved in the VLD (or affected in somehow) should be appropriately represented, involved or at least consulted.

3 Introduction

3.1 Scope of the document

The purpose of this document is to describe as clearly as possible what should be done and by whom during the Very Large Demonstration. This guidance material defines a step by step approach and the activities to be conducted are presented in a chronological order.

The objective of this guidance material is:

- To define a step by step process for its harmonized application by the relevant SESAR Stakeholders of the VLD Projects.
- To establish the respective actor's responsibilities for each step of this process. This is a key element for efficient execution of the Very Large Demonstration. Clear identification of who is doing what among the main actors should bring clarity and facilitate the overall process.

Two types of stakeholders will have to be involved: the "makers" and the "facilitators". The "makers" are the VLD primary stakeholders who are leading and making the demonstration. The "facilitators" are the stakeholders who are supporting, monitoring and approving the demonstration.

The "facilitators" for the VLD should be the Network Manager, the EASA, NSAs & NAAs and the Deployment Manager. The Network Manager should support and validate the network performance aspect of the VLD, when needed. The EASA should support and validate the overall safety case in coordination with the local authorities and grant airworthiness approval. The Deployment Manager should support and validate the business case. The local authorities will grant the ANSP and Airport operator and aircraft operator's approvals.

The "makers" are those who are taking decision and producing the demonstration record the project leader such as the operational and safety task leaders, ANSPs, Network Manager, Airport operators, TC/STC holders and Aircraft operators.

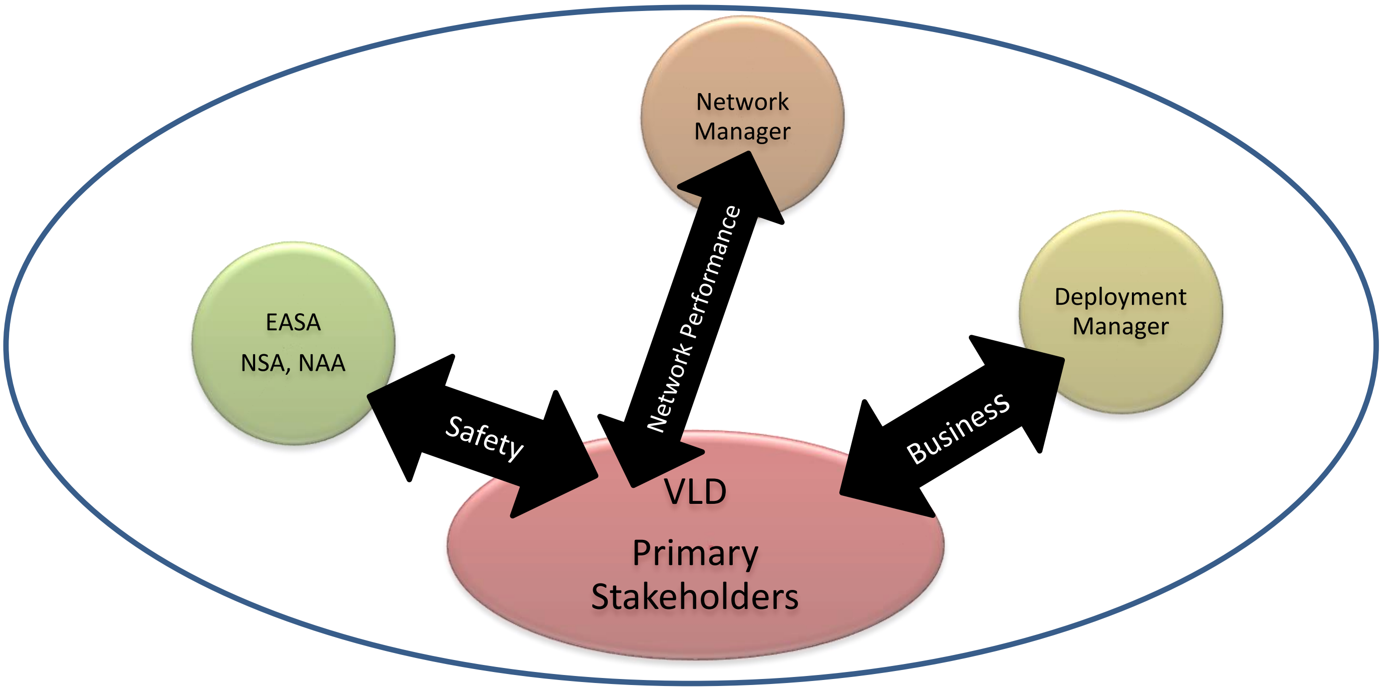


Figure 2: VLD Stakeholders

⬭ Makers

● Facilitators

3.2 Who is doing what

The preparation of the POC/VLD trials will set up the operational context to conduct the live trials. This activity will be done by the designated VLD Project Consortium (e.g. the “makers”) in close coordination with the “facilitators”.

The activities for making the demonstration for the approvals to conduct the VLD trials fall under the responsibility of the TC/STC Holder(s), Aircraft Operator(s), Network Manager*, and the ANSP(s) and/or Airport Operator(s). To conduct VLD trials, at least three approvals will be necessary, independently delivered but that will be closely coordinated through the application of this guidance material. The TC/STC Holder and Network Manager* will have to obtain authorization from EASA, the Aircraft Operator will have to obtain authorization from his National Aviation Authority (NAA) and the ANSP and/or the Airport operator will have to obtain authorization from his National Supervisor Authority (NSA).

The execution of the VLD trials falls under the responsibility of the TC/STC Holder(s), Aircraft operators, Network Manager and ANSP(s) and/or Airport Operators. The analysis of the results and dissemination of information will be the responsibility of the designated VLD Project Stakeholders.

3.3 Structure of the document

Section 1 & 2 provide general information on proof of concept / Very Large Demonstration (e.g. what is a proof of concept and what benefit could it bring to SESAR). Furthermore, as proof of concept/VLD goes beyond the development phase, this section establishes clear relations between the aviation community and the different actors of SESAR bridging the gap between the concept phase (research) and the operational implementation phase (industry).

Section 3 & 4 recall the definition of specific vocabulary for common understanding developed for SESAR.

Section 5 provides an overview of the process to be carried out to conduct a proof of concept exercise. It explains how proof of concept / very large demonstration can be integrated within SESAR framework.

Section 6 defines a proposed new certification approach to address the end-to-end system considerations.

Section 7 calls for the establishment of a project management approach.

Sections 8 to 10 describe all the tasks that have to be carried out by the different stakeholders to successfully conduct proof of concept / very large demonstration. Particular highlight is put on the SESAR stakeholders’ activities but also on the SESAR extended community when it relates to the holistic safety approach necessitating an activity of coordination and collaboration.

3.4 Intended readership

This document interests all the actors that play a role in the Very Large Demonstrations: the SJU, the members of the VLD project consortium, the Network Manager, the Competent Authorities and the Deployment Manager.

3.5 How to use this document

Figure 1 below presents the overall structure of the Guidance Material to execute proof of concept.

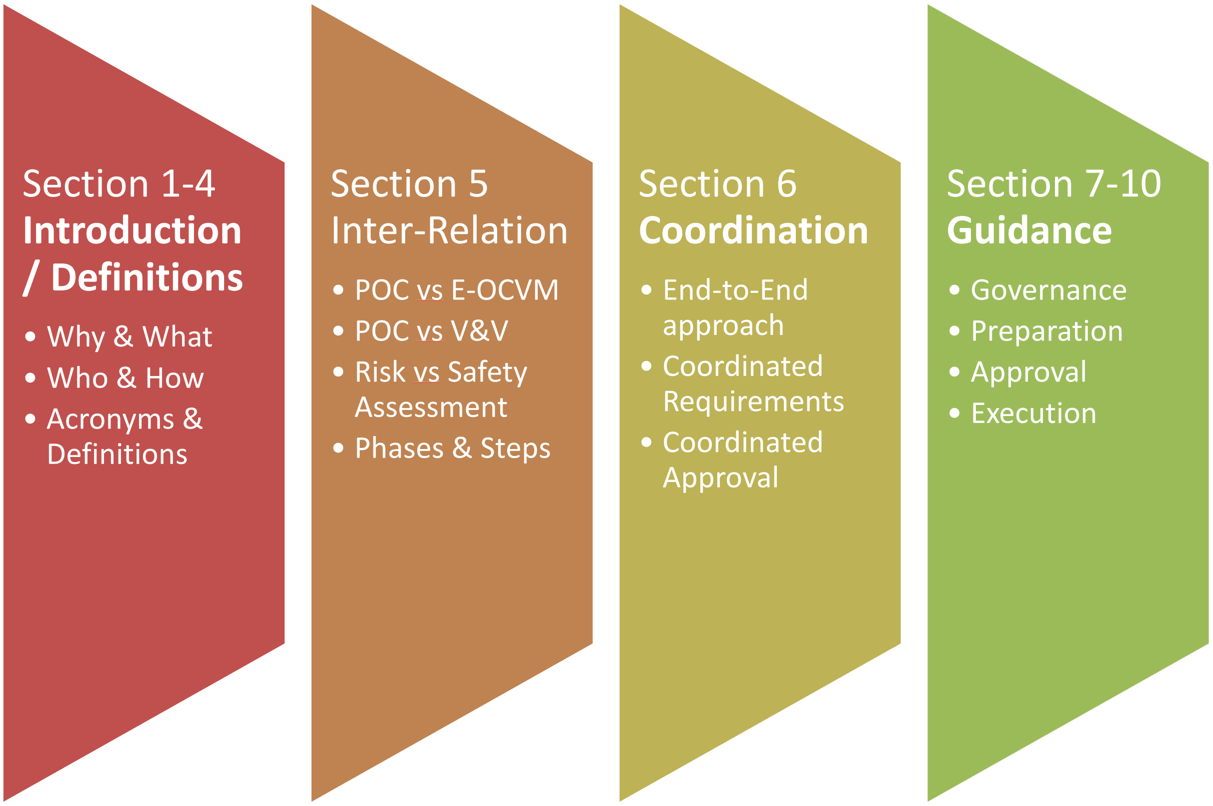


Figure 3: Structure of POC Guidance Material

3.6 Acronyms and Terminology

Term	Definition
ADR	Aerodrome
AFM	Aircraft Flight Manual
AIM	Accident Incident Model
ANSP	Air Navigation Service Provider
ASAS	Airborne Separation Assistance System
ATM	Air Traffic Management
A/W	Airworthiness
CDL	Configuration Deviation List

Term	Definition
CFT	Call For Tender
CNS/ATM	Communication Navigation Surveillance / Air Traffic Management
CS	Community Specification (SES System)
CS	Certification Specification (EASA System)
DM (SDM)	Deployment Manager (SESAR Deployment Manager)
DoW	Description of Work
EASA	European Aviation Safety Agency
EATMN	European Air Traffic Management Network
E-ATMS	European Air Traffic Management System
EFB	Electronic Flight Bag
E-OCVM	European Operational Concept Validation Methodology
ETSO	European Technical Standard Order
FAB	Functional Airspace Block
FDM	Flight Data Monitoring
FTS	Fast Time Simulation
GBAS	Ground Based Augmentation System
HITL	Human-In-The-Loop
INTEROP	Interoperability Requirement document
IR	Implementing Rule
MEL	Minimum Equipment List
MSN	Manufacturer Serial Number
NAA	National Aviation Authorities
NOTAM	Notices for airmen
NM	Network Manager
NMO	Network Manager Operator
NMOC	Network Manager Operator Centre
NSA	National Supervisory Authorities

Term	Definition
OFA	Operational Focus Area
Ops	Operational
OSED	Operational Service Environment Document
PID	Project Interface Document
POC	Proof of Concept
RCA	Relevant Competent Authority
RTS	Real Time Simulation
SAC	Safety Criteria
SAR	Safety Assessment Report
SC	Special Condition
SES	Single European Sky
SESAR	Single European Sky ATM Research Programme
SESAR Programme	The programme which defines the Research and Development activities and Projects for the SJU.
SJU	SESAR Joint Undertaking (Agency of the European Commission)
SJU Work Programme	The programme which addresses all activities of the SESAR Joint Undertaking Agency.
SMS	Safety Management System
SPR	Safety Performance Requirement document
SPV	Separation Performance Visualizer
SRM	Safety Reference Material
STC	Supplemental Type Certificate
TC	Type Certificate
TEM	Threat-and-Error Management
TRL	Technology Readiness Level
VLD	Very Large Demonstration
Vs	Versus
V&V	Verification and Validation

3.7 Applicable Documents

This guidance material has been developed in accordance with the applicable regulations for obtaining authorizations from EASA, NSA and NAA, listed below:

Origin	Contents
European Commission **(Airworthiness & Flight Operation)**	(EC) 216/2008 – common rules in the field of civil aviation and establishing a European Aviation Safety Agency. (EC) 1108/2008 - amending EC 216/2008 in the field of aerodromes, air traffic management and air navigation services. (EU) 748/2012 – laying down implementation rules for the airworthiness and environment certification of aircraft and related products, parts and appliances as well as for the certification of design and production organization (EC) 859/2008 – amending EEC 3922/91 as regards common technical requirements and administrative procedures applicable to commercial transportation by aeroplane. (EC) 375/2007 – amending EC 1702/2003 (EU) No 965/2012 laying down technical requirements and administrative procedures related to air operations pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council

European Commission **(SES Regulations)**	(EC) 549//2004 – laying down the framework for the creation of single European sky (EC) 550/2004 – on the provision of air navigation services in the single European sky (EC) 551/2004 – on the organisation and the use of the airspace in the single European sky (EC) 552/2004 – on the interoperability of the European air traffic management network (EU) 176/2011 – on the information to be provided before the establishment and modification of Functional Airspace Block. (EU) 1035/2011 – laying down common requirements for the provision of air navigation services and amending (EC)482/2008 and (EU) 691/2010 (EU) 1034/2011 – on Safety Oversight in air traffic management and air navigation services and amending regulation (EU) 691/2010 (EC) 1070/ 2009- amending regulations n°549/2004, n°550/2004, n°551/2004 and n°552/2004. (EC) 482/2008 – Software safety assurance system (EC) No 255/2010 laying down common rules for air traffic flow management (EU) 139/2014 laying down requirements and administrative procedures related to aerodromes pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council. (EU) 716/2014 – on establishment of the Pilot Common Project supporting the implementation of the European Air Traffic Management Master Plan of 27 June 2014 (EU) 409/2013 – on the definition of common projects, the establishment of governance and the identification of incentives supporting the implementation of the European Air Traffic Management Master Plan (EU) 677/2011 laying down detailed rules for the implementation of air traffic management (ATM) network functions and amending Regulation (EU) N°691/2010
EASA	Initial Airworthiness CS 23 – Normal, utility, aerobic and commuter aeroplanes CS 25- Large aeroplanes CS 27- Small Rotorcraft CS 29 – Large Rotorcraft CS-MMEL - Master Minimum Equipment List

	Aircrew: Commission Regulation(EU) No 1178/2011 of 3 November 2011 laying down technical requirements and administrative procedures related to civil aviation aircrew pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council CS-FST(A), CS-FST (H), CS-CCD, CS-FCD
	Air Operation: CS-FSTD(A), CS-FSTD(H), CS-FTL.1, CS-MMEL
	ATM/ANS: CS A-CNS – Approval Requirements for Airborne Communications, Navigation and Surveillance (safety + Interoperability)
	ATCO: Commission Regulation (EU) 2015/340 of 20 February 2015 laying down technical requirements and administrative procedures relating to air traffic controllers' licenses and certificates pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council, amending Commission Implementing Regulation (EU) No 923/2012 and repealing Commission Regulation (EU) No 805/2011
	Aerodromes: CS ADR-DSN - Aerodromes Design

This guidance material has been developed in accordance with the applicable SESAR documents, listed below:

Origin	Contents
SESAR	SESAR Safety Reference Manual (SRM) Ed 00.02.02 or any subsequent version Guidance to apply the SESAR safety Reference Manual Ed 00.01.02 or any subsequent version

4 Definitions

Pre-operational products or **pre-industrial prototypes**: are early/simplified versions of a potential design solution used to further explore requirements, problem characteristics or the applicability of solutions.

Operational Package: is a deployment focused grouping of performance driven operational changes and associated technical and procedural enablers.

Operational Sub-Package: is a sub-grouping of connected operational and technical improvements related to the Operational Package with closely related operational focus, designed to meet performance expectations of the ATM Performance Partnership.
Furthermore, to ensure that both Operational and Technical projects are structured in a way that dependencies are respected and that common work areas lead to coherent and integrated set of validation results, a third grouping based on common focus and linked to the Operational Sub-Packages was defined as Operational Focus Area.

Operational Focus Area: is a limited set of dependent operational and technical improvements related to an Operational Sub-Package, comprising specific interrelated Operational Improvements and associated enablers designed to meet specific performance expectations of the ATM Performance Partnership. .

Safety Criteria: means explicit and verifiable criteria, the satisfaction of which results in acceptable safety following the change. These are 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.

Accident Incident Model: The AIM tool is used to specify the safety targets for the SESAR concept element and will allow an estimation of the impact of SESAR Projects on the ATM contribution to safety. This process is described in the guidance D of the SESAR SRM.

5 POC/VLD in the Development Process

The purpose of this section is to place the Proof of Concept / Very Large Demonstration within the development life cycle.

5.1 Development Lifecycle Phase

The activities at individual VLD project level which are necessary to conduct live trials are activities accounted for in the SESAR 2020 operational work programme.

The planning of POC/VLD activities can be spread out from V1 to V3 (E-OCVM concept lifecycle model). Ideally, the POC/VLD preparation phase should be carried out during V1. Depending on the criticality of the ATM functionality to be demonstrated, the approval phase and execution phase of proof of concept can start at V3 or V3+:

- At V3+, with early industrial product for airborne or ground systems to ensure safe flight & safe ATM and for which no acceptable solution can be found with pre-operational product. Only early operational product can be used, typically FMS implementing 4D.
- At V3, for non-critical ATM functionality, when pre-operational products (pre-industrial prototypes) are built, integrated and partially validated as illustrated in **figure 4** below:

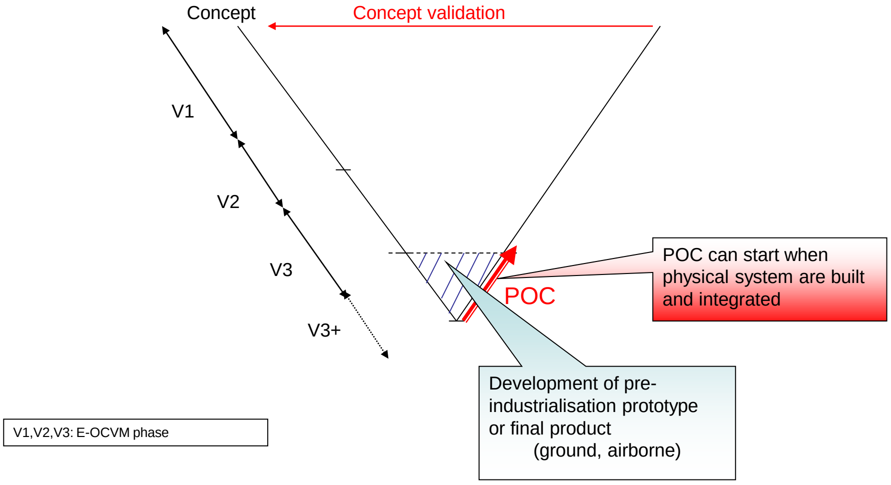

Concept
Concept validation
V1
V2
V3
V3+
POC
POC can start when physical system are built and integrated
Development of pre-industrialisation prototype or final product (ground, airborne)
V1,V2,V3: E-OCVM phase

Figure 4: V&V cycle and POC/VLD

5.2 Proof of Concept, V&V and Certification process relationship

The Proof of Concept shall be distinguished from traditional Verification and Validation activities, as illustrated in **figure 5** below, that will serve certification / approval of final products. Laboratory tests, simulator sessions and flight testing are appropriate means to verify system safety & performance at the different phases of the product development. Proof of Concept is appropriate means to verify the achievability of the benefits for the ATM community.

As such, V&V activities are appropriate means to assess maturity and acceptability of the SESAR operational and technical solutions for POC/VLD trials. Proof of Concept / Very Large Demonstration approval phase can start when all relevant V&V activities of the SESAR proposed solution have been successfully carried out, e.g. V3 or V3+ (concept, system architecture, development and test of subsystem/individual equipment). The results of all these V&V activities will provide an accurate indication on the level of maturity of the VLD project before deciding to go in the approval/execution phase.

In addition, compliance of pre-operational products or early industrial products with the regulatory framework applicable to each domain (ATM/ANS, Airworthiness, and Flight Ops) shall be shown to be satisfied. The regulatory aspect is certainly the most challenging area for an operational trial in particular for innovative solutions and/or brand new operational procedures. In order to show compliance against the regulatory framework, performances of pre-operational products should generally be complemented by “human monitoring” and back-up procedures including during normal aircraft / ATM operations.

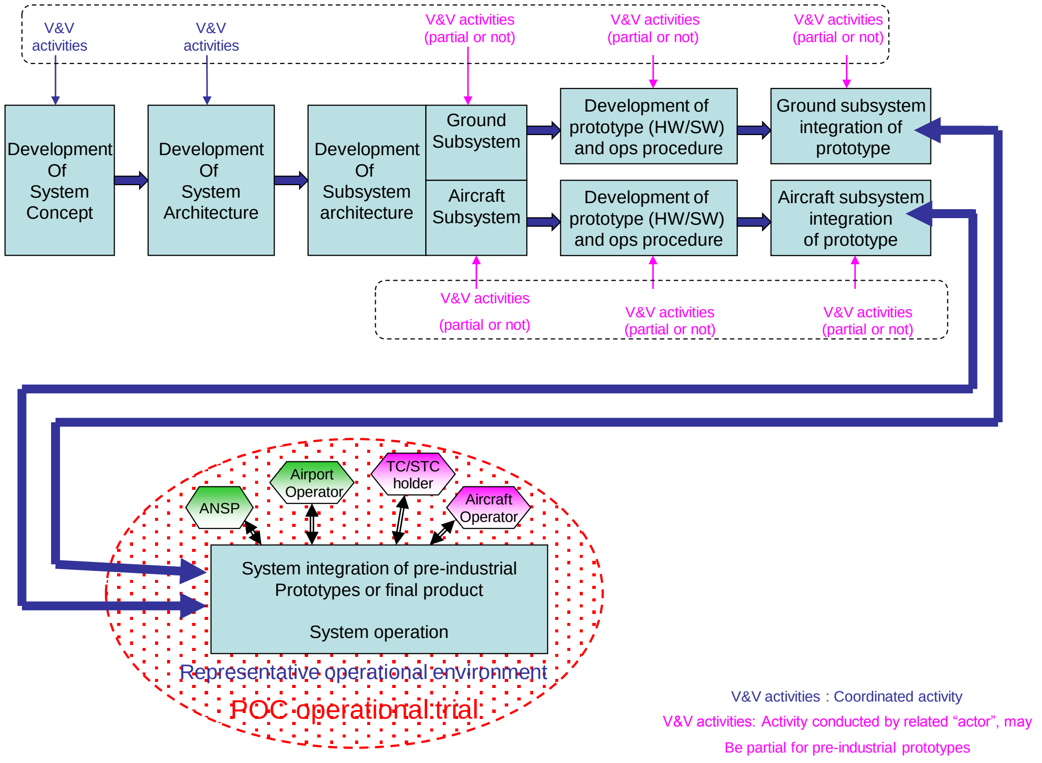

V&V activities
V&V activities
V&V activities (partial or not)
V&V activities (partial or not)
V&V activities (partial or not)
Development Of System Concept
Development Of System Architecture
Development Of Subsystem architecture
Ground Subsystem
Aircraft Subsystem
Development of prototype (HW/SW) and ops procedure
Development of prototype (HW/SW) and ops procedure
Ground subsystem integration of prototype
Aircraft subsystem integration of prototype
V&V activities (partial or not)
V&V activities (partial or not)
V&V activities (partial or not)
Airport Operator
TC/STC holder
ANSP
Aircraft Operator
System integration of pre-industrial Prototypes or final product
System operation
Representative operational environment
POC operational trial
V&V activities : Coordinated activity
V&V activities: Activity conducted by related “actor”, may Be partial for pre-industrial prototypes

Figure 5: POC/VLD within the development lifecycle process

The following **Figure 6** illustrates the different types of assessment (safety, risk) to be carried out when POC/VLD is conducted.

It should be noted that we intentionally make a distinction between safety assessment and risk assessment. This is considering there may be other risks than safety risks. For the VLD, the Network Manager or Deployment Manager may identify risks based on their specific criteria (financial, industrial, performance…).

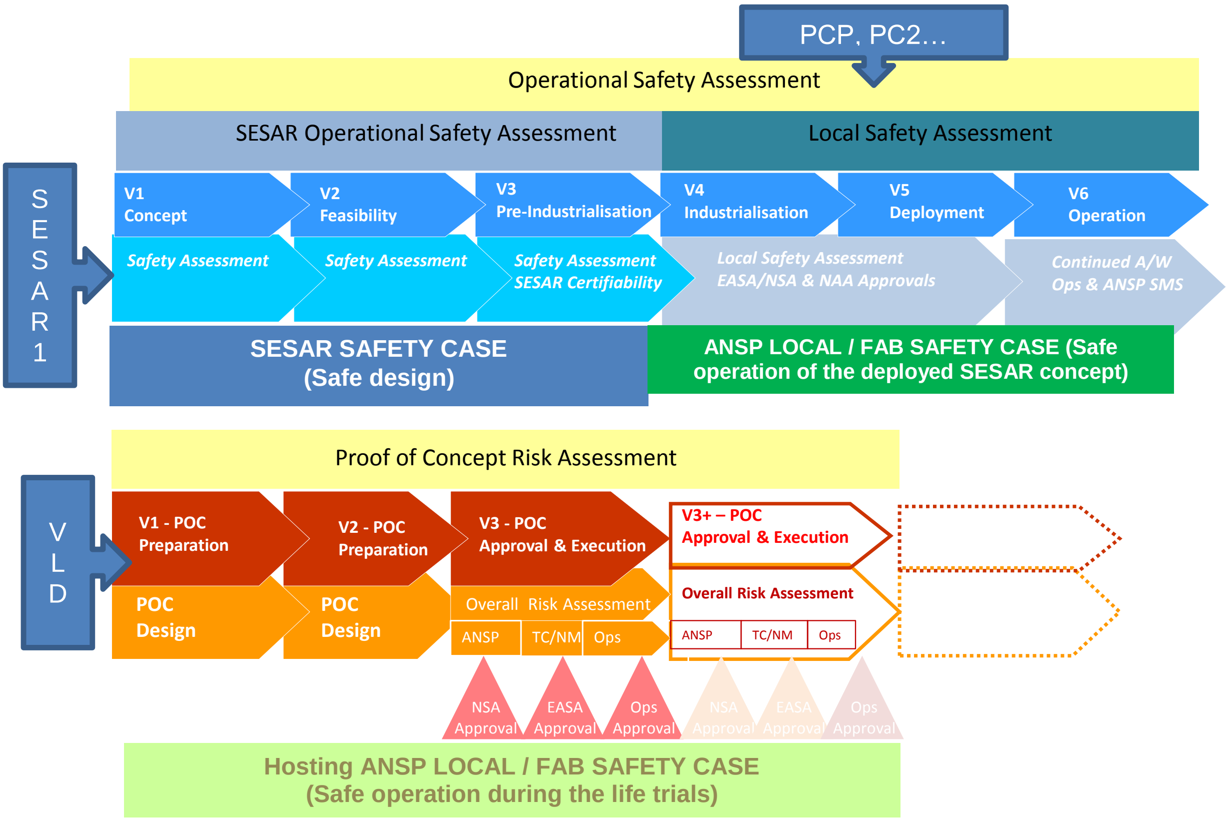

PCP, PC2…
Operational Safety Assessment
SESAR Operational Safety Assessment
Local Safety Assessment
S E S A R 1
V1 Concept
V2 Feasibility
V3 Pre-Industrialisation
V4 Industrialisation
V5 Deployment
V6 Operation
Safety Assessment
Safety Assessment
Safety Assessment SESAR Certifiability
Local Safety Assessment EASA/NSA & NAA Approvals
Continued A/W Ops & ANSP SMS
SESAR SAFETY CASE (Safe design)
ANSP LOCAL / FAB SAFETY CASE (Safe operation of the deployed SESAR concept)
Proof of Concept Risk Assessment
V L D
V1 - POC Preparation
V2 - POC Preparation
V3 - POC Approval & Execution
V3+ – POC Approval & Execution
POC Design
POC Design
Overall Risk Assessment
ANSP
TC/NM
Ops
Overall Risk Assessment
ANSP
TC/NM
Ops
NSA Approval
EASA Approval
Ops Approval
NSA Approval
EASA Approval
Ops Approval
Hosting ANSP LOCAL / FAB SAFETY CASE (Safe operation during the life trials)

Figure 6: Safety / Risk Assessment Activities related to POC/VLD

The SESAR Operational Safety Assessment conducted for a SESAR solution (e.g. at OFA/OI level) is addressing V1 to V3 phases. It should be noted that the industrial and deployment phases (respectively V4 & V5) are outside the scope of SESAR. The main objective of the SESAR operational safety assessment is to show that the design of the change associated to this SESAR solution satisfies the safety criteria (SAC) and therefore could be safely implemented and deployed.

The POC/VLD Risk Assessment has to show that air operations in the operational environment where POC/VLD trial will be conducted are acceptably safe while satisfying the scope & goals of the VLD. The "acceptability" criteria will have to be established considering the specificities of the trial and accepted by the authorities. In addition, for the pre-operational product, it is agreed that an "operational stopping" criteria is defined in order to revert safely to normal ATM operation at any moment during the trial e.g. due abnormal or failure conditions.

The POC/VLD Risk Assessment should be composed of:

- The overall risk assessment performed by the VLD project for coordinating the different approvals needed from each competent authority.
- The local ANSP Safety Assessment or/and the local Airport Safety Assessment,
- The Network Manager Safety Assessment,
- The TC/STC holder Safety Assessment and,
- The aircraft operator Safety Assessment.

It has to be noted that in some cases, the local ANSP Safety Assessment may be

- *Complemented or replaced by the FAB Safety Case for the trials,*
- *Complemented by the local Airport operator safety assessment when installation of equipment in the aerodrome is required to execute the VLD.*

The POC Risk Assessment conducted at V3 or V3+ is rather similar in principle except that for a risk assessment conducted at V3 level only prototype are available whereas at V3+ level industrial products are available which should ease the approval process.

Based on the figures 5 and 6, the following figure 7 is illustrating the relationship between the project lifecycle development, POC/VLD and the different assessments to be produced. These assessments are:

- For the POC/VLD live trials: the POC/VLD risk assessment
- For the design of the SESAR solution: the SESAR Operational Safety Assessment.
- For the deployment of the SESAR solution: the Local Safety Assessment.

As shown in **Figure 7**, the results of the V&V activities (evidence) carried out during V1, V2 and V3 are feeding the POC/VLD risk assessment and the SESAR operational safety assessment for the SESAR solution. Their main objectives are towards the later one but they participate also to demonstrate that a sufficient level of maturity of the SESAR solution is reached to execute POC/VLD.

The POC/VLD execution can be launched only when the POC/VLD risk assessment has demonstrated that the exercise can be conducted safely and according to expectations. POC/VLD results will in turn feed the SESAR operational safety assessment as new evidence.

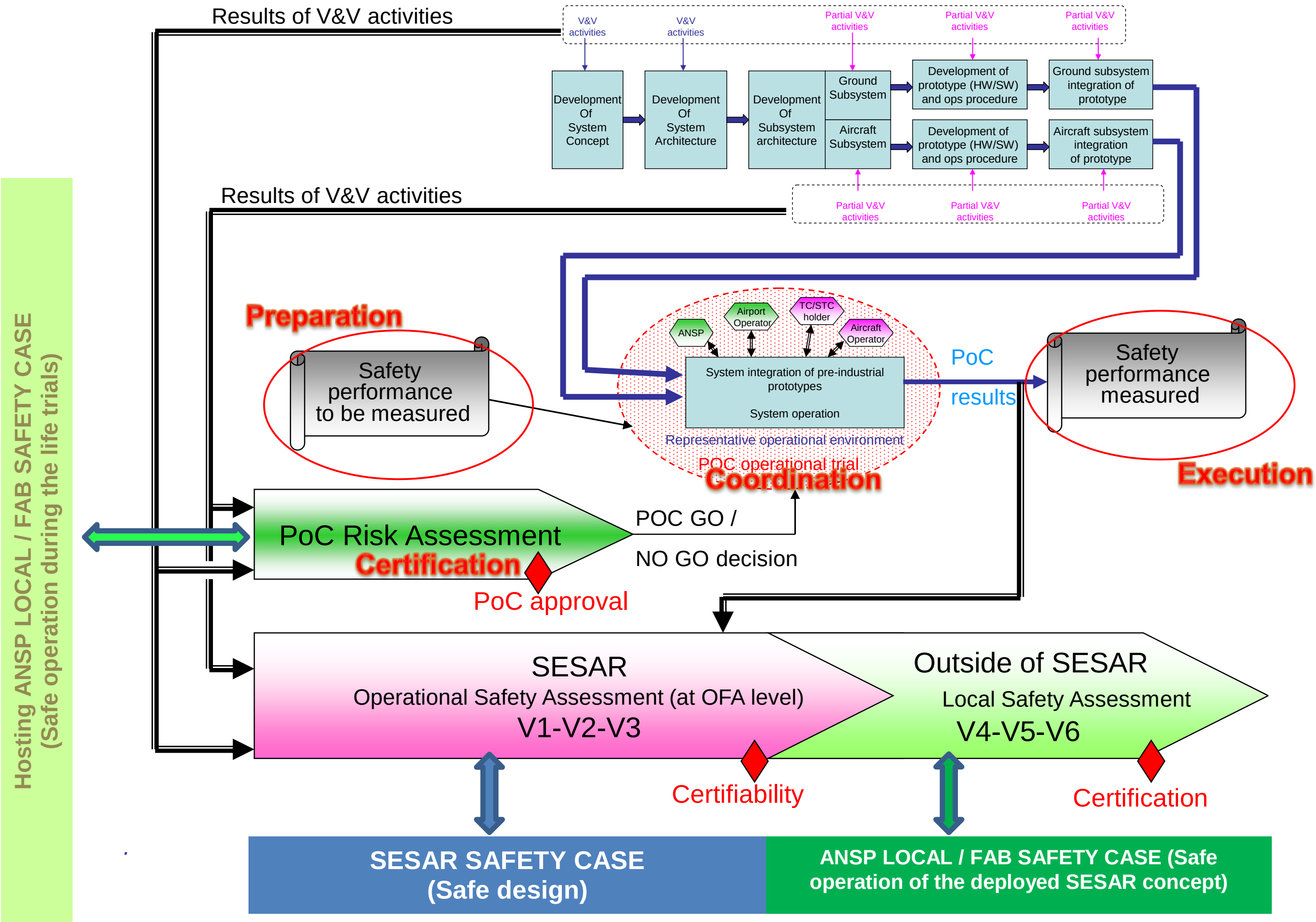

Results of V&V activities
V&V activities
V&V activities
Partial V&V activities
Partial V&V activities
Partial V&V activities
Development Of System Concept
Development Of System Architecture
Development Of Subsystem architecture
Ground Subsystem
Aircraft Subsystem
Development of prototype (HW/SW) and ops procedure
Development of prototype (HW/SW) and ops procedure
Ground subsystem integration of prototype
Aircraft subsystem integration of prototype
Partial V&V activities
Partial V&V activities
Partial V&V activities
Results of V&V activities
Preparation
Safety performance to be measured
ANSP
Airport Operator
TC/STC holder
Aircraft Operator
System integration of pre-industrial prototypes
System operation
Representative operational environment
POC operational trial
Coordination
PoC results
Safety performance measured
Execution
PoC Risk Assessment
Certification
POC GO / NO GO decision
PoC approval
SESAR
Operational Safety Assessment (at OFA level)
V1-V2-V3
Outside of SESAR
Local Safety Assessment
V4-V5-V6
Certifiability
Certification
SESAR SAFETY CASE (Safe design)
ANSP LOCAL / FAB SAFETY CASE (Safe operation of the deployed SESAR concept)
Hosting ANSP LOCAL / FAB SAFETY CASE (Safe operation during the life trials)

Figure 7: POC/VLD development lifecycle and assessment relationship

5.3 Phases and Steps to follow for POC/VLD

The **Figure 8** below shows the different phases and steps to be followed during proof of concept / very large demonstration. All these phases and steps are fully detailed in Section 7 for the governance aspect, Section 8 for the preparation phase, Section 9 for the approval phase and Section 10 for the execution phase.

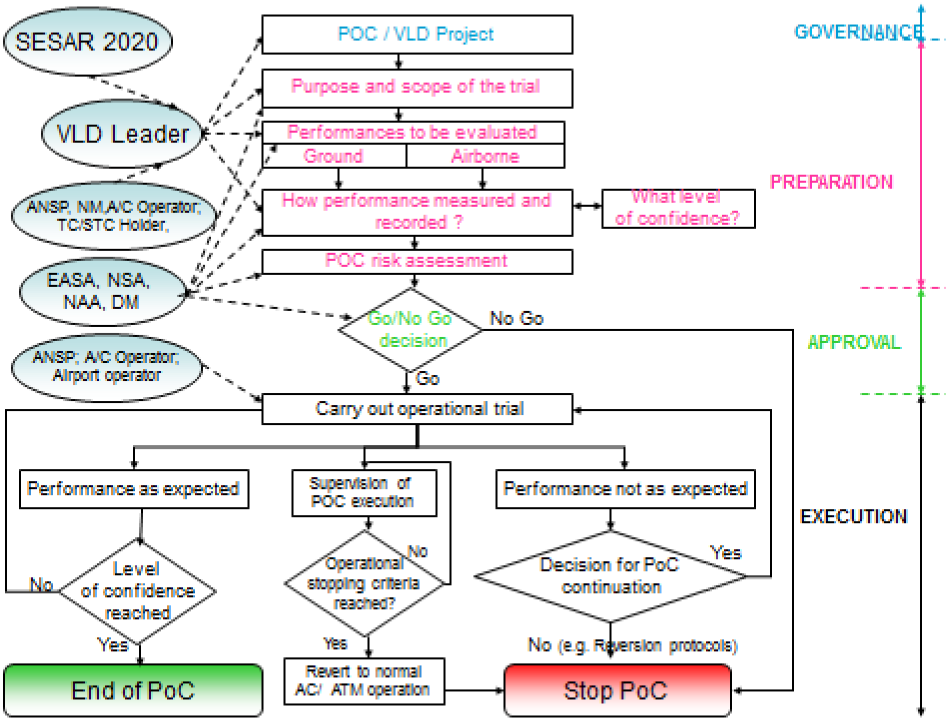

SESAR 2020
VLD Leader
ANSP, NM,A/C Operator, TC/STC Holder,
EASA, NSA, NAA, DM
ANSP; A/C Operator; Airport operator
POC / VLD Project
Purpose and scope of the trial
Performances to be evaluated
Ground
Airborne
How performance measured and recorded ?
What level of confidence?
POC risk assessment
Go/No Go decision
No Go
Go
Carry out operational trial
Performance as expected
Supervision of POC execution
Performance not as expected
Level of confidence reached
No
Yes
Operational stopping criteria reached?
No
Yes
Decision for PoC continuation
Yes
No (e.g. Reversion protocols)
End of PoC
Revert to normal AC/ ATM operation
Stop PoC
GOVERNANCE
PREPARATION
APPROVAL
EXECUTION

Figure 8: Phases and Steps of POC/VLD

6 Coordinated & Integrated Approach

6.1 Holistic Approach (Performance & Safety)

There are two essentials aspects associated to POC/VLD that should be addressed:

1. Confirm with the POC/VLD exercise that the identified performances (safety, capacity, and efficiency, environment....) to support the SESAR business case are reachable. The performances to be evaluated (impacting safety, capacity, efficiency, environment....) are normally identified from draft SPR and it should be proved, through wide scale live trial, that those performances are reachable in a representative environment.

   The SESAR OSED/SPR/TS documents will contribute to the development of the industrial standards produced by the international standardization organizations (e.g. EUROCAE/RTCA); standards which through the applicable national procedures are defined as acceptable means of compliance. The Proof of Concept supports the validation or confirmation of the functional & safety & performance requirements which will contribute to the final industrial standards

2. Demonstrate that during the POC/VLD exercise the safety is not compromised. The Competent Authorities will have to approve the installation and use of industrial products or pre-industrial products. For the pre-industrial products, ad-hoc mitigations satisfying the applicable requirements could be proposed to compensate the possible lack of design assurance. The POC/VLD risk assessment that includes the safety assessments performed by TC/STC holders, the aircraft Operators, NM and ANSP/ADR will be submitted to support Competent Authorities Approvals (EASA, NAA and NSA) under EASA coordination.

6.2 Coordinated Requirements (Performance & Safety)

The transition to new concept / technology, performance based concept, introduces new dependencies between Airborne/ Ground equipment and Pilot / Controller procedures that require a new approach for ATM risk assessment by considering the ATM system which is changed in a holistic way (end-to-end).

Within SESAR and for each SESAR solution, OSED/SPR/TS documents provide –inter alia- a set of operational requirements, performance requirements and safety requirements.
Those requirements are derived using SESAR engineering processes.

The safety "performances" are derived in accordance with the SESAR Safety Reference Material (SRM) process (new integrated approach to ATM safety assessment) which includes a success approach and a failure approach. The combination of these two perspectives is called the broader approach. Safety "performances" to be validated during POC/VLD are those derived during the success approach. Literally translated, it means identifying what benefits should be delivered by the SESAR solution from a safety perspective in normal conditions to e.g. reduce the number of ATC tactical conflict, level burst, etc.

6.3 Coordinated Authority Involvement

A dedicated process will have to be set up to initiate the involvement of the stakeholders who will have to support, monitor and approve the demonstration. The competent authorities of each domain (A/W, ATS & OPS) as well as the network manager and the deployment manager will have to be informed in a synchronized manner of the VLD goals & scope, planning, role of each one. The EASA should discuss with the European Commission to find out what could be the best solution.

In the meantime, here below what may be done at local applicant and VLD Project levels:

- Initiate approval process for each impacted domain using existing forms & current practices,

- Organize a kick-off meeting to define the details of the coordination arrangements between the facilitators (EASA, NSA, NAA and DM). The outcome of that meeting will serve as basis for the “Project Interface Document” [PID].

> *The PID is an overarching document to clearly explain the new dependencies being introduced by the VLD Project. The PID should include all the relevant information that need to be shared between the competent authorities and SESAR Deployment Manager.*

6.3.1 Airworthiness Process Initiation

The early involvement of the EASA in the VLD could be done in different ways, each with its own pros & cons:

- TC/STC Holder to submit an application for Major Change FORM 31 / FORM 33 (without MOD N°) for experimentation (well-known process but needs EASA Management decision).
- Other solutions to be explored with EASA Technical Advise Contact (TAC).

Note: Permit to Fly is not fit for purpose (commercial flights).

> *It should be noted that the solution best adapted to the needs will be decided on a case by case basis, but for the sake of simplicity, the general process of FORM 31/ FORM 33 for initiating early discussion with EASA is retained in the rest of the document.*

6.3.2 Notification of Change in the ATC System

The early involvement of the NSA in the VLD could be done following the current practices:

- ANSP to provide the Notification of Change for life trials without particular FORM, but mentioning VLD as criteria for NSA involvement.

6.3.3 Application for Specific Aircraft Operator Approval

The early involvement of the NAA in the VLD could be done following the current practices:

- Air Operator Certificate Holder to submit the application for specific approval mentioning VLD as criteria for NAA involvement.

6.4 Coordinated Risk Assessment & Approval

The POC/VLD Risk assessment incorporates the overall risk assessment, the local safety assessments and the coordination of the safety demonstration / approval.

The POC/VLD Risk Assessment results will support the decision to conduct the operational trials.

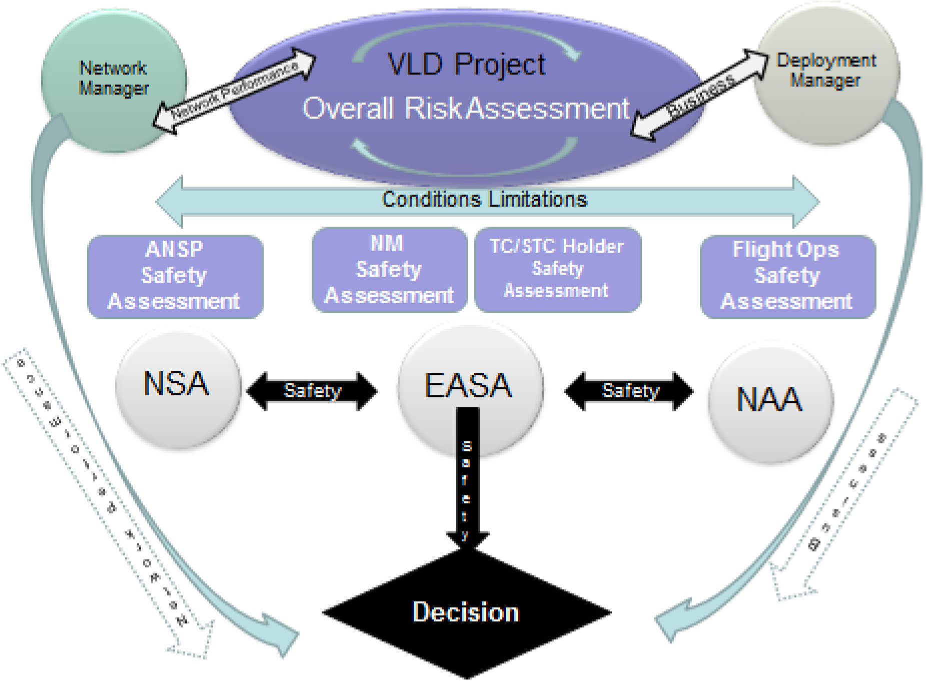


Figure 9: POC/VLD Risk Assessment

6.4.1 Overall Risk Assessment

The overall risk assessment addresses all identified risks linked to the goal & scope of the VLD:

- Certification / Safety,
- Performance,
- Business.

The overall risk assessment is detailed in section 8, covered by Risk #01 & Risk #02 for certification / safety risks. This activity is led by the VLD project in close collaboration with the safety specialists responsible for the local safety demonstrations. It sets the scene for the conditions and limitations of the life trials (mixed traffic, need for operational stopping criteria, contingency plan, performance, human task analysis, training needs…) under which the approvals are granted. This task will pave the way towards the three or four independent safety assessments that will be performed locally by the TC/STC Holder, NM, ANSP and or Aerodrome operation and the aircraft operator.

The overall risk assessment is also developed in cooperation with the network manager and the deployment manager to cover the business and performance risks versus the overall goals of the VLD.

The overall risk assessment will be submitted to the authorities for review.

6.4.2 Approval Coordination

EASA will have a key role to play in:

- Validating and approving the overall risk assessment and in particular the Conditions and limitations resulting from this analysis and that will have to be considered for the local safety assessments.
- Reviewing and coordinating the local safety assessment, ensuring the assumptions taken locally are correctly managed, validated and properly documented in the “Conditions & Limitations” document attached to the approval.
- Coordinating the local approvals,
- Providing inputs regarding the safety of the trials to support the decision to perform the VLD.

6.5 Liaison Documents

It is proposed to submit respectively the following documents to Competent Authorities:

- During Preparation Phase:
    - "POC/VLD "Intent" dossier (summary of the VLD Technical Dossier) submitted to all Competent Authorities providing details on the POC/VLD exercise (purpose, scope, mitigating measures, performances to be evaluated, performance measurement and recording). Such dossier is described in Section 8.5 (Preparation Phase Step 5 - *Docu#01)*
    - "POC/VLD "Risk" dossier (Overall Risk Assessment & Initial coordinated "Conditions/Limitations" document) submitted to all Competent Authorities providing details on the POC/VLD live trials from a safety perspective (potential hazards on all domains, coordinated assumptions and risk mitigations). Such dossier is described in Section 8.5 (Preparation Phase Step 5 - *Docu#02)*
    - The local Safety Assessments submitted to the relevant Competent Authorities:
        - ANSP POC/VLD Safety Assessment to NSA, *Risk#03*
        - ADR POC/VLD Safety Assessment to NAA, *Risk#03*
        - Airworthiness POC/VLD Safety Assessment to EASA, *Risk#04*
        - Network Manager POC/VLD Safety Assessment to EASA (if relevant), *Risk#03*
        - Flight Ops POC/VLD Safety Assessment to NAA, *Risk#05*

In some cases, attendance of Authorities during some POC/VLD trials may be beneficial to gain confidence on the trials and results. The discussion on the possible participation of Authorities to the POC/VLD trials should take place during the preparation phase Step 6, *Coor#01*.

- During Execution Phase:
    - Status Report sent to all Competent Authorities providing brief summary and major events on the progress of the POC/VLD trials, *Coor#03*
    - Significant results of the demonstrated performance sent to all Authorities providing main achievements of SESAR targets, *Coor#04*

7 Governance

Not every SESAR proposed solutions will be targeted for a VLD (proof of concept). The eligible criteria for proof of concept are not formally defined yet; the need for VLDs is to be confirmed on a case by case basis along the deployment oriented criteria (e.g. business case, maturity, need for air / ground and ground-ground integration, global interoperability).

The decision to launch Very Large Demonstrations on specific SESAR Solutions considering the SESAR proof of concept context (e.g. the POC/VLD Guidance Material) is part of the VLD Call for Tender (CFT). The final list of VLDs has been published as an outcome of the SESAR 2020 Steering Committee (SC05) based on DOW 0.95.

The SESAR Deployment Manager (SDM), mandated to supervise and manage the implementation of the SESAR solutions, should have a significant role in planning, synchronizing and coordinating the "early" implementation of the technical solution for the VLDs.

7.1 VLD CFT Process

The VLDs will be in two waves: VDL wave 1 is related to SESAR 1 solution (V1 – V3) validation and VLD wave 2 is related to SESAR 2020 solution (V1-V3) validation.

The organizational aspects including governance mechanisms (project organization and project management) should be finalized during the VLD CFT process. However, the SJU has already retained that for the VLD wave 1, the relevant SESAR 1 project managers should be involved to ensure complementarity and consistency with the relevant SESAR 1 validation road maps.

With respect to the representation of the POC/VLD project management in this guide, the assumption was made, for the sake of clarity and simplicity, that there will be a consistency in the VLD Project consortium between SESAR 1 and SESAR 2020 VLD wave 1; e.g. expected continuity in SESAR Operational Project in charge of the validation plan at the OFA/OI level (WP 4-15) for SESAR 1 and the designated Project Consortium in charge of the demonstration plan for the preparation and execution of the POC/VLD live trials.

7.2 POC /VLD Template

In order to ensure harmonization in the way this POC/VLD guide is applied by the various VLD Projects and also traceability between task and supporting document, a template is provided in Appendix of this document.

The POC/VLD Template has been developed at the request of EASA. This activity was set up through P16.01.04 T008 / D8 Deliverable.

It should be noted that the assumption that the POC/ VLD GM / Template is used to produce the POC/VLD Plan & Report is retained in the rest of the document.

7.3 VLD Organization

This section aims at defining the organizational structure and management of the POC/VLD project, project managed under the leadership of the SESAR VLD project leader.

This organizational structure should define how activities such as task definition & allocation, coordination and supervision are directed towards the achievement of the VLD goals.

This organizational management should define the process of organizing, planning, leading and controlling resources within the entities which can be internal (SESAR stakeholders) but also and external such as Authorities, Network Manager and Deployment Manager of the VLD project with the overall aim of ensuring a smooth transition from VLD to PCP.

Management PHASE			
Responsible Actor	***Task reference***	***Task description***	***Guidance***
VLD Project Leader	Gove#01	Describe the POC/VLD live trials purpose / scope and work arrangement within the VLD Project. Deliver POC/VLD Plan & Report compliant with POC / VLD Guidance Material, including the following information: - Project Management - Project Organization - Role in Team - Project schedule - Project Monitoring (Progress reports, key events…)	This task identifies: • The list of SESAR Projects involved, • The list of OFA / OI addressed, • The list of ATM Functionality (as per PCP) addressed, • The list of the applicable SESAR Documents, • The list of tasks including task allocation and work breakdown structure, • The list of the different actors involved in the live trials [(ANSP(s), Network Manager or Airport operator(s) hosting the VLD, the aircraft operator(s) and the TC/STC holder(s)] as well as their respective role and responsibility.
VLD Project Leader EASA	Gove#02	Define the POC/VLD live trials work arrangement within EASA Deliver the POC/VLD Plan & Report compliant with POC / VLD Guidance Material, including the following information: - Definition of Tasks and Roles of the Competent Authorities to be involved in the	This task involves determining the organizational, administrative and technical arrangement within EASA. This task is aimed at improving and streamlining the involvement of the authorities in the VLD. To secure the overall process to execute VLD, EASA should supervise the safety & certification aspects in a cross-functional approach that may

		project - Plan setting out the operational arrangement between EASA and NSA/NAA in charge of the approvals at local level. - Project Gating & Review Plan with Authorities	facilitate the discussion about the ultimate goal and to decide who is doing what and the timescales as approval authority. This task identifies: - The list of the different actors from the Competent Authorities to be involved in the live trials [NSA, NAA and EASA] as well as their respective role and responsibility. - The list of milestones and coordination arrangements between Competent Authorities and SESAR Deployment Manager
VLD Project Leader SESAR Deployment Manager	Gove#03	Define the POC/VLD live trials work arrangement within the SESAR Deployment Manager Deliver the POC/VLD Plan & Report compliant with POC / VLD Guidance Material, including the following information: - Definition of Role and responsibility of SDM in the project.	This task involves determining the cooperative arrangement within the SESAR Deployment Manager. This task is aimed at ensuring consistency between “early” and “final” implementation and smooth transition from VLD to PCP. The VLD scope & objective should be consistent with the deployment objectives and priorities. This task identifies: - The list of the different actors from the SDM as well as their respective role and responsibility. - The list of resources required to support positive business case.
VLD Project Leader Network Manager	Gove#04	Define the POC/VLD live trials work arrangement within the Network Manager	This task involves determining the cooperative arrangement within the SESAR Network Manager. This task is aimed at optimizing the resource management providing access to common resources, such as tools, processes and consistent data to support the deployment of the VLD.

			This task identifies: - The list of the different actors from the Network Manager as well as their respective role and responsibility. - The list of tasks the Network Manager can support to make a most efficient use of the resources. In particular, the Network Manager will have to ensure consistency of the VLD performance targets are aligned with the network performance targets.

8 Preparation

The preparation phase shall be managed by the OPS Task Leaders of the VLD Project and consists of five steps:

- Purpose and scope of the POC/VLD trials,
- Performances to be evaluated,
- Performance measurement and recording,
- Risk assessment of the POC/VLD trials,
- Ad-hoc dossier for Competent Authorities

The preparation phase will be conducted in a collaborative way with the different POC/VLD trials actors: ANSP(s), Network Manager or Airport operator(s) hosting the POC/VLD, the aircraft operator(s) and the TC/STC holder(s).

The following sub-sections are describing all activities to be conducted per step. Steps are proposed in a logical order as it corresponds to the implementation order however it does not prevent to proceed in a different order provided all activities are carried out.

8.1 Preparation Phase Step 1: Purpose and Scope of the POC/VLD

This step describes the process to be followed to define the context of the POC/VLD. The definition of the operational context of the POC/VLD is a key element to obtain approvals from competent authorities for the POC/VLD.

PREPARATION PHASE

Step 1 Purpose and Scope of the POC/VLD

Responsible Actor	***Task reference***	***Task description***	***Guidance***
VLD OPS Task Leader(s)2	Prep#01	Describe the POC/VLD live trial objective within the complete project validation process	This task provides the rationales for conducting the POC/VLD. Explain why a wide scale operation is necessary for the given project(s). Explain the fundamental aspects of the performance demonstration through wide scale operation. Identify the different safety and performance aspects (operational criteria, safety criteria, safety and performance requirements, validation objectives / results....) to be explored considering the available SESAR solution documents: OSED, SPR, VAL Plan / VAL Report,
VLD OPS Task	Prep#02	Describe the operational context needed for POC /	This task determines the required POC/VLD operational environment and

[2] VLD Project Stakeholders in charge of Demonstration Plan

Leader(s)		VLD trials.	the necessary operational procedures. Describe if POC/VLD will be conducted in segregated airspace or in "normal" environment. Determine such "normal" environment: traffic density (low, medium, and high), aircraft separation standard (e.g. progressively reduced so as human stress is progressively increased), secondary airport versus HUB, … Determine ad-hoc location(s) to place the trials. POC/VLD may involve multiple places, thus several ANSPs/airport operators/NSAs. Describe in a generic manner the planned ATCO and pilot procedures to be respected during POC trials. The trial operational context should provide conditions similar to those that will be encountered in service.
VLD OPS Task Leader(s)	Prep#03	Describe the necessary infrastructure/ airspace users carriage for POC/VLD trials	This task determines the technical solution to be put in place for POC/VLD. Describe what should be put in place in term of ground infrastructure (equipment, controller HMI, new NMOC release…) and aircraft equipage to satisfy the POC/VLD objective. Such description should include which category of aircraft is targeted (CAT, GA, GAT, OAT…), if mix-fleet is foreseen (aircraft equipped or not), how many aircraft have to be equipped in the considered environment, etc…
VLD OPS Task Leader(s)	Prep#04	Show that the proposed technical solution and operational procedures are sufficiently mature for the POC/VLD trials	In case of pre-operational products, provide indication on the level of maturity of these products (ground and airborne). Proof of Concept could start only when all relevant V&V activities have been successfully carried out (concept, system architecture, development and test of pre-industrial prototype). Results of V&V activities already carried out during the development process (e.g. FTS, RTS, laboratory test, shadow mode) might be used to support the maturity demonstration.
VLD OPS Task Leader(s)	Prep#05	Consult the local ANSP for feedback on feasibility (or local aerodrome operator [or Network Manager]) where POC/VLD will be carried out	ANSP(s) / ADR(s) where POC / VLD will be carried out should be consulted on POC solutions for their suitability, feasibility and operability.

ANSP/ADR[3] / NM		and involve controller, supervisor, ATSEP, [NMOC staff] in the POC/VLD trials preparation phase. The POC/VLD exercise might be conducted in different countries. In such case a consistent approach shall be defined between the different ANSPs to come up with common procedures and whenever practicable common technical solutions.	ATCO procedures (*Prep#02)* should be developed in close cooperation with the local ANSP(s)/ADR(s). When necessary appropriate ATCO training should be identified. When necessary, NMOC operator's procedures should be developed and appropriate training should be identified. ATSEP specific procedures should be developed whenever necessary (e.g. for specific equipment maintenance). In case of cross-country VLD, coordination between ANSPs and NSAs will be done according to the applicable FAB procedures.
VLD OPS Task Leader(s) Aircraft operator(s)4	Prep#06	Describe the level of involvement of the aircraft operators (airline, pilots,..) in the POC/VLD trials preparation phase	Aircraft operators should be consulted on POC/VLD solutions for their suitability, feasibility and operability. Flight crew operational procedures *(Prep#02)* should be developed in close cooperation with airspace users. When necessary appropriate flight crew training should be identified.
VLD OPS Task Leader(s) EASA and other Competent Authorities	Prep#07	Involve EASA in the POC/VLD trials preparation phase and inform other Competent Authorities (NSA, NAA) about the purpose and Scope of the POC/VLD	EASA should be consulted on VLD content & context for securing the level of assessment and coordination with the relevant competent authorities that would be required to deliver approvals in a timely manner. This task allows competent authorities to be informed in an early stage about the purpose and scope of the POC/VLD. It will set up the scene for the trial and will allow starting the arrangements and activities planning based on the involved actors.

8.2 Preparation Phase Step 2: Performances to be evaluated

This step describes the process to be followed to determine the performances to be evaluated or confirmed. The selection of key performance criteria is essential for the determination of what parameters have to be evaluated / confirmed during POC / VLD trials.

PREPARATION PHASE

Step 2 Performances to be evaluated

[3] ANSP(s) or ADR(s) where POC / VLD will be carried out, when POC / VLD is conducted in different countries, it shall include the different ANSPs or ADRs providing air navigation services during the POC /VLD exercise.

[4] Aircraft Operators involved in the POC / VLD trials

Responsible Actor	*Task reference*	*Task description*	*Guidance*
VLD OPS & Safety Task Leader(s)	Perf#01	Describe the different performances to be evaluated during the POC/VLD.	Performances to be collected and evaluated are based on requirement or assumption identified in the SESAR solution SPRs or Validation Plan. It should be determined if those identified Performance could be measured and recorded during the POC/VLD. Note: Safety Criteria (SAC) are generally defined for a given category of accident at the accident precursor level (e.g. for Mid Air Collision and if considering ASAS, tactical conflict precursors like ATC induced conflict or flight Crew induced conflict could be the performances to be evaluated during the ASAS POC/VLD).
VLD OPS & Safety Task Leader(s) TC/STC holder(s)[5] Aircraft operator(s)	Perf#02	Identify the performance to be evaluated at the aircraft level and the associated Pass/Fail criteria	Indicate SAC or performance requirements associated to flight crew or airborne equipment coming from relevant Project Deliverables (SPRs or Validation Plan / Report). Consideration of the SESAR solution SPR or Validation Plan / Report is essential at that stage to identify the performance to be evaluated or confirmed. The Pass/Fail criteria are defined so as to ensure the quality of the measures for a fruitful post trial analysis. For all performance requirements to be evaluated / confirmed during POC/VLD, these criteria should be determined based on the applicable SPR or OSED (e.g. accuracy, statistical value to be reached, etc...)
VLD OPS & Safety Task Leader(s) ANSP/ADR NM	Perf#03	Identify the performance to be evaluated at the ground level and the associated Pass/Fail criteria	Indicate SAC or performance associated to controller, NMOC operator or ground equipment coming from relevant Project Deliverables (SPRs or Validation Plan / Report). Consideration of the SESAR solution Validation Plan / Report is essential at that stage to identify the performance to be evaluated / confirmed. It should be noted that certain precursors/proxies like the number of aircraft/pilot induced conflict, tactical conflicts, runway incursions could be evaluated by the ANSP(s) if deemed

[5] TC / STC holder(s) involved in POC / VLD trials

			relevant. The Pass/Fail criteria are defined so as to ensure the quality of the measures for a fruitful post trial analysis. For all performance requirements to be evaluated / confirmed during POC/VLD, these criteria should be determined based on the applicable SPR or OSED (e.g. accuracy, statistical value to be reached, etc...)
VLD OPS & Safety Task Leader(s) TC / STC holder(s) Aircraft Operators ANSP/ADR/NM	Perf#04	Make the link between the performance to be evaluated against reference case and the measurable parameters / indicators to satisfy with the objective of the POC/VLD trials.	This task shall be carried out in two phases: - 1- Define metrics associated to the performance of the SESAR solution to be evaluated in comparison with the reference case (baseline scenario) (*Ex: if SAC is related to the number of pilot induced conflict then metrics could be associated to the aircraft lateral or vertical deviations).* 2 - Establish the list of the parameters / indicators which can be measured in correlation with the metrics (expected performance & baseline performance). (Ex: if the metrics is associated to the aircraft vertical deviations then the following parameters / indicators are relevant: pilot handling error causing level bust, aircraft technical failure causing level bust, ACAS RA causing level bust, weather causing level bust...

8.3 Preparation Phase Step 3: Performance measurement and recording

The performance criteria identified for a large scale validation through proof of concept shall be measurable with an adequate level of confidence.

PREPARATION PHASE ***Step 3 Performance measurement and recording***			
Responsible Actor	***Task reference***	***Task description***	***Guidance***
VLD OPS & Safety Task Leader(s)	Meas#01	Describe how flight crew performance (*Perf#02 & Perf#04)* will be measured and recorded	Human Factor is an essential element to be considered during POC / VLD by gathering, recording and analyzing feedback from pilots on the operational use of the SESAR

TC/STC holder(s) Aircraft operator(s)			change. There should be specific information to be recorded to allow a post flight data processing. As a minimum, those data must inform: - about the success of the trial (e.g. satisfactory if completed as planned) - about the reason for unsatisfactory trials - about the necessary information to be collected via Flight Crew /ATCO reports and questionnaires.... - about the operating or crew factors, such as: dispatch under MEL, CDL, experience on type, route/airport familiarization, duty time, weather conditions, NOTAMs... - on the adherence of the staff to the live trials scenarios
VLD OPS Task Leader(s) TC/STC holder(s) Aircraft operator(s)	Meas#02	Describe how airborne equipment performance will be measured and recorded	The TC/STC holder should explain how to use the existing hardware and software platform to measure and record the equipment performances identified in *Perf#02* & *Perf#04*.
VLD OPS & Safety Task Leader(s) ANSP/ADR	Meas#03	Describe how controller performance will be measured and recorded	Human Factor is an essential element to be considered during POC by gathering, recording and analyzing feedback from controllers on the operational use of the SESAR change and more generally stressing adherence of their staff to the live trial scenarios. The ANSP(s) (or ADR operators) should define the hardware and software based platform to measure and record the controller performances identified in *Perf#03 &Perf#04*. When several ANSPs / ADRs are involved, compatible tools & methods shall be defined to ensure consistency of the results. Use of tool like the SPV (Separation Performance Visualizer) can complete the current safety measures and provide a holistic picture of controller separation performance. Indeed SPV predicts the aircraft trajectory and dynamically defines the closest

			approach distance between two aircrafts. If the predicted closest approach distance in the horizontal or vertical plane is less than the separation minima, then the situation will be classified as a potential loss of separation. When a potential loss is detected, the tactical controller's actions to resolve that conflict are recorded. For more information, see SESAR Safety Reference Material (SRM) appendix on the gaining safety insights in real-time Human-in-the-loop (HITL) simulations. Data acquired from suitable instruments can be supplemented by the use of rating scales. For example, workload and task difficulty scales can be used to demonstrate acceptable levels of performance or to show the extent of any performance enhancement.
VLD OPS & Safety Task Leader(s) ANSP/ADR/NM	Meas#04	Describe how ground equipment performance or network performance will be measured and recorded	The ANSP (or ADR operator) should define the necessary hardware and software platform to measure and record the equipment performances identified in *Perf#03* & *Perf#04*. When several ANSPs / ADRs are involved, compatible tools & methods shall be defined to ensure consistency of the results. The Network Manager should define the necessary hardware and software platform to measure and record the network performance identified in *Perf#03* & *Perf#04*.
VLD OPS & Safety Task Leader(s)	Meas#05	Determine the minimum POC / VLD duration (exposure time) necessary to reach an acceptable of level of confidence to draw conclusive results.	Define the conditions of the tests that would be necessary to solve the concept uncertainties. The sample size used should be sufficient to ensure that the results obtained during the POC trials will be representative of the likely in-service performance. Determine the minimum number of e.g. Flight hours, departure, arrival and/or landing to reach the necessary level of confidence.
VLD OPS Task Leader(s)	Meas#06	Establish a process to record relevant trial data for archiving and traceability purposes (e.g. central repository system & process).	An appropriate format shall be defined to store all the results in a consistent and manageable way. Flight crew/air operator and ATCO/local ANSP/ local ADR operator/NM will have to report

			their results in such defined format.
VLD OPS & Safety Task Leader(s)	Meas#07	Identify the different safety assurance activities where POC/VLD will be used to provide safety evidence.	The POC/VLD Intent Dossier should identify the different safety assurance activities which rely on the results of the POC/VLD in order to obtain or confirm appropriate safety evidence.
VLD OPS Task Leader(s)	Meas#08	Identify and summarize performances to be evaluated / confirmed (with pass/fail criteria) and measured during POC / VLD trials in the POC/VLD Intent Dossier	The POC/VLD Intent Dossier should include a specific section addressing the POC/ VLD objectives, the performances to be evaluated or confirmed and how they will be measured and recorded.

8.4 Preparation Phase Step 4: POC/VLD Risk assessment

This step should show that POC/VLD trials could be executed safely.

PREPARATION PHASE

Step 4 Risk Assessment

Responsible Actor	***Task reference***	***Task description***	***Guidance***
VLD OPS & Safety Task Leader(s) ANSP/ADR/NM TC/STC holder(s) Aircraft operator(s)	Risk#01	Identify the regulatory framework applicable to the POC/VLD from the three perspectives: • Service provider / aerodrome operator (including also the ground equipment aspect) and Network Manager if needed • Aircraft operator (Flight OPS aspect) • TC/STC holder (airworthiness aspect)	Explain what are the ICAO materials and OSED, SPR, INTEROP applicable to the project (if any). Describe the applicable SES, EASA regulations and national regulations: • Applicable SES & EASA regulations: see § 2.4 and 2.5. • Applicable national regulations depend on the POC/VLD location(s). POC/VLD may involve several ANSPs in different countries/ NSAs. *Note: When all the ANSPs involved in the VLD belong to the same FAB, it may be envisaged, on a voluntary basis, that the local safety cases are harmonized between the ANSPs and the NSAs through the FAB Safety Case as specified in IR N°176/2011(IR Annex Part II). The Article 9a (2) of Annex Part II describes the collaborative Safety Process (e.g. common safety policy, description of arrangements,…) applicable within a given FAB.*

VLD OPS & Safety Task Leader(s) ANSP/ADR/NM TC/STC holder(s) Aircraft operator(s)	Risk #02	Identify in a collaborative way the potential risks associated with the trial in order to conduct properly the different Assessments (ANSP, NM, Airworthiness and Flight Ops)	The main objective of this task is to have a collaborative process between all stakeholders which should lead to the same understanding of risk associated to the execution of POC/VLD trials. The type of risk assessment undertaken will vary depending upon the safety criticality of the SESAR change (En route, TMA, approach …). The risk assessment shall assess the impact of the POC/VLD trial on current ATM System encompassing people, procedures and equipment from the ground and airborne sides. The following aspects shall be identified and validated during this collaborative process: *Operational Hazards *Common assumptions and common risk mitigations *Most probable outcome of the operational hazard in term of severity. It should be identified if EATMN interoperability could be affected by the POC / VLD trial especially for flights not participating to the trials (e.g.; operation in non-segregated airspace). The risk assessment will have to define “operational stopping” criteria which will permit to revert safely to normal ATM operation via the reversion to standard procedure. The “operational stopping” criteria will have to be defined at the aircraft level (flight crew) and at the ATC level (controller). The stopping criteria should be determined in order to prevent sufficiently in advance any infringement (e.g. before the separation infringement). The contingency plan (including reversion & transition procedures) should be developed by considering the SESAR solution under POC / VLD. When POC/VLD is conducted in different countries, the operational stopping criteria in the different countries / sectors / aerodromes and the different contingency plans must be coherent between them. Stopping criteria should not be mixed with pass/fail criteria. Stopping criteria are defined to maintain the safety of the flight operation during POC exercise whereas pass/fail criteria are defined to verify that the specified SESAR performances could be delivered during

			POC/VLD with the required level of quality for fruitful post trials analysis.. A good mental model is crucial for safe and efficient system use of pre-operational products. To ensure a good mental model, Human Factors / Performance analysis will be undertaken for ground and air components considering the POC context. The HP analysis will include, but not necessarily limited to: - Task analysis and subsequent cognitive task analysis of the expected controller and pilot activities - Analysis of the deltas between current and expected behaviors - Predictions of impacts on ground and air situational awareness and workload - Prediction analysis and design resolution of any potential human errors. The analysis described above will be used to drive a series of mitigation activities that will include: - Training needs analysis focusing on the expected impacts of the change and considering the partial validation of products - Staffing, in terms of roles to be performed, numbers and experience - Human engineering design recommendations to ensure best design and the avoidance of non-revealed failures - Fall back and contingency procedures for management of degraded modes in particular when operational stopping criteria are reached. - Close alignment with safety and the deliverance of assurance activities that claims made for safety can be satisfied by the operators (ground and airside)
ANSP/ADR/NM	Risk #03	Carry out a local safety assessment to identify any hazards or risks that may be encountered during the trial from an ANSP or ADR	This safety assessment shall be carried out considering of *Risk#01*. The ANSP/ADR is the local ANSP/ADR

		perspective and eventually from a Network Manager perspective.	hosting the POC trials. This safety assessment should be built on the outcome of *Risk#02* and should consider the local implementation aspect (technical and operational). Based on safety assessment results, fallback procedures might be necessary in such case an “ATCO operational stopping” criteria shall be clearly identified to indicate when controllers shall revert to standard procedures. It might be necessary, for certain operational trials, to have a “shadowing” controllers helping recognition of such situation necessitating reversion or contingency procedures. Finally the safety assessment shall consider – inter alia- effect on adjacent sectors, on operations conducted by aircraft operators not participating to the POC / VLD trials, on military operations,...., The reversion back to normal ATM conditions should be performed in a manner and with a response time such that safety is preserved. Controller shall be properly trained for the operation associated to the POC / VLD trials. Controller shall be able, at any moment, to deliver a safe ATS services to airspace users in case of failure of the SESAR solution under POC. When POC/VLD is conducted in different countries / sectors / aerodromes, each ANSP/ADR will have to carry out its local safety assessment and to define its local contingency plan in coordination with the other ANSP(s)/ADR(s) to ensure consistency of the overall risk assessment for the POC /VLD trials.
TC/STC holder(s)	Risk #04	Carry out an airborne safety assessment (airworthiness) to identify any hazards or risks that may be encountered during the POC/VLD trial.	The safety assessment shall be carried out considering of *Risk#01* and in accordance with the applicable regulation (e.g. CS25.1309). This safety assessment should be carried out by each TC/STC holder involved in POC /VLD trials. This safety assessment should consider the outcome of *Risk#02*. It should determine whether the technical solution is safe or not considering the operational hazard and the associated Severity identified during *Risk#02*. Any type of limitation should be identified and

			promulgated (e.g. through AFM). The design of the airborne system shall consider that any failure shall not impact the airworthiness of the aircraft. For that purpose, reversion to the "fully certified" aircraft functions (e.g. basic aircraft) should be possible at any moment in a manner and with a response time such that safety is preserved.
Aircraft operator(s)	Risk #05	Carry out an operational safety assessment to identify safety risks that may be encountered during the trial.	This safety assessment shall be carried out considering *Risk#01.* This safety assessment should be carried out by each aircraft operator involved in POC / VLD trials. This safety assessment should consider the outcome of *Risk#02*. Flight crew shall be properly trained for POC / VLD trials. Based on safety assessment results, fallback procedures might be necessary in such case a "Flight crew operational stopping" criteria shall be clearly identified to indicate when pilots shall revert to standard procedures. In such situation, the flight crew shall coordinate with the responsible controller in accordance with the contingency procedures.
VLD OPS & Safety Task Leader(s)	Risk #06	Capture in POC/VLD risk register all safety assumptions, issues, limitations and requirements (including contingency aspect). This will form the coordinated Assumptions/Conditions /Limitations file.	The safety register repository is a common placeholder identifying all safety elements to be respected by each POC/VLD trial actor (local ANSP, NM, TC/STC holder and aircraft operator) for safe POC/VLD trials. The POC risk register is fed by results of *Risk#02*, *Risk#03*, *Risk#04* and *Risk#05.*

8.5 Preparation Phase Step 5: Liaison with Authorities

This step describes the documents which will be submitted to the Competent Authorities. These activities, resulting from a collaborative work within SESAR, are aimed to support the Competent Authorities for having a holistic view of the new dependencies introduced by SESAR (see Section 6).

PREPARATION PHASE

Step 5 Documents to be delivered to Authorities

Responsible Actor	***Task reference***	***Task description***	***Guidance***
VLD OPS & Safety Task Leader(s)	Docu#01	Build ad hoc "POC / VLD intent" dossier to support approvals by EASA, NAA & NSA. (Same information delivered to all Authorities)	Based on the activities listed in Step 1, 2 and 3 of the preparation phase, provide the competent authorities with a comprehensive picture of how POC/VLD trials will be conducted (objective, context, technical solutions & operational procedures and needs for pilots & ATCO training). Furthermore the ad hoc dossier will list the performances to be evaluated / measured in order to conclude on the POC/VLD results.
VLD OPS Task Leader(s)	Docu#02	Build ad hoc "POC/VLD Risk" dossiers to support approval by EASA, NAA & NSA One "POC/VLD Risk" dossier for each Competent Authority that contains the Overall Risk Assessment + the relevant Safety Assessment dossier for each domain elaborated by the responsible actor (ANSP/ADR, Network Manager, Airworthiness and Flight Ops) submitted to the relevant Competent Authorities *(*Same information: outcome of *Risk#02* delivered to all Authorities)	Based on the activities listed in Step 4 of the preparation phase*(Risk#02)*, provide each relevant Authority with the Overall Risk Assessment and the local safety assessments for their respective domains. Outcomes of *Risk#03*, *Risk#04* & *Risk#05* in order to demonstrate that POC/VLD trials will be acceptably safe: - ANSP/ADR Safety Assessment submitted to NSA - Network Manager Safety Assessment submitted to EASA if needed. - Airworthiness Safety Assessment submitted to EASA - Flight Ops Safety Assessment submitted to NAA. Each dossier will contain an overview of the integrated safety approach which has been conducted (*Risk#02*).

8.6 Preparation Phase Step 6: Authority Involvement & Coordination

This step describes the Competent Authority procedures to achieve coordinated approvals and the integrated approach to the VLD safety. These activities, resulting from a collaborative work within the Competent Authorities, are aimed to support the coordinated approval process (see Section 6)

PREPARATION PHASE

Step 6 Coordinated Safety Assessments & Approvals

Responsible Actor	***Task reference***	***Task description***	***Guidance***
EASA RCA	Coor#01	Manage the level of involvement of the Competent Authorities, and the level of coordination needed for a given VLD (e.g. commensurate to the safety risk posed by the VLD). When potentially beneficial, organize and negotiate participation of RCA to some POC/VLD live trials. Ensure that necessary approvals are timely delivered in accordance with EASA Basic Regulation. Set up coordination arrangements establishing monitoring and supervision role of EASA in the VLD.	This task involves supporting and monitoring the activities to be carried out to ensure authorities' views are the same and not fragmented. Manage "Early" Involvement of Competent Authorities for timely delivered approvals, Support familiarization with SESAR solution to be validated by VLD; Facilitate the discussion about scope of VLD, ways for working together and timescales. Issue the supporting regulatory material [Project Interface Document] laying down the coordination arrangements among the Relevant Competent Authorities.
EASA RCA	Coor#02	Coordinate review of the Overall Risk Assessment performed by the VLD Project. Ensure consistency of the local Safety Assessment Coordinate the different approvals at local levels Coordinate the Go /No Go Decision	This task involves supervising the whole process of the VLD safety demonstration [POC/VLD Risk Assessment] Monitor the application of this guidance [POC/VLD GM) Coordinate review of Overall Risk Assessment with the Relevant Competent Authorities. Coordinate discussion on local Safety Assessments with the Relevant Competent Authorities, ensuring that all the assumptions risk mitigations made at local level are commonly agreed.

			Issue the supporting regulatory material [Conditions/Limitations" document] laying down the common assumptions & Mitigations based on results of Risk#06.

9 Approval

The approval or notification phase shall be managed by the TC/STC Holders, Aircraft operators and ANSPs/ ADR Operators, Network Manager in accordance with the applicable regulations (see §2.4 and 2.5) considering:

- NAA approval of aircraft operator,
- NSA acceptance* of service provider.
- EASA approval of new release of Network application, if needed.

> *Note*: An ANSP involved in a Proof of Concept / Very Large Demonstration will provide to his corresponding NSA the safety assessment of the related modifications of the ATM/ANS functional systems. Assumption is taken that acceptance is required: either a formal acceptance in accordance with (EU) n°1034/2011 regulation or at least an informal acceptance of the safety assessment to include a generic statement reference to the agreements between ANSP and NSA.*

Unless it is decided differently by EASA and formalized in the “Project Interface Document”, the approval phase will be conducted in two phases – the known framework: each applicant discussing with his competent authority and the new framework for the coordinated approvals under EASA supervision.

The following sub-sections are describing all activities to be conducted per step. This section is not introducing new approval process at local level; it just describes the overall approval process. This section is introduced to facilitate common understanding of all stakeholders involved in VLD Projects. On purpose this section does not detailing a lot to allow possible local adaption, e.g. introducing local flexibility.

9.1 Approval Phase Step 1: EASA Approval of the aircraft configuration / condition for the POC/VLD

This section describes the approval process at EASA level. This step lists the tasks to be carried out and provides guidance for the SESAR specific activities.

APPROVAL PHASE ***Step 1 EASA Approval of the POC/VLD***			
Responsible Actor	***Task*** ***reference***	***Task description***	***Guidance***
TC/STC Holder(s)	EASA#01	Fill and send the EASA Form 31 (TC) or EASA Form 33 (STC)- Application For Major Change. Modification with limited validity: • Limited period (about 6 months) • Limited to MSN participating to the trials (maximum 20)	This task provides EASA with the minimum information on the design change which is necessary to start involvement of EASA Specialists for a given type of POC/VLD trials.
TC/STC	EASA#02	Set up certification meetings(s) with	This task provides EASA with

Holder(s)		EASA to agree on the certification strategy specifically tailored to the operational context for the POC/VLD trials	the full picture of the operational context of the POC / VLD trials and the SESAR work which has been prepared in a collaborative way during the preparation phase (*Prep#05, Prep#06 & Risk#04).* Explain the expected benefit of POC/VLD trials from a certification standpoint for guidance see Proof of Concept Supporting Document – 16.1.4 – D04 V00.01.00. Present the proposed technical solution for airborne equipment, the operational environment / context and pilot & ATCO procedures. Present the results of the risk assessment dedicated to POC/VLD trials. When necessary, explain by which means the use of pre-operational SESAR products will be compensated by operational precautions to render the POC/VLD trials acceptably safe. Provide full cooperation to EASA to develop the Certification Review Item (CRI), addressing particular case of early industrial product or pre-operational product and making the bridge with the operational safety assessment. Present & discuss first draft of certification plan (including V&V plan). Present proposed limitations / restricted operational context to be put in the AFM. Present the operating Manual (Flight Crew & ATCO Procedures for POC/VLD Trials)
TC/STC Holder(s) EASA	EASA#03	Produce the Certification Basis	This task determines the certification & airworthiness basis applicable to a specific type of POC/VLD trials.
TC/STC Holder(s)	EASA#04	Produce the Certification Plan	This task finalizes the discussion on the certification plan to show compliance with the applicable requirements as

			per Certification Basis above; feedback to the VLD OPS Project in charge of POC/VLD Plan may be necessary if additional activities are required by EASA
TC/STC Holder(s)	EASA#05	Produce the Certification Documents (including AFM) according to certification plan.	This task corresponds to the elaboration of the relevant certification documents; maximum re-use of the material produced by the OPS Project in charge of SESAR solution validation strategy (SESAR V1-V3) during the preparation phase will be made.
EASA TC/STC Holder(s)	EASA#06	Review the compliance documents – Check the acceptability of the AFM - Approve the Major Change together with AFM if found acceptable.	The task corresponds to the review by the EASA Specialists of the compliance demonstration; the OPS Project in charge of SESAR solution validation strategy (SESAR V1-V3) should be ready to support TC/STC holder when answering EASA questions / requests for clarification.
VLD OPS Task Leader(s) TC/STC Holder(s)	EASA#07	Receive and acknowledge EASA feedback Take Go / No Go Decision	This task provides the EASA feedback to the OPS Project in charge of SESAR solution validation (SESAR V1-V3). Some changes may be required by EASA leading to iteration (e.g.; reconsidering some aspects of the preparation phase).

9.2 Approval Phase 2: NAA Approval of the Aircraft Operator for the POC/VLD

This section describes normal approval process at NAA level. This step lists the tasks to be carried out and provides guidance for the specific SESAR activities.

APPROVAL PHASE

Step 2 NAA Approval of the POC/VLD

Responsible Actor	***Task reference***	***Task description***	***Guidance***
Aircraft Operator(s)	NAA#01	Fill and send the letter of Application	This task provides NAA with the minimum information on the aircraft operation change which

			is necessary to start involvement of NAA Specialists for a given type of POC/VLD trials.
Aircraft Operator(s) VLD OPS Task Leader(s)	NAA#02	Set up meeting(s) with NAA to agree on the operational approval strategy specifically tailored to the operational context for the POC/VLD trials Decide review gate(s) to monitor progress of operational approval process.	This task provides NAA with the full picture of the operational context of the POC/VLD trials and the SESAR work which has been prepared in a collaborative way during the preparation phase (*Prep#05, Prep#06 & Risk#05).* Explain the expected benefit of POC/VLD trials from an operational standpoint for guidance see Proof of Concept Supporting Document – 16.1.4 – D04 V00.01.00. Present the proposed solution to manage mixed fleet aspects: means to track modified fleet, aircraft configuration management, dispatching rules, criteria for flight crew selection, means to ensure appropriate training. Present the results of the operational risk assessment. The POC / VLD risk register is the repository to be used during this presentation (*Risk#06*). Furthermore, the “flight crew operational stopping” criteria should be detailed at that stage of the discussion. Present the operating Manual and contingency plan (Flight Crew Procedures for POC/VLD Trials) in line with the limitations / restricted operational context put in the AFM. Present the Flight Crew training programme.
Aircraft Operator(s)	NAA#03	Finalize the applicable regulation (EC 965/2012 & National rules).	This task determines the operational approval basis applicable to a specific type of POC/VLD trials.
Aircraft Operator(s)	NAA#04	Produce the Ops Approval plan & activity roadmap	This task finalizes the discussion on the ops approval plan to show compliance with the applicable requirements; feedback to the OPS Project in charge of SESAR solution

			validation strategy (SESAR V1-V3) may be necessary if additional activities are required by NAA
Aircraft Operator(s)	NAA#05	Produce the compliance documents according to the ops approval plan.	This task corresponds to the elaboration of the relevant simulator / flight reports; maximum re-use of the material produced by the OPS Project in charge of SESAR solution validation strategy (SESAR V1-V3) during the preparation phase will be made.
NAA[6]	NAA#06	Review the operational documentation & compliance documents – Validate the Flight Crew Training programme – Authorize POC/VLD trials if found acceptable.	The task corresponds to the review by the NAA Specialists of the compliance demonstration; the OPS Project in charge of SESAR solution validation (SESAR V1-V3) should be ready to support aircraft operator when answering NAA questions / requests for clarification.
Aircraft Operator(s) VLD OPS Task Leader(s)	NAA#07	Receive and acknowledge NAA feedback Take Go / No Go Decision	This task provides the NAA feedback to the OPS Project in charge of SESAR solution validation (SESAR V1-V3). Some changes or additional activities may be required by NAA leading to an iteration (e.g. by reconsidering some aspects of the preparation phase.

9.3 Approval Phase Step 3: RCA Acceptance for the POC/VLD

This section describes Relevant Competent Authority acceptance which are not relative to TC/STC holder and Aircraft Operator. This step lists the tasks to be carried out and provides guidance for the SESAR specific activities.

When POC/VLD is conducted in different countries, different NSAs are involved in the POC/VLD acceptance process. It is recommended that a coordination process is established between the different NSAs to have consistent acceptance process.

[6] National Aviation Authority of the aircraft operator

APPROVAL PHASE

Step3 Relevant Competent Authority Acceptance of the POC/VLD [NSA for ANSP, NAA for ADR operator, EASA for Network Manager and EASA for final coordination]

Responsible Actor	*Task* *reference*	*Task description*	*Guidance*
ANSP/ADR/NM	RCA#01	Inform relevant Competent Authority (RCA) of the change impacting the ATM/ANS functional system.	This task provides RCA with the minimum information on the change to the ATM/ANS functional systems (including network application when applicable) which is necessary to start involvement of NSA/NAA/EASA Specialists for a given type of POC/VLD trials.
ANSP/ADR/NM	RCA#02	Set up meetings(s) with RCA(s) to establish the rule to authorize “proof of concept” in the airspace of the service provider responsibility, in the Network application domain field of the NM responsibility, or at aerodrome of the aerodrome operator responsibility. If necessary, establish special measures for prototype permit to use, in particular ATM/ANS systems prototypes from the ANS constituent manufacturer. Decide review gate(s) to monitor progress of the RCA approval.	This task provides RCA with the full picture of the operational context of the POC/VLD trials and the SESAR work which has been prepared in a collaborative way during the preparation phase *(Prep#02, Prep#05, Prep#06 & Risk#03).* Explain the expected benefit of POC/VLD trials from an air navigation service provider, NM, or aerodrome operator standpoint for guidance see Proof of Concept Supporting Document – 16.1.4 – D04 V00.01.00. Present the proposed technical solution for the ground systems, the operational environment / context and pilot & ATCO procedures or NM Operator. Present the proposed solution to manage mixed fleet aspects (segregated airspace, defined solution for “best equipped best served “concept...), criteria for ATCO selection, means to ensure appropriate training. Present the results of the local safety assessment dedicated to POC/VLD trials (compliant with EU 1035&1034). The POC/VLD risk register is the repository to be used during this presentation *(Risk#06).* Furthermore, the “ATCO (or NMO) operational stopping” criteria should be detailed at that stage of the discussion. Present the Operating Manual and contingency plan (ATCO *o*r NMOC Procedures for POC/VLD Trials) in line

			with the limitations / restricted operational context. Present the ATCO and when necessary NMOC personnel training programme.
ANSP/ADR/NM	RCA#03	Set up the regulatory context - Finalize the applicable regulations in accordance with the local regulation if relevant.	This task determines the regulatory basis applicable to a specific type of POC/VLD trials.
ANSP/ADR/NM	RCA#04	Produce the activity roadmap	This task finalizes the discussion on the activities to be carried out to show compliance with the applicable requirements; NSA/NAA/EASA feedback to the OPS Project in charge of SESAR solution validation (SESAR V1-V3) may be necessary if additional activities are required by NSA/NAA/EASA.
ANSP/ADR/NM	RCA#05	Produce the compliance documents according to the activity roadmap.	This task corresponds to producing the evidence to show compliance against the applicable regulation (*RCA#03*); maximum re-use of the material produced by the OPS Project in charge of SESAR validation (SESAR V1-V3) during the preparation phase will be made (ATCO, NMOC procedure, training, and result of safety assessment...) Note: (EC) 552/2004 is applicable but a DoV/C will not systematically be required.
RCA[7] ANSP/ADR/NM VLD OPS Task Leader(s)	RCA#06	Review the local safety assessment made for the POC/VLD trials – Check the POC/VLD acceptability – The competent authority authorize POC/VLD trials if found acceptable.	The task corresponds to the review by the NSA/NAA/EASA Specialists of the compliance demonstration; the OPS Project in charge of SESAR solution validation (SESAR V1-V3) should be ready to support ANSP/ADR/NM when answering NSA/NAA/EASA questions / requests for clarification.
VLD OPS Task Leader(s)	RCA#07	Receive and acknowledge NSA/NAA/EASA feedback Take Go / No Go Decision	This task provides NSA/NAA/EASA feedback to the OPS Project in charge of SESAR solution validation (SESAR V1-V3). Some changes may be required by the NSA/NAA/EASA leading to iteration (e.g.; by reconsidering some aspects of the preparation phase).

[7] National Supervisory Authority of the ANSP, National Aviation Authority for ADR Operator EASA for Network Manager.

10 Execution

The execution phase shall be managed by the TC/STC Holders, Aircraft operators and ANSPs, Network Manager or ADR operators in accordance with the preparation phase. The analysis of the results and dissemination of information will be the responsibility of the SESAR OPS Project in charge of SESAR solution validation (SESAR V1-V3). POC / VLD trials will be normally continued until necessary level of confidence is reached.

The execution phase consists of three steps:

- Execution of flight trials according to the defined procedures (flight crew and controllers / NM operator)
- Monitoring of performance to be evaluated during flight trials
- Analysis and dissemination,
- Feedback to Authorities

The following sub-sections are describing all activities to be conducted per step. A template format is used for each step to facilitate the standardization between SESAR projects. Steps are proposed in a logical order however it does not prevent to proceed in a different order provided all activities are carried out.

10.1 Execution Phase Step 1: Preparation of the Execution & Monitoring of the POC/VLD

This step describes the preparation activities to be carried when the approvals are obtained.

Execution PHASE **Step 1 Execution Initiation of the POC/VLD**			
Responsible Actor	***Task reference***	***Task description***	***Guidance***
Aircraft Operator(s)	Pre-Exec#01	Install the Service Bulletin corresponding to the EASA approved Major Change / STC for airborne system Service Bulletin with limited validity: • Limited period as agreed with EASA • Applicable to MSN participating to the trials as agreed with EASA	No guidance is needed (Airline own business)
Aircraft Operator(s)	Pre-Exec#02	Carry out flight crew training	This task is accomplished considering results of *Prep#06*.
Aircraft Operator(s)	Pre-Exec#03	Set up a line operations assessment process.	This process will address the need for developing an educated mind-set and alertness to the challenging operating context. This process will have to define the means to capture and identify the early

			key safety & performance indicators from multiple reporting schemes, such as: • Training feedback, • Operational feedback: pilots' report – air safety reports – human factors reports - Line observations – Flight data analysis – data trend analysis – deviations analysis – crew interviews.... • Organizational feedback • Information sharing This task works towards two ends, firstly to ensure that the POC/VLD trials are conducted in a safe manner (e.g. no degradation of the flight safety) and secondly to ensure that data are collected with the required quality and diversity.
Aircraft Operator(s)	Pre-Exec#04	Configure airborne recording means to support the need for measurements as identified in *Perf#04* (capture of accident/incident precursors of unsuccessful barrier, early warnings...).	The on-board flight data recording shall be capable of record the necessary data. The Flight Data Monitoring (FDM) techniques could be used to aid the assessment of the finally achieved performance. This involves: - Upgrading the aircraft parameter recording capabilities to enable FDM, and, - Collecting data from dedicated FDM software tools on the ground in a post flight analysis environment.
Aircraft Operator(s)	Pre-Exec#05	Specify Pilots 'data reporting and line observations	This task is an adaptation of *Meas#01* in line with the airlines internal processes (airline SMS). The quality and diversity of reported data is crucial for the benefits of the POC/VLD trials; due to the subtle nature of the data / information required to enable the capture and identification of positive or

			negative contribution to ATM safety and efficiency.
ANSP/ADR/NM	Pre-Exec#06	Install the ground systems for POC/VLD trials	The ground systems shall be installed in accordance with the change process described in the ANSP, NM (or ADR) SMS.
ANSP/ADR/NM	Pre-Exec#07	Carry out ATCO / ATSEP / NMOC staff training specific for the POC/VLD trials	This task is accomplished considering results of *Prep#05.*
ANSP/ADR/NM	Pre-Exec#08	Configure ground recording means to support the measurements need as identified in *Perf#04* (capture of accident/incident precursors of unsuccessful barrier, early warnings...)	Upgrade or install ground data recording capabilities to allow the measurement of the performance to be evaluated. It might be possible to use dedicated software tools for data collection during the POC/VLD trials and the assessment will be made in post data processing.
ANSP/ADR/NM	Pre-Exec#09	Specify ATCO /NMOC staff data reporting process consistent with the local ANSP or NM practices.	This task is a refinement of *Meas#03* in the context of local practices. The quality and diversity of reported data is crucial for the benefits of the POC/VLD trials; due to the subtle nature of the data / information required to enable the capture and identification of positive or negative contribution to ATM safety and efficiency

10.2 Execution Phase Step2: Execution and Monitoring of the POC/VLD

The execution of the POC/VLD trials shall be monitored: specific POC procedures, measurements, recordings, stopping criteria...

Execution PHASE

Step 2 Execution & Monitoring of the POC/VLD

Responsible Actor	***Task reference***	***Task description***	***Guidance***
Aircraft Operator(s) ANSP/ADR/NM	Exec#01	Perform "normal" revenue flight in accordance with the POC/VLD preparation phase	Flight crew operational procedures determined during the preparation phase must be respected (see *Prep#06*)

			including the adherence to the pilot operational stopping criteria (see *Risk#05*) ATCO operational procedures determined during the preparation phase must be respected (see *Prep#05*) including the adherence to the ATCO operational stopping criteria (see *Risk#03*) NMO procedures determined during the preparation phase must be respected (see *Prep#05*) including the adherence to the NMOC operational stopping criteria (see *Risk#03*)
Aircraft Operator(s) ANSP/ADR/NM	Exec#02	Stop the POC/VLD trials when operational stopping criteria are encountered during revenue flight	Reason for triggering “operational stopping criteria” must be understood and solved before continuing the POC/VLD trials.
Aircraft Operator(s) ANSP/ADR/NM	Exec#03	Measure during revenue flights the performances to be evaluated as determined during the preparation phase	Measurement and recording at aircraft/flight crew level shall be carried out in accordance with *Meas#01* and *Meas#02* Measurement and recording at ATCO/local ANSP (or ADR), NMOC level shall be carried out in accordance with *Meas#03* and *Meas#04*
Aircraft Operator(s) ANSP/ADR/NM	Exec#04	Record the required “measurements” associated to each flight at airborne and ground level.	Performance measurement of each flight must be recorded using the appropriate format (see *Meas#06*)
Aircraft Operator(s) ANSP/ADR/NM	Exec#05	Terminate the execution of the POC/VLD trials when the determined level of confidence is reached as defined in the preparation phase.	The minimum POC/VLD duration (exposure time) necessary to reach an acceptable level of confidence to draw conclusive results is determined during *Meas#05*.

10.3 Execution Phase Step 3: Analysis and dissemination of the results of POC/VLD

All the stakeholders should take part in the analysis of results of POC/VLD, each one according to its respective field of competence.

Execution PHASE ***Step 3 Analysis & Dissemination of the results of the POC/VLD***			
Responsible Actor	***Task reference***	***Task description***	***Guidance***
Aircraft Operator(s)	Resu#01	In addition to the recording of the required "measurements" associated to each flight (*Exec#04*), the aircraft operator is supporting the analysis of the safety & performance data making use of the analytical methods and tools deployed within the operator's organization to challenge the human performance aspects.	This task provides, to the OPS Project in charge of SESAR solution validation strategy (SESAR V1-V3), the feedback of the operator on the influencing factors affecting human performance in dynamic environment. Most of the operators tend to adopt a threat-and-error-management (TEM) approach in the analysis of safety data. Threat and error management is a concept that recognizes the influence of threatening outside factors, affecting human performance in the dynamic work environment.
TC/STC Holder(s)	Resu#02	Support the analysis of the safety & performance data making use of the analytical methods and tools deployed within the aircraft manufacturer organization to challenge the human & technical performance aspects.	This task provides, to the OPS Project in charge of SESAR solution validation strategy (SESAR V1-V3), the feedback of the aircraft manufacturer on the influencing factors affecting human & technical performance in dynamic environment.
ANSP/ADR/NM	Resu#03	In addition to the recording of the required "measurements" associated to each flight (*Exec#04*), the ANSP and/or ADR), or NM is supporting the analysis of the safety & performance data making use of the ANSP/ADR/NM's experience associated to ATM operations.	This task provides, to the OPS Project in charge of SESAR solution validation strategy (SESAR V1-V3), the feedback of the operator on the influencing factors affecting human performance in dynamic environment.
VLD OPS & Safety Task	Resu#04	Conclude the POC/VLD trials. Analyse and validate or confirm the expected performance and safety	An effective analysis of the performance to be evaluated during the POC/VLD trials

Leader(s) Aircraft Operator(s) ANSP/ADR/NM		data to conclude on the capability of the new concept and/or technology to satisfy their operational objectives. Conclusion shall be based on the satisfaction of the performance to be evaluated considering the pass/fail criteria: - if all requirements are fulfilled, it could be concluded that the proposed concept could deliver the identified performances (POC/VLD is successful) - If one or few requirements are not fulfilled but if relaxation of these performances is acceptable. POC/VLD can be declared successful provided the performance requirements are amended in the relevant document (SPR) and duly justified by re-assessing the impact of the performance relaxation (e.g. safety assessment iteration). - If one or few requirements are not fulfilled and if relaxation is not possible, the proposed concept could not deliver the identified performances (POC / VLD is not successful). A new development phase at project level might be launch to address the lack of performance (e.g. re-design)	must be based on a well-dosed mix of factual data, subjective data, knowledge and experience. The analysis of the evaluated performance should not be limited to recurring events but should also include selected first-time occurrences / single-occurrences, based on their potential for a more severe outcome under different circumstances. Data analysis must support a holistic approach that considers all actors and all factors and the way they interface between each other. Collect and analyze data from multiple reporting channels allows confirming of where the contribution to performance and safety improvement comes from, painting a more comprehensive integrated risk picture and thus reach more balanced and complete conclusions.
VLD OPS Task Leader(s) SJU	Resu#05	Identify lessons learned and actions associated to the new concept and/or technology under POC	This task formulates the lessons learned, recommendations for actions and aids to decision-making. The actions / interventions shall be defined in order to be precise, relevant, effective, affordable and timeliness. The interventions can be as broad as: within the SESAR framework, enhancing technologies, operations, training, and safety practices but also outside the SESAR framework aimed to enhance the relevant ICAO standards and recommended practices

			as well as European / National laws and associated regulations.
VLD OPS & Safety Task Leader(s)	Resu#06	Include the safety related evidence generated from POC/VLD trials in the SESAR solution Safety Assessment Report (integrated or not to SPR, Validation Report)	The SESAR solution Safety Assessment Report or relevant sub-part of SESAR solution Validation Report / SPR should capture the relevant evidence generated during POC/VLD (see *Meas#07*)
VLD OPS Task Leader(s)	Resu#07	Include the POC/VLD results in the SESAR solution validation report.	The SESAR solution validation report should include a specific section addressing POC/VLD (see *Meas#08*)

10.4 Execution Phase Step 4: Reporting to Authorities

The Authorities shall be kept informed of the functioning of the POC/VLD process, positive or negative feedback should be provided during and after the trials.

EXECUTION PHASE

Step 4 Feedback to Authorities during the POC/VLD

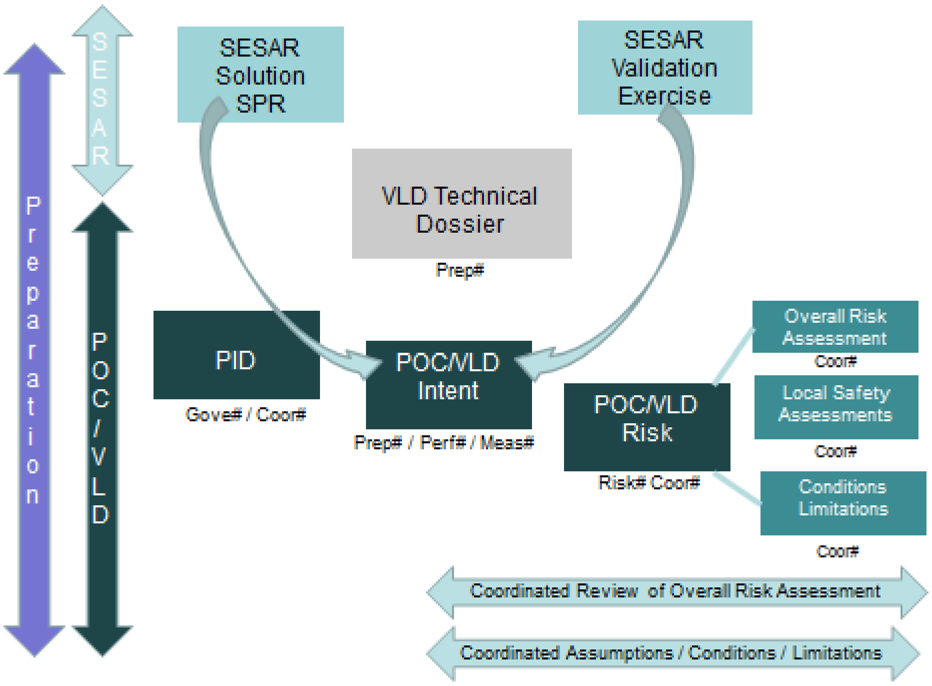
Responsible Actor	***Task reference***	***Task description***	***Guidance***
VLD OPS & Safety Task Leader(s) Aircraft Operator(s) ANSP/ADR/NM TC/STC Holder(s) SJU	Coor#03	Build & Deliver to RCA ad hoc “POC/VLD Status” report. (Same information delivered to all Authorities)	Based on the activities listed in Step 2 and 3 of the execution phase, provide the competent authorities with the outlines of the progress of the POC/VLD trials (on regular or as dictated by events (*Exec#02)*
VLD OPS Task Leader(s) SJU	Coor#04	Build & Deliver to RCA ad hoc “POC / VLD Result ” report	Based on the activities listed in Step 2 (significant events or monitoring results) and Step 3 of the execution phase (*Resu#04*, *Resu#06*), provide each relevant Competent Authority with the most important and obvious results of POC/VLD trials for their respective domain.

Appendix A POC/VLD Template

The purpose of this Template is support the application of the POC/VLD Guidance Material.

A.1 Process Overview

This section provides overview information on the whole process developed in the POC/VLD document.



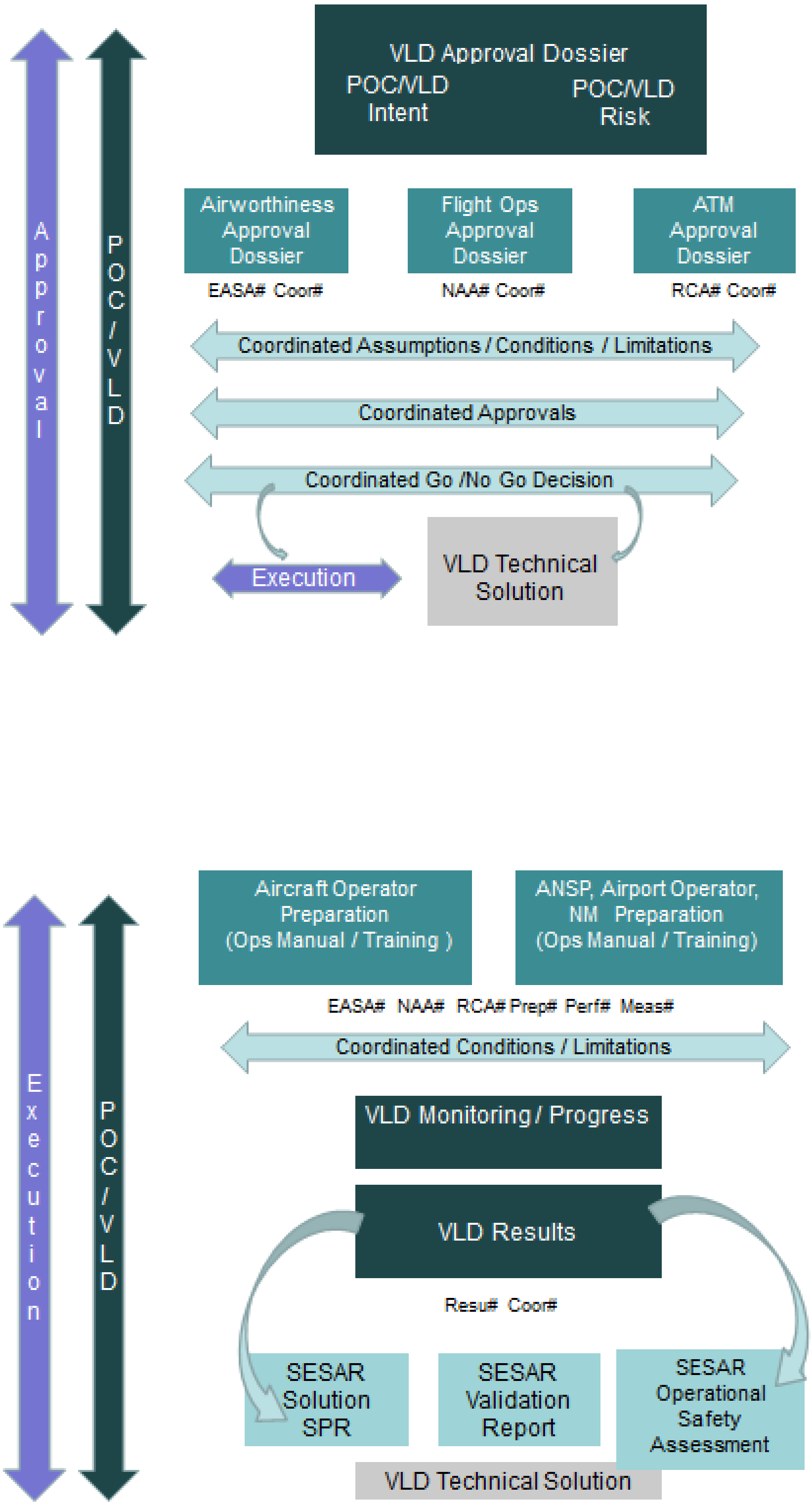

VLD Approval Dossier
POC/VLD Intent
POC/VLD Risk
Approval
POC/VLD
Airworthiness Approval Dossier
Flight Ops Approval Dossier
ATM Approval Dossier
EASA# Coor#
NAA# Coor#
RCA# Coor#
Coordinated Assumptions / Conditions / Limitations
Coordinated Approvals
Coordinated Go /No Go Decision
Execution
VLD Technical Solution
Execution
POC/VLD
Aircraft Operator Preparation (Ops Manual / Training)
ANSP, Airport Operator, NM Preparation (Ops Manual / Training)
EASA# NAA# RCA# Prep# Perf# Meas#
Coordinated Conditions / Limitations
VLD Monitoring / Progress
VLD Results
Resu# Coor#
SESAR Solution SPR
SESAR Validation Report
SESAR Operational Safety Assessment
VLD Technical Solution

Figure 10: Traceability between Tasks & Documents

A.2 Summary Table

This section provides in a synoptic manner the interrelationship between tasks and documents.

Task Reference	Task Description	Owner(s)	Cross-Reference with other tasks	Related Document	Ticking box
VLD Organization - Management Phase					
Gove#01	VLD Project Arrangements	VLD Project	Prep#01	**PID**	
Gove#02	EASA/VLD Project Arrangements	VLD Project & EASA	Gove#01 Coor#01	PID	
Gove#03	DM/VLD Project Arrangements	VLD Project & DM	Gove#01 Prep#01 Perf#0x	PID	
Gove#04	NM/VLD Project Arrangements	VLD Project & NM	Gove#01 Prep#01 Perf#0x	PID	
Preparation Phase					
Preparation / Purpose and Scope of the POC/VLD					
Prep#01	VLD Scope, Goals & Objectives	VLD Project	Gove#01 Gove#02 Gove#03 Gove#04	VLD Technical Dossier	
Prep#02	OPS Context	VLD Project	Gove#01 Gove#02 Gove#03 Gove#04	VLD Technical Dossier	
Prep#03	ATM Context	VLD Project	Gove#01 Gove#02 Gove#03 Gove#04	VLD Technical Dossier	
Prep#04	Maturity of Technical Solution	VLD Project		VLD Technical Dossier	
Prep#05	Feedback on feasibility from ANSP/ADR or NM	VLD Project & ANSP or ADR Operator	Prep#02 Prep#03	VLD Technical Dossier	
Prep#06	Feedback on feasibility from Aircraft Operator	VLD Project & Aircraft or ADR Operator	Prep#02 Prep#03	VLD Technical Dossier	
Prep#07	Early Involvement of EASA & RCA Feedback on feasibility from EASA & RCA	VLD Project & EASA & RCA	Prep#01 Prep#02 Prep#03	VLD Technical Dossier	
Preparation / Performance to be evaluated					
Perf#01	Overall Performances to be evaluated [SESAR SPR / Validation Plan]	VLD Project	Gove#01 Gove#02 Gove#03 Gove#04	VLD Technical Dossier	
Perf#02	Performance to be evaluated at aircraft level [SESAR SPR /	VLD Project & TC / STC Holder		VLD Technical Dossier	

	Validation Plan]				
Perf#03	*Performance to be evaluated at ground level* *SESAR SPR / Validation Plan]*	*VLD Project & ANSP (NM) / ADR*		*VLD Technical Dossier*	
Perf#04	*Reference case / Metrics & List of parameters/indicators to be measured*	*VLD Project & TC / STC H. & ANSP/ NM / ADR*	Perf#01 Perf#02 Perf#03 *Docu#01*	*VLD Technical Dossier*	
Preparation / Performance measurement and recording					
Meas#01	*Flight Crew Performance Measurements*	*VLD Project & TC/STC H. & Aircraft Operator*	*Perf#02*, *Perf#04* Meas#08	***VLD Technical Dossier***	
Meas#02	*Airborne Equipment Performance Measurements*	*VLD Project & TC/STC H. & Aircraft Operator*	*Perf#02*, *Perf#04* Meas#08	***VLD Technical Dossier***	
Meas#03	*ATCO Performance Measurements*	*VLD Project & ANSP/ADR*	*Perf#03*, *Perf#04* Meas#08	***VLD Technical Dossier***	
Meas#04	*Ground Equipment Performance Measurements*	*VLD Project & ANSP/ADR/NM*	*Perf#03*, *Perf#04* Meas#08	***VLD Technical Dossier***	
Meas#05	*VLD Duration*	*VLD Project*	*Docu#01*	***POC/VLD Intent dossier***	
Meas#06	*Data Recording*	*VLD Project*	*Docu#01*	***VLD Technical Dossier***	
Meas#07	*Safety Evidence*	*VLD Project*	*Docu#01*	***POC/VLD Intent dossier***	
Meas#08	*Summary table: list of performances and related data*	*VLD Project*	Meas#01 Meas#02 Meas#03 Meas#04 *Docu#01*	***POC/VLD Intent dossier***	
Preparation / Risk Assessment					
Risk#01	*Applicable Safety Requirements*	*VLD Project & TC/STC H. & Aircraft Operator*	*Docu#01*	***POC/VLD Intent dossier*** *Overall Risk Assessment*	
Risk#02	*Common Method for overall risk assessment - identification of potential Hazards on all domains*	*VLD Project & TC/STC H. & Aircraft Operator/ ANSP/ADR/NM*	*Docu#02*	*Overall Risk Assessment*	
Risk#03	*ANSP/ADR or NM Safety Assessment*	*ANSP/ADR/NM*	*Risk#01* *Ris#02* *Risk#06*	*Local Safety Assessment* *(ANSP/ADR or NM)*	
Risk#04	*Airborne Safety Assessment*	*TC/STC Holder*	*Risk#01* *Ris#02* *Risk#06*	*Local Safety Assessment* *(Airborne)*	
Risk#05	*Operational Safety Assessment*	*Aircraft Operator*	*Risk#01* *Ris#02* *Risk#06*	*Local Safety Assessment* *(Flight Operation)*	

Risk#06	*Coordinated Safety Assessments – Coordinated Assumptions & Risk Mitigations*	*VLD Project & TC/STC H. & Aircraft Operator & ANSP/ADR/NM*	*Risk#02 Risk#03 Risk#04 Risk#05*	*Safety Register &* *Initial “Conditions / Limitations” Document*	
Preparation / Pre-Approval / Liaison with Authorities					
Docu#01	*POC/VLD “Intent” dossier* *[*Information from VLD Technical Dossier]	*VLD Project*	*Perf#04*	***Approval Dossier***	
Docu#02	*POC/VLD “Risk” dossier* [Overall Risk Assessment + Local Safety Assessment + Initial “Conditions / Limitations” Document]	*VLD Project*	*Risk#06*	***Approval Dossier***	
Preparation / Pre-Approval / Coordinated Safety Assessment & Approval					
Coor#01	*EASA Supervision framework & RCA involvement & coordination framework*	*EASA*	*Gove#02*	*PID*	
Coor#02	*Supervision of POC/VLD Risk Dossier – Coordinated Go / No Go decision*	*EASA*	Coor#01 Docu#02 EASA#07 NAA#07 RCA#07	*Conditions / Limitations Documents*	
Approval Phase					
TC/STC Holder Approval					
EASA#01	*EASA Form 31/33*	*TC/STC Holder*	*Docu#01*	*A/W Approval Dossier*	
EASA#02	*Certification Meeting*	*TC/STC Holder*	*Docu#02* *Prep#05 Prep#06 Risk#04 Risk#06*	*A/W Approval Dossier*	
EASA#03	*Certification Basis*	*TC/STC Holder* *EASA*	*Docu#01*	*A/W Approval Dossier*	
EASA#04	*Certification Plan*	*TC/STC Holder*	*EASA#03*	*A/W Approval Dossier*	
EASA#05	*Certification Documents*	*TC/STC Holder*	*EASA#04*	*A/W Approval Dossier*	
EASA#06	*Review of Certification Document*	*EASA* *TC/STC Holder*	*EASA#05*		
EASA#07	*EASA feedback*	*EASA*	*EASA#06* *Coor#02*	*EASA Approval or rejection* *[Go / No Go]*	

Aircraft Operator Approval					
NAA#01	Application Letter	Aircraft Operator	Docu#01	Flight Ops Approval Dossier	
NAA#02	Meeting with NAA	Aircraft Operator	Docu#02 Prep#05 Prep#06 Risk#05 Risk#06	Flight ops Approval Dossier	
NAA#03	Applicable Regulation	Aircraft Operator	Docu#01	Flight Ops Approval Dossier	
NAA#04	Approval Plan	Aircraft Operator	NAA#03	Flight Ops Approval Dossier	
NAA#05	Compliance Documents	Aircraft Operator	NAA#04	Flight Ops Approval Dossier	
NAA#06	Review of Compliance Document	NAA Aircraft Operator	NAA#05		
NAA#07	NAA feedback	NAA	NAA#06 Coor#02	NAA Approval or rejection [Go / No Go]	
ANSP, Airport Operator and Network Manager Approval					
RCA#01	Change Notification	ANSP, and/or Airport Operator or Network Manager	Docu#01	ANSP ADR or NMOC Approval Dossier	
RCA#02	Meeting with RCA	ANSP, and/or Airport Operator or Network Manager	Docu#02 Prep#02 Prep#05 Prep#06 Risk#03 Risk#06	ANSP ADR or NMOC Approval Dossier	
RCA#03	Applicable Regulation	ANSP, and/or Airport Operator or Network Manager	Docu#01	ANSP ADR or NMOC Approval Dossier	
RCA#04	Activity Road map	ANSP, and/or Airport Operator or Network Manager	RCA#03	ANSP ADR or NMOC Approval Dossier	
RCA#05	Safety Assessments	ANSP, and/or Airport Operator or Network Manager	RCA#04	ANSP ADR or NMOC Approval Dossier	
RCA#06	Review of Safety Assessment	NSA, NAA or EASA	RCA#05		
RCA#07	RCA feedback	NSA, NAA or EASA	RCA#06 Coor#02	RCA Approval or rejection [Go / No Go]	
Execution Phase					
Execution Phase / Preparation					

Pre-Exec#01	*Install Service Bulletin*	*Aircraft Operator*	EASA#07	*TC/STC Service Bulletin*	
Pre-Exec#02	*Perform Flight crew training*	*Aircraft Operator*	*Prep#06* *Risk#06*	*POC/VLD Intent Dossier* *Conditions / Limitations Document*	
Pre-Exec#03	*Install line operation assessment process*	*Aircraft Operator*	*Meas#06*	*POC/VLD Intent Dossier*	
Pre-Exec#04	*Configure airborne recording means*	*Aircraft Operator*	*Meas#02 Perf#04*	*POC/VLD Intent Dossier*	
Pre-Exec#05	*Specify Pilot data reporting (internal process)*	*Aircraft Operator*	*Meas#01*	*Aircraft Operator Internal Procedure*	
Pre-Exec#06	*Install airborne equipment*	*ANSP, Airport operator, NM*		*POC/VLD Intent Dossier*	
Pre-Exec#07	*Perform ATCO / NMOC stall training*	*ANSP, Airport operator, NM*	*Prep#05*	*POC/VLD Intent Dossier*	
Pre-Exec#08	*Configure ground recording means*	*ANSP, Airport operator, NM*	*Perf#03*	*POC/VLD Intent Dossier*	
Pre-Exec#09	*Specify ATCO / NMOC Staff data reporting (internal process)*	*ANSP, Airport operator, NM*	*Meas#03*	*ANSP / Airport Operator / NMOC Stall Internal Procedure*	
Execution Phase / Execution & Monitoring					
Exec#01	*Conduct live trials*	*Aircraft Operator* *ANSP, Airport operator, NM*	*Prep#05 Prep#06, Risk#03, Risk#05*	*POC/VLD Monitoring Report*	
Exec#02	*Investigate if stopping criteria triggered*	*Aircraft Operator* *ANSP, Airport operator, NM*		*POC/VLD Monitoring Report*	
Exec#03	*Measure performance*	*Aircraft Operator* *ANSP, Airport operator, NM*	*Meas#06*	*POC/VLD Monitoring Report*	
Exec#04	*Record Performance Measurements*	*Aircraft Operator* *ANSP, Airport operator, NM*	*Meas#06*	*POC/VLD Monitoring Report*	
Exec#05	*Stop Live trials when confidence reached*	*Aircraft Operator* *ANSP, Airport operator, NM*	*Meas#05*	*POC/VLD Monitoring Report*	
Execution Phase / Analysis & Dissemination					
Resu#01	*Flight Operational feedback*	*Aircraft Operator*	*Exec#04*	*POC/VLD Results Report*	
Resu#02	*Airborne system manufacturer feedback*	*TC/STC Holder*		*POC/VLD Results Report*	

Resu#03	*ATM Operational feedback*	*ANSP, Airport operator, NM*	*Exec#04*	*POC/VLD Results Report*	
Resu#04	*Feedback consolidation*	*VLD Project Aircraft Operator ANSP, Airport operator, NM*		*POC/VLD Results Report*	
Resu#05	*Lessons Learnt*	*VLD Project*		*POC/VLD Results Report*	
Resu#06	*Provide feedback on SESAR OSED/SPR & SESAR Operational Assessment*	*VLD Project*	*Meas#07*	*POC/VLD Results Report*	
Resu#07	*Provide feedback on SESAR validation report*	*VLD Project*	*Meas#08*	*POC/VLD Results Report*	
Execution Phase / Reporting to Authorities					
Coor#03	*Deliver summary of execution activities to RCA*	*VLD Project Aircraft Operator ANSP, Airport operator, NM*	*Exec#02*	*POC/VLD Monitoring Report*	
Coor#04	*Deliver POC/VLD Result report to RCA*	*VLD Project*	*Resu#04 Resu#06*	*POC/VLD Results Report*	

END OF DOCUMENT-

POC/VLD Template

Document information	
Project Title	Develop “proof of concept” for aircraft certification when introducing a new concept of operations
Project Number	16.1.4
Project Manager	AIRBUS
Deliverable Name	POC Template
Deliverable ID	16.01.04 – D08
Edition	00.01.00
Template Version	03.00.00
Task contributors	
AIRBUS, EUROCONTROL	

Please complete the advanced properties of the document

Abstract

The aim was to produce a template for effective and harmonized application of the POC/VLD Guidance Material by the various VLD projects also in SESAR 2020.

Authoring & Approval

Prepared By - *Authors of the document.*		
Name & Company	Position & Title	Date
Joelle Monso / AIRBUS	Project Leader	31/08/2015
Bruno Rabiller / EUROCONTROL	Project Contributor	

Reviewed By - *Reviewers internal to the project.*		
Name & Company	Position & Title	Date
Bruno Rabiller / EUROCONTROL	Project Contributor	31/08/2015
Patrick Lelievre	Contributor Manager	

Reviewed By - *Other SESAR projects, Airspace Users, staff association, military, Industrial Support, other organisations.*		
Name & Company	Position & Title	Date

Approved for submission to the SJU By - *Representatives of the company involved in the project.*		
Name & Company	Position & Title	Date
Joelle Monso / AIRBUS	Project Leader	
Bruno Rabiller / EUROCONTROL	Project Contributor	

Rejected By - *Representatives of the company involved in the project.*		
Name & Company	Position & Title	Date

Rational for rejection
None.

Document History

Edition	Date	Status	Author	Justification
00.01.00	31/08/2015	Final	Joelle Monso	Initial Version

Intellectual Property Rights (foreground)

This deliverable consists of SJU foreground.

Table of Contents

List of figures

Executive summary

The purpose of this template is to provide a means to ensure effective and harmonized application of the POC/VLD Guidance Material.

This template is a digest that will help to highlight the tasks defined in the POC/VLD Guidance Material.

1 Introduction

1.1 Scope of the document

The purpose of this document is to provide an abstract suitable for ensuring adherence to the POC/VLD guidelines.

1.2 Structure of the document

This template contains two main sections:

- the first section contains a synthetic view of the whole process for VLD highlighting the different aspects of the VLDs
- the last section contains a comprehensive checklist of the tasks to be performed together with supporting documentation.

1.3 Intended readership

This document interests all the actors that play a role in the Very Large Demonstrations: the SJU, the members of the VLD project consortium, the Network Manager, the Deployment Manager, EASA and the Competent Authorities.

1.4 How to use this document

Figure 1 below presents the overall structure of the POC/VLD Template.

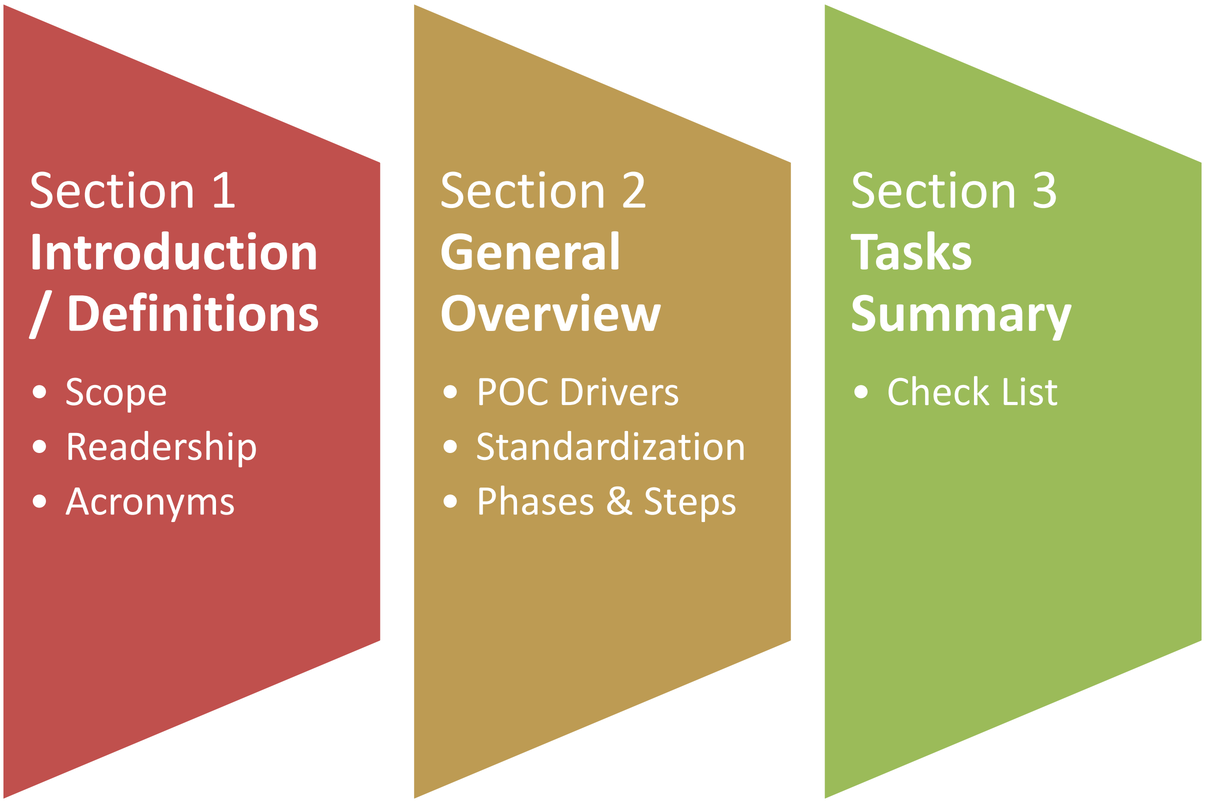


Figure 1: Structure of POC/VLD Template

1.5 Acronyms and Terminology

Term	Definition
ADR	Aerodrome
ANSP	Air Navigation Service Provider
ATM	Air Traffic Management
A/W	Airworthiness
DM (SDM)	Deployment Manager (SESAR Deployment Manager)
EASA	European Aviation Safety Agency
INTEROP	Interoperability Requirement document
NAA	National Aviation Authorities
NM	Network Manager
NMO	Network Manager Operator
NMOC	Network Manager Operator Centre
NSA	National Supervisory Authorities
Ops	Operational
OSED	Operational Service Environment Document
PID	Project Interface Document
POC	Proof of Concept
RCA	Relevant Competent Authority
SES	Single European Sky
SESAR	Single European Sky ATM Research Programme
SESAR Programme	The programme which defines the Research and Development activities and Projects for the SJU.
SJU	SESAR Joint Undertaking (Agency of the European Commission)
SJU Work Programme	The programme which addresses all activities of the SESAR Joint Undertaking Agency.
SPR	Safety Performance Requirement document
STC	Supplemental Type Certificate
TC	Type Certificate

Term	Definition
VLD	Very Large Demonstration

2 General Overview

2.1 Key Drivers for POC/VLD

Two of the main drivers for proof of concept are mature standards and credible business case.

The maturity of the operational concept and its standardization is even more essential for the new technologies in ATM. Indeed, merging airborne and ground technology introduces new dependencies that necessitate a more integrated and coordinated approach for standardization and certification / approval. Moreover, the close link between airborne and ground segments amplifies the consequences of immature standard, which leads to consider POC/VLD for credible business case.

2.2 SESAR / Standardization Relationship

The first set of SESAR activities are distinguished from the VLD activities also in SESAR 2020 because of the timescale and the different organization put in place.

The figure 2 below outlines the relationship between the major steps in the standardization of the new technologies in ATM:

- <u>“Standardization” by SESAR</u>:

  The main activities of SESAR are related to the development of the SESAR solutions. This includes the production of the Safety & Performance and Interoperability requirements and the validation of those requirements through the SESAR validation exercise.

- <u>Validation by POC/VLD</u>

  The prototypes or the final products implementing the new technologies in ATM and that will be installed on aircraft and on ground and operated during revenue flights are built from initial Industry standard complemented with the SESAR outputs: e.g. SESAR OSED , SPR and INTEROP Documents. The results of the VLD will support the maturity of the International and the Industry Standards.

- <u>Consideration by Recognized Organization</u>

  The whole aviation community will benefit from the VLD experience, as indicated in figure 3. The dissemination of the lessons learnt and best practices will occur in several ways, inside and outside SESAR. SJU will share VLD knowledge and lessons learnt with ICAO and NEXTGEN. The VLD applicants and authorities should also learn from the experience of the VLD; it could be that the new approach for standardization, certification / approval and deployment, are recognized as good practice.

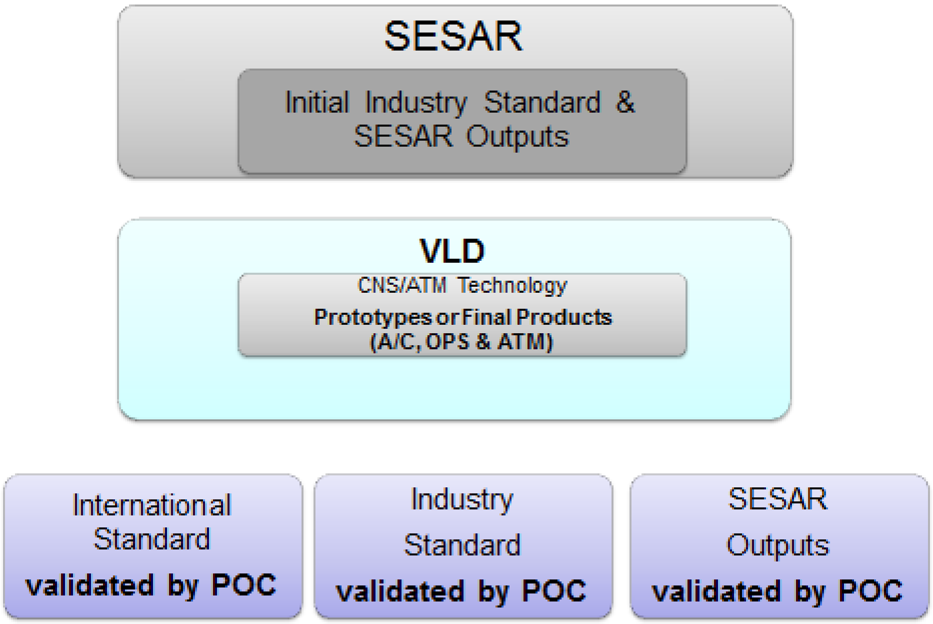

SESAR
Initial Industry Standard & SESAR Outputs
VLD
CNS/ATM Technology
Prototypes or Final Products (A/C, OPS & ATM)
International Standard validated by POC
Industry Standard validated by POC
SESAR Outputs validated by POC

Figure 2: VLD and Standardization

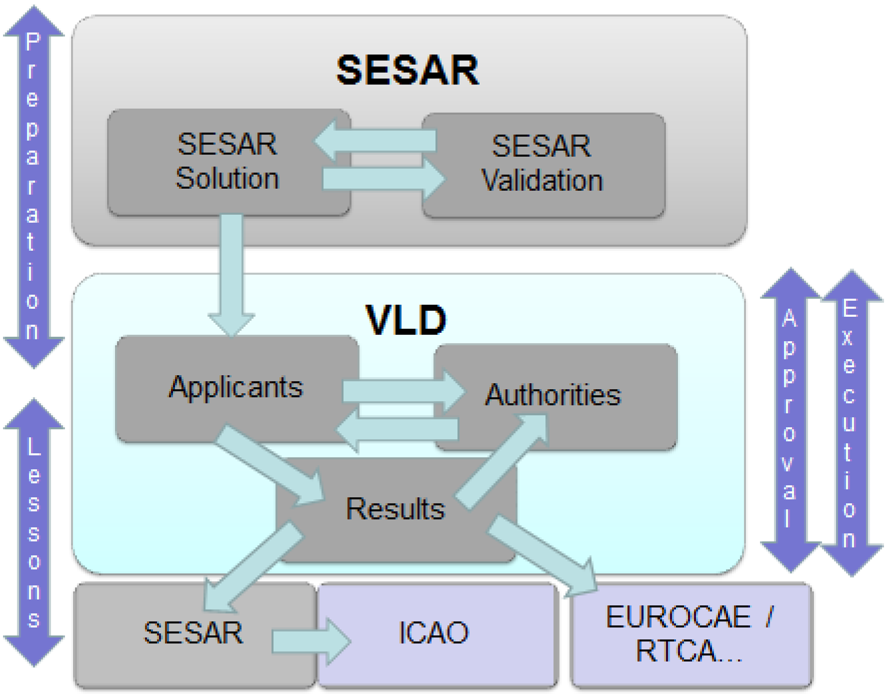


Figure 3: Scoping of VLD

2.3 POC Phases and Tasks

This section contains an overview of the whole process developed in the POC/VLD Guidance Material.

The figure 4 below provides an overview of the tasks together with supporting documentation that will have to be performed during the preparation phase of the VLD.

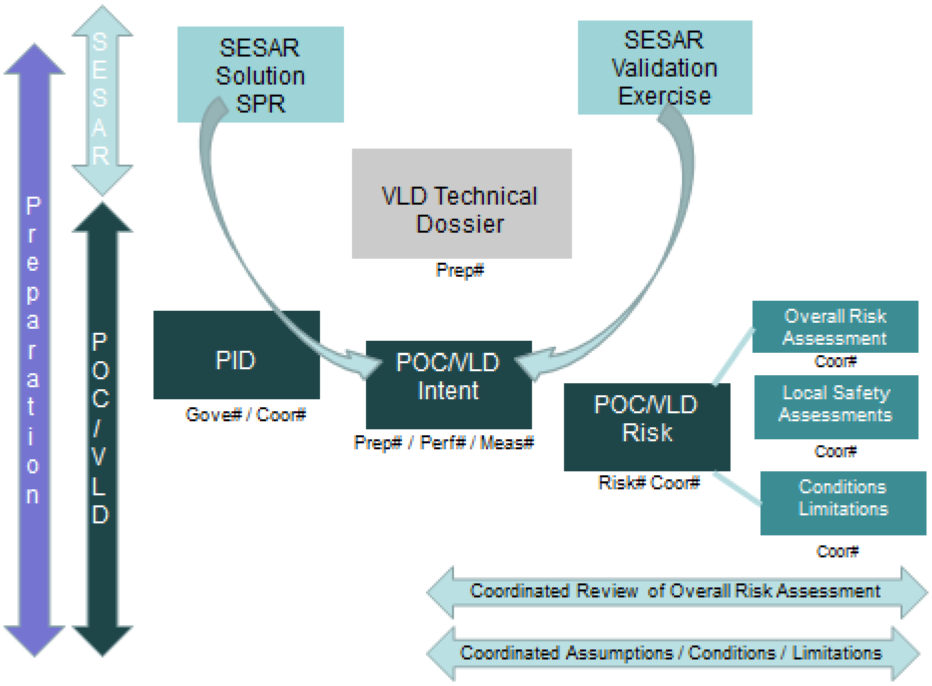


Figure 4: Tasks & Documents for VLD Preparation

The Project Interface Document (PID) is an overarching document. It explains the new dependencies being introduced by the VLD. It includes all the relevant information that need to be shared with the competent authorities. It lays down the coordination arrangements set up with the stakeholders involved in the VLD.

The VLD Technical Dossier is a working paper not released outside VLD project that contains the relevant information regarding the maturity of the technical and operational solution for the live trials together with the objectives of the demonstration. This working paper will serve as basis for the documents released to the authorities (PID, POC/VLD Intent, and POC/VLD Risk)

The POC/VLD Intent document summarizes the objectives of the VLD and the performances to be evaluated. This document is part of the "Approval Dossier" package sent to the authorities.

The POC/VLD Risk document gathers the safety/risk assessments performed by different stakeholders.

The Overall Risk Assessment document is part of the "Approval Dossier" package sent to the authorities. It results from a collaborative work between the applicants and VLD Project team, aimed at identifying all the potential risks and the different mitigations commonly agreed

The Local Safety Assessment is performed by each involved applicant. It focuses on the safety risks considering the implementation of the relevant mitigations at local level.

The figure 4 & 5 below provides an overview of the activities of coordination that are recommended during the approval phase of the VLD.

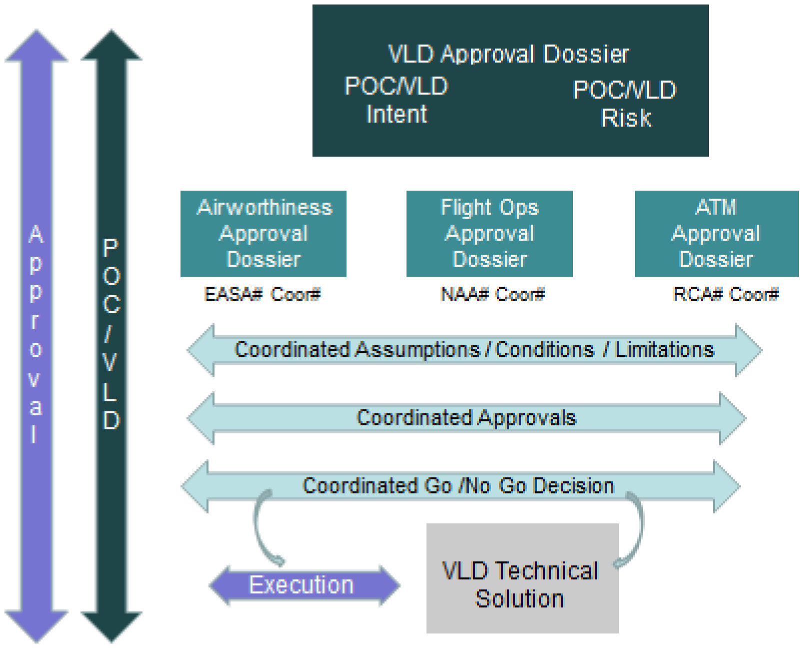


Figure 5: Coordination Tasks for VLD Approval

The involvement of the relevant authorities is to be coordinated as early as possible. This guidance material recommends that it starts during the preparation phase when the overall risk assessment is released. The coordination should be exercised on the acceptability of the methodology used for the overall risk assessment as well as on the acceptability of the results of the application of this methodology.

The relevant authorities should also ensure in a coordinated manner the consistency between the assumptions and mitigations of the overall safety assessment and their effective realisation at local level. All the local Conditions /Limitations resulting from the local safety assessments should have to be laid down in a common "Conditions & Limitations" document agreed by all.

The figure 6 below provides an overview of the monitoring and dissemination activities within the context of the VLD during the execution phase.

The VLD Monitoring / Progress Report and the VLD Result Report will be sent to the relevant authorities during and after the execution of the VLD. The results & lessons learnt would be shared with the relevant standardization bodies.

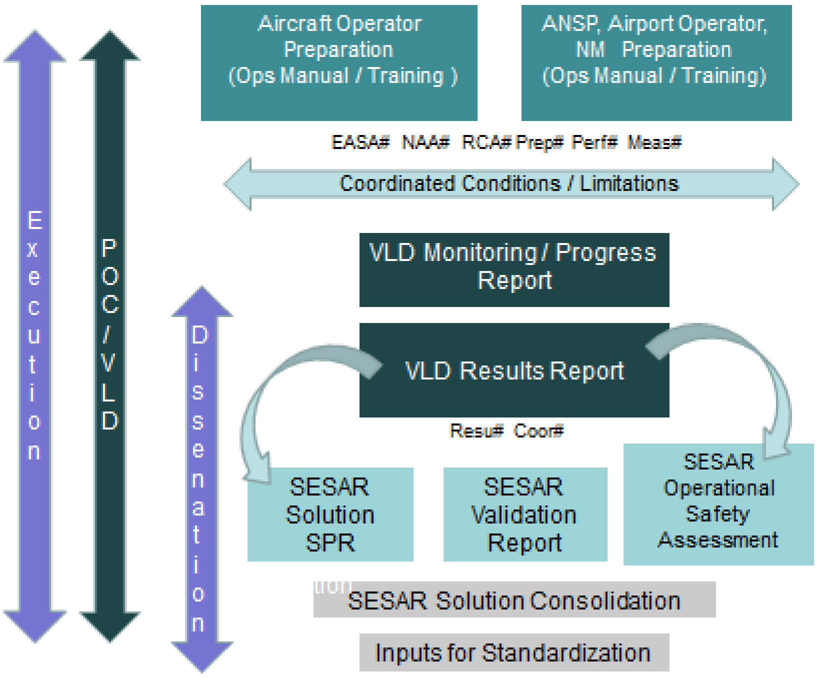

Aircraft Operator Preparation (Ops Manual / Training)
ANSP, Airport Operator, NM Preparation (Ops Manual / Training)
EASA# NAA# RCA# Prep# Perf# Meas#
Coordinated Conditions / Limitations
Execution
POC/VLD
Dissenation
VLD Monitoring / Progress Report
VLD Results Report
Resu# Coor#
SESAR Solution SPR
SESAR Validation Report
SESAR Operational Safety Assessment
SESAR Solution Consolidation
Inputs for Standardization

Figure 6: Monitoring & Dissemination Activities during Execution phase

3 Summary Table / Checklist

This section provides in a synoptic manner the interrelationship between tasks and documents.

Task Reference	*Task Description*	*Owner(s)*	*Cross-Reference with other tasks*	*Related Document*	*Ticking box*
VLD Organization - Management Phase					
Gove#01	*VLD Project Arrangements*	*VLD Project*	*Prep#01*	***PID***	
Gove#02	*EASA/VLD Project Arrangements*	*VLD Project & EASA*	Gove#01 *Coor#01*	*PID*	
Gove#03	*DM/VLD Project Arrangements*	*VLD Project & DM*	Gove#01 *Prep#01 Perf#0x*	*PID*	
Gove#04	*NM/VLD Project Arrangements*	*VLD Project & NM*	Gove#01 *Prep#01 Perf#0x*	*PID*	
Gove#05	*SJU / VLD Project Arrangements*	*VLD Project*	Gove#01 *Prep#0x Perf#0x*	*PID*	
Preparation Phase					
Preparation / Purpose and Scope of the POC/VLD					
Prep#01	*VLD Scope, Goals & Objectives*	*VLD Project*	Gove#01- 05	*VLD Technical Dossier*	
Prep#02	*OPS Context*	*VLD Project*	Gove#01- 05	*VLD Technical Dossier*	
Prep#03	*ATM Context*	*VLD Project*	Gove#01- 05	*VLD Technical Dossier*	
Prep#04	*Maturity of Technical Solution*	*VLD Project*		*VLD Technical Dossier*	
Prep#05	*Feedback on feasibility from ANSP/ADR or NM*	*VLD Project & ANSP or ADR Operator*	*Prep#02 Prep#03*	*VLD Technical Dossier*	
Prep#06	*Feedback on feasibility from Aircraft Operator*	*VLD Project & Aircraft or ADR Operator*	*Prep#02 Prep#03*	*VLD Technical Dossier*	
Prep#07	*Early Involvement of EASA & RCA* *Feedback on feasibility from EASA & RCA*	*VLD Project & EASA & RCA*	*Prep#01 Prep#02 Prep#03*	*VLD Technical Dossier*	
Preparation / Performance to be evaluated					
Perf#01	*Overall Performances to be evaluated* *[SESAR SPR / Validation Plan]*	*VLD Project*	Gove#01 Gove#02 Gove#03 Gove#04	*VLD Technical Dossier*	
Perf#02	*Performance to be evaluated at aircraft*	*VLD Project &*		*VLD Technical Dossier*	

	level *[SESAR SPR / Validation Plan]*	*TC / STC Holder*			
Perf#03	*Performance to be evaluated at ground level* *SESAR SPR / Validation Plan]*	*VLD Project & ANSP (NM) / ADR*		*VLD Technical Dossier*	
Perf#04	*Reference case / Metrics & List of parameters/indicators to be measured*	*VLD Project & TC / STC H. & ANSP/ NM / ADR*	Perf#01 Perf#02 Perf#03 *Docu#01*	*VLD Technical Dossier*	
Preparation / Performance measurement and recording					
Meas#01	*Flight Crew Performance Measurements*	*VLD Project & TC/STC H. & Aircraft Operator*	*Perf#02*, *Perf#04* Meas#08	***VLD Technical Dossier***	
Meas#02	*Airborne Equipment Performance Measurements*	*VLD Project & TC/STC H. & Aircraft Operator*	*Perf#02*, *Perf#04* Meas#08	***VLD Technical Dossier***	
Meas#03	*ATCO Performance Measurements*	*VLD Project & ANSP/ADR*	*Perf#03*, *Perf#04* Meas#08	***VLD Technical Dossier***	
Meas#04	*Ground Equipment Performance Measurements*	*VLD Project & ANSP/ADR/NM*	*Perf#03*, *Perf#04* Meas#08	***VLD Technical Dossier***	
Meas#05	*VLD Duration*	*VLD Project*	*Docu#01*	***POC/VLD Intent dossier***	
Meas#06	*Data Recording*	*VLD Project*	*Docu#01*	***VLD Technical Dossier***	
Meas#07	*Safety Evidence*	*VLD Project*	*Docu#01*	***POC/VLD Intent dossier***	
Meas#08	*Summary table: list of performances and related data*	*VLD Project*	Meas#01 Meas#02 Meas#03 Meas#04 *Docu#01*	***POC/VLD Intent dossier***	
Preparation / Risk Assessment					
Risk#01	*Applicable Safety Requirements*	*VLD Project & TC/STC H. & Aircraft Operator*	*Docu#01*	***POC/VLD Intent dossier*** *Overall Risk Assessment*	
Risk#02	*Common Method for overall risk assessment - identification of potential Hazards on all domains*	*VLD Project & TC/STC H. & Aircraft Operator/ ANSP/ADR/NM*	*Docu#02*	*Overall Risk Assessment*	
Risk#03	*ANSP/ADR or NM Safety Assessment*	*ANSP/ADR/NM*	*Risk#01* *Ris#02* *Risk#06*	*Local Safety Assessment* *(ANSP/ADR or NM)*	
Risk#04	*Airborne Safety Assessment*	*TC/STC Holder*	*Risk#01* *Ris#02* *Risk#06*	*Local Safety Assessment* *(Airborne)*	

Risk#05	*Operational Safety Assessment*	*Aircraft Operator*	*Risk#01 Ris#02 Risk#06*	*Local Safety Assessment* *(Flight Operation)*	
Risk#06	*Coordinated Safety Assessments – Coordinated Assumptions & Risk Mitigations*	*VLD Project & TC/STC H. & Aircraft Operator & ANSP/ADR/NM*	*Risk#02 Risk#03 Risk#04 Risk#05*	*Safety Register &* *Initial "Conditions / Limitations" Document*	
Preparation / Pre-Approval / Liaison with Authorities					
Docu#01	*POC/VLD "Intent" dossier* *[*Information from VLD Technical Dossier]	*VLD Project*	*Perf#04*	***Approval Dossier***	
Docu#02	*POC/VLD "Risk" dossier* [Overall Risk Assessment + Local Safety Assessment + Initial "Conditions / Limitations" Document]	*VLD Project*	*Risk#06*	***Approval Dossier***	
Preparation / Pre-Approval / Coordinated Safety Assessment & Approval					
Coor#01	*EASA coordination framework & RCA involvement*	*EASA*	*Gove#02*	*PID*	
Coor#02	*Coordinated review of POC/VLD Risk Dossier – Coordinated Go / No Go decision*	*EASA*	Coor#01 Docu#02 EASA#07 NAA#07 RCA#07	*Conditions / Limitations Documents*	
Approval Phase					
TC/STC Holder Approval					
EASA#01	*EASA Form 31/33*	*TC/STC Holder*	*Docu#01*	*A/W Approval Dossier*	
EASA#02	*Certification Meeting*	*TC/STC Holder*	*Docu#02* *Prep#05 Prep#06 Risk#04 Risk#06*	*A/W Approval Dossier*	
EASA#03	*Certification Basis*	*TC/STC Holder* *EASA*	*Docu#01*	*A/W Approval Dossier*	
EASA#04	*Certification Plan*	*TC/STC Holder*	*EASA#03*	*A/W Approval Dossier*	
EASA#05	*Certification Documents*	*TC/STC Holder*	*EASA#04*	*A/W Approval Dossier*	
EASA#06	*Review of Certification Document*	*EASA* *TC/STC Holder*	*EASA#05*		
EASA#07	*EASA feedback*	*EASA*	*EASA#06* *Coor#02*	*EASA Approval or rejection* *[Go / No Go]*	

Aircraft Operator Approval					
NAA#01	*Application Letter*	*Aircraft Operator*	*Docu#01*	*Flight Ops Approval Dossier*	
NAA#02	*Meeting with NAA*	*Aircraft Operator*	*Docu#02* *Prep#05 Prep#06 Risk#05 Risk#06*	*Flight ops Approval Dossier*	
NAA#03	*Applicable Regulation*	*Aircraft Operator*	*Docu#01*	*Flight Ops Approval Dossier*	
NAA#04	*Approval Plan*	*Aircraft Operator*	*NAA#03*	*Flight Ops Approval Dossier*	
NAA#05	*Compliance Documents*	*Aircraft Operator*	*NAA#04*	*Flight Ops Approval Dossier*	
NAA#06	*Review of Compliance Document*	*NAA* *Aircraft Operator*	*NAA#05*		
NAA#07	*NAA feedback*	*NAA*	*NAA#06* *Coor#02*	*NAA Approval or rejection* *[Go / No Go]*	
ANSP, Airport Operator and Network Manager Approval					
RCA#01	*Change Notification*	*ANSP, and/or Airport Operator or Network Manager*	*Docu#01*	*ANSP ADR or NMOC Approval Dossier*	
RCA#02	*Meeting with RCA*	*ANSP, and/or Airport Operator or Network Manager*	*Docu#02* *Prep#02 Prep#05 Prep#06 Risk#03 Risk#06*	*ANSP ADR or NMOC Approval Dossier*	
RCA#03	*Applicable Regulation*	*ANSP, and/or Airport Operator or Network Manager*	*Docu#01*	*ANSP ADR or NMOC Approval Dossier*	
RCA#04	*Activity Road map*	*ANSP, and/or Airport Operator or Network Manager*	*RCA#03*	*ANSP ADR or NMOC Approval Dossier*	
RCA#05	*Safety Assessments*	*ANSP, and/or Airport Operator or Network Manager*	*RCA#04*	*ANSP ADR or NMOC Approval Dossier*	
RCA#06	*Review of Safety Assessment*	*NSA, NAA or EASA*	*RCA#05*		
RCA#07	*RCA feedback*	*NSA, NAA or EASA*	*RCA#06* *Coor#02*	*RCA Approval or rejection* *[Go / No Go]*	
Execution Phase					
Execution Phase / Preparation					

Pre-Exec#01	Install Service Bulletin	Aircraft Operator	EASA#07	TC/STC Service Bulletin	
Pre-Exec#02	Perform Flight crew training	Aircraft Operator	Prep#06 Risk#06	POC/VLD Intent Dossier Conditions / Limitations Document	
Pre-Exec#03	Install line operation assessment process	Aircraft Operator	Meas#06	POC/VLD Intent Dossier	
Pre-Exec#04	Configure airborne recording means	Aircraft Operator	Meas#02 Perf#04	POC/VLD Intent Dossier	
Pre-Exec#05	Specify Pilot data reporting (internal process)	Aircraft Operator	Meas#01	Aircraft Operator Internal Procedure	
Pre-Exec#06	Install airborne equipment	ANSP, Airport operator, NM		POC/VLD Intent Dossier	
Pre-Exec#07	Perform ATCO / NMOC stall training	ANSP, Airport operator, NM	Prep#05	POC/VLD Intent Dossier	
Pre-Exec#08	Configure ground recording means	ANSP, Airport operator, NM	Perf#03	POC/VLD Intent Dossier	
Pre-Exec#09	Specify ATCO / NMOC Staff data reporting (internal process)	ANSP, Airport operator, NM	Meas#03	ANSP / Airport Operator / NMOC Stall Internal Procedure	
Execution Phase / Execution & Monitoring					
Exec#01	Conduct live trials	Aircraft Operator ANSP, Airport operator, NM	Prep#05 Prep#06, Risk#03, Risk#05	POC/VLD Monitoring Report	
Exec#02	Investigate if stopping criteria triggered	Aircraft Operator ANSP, Airport operator, NM		POC/VLD Monitoring Report	
Exec#03	Measure performance	Aircraft Operator ANSP, Airport operator, NM	Meas#06	POC/VLD Monitoring Report	
Exec#04	Record Performance Measurements	Aircraft Operator ANSP, Airport operator, NM	Meas#06	POC/VLD Monitoring Report	
Exec#05	Stop Live trials when confidence reached	Aircraft Operator ANSP, Airport operator, NM	Meas#05	POC/VLD Monitoring Report	
Execution Phase / Analysis & Dissemination					
Resu#01	Flight Operational feedback	Aircraft Operator	Exec#04	POC/VLD Results Report	
Resu#02	Airborne system manufacturer feedback	TC/STC Holder		POC/VLD Results Report	

Resu#03	*ATM Operational feedback*	*ANSP, Airport operator, NM*	*Exec#04*	*POC/VLD Results Report*	
Resu#04	*Feedback consolidation*	*VLD Project Aircraft Operator ANSP, Airport operator, NM*		*POC/VLD Results Report*	
Resu#05	*Lessons Learnt*	*VLD Project*		*POC/VLD Results Report*	
Resu#06	*Provide feedback on SESAR OSED/SPR & SESAR Operational Assessment*	*VLD Project*	*Meas#07*	*POC/VLD Results Report*	
Resu#07	*Provide feedback on SESAR validation report*	*VLD Project*	*Meas#08*	*POC/VLD Results Report*	
Execution Phase / Reporting to Authorities					
Coor#03	*Deliver summary of execution activities to RCA*	*VLD Project Aircraft Operator ANSP, Airport operator, NM*	*Exec#02*	*POC/VLD Monitoring Report*	
Coor#04	*Deliver POC/VLD Result report to RCA*	*VLD Project*	*Resu#04 Resu#06*	*POC/VLD Results Report*	

END OF DOCUMENT-o

SESAR Safety Reference Material

Document information

Project title	Safety support and coordination function
Project Number	16.06.01
Project Manager	EUROCONTROL
Deliverable Name	SESAR Safety Reference Material
Deliverable ID	D27
Edition	00.04.00
Template Version	03.00.00

Task contributors

EUROCONTROL, AENA, AIRBUS, DFS, DSNA, FREQUENTIS, INDRA, NATS, NORACON, SELEX, THALES

Please complete the advanced properties of the document

Abstract

The SESAR Safety Reference Material presents a clear, complete, coherent and integrated approach to safety assessment to meet the needs of both the Industrial Research & Validation (R&I) (from TRL2-6) and Very Large Scale Demonstration (VLD) (from TRL6-7+) of the SESAR 2020 wave 1 work programme. It provides a practical guide on how to perform safety assessments in wave 1 of IRV activities (PJ01 to 18) as well as on the safety management of VLDs (PJ23-28 & 31) and develop safety assurance throughout V1-V4 lifecycle stages. It ensures that common method, tools and techniques will be used by all SESAR 2020 wave 1 Solutions, thereby greatly facilitating the collection of evidence/information and their integration into aggregated PJ19 Safety Cases to support the eventual deployment.

Authoring & Approval

Prepared By - Authors of the document.		
Name & Company	Position & Title	Date
Eric Perrin, EUROCONTROL	Project Manager / Content coordinator	11/03/2016
Juan Jesús Cano Quiñones, ENAIRE	Contributor	11/03/2016
Miguel Capote, ENAIRE (INECO)	Contributor	11/03/2016
Joelle Monso, AIRBUS	Contributor	11/03/2016
Viktoria Weigel, DFS	Contributor	11/03/2016
Yann CARLIER	Contributor	11/03/2016
Cécile MOURA, DSNA	Contributor	11/03/2016
Marta Llobet, EUROCONTROL	Contributor	11/03/2016
Bruno Rabiller, EUROCONTROL	Contributor	11/03/2016
Werner Winkerbauer, FREQUENTIS	Contributor	11/03/2016
Santoyo Pastor, Luis Víctor, INDRA	Contributor	11/03/2016
Sam Espig, NATS	Contributor	11/03/2016
Craig Foster, NATS	Contributor	11/03/2016
Massimo Capuano, SELEX	Contributor	11/03/2016
Bernard Pauly, THALES	Contributor	11/03/2016

Reviewed By - Reviewers internal to the project.		
Name & Company	Position & Title	Date
Jesus Romero Hernandez, ENAIRE	Contributor	18/03/2016
Joelle Monso, AIRBUS	Contributor	18/03/2016
Diana Durrett, DFS	Contributor	18/03/2016
Hans de Jong, DFS	Contributor	18/03/2016
Viktoria Weigel, DFS	Contributor	18/03/2016
Karim Mehadhebi, DSNA	Contributor	18/03/2016
Gabriele Schedl, FREQUENTIS	Contributor	18/03/2016
Amada Bernáldez de Aranzábal, INDRA	Contributor	18/03/2016
Sam Espig, NATS	Contributor	18/03/2016
Craig Foster, NATS	Contributor	18/03/2016
Bill Becton, NORACON	Contributor	18/03/2016
Lilla Hartyani, NORACON	Contributor	18/03/2016
Matthieu BRANLAT, SINTEF	Contributor	18/03/2016
Fateh KAAKAI, THALES	Contributor	18/03/2016

Reviewed By - Other SESAR projects, Airspace Users, staff association, military, Industrial Support, other organisations.		
Name & Company	Position & Title	Date
Andrew Kilner, EUROCONTROL	16.06.05 Project Manager	24/03/2016
Peter Martin, EUROCONTROL	SWP16.06 Manager -	24/03/2016

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

Name & Company	Position & Title	Date

Rejected By - Representatives of the company involved in the project.		
Name & Company	Position & Title	Date

Rational for rejection
None.

Document History

Edition	Date	Status	Author	Justification
00.00.01	15/09/2010	Draft	Eric Perrin	Strawman structure confirmed as basis for initial drafting & initial draft for review
00.00.02	22/09/2010	Revised Draft	Eric Perrin	Update following internal (16.06.01) review
00.00.03	07/10/2010	Revised Draft	Eric Perrin	Update following internal (16.06.01) review
00.00.04	08/10/2010	Revised Draft	Eric Perrin	Update following 2nd workshop on 7-8 October 2010
00.00.05	14/10/2010	Revised Draft	Eric Perrin	Update following internal (16.06.01) review
00.00.06	28/10/2010	Revised Draft	Eric Perrin	Update following internal (16.06.01) and SJU reviews – version shared with the Safety Assessment Task Force (SATF) of EASA ATM001
00.01.00	15/12/2010	Revised Draft	Eric Perrin	Proposed version for SJU review
00.01.01	24/09/2011	Revised Draft	Eric Perrin	Updated as a result of experience in applying SRM to pilot and release 1 Projects.
00.01.02	07/11/2011	Revised Draft	Eric Perrin	Global revision following comments from the SJU at 16.06.01 Gate on 16th August 2011 and resulting Gate Report.
00.02.00	15/12/2011	Revised Draft	Eric Perrin	Update to take into account EC regulation 1035/2011 and proposed issue for SJU review
00.02.01	30/01/2012	Final	Eric Perrin	Update to take into account SJU comments and proposed issue.
00.02.02	10/20/2012	Final	Eric Perrin	Update following formal review by the SJU
00.03.00	11/04/2014	Final - proposed	Eric Perrin	Update following review by National Authorities and EASA
00.03.00	12/12/2014	Final	Eric Perrin	Released version following 16.06.01 review
00.03.01	09/03/2015	Final	Eric Perrin	Usage of latest version of the template following SJU review
00.04.00	24/03/2016	Final - proposed	Eric Perrin	Update to support transition to SESAR 2020

Intellectual Property Rights (foreground)

This deliverable consists of SJU foreground.

Table of Contents

Executive summary

The aim of this document is to present a clear, complete, coherent and integrated approach to safety assessment that meets the need 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 wave 1 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 material generated by the SRM process and the SRM per se provide practical guidelines to assist.

It has been written for SESAR staff who are involved in:

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

In order to properly conduct the safety assessments of the SESAR solutions, the SRM details a broader approach to safety assessment in which ATM's positive contribution to aviation safety (a *success approach*), as well as ATM'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. Currently, only the latter is explicitly required by EC regulation CR 1035/2011.

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 should contact the SESAR 2020 PJ19.3 project when conducting safety assessments in accordance with this document. Please contact the 19.3 Helpdesk through extranet@sesarju.eu for help in applying this document.

1 Introduction

1.1 Purpose of the Document

The formalised, explicit and proactive approach to safety management across the SESAR work programme is presented in the "*SESAR Safety Approach*" (see **Reference 1**).

The SESAR Safety Reference Material (SRM) – this document - is a fundamental and critical component of the systematic safety management approach employed in SESAR through which the five elements of the Safety Approach will be discharged in SESAR 2020.

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 2020 wave 1 PJ1-18 projects (organized at a SESAR solution level) throughout the typical system development lifecycle being considered in the SESAR Development Phase that is[1]:
  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 wave 1 Very Large Demonstrations (VLD) (V4 *i.e.* from TRL6-7+) for which it is recommended to read the document in conjunction with the SESAR 1 P16.01.04 Final Guidance Material to Execute Proof of Concept (PoC) (see reference **17**). Both the local safety assurance and approval process of VLD are not necessarily within the remit of the SRM but material generated by the SRM process and the SRM per se intend to provide practical guidelines to assist.

It predetermines the safety assurance *objectives* and *activities* throughout the system development lifecycle (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) required to address the *asked questions* in section **1.5** concerning SESAR safety.

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*" (**Reference 2**).

The SESAR 2020 Project Hand-Book based on this document has been produced (see **Reference 3**). It provides:

- a high level introduction to the SRM and the concepts embedded within it
- 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 aspects of industrialization and approval that apply to VLD. It does not currently[2] intend to cover the complete life cycle of the constituent part of the ATM functional system[3] under consideration (Regulation (EC) No 1035/2011, Annex II, 3.2.1a – see **reference 16**).

In order for stakeholders to then produce their local safety assessment / safety case for deployment and operation, the local adaptation and development of SESAR Safety documentation should

[1] See Concept Lifecycle Model as per **Reference 9**.

[2] Should there be a need, this document could be augmented to address the post V3 phases, building upon, for example **Reference 5**.

[3] 'functional system' means a combination of equipments, procedures and human resources organised to perform a function within the context of ATM

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 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. 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 safety material developed using the SESAR SRM should be aware that it may be generic in nature or may come with caveats on the applicability of the analysis which have been taken to further the safety assessment. Safety practitioners should consider using SESAR safety assurance material as input to their local safety analysis, for example as a reference system. The safety material developed in SESAR may then be used to support proportionate safety assessments, where the safety assessment is limited to a review of the reference argument and an assessment of its applicability in the local context with an accompanying analysis of any gaps or deviations with additional mitigations applied as required or 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 a fresh assessment rather than attempt to re-use generic arguments.

1.3 Coverage and intended readership

This document is aimed mainly at safety practitioners in R&I (PJ1-18) and VLD (PJ23-28 & 31) projects of SESAR 2020 wave 1. The intended audience also includes SESAR JU and SJU members, SESAR 2020 PJ19, 20 and 22, 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 (total aviation system approach).

Safety practitioners should contact the SESAR 2020 PJ19.3 project when conducting safety assessments in accordance with this document. Please contact the 19.3 Helpdesk through extranet@sesarju.eu for help in applying this document.

1.4 Finding your way around

1.4.1 Layout

This document consists of nine further Chapters, as follows.

Section 2 introduces 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 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 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 SESAR Concept is to be used to decompose the ECAC-wide SESAR safety target into lower level targets for constituent components of the SESAR System[4] as a whole. Finally, it presents how critical it is that 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, mainly OSED, SPR and TSs.

Sections 5 to **8** address, respectively, the four steps of the safety assessment *i.e.* (1) planning the safety activities on an Solution; (2) executing the plan and documenting the results in the Solution OSED; (3) executing the plan and documenting the results in the Solution SPR; and (4) executing the plan and documenting the results in the Solution TSs.

Section 9 presents the need to inform and maintain a SESAR Safety Register to manage the large amount of information involved in doing safety assessments for the various Solutions as well as to ensure the consistency of the safety data (safety requirements, assumptions, etc.) across the SESAR work programme.

Section **10** 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 **Section11**.

1.4.2 Pictograms used to help you

The following set pictograms and meaning they convey are used throughout this document:

🧭	Guidance
❗	Important information
💡	Tip
🔍	For further reading…
ℹ	Safety Assessment results to be documented
✈	Safety assurance activities mainly aimed at the Operational level
🌐	Safety assurance activities mainly aimed at the technical system level

[4] The eATM Portal, https://www.eatmportal.eu/working, provides an integrated view of the European ATM System.

1.5 Important messages at this stage…

1. Safety Assessments done in accordance with this document must be done at the **Solution level**.[5]

2. When considering a package made up of several Solutions, the SESAR 1 P16.06.01:

a). Has developed a safety argument template addressing in particular the internal consistency of the package (for example concerning interfaces and dependences), the assumptions made in various individual safety assessments for the, at the time, relevant Solutions, as well as emergent properties coming from packing several Solutions together (see **Reference 15**)

b). Has developed a Safety Register implemented in Remedy (see **section 9** herein and Guidance H in **Reference 2**) to be informed and maintained by the SESAR R&I Projects to enable P19.3 to control the portfolio of Solutions safety assessments. It enables queries to be made to check the x-Solutions consistency of safety objectives, safety requirements, assumptions, issues, etc. as well as providing an accessible overview of the safety assessment of a specific Solution.

3. SESAR brings about significant changes to ATM 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?
- 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?

4. Since the properties of the operational environment are crucial to a safety assessment – specifically, a safety assessment that is valid for one (reference) operational environment may not be valid for a different operational environment – the safety assessment cannot be "*generic*". It has to be "***specific***" to a particular environment and to a "***typical***" application in each phase of flight. For instance, 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 PJ19.3 to ensure that the selected specific validation environment is as generic as possible.

[5] 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 the wave 1 of R&I projects does not accord with this objective (e.g. PJ14 to 17). 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 PJ19.3.

Examples of instantiation of 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?[6]

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 have tended to assess how reliable the ATM system (as a combination of equipments, procedures and human resources organised to perform a function within the context of ATM) needs to be to ensure that the system is adequately protected against internal failures. This restricted view of safety has been sufficient since ATM systems have gradually evolved and it has been adequate to rely on the assumption that ATM system is intrinsically safe when no failure occurs. Given the nature of SESAR concepts, the development of new technologies and the increasing use of automation, this assumption is no longer valid.

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

Consequently, 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 already in aviation will be reduced by the ATM changes. This is concerned with the *positive contribution to aviation safety* that the ATM changes make in the absence of failure.
- Secondly, a ***failure approach*** in which we assess the ATM system generated risks, *i.e.* induced by the ATM changes failing. This is concerned with the *negative contribution to the risk of an acciden*t that the ATM changes might make in the event of failure(s), however caused.

The SESAR SRM building on EUROCONTROL SAME (see **Reference 5**):

- puts the SAM (see **Reference 4**) in into an argument framework to support the failure approach, and
- despite an explicit regulatory requirement, adds a success approach to show whether the concept is intrinsically safe, in the absence of failure.

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

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.

EUROCONTROL “Safety Assessment Made Easier” Part 1 (see **Reference 5**) explains in more detail why a failure-based approach to ATM safety assessment is not sufficient to support the new ATM concepts that are currently being planned for SESAR. It shows how the addition of a success-based approach leads to a more complete specification of an ATM functional system’s safety properties.

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, and that as a consequence, it is increasingly difficult to deliver further safety benefits based using standard approaches to safety (hence the broader approach as per **section 2.1** herein)
- 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 system behaviour.

The SRM enables to identify:

- small variations in ATM system performance that may “coincide and combine” to produce variations in safety performance outcomes;
- dependencies in the ATM 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; as well as
- the different safety features that can interact in a positive way to make for better safety performance.

	Guidance I in **Reference 2** 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, the practice aims to support 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.
	Reference 13, 'Final Resilience Guidance Material for Safety Assessment (SRM) and Design', provides 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 Guidance A1 to A4 in Reference **2**. **Reference 14**, 'From Safety-I to Safety-**II**.', 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 2020) 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 measure that defines **what has to be achieved in terms of safety for specific concepts of operation** in order to satisfy the ECAC-wide safety target. At the level of the individual concepts, what is tolerably safe is referred to as the **SAfety Criterion(a) (SAC)**.

A major problem is the sheer complexity of the SESAR 2020 Concept (18 R&I projects, 53 solutions, 285 Operational Improvements steps (OIs)), 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. So, the problem arises as to how to derive suitable SAfety Criterion(a) 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) from project SESAR 1 P16.01.01 which lies at the heart of this delicate apportionment exercise.[7] **Reference 11** summarises the qualitative and quantitative validation / verification for the AIM.[8]

[7] Guidance M in **Reference 2** Guidance M 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.

[8] Since the closure of Project 16.01.01 in 2014, the SESAR 1 Project 16.06.01 took over responsibility for developing the AIM models to reflect the needs of SESAR at an ECAC level. Project 16.06.01 will finish in July 2016 and within the framework of

The AIM risk model provides a set of templates (one for each accident type – see **Reference 10**) that all SESAR Solutions have to use[9] to identify where and how the operational changes brought by a specific Solution will impact the safety of ATM provision.[10]

AIM consists of a risk model, which shows the risks of aviation accidents[11] and provides a structured breakdown of their causes, with particular emphasis on ATM 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 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 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 necessary[12] to satisfy the ECAC wide safety targets.

Once the overall SESAR ATM risks meet the overall ECAC-wide target (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 Criterion(a). 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 affect on safety). The setting of suitable and consistent SAfety Criteria is further explained in **Reference 2, Guidance D**. 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. Using AIM for the determination of the severity of the effects of hazards and associated safety objectives is described in **Reference 2, Guidance E**.

> ❗
>
> Of course data-based, static models such as AIM, whilst providing the view of how ATM 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 system.
>
> Consequently the AIM models are NOT 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

SESAR 2020 there shall be no further methodological development of the AIM models. At an ECAC level therefore there is no future vehicle for refining the AIM models and they should remain static.
Parties (ANSPs mainly), that expressed an interest in deploying the AIM models locally (a local instantiation of the model shall be in the future known as an IRiS model) have, with EUROCONTROL, formed a users forum to discuss further development and refinement of the models, primarily for local deployment. EUROCONTROL chairs the bi-annual meeting with a view to extracting best practice within ANSPs and delivering that best practice into the IRiS models. The IRiS models are modified – lightly – during the meetings and participants are asked to agree the changes. Thus the IRiS user forum is the means by which the models are revised and those revisions agreed for broader dissemination.
Should within the scope of S2020 an update to the AIM model be required, it could realistically, only be delivered from the IRiS user group. Effectively therefore the IRiS user forum provides the basis for the continued refinement of the IRiS models and offers the opportunity to manage further releases of the AIM ECAC model despite there being no specific SESAR vehicle that allows this to take place.

[9] For validation and verification aspects, see **Reference 11**.

[10] 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.

[11] Models currently exist for MAC En-route, TMA, Oceanic, CFIT, RWY INC, TWY accidents, and Wake-related accidents. At the time of the development of this version of the SRM, a RWYEXC model is being developed.

[12] 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 **Reference 2**. 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 **Reference 2**). 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.

	system hierarchy (Aggregation of Solutions, and individual Solutions) and for specific phases of flight. ***Within the scope of this document, a SAfety Criterion shall be defined for each Solution.*** ▪ They provide SAfety Criteria that take account of future changes to the ATM/ANS functional system and / operational environment, rather than being tied to the past / current situation.

💡	In SESAR 2020, PJ19.3 provides all required support to R&I projects and Solutions for the identification of the SAfety Criteria. Indeed, in doing so, PJ19.3 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 successful implementation of ATM evolutions. It is critical therefore that the concepts being developed take account of human strengths and weaknesses in their development. By fully addressing the Human components of System safety, this document intends to maximize human performance and minimize 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 **Reference 2**, the SRM has moved towards an integrated approach to performance management with, as a first step, the establishment of a Safety and Human Performance[13] (HP) collaboration to improve the performance of the overall Total Aviation System.

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

For any change to ATM/ANS function systems, the following 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.

[13] As **per Reference 12**, 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, 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: The capability of a human to successfully and safely accomplish tasks depends on a number of variables. Understanding these variables and the interplay with 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.

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 of human tasks and safety impact that an appropriately thorough HF analysis has been undertaken.

3 SRM: process and lifecycle

3.1 Safety Assessments and the OSED, SPR and TSs

With respect to the formal SESAR deliverables, the SESAR 2020 Solution OSED/SPR/INTEROP and TS formally capture from a safety perspective the safety requirement hierarchy[14] 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 PJ19.3 with the assistance of the Solution operational and technical experts to determine what proportion of the x10 SESAR safety performance target the Solution is expected to deliver.

🔍

Reference 6 interprets the x10 SESAR safety performance target 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 entirely applicable to SESAR programme but also to some other non-SESAR ATM improvements (see sections corresponding to Airspace and Airport capacity KPAs)
- 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

[14] The safety requirement hierarchy is the safety requirement cascade from the SAfety Criteria to the safety objectives to the safety requirements.

	with ATM contribution in relation with the airspace capacity and airport capacity KPAs.

SAfety Criteria (SAC) are derived during V1 through safety assessment of the AIM and are presented in the Solution OSED. As the Solution progresses to V2 and the Solution concept is further refined, the safety assessments at the OSED level will establish the ***safety objectives*** to deliver the SAfety Criteria and the SPR level ***safety requirements*** to satisfy the safety objectives, respectively. The safety objectives and interim safety requirements are presented in the updated OSED and SPR sections of the Solution OSED/SPR respectively. As the design further develops from what is still a fairly abstract concept towards physical realisation in V3, safety assessment activities at the physical level will determine the lower level human task and technological elements ***detailed safety requirements*** which satisfy the SPR level safety requirements. These are presented in both the refined Solution SPR section for the human task requirements and in the Solution TS for the technological elements. Traceability from the lower level requirements to the SAfety Criteria must be explicit and presented in OSED, SPR 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 pictorially in **Figure 1**. **Figure 1** is a top-level view of the System Engineering/development process and how the main outcomes from the safety assessment as per the SRM 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 design requirements. These new requirements may necessitate further design changes. The safety assessment process ends with the verification that the design meets the safety requirements. For the sake of keeping this figure simple, the iterative nature is not explicitly shown.

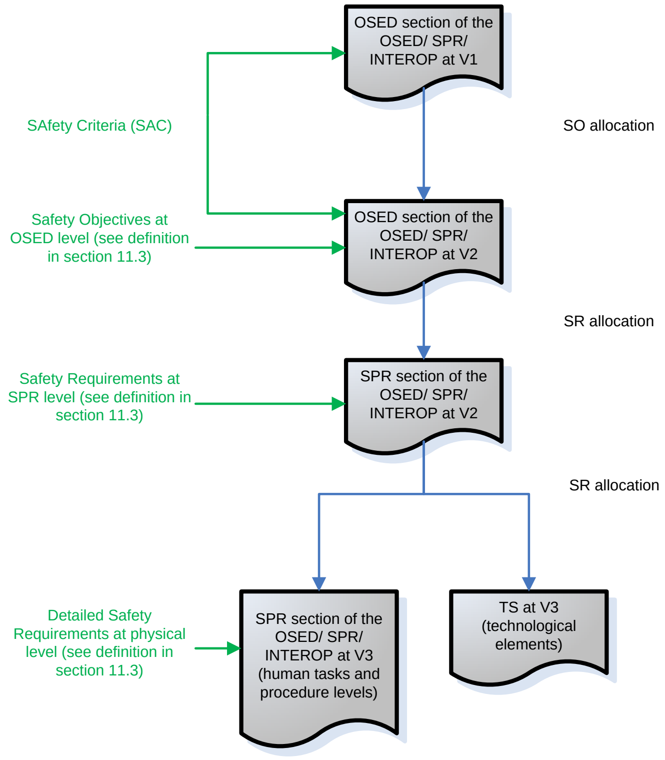

OSED section of the OSED/ SPR/ INTEROP at V1
SAfety Criteria (SAC)
SO allocation
Safety Objectives at OSED level (see definition in section 11.3)
OSED section of the OSED/ SPR/ INTEROP at V2
SR allocation
Safety Requirements at SPR level (see definition in section 11.3)
SPR section of the OSED/ SPR/ INTEROP at V2
SR allocation
Detailed Safety Requirements at physical level (see definition in section 11.3)
SPR section of the OSED/ SPR/ INTEROP at V3 (human tasks and procedure levels)
TS at V3 (technological elements)

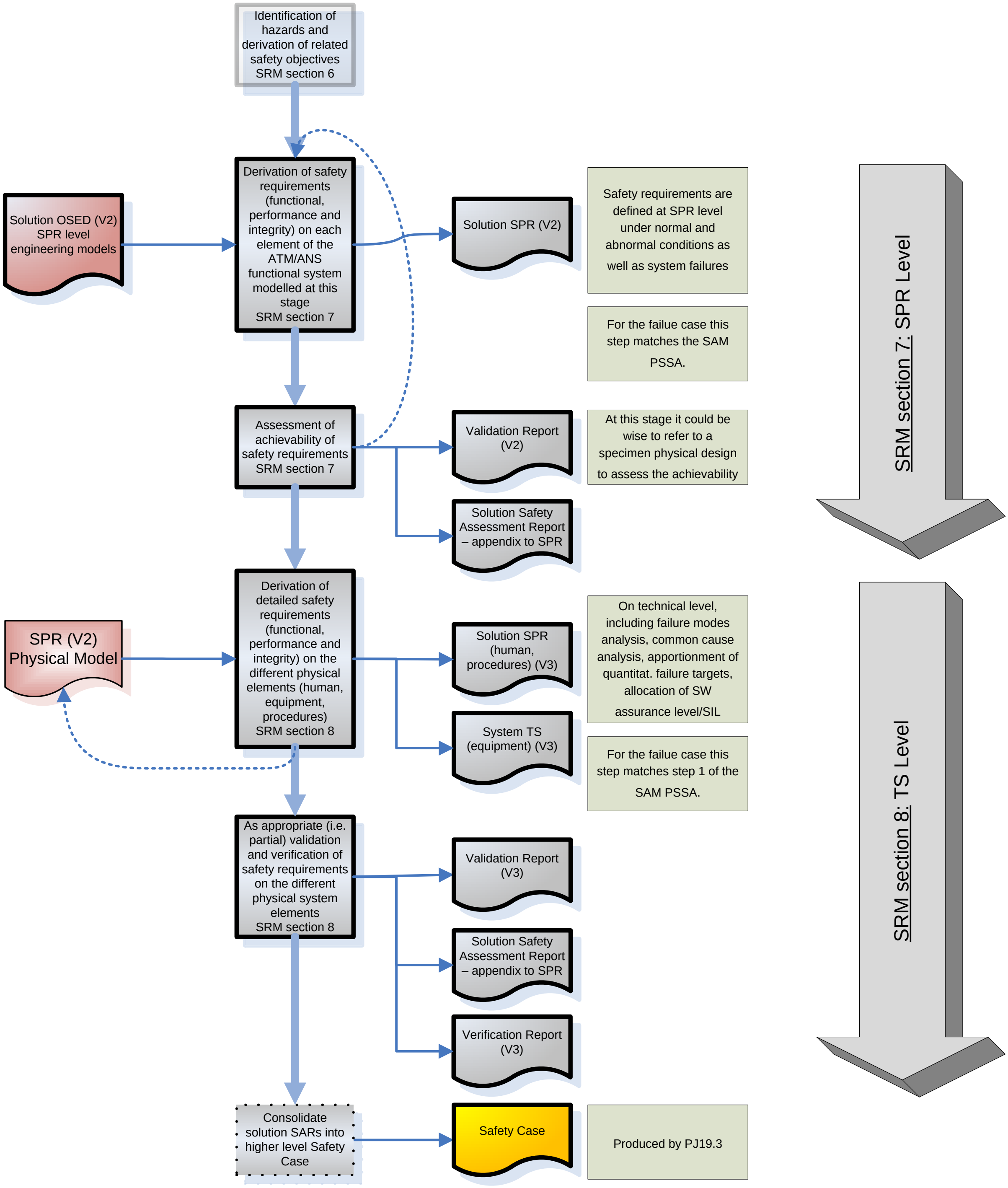
Figure 1: Safety Requirements and the Solution OSED, SPR and TS

❗	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) which set both the minimum positive (success approach), and maximum negative (failure approach), safety contributions of the ATM system. Overall this is an iterative requirements specification – a requirements satisfaction exercise that is

	completed when it is demonstrated that the actual design is realistic, *i.e.* achievable in terms of the safety requirements it places on the human, procedural and technological elements of the System. The safety objectives from the success approach are concerned with what the ATM system has to do in a particular Operational Environment but not how 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 how the design of the ATM system satisfies the Safety Objectives.

3.2 Safety Assurance Activities & SESAR Deliverables

As explained above, the Solution OSED/SPR/INTEROP, 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 implementation related safety requirements. Their relationship is depicted in **Figure 2** below. 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


Identification of hazards and derivation of related safety objectives SRM section 6
Solution OSED (V2) SPR level engineering models
Derivation of safety requirements (functional, performance and integrity) on each element of the ATM/ANS functional system modelled at this stage SRM section 7
Solution SPR (V2)
Safety requirements are defined at SPR level under normal and abnormal conditions as well as system failures
For the failue case this step matches the SAM PSSA.
Assessment of achievability of safety requirements SRM section 7
Validation Report (V2)
At this stage it could be wise to refer to a specimen physical design to assess the achievability
Solution Safety Assessment Report – appendix to SPR
SRM section 7: SPR Level
SPR (V2) Physical Model
Derivation of detailed safety requirements (functional, performance and integrity) on the different physical elements (human, equipment, procedures) SRM section 8
Solution SPR (human, procedures) (V3)
On technical level, including failure modes analysis, common cause analysis, apportionment of quantitat. failure targets, allocation of SW assurance level/SIL
System TS (equipment) (V3)
For the failue case this step matches step 1 of the SAM PSSA.
As appropriate (i.e. partial) validation and verification of safety requirements on the different physical system elements SRM section 8
Validation Report (V3)
Solution Safety Assessment Report – appendix to SPR
Verification Report (V3)
SRM section 8: TS Level
Consolidate solution SARs into higher level Safety Case
Safety Case
Produced by PJ19.3

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 Solution OSED presents the overarching operational concept for the Solution. From a safety perspective, it presents the operational 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 basis of the V1 Validation Plan.

The Solution OSED is also updated during V2 to present the safety objectives (success and failure approach) derived during the V2 safety assessment. It will also provide full traceability from the SAfety Criteria to the safety objectives identifying which services are supporting the SAfety Criteria. During V2, it is envisaged that the safety objectives will be used to drive the validation activities and will form the basis of the V2 Validation Plan.

3.2.2 Solution Safety and Performance Requirements (SPR)

The SPR is written at the Solution level and is also issued during V2. It reflects the increased maturity of the intended design solution. The SPR presents the traceability from the safety objectives, down to safety requirements at the SPR level which will have been determined during the V2 safety assessment. The safety requirements are presented at a level sufficient to enable 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. It is envisaged that the safety requirements can then be used to drive the validation activities and will form the basis of the V2 Validation Plan.

The SPR is also updated in V3 to reflect the outcome of the V3 safety assessment of the physical model. It will present the lower level human task safety requirements and show traceability to the safety requirements developed in V2.

3.2.3 Technical Specification (TS)

The TS is written for each Solution by the R&I Project at the physical level during V3. It is written at a level of detail sufficient to allow the technological element 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, it presents the safety requirements (*functional, performance and integrity properties*) from the success and failure approaches of the relevant technological elements.

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. The Project Content Integration Team (PCIT) for each R&I project has a vital role in ensuring consistency within the Solutions.

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 2.2** and expanded in **Reference 2, Guidance D**. 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 "*Solution X shall provide a 5% demonstrable reduction in ATC Induced Conflicts per flight hour despite a x% increase in traffic.*"

2. Another example could read: "*Solution Y shall provide a 30% demonstrable reduction in Controlled Flights Towards Terrain per approach.*"

It is also mandated 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 discounted 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[15] and failure) in support of the SAfety Criteria.

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

1. An example safety objective (success approach) in normal conditions could read (in that case for Point Merge System): *as each aircraft turns off the Sequencing Leg towards the Merge Point, vertical separation shall be maintained between it and all aircraft on the adjacent sequencing leg until horizontal separation is established (and can be maintained) between them*

2. Examples of abnormal conditions could be:

- Aircraft Emergency - medical, technical (e.g. engine failure) etc.
- Runway change - e.g. unplanned change of direction
- Sudden reduction in runway capacity - e.g. due to sudden drop in visibility
- Unforeseen runway closure
- Very strong winds (e.g. > 50 kts)
- Sudden and significant change in wind direction - moderate to strong wind conditions
- Severe weather
- Solar storms (ionosphere events)
- failures (human or technical) external to the ATM change being considered

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".

3. An example safety objective (success approach) in abnormal conditions could read (still in that case for Point Merge System): *In the event of a sudden runway closure all traffic shall be diverted to alternative aerodromes (or runway) in accordance with standard practice, making use of Point Merge System holding points*

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

To avoid System-generated hazards to be inconsistently defined across the SESAR 2020 work programme, they have to be identified at the level of the Operational services, *i.e.* a level that is independent of the actual design of the System and is related to the failure of an operational service.

[15] Measurements of precursors to serious incidents or accidents as part of a validation exercise, on the basis of simulations for both a Do Nothing Case and a With Change Case, should permit to assess how successful (or otherwise) a change is in meeting the safety validation objectives and from there the safety objectives (success approach). This may lead for a feedback loop to revisit the safety objectives and the SAC if so required.

Examples of System-generated hazards could read (still in that case for Point Merge System):

- *Aircraft turns to Merge Point at wrong time*
- *Aircraft descends below the minimum sector altitude along Direct-to path*

Guidance on the usage of Risk Classification Schemes to generate safety objectives (failure approach) is provided in **Reference 2, Guidance E**.

As with V1, assurance that the objectives are realistic and can be achieved will also have to be included within the phase one V2 safety assessment, plus any new assumptions.

Phase Two

The phase two V2 safety assessment involves the analysis of the ***SPR level model*** 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.

It is expected that safety requirements (success and failure) will be documented in V2 SPR document, as well as the allocation process (e.g. fault trees, qualitative argumentation for the apportionment or derivation of safety requirements from one level to lower level, in line with the SPR level model).

1. Examples of safety requirement (success approach) in normal conditions could read (in that case for Point Merge System):

EXEC controllers shall, as far as practicable, use IAS instructions to maintain homogeneous groundspeeds of all aircraft between Point Merge System entry and exit points, taking account of the need for each aircraft to reduce its airspeed over this period

Procedure Design shall ensure that the two P-RNAV routes that converge laterally at the Common Point are vertically separated by at least 1000 feet at the Common Point by means of published altitude restrictions

2. An example safety requirement (success approach) in abnormal conditions could read (still in that case for Point Merge System): *In the event of a sudden change in wind direction, EXEC controllers shall issue updated speed instructions to aircraft as necessary to maintain the required spacing and a homogenous groundspeed throughout the PMS structure*

V3 Safety Assessment – requires the analysis of a physical model to represent the intended final design solution. The V3 safety assessment is expected to analyse the physical model in order to derive low level physical safety requirements (success and failure). For the safety requirements (failure approach), this is achieved through the application of the first stage of SSA equivalent activities. Resultant requirements that relate to the human task are expected to be documented in the V3 Solution SPR whereas technological element level requirements are expected to be documented in the Solution Technical Specification document. Traceability from higher level safety requirements to lower level safety requirements must be made explicit as well as the means of requirement allocation.

Assurance that the requirements are realistic and can be satisfied by the intended physical design must be provided as part of the first stage of SSA equivalent activities and included within the safety assessment.

It should be noted that the SPR- and physical-level models mentioned herein should already be available as part of the normal operational, project-management and /or systems-engineering processes[16] (in particular from PJ19.2, 19.3 and 19.4 (EATMA)). Maximum use should be made of such information subject to it being possible to show sufficient confidence in its completeness and correctness, for safety purposes. 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.

It is impossible in the safety assessments done in SESAR 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 showing the potential for the Solution to meet the SAC can be achieved 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 **L** of **Reference 2** 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 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 requirements since they drive the design and validation process.

By their nature these requirements may not be traceable and should have rationale that is visible eventually for the deployment.

Configuration and assumptions management is facilitated by maintaining a Safety Register throughout the life of the project / solution. This is addressed in section **10.**

For generic guidance on engineering models, go to **Reference 2, Guidance G**

[16] In particular with the European ATM Architecture (EATMA).

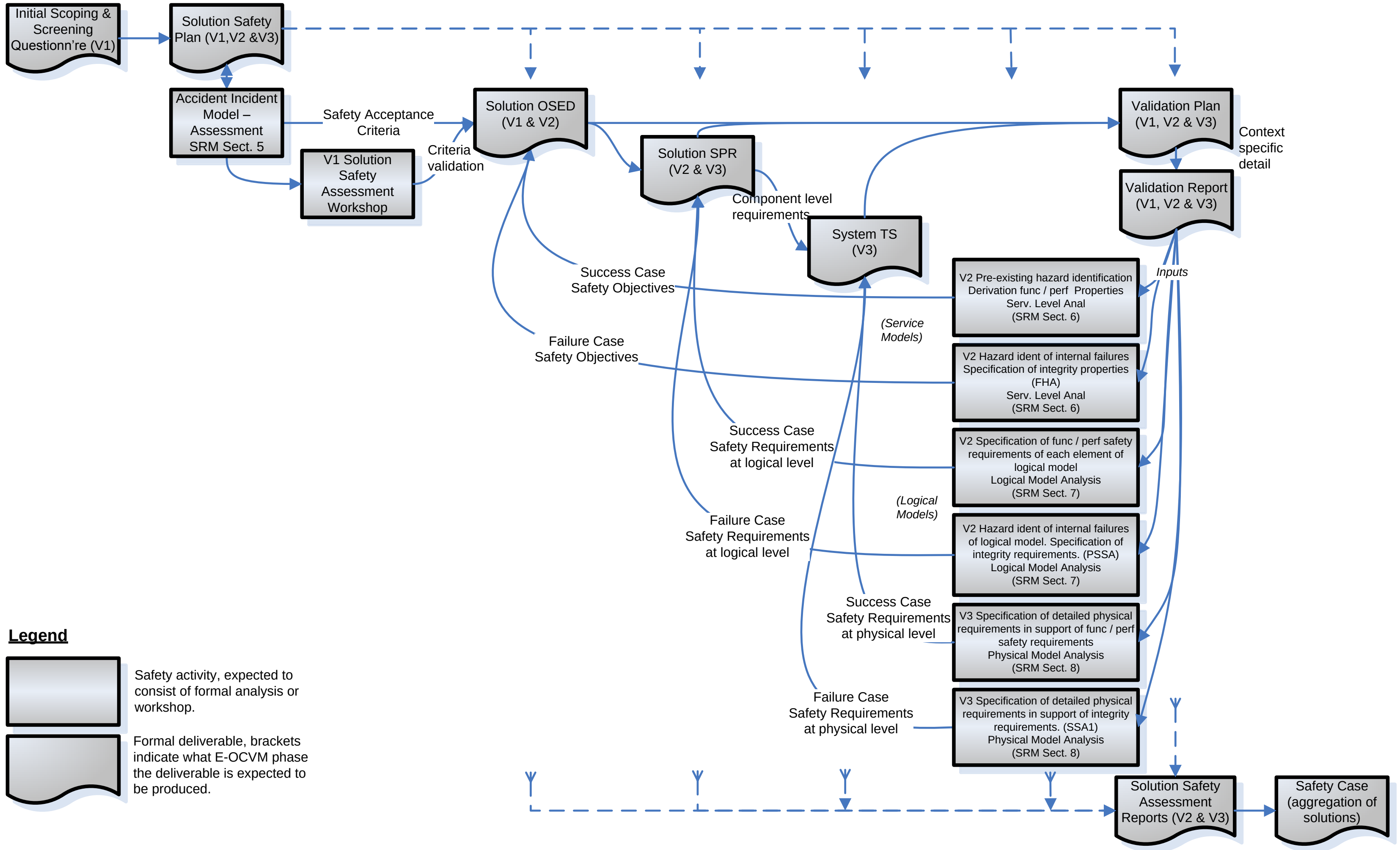

Initial Scoping & Screening Questionn're (V1)
Solution Safety Plan (V1,V2 &V3)
Accident Incident Model – Assessment SRM Sect. 5
Safety Acceptance Criteria
V1 Solution Safety Assessment Workshop
Criteria validation
Solution OSED (V1 & V2)
Solution SPR (V2 & V3)
Component level requirements
System TS (V3)
Validation Plan (V1, V2 & V3)
Context specific detail
Validation Report (V1, V2 & V3)
Inputs
Success Case Safety Objectives
Failure Case Safety Objectives
(Service Models)
V2 Pre-existing hazard identification Derivation func / perf Properties Serv. Level Anal (SRM Sect. 6)
V2 Hazard ident of internal failures Specification of integrity properties (FHA) Serv. Level Anal (SRM Sect. 6)
Success Case Safety Requirements at logical level
V2 Specification of func / perf safety requirements of each element of logical model Logical Model Analysis (SRM Sect. 7)
(Logical Models)
Failure Case Safety Requirements at logical level
V2 Hazard ident of internal failures of logical model. Specification of integrity requirements. (PSSA) Logical Model Analysis (SRM Sect. 7)
Success Case Safety Requirements at physical level
V3 Specification of detailed physical requirements in support of func / perf safety requirements Physical Model Analysis (SRM Sect. 8)
Failure Case Safety Requirements at physical level
V3 Specification of detailed physical requirements in support of integrity requirements. (SSA1) Physical Model Analysis (SRM Sect. 8)
Solution Safety Assessment Reports (V2 & V3)
Safety Case (aggregation of solutions)
Legend
Safety activity, expected to consist of formal analysis or workshop.
Formal deliverable, brackets indicate what E-OCVM phase the deliverable is expected to be produced.

Figure 2: Relationship between Safety Assurance Activities and Solution OSED, SPR and TS

4 The SRM process in full

The full process for deriving the SAfety Criteria (SAC), safety objectives (SOs), and then 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 that section **2.4** above describes.

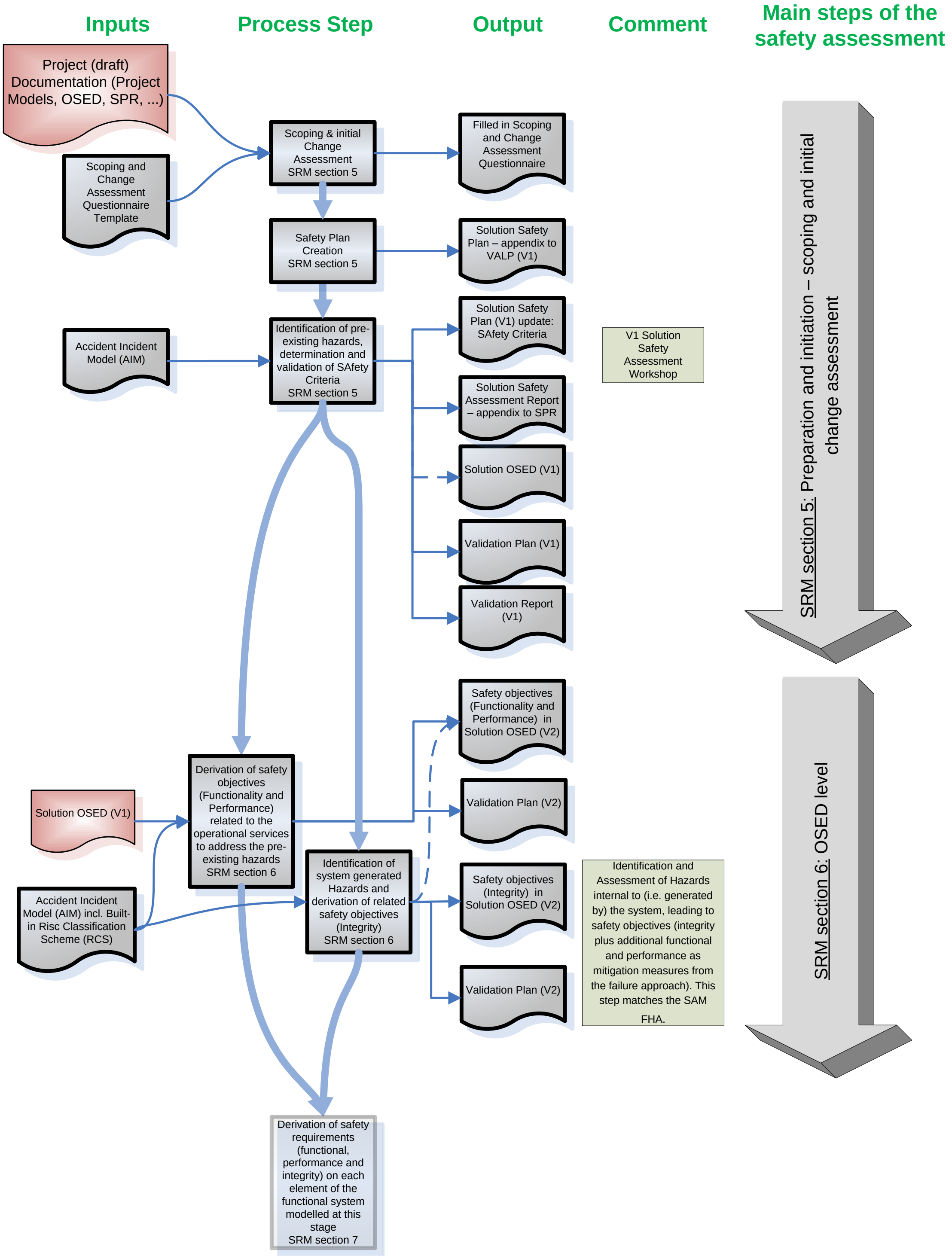

Inputs
Process Step
Output
Comment
Main steps of the safety assessment
Project (draft) Documentation (Project Models, OSED, SPR, ...)
Scoping and Change Assessment Questionnaire Template
Scoping & initial Change Assessment SRM section 5
Filled in Scoping and Change Assessment Questionnaire
Safety Plan Creation SRM section 5
Solution Safety Plan – appendix to VALP (V1)
Accident Incident Model (AIM)
Identification of pre-existing hazards, determination and validation of SAfety Criteria SRM section 5
Solution Safety Plan (V1) update: SAfety Criteria
V1 Solution Safety Assessment Workshop
Solution Safety Assessment Report – appendix to SPR
Solution OSED (V1)
Validation Plan (V1)
Validation Report (V1)
SRM section 5: Preparation and initiation – scoping and initial change assessment
Safety objectives (Functionality and Performance) in Solution OSED (V2)
Solution OSED (V1)
Derivation of safety objectives (Functionality and Performance) related to the operational services to address the pre-existing hazards SRM section 6
Validation Plan (V2)
Accident Incident Model (AIM) incl. Built-in Risc Classification Scheme (RCS)
Identification of system generated Hazards and derivation of related safety objectives (Integrity) SRM section 6
Safety objectives (Integrity) in Solution OSED (V2)
Identification and Assessment of Hazards internal to (i.e. generated by) the system, leading to safety objectives (integrity plus additional functional and performance as mitigation measures from the failure approach). This step matches the SAM FHA.
Validation Plan (V2)
SRM section 6: OSED level
Derivation of safety requirements (functional, performance and integrity) on each element of the functional system modelled at this stage SRM section 7

Figure 3: SAC, SO and SR specification process

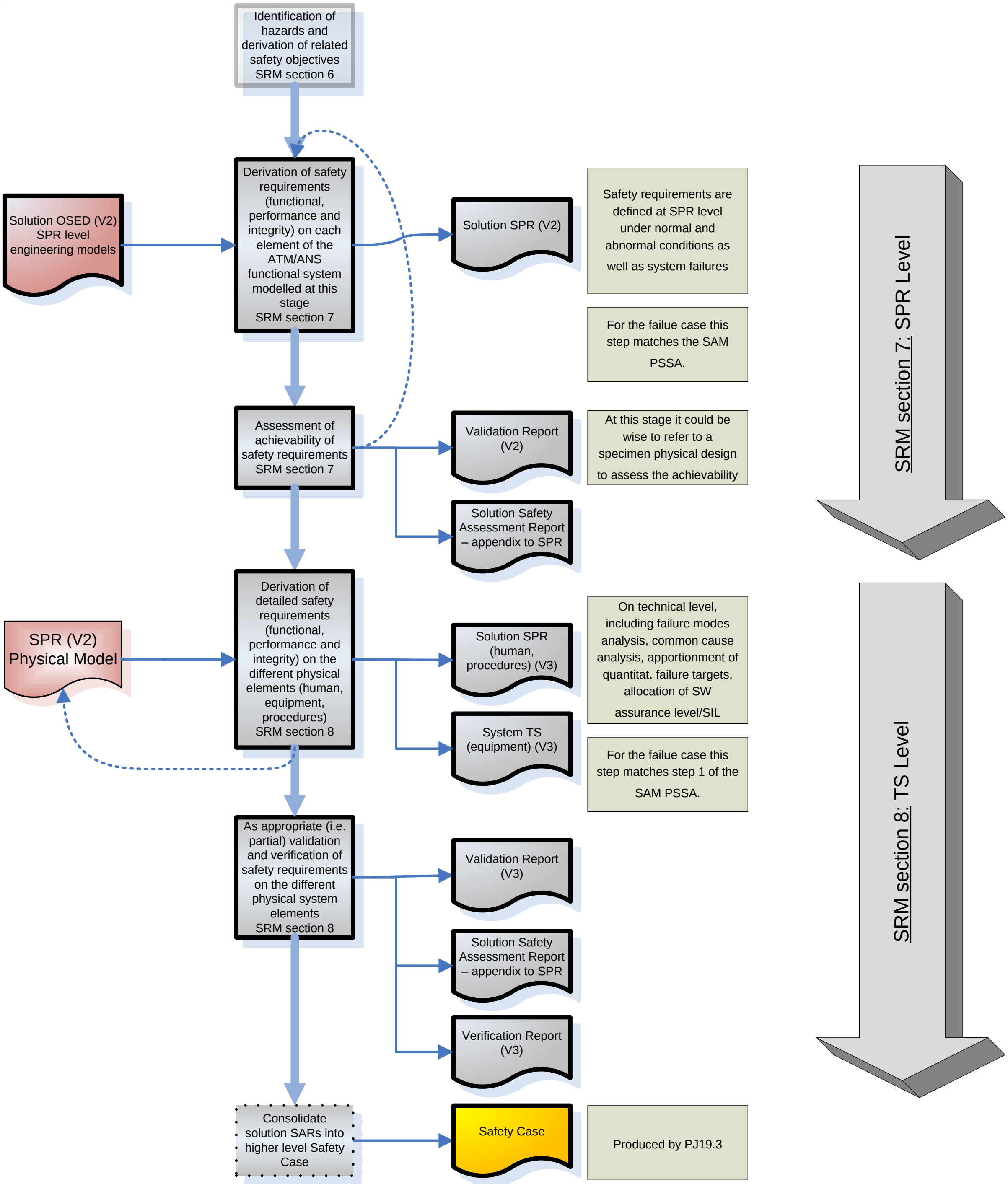
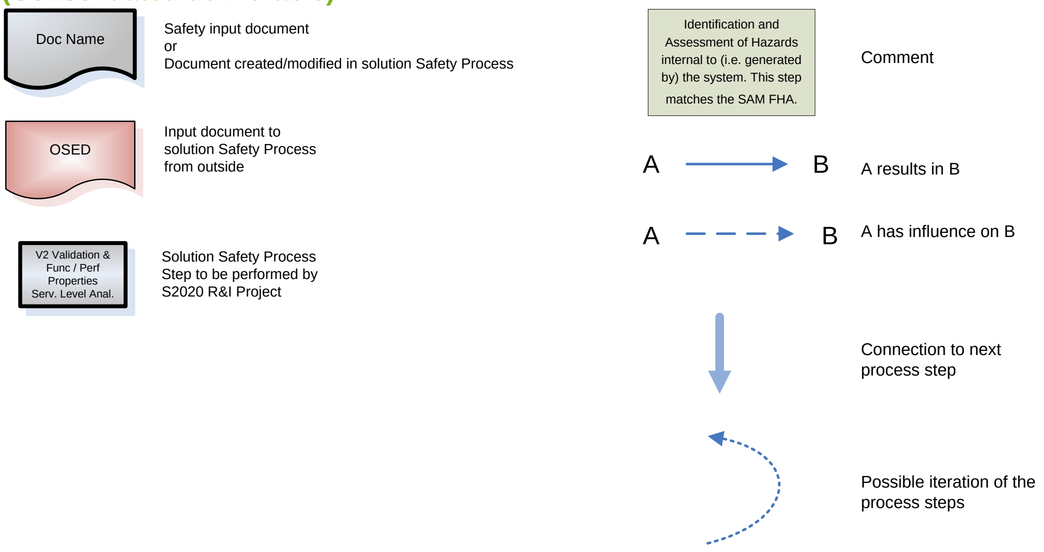

Identification of hazards and derivation of related safety objectives SRM section 6
Solution OSED (V2) SPR level engineering models
Derivation of safety requirements (functional, performance and integrity) on each element of the ATM/ANS functional system modelled at this stage SRM section 7
Solution SPR (V2)
Safety requirements are defined at SPR level under normal and abnormal conditions as well as system failures
For the failue case this step matches the SAM PSSA.
Assessment of achievability of safety requirements SRM section 7
Validation Report (V2)
At this stage it could be wise to refer to a specimen physical design to assess the achievability
Solution Safety Assessment Report – appendix to SPR
SRM section 7: SPR Level
SPR (V2) Physical Model
Derivation of detailed safety requirements (functional, performance and integrity) on the different physical elements (human, equipment, procedures) SRM section 8
Solution SPR (human, procedures) (V3)
On technical level, including failure modes analysis, common cause analysis, apportionment of quantitat. failure targets, allocation of SW assurance level/SIL
System TS (equipment) (V3)
For the failue case this step matches step 1 of the SAM PSSA.
As appropriate (i.e. partial) validation and verification of safety requirements on the different physical system elements SRM section 8
Validation Report (V3)
Solution Safety Assessment Report – appendix to SPR
Verification Report (V3)
SRM section 8: TS Level
Consolidate solution SARs into higher level Safety Case
Safety Case
Produced by PJ19.3

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

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



Doc Name

Safety input document
or
Document created/modified in solution Safety Process

OSED

Input document to
solution Safety Process
from outside

V2 Validation & Func / Perf Properties Serv. Level Anal.

Solution Safety Process
Step to be performed by
S2020 R&I Project

Identification and Assessment of Hazards internal to (i.e. generated by) the system. This step matches the SAM FHA.

Comment

A → B

A results in B

A - - → B

A has influence on B

Connection to next
process step

Possible iteration of the
process steps

5 Application of the SRM: what it delivers to the Validation Plan

The VALP is extended with supplementary information to cover the Transversal Areas assessment activities beyond the validation "exercises" per-se. This is essential if we are to move validation on from a technical/operational demonstration through FTS/RTS/trial to a situation where we can gather evidence that is of use for the Business Case(s). For safety, this is addressed in a Safety Plan, which is appended to the VALP. The Safety Plan (see **Reference 7**) describes the safety assurance activities that are 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) and eventually SPR. The Safety Plan also clearly defines the roles and responsibilities amongst the SJU, PCIT, Project, Solution staff working on Safety related tasks, PJ19.3 staff, etc. using a ‘Lead, Do, Consult, Inform’ scheme.

The Safety Scoping & Change Assessment process aims at specifying the detailed safety assessment activities to be undertaken by the Solution. With the support of PJ19.3 and the active participation of the Solution, this preparatory process identifies the main safety issues associated with projects within the specific 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, amongst other things, 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 SESAR Safety Reference Material requires the safety assessment to start in the operational environment with the aim of first understanding and documenting the properties of the operational environment and deriving the SAfety Criteria (*i.e.* the operational services-user requirements).

Consequently, the following activities will be addressed (details of the planned safety assurance activities are provided in **Reference 2, section A.1**, hereto):

- 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 that support 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 **Reference 2, Guidance A.2** to **A.4** are all generic. The execution of the Safety Scoping and Change assessment process defined in **Reference 2, Guidance C** will help identify what will / will not change as a result of the primary projects concerned, and to specify the detailed safety assessment activities. 2. The purpose of most safety-related systems is to mitigate the hazards (and associated risks) that are *pre-existing* in the operational environment of the system concerned. These hazards are, therefore, 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 system the *pre-existing hazards* and risks are generally those that are inherent in aviation and for which the main raison d'être of ATM is to provide as much mitigation as possible. Example of pre-existing hazards: ▪ *a situation in which the intended trajectories of two or more aircraft are in conflict* ▪ *a situation where the intended trajectory of an aircraft is in conflict with terrain or an obstacle* ▪ *penetration of restricted airspace – this category is quite distinct from Mid-Air Collision for military danger areas where the end effect could be being shot down*

✥	1. For guidance on the safety scoping and change assessment process, go to **Reference 2, Guidance C** 2. For guidance on describing the operational environment, go to **Reference 2, Guidance B** 3. For guidance on identifying pre-existing hazards, go to **Reference 2, Guidance F** 4. For guidance on setting SAfety Criteria, go to **Reference 2, Guidance D** 5. P16.06.01 has developed a Safety Plan Template (see **Reference 7**) to enable the Solution to specify, *inter alia*, the safety assurance activities that are to be carried out by a Solution. This Template is available on the SJU Extranet at https://extranet.sesarju.eu/Programme%20Library/Forms/Templates.aspx.

6 Application of the SRM: what it delivers to the Solution OSED

The purpose of this section is to derive safety objectives under normal and abnormal operational conditions as well as in the case of internal failures.

The safety objectives are specified at the OSED level for three purposes:

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

In the first two cases, the safety objectives address the *functionality & performance* to be achieved and, in the third case, they address the *integrity/reliability* to be achieved. Taken as a whole, therefore, 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 OSED 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.

Consequently, the following activities will be addressed (details of the planned safety assurance activities are provided in **Reference 2, Guidance A.2** hereto):

- Refined description of the operational services that support the Solution operations, and the derivation of Safety Objectives (from the success approach *i.e. functionality and performance*) in order to mitigate the pre-existing risks under normal conditions of the Operational Environment
- assessment of the adequacy of the operational services under abnormal conditions of the Operational Environment
- assessment of the adequacy of the operational services in the case of internal failures and mitigation of the ***system-generated hazards***
- assessment of the impact of the Solution operations within the operational environment (including adjacent airspace if relevant)
- satisfaction[17] of the Safety Criteria
- validation & verification of the safety objectives

❗	1. *System-generated hazards* are those that are associated with potential failures modes of the system itself 2. At the core of the task related to those system-generated hazards is the **FHA process**, carried out on a representation of the system under consideration at the level of the operational service.

[17] This would require in particular both the identification of appropriate safety validation objectives as well as the use of the SEV and RCS Schemes as promulgated by the companion Guidance Material.

For each system-generated hazard, there is a need to provide:

- the assessed immediate operational effect(s)
- the possible mitigations in terms of defences to be implemented to protect against the risk-bearing hazards
- the assessed severity of the mitigated effect(s), in accordance with the severity scheme in **Reference 2, Guidance E**
- safety objective (from the failure approach, *i.e. integrity safety property*) in accordance with **Reference 2, Guidance E**, in order to limit the tolerable frequency with which the system-generated 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 **Reference 2**, **section A.2** hereto

For the system-generated hazards, a good starting point for deriving the failure scenarios is 'negating' the Safety Objectives derived with the success approach – *i.e.* asking what if Safety Objective #nn is not achieved.

1. For guidance on the relevant Risk Classification Scheme (RCS) and Hazard Severity Classification Scheme to be used to generate safety objectives (failure approach), go to **Reference 2, Guidance E**

2. Further details of the FHA are given in the SAM (see **Reference 4**)

3. P16.06.01 has developed a Safety Assessment Report (SAR) Template (see **Reference 8**) to record the results of the safety assessment processes described in **sections 6**, **7**, and **8**. This Template is available on the SJU Extranet at https://extranet.sesarju.eu/Programme%20Library/Forms/Templates.aspx.

As appropriate[18], the Safety Assessment Report (SAR) and OSED shall include:

- a list of the key properties of the Operational Environment (or User Domain) that could have an effect on safety
- the SAfety Criteria, which cover both pre-existing and system-generated risk, and the justification for their selection
- 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 system, at the level of the operational services

and 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.

[18] What is 'appropriate' is given by the execution of the change assessment as part of the Safety Scoping and Change assessment process described in **Reference 2, section C** hereto.

7 Application of the SRM: what it delivers to the Solution SPR

Safety requirements, being properties of the design, 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 SPR-level system design. The SESAR SRM also requires the 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 system under consideration, and both the success and failure approaches.

The safety assurance activities, at the SPR level are (details of the planned safety assurance activities are provided in **Reference 2, Guidance A.3** hereto):

- description of the SPR level model of the Solution system
- derivation, from the Safety Objectives (*Functionality and Performance* from the success approach) of Safety Requirements for the SPR-level design
- analysis of the operation of the SPR-level design under normal conditions of the Operational Environment
- analysis of the operation of the SPR-level design under abnormal conditions of the Operational Environment
- assessment of the adequacy of the SPR-level design in the case of internal failures and mitigation of the system-generated hazards
- satisfaction of Safety Criteria by the SPR-level design
- realism of the SPR-level design (it is necessary at this stage to show, not only that the Safety Requirements are sufficient to ensure safety but also that these Safety Requirements are achievable (this includes feasibility in terms of timescale, cost, technical development).
- verification of the safety requirements

1. At the core of the task related to the 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 integrity[19] derived in the FHA.

2. To fully address the needs of the broader approach SAM should be read in conjunction with the following text and **Reference 2**, **section A.3** hereto.

Details of the PSSA are given in the SAM (see **Reference 4**).

As appropriate (see footnote **18**), the SAR and SPR shall include:

- The safety requirements (*functionality and performance properties* from the success approach) that are necessary to satisfy the operational services specification
- The static and dynamic analysis to show that the SPR-level design will

[19] 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.

	deliver this functionality and performance under all normal and abnormal 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 SPR-level design will deliver this functionality and performance under all abnormal conditions of the operation environment that the system may exceptionally encounter • The evidence that the SPR-level design is robust against (i.e. work through), or at least resilient to any varying conditions of the operational environment • The safety requirements (*integrity property* from the failure approach) that are necessary to satisfy the operational service-level specification. • The evidence that safety requirements are capable of being satisfied in a typical implementation • The evidence that safety requirements are verifiable (*i.e.* verify that the safety properties are satisfied in practice) and presents the assurance that these outputs are complete and correct.

8 Application of the SRM: what it delivers to the TSs and refined version of the SPR

Implementation (Physical level) covers the detailed design, construction and test of the physical system, in a conventional manner.

	The detailed design and building and evaluation of the physical Solution system are only partly addressed since V3 deals with pre-industrialization prototypes only. In particular, while the specification of a detailed set of safety requirements for the physical system design can be obtained, the requirements-satisfaction process (i.e. proving system functionality and performance and proving system integrity) could only be partly done at best.

The safety assurance activities, at the Physical level are (details of the planned safety assurance activities are provided in **Reference 2, Guidance A.4** hereto) as far as practicable:

- definition of the set of safety requirements (*functionality and performance* from the success approach) for the physical design that satisfy the safety requirements (*functionality and performance* properties) that were derived at the SPR level.
- definition of the failure-rate targets for the hardware components and required reliability for the software elements of the Technical System (e.g. with the setting of a Software Assurance Level) that are sufficient to satisfy the related Safety Requirements (*integrity* property from the failure approach) of the SPR-level model.
- Looking for emergent properties of the design that may not be revealed by top-down (deductive) techniques such as Fault Tree Analysis.
- justification of the technical system design options
- definition of:
    - the ATC/flight crew procedure requirements
    - the controller competence requirements
    - Engineering procedure / training requirements (incl. maintenance aspects)

- assurance that safety-related and non-safety functions[20] are segregated adequately
- assessment of the consequence of deliberately or inadvertently allowing a margin of functional or performance variability in the specification of technical systems and / or human tasks
- assurance that these outputs are complete and correct.

1. At the core of this phase is a **part 1 of the SSA process** (SSA1). This first stage is the specification of a set of detailed Safety Requirements for the physical system design. The detailed Safety Requirements are obtained by allocating the Safety Requirements for SPR level design (derived as above) on to the physical architecture (see section **3.2.3** related to TS).

2. To fully address the needs of the broader approach, SAM should be read in conjunction with the following text and **Reference 2**, **section A.4** hereto.

Details of the SSA are given in the SAM (see **Reference 4**).

As appropriate (see footnote **18**), the SAR, TSs and SPR (with respect to human tasks level only) shall include:

- The set of safety requirements (success approach) for the physical design that satisfy the Safety Requirements (success approach) that were derived for the SPR level design.
- Failure-rate targets for the hardware components and required reliability for the software elements of the Technical System (e.g. with the setting of a Software Assurance Level) that are sufficient to satisfy the related Safety Requirements (integrity property) of the SPR level design.
- The justification of the technical system design options
- The ATC/flight crew procedure requirements
- The controller competence requirements (related to controller training, controller licensing, controller selection & management)
- Engineering procedure / training requirements (incl. maintenance aspects)
- The evidence to show that safety-related and non-safety functions are segregated adequately
- The consequence or deliberately or inadvertently allowing a margin of functional or performance variability in the specification of technical systems and / or human tasks

and presents the assurance that these outputs are complete and correct.

[20] Those functions making no direct or even indirect contribution to aviation safety. Examples are business support functions (route charges, statistics collection generally).

9 Application of the SRM: Safety Management of VLD

9.1 Objectives of a VLD

A Very Large Demonstration (VLD) aims at assessing the benefits of a SESAR solution, but as the title suggests, on a broad and almost industrialised scale i.e. post V3, V4 and demonstrating that V5 is attainable. It is worth noting that meeting this high level objective implies that the VLD is run in a scientifically controlled way with a true reference for comparison with the 'with-Solution' case.

It aims at serving as a Proof of Concept (PoC) for an existing ATM functionality as per (EU) No 716/2014 of 27 June 2014 (on the establishment of the Pilot Common Project (PCP) supporting the implementation of the European Air Traffic Management Master Plan) or a future ATM functionality within a forthcoming Common Project (CP) Commission Implementing Regulation (IR).

The 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 (e.g. ACAS-X as part of SESAR.IR-VLD.Wave1-15-2015), a VLD aims at providing inputs and influencing the work at global and regional standardisation level, within ICAO, EUROCAE and/or RTCA.

In relation to V-cycles stages and associated Technical Readiness Levels (TRLs), this is demonstrated in **Figure 5** below:

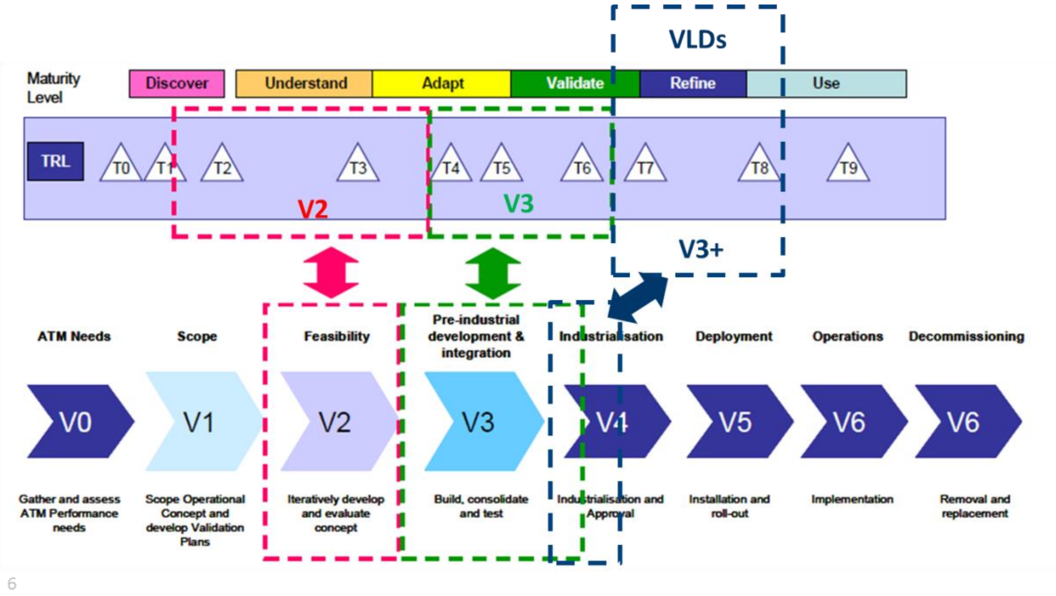

VLDs
Maturity Level
Discover
Understand
Adapt
Validate
Refine
Use
TRL
T0
T1
T2
T3
T4
T5
T6
T7
T8
T9
V2
V3
V3+
ATM Needs
Scope
Feasibility
Pre-industrial development & integration
Industrialisation
Deployment
Operations
Decommissioning
V0
V1
V2
V3
V4
V5
V6
V6
Gather and assess ATM Performance needs
Scope Operational Concept and develop Validation Plans
Iteratively develop and evaluate concept
Build, consolidate and test
Industrialisation and Approval
Installation and roll-out
Implementation
Removal and replacement
6

Figure 5: E-OCVM Vs, TRLs and VLDs (source SJU)

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 onboard) to support the demonstration in the targeted operational environment involving target audience end-users. This also requires proper System Engineering (SE) data management for a solution to ensure that both:

- proper coverage (incl. operational concept, SESAR solution vs. OI steps & Enablers, traffic expectations, equipage level); and
- traceability matrixes between (i) operational & performance requirements vs. technical requirements; and (ii) validation objectives vs. operational & performance requirements; (iii) etc.

are available to support the content integration work. Finally a PoC needs to provide the evidence (SE data and deliverables) with the sufficient quality to guarantee their usability and significance for the SESAR Community, including for eventual deployment.

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, 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 material generated by the SRM process and the SRM per se (see sections **9.2** and **9.3** below as well as **Guidance M** in Reference **2**) provide practical guidelines to assist.

9.2 Scope of safety assurance of and *wrt* a VLD

The activities are twofold and relate to:

i. The non-interference of the VLD with other surrounding operations and components of the ATM/ANS System; and
ii. The suitability of the Solution(s) for the required application/operation.

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 (see figure above). 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. Determining and documenting in a VLD safety Plan the safety assurance needs for the VLD per se;
3. Documenting the VLD Safety Case. The VLD Safety Case is here a means of structuring and documenting a summary of the results of a VLD Safety Assessment in a way that a reader can readily follow the logical reasoning as to why the VLD can be considered safe. It follows that the VLD Safety Case will serve both the primary purpose of ensuring that those participant service providers who are accountable for safety discharge their safety responsibilities properly and also provide an adequate level of safety assurance to obtain the necessary regulatory approval;
4. Enabling the use of VLDs as a new dimension in the validation approach and providing further evidence as a support to standardization. This includes, but is not limited to, (i) building and evaluating the physical Solution System against that detailed 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 onboard) to support the demonstration of the achievement / achievability of the safety validation objectives and higher-level safety requirements; and, finally;
5. Enabling significant levels of engagement and co-ordination of both the end-users (e.g. ANSPs, Network Manager, airports; airspace users, AOC; etc.) and appropriate regulatory authorities (National Authorities (NAAs; NSAs) and/or EASA) as fully detailed in reference **17**.

9.3 Safety assurance of and wrt a VLD

Each ANSP has approved safety assurance processes and procedures for the implementation of changes that are in accordance with the common requirements (1034/2011 and 1035/2011) 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 required to be followed when the NSA advises that they wish to review a planned safety related change, in that case a VLD.

With this in mind, **Guidance M** in reference **2** 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 M** in conjunction with reference **17**.

Guidance M seeks neither to replace local processes nor replicate reference **17**, 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 NSA and/or EASA.

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

10 The SESAR Safety Register

One of the challenges in doing safety assessments for the Solutions is managing the large amount of information involved, in such a way that the Evidence produced is complete, correct, consistent, sufficient and traceable to satisfy the Safety Argument for a package of Solutions.

This is facilitated by informing and maintaining a **Safety Register** throughout the life of the project in order to:

- provide an access to the various set of safety requirements (incl. SAC, SO, SR, etc.) with proper relationships to the elements of the System Architecture (e.g. ATM services); and
- track progress and provide visibility of the status of the various safety assurance objectives and activities for each phase of the lifecycle and for all relevant OIs within a specific Solution and for all relevant Solutions for a specific package.

The Safety Register has to be informed and maintained by the Solution and is accessible at:

https://remedyweb.eurocontrol.fr/arsys/shared/login.jsp?/arsys/forms/remedy/SESAR+WP16+-+Safety+Register

11 Document Information

11.1 References

The following documents are referenced within the document:

1. P16.06.01, SESAR Safety Approach, Ed05.00.00, approved at SESAR PC#29 on 14/10/2014 (can be found on the SJU Extranet (16.06.01 – Execution - T002 Directory))

2. P16.06.01, Guidance to Apply the SESAR Safety Reference Material, Ed03.00, April 2016 (can be found on the SJU Extranet (16.06.01 – Execution - T006 Directory))

3. SJU, SESAR 2020 Programme Execution Framework - Project Hand-Book, May 2016 (can be found on the SJU Extranet)

4. EUROCONTROL, 2007, Air Navigation System Safety Assessment Methodology (SAM), SAF.ET1.ST03.1000-MAN-01, Edition 2.1

5. EUROCONTROL, 2010, Safety Assessment Made Easier, Part 1, Safety Principles and Introduction to Safety Assessment, Ed1.0 released issue
6. EC, EP3, D2.4.3-01, 2008, White Paper on the SESAR Safety Target, http://www.episode3.aero/public-documents
7. P16.06.01, Solution Safety Plan Template, Edition 00.03.00, May 2016 (can be found on the SJU Extranet)
8. P16.06.01, Solution Safety Assessment Report Template, Edition 00.03.00, May 2016 (can be found on the SJU Extranet)
9. EC/EUROCONTROL, E-OCVM Version 3.0 Volume I, February 2010
10. P16.01.01, Accident Incident Models in MS Visio and Isograph Fault Tree + format, March 2013
11. P16.01.01, Validation / Verification of the SESAR Accident Incident Model (AIM), Edition 00.01.00, May 2014
12. P16.06.05, HP Reference Material, Edition 00.03.00, March 2016
13. P16.01.01b, Final Resilience Guidance Material for Safety Assessment (SRM) and Design, Edition 00.01.00, May 2016
14. EUROCONTROL, 2013, White Paper, 'From Safety-I to Safety-II.
15. P16.06.01, Safety argument template for SESAR Operational Packages, Edition 00.01.02, Feb 2012
16. (EU) No 1035/2011 of 17 October 2011 laying down common requirements for the provision of air navigation services and amending Regulations (EC) No 482/2008 and (EU) No 691/2010
17. SESAR P16.01.04, Final Guidance Material to Execute Proof of Concept, Ed00.04.00, August 2015

11.2 Acronyms

AIM	:	Accident Incident Model
ANS	:	Air Navigation Services
ANSP	:	Air Navigation Service Provider
ATC	:	Air Traffic Control
ATM	:	Air Traffic Management
BM	:	Barrier Model
DOD	:	Detailed Operational Description
EASA	:	European Aviation Safety Agency
EATMA	:	European Air Traffic Management Architecture
EC	:	European Commission
ECAC	:	European Civil Aviation Conference
EP3	:	EC Funded Episode 3 project
FHA	:	Functional Hazard Assessment

FM	:	Functional Model
FOC	:	Final Operating Capability
FTS	:	Fast-Time Simulation
HF	:	Human Factors
HP	:	Human Performance
INTEROP	:	Interoperability requirements
IOC	:	Initial Operating Capability
IRV	:	Industrial Research & Validation
JU	:	Joint Undertaking
KPA	:	Key Performance Area
KPI	:	Key Performance Indicator
NAA	:	National Aviation Authority
NSA	:	National Supervisory Authority
OCVM	:	Operational Concept Validation Methodology
OI	:	Operational Improvement
OSED	:	Operational Service & Environment Description
PCIT	:	Project Content Integration Team
PMS	:	Point Merge System
PoC	:	Proof of Concept
PRNAV	:	Precision-Area Navigation
PSSA	:	Preliminary System Safety Assessment
RCS	:	Risk Classification Scheme
RE	:	Resilience Engineering
RTS	:	Real-Time Simulation
SAC	:	SAfety Criteria
SAM	:	Safety Assessment Methodology
SAME	:	Safety Assessment Made Easier
SAR	:	Safety Assessment Report

SATF	:	Safety Assessment Task Force
SE	:	System Engineering
SES	:	Single European Sky
SESAR	:	Single European Sky ATM Research programme
SEV	:	Severity
SJU	:	SESAR JU
SME	:	Subject Matters Expert
SO	:	Safety Objective
SPR	:	Safety & Performance Requirements
SR	:	Safety Requirements
SRM	:	Safety Reference Material
SSA	:	System Safety Assessment
SWAL	:	SoftWare Assurance Level
TA	:	Transversal Area
TMA	:	Terminal Manoeuvring Area
TRL	:	Technical Readiness Level
TS	:	Technical Specification
VALP	:	Validation Plan
VLD	:	Very Large Demonstration
WP	:	Work Package
WX	:	Weather

11.3 Definitions

The following definitions shall apply:

a. ‘Abnormal conditions’ are those external changes in the operational environment that the ATM/ANS functional system may exceptionally encounter (e.g. severe WX, airport closure, etc.) under which 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’ 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’ 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 – from Article 2(10) of Regulation (EC) No 1035/2011;

> In Regulation (EC) No 1035/2011, the following definition currently applies: “’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”.

g. ‘ATM/ANS’ shall mean the air traffic management functions as defined in Article 2(10) of Regulation (EC) No 549/2004, air navigation services defined in Article 2(4) of that Regulation, and services consisting in the origination and processing of data and formatting and delivering data to general air traffic for the purpose of safety-critical air navigation – as defined in Article 3(q) of Regulation (EC) No 216/2008;

h. ‘Certification’ shall mean any form of recognition that a product, part or appliance, organisation or person complies with the applicable requirements including the provisions of Regulation (EC) No 216/2008 and its implementing rules, as well as the issuance of the relevant certificate attesting such compliance – as defined in Article 3(q) of Regulation (EC) No 216/2008;

i. ‘Degraded mode of operation’ is a pre-defined reduced level of operational service invoked by equipment outage or malfunction, staff shortage or procedures.

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. ‘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;

l. ‘Functional Model (FM)’ shall mean an abstract representation of the design of the ATM/ANS functional system that is entirely independent of the design and of the eventual physical Implementation of the system. The FM describes what safety-related functions are performed and the data that is used by, and produced by, those safety functions – it does not show who or what performs the safety functions.

m. ‘Functional system’ shall mean a combination of equipment, procedures and human resources organised to perform a function within the context of air navigation services – from Article 2(3) of Regulation (EC) No 1035/2011;

> Definition in Regulation (EC) No 1035/2011 expanded to address air navigation services. Indeed, currently in Regulation (EC) No 1035/2011, the following definition applies: “‘functional system’ means a combination of systems, procedures and human resources organised to perform a function within the context of ATM”.

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 introduced by 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, which are created by failure of the ATM/ANS functional system.

Currently, in Regulation (EC) No 1035/2011, the following definition applies: "'hazard' means any condition, event, or circumstance which could induce an accident".

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 un-commanded 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. 'OSED level' is used herein as the highest level at which the safety properties of the ATM system are specified – see 'Specification' below.

s. 'OSED level 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.

t. '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;

u. 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";

v. '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;

w. 'Primary Project (PP)' shall mean a 3-digit project within the SESAR WP4 to 15;

x. 'Process' shall mean a set of interrelated or interacting activities which transform inputs into outputs;

y. '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;

z. 'Reliability' shall mean the ability of a system / element to perform a given function within a certain period of time without failure.

aa. '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.

bb. '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 Article 2(9) of Regulation (EC) No 1035/2011;

cc. '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;

dd. 'Safety Assessment' as per the SRM coverage (lifecycle) means an *a priori* risk assessment and mitigation of changes to the ATM/ANS functional system

ee. '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 – from Article 2(10) of Regulation (EC) No 1035/2011;

ff. 'Safety assurance objective' shall mean a goal (or similar) that has to be achieved in order to satisfy a higher-level safety Argument.

gg. '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;

hh. 'Safety objective' shall mean the functional, performance and integrity safety properties of the air navigation system, derived at the OSED 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 – from Article 2(11) of Regulation (EC) No 1035/2011;

> This definition relates to the 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.
>
> Currently, in Regulation (EC) No 1035/2011, the following definition applies: "'safety objective' means a qualitative or quantitative statement that defines the maximum frequency or probability at which a hazard can be expected to occur"

ii. '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;

jj. 'Safety requirement' shall mean the necessary risk reduction measures identified in the risk assessment to achieve a particular safety objective. They describe the functional, performance and integrity safety properties at the system-design level as well as organisational, operational, procedural, and interoperability requirements or environmental characteristics – from Article 2(12) of Regulation (EC) No 1035/2011;

> Currently, in Regulation (EC) No 1035/2011, the following definition applies: "'safety requirement' means a risk-mitigation means, defined from the risk-mitigation strategy that achieves a particular safety objective, including organisational, operational, procedural, functional, performance, and interoperability requirements or environment characteristics"

kk. 'Specification' shall mean what the ATM system has to provide across the interface between the service provider and service user in order that the User Requirements can be satisfied – *i.e.* a specification takes a "black-box" view of the system, at the OSED level

ll. SPR-level 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. The SPR-level 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 SPR-level 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.

mm. ‘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.

nn. ‘User Requirements’: User(s) in this context are the user(s) of the air navigation service(s) concerned. In general, User Requirements are what the Users want to have happen in their domain of operation. From a safety viewpoint, the User Requirements are generally the SAfety Criteria.

oo. ‘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)

pp. ‘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.

Guidance to Apply the SESAR Safety Reference Material

Document information	
Project title	Safety support and coordination function
Project Number	16.06.01
Project Manager	EUROCONTROL
Deliverable Name	Guidance to Apply the SESAR Safety Reference Material
Deliverable ID	D27
Edition	00.03.00
Template Version	03.00.00
Task contributors	
EUROCONTROL, AIRBUS, DFS, DSNA, ENAIRE, FREQUENTIS, INDRA, NATS, NORACON, SELEX, THALES	

Please complete the advanced properties of the document

Abstract

The purpose of this document is to provide detailed guidance on how to implement the SESAR safety assessment approach defined in the SESAR Safety Reference Material (SRM). This document intends to illustrate the meaning of safety assurance requirements from the SRM and should be used to support the deployment of the safety process as further detailed in Guidance A herein. This does not prevent alternative tools and techniques from being used by safety practitioners.

Authoring & Approval

Prepared By - Authors of the document.		
Name & Company	Position & Title	Date
Eric Perrin, EUROCONTROL	Project Manager / Content coordinator	25/03/2016
Juan Jesús Cano Quiñones, ENAIRE	Contributor	25/03/2016
Miguel Capote, ENAIRE (INECO)	Contributor	25/03/2016
Joelle Monso, AIRBUS	Contributor	25/03/2016
Viktoria Weigel, DFS	Contributor	25/03/2016
Yann CARLIER	Contributor	25/03/2016
Cécile MOURA, DSNA	Contributor	25/03/2016
Marta Llobet, EUROCONTROL	Contributor	25/03/2016
Bruno Rabiller, EUROCONTROL	Contributor	25/03/2016
Werner Winkelbauer, FREQUENTIS	Contributor	25/03/2016
Santoyo Pastor, Luis Víctor, INDRA	Contributor	25/03/2016
Sam Espig, NATS	Contributor	25/03/2016
Craig Foster, NATS	Contributor	25/03/2016
Massimo Capuano, SELEX	Contributor	25/03/2016
Bernard Pauly, THALES	Contributor	25/03/2016

Reviewed By - Reviewers internal to the project.		
Name & Company	Position & Title	Date
Jesus Romero Hernandez, ENAIRE	Contributor	11/04/2016
Joelle Monso, AIRBUS	Contributor	11/04/2016
Diana Durrett, DFS	Contributor	11/04/2016
Hans de Jong, DFS	Contributor	11/04/2016
Viktoria Weigel, DFS	Contributor	11/04/2016
Karim Mehadhebi, DSNA	Contributor	11/04/2016
Gabriele Schedl, FREQUENTIS	Contributor	11/04/2016
Werner Winkelbauer, FREQUENTIS	Contributor	25/03/2016
Amada Bernáldez de Aranzábal, INDRA	Contributor	11/04/2016
Sam Espig, NATS	Contributor	11/04/2016
Craig Foster, NATS	Contributor	11/04/2016
Bill Becton, NORACON	Contributor	11/04/2016
Lilla Hartyani, NORACON	Contributor	11/04/2016
Matthieu BRANLAT, SINTEF	Contributor	11/04/2016
Fateh KAAKAI, THALES	Contributor	11/04/2016

Reviewed By - Other SESAR projects, Airspace Users, staff association, military, Industrial Support, other organisations.		
Name & Company	Position & Title	Date
Andrew Kilner, EUROCONTROL	16.06.05 Project Manager	18/04/2016
Peter Martin, EUROCONTROL	SWP16.06 Manager -	18/04/2016

Approved for submission to the SJU By - Representatives of the company involved in the project.		
Name & Company	Position & Title	Date

Rejected By - Representatives of the company involved in the project.		
Name & Company	Position & Title	Date

Rational for rejection
None.

Document History

Edition	Date	Status	Author	Justification
00.00.01	25/10/2011	Draft	Eric Perrin	Creation
00.01.00	15/12/2011	Revised Draft	Eric Perrin	Responses to key comments and submission to SJU for review
00.01.01	30/01/2012	Final	Eric Perrin	Update to take into account SJU comments and proposed issue.
00.01.02	10/02/2012	Final	Eric Perrin	Update following formal review by the SJU
00.01.03	05/05/2014	Final - proposed	Eric Perrin	Update following review by National Authorities and EASA as well as capturing inputs from P16.01.02.
00.02.00	12/12/2014	Final	Eric Perrin	Released version following 16.06.01 review and capturing inputs from P16.01.03
00.02.01	09/03/2015	Final	Eric Perrin	Usage of latest version of the template following SJU review
00.02.02	05/04/2016	Final for review	Eric Perrin	Updates to transition to SESAR 2020
00.03.00	09/05/2016	Final	Eric Perrin	Including feedback from 16.06.01 review

Intellectual Property Rights (foreground)

This deliverable consists of SJU foreground.

Table of Contents

List of Figures

List of Tables

Executive summary

The purpose of this document is to provide practical guidance to support the safety assessment activities as defined in the SESAR Safety Reference Material (SRM). This document should be used in conjunction with the SRM.

The detailed safety assurance activities are shown in **Table 1** to **Table 4** in **Guidance A.1** to **A.4**. The Safety Assurance Activities are guide only and are intended to be neither prescriptive nor exhaustive. They would need to be revised for specific SESAR Solutions as per the Scoping and Change Assessment process detailed in **Guidance C**.

It should be noted that information necessary for many of the Safety Assurance Activities described in this section might already be available as part of the normal operational, project-management and /or systems-engineering processes. Where possible maximum use should be made of such information subject to it being possible, to show sufficient confidence in its completeness and correctness, for safety purposes. Such information includes but is not limited to:

- *In the Solutions' OSEDs: (i) operational environment; (ii) existing (baseline) ATM/ANS / functional system; (iii) how the change under consideration changes the ATM/ANS / functional system; (iv) normal and abnormal conditions; and (v) Operational scenarios*
- *In the Solutions OSEDs / SPR's: required functionality & performance of the ATM/ANS / functional system*
- *In the Solutions TS's: system requirements*
- *From PJ19.3, TA Register of TA Data recording data including project assumptions, assessment baselines, benefit mechanisms, TA case objectives/ requirements/ caveats/ open issues*
- *From the System Engineering tools:*
  - *Enterprise Architecture Models i.e. a set of consistent "views" labelled "performance", "business", "service" etc. of a database comprising the docs/records detailing and organising the SESAR concept and its artefacts;*
  - *Requirements data describing operational and system requirements with traceability, also incl. performance and TA requirements;*
  - *Validation & Verification data containing the summary results of V&V objectives, evidence and status (though not the detailed results);*
  - *Etc.*

Such Safety Assurance Activities have their reference numbers annotated thus"*", in the assurance Tables Guidance A.1 to **A.4 below.**

Initial Guidance included in these Tables in **Guidance A.1** to **A.4** is expanded in further Guidance as referenced from the appropriate parts of the Tables.

Finally, this document provides, for further reading:

- The rigorous logic applied to derive the safety assurance activities which produce the required evidence in **For further reading 1**; and

Safety practitioners should contact the SESAR 2020 PJ19.3 project when conducting safety assessments in accordance with this document. Please contact the PJ19.3 Helpdesk through extranet@sesarju.eu for help in applying this guidance.

Safety Plan and Safety Assessment Report Templates are available on the SESAR Programme Library.

Guidance A On Detailed Safety Assurance Activities, Tools & Techniques

Forewords:

1. **Table 1** to **Table 4** include, for completeness and traceability only, cross references to the set of Principles (*P_x*) and Safety Assurance Objectives (*AO_y*) defined in section **For further reading 1**. **For further reading 1** provides background information and rationale on the list of Principles, Safety Assurace Objectives and Safety Assurance Activities.

Projects should concentrate on safety assurance activities (*a_z*) that are grouped under the various types of formal deliverables i.e. Validation Plan, OSED, SPR and TS respectively.

2. Safety Assurance Activities involving information that might already be available as **part of the normal operational, project-management and /or systems-engineering processes** have their reference numbers **annotated " * "** , in the assurance **Tables Guidance A.1** to **A.4** below.

A.1 Detailed safety assurance activities to inform the Validation Plan (*i.e.* Solution Safety Plan as an Annex to the VAL Plan)

Ref			Scoping & initial Change Assessment	Guidance and Proposed Tools & Techniques
P1	**AO1**	**a1***	Describe what the Solution is seeking to achieve (e.g. understand the operational concept, benefits delivered in capacity, efficiency and/or safety, Implementation strategy)	Items #1 to #6 in **Guidance C** on "scoping the safety assessment and change assessment". This shall be done in coordination with PJ19.3.
P1	**AO2 & AO3**	**a1**	Perform an initial assessment of the safety implications of the Solution: ▪ Baseline for the change assessment ▪ Operational Environment for the change (incl. Identify other parts of the ATM/ANS operations that will be affected) ▪ Details of the change ▪ Depth and breadth of the change ▪ Need for new or modified Regulations	Item #7 in **Guidance C** Item #8 in **Guidance C** Item #9 in **Guidance C** Item #10 in **Guidance C** Item #11 in **Guidance C** Step 1 of the Resilience Engineering method described in **Guidance I** supports the development of an initial understanding of the work-as-done in the current operations and of the way that future ATM operations are expected to be done.
P2		**a1**	Define the safety strategy in addressing the change through: ▪ Identification of the pre-existing hazards and	Item #12 in **Guidance C**. By definition, these hazards exist in the operational

Ref			Scoping & initial Change Assessment	Guidance and Proposed Tools & Techniques
			risks that fall within the scope of the safety assessment (i.e. the pre-existing hazards and risks that ATM/ANS is intended to mitigate)	environment before any form of ATM de-confliction has taken place. It is therefore the primary purpose of the relevant Solution operational services to mitigate (some of) them). See Guidance **F.2.2**.
			▪ Definition and justification of appropriate SAfety Criteria, according to the scope of the safety assessment (i.e. what is “safe” in the context of the Solution and, in broad terms, the strategy for demonstrating safety) and incl. the usage of field data	Item # 13 in **Guidance C**. Eventually, the SAC will be used to set measurable and quantifiable safety performance objectives. It is recommended to include the SAC into the Safety Register maintained by PJ19.3. General description of the Safety Register is given in **Guidance H** *Note: In case the subsequent analysis carried out at OSED and SPR-level (as described in **Guidance A.2** and **A.3**below) shows that a SAC needs to be modified or a new SAC is identified, that would require an iteration for updating the list of SAC with the subsequent cascading effect on the OSED and SPR levels in terms of safety objectives and safety requirements.*
			▪ Definition of the safety assurance activities, safety deliverables, accountability and responsibility	Items #14, 15 & 16 in **Guidance C** The results of activities within this Guidance A.1 will allow to issue a Safety Plan (in accordance with SAF PLN template) aimed at specifying the safety assurance activities to be carried out by the Solution, whilst recording the relevant safety assessment information available at this initial stage (to be further used as input to the Safety Assessment Report).

Table 1: Detailed safety assurance activities to inform the Validation Plan

A.2 Detailed safety assurance activities to inform the OSED

Ref			Operational Level Safety Assurance Activities	Guidance and Proposed Tools & Techniques
P3P4	**AO1**	**a1***	Identify and describe the Solution ATM/ANS services aiming at mitigating the risks associated to the pre-existing hazards defined in P2_a1.	These services are not necessarily specific to the change brought by the Solution. The delivery of the operational services and sub-services (if relevant) are mapped onto the Accident Incident Model (AIM) barriers (ATM layers) - see Guidance **G.1.1** (**F.2.4**). Another source of information for the identification of the services is the European ATM Architecture. (https://www.atmmasterplan.eu/architecture/views/).
P3P4	**AO1**	**a2***	Define the safety objectives (functionality and performance – related to the ‘success’ approach) specifying the above ATM/ANS services. Safety objectives are defined in order to mitigate the pre-existing risks under normal operations, i.e. those conditions that are expected to occur on a day-to-day	The definition of the safety objectives can be achieved by considering the full range of possible operational scenarios / use cases as defined in the OSED. Further guidance on this is provided in **Guidance F**. It is required to check the completeness of the list of operational scenarios / use

Ref			Operational Level Safety Assurance Activities	Guidance and Proposed Tools & Techniques
			basis.	cases by describing the relevant phases of a typical normal flight as a continuous process and addressing in particular the transition modes (if relevant, e.g. inputs/outputs, separation responsibilities, etc.). In case new operational scenarios / use cases are identified, define additional safety objectives. In particular attention should be paid to additional operational scenarios / use cases related to variations in key OE conditions as identified with the 'Scoping and Change assessment' process (**Guidance C**). Step 2 of the RE Method described in **Guidance I** supports the identification of the varying conditions, inherent in complex systems such as ATM, which the new design will need to handle.. To assess the impacts of the Solution operations on adjacent airspace or on neighbouring ATM Systems, check the changes in the Operational Environment to host the Solution operations and derive any required additional safety objectives (functionality and performance) for compatibility (e.g. Service Level Agreement (SLA)). *Note: In case the subsequent analysis carried on at SPR-level (as described in **Guidance A.3** below) identifies additional normal operational scenarios/use cases or another need for new or modified Safety Objectives (functionality and performance), that would require an iteration for updating the list of Safety Objectives.*
P3P4	**AO1**	**a3***	Identify external abnormal conditions, e.g. aircraft emergency, RWY closure / change, sudden change in WX conditions, severe WX, sudden activation of restricted airspace, low-performance aircraft, aircraft encounters TCAS RA, etc.	Abnormal conditions are those under which the system has to operate in a reversionary mode due to, for example: 1) Conditions of the operation environment that the system may exceptionally encounter 2) Equipment failures external to the ATM system concerned, 3) Maintenance interventions – out of scope for SESAR Development Phase Abnormal conditions are normally identified in the OSED but it is the role of this activity to ensure the completeness of those conditions as far as possible. In particular attention should be paid to additional operational scenarios / use cases related to variations in key OE conditions as identified with the 'Scoping and Change assessment' process (**Guidance C**). **Guidance I** provides additional techniques for identifying the varying conditions

Ref			Operational Level Safety Assurance Activities	Guidance and Proposed Tools & Techniques
				which may be expected in the operational environment
P3P4	AO1	a4*	For each abnormal condition identify existing/define new Safety Objectives (functionality and performance) specifying the above ATM/ANS services.	This is done by assessing the immediate operational safety effect, considering the mitigations provided through the Safety Objectives (functionality & performance) derived for normal conditions (as per P3P4_AO1_a2 above). If necessary, new Safety Objectives (dedicated to abnormal conditions) need to be derived. If, during this activity, detailed mitigating solutions (*i.e.* anticipating the SPR design level) are identified, they need to be captured as candidate Safety Requirements to be further confirmed at SPR level. Under an abnormal condition of the OE, the System may be allowed to enter a degraded state PROVIDED that it can easily be recovered when the abnormal condition passes. The specified SOs shall be sufficient for mitigating the safety risk associated to the abnormal condition occurrence and the subsequent recovery. Step 3 of the RE method in **Guidance I** supports the description of the strategies which operators may use to deal with the varying conditions in the current and future ATM operation. *Note: In case the subsequent analysis carried on at SPR-level (as described in **Guidance A.3** below) identifies additional abnormal conditions or another need for new or modified Safety Objectives (functionality and performance), that would require an iteration for updating the list of Safety Objectives.*
P3P4	AO2	a1	Identify Operational Hazards caused by failures internal to (i.e. generated by) the system	This is the application of the SAM FHA carried out at the OSED level. Alternatively, the Operational Hazard Assessment (OHA) process from ED-78A may be adapted for the purpose. The standard questions related to the SWITF/HAZOP/HAZID/etc. processes at an FHA workshop should be enriched considering the following: 1. The Resilience Engineering method described in **Guidance I** (in particular Step 2 on varying conditions) 2. questions from the HP Issue Analysis (see HP RM, Appendix E)
P3P4	AO2	a2	Assess the severity of the effects from each Operational Hazard, using the AIM-based Severity Classification Schemes. Since the severity classification approach considers the most probable effects from hazard occurrence, the efficiency of the forthcoming barriers must be captured as consequential (protective) mitigations (which accounts for the external mitigation means)	Guidance is provided in **Guidance E.3**.

Ref			Operational Level Safety Assurance Activities	Guidance and Proposed Tools & Techniques
P3P4	**AO2**	**a3**	Set Safety Objectives (failure approach) (expressed as the tolerable probability of occurrence of each Operational Hazard) driven by the AIM-based Risk Classification Schemes	Guidance is provided in **Guidance E.2** and **E.3.5**. If during the activities P3P4 AO2 a1 to a3, detailed mitigating solutions (*i.e.* anticipating the SPR design level) are identified, they need to be captured as candidate Safety Requirements to be further confirmed at SPR level (see Guidance **A.3**)
P3P4	**AO2**	**a4**	Verify that the Safety Objectives (both *functionality & performance properties* from the success approach as well as *efficiency of mitigation measures* for the failure approach) are complete and correct by reference to the SAfety Criteria by: ▪ Ensuring forward and backward traceability between SO to SAC ▪ Definition observable and measurable safety validation objectives in the VAL Plan ▪ Collection from the validation exercise (VAL Report) the required evidence with respect to the safety validation objectives and amend (or otherwise) the set of safety objectives.	The method used to derive safety performance targets in support to B4.1 is quickly summarized in Guidance **D.2** including the review done as part of the well-established B4.1 consultation process. How SAC are further defined on that basis is detailed in **Guidance D** per se. This is done by mapping the Safety Objectives (functionality and performance) for normal and abnormal conditions to the SAfety Criteria. *Note: there is here no need to ensure the traceability of the SO (integrity / reliability) to the SAC since this is implicitly achieved by using the AIM-based RCS schemes.* The Safety Objectives (functionality & performance derived for normal and abnormal conditions as well as mitigations measures for the failure approach), together with the information captured within the OSED Level Safety assurance activities, allow to refine and complement the safety-related Validation objectives and issues derived within the Scoping & Change assessment process (**Guidance A.1**). The subsequent analysis carried out at SPR-level (as described in **Guidance A.3** below) will allow to further refine and complement this set of safety-related Validation objectives and issues. Coordination with HP is here required in: ▪ ensuring a consistent set of validation objectives and associated success criteria (as per the VAL Plan Template); as well as ▪ analysing the evidence being collected against the validation objectives. For guidance on gaining safety insights from validation exercises, consider **Guidance L**.
P3P4	**AO3**	**a1**	Present directly, and/or by reference, all the assumptions on which the safety objectives depend.	Assumptions usually relate to matters outside of the direct control of the organisation responsible for the Safety Assessment but which are essential to the completeness and/or correctness of the safety assessment results. They may also be matters that have to be assumed in one stage of the lifecycle (e.g. in the OSED-level) until they are verified in a later stage (e.g. in the SPR or TS levels). Assumptions as they arise during the safety assessment will be captured as follows:

Ref			Operational Level Safety Assurance Activities	Guidance and Proposed Tools & Techniques
				• Description • Source (where and when raised) • Rationale / reason for the Assumption • How and when the Assumption was (or will be) validated – informed by varying conditions from resilience engineering (**Guidance I**).
P3P4	**AO4**	**a1**	Ensure that the OSED level safety assessment results correspond to the applicable Solution OSED version	Satisfaction of this objective requires maintaining consistency between the OSED level safety assessment results and the evolution of successive Solution/OSED versions. It is also recommended to include into the Safety Register maintained by PJ19.3 (**Guidance H)** the following information derived at OSED level: • Solution ATM/ANS services • Safety Objectives (functionality & performance for normal and abnormal conditions) • Operational Hazards • failure Safety Objectives (expressed as the tolerable probability of occurrence of each Operational Hazard) • Assumptions • Safety recommendations (encompassing candidate Safety Requirements) • Operational limitations • Safety Issues
P3P4	**AO5**	**a1**	Ensure that the OSED level safety assessment results are trustworthy	*Backing* evidence is obtained from the properties of the ***processes*** by which Direct Evidence (products) was obtained, and shows that those processes, tools and techniques, human resources etc. were appropriate, adequate and properly deployed. Evidence must be shown to be *trustworthy,* by demonstrating, *amongst other things*: • the suitability of the processes, tools and techniques etc. that are used to generate the evidence obtained from the safety assessment • the correct application of those processes, tools and techniques • the competence of the personnel applying those processes, tools and techniques.

Table 2: Detailed safety assurance activities to inform the OSED

A.3 Detailed safety assurance activities to inform the SPR

			SPR-level Safety Assurance Activities	Guidance and Proposed Tools and Techniques
In most of the cases in SESAR, a SPR-level model definition can be directly developed from the OSED-level specification (incl. Safety Objectives) as per P5P6_AO1_a4*. For those cases, P5P6_AO1_a1* to a3* can be skipped. P5P6_AO1_a1* to a3* are retained in the rows below for those rare, but possible situations, where an architectural design is not yet sufficiently mature at this stage of the lifecycle.				
P5P6	**AO1**	**a1***	Produce a Functional Model (FM) to deliver the OSED level specification under activity P3P4_AO1_a2* and 4* above. *For this activity, as well as P5P6-AO1-a2* & P5P6-AO1-a3* below, it is optional as to whether the Solution develops a functional model or goes straight from the OSED level model (based on AIM) to the SPR-level model (highly dependent upon the type of Solution being considered).*	Even though P5P6_AO1 is made in the context of SPR-level Design, the first step in the process is development of a functional model of the ATM/ANS functional system. This is necessary because: • experience has shown that to get sufficient assurance of the completeness of the SPR-level design of the ATM system, with respect to the OSED level specification, it is necessary to bridge the two with a functional representation of the system, and • it is considered to be good system-engineering practice for deriving the requirements for a functionally rich system such as ATM/ANS. Guidance on functional model is given in **G.1.2** of **Guidance G**.
P5P6	**AO1**	**a2***	Describe how the FM is intended to operate	Describe with respect to normal operational scenario(s) as per the Concept of Operations and show that the FM is complete and internally coherent noting any issues that need to be addressed in the SPR-level Model. Consideration should be given to the work-as-done in the current operation as forming part of the baseline for the Functional Model (**Guidance I**). Show traceability between the FM and the Barrier Model. For relatively simple, or relatively unchanged FMs, a straight forward paper description and analysis may well suffice. For more complex, more critical systems, use of structured analysis techniques and tools may be required.
P5P6	**AO1**	**a3***	Derive safety requirements (*Functionality and performance properties* from the success approach) for the FM from the Safety Objectives (success approach) derived under Activity P3P4_AO1_a2* and 4* above.	Where the AIM Barriers Model is used to describe the OSED level, the safety objectives (success approach) are the probability of success of each Barrier
P5P6	**AO1**	**a4***	Produce a SPR-level model, to either interpret the FM described under Activities P5P6_AO1_a1* and a2* above or directly from the OSED-level specification (incl. Safety Objectives) in case there is an obvious architectural design.	Guidance on SPR-level Models is given in **G.2** of **Guidance G**. A Hierarchical Task Analysis (HTA), to be developed by HP experts (see HP Reference Material, chapter 3.4.6.4), should support the process of developing and explaining the SPR-level model. The HTA should be enriched by applying the resilience engineering principle 'work –as- done' (see **Guidance I**, Step 1).

			SPR-level Safety Assurance Activities	Guidance and Proposed Tools and Techniques
				Describe the components of the SPR-level model. Main human tasks, information exchange and interfaces with machine-based functions will be generated by the HTA.
P5P6	**AO1**	**a5***	Specify safety requirements (*functionality and performance properties* from the success approach) for each element of SPR-level model, including external elements as necessary	▪ For each scenario/used case (incl. those related to varying conditions, see **Guidance I** Step 2), describe how the elements of the SPR-level design (equipment functions, human tasks and data) combine to deliver the aspects of the air navigation services associated with the scenario Thread analysis (see **G.3** of **Guidance G**) is one of the recommended static techniques for this assurance activity. This analysis should consider Resilience Engineering (see **Guidance I**) which can support the description of work-as-done in the current operation and use this to inform the way that future ATM operations are expected to be done. Deliberate under-specification might sometimes be necessary in order to optimise the behaviour of the system – for example, allowing a human element of the system some discretion in when / how to execute a task according to his/her professional judgement and experience. On the other hand, <u>un</u>intentional under-specification can be a source of unwanted variability and coupling in the system that could be a source of system-generated risk. ▪ Where necessary (e.g. for the relevant sub-set of scenarios / use cases) check that the performance properties are complete, correct and mutually consistent by bringing into play dynamic risk modelling. Specific guidance on Dynamic Risk Modelling is given in **Guidance J** including a set of criteria to be used to decide on whether DRM is required to generate the evidence. ▪ Update/complement the existing list of safety requirements as necessary (**Guidance I** Step 4 provides guidance on how recommendations to strengthen the resilience of the future ATM operation can be derived.) **<u>In case, the project has not (yet) formalized requirements at SPR-level:</u>** A pre-requisite to the list of activities above is the following: ▪ For each Safety Objectives (Functionality and Performance) derived above, identify the participating SPR-level Model components in achieving the SO; their contribution is captured as safety requirements. ▪ Then proceed as per the list above. Where the external entities are pre-existing and fixed, and/or beyond managerial control / sphere of influence, then their safety properties may be assumed provided such Assumptions are shown to be valid.

			SPR-level Safety Assurance Activities	Guidance and Proposed Tools and Techniques
P5P6	**AO2**	**a1**	Check that the system design operates in a way that does not have a negative effect on the operation of related ground-based and airborne safety nets	For some cases, it may be possible to show that there is absolutely no coupling between the system under consideration and any ground-based or airborne safety nets – this would have to be demonstrated positively, not merely asserted!
P5P6	**AO3**	**a1***	Specify operational scenarios that are sufficient to fully describe the ***ab****normal* operational environment in which the ATM/ANS functional system will be required to operate	Each scenario should identify all the abnormal operational conditions / range of inputs that system might encounter exceptionally and under which 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 within the context of satisfying the SAfety Criteria – cf normal conditions under P5P6_AO2_a1 above. Check the scenarios against the OSED, if one is available.
P5P6	**AO3**	**a2**	For each scenario, assess the degree and extent to which the elements of the SPR-level design (equipment functions, human tasks and data) can continue to deliver the aspects of the air navigation service associated with the scenario	Thread analysis (see **G.3** of **Guidance G**) is the recommended technique for this Activity. Update the safety requirements (*functionality and performance properties* from the success approach) as necessary
P5P6	**AO3**	**a3**	Check that the system design operates in a way that does not have a negative effect on the operation of related ground-based and airborne safety nets	This is a follow-up to Assurance activity P5P6_AO2_a1 above. It requires confirmation that no modes of operation of the ATM/ANS functional system that could reduce the effectiveness of safety nets could be triggered by external abnormal events.
P5P6	**AO4**	**a1**	Where it is shown that the ATM/ANS functional system could not continue to operate as required, assess the risk associated with degradation in the system performance	This is a form of system-generated risk, albeit that the initiating cause is (by definition) external to the system in question. The risk assessment must take account of the likelihood that the abnormal events would occur in the first place.
P5P6	**AO4**	**a2**	Where the system could not continue to operate as required, describe the conditions and mechanisms for recovering the system to its full functionality and performance	Thread analysis (see **G.3** of **Guidance G**) and Resilience Engineering (see **Guidance I**) are the recommended techniques for this Activity Update the safety requirements (*functionality and performance properties* from the success approach) as necessary
P5P6	**AO5**	**a1**	Identify all potential causes of each hazard derived under Assurance objectives P3P4_AO1 and AO2_ above (deductive analysis)	This is the application of the SAM PSSA. This is a top-down (i.e. deductive), apportionment process and needs to be supplemented by Assurance activity P5P6_AO7_a1 below.
P5P6	**AO5**	**a2**	Specify Safety Requirements (*Integrity* property from the failure approach) and / or Assumptions for the causes of each hazard, such that the Safety Objectives (and/or SAfety Criteria) are satisfied,	This is the application of the SAM PSSA. This is a top-down (i.e. deductive), apportionment process and needs to be supplemented by Assurance activity P5P6_AO7_a1 below. Safety Requirements are always preferred to Assumptions. However, where the mitigations relate to items that we don't need to change (because they already

			SPR-level Safety Assurance Activities	Guidance and Proposed Tools and Techniques
			taking account of any internal mitigation means.	exist) or cannot change (because they lie outside our managerial control / sphere of influence) then capturing their safety properties as Assumptions would normally be acceptable provided evidence is presented to show that each Assumption is valid.
P5P6	**AO5**	**a3**	Capture all internal mitigations as either functional, performance or safety requirements (*integrity property* from the failure approach) or Assumptions, as appropriate	This is the application of the SAM PSSA. Safety requirements and assumptions shall be captured by the Solution team into the Safety Register (see **Guidance H**)
P5P6	**AO5**	**a4**	Check that the system can actually operate safely under, and recover from, all degraded modes of operation implicit in P5P6_AO5_a1.	**Guidance I** provides a method to examine variations in ATM System performance which may coincide and combine to generate unexpected conditions which the System can be expected to deal with. Step 3 of the RE method outlines an approach to identifying the strategies used by operators to adapt to these varying conditions. *This takes account of the fact that in many industries (including ATM) a disproportionate number of accidents seem to occur when the system concerned was in a degraded mode of operation immediately before the accident*.
P5P6	**AO5**	**a5**	Verify that the Safety Requirements (both *functionality & performance properties* from the success approach as well as *efficiency of mitigation measures* for the failure approach) are complete and correct by reference to the Safety Objectives by: ▪ Ensuring backward traceability between SR to SO ▪ For each scenario, identify those aspects / properties of the SPR-level design that it has not been possible to model in the above (static) analyses ▪ From those, define observable and measurable safety validation objectives in the VAL Plan ▪ Checking that the system design operates correctly in a dynamic sense, under all conditions (although only a subset of conditions can be modelled in RTS) ▪ Collection from the validation exercise (VAL Report) of the required evidence with	Fast-time and Real-time Simulations (FTS and RTS) are usually an effective way of achieving this objective. Where significant HF issues are involved, specific HF Lab techniques can be used to supplement the data from simulations (see **Guidance L**). ▪ Update/complement the existing list of safety requirements as necessary ▪ Human factors (see **Guidance K**) and timing properties issues are examples of issues that may require dynamic modelling (see **Guidance J**).

			SPR-level Safety Assurance Activities	Guidance and Proposed Tools and Techniques
			respect to the safety validation objectives and amend (or otherwise) the set of safety requirements.	
P5P6	**AO6**	**a1**	For the Functional Model (FM), show that the safety aspects of the design (safety functions and data sources / flows) cannot be interfered with by non-safety functions	No further guidance.
P5P6	**AO6**	**a2**	Show that the immunity provided in the FM is captured in the SPR-level model.	No further guidance.
P5P6	**AO7**	**a1**	Show that all other possible failure modes associated with the SPR-level design have been identified and mitigated such that Safety Objectives, derived under Assurance Objective P3P4_AO2 above are still met	This is a bottom-up (i.e. inductive) analysis process additional to Assurance activities P5P6_AO5_a1 and P5P6_AO5_a2 above. It is looking for emergent properties of the design that may not be revealed by top-down (deductive) techniques such as Fault Tree Analysis Some of the failure modes can be generated by seeding failed or incorrect functions / transactions in the scenarios / threads of Assurance activity P5P6_AO2_a2. Otherwise a Failure Modes Effects & Criticality Analysis (FMECA) – for more information see SAM Guidance, Part IV, Annex D
P5P6	**AO7**	**a2**	For the SPR-level model, show also that there are no emergent properties of the design that could allow non-safety functions to interfere with safety functions and data sources / flows	This can be done with: • a static perceptive using, for example, thread analysis – see G.3, the RE method – see **Guidance I,** and/or • a dynamic perceptive using, for example, real-time and fast-time simulations.
P5P6	**AO8**	**a1***	Describe the specimen physical design against which the realism of the Safety Requirements is to be demonstrated.	This is made in the context of a specimen physical design, comprising hardware, software, people and procedures that should be based on an appropriate, typical implementation of the SPR-level Design. This activity refers to a first sketch of a physical design.
P5P6	**AO8**	**a2**	Show that all Safety Requirements are capable of being satisfied in the physical system comprising hardware, software, people and procedures	*For Safety Requirements related to hardware and software, evidence could be obtained by analogy with known equipment for which similar Safety Requirements have already been satisfied or, where this is not available, by consulting the appropriate ATM/ANS equipment technical experts. *For the human tasks identified in the Safety Requirements, it would be appropriate to use some form of Tasks Analysis to show that the tasks are reasonable for the conditions under which they are expected to be performed and to use some form of Human Reliability Assessment to show that the integrity required of (or assumed for) each task is itself reasonable given the nature of the task and the conditions under which it is expected to be performed – see **Guidance K** and HP Reference Material (HPRM) **[Ref. 10]**

			SPR-level Safety Assurance Activities	Guidance and Proposed Tools and Techniques
				*For Safety Requirements related to procedures, evidence could be obtained by analogy with existing, proven procedures or, where this is not available, by consulting the appropriate operational experts
P5P6	**AO8**	**a3**	Show that all Assumptions that have been made in the Definition and Design & Validation phases, on which the Safety Requirements depend, are necessary and valid	See SAM Part IV Annex I – Safety Case Development Manual
P5P6	**AO9**	**a1**	Show that the satisfaction of all Safety Requirements in the physical system can be demonstrated with the appropriate degree of confidence	*Describe how satisfaction of hardware Safety Requirements will be demonstrated – e.g. system testing, reliability-demonstration etc. *Describe how satisfaction of software Safety Requirements will be demonstrated – e.g. through Software Assurance techniques – see SAM SWAL *Describe how satisfaction of human Safety Requirements will be demonstrated – e.g. through Human Assurance techniques SAM HAL as developed by the former EUROCONTROL SAM Task Force or equivalent. *Describe how satisfaction of procedures Safety Requirements will be demonstrated – e.g. through Procedure Assurance techniques SAM PAL as developed by the former EUROCONTROL SAM Task Force or equivalent. Note: *The usage of Assurance levels can be helpful in providing assurance, with sufficient confidence, via a complete, documented and valid argument that the safety will be satisfied and will remain satisfied (see ATS.OR.205 in the Annex to EU No. TBD (at the time of developing this document) repealing in particular 1034/2011 and 1035/2011).*
P5P6	**AO10**	**a1**	Show that all assurance in **Guidance A.3** applies to a known system configuration and which is consistent with the system configuration of Assurance activities belonging to P3P4 _AO4.	Satisfaction of this objective requires careful configuration control of the various representations of the system throughout the lifecycle. See also SAM, PSSA Introduction, section 6
P5P6	**AO11**	**a1**	Show that the evidence for the safety requirements is trustworthy	*Backing* evidence is obtained from the properties of the ***processes*** by which Direct Evidence (products) was obtained, and shows that those processes, tools and techniques, human resources etc. were appropriate, adequate and properly deployed. Evidence must be shown to be *trustworthy,* by demonstrating, *amongst other things*: • the suitability of the processes, tools and techniques etc. that are used to generate the evidence obtained from the safety assessment

			SPR-level Safety Assurance Activities	Guidance and Proposed Tools and Techniques
				• the correct application of those processes, tools and techniques the competence of the personnel applying those processes, tools and techniques.

Table 3: Detailed safety assurance activities to inform the SPR

A.4 Detailed safety assurance activities to inform the TS and refined version of the SPR

Ref			Physical Level Safety Assurance Activities	Guidance and Proposed Tools & Techniques
P7	AO1	a1	Define detailed Safety Requirements (*Functionality and Performance properties* from the success approach) for the physical system design	* Ensure the existence of an adequately detailed model of the physical design. *Note: this should be derived from engineering activities; it is not a process specifically undertaken by safety specialists.* * Provide traceability between SPR-level model elements and physical elements/subsystems * Ensure that new equipment items, equipment elements which have to be modified as part of the system change, and nominally unchanged equipment elements are clearly identified in the physical design. *SPR-level elements can include functional elements and data flows/interfaces; the physical design must provide realisations for all interfaces including air-ground comms, ground-ground comms and HMI. A physical element may realise more than one element of the SPR-level model, conversely one SPR-level model element may be realised by more than one physical element.* * Create detailed safety requirements for each new equipment items; this is required for inclusion in contracts for external suppliers or for internal developments * Establish bi-directional traceability between the SPR-level model Safety Requirements (success approach) and the equipment safety requirements (new, modified or existing)
P7	AO1	a2	Show that all new, expanded or refined safety requirements introduced in P7_AO1_a1 at the physical design level are necessary	* Perform analysis and provide justification of introduced or expanded requirements. * Perform analysis of human-machine interactions to determine required average and worst case response times * Perform analysis of expected message traffic (internal and from external systems) *Note: the effect of failures of all functions, inherited from the SPR-level model or introduced here, will be determined in P7_AO1_a4 below*
P7	AO1	a3	Show that the HMI requirements are fit for purpose in supporting controller and other ATC staff tasks	* Carry out HF expert review of HMI supported by expanded task analysis based on operational procedures * Perform evaluation of prototype and final HMI displays (can be combined with staff

Ref			Physical Level Safety Assurance Activities	Guidance and Proposed Tools & Techniques
				training and procedure-validation simulations) *This is a further step in the Human Factors analysis discussed in **Guidance K**, and can either use existing task analysis information or extend this information as required, following the HP Reference Material (HPRM) [Ref. 10].* The RE method in **Guidance I** can support the review of HMI requirements through an analysis of current work-as-done, adaptive capacity changes and the capture of design recommendations to strengthen the resilience of the design.
P7	**AO1**	**a4**	Identify all hazardous failure modes of the technical system at the functional-requirements level	* Perform, for instance, a Functional FMEA at the equipment functional requirements level for elements which have a direct operational functionality. * Identify functions which have no safety effect. * Provide traceability of equipment level failure modes to SPR-level model failure analyses and reconcile any discrepancies.
P7	**AO1**	**a5**	Assign quantitative failure rate targets to Functional failure modes	* Use failure rate targets derived at a higher level (from safety objectives (failure approach) or FM/ SPR-level model safety requirements (integrity)) and apportion to physical equipment failure modes.
P7	**AO1**	**a6**	Identify all reasonably foreseeable sources of common cause or other dependent failures	For instance: * Perform Common Cause Failure Analysis (including identification of CCF groups from minimal cutsets of fault tree, zonal hazard analysis and expert judgement) – see **Guidance N**. * Perform design HAZOPS applied to system elements and their interactions * Perform Single-point-of failure-analysis (part of FTA). * Perform FMEA at design element level to confirm that that there are no unexpected consequences of individual element failures (bottom-up analysis)
P7	**AO1**	**a7**	Show that measures are in place to mitigate sources of dependent failure	* Design reviews. * Review of engineering procedures/activities which might affect multiple equipments at the same time; design of procedures
P7	**AO1**	**a8**	Apportion quantitative failure targets to all equipment elements	*Note: it is assumed that some level of redundancy will be provided to ensure system reliability in all but the lowest integrity systems.* For instance: * Perform Fault Tree Analysis (or for simple designs Reliability Block Diagrams) for apportionment. Typically each equipment-level hazard as identified in the functional FMEA would be a candidate top event for a fault tree. * Identify existing items of equipment for which in-service reliability data is available

Ref			Physical Level Safety Assurance Activities	Guidance and Proposed Tools & Techniques
				(to assist in apportionment process) * Ensure that hardware element reliability requirements are not unreasonably stringent (design modification may be needed in the normal way if it appears unlikely that element reliability requirements can be met). * Identify realistic Mean Time to Restore values for each equipment item for inclusion in reliability calculations. * Show that reliability calculations have been moderated to take account of possible residual common cause failures – *includes selection and justification of any beta-factors or other methods used for moderating reliability calculations* (see **Guidance N**) * Show that the integrity of the links between the elements of the system is included in the analysis *The level to which the apportionment is performed will depend on system complexity and required system reliability – at least it should be undertaken to the level of individual computers, display screens, input devices and network elements. For typical ATM systems, more detailed analysis is not generally required.*
P7	**AO1**	**a9**	Allocate an appropriate Software Assurance (or Safety Integrity) level to all software elements	* For instance it can be done by: 1) Assigning a Software Assurance Level (SWAL). See **Guidance O**. To apply this process the equipment level FMEA and the upward traceability of equipment level failures to SPR-level model, FM and OSED level failure analysis will be helpful in understanding the implications of software' or 2) Following the guidance in Part 1 of IEC 61508 Edition 2 (2010) and obtain a Safety Integrity Level (SIL) for each function from its quantitative failure rate requirement. *The software SWAL or SIL is then, by default, the highest SWAL/SIL of all software functions in a single computer system, unless it can be shown by analysis of the software architecture that failure of a lower-integrity element cannot adversely affect higher integrity elements. Guidance on this topic is given in IEC 61508 Part 3 Edition 2. See **Guidance O**. *The reference to IEC 61508 is given here, as an option, because some ATM equipment manufacturers have a preference for using this standard for their software development.*
P7	**AO1**	**a10**	Evaluate design options and show that the selected design meets the AFARP criterion	* Propose physical design alternatives and describe the basis for choice of the final design solution * In addition, it is usually important to show that physical-design decisions are made

Ref			Physical Level Safety Assurance Activities	Guidance and Proposed Tools & Techniques
				with due regard to considering to even further reducing risk. In practice this means showing that implementing any other design solution other than the one chosen would not bring other safety benefits or that the associated costs would be grossly disproportionate to any additional safety benefit that would accrue. *For the airborne and space elements, it will often be the case that the equipment aspects are already defined – e.g. a new /modified operational concept making use of existing aircraft RNAV capabilities. In those cases, the aircraft / satellite equipment properties would normally have to be treated as "fixed" and the ground-based equipment properties as "variable" and requiring adjustment to ensure that, overall, the specified safety criteria are satisfied.*
P7	**AO1**	**a11**	Define new ATC /flight crew procedures requirements	* Perform Impact analysis of SPR-level model SRs against existing procedures (including LOAs with adjacent ATSUs) and define requirements for modified procedures. * Provide the rationales for deciding which aspects of the Human Tasks need to be 'proceduralized' * Identify obsolete procedures for removal. * Define requirements for new procedures to be developed by analysis of SPR-level model SRs and technical system design (for example, any operational procedures needed in connection with the system HMI). * Review of all new and modified procedural requirements and HMI design by expert controller group. * Provide traceability of new and modified procedural requirement to SPR-level model SRs and any further SRs derived from specific design features (such as HMI details
P7	**AO1**	**a12**	Show that all new, expanded or refined ATC/flight crew procedures requirements are necessary for the operation of the Technical System under all *normal* operating conditions	*Knowledge of the physical design, that was not available at the time that the SPR-level model was derived and analysed, can often lead to additions to, or refinement of, the Human tasks that in turn may lead to new, expanded or refined requirements for ATC Procedures* *Normal conditions are those under which the system is operating as designed, with full functionality and performance*
P7	**AO1**	**a13**	Show new ATC/flight crew procedures requirements are sufficient to ensure the safest operation of the Technical System under all *abnormal* operating conditions, <u>and</u> recovery from those conditions	*Abnormal conditions are those under which the system has to operate in a reversionary mode due to, for example:* *1) Abnormal conditions external to the ATM system concerned* *2) External Equipment failures,* *3) Maintenance interventions – out of scope for SESAR Development Phase*

Ref			Physical Level Safety Assurance Activities	Guidance and Proposed Tools & Techniques
				For instance this can be achieved with the following: * Analyse abnormal external conditions and develop procedure requirements (use information in FM and SPR-level model analyses of abnormal external conditions) * Use results of FMEA and existing knowledge to identify failures internal to the technical system. * Identify appropriate operational response to system failures and define requirements (normally there will be some level or levels of fallback system) * Identify necessary actions when system has been restored to full operation and define requirements for recovery procedures
P7	**AO1**	**a14**	Define Controller Competence Requirements	In close coordination with 16.06.05 and by using the HP Reference Material: * Derive requirements for Controller training, as necessary * Derive requirements for Controller licensing, as necessary * Derive requirements for Controller selection & management, as necessary * Show that all three sets of requirements together are sufficient to satisfy the relevant safety requirements (*functionality and performance properties* from the success approach) placed on human elements in the SPR-level model *See also SAM, SSA Introduction, section 3.1.2A and ESARR 5, section 5.2*
P7	**AO2**	**a1**	Show that non-safety elements of the physical design do not adversely affect safety	*Adverse safety properties that may get included inadvertently in the physical design cover:* • *adverse interactions with functions that are included in the design for non-safety reasons* • *a relatively new consideration of the inadvertent / unjustified under-specification of human tasks (see P7_AO2_a2 below)* For instance: * Carry out two-way traceability between the SPR-level model -required safety functionality and all of the functionality provided in the physical Technical System *Identify any functionality in the physical Technical System that is not required by the safety requirements (success approach) of the SPR-level model and justify its inclusion in the former *Because the SPR-level model is defined at a SPR level, real equipment elements may have functions not specifically derived from the SPR-level model safety requirements (success approach). Examples are business support functions (route charges, statistics collection generally) and operational monitoring and control functions. While not directly related to the provision of the ATC service these latter are typically necessary to ensure rapid fault diagnosis and recovery, and to facilitate*

Ref			Physical Level Safety Assurance Activities	Guidance and Proposed Tools & Techniques
				in-service monitoring. Also included may be functions within a COTS product that are not required by the SPR-level model (and therefore by the OSED level specification) * Perform a design analysis to show that non-safety elements cannot adversely affect safety related elements by (for example) consuming excessive computing or bandwidth resources (such as internal or external communications networks) or by interfering with the operation of safety-related elements. * Perform a Functional FMEA on physical system elements which have no direct operational functionality to establish hazardous failure modes. – note that this process is essential because only when the physical design is complete can its hazardous failure modes be properly assessed. Physical design elements which have no immediate operational interface (such as system monitoring elements) could have failure modes which affect operational services. *Note: ideally non-safety elements should not request information from safety related element but should only receive it at the discretion of the latter.* *Note: where non-safety functions and safety functions are implemented in the same computer system, ESARR 6 requires a demonstration of independence*
P7	**AO2**	**a2**	Show that any deliberate under-specification of Human actions that is done for safety reasons has a substantial net safety benefit	*Leaving specific actions to the discretion of a human operator – especially in the case of reaction to abnormal events – can have positive safety benefits (as in the case of the Hudson River major incident in New York in 2009.* *However, in the case of, for example, the latitude enforced on pilots by PANS-OPS (Chapter 3 section 3.1.2) in the event of a TCAS RA, may have both positive benefits and (possibly in the case of the Überlingen mid-air collision) negative side effects. Thus the analysis must consider both possibilities* Under-specification is a principle of Resilience Engineering. **Guidance I** may support the identification of scenarios where under-specification occurs and can assist in identifying the strategies adopted by operators to a range of varying conditions which can inform the design.
P7	**AO2**	**a3**	Show that any deliberate under-specification of Human actions that is done for non-safety reasons cannot have a significant adverse effect on safety	*Leaving specific actions to the discretion of a human operator can also have non-safety benefits even under normal conditions – this is currently the case, for example, in Terminal Area operations where optimisation of the sequencing of traffic is (in the absence of automation such as Arrival Managers) often left to the skills of the Controller.* *The analysis here must therefore show that such benefits are not sought at the expense of the overriding need for safety* Under-specification is a principle of Resilience Engineering. **Guidance I** may support the identification of scenarios where under-specification occurs and can

Ref			Physical Level Safety Assurance Activities	Guidance and Proposed Tools & Techniques
				assist in identifying the strategies adopted by operators to a range of varying conditions which can inform the design.
P7	AO2	a4	Show that all necessary attributes of technical system specifications have been addressed	*Review of equipment element requirements to ensure that all attributes (function, performance and timing, capacity, accuracy, overload tolerance, robustness) have been properly specified or are not relevant. *Apart from in Artificial Intelligence (AI) systems, functional and performance variability in technical systems is usually the result of pragmatic limitations or inadvertent under-specification, rather than deliberate intent.*
Note on P8 and P9			Safety Assurance objectives and activities related to Principles P8 and P9 refer to V-cycle stages post V3. As a result there are not further developed in the current version of the Guidance document.	

Table 4: Detailed safety assurance activities to inform the TS

Guidance B On describing the operational environments

B.1 Introduction

It is impracticable to present the full scope of this activity in a generic way. However, as examples, a description of the operational environment for En-route / Terminal Area operations, and Airport operations would normally include some or all of the points listed in paragraphs **B.2**and **B.3** below.

Where there is no change from the current (pre-change) operational environment, this should be stated in the description.

Note that there should be consistency between what is in the environment description and what are shown as external entities in the engineering models (e.g. SPR-level).

The methodology in **Guidance I**, in particular Step 1, describes how it is important to build an understanding of how work is currently performed in the operating environment which needs to include a detailed description of the operating environment.

B.2 En-route and Terminal Area Operations

Include a description of the following, as applicable:

- airspace structure and boundaries
- types of airspace / ICAO classifications
- route structures (as applicable) and any restricted airspace (temporary or otherwise)
- airspace users – e.g. commercial jets, military aircraft (flying as OAT) general aviation, very-light jets, unmanned aerial vehicles etc.
- flight rules – IFR and/or VFR and/or OAT
- traffic levels and complexity
- aircraft ATM capabilities
- significant weather and other meteorological conditions
- local terrain features, obstacles etc.
- navigation aids
- environmental constraints
- the Air Navigation Services to be provided, and the associated separation minima (stating whether they are existing or proposed).

Include also any other points (*i.e.* not listed above) that are relevant to the safety assessment in question.

B.3 Airport Operations

Include a description of the following, as applicable:

- airspace structure and boundaries relevant to airport operations (including classification of airspace adjacent to the airport)
- runway, taxiway, apron and/or stands configuration, geometry and dimensions
- runway-Taxiway and/or Taxiway-Apron interface
- traffic amount
- traffic distribution in time

- traffic distribution in space around airport
- effect of other airports in the vicinity including military airfields
- airport users – e.g. commercial jets, military aircraft (flying as OAT) general aviation, very-light jets, unmanned aerial vehicles etc.
- aircraft characteristics and ATM capabilities – mix of aircraft types using airport.
- traffic characteristics (passenger, freight, training, general aviation and others)
- local terrain features, obstacles etc.
- weather / other meteorological and visibility conditions
- navigation / landing aids
- environmental constraints
- the Air Navigation Services to be provided, and associated airborne separation minima (stating whether they are existing or proposed).

Include also any other points (*i.e.* not listed above) that are relevant to the safety assessment in question.

Guidance C On Safety scoping and change assessment

C.1 Process

Safety Scoping & Change Assessment is the preparatory process of identifying the main safety issues associated with a specific Solution as soon as possible after an Operational Concept has been developed and to help in deciding whether a full (i.e. carrying out all safety assurance activities defined in **Guidance A.2, A.3, and A.4**) safety assessment is required.

It provides an initial assessment of the safety implications of the Solution. It should address, *amongst other things*, 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 and, in broad terms, the strategy for demonstrating safety.

The results of this process will allow to issue a Safety Plan (in accordance with SAF PLN template) aimed at specifying the safety assurance activities to be carried out by the Solution, whilst recording the relevant safety assessment information available at this initial stage (to be further used as input to the Safety Assessment Report).

The different steps in the process are shown in the following table. The tasks are logically organized. However, the dynamic of the workshop might lead to some adaptations in order, merging, etc. The process described herein will be carried out within a workshop with the various projects belonging to the relevant Solution and involving the HP expertise to ensure full co-ordination between SAF and HP.

Task	Guidance
General Solution Issues	
• Determine the content, deliverables, scope and major milestones for the Solution.	Refer to the general Project documentation for the Solution
• Determine who the Solution Stakeholders are and what: • expectations • issues • responsibilities towards the Solution they may have	Refer to the general Projects documentation and elicit further during the Safety Scoping & Change Assessment workshop.
• Understand Operational Concept	An outline should be presented at the Safety Scoping & Change Assessment workshop to ensure a common understanding / agreement.
• Describe the benefits expected from the Solution in terms of: Capacity, Environment, Efficiency, Economy, Safety, Interoperability, etc.	Refer to the general Projects documentation, including its Business Case. The benefits sought by the stakeholders, incl. users requirements, may vary between different ANSPs – e.g. the introduction of automation may be used to improve safety by one ANSP and to improve capacity by another ANSP – therefore, **agreement amongst members of the Solution at this stage is essential** to ensuring that the aim of the safety aspects of the Solution is established in the most beneficial way.

• If the Solution has to deliver a safety benefit, determine what is expected and how achievement will be judged. If the Solution is to be safety neutral, how is this to be expressed?	Refer to the general Projects documentation and elicit further during the Safety Scoping & Change Assessment workshop. This documentation includes but is not limited to e.g. X.2 Validation Strategy, the Solution Validation Plan, initial version of the OSED to get a first understanding of how declared (if relevant) safety benefits will be assessed (e.g. specification of suitable and measurable validation objectives in the validation plans), etc.
• Identify whether the deployment is to be "one shot" or incremental (e.g. in terms of OI steps, geographical coverage, etc.). If it is to be incremental, determine what order, and in what timescales, does the deployment take place?	Refer to the general Projects documentation and elicit further during Safety Scoping & Change Assessment workshop (see list above).
Change assessment	
• Determine the baseline for the Change Assessment in terms of: • the Operational Environment • the ATM/ANS & underlying functional systems and operations • regulations (safety and general) and standards (safety, operational and equipment) apply to the Solution	Guidance is provided in Guidance B for the description of the 'specimen' OE. Key variability in OE conditions can be captured here by using the method described in **Guidance I** (Step 2). Any change is, by definition, assessed relative to what existed before the change. The baseline for the assessment may be what exists at the time of the assessment or, in some cases, what will exist when the change is introduced into service. Clearly, not all ANSPs will be starting from the same current OE and system configuration and, therefore, **stakeholder agreement** at this stage is essential to ensuring that the baseline for the Solution is established in the most beneficial way. *Important note on OE: Indeed a set of safety requirements satisfying a set of safety criteria can only be true for a given environment. Changing the environment, then the requirements-satisfaction demonstration might be invalidated. The SESAR work programme, in particular X.2's should define the given environment for which the validation activities will be carried out. Eventually, i.e. once a Solution is declared an eligible candidate to move to V4, then ANSPs in particular would have to adapt the SESAR assessments to take into account local environments.* Refer to the general Projects documentation and elicit further during the Safety Scoping & Change Assessment workshop.

• Determine the Operational Environment (OE) in which the new/modified ATM/ANS Functional System is indented to operate.	Refer to the Operational Concept and elicit further during the Safety Scoping & Change Assessment workshop. Guidance is provided in Guidance B. The properties of the OE are crucial to a safety assessment – specifically, a safety assessment that is valid for one (reference) OE may not be valid for a different OE. Thus, in order to be complete, a safety assessment cannot be *generic* – it has to be specific, to a particular OE – therefore, **stakeholder agreement** at this stage is essential to ensuring that the OE selected for the Solution is established in the most beneficial way.
• Elicit the details of the change(s) to be brought by the Solution, with respect to the baseline (see item 6 above) for the following: ▪ Operating methods (procedures), tasks, practices ▪ Technical systems (incl. performance) ▪ Human and technical systems • Roles and responsibilities • Allocation of tasks • HMI ▪ Change in Teams and Communication ▪ Change in HP-related transition factors (staffing, competence, acceptance and job satisfaction)	Definitions available in HP Reference Material (HP RM) Chapter 3.3.6 and Annex I.
• On that basis, summarize what is removed, added and modified at the level of: ▪ OSED level Specification ▪ SPR-level design ▪ Physical design	This is an initial assessment only but must be rigorous enough to decide to which extent (*proportionality*) the safety assessment of the Solution will be conducted
• Identify the need for new or modified regulations	This is an initial assessment only but must be rigorous enough to assess whether changes to regulations (incl. PANS-ATM, PANS-OPS, etc.) is required
Safety Strategy	
• Determine the relevant pre-existing hazards that the Solution operational services have to mitigate in the relevant operational environment.	By definition, these hazards exist in the operational environment before any form of ATM de-confliction has taken place. It is therefore the primary purpose of the relevant Solution operational services to mitigate (some of) them). See Guidance F.2.2.

• Determine and justify the Safety Criteria, including criteria as per **Guidance D** but also, where applicable, the regulatory and organisational requirements as well as any standards to be applied (e.g. ICAO Annexes)	The SESAR Consortium has defined a safety target for future ATM (SESAR Deliverable D2 from the SESAR Definition Phase). The "**White Paper on the SESAR Safety Target**" from EC Episode 3 Project (D2.4.3-01) interprets the target very precisely and supplies the necessary detail. General guidance on Safety Criteria is given in **Guidance D.3**. This **shall** be done in coordination with PJ19.3 and WPB4.1 to ensure the consistency of the safety criteria across all Solutions. This is achieved by using the Accident-Incident Models (AIM) from P16.01.01 and the methodology to allocate performance requirements of WPB4.1 Task 15 to generate quantitative Safety Performance Targets. As the Safety Criteria are directly related to the consideration of safety benefits, **stakeholder agreement** at this stage is essential
• Decide the safety deliverables to be produced and for whom (i.e. for which stakeholders) they are intended.	It is very important to get **stakeholder agreement** on these so that what is produced is of more benefit to them.
• Determine whether or not the Solution affects, and/or depends on, the safety activities associated with other Solutions or on-going operations.	This will help determine the purpose and scope of the Safety Assessment
• Record any other safety/HP issues / uncertainties that were identified during the Safety Scoping & Change Assessment process and which need to be addressed during the subsequent safety assessment.	HP issue analysis (see Appendix E of the HP RM and record in HP Log – Appendix B of the HP RM).

C.2 Tailored Safety Assurance Objectives and Activities per type of change

The Safety Assurance Objectives and Activities presented in section **Guidance A** are all generic. This means that they cover the case of a change to the ATM/ANS functional system that is so fundamental that all of the Safety Assurance Objectives (but not necessarily all of the Activities) specified in this document need to be completed.

In many cases, however, this is not the situation – for example, a purely technology-replacement project would normally have no effect on the operational environment, the user requirements, the service delivered, or the functional or logical aspects of the functional system design.

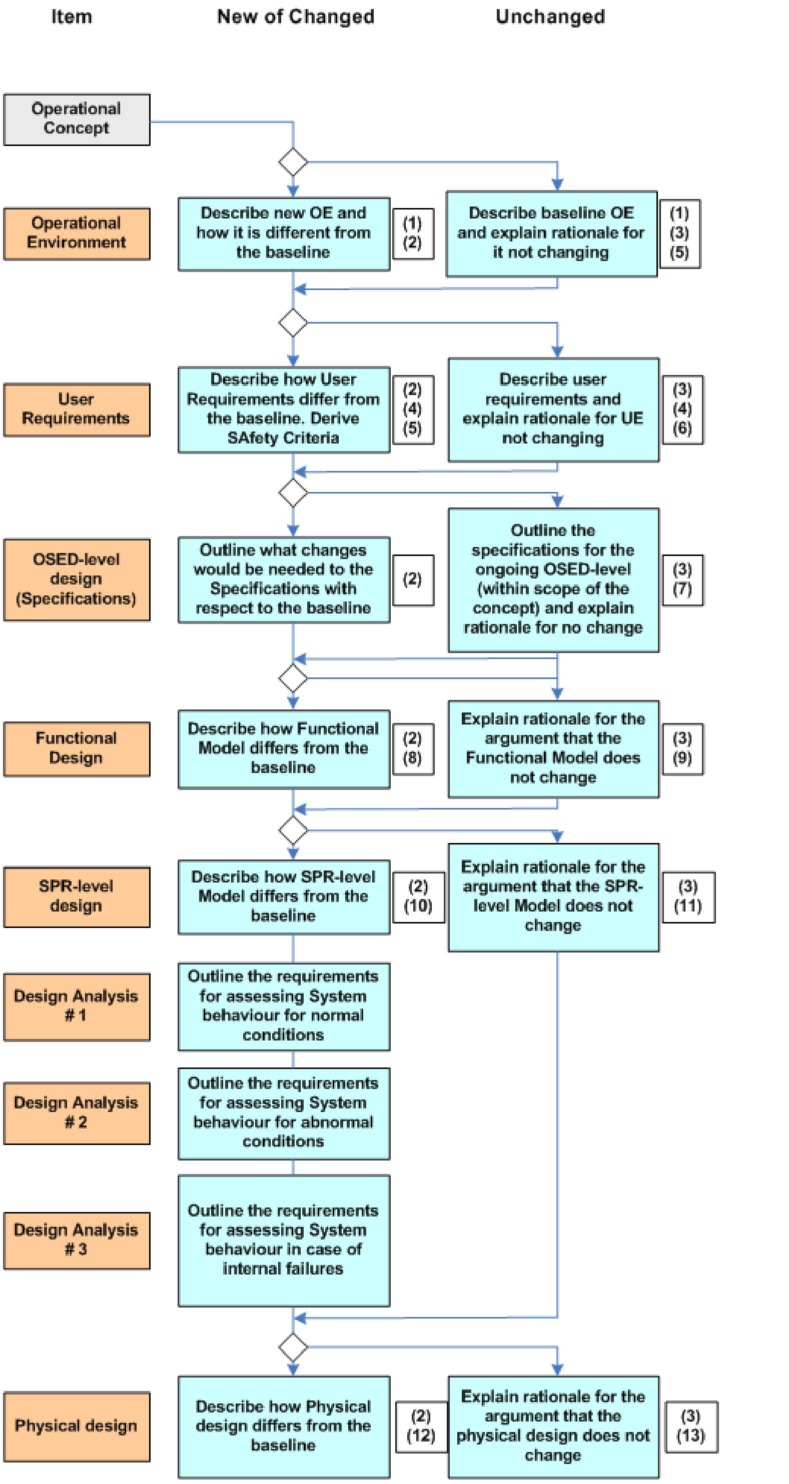
For such cases it would probably not be cost effective to carry out all the Safety Assurance Objectives and Activities at the OSED and SPR levels – rather, it would be better to focus resources on Implementation.

However, it has been emphasized in the main body of this document that the Safety Assurance Objectives and ultimately the Activities are driven by the Principles – not the other way around.

Therefore, if we wish to "miss out" some of the generically defined Objectives and Activities then we must justify that.

There are two aspects to the process:

- execution of a Change Assessment as part of the Safety Scoping & Change Assessment process defined in **C.1**
- definition of a tailored set of assurance activities (see **Figure 1** below)


Item
New of Changed
Unchanged
Notes
Operational Concept
Operational Environment
Describe new OE and how it is different from the baseline
(1) (2)
Describe baseline OE and explain rational for it not changing
(1) (3) (5)
User Requirements
Describe how User Requirements differ from the baseline. Derive SAfety Criteria
(2) (4) (5)
Describe user requirements and explain rationale for UE not changing
(3) (4) (6)
OSED-level design (Specifications)
Outline what changes would be needed to the Specifications with respect to the baseline
(2)
Outline the specifications for the ongoing OSED-level (within scope of the concept) and explain rationale for no change
(3) (7)
Functional Design
Describe how Functional Model differs from the baseline
(2) (8)
Explain rationale for the argument that the Functional Model does not change
(3) (9)
SPR-level design
Describe how SPR-level Model differs from the baseline
(2) (10)
Explain rationale for the argument that the SPR-level Model does not change
(3) (11)
Design Analysis # 1
Outline the requirements for assessing System behaviour for normal conditions
Design Analysis # 2
Outline the requirements for assessing System behaviour for abnormal conditions
Design Analysis # 3
Outline the requirements for assessing System behaviour in case of internal failures
Physical design
Describe how Physical design differs from the baseline
(2) (12)
Explain rationale for the argument that the physical design does not change
(3) (13)

1) Don't forget to consider increased traffic levels

2) Include safety assessment activities in OFA Safety Plan

3) OFA Safety Plan must argue that the item has not changed. PAC Safety Case must present the rationale as evidence

4) Consider capacity, safety, environment, efficiency, economy, flexibility, interoperability, etc.

5) Note that URs may change the OE – e.g. increased capacity leading to increased traffic

6) Applies only if none of URs change

7) Applies only if URs and OE are BOTH unchanged

8) Need to consider Safety Functions, Data and interactions, and the performance and integrity of Safety Functions and Data

9) FM may change even though Spec hasn't changed. Conversely, if the Spec has changed it is unlikely that FM remains unchanged

10) Need to consider human tasks, equipment functions and interfaces, and the performance and integrity of each.

11) SPR-level model may change even though FM hasn't changed. Conversely, if the FM has changed it is highly unlikely that SPR-level model remains unchanged

12) Need to consider human tasks, equipment functions and interfaces, and the performance and integrity of each.

13) If PM hasn't changed, it would be difficult to see what had changed! Conversely, if the SPR-level model has changed it is highly unlikely that PM remains unchanged

Figure 1: Selection of safety assurance activities from a change assessment

Guidance D On defining SAfety Criteria

> As per the SRM definition:
>
> *'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.*
>
> Note that despite the terms Safety Criteria – SAC is used here this guidance only focuses on the risk targets part of the SAC.

D.1 Overview

One of the first actions after identifying the nature and scope of the Solution is the setting of quantitative safety targets that define what is considered tolerably safe for the change being introduced by the Solution and permit the validation of the expected safety impact of a Solution on ATM provision. In SESAR, due to the multitude of operational projects involved and to the necessity to assure that overall SESAR Safety Performance Ambition for future ATM is to be satisfied at the different concept development steps, it is essential that these targets are identified and described based on a common framework. In SESAR, this framework is supplied by the Accident Incident Model (AIM) developed within the SESAR 1 P16.06.01.

The AIM risk model provides a set of templates (one for each accident type) that are used to identify where and how each the operational improvements that each Solution are making will impact the safety of ATM provision. The method involves the identification of those parts in the risk models that would be impacted and thereby the measurable elements that would be either increased if safety was reduced, decreased if safety improved or unchanged in the case of operational changes that should not impact safety. Glossaries of term for the barriers, precursors and base events of the different models are available on the SESAR 1 Project 16.01.01 Library ([Ref. 20]).

D.1.1 AIM description

The AIM model, as shown in **Figure 2** below, is a set of accident risk models for the accident types listed below based upon ECAC incident data and developed using operational experts (information related to the quantification of the models as well as the source of data is detailed in [Ref. 19]. The models include:

- Mid-Air Collision (MAC) for en-route and TMA
- MAC in Oceanic environment (only qualitative currently)
- Runway Collision
- Taxiway Collision
- Controlled Flight Into Terrain
- Wake Induced Accidents
- Runway Excursion

The latest version of the AIM models is available in the AIM release AIM V10-3 [Ref 18].

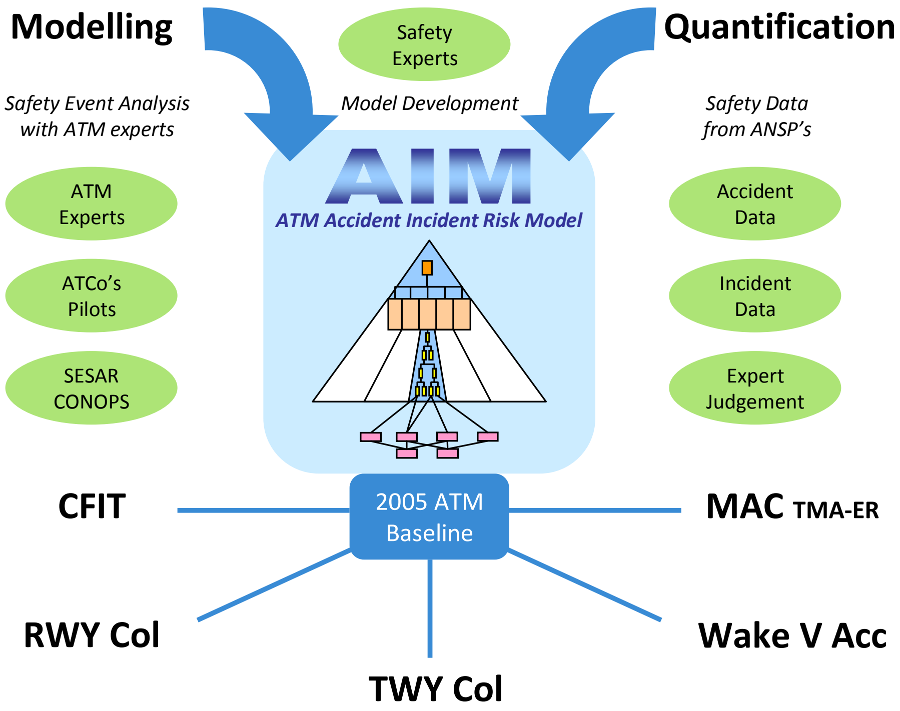


Figure 2: AIM – an helicopter view

The models have been reviewed and refined by many ANSPs and represent a 2012 baseline that describes ATM risks to be used for SESAR 2020. The underlying structure of the AIM is also adapted to represent the SESAR ConOps, while ensuring that a similar structure can be used for both generic (The SESAR 2020 baseline will be 2012) and predictive (setting of the SACs for SESAR 2020 solutions) modes .

The “Validation / Verification of the SESAR Accident Incident Model (AIM)” report summarizes the qualitative and quantitative validation / verification for the SESAR Accident Incident Model (AIM). The document is divided into two sections, the first describing the activities of qualitative validation and the second describing the quantitative validation It is accessible at the following URL: *https://extranet.sesarju.eu/WP_16/Project_16.01.01/Project%20Plan/Forms/AllItems.aspx?RootFolder=%2fWP_16%2fProject_16.01.01%2fProject%20Plan%2f05_Testing_Verification&FolderCTID=0x0120008A484F3C05865E4AA1215372A38CAE35&View={1B23E4D6-CEF8-4152-AAFE-7BF6CCF09257}*

D.1.2 Process overview

The definition of safety targets for each Solution from the SESAR Safety Performance Ambition is done at 2 levels as shown in **Figure 3** .

A first level definition has been done by SESAR 1 P16.06.01 in support of B4.1 and maintained by PJ19.3, in which Safety Validations Targets are defined for each Solution in order to ensure that the overall SESAR Safety Performance Ambition is to be satisfied. An overview of the method used to define the Safety Validation Targets is presented in D.2. The Safety Validation targets assignment by PJ19.3 will also take account of the Performance Expectations for each Solution, which are assessed as part of the CONOPS development led by PJ19.1.

A second level definition is done in the frame of each Solution, in which those Safety Validation Targets are defined in more detail as SAfety Criteria - SAC, i.e. measurable safety targets defined at a lower level to be used in their corresponding safety assessment and validation activities. Guidance **D.3** presents the way SAC are to be defined in the frame of each Solution.

A feed back to PJ19.3 from each Solution based on detailed SAC and evidences from validation activities ensuring they are met is necessary in order to keep ensuring that overall SESAR Safety Performance Ambition is to be satisfied. D.4 provides more detail on this.

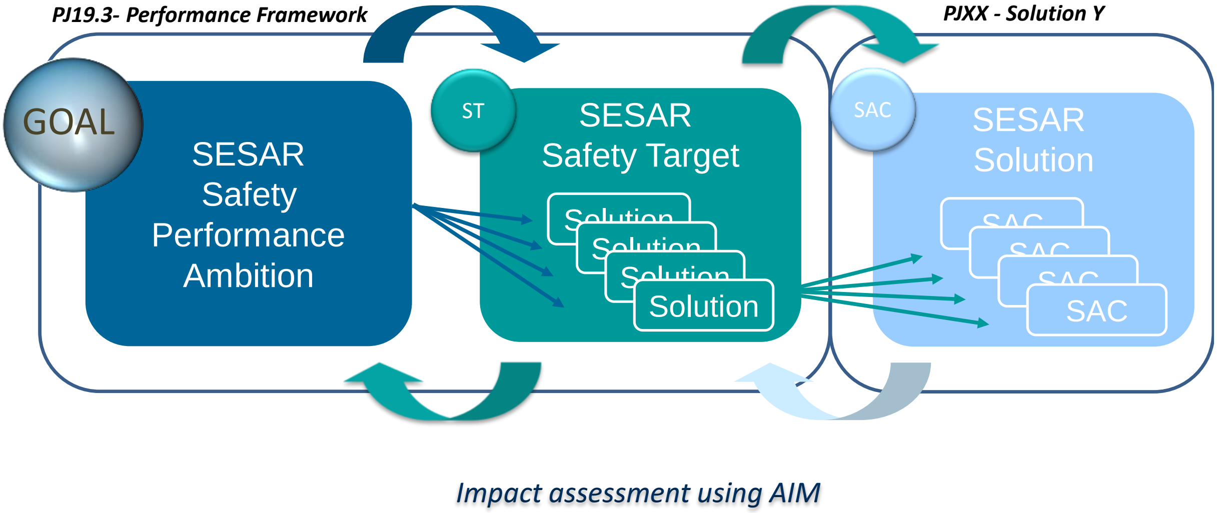


Figure 3: Safety targets definition – process overview

An example of the process for setting the SAC as described in this guidance is provided in **D.5**.

D.2 Safety Validation Targets defined in the frame of PJ19.3

Unlike for the other KPAs, the approach applied for defining the safety validation targets has a large amount of “bottom-up” assessment of the performance contribution from the Solutions. Despite this fact, the apportionment can still be regarded as representing required contributions as aggregated impacts are tested against overall requirements and only accepted where sufficient ‘performance’ results.

To achieve this, impacts of traffic, deployment baseline and SESAR changes are modelled to obtain a prediction of the safety performance. This set out to be a stepwise, iterative process where the estimates were made and if they did not demonstrate sufficient safety (i.e. that the absolute number of accidents would not increase despite the traffic increase) then further safety benefits would be sought for the Solution to obtain a compliant target.

These Safety Validation Targets are being defined by PPJ19.3, in workshops involving projects SMEs and PJ19.3 safety experts and eventually reviewed and endorsed as part of the established Performance Framework consultation process. Initially a qualitative review of the impact of each Solution is undertaken. This can take account of the Performance Expectations in the CONOPS (PJ19.1). This is then augmented with a relative qualitative assessment of safety impact, before finally being quantified. This initial quantification was then used as input to more detailed modelling to estimate the impact of traffic growth on the assumptions made about safety. Finally, a review (sanity check) is undertaken to ensure that assumptions and estimations about the impact of the Solutions on safety are appropriate and that typical workshop errors, such as double counting or over-focus on a specific Solution, had been accounted for.

An overview of the process applied is presented in next section.

	More details on this process as well as the results of this task are available in corresponding PJ19.3 Performance Framework documentation. Note: Please check in SJU extranet for the latest version of the “Validation Targets” document.

D.2.1 Process overview

The Performance Ambition target for safety in SESAR 2020 is that given the implementation of SESAR, the absolute number of accidents shall not increase despite the increase in traffic. The traffic increase will be as per the EUROCONTROL STATFOR LTF. Within the SESAR 2020 programme, this has been taken to mean a 80-100% increase in IFR movements for Airspace environments and 5-10% runway throughput increase for Airport environments – in consistency with the respective Airspace and Airport capacity targets for 2035.

In order to ensure that the SESAR Safety Validation Targets generated within the Performance Framework are complete and make use of available data (also proposed for use in the SESAR programme), the Accident Incident Model (AIM) tool is used to specify safety targets (design hurdles *i.e.* validation targets). The process is described below.

The Safety Validation Targets are defined thought the following steps:

A. Qualitative safety impact assessment: based on safety and operational expert judgement during dedicated PPJ19.3 workshops, the potential safety impact of each Solution is assessed at the level of the relevant AIM model, barriers, contributors and precursors. This can build on the preliminary impact assessments as part of the PJ19.1 work on the CONOPS.

B. Quantitative safety impact assessment: starting with a qualitative assessment of the impact (high, medium, low impact), this impact is then quantified as a % of improvement / reduction in barriers performances and/or precursors occurrences. Those figures are at the end 'normalised' among the several Solutions.

C. Estimation of the overall impact taking into account the traffic growth: then AIM is used to estimate the overall impact on the number of fatal accidents per year, taking into account quantitatively those changes introduced by the several Solutions in the corresponding Step (as explained above) as well as the corresponding traffic increase estimated for this same step (as per the corresponding intermediate target for Airspace and Airport Capacity).

D. Final target refinement: in this (iterative) process the overall result is considered acceptable only when it satisfies the SESAR Safety Performance Ambition which is "no increase in the number of accidents despite an increase of traffic".

D.2.2 Safety Validation Targets: what they are and they are not

In the frame of PJ19.3 Safety Validation Targets are defined at Solution, level.

Safety Validation Targets are expressed as *a percentage defining the expected reduction due to SESAR in the "total number of fatal accidents per year" with ATM contribution with respect to a potential outcome in a hypothetical "do nothing" case (no changes to ATM safety, while traffic is allowed to increase).*

They are then defined at overall level and per type of accident. Their corresponding translation into safety targets at AIM barriers/precursors level (at which SAC are defined) is to be done at the level of each Solution. .

	Safety targets resulting from preliminary assessment done by PJ19.3 to be used to set SAC in the frame of each SESAR Solution are available in the SJU extranet. Justification related to these safety targets is available from PJ19.3.

Those safety targets are then the starting point for the safety assessment at the level of the Solution (explained in Guidance **D.3** below). They need to be reviewed by the experts involved in the Solution (see detailed explanation in section **D.3.1**) and updated as necessary afterwards at the level of the PJ19.3 to ensure that the SESAR Safety Performance Ambition is still met (see detailed explanation in section **D.4**).

D.3 SAC defined at Solution level

Starting from high level assessment done by PJ19.3 as explained in previous section **D.2.2**, the assessment is to be done in more detail by the Solution's team in order to define the refined safety targets for the corresponding Solution, i.e. the SAC.

SAC are set during the Scoping and Change Assessment activities (see **Guidance C**) that are part of the safety planning process. AIM models are used by safety experts within the Solution team with the assistance of operational and technical experts on the changes involved.

The setting of SAC targets is done in two steps:

- **Qualitative impact assessment**: similar to the one performed in the frame ofPJ19.3, this assessment allows to identify the type of accident, the safety barriers and the causal factors impacted by the corresponding change(s). See more detail in D3.1.
- **Quantitative impact assessment**: to decide if these impacted risks are increased, decreased or must remain the same. Based on this quantification SAC targets are then defined at the Solution level. See more detail in D3.2.

As mentioned above, Safety Validation Targets from PJ19.3 and the related information (safety targets at barriers and precursors level and corresponding justifications) are used as inputs in this process.

D.3.1 Qualitative Impact assessment

The qualitative assessment is performed by the safety experts within the Solution team (and PJ19.3 as necessary) on the basis of the AIM models. But it also requires the participation of operational and technical experts that have a good understanding of the ATM concepts brought by the Solution and processes / procedures involved.

The objective of the assessment (as show in **Figure 4**) is to identify where the operational change will impact the ATM risk, at the level of induced precursors and the base events (lowest level risks) in the relevant model(s) for each impacted barrier(s). For that, the preliminary assessment done in the frame of PJ19.3 is to be used, as well as more detailed information available in the OSED (for example scenarios identifying particular failures or description of the operational change and the corresponding potential hazards).

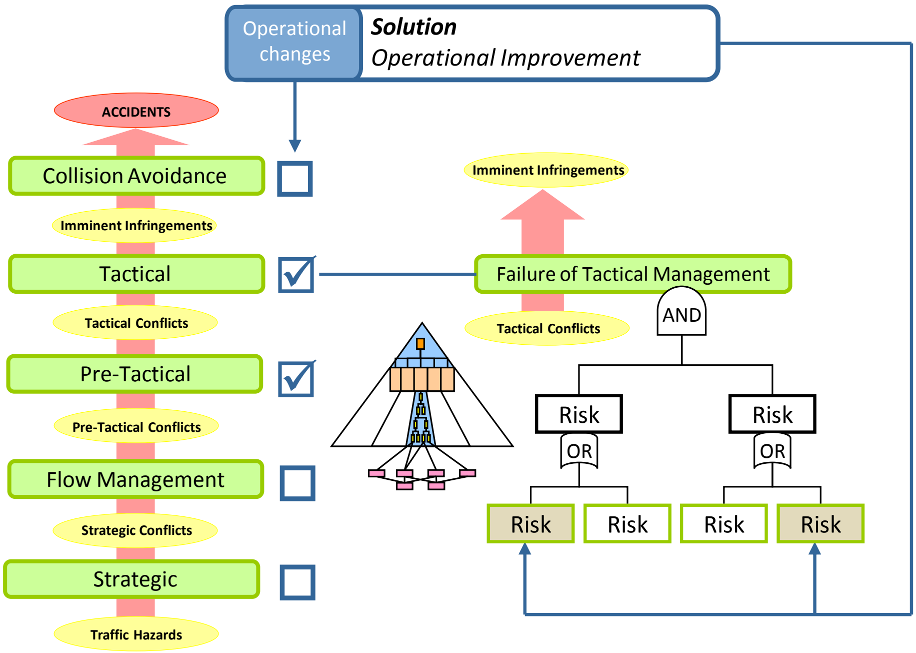


Figure 4: The base events affected in the AIM fault tree for each barrier

Note: in the diagram above and for the sake of not copying the entire tree, lower level contributors have been 'replaced' generically by 'Risk'.

For completely new concepts (such as ASAS) the AIM model has additional base events to permit the impacts to be modelled in the future systems. It is of course necessary in such cases for the operational experts to determine the impacts of these new ATM elements on the risks of the considered baseline at the barrier level.

D.3.2 Quantitative Impact assessment

For each identified risks in the AIM model(s) that the operational change will impact it is necessary to first qualitatively estimate if the result will be an increase or decrease in risk or if an increase is expected and that the result must be neutral (i.e. the increase has to be mitigated). Identification of whether there is a safety benefit or dis-benefit and an estimate of the level of the safety impact (significant, minor, neutral) enables to agree the extent to which this could be translated into a percentage effect on safety.

Then experts have to decide on a quantitative estimate of the impact. This would normally result in a percentage improvement or deterioration on corresponding barriers performance and/or induced events occurrence. This estimate will be used to determine the predicted safety impact on precursors and thereby allow the setting of quantified SAC. It is acknowledged that the quantification of the expected level of the impacts may move the assessor into an area of uncertainty in particular in the early stage of a project. Preliminary assessment done by PJ19.3 provides an initial indication of this quantification.

❗	While assessment the impact on the changes, the impact of any change should include the effects of traffic increases on risk. Besides, not only safety aspects are to be taken into account for the setting of the Safety Criteria. Other relevant aspects concerning traffic increase and other KPAs are also to be identified and considered in these discussions (e.g. impact on airspace capacity). This trade-off analysis between the several Solution goals should take place considering **Guidance I** (Goal trade-offs resilience principle # 4). Outcomes from the Benefit Mechanisms performed by the Solution team are also to be taken into account. As the SAfety Criteria are directly related to the consideration of safety impacts, stakeholder agreement is essential in this process.

More support to estimate the impacts of a change can be found in the training pack developed by PJ19.3.

Setting the Safety Criteria

SAfety Criteria are defined at AIM precursor level and can be:

- in a ***Relative*** way to respect to a 'do nothing case' (see section **D.2.2**) in which traffic increase is taken into account. Example of SAC:

  There shall be a reduction of 5% in Imminent Infringements due to "operational change X", taking into account a % traffic increase.

  Such SAC are useful for validation where the baseline used may not be comparable with the SESAR baseline situation and so where a relative change has to be measured. This is often the case where validations occur in a particular operational environment or where the concept tested needs special pre-conditions.

- in an ***Absolute*** way in which traffic increase is also taken into account. Example of SAC:

Imminent Infringement shall be less than 5e-5 per flight hour with the introduction of "operational change X", taking into account a % traffic increase.

Such SAC are useful to allow overall predicted performances to be calculated for sets of changes across SESAR. The values give the expected impacts on the baseline situation.

Where an operational change is expected to increase a risk but it is intended to prevent this resulting in an increase in accident precursors by mitigation means, then the SAC will state that no change in the frequency of the accident precursor will result.

D.4 Closing the loop between the Solution and PJ19.3 Performance Framework

Once the SAC are defined at the level of the Solution, and more particularly in case they differ from the ones derived from PJ19.3, a feed back to the SESAR Performance Framework is required in order to ensure that overall SESAR Safety Performance Ambition is still met.

This feedback is done by ensuring information related to SAC (among other relevant information for each Solution) is entered in the Safety Register (see **Guidance H**) so PJ19.3 can check it periodically and reassess the Safety Validation Targets as relevant in the frame of PJ19.3.

D.5 Example for SESAR 1 OFA 01.02.01 Airport Safety Nets in Step 1

As per the allocation done within the SESAR Performance Framework, the OFA 01.02.01 "Airport Safety Nets" is expected to provide, for Step 1, an overall safety improvement of 4.9% (safety improvement meaning, as explained above, reduction of potential number of fatal accidents per year with respect to an hypothetical "do nothing case"). This improvement is decomposed as follows:

- 4.8% reduction of Runway Collision
- 0.1% reduction of Taxiway Collision

These values have been determined taking into account the traffic increase foreseen for Step 1 which is 14% with respect to the SESAR 1 baseline.

In order to obtain these safety benefits defined above, the following improvements are needed in the performance of the barriers of AIM listed here after:

Concerning Runway collision model:

- 2.5% improvement of barrier B3A: Runway Monitoring
- 10% improvement of barrier B3: Runway Conflict Prevention
- 17.5% improvement of barrier B2: ATC Runway Collision Avoidance
- 5% improvement of barrier B1: Pilot Runway Collision Avoidance

Concerning Taxiway collision model:

- 5% improvement of barrier B3: Taxiway Conflict Management
- 25% improvement of barrier B2: ATC Taxiway Collision Avoidance
- 5% improvement of barrier B1: Pilot Taxiway Collision Avoidance

By applying these improvements in those barriers the impact on the corresponding precursors are (on which the SACs are usually defined) for Runway collision model (the ones for the Taxiway are not shown here but are defined in the same way):

SACs are expressed with respect to the 'do nothing' case described above:

- SAC#1 : There shall be a reduction of 3 % of the Runway Incursions due to the introduction of the Airport Safety Nets concept Step 1, taking into account the traffic for Step 1.

- SAC#2 : There shall be a reduction of 7% of the Runway Conflicts due to the introduction of Airport Safety Nets concept Step1, taking into account the traffic for Step 1.
- SAC#3: There shall be a reduction of 27% of the Imminent Runway Collisions due to the introduction of Airport Safety Nets concept Step1, taking into account the traffic for Step 1.

The same SACs can also be expressed in an absolute way, as shown here after for SAC#1:

- SAC#1 : Runway Incursions shall be less than 3.2e-5 per fh with the introduction of the Airport Safety Nets concept Step 1, taking into account the traffic for Step 1.

As explained before, these SAC are the starting points for the Solution safety assessment. They need to be reviewed in detail by the Solution team, and split as necessary into the different Working Areas or projects being part of the same Solution.

In case a difference is found during this review, PJ19.3 has to be informed in order to update safety validation targets and recheck the satisfaction of the SESAR Safety Performance Ambition.

Guidance E On setting Safety Objectives (failure approach)

E.1 Introduction

This guidance is about setting ***safety objectives*** (***failure-approach***) in terms of a hazard's maximum tolerable frequency of occurrence / probability, derived from the severity of its effect. This is based on the usage of Hazard Severity Classification and Risk Classification Schemes (RCS). A Risk Classification Scheme (RCS) such as the one outlined in section A-2 of Appendix A to ESARR 4 is based on:

- an assessment of the effects a hazard may have on the safety of aircraft, as well as an assessment of the severity of those effects, using the severity classification scheme provided, and
- the determination of their tolerability, in terms of the hazard's maximum probability of occurrence, derived from the severity and the maximum probability of the hazard's effects.

However, experience has shown that a potential of misunderstanding by the user as to how this RCS was originally derived can lead to inappropriate use and incorrect Safety Objectives. If RCS are used, it is important that the user understands:

- at what level in the ATM System engineering hierarchy (i.e. hazards not always defined at the operational/service level), and within what scope (e.g. phase of flight), the values are intended to be applied (i.e. the level at which the operational hazards have to be defined);
- where the probability / frequency values used in the scheme came from and whether they are (still) valid (e.g. airport-operation-related hazards using schemes with field data from, say, an en-route environment);
- to what operational environment the values apply – e.g. type of airspace, traffic patterns, traffic density, spatial dimension, phase of flight, separation minima etc.; and
- how the aggregate risk, as specified in ESARR 4 for example, can be deduced from analysis of individual hazards, in restricted segments of the total system.

The Accident Incident Model (AIM) includes a set of incidents of different severities, which are precursors[1] of each accident category[2]. As such, AIM models contain built-in RCSs. These can be used to derive quantitative targets for such severities. The use of a common accident precursor based RCS (derived from AIM) would solve many of the underlying problems (mentioned above) existing in current RCS approaches when applied to a program as wide reaching as SESAR. Namely it would provide a common template across a wide range of projects based directly on accident modelling. In more details, AIM-based RCSs offer a number of advantages over many risk-classification schemes as follows:

- they are based on real, historical accident and incident data;
- they can provide valid safety targets at many levels in the ATM system hierarchy and for specific phases of flight; and
- they can provide safety targets that take account of future changes to the ATM system and / operational environment, rather than being tied to the past / current situation.

AIM-Based RCSs are determined on the basis of a risk based approach as they are based on the conditioned probabilities / effectiveness already contained in AIM.

The process for setting Safety Objectives (failure approach) based on these RCSs is described in the following sections below.

[1] *A precursor is an occurrence that remained an incident but that might recur in different conditions and become an accident (Skybrary).*

[2] More information is available in Guidance D and in *[references to AIM model from 16.1.1].*

E.2 Process for Setting Safety Objectives (failure approach)

The following steps apply for setting safety objectives for the failure approach using an accident precursor based Risk Classification Scheme:

1. Identification of operational hazards (see detail in E2.1).
2. Determine the relevant severity class to the hazards (see detail E2.2)
3. Calculate the corresponding safety objective (see detail E2.3)

Two examples of how to apply this process is presented in section E2.4.

E.2.1 Operational Hazards identification

The Operational hazards, as per SRM (definition 'n', SRM, section 10.3) definition, shall be identified at the level of the Operational services i.e. a level that is independent of the physical architecture of the system and is related to the failure of an operational service. Note that we refer here to "system-generated" hazards, which result from failure of the ATM/ANS functional system affected by the Change.

An initial way for identifying these hazards is based on the analysis of the corresponding operational services (ref to assurance activity) and by considering, for each safety objective from the success approach (ref to assurance activity), what would happen if the objectives were not satisfied (i.e. negate the safety objectives derived with the success approach),

Then, this list of "system-generated" hazards is to be completed / updated using standard methods (e.g. HAZOP, HAZID, SWIFT (Structured What-If Technique) etc.) as per SAM FHA, mainly through a dedicated FHA workshop (see Reference 4 in the SRM, section 10.1). It has to be noted that those methods may require additional "compilation" in order to define the hazards at the appropriate service level as mentioned above. Alternatively, the Operational Hazard Assessment (OHA) process from ED-78A may also be adapted for the purpose.

The standard questions related to the HAZOP/HAZID/etc. processes at a FHA workshop should be enriched considering the following principles from Resilience Engineering (**Guidance I**):

- Work-as-done (Resilience Principle # 1).
- Margins and adaptive capacity (Resilience Principle # 5)
- Coupling and interactions cascading (Resilience Principle # 6)

In order to optimise resources and time, the FHA workshop should be organised jointly with HP experts. Thus, questions from the HP Issue Analysis are considered (see Guidance K).

E.2.2 Determination of the corresponding severity class

Once the hazards are identified, the next step is to assess their operational effects by determining the impact of each of them in the relevant AIM model. Potential causes of the assessed hazard affecting several barriers at the same time are to be taken into account for determining the operational consequence of that hazard.

The Severity Class (SC) for a hazard is then determined based on the last barrier negatively impacted by the corresponding hazard (taking into account potential common causes as mentioned above), i.e. stopping at the level of the precursor for which the subsequent non-impacted barrier will work nominally. The SC is to be determined as per the Severity Classification Scheme(s) from Guidance **E.3**.

If a hazard impacts several barriers or several accident models (such as MAC & CFIT for example) then safety objectives should be calculated as defined in Guidance **E.2.3** below and the most demanding objectives should be retained.

Using AIM supports consistency by choosing the consequences for a hazard and, consecutively, the associated severity class. However, despite the use of the models, this process still needs operational experts in the determination of effects and severity classes, as in the identification of hazards (see E

2.1). Operational experts are then to be involved in this assessment (preferably during the FHA workshop mentioned in Guidance **E.2.1**).

E.2.3 Quantitative definitions for the safety objectives

E.2.3.1 Presentation of the Method

Safety objectives (according to the failure approach) limit the frequency of occurrence or probability on demand of system-generated hazards (defined at the level of the Operational services) to keep risks in line with the Safety Criteria (SAC).

Safety objectives are calculated based on the severity of the impact of the hazard (as explained in Guidance E.2.2) and the corresponding maximum tolerable frequency of occurrence for this severity class as defined in the Risk Classification Schemes presented in Guidance **E.4.**

Before indicating how to calculate safety objectives, it is worth noting that:

1. The entire “risk budget” for operational hazards at a certain level has to be distributed amongst all the operational hazards that affect the barrier. It is therefore necessary to divide the overall risk budget by the number of operational hazards (N) affecting a barrier (i.e. belonging to the same severity class). This requires an estimate of the maximum number of operational hazards (these numbers are derived in E.2.3.3 below).
2. The impact of a hazard can be a single conflict (e.g. Failure to prevent a planned conflict becoming a tactical conflict) or it can have an impact on several aircraft or even on all those in a sector or in an entire operation. Conversely, it can even affect one single aircraft (e.g. in case of CFIT). Ideally, the safety objective even takes this into account and therefore an Impact Modification factor (IM) is employed. Further information in defining the IM to fit special situations is further detailed in the paragraph E.2.3.2 below.

The result of this is that safety objectives (SO) that are derived using this method are linked to a set of accident models representing the baseline operational risks. The SO directly represent contributions to barrier failures and are consistent with the approach used for Safety Criteria in the SRM.

The method to calculate SO for a given hazard is as follows:

$$SO = \frac{MTFoO_{relevant\_severity\_class}}{N \times IM}$$

where:

- $MTFoO_{relevant\_severity\_class}$ stands for the Maximum Tolerable Frequency of Occurrence being the maximum probability of the hazard’s effect as defined in **Table 6** to **Table 9** in Guidance **E.4**.
- N is the overall number of operational hazards for a given severity class at a given barrier as obtained from **Table 5** in **E.4** below.
- IM is the Impact Modification factor to take account of additional information regarding the operational effect of the hazard, in particular related to the number of aircraft exposed to the operational hazard. See more detail here below.

E.2.3.2 On the Impact Modification Factor (IM)

The way the AIMs have been developed and the Severity Classes have been derived from them do not directly take into account the number of aircraft exposed to a hazard. In reality, one might wish to allocate a more stringent Safety Objective to a situation where multiple aircraft are affected, compared to the same situation concerning one or few aircraft. This is accounted for through the calculation of the Safety Objective, i.e. through the outcome frequency / probability on demand affected with a modification factor called Impact Modification factor (IM) related to the number of aircraft exposed to the hazard.

As a general rule, in case a hazard involves multiple (many aircraft) then an impact of one order of magnitude should be considered i.e. use IM=10 (instead of the reference value IM = 1 corresponding to the case of one or only few aircraft involved). However, the IM might be more finely estimated based on operational expert judgment.

The IM can also be used to account for cases where the last barrier negatively impacted by the corresponding hazard is not completely broken, but its efficiency is only reduced to some extent. A value IM < 1 needs to be applied in such cases (instead of the reference value IM=1 corresponding to the case where the barrier is completely lost). That value shall be carefully commensurate with the reduction in the efficiency of the safety barrier to be estimated based on operational expert judgment.

Another element that the IM can also account for is the exposure time before the hazard detection and subsequent mitigation; the longer the exposure time, the higher the risk is for which a greater IM may be more appropriate.

E.2.3.3 Estimation of the number of hazards (N) for each severity class

To generate the safety objectives it is necessary to make an estimation of the total number of contributing operational hazards for each severity class thereby appropriately managing the aggregate risk which is crucial in SESAR.

Currently, this estimation is based on operational judgment and previous experience in safety assessment[3]. Within a given accident type, the number of hazards N for each severity class depends on the nature of the barriers and the induced events in input to the barriers. As an example, the potential number of hazards related to the STCA barrier (within MAC model) is not the same as the ones related to a barrier as Traffic Coordination and Synchronisation which encompasses several ATM system functions in it.

Table 5 provides the current values of N to be used in the calculation of Safety Objectives as per the process explained in section E.2.

CAUTION	Values in **Table 5** could be refined as the result of maintaining the SESAR Safety Register (see **Guidance H**) with hazards and associated severity classifications from the various safety assessments across the work programme. As a consequence, it may be subject to further refinements.

Severity Class	***Number of hazards per Severity Class per Accident Type***			
	MAC (ER&TMA)	***RWY Coll.***	***CFIT***	***TWY Coll.***
SC1	1	1	5	1
SC2	n/a	n/a	10	n/a
SC2a	5	5	n/a	5
SC2b	10	10	n/a	10
SC3	25	20	n/a	20
SC3a	n/a	n/a	50	n/a

[3] However, in SESAR the validity of this judgment is continuously assessed through the usage of the Safety Register as explained in the 'Caution' message below.

Severity Class	***Number of hazards per Severity Class per Accident Type***			
	MAC (ER&TMA)	***RWY Coll.***	***CFIT***	***TWY Coll.***
SC3b	n/a	n/a	50	n/a
SC4	n/a	30	n/a	30
SC4a	30	n/a	n/a	n/a
SC4b	30	n/a	n/a	n/a
SC5	100	100	n/a	100

Table 5: Maximum Hazard Numbers per Severity Class

E.2.4 Examples of setting Safety Objectives

The examples provided in this section are based on the safety assessment done in the frame of two SESAR 1 OFAs. Note that as these assessments were performed using previous version of this guidance, they have been updated here taking into account the latest development of the SO setting process and of the Risks Classifications Schemes.

Example from OFA04.01.05 – i4D + CTA

More information related to this example is available in [i4D&CTA (OFA04.01.05) Safety Assessment Report (SAR) Ed 00.02.00]

Hazard description

The following hazard was identified in the safety assessment done by P5.6.1 & 4.3 within the OFA:

> HAZARD: Incorrect trajectory synchronization induces tactical conflict by lateral deviation in current sector

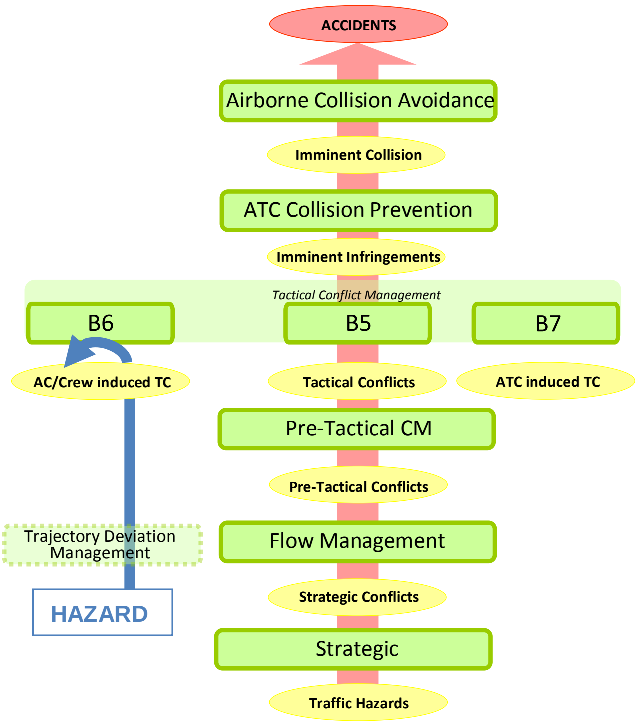
This operational hazard is caused by situations where airborne and ground trajectories are not or wrongly synchronized, not timely mitigated by a consistency check (via next Extended Projected Profile EPP downlink) or by a conformance monitoring tool alert, which involve an aircraft lateral deviation from the trajectory expected by ATCO_EXE with other aircraft in potential conflict in the proximity.

Hazard assessment – Mitigation Means

The assessment of this hazard was done using the simplified model of Mid-Air Collision (see section E3.1 **Figure 5**). Once this hazard has occurred, the ATC_EXE would detect the conflict via radar monitoring and undertake appropriate tactical conflict resolution (B6 which is not impacted).

Hazard within AIM

This operational hazard is the collection of a sub-set of scenarios leading to the pre-cursor MF6.1: Crew / Aircraft induced conflict". Following scheme positions this operational hazard within the MAC-ER model:



Assigned Severity Class

The operational effect of this hazard is then a situation where an imminent infringement coming from a crew/aircraft induced conflict was prevented by tactical conflict management.

Consequently the severity allocated is MAC-SC4a as per **Table 6**.

Allocated Safety Objective

The corresponding safety objective to this hazard, based on the assessment explained above is then:

> **SAFETY OBJECTIVE:** The likelihood that incorrect trajectory synchronization induces tactical conflict by lateral deviation in current sector shall be no more than 2e-04 per sector operational hour.

It has been calculated applying the formula in E2.3, using the following values:

> MTFoF $_{\text{MAC-SC4a}}$ = 1E-03 [per fh] as per **Table 6**.
>
> N = 30 as per **Table 5**
>
> IM = 1 as no particular correction was required related to: (a) number of aircraft affected or (b) exposure time before detection or (c) alteration of probability of last barrier negatively impacted by the hazard.

With these values a SO of 3.3E-05 [per fh] is obtained. It can be converted per sector operational hour using the assumption of 6 flight hours controlled per one sector operational hour:

> SO= 3.3E-05 * 6 = 2E-04 [per sector operational hour]

Example from OFA06.03.01 – Remote Tower

More information related to this example is available in [SAR for Single Remote Tower – 00.01.01 March 2014].

Hazard description

The following operational hazard was identified during the safety assessment of Remote Tower for a Single Aerodrome (performed by P6.9.3 within this OFA):

> **HAZARD**: Remote ATC incorrectly manage runway crossing for a vehicle or an aircraft

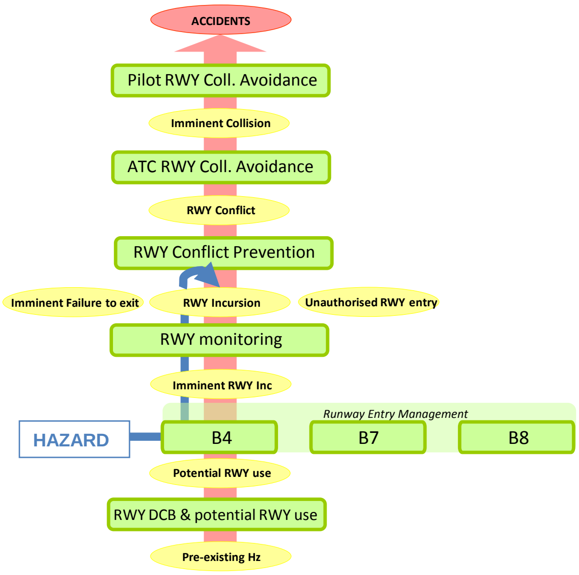
This hazard is related to a failure of the service ATC runway entry management (covered by Barrier 4 in the Runway Collision model). It addresses the fact that ATC provides inappropriate instructions to a vehicle or and aircraft resulting in a potential runway incursion.

Hazard assessment – Mitigation Means

The assessment of the hazard was done using the simplified model for Runway Collision (see section E3.2). While B4 is the last barrier negatively impacted by the hazard, it was felt during the assessment workshop that the subsequent Runway Monitoring barrier was not efficient enough to prevent a potential runway incursion as a result of this specific hazard (since induced by ATC). As the runway could be already occupied / used for another operation when the hazard occurs, the failure of the Runway Monitoring barrier could then lead to a potential conflict on the runway. In that case, the "ATC collision prevention" barrier will most likely detect and solve the conflict.

Positioning the Hazard within AIM

This operational hazard is the collection of a sub-set of scenarios leading to the pre-cursor RP3: Runway Incursion. Following scheme positions this operational hazard within the Runway Collision model:



Severity Class Assignment

The result of the assessment was that the hazard can lead to a situation where an encounter between a vehicle or and aircraft on the runway and another a/c approaching occurs but ATC runway Collision avoidance prevents it to become an Imminent Runway Collision.

Thus the allocated severity class is RWY-SC3 (Runway Incursion) as per RCS in **Table 7**.

Allocated Safety Objective

The corresponding safety objective to this hazard, based on the assessment explained above is then:

> **SAFETY OBJECTIVE**: The likelihood that Remote ATC incorrectly manage runway crossing for a vehicle or an aircraft shall be no more than 5e-7 per movement.

It has been calculated applying the formula in E2.3, using the following values:

> MTFoF $_{\text{RWY-SC3}}$ = 1e-5 as per **Table 7**

N = 20 as per **Table 5**

IM = 1 as no particular correction was required related to: (a) number of aircraft affected or (b) exposure time before detection or (c) alteration of probability of last barrier negatively impacted by the hazard).

E.3 Severity Classification Schemes

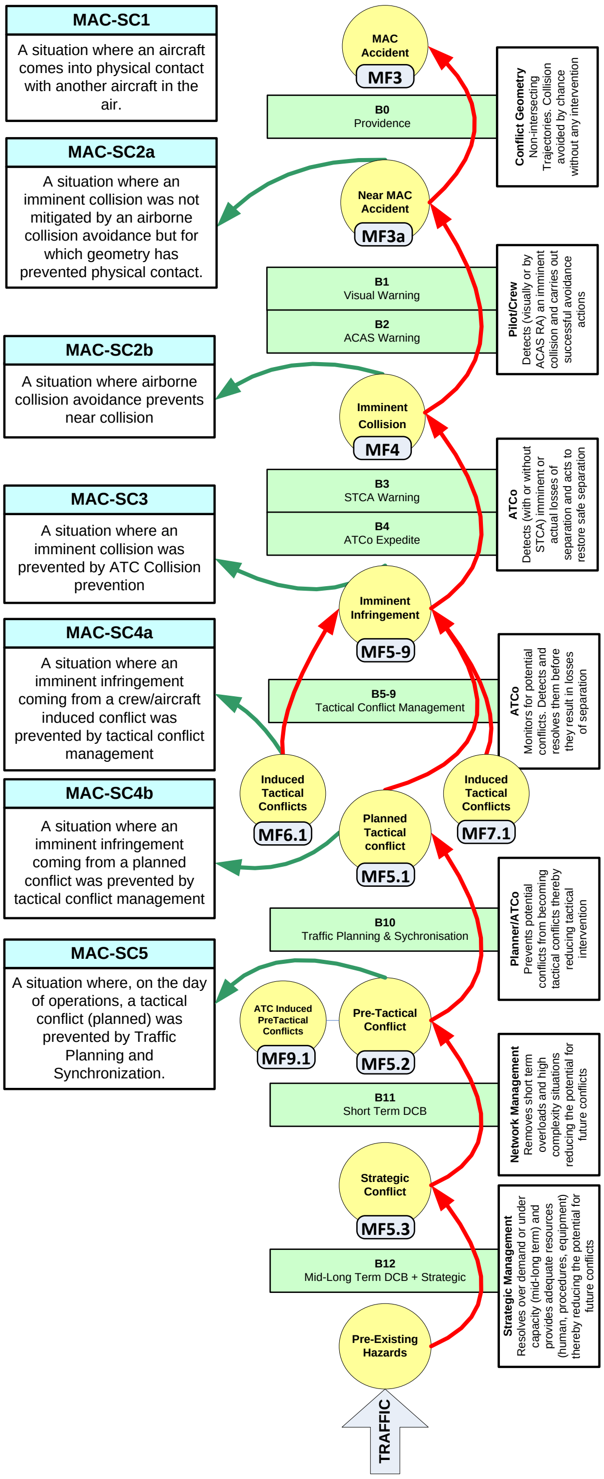
Diagrams in Guidance **E.3.1** to **E.3.4** show the Severity Classification Schemes for the following accident types covered by the AIM accident models:

- MAC accident (version v0.2a) – relating to for TMA and ER operations
- Runway Collision (version v0.2a)
- Taxiway Collision (version v0.2a)
- Controlled Flight Into Terrain (version v0.2)
- Wake Induced accident (version v1.5) – only relating to final approach operations
- Runway Excursion (version v0.3) – only relating to landing operations

All these models are part of the AIM release [AIM V10-3] (Ref 18).

The Severity Classification scheme for MAC Oceanic is still under development.

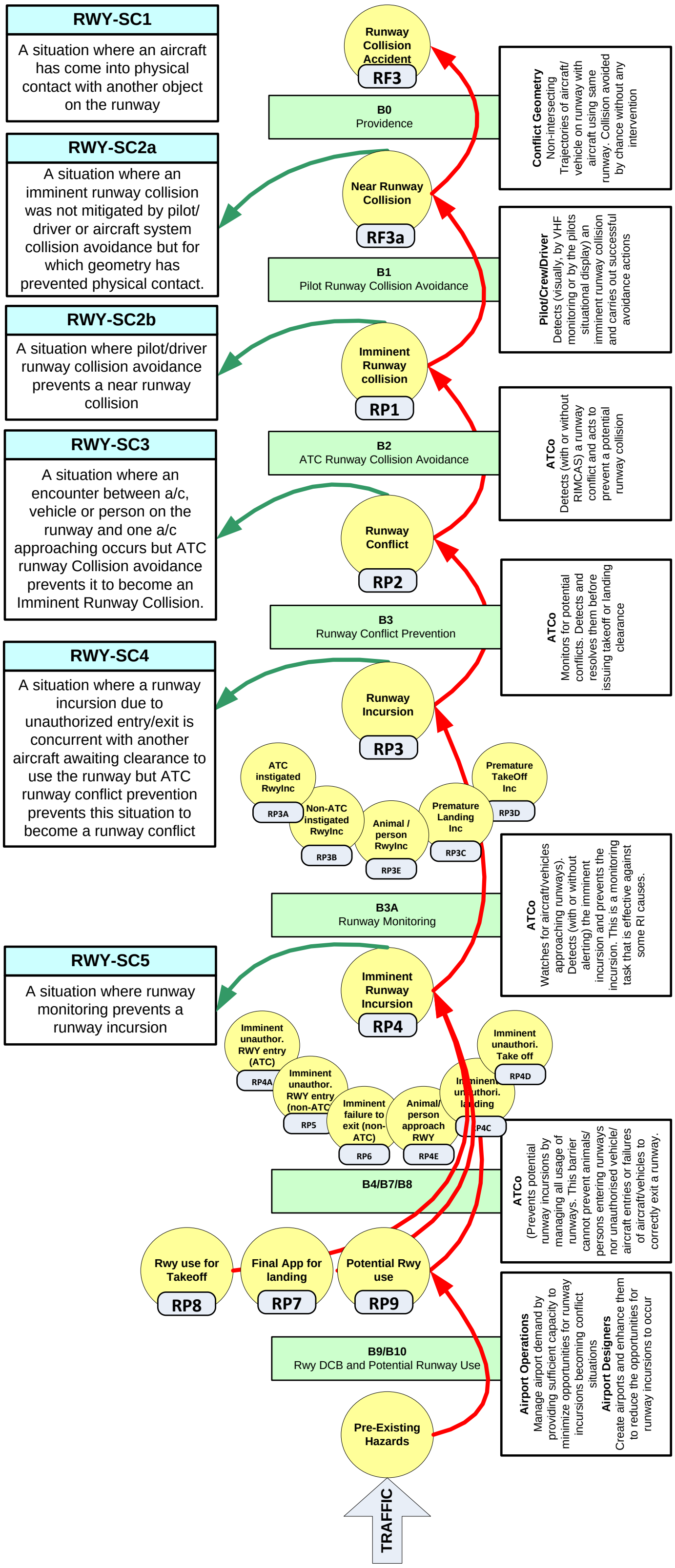
E.3.1 Severity Classification Scheme for MAC accident model


MAC-SC1
A situation where an aircraft comes into physical contact with another aircraft in the air.
MAC-SC2a
A situation where an imminent collision was not mitigated by an airborne collision avoidance but for which geometry has prevented physical contact.
MAC-SC2b
A situation where airborne collision avoidance prevents near collision
MAC-SC3
A situation where an imminent collision was prevented by ATC Collision prevention
MAC-SC4a
A situation where an imminent infringement coming from a crew/aircraft induced conflict was prevented by tactical conflict management
MAC-SC4b
A situation where an imminent infringement coming from a planned conflict was prevented by tactical conflict management
MAC-SC5
A situation where, on the day of operations, a tactical conflict (planned) was prevented by Traffic Planning and Synchronization.
MAC Accident
MF3
B0
Providence
Near MAC Accident
MF3a
B1
Visual Warning
B2
ACAS Warning
Imminent Collision
MF4
B3
STCA Warning
B4
ATCo Expedite
Imminent Infringement
MF5-9
B5-9
Tactical Conflict Management
Induced Tactical Conflicts
MF6.1
Planned Tactical conflict
MF5.1
Induced Tactical Conflicts
MF7.1
B10
Traffic Planning & Sychronisation
ATC Induced PreTactical Conflicts
MF9.1
Pre-Tactical Conflict
MF5.2
B11
Short Term DCB
Strategic Conflict
MF5.3
B12
Mid-Long Term DCB + Strategic
Pre-Existing Hazards
TRAFFIC
Conflict Geometry
Non-intersecting Trajectories. Collision avoided by chance without any intervention
Pilot/Crew
Detects (visually or by ACAS RA) an imminent collision and carries out successful avoidance actions
ATCo
Detects (with or without STCA) imminent or actual losses of separation and acts to restore safe separation
ATCo
Monitors for potential conflicts. Detects and resolves them before they result in losses of separation
Planner/ATCo
Prevents potential conflicts from becoming tactical conflicts thereby reducing tactical intervention
Network Management
Removes short term overloads and high complexity situations reducing the potential for future conflicts
Strategic Management
Resolves over demand or under capacity (mid-long term) and provides adequate resources (human, procedures, equipment) thereby reducing the potential for future conflicts

Severity Class Scheme for Mid-air Collision
AIM MAC BARRIER MODEL (TMA&ER) v0.2a

Figure 5: Severity Classifications for the MAC model

E.3.2 Severity Classification Scheme for Runway Collision model


Runway Collision Accident
RF3
B0
Providence
Near Runway Collision
RF3a
B1
Pilot Runway Collision Avoidance
Imminent Runway collision
RP1
B2
ATC Runway Collision Avoidance
Runway Conflict
RP2
B3
Runway Conflict Prevention
Runway Incursion
RP3
ATC instigated RwyInc
RP3A
Non-ATC instigated RwyInc
RP3B
Animal / person RwyInc
RP3E
Premature Landing Inc
RP3C
Premature TakeOff Inc
RP3D
B3A
Runway Monitoring
Imminent Runway Incursion
RP4
Imminent unauthor. RWY entry (ATC)
RP4A
Imminent unauthor. RWY entry (non-ATC)
RP5
Imminent failure to exit (non-ATC)
RP6
Animal/ person approach RWY
RP4E
Imminent unauthori. landing
RP4C
Imminent unauthori. Take off
RP4D
B4/B7/B8
Rwy use for Takeoff
RP8
Final App for landing
RP7
Potential Rwy use
RP9
B9/B10
Rwy DCB and Potential Runway Use
Pre-Existing Hazards
TRAFFIC

RWY-SC1
A situation where an aircraft has come into physical contact with another object on the runway

RWY-SC2a
A situation where an imminent runway collision was not mitigated by pilot/ driver or aircraft system collision avoidance but for which geometry has prevented physical contact.

RWY-SC2b
A situation where pilot/driver runway collision avoidance prevents a near runway collision

RWY-SC3
A situation where an encounter between a/c, vehicle or person on the runway and one a/c approaching occurs but ATC runway Collision avoidance prevents it to become an Imminent Runway Collision.

RWY-SC4
A situation where a runway incursion due to unauthorized entry/exit is concurrent with another aircraft awaiting clearance to use the runway but ATC runway conflict prevention prevents this situation to become a runway conflict

RWY-SC5
A situation where runway monitoring prevents a runway incursion

Conflict Geometry
Non-intersecting Trajectories of aircraft/ vehicle on runway with aircraft using same runway. Collision avoided by chance without any intervention

Pilot/Crew/Driver
Detects (visually, by VHF monitoring or by the pilots situational display) an imminent runway collision and carries out successful avoidance actions

ATCo
Detects (with or without RIMCAS) a runway conflict and acts to prevent a potential runway collision

ATCo
Monitors for potential conflicts. Detects and resolves them before issuing takeoff or landing clearance

ATCo
Watches for aircraft/vehicles approaching runways). Detects (with or without alerting) the imminent incursion and prevents the incursion. This is a monitoring task that is effective against some RI causes.

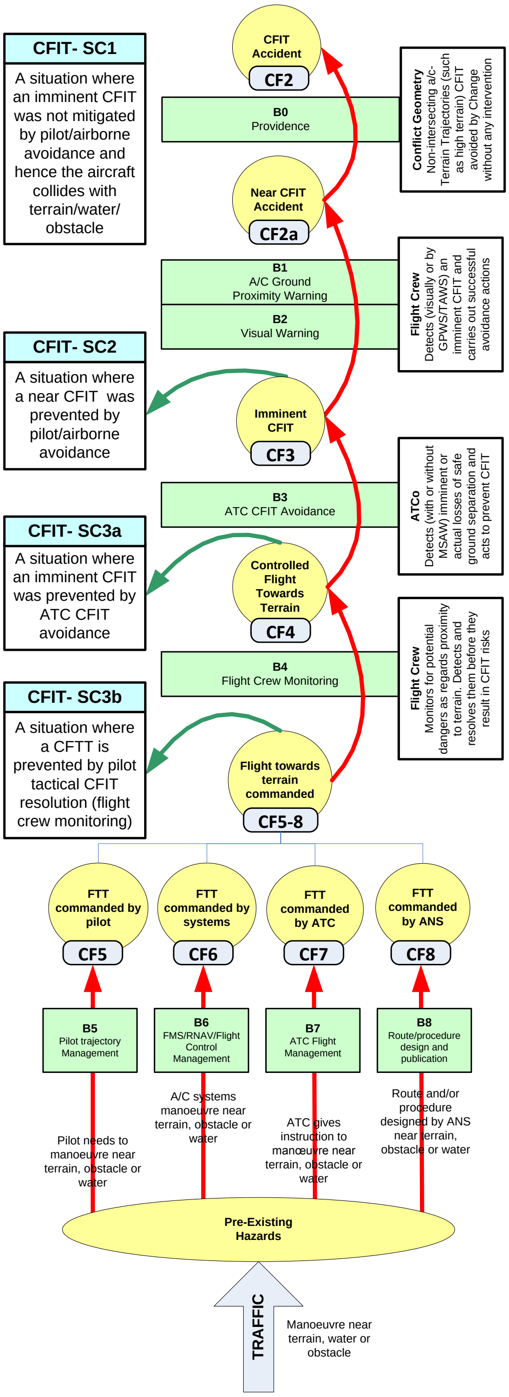
ATCo
(Prevents potential runway incursions by managing all usage of runways. This barrier cannot prevent animals/ persons entering runways nor unauthorised vehicle/ aircraft entries or failures of aircraft/vehicles to correctly exit a runway.

Airport Operations
Manage airport demand by providing sufficient capacity to minimize opportunities for runway incursions becoming conflict situations
Airport Designers
Create airports and enhance them to reduce the opportunities for runway incursions to occur

Severity Class Scheme for Runway Collision
AIM RWY BARRIER MODEL v0.2a

Figure 6: Severity Classifications for the RWY accident model

E.3.3 Severity Classification Scheme for CFIT accident model

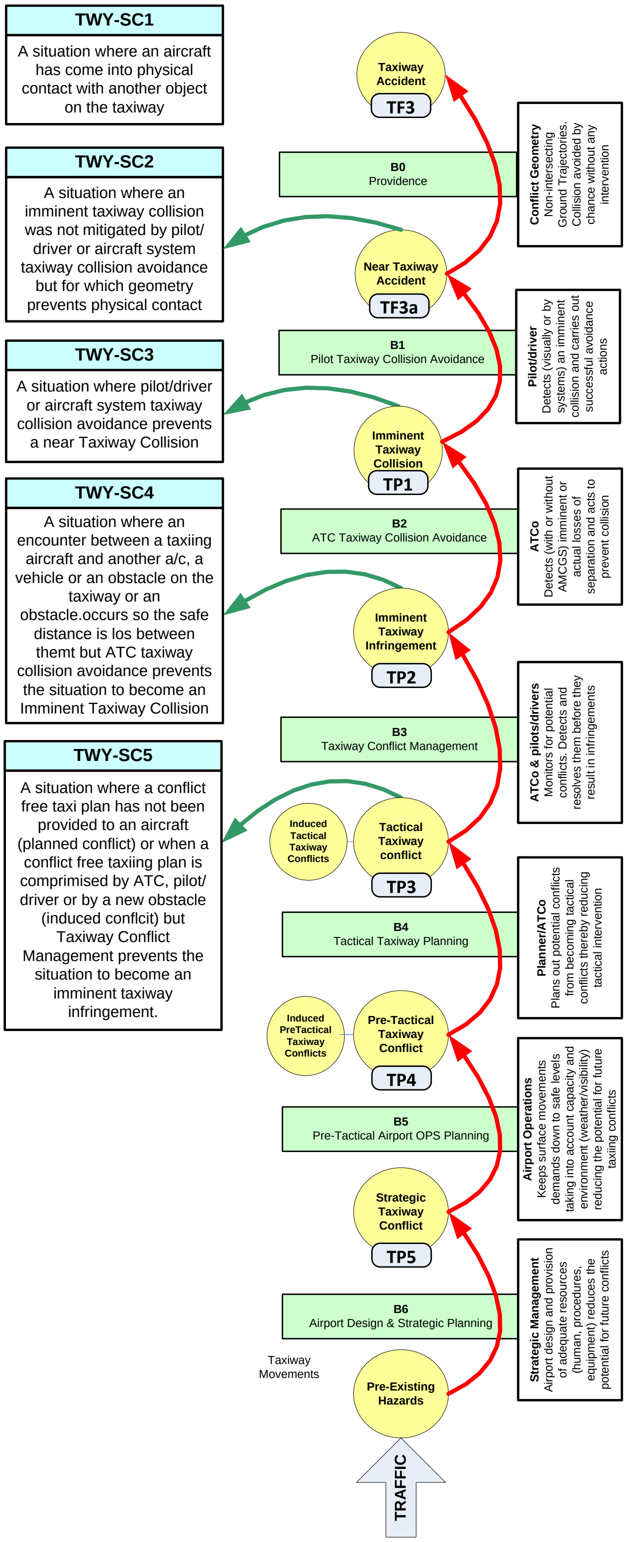

CFIT- SC1
A situation where an imminent CFIT was not mitigated by pilot/airborne avoidance and hence the aircraft collides with terrain/water/ obstacle
CFIT Accident
CF2
B0
Providence
Conflict Geometry
Non-intersecting a/c-Terrain Trajectories (such as high terrain) CFIT avoided by Change without any intervention
Near CFIT Accident
CF2a
B1
A/C Ground Proximity Warning
B2
Visual Warning
Flight Crew
Detects (visually or by GPWS/TAWS) an imminent CFIT and carries out successful avoidance actions
CFIT- SC2
A situation where a near CFIT was prevented by pilot/airborne avoidance
Imminent CFIT
CF3
B3
ATC CFIT Avoidance
ATCo
Detects (with or without MSAW) imminent or actual losses of safe ground separation and acts to prevent CFIT
CFIT- SC3a
A situation where an imminent CFIT was prevented by ATC CFIT avoidance
Controlled Flight Towards Terrain
CF4
B4
Flight Crew Monitoring
Flight Crew
Monitors for potential dangers as regards proximity to terrain. Detects and resolves them before they result in CFIT risks
CFIT- SC3b
A situation where a CFTT is prevented by pilot tactical CFIT resolution (flight crew monitoring)
Flight towards terrain commanded
CF5-8
FTT commanded by pilot
CF5
FTT commanded by systems
CF6
FTT commanded by ATC
CF7
FTT commanded by ANS
CF8
B5
Pilot trajectory Management
B6
FMS/RNAV/Flight Control Management
B7
ATC Flight Management
B8
Route/procedure design and publication
Pilot needs to manoeuvre near terrain, obstacle or water
A/C systems manoeuvre near terrain, obstacle or water
ATC gives instruction to manœuvre near terrain, obstacle or water
Route and/or procedure designed by ANS near terrain, obstacle or water
Pre-Existing Hazards
TRAFFIC
Manoeuvre near terrain, water or obstacle

Severity Class Scheme for CFIT

AIM CFIT BARRIER MODEL v0.2

Figure 7: Severity Classification Scheme for the CFIT accident model

E.3.4 Severity Classification Scheme for Taxiway accident model



TWY-SC1

A situation where an aircraft has come into physical contact with another object on the taxiway

TWY-SC2

A situation where an imminent taxiway collision was not mitigated by pilot/ driver or aircraft system taxiway collision avoidance but for which geometry prevents physical contact

TWY-SC3

A situation where pilot/driver or aircraft system taxiway collision avoidance prevents a near Taxiway Collision

TWY-SC4

A situation where an encounter between a taxiing aircraft and another a/c, a vehicle or an obstacle on the taxiway or an obstacle.occurs so the safe distance is los between themt but ATC taxiway collision avoidance prevents the situation to become an Imminent Taxiway Collision

TWY-SC5

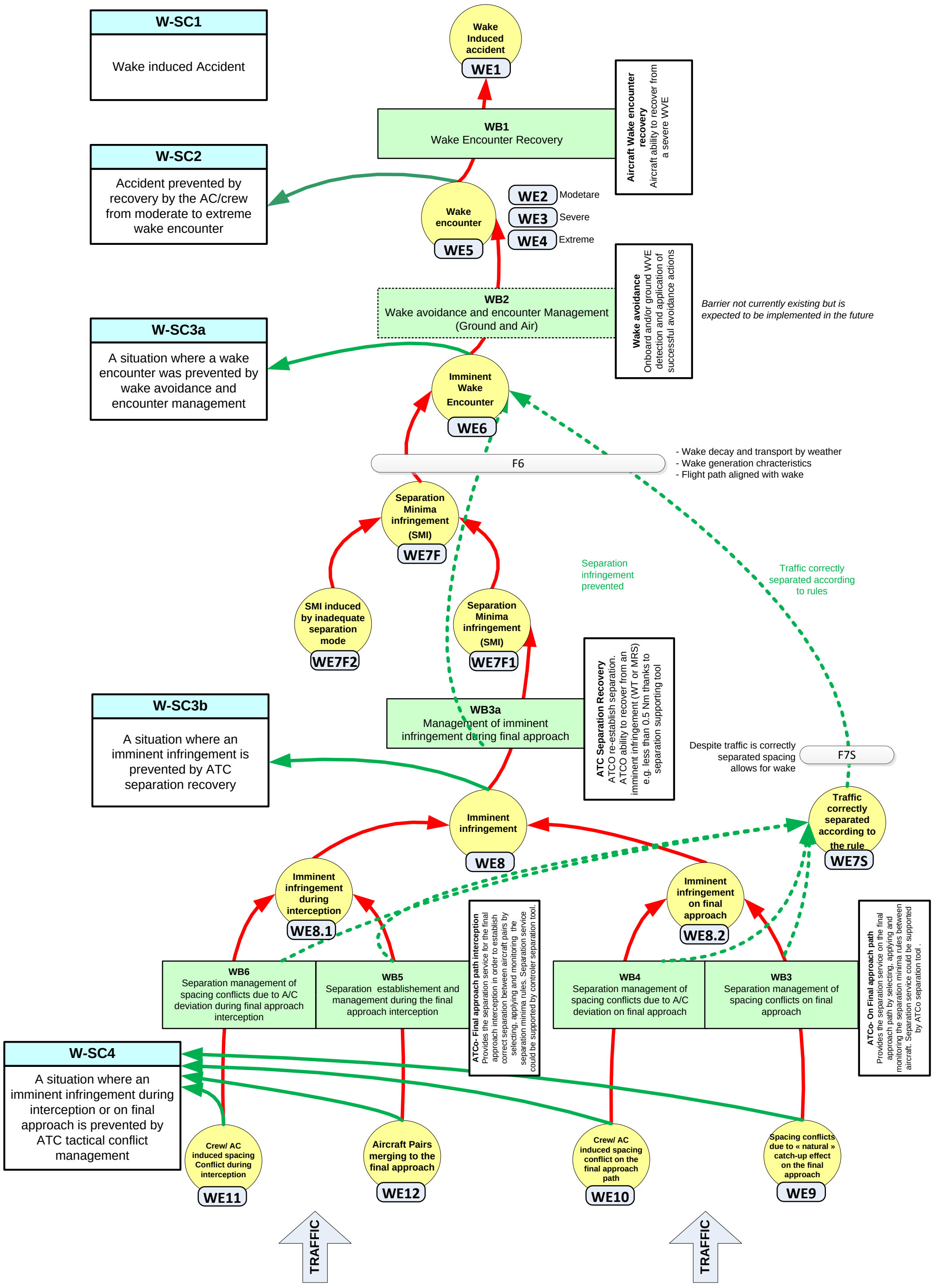
A situation where a conflict free taxi plan has not been provided to an aircraft (planned conflict) or when a conflict free taxiing plan is comprimised by ATC, pilot/ driver or by a new obstacle (induced conflcit) but Taxiway Conflict Management prevents the situation to become an imminent taxiway infringement.

Taxiway Accident
TF3
B0
Providence
Conflict Geometry
Non-intersecting Ground Trajectories. Collision avoided by chance without any intervention
Near Taxiway Accident
TF3a
B1
Pilot Taxiway Collision Avoidance
Pilot/driver
Detects (visually or by systems) an imminent collision and carries out successful avoidance actions
Imminent Taxiway Collision
TP1
B2
ATC Taxiway Collision Avoidance
ATCo
Detects (with or without AMCGS) imminent or actual losses of separation and acts to prevent collision
Imminent Taxiway Infringement
TP2
B3
Taxiway Conflict Management
ATCo & pilots/drivers
Monitors for potential conflicts. Detects and resolves them before they result in infringements
Induced Tactical Taxiway Conflicts
Tactical Taxiway conflict
TP3
B4
Tactical Taxiway Planning
Planner/ATCo
Plans out potential conflicts from becoming tactical conflicts thereby reducing tactical intervention
Induced PreTactical Taxiway Conflicts
Pre-Tactical Taxiway Conflict
TP4
B5
Pre-Tactical Airport OPS Planning
Airport Operations
Keeps surface movements demands down to safe levels taking into account capacity and environment (weather/visibility) reducing the potential for future taxiing conflicts
Strategic Taxiway Conflict
TP5
B6
Airport Design & Strategic Planning
Strategic Management
Airport design and provision of adequate resources (human, procedures, equipment) reduces the potential for future conflicts
Taxiway Movements
Pre-Existing Hazards
TRAFFIC

Severity Class Scheme for Taxiway Collision
AIM TWYCol BARRIER MODEL v0.2a

Figure 8: Severity Classifications for the Taxiway accident model

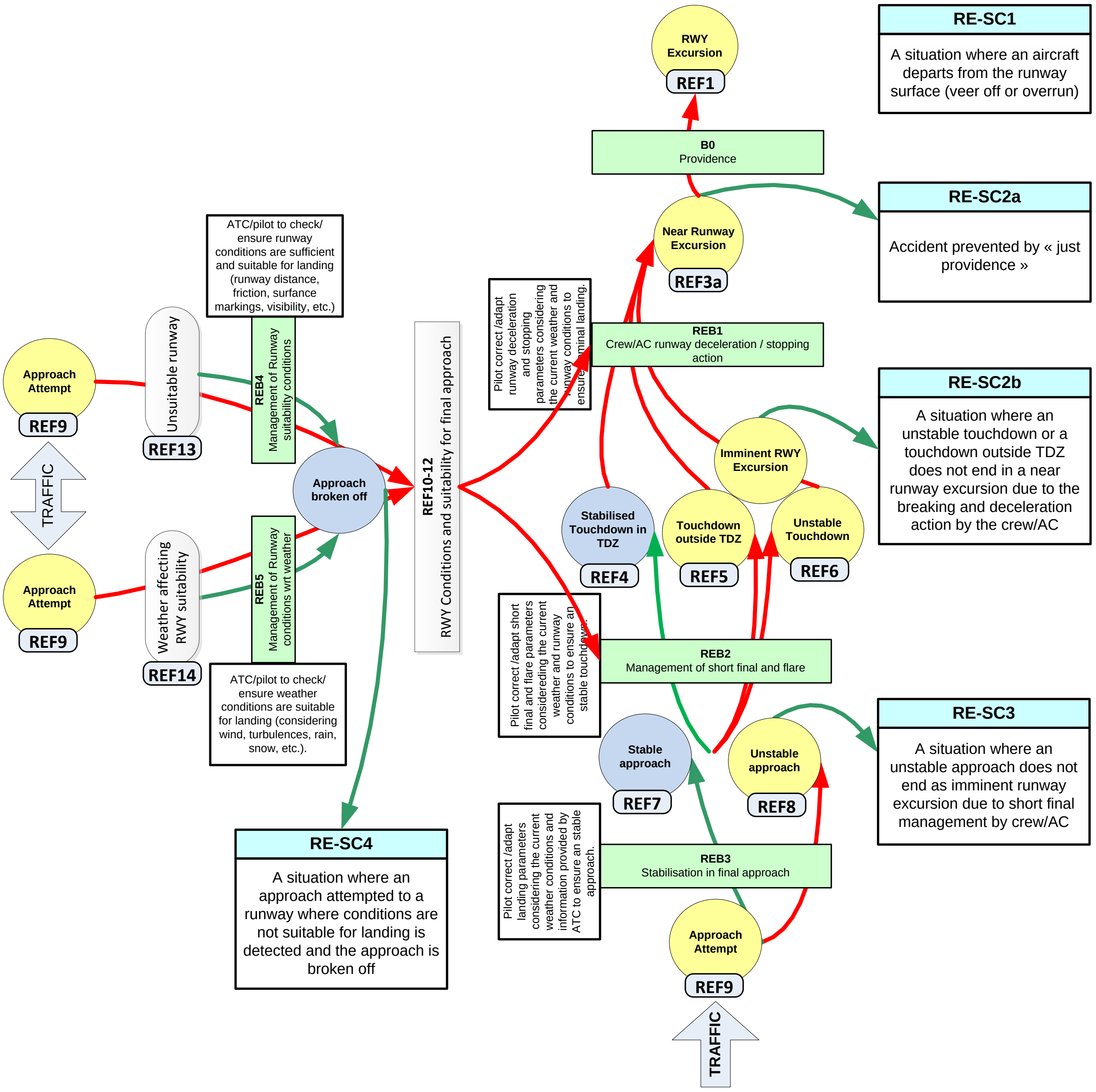
E.3.5 Severity Classification Scheme for Wake Induced accident model


W-SC1
Wake induced Accident
W-SC2
Accident prevented by recovery by the AC/crew from moderate to extreme wake encounter
W-SC3a
A situation where a wake encounter was prevented by wake avoidance and encounter management
W-SC3b
A situation where an imminent infringement is prevented by ATC separation recovery
W-SC4
A situation where an imminent infringement during interception or on final approach is prevented by ATC tactical conflict management
Wake Induced accident
WE1
WB1
Wake Encounter Recovery
Aircraft Wake encounter recovery
Aircraft ability to recover from a severe WVE
Wake encounter
WE5
WE2 Modetare
WE3 Severe
WE4 Extreme
WB2
Wake avoidance and encounter Management (Ground and Air)
Wake avoidance
Onboard and/or ground WVE detection and application of successful avoidance actions
Barrier not currently existing but is expected to be implemented in the future
Imminent Wake Encounter
WE6
F6
- Wake decay and transport by weather
- Wake generation chracteristics
- Flight path aligned with wake
Separation Minima infringement (SMI)
WE7F
SMI induced by inadequate separation mode
WE7F2
Separation Minima infringement (SMI)
WE7F1
Separation infringement prevented
Traffic correctly separated according to rules
WB3a
Management of imminent infringement during final approach
ATC Separation Recovery
ATCO re-establish separation.
ATCO ability to recover from an imminent infringement (WT or MRS) e.g. less than 0.5 Nm thanks to separation supporting tool
Despite traffic is correctly separated spacing allows for wake
F7S
Traffic correctly separated according to the rule
WE7S
Imminent infringement
WE8
Imminent infringement during interception
WE8.1
Imminent infringement on final approach
WE8.2
WB6
Separation management of spacing conflicts due to A/C deviation during final approach interception
WB5
Separation establishement and management during the final approach interception
ATCo- Final approach path interception
Provides the separation service for the final approach interception in order to establish correct separation between aircraft pairs by selecting, applying and monitoring the separation minima rules. Separation service could be supported by controler separation tool.
WB4
Separation management of spacing conflicts due to A/C deviation on final approach
WB3
Separation management of spacing conflicts on final approach
ATCo- On Final approach path
Provides the separation service on the final approach path by selecting, applying and monitoring the separation minima rules between aircraft. Separation service could be supported by ATCo separation tool .
Crew/ AC induced spacing Conflict during interception
WE11
Aircraft Pairs merging to the final approach
WE12
Crew/ AC induced spacing conflict on the final approach path
WE10
Spacing conflicts due to « natural » catch-up effect on the final approach
WE9
TRAFFIC
TRAFFIC

Severity Class Scheme for final approach Wake Induced Accident
AIM WAKE BARRIER MODEL (Final Approach) v1.5

Figure 9: Severity Classifications for the Wake Induced accident model

E.3.6 Severity Classification Scheme for Runway Excursion model


RWY Excursion
REF1
RE-SC1
A situation where an aircraft departs from the runway surface (veer off or overrun)
B0
Providence
RE-SC2a
Accident prevented by « just providence »
Near Runway Excursion
REF3a
ATC/pilot to check/ ensure runway conditions are sufficient and suitable for landing (runway distance, friction, surface markings, visibility, etc.)
Pilot correct /adapt runway deceleration and stopping parameters considering the current weather and runway conditions to ensure nominal landing.
REB1
Crew/AC runway deceleration / stopping action
Approach Attempt
REF9
Unsuitable runway
REF13
REB4
Management of Runway suitability conditions
REF10-12
RWY Conditions and suitability for final approach
RE-SC2b
A situation where an unstable touchdown or a touchdown outside TDZ does not end in a near runway excursion due to the breaking and deceleration action by the crew/AC
Imminent RWY Excursion
TRAFFIC
Approach broken off
Stabilised Touchdown in TDZ
REF4
Touchdown outside TDZ
REF5
Unstable Touchdown
REF6
Approach Attempt
REF9
Weather affecting RWY suitability
REF14
REB5
Management of Runway conditions wrt weather
ATC/pilot to check/ ensure weather conditions are suitable for landing (considering wind, turbulences, rain, snow, etc.).
Pilot correct /adapt short final and flare parameters considereding the current weather and runway conditions to ensure an stable touchdown.
REB2
Management of short final and flare
RE-SC3
A situation where an unstable approach does not end as imminent runway excursion due to short final management by crew/AC
Stable approach
REF7
Unstable approach
REF8
RE-SC4
A situation where an approach attempted to a runway where conditions are not suitable for landing is detected and the approach is broken off
Pilot correct /adapt landing parameters considering the current weather conditions and information provided by ATC to ensure an stable approach.
REB3
Stabilisation in final approach
Approach Attempt
REF9
TRAFFIC

Severity Class Scheme for Runway Excursion (related to landing only)

AIM RWY EXC BARRIER MODEL (Landing) v0.3

Figure 10: Severity Classifications for the Runway Excursion model

E.4 AIM-based Risk Classification Schemes

This section provides Risk Classification schemes for the different accident types covered by the AIM accident models. They provide a barrier based risk classification with a decreasing “risk distance” as we approach the accident. In these schemes, a Severity Class is associated with a tolerable frequency of occurrence (*i.e.* a maximum tolerable frequency of occurrence of ATM contributing to safety occurrences); the more severe the effect of the hazard the less frequent the hazard shall occur.

The definition of “ATM contribution” includes accidents with causes that either are part of the ATM system (whether ground-based, space-based or airborne) or that ATM could reasonably have been expected to mitigate. In the present study, this means that any accident in the modelled categories would inevitably include an ATM involvement. Tables presented in Guidance **E.4.1** to **E.4.4** below include definitions for the hazardous situations. Cross-references to accident precursors in **Figure 5** to **Figure 8** above are made in the column ‘Operational Effect’. The Maximum Tolerable Frequency of occurrence (MTFoO) is expressed per flight hour (fh) or per flight (flt) /movement (mov) depending on the type of accident. The numbers in the RCSs for the different models are related to quantitative values contained in the relevant AIM models at precursors, barrier efficiencies and criteria levels for which (in particular, but not limited to) the 16.01.01 “Validation / Verification of the Accident Incident Model (AIM)” mentioned earlier provides full information.

!	Compared to the AIM probabilistic values for precursors, the figures in **Table 6** to **Table 9** below have been rounded to 10^{-X} granularity in order to facilitate their usage in practical applications. The impact of this rounding on the derived Safety Objectives and subsequently on the allocated Safety Requirements is negligible. The rounding to 10^{-x}enables[4] to render transparent both the evolutions in traffic as per Steps 1 and 2 in SESAR as well as the foreseen impacts of the various Solutions. As a consequence, the same RCS can be used unchanged for Step 1 and Step 2, irrespective of the traffic increase (as per SESAR Target) and foreseen ATM system changes (Solutions).

CAUTION	Values in E.4.1 to E4.5 below could be refined as the result of ongoing activities in 16.01.01 to enrich the dataset used by AIM. This approach is currently being validated on a number of pilot projects. As a consequence, it may be subject to further refinements.

The Risk Classification Schemes provided in this guidance are related to the following accident types and models:

- Mid Air Collision in TMA and En-Route (version v0.2a)
- Controlled Flight Into Terrain (version v0.2)
- Runway collision (version v0.2a)
- Taxiway Collision (version v0.2a)

All these models are part of the AIM release [AIM V10-3] (Ref 18).

The Risk Classification Schemes for MAC Oceanic, for Wake Induced accidents and for Runway Excursion will be provided once the corresponding AIM models will be more mature, in terms of quantification.

[4] An estimation of the impact of these factors in Step 1 and Step 2 was performed and the conclusion was that the resulting magnitude of the impact is commensurate with the magnitude involved by the rounding

E.4.1 RCS for MAC in En-route & TMA operational environments

Table 6 shows the maximum tolerable frequency of occurrence for each severity class related to MAC accidents as defined in Guidance **E.3.1**.

Note that due to the rounding of values, the same RCS is to be used for En route and TMA operations.

Severity Class	***Hazardous situation***	***Operational Effect***	***MTFoO [per fh]***
MAC-SC1	A situation where an aircraft comes into physical contact with another aircraft in the air.	Accident - Mid air collision (MF3)	1e-9
MAC-SC2a	A situation where an imminent collision was not mitigated by an airborne collision avoidance but for which geometry has prevented physical contact.	Near Mid Air Collision (MF3a)	1e-6
MAC-SC2b	A situation where airborne collision avoidance prevents near collision	Imminent Collision (MF4)	1e-5
MAC-SC3	A situation where an imminent collision was prevented by ATC Collision prevention	Imminent Infringement (MF5-8)	1e-4
MAC-SC4a	A situation where an imminent infringement coming from a crew/aircraft induced conflict was prevented by tactical conflict management	Tactical Conflict (crew/aircraft induced) (MF6.1)	1e-3
MAC-SC4b	A situation where an imminent infringement coming from a planned conflict was prevented by tactical conflict management	Tactical Conflict (planned) (MF5.1)	1e-2
MAC-SC5	A situation where, on the day of operations, a tactical conflict (planned) was prevented by Traffic Planning and Synchronization.	Pre tactical conflict (MF5.2)	1e-1

Table 6: Risk Classification Scheme for Mid Air Collision (TMA and En-Route)

E.4.2 RCS for Runway Collisions

Table 7 shows the maximum tolerable frequency of occurrence for each severity class related to Runway Collision accidents as defined in Guidance **E.3.2**.

Severity Class	***Hazardous situation***	***Operational Effect***	***MTFoO [per movt.]***
RWY-SC1	A situation where an aircraft has come into physical contact with another object on the runway	Accident - Runway Collision (RF3)	1e-8
RWY-SC2a	A situation where an imminent runway collision was not mitigated by pilot/driver or aircraft system collision avoidance but for	Near Runway Collision (RF3a)	1e-7

Severity Class	*Hazardous situation*	*Operational Effect*	*MTFoO [per movt.]*
	which geometry has prevented physical contact.		
RWY-SC2b	A situation where pilot/driver runway collision avoidance prevents a near runway collision	Imminent runway collision (RP1)	1e-6
RWY-SC3	A situation where an encounter between a/c, vehicle or person on the runway and one a/c approaching occurs but ATC runway Collision avoidance prevents it to become an Imminent Runway Collision.	Runway Conflict (RP2)	1e-5
RWY-SC4	A situation where a runway incursion due to unauthorized entry/exit is concurrent with another aircraft awaiting clearance to use the runway but ATC runway conflict prevention prevents this situation to become a runway conflict	Runway incursion (RP3)	1e-4
RWY-SC5	A situation where runway monitoring prevents a runway incursion	Imminent Runway incursion (RP4)	1e-4

Table 7: Risk Classification Scheme for Runway Collision related to Incursions

Note that the MTFoO values for severity RWY-SC4 and RWY-SC5 are the same. This is due to the relatively weak performance of the barrier between these two events, and the fact that figures from the AIM model have been rounded.

E.4.3 RCS for Controlled Flight Into Terrain

Table 8 shows the maximum tolerable frequency of occurrence for each severity class related to Controlled Flight Into Terrain as defined in Guidance **E.3.3**.

Severity Class	*Hazardous situation*	*Operational Effect*	*MTFoO [per flgt]*
CFIT-SC1	A situation where an imminent CFIT is not mitigated by pilot/airborne avoidance and hence the aircraft collides with terrain/water/ obstacle [note 1]	CFIT Accident (CF2) Near CFIT (CF2a)	1e-8
CFIT-SC2	A situation where a near CFIT is prevented by pilot/airborne avoidance	Imminent CFIT (CF3)	1e-6
CFIT-SC3a	A situation where an imminent CFIT is prevented by ATC CFIT avoidance	Controlled flight towards terrain (CF4)	1e-5
CFIT-SC3b	A situation where a controlled flight towards terrain is prevented by pilot tactical CFIT resolution (flight crew monitoring)	Flight towards terrain commanded (CF5-8)	1e-5

Table 8: Risk Classification Scheme for CFIT

[note 1] as per the CFIT model, the aircraft trajectory geometry does not allow to prevent the collision with terrain/water/ obstacle for a near CFIT. Thus Near CFIT is classified as an accident (severity class CFIT-SC1).

Note that the MTFoO values for severity CFIT-SC3a and CFIT-SC3b are the same. This is due to the relatively weak performance of the barrier between these two events, and the fact that figures from the AIM model have been rounded.

E.4.4 RCS for Taxiway Collisions

Table 9 shows the maximum tolerable frequency of occurrence for each severity class related to Taxiway Collision accidents as defined in Guidance **E.3.4**.

Severity Class	***Hazardous situation***	***Operational Effect***	***MTFoO [per movt.]***
TInc-SC1	A situation where an aircraft has come into physical contact with another object on the taxiway	Accident -Taxiway Collision (TF3)	1 e-7
TInc-SC2	A situation where an imminent taxiway collision was not mitigated by pilot/driver or aircraft system taxiway collision avoidance but for which geometry prevents physical contact.	Near Taxiway Collision TF3a	1 e-6
TInc-SC3	A situation where pilot/driver or aircraft system taxiway collision avoidance prevents a near Taxiway Collision	Imminent Taxiway Collision TP1	1 e-2
TInc-SC4	A situation where an encounter between a taxiing aircraft and another a/c, a vehicle or an obstacle on the taxiway or an obstacle.occurs so the safe distance is los between themt but ATC taxiway collision avoidance prevents the situation to become an Imminent Taxiway Collision	Imminent Taxiway infringement TP2	1e-1
TInc-SC5	A situation where a conflict free taxi plan has not been provided to an aircraft (planned conflict) or when a conflict free taxiing plan is comprimised by ATC, pilot/driver or by a new obstacle (induced conflcit) but Taxiway Conflict Management prevents the situation to become an imminent taxiway infringement.	Tactical Taxiway conflict TP3	1

Table 9: Risk Classification Scheme for Taxiway Collision

Guidance F On specifying ATM/ANS at the OSED level

F.1 Introduction

This Annex describes how to describe ATM/ANS at the OSED (Operational Service and Environment Description) level. Section **F.2** covers ATM functions and section **F.3** covers other air navigation services (C, N, S, MET, AIS).

It is at this level that the high-level safety properties (known as Safety Objectives) of the system are specified in response to the SAfety Criteria. The resulting set of OSED level safety properties is known as the safety Specification for the system.

F.2 ATM Specification Process

The full process for deriving the OSED level safety properties for an ATM system is shown in **Figure 11** and described in the text that follows it.

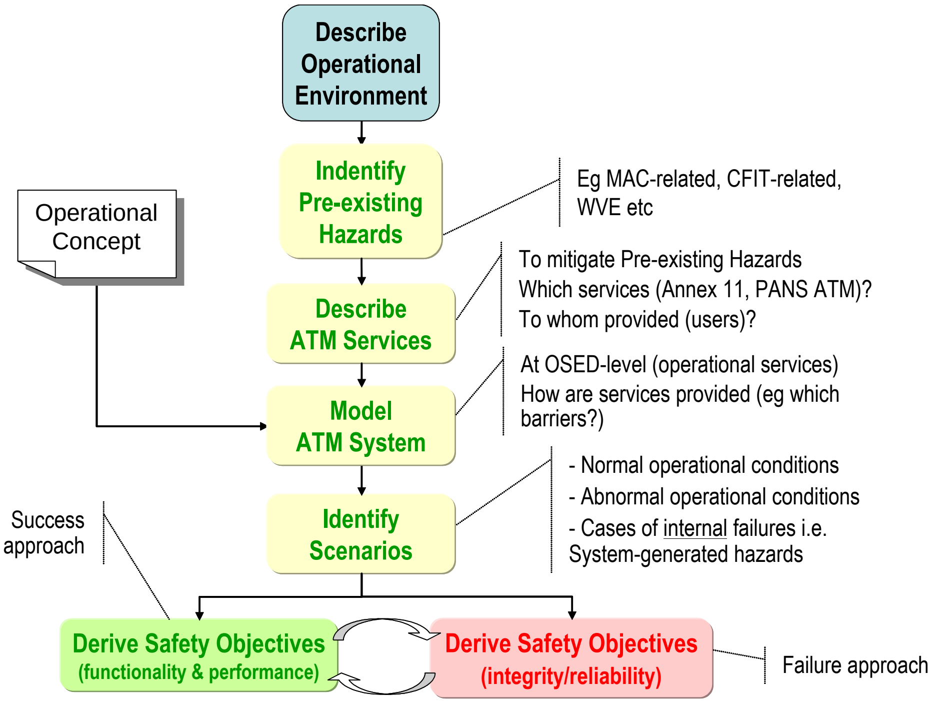

Describe Operational Environment
Indentify Pre-existing Hazards
Eg MAC-related, CFIT-related, WVE etc
Operational Concept
Describe ATM Services
To mitigate Pre-existing Hazards
Which services (Annex 11, PANS ATM)?
To whom provided (users)?
Model ATM System
At OSED-level (operational services)
How are services provided (eg which barriers?)
Identify Scenarios
- Normal operational conditions
- Abnormal operational conditions
- Cases of internal failures i.e. System-generated hazards
Success approach
Derive Safety Objectives (functionality & performance)
Derive Safety Objectives (integrity/reliability)
Failure approach

Figure 11: ATM System Specification Process

F.2.1 Operational Environment

Guidance on this is provided at **Guidance B**.

F.2.2 Identifying Pre-existing Hazards

The purpose of most safety-related systems is to mitigate the hazards (and associated risks) that are pre-existing in the operational environment of the system concerned. These hazards are, therefore, 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 system the pre-existing hazards and risks are generally those that are inherent in aviation and for which the main raison d'être of ATM is to provide as much mitigation as possible.

For **Terminal Area** and **En-route** operations, the pre-existing hazards will normally include the following:

- a situation in which the intended trajectories of two or more aircraft are in conflict
- a situation where the intended trajectory of an aircraft is in conflict with terrain or an obstacle
- penetration of restricted airspace – this category is quite distinct from MAC for military danger areas where the end effect could be being shot down
- wake vortex encounters (WVE)
- encounters with adverse weather

For **Runway / Taxiway** operations[5], the pre-existing hazards may include the following:

- a situation in which the intended trajectories of two or more aircraft are in conflict
- a situation where the intended trajectory of an aircraft is in conflict with terrain or an obstacle
- another aircraft or vehicle inside OFZ during a Cat II / III instrument approach
- another aircraft or vehicle inside landing-aid protection area during instrument approach
- a situation in which the intended 3-D[6] route of a taxiing aircraft would lead to collision with an obstacle, a ground vehicle or another aircraft on ground or close to ground on landing / take-off
- wake vortex encounters (WVE)
- violent wind effects (thunderstorm, windshear) affecting aircraft vertical speed
- tailwind or severe crosswind on landing / take-off
- birds close to / in path of aircraft
- FOD (within runway protected area)
- low runway-surface friction
- snow / slush on runway (high rolling drag situation)
- aircraft uses closed runway / taxiway
- aircraft attempts a landing with undercarriage retracted.

It should be noted that the list for Runway / Taxiway operations was derived for SESAR and some hazards might therefore appear to be beyond the scope of “traditional” airport ATM.

F.2.3 Describing the Operational services

In the specific case of ATM, the services at a high level are defined as follows:

- Air traffic Control (ATC)
- Air Traffic Advisory Service (ATAS)
- Flight-information Service (FIS)
- Alerting Service (ALR)
- Air Traffic Flow Management (ATFM)
- Airspace Management (ASM)

The important point about these services from a safety perspective is that they are all provided in order to address *pre-existing* hazards / risks.

[5] Runway operations are assumed to start soon after an aircraft is stabilised on Final Approach
[6] In the horizontal dimensions and time

Thus, before we try to model the system at the OSED level, we need to describe the services involved and relate them to the pre-existing hazards. For example, for arrival traffic in Terminal Areas we might have the following:

- provide separation within particular arrival flows
- provide separation from other flows
- provide separation from terrain/obstacles
- prevent entry into unauthorized areas
- Minimize wake-vortex encounters
- avoid adverse-weather encounters

All of which is needed in order to mitigate the hazards listed in section **F.2.2** above, and has to be accomplished while integrating arrival flows efficiently into a landing sequence to the runway.

Performance from an EATMA viewpoint and more precisely the "Capabilities" architectural elements (the following pictogram is used by EATMA ATM) that are relevant to the SESAR Solution should be considered when defining the Operational services.

ICAO Annex 11 and PANS-ATM also provide a valuable source of information for describing in detail which Operational services are provided – it is necessary then to show how they map on to the pre-existing hazards.

In describing the Operational services, in relation to the pre-existing hazards, it is important to explain to whom (i.e. to which airspace users) the services are provided, according to (for example) the types of user, the flight rules (IFR, VFR, OAT etc.) and the class of airspace concerned – see **Figure 11**.

F.2.4 Modelling the ATM System at the OSED level

The next stage is to explain how the above services are delivered by the ATM system, at the OSED level – i.e. across the interface between the service provider and the service user(s). Clearly, this must fully reflect the Operational Concept at this level, as shown in **Figure 11**.

For many ATM applications, the system can be modelled very effectively at the OSED level by means of a Barrier Model, as follows. This description is followed by guidance on other ways of modelling ATM systems at this level.

ATM Barrier Models

For the purposes of this guidance take the example of a Barrier Model for typical current (i.e. pre-SESAR[7]) En-route or ARR/DEP operations. In SESAR, this type of model is the Accident Incident Model (AIM).

[7] The term "pre-SESAR" is used here to make the point that SESAR concepts such as trajectory-based operations and new separation modes can result in a somewhat different Barrier Model. The Accident-Incident Model (AIM) developed by 16.01.01 provides the Barrier Models for SESAR operations for the En-Route, TMA and airport environments.

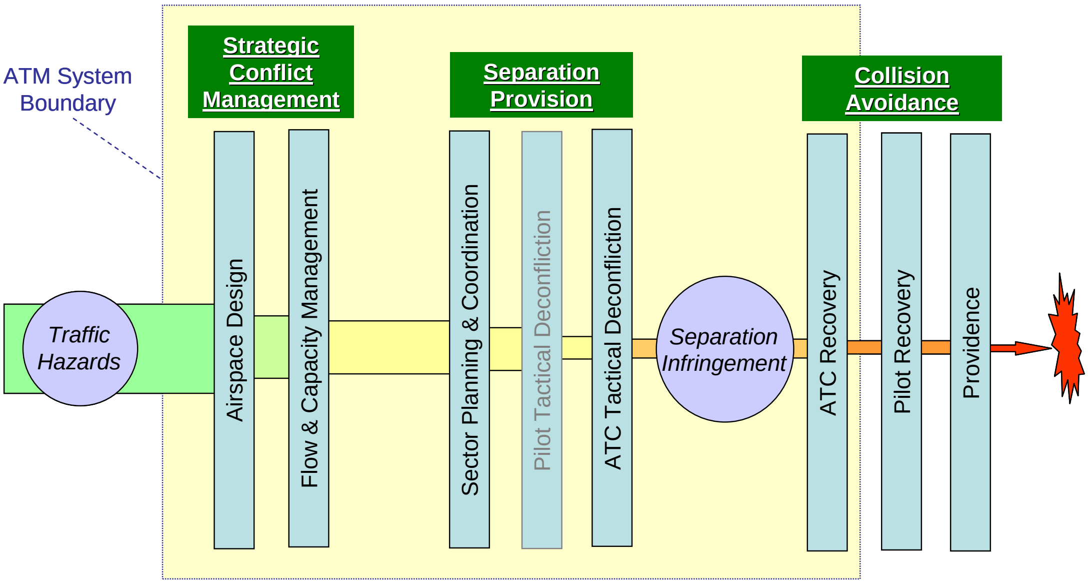


Figure 12: ATM Barrier Model for Current En-route and ARR/DEP Operations

Overall, the model, shown in **Figure 12** above conforms generally to the ICAO Doc 9854 description of Conflict Management:

- whose purpose is to limit, to a tolerable level, the risk of collision between aircraft and hazards (sic), and
- which is applied in three layers: Strategic Conflict Management; Separation Provision; and Collision Avoidance.

The inputs to the model are the (pre-existing) hazards that are inherent in the existence of air traffic, in the various phases of flight – the level and complexity of the traffic, amongst other things, will determine the subsequent behaviour of the barriers within each layer of Conflict Management.

The barriers are grouped under the three, ICAO-defined layers of ATM. Each barrier is defined so as to be largely self-contained[8], and contributes positively to aviation safety by removing a percentage of the conflicts which exist in the operational environment, as follows[9].

Within the *Strategic Conflict Management* layer:

- **Airspace Design** provides structuring of the airspace so as to keep aircraft apart spatially, in the lateral and/or vertical dimensions
- **Flow and Capacity Management** mainly prevents overload of the Separation Provision barriers although, by simply smoothing out the flow of traffic, it does in effect reduce the peak number of potential conflicts in the areas affected

Within the *Separation Provision* layer:

- **Sector Planning & Coordination** involves planning the routing and timing of individual flights so that the aircraft, if they followed their planned trajectories, would not pass each other within the prescribed minimum separation. It includes the whole of the proactive role of ATC in avoiding conflicts – cf. ATC Tactical Deconfliction – including coordination with adjacent sectors

[8] For example, the Airspace Design barrier is not limited to solely the design of the airspace, including pre-defined routes – it includes also whatever monitoring and corrective action is necessary to ensure that the aircraft actually conform to their cleared routes and altitude / speed constraints that are necessary for the barrier to be fully effective under all normal operational conditions. This does not, however, mean that the barriers are independent – on the contrary, it can often be seen in the description of the subsequent Functional and Logical models that many elements of the ATM system are shared by a number of barriers

[9] It should be noted that the Barrier Model is a simplified illustration, not a precise model, but can be useful in gaining a high-level understanding of major operational changes.

- **ATC Tactical Deconfliction** reflects the more reactive ATC role in monitoring the execution of the *plan* (see Sector Planning & Coordination) by detecting conflicts if and when they do occur and resolving the situation by changing the heading, altitude or speed of the aircraft
- **Pilot Tactical Deconfliction** involves the Flight Crew detecting conflicts when they do occur and resolving the situation by changing the heading, altitude or speed of the aircraft appropriately – pre-SESAR, this barrier (shown “greyed out”) applies only to VFR aircraft in managed airspace and to all traffic in unmanaged airspace.

The *Collision Avoidance* layer is intended to recover the situation only for those potential accidents that Strategic Conflict Management and Separation Provision have failed to remove from the system. In general, these may be considered as:

- **ATC Recovery** – this represents “late” intervention by ATC, triggered, for example, by STCA and / or MSAW
- **Pilot Recovery** – intervention by the Flight Crew triggered, for example, by an ACAS RA and / or GPWS
- **Providence** – *i.e.* the chance that aircraft involved in a given encounter, albeit in close proximity, would not actually collide.

A very important thing that the barriers have in common is that, because of inherent finite limits in their functionality and performance, none of them (neither singly nor in combination) is 100% effective even when working to full specification. The degree and extent to which the barriers are able to reduce risk (by removing conflicts or avoiding collisions, as appropriate) depends primarily on the operational concept and on the functionality and performance of the various elements of the ATM system that underlie each barrier.

Of course, should any of the barriers fail then the risk will increase during the period of failure because the barrier is simply ineffective and / or a new source of risk is induced by the failure.

Guidance on non-Barrier Models at the Operational OSED level

For some ATM safety assessments, a Barrier Model might not be the most effective way of representing the ATM system at the OSED level.

For such cases, it might be more appropriate to use, for example, an element (or elements) of the Functional Model provided such elements can be considered to exist in the interface between the ATM system and the Airspace Users.

For example, taking the Functional Model in **Guidance G**:

- it would be valid to consider Tactical Conflict Resolution (TCR) as part of the ATM system at the OSED level since the outputs of the function are directly “visible” to the Airspace Users
- it would not normally be valid, however, to consider Tactical Conflict Detection (TCD) as part of the OSED level system description since the outputs of the function are “transparent” to the Airspace Users – this is because TCD is an enabler for TCR.

F.2.5 Identifying the Initial Scenarios

Scenarios are used initially to expand on, and analyse, the OSED level model of the ATM system in order to facilitate the derivation of Safety Objectives (*functionality & performance properties* from the success approach) for the success approach. **Guidance I** describes a method based on observation and examination of the work-as-done and the varying conditions which can support the identification of scenarios.

Such scenarios should fully reflect the Operational Concept and must include[10]:

[10] It is a requirement of interoperability Regulation (EC) No 552/2004 that “A harmonized set of safety requirements for the design, implementation, maintenance and operation of systems and their constituents, both for normal and degraded modes of

- all *normal* conditions of the operation environment that the system is expected to encounter in day-to-day operations
- all *abnormal* conditions of the operation environment that the system may exceptionally encounter.

F.2.6 Deriving the Safety Objectives (functionality & performance properties from the success approach)

The initial set of Safety Performance Objectives must capture everything that is needed for the success approach, for all of the normal and abnormal scenarios (see **F.2.5** above), from a safety perspective.

Having described (under section **F.2.4** above, at the level of abstraction of the Barrier Model) how the ATM system delivers the services necessary to address the pre-existing hazards sufficiently to meet the SAfety Criteria, the Safety Objectives (success approach) specify formally the fundamental safety properties of the system to ensure that this will actually happen in the subsequent design and implementation of the system.

EATMA “Nodes” (the following pictogram is used by EATMA N) and “Information exchanges” (the following pictogram is used by EATMA ‹i›) architectural elements that are relevant to the SESAR Solution should be considered when deriving the initial set of Safety Performance Objectives.

F.2.7 Deriving the Safety Objectives (failure approach)

In line with the definition in ESARR 4 (and equivalent EC 1035/2011 regulations), Safety Objectives (failure approach) address the failure approach by limiting the frequency or probability of occurrence of (OSED level) *system-generated* hazards to keep within the SAfety Criteria.

This is the application of the SAM FHA at the OSED level (and equivalent to the OHA in ED-78A). Guidance is provided in **Guidance E**.

The two curved arrows on **Figure 11** indicate that:

- a good starting point for deriving the failure scenarios is ‘negating’ the Safety Objectives (*functionality and performance properties* from the success approach) – *i.e.* asking what if Safety Objective #nn (success approach) is not achieved
- the mitigations of the consequences of the system-generated hazards are captured as additional Safety Objectives (functionality and performance).

Further sources of failure scenarios may be the description of varying conditions developed through an RE workshop (**Guidance I**).

F.3 Guidance on Specifying non-ATM Systems at the OSED level

In most cases, non-ATM Air Navigation systems provide data services to ATM systems and / or, in some cases, direct to Airspace Users.

Therefore, the (OSED level) *Specification* can be expressed in terms of the data provided according to its required properties such as:

- type
- scope / applicability
- format

operation, shall be defined with a view to achieving the agreed safety levels, for all phases of flight and for the entire EATMN”. This can be interpreted as covering the *normal*, and *abnormal* conditions as well as *failures* defined in this Annex.

- interface protocols
- accuracy
- resolution
- latency / refresh rate
- integrity
- etc.

Provided these properties are agreed by the service users, then they can be considered to be the Safety Objectives (success and failure) for the (non-ATM) system, without further modelling or analysis being required.

Also, maximum relevant use should be made of existing standards (including ICAO Annexes) in developing these safety properties.

Guidance G On system-engineering models

G.1 Operational (service) Level

The ATM service is what exists in the interface between the ATM System and the Airspace Users. From a safety point of view at least, the ATM services are determined by the need for ATM to mitigate the (pre-existing) hazards and risks that are inherent in aviation. Thus, we've seen that the process starts by:

- defining the pre-existing hazards that are within the scope of the safety assessment
- describing the ATM services that are needed in order to mitigate those hazards

For the safety assessments, two models are useful to describe the ATM system at the service level. They are presented in **G.1.1** and **G.1.2** below.

G.1.1 Guidance on Barrier Model

An effective way of describing the ATM System at this level is an expansion of the simple Barrier Model as provided in **F.2.4** of **Guidance F**. This expansion is addressed by AIM models. An illustration for current En-route / TMA operations Guidance on AIM is provided in **Guidance D**. More information can be obtained from **Ref. 18** and **20** and directly from PJ19.3.

G.1.2 Guidance on Functional Model

A Functional Model (FM) is a high-level, abstract representation of the design of the system that is entirely independent of the SPR-level design and of the eventual physical implementation of the system. The FM describes what functions are performed and the data that is used and produced by those functions – it does not show who or what performs the safety functions.

The important point about functional design is that it provides a bridge between the OSED level representation of the system (e.g. the AIM-Barrier Model – see F.2.4) and the SPR-level design (see **G.2**). In many cases, this would provide a lot of assurance about the completeness of the SPR-level design with respect to the OSED level requirements. However, in other cases a functional representation might not add significant value and could be omitted.

Operational Concept from an EATMA viewpoint and more precisely the "Activities" architectural elements (the following pictogram is used by EATMA:) that are relevant to the SESAR Solution should be considered when developing the functional Model.

It is not practicable to fully describe a typical FM in this guidance but to illustrate its engineering level, structure scope and complexity. **Figure 13** shows the graphical representation of a typical FM for current Arrival / Departure (ARR/DEP) operations.

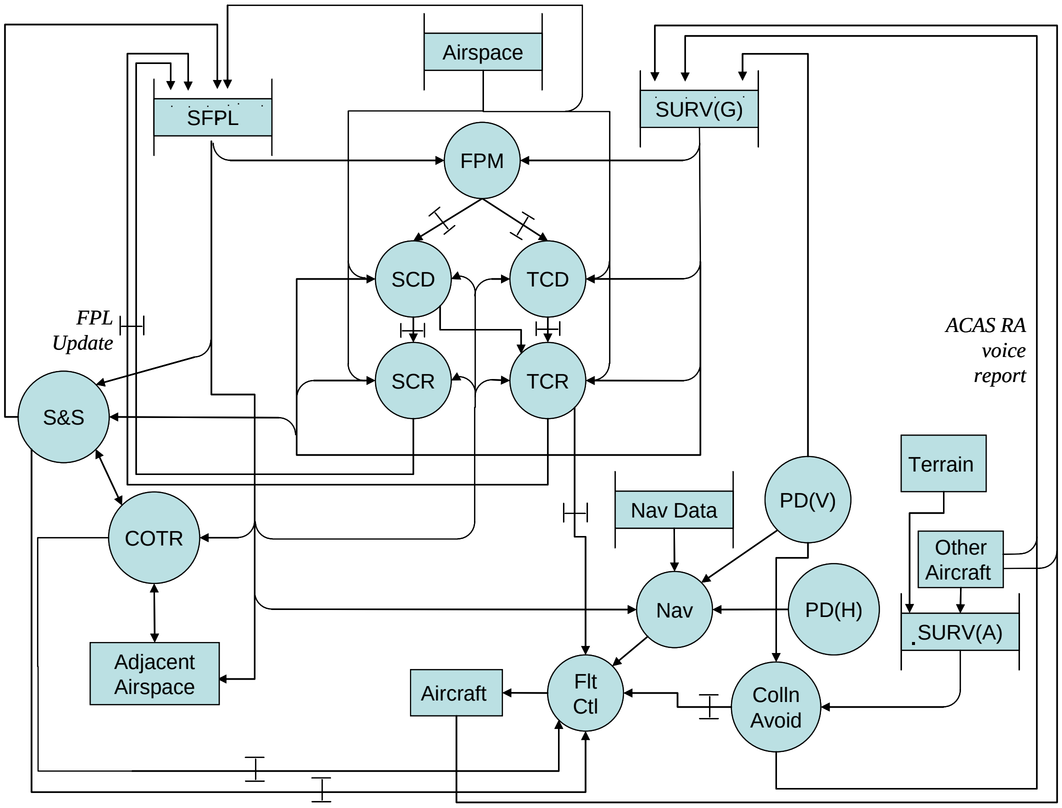


Figure 13: Typical Functional Model – Current ARR/DEP Operations

The functional design should describe in detail what each element of the FM does and, where necessary, what level of performance is required of the concerned element (e.g. accuracy, timing, etc.).

The symbols used in the model are as follows:

○ <title>	Function – *i.e.* the basic element of a FM for which the functionality and performance (accuracy, timeliness etc.) are specified in each case, as applicable
|<title>|	Data Source – from which data is continually or continuously available
<title>	External entity – i.e. elements that lie outside the boundary of the system under consideration.
→	Data Flow (continual / continuous) between Functions or between a Data Source and a Function
⊥→	Control Channel – along which instructions, clearances, requests and one-off data items are passed

The acronyms used in the model are as follows:

Colln Avoid	Collision Avoidance
COTR	Coordination and Transfer
Flt Ctl	Flight Control
Nav	Aircraft Navigation Processing
PD(H)	Position Determination (Horizontal)
PD(V)	Position Determination (Vertical)

SCD	Strategic Conflict Detection
SCR	Strategic Conflict Resolution
SFPL	System Flight Plans
S&S	Sequencing & Spacing
SURV(A)	Airborne Surveillance
SURV(G)	Ground-based Surveillance
TCD	Tactical Conflict Detection
TCR	Tactical Conflict Resolution

A typical ATM function is Strategic Conflict Detection (SCD). It is effectively an abstraction of one of the main roles of the multi-sector planner controller / planning tools – however, as indicated in the introductory remarks for this Annex, the description of the function should be entirely independent of whether it was subsequently implemented as a human tasks or a machine-based function.

It is normally triggered by Flight Progress Monitoring (FPM) or directly from Airspace / System Flight Plan (SFPL) information, and provides a warning of conflicts between SFPL-defined trajectories and between a trajectory and prohibited airspace.

The safety properties associated with the FM are known as *intermediate* safety requirements since they sit between the OSED level safety objectives and the final, SPR-level safety requirements.

G.2 System architectural representation at SPR-level

A SPR-level Model is a high-level, architectural representation of the ATM/ANS system design that it is entirely independent of the eventual physical implementation of that design. It describes the main human tasks, machine-based functions and airspace structures and explains what each of those "actors" provides in terms of functionality and performance. The SPR-level model normally does not show elements of the physical design, such as hardware, software, procedures, training etc.

The SPR-level model is the representation of the system for which the final Safety Requirements are derived, in response to the Safety Objectives specified at the OSED level (for which see **F.2.7** of **Guidance F**).

Operational Concept from an EATMA viewpoint and more precisely the "Activities" (the following pictogram is used by EATMA: A A) and "Roles" (the following pictogram is used by EATMA: 👤) architectural elements that are relevant to the SESAR Solution should be considered when developing the SPR-level Model.

Figure 14 shows a typical graphical representation of the SPR-level model for current Terminal Area operations.

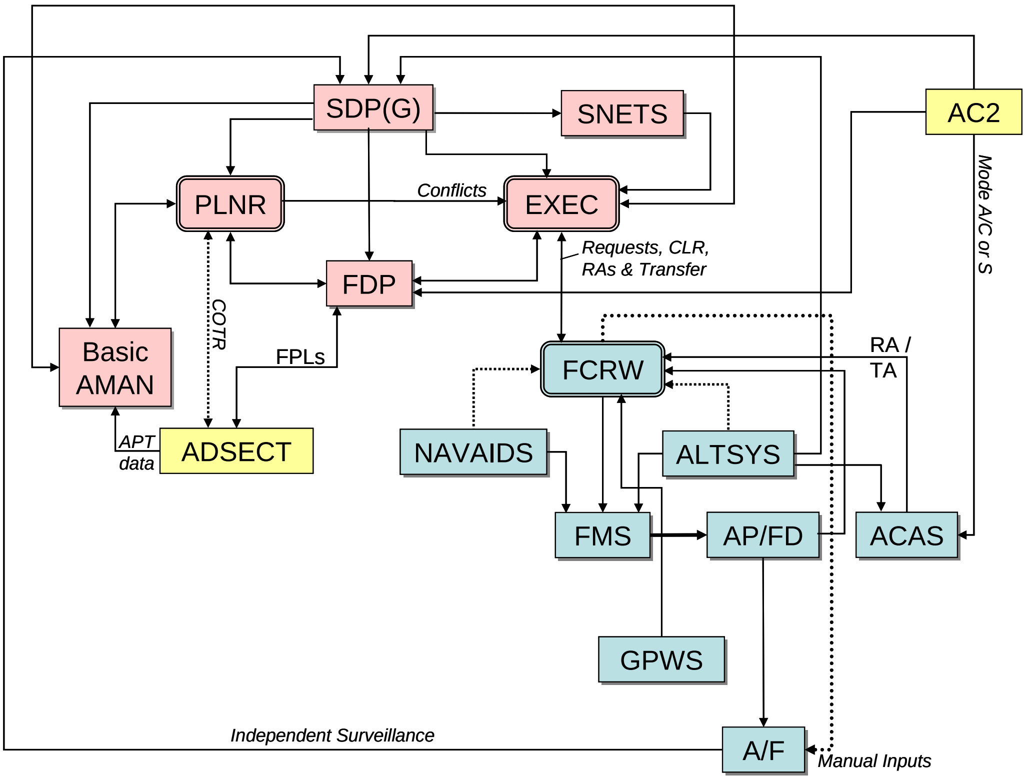


Figure 14: Typical SPR-level Model – Current ARR/DEP Operations

The symbols used in the model are as follows (box titles are illustrative):

PLNR	Human actor – ground
SDP(G)	Equipment function – ground
FCRW	Human actor – airborne
FMS	Equipment function – airborne
ADSECT	External Entity
→	Main interfaces

The acronyms used in the model are as follows:

AC2	Other aircraft
ACAS	Airborne Collision Avoidance System
ADSECT	Adjacent sector(s) / ATSU
A/F	Airframe
ALTSYS	Altimetry System
AMAN	Arrival Manager
AP/FD	Autopilot / Flight Director
EXEC	Executive (Tactical) Controller

FCRW	Flight Crew
FDP	Flight Data Processing
FMS	Aircraft Flight Management System
GPWS	Ground Proximity Warning System
NAVAIDS	Aircraft Navigation Aids
PLNR	Planner Controller
SDP(G)	Surveillance Data Processing (Ground)
SNETS	Ground-based Safety Nets

Human-machine interfaces (HMIs) are not represented explicitly on the SPR-level model, but are implicit in each link between human and machine shown on the model. The rationale for this is twofold:

- It would be unnecessary detail for what are already quite complex diagrams
- more importantly, they can obscure the detail of which machine inputs / outputs are linked directly with the human and which are not.

Safety Requirements (*Functionality and Performance properties* from the success approach) describe in detail what each element of the SPR-level model must do from a safety perspective and, where necessary, what level of performance is required of it. As an example, the following are two of the many safety requirements specified for Surveillance Data Processing (SDP(G)) and Flight Data Processing (FDP), respectively:

- **SDP(G)** shall correlate and output the available sources of surveillance data, flight plans and other data to provide at least the following information:
    - Aircraft Identification
    - Position and Altitude
    - Aircraft ATM capability
    - Emergency indication
    - Ground Velocity (3-axis)
    - Sector and other Airspace boundaries
    - Restricted Airspace
    - Route Structures
    - NOTAM, ATIS, METAR, SIGMET etc.
- **FDP** shall:
    - perform SSR code management and assignment
    - perform Track / Flight correlation
    - provide facilities for Sectorization changes

Safety requirements (*Integrity property* from the failure approach), on the other hand, specify the maximum failure rate of the SPR-level model elements, in terms of loss, credible corruption etc. Internal mitigation means, which are taken into account in the derivation of safety requirements (failure approach) (from Safety Objectives (failure approach)) are captured as additional safety requirements (*functionality and performance* properties).

G.3 Guidance on Thread Analysis

G.3.1 Introduction

Thread Analysis can be used in the static analysis of a SPR-level Design for all normal and abnormal conditions of the operational environment and for internal failures of the system.

Thread Analysis is similar to Use Case analysis except that it uses a particular graphical presentation in which the actions of the individual elements of the SPR-level Model, and the interactions between those elements, are represented as a continuous 'thread', from initiation to completion.

The main equipment functions and human tasks are described by reference to the related Safety Requirements (*functionality and performance properties* from the success approach) although some relatively minor functions / tasks may be represented only in the Threads themselves.

The Threads tell us more about the intended operation of the ATM system than could the SPR-level Model or Safety Requirements (success approach) on their own; therefore, they are regarded as an integral part of the design and of the corresponding set of Safety Requirements (*functionality and performance* properties).

G.3.2 Example

An example of a Thread Analysis is shown in **Figure 15**.

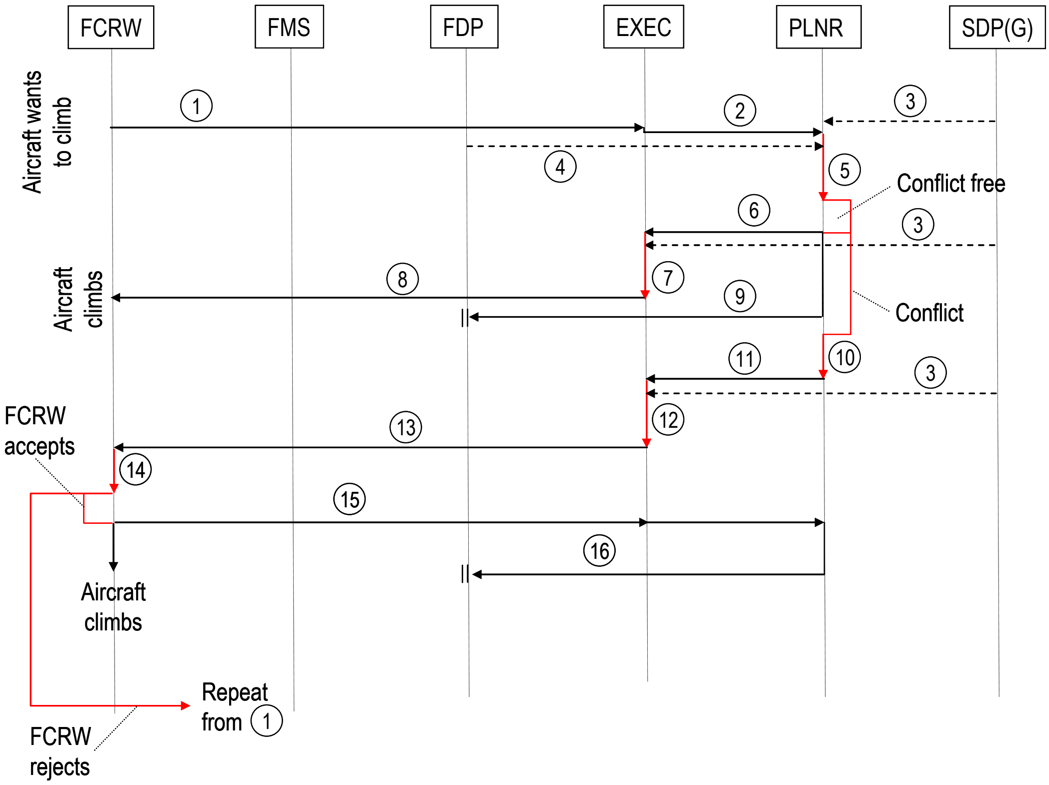
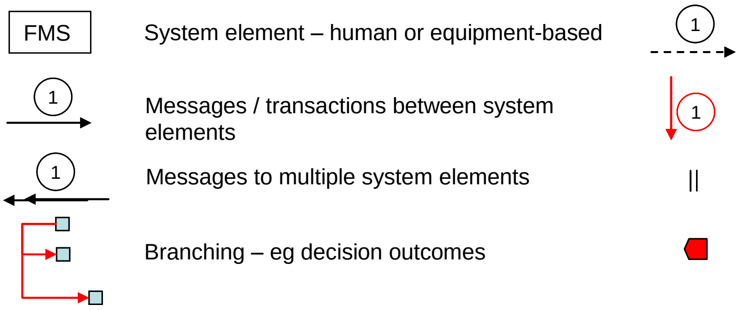


Figure 15: Example of a Thread Diagram

Key:



System element – human or equipment-based

Messages / transactions between system elements

Messages to multiple system elements

Branching – eg decision outcomes

Continuous flow of information

Processing internal to system element

Terminator

Connection to another Thread

Pre-condition

A flight needs to change its agreed trajectory – e.g. to avoid bad weather. The example shown is a requested climb.

Actions:

1. Flight Crew (FCRW) requests climb to a new flight level
2. Executive Controller (EXEC) asks Planner (PLNR) to coordinate with next Sector
3. Surveillance Data Processing (Ground) – SDP(G) – passes continuous ground surveillance data to EXEC and PLNR: Safety Requirement (success approach) [SG01]
4. Flight Data Processing (FDP) provides continuous Flight Plan information to PLNR [FD01]
5. PLNR coordinates change of FL with next Sector

   [If conflict-free go to (6) else go to (10)]
6. PLNR advises EXEC that the proposed FL is conflict-free (or at least acceptable to next sector)
7. EXEC decides (on basis of SDP(G)) whether / when the aircraft can start its climb [EX05]
8. EXEC clears aircraft to the requested new FL
9. PLNR updates the Flight Plan on the FDP [PL03]
10. PLNR chooses and coordinates alternative new FL with next sector [PL05]
11. PLNR advises EXEC of alternative new FL
12. EXEC decides (on basis of SDP(G)) whether / when the aircraft can start its climb [EX05]
13. EXEC clears aircraft to the alternative new FL
14. FCRW decides if the alternative new FL is acceptable operationally

    [If not acceptable, FCRW must request preferred alternative – i.e. go back to (1) – else go to (15)]
15. FCRW confirms climbing to << the alternative new FL>> [FC06]
16. PLNR updates the Flight Plan on the FDP [PL03]

G.3.3 Benefits

The above example does not necessarily show the strengths of the Thread Analysis technique to full effect.

However, its use should show the following benefits:

- it leads to a much better understanding of how the Operational Concept should work in practice – this should be of benefit to the rest of a Solution, not just to the safety assessment;
- it helps correct many errors, inefficiencies and inconsistencies in the SPR-level Models; and

- it proves very effective in identifying missing or incorrect safety requirements (*functional and performance* from the success approach).

G.3.4 Application

Because the Threads provide an understanding of the system behaviour that cannot be shown solely through the SPR-level Models and individual Safety Requirements (success approach), it follows that the Threads themselves should form part of the SPR-level Design, and each Thread should be a Safety Requirement in its own right.

Of course, what Thread Analysis cannot assess are the dynamic aspects of the system behaviour – hence there is a need for the safety assessment to make use also of the real-time and fast-time simulation exercises, which form a very important part of SESAR Development Phase. Nevertheless, Thread Analysis is a very cost-effective way of proving the correctness of the SPR-level Design under a wide range of normal and abnormal conditions.

Furthermore, by “breaking” Threads or inserting spurious Threads, it should be possible to get a better understanding of the effects of failures within the system, and identify reversionary modes of operation – *i.e.* it can be used to enhance the conventional, failure-based safety assessment.

Finally, it is proposed that the above notation be used only during the drafting and operational-review stages of Thread development, and to present the final versions in a modified version of UML System Sequence Diagram (or equivalent) format, in line with current ATM and avionics industrial practices.

Guidance H On the SESAR Safety Register

One of the challenges to be faced by PJ19.3 is managing the large amount of information involved, in such a way that the Evidence produced is complete, correct, consistent and sufficient to satisfy the Safety Argument for a set of Solutions (e.g. forming the scope of a SESAR Safety Case). In addition, for a specific Solution, it is necessary to provide an access to the various set of safety requirements (incl. SAC, SO, SR, etc.) with proper relationships to the elements of the System Architecture (e.g. ATM services).

Across the SESAR work programme, this is achieved by developing and maintaining a **Safety Register** throughout the life of the project in order to track progress and provide visibility of the status of the various safety assurance objectives and activities for each phase of the lifecycle of a specific Solution and for all relevant Solutions for a specific package. The safety information defined herein with relation to a specific assessment should be input in the Register and maintained by the person in charge of the safety assessment.

For a specific Solution, the Safety Register includes the following:

Generic information related to the Solution

- SESAR Step, Solution ID, project ID, OI steps, etc.
- Related Solutions
- Maturity of the safety assessment (incl. SAR version)

Safety 'requirements' in the form of:

- SAfety Criteria with proper references the relevant AIM models, barriers, precursors and backward traceability to the Safety Performance Target as per the work of B4;1 for the related step
- Information related to the Safety Objectives incl.
    - ATM services
    - Conditions (normal, abnormal, failure)
    - List of Hazards ('OSED' level hazards), and including, for each Hazard:
        - Description
        - Severity Class
    - Safety Objectives (*Controls, Functionality and Performance properties* from the success approach), Safety Objectives (*Integrity properties* from the failure approach)
- Information related to the Safety Requirements (*Functionality and Performance properties* from the success approach), Safety Requirements (*Integrity property* from the failure approach) mapped to ATM System elements (actors and Architectural element).
- Overall forward and backward traceability from SAC to SR through SO with queries programmed in the Remedy software

Assumptions as they arise during the safety assessment and development of the Safety Assessment, and including:

- Description
- Source (where and when raised)
- Rationale / reason for the Assumption
- How and when the Assumption was (or will be) validated

Safety Issues – i.e. those safety concerns that arise during the safety assessments and which cannot be resolved at the time.. The Issues Log should include:

- Description
- Source (where and when raised)
- Responsibility and Recommendations for Resolution
- Status

Any **Limitations** (very similar nature as a safety requirement) which need to be placed on the related ANS operations as a result of the safety assessment.

Safety Recommendations – including safety-driven recommendations to the design (operational concept) and/or recommendations for further safety and/or HP activities, etc. and their status in terms of acceptance/inclusion by the Solution

USAGE

The Safety Register is implemented in BMC Software Remedy ITSM (IT Service Management) suite and is accessible at:

https://remedyweb.eurocontrol.fr/arsys/shared/login.jsp?/arsys/forms/remedy/SESAR+WP16+-+Safety+Register

The Solution shall create a 'new assessment' and inform the database while the safety assessment progresses. The user manual on how to use the register in both creation and consultation/modification modes is accessible at:

https://extranet.sesarju.eu/WP_16/Project_16.06.01/Project%20Plan/T16.06.01-009%20(Cross-TA%20Register)/Safety%20Register%20Tool%20end-user%20Handbook%20Ed%201.0.doc

In consultation/interrogation modes, the following queries are currently available:

- Find all SAC for a specific AIM model
- Find all safey information for a specific Solution
- Find and show all hazard organised by severity class
- SR queries
    - F&P SR
    - Integrity SR

Guidance I On the usage of Resilience Engineering

I.1 Overview

The guidance describes the Resilience Engineering activities that provide a means to investigate everyday operations based on analysis of varying conditions, work-as-done and adaptive capacity to improve the resilience of ATM/ANS functional systems. The guidance recommends the usage of resilience engineering to complement the safety assurance activities performed in support of the SESAR Safety Reference Material, including the success approach.

I.2 Introduction

While safety is traditionally viewed as the absence of unwanted outcomes, such as errors and accidents, recent trends in safety research insist on the necessity to understand and support how safety is actively produced. In the latter view, operators are not seen as the fallible elements of a system that otherwise functioned as designed, but as major sources of reliability necessary for successful operations. Indeed, even well-engineered systems cannot anticipate all potential variability they might face, and rely on operators' capacity to understand and adapt to changing, potentially surprising conditions to ensure safe operations. Ironically, because operators are successful in doing so, those adaptations remain unnoticed if they are not explicitly investigated.

In the context of the increased complexity of the ATM system, safety assessments may benefit from techniques based on system-oriented conceptual and methodological approaches. Especially in the context of innovative SESAR concepts that may transform the nature of operations, a safety assessment approach needs to adopt a view of the system as a whole and purposefully consider the different responsibilities and interactions between components (human and/or technological).

The activities described in this guidance provide the means to address these two fundamental issues, based on the philosophy and concepts of Resilience Engineering (RE). RE aims to investigate how work systems successfully handle varying conditions, whether expected or not, in order to improve their design. This aim involves understanding how those systems are capable of adjusting their behaviour to pursue essential goals in the face of changing conditions that can represent challenges, surprises or opportunities. RE is explicitly based on the study of the complex work system.

I.3 Core Principles

The activities are based upon a few core elements and principles from Resilience Engineering:

- **Varying conditions**: Variability and uncertainty are inherent in complex work such as ATM; the conditions and challenges that manifest themselves are many and various. These can take the form of changes experienced in the daily life of operational units everywhere; or surprises that emerge from the interface of system elements that interact in unusual ways (e.g., hidden interactions); or challenges such as volcanic ash that defy any form of prediction. The RE activities aim to reveal the varying conditions the new design will need to handle.
- **Adaptive capacity**: Adaptive capacity is the potential for adjusting patterns of action to handle the varying conditions described above. It is useful to distinguish between two forms: a base adaptive capacity, which represents the ways the system handles varying conditions by design (e.g., procedures and experience for a specific unusual situation); and an extra adaptive capacity, which represents the system's capacity to handle situations that fall outside of the typical and planned for situations (e.g., operators solve a novel problem based on their expertise). Adaptive capacity, especially the latter form, is at the heart of the notion of

resilience, and the RE activities aim at capturing, analysing and explaining how the new design impacts the system's adaptive capacity.

- **Work-as-done**: refers to work as it is actually performed in everyday operations; work-as-done (WAD) is understood in contrast with work-as-imagined (WAI), i.e., work as it is designed, how it occurs in principle or is planned to occur. Indeed, varying conditions cannot be fully specified, and adjustments are inevitable, leading to a difference between WAD and WAI. The RE activities are based on describing how systems work through exploring WAD. Consistent with user-centric methods, they rely on the inputs of the people who will work with the new design when it is implemented. This is achieved by letting operators and managers explain how they intend to use the new design and thereby explore the possibilities that will emerge. The RE activity aims to close the gap between the operational world and the people who are implementing the new design.

I.4 When to use Resilience Engineering in the SRM process

Assessments which use the RE guidance will have a broader scope and include activities which extends the SESAR Safety Assessment Process. Understanding changes between the current operation and new design can provide additional safety narratives that inform project decision making, support the derivation of new or modified requirements or validation objectives or can be included in safety cases.

The RE guidance provides qualitative support to the initial V1 stages of the concept development process. It supports the exploration of how safety is created in the current operation (by design or by innovative behaviour at different levels of the system). The RE activities also help develop an understanding of the purpose of the current system which informs the setting of goals for the future system.

As a concept becomes more mature, the RE activities support the investigation of the resilient properties of the current system and how these will be impacted in the future system. Scenarios for validation are enriched by an improved understanding of the likely varying conditions which may be encountered in operations. Recommendations for new or amended systems engineering requirements which capture the resilient properties required in the future system are generated. The argument for the completeness of the safety assessment is supported because a comprehensive and structured analysis of these scenarios will have been generated.

A table which describes how RE may complement the SRM process steps has been developed (Table 10). Additionally, for each Step of the RE process, the specific SRM Guidance which may be supported has been listed.

The RE guidance provides an alternative and complementary perspective on system performance not just on safety. This additional perspective is particularly relevant for innovative designs that significantly impact operational working methods.

The RE activities described here are intended as a complement to the established processes used in the SESAR Safety Reference Material. The RE principles may be integrated into existing SRM activities. Alternatively, it may be more appropriate to conduct the RE activities separately and then use the results of the RE analysis to enrich the processes described in the SRM. The RE processes should be conducted as a complete set of Steps 1-4 and iterated as required. For example, it may be beneficial to undertake an RE assessment early in the concept development e.g. to support the V2 OSED and explore concept ideas and set validation aims, and then repeat the exercise in the V2 SPR stage when the concept is more mature and validation results may be available to support requirements development.

The RE activities are intended to support the efficacy and rigour of the SRM requirements generation process.

I.5 Description of the RE Activities

The RE activities are organised in 5 steps, which follow **Figure 16** below.

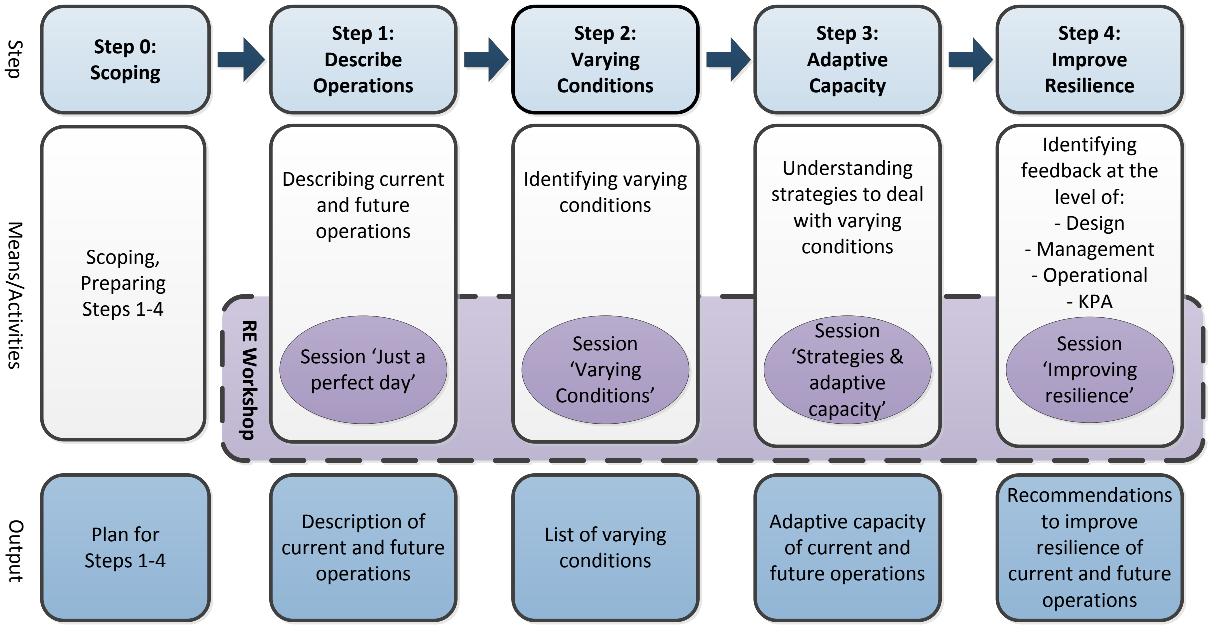

Step
Means/Activities
Output
Step 0: Scoping
Step 1: Describe Operations
Step 2: Varying Conditions
Step 3: Adaptive Capacity
Step 4: Improve Resilience
Scoping, Preparing Steps 1-4
Describing current and future operations
Identifying varying conditions
Understanding strategies to deal with varying conditions
Identifying feedback at the level of:
- Design
- Management
- Operational
- KPA
RE Workshop
Session 'Just a perfect day'
Session 'Varying Conditions'
Session 'Strategies & adaptive capacity'
Session 'Improving resilience'
Plan for Steps 1-4
Description of current and future operations
List of varying conditions
Adaptive capacity of current and future operations
Recommendations to improve resilience of current and future operations

Figure 16: The RE activities are organised into 5 main steps

I.5.1 Step 0: Scoping

Objective - Scope and plan the work to be undertaken.

- Studying background information on RE, including documentation on the RE principles and on previous applications. Novice practitioners are recommended to take an RE training course.
- Developing a plan for the activities to be conducted in Steps 1-4. As part of the planning activities it should be decided whether these activities are to be conducted as a separate activity to inform the safety assessment, for example as RE workshop(s) (Figure 1 shows the recommended main sessions to be conducted as part of such RE workshop), or whether they should be integrated into other SRM activities to be conducted as part of the safety assessment. In the latter case the RE Steps should be reviewed and the safety plan should describe how the RE Steps will be integrated into other SRM activities. The next sections provide some guidance on the alignment with the stages of the SRM safety assessment, for the case when an integrated/augmented approach is to be followed.

Output - An update to the Safety Plan document that describes the plan for how RE Steps 1-4 will be conducted, including the structure of the RE workshop(s) or the integration of the RE steps with other activities conducted as part of the SRM safety assessment.

I.5.2 Step 1: Describe Operations

Objective - Build an initial understanding of the work-as-done in current ATM operations and of the way that future ATM operations are expected to be done.

Alignment to SRM - This activity can support the description of the Operational Environment before the proposed change and the development of the Functional Model as required by the SRM (Guidance A.1-A.2, Guidance B & Guidance F.2.1-F2.3).

Means - These include:

- Studying available documentation on current and future ATM operations e.g. OSED, validation plans, safety and human performance assessments reports, validation reports, procedure and rule sets, etc.
- Observations of current and future ATM operations to determine how operators (such as controllers, pilots, supervisors, engineers), act and interact with each other and with their human machine interface (HMI) and environment. For current ATM, actual operations can be observed. For future ATM operations, in later stages of the development lifecycle, real time simulations may be available for such observations.
- Interviewing the design experts of the future ATM operational concept regarding the context and details of the design that may not be available by the above means.
- Operational expert groups (controllers, pilots, supervisors, etc.) explain what a typical day of operations without considerable varying conditions ('just a perfect day') looks like for them in their current work. Next they are asked to express their expectations of what such a perfect day would look like in the future operation. This session serves to achieve a common understanding of the operations from various perspectives and to set the basis for identifying varying conditions and strategies in later sessions.

Output - An initial description of the work-as-done in current ATM operations and of the way that future ATM operations are expected to be done.

I.5.3 Step 2: Varying Conditions

Objective - Identify a list of expected and unexpected varying conditions that ATM operators and managers may have to deal with in the current and future ATM operation.

Alignment to SRM - The identification of varying conditions supports the development of the success case of the SRM and can be used to inform the capture of abnormal conditions which the proposed concept may be expected to encounter during its lifetime (Guidance A.2 & Guidance F.2.5). This Step, when combined with Step 3, identifies, and provides justification for, the design features necessary to support the future operation.

Means - These include a combination of the following:

- Using results of Step 1 such as validation reports or field observations to identify varying conditions.

- Using dedicated sessions with ATM operational experts, e.g. as part of an RE workshop or a FHA (Functional Hazard Assessment) workshop, to identify as many conditions as possible; rare conditions as well as normal conditions, and to consider situations both within as well outside of their control.

Output - The raw list of identified varying conditions can then be clustered into common areas and some which may be out of scope of the assessment can be removed. This list is used in Step 3.

I.5.4 Step 3: Adaptive Capacity

Objective - To obtain narrative descriptions of the strategies that operators use to deal with varying conditions in the current and the future ATM operation, and to analyse the adaptive capacity in the current and the future ATM operations.

Means - These include the following:

For each varying condition, the operational experts (controllers, pilots, supervisors) explain the strategy or strategies they use or envisage to use when dealing with this varying condition; first in current operations, and next in future operations. Some supporting questions are presented below

- In what way and how often could the varying condition occur?
- Who or what would detect the varying condition, and how?
- What is the strategy to deal with the varying condition, i.e.: How would you act / adapt to the varying condition, with whom would you interact and coordinate, what resources are used?
- How is the strategy acquired, for instance is it part of basic training, is it learned by experience?
- What are the trade-offs and what are the effects of applying the strategy on ATM key performance areas such as safety, capacity, costs, and environment?

The raw data obtained is used as input to an adaptive capacity analysis. Many techniques are available to support this analysis [Refs final P16.06.01B reports] and these aim at organising the raw data by identifying actors, interactions, dependencies, goal conflicts, patterns of behaviour, cascade effects, and sources of resilience. They are applied to the raw data for both the current and the future operation, thus supporting a comparative discussion. For the selection of a technique it is important to keep in mind that its application should provide effective input to Step 4.

Output - A narrative description of the strategies that are available when dealing with varying conditions, for the future ATM operation as well as for the current operation, and insight into the adaptive capacity of both the current and the future ATM operation.

I.5.5 Step 4: Improve Resilience

Objective - Derive recommendations for strengthening the resilience of current and future ATM operations.

Alignment to SRM - This step supports the SRM processes which develop systems engineering requirements for the future concept. This step supports the capture of user requirements and helps develop the rationale for design features to be included in the Functional Model, design-level specifications, system behaviour and the physical design. This step can help inform the development of Safety Criteria in the SRM. It can also support the rationale for such changes (or for why there are no changes) and capture operational safety effects and mitigations for possible failures (Guidance A.2 & Guidance E.2.1).

Means - These include a combination of the following:

Organisation of a session with operational experts to identify measures to improve the resilience of current and future ATM operations focussing on improvements at four levels:

- Design level, including hardware and software, human factors, procedures, airspace structure, layout of the workplace, etc.

- Management level, including supervisors, managers and their procedures and processes for managing and controlling the organisation.

- Operational level, including training, organisational learning, team considerations, safety culture, etc.

- KPA (Key Performance Areas) level, including effects on safety, capacity, environment, cost-benefit.

Output - Depending on maturity of the concept, Step 4 can deliver new or amended design recommendations to support SRM activities such as Safety & Performance Requirements (SPR), Safety Acceptance Criteria (SAC), Safety issues, Human performance issues / benefits, Human Performance (HP) Recommendations, Limitations, Assumptions, and Validation needs and scenario inputs. These outputs are recorded in the regular SESAR documentation.

I.6 SRM Integration

The following sections and tables describe the SRM steps organised by V-phase at a high level. The input that the RE activities can have to these steps is described along with the documentation impacted and the possible benefits.

I.6.1 V1 – Safety scoping and change assessment (P stage P1, P2)

OVERVIEW –RE provides a perspective that broadens the scope of the safety assessment conducted by the SRM to, in particular, to support the identification of unintended risks which may impair operators' adaptive capacities. RE provides a method to explore how safety is created in the current operation (by design or through ad-hoc innovative behaviour at different levels of the system). To develop an understanding of the purposeful activity conducted in the current system to inform the goals of the future system. There are pre-existing properties of resilience in the system today which could be identified (in the same way that there are pre-existing hazards in the system). The RE approach aims to ensure that the new design does not jeopardise these sources of resilience. The RE approach may also identify ways which can create additional safety. Step numbers as per **Figure 16** are represented on the right column of **Table 10** to **Table 12**.

SRM Activities	Correspondence with Guidance I	
Description of the key properties of the operational environment that are relevant to the safety assessment	**Practical Application** – Planning of the Safety Activities to be conducted in the SESAR Solution should be proportionate to the scale and nature of the change. A decision about whether the RE activities are conducted in a separate workshop or are integrated into the SRM activities should be taken during planning. **Output / SESAR Deliverable** – Scoping & Change Assessment Questionnaire	0 1 2 3 4
• Identification of the pre-existing hazards that are inherent in aviation within the scope of the SESAR SOLUTION • Determine the baseline for the assessment • Explain how the SESAR SOLUTION might impact on human performance e.g. tasks, workload, training • Determination of the	**Practical Application** – same as above **Output / SESAR Deliverable** – SESAR Solution OSED (V1) **Added Value to the SRM** – Augmented descriptions of the current operation. Greater appreciation of interaction with human tasks. Enriched description of Operational Services.	0 1 2 3 4

Operational Services which support the SESAR SOLUTION		
Determination of the Safety Targets to be supported and Derivation of Safety Criteria (SAC)	**Practical Application** – Use the RE principles to probe the resilient performance of the existing system to determine 'what is safe' in the current system. Note: RE typically operates at a qualitative level and does not define quantitative criteria in the same way as the SRM processes **Output / SESAR Deliverable** – SESAR Solution Safety Plan (V1) **Added Value to the SRM** – Augment and/or derive new SAC with an RE perspective.	0 **1** **2** **3** **4**

Table 10: Alignment of Resilience Engineering Processes to the V1 phase SRM stages

I.6.2 V2 – OSED (P stage P3P4)

OVERVIEW – RE Activities conducted during these stages involve: studying available documentation on current and future ATM operations (Step 1); interviews or workshops with concept developers and/or operational managers / network managers / controllers engineers (Step 1); development of RE validation objectives (Step 2); development of the RE questionnaire (Step 3). Guidance I Step 4 can also be used to support the development of validation objectives/requirement.

These activities support the delivery of OSED (V2).

SRM Activity	**Correspondence with Guidance I**	
Description of what has to happen for the operational services to work in the defined environment. Derivation of Safety Objectives for functionality & performance related to the mitigation of the identified pre-existing hazards	**RE Activity** – Understanding the resilient properties of the current system and how this will be impacted in the future system. Better understanding of the future design. Identification of varying conditions which should be explored in validation. Identification of strategies used to deliver adaptive capacity in current system and the applicability to the future system design. **Added value to the SRM** – Understanding the resilient properties of the current system. Identification of new/augmented scenarios to support validation objectives to explore the impact on these resilience properties with the future system (e.g. controllers place a lot of trust in pilots monitoring a CTA trajectory - can pilots monitor the trajectory in reality).	**0** **1** **2** **3** 4

Demonstrate completeness and consistency of the safety objectives (functionality & performance)	**RE Activity** – The basis of RE is the examination of normal and abnormal conditions and it provides a structure to better uncover these conditions. Examination of normal, abnormal and degraded modes of operation and the adaptive strategies which are used to manage operations in the current and future operations. **Added value to the SRM** – Demonstration of completeness of analysis through the use of a wide range of operational scenarios. RE provides a more comprehensive, reliable and structured analysis to demonstrate completeness. Additional or more detailed Use Cases and Operational Scenarios to support Validation Planning.	0 1 **2** 3 4
Identify hazards caused by failures internal to the concept/system	**RE Activity** – Identification of conditions and scenarios for which new or revised hazards (in traditional SRM terminology) can be derived **Added value to the SRM** – New or revised hazards to support traditional failure case assessment processes.	0 1 **2** 3 4
Document any assumptions or limitations which have been made in the analysis	**Added value to the SRM** – The RE activities will identify assumptions and limitations which may be in addition to those captured by the SRM.	**0** **1** **2** **3** 4

- Table 11: Alignment of Resilience Engineering Processes to the V2 OSED phase SRM stages

I.6.3 V2 – SPR (P stage P5, P6)

OVERVIEW – RE Activities conducted during these stages support the delivery of SPR (V2)

SRM Activity	Correspondence with Guidance I	
Describe the functionality of the system through the derivation of a functional model	**RE Activity** – RE complements the functional modelling processes of the SRM since RE is functionally-oriented. At a lower level of detail and with more granularity, explore the work as done to inform the definition of the functional model. Results from earlier simulations are interpreted with a systems-view. **Practical Application** – Review the outputs from the RE activities in support of the OSED stage and determine whether	**0** **1** **2** **3**

	there is a need for a further iteration of the RE workshop/activities to support the SPR. Guidance I. Studying available documentation on current and future ATM operations using the principles of RE and the results from early simulations (if available) to inform interviews or workshops with concept developers and/or operational managers / network managers / controllers engineers (Step 1). Development of RE validation objectives (Step 2). Development of the RE questionnaire (Step 3). **Added value to the SRM** – Identification of dependencies between functions. Identification of new functionality, revisions of the scope of the change (based on new interactions and relationships).	4
Specify operational scenarios that are sufficient to fully describe the normal operational environment	**RE Activity** – Development of scenarios based on combinations of conditions and variability **Practical Application** – same as above **Added value to the SRM** – Enriched and operational scenarios informed from work as done. New scenarios also generated based on the characteristics of adaptive capacity.	**0** **1** **2** **3** 4
Derive, from the safety objectives, safety requirements which describe the required functionality and performance for the functional system in the operational environment	**RE Activity** – Recommendations from simulations and workshops are captured and used to inform the development of SPR-level requirements **Practical Application** – Review the SPR-level requirements derived from the SRM processes against the outputs from the RE activities and amend. Derive new requirements on functions which were added as a result of the RE assessment. **Added value to the SRM** – Safety requirements, derived on the basis of RE, are captured in the Validation Plan or the SPR. RE supports the design rationale and provides the narrative to justify functionality included in the design. RE supports a Claims, Argument, Evidence argument structure for future Safety Case.	0 1 2 3 **4**
For each scenario show that the specified safety requirements (Success approach - functionality & performance) are complete, correct and mutually	**RE Activity** – The basis of RE is the examination of normal and abnormal conditions and it provides a structure to better uncover these conditions. Examination of normal, abnormal and degraded modes of operation and the adaptive strategies which are used to manage operations in the current and future operations. **Practical Application** – Guidance I. Studying available documentation on current and future ATM operations using the principles of RE and the results from early simulations (if available) to inform interviews or workshops with concept developers and/or operational managers / network managers / controllers engineers (Step 1). Development of RE	0 1 **2** 3 4

consistent Specify operational scenarios that are sufficient to fully describe the abnormal conditions which the functional system can be expected to encounter in the operational environment	validation objectives (Step 2). Development of the RE questionnaire (Step 3). Note that this will be informed by previous activities and simulation results if available. **Added value to the SRM** – Demonstration of completeness of analysis through the use of a wide range of operational scenarios. RE provides a more comprehensive, reliable and structured analysis to demonstrate completeness. Additional or more detailed Use Cases and Operational Scenarios to support Validation Planning. Assessing the consequences of the abnormal and failure situations may uncover additional or revised requirements which sustain the adaptive capacity of the future operation. Check for compatibility of the specified functionality with the capabilities of equipment and the human	
For each abnormal scenario assess the impact on the ability of the functional system to continue to deliver the operational service in the operating environment	**RE Activity** – same as above **Practical Application** – same as above **Added value to the SRM** – same as above	0 1 **2** **3** **4**
Assess the risks associated with the system being unable to operate as required / degradation in system performance (failure case).	**RE Activity** – Identification of conditions and scenarios for which new or revised hazards (in traditional SRM terminology) can be derived **Practical Application** – Testing the operational concept against a range of conditions at the boundaries of performance identified through workshop and previous experience from operators **Added value to the SRM** – same as above	0 1 **2** **3** **4**
Identify and describe the potential causes of each hazard and capture all internal mitigations as either functional requirements (new or amended) or safety (integrity) requirements / assumptions.	**RE Activity** – RE takes a systemic and integrated perspective on the design. Hazards may be caused by system effects and might not be detected by a single task analysis. **Practical Application** – Hazards are analysed from the perspective of varying conditions, hence taking into account a wide spectrum of causes and consequences **Added value to the SRM** – same as above	0 1 **2** **3** **4**

Assess the adequacy of the design in the event of internal failures. Check that the functional system can operate safely under, and recover from all degraded modes of operation.	**RE Activity** – Analysis of the recovery strategies used by controllers in the event of failures. **Practical Application** – Scenarios at the boundaries of performance and the strategies used by controllers are captured and recommendations are developed. **Added value to the SRM** – same as above	0 1 2 **3** **4**
Identify any possible emergent properties in the SPR-level design. Provide assurance that there is sufficient separation in the design between safety-related functions and non-safety related functions (e.g. in data sources and flows).	**RE Activity** – The essence of RE is about examining emergence in complex systems. RE considers the socio-technical system as a whole and therefore it considers emergent properties. **Practical Application** – The principles of RE should be embedded into the development of validation requirements so that emergent properties of a design are captured and understood in simulations. For example, to allow the simulation to explore the difference between the use of the concept as designed and the actual use in simulations. **Added value to the SRM** – A better alignment of the concept with how it may be actually used in practice. The management of emergence in operational practice.	0 1 **2** **3** **4**
Demonstrate that all failure modes associated with the design have been identified and mitigated such that the safety objectives are still met.	**RE Activity** – Examination of varying conditions which can lead to new consequences and system behaviour which can describe how the system might fail **Practical Application** – The analysis of the varying conditions and the adaptive capacity provide additional data to support the traditional failure assessment processes. **Added value to the SRM** – Demonstration of completeness of analysis through the use of a wide range of operational scenarios. RE provides a more comprehensive, reliable and structured analysis to demonstrate completeness.	0 1 **2** **3** **4**

- Table 12: Alignment of Resilience Engineering Processes to the V2 SPR phase SRM stages

I.6.4 V3 – SPR & TS (P stage P7)

SRM Activity	**Correspondence with Guidance I**

• Define a set of safety requirements for the physical design that satisfy the safety requirements described at SPR-level • Define failure targets for hardware components and required reliability for the software elements of the technical system (e.g. a software assurance level) that are sufficient to satisfy the safety requirements from the SPR-level model • Look for emergent properties in the design which may not be revealed through the top-down analysis • Define ATC/flight crew procedure requirements. Demonstrate that these procedure requirements are both necessary and sufficient to ensure the safety of the operation of the technical system in normal and abnormal operating conditions • Show that HMI requirements are fit for purpose in supporting controller and other ATC tasks • Define competence requirements • Identify all reasonably foreseeable sources of common cause or other dependent failures. Show that measures are in place to mitigate these sources of failure. • Examination of the consequences of performance variability (deliberate or inadvertent) from the under specification of the technical system or from human tasks • Perform an analysis to determine whether the safety of the technical system has been improved SFAIRP. Demonstrate that the costs of an alternative design would be grossly disproportionate to any safety benefit which might be gained. • Provide assurance that the outputs of the assessment are complete, correct (necessary and sufficient) to describe the technical system	**Practical Application** – For all of V3: Check that resilient performance and adaptive capacity continue to be considered as the design evolves to the physical (more detailed) requirements for the concept. Ensure that the RE principles adopted in V2 continue to inform the lower-level design with new or revised validation objectives and design requirements specified as a consequence. The analysis of Adaptive Capacity (Step 3) may be performed more thoroughly and additional techniques used since more detailed information about the concept will be available in V3. Validation results should be considered with an awareness of the RE approach steps. **Output / SESAR Deliverable** – SPR (V3) & TS (V3)	**0** **1** **2** **3** **4**

Table 13: Alignment of Resilience Engineering Processes to the V3 phase SRM stages

Guidance J On the usage of Dynamic Risk Modelling (SESAR P16.01.03)

J.1 Forewords and introduction

Where performance variability of both people and equipment are combined, it may lead to varying levels of performance and deviation from normal practice. These in turn may ultimately lead to accidents or, alternatively, contribute to successful operations and greater System robustness.

Dynamic Risk Modelling (DRM) refers to the class of modelling techniques that explicitly models the dynamic performance of operation (people, equipment, procedures, and environment) and their time-dependent interactions.

The technique looks at a variety of possible combinations and permutations of events as they unfold through time. Where necessary (e.g. for the relevant sub-set of scenarios / use cases – see selection criteria below), DRM provides more accurate results that cannot be obtained through linear approaches.

As per **Guidance A** above, DRM can be used to verify that the Safety Requirements are complete and correct and mutually consistent by reference to the Safety Objectives and SAC.

Various DRM approaches are available. They aim at providing augmented insights, with a sharper and more accurate assessment of safety risk (both success and failure). The approaches include (but are not limited to):

- ICAO Collision Risk Modelling (CRM): incl. the guidance available in A Unified Framework for Collision Risk Modelling in Support of the (Doc 9689), ICAO Doc 9274: Manual on the Use of the Collision Risk Model (CRM) for ILS Operations,
- Encounter-model: guidance can be found in, e.g., ICAO Annex 10 VOL 4 to calculate the effect of ACAS on the risk of collision
- Agent-based DRM for which extended method description as well as a case study are available on the 16.01.03 Extranet (see below).

Other methods and tools might be used and P16.01.03 D02 provides an overview of those together with a first assessment of their viability for use in the SESAR work programme. This report is downloadable at:

https://extranet.sesarju.eu/WP_16/Project_16.01.03/Project%20Plan/Task%202%20Identify%20DRM%20for%20SESAR%20needs/T16.01.03-002%20Provide%20an%20overview%20of%20DRM%20methods%20and%20tools/P16.01.03-T002%20products/16%2001%2003-D02-REP-DRM%20forSESARneeds.doc

P16.01.03 in agreement with the SJU has only focused on the use of Agent-Based DRM, and for which:

1. Full Guidance has been developed in P16.01.03 D11 available at:

   https://extranet.sesarju.eu/WP_16/Project_16.01.03/Project%20Plan/Task%205%20Deliver%20final%20guidelines/T16.01.03-011%20Update%20and%20deliver%20final%20guidelines/D11-Final%20Guidelines%20Master/16%2001%2003%20D11%20Final%20guidelines%20for%20DRM%20application.docx

2. A case study has been conducted with the SESAR 1 OFA 01.02.01 - Conflicting ATC Clearances – and focussing on landing versus Line-up use case. The full report of the study case (P16.01.03 D09) is available at:

   https://extranet.sesarju.eu/WP_16/Project_16.01.03/Project%20Plan/Task%204%20Support%20DRM%20test%20case/T16.01.03-

008%20Produce%20DRM%20test%20case/T16.01.03-008%20Produce%20test%20case%20-%20Master%20version/16%2001%2003-D09-%20DRM%20test%20application_2014-06-25_working%20document.docx

As a result, and without being to the detriment of other techniques, this Guidance focuses on Agent-Based DRM only. It should evolve with the forthcoming annual releases of the Guidance Material with the inclusion of other approaches that can eventually be equally applicable.

As a result; it details the pre-requisites and the selection criteria and gives a summarized version of the description of the Agent-Based method. It is obvious that the deployment of the method will require far more insights and understanding. This will in particular require a thorough reading of 16.01.03 D11 and D09 above mentioned as well as appropriate operational, modelling and mathematical skills.

J.2 Pre-requisite and selection criteria

The deployment of Agent-Based DRM is an activity that requires the combination of a series of disciplines as well as time and resources. As a result:

a) The PRE-REQUISITE is that a safety assessment based on 'conventional' (static) methods and tools has been conducted to a level of details that enables to make an informed decision on whether to go to a DRM-based study using the selection criteria below. This 'conventional' assessment has brought into play, in particular, but not limited to, the relevant safety assurance activities as per **Guidance A** above.

b) INFORMATIVE SELECTION CRITERIA are needed. DRM is not '*for everything or everyone*', and identification of when it should be applied is necessary. Those selection criteria are:

Criterion 1.: *Safety can be expressed as a function of physical parameters*: The Project requires that safety risk results are expressed as function of some physical parameters (e.g. separation distance between two parallel routes, descent/climb rate, distance between crossing point and runway threshold…) in order to derive specific requirements regarding the optimal value (from a safety perspective) of those parameters.

Criterion 2.: *System involving complex dynamic interactions*: The System being assessed involves complex dynamic interactions (encompassing human-equipment, equipment-equipment and human-human interactions) which might be characterised according to the following sub-criteria:

2a. *System behaviour (success & failure) depends on system status over time*: The system behaviour, when considering equipment functional variability and failures, human performance variability and errors, involves occurrences which cannot be considered in isolation, as they depend on whether other occurrences have already arisen (*i.e.* stochastic dependencies)

2b. *System behaviour (success & failure) depends on process variables*: The system behaviour when considering equipment functional variability and failures, human performance variability and errors, depends on process variables (e.g. the effect of an avoidance instruction following a short term conflict alert (STCA) depends on avoidance instruction being appropriate, the relative position and movement of involved aircraft, the pilot response and the flight parameters)

Criterion 3.: *Safety "importance" of the Change*: The safety importance of the change associated to the project shall be high. High is defined in terms of reducing or increasing safety risk in relation to the performance of AIM safety barriers. At the OFA level, these are described in B4.1 safety targets, or in terms of the severity of the operational hazards that are impacted or the new ones that emerge. Whether the safety importance is high enough to apply DRM is left to the appreciation of the Project. The Project must be supported by appropriate expert judgment and be aware of the resources that can be reasonably allocated to the safety assessment.

It is worth noting that the above selection criteria apply equally to other techniques presented in P16.01.03 D02 (see link above).

The following table *only* provides a support to decision-making by intending to link the above criteria to the DRM method that might be recommended. However, the ultimate decision on the selection should integrate the consideration of System thinking, constraints of operational effectiveness, time, and cost as well as required rigour attached to the evidence to be derived.

Cr1: Safety expressed as f(physical parameter)	*Cr2: System with complex dynamic interactions*	*Cr3: Safety importance of the Change is high*	*First advise*
YES	NO	YES	**GO** for **ICAO CRM** or **Encounter model-based**
NO	YES	YES	**GO** for **Agent-based DRM**
YES	YES	YES	**GO** for **Agent-based DRM**
Any remaining combination			**NO GO** for DRM

J.3 Description of the method

The following steps provide a high level view of the DRM method:

1. Preparatory activities to scope the application of DRM
2. Develop the dynamic risk model
3. Develop risk decomposition
4. Implement the dynamic risk model into software
5. Run Monte Carlo simulations
6. Assess bias and uncertainty
7. Develop safety risk results

Each of these steps is now further explored below. A full description of each step can be found in 16.01.03 deliverables.

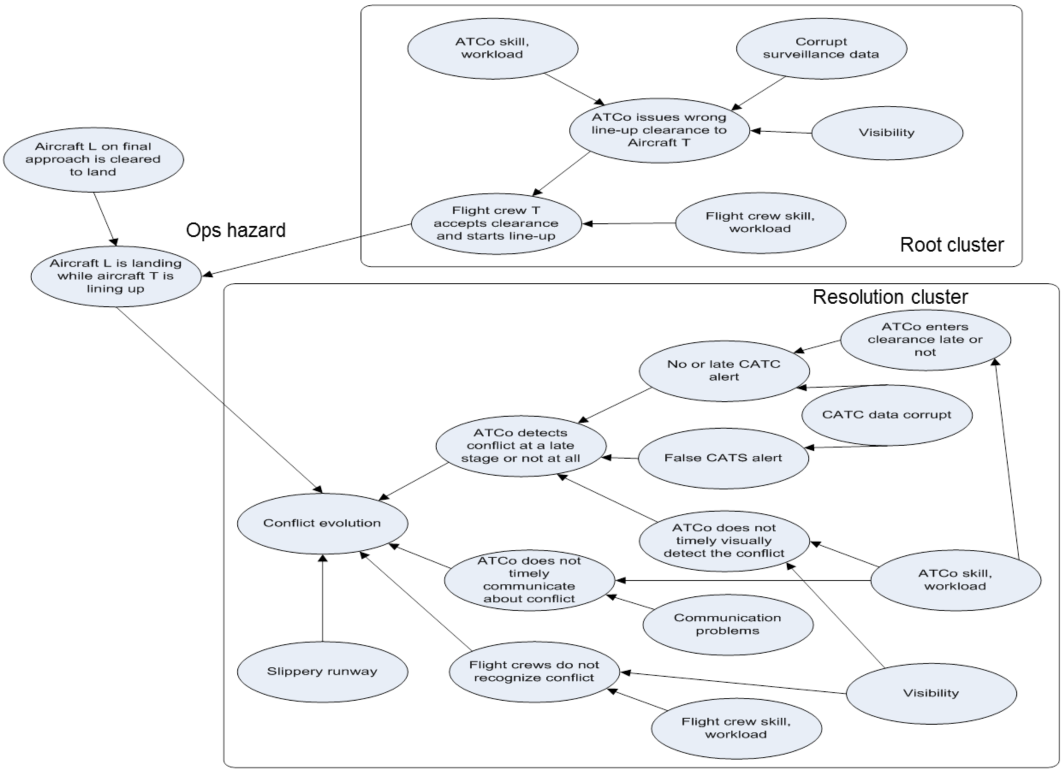
J.3.1: Preparatory activities

This includes:

- Scoping of the DRM assessment; this can be, for instance (but not limited to), the selection of a sub-set of uses cases as per the OSED or a specific aspect of a given use case
- The collection from the 'conventional' (static) safety assessment work already conducted of all relevant (as per the scope defined above) success- and failure-related safety information. This should encompass the definition of System operations in normal/abnormal conditions as well as list of hazards, with relevant causes, effects and mitigations.

- Clearly defining the objectives (i.e. type of evidence) of DRM (e.g. estimation of risk related to an undesired state)
- Developing operational hazard scenarios. Operational Hazard Scenarios are constructed with a view to preparing the agent-based DRM modelling. An Operational Hazard Scenario describes the evolution of an operational hazard, under the influence of related operational conditions (such as flight phase and location, number of traffic, environmental conditions, etc.) and the related hazards (i.e. root hazards, resolution hazards, pre-existing hazards). Each such scenario aims to bring into play all the relevant ways that an operational hazard (e.g. an aircraft conflict) may develop and evolve, under the influence of the related operational conditions and hazards.

  An illustration of an operational scenario is given below (for further details, refer to P16.01.03 D09).


ATCo skill, workload
Corrupt surveillance data
ATCo issues wrong line-up clearance to Aircraft T
Visibility
Aircraft L on final approach is cleared to land
Flight crew T accepts clearance and starts line-up
Flight crew skill, workload
Ops hazard
Root cluster
Aircraft L is landing while aircraft T is lining up
Resolution cluster
ATCo enters clearance late or not
No or late CATC alert
CATC data corrupt
ATCo detects conflict at a late stage or not at all
False CATS alert
Conflict evolution
ATCo does not timely visually detect the conflict
ATCo does not timely communicate about conflict
ATCo skill, workload
Communication problems
Slippery runway
Flight crews do not recognize conflict
Visibility
Flight crew skill, workload

- Appropriate data mining techniques for those parameters making up the dynamic risk model (as per J.3.2 below) as well as the type of distributions to be used for the relevant parameters (normal Gaussian, triangular, etc.)

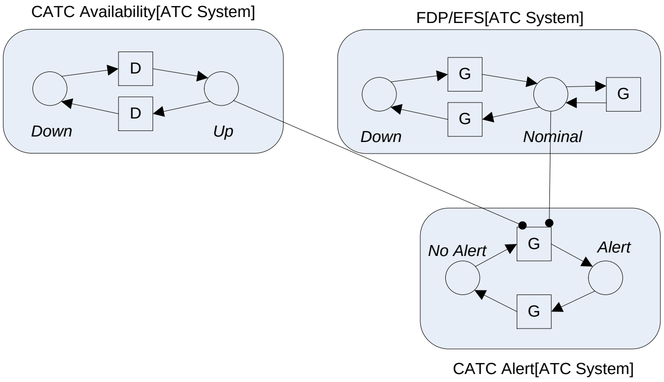
J.3.2: Develop the dynamic risk model

A multi-agent stochastic dynamic model is developed, which describes the stochastic dynamic evolution through time of one (or a selected set of) Operational Hazard Scenarios. Multi-agent refers to an operation or system that consists of multiple interacting agents. An agent is a distinctive element in the operation, which has its own states and situation awareness, operates relatively independently from other agents and interacts with other agents where applicable. The model uses the syntax of Stochastic Dynamically Coloured Petri Net (SDCPN) (for further details, refer to P16.01.03 D09 and D11 as well as references in **J.6**). This is developed with the following six iterative steps that are:

1. Identify the relevant Agents
2. Identify the relevant entities per Agent
3. Specify a Local dynamically coloured Petri Net (LPN) per entity

4. Interconnect the LPNs within each Agent
5. Interconnect the Agent models
6. Check how the operation and each hazard has been modelled, and iterate

The syntax of the Dynamically Coloured Petri Net (DCPN) consists of Places (circles), Transitions (squares) and Arcs (arrows) that connect the Places with the Transitions is fully defined and explained in P16.01.03 D11. For illustration only, the figure below shows a LPN network for the Conflicting ATC Clearances detection system and interactions with the Flight Data Processing (FDP)/Electronic Flight Strips System (EFS).



J.3.3: Develop risk decomposition

Once the SDCPN-based model is completed, it can then be used as basis for a Monte Carlo (MC) simulation to determine the probability of occurrence of a safety event, e.g. an aircraft collision. In principle, the number of occurrences of the safety event are counted and divided by the number of runs (or by the number of associated flight hours or movements). The accurate assessment of such low collision probability values through brute force Monte Carlo simulation of a dynamic risk model might require high investment in terms of simulation times or computing resources. To overcome this resource demand and speed up MC simulations, risk decomposition is applied.

Risk decomposition involves identifying some conditions or states in which the system can enter or which it can leave as a result of events (normal evolution, reconfiguration, failure) occurring in a specific group of agents with no dependence on the status/evolution of the remaining agent entities. When such an appropriate set of conditions *(Condition_k)* has been identified, they would be pre-conditions of the occurrence of the Safety Event (e.g. collision), with the probability:

$$P(\text{Safety Event}) = \sum_k P(\text{Condition\_k}) \cdot P(\text{Safety Event} \mid \text{Condition\_k})$$

(where (Condition_k) and (Safety Event | *Condition_k) are independent*

The probabilities on the right-hand side of the equation are determined as follows:

- The probabilities *P(Condition_k)* can be determined analytically (given the way these conditions have been selected),
- The probabilities *P(Safety Event* | *Condition_k)* are determined (“simulated”) separately for each *k*. The procedure is to make a conditional SDCPN model that starts in the situation of *(Condition_k)*, and then to run MC simulations on the conditional SDCPN model to count occurrences of the Safety Event. This process determines *P(Safety Event* | *Condition_k)*.

J.3.4: Implement the dynamic risk model into software

In this step, when the specification of the DCPN-based model and the risk decomposition are fully defined, they are implemented in software language in order to be able to run Monte Carlo simulations. Many software languages are suitable for this, as long as they accept all SDCPN syntax principles. A major step in the software implementation is to test the code against all elements of the SDCPN-based model and Risk decomposition. For instance, for the study case described in P16.01.03 D09, the model has been coded in Delphi using Embarcadero RAD Studio XE3

J.3.5: Run Monte Carlo simulations

In this step, the software implementation of the DCPN-based model is used to perform Monte Carlo simulations and compute safety risk results. Any Safety Event that can be observed in such simulation can be counted, and the number of counts, divided by the number of runs or the number of associated flight hours or movements, provides an estimate for the probability of occurrence of the Safety Event (e.g. a collision).

In addition, several potentially representative parameters need to be varied (e.g. at least between a baseline, a low and a high value), in order to observe trends regarding impact on the safety event probability. These trends provide the most valuable indication on the validity of the model, i.e. whether it correctly represents the reality. In case errors are identified, the dynamic risk model needs to be corrected and the subsequent risk decomposition updated accordingly.

J.3.6: Assess bias and uncertainty

By definition, any model is not the exact image of reality. The purpose of a bias and uncertainty assessment is to identify how the differences would impact on the evaluation of the risk level in terms of bias and uncertainty:

- Bias: the model-based accident risk is systematically higher or lower than the risk of the real operation.
- Uncertainty: the model-based accident risk lies in a range of credible values for the risk of the real operation (e.g. a 95 % credibility interval).

This is done by assessing each parameter value in the dynamic risk model on uncertainty (represented by a credibility interval around the chosen value) and sensitivity (how much does the Safety Event probability change if the parameter value changes), and by assessing each model assumption (i.e. modelling choice with potential to create a difference between model and reality) on bias and direction. In line with the logic explained at the Risk decomposition step, these assessments might be performed analytically or might require dedicate MC simulations.

All results are combined to determine the bias and uncertainty around the Safety Event probability. Those parameters and assumptions with the highest bias and uncertainty contribution can be used to determine the most effective improvements in the model (either in improving its structure or in guiding additional data collection, where possible). In addition, the final safety risk results (as per next step) shall not be interpreted in isolation but combined with the bias and uncertainty results.

Last but not least, when modelling errors are discovered late in the process and are controllable, they can be fixed by affecting the results with the adequate bias.

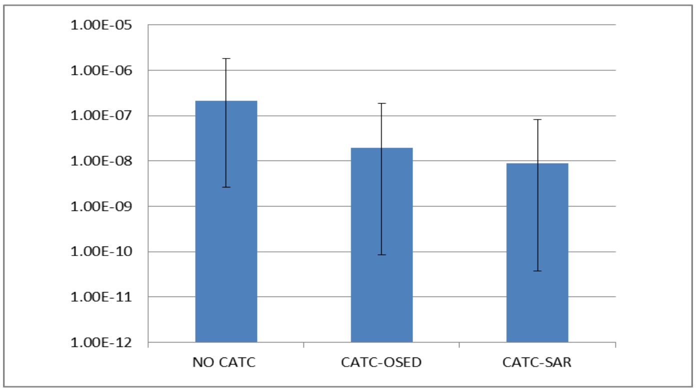
J.3.7: Develop safety risk results

The results of the previous steps provide point estimates and credibility intervals for the probabilities of safety events in various conditions. Checking these results against safety criteria (expressed in absolute or relative terms) provides insight in risk tolerability and risk margins.

Furthermore, the results of the sensitivity analysis for variation of particular parameter values (e.g. those conducted within the Bias & Uncertainty step) can be used to identify safety bottlenecks (aspects of the operation that contribute to unacceptable risk levels) and they provide a basis to determine any additional safety requirements and safety objectives.

Finally, remaining safety issues from the 'conventional' (static) safety assessment can be addressed taking advantage of the capability to account for the time-dependant behaviours and/or dynamic interactions (e.g. regarding effectiveness of a recovery procedure involving a combination of system data processing & information display, Controller detection & decision & instruction and Pilot implementation or concurrent action based on its own situation awareness).

For illustration only within this Guidance, the figure below shows the risk comparison for three different scenarios that have been analysed in the case study.



J.4 Required skills and competence

This section provides a description of the main skills and competence require to deploy a DRM capability appropriately.

1. **Resources & Skills** –DRM modelling is technically demanding work that requires significant resources and skills. The necessary DRM skills can be acquired through adequate training. The pre-requisites are: being familiar with (classical) safety assessment and having a strong mathematical background. Note that the amount of resources required, in terms of person hours and throughput time, depends highly on the complexity of the operation to be analysed, the previous experience of the DRM practitioner and the possibility in re-using previous related sub-models.
2. Currently, **SW implementation** of the model and subsequent modifications are cumbersome and create work. This is because there is no automatic coding of the DCPN into software. This coding of the DCPN into software would be unnecessary if graphical tools to implement the DCPN model were available. These tools would increase productivity significantly by supporting iterative model building, validation of input parameters and risk decomposition.
3. **Availability of data** – Similar to static approaches, it is often hard to give values to input parameters when data is not available. Many parameter values are therefore estimated by experts, but validation of these values is very difficult. This is partly mitigated through the Bias & Uncertainty (B&U) assessment; in case the safety results appear to be sensitive to a parameter

J.5 Conclusions

This chapter of the Guidance material for the application of the SRM has summarised the DRM approach developed for SESAR. It is acknowledged that Agent Based DRM is not the only method that is available and similarly is not the only method that may be deployed within SESAR. However, the research project 16.01.03 in collaboration with the SJU determined that Agent based DRM was the approach to be further explored in SESAR.

The method requires careful consideration before application and this guidance contains criteria that support the choice of method and the choice of project upon which this powerful tool could be deployed.

DRM has the ability to provide insights to safety that static methods do not afford (in particular addressing dynamic interactions, variability of performance, coupling aspects, etc.).

J.6 Additional References

In addition to references made above to both P16.01.03 and ICAO documentations, the following can provide useful information for the deployment of Agent-based DRM:

- [Blom et al., 2006] H.A.P. Blom, S.H. Stroeve, H.H. De Jong, Safety risk assessment by Monte Carlo simulation of complex safety critical operations, Proc. 14th Safety-critical Systems Symposium, Bristol, UK, February 2006, Eds: F. Redmill and T. Anderson, Springer, London, 2006
- [Everdij, 2010] M.H.C. Everdij, Compositional modelling using Petri nets with the analysis power of stochastic hybrid processes, PhD Thesis, June 2010, available at http://www.nlr-atsi.nl/eCache/ATS/15/060.pdf
- [Everdij et al, 2006] M.H.C. Everdij, H.A.P. Blom, S.H. Stroeve, Structured assessment of bias and uncertainty in Monte Carlo simulated accident risk, Proc. 8th Int. Conf. on Probabilistic Safety Assessment and Management (PSAM8), May 2006, New Orleans, USA.

Guidance K On Safety and Human Performance (HP)

K.1 Introduction

ATM will continue to depend upon the successful management and use of systems by "human operators", which will relate directly (or indirectly) to the Safety of the Operational service. It is not sufficient therefore to simply ensure that technical equipment delivers functionality reliably in order to guarantee Safety. The relationship between people, equipment and procedures must be assured such that where Safety depends upon the actions of the operator (controllers, engineers and all other related human roles) that those actions can be delivered reliably, with the desired outcomes within the required timeframes. This infers that in delivering safety, one must ensure Human Performance (HP). This is addressed in sections **K.1.1** and **K.2** below.

In addition, Guidance **K.3** proposes a process that facilitates the claim of a quantitative reduction in risk for the human contribution within a Fault Tree without placing a direct quantitative failure rate on the human. It may be used wherever a human failure event contributes, in conjunction with an equipment failure, to a higher level failure in the fault tree.

K.1.1 Safety assessment & HP overview

Safety assessments need to be coherent, integrated and holistic so that there are clear links between the Safety analysis, design/engineering substantiation and demands made upon the operators. Therefore, the understanding and adequacy of Safety claims made on operators, procedures and other resources should be demonstrated, to a degree that is proportionate with the potential for hazard.

The Safety assessment should clearly indicate the claims made on operator action and procedures and demonstrate understanding of the role and contribution of the operator to assuring Safety and detail how these have been substantiated.

An important point to note is that system performance includes HP. It should be recognised that engineered Safety systems can be affected differently by human, management and organisational failures. Therefore, the HP analysis should also consider how HP may affect the operation and availability of engineered systems and vice versa.

The Safety claims on operator action, including operational actions if not performed as planned that may initiate significant hazards, and procedures should be clearly identified and link to supporting analysis. The analysis should demonstrate that claims being made on operators have been understood and can be delivered feasibly with evidence provided by a systematic analysis process. The Safety assessment will show how HP issues (relevant to Safety) have been assessed, supported and/or mitigated to ensure that reliance on operators and human.

Early in the design phase of projects, a high level task listing can be used to predict where human involvement will be expected, and how these relate to the initiation of Safety significant tasks. Where Safety significant tasks can be identified, then these should be subject to a more detailed qualitative HP assessment.

A generic HP approach to the analysis of Safety issues is presented in more detail within subsequent section of this guidance. Following this approach also ensures a mutual and reciprocal development of the HP and Safety approaches within an assessment. The approach is summarised here for completeness.

- Scoping and screening: Data and information collection, walk-throughs talk-through, interview, observations, workshops.
- Review of HP argument structure in Appendix A of the HP Reference Material (**Ref. 10**):
  - Arg1: The role of the human is consistent with human capabilities and limitations
  - Arg2: Technical systems support the human actors in performing their tasks

        - Arg3: Team structures and team communication support the human actors in performing their tasks
        - Arg 4: HP related transition factors are considered
    - Task representation, where appropriate (considering the Solution / OIs), using, for example: Cognitive or hierarchical task analysis, tabular task analysis, time line Analysis, critical thread analysis.
    - Issues generation & analysis; to be substantiated during the project lifecycle and validated as simulation requirements
    - Design mitigation expressed as issues in the HP issues log for subsequent assessment duing valdiation exercises.

The process described above effectively targets HP assessment to address issues that that the Safety assessor considers critical. The application of the HP assessment process by a suitably qualified practitioner will assist in identifying common HP and safety issues.

The assessment performed here, could be conducted in order to substantiate: the feasibility of operator actions; that task design and organisation, and operator support for the task will result in optimised HP; that all significant HP variability has been identified and that it can be demonstrated that it is mitigated through the application of good System design. It should be remembered that the HP assessment process is not limited to consideration of the user interface but also addresses communication, selection, training, and impacts of automation.

For projects where no Safety significant tasks are identified, e.g. low risk modifications, classified according to the SRM RCS (Appendix E.4) or a low category engineered Safety system that involves little human action to deliver the Safety function, the HP assessment might be limited to an audit process rather than a full assessment. As stated earlier however, the operator is central to delivering Safety within the ATM environment and it must be very clear that the Safety assessment makes no calls on the operator.

K.2 V Cycle HP and Safety Assessment

It is not possible to prescribe how HP activities should be integrated into every project and or Safety assessment. The precise requirements and depth of detail and analysis that is required will be dependent on the size, complexity and Safety aspects identified within the project. It remains therefore be the responsibility of the relevant safety assessment lead and HP lead to determine the precise requirements and specification of the HP content for any particular Safety assessment.

The aim of this Section is to describe the approach that could be taken to integrate HP into a Safety assessment. In general, successful integration of HP into a project will require the HP assessment activities are referenced within the Safety plan. Information in the remainder of this Section describes typical HP activities that could be performed within each phase of a lifecycle stages and how these interface with similarly staged Safety deliverables.

K.2.1 V1

The following bullets summarise the requirements for HP & Safety at the end of V1.

- Scoping

Agreement and alignment on the concept and the assumptions associated with the Solution. This mutual understanding is best derived through preparation meetings with between HP & Safety before the scoping and change assessment, followed by joint attendance at the scoping and change assessment meetings. HP support may (bus is not obliged to) produce a high level task analysis to better understand the wider implications of the proposed change.

- Safety Target setting

HP will work with Safety in determining the human impact of the proposed changes. As an outcome this will determine the HP arguments affected by safety given the proposed change, and help ensure a complete set of SAC defined using the AIM model. Jointly determining the SAC and the HP arguments affected by safety will ensure that the HP and Safety assessments are aligned from the outset.

- Planning activities

Derive and produce a high level HP and Safety plan that describe specifically what areas need to be investigated from a Safety and HP perspective. Ensure that the plans are cross references to show what HP activities will provide for the Safety assessment process.

At the end of V1, the scop of the HP assessment required to support Safety should be documented.

K.2.2 V2

The following bullets summarise the requirements for HP & Safety interaction at the end of V2.

- Detailed planning

Based on a high level HP analysis refined and augmented from V1 a fuller description of the impacts of the proposed changes on potential operational roles can be derived. The impacts of the change will be recorded within the “HP log”, a repository of HF issues, managed by the HP specialist. Safety and HP should work together to review the log and prioritise the issues with respect to Safety.

Safety may adopt the content of the HP issues to support the definition of Safety objectives. During V2, a fuller discussion between Safety and HP should also take place on identifying normal and abnormal conditions (of the operational environment).

HP variability may affect hazards, and similarly, the discussions surrounding hazard identification will reveal assumptions about human behaviour made by the Solution. In this case, HP should be invited to participate in hazard identification meetings run by Safety, and similarly Safety should be invited to HP workshops to discuss HP assessment. The HP log for HP will be updated with the output of the hazard identification exercise and assumption made by the project recorded. Assumption should be subsequently tested within a validation environment and ultimately expressed as design requirements.

The HP specialist should develop a plan of activities to address the HP issues identified during project meetings in order to satisfy the HP argument structure. The resulting activities are recorded as a HP assessment plan and form an annexe to HP validation plan. HP and Safety should review the proposed activities for HP to ensure adequate coverage of the priority areas for Safety.

- Execution of activities

During this phase both HP and Safety deliver the analysis proposed within their planning documentation. HP should ensure that Safety is aware of the outcomes of the analysis relating to roles, responsibilities and allocated tasks in normal and abnormal condition. Most importantly HP should communicate to Safety, where information necessary to successfully perform operational tasks is required

The Safety expert should ensure that as requirements arise that make demands upon the operator that they are communicated to the HP specialist assigned to the SESAR solution. In this way, where a demand is made on an operator to fulfil a Safety function, the necessary substantiation activities can be delivered by the HP specialist. In delivering a substantiated Safety requirement, the project can affect its design in response to a well-articulated Safety requirement backed up by HP evidence.

At the end of V2 it is expected that HP and Safety have coordinated and mutually supported, planning and execution of assessment activities such that Safety related HP needs are cross referenced and addressed by Safety, and Safety activities focussing on operational staff are cross referenced by HP. This mutual approach to planning and executing assessments ensures a complete and coherent set of requirements at V3.

K.2.3 V3

The following bullets summarise the requirements for HP & Safety interaction at the end of V3.

- Validation exercises

During validation exercises the HP log forms the basis for derivation of HP assessment objectives. It is important therefore that it is complete with respect to priorities established by Safety. Establishing Safety priorities for issues and benefits in the HP log can effectively scopes the HP objectives for validation exercises ensuring resources are available for safety issues.

- Specification of requirements

At the end of V3 a set of requirements for the physical design should have been articulated. The requirements for HP will be articulated as a function of the argument structure, and will necessarily cover people, equipment and procedures. HP and Safety should have coordinated a joint approach to assessment, and HP requirements supporting Safety should be cross referenced.

- Generation of evidence

At the end of V3 the Solution should expect to receive Safety requirements. Where a Safety requirement makes a demand on operational staff, then the actions required by the operator should have been substantiated by HP analysis. Thus evidence exists that the requirement can be fulfilled by the operator. Safety support to a Solution should ensure that the required evidence from HP is available in the validation exercise report.

- Transition readiness

At the end of V3 HP and Safety are expected to make judgement as to whether the concept is sufficiently mature to progress to V4. HP & Safety should coordinate their assessment to ensure that a coherent view is presented to the project.

At the end of V3 the requirements for the project (Solution) should be complete Safety requirements make demands on operational staff these should be substantiated with evidence from HP.

K.3 Hybrid Fault Tree method

The quantification of the human error is not required by regulation and not generally accepted by the Authorities. Effectively, in a human and software rich environment such as the aviation System, there is an apparently unsurmountable problem of how to quantify a fault tree when several elements 'should not' be quantified.

This section summarises the Hybrid Fault Tree Method as a means to resolve the problem of no acceptable method being available to quantify human error within the fault tree (causal analysis). The full description of the methodology (**[Ref. 1]** in section Error! Reference source not found.) can be found at:

https://extranet.sesarju.eu/WP_16/Project_16.06.01/Project%20Plan/SESAR%20Safety%20Reference%20Material/Hybrid%20Fault%20Tree%20Ed00.01.00.docx

The term *hybrid* as used throughout this guidance refers to the use of both qualitative and quantitative means within a fault tree to apportion / allocate the quantitative safety objective from the top to the several qualitative and quantitative safety requirements.

The main lines of the Qualitative / Quantitative Allocation Process are described below.

Related SRM principles – safety assurance activities are detailed below:

P5P6	**AO5**	**a1**	Identify all potential causes of each hazard derived under Assurance objectives P3P4_AO1 and AO2_ above (deductive analysis)
P5P6	**AO5**	**a2**	Specify Safety Requirements (*Integrity* property from the failure approach) and / or Assumptions for the causes of each hazard, such that the Safety Objectives (and/or SAfety Criteria) are satisfied, taking account of any internal mitigation

			means.
P5P6	**AO5**	**a3**	Capture all internal mitigations as either functional, performance or safety requirements (*integrity property* from the failure approach) or Assumptions, as appropriate

K.3.1 Establishing the Prerequisites

The purpose is to derive safety requirements to satisfy the safety objectives defined for each hazard.

The operational hazards are identified and for each hazard a severity class and a Safety Objective (SO) have been allocated in accordance with the SRM principle (see **Guidance E**). The conventional Fault Tree for each hazard is produced; and the basic causes leading to top event are identified.

The safety related human tasks that interface with technical element are identified. The HF data from field experience that provides evidence that design of the functional system is efficient are available for use in evaluating the human mitigation effectiveness. For new concepts, the HP assessment process has been carried out and the HP process outcomes are available to provide evidence of the appropriateness of the design.

K.3.2 Process Overview

The process of allocating criticality for lower level events follows standard fault tree processes where no human mitigation is present. Where a gate exists that considers human mitigation in one of the events directly below it the hybrid fault tree processes are used to determine the cascade of criticality from the top event to the lower level events.

In the example below F represents a fault condition in hardware, and H represents a human failure event.

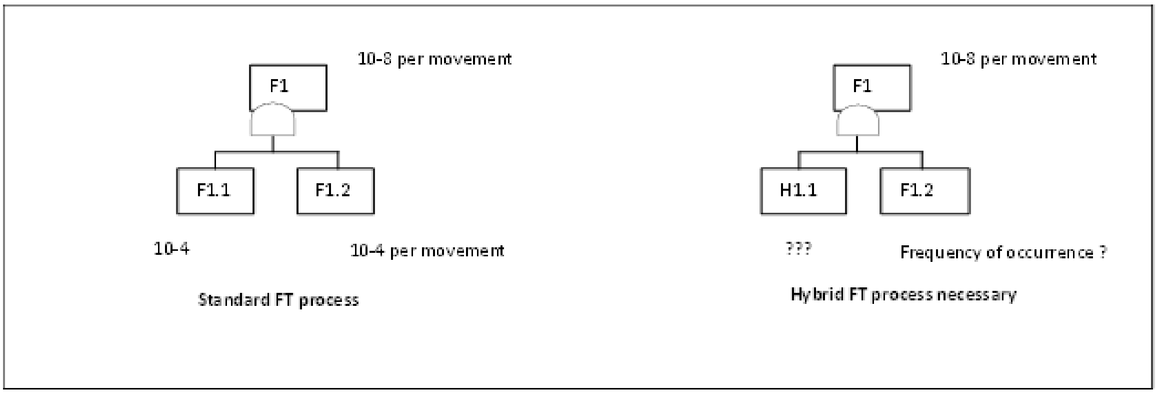


Figure 17: Example of a propagation of criticality for an AND gate

The relevance of the HP evidence and its quality drives the allocation.

The HF data from field experience that provides evidence that design of the functional system is efficient is to be used in evaluating the human mitigation effectiveness.

For new concepts, the HP assessment process is been carried out and the HP process outcomes are available for providing evidences of the appropriateness of the design.

Note that the evaluation of human mitigation effectiveness and the allocation of criticality in the fault tree based on this effectiveness is an iterative process that takes into account the evidences being providing all long the HP assessment process.

The main steps are:

- Step 1: Allocating criticality
- Step 2: Propagating criticality
- Step 3: Setting requirements for equipment elements
- Step 4: Setting requirements for Human tasks / procedures

K.3.3 Step 1: Allocating Criticality

The Level of Criticality is allocated based on the quantitative SO derived from the standard SO setting process in the SRM.

Level of Criticality		Frequency
Extreme Criticality	E1	< 10^{-9} per movement
	E2	< 10^{-8} per movement
High Criticality	H1	< 10^{-7} per movement
	H2	< 10^{-6} per movement
Medium Criticality	M1	< 10^{-5} per movement
	M2	< 10^{-4} per movement
Low Criticality	L1	< 10^{-3} per movement

Table 14: Frequency & level of criticality

Conversion of the frequency of occurrence to different units is to be done as necessary depending on the different AIM metrics used to define the Safety Objective (per approach, per flight, per flight hour) and the needs of the project safety assessment.

K.3.4 Step 2: Propagating Criticality

Propagate the level of criticality of the top event in the Fault Tree down to the base events. The aim here is to determine a tolerable level of criticality for lower level event using a set of four principles.

The relevance of the HP evidence and its quality drives the allocation of one of four principles. Each of these principles provides an approach to allow consideration of a quantitative value for the technical part of a join human / equipment failure.

Rules

A set of rules are proposed in the hybrid FT method. They suggest an approach for preventing unsafe design and for "Downgrading" the Criticality level through the fault tree on the several elements based on the quality of evidence from the HP assessment.

Rule A –

For an OR gate, the Level of Criticality of each "child" event shall be the same as the Level of Criticality of the "parent" event, except for OR Gate having 5 or more branches.

In this case, a higher Level of criticality is to be allocated to all the children

Rule B –

For an AND gate, the Level of Criticality of the "parent" event shall be propagated at child level provided the child events are independent and the human mitigation principles defined are applied with a possible downgrading of the level of criticality.

The mechanisms for this possible downgrading of the criticality are described in Principle 2, 3 and 4 applies

The approach can only be used to downgrade the criticality level to 1 class or 2 levels of criticality maximum.

Rule C –

Rules above shall not prevent to propagate quantitative value when "quantitative" mitigations are duly justified.

A part from the rules presented above, a set of 4 Principles are also proposed in the hybrid FT method supporting the mentioned rules:

P1 – Preventing unsafe design

(P1a) No single human error should lead directly to an event defined as extremely critical

(P1b). No flight crew / ATCO error combining with a maintenance staff error should lead directly to an event defined as extremely critical

Note related to P1b: the design of the maintenance procedures has to be included within the scope of the system design.

In this case P1 forms a design goal to minimise the contribution of human error to systems failure. It is not dependent upon evidence, it is a design goal, i.e. no evidence is required.

P2 – Evidence exists of the human contribution to safety

P2: The human contributes positively to the safety objective; evidence is available and is of a high or medium quality.

P3 – No evidence for the human contribution to safety

P3: The human may contribute positively to the safety objective, but no evidence is available or is of low quality

At the lowest level of the fault tree, if:

- A "Parent" event has a critically class which has been defined as extremely critical (E1) and that the "child" event for the Human element has been set with a HIGH level of evidence quality then the "child" event for the technical event will have to be defined as "HIGH (H1)" (e.g. criticality of the Equipment being two levels lover that the "parent" failure). Credit is taken for the human mitigation by two levels of criticality.
- A "Parent" event has a critically class which has been defined as extremely critical (E1) and that the "child" event for the Human element has been set with a MEDIUM level of evidence quality then the "child" event for the technical event will have to be defined as extremely critical (E2) (e.g. criticality of the Equipment being one level lower that the "parent" failure). Credit is taken for the human mitigation by one level of criticality
- A "Parent" event has a critically class which has been defined as extremely critical (E1) and that the "child" event for the Human element has been set with a LOW level of evidence quality then the "child" event for the technical event will have to be defined as extremely critical (E1) (e.g. criticality of the Equipment being at same level that the "parent" failure). No credit is taken of the human mitigation.

P4 – A change that affects behaviour, but is not a result of equipment

Human Mitigation principle (P4) is defined in order to consider a change in the operational concept that is based on existing equipment: .e. g. a new procedure to be followed by pilots or controllers which requires no technical system changes.

In this case, there is no requirement for new equipment, in the ground or in the air. Changes are likely to impact most heavily on procedures and training. In this case, the HP assessment is expected to provide detailed insight, not only into the requirements for training and changes to procedures, but also that the change has been:

- Analysed,
- Assessed; and
- Demonstrated to be effective in a real or simulated setting.

P4 provides the opportunity to complement the existing top down approach for with a bottom up approach. These two complementary approaches are considered in this Hybrid Fault Tree methodology. The top-down approach is for designing an ATM functional system which implements new technical design and the bottom-up approach is for designing an upgraded ATM functional system which uses existing technical design.

The P1 to P3 principles apply to the top-down approach while P4 applies to the bottom-up approach.

K.3.5 Step 3: setting requirements for technical elements

The quantitative requirement is established in terms of maximum probability of occurrence using the same unit of measurement for both the airborne and ground technical elements. When direct quantification is not possible, quantitative requirements are based on the allocated level of criticality. The qualitative requirement is established as per the current quality assurance practices for airborne and ground technical elements. E.g. for an extreme criticality – the quantitative requirement at E1 would be “< 10-9 per *AIM Metrics*”.

This step is further described in **[Ref. 1]** in section **K.5**.

The qualitative requirement for the software (and development process for the airborne equipment) is established as per the current quality assurance practices for the airborne and the ground technical elements.

The same AIM metrics (units of per approach, movement, fight or flight hour) as determined in Step 1 for the top event operational hazard are used to express the quantitative requirements for the equipment / system failure; together with an agreed unit conversion formula to properly allocate the safety requirement of the ground equipment / system when supporting Air Traffic Services.

Depending on the Accident Type (AIM Model) the SESAR solution is associated with, the metrics used to set the MTFoO values are of different units. Conventionally, the unit used for En-Route & TMA is: per Flight Hour, for Surface it is: per movement but it may be in different ways using conversion factors between the metrics. The conversion factor is not fixed; it is normally adapted for each SESAR solution within its targeted environment.

Further detail on this process is described in **[Ref. 1]** in section **K.5**.

K.3.6 Step 4: setting requirements for human tasks / procedures

This step allocates the qualitative requirements for human tasks/procedures to achieve the top level safety objectives. The process is driven by considering the availability and quality of evidence from the human performance assessment that has been conducted in support of the design project.

Evidence from the HP assessment should be directly relevant and sufficiently detailed to provide clarity on the failure being investigated in the fault tree. This provides a measure of Evidence Quality (EQ) of High (H) Medium (M) or Low (L). Where evidence is not considered relevant or of sufficiently high quality, i.e. it does not address all the areas of interest to safety, it should not prevent the safety expert requesting further information from the HP Assessment team.

The relevance of the HP evidence and its quality drives the allocation of one of four principles. Each of these principles provides an approach to allow consideration of a quantitative value for the technical part of a join human / equipment failure.

HP evidence is considered as follows:

- HP evidence should have arisen from a HP evaluation or observation.
- An EQ judgment is possible from an analysis of the HP assessment as judged by the safety specialists.
- An EQ judgment is possible and reflects the effectiveness of the assessed or observed mitigation by human actions. The EQ shall be judged high, medium or low in terms of quality of the evidence for the effectiveness to the proposed solution / design.
- High quality evidence from HP Assessments (well written, well analysed, complete etc.) that do not demonstrate the effectiveness of the proposed human mitigation actions shall not permit a down grading of criticality.
- On the airborne side, risk reduction results from observation containing commonly agreed quantification (e.g. figures from ICAO docs).
- On the ground side, risk reduction may result from formal methods, expert judgment or previously agreed values.

More detail on the derivation of the standard and source of Evidence is presented in in **[Ref. 1]** in section **K.5**.

Content of the HP Assessment	EQ	Guidance for HP Requirement
The assessment found evidence of a highly effective concept present in the design which specifically addresses the human component of the issue	High	Adequate System Design Procedures and training of the human operator in the specified task is sufficient to achieve the safety objective
The assessment found evidence of an effective design or a request for change in concept related to the issue.	Medium	Adequate training of the human operator in the specified task coupled with associated adequate mitigation means is sufficient to achieve the safety objective
The assessment found no evidence concerning design effectiveness relating to the issue. Open issues and /or Assumptions requiring further attention and validation are described in the HP report.	Low	Further validation is required to address Open Issues and Assumptions to achieve the safety objective.

Table 15: HP Assessment Evidence Quality considerations

K.4 Closing remarks

In identifying and assuring the human actions required to deliver Safe operations, the assumption and inherent design constraints (requirements) can be captured within the Safety assessment process and the resulting Safety Case. It is necessary therefore for PJ19.3 to identify areas of operation where Safety may be impacted by the "human" component of the system. Similarly, where Safety identifies areas where Safety is delivered as a function of the operator, these functions need to be substantiated by PJ19.3. This guidance has explained how the Safety-related issues, from HP analyses, might be integrated into the Safety Lifecycle. In addition, this guidance has summarized the so-called Hybrid Fault Tree approach to dealing with human errors in fault tree when several elements will not be quantified.

K.5 Reference for this Guidance

[Ref. 1] SESAR 1 P16.06.01, Hybrid Fault Tree Methodology, Ed00.01.00, March 2016 – available at

https://extranet.sesarju.eu/WP_16/Project_16.06.01/Project%20Plan/SESAR%20Safety%20Reference%20Material/Hybrid%20Fault%20Tree%20Ed00.01.00.docx

Guidance L On gaining safety insights in real-time simulations

L.1 Introduction

SESAR affects all areas of Operational service provision impacting the tasks, procedures, tools, environment and the roles of operational personnel. It will impact all areas of the service, from strategic planning to tactical operations and embraces a lot of new technology in the provision of the service. The existing ATM provision is provided as a set of loosely linked processes involving a high level of reactivity in tactical ATC due to limited predictability in demand and capacity mainly caused by inaccurate trajectory planning. SESAR is based around a gate to gate accurate trajectory planning process which starts in long term strategic planning and becomes more and more accurate as the day of operations approaches.

During the SESAR Development Phase, real-time human-in-the-loop (HITL) simulations have been intensively used to support the validation of the changes brought to the ATM/ANS concept of operations. They will be equally used in SESAR 2020. Consequently, gaining safety insights from simulations is very important to support the collection of safety measures showing that the significant increase of safety (3-10 fold) could be achieved with SESAR 2020. Setting measurable safety objectives for the safety impact of the different operational changes brought by SESAR 2020 is therefore critical to assuring that in principle we can meet this target, to demonstrate that this is achievable during validation and to prove it is met during operations (although the latter is not within the scope of the SESAR and SESAR 2020 work programmes).

This Guidance should be used to determine specific safety validation objectives for a validation exercise based on a real-time human-in-the-loop (HITL) simulation. It also provides the description of two safety assurance tools – namely the Flight plan Hotspots Visualizer (FHV) and enhanced Separation Performance Visualizer (eSPV) that can be used on a voluntary basis within validation exercises to generate evidence of safety performance. Tools other than those defined herein can be used to deliver similar outcomes.

In using this Guidance, the objective is to derive the requirements for safety insights with the expectations that those requirements will be appropriately captured by Validation Plans and measured against during validation exercises. This in particular addresses the expectations as per safety assurance activities:

P3P4	AO2	a4; and
P5P6	AO5	a5

as per Guidance **A.2** and **A.3**.

L.2 About the usage of real-time simulations in validation

Real-time simulations occur mid-way until late in the concept development life cycle (*i.e.* a detailed stage of design at which at least provisional controller procedures and working methods have been developed, and at least a preliminary working HMI exists). Real time human-in-the-loop (HITL) simulations are a flexible approach, able to address airspace design, new automation tools and concepts, controller working methods and Human-Machine Interface (HMI) design for example. Real time simulations are also particularly useful in examining impacts on controller performance. Real time simulations are less used for software and hardware evaluation, because firstly other methods are available and more efficient, and also simulation 'platforms' are themselves usually a simplified abstraction of the real system, so can only test hardware and software aspects in principle or functionally. Nevertheless, they are good overall tests of an ATM/ANS system, able to confirm benefits and/or find problems in the intended system architecture and implementation. For this reason often large-scale tests may be carried out on site, in a simulation facility at or adjacent to an air traffic control centre. If a system is tested in the centre itself, this constitutes either a 'shadow-mode trial' (controllers using the system are not in control but are 'following' live traffic), or else it can be an actual 'live trial' in which the new system is actively used to control/monitor traffic. In both of these cases, there must be an assessment of the safety of the trial itself, so that the trial cannot induce actual incidents or reduce the real system's ability to respond to actual incidents during or after the trial. However the safety of the live trials is out of scope for this Guidance.

L.3 Purpose of this Guidance

This Guidance describes a process as well as a proposed toolbox to take measures during SESAR real-time human-in-the-loop (HITL) simulations to derive safety insights. It is important to note that tools other than those defined herein can be brought into play in order to collect relevant evidence about safety achievements (performance, requirements, etc.). The process involves both:

- The measurement of the safety of controller performance when faced with specific safety safety-related events (e.g. hazards) in a simulation,
- General safety monitoring using less intrusive procedures to see if any safety-relevant information arises during a real time simulation, and
- The generation of evidence of safety performance arising from post-processing trajectory data (flight plans, plot data) from simulations and which relate to:
    - Potential network operations' impacts on safety – with a focus on SESAR 2020 exercises related to optimising the ATM Network Services (Collaboration, Balancing Demand & Capacity, Environment, Efficiency)
    - Analysis of the air traffic controllers' interventions and the impacts of supporting automations on separation management performance – with a focus on SESAR 2020 exercises related to Advanced Air Traffic Services in En-route and TMA.
- Section **L.4** of this Guidance provides an overview of the process to gain safety insights from simulations.
- Section **L.5** presents typical Measures/techniques/tools for gaining insights from Real Time Simulations
- Chapter L.6 focuses on the measure of the number of potential losses of separation at two key time periods before operations with the potential usage of the Flight plan Hotspot Visualizer (FHV) tool developed by EUROCONTROL
- Chapter L.7**6** focuses on the assessment and visualisation of separation performance between flights within a particular piece of En-route and/or TMA airspace, with, in particular, the potential usage of the enhanced Separation Performance Visualization (eSPV) tool developed by EUROCONTROL.

L.4 Process Steps

The process steps are as follows:

Step 1: Determine whether there are specific safety objectives for a simulation – these may arise from:

- A hazard analysis (e.g. particular hazards that are of concern and may be seen during a simulation);
- other sources (e.g. review of operational incident data or controllers' opinion about pertinent safety issues); and
- Safety proxies, *i.e.* relevant safety performance indicators that can be used to demonstrate the achievement / achievability of the SAfety Criteria (SAC); Safety Objectives (SO) and/or Safety Requirements (SR), which must be measurable and can be demonstrated in validation exercises

Step 2: If there are specific safety-related events of interest for the simulation these must be related to the simulation environment and objectives, to see how they can be integrated into the overall simulation plan (VAL Plan for the relevant Solution) and its execution. This will lead to the definition of specific safety events or scenarios that must occur during the simulation in a planned and measurable fashion, less intrusive observations and/or post-processing of simulation data. Examples of safety events could be failure or ‘bad data’ resulting from a proposed controller tool, or adverse weather events, or pilot error. If there are no specific safety events of interest, then a standard set of general measures can be applied to the simulation (see *Step 3* below).

Step 3: Measures must be chosen for the simulation that will allow safety conclusions or at least insights to be drawn. General measures include automatic monitoring of reductions in standard ATM-relevant safety criteria (e.g. losses of separation; runway incursions; ACAS/TCAS activation, etc.) via automatic event logging systems or more specialized safety performance assurance tools as described in sections**L.6** and **L.7** below. Such approaches may also be facilitated by controller self-report and simulation observer report. Standard debriefs and questionnaires after each exercise and at the end of the simulation should also include general safety questions. For more safety-related-event oriented simulations, e.g. considering the potential impacts of a hazard on situation awareness, workload or teamwork, tools to support improvement of controller productivity, change of paradigm of ATC in E-R and TMA, more specific measurements will be used (see Table in section **L.5** below). For all measures, it must be decided in the VAL Plan how the measure will be administered, the expected direction of the effect, and how to analyse the measure, and the safety criterion (qualitative or quantitative) from which to judge the extent of the impact. In a number of cases this may include the need for a classification of the severity (e.g. for losses of separation), controllers’ interventions, but in other cases may be more subjective or interpretative by the simulation ‘experimenters’ e.g. interpretations of workload or situation awareness impacts.

Step 4: The simulation is then run. For general safety measurement, there may be a need for debrief and clarification sessions with the controller subjects. For more focused measures these debrief sessions (with single controllers or multiple controllers) may be expected to be more intensive. In other cases, post-processing of data from simulations will generate evidence of safety performance / validation objectives. Some measures (e.g. situation awareness or physiological measures) may also be more ‘intrusive’ in that they may actually require a short temporary interruption of the simulation itself whilst key questions or measurements are taken, or in the case of psycho-physiological measurements (e.g. heart rate, eye movement tracking, electro-dermal activity, etc.) the measures may not actually interrupt the simulation but the controller will be required to wear monitoring equipment. In all such cases the impacts of the measurements and measurement methods themselves on behaviour must be assessed to determine how they affect the validity of results on safety and other simulation objectives.

Step 5: Analysis and determination of safety insights then occurs. This should usually lead to a conclusion that safety as evidenced in the simulation and/or from pots-processing of simulation data, was either enhanced, degraded, no change occurred, or the measure/simulation/scenario was insufficiently sensitive to the intended safety aspect being investigated, or finally that the observed change was an artefact from the measure itself (and therefore may not appear in a real situation). Interpreting such safety insights or evidence requires careful interpretation however as well as operational support in analysing the outcomes from data processing. In particular, for hazards that are ‘fed into’ the simulation, these will often have a far higher occurrence rate in the simulation than in reality – therefore the controller reactions may differ from reality, particularly when considering rare hazards or events. Secondly, in terms of errors or events that ‘arise’ during a simulation (i.e. they were not pre-planned into the simulation), it must be remembered that these safety-related events may sometimes occur more easily in simulations than in reality, due to lack of familiarity of controllers with the simulation and scenarios (e.g. HMI, new concept and airspace unfamiliarity), and also simply because it is ‘just a simulation’ and so controllers may act less safely than when handling real traffic in the controllers’ normal working environment. This does not mean that observed events (e.g. controller errors) are artificial, but rather the ‘rate’ may be significantly higher than in normal activities. As an important counterpoint to this potential ‘bias’ however, if an event predicted as possible (e.g. a human error) does not appear during a simulation, it does not mean it will never appear in reality. Whilst a typical simulation is always a substantial test of a system, in safety and risk terms it will not be a reliable measure of rare events (e.g. less than one in a thousand in terms of anticipated likelihood). Care is therefore needed in drawing conclusions from simulations to inform the Solution safety assessments and eventually the safety case conclusions. Real time simulations can provide important insights for safety cases, but will not always be definitive. This is why this Guidance deals only with 'Safety insights in simulations' – because a simulation can rarely be exhaustive due to practical limitations (simulation costs and availability of controllers), and so it is insufficient as a means to judge safety conclusively when considering rare events. Nevertheless, the controller reactions and experiences associated with such simulations and/or post-processing of simulation data can lead to important insights about safety of the concept being simulated, the achieved safety performance and associated errors and failure-recovery paths. These experiences can still inform the safety of the Solution, and can lead to the derivation of additional safety requirements (e.g. training and procedural improvements).

Step 6: Safety insights are fed into the safety documentation for the involved Solution. This covers VAL Report, Safety Assessment Report and OSED/SPR/TS.

L.5 Typical Measures/techniques/tools

Table 16 below depicts typical measures for gaining insights from RTS on controllers' performance. The psycho-physiological measures mentioned in the table below require the involvement of experienced specialists for appropriate interpretations.

Event Logging (automatic recording)	Safety-related measures & techniques	HP- related measures[11]	Psycho-physiological measures[12]
Impact on separation provision of Optimised ATM Network Services	- predicted separation losses or conflicting trajectories - numbers of flight hours or occupancy FHV (see section **L.6**) or similar tools		
Impact on separation performance of: - Improvement of controller productivity Change of paradigm of ATC (Sector-less control) - TMA optimisation: - ACAS X in European context - etc.	- 'Seeding' hazards and safety-related scenarios into simulations - tactical interventions from the plot data - potential losses of separation along the "intent" trajectory - actual LoS by time, types, severity eSPV (see section **L.7** below) or similar tools	- Workload (various measures such as NASA-TLX; ISA; SWAT; etc.) - changes in ATCO's behaviours in separation management (eSPV (see **L.7** below) or similar tools)	Heart Rate Variability (note that HRV should not be used while speaking since it strongly influences the HRV. As a result those 'speaking times' should be excluded / or only the Heart Rate should be used.
More generally measures of precursors for the AIM Mid-Air Collisions Models (E-R and TMA)	Separation Performance Visualisation Tool + Automatic Safety Monitoring Tool (ASMT), or other similar tools (see Sections **L.6** and **L.7** below for more details)	Situation Awareness (e.g. SASHA; SAGAT)	Eye movement tracking and pupil diameter measurement
Safety net activations (e.g. ACAS/TCAS; short-term conflict alert occurrence;	Time to recover from hazards	Teamwork impacts	Electro-dermal activity (note that this is only a measure for the emotional but not for the

[11] Could be refined based on further inputs from P16.06.05
[12] Could be refined based on further inputs from P16.06.05

other)			mental workload)
Video recording; radar screen and strips recording; voice recording; other event logging	Subjective questions and debriefs on perceived safety impacts	Skill degradation (SHAPE toolkit)	Brainwave measures (e.g. P300)
Time (for various measures – e.g. time to detect or respond to events)	HERA – Human Error in ATM – used to classify and understand human error events (see HP Reference Material)	Trust (e.g. in automation or fellow controllers – SHAPE toolkit)	

Table 16: Typical Measures for Gaining insights from Real Time Simulations on Controllers' performance

L.6 FHV

L.6.1 Purpose

Within the context of SESAR the FHV is intended to be used to generate evidence of safety performance arising from projects related to NETWORK. The FHV works on analysing the safety performance aspects of the flight planning process.

FHV is one way of generating evidence of the impact on separation provision within flight planning of, for example:

- Re-sectorisation;
- Free-routing;
- Concepts to be implemented to aid flight planning and demand capacity balancing; and
- The impact of safety nets on separation provision.

Within the context of examining operationally recorded Flight planning data and data recorded from simulators and validation exercises relating to flight plans; this annexe describes the functions and output from the FHV. It can be used to generate:

- Geographical views of separation performance;
- Charted views showing histograms of separation performance; and
- Quantitative values for separation performance that can be used to feed AIM precursors.

L.6.2 Use

The FHV has been developed by EUROCONTROL to allow the analysis of flight planning updates during the day of operations using Network Operations log files (ETFMS Flight Data (EFD) files) from the Network Manager. This tool provides an analysis of the potential losses of separation if aircraft follow their flight plans. This provides a quantitative measure of the number of potential losses of separation at two key time periods before operations.

More precisely, the Flight plan Hotspot Visualizer (FHV) is used to both:

- Generate real safety measures (related to conflicting situations, density, complexity, etc.) of the performance of the Network Collaborative Management functionality that includes all

'Network Collaborative Management & Dynamic Capacity Balancing' –related SESAR changes

- Quantify the strategic and pre-tactical related precursors in the AIM MAC models (E-R and TMA). Those are:
  - The number of strategic conflicts *i.e.* the number of potential conflicts that exist before regulation and dynamic flow management measures have been carried out.
  - The number of pre-tactical conflicts *i.e.* the number of potential conflicts that remain and there nature (geometry / severity) after all regulations and dynamic flow management measures have been carried out.

L.6.3 General Description of FHV

FHV is designed to provide a time based view of all performance aspects of the flight planning process. Specifically its use in SESAR permits investigation of the impacts of strategic and pre-tactical dynamic capacity balancing (dDCB) on the different performance measures. FHV has been developed first starting with safety but is able to be employed for a global set of measures (capacity, efficiency, delay and potentially environmental; the latter in a foreseeable future).

The tool generates trajectories in a projected time window in advance of real time using all the flight plan data that was available at that instant. This provides a "snapshot" of the situation that would occur if the flight planning process was stopped at a particular time before operations. This provides a practical method of observing the progress of the regulation, DCB and dDCB process and its impacts on flights.

L.6.4 Main modules

The FHV consists of 3 main elements:

- EFD Processor
- GASEL Manager
- FHV Display

Each of the elements is further described in sections below.

L.6.5 Data preparation

The tool uses the following files:

- EFD file - XML based file containing an entire day of flight processing.
- Navigation file – All navigational points used in flight planning (for the relevant ARINC cycle (every 28 days)).
- Airports file – All airport data used in flight planning (for the relevant ARINC cycle),

The data preparation has two distinct steps:

- Flight Plan database generation
- Conflict and Trajectory generation

The EFD processor

The EFD files have all the flight plan update messages from the operational systems from all components of the flight planning process from manual input to automated flight planning tools used in airport and airspace performance optimization. They permit a complete analysis of the evolution of each flight plan from the original filing, through pre-flight planning, tactical updates and flight plan termination.

The EFD Processor allows the extraction of data from the original EFD files in an Extensible Mark-up Language (xml) format into a database of flight data. The Processor permits the selection of a particular time period and a time ahead to generate results. It is the pre-processor that (1) makes all the performance calculations, (2) reconstructs trajectories based on the plans, and (3) generates events on the basis of potential proximities between flights. The Processor has to filter out numerous duplicate and sometimes contradictory flight messages and generates a report on its processing.

The EFD Processor works in two phases. It first generates a set of flight plan records and secondly it permits the use of this data to generate trajectories and events for the performance analysis. The generation of the flight plan data has to be done once for each targeted day of data.

Operational volume

The FHV is able to work with all operational volumes that are used by network operations (GASEL airspace files). These consist of volumes that describe regions, areas of responsibility, sectors, airspace blocks and temporary airspace elements. These volumes are regularly updated and so have to be regenerated for the analysis based on that airspace.

Airspace volumes are a very complex nested set of volume definitions which cannot be manually input into a tool like the FHV. Consequently it has been decided to produce an airspace volume manager: it is referred to as the GASEL Manager. The GASEL Manager allows the selection of a set of 3D volumes from the GASEL data for import into the FHV. It allows the visualization of the areas and also the setting of time periods of use during a day of operations for each area. As a result, very complex volumes from the latest airspace definitions can be easily used in FHV.

Conflicts and Trajectory generation

This takes the flight plan database created as per the description in section 3.1 above, and uses user parameters (e.g. 5NM, 1,000ft) to generate conflicts and trajectories based on a sliding window of time ahead of operations.

A trajectory file is created representing the observed flights if they are used in the flight plan data at the selected time ahead or beforehand, each time using the latest plan available. This is described in **Figure 18** below:

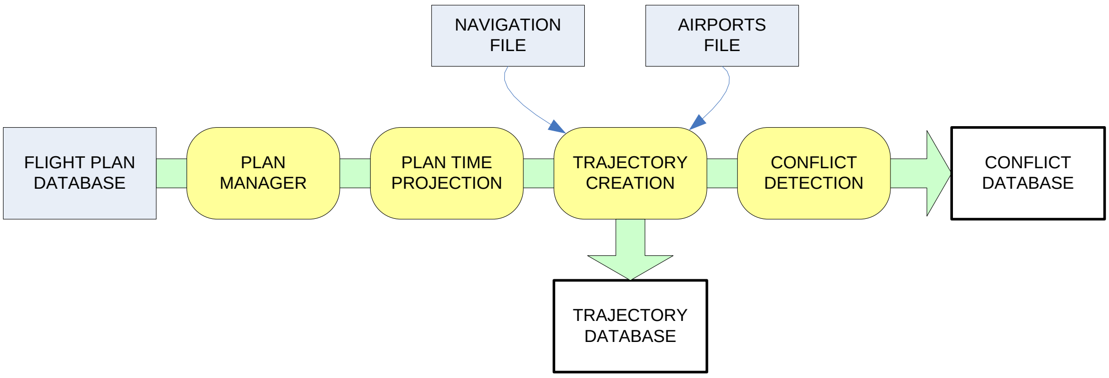


Figure 18: Overall process with the FHV tool

1. The flight plan database contains all valid flight plan data in time order for all traffic on the day of operations. The plan manager maintains a current situation based upon the processed plan data for each flight. It has the latest plan and all historical ones for the flights in a linked list.

2. The plan time projection provides a view of each flight plan with the selected time ahead. This is updated minute by minute from the plan manager.
3. The trajectory creation has to take the plans which have named navigation and airport points, geographical points with positions, and relative altitude updates between points. Many named points have several possible matches to the navigational file and the best one (based upon previous and next points is selected).
4. Based upon the criteria given by the user for each set of flights minute by minute the projected trajectories are compared in 5 second increments to detect potential conflicts. For each conflict a record is generated giving details of the conflict and aircraft involved.

This process has to be repeated for each time ahead and for each different separation criteria used. All data for the same EFD file use the same flight plan database generating different trajectory databases and conflict databases.

Figure 19 below describes the trajectory and conflict generation process in more detail:

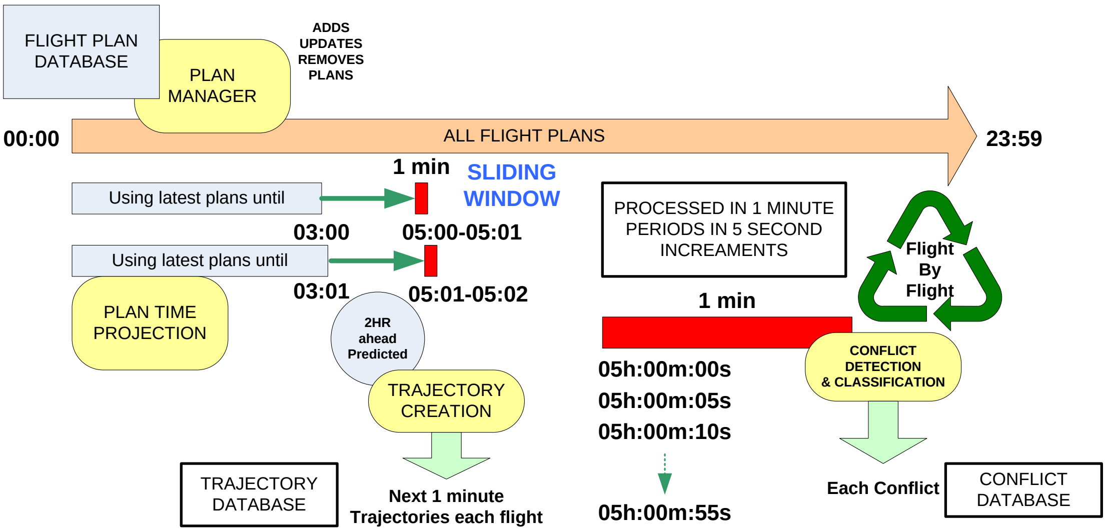


Figure 19: Trajectory and conflict generation process

The key points are:

- Flight plan data is processed minute by minute.
- A sliding window in front the “Time Ahead” is used to determine the projected minute for a 4D trajectory generation and for conflict detection. All active flights are used to generate a one minute set of 5 second data points based upon the flight plan data. Points between any two references in the flight plan are interpolated. A basic mode of flight is developed that categorizes each flight into maneuvering or not in vertical and horizontal senses. This is used to restrict or relax the conflict detection to take into account turns and vertical changes (avoiding treating a turn as instantaneous).
- In the example a time ahead of 2hrs is being used so that when flight plans up to 03:00 have been processed the projection of 05:00 to 05:01 based on these plans will be made. The next cycle will be at 03:01 for the period 05:01-05:02. This way, a single predicted position based upon the latest flight plan available for each aircraft at the time ahead is used.
- Conflict detection is aircraft by aircraft using a one minute flight reconstruction window from all active flights. This is sampled in twelve 5 second intervals. Each aircraft is compared with all other candidate aircraft in the locality (within 10NM and 2000ft). The separation criteria are used to generate a conflict database that is updated as a conflict continues. At the end of a

conflict, the conflict is classified according to the geometry, separations, flight levels involved and aircraft types.

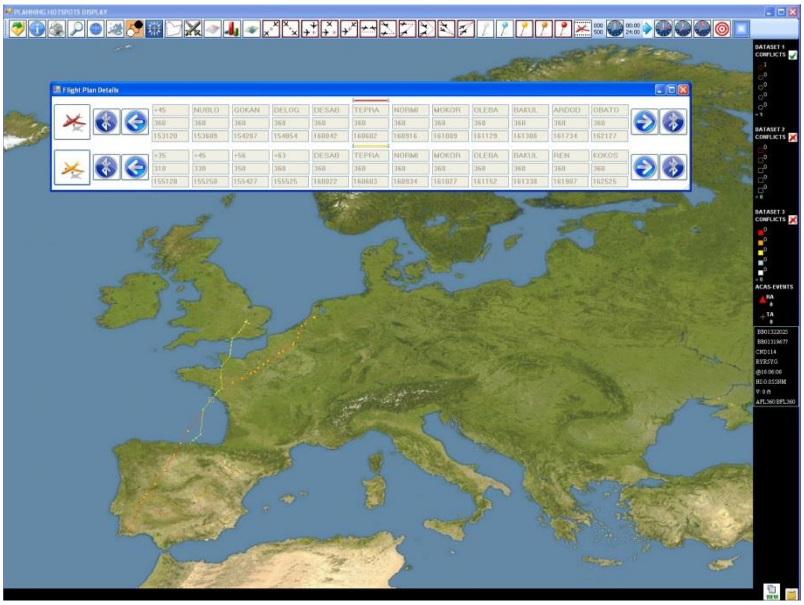
L.6.6 Display programme and analysis

The final element of the FHV is the display program that permits the viewing and display of selected results from the EFD Processor and can use volumes from the GASEL Manager to filter results.

The display program can load several sets of results from different EFD Processor runs (different time windows or separation criteria) and provides many filters to permit analysis of flight plan performances. These include time, geometry, severity, user defined volumes and altitude bands.

The display provides three different types of visualization:

- One which is geographical showing events such as predicted separation losses or conflicting trajectories,
- one which is grid based that show numbers of events or flight hours or occupancy of each grid element
- Finally a histogram display of results is provided to give a statistical view of distributions of separations or occupancy of selected volumes.

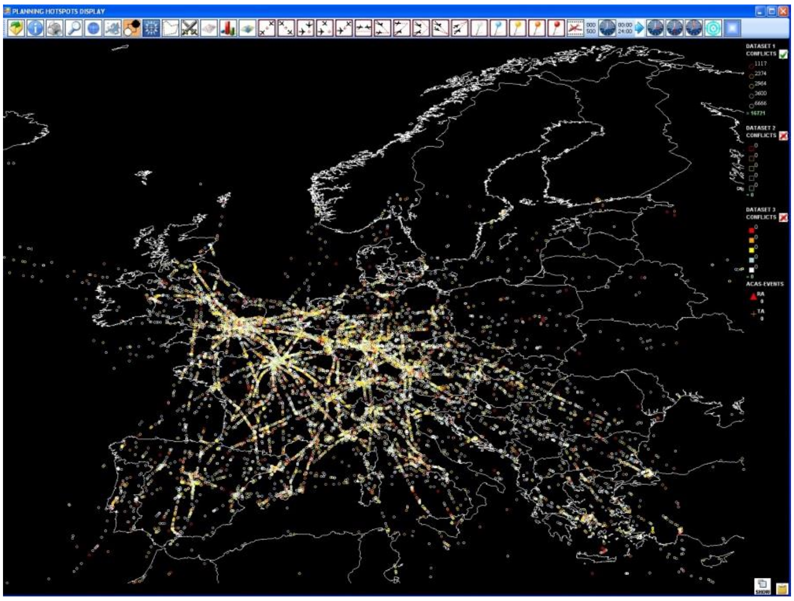


Flight Plan Details

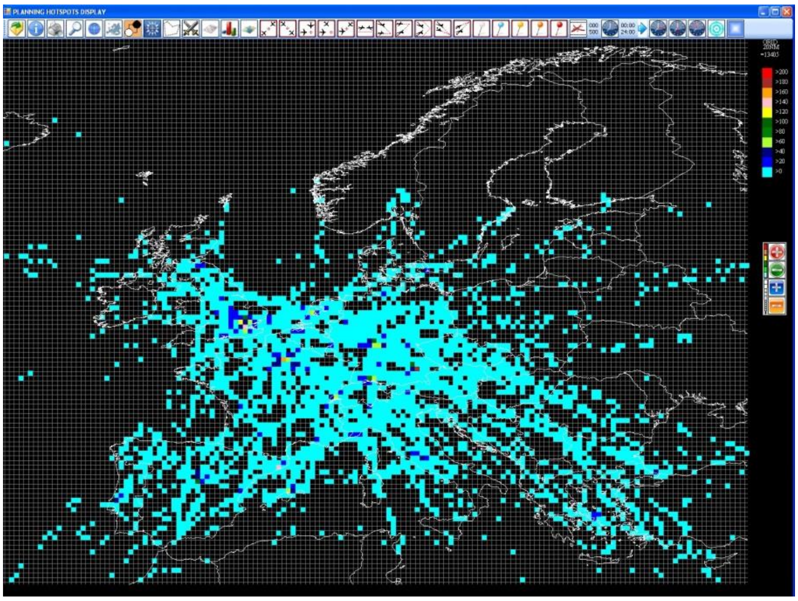
+45	NUBLO	GOKAN	DELOG	DESAB	TEPRA	NORMI	MOKOR	OLEBA	BAKUL	ARDOD	OBATO
360	360	360	360	360	360	360	360	360	360	360	360
153128	153609	154207	154854	160042	160602	160916	161009	161129	161308	161734	162127
+35	+45	+56	+63	DESAB	TEPRA	NORMI	MOKOR	OLEBA	BAKUL	REN	KOKOS
310	330	350	360	360	360	360	360	360	360	360	360
155128	155250	155427	155525	160022	160603	160934	161027	161152	161338	161907	162525

The tool can show hotspots via a stepped view in time through the data. It can show individual events by user selection and show the flight plans involved highlighting the critical element in the plans. The tool can also create reports concerning the events for use in validation reports.

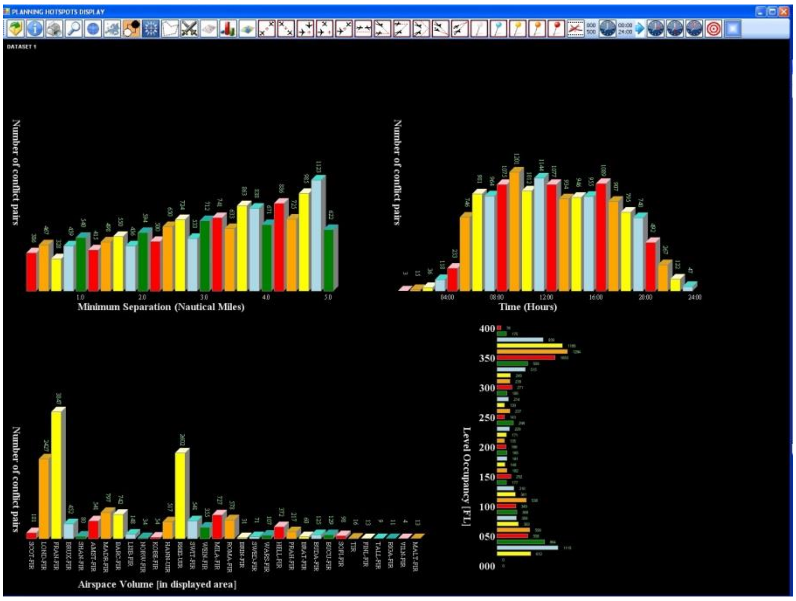
In summary, the geographical display:



In summary, the data grid display:



In summary, the histograms display:



L.6.7 Technical environment requirements

The Flight-plan Hotspots Visualizer (FHV) has been developed using the Visual Studio development environment (Microsoft). It has been developed in Visual C# using application frameworks libraries (standard Microsoft libraries).

It uses no external libraries and is completely standalone.

L.6.8 Software configuration and version

a) Maintenance & development

- 3.5GHz CPU. 8GB RAM. 10GB HD for dev
- Windows 7
- Visual Studio 2008 or better
- Application Frameworks (Free)

b) Use and application

- 3GHz CPU. 4GB RAM. 10MB HD space (soft)
- + 10GB HD per EFD file kept or 1GB results
- Windows XP, Vista, & or 8

L.7 The enhanced Separation Performance Visualizer (eSPV tool)

L.7.1 Scope

The eSPV is a tool for assessing and visualising separation performance between flights within a particular piece of airspace. The e-SPV has been enhanced to deal with TMA and Approach type airspace where there is considerable manoeuvring of flights, and the nature of the airspace means that flights will inevitably be closer together during arrival and departure phases.

Within the context of SESAR 2020 the eSPV can be used within validation exercises to generate evidence of safety performance. This infers that a well-designed and balanced experimental design is implemented for the validation exercise that allow for a suitable comparison of baselines with experimental conditions.

eSPV is one way of generating evidence of the impact on separation provision of, for example:

- Re-sectorisation;
- Free-routing;
- Tactical controller tool development and deployments; and
- The impact of safety nets on separation provision.

eSPV may also be used to investigate a number of safety impacts arising from operational environment conditions arising from a post hoc analysis of:

- CB activity;
- Cross winds; and
- Changes in operations – such as runway changes.

Within the context of examining operationally recorded radar data and data recorded from simulators and validation exercises; this guidance describes the functions and outputs from the eSPV that include:

- Geographical views of separation performance;
- Charted views showing histograms of separation performance; and
- Quantitative values for separation performance that can be used to feed AIM precursors (see **E.3** and **E.4**).

L.7.2 Overview

The eSPV processes plot data from simulations or live systems. It uses the plot data to identify aircraft manoeuvres in the data. It is assumed that each manoeuvre corresponds to three different sources:

- Controller instructions provided for
  - Separation provision
  - Facilitating the flow of aircraft
- Procedures - such as entering a stack
- Pilot interventions

eSPV attempts to determine whether identified manoeuvres/instructions were made in order to avoid conflict with other aircraft. It does this by predicting the trajectory of a flight based upon its velocity prior to the manoeuvre. Using the predicted trajectory, an assessment of potential conflicts with all active aircraft is made. The results of this analysis are then presented on a series of histograms and geographic map charts.

Because TMA and Approach airspace is characterised by high density, high manoeuvre aircraft behaviour, it is necessary to remove potential conflicts that are caused by “normal” operating behaviour. This is achieved by the provision of a set of filters that can exclude selected manoeuvres from the results.

In addition to the standard filters, such as horizontal and vertical separation, time to loss of separation, eSPV also provides a sophisticated geographic filter mechanism that enables users to defined ‘Areas of Interest’ (AOIs) and then apply different filter parameters depending on where the subject and threat aircraft are within these AOIs.

L.7.3 eSPV metrics

eSPV provides a series of capacity and safety metrics. At the time of writing these are being finalised and this section is subject to minor modification. The Capacity & Safety Metrics executable generates the data used in the Separation Charts.

1) Determine tactical interventions from the plot data, tactical interventions are:

   - Turns;
   - Speed changes; and
   - Climbs and descents.

2) For each intervention, generate an “intent” trajectory.

   - This trajectory is calculated assuming that the tactical intervention has not happened, although it does include any previous interventions that are still active

3) For each intervention, probe for potential losses of separation along the “intent” trajectory;

   For each time step, an “intent” trajectory is generated for each active aircraft, which is stored for that time step and can be probed to determine potential losses of separation. There are two triggers to probe for potential losses of separation, as follows:

   - When a tactical intervention is about to take place (i.e. in the next time step), the subject aircraft’s “intent” trajectory is probed to determine any potential loss of separation before applying the intervention. The probe is performed in the time step before the intervention to ensure any potential loss of separation would be based on the predicted “intent”.
   - During each time step using the actual position data, each active aircraft is probed to measure the predicted separation for that aircraft. This allows the comparison of the actual separation to be compared to the predicted “intent” of the aircraft.

4) Record & present the result for each intervention

L.7.4 Creating Charts

A series of configurable charts are available in eSPV. To create a new chart, in the main menu bar, select:

- Chart → New Chart

This displays the Chart Configuration Wizard. The first page determines the type of chart to create and is displayed in **Figure 20** below:

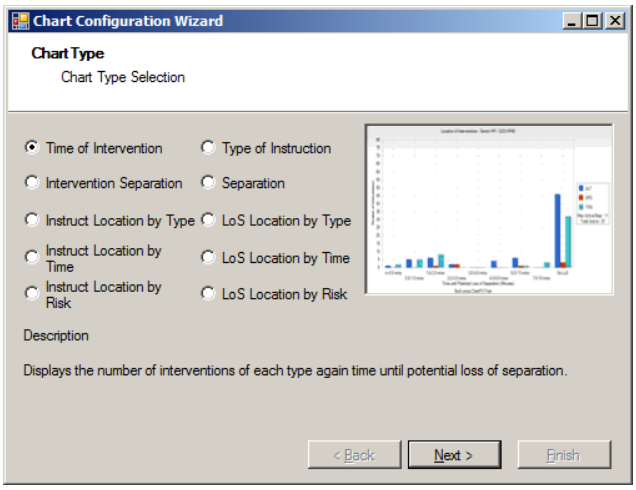


Chart Configuration Wizard

Chart Type

Chart Type Selection

● Time of Intervention ○ Type of Instruction
○ Intervention Separation ○ Separation
○ Instruct Location by Type ○ LoS Location by Type
○ Instruct Location by Time ○ LoS Location by Time
○ Instruct Location by Risk ○ LoS Location by Risk

Description

Displays the number of interventions of each type again time until potential loss of separation.

Figure 20: Chart Type Selection Page

There are ten charts currently available, these are listed below:

Chart	Description
• Time of Intervention	• This chart shows the number of interventions as a histogram for each type of Intervention. Only the y-axis range can be manually configured. The bars are colour coded according to the style configured for each Intervention type.
• Intervention Separation	• The intervention Separation chart displays the severity of predicted loss of separation for each tactical intervention in terms of time to loss of separation and closest approach distance. • The bars are colour coded according to the severity of the predicted loss of separation. Only the y-axis range can be manually configured
• Type of Instruction	• This chart displays the relative percentages of the different types of intervention (Altitude, Turn and Speed) in terms of time to loss of separation against the configured separation categories. Neither the X nor Y axis range scale can be manually configured.
• Separation	• This chart compares separation performance measured before and after tactical interventions. The chart shows the total flight time (in minutes) for each loss of separation category. Only the y-axis range can be manually configured.
• Instruction Locations by Type	• This chart displays the geographical distribution of interventions grouped by each instruction type as a map chart.
• Instruction Locations by Time	• This chart displays the geographical distribution of interventions grouped by time to loss of separation categories and instruction types as a map chart.
• Instruction Location by Risk	• This chart displays the geographical distribution of interventions grouped by separation risk categories and instruction types as a map chart.
• LoS Location by Type	• This chart displays the geographical distribution of the predicted location for the loss of separation event grouped by each instruction type as a map chart.
• LoS Location by Time	• This chart displays the geographical distribution of the predicted location for the loss of separation event grouped by Time until the LoS as a map chart..

• LoS Location by Risk	• This chart displays the geographical distribution of the predicted location for the loss of separation event grouped by associated Risk of the LoS as a map chart.

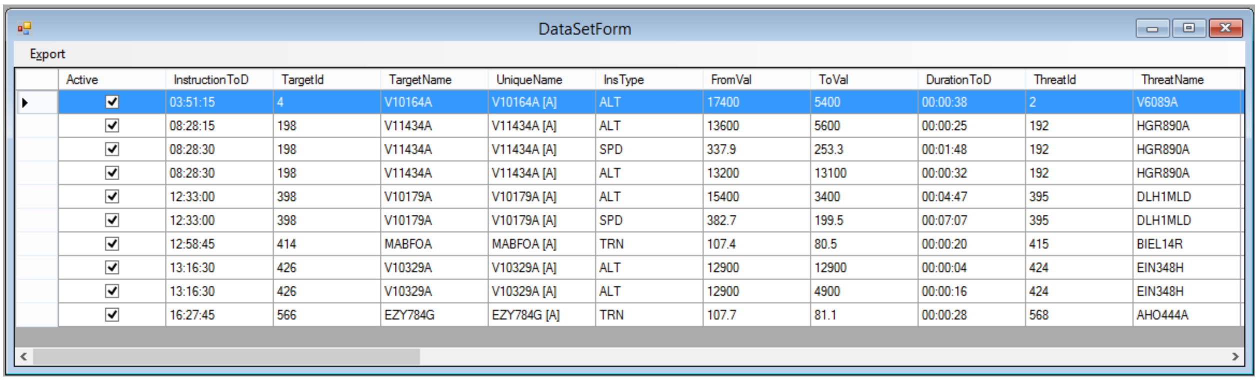
Charting features

Figure 26 below shows an example of a geographic map chart. On this chart an event symbol has been selected. This causes the potential conflict to be displayed. This is represented as two red lines. At the start of the line is a ▶ symbol, and at the end of the line is the ▶I symbol**.** Start and stop points are joined by thinner red lines.

The chart also illustrates legend and labels. Top tip labels are also displayed when the cursor is placed other an event symbol. The comments on each chart 'Max Step' and 'Active Step'. Max step refer to the maximum number of aircraft being processed in each processing step of 2 minutes. Active step refers to the number of aircraft manoeuvres that are recorded in in the processing pass

Four types of events are shown on the charts. These are turns, altitude changes, speed changes, and also actual conflicts where no instruction was issued. The symbol used for each of these events is configurable.

In addition to the charts listed above, the Charter also provides a list of events that are on display. This is access from the **View Dataset** menu item on the **Charts** menu. **Figure 21** shows a sample of events. The data can be exported to a file using the **Export** feature on the window's menu bar.



	Active	InstructionToD	TargetId	TargetName	UniqueName	InsType	FromVal	ToVal	DurationToD	ThreatId	ThreatName
▶	☑	03:51:15	4	V10164A	V10164A [A]	ALT	17400	5400	00:00:38	2	V6089A
	☑	08:28:15	198	V11434A	V11434A [A]	ALT	13600	5600	00:00:25	192	HGR890A
	☑	08:28:30	198	V11434A	V11434A [A]	SPD	337.9	253.3	00:01:48	192	HGR890A
	☑	08:28:30	198	V11434A	V11434A [A]	ALT	13200	13100	00:00:32	192	HGR890A
	☑	12:33:00	398	V10179A	V10179A [A]	ALT	15400	3400	00:04:47	395	DLH1MLD
	☑	12:33:00	398	V10179A	V10179A [A]	SPD	382.7	199.5	00:07:07	395	DLH1MLD
	☑	12:58:45	414	MABFOA	MABFOA [A]	TRN	107.4	80.5	00:00:20	415	BIEL14R
	☑	13:16:30	426	V10329A	V10329A [A]	ALT	12900	12900	00:00:04	424	EIN348H
	☑	13:16:30	426	V10329A	V10329A [A]	ALT	12900	4900	00:00:16	424	EIN348H
	☑	16:27:45	566	EZY784G	EZY784G [A]	TRN	107.7	81.1	00:00:28	568	AHO444A

Figure 21: Data Set Window

Charting types

A series of screen grabs are shown below for a number of the different charts available in eSPV.

Figure 22 shows an example of the vertical profile view of the two aircraft involved in the selected event, with their vertical profiles. The chart shows the events for the subject aircraft, its trajectory in purple, its CFLs in red and the threat aircraft trajectory in blue.

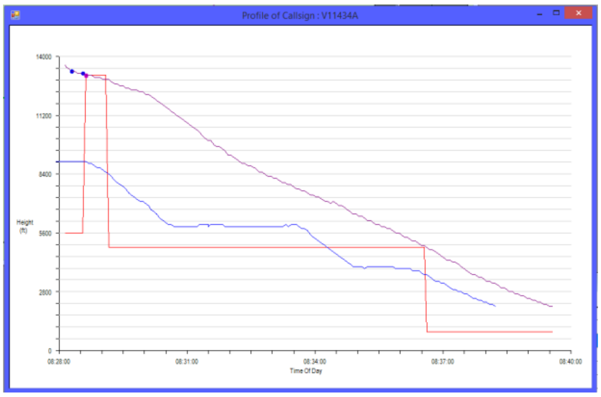


Figure 22: Vertical Profile Window

Figure 23 shows the number of interventions as a histogram for each type of Intervention. Only the y-axis range can be manually configured. The bars are colour coded according to the style configured for each Intervention type.

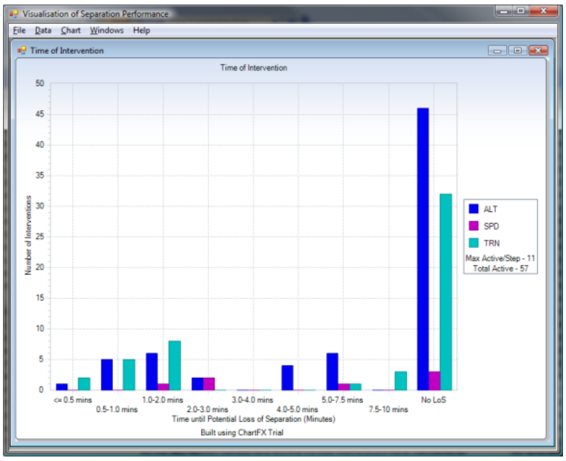


Figure 23: Timing of tactical interventions

Figure 24, the intervention Separation chart, displays the severity of predicted loss of separation for each tactical intervention in terms of time to loss of separation and closest approach distance.

The bars are colour coded according to the severity of the predicted loss of separation. Only the y-axis range can be manually configured.

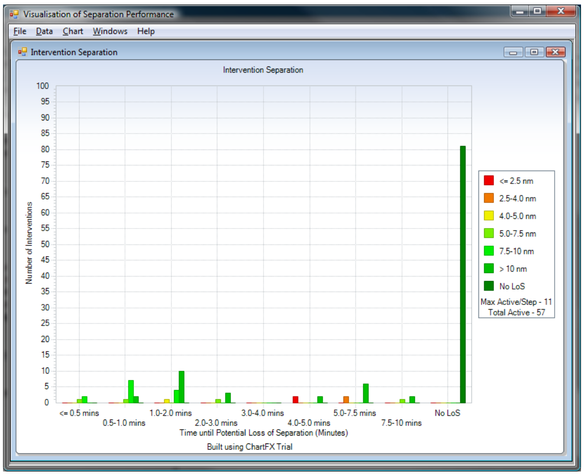


Figure 24: Time to Potential LoS

Figure 25 shows the geographic location of losses of separation.

The map can be zoomed in an out by right-clicking over the map and then selecting the appropriate pop-up menu item – however automatic processing takes place to maintain the default aspect ratio. The pop-up menu also provides features to reset the map, switch on and off labels and legends, and map data. The legend shows counts of the number of events shown on the screen.
Sector data can also be shown.

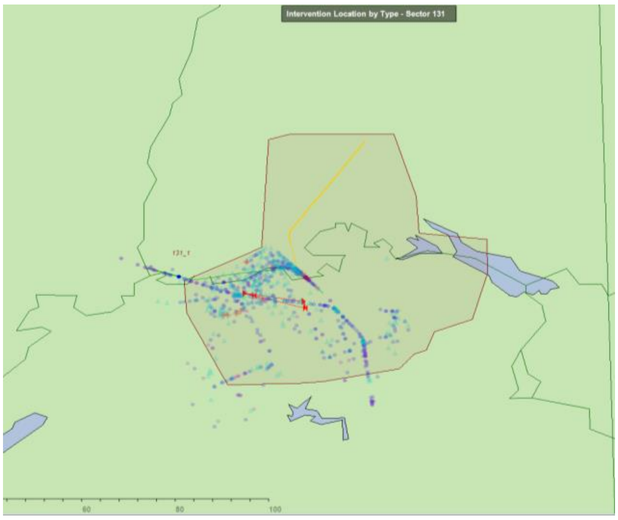


Figure 25: Geographic location of LoS

Figure 26 displays the geographical distribution of the predicted location for the loss of separation event grouped by time until LoS as a geographic map chart.

All windows are synchronised so that the same data shows in all views.

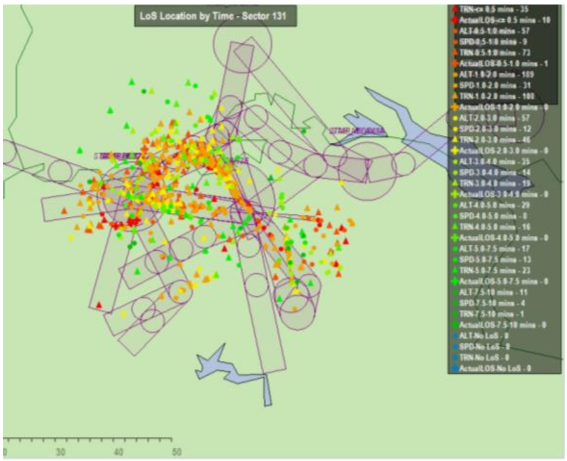


Figure 26: LoS by Time

L.7.5 Filtering data

eSPV contains a series of filters to provide an appropriate display of data for the charting application. Each filter can be turned on or off using the Active Boolean value. This can be set to either TRUE (apply filter) or FALSE (Do not apply filter). Each filter can be configured. As each filter has different characteristics, the sub-sections below describe them.

Aircraft filter

The Aircraft Filter consists of a two elements: the Active Switch and the list of call signs. On clicking the collection button, a pop-up appears containing a tree view listing each aircraft. Each aircraft can be toggled active or inactive individually, or can be set all Active or all Inactive using the buttons to the bottom of the list.

Altitude filter

The Altitude Filter consists of a Boolean switch value displays TRUE for active along with two altitude values which represent the minimum and maximum altitudes for data to be included.

AOI filter

The Area of Interest (AOI) filters are used to exclude events from the charts by applying different separation rules based upon the locations of the aircraft or the loss of separation. A series of filters are defined in a pair of configuration files. The filter definition file creates one or more volume filter volumes. For each filter volume parameters are defined: activation times, minimum and maximum horizontal and vertical separation values, and also deemed separations. A shape file is associated with each filter definition file to describe the geometries of the filters.

Where a subject aircraft is in conflict with a threat aircraft, the charter checks if the aircraft are within any AOI volumes. If they are then the AOI specific separation values are applied, and if the aircraft are outside of the separation values than the event is excluded from display. If the aircraft are in different AOIs and the AOIs have different separation parameters the lowest values are applied. If the AOIs are in different AOIs and these a deemed separated than the events are excluded from display. For example AOIs could be drawn around two runways, when there are aircraft on both runways these would be deemed separated even though the aircraft were within normal separation parameters.

Event filter

Each Instruction may be associated with one or more specific events from the following:

- ACAS
- STCA
- TCT
- MTCD

The Event Filter consists of a tristate check box for each event type. Each Event Filter can be toggled active, inactive or disabled individually.

Horizontal Geometry Filtering

When a LoS is predicted it is assigned a Horizontal geometry classification according to the relative headings of the two aircraft at the point of LoS. These classifications are:

- Overtaking (abs(diff) < 20 degs)
- Acute (20 ≤ abs(diff) < 60 degs)
- Crossing (60 ≤ abs(diff) < 120 degs)
- Obtuse (120 ≤ abs(diff) < 160 degs)
- Head On (abs(diff) ≥ 160 degs)

The Horizontal Geometry Filter consists of a Boolean value represented by a check box control for each classification to determine whether the data should be displayed.

Instruction Type

The Instruction Type Filter consists of a Boolean value represented by a check box control which displays if the filter is active for each of the three types of instruction, Altitude Change, Speed Change or Heading Change.

No LoS Data Filter

The No LoS Data Filter consists of a single value represented by TRUE or FALSE. This determines if data that is not associated with a Loss of Separation (LoS) event is included for display (TRUE to display).

Time Filter

The Time Filter consists of a Boolean value represented by a check box control which displays if the filter is active along with two time controls which represent the start and end times of data to be included.

Vertical Geometry Filtering

When a LoS is predicted it is assigned a Vertical geometry classification according to the relative vertical profiles of the two aircraft at the point of LoS. These classifications are:

- Climbing – Climbing
- Climbing – Descending
- Climbing – Levelled
- Levelled – Descending
- Levelled – Levelled
- Descending – Descending

The Vertical Geometry Filter consists of a Boolean value represented by a check box control for each classification to determine whether the data should be displayed.

L.8 Application environment

The eSPV application suite runs on any modern Personal Computer. The performance of the machine will depend upon the amount of data being processed. However, for a day's worth of data from any normal size airspace it is recommended that the machine has a 3GHz Processor, 8 GBytes of RAM, and a Solid State Hard Drive. The programs all run in single threads so they do not benefit from the use of multi-core processors.

Microsoft Windows 7 or later is needed, with a .NET framework (3.5 or later).

A full version of SoftwareFX ChartFX is used to support the eSPV Charter and is required to be installed on the system.

L.9 eSPV Application Overview

The eSPV is composed of a suite of applications that process raw data from either a simulation or a live system, and then generate charts and statistics to support further analysis. The following executable components comprise e-SPV:

Name	Description
SPV Win	Windows program which provides a user interface for controlling the Pre-processor, capacity metric, and safety metric executables.

SPV Pre-processor	Data pre-processor which can adjust the sector names, and populate Cleared Flight Levels (CFLs) if required. Also can filter out VFR flights and IFR flights in unselected sectors.
Capacity Metric	Carries out processing to calculate capacity metrics.
Safety Metric	Carries out processing for measuring separation performance, and safety metrics.
SPV_Charter	Draws geographic charts and histograms.

Guidance M Safety Management of VLD: an ANSP and Network Manager perspective

M.1 Objectives

When used in conjunction with the existing P16.01.04 Final Guidance Material to Execute Proof of Concept (**Ref. 17**), this guidance provides, as a recommendation, a clear, complete, coherent and integrated 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)). It has been produced in response to:

- Providers of air traffic services' requests for a guidance supporting a formalised, explicit and proactive approach to the systematic safety management of VLD thereby meeting their safety responsibilities within the provision of their services

It seeks neither to replace nor replicate **Ref. 17**, which main focus is 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 provide a theoretical and practical guide to safety assessment and assurance to the participant air traffic service providers who have to discharge their safety responsibilities properly and also provide an adequate level of safety assurance to obtain the necessary regulatory approval for the conduct of a VLD from their NSA and/or EASA.

The material is intended to apply to the full range of VLDs in SESAR 2020. Having said that, it is not intended to be prescriptive – rather it may be adopted and adapted for particular VLD applications as appropriate and necessary; in particular the guidance includes in **M.6** some criteria to assess the significance of the VLD and, as a result, enables a proportionate approach to the safety assurance of the VLD.

M.2 Introduction

A Very Large Demonstration (VLD) aims at assessing the benefits of a SESAR solution, but as the title suggests, on a broad and almost industrialised scale i.e. post V3, V4 and demonstrating that V5 is attainable. It is worth noting that meeting this high level objective implies that the VLD is run in a scientifically controlled way with a true reference for comparison with the 'with-Solution' case.

It aims at serving as a Proof of Concept (PoC) for an existing ATM functionality as per (EU) No 716/2014 of 27 June 2014 (on the establishment of the Pilot Common Project (PCP) supporting the implementation of the European Air Traffic Management Master Plan) or a future ATM functionality within a forthcoming Common Project (CP) Commission Implementing Regulation (IR).

The 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 (e.g. ACAS-X as part of SESAR.IR-VLD.Wave1-15-2015), a VLD aims at providing inputs and influencing the work at global and regional standardisation level, within ICAO, EUROCAE and/or RTCA.

In relation to V-cycles stages and associated Technical Readiness Levels (TRLs), this is demonstrated in **Figure 27** below:

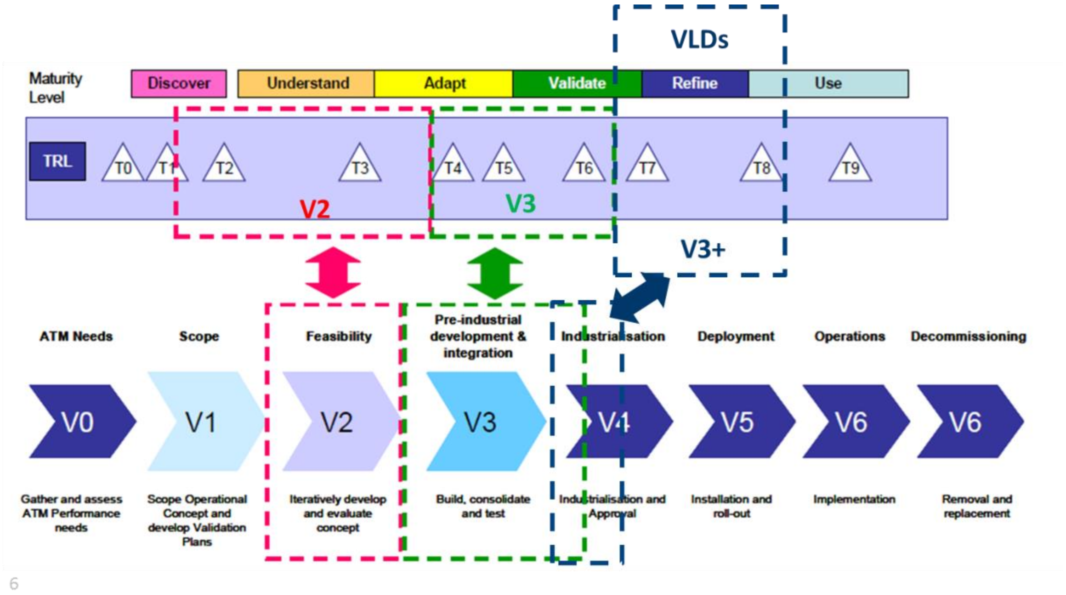

VLDs
Maturity Level
Discover
Understand
Adapt
Validate
Refine
Use
TRL
T0
T1
T2
T3
T4
T5
T6
T7
T8
T9
V2
V3
V3+
ATM Needs
Scope
Feasibility
Pre-industrial development & integration
Industrialisation
Deployment
Operations
Decommissioning
V0
V1
V2
V3
V4
V5
V6
V6
Gather and assess ATM Performance needs
Scope Operational Concept and develop Validation Plans
Iteratively develop and evaluate concept
Build, consolidate and test
Industrialisation and Approval
Installation and roll-out
Implementation
Removal and replacement
6

Figure 27: E-OCVM Vs, TRLs and VLDs (source SJU)

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 onboard) to support the demonstration in the targeted operational environment involving target audience end-users. This also requires proper System Engineering (SE) data management for a solution to ensure that both:

- proper coverage (incl. operational concept, SESAR solution vs. OI steps & Enablers, traffic expectations, equipage level); and
- traceability matrixes between (i) operational & performance requirements vs. technical requirements; and (ii) validation objectives vs. operational & performance requirements; (iii) etc.

are available to support the content integration work. Finally a PoC needs to provide the evidence (SE data and deliverables) with the sufficient quality to guarantee their usability and significance for the SESAR Community, including for eventual deployment.

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, 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 material generated by the SRM process and the SRM per se (see as well sections 9.2 and 9.3 in reference **1**) provide practical guidelines to assist.

M.3 Scope of safety assurance of and wrt a VLD

The activities are twofold and relate to:

i. The non-interference of the VLD with other surrounding operations and components of the ATM/ANS System; and
ii. The suitability of the Solution(s) for the required application/operation.

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 (see figure above). 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 and training before the VLD takes place;
2. Determining and documenting in a VLD safety Plan the safety assurance needs for the VLD per se;
3. Documenting the VLD Safety Case. The VLD Safety Case is here a means of structuring and documenting a summary of the results of a VLD Safety Assessment in a way that a reader can readily follow the logical reasoning as to why the VLD can be considered safe. It follows that the VLD Safety Case will serve both the primary purpose of ensuring that those participant service providers who are accountable for safety discharge their safety responsibilities properly and also provide an adequate level of safety assurance to obtain the necessary regulatory approval;
4. Enabling the use of VLD’s as a new dimension in the validation approach and providing further evidence as a support to standardization. This includes, but is not limited to, (i) building and evaluating the physical Solution System against that detailed 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 onboard) to support the demonstration of the achievement / achievability of the safety validation objectives and higher-level safety requirements; and, finally;
5. Enabling significant levels of engagement and co-ordination of both the end-users (e.g. ANSPs, Network Manager, airports; airspace users, AOC; etc.) and appropriate regulatory authorities (National Authorities (NAAs; NSAs) and/or EASA) as fully detailed in **Ref. 17**.

All of the above is now further detailed in sections **M.4** to **M.8** below.

M.4 Solution Readiness for VLD – an overview

It is essential for the SESAR Solution(s) to be delivered by the VLD to show:

1. That the Safety Assessment Report (SAR) and companion SPR and, if relevant, TS, include all requirements about completeness and correctness of the design as specified in section 8 of **Ref. 1** thereby providing all safety evidence in support of a V3 maturity declaration.
2. That all safety assurance activities as per **M.6** and **M.7** have been conducted; and
3. That a VLD System-configuration evidence has been provided immediately before the Solution(s) System is approved for entry into the VLD service

M.5 About the VLD Safety Plan

The VLD Safety Plan specifies, *inter alia*, the safety assurance activities (using the generic list as provided by **M.7** herein) that are to be carried out in order to create necessary and sufficient Evidence for the production of the VLD Safety Case. The Safety Plan should:

a) Determine the scope and boundaries of the safety assessment / safety case

b) Develop the specific Safety Argument from the generic examples herein (**M.6**)

c) Develop specific Safety Assurance Objectives and activities from the generic set (**M.7**)

d) Assess the resources and skills needed to execute the Safety Plan and identify any dependencies on the non-safety activities / processes on the VLD project and / or other SESAR 2020 projects (e.g. Pj#19 or Pj#22)

e) Determine the safety organisation for the VLD project, and the roles and responsibilities of the personnel, departments and organisations involved in the execution of the Safety Plan

f) Schedule the Safety Assurance Activities in line with the resource requirements / availability and any dependencies

g) Determine the safety-regulatory arrangements for the project on the basis of **Ref. 17**

M.6 Structuring the VLD Safety Case – generic guidance for ANSPs / NM

Obviously:

- Each ANSP may have approved safety assurance processes and procedures for the implementation of changes that are in accordance with the common requirements (1034/2011 and 1035/2011) and may have specific additional criteria contained within them to comply with other national legislation beyond just ensuring direct compliance.
- Each ANSP may also have specific approved processes that are required to be followed when the NSA advises that they wish to review a planned safety related change. And they may need NSA approval for a deviation from those procedures.
- 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, 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, is transition proposed to be implemented as a single one off event; 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.

As a result, this section is intended primarily for the willing developers of Safety Cases for VLD within ANSPs and, as such, it aims at providing guidance on the development of Safety Cases as a means of structuring and documenting the demonstration of the safety of a VLD. It provides a generic example of a structured Safety Arguments for *a* VLD. Variations of that Safety Argument for a specific VLD with a specific scope are also explained. The argument should be structured as follows:

1. It must start with a top-level statement (Claim) about what the VLD Safety Case is trying to demonstrate in relation to the safety of the relevant SESAR Solution(s). The Claim must be supported by:
    a. The safety target, which define 'what is *safe*' in the context of the VLD. This safety target should include the relevant SAfety Criteria (SAC) for the Solution(s)
    b. The Justification for introducing the changes brought by the VLD to the service or system concerned
    c. Operational Context for the Claim
    d. any fundamental Assumptions on which the Claim relies
2. The decomposition of the Claim into the following lower-level:
    a. non-interference of the VLD with other surrounding operations and components of the ATM/ANS System
    b. The suitability of the Solution(s) for the required application/operation. This includes:
        i. Showing that the Solution(s) technical system, procedures (for controllers, pilots, operational engineers and maintenance staff) and training (for the same four groups) satisfy their respective safety requirements (from V3) from the physical design AND that all three components are shown to operate correctly. This includes evidence:
            - That the Detailed Solution(s) design has been completed (as per section 8 of **Ref. 1**
            - Of the tailoring of the V3 Safety Assessment Report (SAR) to the VLD local 'implementation' incl. the Operational Environment (OE) and the completeness of the definition of normal / abnormal conditions
            - That all safety assurance activities as per **M.7** have been conducted addressing both the technical Solution system , the ATC, Aerodrome, NM (FMP) and Flight Crew Procedures Design plus any Contingency procedures (*wrt* covering all abnormal conditions), the engineering procedure and training design
            - That transition procedures have been defined
            - That the installation and commissioning / evaluation of the complete Solution(s) System have been carried out; then it can be argued that the physical design has been implemented completely and correctly
        ii. Defining appropriate safety validation objectives to show that the safety target (incl. SAC and/or proxies) are met; validation objectives have to be commensurate to the time exposure and scale;
        iii. Defining and implementing appropriate means to measure those indicators; this includes the preparation and the VLD platform availability (ground and onboard) to support the demonstration in the targeted operational environment involving target audience end-users measure and analysis. This is addressed in sections 8.2 and 8.3 of **Ref. 17**

iv. The appropriate definition of start / stop criteria/procedures with respect to the VLD incl. requirements (means: equipment, staffing, …) and procedures for reversion. In addition to START/STOP criteria, also need to be defined:

- Temporary AIP and NOTAM
- Special approvals that are required (wrt targeted airspace users)
- LoA between involved ANSPs including but not limited to any airspace or traffic limitations that may need to be implemented while running a VLD in an operational environment

M.7 VLD as a new dimension of the validation approach

M.7.1 Safety assurance in the industrialization and deployment phases

This stage assumes that the detailed design of the end-to-end Solution System[13] has been achieved by the end of V3. Clearly, it will be necessary to check that this is a valid assumption to make as per section **M.3** above. The assurance activities to ensure that:

- The physical design of the technical system (*i.e.* equipment) satisfies the safety requirements that were derived for the logical model (LM)
- A similar argument is made for the operational procedures except that we must take account of any additional procedures that are specific to the operation of the physical VLD Solution System and would not have been apparent at the LM level
- A similar argument is made for the operational procedures except that we must take account of any additional competence needs arising from the procedure (and, where applicable, the technical system)

(…) are specified in **Guidance A.4**. The possibility of new, unwanted safety properties emerging as a result of the physical design is also addressed in **Guidance A.4**. This includes that the causes or effects of any adverse, emergent safety properties have been mitigated such that they do not jeopardize the satisfaction of the SAfety Criteria (SAC).

As a result, this stage is concerned with showing that the technical system, procedures (for controllers, pilots, operational engineers and maintenance staff) and training (for the same four groups) satisfy their respective safety requirements from the physical design AND that all three components are shown to operate correctly and completely during commissioning / evaluation of the complete Solution System during the VLD. On that basis, it can be then be argued that the physical design from V3 has been implemented completely and correctly.

As a summary this stage relates to:

a) Technical Solution system industrialization:
This stage of the process is about building and testing the Technical Solution system, against the requirements derived by the end of V3 (**Guidance A.4**).

This should be part of the normal systems-engineering process at this stage of the project lifecycle, except that it focuses on the safety perspective.

[13] It is very important to remember that the Solution System is not limited to what is on the ground – i.e. it normally includes airborne (humans, equipment and procedures) elements and sometimes space elements as well.

b) ATC and Flight Crew Procedures Design
This stage is concerned with the development of ATC and Flight Crew Procedures and showing that the design of the Procedures satisfies the safety requirements derived by the end of V3 (**Guidance A.4**).

Where Procedure Assurance Levels (PALs) have been used in the ATC Procedure safety requirements, it is necessary also to show that the processes used in the development of the Procedures comply with those prescribed for the PALs concerned.

c) Engineering Procedure Design
This stage is directly equivalent to the previous stage, for ATC and Flight Crew Procedures.

d) ATC and Flight Crew Training Design
This stage is concerned with the design of training material and courses for Controllers and Pilots and showing that the design satisfies the safety requirements derived by the end of V3 (**Guidance A.4**).

e) Engineering Training Design
This stage is directly equivalent to the previous stage, for ATC and Flight Crew Training.

f) Installation and Commissioning

- Preparation for is mainly about mitigating the risks that the commissioning process may present to the on-going ATM service through, for example, inadvertent coupling between the SESAR Solution System-under-test and the current operational system.
- Execution of the commissioning process is concerned with validating the complete Solution System (*i.e.* equipment, procedures and a team of trained Controllers / trained Pilots / operational Engineers) against the higher level requirements – from the Safety criteria down to the LM Safety Requirements.
  It can be carried out only after the individual elements of the Solution System have been verified against their respective safety requirements.

M.7.2 Detailed safety assurance activities

Points a) to f) above lead to the safety assurance activities as per **Table 17** below. This is a proposed approach to the assurance of the VLD (safety of the concept) with proper acknowledgement that local assessments may use prominently local procedures / processes as well as material from the SRM.

a) Technical System Implementation		
1	Show that equipment validation tests and other validation measures are adequate to demonstrate that all technical system functional (including performance) requirements are satisfied as per the safety requirements	*Traceability of tests and validation measures to physical element Safety requirements *Expert peer review of test and other validation measures. *Provision of test environment which adequately reproduces the intended system environment for all new or changed physical elements **Note: the software assessment will also provide evidence from verification and testing that the software meets its requirements, but this assurance objective is specifically concerned with total system (hardware/software) behaviour*
2	Show that technical system safety requirements (success) are satisfied and identify any which are not fully satisfied	*Perform system validation testing *Carry out and document a review of test results to confirm the extent to which the safety requirements (success) are met.
3	Show that any residual non-conformances to Safety requirements (success) are suitably mitigated	*Document all justifications for accepting observed defects. *Define and agree with Ops and Engineering stakeholders documented mitigation measures (such as additional procedures) and/or operating limitations necessary to mitigate known defects in system behaviour.
4	Show that equipment elements/subsystems will meet their overall failure rate targets	*Perform reliability analysis (using for example FTA) on the as-implemented system using actual element failure rates. *Note: useful guidance on design measures to achieve system reliability and means for assessing the achieved reliability are given in Part 2 of IEC 61508 Ed 2 (2010)*
5	Show that new software elements have been developed to the allocated SIL/SWAL	*Assessment of the software development process against the detailed requirements of the chosen standard (e.g. IEC 61503-3 and EUROCAE ED-153 - Guidelines for ANS Software Safety Assurance) *Software audits to provide evidence that process has been performed in a satisfactory way. *Provision of software safety folder as per ED-153.
6	Show that modifications to existing software elements has not degraded their integrity	*Assessment as per new software (where required) *Audit of application of SMS software maintenance processes
7	Show that pre-existing off-the-shelf software is of sufficient integrity to meet the software integrity requirements	*Software failure modes and effects analysis to determine impact of failures of pre-existing software *Design of wrappers or other means of isolating and recovering from failures in pre-existing software *Provide evidence from existing use of software and/or testing *Analysis of COTS or other software – for guidance in this difficult area, see IEC 61508 Ed 2

		Part 3 or the UK HSE Guidelines Note: for Linux, a safety assessment report is available.
8	Show that any residual non-conformances to integrity requirements in the Safety requirements are suitably mitigated	*Document all justifications for accepting observed defects. *Define and agree with Ops and Engineering stakeholders documented mitigation measures (such as additional procedures) and/or operating limitations necessary to mitigate known defects in system integrity.
b) ATC and Flight Crew Procedure Design		*Promulgation of ATC and Flight Crew Procedures is not covered here*
1	Show that all new or modified ATC and Flight Crew Procedures have been designed to satisfy the ATC and Flight Crew Procedure safety requirements from V3	*Design new ATC and Flight Crew Procedures in detail. *Design modified ATC and Flight Crew Procedures in detail. *Provide traceability of new or modified procedures to their safety requirements
2	Show that all new or modified ATC and Flight Crew Procedures have been validated	*Review by expert Controller and Flight Crew group(s). *Safety analysis (HAZOPS) of procedures to identify any unforeseen issues introduced at the detailed level. *Real-time simulations of operations using technical system and procedures with realistic traffic loads and patterns (will also contribute to HMI validation objective) with feedback to modify procedures where required. *Note: evidence should include written or captured verbal feedback from ATC and Flight Crew operational staff, and ideally observation by HF experts*. *Note: real-time simulations should include rehearsal of abnormal external conditions and internal failure scenarios*.
c) Engineering Procedure Design		*Promulgation of Engineering Procedures is not covered here*
1	Show that all new or modified Engineering Procedures have been designed to satisfy the Engineering Procedure safety requirements from V3	*Design new Engineering Procedures in detail. *Design modified Engineering Procedures in detail. *Provide traceability of new or modified procedures to their safety requirements
2	Show that all new or modified Engineering Procedures have been validated	*Review of procedures by Engineering staff. *Trial of procedures in a simulated operational environment with feedback to modify any aspects which are incorrect or difficult to execute.
d) ATC and Flight Crew Training Design		*Deliveries of ATC and Flight Crew training, and satisfaction of other ATC and Flight Crew competence requirements, are not covered here.*
1	Conduct a Training Needs Analysis (TNA)	This drives the elements of training
2	Show that Controller and Flight Crew Training Design satisfies the safety requirements established at V3	*Develop classroom-based briefing and training materials by reference to training requirements.

		*Develop CBT training materials by reference to training requirements *Develop scenarios for simulator-based training
3	Show that Controller and Flight Crew Training Design has been validated	*Provide traceability of training courses and simulation exercises to training requirements. *Provide traceability of CBT materials to HMI specifications *Carry out pilot runs of training courses, CBT modules and simulation exercises and modify based on feedback from the pilot courses.
e) Engineering Training Design		*Delivery of Engineering training, and satisfaction of other Engineering competence requirements, are not covered here*
1	Conduct a Training Needs Analysis (TNA)	This drives the elements of training
2	Show that Engineering Training Design satisfies the safety requirements established at V3	*Develop classroom-based training materials by reference to training requirements, where not provided by supplier *Develop practical training exercises for operating procedures and maintenance routines
3	Show that Engineering staff Training Design has been validated	*Review training materials *Try out practical exercises and modify as required
f) Installation and Commissioning		
-	**Preparation**	
1	Show, prior to installation of the VLD equipment, that all hazardous effects of Installation & Commissioning have been identified on local equipment, local operations and external agencies	*Analyse the requirements for the temporary removal of existing equipment and cabling to allow installation of VLD equipment *Analyse any internal network load (average and peak) which may be extra during commissioning (e.g. due to co-existence of current and new equipment) *Analyse any external network load (average and peak) which may be extra during *commissioning (e.g. due to co-existence of old and new equipment) *Identify any necessity for operating existing equipment in degraded modes and effect on the ATM service *Identify any necessity interrupting or degradation of service
2	Show that potential adverse effects of installation & Commissioning have been mitigated by suitable means	*Identify suitable times of day to perform installation & Commissioning activities *Describe and validate arrangements for any temporary disconnection/removal of existing equipment *Describe and validate arrangements for installation and connection of new equipment *Provide evidence that communication capacity will be adequate during commissioning

		*Ensure that any temporary limitations to connections to external ANSPs are duly notified *Ensure that any ATM capacity restrictions are notified to the Network Manager *Promulgate NOTAMs necessary to inform flight crew of temporary degradations of facilities
3	Show that building infrastructure services are adequate to support new equipment	*Analysis permanent and transient requirements for additional power supplies and make provision for them *Analyses any extra cooling arrangements necessary and ensure that they are provided. *Floor loading / space / accessibility
-	**Execution**	
1	Show that commissioning trials and other validation measures are adequate to demonstrate that all technical system requirements are satisfied	*Traceability of test scenarios and validation measures to physical element safety requirements (success) *Expert peer review of test and other validation measures. *Provision of test environment which adequately reproduces the intended system environment for all new or changed physical elements *Describe arrangements for conducting the VLD in a live operational environment and recording results
2	Show that the majority of technical system requirements are satisfied and identify any which are not fully satisfied	*Perform commissioning testing. *Perform operational trials. *Carry out and document a review of test and trials results to confirm the extent to which safety requirements (success) are met.
3	Show that any residual non-conformances to safety requirements (success) or integrity requirements are suitably mitigated	*Document all justifications for accepting observed defects. *Define and agree with Ops and Engineering stakeholders documented mitigation measures (such as additional procedures) and/or operating limitations necessary to mitigate known defects in system behaviour or integrity.

Table 17: Proposed approach to safety assurance of VLD in the industrialization and deployment phases

M.8 End-users & Regulatory Authorities: engagement & co-ordination

This is fully described in **Ref. 17** and consequently not replicated here.

Guidance N On a basic Approach to Common Cause Analysis

N.1 Introduction

Systems in the aviation environment often demand high availability which is usually achieved, amongst others, via redundancy. In the absence of dependent failures (this means the separate branches of a redundant system are regarded as independent) the unavailability of the function is essentially the product of the unavailability of the separate branches. While this is very effective to avoid loss of system functionality due to random component failures (which is a main factor for e.g. hardware loss), this method can be subverted by failures, which systematically affect all redundant branches and thus results in much higher system unavailability

Multiple failures of components due to shared causes, also known as Common Cause Failures (CCF), therefore comprise an important class of failure types, which is responsible for a substantial amount of system failures in the high availability domain. They have to be taken into account in any serious assessment of safety critical systems deploying a redundancy concept.

While common cause analysis is not specific to the Safety Reference Material, the SRM requires common cause analysis in **Guidance A.4** “Detailed safety assurance activities to inform the TS and refined version of the SPR”, specifically in:

- P7|AO1|a6:
  Identify all reasonably foreseeable sources of common cause or other dependent failures
  … Perform Common Cause Failure Analysis (including identification of CCF groups from minimal cut-sets of fault tree, zonal hazard analysis and expert judgement); and
- P7|AO1|a8:
  Apportion quantitative failure targets to all equipment elements
  * Show that reliability calculations have been moderated to take account of possible residual common cause failures – includes selection and justification of any beta-factors or other methods used for moderating reliability calculations

There are a number of CCF assessment methods established for very specific domains such as the Zonal Hazard Analysis or the Particular Risk Assessment, which are often used e.g. in aviation or maritime. They have a strong focus on risk associated to physical containment zones and interaction of adjacent systems that is very specific for a given design (e.g. fan burst for a jet turbine, which could affect redundant hydraulics or electrical lines). They are therefore not fully applicable to many ground based electronics or IT systems. Quite common is also the approach to draw fault trees or Bayesian networks of the considered system and check for identical basic events appearing on the root of redundant branches or basic events leading via unexpected combinations of branches to top-events. While this can be very powerful, if the system is modelled to a very high granularity, the related effort can quickly go beyond given budgets in many domains.

Another way to treat common cause failures is the calculation of common cause effects within fault trees or reliability block diagrams, based on estimated factors of interference between redundant systems. This approach, which is e.g. detailed in [IEC61508], gives more realistic system availability figures, but does not help to remove CCFs.

There are many standards, which describe CCF analyses, but most with very limited detail. [SAE_ARP4761] (See reference in section **N.7**) describes a so called “Common Mode Analysis” in reasonable detail, including a comprehensive checklist and details on reports, etc. and is therefore suggested for further reading. In the nuclear power plant domain, there are several standards with explicit procedures on how to treat CCF in safety and reliability studies to enhance specifically nuclear power plant safety, e.g. [NUREG 4780].

This guidance aims to present a very general but still structured approach to a basic Common Cause Analysis (CCA), which can be adopted for a specific domain and thus enables safety experts to derive their specific CCA in their field of work. It is based on the paper [GenAppCCA].

While the presented implementation example (section **N.4.1**) details a physical design of a system, i.e. works on physical level, the underlying approach can be applied to any level.

N.2 Definitions

Common Cause Failure (CCF): One simple definition of a common cause failure is “a failure of two or more components, system, or structures due to a single specific event or cause.” A more complex definition is “an event or cause which bypasses or invalidates redundancy or independence, i.e., an event which causes the simultaneous loss of redundant or independent items which may or may not include inadvertent operation, or an unintended cascading effect from other operations or failure within the system.” [CCFM].

Another definition is given in [SRD R196]: “A Common-Mode Failure is the result of an event(s) which because of dependencies, causes a coincidence of failure states of components in two or more separate channels of a redundancy system, leading to the defined system failing to perform its intended function.”

The most straight forward definition is given in [NUREG 4780]: “Common cause failures are defined as that cutset of dependent failures for which causes are not explicitly included in the logic model as basic events.”

Root Cause: (based on [NUREG 4780]): Ideally, the cause of an event can be traced to an event that occurred at some distinct but possibly unknown point in time. These causal events are known as "root cause." There are three general types of root causes.

a) Hardware: Isolated random equipment failures due to physical causes inherent in the affected component.

b) Human: Errors during system operations (dynamic), errors during equipment testing or maintenance, and errors during design, manufacturing, and construction.

c) External: Events that initiate external to the system that result e.g. in abnormal environmental stresses being applied to the equipment.

System: In this guidance “system” refers to a “Functional system” as of the Safety Reference Material definitions (“…combination of equipment, procedures and human resources organised to perform a function within the context of air navigation services…”), i.e. the entity on operational or architectural level, which is considered within the specific safety analysis. There have to be defined boundaries, sub-systems, interfaces to the external world (environment) and within sub-systems. Sub-systems can be defined on any level below (component-, Line Replaceable Unit-, software unit-, software function-,…level), depending on the need of the current analysis.

Basic Event: “Basic event” in this guidance refers to an event on the lowest level modelled in the current analysis.

N.3 Classification of Common Cause Failures

There are some differentiators of common cause failures, which can be used for classification for easier understanding and communication of analysis targets and focus. They have in common, that always two or more systems, sub-systems or system functions, which were considered as independent in the previous modelling, are in some way interrelated/coupled, i.e. there is interference.

Effect: The first differentiator distinguishes according to the effect:

a) More than one branch of a redundant system or

b) More than one system function

(…) are affected by the same common cause. This guidance focuses on the redundant system branches, but the considerations mostly apply for the second type, too.

Causal Factor: The cause can result from two basic levels:

a) Sub-system level: One sub-system (this can go down to e.g. single component or software unit) affects another via an internal interface. Within the sub-system level many sub-levels are possible.

b) System level: An external system influences the considered system via an external interface. This also includes environmental conditions.

Interfaces can in both cases either be an intentionally constructed interface or an "emergent" interface.

Coupling Mechanism: A coupling mechanism is a way to explain how a root cause propagates to involve multiple sub-systems or functions. It can in itself be distinguished in several classes, which are detailed in the following chapter.

The first differentiator for coupling mechanisms is the
"Reason" for coupling:

a) Shared resources: Commonly used equipment, space, memory, bandwidth, CPU processing power, software, common reservoir for hydraulic system, etc. This can be used either in parallel or sequentially and either internal or external to the considered system.

b) Common input: There is a common input/information to the redundant system branches. This mainly refers to the IT domain or the operational level, as for physical systems this often can be considered as shared resource. It can as well be both from within or from outside the considered system.

c) Common characteristic: Common characteristics like e.g. supplier, age of the component or time after putting it operational

d) Human coupling: Refers to human activities, such as requirements engineering, design, manufacturing, construction, installation, system integration, testing, quality control, transportation procedures, system management, training (procedures), operating (procedures), emergency procedures, maintenance (procedures), etc.

Many contributing factors are related to reason a) "Shared resources" - "space", e.g.:

i. Environmental conditions

(1) Electromagnetic interference/radiation
(2) Static charge
(3) Thermal conditions
(4) Vibration
(5) Humidity (may e.g. lead to corrosion, condensed moisture and thus short circuits, etc.)
(6) Contamination (foreign object, chemical degradation, etc.)
(7) Pressure
(8) Dust, smoke, etc.

ii. b) Major external events

(1) Fire
(2) Flood
(3) Earthquake
(4) Lightning
(5) Severe weather (ice, rain, winds)

iii. c) Mechanical impact (moving parts in vehicle)

iv. d) Physical impact within the system, i.e. any of the environmental conditions influenced by another sub-system, e.g. air-condition fails thus leading to both redundant branches of IT equipment to fail, hydraulic leak in plane affects redundant electronics.

The second differentiator for coupling mechanisms looks at the
Basic interrelation:
a) One or several underlying causes affect all redundant system branches
b) One of the redundant system branches affects the other branches, e.g. when electrical power supplies are operated in load sharing mode and one fails, the other may be more likely to fail due to the higher load.

Please note that coupling mechanisms do not have to be deterministic, but can also be probabilistic, e.g. overheating of one branch can heat up the second branch and thus lead to higher probability of failure.

Typical sources for identification of coupling mechanisms are:
*) Historical data
*) Check-lists, from standards, previous analyses, etc.; typically based on historical data
*) Failure modes and effects or event tree type analyses, where focus is put on possible effects on other sub-systems

In the IT domain and especially with IP based networks security is getting more and more an issue, which can easily have major influence on system functionality and subsequently on safety, independent of any redundancy. It therefore represents a typical common cause failure. Safety and security should not be considered completely independent, as currently usual, but treated in a combined analysis, where identified security threats and also security mitigations are checked for relevance as causal factors of safety issues (possibly representing a common cause, which may lead to system failure).

N.4 Common Cause Analysis Method Overview

N.4.1 Common Cause Analysis for System Redundancies

The following list depicts a brief overview of the suggested process for a Common Cause Analysis:

1. Identification of the system to be analysed.

2. Identification of redundancies within the system (Redundancy Clusters – RC which can be represented e.g. by successive safety barriers or redundant hardware components.

3. Identification of Common Cause Redundancy Groups (RG): Categories of redundant parts of the system or of successive safety barriers (which essentially are redundancies, see also AIM) with a common attribute or dependence on a common resource, which may impose susceptibility to a specific common cause.

4. Allocation of system parts to Redundancy Groups.

5. Identification of possible coupling mechanisms and related Common Root Causes (CRC), i.e. basic common cause failure modes which could affect redundant components.

6. Allocation of possible Common Root Causes to Redundancy Groups.

7. Assessment of worst (credible) case system level effects of common cause failures for every Redundancy Cluster, which can be performed e.g. by linking to (existing or emerging) system level hazards. This step does not need to be in this sequence (it can basically be done from step 2. onwards).

8. Identification of specific Common Cause Failures (CCF) by application of allocated basic Common Root Causes to the Redundancy Groups.

9. Assignment or derivation of respective defences/mitigations for each Common Cause Failure Mode.

10. Derivation of safety requirements to facilitate defined defences/mitigations.

Please note, that this analysis can be performed on several levels (function, sub-function, technical level,…) and it may be necessary to perform it first on a high level, subsequently in more detail on a lower level and feedback results to the high level analysis. The strategy behind each step of the analysis has to be thoroughly considered and documented. A database based tool may be necessary to cope with the complexity of the analysis, to guarantee consistency and to maintain traceability between all involved artefacts.

A graphical representation of the above sequence is given in **Figure 28** below.

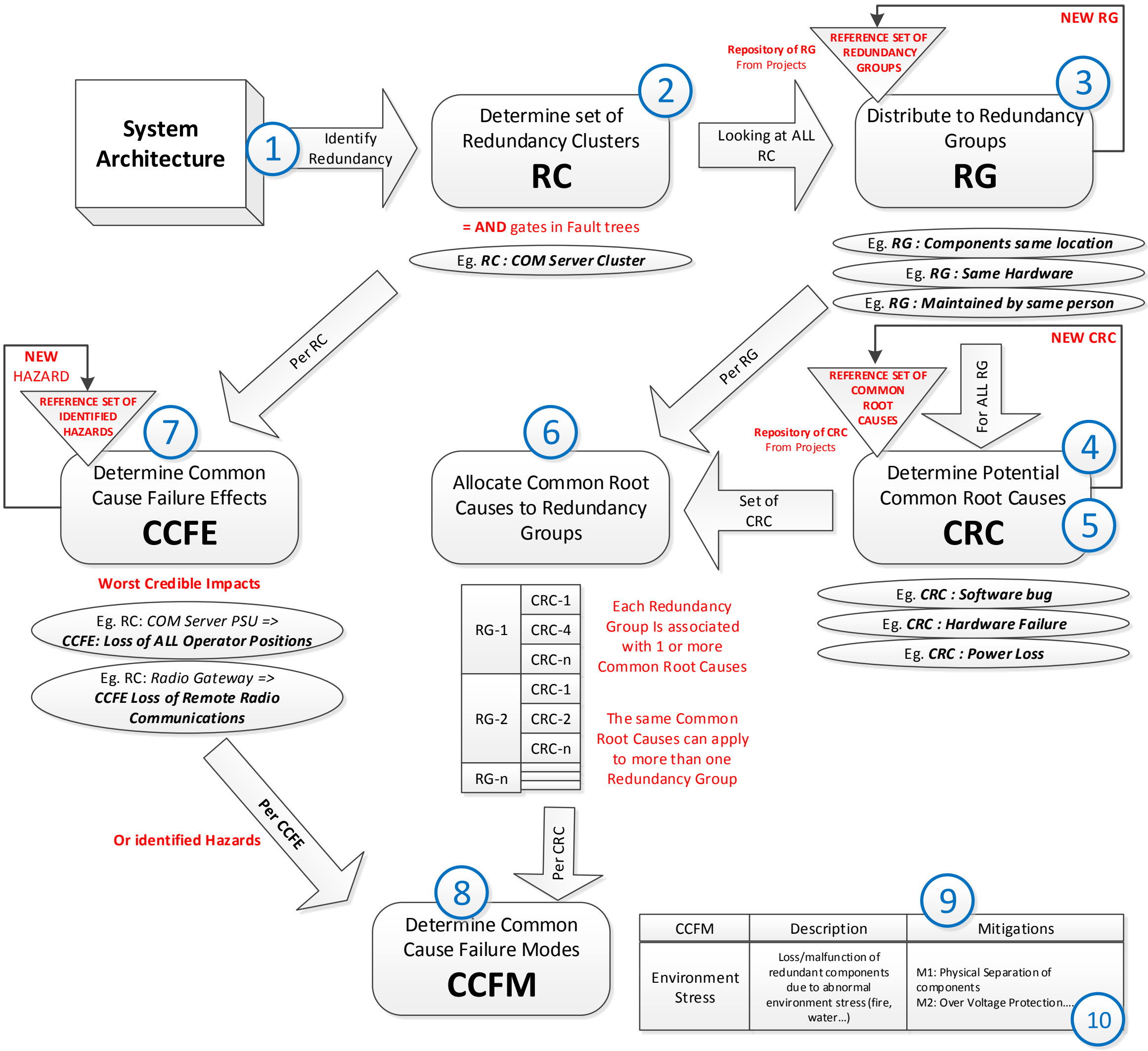

System Architecture
1
Identify Redundancy
Determine set of Redundancy Clusters
RC
2
= AND gates in Fault trees
Eg. RC : COM Server Cluster
Looking at ALL RC
Repository of RG From Projects
REFERENCE SET OF REDUNDANCY GROUPS
NEW RG
3
Distribute to Redundancy Groups
RG
Eg. RG : Components same location
Eg. RG : Same Hardware
Eg. RG : Maintained by same person
Per RC
Per RG
NEW CRC
REFERENCE SET OF COMMON ROOT CAUSES
Repository of CRC From Projects
For ALL RG
4
Determine Potential Common Root Causes
CRC
5
Eg. CRC : Software bug
Eg. CRC : Hardware Failure
Eg. CRC : Power Loss
Set of CRC
6
Allocate Common Root Causes to Redundancy Groups
NEW HAZARD
REFERENCE SET OF IDENTIFIED HAZARDS
7
Determine Common Cause Failure Effects
CCFE
Worst Credible Impacts
Eg. RC: COM Server PSU => CCFE: Loss of ALL Operator Positions
Eg. RC: Radio Gateway => CCFE Loss of Remote Radio Communications
RG-1
CRC-1
CRC-4
CRC-n
RG-2
CRC-1
CRC-2
CRC-n
RG-n
Each Redundancy Group Is associated with 1 or more Common Root Causes
The same Common Root Causes can apply to more than one Redundancy Group
Per CCFE
Or identified Hazards
Per CRC
8
Determine Common Cause Failure Modes
CCFM
9
CCFM
Description
Mitigations
Environment Stress
Loss/malfunction of redundant components due to abnormal environment stress (fire, water…)
M1: Physical Separation of components
M2: Over Voltage Protection….
10

Figure 28: Suggested process for process for a Common Cause Analysis

N.4.2 Common Cause Analysis for Multiple System Functions

A very similar process can be applied for the analysis of common causes affecting more than one system function:

1. Identification of the system to be analysed.

2. Identification of dependencies of more than one system function on any item or resource within the architecture (people, procedure, equipment) => Dependency Clusters – DC. Please Note: This can be

a) one instance of an element/item, which is influencing more than one system function (e.g. one server used for Voice Communication and for Surveillance) => any failure of this item is a common cause failure and this process is to be continued with step 7, 9 and 10

or

b) the same type of element/item (e.g. one server for Voice Communication and one server for Surveillance, but the same type of server) used for more than one function (e.g. Voice Communication and Surveillance) => every systematic failure can be a CCF and such a dependency cluster represents already a dependency group as of step 3.

3. Identification of Common Cause Dependency Groups (DG): Categories of dependent parts of the system with a common attribute or dependence on a common resource, which may impose susceptibility to a specific common cause. These DGs include but are not limited to the Dependency Clusters of step 2.

4. Allocation of system parts to Dependency Groups.

5. Identification of possible coupling mechanisms and related Common Root Causes (CRC), i.e. basic common cause failure modes which could affect dependent components. These CRCs can additionally be investigated for simultaneous effects on independent items used for different system functions, which would then also represent a common cause failure.

6. Allocation of possible Common Root Causes to Dependency Groups.

7. Determine Common Cause Failure Effect (CCFE) by consideration of the combined occurrence at all affected system functions.

8. Identification of specific Common Cause Failures (CCF) by application of allocated basic Common Root Causes to the Dependency Groups.

9. Assignment or derivation of respective defences/mitigations for each Common Cause Failure Mode.

10. Derivation of safety requirements to facilitate defined defences/mitigations.

A graphical representation is shown in **Figure 29** below.

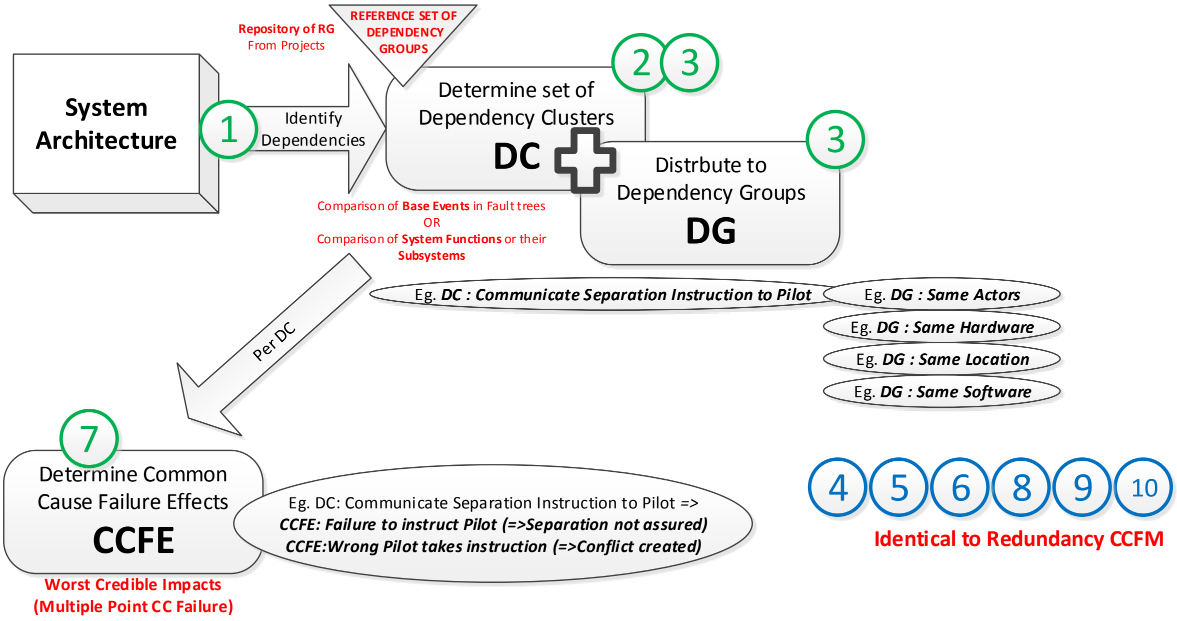

Repository of RG
From Projects
REFERENCE SET OF DEPENDENCY GROUPS
System Architecture
1
Identify Dependencies
2
3
Determine set of Dependency Clusters
DC
3
Distrbute to Dependency Groups
DG
Comparison of Base Events in Fault trees
OR
Comparison of System Functions or their Subsystems
Eg. DC : Communicate Separation Instruction to Pilot
Eg. DG : Same Actors
Eg. DG : Same Hardware
Eg. DG : Same Location
Eg. DG : Same Software
Per DC
7
Determine Common Cause Failure Effects
CCFE
Worst Credible Impacts
(Multiple Point CC Failure)
Eg. DC: Communicate Separation Instruction to Pilot =>
CCFE: Failure to instruct Pilot (=>Separation not assured)
CCFE:Wrong Pilot takes instruction (=>Conflict created)
4
5
6
8
9
10
Identical to Redundancy CCFM

Figure 29: Case of common causes affecting more than one system function

N.5 Common Cause Analysis for Multiple System Functions

In the following an example CCA implementation on physical level is given, to further illustrate the above method.

Considered System:

The system considered in this analysis is a Voice Communication System for Air Traffic Management.

Assumptions:
This analysis is based on the following assumptions:

ID	Assumption
ASS_001	The system configuration provides more than one Operator Position per controlled air-space sector.
ASS_002	The system is used within the specified environmental conditions.
ASS_003	The system is monitored by the system monitoring and control department via the monitoring system during its entire System Operating Time (SOT) and component failures are repaired immediately after detection.
ASS_004	Required maintenance staffs of customer and sufficient number of spares are available at any point in time during SOT.

Table 18: Assumptions - Voice Communication System for Air Traffic Management

Redundancy Clusters:

The first step of the analysis itself is the identification of areas of the system architecture with redundancy.
The Redundancy Clusters are those parts of the system, which provide a specific technical core functionality and have the same kind of redundancy concept (e.g. the Operator Positions Cluster with the redundancy via spare positions, which can be used by operators in case of position loss; the Comm Server Core cluster, which provides basic switching capability and is fully redundant in hot standby mode; etc.).
The Redundancy Clusters are listed in the **Table 19** below:

ID	Redundancy Clusters	Redundancy Type
RC_1	Operator Positions	Spare positions, k out of n, operator has to change positions in case of loss (as long as enough operational positions are remaining).
RC_2	Comm Server Switches	Full hot-hot redundancy (both Ethernet switch branches continuously working, end-node decides, from where it takes the signal). Transparent to operator.
RC_3	Comm Server Core	Full hot-hot redundancy (both switch halves continuously working, end-node decides, from where it takes the signal). Transparent to operator.
RC_4	Comm Server PSU	Fully hot-hot redundant. Loss of redundancy is transparent to operator.
RC_5	Phone Interfaces	Redundancy via trunking or use of alternative lines by operator.

RC_6	Radio Interfaces IP	Full hot-hot redundant connection to one radio with automatic switchover to parallel session plus use of backup radio, with automatic switchover and partially multi frequency spare radios.
RC_7	Radio Interfaces Analogue	Use of backup radios
RC_8	IT Infrastructure	Redundancy by automatic routing via alternative Ethernet-switches. Loss of redundancy is transparent to operator (except for phone call, which may be terminated and then has to be re-initiated by user).
RC_9	VCMS (Monitoring System)	Redundant servers and access via more than one client-workstation possible.
RC_10	Role Location Server	Fully redundant. Loss of redundancy is transparent to operator.
RC_11	Radio Gateway	Functional redundancy via automatic routing to alternative radio gateway.

Table 19: Redundancy Clusters

Common Cause Redundancy Groups:

The next step of the analysis aims at the identification of all categories of redundant components with a common attribute, which may impose susceptibility to a specific common cause.

ID	Common Cause Redundancy Groups
RG_001	Redundant components at the same location
RG_002	Redundant components with the same hardware
RG_003	Redundant components with the same software
RG_004	Redundant components operated or maintained by same staff
RG_005	Redundant components connected to the same power supply/mains
RG_006	Redundant components with the same data feed

Table 20: Common Cause Redundancy Groups

Allocation of System Components to Common Cause Redundancy Groups:

The allocation of system components to the Common Cause Redundancy Groups is based on the analysis of which of the common attributes of the Redundancy Groups are relevant for the Redundancy Clusters. Via this allocation, it is possible to explicitly identify which system components are affected by a specific common cause failure mode, as derived from the Redundancy Groups in a later step.

ID	Common Cause Redundancy Group	Redundancy Cluster
RG_001	Redundant components at the same location	On building level: RC_1, RC_2, RC_3, RC_4, RC_5, RC_6, RC_7, RC_8, RC_9; On room level: RC_1, RC_2, RC_4,
RG_002	Redundant components with the same hardware	RC_1, RC_2, RC_3, RC_4, RC_5, RC_6, RC_7, RC_8, RC_9, RC_10, RC_11
RG_003	Redundant components with the same software	RC_1, RC_2, RC_3, RC_5, RC_6, RC_7, RC_8, RC_9, RC_10, RC_11
RG_004	Redundant components operated or maintained by same staff	RC_1, RC_2, RC_3, RC_4, RC_5, RC_6, RC_7, RC_8, RC_9, RC_10, RC_11
RG_005	Redundant components connected to the same power supply/mains	RC_1, RC_2, RC_3, RC_4, RC_5, RC_6, RC_8, RC_9
RG_006	Redundant components with the same data feed via interfaces	RC_1, RC_2, RC_3, RC_6, RC_7, RC_8, RC_9

Table 21: Allocation of System Parts to Redundancy Groups

Possible Common Root Causes:

Based on the Common Cause Redundancy Groups and with consideration of relevant coupling mechanisms due to the specific system architecture and used technologies, possible Common Root Causes are identified.

ID	Description	Condensed
CRC_1.	Software design bug (triggered via data/parameter/time/race condition)	SW bug
CRC_2.	Hardware design bug	HW bug
CRC_3.	Erroneous manufacturing/installation	Err. manufact./install.
CRC_4.	Erroneous operation	Err. Operation
CRC_5.	Erroneous maintenance (including configuration/parameterisation, damage to cables)	Err. Maintenance
CRC_6.	Corrupt/malicious Data from adjacent system	Corrupt data
CRC_7.	Loss/malfunction of power (instable, increased, too low - e.g. at loss of one redundant PSU, …)	Power loss/malfct.
CRC_8.	Abnormal environmental stress (fire, water, earthquake, lightning related overvoltage, electromagnetic radiation ...)	Environment. Stress

Table 22: Common Root Causes

Allocation of Root Causes to Common Cause Redundancy Groups:

In this step, Possible Common Root Causes are allocated to those Common Cause Redundancy Groups, where they are most relevant with respect to the common attribute. This serves as basis for the subsequent common cause failure modes analysis.

ID	Common Cause Redundancy Groups	Relevant Possible Common Root Causes
RG_1	Redundant system parts at the same location	CRC_8. Abnormal environmental stress (fire, water, earthquake, lightning related overvoltage, electromagnetic radiation ...)
RG_2	Redundant components with the same hardware	CRC_2. Hardware design bug CRC_3. Erroneous manufacturing/installation
RG_3	Redundant components with the same software	CRC_1. Software design bug (triggered via data/parameter/time/race condition)
RG_4	Redundant components operated and maintained by same maintenance staff	CRC_4. Erroneous operation CRC_5. Erroneous maintenance (including configuration/parameterisation, damage to cables)
RG_5	Redundant components connected to the same power supply/mains	CRC_7. Loss/malfunction of power (instable, increased, too low - e.g. at loss of one redundant PSU, …)
RG_6	Redundant components with the same data feed via interfaces	CRC_6. Corrupt/malicious Data from adjacent system

Table 23: Allocation of Root Causes to Redundancy Groups

Effects of Common Cause Failures:

Table 24 below details the worst case system level effects (**Common Cause Failure Effect)**, which may result of a common cause failure within a specific Redundancy Cluster.

ID	Redundancy Clusters	Common Cause Failure Effect
RC_1	Operator Positions	Loss of all Operator Positions
RC_2	CommServer Switches	Loss of all Operator Positions
RC_3	CommServer Core	Loss of all Operator Positions

RC_4	CommServer PSU	Loss of all Operator Positions
RC_5	Phone Interfaces	Loss of all phone connections
RC_6	Radio Interfaces IP	Loss of all IP radio connections
RC_7	Radio Interfaces Analogue	Loss of all analogue radio connections
RC_8	IT Infrastructure	Loss of all phone and radio connections
RC_9	VCMS	Loss of system monitoring and control capability
RC_10	Role Location Server	Loss of role allocation capability
RC_11	Radio Gateway	Loss of all remote radio connections

Table 24: Effects of Common Cause Failures

Identification of Common Cause Failures and Derivation of Mitigations:

In the following section of the analysis, the relevant specific Common Cause Failures (CCF) of the Redundancy Groups are derived via application of the allocated basic Common Root Causes. Subsequently existing mitigations are assigned or new mitigations defined, if considered necessary.
In this context "T:" refers to a technical mitigation, which is built into the system, "O:" relates to an operational mitigation, which has to be covered with respective procedures and "P:" refers to a process related mitigation, which is covered by a supplier's company process.

In this guidance only one table with the CCFs based on one Common Root Cause of one Redundancy Group is presented as example (see **Table 25** below). Derivation of respective Safety Requirements is not shown, as this step is mainly a transformation of the mitigations into requirements language.

Common Cause Failures of: RG_001 - Redundant components at the same location			
ID	CRC	Description	Mitigations
CCF _005	CRC_8. Environment. Stress	Loss/malfunction of redundant components due to abnormal environmental stress (fire, water, earthquake, lightning related overvoltage, electromagnetic radiation ...)	- Mit_005: T: Physical separation of redundant components (e.g. located on different floors or in different fire compartments). - Mit_006: T: Each power supply is provided with an over-voltage protection. In combination with a lightning protection at the main power distribution frame, this is sufficient protection against indirect lightning strike. - Mit_007: T: Each interface is provided with an over-voltage protection. In combination with a lightning protection at the main power distribution frame, this is a sufficient protection against indirect lightning strike. - Mit_008: T: Earthquake resistant building, protection of the cabinets by anchorage, screw connection or shock absorber. - Mit_009: T: Installation of the system above ground level. - Mit_010: T: All equipment is EMC (ElectroMagnetic Compatibility) protected in line with EN 55024 - Mit_011: T: Proper grounding concept; protected equipment room; filter at external lines. - Mit_015: T: Labelling, physical

			protection and separation of cables (cable routing through different cable ducts). - Mit_021: T: Built In Test (BIT) applications and watchdogs are used to monitor the hardware and internal states and report the alarms to the monitoring system.

Table 25: Derivation of Common Cause Failures

N.6 Conclusion

The presented approach is only a framework of common cause analysis of redundant systems (at different levels), which is intended to be adopted and refined for specific domains. Over time relevant common causes for this area will get better known and respective checklists and/or templates can be developed. The analysis may need to be performed on several levels. To get reasonable and consistent results appropriate knowledge of the system and proper management of the whole process is essential.

Further details can be found e.g. in [SAE_ARP4761] and [NUREG 4780].

N.7 References for Guidance N

1. [CCFM] Common Cause Failure Modes; Paper, NASA Archive; Jon Wetherholt, NASA Marshall Space Flight Center, Huntsville, Alabama, USA; Timothy J. Heimann, NASA Marshall Space Flight Center, Huntsville, Alabama, USA
2. [GenAppCCA] General Approach to Common Cause Failures Analysis, ISSC 2015, W. Winkelbauer, G. Schedl, Frequentis AG; Vienna, Austria
3. [IEC61508] Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES)
4. [NUREG 4780] Procedures for Treating Common Cause Failures in Safety and Reliability Studies; NUREG/CR-4780, EPRI NP-5613
5. [SAE_ARP4761] SAE Aerospace Recommended Practice: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment
6. [SRD R196] Defences against Common-Mode Failures in Redundancy Systems – A Guide for Management, Designers and Operators, SRD R196, AJ Bourne, GT Edwards, DM Hunns, DR Poulter, IA Watson, January 1981

Guidance O On the Allocation of Software Assurance Level to ground system components

O.1 Introduction

The objective of this section is to provide guidance to the following physical level safety assurance activity defined in **Guidance A.4** “Detailed safety assurance activities to inform the TS and refined version of the SPR”:

> ***P7-AO1-a9:*** *Allocate an appropriate Software Assurance (or Safety Integrity) level to all software elements*

The process for the allocation of the software assurance level (SWAL) to software elements of ground components proposed in this guidance has been defined:

- Taking into account current regulation and standards on SWALs (see **O.2** below)[14]
- Being in line with the SRM approach (hazards identification, severity classes, etc.)
- Using, as relevant, existing tools, techniques and processes already defined in the SRM (AIM, fault trees, …)

This guidance provides the following information:

- Regulation framework in which the guidance have been developed
- A description of the proposed SWAL allocation process, as an overview and in detail
- The tables for the allocation of SWAL with respect to the several accidents types

O.2 Regulatory framework

The regulatory framework in which this guidance has been defined is the EC 482/2008[15]:

> ***Article 4****: Requirements applying to the software safety assurance system*
>
> *The organisation shall ensure, as a minimum, that the software safety assurance system:*
>
> *[…]*
>
> *2. allocates software assurance levels to all operational EATMN software in compliance with the requirements set out in*
>
> ***Annex I****: Requirements applying to the software assurance level referred to in Article 4(2)*
>
> *1. The software assurance level shall relate the rigour of the software assurances to the criticality of EATMN software by using the severity classification scheme set out in Section 4 of point 3.2.4 of Annex II to Regulation (EC) No 2096/2005 combined with the likelihood of the occurrence of a certain adverse effect. A minimum of four software assurance levels shall be identified, with software assurance level 1 indicating the most critical level.*

[14] While not explicitly mentioned in EU No. TBD repealing EC 482/2008 and EU Nos 1034/2011 and 1035/2011, the use of assurance level concepts (incl. SWAL) can be helpful in generating the relevant body of evidence.

[15] Commission Regulation (EC) No 482/2008 of 30 May 2008 establishing a software safety assurance system to be implemented by air navigation service providers and amending Annex II to Regulation (EC) No 2096/2005 (OJ L 141, 31.5.2008, p. 5).

2. An allocated software assurance level shall be commensurate with the most severe effect that software malfunctions or failures may cause. This shall, in particular, take into account the risks associated with software malfunctions or failures and the architectural and/or procedural defences identified.

3. EATMN software components that cannot be shown to be independent of one another shall be allocated the software assurance level of the most critical of the dependent components.

O.3 Definitions

Equipment hazard contributor (EHC): for a given equipment, event observed at the limits of this equipment, and which is an effect of a failure occurring inside this equipment, and that may lead to an operational Hazard (c.f. Hazard definition). EHCs are used by equipment manufacturers to carry out safety engineering analyses in order to design appropriate technical mitigations means and define appropriate SWAL levels to software components

Hazard (as per SRM definition): 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 introduced by 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, which are created by failure of the ATM/ANS functional system.

Currently, in Regulation (EC) No 1035/2011, the following definition applies: “‘hazard’ means any condition, event, or circumstance which could induce an accident”.

Software malfunction (as per EC 482/2008): means the inability of a programme to perform a required function correctly

Software failure (as per EC 482/2008): means the inability of a programme to perform a required function

O.4 Software Assurance Level allocation process - Overview

The proposed Software Assurance Level allocation approach method aims at complying with EC 482/2008. It only considers the software causes of operational hazards. The SWAL allocation process considers then the software malfunction of equipment, the corresponding identified hazards and their respective effects.

Based on that, it has firstly to be understood at what V-phase in SESAR the software malfunctions can be identified. The equipment item specification is defined at V3 and documented in the Technical Specification[16] (TS). The TS provides the description of “*What*” the technical system does. The software and hardware components of the equipment item are identified during the definition of the equipment architectural design activity that is beyond V3[17], where the equipment requirements are allocated to the hardware and software components or a combination of them, so it is during this activity when the design decisions are taken regarding the equipment implementation of the functionalities by software, hardware, or a combination of them. These hardware and software components specification is defined and documented beyond V3. The SRD/SRS[18] provides the software specification describing “*How*” the software implements the technical system function specified in the TS.

[16] The TS is equivalent to the SRS/SSS (IEEE/EIA 12207.2 and MIL-STD-498 terminology respectively).

[17] This is documented in the SARAD/SSDD (IEEE/EIA 12207.2 and MIL-STD-498 terminology respectively).

[18] Each SW component is documented in a SRD/SRS (IEEE/EIA 12207.2 and MIL-STD-498 terminology respectively).

The approach proposed in this guidance is then focused on

- **Software systems** (systems where all the functionalities are implemented by software that runs on COTS HW), where the functional system (people, procedures and equipment) architectural design is known (at the technical architectural level in the SESAR SRM - SPR at V3), and the Technical Specification (TS) is known, so it can be known at a high level ”what” the software does, but not “How” the technical function has been implemented by the software.

- **Ground systems** only.

This approach does not apply to Airborne Systems for which specific processes are already defined and to be used.

The process proposed here takes as basis, as mentioned before, the ED-153 approach, adapting it to the specificities of the Safety Reference Material, in particular in terms of the several severity classes to be considered (per type of accident) and the way they are defined.

The following considerations have been taken into account in this process of SWAL allocation:

A. The severity class of the hazard due to software malfunction is the one corresponding to the severity associated to the worst credible hazard effect as per Guidance E.

B. Likelihood of occurrence (usually known as ‘distance’) of a certain effect of the hazard due to software malfunction is the combination of:

  - The likelihood that once the software has malfunctioned or failed this malfunction/failure generates a hazard. This likelihood is called ‘Ph’ and it’s usually identified during the PSSA.

  - The likelihood that the hazard generates an effect, having a severity associated. This likelihood is called ‘Pe’ and it’s usually identified during the FHA.

The assessment of the quantification of the likelihood of the occurrence of an effect of the hazard due to software malfunctions is done after the failure in the software of the EHC has happened, so that likelihood is a function of the efficiency of the risk mitigation means (prevention/detection and protection) implemented in the functional system regardless of the software failure frequency (which is impracticable to predict).

This requires that the technical solution is "a little bit mature" (in V3) in terms of a preliminary technical architecture, due to this method needs to identify the software components whose failure would cause an operational hazard. Nevertheless, and as explained in the following sections, the process is proposed to be done in two steps, starting in V2 once the EHC can be already identified, and then refining it in V3 once the detail of the technical solution starts to be defined.

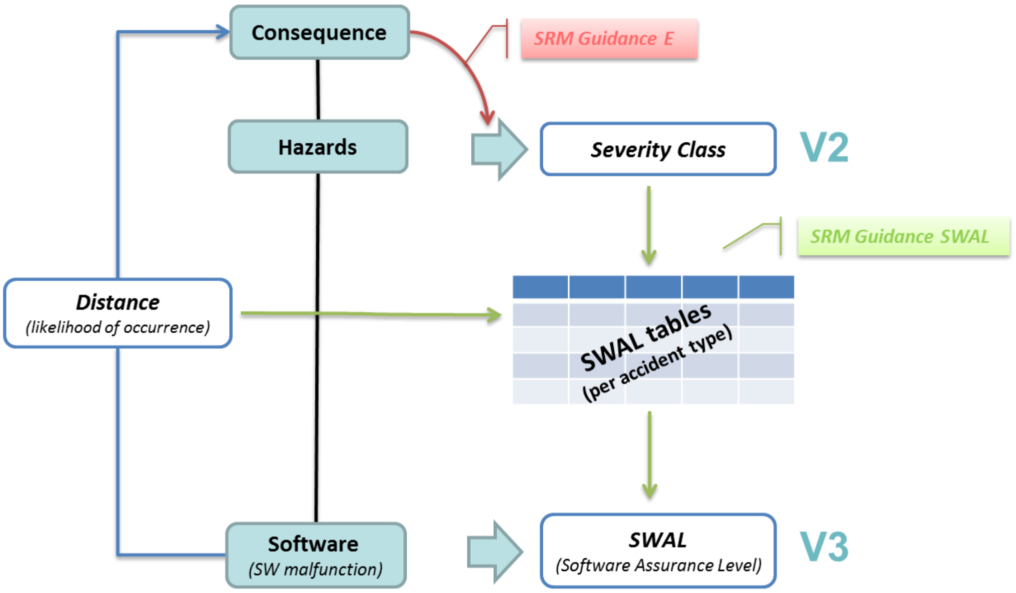


Figure 30: SWAL allocation process overview

Figure 30 provides an overview of the proposed allocation process for software assurance level. Following sections provide more detail on the several steps and the two key elements of the proposed SWAL allocation process.

O.5 Defining the Severity class

During the V2 safety assessment phase, a set of hazards are identified and the corresponding safety objectives are defined. The process for the allocation of the severity class to the identified hazards, which is the basis for defining the corresponding safety objective, is described in **Guidance E**.

In this proposed approach, the ‘Pe’ mentioned above is already included in the allocation of the severity class as the potential protection means are to be considered when defining the consequence of the hazard and the corresponding safety objective.

O.6 Defining the ‘distance’

Concerning the distance ‘Ph’ mentioned above, i.e. the likelihood of the occurrence of the hazard once the software malfunction occurs, it is to be defined taking into account those mitigations means preventing the hazard to occur. Two types of prevention mitigation means are to be considered for that:

- Operational mitigations means and
- Technical mitigation means.

These prevention mitigation means are identified during the following two phases, and thus the corresponding ‘distance’ is defined in two steps as shown in **Figure 31** below:

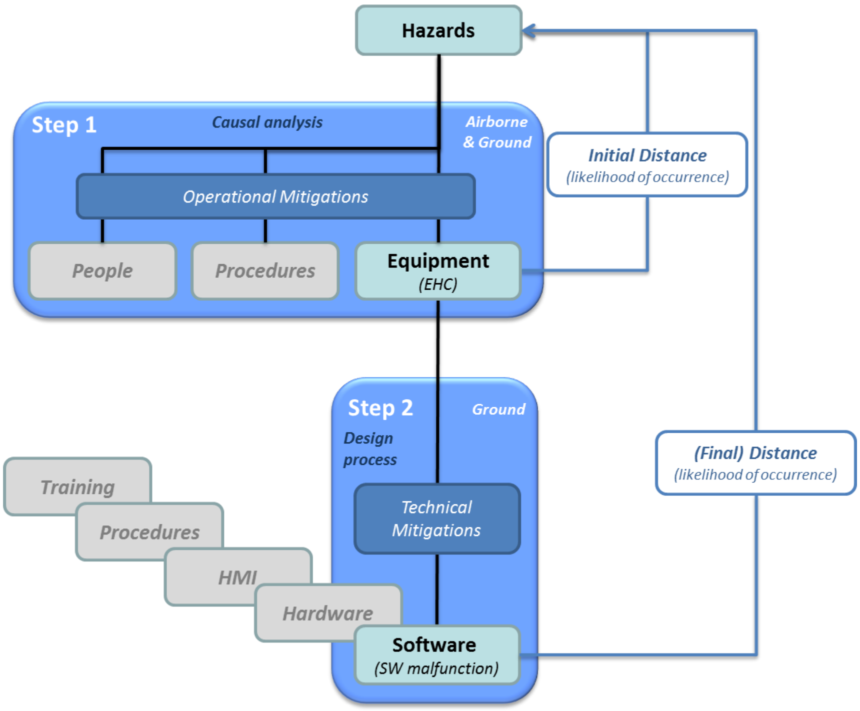


Figure 31: Distance definition process in 2 steps

- **Step 1** [OSED and SPR V2 phases]: allocation from the relevant safety objectives on hazards of the corresponding requirements at the level of the functional system items (i.e. people, procedure and equipment). In this step an '*Initial Distance*' is provided taking into account Operational mitigation means identified during the performed causal analysis.

- **Step 2** [SPR V3 and TS phases]: allocation from the corresponding functional system requirements to the equipment and description of "What" the equipment does. During this second step the Initial Distance is refined taking into account the architecture mitigation means specified during the physical design phase and thus the '*Final Distance*' is obtained (i.e. the likelihood of a certain effect of a hazard due to the software malfunction). "How" the architectural mitigations have been implemented by the technical system architecture and the software functions, can only be assessed beyond V3, when the SARAD/SSDD and SRD/SRS respectively are defined and documented, so then the '*Final Distance*' can be confirmed.

These two steps are described in more detail in the next sections.

O.6.1 Step 1: "Initial Distance" considering operational mitigation means

The purpose of Step 1 is to define an initial distance between the equipment contributing to a hazard and the corresponding hazard. This is to be done during the causal analysis done for each hazard in SPR V2 phase as per the SRM (assurance activity P5P6-AO5-a1).

This distance has to be defined taking into account operational mitigation means that are also identified during this causal analysis. They are defined at the same level as the several components of the functional system contributing to the hazard, i.e. to:

- Procedures

- Human Performance

- Equipment

Causal analysis is usually done during the PSSA in V2. It takes into account elements from airborne and ground domains in order to allocate the risk defined at the hazard level to the several components of the functional system contributing to it.

Figure 32 below shows an overview of Step 1:

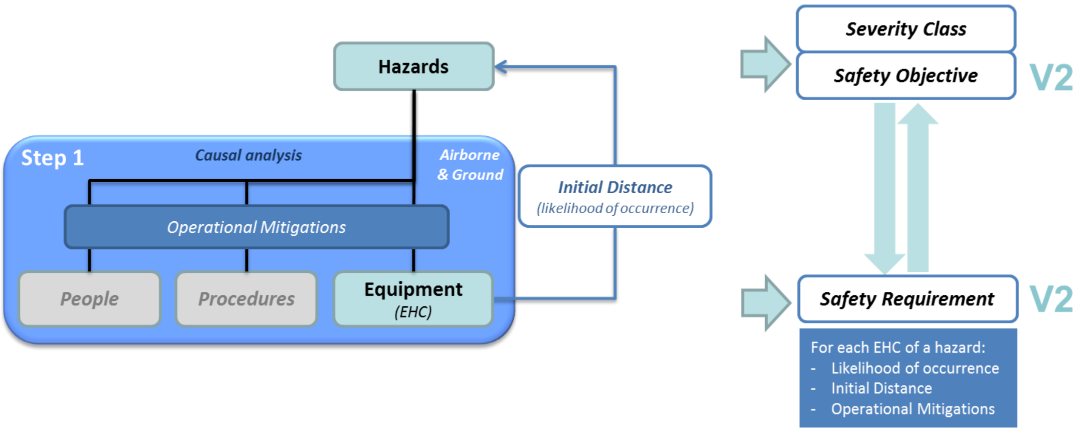


Figure 32: Distance definition: Step 1 – Initial Distance

The usual tool used for the causal analysis is the fault tree. Several approaches can be used when this technique is applied; some of them are mentioned here:

- Full quantified and dedicated fault tree based on existing data and/or expert judgement.

- Fault tree based on AIM: taking use of the quantification provided in the several AIM models.

- Hybrid fault tree (see Guidance HFT): this process allows deriving quantitative requirements for equipment considering Human interaction within the ATM functional system while addressing human error in Fault Tree not based on the quantification of the human contribution.

- Qualitative fault tree: no quantification is provided but the list of contributors to the corresponding hazard and potentially a qualitative estimation of the corresponding contribution to the associated risk.

After the causal analysis, the expected outcomes for each EHC are then:

- **The likelihood of occurrence of the identified EHC**

- **The likelihood of the occurrence of the consequence once the EHC occurs (i.e. an "initial distance") and the list of mitigations means taken into account to define this likelihood.**

- **The severity class of the corresponding hazard**

Note even if either a quantitative or a qualitative likelihood can be obtained at the end of this first step depending on the way the causal analysis has been performed, a quantitative approach is preferred.

O.6.2 Step 2: "Final distance" considered also Technical Mitigation means

The purpose is to complete the assessment of software (SW) contribution on former causal analysis through the assessment of the consequences of SW abnormal behaviour on system function(s) by taking into account properties of physical architecture. This is done in during the V3 design phase as per the SRM. Only the ground elements of the physical system are addressed here.

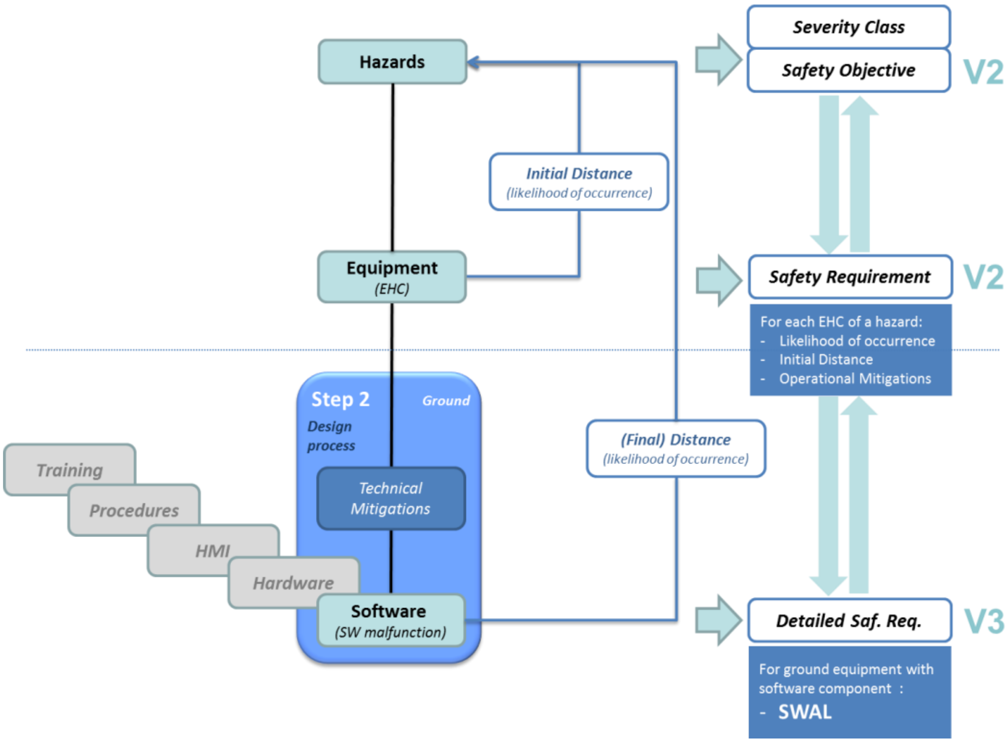


Figure 33: Distance definition: Step 2 – (Final) Distance

The steps to be following in this design process during Step 2 are mainly:

A. Define what could be a software malfunction

Failure modes to be considered (abnormal behaviour modes) are for example:

- Omission: a necessary action does not occur
- Commission: an unwanted action is performed (i.e. a perfectly functioning system would have done nothing)
- Early: an action is performed before the time (either real time, or relative to some other action) at which it is required
- Late: an action is performed after the time at which it is required
- Value: the timing of the action is correct, but the data it is performed with or upon is incorrect.

B. Define the life cycle of the technical mitigations

Architectural Mitigations should follow the life cycle of the equipment (specification, design, implementation/ coding, verification, validation)

C. Identify relevant areas of equipment architecture where technical mitigations should / could operate; and how and when these mitigations manage the occurrences of abnormal behaviour

These mitigations could be derived from the following relevant design areas:

- Architectural dependencies → Dependencies management in terms of Data coupling and Control coupling (e.g. Data Control, Time Control), data flow and control flow of the design (e.g. scheduling), redundancies (e.g. switchover mechanisms).
- Data management → how the data life cycle is managed? - origination, use, update, share, deletion (e.g. publish/ subscribe pattern)
- Communication → inside/ outside the system (e.g. communication protocols, messages management), input/output description (e.g. a data dictionary, both internally and externally throughout the software architecture)
- HW/ SW interfaces → distribution of SW components on HW platforms (e.g. avoidance of complexity)
- Resource limitations → what the strategy for managing each resource and its limitations, margins, and methods for measuring those margins is? (e.g. timing and memory).
- Safety monitoring and Alerting → how is the software monitored and the user informed of events? (e.g. event services reports, heartbeats, error return, queue error).

Architectural mitigations should be identified in the areas listed above according to their ability to manage occurrences of abnormal behaviour:

- BEFORE (Prevent issues)
- DURING (Detect issues ASAP)
- AFTER (Control the propagation of issues)
- AFTER (Recover the issues)

Examples of Fault Tolerance mechanisms related to error prevention per design areas:

- Architectural dependencies: Data Control, Time Control mechanisms; enforcing a specific sequence of events or actions to prevent unintended functions, send messages in order, etc.
- Communication: The checksum processes performed on the different IP layers, use of acknowledge messages, use of sequence numbers, etc.
- Defensive programming techniques to prevent code from executing unintended or unpredictable operations. Here are some examples (this is not an exhaustive list):
  - Avoidance of input data errors (e.g. Communication area)
  - Avoidance of non-determinism (e.g. Data management area)
  - Avoidance of complexity (e.g. Architectural dependencies and HW/ SW interfaces areas)
  - Avoidance of interface errors (e.g. HW/ SW interfaces and Communication areas)
  - Avoidance of logical errors (e.g. Data management area)

Examples of Fault Tolerance mechanisms related to detection of error occurrence per design areas:

- Resource limitations: Resources consumption monitored and limited by configuration.

- Safety Monitoring and Alerting: Event services reports to inform the users of the relevant errors of interest, Heartbeats, Error Return, and Queue Error.

Examples of Fault Tolerance mechanisms related to protection against propagation of error occurrence per design areas:

- Architectural dependencies: Partitioning (provides isolation between software components to contain and/or isolate faults).
- Architectural dependencies: Fault Containment in Redundant Elements (e.g. the Main is only synchronised with the Standby if the data has been correctly processed by the Main, Use of Dissimilar Software, Use of an independent Supervisory Function for each redundant channel).
- Data management: Transaction and Rollback Functionality, publish/subscribe pattern, demotion functionality.
- Communication: Wrappers (the OS accessing calls are hidden by using proprietary packages (wrappers) which isolate the application errors from the OS).

Examples of Fault Tolerance mechanisms related to recover (i.e. protection from an error occurrence) per design areas:

- Resource limitations: Graceful Degradation (degrading the system to a controlled "Reduced Functionality mode", a "degraded mode" (i.e. those different from "Full Operation") when a configured overload situation of a resource is reached).
- Architectural dependencies: Fault Recover with Redundant Elements (e.g. Fallback Modes in a Main/Standby or parallel configuration).
- Data management: Exception handling mechanisms (Defensive programming).
- Communication: Using reliable communication protocols protects against loss of messages.

D. Assess the independence between the mitigation and the software being analysed

The conclusion about the “Final Distance”, and then about the SWAL, is depending on the independence between software malfunctions (leading to the EHC) and appropriate mitigation means. This level of independence should be then evaluated via a Common Mode Analysis.

E. Assess efficiency of these architectural mitigation means

The efficiency of architectural mitigations means depends on their:

- Number
- Diversity
- Completeness or appropriate distribution of the technical mitigations:
  - Along the life cycle of equipment (specification, design, implementation/ coding, verification, validation)
  - Areas of equipment architecture (architectural dependencies, data management, communications, HW/ SW interfaces)
  - Coverage of abnormal behaviour modes (omission, commission, early, late, value)
  - Ability to manage occurrences of abnormal behaviour (prevent, detect, control the propagation, recover the issues)
- Independence of the software being analysed

The “initial distance” obtained from Step 1 is then refined based on the assessment of the ‘distance’ between software issues occurrence and functions abnormal behaviour (e.g. inadequate traffic picture…). This assessment is proposed to be done according to the following considerations:

- **Rule 1:** The order of magnitude could be increased by 1 if for appropriate areas (data management, communication…) and for each potential mode of software issue (omission, commission….) there is at least 1 external mitigation (to detect, control the propagation, recover the issue) and there is no identified common mode
- **Rule 2**: The order of magnitude could be increased by 2 if additional mitigations following Rule 1 could be identified with a reasonable diversity criteria

Once the previous rules are applied, the final distance is then obtained. This is the distance to be used to define the SWAL to the corresponding equipment. Tables providing the corresponding SWAL are presented in next section.

O.6.3 SWAL allocation per Severity class and Distance

Then, taking into account the considerations above in order to associate a SWAL to the software, the severity of the effect of the hazard given by the Severity Classification Schemes from SRM Guidance E.3 will be used thereby leading to dedicated tables.

Note on SWAL 5: Software whose malfunction or failure, as shown by the system safety assessment process, would cause or contribute to a failure of a system function with no effect on operational capability or human workload, so no immediate effect on safety, corresponding to a SC 5 [Least Severe] according to the EC 1035/2011 (for the ATM/CNS Ground Industry implementing the ANSP equipment). If a software component is determined to be SWAL5 and this is confirmed by the Approval Authority, no further guidance contained in ED-153 applies for the software development (the ED-153 scope is for the software safety assessment as part of the System Safety Assessment (SSA) although it contains activities for the software system development that run aligned with the FHA and PSSA in the project life cycle). It should be noted that ED-153 does not use a SWAL 5, due to current version of ED-153 does not consider the case of no immediate effect on safety. The SWAL 5 in the tables below is in order to take into account that case in compliance with the EC 1035/2011.

Note: In case the same software component leads to several different consequences the SWAL corresponding to the most severe consequence is to be used.

MAC-ER/TMA	Severity Class							
Likelihood of generating such an effect	*MAC-SC1*	*MAC-SC2a*	*MAC-SC2b*	*MAC-SC3*	*MAC-SC4a*	*MAC-SC4b*	*MAC-SC5*	*No immediate effect on safety*
Very Possible	SWAL1	SWAL3	SWAL3	SWAL3	SWAL3	SWAL4	SWAL4	SWAL5
Possible	SWAL2	SWAL3	SWAL3	SWAL3	SWAL4	SWAL4	SWAL4	SWAL5
Very Unlikely	SWAL2	SWAL3	SWAL3	SWAL4	SWAL4	SWAL4	*SWAL4*	SWAL5
Extremely Unlikely	SWAL3	SWAL3	SWAL4	SWAL4	SWAL4	*SWAL4*	*SWAL4*	SWAL5

RWY Col	Severity Class						
Likelihood of generating such an effect	*RWY-SC1*	*RWY-SC2a*	*RWY-SC2b*	*RWY-SC3*	*RWY-SC4*	*RWY-SC5*	*No immediate effect on safety*
Very Possible	SWAL1	SWAL2	SWAL2	SWAL2	SWAL3	SWAL3	SWAL5
Possible	SWAL2	SWAL2	SWAL2	SWAL3	SWAL3	SWAL3	SWAL5
Very Unlikely	SWAL2	SWAL3	SWAL3	SWAL3	SWAL3	SWAL3	SWAL5
Extremely Unlikely	SWAL3	SWAL3	SWAL3	SWAL3	SWAL4	SWAL4	SWAL5

CFIT	Severity Class				
Likelihood of generating such an effect	*CFIT-SC1*	*CFIT-SC2*	*CFIT-SC3a*	*CFIT-SC3b*	*No immediate effect on safety*
Very Possible	SWAL1	SWAL2	SWAL2	SWAL2	SWAL5
Possible	SWAL2	SWAL3	SWAL3	SWAL3	SWAL5
Very Unlikely	SWAL2	SWAL3	SWAL3	SWAL3	SWAL5
Extremely Unlikely	SWAL3	SWAL3	SWAL3	SWAL3	SWAL5

TWY Col	Severity Class					
Likelihood of generating such an effect	*TWY-SC1*	*TWY-SC2*	*TWY-SC3*	*TWY-SC4*	*TWY-SC5*	*No immediate effect on safety*
Very Possible	SWAL2	SWAL2	SWAL4	SWAL4	SWAL4	SWAL5
Possible	SWAL3	SWAL3	SWAL4	SWAL4	SWAL4	SWAL5
Very Unlikely	SWAL3	SWAL3	SWAL4	SWAL4	*SWAL4*	SWAL5
Extremely Unlikely	SWAL3	SWAL3	*SWAL4*	*SWAL4*	*SWAL4*	SWAL5

O.6.4 SWAL development process

The level of rigour of the development process for the hardware (even if out of scope of this guidance they are mentioned here for information) and software equipment components is then given by:

- For Ground software: ED-153, ED-109A or IEC 61508-Part 3.

- For Ground hardware: ED-80 or IEC 61508-Part 2.

Note 1: For the Ground Systems there is not an EC Regulation for hardware equivalent to the EC 482/2008 (for software), so the AL allocation to hardware and the compliance of the objectives according to the level of rigour specified by that AL is not enforced by the EC Regulation for the Ground Systems.

Note 2: For information, specific processes are to be applied for Airborne software (ED-12C) and for Airborne hardware (ED-80).

References

1. PPJ19.3, SESAR Safety Reference Material, Ed04.00, March 2016 (can be found on the SJU Extranet (PJ19.3 – Execution - T006 Directory))
2. International Electro technical Commission, IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems, Edition 2.0, April 2010
3. EC, EP3, D2.4.3-01, 2008, White Paper on the SESAR Safety Target, http://www.episode3.aero/public-documents
4. (EU) No 1035/2011 of 17 October 2011 laying down common requirements for the provision of air navigation services and amending Regulations (EC) No 482/2008 and (EU) No 691/2010
5. (EC) No 552/2004 of 10 March 2004 on the interoperability of the European Air Traffic Management network (the interoperability Regulation)
6. EC/EUROCONTROL, E-OCVM Version 3.0 Volume I, February 2010
7. P16.01.01, Accident Incident Models in MS Visio and Isograph Fault Tree + format, March 2013
8. P16.01.01, Validation / Verification of the SESAR Accident Incident Model (AIM), Edition 00.01.00, May 2014
9. P16.04.01, HP assessment process for projects in V1, V2 and V3, Edition 00.02.00, Dec. 2013
10. P16.06.05, HP Reference Material, May 2016
11. P16.01.02, Final Resilience Guidance Material for Safety Assessment (SRM) and Design, Edition 00.01.00, December 2013
12. ICAO Collision Risk Modelling incl. the guidance available in A Unified Framework for Collision Risk Modelling in Support of the (Doc 9689)
13. ICAO, Annex 10, Volume IV, 4th Edition, July 2007
14. P16.01.03 D02, Identification of Dynamic Risk Modelling for SESAR needs, Ed00.00.03, October 2011
15. P16.01.03, D11, Final guidelines for Dynamic Risk Modelling (DRM) application, Ed00.01.01 August 2014
16. P16.01.03 D09, Dynamic Risk Modelling (DRM) test case application and lessons learned, Ed00.01.03, September 2014
17. SESAR P16.01.04, Final Guidance Material to Execute Proof of Concept, Ed00.04.00, August 2015
18. P16.06.01, Accident Incident Models in MS Visio – AIM V10-3, December 2015.
19. P16.01.01, Validation / Verification of the Accident Incident Model (AIM), Ed03.00.00, D17, May 2014
20. P16.01.01, AIM Glossaries, available at:

    https://extranet.sesarju.eu/WP_16/Project_16.01.01/Project%20Plan/03_AIM%20Development/Gossaries/CFIT-GLOSSARY.doc

Acronyms

ADD	:	Architecture Definition Document
AIM	:	Accident Incident Model
BM	:	Barrier Model
CARA	:	Controller Action Reliability Analysis
CCF	:	Common Cause Failure
COTS	:	Commercial Off-The-Shelf
DOD	:	Detailed Operational Description
DOORS	:	Data Object Oriented Repository System
EASA	:	European Aviation Safety Agency
EATMA	:	European ATM Architecture
EP3	:	EC Funded Episode 3 project
ESARR	:	EUROCONTROL Safety Regulatory Requirements
ETA	:	Event Tree Analysis
FOD	:	Foreign Object Debris
FCRW	:	Flight Crew
FHA	:	Functional Hazard Assessment
FM	:	Functional Model
FMEA	:	Failure Modes & Effects Analysis
FTA	:	Fault Tree Analysis
FTS	:	Fast-time Simulation
HAL	:	Human Assurance Level
HFIA	:	HP Issue Analysis
HMI	:	Human-Machine Interface
HP	:	HP
HRA	:	Human Reliability Assessment
IEC	:	International Electrotechnical Commission
JU	:	Joint Undertaking

NAA	:	National Aviation Authority
NSA	:	National Supervisory Authority
OCVM	:	Operational Concept Validation Methodology
OFA	:	Operational Focus Area
OHA	:	Operations Hazard Analysis
OI	:	Operational Improvement
OSED	:	Operational Service & Environment Description
PAL	:	Procedure Assurance Level
PP	:	Primary Project
PSSA	:	Preliminary System Safety Assessment
RCS	:	Risk Classification Scheme
RTS	:	Real-Time Simulation
SAC	:	SAfety Criteria
SAM	:	Safety Assessment Methodology
SAR	:	Safety Assessment Report
SATF	:	Safety Assessment Task Force
SE	:	System Engineering
SES	:	Single European Sky
SESAR	:	Single European Sky ATM Research programme
SIL	:	Safety Integrity Level as per IEC 61508
SJU	:	SESAR JU
SPR	:	Safety & Performance Requirements
SR	:	Safety Requirements
SRM	:	Safety Reference Material
SSA	:	System Safety Assessment
STAR	:	Safety Target Achievement Roadmap
SWAL	:	SoftWare Assurance Level
TA	:	Transversal Area

TAD	:	Technical Architecture Document
TLS	:	Target Level of Safety
TS	:	Technical Specification
UML	:	Unified Modelling Language

For further reading 1 Safety Assurance in SESAR

1.1 Introduction

Although the safety assurance process follows a typical safety lifecycle, the safety assurance activities that constitute the process are driven entirely by the need for the activities to generate evidence with the right rigour to show that the subject of the safety assessment is (will be) tolerably safe, as defined by the SAfety Criteria. The rigorous logic applied by this document is as follows:

- *principles* which are the essential foundations for capturing and demonstrating satisfaction of a complete and correct set of safety requirements for SESAR before bringing it into service and maintaining it throughout its operational life
- *safety assurance objectives*, which state what has to be achieved in order to satisfy the related *principles*; and
- *safety assurance activities* which state how the safety assurance objectives will be satisfied – including the tools and techniques to be used

The definition of the *principles* was done in a workshop by PPJ19.3 starting with a top-level statement (claim) about what a safety assessment / case is trying to demonstrate in SESAR in relation to the safety of the service or System. The decomposition of the claim into lower-level arguments into *safety assurance objectives* and *safety assurance activities* then provided the essential links between the Claim and the wealth of Evidence needed to show that the Claim is valid. Rather than using a standard Goal Structured Notation (GSN) as proposed in, e.g. the EUROCONTROL Safety Case Development Manual (SCDM), the required generic safety assurance objectives and activities to generate the required evidence are presented in a tabular format in **Guidance A.1** to **A.4**. Then obviously, in order to develop specimen safety assessments for specific concepts, **Guidance C** provides the means to define the tailored set of goals for the Safety Plan to address and associated assurance activities.

Thus the safety assurance objectives are determined solely and entirely by the need to satisfy the higher-level principles. The output of the safety assurance activities is then the evidence that is needed to show in turn that each safety assurance objective has been achieved and eventually, therefore, that the principles are satisfied.

This is illustrated in **Figure 34** below:

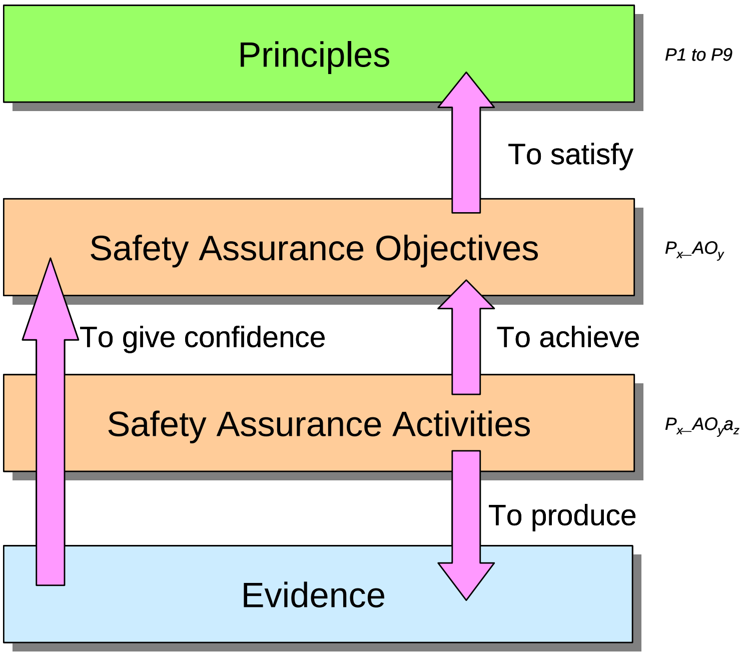


Figure 34: Safety Assurance Structure

Note: Safety Objectives and Safety Requirements developed to satisfy the SAfety Criteria (with forward and backward traceability) are part of the evidence as outputs of the Safety Assurance activities.

1.2 Generic Principles – fundamental aspects

For any changes to ATM/ANS functional systems, operational and system experts within a specific Solution shall collectively[19] conduct a risk assessment and mitigation in order to:

P1. Define the scope, boundaries and interfaces of the functional system being considered, or other affected parts of the remainder air navigation services and underlying functional systems, its intended functions as well as the environment(s) of operations in which the change is intended to operate.

P2. Derive SAfety Criteria specific for the change that are consistent with the overall criterion in terms of safety for SESAR and operational environment(s).

P3. As appropriate[20], specify OSED level safety objectives for the change which seek to maximise the positive contribution of the air navigation services to aviation safety and minimize their contribution to the risk of an accident.

P4. Show that if the safety objectives are achieved, then the SAfety Criteria will be satisfied.

P5. As appropriate (see footnote **20**), derive safety requirements for the design induced by the change in order to achieve the safety objectives.

P6. Show that, if the safety requirements are satisfied, then the safety objectives will be achieved.

P7. Show (through the construction and evaluation of pre-industrialization prototypes) that the safety requirements for the design are complete, correct and consistent.

P8. Show that the change can be safely transitioned into operation.

P9. Propose how the safety performance related to the change could be demonstrated and maintained during its operational lifecycle.

1.3 Generic Safety Assurance Objectives (about the satisfaction of principles)

1.3.1 To inform the Validation Plan

Operational and system experts within a specific Solution shall collectively provide assurance that:

P1_AO1. the properties of the particular operational environment(s) have been captured to ensure that they are a true representation of the environment to which the change to ATM/ANS functional systems will be exposed;

P1_AO2. the change brought by the Solution to, the ATM/ANS functional systems in terms of what is removed, added, modified or affected at the level of the OSED level specification, SPR-level- and/or system design has been identified;

P1_AO3. other affected parts of the ATM/ANS operations have been identified.

For Principle P2, no assurance objectives are specified[21]. Rather a detailed set of assurance activities is given in **Guidance A.1**.

[19] What collectively means in terms of roles and responsibilities is expanded in sections **1.3.1** to **1.3.4** below and **Guidance A.1** to **A.4** above.

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

[21] In any type of argument, in case of full equivalence between the argument and the sub-argument, nothing prevents you to move straight to the evidence (in this case safety assurance activities to generate the evidence).

1.3.2 To inform the OSED

The Solution shall, as appropriate (see footnote **20**), provide assurance that:

P3P4_AO1. the safety objectives resulting from the success approach define functional and performance safety properties to ensure adequate positive contribution to aviation safety, in accordance with the SAfety Criteria for the change;

P3P4_AO2. the safety objectives resulting from the failure approach define integrity safety properties to limit the negative contribution to the risk of accident/incident (and additional functional and performance properties to provide mitigation of the consequences of the system-generated hazards), in accordance with the SAfety Criteria for the change;

P3P4_AO3. all assumptions upon which safety objectives are dependent shall be captured;

P3P4_AO4. the safety objectives apply to known configuration(s)[note] of OSED level system description and its operational environment(s).

P3P4_AO5. the evidence for the safety properties of the Operational Environment(s), the SAfety Criteria and the safety objectives is trustworthy.

Note: It is essential to show that all evidence in support of the safety arguments applies to a known system configuration and one which is consistent for all phases the development 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 system throughout the lifecycle, and iterations back through previous phases whenever a change invalidates (to some degree or extent) evidence that was collected prior to that change.

1.3.3 To inform the SPR

The Solution shall, as appropriate (see footnote **20**), collectively provide assurance that at the SPR-level:

P5P6_AO1. the safety requirements resulting from the success approach define functional and performance safety properties to achieve the corresponding OSED level safety objectives

P5P6_AO2. these functional and performance safety properties will be delivered under all normal conditions[22] of the operation environment that the ATM/ANS functional system is expected to encounter in day-to-day operations;

P5P6_AO3. the degree and extent to which the elements of the SPR-level architecture can continue to deliver the functional and performance safety properties under any external abnormal conditions[23] that the ATM/ANS functional system may exceptionally encounter shall be assessed

P5P6_AO4. additional safety requirements are defined so that the risk during the period of the degraded state is shown to be within the SAfety Criteria

P5P6_AO5. the safety requirements resulting from the failure approach define the necessary safety-integrity attributes to achieve the corresponding OSED level safety objectives (and additional functional and performance properties for internal mitigation of failures);

P5P6_AO6. any non-safety functionality in the SPR-level design cannot adversely affect the safety of the SPR-level design;

P5P6_AO7. additional safety requirements are defined to ensure that any adverse emergent properties have been eliminated or mitigated sufficiently, in the SPR-level design;

P5P6_AO8. all safety requirements are achievable in a typical implementation;

P5P6_AO9. all safety requirements are verifiable;

P5P6_AO10. all assurance for the safety requirements applies to a known configuration(s) of the ATM/ANS functional system and its operational environment(s);

P5P6_AO11. the evidence for the safety requirements is trustworthy.

[22] For those conditions, the ATM/ANS functional system is expected to deliver full functionality and performance.

[23] For those conditions, the ATM/ANS functional system design is expected to be Robust against (*i.e.* work through), or at least Resilient to (*i.e.* recover easily from).

1.3.4 To inform the TS and refined version of the SPR

Given that the scoping of SESAR is limited to the pre-industrialization phase, the Solution shall, as appropriate (see footnote **20**) and as far as practicable, collectively provide assurance that:

P7_AO1. Safety requirements for the ATM/ANS at the physical level satisfy all the safety requirements derived for the SPR-level system architecture;

P7_AO2. Additional safety requirements are defined to ensure that any adverse emergent properties have been eliminated or mitigated sufficiently, in the physical system design.

P8_AO1. The physical system could be introduced without adversely affecting the safety of the ongoing air navigation services during its transition into operational service; this includes:

a. the physical system has been fully prepared for operational service;
b. the risk during transition to the functional system has been reduced as far as reasonably practicable;
c. all assurance for the safety objectives and safety requirements relates to known and consistent configuration(s) of the functional system;
d. the evidence for the transition into operation of the functional system is trustworthy

P8_AO2. Necessary coordination between PP's transitions, both individually and collectively, is achieved to demonstrate overall compliance with the overall criterion in terms of safety for SESAR.

The Solution shall collectively:

P9_AO1. identify appropriate safety measures/indicators for monitoring the safety performance of the functional system in operational service