Preliminary guidelines for advanced automation systems design and toolkit for guidelines application

Deliverable ID:	**D5.2**
Project acronym:	**HUCAN**
Grant:	**101114762**
Call:	**HORIZON-SESAR-2022-DES-ER-0**
Topic:	**HORIZON-SESAR-2022-DES-ER-01-WA1-2**
Consortium coordinator:	**Deep Blue**
Edition date:	**25 August 2025**
Edition:	**01.01**
Status:	**Official**
Classification:	**PU**

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Abstract

This document represents the deliverable D5.2 describing the SESAR solution 0446. These preliminary guidelines aim to support the harmonization between SESAR innovation and EASA certification processes, particularly for solutions involving high levels of automation. The document outlines key gaps and overlaps across selected subprocesses—such as operational concept, safety, security, ethics, and human factors—offering practical insights and methodological steps for alignment. While the guidelines offer a solution at TRL2, they provide a structured foundation for future work and are intended to facilitate more efficient, coherent, and certifiable development of AI-enabled aviation systems.

Authoring & approval

Author(s) of the document

Organisation name	Date
CIRA	01.03.2025

Reviewed by

Organisation name	Date
DBL	23.07.2025
NLR	24.06.2025
EUI	30.05.2025
EASA	03.07.2025

Approved for submission to the SESAR 3 JU by

Organisation name	Date
DBL	29.07.2025
NLR	29.07.2025
EUI	29.07.2025
CIRA	29.07.2025
DLR	29.07.2025
D-Flight	29.07.2025

Rejected by[1]

Organisation name	Date

Document history

Edition	Date	Status	Company Author	Justification
00.01	29.05.2025	Draft	CIRA	First drafting for internal review cycle

[1] Representatives of the beneficiaries involved in the project.

00.02	21.07.2025	Draft	CIRA	Second drafting for internal review cycle, including EASA review
00.03	29.07.2025	Draft	CIRA	Final drafting for internal review cycle
01.00	31.07.2025	Official	CIRA DBL	Final and quality check
01.01	25.08.2025	Official	CIRA DBL	Implementation of comments from SJU and quality check

HUCAN

HOLISTIC UNIFIED CERTIFICATION APPROACH FOR NOVEL SYSTEMS BASED ON ADVANCED AUTOMATION

HUCAN

This document is part of a project that has received funding from the SESAR 3 Joint Undertaking under grant agreement No 101114762 under European Union's Horizon Europe research and innovation programme.

Table of contents

Abstract 2
1 Executive Summary 13
2 Introduction 15
2.1 Purpose of the document 15
2.2 Scope of the document 18
2.3 Target Audience 18
2.4 Structure of the document 18
3 Development Approach 19
3.1 Background 19
3.2 Guideline Definition Approach 19
3.2.1 Step 1: Definition of Research Questions 21
3.2.2 Step 2: Identification of the sub-processes to be analysed 23
3.2.3 Step 3: Comparative Analysis of Sub-processes – Gaps and Synergies 23
3.2.4 Step 4: Development of preliminary guidelines 24
3.2.5 Step 5: Methodological Framework and Roadmap for Future Work 25
3.3 Benefits and Barriers 26
3.4 Toolkit Definition Approach 27
3.5 Guidelines Validation 28
4 Preliminary Guidelines 29
4.1 Operational Concept Subprocess 29
4.1.1 Key Differences 29
4.1.2 Overlaps 30
4.1.3 Main Findings 31
4.2 Safety Subprocess 31
4.2.1 Key Differences 31
4.2.2 Overlaps 33
4.2.3 Main Findings 34
4.3 Security Subprocess 35
4.3.1 Key Differences 35
4.3.2 Overlaps 36
4.3.3 Main Findings 38
4.4 Ethics Subprocess 38
4.4.1 Key Differences 38
4.4.2 Overlaps 40
4.4.3 Main Findings 40
4.5 Human Factors Subprocess 41

4.5.1 Key Differences 41
4.5.2 Overlaps 42
4.5.3 Main Findings 43
5 Toolkit 45
5.1 Traceability Matrix 45
5.1.1 Examples 48
5.2 Gap Analysis Checklist 52
5.3 SESAR Templates for Documentation 53
6 Conclusions and Future Work 57
6.1 Conclusions 57
6.2 Key findings 58
6.3 Next Steps 59
7 References 61
8 List of acronyms 64
Appendix A Operational Concept Subprocess 65
A.1 Purpose and Objectives 65
A.2 Target Audience 67
A.3 Scope 68
A.4 Terminology and Definitions 72
A.5 Inputs 74
A.6 Outcomes 75
A.7 Assessment Methodology 76
A.8 Performance Indicators 76
A.9 Support and Resources 76
Appendix B Safety Subprocess Analysis 78
B.1 Purpose and Objectives 78
B.2 Target Audience 84
B.3 Scope 85
B.4 Terminology and Definitions 88
B.5 Inputs 88
B.6 Outcomes 89
B.7 Assessment Methodology 90
B.8 Performance Indicators 91

B.9 Support and Resources 91
Appendix C Security Subprocess Analysis 93
C.1 Purpose and Objectives 93
C.2 Target Audience 97
C.3 Scope 98
C.4 Terminology and Definitions 101
C.5 Inputs 101
C.6 Outcomes 102
C.7 Assessment Methodology 103
C.8 Performance Indicators 104
C.9 Support and Resources 105
Appendix D Ethics Subprocess 107
D.1 Purpose and Objectives 107
D.2 Target Audience 111
D.3 Scope 112
D.4 Inputs 113
D.5 Outcomes 115
D.6 Assessment Methodology 116
D.7 Support and Resources 117
Appendix E Human-Factors Subprocess 119
E.1 Purpose and Objectives 119
E.2 Target Audience 121
E.3 Scope 123
E.4 Terminology and Definitions 124
E.5 Inputs 125
E.6 Outcomes 128
E.7 Assessment Methodology 129
E.8 Performance Indicators 130

List of figures

Figure 1: Harmonization Process Scope 17

Figure 2: Representation of deliverable purpose 17
Figure 3: End users of the document 18
Figure 4: HUCAN Preliminary Guidelines Methodological Approach 20
Figure 5: From the guidelines to the toolkit 45
Figure 6: Template of the Traceability Matrix EASA MOC vs SESAR Methodologies 46
Figure 7: Template of the Traceability Matrix EASA Evidences needs vs SESAR Deliverables 47
Figure 8: Traceability Matrix for MoC - operational concept subprocess 48
Figure 9: Traceability Matrix for MoC - security sub-process 49
Figure 10: Traceability Matrix for Objectives - operational concept sub-process 50
Figure 11: Traceability Matrix for Objectives - security sub-process 51
Figure 12: SESAR Solution XXX SPR-INTEROP/OSED template - Table of Contents 54
Figure 13: DES HE SESAR Solution XXX TS/IRS template - Table of Contents 55
Figure 14. DES HE concept outline template for TRL1 - Table of Contents 56
Figure 15: Next steps – Include as end-users the developers 59
Figure 16: HUCAN maturity evolution 59
Figure 17. Risk-based levelling of objectives - Operational Concept Objectives 66
Figure 18. Safety Requirements and the Solution SPR-INTEROP/OSED and TS/IRS 81
Figure 19. Activities to perform a Safety Analysis 87
Figure 20. Threat scope to be used as a reference for the information security risk assessment of AI/ML constituents according to EASA [1]. 99
Figure 21. Threat scope and defensive techniques suggested by EASA for the ATM/ANS use case [1] [8] 99
Figure 22. SecRAM process [6]. 100
Figure 23. Mapping of 7 gears to the AI trustworthiness building blocks 107
Figure 24. The 5-layer Model of Ethics by Design 109
Figure 25. The generic model for AI Development 110
Figure 26. Steps of the HP assessment process 123

Figure 27. Levels of automation - taxonomy and correspondence to EASA AI levels..... 125

List of tables

Table 1. General key differences for operational concept subprocess..... 30
Table 2. General overlaps for operational concept subprocess..... 31
Table 3. General key differences for safety subprocess. 33
Table 4. General overlaps for safety subprocess. 34
Table 5. General key differences for security subprocess..... 36
Table 6. General overlaps for security subprocess. 38
Table 7. General key differences for ethics subprocess..... 40
Table 8. General overlaps for ethics subprocess..... 40
Table 9. General key differences for human factor subprocess. 42
Table 10. General overlaps for human factor subprocess. 43
Table 11. List of acronyms..... 64
Table 12. Key Differences for Operational Concept subprocess – Target Audience 68
Table 13. Overlaps for Operational Concept subprocess – Target Audience 68
Table 14. Key differences for Operational Concept subprocess – Scope..... 72
Table 15. Overlaps for Operational Concept subprocess – Scope. 72
Table 16. Key differences for Operational Concept subprocess – Terminology and definitions..... 73
Table 17. Overlaps for Operational Concept subprocess – Terminology and definitions. 74
Table 18. Overlaps for Operational Concept subprocess – Inputs..... 75
Table 19. Key differences for Operational Concept subprocess – Outcomes..... 76
Table 20. Comparison between 'Initial' and 'Continuous' safety assessments in Aviation domains.... 80
Table 21. Key Differences for Safety Assessment subprocess - Purpose and Objectives 84
Table 22. Overlaps for Safety Assessment – Purpose and Objectives 84
Table 23. Key differences for safety subprocess – Target Audience..... 85
Table 24. Overlaps for safety subprocess – Target Audience 85

Table 25. Key differences for Safety subprocess – Scope 87
Table 26. Overlaps for Safety subprocess – Scope 88
Table 27. Key differences for Safety subprocess – Terminology 88
Table 28. Key differences for Safety subprocess – Inputs 89
Table 29. Key differences for Safety subprocess – Outcomes 90
Table 30. Overlaps for Safety subprocess – Outcomes 90
Table 31. Key differences for Safety subprocess – Assessment Methodology 90
Table 32. Key differences for Safety subprocess – Performance Indicators 91
Table 33. Overlaps for Safety subprocess – Performance Indicators 91
Table 34. Key differences for Safety subprocess – Support and Resources 92
Table 35. SecRAM security risk levels [6]. 94
Table 36. SESAR security requirements vs TRL 95
Table 37. Key differences for security subprocess – purpose and objectives 96
Table 38. Overlaps for security subprocess – purpose and objectives. 97
Table 39. Key differences for security subprocess – target audience 98
Table 40. Overlaps for security subprocess – target audience. 98
Table 41. Key differences for security subprocess – scope 101
Table 42. Overlaps for security subprocess – scope. 101
Table 43. Overlaps for security subprocess – terminology and definitions. 101
Table 44. Key differences for security subprocess – inputs. 102
Table 45. Key differences for security subprocess – outcomes. 103
Table 46. Overlaps for security subprocess – outcomes. 103
Table 47. Overlaps for security subprocess – assessment methods. 104
Table 48. Key differences for security subprocess – performance indicators. 105
Table 49. Key differences for security subprocess – support and resources. 106
Table 50. Key differences for ethics subprocess – goals 110

Table 51. Overlaps for security subprocess – goals 110
Table 52. Key differences for ethics subprocess – boundaries 111
Table 53. Overlaps for ethics subprocess – boundaries 111
Table 54. Key differences for ethics subprocess – activities and steps 113
Table 55. Key differences for ethics subprocess – inputs 115
Table 56. Overlaps for ethics subprocess – inputs 115
Table 57. Key differences for ethics subprocess – outputs 116
Table 58. Key differences for ethics subprocess – methods 117
Table 59. Overlaps for ethics subprocess – methods 117
Table 60. Key differences for HF subprocess - purpose and objectives 121
Table 61. Overlaps for HF subprocess - purpose and objectives 121
Table 62. Key differences for HF subprocess – target audience 122
Table 63. Overlaps for HF subprocess – target audience 122
Table 64. Key differences for HF subprocess - scope 124
Table 65. Overlaps for HF subprocess – scope 124
Table 66. Steps of the HP assessment process 127
Table 67. Key differences for HF subprocess – inputs 127
Table 68. Overlaps for HF subprocess – inputs 128
Table 69. Outcomes of the HP process 129
Table 70. Key differences for HF subprocess – outcomes 129
Table 71. Overlaps for HF subprocess – outcomes 129

1 Executive Summary

This document aims to establish preliminary guidelines to harmonize SESAR innovation processes with EASA certification processes, particularly for solutions that incorporate high levels of automation and Artificial Intelligence (AI)-based technologies in the Air Traffic Management (ATM) domain. The main objective of the Guidelines is to facilitate the development of aviation systems in a way that is more efficient, consistent, and certifiable, by encouraging the early integration of certification principles into the design phase. These guidelines represent an initial, structured version that will be refined, validated, and expanded over time.

The aviation sector is undergoing a profound transformation driven by advanced automation and AI-based technologies. While traditional automated systems follow well-established certification processes, highly automated and AI-powered systems introduce new technical and regulatory challenges. These include non-deterministic behavior, lack of explainability, and strong dependence on training data, which challenge traditional verification and validation methods. It is essential to maintain continuous situational awareness and avoid over-reliance on automated systems, considering human factors, transparency, trust calibration, and fallback procedures.

The document acknowledges that SESAR and EASA, while both key players in this advancement, have distinct scopes and responsibilities. SESAR focuses on research, development, and innovation, ensuring the dissemination of innovation while maintaining high operational safety standards. However, the ultimate responsibility for safety lies with EASA, which oversees regulation and certification. A thorough comparative analysis of their subprocesses is fundamental to identify commonalities and differences, such as particularly gaps, overlaps, and complementarities.

Based on the preliminary guidelines, a practical toolkit has been developed to support harmonization activities. This includes checklists for gap analysis, overlap mapping, a traceability matrix, documentation templates, and recommendation forms. This approach aims to improve transparency, consistency, and mutual understanding between innovation and regulatory compliance processes. Next steps in the work will include refining the analysis of the identified subprocesses, extending the analysis to all relevant subprocesses, identifying and prioritizing the actions needed to implement harmonization, and extending the guidelines and toolkit to solution developers. It will be crucial to analyze the impact of the identified gaps and define targeted actions, as well as explore how overlaps can be effectively leveraged to maximize efficiency gains.

The document is designed to build a shared understanding, identify gaps and synergies, and formulate preliminary guidelines for harmonization. To achieve this, a methodological flow is proposed, consisting of five steps: definition of key questions; selection of specific subprocesses for detailed analysis; use of a standardized checklist to compare each subprocess; development of structured recommendations on where alignment is needed and which activities or evidence can be shared; and definition of a framework for validating and refining the guidelines, extending them to other subprocesses or domains, and engaging stakeholders.

Harmonizing these processes leads to significant strategic and operational benefits, including:

- Reduction of duplicated activities.

- Faster time-to-market.
- Improved resource efficiency.
- Enhanced traceability and consistency.
- Strengthened interdisciplinary collaboration.
- More predictable and cost-effective certification.
- Early identification of gaps and risks.

Finally, a detailed analysis of differences and overlaps in various subprocesses is presented, including: Operational Concept; Safety; Security; Ethics; Human Factor.

The development of the guidelines and of the toolkit have considered the feedbacks of external experts, who are not part of the HUCAN Consortium.

2 Introduction

2.1 Purpose of the document

The aviation sector is undergoing a deep transformation driven by increasingly sophisticated automation and emerging AI-based technologies. While traditional automated systems follow well-defined certification processes, highly automated and AI-enhanced systems introduce new technical and regulatory challenges. The increasing integration of high-level automation introduces significant challenges, especially considering the potential overreliance on automated systems and the essential requirement to preserve continuous situational awareness. These factors not only affect operational safety but also complicate certification, which must now consider human factors, transparency, trust calibration, and fall-back procedures.

Furthermore, the integration of Artificial Intelligence—especially machine learning—introduces additional certification barriers due to its non-deterministic behaviour, lack of explainability, and strong dependence on training data. These characteristics challenge traditional verification and validation methods, requiring new assurance approaches that can demonstrate safety, predictability, and accountability in AI-driven decision-making processes.

As the boundary between human and automated roles becomes less distinct, regulatory bodies are adapting frameworks to ensure that future systems are not only technically robust but also usable, understandable, and controllable by humans in all conditions.

This project positions itself within the broader evolving landscape of certification for highly automated aviation systems, with the ambition to contribute to the definition of a holistic certification-aware approach to advanced automation design. The focus is on the Air Traffic Management (ATM) domain, addressing two main perspectives:

- ✓ **Novel holistic approach for certification-aware design:** Development of a novel holistic approach for certification-aware design of intelligent automation and AI-based solutions in aviation that focuses on two main pillars: the EASA concept paper, and the operational needs emerging from the development of AI-based solutions.
- ✓ **Harmonizing the SESAR current development process and EASA concept paper:** Leveraging existing development efforts with the main goal of maximizing synergies with the ongoing work under SESAR, aiming to ensure that new concepts, systems, and operational solutions developed are not only elements of the Single European Sky concept, architecture and deployment, but can also be aligned also with certification objectives.

This approach aims to **promote the early integration of certification principles into system design**, in order to improve the overall efficiency of the process.

The above cited two perspectives are reflected in the project by the WPs- the first one is developed through WP3 and by WP4, the last one is developed by WP5.

This document specifically addresses the **second perspective** described above: the opportunity to **leverage and align ongoing development activities** within the SESAR framework with the needs and constraints of the **certification process**. The title *"Preliminary Guidelines"* reflects the intent to lay the

foundational principles for the **harmonization between SESAR system development and compliance pathways** when high automation is addressed (see Figure 1 and Figure 2).

To these purposes, it is worth of highlighting that:

- The SESAR framework and the EASA concept paper **have distinct scopes and involve different responsibilities.** SESAR is tasked with ensuring the deployment of innovation while maintaining high standards of operational safety. However, the ultimate responsibility for safety lies with EASA
- **SESAR** primarily focuses on **ground-based systems and methodologies**, which means that many of its outputs are mainly tailored to **ground equipment** and operational environments. In contrast, the **EASA Concept Paper (issues 02)** appears to be oriented towards both **ground** and **airborne systems**, with a stronger emphasis on the **aircraft perspective** and the associated certification aspects.
- The EASA concept paper is specifically focused on automation and AI-based systems, while SESAR is not.

Furthermore, the key concept derived regarding the guidelines and the harmonization of the processes are summarized considering a specific toolkit.

First, it is worth noting that the harmonization process will take into account the overall SESAR project life cycle on one hand and the **EASA concept paper on the other hand[2].**

Second, HUCAN is a low-TRL project that lays the groundwork for further technological maturation. In this context, the guidelines presented in this document should be regarded as preliminary, as they focus on selected subprocesses within the broader processes of interest. Moreover, the analysis of these subprocesses can be further enriched and expanded in future phases, for example, by incorporating broader validation with stakeholders.

Accordingly, in this preliminary analysis phase, the following subprocesses have been considered: **operational concept definition, safety, security, human factors, and ethics**.

[2] From now on in the document when EASA work is mentioned refers to EASA concept paper as declared in the purpose od the document

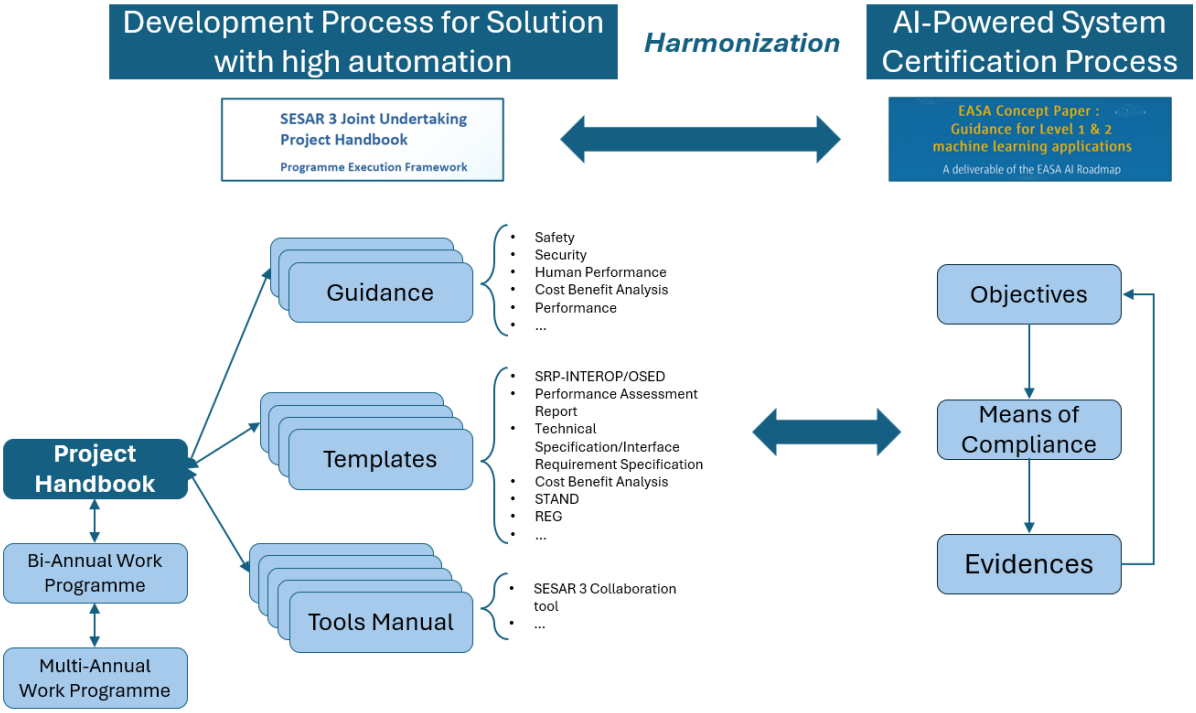

Figure 1: Harmonization Process Scope

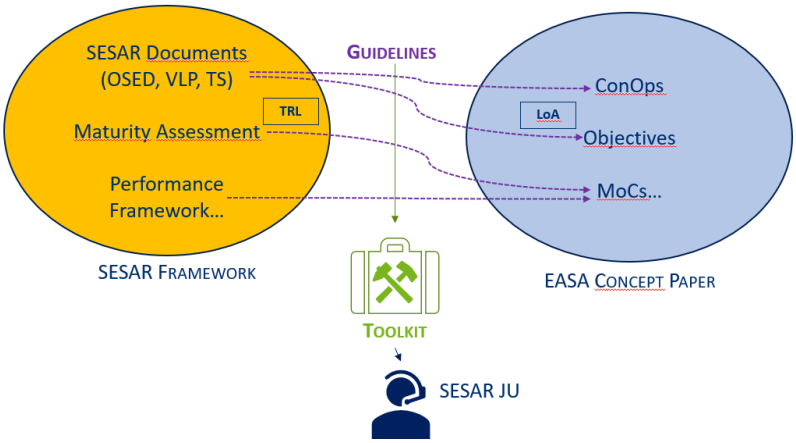

Figure 2: Representation of deliverable purpose

Accordingly, the preliminary guidelines aim to provide a first analysis.

The preliminary guidelines have been validated with input from a selected group of relevant stakeholders, including a SESAR solution focused on high automation—identified by the HUCAN team. Stakeholders feedback has been incorporated into the guidelines report, contributing to the refinement of the guidelines and the development of the supporting toolkit.

2.2 Scope of the document

This document represents the deliverable D5.2. “Preliminary guidelines for advanced automation systems design and toolkit for guidelines application” developed within WP5.

The document contributes to the SESAR Solution 0446 “Preliminary Guidelines to design ATM-related systems based on higher levels of automation”.

2.3 Target Audience

The target audience of this document includes end users who can leverage it for further analysis and insights. These are SESAR Joint Undertaking and EASA, i.e., the owners of the processes compared. In this context, the guidelines aim to provide key highlights and a structured approach to comparison, which can support subsequent in-depth assessments and decision-making. SESAR could benefit from areas of overlap between both approaches and implement possible adjustments in the development workflows, and generate supporting evidence, ultimately helping to reduce existing gaps.

Figure 3: End users of the document

Secondly, the document also targets all stakeholders involved in both ATM development and certification processes to get their feedback.

2.4 Structure of the document

Following an introductory section outlining the main objectives of the document and its relevance to the project, the document presents the approach used to derive the guidelines. Section 2 describes this approach in detail, outlining the logical flow and the associated steps. Section 3 presents the preliminary guidelines, which reflect the main findings of the analysis. A more detailed analysis of the subprocesses is provided in the Appendixes. Section 4 summarizes the key findings and identifies actionable elements to support the development of a toolkit for decision-makers. Finally, Section 5 presents the main conclusions and sets the basis for future work.

3 Development Approach

3.1 Background

The rapid evolution of advanced-automation digital technologies within the aviation domain requires a harmonized approach to the development, assessment, and certification of new solutions. Within Europe, two key actors drive this advancement: SESAR, focused on research, development, and innovation; and EASA, responsible for regulation and certification.

Both SESAR and EASA have developed subprocess frameworks that address critical dimensions such as operational concept, safety, security, ethics, and human factors, which are all essential for the successful integration of AI-based technologies in ATM and aviation systems. However, their differing remits imply that SESAR's subprocesses primarily support exploratory research, validation, and operational impact assessment, while EASA's subprocesses are oriented towards regulatory compliance and certification.

Recognizing the complexity of the evolving AI-based solutions, a comprehensive comparative analysis of SESAR and EASA subprocesses is advisable to map commonalities and differences across the main thematic areas—safety, security, ethics, operational concept, and human factors—with a particular focus on identifying gaps, overlaps, and complementarities.

Such analysis serves as the foundational step for defining an integrated set of guidelines to be used as a reference for setting up a future certification approach tailored specifically for SESAR-developed AI-based solutions. By bridging SESAR's R&D methodologies and EASA's compliance-driven frameworks, these guidelines aim to support a coherent and streamlined design of automated systems towards their eventual certification, considering also evidences available at low TRL stages. This may ensure that innovative AI technologies can be already assessed at the earliest design stages, for effectively and efficiently meeting regulatory requirements and operational needs.

Ultimately, the comparative analysis is instrumental in fostering collaboration between research and regulatory domains, enabling the development of AI-enabled aviation systems that are not only technologically advanced but also safe, secure, ethical, and human-centric.

3.2 Guideline Definition Approach

The analysis to harmonize the processes considers the overall SESAR project life cycle on one hand and the **EASA concept paper**.

The harmonization of development and certification processes represents a strategic objective for organizations aiming to bring innovative solutions to market more efficiently. In this context, the work undertaken in the project aims to explore and structure a methodology that enables this harmonization, starting from a low Technology Readiness Level (TRL) perspective.

The approach is designed with a dual perspective:

- ✓ On one hand, to provide a practical example of gap analysis that can serve as a basis for initiating targeted harmonization actions.
- ✓ On the other hand, to identify a repeatable methodological framework that offers a foundation for future work, supporting the evolution of the current solution towards higher levels of maturity.

The approach is based on a structured, step-by-step analysis (Figure 4), designed to progressively build a shared understanding of the processes, identify critical gaps and synergies, and ultimately support the formulation of preliminary harmonization guidelines. These guidelines are intended as a foundation for further refinement and practical application in future, higher-TRL phases.

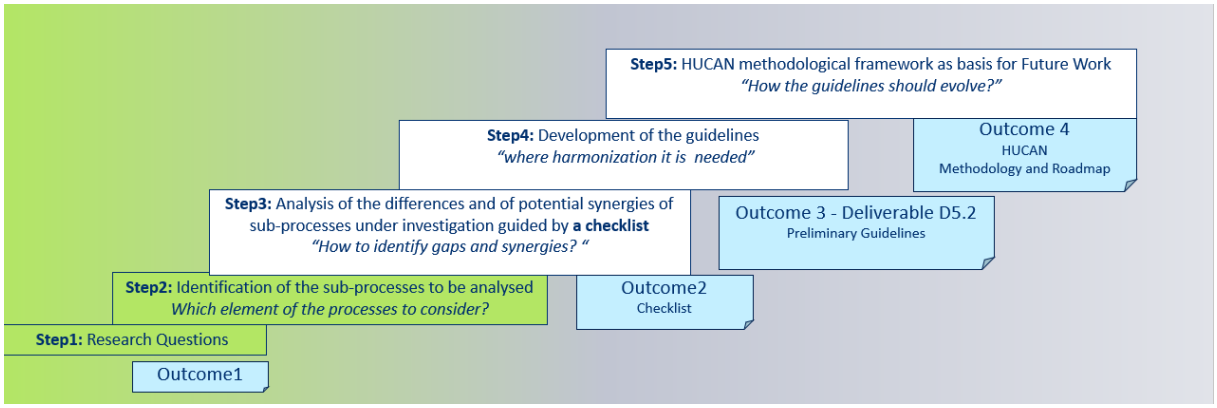

Figure 4: HUCAN Preliminary Guidelines Methodological Approach

The following steps summarize the methodological workflow adopted to reach this goal:

❖ **Step 1: Definition of Research Questions**
"Framing the scope"
Outcome 1 – Key Research Questions
The process begins with the formulation of key research questions that guide the overall investigation. These questions define the scope, identify the main challenges of harmonization, and clarify the added value of aligning development and certification workflows from the earliest design phases.

❖ **Step 2: Identification of the Sub-processes to Be Analysed**
"Which elements of the processes should be considered?"
At this stage, specific sub-processes from the broader development and certification frameworks are selected for detailed analysis. These include areas such as:

- Operational concept definition
- Safety
- Security
- Human factors
- Ethics

This selection provides a focused yet representative basis for exploring process interactions and harmonization opportunities.

❖ **Step 3: Comparative Analysis of Sub-processes – Gaps and Synergies**

"How can we identify gaps and synergies?"

Outcome 2 – Checklist for Gap & Synergy Identification

A dedicated checklist is defined to be applied and to guide the comparative analysis of each sub-process. This checklist helps identify differences in objectives, documentation, stakeholders, and timing between the development and certification paths. The analysis aims at highlighting:

- Redundancies and duplications
- Points of misalignment
- Potential synergies and shared activities

The result is a detailed analysis of the sub-processes.

❖ **Step 4: Development of Preliminary Guidelines**

Outcome 3 – Deliverable D5.2: Preliminary Guidelines

"Where is harmonization needed?"

Based on the findings from Step 3, a set of preliminary guidelines is developed. These guidelines provide structured recommendations on:

- Where an alignment would be needed
- Which activities or evidence can be shared

The result is a preliminary understanding of where harmonization could be considered in the targeted sub-processes. The guidelines are captured in Deliverable D5.2 and represent a first, foundational version, to be validated and enhanced in future work.

Subsequently, a toolkit is developed to distil the guidelines into more practical and actionable information.

❖ **Step 5: Methodological Framework and Roadmap for Future Work**

"How should the guidelines evolve?"

Outcome 4 – Methodology and Roadmap

The final step outlines a methodological framework and roadmap to guide future work. This includes:

- Assessing the impact of the gaps and overlaps, and defining actions to leverage them
- Defining next steps for validating and refining the guidelines
- Proposing extensions to additional sub-processes or domains
- Engaging stakeholders to ensure relevance and adoption
- Linking the approach to TRL advancement and time-to-market optimization

The roadmap is a forward-looking means to support continued alignment between innovation and regulation, reducing effort duplication and enabling more efficient product deployment.

3.2.1 Step 1: Definition of Research Questions

The research questions aim to drive the exploration of the harmonization of SESAR's development lifecycle (including the E-OCVM maturity gates) and EASA's certification processes, in the context of

advanced automation systems in Air Traffic Management (ATM). The objective is to identify opportunities to streamline development and certification activities, improve efficiency, and support effective safety and performance assurance.

The identified research questions have guided the selection of subprocesses to be analysed and the design of the checklist used for their analysis.

Here below the identified research questions:

Alignment of Development and Certification Processes

- Are there any interaction and correlation between SESAR's technology development timelines and EASA's certification timelines?
- What synergies exist between the SESAR pipeline (E-OCVM) and an incremental certification methodology for advanced automation in ATM?
- What benefits can be gained by aligning the SESAR development process with the EASA certification approach (e.g., increased efficiency, reduced time-to-market)?
- Are there any misalignments or gaps between SESAR innovation cycles and EASA certification cycles that need to be addressed?
- What are the key inputs, outputs, and intermediate stages for each process, and how do they relate to each other?

Integration and Calibration of Objectives and Methodologies

- Does it make sense to calibrate EASA's objectives with respect to different TRLs within the E-OCVM maturity gates?
- How should the different categories of EASA objectives be integrated into the E-OCVM process, and at which stages of the software lifecycle should they be addressed?
- Is there a need to harmonize the SESAR taxonomy with the terminology used in the EASA concept paper?
- How do the documentary evidence requirements for SESAR solutions compare to those outlined in the EASA concept paper?

Safety Assurance and Compliance

- What safety assurance processes are implemented for high automation systems within both SESAR and EASA frameworks?

Performance Measurement and Metrics

- Is there any relation between performance in the EASA concept paper and SESAR's High-Performing (HP) KPIs for advanced automation?
- How can man-machine teaming metrics be integrated into the SESAR performance framework for advanced automation?
- How can ethics-related metrics be incorporated into the SESAR performance framework for advanced automation?

Validation and Testing

- What data, simulations, and test procedures are used to validate high automation systems in both SESAR and EASA contexts?
- Is there any possibility to standardize validation?

3.2.2 Step 2: Identification of the sub-processes to be analysed

In any effort to harmonize two complex processes, it is crucial to move beyond high-level alignment and focus on identifying and comparing low-level, concrete subprocesses or components. This granular approach provides several key advantages:

- **Clarity of Scope and Meaning:** High-level processes often use similar terminology to describe different concepts or activities. By analysing low-level elements, one can disambiguate these terms and understand their actual implementation in each context.
- **Operational Relevance:** Harmonization becomes effective only when it addresses the operational reality of those implementing the processes. Low-level subprocesses represent the actual tasks, inputs, outputs, and methods that practitioners deal with daily.
- **Identification of Reusable Evidence and Artifacts:** At the detailed level, it is possible to identify where documents, models, reports, or tests produced in one process can serve as valid inputs or evidence in the other. This directly supports efficiency and reduces duplication of effort.
- **Targeted Gap Analysis:** Low-level comparison allows for a more precise identification of gaps and misalignments. This enables more focused and actionable harmonization strategies, rather than broad or generic recommendations.
- **Foundation for Automation and Tool Support:** Harmonized low-level elements can become the basis for developing shared tools, templates, and digital workflows—supporting long-term scalability and integration.

In summary, focusing on comparable low-level elements enables a more accurate, practical, and implementable harmonization between processes. It provides the necessary detail to translate alignment principles into tangible actions and measurable benefits.

3.2.3 Step 3: Comparative Analysis of Sub-processes – Gaps and Synergies

This checklist has been designed to support a structured comparison between EASA and SESAR subprocesses as part of the broader effort to explore harmonization opportunities. The objective is to identify overlaps that may facilitate efficiency and evidence reuse, as well as gaps that may require specific alignment or mitigation strategies.

The use of a standardized checklist offers several key advantages:

- It ensures consistency across the analysis of different subprocesses.
- It facilitates comparability by framing the same questions across both EASA and SESAR contexts.
- It supports traceability by documenting rationale, assumptions, and observed gaps or alignments.

- It helps identify quick wins for harmonization (e.g. overlapping documentation or shared metrics) and priorities for addressing misalignments.
- It enhances collaboration among stakeholders from different domains, providing a common language and structure for joint assessment.

By analysing each subprocess across a set of common dimensions (e.g., purpose, scope, inputs, assessment), stakeholders can better understand where synergies exist and where deviations may hinder harmonized development and certification. The checklist is intended for use in the early maturity stages to address preliminary guidelines and can serve as a reference for future refinement.

The questions have been identified based on the following main topics, which serve as the foundation for comparing the two processes.

- ✓ **Dimension1. Purpose and Objectives**
  It addresses the overall aim of the sub-process under analysis and the specific goals it is intended to achieve.
- ✓ **Dimension 2. Target Audience**
  Identifies the primary users or stakeholders for whom the sub-process is designed.
- ✓ **Dimension 3. Scope**
  Addresses the boundaries of the sub-process, including what is covered and what is excluded.
- ✓ **Dimension 4. Terminology and Definitions**
  It addresses the definitions of key terms and concepts of the sub- process to ensure a common understanding.
- ✓ **Dimension 5. Inputs**
  Lists the required data, documents, or conditions needed to effectively start/execute the sub-process
- ✓ **Dimension 6. Outcomes**
  Specifies the expected results or deliverables once the sub-process has been completed
- ✓ **Dimension 7. Assessment Methodology**
  Outlines the approach or criteria used to execute the sub-process or a specific part of it
- ✓ **Dimension 8. Performance Indicators**
  Identifies measurable indicators that can serve as the evidences of the sub-process
- ✓ **Dimension 9. Support and Resources**
  Identifies the tools, personnel, guidance, or funding required to implement the sub-process effectively.

The checklist itself represents a specific tool to be applied for the comparison analysis of each sub-process, thus it is part of the toolkit described in section 5.1.

3.2.4 Step 4: Development of preliminary guidelines

Once the gaps and the overlaps have been identified – a detailed analysis can lead to the guidelines reporting the key highlights that end users could consider triggering harmonization and take the proper actions.

Gap analysis involves identifying and understanding the differences between the current state of each sub-process and the desired level of alignment. It starts with a clear understanding of how each subprocess is structured, what requirements and outputs are expected, and where these may diverge. The purpose of gap analysis is to focus harmonization efforts on the areas that will yield the greatest benefit, avoiding broad or generic recommendations and ensuring that improvements are practical and actionable. By carefully examining these discrepancies—whether they concern methodologies, documentation, timing, or compliance criteria—organizations can assess how these gaps impact efficiency, risk introducing delays, or cause redundant efforts. This understanding then guides the development of targeted harmonization actions, such as aligning methods, sharing evidence, or adapting workflows to bridge these gaps.

At this level of maturity of the project, where this document represents the solution at TRL2, the gap analysis aims at identifying key differences laying foundation for the future work and progressing in maturity completing the analysis with the impact of the gaps and the possible actions and the prioritization.

Overlap analysis focuses on identifying areas where the two processes already share common elements, such as objectives, deliverables, methods, or validation steps. It involves mapping these shared components to understand how they can be leveraged to reduce duplication of efforts. By recognizing these overlaps, organizations can explore opportunities to reuse documentation, models, or test results, which ultimately streamlines both development and certification activities.

3.2.5 Step 5: Methodological Framework and Roadmap for Future Work

Finally, it is necessary to provide a strategic vision for the progression and refinement of the harmonization between SESAR innovation processes and EASA certification processes. In particular, the roadmap for future work should address the following key directions:

- **Assessment of Gap Impacts and Leverage of Overlaps**: A deeper analysis should be conducted to identify and quantify the impact of existing gaps between the processes. At the same time, opportunities should be explored to effectively leverage the identified areas of overlap in order to maximise efficiency gains. Not all gaps may need to be bridged, nor would it always be appropriate to do so, considering the differing purposes of SESAR and EASA.

- **Definition of Next Steps for Validation and Refinement**: The preliminary guidelines, which currently correspond to TRL2, require continuous validation and refinement. This includes the need to involve end-users—namely solution developers—in the maturation process.

- **Extension to Additional Subprocesses or Domains**: The initial analysis has focused on specific subprocesses such as the operational concept, safety, security, ethics, and human factors. The next step is to extend this analysis to all relevant SESAR subprocesses and to address the new objectives outlined in future updates of the EASA Concept Paper.

- **Stakeholder Engagement**: Actively involving stakeholders is essential to ensure the relevance and adoption of the guidelines. This includes collecting feedback from experts outside the HUCAN consortium.

- **Link to TRL Progression and Time-to-Market Optimisation**: The roadmap aims to tightly integrate the harmonisation approach with the progression of Technology Readiness Levels (TRL), facilitating a smoother transition of new technologies towards commercialisation. This also includes a comparison between the SESAR maturity assessment process and EASA's conformity verification expectations.

Step 5 can be seen as the evolution plan that transforms the initial findings into a dynamic strategy for the future. It represents a commitment to building an increasingly robust and integrated bridge between technological innovation and regulatory compliance, ensuring that advanced aviation solutions are not only cutting-edge but also inherently safe and certifiable.

3.3 Benefits and Barriers

The ultimate goal of the ongoing work is to enable the harmonization of two key processes that organizations must manage when bringing a product to market: development and certification.

In general, harmonizing processes lead to increased efficiency and better resource optimization by avoiding unnecessary time and effort waste. However, when the two processes are directly linked to the time-to-market of a product, the need for harmonization becomes even more critical. In this context, harmonization is not just a matter of improving internal workflows—it becomes a key enabler for accelerating deployment, ensuring alignment between technical progress and regulatory compliance, and ultimately supporting the competitiveness and readiness of the product

Harmonizing the development and certification processes within an organization would bring a range of strategic and operational benefits. These benefits not only would support a smoother and faster path to market but also contribute to improved quality, compliance, and cost-efficiency.

Some of the key advantages could be:

- ✓ **Reduction of duplicated activities**
  By aligning evidence generation and documentation requirements, teams can avoid performing the same tasks twice.
  → *Indicator: % reduction in duplicated validation or verification tasks*

- ✓ **Faster time-to-market**
  Streamlining interactions between development and certification allows early identification of regulatory constraints and enables parallel planning.
  → *Indicator: Time from final design freeze to certification approval / operational deployment*

- ✓ **Improved resource efficiency**
  Shared use of simulation, testing environments, and data across both processes leads to more efficient use of personnel and infrastructure.
  → *Indicator: Staff hours saved per project / % reuse of test data or reports*

- ✓ **Better traceability and consistency**
  Ensuring alignment from requirements definition to certification evidence improves traceability and reduces the risk of non-compliance.

→ *Indicator: Effort of reworks raised during certification process*

- ✓ **Enhanced collaboration across domains**
  Interdisciplinary collaboration is fostered earlier in the lifecycle, especially across engineering, safety, security, human factors, and regulatory teams.
  → *Indicator: Number of cross-domain reviews completed during development*

- ✓ **More predictable and cost-effective certification**
  By anticipating certification needs, organizations can reduce last-minute redesigns and unplanned iterations.
  → *Indicator: % reduction in certification-related rework costs*

- ✓ **Early identification of gaps and risks**
  Harmonization allows earlier detection of potential gaps between what is being developed and what can be certified or accepted by regulators.
  → *Indicator: Number of risks mitigated before entering formal certification phase*

While it is true that SESAR deliverables are often oriented toward R&D and operational deployment, whereas EASA's certification process focuses on safety, reliability, and compliance, some potential barriers could be the followings:

- ✓ Different timelines: SESAR operates on R&D programme cycles, while certification progresses according to regulatory readiness and industry uptake.

- ✓ Evolving regulatory framework: EASA's approach to AI (and related certification baselines) is still under development, which may create uncertainty for how SESAR results can be used as evidence.

- ✓ Resource and effort constraints: High effort may be required to adapt SESAR outputs into certification-ready documentation.

Furthermore, EASA cannot provide support to the development phase of a SESAR solution prior to the official start of the certification process. However, certain coordination points between the two processes could be planned. To enable this, a clear and structured approach should be established, aiming to minimise potential ambiguities that may arise when applying certification objectives.

3.4 Toolkit Definition Approach

Chapter 3.2 outlined the methodological approach adopted to formulate the preliminary guidelines, which are intended to support the harmonisation between SESAR innovation processes and EASA certification processes, particularly for solutions involving high levels of automation.

To translate these preliminary guidelines from conceptual elements into operational tools, a practical toolkit has been designed and developed. This section introduces the approach used to define the toolkit, explaining its rationale, structure, and the methodology for its application.

The development of the toolkit stems from the fundamental need to make the preliminary guidelines truly actionable and to maximise their practical impact. The primary objective is to actively support the harmonisation efforts between SESAR innovation development processes and EASA certification requirements. Specifically, the toolkit aims to:

- **Enhance transparency and consistency**, by providing a common language and clear steps to approach the harmonization, reducing ambiguity and facilitating understanding.
- **Provide concrete support**, by equipping end-users with practical tools to integrate certification principles from the early design stages.

3.5 Guidelines Validation

The guidelines presented, although structured and positioned as an initial contribution at TRL2, are by nature preliminary. Validation is a crucial step to refine, confirm, and expand them over time.

The primary objective of the validation process is to ensure that the guidelines and the associated toolkit are practical, robust, and fully applicable to support the harmonisation between SESAR innovation processes and EASA certification processes. This harmonisation is a strategic objective that enables the benefits outlined in Chapter 3.3.

The validation activities were carried out in parallel and the outcomes are summarized in the deliverable D5.1 already submitted and approved. Accordingly, this version of the document also benefits from the results achieved in this contexts.

4 Preliminary Guidelines

4.1 Operational Concept Subprocess

4.1.1 Key Differences

The differences between the EASA and SESAR interpretations of the Operational Concept subprocess are rooted in their distinct scopes and strategic objectives. EASA adopts a more targeted focus, concentrating on end-users who will directly interact with the AI system and analyzing how these users collaborate with the AI during task execution. SESAR, on the other hand, adopts a broader systems-level perspective, targeting the wider ATM stakeholder community—including ANSPs, airports, and airspace users—and focusing on the expected benefits and integration of the solution within the overall ATM environment.

One key area of differentiation lies in the treatment of explainability. EASA explicitly tailors its requirements based on the audience, requiring simpler, outcome-oriented explanations for operational users and more detailed technical transparency for developers and validation teams. SESAR does not adopt such a differentiated explainability approach.

From a scope standpoint, EASA emphasizes the definition of the Operational Domain (OD) and Operational Design Domain (ODD) as critical frameworks for AI reliability and data integrity. These serve as reference contexts for performance monitoring and system validation. In contrast, SESAR requires a precise definition of the external operational environment and its integration within the broader ATM architecture. However, SESAR does not mandate a functional analysis nor an exploration of specific contextual parameters upon which AI may base its reasoning.

EASA and SESAR differ in terms of what is considered the main subject of the operational concept. EASA focuses specifically on the AI system itself, while SESAR addresses the broader solution, which may incorporate AI but also includes other technological and procedural components. In addition, EASA uniquely requires a classification of the system's level of automation—an element that is not formally mandated in the SESAR framework and is only optionally included in use case descriptions.

Finally, there is a clear divergence in the expected outputs of the process. SESAR calls for the development of formalized operational models, such as interaction and activity models, as explicit deliverables. EASA, while requiring a functional analysis of the system, does not define such structured documentation as necessary outputs of the ConOps process.

Topic	EASA	SESAR
Target Audience	Focuses on end-users interacting directly with AI systems.	Broader focus on ATM stakeholders (ANSPs, airports, airspace users).

Topic	EASA	SESAR
Scope	Emphasizes AI application characterization and ODD definition; focuses on AI system;	Defines operational environment and ATM context; focuses on broader solution; does not require automation level classification.
Terminology	Emphasizes AI/ML, task allocation, and formal OD/ODD concepts; uses task allocation to define AI-user interaction.	Uses definitions for operating/sub-operating environments; uses roles and responsibilities to describe changes in user work.
Inputs	Uses “Operational Domain (OD)” and emphasizes stakeholder roles and responsibilities; values direct stakeholder input.	Uses “Operational Environment (OE)” and emphasizes stakeholder roles and responsibilities; values direct stakeholder input.
Outcomes	Requires functional analysis but not specific operational models.	Requires documented operational models like interaction and activity models.

Table 1. General key differences for operational concept subprocess.

4.1.2 Overlaps

Concerning the Operational Concept subprocess, several areas of alignment can be observed. Both frameworks identify team members and operational stakeholders as key target audiences. They also emphasize the importance of involving oversight and regulatory bodies—such as EASA, SESAR JU, and certification authorities—as essential contributors to the process. This shared focus reflects a common commitment to ensuring transparency, accountability, and regulatory compliance.

Another significant overlap lies in the way both EASA and SESAR describe how the system or solution will be used in practice. Each employs a structured operational concept model—referred to as ConOps by EASA and OSED by SESAR—that encompasses user interaction, operational tasks, and the surrounding environment. While the terminology may differ, the objective of defining real-world use is clearly aligned.

Additionally, both initiatives stress the importance of describing user interaction with the system. SESAR addresses this through detailed role and responsibility definitions embedded in use case formalism, whereas EASA employs a task allocation model to delineate the collaboration between human operators and AI systems. Despite these shared goals, no substantial overlaps were identified with regard to expected outputs or required inputs of the subprocess, where the approaches diverge more significantly.

Topic	Commonality
Target Audience	Both SESAR and EASA identify development/project team members and operational stakeholders as relevant audiences, including regulatory bodies.
Scope	Both consider how the system will be operated by end-users. SESAR details roles/responsibilities; EASA focuses on task allocation.
Terminology	Both use a concept (ConOps/OSED) to describe how a new system or solution will be used in practice, involving users, activities, and environment.

Table 2. General overlaps for operational concept subprocess.

4.1.3 Main Findings

The comparison between the operational concepts of EASA and SESAR highlights distinct approaches to the integration of artificial intelligence within the ATM context. EASA focuses on the interaction between AI systems and end-users, promoting differentiated levels of explainability and defining the Operational Design Domain (ODD) to ensure data quality and system transparency. SESAR adopts a broader perspective, addressing the entire ATM stakeholder ecosystem and requiring a detailed contextualization of the solution within the operational architecture, though without a specific functional analysis.

EASA's concept is centered on the AI system itself and mandates classification according to the level of automation, whereas SESAR refers to a more general "solution," without formal requirements regarding automation. From a terminological standpoint, EASA introduces formal models such as task allocation, while SESAR uses more generic notions of roles and responsibilities. SESAR also requires more structured documentation of operational models compared to EASA. Both frameworks emphasize the importance of stakeholder involvement and the definition of the operational context, but they differ significantly in their implementation approaches.

4.2 Safety Subprocess

4.2.1 Key Differences

The target audiences of EASA and SESAR safety guidance differ in scope and focus. EASA's guidance is broadly aimed at applicants who must demonstrate that systems embedding AI/ML constituents operate at least as safely as traditional systems. This includes a wide range of aviation stakeholders such as end users, applicants, and certification authorities. In contrast, SESAR primarily addresses safety practitioners engaged in research, innovation, and very large-scale demonstration projects, as well as members of SESAR JU, national supervisory authorities, and others involved in air traffic management and navigation services.

Regarding scope, EASA's safety process encompasses the entire aviation system lifecycle, including on-board systems, ground systems, ATM/ANS, maintenance, and training. It addresses all phases from

development through deployment to continuing airworthiness. SESAR's scope is more narrowly focused on ATM/ANS systems, particularly during the system development phases, applying a dual perspective that considers both the success (effectiveness) and failure (risk) of new concepts and technologies.

In terms of terminology, EASA's documentation assumes foundational knowledge of safety processes and focuses on defining AI-specific techniques to delimit the scope of AI/ML applicability. SESAR offers a broader set of safety and program-specific definitions, covering a wider range of terms beyond AI.

The inputs to the safety process also differ. EASA relies heavily on established aviation standards such as ARP4761 and EU regulations for ATM/ANS, considering these as major inputs to certification and safety activities. SESAR, on the other hand, treats all existing project documentation, such as Operational and System Environment Descriptions (OSED) and System Performance Requirements (SPR), as relevant inputs.

When it comes to outcomes, EASA emphasizes documenting safety assessments and means of compliance but does not mandate formal deliverables. In contrast, SESAR requires a strict documentation regime including Validation Plans and Safety Reports that clearly capture the safety argument and criteria at various project stages.

The assessment methodology in EASA is characterized by extensive guidance to ensure compliance with AI trustworthiness frameworks and regulatory standards, referencing certification specifications and international standardization bodies. SESAR delegates much of the compliance responsibility to ANSP Safety Managers who apply expert judgment within approved national processes.

Performance indicators further highlight differences. EASA leaves the definition of relevant metrics to project developers, allowing flexibility tailored to each AI/ML application. SESAR provides predefined Key Performance Areas and Indicators at the solution level, guiding projects in their selection of relevant safety metrics.

Finally, support and resources vary significantly. SESAR offers extensive templates for deliverables and organizes training courses on safety issues, fostering consistency across projects. EASA's Concept Paper is a recent publication and currently lacks such supporting tools and materials.

Topic	EASA	SESAR
Target Audience	Broad: Applicants demonstrating AI/ML system safety across all aviation stakeholders	Focused: Safety practitioners in R&I, VLD projects, SESAR JU members, NSAs, EASA in rulemaking
Scope	Complete aviation system lifecycle: on-board, ground, ATM/ANS, maintenance, and training	ATM/ANS systems during development phases; dual perspective of success and failure
Terminology	AI-specific terms; assumes basic safety process knowledge	Comprehensive safety and SESAR-related definitions

Topic	EASA	SESAR
Inputs	Aviation standards (e.g., ARP4761, EU regulations, etc) as major inputs[3]	All existing project documentation (OSED, SPR, etc.)
Outcomes	General documentation of safety assessment and Means of Compliance	Strict deliverables: Validation Plan and Validation Report including safety documentation
Assessment Methodology	Detailed guidance for compliance with AI trustworthiness and regulatory standards	Compliance responsibility assigned to ANSP Safety Managers using expert judgment
Performance Indicators	Metrics defined by system developers for each application	Predefined KPAs and KPIs guide projects
Support and Resources	No templates or extensive supporting materials	Extensive templates and training courses

Table 3. General key differences for safety subprocess.

4.2.2 Overlaps

Despite their differences, EASA and SESAR share several commonalities in their approach to safety processes. Both frameworks emphasize the importance of a structured and systematic approach to ensuring the safety of aviation systems that are being developed or deployed. They recognize the necessity of integrating safety considerations throughout the system lifecycle, ensuring that safety objectives and requirements are clearly defined, assessed, and documented.

In terms of terminology, although EASA focuses on AI-specific terms and SESAR covers a broader safety vocabulary, both recognize the critical role that a common understanding of key concepts plays in the safety assessment process. This shared focus on terminology helps align stakeholders on essential safety principles and definitions.

Regarding inputs, both EASA and SESAR acknowledge the value of leveraging comprehensive documentation early in the safety process. While EASA centres on aviation standards, and SESAR includes all project documentation, both consider these inputs fundamental to framing safety assessments and supporting subsequent activities.

[3] It is worth noting that the inputs to the safety analysis can draw on a wide range of reference materials, and what is presented here represents only a minimal subset.

For outcomes, EASA and SESAR both require thorough documentation that supports safety compliance and decision-making. The extent and format of this documentation may vary, but the underlying principle that safety assessment results must be recorded and traceable is a shared priority.

In performance indicators, both approaches consider the use of appropriate metrics essential to demonstrating that the system meets defined safety levels. This common focus ensures that safety performance is measurable and verifiable.

Finally, both EASA and SESAR require safety expertise from the parties involved, ensuring that safety assessments and compliance activities are performed by knowledgeable professionals capable of addressing the unique challenges posed by AI/ML systems and aviation systems in general.

Topic	Commonality
Approach	Both propose a structured approach to ensure the safety of the system under development
Terminology	Both emphasize the importance of a shared understanding of key safety-related terms
Inputs	Both consider comprehensive documentation as fundamental inputs to the safety process
Outcomes	Both require thorough documentation of safety assessments and decisions
Performance Indicators	Both use performance metrics to demonstrate system compliance with safety requirements
Safety Expertise	Both target audiences require significant knowledge and expertise in safety aspects of AI/ML systems

Table 4. General overlaps for safety subprocess.

4.2.3 Main Findings

The comparison between EASA and SESAR safety subprocesses reveals complementary strengths and some gaps that offer opportunities for alignment and convergence in future aviation safety frameworks.

EASA's comprehensive scope, covering the entire aviation system lifecycle and explicitly addressing AI/ML-specific safety considerations, provides a solid regulatory foundation. It does not provide detailed procedural templates and tools to support applicants, which SESAR offers through its well-established documentation standards and project-level guidance. Bridging this gap by developing harmonized templates and practical guidance would facilitate smoother compliance and certification processes for AI/ML systems.

SESAR's focus on ATM/ANS systems and its dual approach combining success and failure perspectives enhances its robustness in system-level safety evaluation. Yet, its narrower scope, often excluding other aviation domains and limited AI/ML-specific guidance, suggests a need for extension or

integration with EASA's broader regulatory framework to ensure end-to-end safety assurance across all aviation subsystems.

Both frameworks acknowledge the importance of performance indicators, but EASA's open-ended approach leaves indicator definition to individual projects, whereas SESAR provides a predefined set of KPIs. Developing a unified set of safety performance indicators tailored for AI/ML-based aviation systems could promote consistency and comparability across projects.

Lastly, both EASA and SESAR recognize the critical role of safety expertise, yet their target audiences differ in focus. Joint training initiatives or collaborative forums that bring together applicants, safety experts, certification authorities, and operational stakeholders could enhance shared knowledge and foster a more unified safety culture.

In summary, future convergence efforts should aim to integrate EASA's regulatory rigor and AI specificity with SESAR's operational detail and practical support tools. This integration will help close existing gaps, standardize safety practices across aviation domains, and ensure safer deployment of AI/ML-enabled systems in the evolving aviation ecosystem.

4.3 Security Subprocess

4.3.1 Key Differences

The key differences between EASA and SESAR in their approach to the security subprocess largely stem from their differing scopes, methodologies, and focus areas.

Firstly, the scope of the risk assessment is broader in SESAR. While EASA concentrates specifically on information security, particularly from a digital and data protection standpoint—especially concerning AI and machine learning systems—SESAR adopts a more comprehensive security perspective. Through its SecRAM methodology, SESAR includes not only information security but also physical and operational risks, which gives it a more general and inclusive scope.

Another major difference lies in the treatment of residual risk levels. EASA does not define strict thresholds for acceptable residual risk, leaving the judgment to the context of certification. In contrast, SESAR enforces clearer constraints: it explicitly does not accept high residual risks, and any medium-level risks must be justified through supporting documentation. This makes SESAR's stance on risk acceptance more rigid and formalized.

Their assessment methodologies also differ. EASA does not prescribe a specific method and tends to assess risks at the (sub)system level, which aligns with its focus on AI components and their data. On the other hand, SESAR applies a service-oriented approach, analysing risks at the service level, considering interactions between services, data flows, and interfaces. This distinction reflects two fundamentally different analytical perspectives.

When considering the impact areas of potential risks, EASA focuses primarily on safety impacts. SESAR, however, evaluates a wider range of impacts, including performance, economic factors, environmental consequences, and reputational damage. While both approaches account for safety (since SESAR includes "people" as an impact area), SESAR provides a more holistic view of possible consequences.

A significant difference also emerges in relation to Technology Readiness Levels (TRLs). EASA does not tie its objectives or requirements directly to the TRL of the AI/ML system. Conversely, SESAR's approach is explicitly TRL-driven. Security requirements and evidence are expected to progress incrementally with each TRL stage, starting as early as TRL2. This creates a structured roadmap for security development, which EASA does not define.

Finally, in terms of validation and verification of security controls, EASA requires specific activities to validate the effectiveness of controls aimed at mitigating AI/ML-specific risks. SESAR limits direct validation and testing—such as penetration tests—to later development stages (specifically TRL8), although it still expects security requirements to be defined and verified at earlier stages. Thus, EASA emphasizes early validation, while SESAR focuses on final-stage assurance supported by earlier documentation.

Topic	EASA	SESAR
Scope of Risk Assessment	Focuses on information security, particularly for AI/ML systems	Broader scope including information, physical, and operational security via SecRAM
Treatment of Residual Risk	No strict thresholds; contextual judgment in certification	High residual risks not accepted; medium risks require documented justification
Assessment Methodology	Subsystem-level focus, especially AI components and data	Service-oriented, evaluating service interactions, data flows, and interfaces
Impact Areas of Risk	Primarily safety impacts	Multiple impacts considered: safety, performance, economic, environmental, reputational
Technology Readiness Level	Not tied directly to TRLs	TRL-driven security requirements; structured progression from TRL2 to TRL8
Validation of Security Controls	Early validation of AI/ML-specific controls required	Focus on final-stage testing (e.g., TRL8) with earlier-stage documentation

Table 5. General key differences for security subprocess.

4.3.2 Overlaps

Despite their differences in scope and methodology, EASA and SESAR share several important commonalities in their treatment of security within AI/ML and ATM systems.

One key area of overlap is their recognition of the importance of security risk assessment in ensuring the safe and reliable operation of complex systems. Both frameworks emphasize the need to identify, evaluate, and mitigate security threats, particularly in relation to digital information and AI/ML technologies. While EASA focuses more narrowly on information security, and SESAR takes a broader view, both agree that security is a critical enabler of system trustworthiness.

Another important point of alignment is their shared concern for safety impacts. Although SESAR considers a wider range of impact domains (such as economic, environmental, and reputational factors), it includes "people" as one of its categories—effectively covering safety-related impacts, which is EASA's primary focus. This means that, at a fundamental level, both frameworks consider the safety of people to be central to their risk evaluation.

In addition, both approaches emphasize the need for security controls and the verification of their effectiveness. EASA requires explicit validation and verification activities tailored to AI/ML-related risks, while SESAR, though more focused on final-stage testing (e.g., at TRL8), also calls for security requirements to be defined early and subject to verification as the system evolves. In this way, both acknowledge that security cannot be an afterthought—it must be planned and demonstrated throughout the development lifecycle.

Moreover, both frameworks are compatible with a lifecycle-based view of system development. While SESAR explicitly integrates Technology Readiness Levels (TRLs) to structure its security evidence over time, EASA also considers security across the design, production, and operational phases. This shared recognition of the need to address security across multiple development stages reflects a common systems-thinking approach.

Finally, although their methodological levels differ, both EASA and SESAR are risk-based and context-driven. They allow for some flexibility in how security risks are identified and managed, encouraging organizations to adapt the assessment process based on the specific characteristics and risks of the system being developed or certified.

Topic	Commonality
Security Risk Assessment	Both EASA and SESAR recognize the importance of conducting security risk assessments to ensure trustworthy and safe system operation.
Focus on Safety Impacts	Both frameworks ultimately prioritize the safety of people, even though SESAR includes broader impact categories like environment and economics.
Security Controls Verification	Both require that security controls are defined and their effectiveness verified, acknowledging that security must be addressed throughout the lifecycle.
Lifecycle Perspective	Both EASA and SESAR consider security across multiple development phases, with SESAR using TRLs and EASA aligning with system lifecycle phases.

Topic	Commonality
Risk-Based Flexibility	Both adopt a risk-based, context-aware approach that allows flexibility in how organizations perform security assessments and mitigations.

Table 6. General overlaps for security subprocess.

4.3.3 Main Findings

EASA and SESAR represent two distinct yet complementary approaches to security risk assessment in aviation. EASA emphasizes information security for AI/ML systems, using a flexible, context-driven method aligned with certification processes. SESAR, on the other hand, applies a broader and more structured approach through its SecRAM methodology, covering a wider range of risks and integrating security requirements with TRLs.

While their scopes and methodologies differ, both frameworks share key principles: a risk-based approach, attention to safety impacts, and the requirement to validate and verify security controls. EASA offers depth at the product level, particularly for AI components, while SESAR ensures comprehensive coverage across complex ATM services and systems.

To enable future convergence, several gaps may be addressed. These include the need for more harmonized methods, earlier alignment on validation activities, and improved support materials. Bridging these differences could be achieved through joint guidance and interoperable tools, fostering a more unified and effective security framework for AI-enabled aviation systems.

For example, establishing a common vocabulary and threat taxonomy for AI-related security risks would enhance interoperability and reduce ambiguities across frameworks. This would facilitate clearer communication between stakeholders and ensure consistent interpretation of requirements. Encouraging convergence on the timing and depth of validation and verification activities—e.g., earlier inclusion of AI-specific tests in SESAR or more structured TRL guidance within EASA—would support smoother integration of AI technologies from concept to deployment. A shared database of use cases, risk scenarios, mitigations, and assessment results from both EASA and SESAR projects could support cross-learning, accelerate maturity, and foster reuse of validated security approaches.

4.4 Ethics Subprocess

4.4.1 Key Differences

The main differences between the EASA and SESAR ethics subprocesses lie in their respective goals, methodological structures, and areas of application. EASA adopts a certification-oriented approach aimed at ensuring regulatory and legal compliance for AI solutions, particularly for Level 1 and Level 2 machine learning systems. Its framework requires formal documentation and integration with system validation processes, including assessments related to human oversight, explainability, and data governance. By contrast, SESAR operates within a research-driven context, with a focus on ethical oversight of EU-funded projects. SESAR follows structured guidelines, procedures, and templates issued by the European Commission, applying them more flexibly to support ethical consistency throughout the entire project lifecycle, rather than system-level certification. Input sources also differ:

EASA relies on technical elements derived from the AI trustworthiness analysis, such as ConOps, system characterization, and safety/security assessments, while SESAR draws from project management documentation such as the Project Management Plan (PMP) and Data Management Plan (DMP). Finally, the nature of the expected outputs reflects this divergence: EASA generates documentation supporting risk assessment and certification readiness, whereas SESAR focuses on demonstrating compliance with ethical requirements at the project and institutional levels.

Topic	EASA	SESAR
Scope and purpose	Focused on evaluating the trustworthiness of Level 1 and 2 machine-learning applications in aviation, aiming at long-term certification.	Aims to ensure that EU-funded research projects comply with ethical principles and European values throughout their lifecycle.
Coverage of ethical dimensions	Not all ALTAI requirements are fully applicable or implementable in aviation; most are relevant mainly for design implications.	Research projects are expected to comply with all AI ethics requirements as part of an Ethics by Design approach.
Approach	No definitive official methodology; applicants may refer to ALTAI questions adapted to aviation, with some flexibility in implementation.	Structured approach based on guidelines, tools, and templates provided by the European Commission and implemented in SESAR.
Inputs	Inputs stem from AI trustworthiness analysis, especially ConOps, solution characterization, and safety/security assessments.	Inputs come from project documentation such as PMP, DMP, and the requirements from EC ethics reviews, including tasks related to AI ethics.
Ethics impact documentation	Outputs include at minimum a documentation of impact (via ALTAI); ideally, a report on technical and ethical decisions made.	Outputs consist of documentation proving that the research complies with the ethical standards and procedures set by the EC.
Compliance and governance	Oriented toward system certification, requiring formal documentation and integration with validation processes.	Oriented toward ethical governance of research projects, using flexible tools like ALTAI and high-level foresight mechanisms.

Table 7. General key differences for ethics subprocess.

4.4.2 Overlaps

EASA and SESAR share a common understanding of the importance of adopting an "Ethics by Design" approach in the development of AI-based solutions in the aviation domain. Both initiatives promote the early integration of ethical principles as a core component of system development, aiming to ensure responsible, transparent, and value-aligned AI. They rely on structured tools for ethical assessment—such as the ALTAI checklist and Data Protection Impact Assessments (DPIAs)—and both refer to EU-level frameworks, although with different end goals: EASA focuses on operational certification, while SESAR emphasizes ethical governance in research and innovation. In addition, both processes recognize the Concept of Operations (ConOps) as a valuable input to inform ethical design choices. However, the guidance provided by both EASA and SESAR tends to be formulated at a high level of abstraction and may lack the level of specificity required for direct implementation in the aviation sector.

Topic	Commonality
Ethics by design	Both EASA and SESAR promote the integration of ethical principles from the early design phases of AI-based aviation solutions, fostering an "Ethics by Design" approach.
Level of detail	Ethical guidance in both EASA and SESAR is often based on high-level principles and tends to lack operational specificity for direct application in aviation.
Ethical assessment tools	Both make use of structured tools such as ALTAI for assessing ethical risks and include DPIAs when personal data is involved.

Table 8. General overlaps for ethics subprocess.

4.4.3 Main Findings

The comparison between the EASA and SESAR ethics subprocesses reveals a structural divergence in their objectives and scope. EASA focuses on certifying the ethical trustworthiness of AI applications in aviation, specifically targeting Level 1 and Level 2 machine learning technologies. Its approach is grounded in the adaptation of the ALTAI framework, aiming to integrate ethics into the technical certification process. Conversely, SESAR adopts a broader, system-level perspective, emphasizing ethical compliance throughout the entire lifecycle of EU-funded research projects. This includes design, management, implementation, and monitoring, with particular attention to data protection, transparency, and ethical risk prevention.

Both frameworks promote an “ethics by design” approach, though with different emphases: EASA applies it to support certification, while SESAR embeds it as a methodological requirement in research activities. However, both approaches share a degree of generality in their guidelines, which may limit their practical applicability in specific aviation scenarios. EASA’s limitations are mainly related to the

difficulty of adapting certain ethical dimensions—such as societal impact or diversity—to the aviation context. SESAR, while offering more structured tools, relies on general principles that are not always tailored to the specific needs of the aviation sector.

In terms of outputs, EASA aims to produce documentation that supports certification (e.g., ethics-based tests, DPIAs, environmental analyses), whereas SESAR focuses on demonstrating compliance with research ethics regulations through self-assessment reports, data management plans, and periodic ethics reviews. The assessment methods also reflect this distinction: EASA adopts a compliance-oriented approach based on structured documentation and testing, while SESAR emphasizes ethical governance and risk management across the research process.

4.5 Human Factors Subprocess

4.5.1 Key Differences

The HF subprocesses adopted by SESAR and EASA diverge significantly in their goals, scope, and methodological aspects. EASA's subprocess is rooted in a regulatory and compliance-oriented framework, aiming to support the certification of AI-enabled systems with a clear emphasis on aligning human factors with safety and conformity expectations. It caters primarily to certification experts and stakeholders tasked with ensuring adherence to AI-specific guidelines as outlined in the EASA AI Roadmap and associated Concept Papers. In contrast, SESAR's approach is designed to support research and development within the European ATM modernisation context. It is broader in scope, aiming to analyse and refine the impacts of technological solutions on operational environments, including the roles, procedures, and collaboration patterns of human operators.

A key difference lies in the way inputs are handled. EASA's process focuses narrowly on the behaviours of the AI system, particularly how it interacts with human operators in terms of explainability, workload, error and failure management, and interface customization. SESAR takes a more systemic view, incorporating impacts on team structures, transitional dynamics, human-machine interaction patterns, and changes to working methods—often using structured templates and documentation tools such as the SPR-INTEROP/OSED and VALP.

Methodologically, SESAR provides a complete assessment architecture with step-by-step processes, arguments, validation objectives, and maturity criteria mapped to TRLs. In contrast, EASA does not address a formalised methodology and relies on the existing frameworks.

In terms of expected outcomes, EASA outputs focus on compliance and conformity, offering judgments about whether the system meets existing or proposed human factors certification standards, especially in AI use. SESAR focuses on learning and system evolution, generating insights into potential issues, benefits, and recommendations to guide future iterations and validations.

Lastly, when it comes to measuring performance, SESAR employs success criteria tied to arguments and TRLs, whereas EASA currently does not define formal KPIs.

The aforementioned aspects are summarized in Table 9.

Topic	EASA	SESAR
Purpose & Audience	Focuses on regulatory compliance for certification experts, especially concerning AI integration.	Supports R&D teams, with an exploratory focus on operational and organizational impacts.
AI-Specific Integration	Incorporates AI levels and compliance requirements explicitly in HF assessment.	Technology-agnostic with no formal AI-specific objectives.
Input Focus	Narrow scope—focused on human-AI interaction specifics such as explainability and workload.	Broader operational view—examines roles, procedures, transitions, and overall human system impact.
Assessment Methodology	No dedicated methodology, relies on existing frameworks such as SESAR one.	Well-defined methods including arguments, activities, TRL-linked criteria, and documentation.
Outcomes	Compliance-centric; assesses conformity to HF certification requirements.	Exploratory; identifies HF issues and benefits, with design and validation recommendations.
KPIs	No defined KPIs; relies on other frameworks.	Defines evidence-based success criteria mapped to TRL thresholds.

Table 9. General key differences for human factor subprocess.

4.5.2 Overlaps

Despite their differences, SESAR and EASA share several foundational elements in their treatment of HF. Both approaches are grounded in a common understanding of HF disciplines, involving professionals from diverse backgrounds such as engineering, psychology, and ergonomics, all aiming to ensure safety, efficiency, and usability in aviation systems.

A significant area of convergence lies in the procedural foundations: both SESAR and EASA build upon SESAR's Human Performance Assessment Process and its associated documentation templates (e.g., SPR-INTEROP/OSED, VALP, VALR), signifying a mutual recognition of methodological rigor.

In terms of conceptual alignment, SESAR and EASA have taken steps to integrate their automation taxonomies. This alignment supports a shared vocabulary and mutual understanding of automation's role in shaping human-system interaction.

Both processes maintain a strong and consistent focus on key HF elements, including human-machine interaction, error tolerance, explainability, workload, and safety implications. While the orientation differs (regulatory versus exploratory), the core concerns are largely aligned.

Finally, EASA's reliance on SESAR's more mature assessment methods indicates both the compatibility and complementarity of their approaches. EASA acknowledges SESAR's templates, success criteria, and activity documentation as valuable tools to supplement its regulatory pathway, particularly where formal methodologies are still under development.

The aforementioned aspects are summarized in Table 10.

Topic	Commonality
Expertise	Both involve multidisciplinary HF experts: engineers, psychologists, HMI specialists, etc.
Foundational Procedures	Both use SESAR-originated templates and documentation like SPR-INTEROP/OSED, VALP, VALR.
Conceptual Focus	Shared emphasis on human-machine interaction, explainability, workload, and error handling.
Terminology Alignment	Increasing alignment through integrated automation/AI level taxonomies.
Methodological Interdependence	EASA frequently references and leverages SESAR and EUROCONTROL methodologies.

Table 10. General overlaps for human factor subprocess.

4.5.3 Main Findings

The comparative analysis of the HF subprocesses within SESAR and EASA reveals a complementary but fragmented landscape. SESAR's methodology offers a mature, comprehensive, and well-structured framework. It provides detailed guidance on human performance assessment through clearly defined steps, evidence-based criteria, and extensive use of templates and documented outputs, all calibrated to different TRLs. This makes SESAR's approach highly valuable for exploring the broader impact of technological solutions on human operators, team dynamics, and transitional challenges within complex operational environments. On the other hand, EASA's subprocess is still evolving. Rooted in regulatory compliance, it focuses heavily on ensuring conformity with certification requirements.

The principal gap lies in this divergence of maturity and purpose. EASA's compliance-driven subprocess is narrow in scope and insufficiently supported by standardized assessment tools and success metrics, while SESAR's broader, process-oriented framework is not yet fully aligned with AI-specific certification needs. Additionally, the lack of formal KPIs within EASA limits the ability to quantitatively measure progress or success in achieving human factors objectives related to AI.

To bridge these gaps and enable a more integrated, effective approach to HF assessment in the aviation domain, future efforts should focus on harmonizing the regulatory and operational perspectives. This can be achieved by leveraging SESAR's rich methodological assets as a foundation for EASA's evolving certification frameworks. For instance, incorporating SESAR's structured input collection templates, validation activities, and maturity checklists into EASA's compliance processes would add rigor and consistency.

Furthermore, jointly developing clear, AI-specific human factors KPIs—building on SESAR's evidence-based success criteria—would provide measurable targets that serve both certification and operational evaluation needs. The ongoing integration of AI level taxonomies in the European ATM Master Plan serves as a positive example of conceptual alignment that should be extended into assessment practices.

Ultimately, a future convergence should aim to create a unified HF framework that balances the needs for regulatory compliance, operational safety, and human-centred design. Such convergence would facilitate not only more consistent and transparent certification of AI-enabled systems but also foster safer, more effective integration of advanced technologies in aviation operations, benefiting regulators, developers, operators, and end-users alike.

5 Toolkit

Chapter 4 presented an analysis of key differences and overlaps between the EASA concept paper and the SESAR framework. This analysis is referred to as “Preliminary Guidelines”, to reflect the intent to lay the foundational principles for the harmonization between SESAR system development and compliance pathways when high levels of automation are addressed. Based on these preliminary guidelines, a practical toolkit has been derived to support the harmonisation activities. This toolkit includes several key components:

- Gap Analysis Checklists (Section 5.1)
- Traceability Matrix (Section 5.2)
- SESAR Templates for Documentation (Section 5.3)

To make the Preliminary guidelines actionable, a structured step-by-step process is proposed, which uses the key components of the Toolkit:

- Review of Applicable regulatory documents. Identify and analyse the relevant regulatory and operational guidance documents.
- Initial Gap and Overlap Analysis. Use checklists and mapping tools to assess alignment between SESAR solutions and regulatory frameworks.
- Traceability Mapping. Populate the traceability matrix to connect SESAR deliverables with applicable certification objectives and requirements.
- SESAR Templates. Draft and compile the necessary documentation using predefined templates.

This approach aims to enhance **transparency, consistency, and mutual understanding** between innovation deployment and regulatory compliance processes.

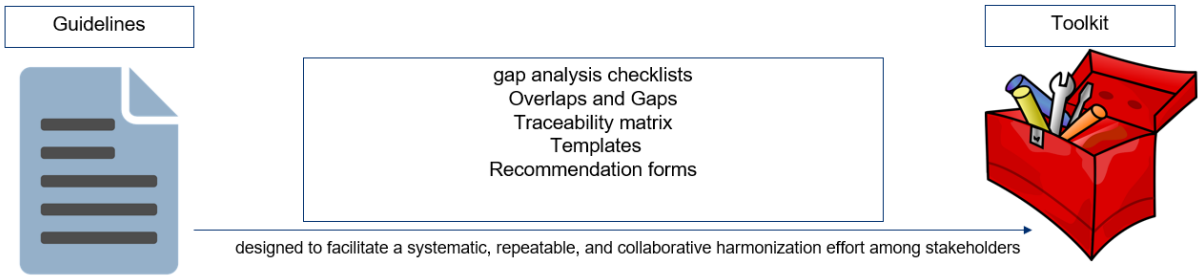

Figure 5: From the guidelines to the toolkit

5.1 Traceability Matrix

The table below presents a structured comparison between EASA Means of Compliance (MoC) and the SESAR methodology, organized by subprocess and objective. For each subprocess, relevant objectives and associated anticipated MoCs are identified. These are then mapped against SESAR development activities at different Technology Readiness Levels (TRLs)—specifically TRL2, TRL4–6, and TRL8.

This mapping aims to provide a clear traceability between regulatory expectations (EASA Concept paper MoCs) and SESAR documentation across various maturity levels. Each TRL entry includes references to specific documents and sections that demonstrate how SESAR activities align (or are expected to align) with EASA objectives.

Key points to note:

- Subprocesses and objectives are broken down to enable fine-grained alignment.
- The mapping shows the progressive coverage of compliance from early research phases (TRL2) to more mature validation stages (TRL8).
- The approach supports gap analysis, helping to identify which compliance elements are already addressed and where further evidence or alignment is needed.
- The structure also enables future updates, as additional documentation or evidence becomes available through the SESAR lifecycle.

Subprocess	EASA MOC		SESAR Methodology		
	Objective	Anticipated MOC	TRL2	TRL4-6	TRL8
Subprocess *ID1*	Objective *ID1-01*	Anticipated MOC *ID1-01.1*	*ID1-01.1-TRL2-reference_doc1 - section_id* *ID1-01.1-TRL2-reference_doc2 - section_id* ...	*ID1-01.01-TRL4-2-reference_doc1 - section_id* *ID1-01.01-TRL4-2-reference_doc2 - section_id* ...	*ID1-01.01-TRL8-reference_doc1 - section_id* *ID1-01.01-TRL8-reference_doc2 - section_id* ...
		Anticipated MOC *ID1-01.2*	*ID1-01.2-TRL2-reference_doc1 - section_id* *ID1-01.2-TRL2-reference_doc2 - section_id* ...	...	...
		...	...	...	...
	Objective *ID1-02*	Anticipated MOC *ID1-02.1*	*ID1-02.1-TRL2-reference_doc1 - section_id* *ID1-02.1-TRL2-reference_doc2 - section_id* ...	...	...
		Anticipated MOC *ID1-02.2*	...	...	...
		...	...	...	...
	...	...	...	...	...
Subprocess *ID2*	Objective *ID2-01*	Anticipated MOC *ID2-01.1*	*ID2-01.1-TRL2-reference_doc1 - section_id* *ID2-01.1-TRL2-reference_doc2 - section_id* ...	*ID2-01.01-TRL4-2-reference_doc1 - section_id* *ID2-01.01-TRL4-2-reference_doc2 - section_id* ...	*ID2-01.01-TRL8-reference_doc1 - section_id* *ID2-01.01-TRL8-reference_doc2 - section_id* ...
		Anticipated MOC *ID2-01.2*	*ID2-01.2-TRL2-reference_doc1 - section_id* *ID2-01.2-TRL2-reference_doc2 - section_id* ...	...	...
		...	...	...	...
	...	...	...	...	...
		...	...	...	...
		...	...	...	...
	...	...	...	...	...

Figure 6: Template of the Traceability Matrix EASA MOC vs SESAR Methodologies

The same reasoning applies to Evidences. In the following the figure representing the template tracing the EASA concept paper evidences needs vs SESAR Deliverables.

Subprocess	EASA Objective	SESAR Evidence		
		TRL2	TRL4-6	TRL8
Subprocess *ID1*	Objective *ID1-01*	*ID1-01-TRL2-solution_doc1 - section_id* *ID1-01-TRL2-solution_doc2 - section_id* ...	*ID1-01-TRL4-2-solution_doc1 - section_id* *ID1-01-TRL4-2-solution_doc2 - section_id* ...	*ID1-01-TRL8-solution_doc1 - section_id* *ID1-01-TRL8-solution_doc2 - section_id* ...
	Objective *ID1-02*	*ID1-02-TRL2-solution_doc1 - section_id* *ID1-02-TRL2-solution_doc2 - section_id* ...	...	...
	...	...	...	...
Subprocess *ID 2*	Objective *ID2-01*	*ID2-01-TRL2-solution_doc1 - section_id* *ID2-01-TRL2-solution_doc2 - section_id* ...	*ID2-01-TRL4-2-solution_doc1 - section_id* *ID2-01-TRL4-2-solution_doc2 - section_id* ...	*ID2-01-TRL8-solution_doc1 - section_id* *ID2-01-TRL8-solution_doc2 - section_id* ...
	Objective *ID2-02*	*ID2-02-TRL2-solution_doc1 - section_id* *ID2-02-TRL2-solution_doc2 - section_id* ...	...	...
	...	...	...	...
	...	...	...	...

Figure 7: Template of the Traceability Matrix EASA Evidences needs vs SESAR Deliverables

Traceability matrix is derived applying the approach supported by the checklist reported in section 5.2.

5.1.1 Examples

In the following an example of the first traceability matrix applied to the Operational Concept Security sub-processes.

EASA MOC		SESAR Methodology		
Objective	Anticipated MOC	TRL2	TRL4-6	TRL8
CO-01 Identification of the end users	N.A.	N.A.	N.A.	N.A.
CO-02 Goals and high-level tasks identification	Anticipated MOC CO-02 Identification of the tasks only at the highest level of interaction between the human and the AI-based system	Not covered	Not covered	Not covered
CO-03 AI-based system identification	Anticipated MOC CO-03 The definition of the system varies between domains (i.e.: airborne systems, ATM/ANS domain, etc.)	Not covered	DES HE INTEROP-OSED - sections 3.1, 3.2, 3.4	DES HE INTEROP-OSED - sections 3.1, 3.2, 3.5
CO-04 Definition of the ConOps for the AI-based system and of the Operational Domain	Anticipated MOC CO-04 The ConOps should be described at the level of the product or of the AI-based system	Not covered	DES HE INTEROP-OSED - section 3.3; DES HE INTEROP-OSED (SAR-SSAR) - section 4.2, 5.3	DES HE INTEROP-OSED - section 3.3; DES HE INTEROP-OSED (SAR-SSAR) - section 4.2, 5.4
CO-05 Documenting end user inputsin the AI-based system development	Anticipated MOC CO-05 The applicant should engage end-user representatives in planning, design, validation, verification and certification/approval of an AI-based system	Not covered	Not covered	Not covered
CO-06 Functional analysis of the AI-based system	Anticipated MOC CO-06 The delineation between AI/ML item and non-AI/ML item is performed at this stage: at least one item has to be considered an AI/ML item	Not covered	Not covered	Not covered

Figure 8: Traceability Matrix for MoC - operational concept subprocess

EASA MOC		SESAR Methodology		
Objective	Anticipated MOC	TRL2	TRL4-6	TRL8
IS-01 Identification of AI/ML information security risks	Anticipated MOC IS-01 Consider evasion, poisoning and oracles attacks, using ENISA ML report as a reference	SESAR 3 Project Handbook - sections 3.3.4, C.2.4 SecRAM - sections 4.1, 4.2, 4.3, 4.4, 4.5 (initialise) SecRAM Catalogue	SESAR 3 Project Handbook - sections 3.3.4, C.2.4 SecRAM - sections 4.1, 4.2, 4.3, 4.4, 4.5 (update) SecRAM Catalogue	SESAR 3 Project Handbook - sections 3.3.4, C.2.4 SecRAM - sections 4.1, 4.2, 4.3, 4.4, 4.5 (update) SecRAM Catalogue
IS-02 Documentation of the mitigation approach to address AI/ML information security risks	Anticipated MOC IS-02 Apply security controls for the specific ML application, using ENISA ML report as a reference	SESAR 3 Project Handbook - section C.2.4 SecRAM - sections 4.6.1, 4.7 (initialise) SecRAM Catalogue	SESAR 3 Project Handbook - section C.2.4 SecRAM - sections 4.6.1, 4.7 (update) SecRAM Catalogue	SESAR 3 Project Handbook - section C.2.4 SecRAM - section 4.6.1, 4.7 (update) SecRAM Catalogue
IS-03 Verification and validation of the security controls	N.A.	SecRAM - sections 4.6.2, 4.6.3, 4.6.4, 4.7 (initialise)	SecRAM - sections 4.6.2, 4.6.3, 4.6.4, 4.7 (update)	SecRAM - section 4.6.4 (validation exercises and/or penetration testing)

Figure 9: Traceability Matrix for MoC - security sub-process

Similarly, examples are provided for the Evidences identified at the various TRL levels, corresponding to the different Objectives outlined in the EASA Guidelines.

EASA Objective	SESAR Evidence		
	TRL2	TRL4-6	TRL8
CO-01 Identification of the end users	Not covered	Covered: DES HE INTEROP-OSED, section 3.1, 3.3.2.1; DES HE INTEROP-OSED (SAR), sections 4.1, 4.2; DES HE INTEROP-OSED (SSAR), section 3.1	Covered: DES HE INTEROP-OSED, section 3.1, 3.3.2.1; DES HE INTEROP-OSED (SAR), sections 4.1, 4.2; DES HE INTEROP-OSED (SSAR), section 3.2
CO-02 Goals and high-level tasks identification	Not covered	Covered: DES HE INTEROP-OSED, section 3.1; DES HE INTEROP-OSED (SAR), sections 3.1, 5.2.1; DES HE INTEROP-OSED (SSAR), section 3.1	Covered: DES HE INTEROP-OSED, section 3.1; DES HE INTEROP-OSED (SAR), sections 3.1, 5.2.1; DES HE INTEROP-OSED (SSAR), section 3.2
CO-03 AI-based system identification	Not covered	Covered: DES HE INTEROP-OSED, sections 2.5, 3.3; DES HE INTEROP-OSED (SAR), section 3.2	Covered: DES HE INTEROP-OSED, sections 2.5, 3.3; DES HE INTEROP-OSED (SAR), section 3.3
CO-04 Definition of the ConOps for the AI-based system and of the Operational Domain	Not covered	Covered: DES HE INTEROP-OSED (SAR), sections 3.1, 4.2, 5.2	Covered: DES HE INTEROP-OSED (SAR), sections 3.1, 4.2, 5.3
CO-05 Documenting end user inputsin the AI-based system development	Not covered	Partially covered: DES HE INTEROP-OSED, sections 1, 2.5, 3; DES HE INTEROP-OSED (SAR), section 3.2; DES HE INTEROP-OSED (SSAR), section 3.2	Partially covered: DES HE INTEROP-OSED, sections 1, 2.5, 3; DES HE INTEROP-OSED (SAR), section 3.2; DES HE INTEROP-OSED (SSAR), section 3.3
CO-06 Functional analysis of the AI-based system	Not covered	Not covered	Not covered

Figure 10: Traceability Matrix for Objectives - operational concept sub-process

EASA Objective	SESAR Evidence		
	TRL2	TRL4-6	TRL8
IS-01 Identification of AI/ML information security risks	ERR: Section 5.1.4 "Conclusions on performance assessments"	SecAP (VALP/TVALP annex): Section 3.2 "Scope of security for the SESAR technological solution" Section 3.3 "Security objectives" Section 3.4.1 "Risk assessment" Section 6 "Schedule and resources" VALR/TVALR: Section 5.1.4 "Conclusions on performance assessments"	PMP: Section 6 "Performance management" DEMOP - Security Annex: Section 3.2 "Scope of security for the SESAR technological solution" Section 3.3 "Security objectives" Section 3.4.1 "Risk assessment" Section 6 "Schedule and resources"
IS-02 Documentation of the mitigation approach to address AI/ML information security risks	ERR: Section 5.2.1 "Recommendations for next R&I phase"	SecAP (VALP/TVALP annex): Section 3.4.2 "Risk treatment" Section 5.1 "Security requirements" Section 6 "Schedule and resources" SPR-INTEROP/OSED: Section 4 "Safety, performance and interoperability requirements (SPR-INTEROP)" TS-IRS: Section 4 "Technical specifications" (related to security specifications)	PMP: Section 6 "Performance management" DEMOP - Security Annex: Section 3.4.2 "Risk treatment" Section 5.1 "Security requirements" Section 6 "Schedule and resources"
IS-03 Verification and validation of the security controls	ERR: Section 5.2.1 "Recommendations for next R&I phase" Section 5.2.2 "Recommendations for future R&I activities"	SecAP (VALP/TVALP annex): Section 4.3 "Other security issues" Section 6 "Schedule and resources" VALR/TVALR: Section 5.1.4 "Conclusions on performance assessments"	PMP: Section 6 "Performance management" DEMOP - Security Annex: Section 4.3 "Other security issues" Section 6 "Schedule and resources" DEMOR: Section 3.3 "Summary of Demonstration Plan" (related to security demonstrations) Section 4.1 "Summary of Demonstration Results" (related to security demonstrations)

Figure 11: Traceability Matrix for Objectives - security sub-process

5.2 Gap Analysis Checklist

In the following are the key questions of the checklist that supports the gap analysis.

Purpose and Objectives

- *What is the main goal of the EASA subprocess?*
- *What is the main goal of the SESAR subprocess?*
- *Are there any key differences and/or overlaps between the goals of EASA and SESAR subprocess?*
- *Which are the main boundaries or limitations of the EASA subprocess?*
- *Which are the main boundaries or limitations of the SESAR subprocess?*
- *Are there any key differences and/or overlaps between the boundaries and limitations of EASA and SESAR subprocesses?*

Target Audience

- *Which is the target audience of the EASA subprocess?*
- *Which is the target audience of the SESAR subprocess?*
- *Are EASA and SESAR subprocesses tailored to similar target audiences and levels of expertise or responsibility within the target audience?*

Scope

- *Which are the main activities and steps involved in the EASA subprocess?*
- *Which are the main activities and steps involved in the SESAR subprocess?*
- *Are there any key differences and/or overlaps between the main activities and steps involved in EASA and SESAR subprocesses?*

Terminology and Definitions

- *Are there any key differences and/or overlap between the terminologies and the definitions of key concepts in EASA and SESAR subprocesses?*

Inputs

- *What are the key inputs required for the EASA subprocess?*
- *What are the key inputs required for the SESAR subprocess?*
- *Are there any key differences and/or overlaps in the type and the scope of inputs used in EASA and SESAR subprocesses?*

Outcomes

- *Which are the main intended outcomes of the EASA subprocess? Identify the main outcomes (design report, design model, simulation report, test report, assessment form, software code, etc.).*
- *Which are the main intended outcomes of the SESAR subprocess? Identify the main outcomes (design report, design model, simulation report, test report, assessment form, software code, etc.).*

- *Are there any key differences and/or overlaps between the outcomes of the EASA and SESAR subprocesses?*

Assessment Methodology

- *Which are the main methods for compliance checking within the EASA subprocess?*
- *Which are the main assessment methods (if any; e.g., analysis, inspection, review, simulation, testing, etc.) within the SESAR subprocess?*
- *Are there possible correspondences between the compliance-checking methods in EASA subprocess and the assessment methods in subprocess?*

Performance Indicators

- *Does the EASA subprocess include criteria or metrics and related targets for measuring success or progress toward the objectives? [Use D4.2 as a starting point.]*
- *Does the SESAR subprocess include criteria or metrics and related targets for measuring success or progress toward the objectives?*
- *Are there any key differences and/or overlaps between criteria or metrics and related targets (at least for common objectives, if any) involved in EASA and SESAR subprocesses?*

Support and Resources

- *Are there any supplementary resources (e.g., tools, templates, training materials) for the EASA subprocess?*
- *Are there any supplementary resources (e.g., tools, templates, training materials) for the SESAR subprocess?*

5.3 SESAR Templates for Documentation

In the context of harmonizing SESAR innovation with EASA certification processes, clear documentation is essential to ensure that solutions are both understandable and assessable.

Within the HUCAN proposed approach, one of the most effective ways to achieve harmonisation is to ensure that the evidence required to demonstrate the fulfilment of the objectives can be consistently guaranteed through the SESAR deliverables. The full package of SESAR deliverables, eventually modified, can in fact be considered as a primary source of evidence for the objectives to which they are connected. Furthermore, deliverables **Standards and Regulations** (STAND and REG) should also be taken into account, as they can provide further insights on the same Means of Compliance (MoC) and on the certification baseline that must be considered.

As part of the project, a preliminary analysis has been carried out as an example of how a modification to the deliverables OSED and TS can ensure the provision of evidence for the coverage of a specific set of objectives from the EASA Concept Paper, particularly those related to the definition of the OD and the ODD.
To support this, two main templates are considered:

- SESAR Solution XX SPR-INTEROP/OSED template, that integrates key aspects related to Safety Performance Requirements (SPR), Interoperability (INTEROP), and the Operational Services and Environment Description (OSED).

- DES HE SESAR solution XXX TS/IRS template, designed to support any TRL, focused on the technical description of the solution and the definition of implementation requirements.
- DES HE concept outline template for TRL1, which defines the structure and content required for the description of concepts, technologies or capabilities aimed at achieving TRL1.

These templates provide a common and traceable structure for documenting SESAR solutions and help ensure consistency with EASA processes, simplifying the identification of gaps, misalignments, and opportunities for regulatory integration. Below are the indexes of the two documents.

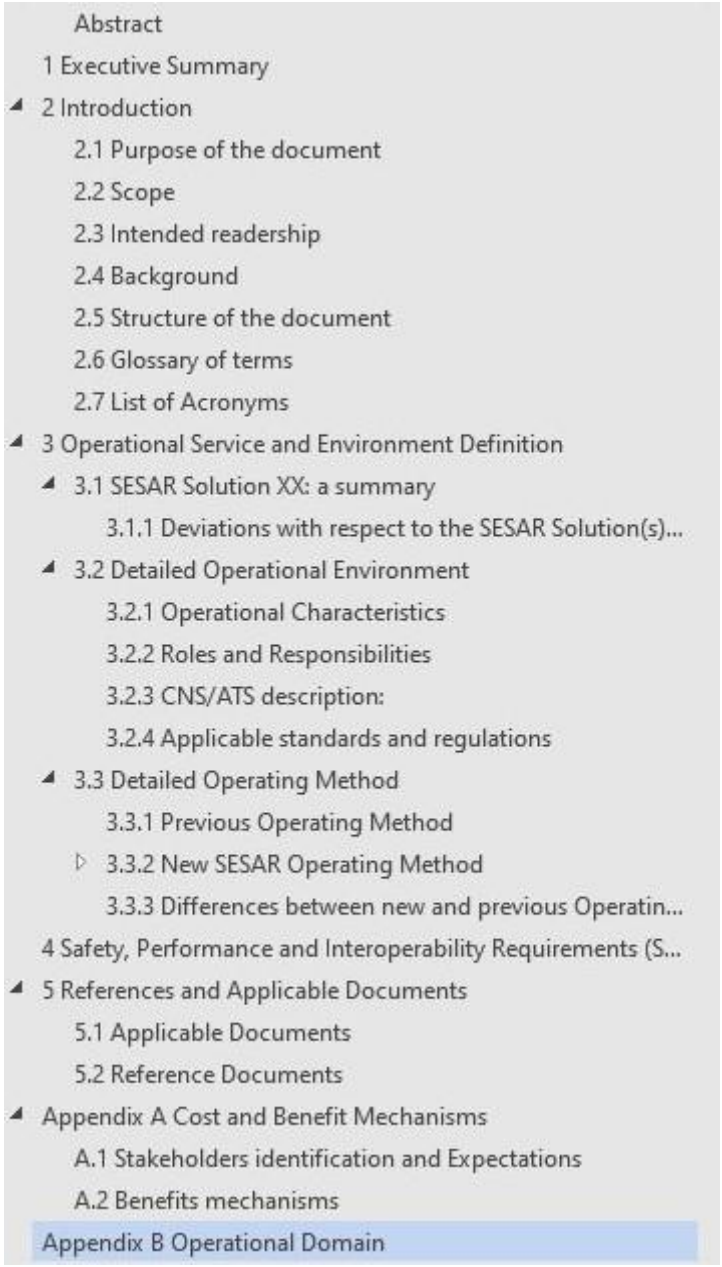

Figure 12: SESAR Solution XXX SPR-INTEROP/OSED template - Table of Contents

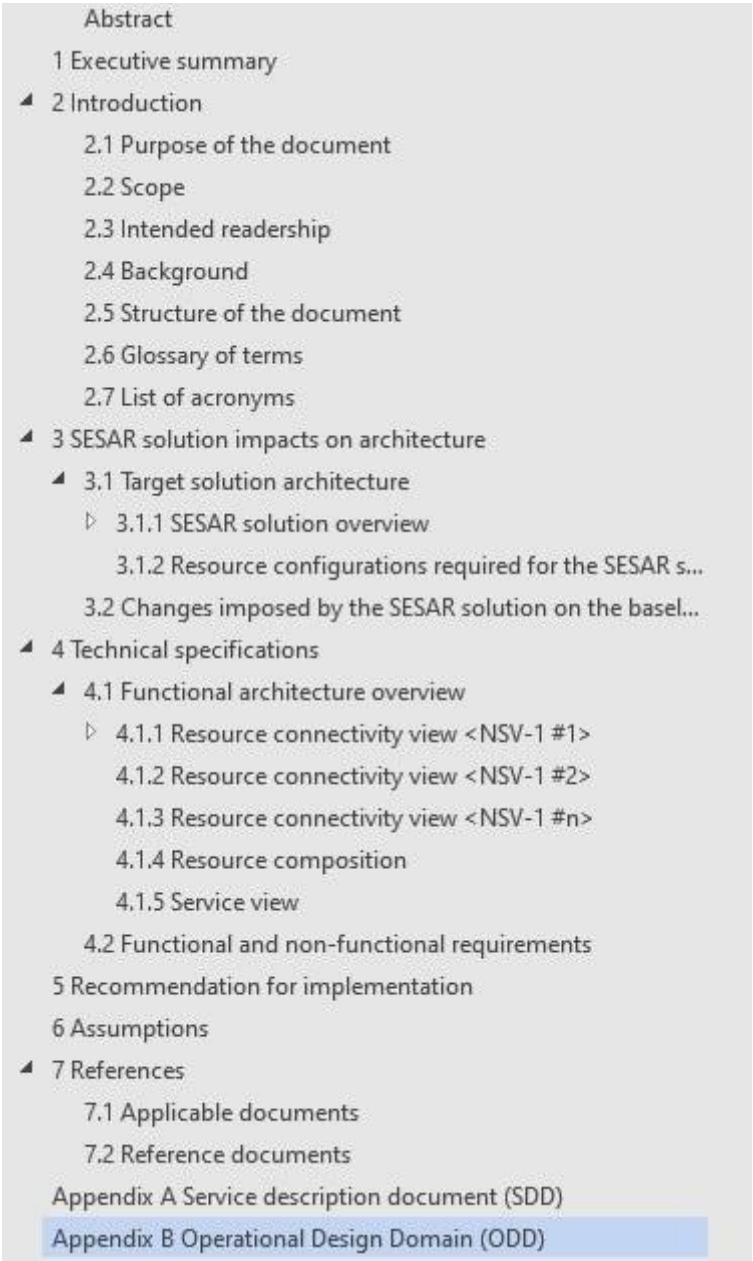

Figure 13: DES HE SESAR Solution XXX TS/IRS template - Table of Contents

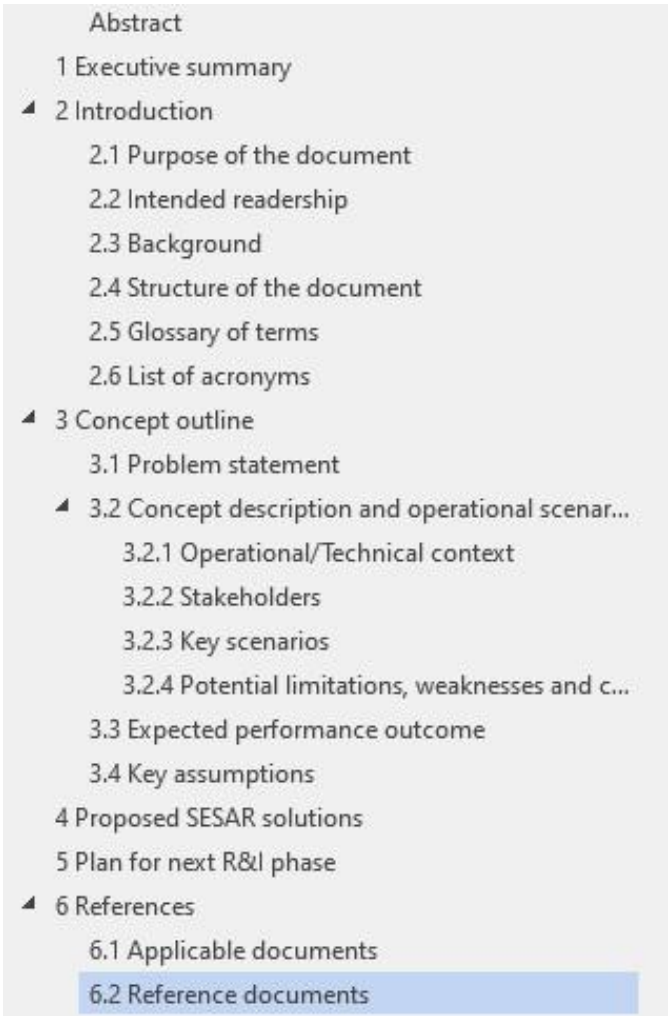

Figure 14. DES HE concept outline template for TRL1 - Table of Contents

6 Conclusions and Future Work

6.1 Conclusions

The aim of this document is to support an integrated approach, ensuring that new ATM solutions providing high automation are conceived and evolved with different levels of "**certification-readiness"** as a guiding criterion from the outset.

Again, it is important to underline and to avoid misunderstanding that on top of all remains the consideration that the **two processes analysed for potential harmonisation have distinct scopes and involve different responsibilities.** SESAR is tasked with ensuring the deployment of innovation while maintaining high standards of operational safety. However, the ultimate responsibility for safety lies with EASA.

In SESAR, safety is one of the key performance aspects to be ensured, but it also considers many others, if safety is preserved. For EASA, it is the primary objective, and all technical system performances are evaluated in relation to their impact on safety. Naturally, this is reflected in the differences observed across their subprocesses. However, by focusing on individual subprocesses and analysing them in detail, it becomes possible to obtain deeper insight into these difficulties and identify areas of alignment despite the overarching differences.

The comparative analysis between the EASA concept paper and the SESAR framework across the key subprocesses—operational concept, safety, security, ethics, and human factors (HF)—highlights distinct but complementary approaches, offering a strong foundation for future harmonization aimed at enabling the safe, secure, and trustworthy integration of AI/ML in ATM:

- **Operational Concept**: EASA emphasizes AI-user interaction, differentiated explainability, and automation classification, while SESAR adopts a wider system-level view, focusing on integration into the ATM architecture and producing structured operational models.
- **Safety**: EASA provides regulatory rigor and AI-specific safety guidance, whereas SESAR contributes operational tools and dual success/failure perspectives. Harmonization could standardize validation processes and reduce certification complexity.
- **Security**: EASA focuses on AI-related information security aligned to certification, while SESAR uses a broader TRL-based approach (SecRAM). Their shared risk-based philosophy supports integrated security across the system lifecycle.
- **Ethics**: EASA targets certification-oriented ethical assurance, using the ALTAI framework, while SESAR ensures ethical governance throughout research projects. Both support "ethics by design," but would benefit from more aviation-specific guidance.
- **Human Factors (HF)**: SESAR offers a mature, structured HF framework with clear guidance, TRL alignment, and practical tools. EASA, while focused on certification, lacks standardized HF assessment methods and AI-specific KPIs. Bridging this gap by integrating SESAR's methodological strength into EASA's compliance-driven process would improve consistency, traceability, and human-centric design assurance.

Based on the preliminary guidelines, a practical toolkit has been developed to actively support harmonisation activities. This toolkit includes several key components, such as gap analysis checklists, overlap mapping tools, a traceability matrix, and SESAR documentation templates.

To make the preliminary guidelines truly actionable, a structured step-by-step process is proposed, making use of the toolkit's key components:

- **Review of Applicable Regulatory Documents.**
- **Initial Gap and Overlap Analysis.**
- **Traceability Mapping.**
- **Use of SESAR Templates.**

This integrated approach aims to improve transparency, consistency, and mutual understanding between innovation development and regulatory compliance processes.

Overall, this preliminary analysis lays **a solid foundation for harmonizing SESAR and EASA processes**, focusing on solutions implementing a high level of automation. The preliminary guidelines developed represent an encouraging milestone, demonstrating that the harmonization process is capable of bringing significant benefits. Furthermore, the **defined methodological approach ensures the soundness and reliability of the analysis**, providing a robust basis for future work aimed at refining and implementing effective harmonization strategies.

6.2 Key findings

- ✓ **The sub-processes analysed are considered by both processes**
- ✓ **Terminology is in specific parts different**
- ✓ **AI and high automation is not managed explicitly in SESAR development process**
- ✓ **SESAR considers TRL and starts addressing LoA: a dual connection is required for harmonization**
- ✓ **Key overlaps consider the emphasis given to the sub-processes , the need of evidences and the need of means to achieve the sub-processed goals:**
- ✓ ***Evidences –*** *key deliverables in SESAR can be used as evidences to comply with set of EASA objectives*
- ✓ **Performance**
    - *In SESAR Safety is translated in actionable indicators to be measured – they can be used as the performance domain to which trace the system performance (AI performance indicator as required by EAA)*
    - *In SESAR, Human Performance (HP) is translated into a set of measurable indicators that can serve as a context for evaluating and analysing human-machine teaming. However, when considering high levels of automation, many additional aspects must also be taken into account.*
    - ***Methodologies -*** *adopted in SESAR can be analysed reviewed and considered as possible Means of Compliance for an objective/ a set of objectives*

6.3 Next Steps

Future work will reflect the progress in maturity of the Preliminary guidelines and Toolkit.

The presented guidelines have to move from preliminary to the guidelines that address the view of both the owners and the users of the processes.

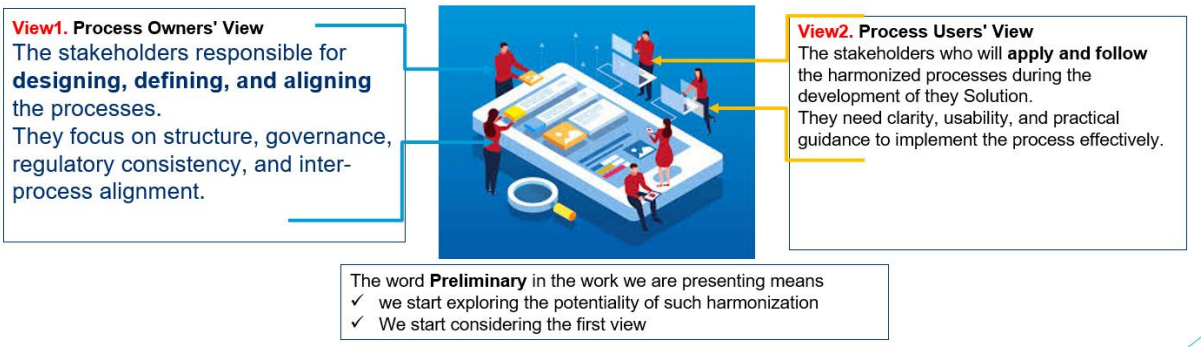

Figure 15: Next steps – Include as end-users the developers

Accordingly, the next steps should include:

- Refinement of the gap and overlap analysis of the identified SESAR sub-processes;
- Extension of the gap and overlap analysis to all the SESAR sub-processes;
- Extension of the gap and overlap analysis to cover the new objectives in the forthcoming update of the EASA concept paper;
- Identification of the actions required to implement the harmonization of SESAR processes with the EASA objectives for AI-based systems, along with their respective priorities;
- Extension of guidelines and toolkit to solution developers.

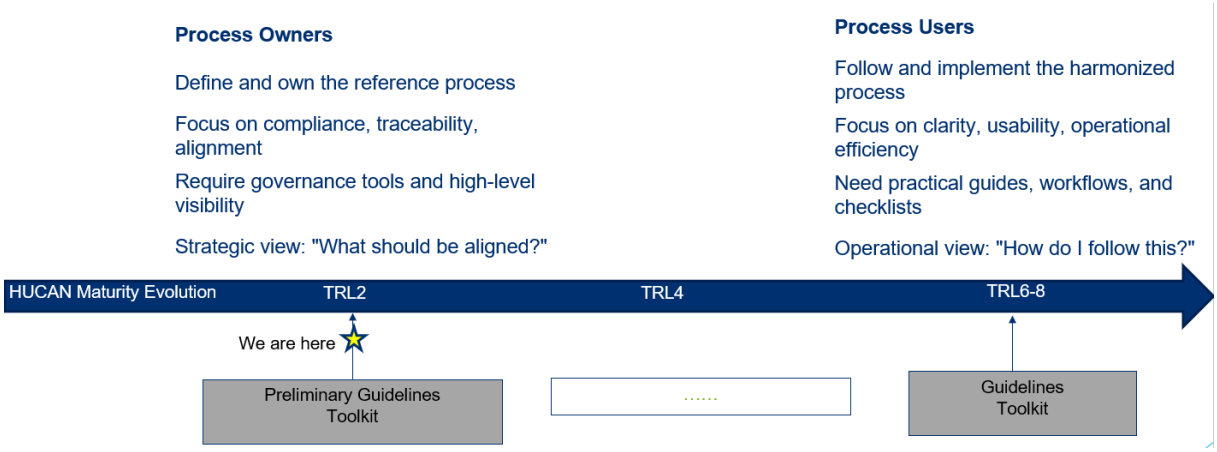

Figure 16: HUCAN maturity evolution

For example, the **gaps analysis could progress in maturity**. It is important to note that, at this stage, the gap analysis has been limited to identifying discrepancies between the SESAR framework and EASA concept paper sub-processes without assessing **the impact of these gaps, defining specific actions** to address them, or **prioritizing their resolution**. The checklist could be refined. A deeper evaluation will be conducted to quantify the effects of identified gaps, develop targeted harmonization measures, and establish priorities based on their significance and feasibility. It could be the case that may not be necessary, or possible, to bridge all gaps, due to the very different scopes. This future phase will be essential to translate the current findings into actionable strategies that effectively bridge the gaps and enhance process alignment. Similarly, **the overlap analysis** conducted so far has focused solely on identifying commonalities. It has not yet **explored in depth how these overlaps can be effectively leveraged** or formalized to maximize efficiency gains, nor has it addressed potential challenges that may arise when integrating shared elements. These aspects will also be examined in future work to develop practical recommendations for exploiting overlaps and fostering collaboration.

Additionally, a comparison between the SESAR maturity assessment process and EASA's expectations in terms of compliance verification has to be done. In SESAR, maturity assessment evaluates whether the solution implements the declared functionalities, demonstrating them through validation activities aligned with the relevant TRL and measured against expected performance in the intended operational environment. On the other hand, EASA focuses on ensuring that the system performs no unintended functions within its designated operational context and that it is validated according to its level of safety criticality. Comparing these two perspectives will be crucial to identifying how validation practices can serve both innovation maturity goals and regulatory compliance.

7 References

[1] EASA, Concept Paper: Guidance for Level 1 & 2 machine-learning applications, Issue 02, March 2024, https://www.easa.europa.eu/en/downloads/139504/en.

[2] COMMISSION REGULATION (EU) No 748/2012 of 3 August 2012 laying down implementing rules for the airworthiness and environmental certification of aircraft and related products, parts and appliances, as well as for the certification of design and production organisations. Document 32012R0748. https://eur-lex.europa.eu/eli/reg/2012/748/oj.

[3] EASA. ED Decision 2020/006/R. Aircraft cybersecurity. 01 Jul 2020. https://www.easa.europa.eu/en/document-library/agency-decisions/ed-decision-2020006r.

[4] COMMISSION DELEGATED REGULATION (EU) 2022/1645 of 14 July 2022 laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations covered by Commission Regulations (EU) No 748/2012 and (EU) No 139/2014 and amending Commission Regulations (EU) No 748/2012 and (EU) No 139/2014. Document 32022R1645. https://eur-lex.europa.eu/eli/reg_del/2022/1645/oj.

[5] COMMISSION IMPLEMENTING REGULATION (EU) 2023/203 of 27 October 2022 laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations covered by Commission Regulations (EU) No 1321/2014, (EU) No 965/2012, (EU) No 1178/2011, (EU) 2015/340, Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664, and for competent authorities covered by Commission Regulations (EU) No 748/2012, (EU) No 1321/2014, (EU) No 965/2012, (EU) No 1178/2011, (EU) 2015/340 and (EU) No 139/2014, Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664 and amending Commission Regulations (EU) No 1178/2011, (EU) No 748/2012, (EU) No 965/2012, (EU) No 139/2014, (EU) No 1321/2014, (EU) 2015/340, and Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664. Document 32023R0203. https://eur-lex.europa.eu/eli/reg_impl/2023/203/oj.

[6] Miriam le Fevre, Birgit Gölz, Ruben Flohr, Tim Stelkens-Kobsch, and Theo Verhoogt. 2017. SecRAM 2.0. Security Risk Assessment methodology for SESAR 2020. (Sept. 2017). https://www.SESARju.eu/sites/default/files/documents/transversal/SESAR%202020%20-%20Security%20Reference%20Material%20Guidance.pdf.

[7] ENISA, Securing Machine Learning Algorithms, December 2021.

[8] Q. Liu, P. Li, W. Zhao, W. Cai, S. Yu and V. C. M. Leung, "A Survey on Security Threats and Defensive Techniques of Machine Learning: A Data Driven View," in IEEE Access, vol. 6, pp. 12103-12117, 2018, doi: 10.1109/ACCESS.2018.2805680.

[9] EASA, AMC 20-42 Airworthiness information security risk assessment, https://www.easa.europa.eu/en/document-library/easy-access-rules/online-publications/easy-access-rules-acceptable-means?page=21.

[10]Microsoft. AI/ML Pivots to the Security Development Lifecycle Bug Bar. https://learn.microsoft.com/en-us/security/engineering/bug-bar-aiml.

[11]Microsoft. Threat Modeling AI/ML Systems and Dependencies. https://learn.microsoft.com/en-us/security/engineering/threat-modeling-aiml.

[12]Microsoft. Failure Modes in Machine Learning. https://learn.microsoft.com/en-us/security/engineering/failure-modes-in-machine-learning.

[13]MITRE. Adversarial ML Threat Matrix. https://github.com/mitre/advmlthreatmatrix/blob/master/pages/adversarial-ml-threat-matrix.md.

[14]SESAR JU (2025). European ATM Master Plan - Making Europe the most efficient and environmentally friendly sky to fly in the world. 12 December 2024. doi: 10.2829/9855255. https://www.SESARju.eu/sites/default/files/documents/reports/SESAR%20Master%20Plan%202025.pdf.

[15]EC, HLEG-AI. Assessment List for Trustworthy AI (ALTAI) for self-assessment. 17 July 2020. Document available at this link: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68342. Tool available on the ALTAI portal at this link: https://altai.insight-centre.org/.

[16]SESAR Safety Reference Material, EUROCONTROL, December 2018, https://www.SESARju.eu/sites/default/files/documents/transversal/SESAR2020%20Safety%20Reference%20Material%20Ed%2000_04_01_1%20(1_0).pdf

[17]Guidance to Apply SESAR Safety Reference Material, EUROCONTROL, December 2018, https://www.SESARju.eu/sites/default/files/documents/transversal/SESAR%202020%20-%20Guidance%20to%20Apply%20the%20SESAR2020%20Safety%20Reference%20Material.pdf

[18]SESAR 3 Joint Undertaking Project Handbook, April 2022, https://www.SESARju.eu/sites/default/files/documents/projects/SESAR3ProjectHandbook.pdf

[19]Horizon Europe ethics guidelines, O. Mongenie, SESAR, June 2024

[20]Ethics and Data Protection, EC, July 2021, https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-and-data-protection_he_en.pdf

[21]Ethics By Design and Ethics of Use Approaches for Artificial Intelligence, EC, Version 1.0, November 2021 https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-by-design-and-ethics-of-use-approaches-for-artificial-intelligence_he_en.pdf

[22]REGULATION (EU) 2021/695 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, April 2021, establishing Horizon Europe – the Framework Programme for Research and Innovation,

laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013

[23]EUROPEAN COMMISSION DIRECTORATE-GENERAL FOR MOBILITY AND TRANSPORT Directorate E – Aviation E.3 - Single European Sky, MODEL GRANT AGREEMENT (20XX)

[24]EUROPEAN COMMISSION, EU GRANTS, AGA Annotated Grant Agreement, EU Funding Programmes 2021-2027, Version 2.0, April, 2025, https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/guidance/aga_en.pdf#page=147.07

[25]Ethics By Design and Ethics of Use Approaches for Artificial Intelligence (version 1.0). p. 11. Figure 1. The 5-layer Model of Ethics by Design, The Development Process. EC (2021).

[26]European Commission: Directorate-General for Communications Networks, Content and Technology and High-Level Expert Group on AI, Ethics guidelines for trustworthy AI, Publications Office, 2019, https://data.europa.eu/doi/10.2759/346720

[27]Human Performance Assessment Process V1 to V3 - including VLD, PJ19 Cl, EUROCONTROL, January 2020, https://www.SESARju.eu/sites/default/files/documents/transversal/SESAR%202020%20-%20Human%20Performance%20Assessment%20Guidance.pdf

[28]Performance based requirements for advanced automation, Horizon, November 2024

[29]https://www.eurocontrol.int/publication/atfcm-users-manual

[30]https://www.eurocontrol.int/publication/ifps-users-manual

8 List of acronyms

Acronym	Description
AI	Artificial Intelligence
ALTAI	Assessment List for Trustworthy AI
AMC	Acceptable Means of Compliance
ATM	Air Traffic Management
CIA	Confidentiality, Integrity, Availability
CS	Certification Specification
DEMOR	Demonstration Report
DES	Digital European Sky
EASA	European Union Aviation Safety Agency
ENISA	European Union Agency for Cybersecurity
HF	Human Factors
ISO	International Organization for Standardization
IT	Information Technology
IUEI	Intentional Unauthorised Electronic Interaction
KPI	Key Performance Indicator
LOAT	Level of Automation Taxonomy
ML	Machine Learning
OD	Operational Design
ODD	Operational Design Domain
OSED	Operational Service and Environment Definition
OT	Operational Technology
PISRA	Product Information Security Risk Assessment
SecAP	Security Assessment Plan
SecRA	Security Risk Assessment
SecRAM	Security Risk Assessment Methodology
SESAR	Single European Sky ATM Research
SPR-INTEROP	Safety and Performance – Interoperability Requirements
TRL	Technology Readiness Level
TS-IRS	Technical Specifications – Interface Requirement Specification

Table 11. List of acronyms.

Appendix A Operational Concept Subprocess

A.1 Purpose and Objectives

EASA

The primary objective of the Operational Concept Analysis required in the EASA concept paper is to characterize the AI system from an operational perspective given by

- the list of end users intended to interact with the AI-based system
- the associated high-level tasks
- the AI-based system definition

The operational concept analysis is applicable to the AI-based system under development.

EASA operational concept analysis sub-process is not explicitly referred in the W life cycle process and could be mapped in subsystems requirements and design engineering activity that triggers life cycle.

Since it is defined by means of objectives that must be complied with, it ends when the objectives considered have been covered.

The table below reports the objectives addressed. They are considered applicable to each assurance level (AL), e.g. development assurance level (DAL) or software assurance level (SWAL).

Objectives	Assurance Level				
	AL 1 DAL A SWAL1	AL 2 DAL B -	AL 3 DAL C SWAL2	AL 4 - SWAL3	AL 5 DAL D SWAL4
CO-01: The applicant should identify the list of end users that are intended to interact with the AI-based system, together with end-user roles, responsibilities (including indication of the level of teaming with the AI-based system, i.e. none, cooperation, collaboration) and expected expertise (including assumptions made on the level of training, qualification and skills).	O	O	O	O	O
CO-02: For each end user, the applicant should identify which goals and associated high-level task(s) are intended to be performed in interaction with the AI-based system.	O	O	O	O	O
CO-03: The applicant should determine the AI-based system taking into account domain-specific definitions of 'system'.	O	O	O	O	O
CO-04: The applicant should define and document the ConOps for the AI-based system, including the task allocation pattern between the end user(s) and the AI-based system. A focus should be put on the definition of the OD and on the capture of specific operational limitations and assumptions.	O	O	O	O	O
CO-05: The applicant should document how end users' inputs are collected and accounted for in the development of the AI-based system.	O	O	O	O	O
CO-06: The applicant should perform a functional analysis of the system, as well as a functional decomposition and allocation down to the lower level.	O	O	O	O	O
CL-01: The applicant should classify the AI-based system, based on the levels presented in Table 2, with adequate justifications.	O	O	O	O	O

Figure 17. Risk-based levelling of objectives - Operational Concept Objectives

SESAR

The primary objective of the Operational Concept Analysis in SESAR is to define, refine, and validate the future operational scenarios that support the evolution of the ATM system by means of the system under development and describing the transition of the operations from the previous to the new operating method.

The operational concept analysis is applicable to the system under development named "ATM solution".

The Operational Concept Analysis sub-process typically represents the first phase of a project, initiated within the first six months and reviewed progressively through incremental steps over the project's duration.

The analysis is Assumptions based, is susceptible to change as the operational concept must adapt to feedback from validation activities, stakeholder input, and evolving policy.

A.2 Target Audience

In SESAR, the OSED must include sections dedicated to identifying stakeholders and their expectations. It is required to describe who the stakeholders are, how they are affected by the SESAR solution, what their current needs and problems are, and how the solution will help address them. The expectations of each stakeholder must also be described.

The Performance Assessment Report (PAR) is a part of the OSED that explicitly lists the target audience. This includes:

- Other members of the SESAR Project team.
- Performance experts at the cross-cutting areas level.
- ATM stakeholders, such as air navigation service providers (ANSPs), airport owners/operators, and airspace users.
- The SESAR JU. The main recipient in the performance management process is the cross-cutting performance project DES (i.e., PEARL), which will aggregate the results for annual monitoring and reporting to the SESAR 3 JU Governing Board.

Regarding EASA, the information contained in the ConOps is intended for various stakeholders for assessment, certification, and operational purposes.

The need for explainability of the behaviour of AI-based systems (including operational aspects) is driven by several role groups:

- Those involved in development (engineers, data scientists, etc.).
- Those involved in approval/certification (certification authorities, NSAs, etc.).
- Those who operate AI-based systems (flight crews, air traffic controllers (ATCOs), etc.). This group constitutes the end users.
- Those who analyse operations post-implementation (maintenance personnel, safety investigators).

The process of defining the ConOps and identifying end users (Objectives CO-01, CO-02, CO-04) applies to different assurance levels. EASA also requires considering and collecting input from end users in the development of the system, as well as considering the need for new skills and the risk of de-skilling for users and end users, mitigating this through training needs analysis and training.

The audience for the ConOps and the associated operational information in EASA therefore includes developers/applicants, regulatory and certification authorities, safety investigators, and the end users who will interact directly with the AI system.

Operational Concept Subprocess – Inputs – Key Differences
Item #1 – Target Audience
EASA – EASA focuses more specifically on end-users who interact directly with the proposed AI system and how they perform tasks in collaboration with it.
SESAR – SESAR has a broader focus on ATM stakeholders as a whole (ANSPs, airports, airspace users as entities) and their general expectations and benefits from the solution.

Operational Concept Subprocess – Inputs – Key Differences
Item #2 – Explainability
EASA – EASA explicitly distinguishes the need for different levels of explainability for end-users (simpler explanations on output) versus development/post-operation stakeholders (deeper transparency on the inner workings).
SESAR – SESAR sources do not detail a similar approach to customisation of OSED content based on different levels of expertise within its wider audience

Table 12. Key Differences for Operational Concept subprocess – Target Audience

Operational Concept Subprocess – Terminology and definitions – Overlaps
Item #1 – Target Audience
Both SESAR and EASA identify development/project team members and operational stakeholders as relevant audiences.
Both also consider the need for information from supervisory/regulatory bodies (SESAR JU, PEARL, EASA, certification authorities).

Table 13. Overlaps for Operational Concept subprocess – Target Audience

A.3 Scope

EASA

The operational concept analysis is completely determined by the following activities:

- Characterisation of the AI application,
- Concept of operations for the AI application,
- Functional analysis of the AI-based system,
- Classification of the AI application.

The scope of the EASA concept paper is the AI system.

The analysis of the operational concept for AI-based systems is guided by a series of interrelated activities that drive its development.

The first step is the characterization of the AI application, which is one of the initial elements for assessing trustworthiness in the system. This activity begins with the definition of the AI system; when necessary, the system is broken down into subsystems, some of which may also be AI-based. The objective is to obtain a clear characterization of the system from an operational perspective. At this stage, it is crucial to identify the end users who will interact with the system, defining their roles, responsibilities, and the expected level of collaboration with the AI system. The expected user experience, level of training, qualifications, and necessary skills are also taken into account. Finally, the main goals and tasks that each user will need to perform in interaction with the AI are identified.

After defining the system, the Concept of Operations (ConOps) for the AI application is developed. The purpose is to define and document the ConOps in detail, with particular focus on the task allocation model between the end user and the AI system. A key aspect of this activity is the definition of the Operational Design Domain (ODD), which serves as the reference framework for data monitoring

during operations and is a fundamental prerequisite for ensuring the quality of the datasets used during the learning phases. It is important to distinguish between the ODD defined at the system or subsystem level and that specific to the AI/ML constituents (AI/ML constituent ODD). The ConOps also includes specific operational limitations and assumptions, as well as identified risks, their mitigations, and any applicable constraints and conditions on the system. The described operational scenarios cover not only nominal cases but also degraded modes, that is, situations where the AI system does not function as intended. The ConOps is described at the product or system level, ensuring a comprehensive view of the expected operations.

In parallel with the ConOps definition, the functional analysis of the AI system is carried out. This phase involves the breakdown and functional allocation of the identified activities, down to the most detailed level. It starts with the identification of the main functions, which are then broken down into sub-functions and assigned to subsystems, AI/ML components, and other elements, following the established architectural choices.

The activities of characterization, ConOps definition, and functional analysis provide the necessary elements for the final phase, namely the classification of the AI application. The objective of this phase is to enable the applicant to classify the system based on the levels defined by EASA. The EASA concept paper focuses particularly on Levels 1 and 2. Level 1 concerns systems that provide informational support, where decisions and actions remain under the exclusive control of the end user, such as a system that merely provides data without operational recommendations. Level 2, on the other hand, includes systems that can autonomously select and implement actions, while still allowing for end-user supervision and override capability. In this case, decisions can be made by both the AI and the user. The classification must always consider the system as a whole and the main tasks assigned to the end users. This is an essential input for the development process, as it allows the guidance objectives to be calibrated according to the AI level and the degree of criticality or assurance required.

SESAR

The operational concept analysis is completely determined by:

- Identification of user needs,
- Definition of the End user and system interactions
- Collection and Analysis of the stakeholder expectations,
- Identification of measurable performance benefits across safety, capacity, efficiency, environment, and cost-effectiveness.

The scope of the operational concept of SESAR is the solution. It can include the AI system, but it is not limited to it.

The analysis of operational concepts is entirely determined by a series of processes described in the SESAR 3 Project Handbook.

Regarding the identification of user needs, the OSED (Operational Services and Environment Definition) is one of the key deliverables; its purpose is to describe the specific activities and interactions of the various stakeholders in relation to a new operational concept. This process necessarily involves identifying and understanding the needs of end users and stakeholders involved. In detail, the OSED for Solution with a TRL from 4, is completely determined by detailed operational environments, detailed operating method, safety performance and inter-operability requirements.

Detailed operational environment

The operational environment topic aims to describe the contextual elements external to the solution in order to get knowledge of the fundamental operational characteristics that govern the set of safety performance and interoperability requirements included in the related topic. It includes at least the following aspects to be fixed:

- **Traffic**
- **Airspace or Airport characteristics**
- **Roles and responsibilities of the end user**
  This point triggers the human factor aspects considered essential for the safe and coherent operation of the Operational Service, particularly in reference to partial implementations, mixed equipage, etc.
- **CNS/ATM**
  It describes the fundamental CNS/ATM services that are part of the context where the set of requirements will be consolidated i.e. CNS airborne-ground technology, other parts of the ATM system that are assumed to be in place when the SESAR solution will be deployed, etc. In particular, this section shall describe the assumptions in terms of CNS infrastructure for the SESAR solution to be deployed.
- **Applicable standards and regulations**

Detailed operating method

1. **Contextual Architecture**

It gives the operational view of the solution in ATM architecture considering the formalism of NATO Architecture Framework (NAF).

At the operational level the NOV-2 and NOV-5 diagrams must be designed. The NOV-2 diagram describes the information exchange between operational nodes. It focuses on who communicates with whom, what they communicate, and how often — but at an abstract, operational level (not technical).

It answers:

- *What are the operational elements (nodes)?*
- *What information is exchanged between them?*
- *How is the connectivity structured between nodes?*

The NOV-5 diagram defines and describes the operational activities that are performed within the architecture. It shows what work needs to be done, by which operational nodes, and how those activities relate to each other.

The operational nodes, the users and the activities are elements defined in ATM architecture.

Furthermore, such topic includes the analysis of enabling elements for the solution. They could be developed by the solution itself, or in other contexts or simply required. Such elements contribute to set up the envelope of the solution when in operation.

2. **Use cases**

The detailed operating method describes the previous operating method and the new one and the formalism suggested in the use cases. This topic shall be filled in incrementally, along the solution development up to TRL6 (TRL7 for fast track and innovation uptake solutions), with increasing refinement and consolidation. It shall further develop the operational concept aspects related to the scope of the SESAR solution introduced in section 3.3.

3. Safety performance and interoperability requirements

This chapter shall be filled in incrementally, along the solution development up to TRL6 (TRL7 for fast track and innovation uptake solutions), with increasing refinement and consolidation.

Requirements shall be developed according to the SESAR requirements and validation guidelines, available in the programme library.

This chapter should be structured based on the specific needs of each SESAR solution. As best practice, it is recommended to include the following sections:

- Operational requirements.
- Safety requirements.
- Performance requirements.
- Interoperability requirements.

Benefit

Finally, the identification of measurable performance benefits in terms of safety, capacity, efficiency, environment, and cost-effectiveness is a central aspect of the solution that must be deployed when the expected benefits for the stakeholders are clear.

Key Differences – Overlaps

- Characterisation of the AI application,
- Concept of operations for the AI application,
- Functional analysis of the AI-based system, Classification of the AI application.

Operational Concept Subprocess – Scope – Key Differences
Item #1 – Operational Scope **EASA –**EASA addresses the operational scope as characterization of the AI application and definition of the definition of the Operational Design Domain (ODD), which serves as the reference framework for data monitoring during operations and is a fundamental prerequisite for ensuring the quality of the datasets used during the learning phases. **SESAR –** SESAR requires the definition of the operational environment in precise terms as the external context of the solution in order to completely address the operational envelope of the solution. SESAR requires a clear contextualization of the solution within ATM architecture. **Note –** SESAR doesn't require a specific analysis of the parameters representing the context on which AI will reason upon to support human that could be the link between them and the operational characteristic given at high level. SESAR doesn't require a functional analysis.
Item #2 – Solution and System The scope of the EASA concept paper is the AI system, whereas the scope of the operational concept of SESAR is the solution. It can include the AI system, but it is not limited to it.
Item #3 – Level of Automation **EASA –**EASA requires a classification in terms of Level of Automation **SESAR –** SESAR OSED doesn't require information on the level of Automation **.** They could potentially be included in the use cases description but neither a formal justification is required nor a tailoring of specific argument to be provided is set-up.

Table 14. Key differences for Operational Concept subprocess – Scope.

Operational Concept – Scope – Overlaps
Item #1 – Concept of operations Both EASA and SESAR consider the specification how the system will be operated by the end-user. SESAR asks in detail elements of roles and responsibilities of the end users that may change by means of use cases formalism. EASA requires an analysis of task allocation.

Table 15. Overlaps for Operational Concept subprocess – Scope.

A.4 Terminology and Definitions

Within the SESAR framework, the operational concept is a fundamental element in the definition and assessment of a "SESAR Solution". It is described in detail in the Operational Service and Environment Definition (OSED). The purpose of the OSED is to describe the operational service and environment, specific activities, involved actors, roles and responsibilities, new and previous operating method, stakeholders impacted by the solution, benefit impact mechanism (BIM) for the impacted stakeholders. In SESAR, the solution is not just the system. In the context of the EASA guidelines on the application of machine learning (ML) in aviation, the operational concept is mainly addressed through the term "Concept of Operations (ConOps)". The ConOps is defined as a human-centric document that

describes the operational scenarios for a proposed system from the users' operational perspective. It is expected to be detailed and well-documented to support compliance with AI reliability objectives. EASA, with its focus on AI/ML, places particular emphasis on the task allocation model between humans and AI within the ConOps, and introduces the more formalized concepts of Operational Domain (OD) and Operational Design Domain (ODD) to define the operational conditions relevant to the reliability of AI-based systems, including aspects related to training and operational data. Conversely, SESAR defines the operational environment in broader terms within the OSED.

A fundamental aspect is the definition of the Operational Environment (OE). It is necessary to consider operational characteristics and the detailed environment. The context in which the change will be implemented and used, in terms of key properties of the operational environment relevant for safety and performance assessments, must be described. Both EASA and SESAR recognize the need to define and understand the environment and conditions in which a new solution or system will operate. EASA, in the context of AI/ML, formalizes the concept of operational environment through the OD and ODD, explicitly linking them to the operational conditions relevant to AI reliability and to data. SESAR uses the concept of operational environment (OE) more broadly to describe the overall operational context relevant to the ATM/ANS solution.

In SESAR, the OSED describes the interactions among various stakeholders. The operational method includes a description of the actors (operators and automated actions). Safety assessments consider the impacted ATM actors. Performance assessments take into account the benefits for service users (e.g., ATS providers, aviation undertakings), including human actors. Regarding EASA, the ConOps is a human-centric document and describes scenarios from the users' operational point of view. It includes a list of potential end users. The focus is on the description of interaction and task allocation between end users and the AI-based system. Operational explainability is intended for the crew and other users.

Operational Concept Subprocess – Terminology and definitions – Key Differences
Item #1 – Operational Concept
EASA – EASA focuses on AI/ML and places special emphasis on the task allocation model between humans and AI within ConOps, and introduces the more formalised concepts of OD and ODD to define the operational conditions relevant to the reliability of AI-based systems
SESAR – SESAR uses specific definition for the operating and sub-operating environment. Furthermore, SESAR addresses the definition of the operational environment, more generally within OSED.
Item #2 – End users
EASA – EASA uses the concept of task allocation to address the interaction between AI and end users.
SESAR – SESAR uses the terms roles and responsibilities to understand how the end users are changing their work.

Table 16. Key differences for Operational Concept subprocess – Terminology and definitions.

Operational Concept Subprocess – Terminology and definitions – Overlaps
Item #1 – Operational Concept Definition of 'How to Operate': both EASA and SESAR use a concept (Operational concept/OSED in SESAR, ConOps in EASA) to describe how a new system or solution will be used in practice, involving users/actors, activities and the environment.

Table 17. Overlaps for Operational Concept subprocess – Terminology and definitions.

A.5 Inputs

To define the operational concept of a system—whether it is the ConOps for EASA or the OSED for SESAR—it is essential to start from a clear understanding of the operational context, the actors involved, and the operational needs. These elements serve as critical inputs for describing what the system is expected to do from an operational perspective.

In the EASA framework, the development of a ConOps for an AI-based system requires the definition of the Operational Design Domain (OD). Furthermore, it is necessary to gather and consider input from end users throughout the system development process. This involves consultation with human performance experts and end-user representatives to understand their tasks, how these tasks will be impacted by the AI system, and how the system should be designed to support these tasks safely. These inputs are then translated into system requirements. The definition of the ConOps and OD provides the foundation for the subsequent capture of requirements (operational, non-functional, and interface) allocated to the AI/ML component, as well as for defining the parameters of the Operational Design Domain of the AI/ML constituent (ODD), and tracing them to the corresponding parameters of the OD.

The development of the OSED requires a description of the operational service and its environment, including the characteristics of the applicable operational environment (e.g., traffic characteristics, airspace or airport features). It is crucial to identify the stakeholders involved in the use of operational activities and define their attributes: roles, business functions, and responsibilities. The OSED must address the following aspects:

- A description of the detailed operational method, including procedures and information flows, often formalized through use cases.
- The identification of the Essential Operational Changes (EOC) to which the solution contributes.
- Dependencies on other solutions/enablers, and the consideration of applicable standards and regulations (as well as the identification of new needs).
- The expected benefits for stakeholders, making use of Benefit Impact Mechanisms (BIM).

Operational Concept Subprocess – Inputs – Overlaps
Item #1 – Operational context and Stakeholders Both EASA and SESAR, provide for the need to clearly define the operational context in which the system is to operate, referred to as Operational Domain (OD) in the case of EASA and Operational Environment (OE) in the case of SESAR. In addition, both frameworks place great importance on identifying the users or stakeholders involved, paying particular attention to defining their roles and respective responsibilities.
Item #2 – Stakeholders participation In both EASA and SESAR, direct input from users and stakeholders within the development process is considered essential to guide system design and implementation.

Table 18. Overlaps for Operational Concept subprocess – Inputs.

A.6 Outcomes

In the EASA context, the ConOps is a fundamental starting point for a series of development and assurance activities. The main outcomes of the Operational Concept subprocess are mostly a series of documents, such as:

- The document that defines and describes the Concept of Operations (ConOps) for the AI-based system, addressing the following documentation:
    - The detailed documentation of the identified end users, including their roles, responsibilities (including the level of collaboration with the AI system), and the expected expertise (as well as assumptions regarding their training, qualification, and competencies).
    - The documentation of the high-level goals and tasks that each end user intends to perform in interaction with the AI-based system.
    - The documentation of the task allocation scheme between the end users and the AI-based system.
    - The definition and documentation of the Operational Design Domain (ODD) of the AI-based system.
    - The documentation of specific operational limitations and assumptions.
    - The documentation of the functional analysis of the system, including its decomposition and functional allocation to lower levels.
    - A documented description of the system and its subsystems, identifying inputs, outputs, and functions. This also includes the documentation of the system/subsystem architecture as a reference for safety and learning assessments.
    - The documentation of how input from end users was collected and considered during the development of the AI system.

In SESAR, the main outcome related to the operational concept is represented by the SPR-INTEROP/OSED document, which includes:

- A documented description of the service and the operational environment, including stakeholder activities and interactions.

- A description of the SESAR solution and its enabling elements.
- The identification of any dependencies on other SESAR solutions.
- A description of the applicable operational environments, including traffic, airspace, or airport characteristics.
- The identification and description of the roles and responsibilities of the actors.
- A description of the operational method, including procedures, inputs/outputs, actor actions, service sequences, and additional functionalities.
- Documented use cases, for both nominal and non-nominal situations, including process models.
- The architectures of the business functions of the services.

Operational Concept Subprocess – Outcomes – Key Differences
Item #1 – Operational models documentation
SESAR – SESAR explicitly requires the production of specific documented operational models, such as the operational interaction model and the activity model.
EASA – EASA requires a functional analysis but does not specify these types of operational models as direct outputs of the ConOps process.

Table 19. Key differences for Operational Concept subprocess – Outcomes.

A.7 Assessment Methodology

Not applicable.

A.8 Performance Indicators

EASA does not explicitly describe criteria or metrics to assess the quality or completeness of the document or the definition of the operational concept, but rather uses metrics and criteria to assess the performance and safety of the AI/ML system operating within the context defined by ConOps.

SESAR does not have direct criteria or metrics to evaluate the OSED description but has a process and document structure in which the validation of the performance and safety of the operational solution described in the OSED is carried out using an extended set of metrics (KPI/PI) and criteria (Safety Criteria, SAC), comparing the results with targets (Estimated Performance Contributions, EPCs) to demonstrate success and justify the requirements derived from the operational concept. This assessment of performance and safety is intrinsically linked to OSED, as it evaluates the solution in the operational context defined by it.

A.9 Support and Resources

In order to develop the Concept of Operations, several sources are referenced.

In SESAR, for example, *Guidance J.3.1 of the E-SRM* is cited as a reference for the "behavioural operational representation" (functional process diagrams and information flows). This representation serves as a way to describe the "operational method", which is a key element in the definition of the OSED.

In EASA, several manuals and standards are referenced:

- Regulation (EU) 2017/373: provides definitions of functional systems and performance requirements for ATM/ANS service providers, establishing the regulatory framework within which the Concept of Operations must be developed.
- ED-79A/ARP-4754A: an aircraft system definition standard, useful for describing the aircraft system architecture that supports the Concept of Operations, but not the concept itself.
- EUROCONTROL ATFCM Users Manual [29] and IFPS Users Manual [30]: manuals describing existing procedures and systems, useful for defining the reference scenario or the operational environment within the Concept of Operations.

Appendix B Safety Subprocess Analysis

B.1 Purpose and Objectives

EASA

The EASA Concept Paper Issue 02 [1] aims to guide applicants when introducing AI/ML technologies into systems intended for use in safety-related applications in all domains covered by the EASA Basic Regulation (Regulation (EU) 2018/1139).

The objective of the EASA safety assessment process is to demonstrate that an aviation system achieves an acceptable level of safety as defined in the applicable regulations. This is achieved by ensuring that a fundamental inverse relationship exists: the higher the potential severity of a failure's effect, the lower its probability of occurrence must be. Acknowledging the predictability and uncertainty challenges of complex ML applications, the guidance aims to ensure AI/ML systems are demonstrably at least as safe as traditional counterparts. The fundamental requirement is that introducing AI/ML technology must not increase risk compared to an equivalent traditional system.

Moreover, the concept paper recognizes that achieving and maintaining an adequate safety level throughout the product life cycle necessitates a two-pronged approach. Firstly, it calls for an *initial safety assessment* during development, which must evaluate the AI/ML component's contribution to potential system failures and include specific AI-related architectural considerations. Secondly, the paper emphasizes the need for *continuous safety assessment* post-deployment, involving a data-driven safety risk analysis using operational data and occurrences. It notes that this continuous monitoring may adapt existing in-service processes, but these must be modified for AI. The paper further acknowledges that the specific activities and documentation needed for EASA approval vary significantly by domain. Table 21 , adapted from EASA's concept paper, outlines expected analyses for different applications embedding AI/ML. Note that Annex 1 of EASA's concept paper provides a more detailed overview of the anticipated impact on regulations and MOC for the domains.

Aviation domains	'Initial' safety assessment	'Continuous' safety assessment
Initial and continuing airworthiness	Impact on safety assessment methodologies (functional hazard assessment in the context of the ConOps, Safety assessment activities supporting design and validation phases, and verification phase) Impact on safety support assessment (for embedded systems ED-79B/ARP4754B and ARP4761 may be used with adaptation)	To ensure continuing airworthiness of the type design are required by Part 21 [2] . Such activities consist mainly in the following steps: 21.A.3A(a, b, c), 21.A.3B(b), 21.A.3B(d)(3, 4) 21.A.3B(b)) and Provision ORG-03

Co-funded by the European Union

Air operations	An AI-specific risk assessment process is intended to be developed (not having guidance on initial safety assessment) through RMT.0742 to support Objective SA-01 and anticipated MOC	As per Section C.2.2.4 'continuous safety assessment' and Provision ORG-03
ATM/ANS	For ATS providers: • ATS.OR.205 Safety assessment and assurance of changes to the functional system • ATS.OR.210 Safety criteria For non-ATS providers: • ATM/ANS.OR.C.005 Safety support assessment and assurance of changes to the functional system. Regulation (EU) 2017/373 that addresses ATS and non-ATS providers has introduced the need of a 'safety support assessment' for non-ATS providers rather than a 'safety assessment'. The objective of the safety support assessment is to demonstrate that, after the implementation of the change, the functional system will behave as specified and will continue to behave only as specified in the specified context. For these reasons, a dedicated Section C.2.2.2.2 has been created for non-ATS providers.	ATS providers shall continue to meet the safety criteria (ATS.OR.205(b)(6)) Non-ATS providers shall meet ATM/ANS.OR.C.005(b)(2) For both ATS providers and non-ATS providers: The monitoring criteria are then used as means to monitor the safety performance in the operations (AMC2 ATM/ANS.OR.B.005(a)(3) with their associated GM like e.g. GM1 ATM/ANS.OR.B.005(a)(3)). Provision ORG-03 For ATS the 'Safety performance monitoring and measurement' and 'Performance monitoring and measurement' for non-ATS providers.
Maintenance	An AI-specific risk assessment process is intended to be developed through RMT.0742 to support Objective SA-01 and anticipated MOC. Whenever new equipment is used, it should be qualified and calibrated.	As per Section C.2.2.4 'continuous safety assessment' and Provision ORG-03

Training	An AI-specific risk assessment process is intended to be developed through RMT.0742 to support Objective SA-01 and anticipated MOC developed in Section C.2.2.3. The entry into service period should foresee an overlapping time to enable validation of safe and appropriate performance	Managed from an organisation, operations and negative training, as per Section C.2.2.4 'continuous safety assessment' and Provision ORG-03
Aerodromes	An AI-specific risk assessment process is intended to be developed (not having guidance on initial safety assessment) through RMT.0742 to support Objective SA-01 and anticipated MOC	As per Section C.2.2.4 'continuous safety assessment' and Provision ORG-03
Environmental protection	The demonstration of compliance with the applicable environmental protection requirements	Currently not applicable

Table 20. Comparison between 'Initial' and 'Continuous' safety assessments in Aviation domains

Note: In the EASA Artificial Intelligence (AI) Concept Paper Issue 02, Provision ORG-03 advises organizations to implement a data-driven 'AI continuous safety assessment' process based on operational data and in-service events. This process aims to ensure the ongoing safety and reliability of AI-based systems throughout their operational life.

SESAR

The SESAR safety assessment framework [16][17][18] introduces a dual approach to evaluating changes in the ATM/ANS system: the *success approach* and the *failure approach*. The success approach evaluates how a new concept or technology, when functioning as intended, contributes positively to aviation safety—essentially assessing how pre-existing aviation risks are reduced. The failure approach, on the other hand, examines risks introduced by the potential failure of the ATM/ANS changes, focusing on negative contributions to safety.

Central to this methodology is the Accident Incident Model (AIM), which informs the success and failure based safety assessment and it does not replace the safety assessment. AIM provides accident-type-specific models using historical accident and incident data to define Safety Criteria across operational hierarchies and flight phases, helping identify how operational changes affect safety. These criteria are then developed and refined through the SESAR solution lifecycle—from early validation to system refinement.

The SESAR Safety Risk Management (SRM) process is embedded into the solution development lifecycle through three phases:

V1: Safety Criteria (SAC) are derived from AIM analysis and outlined in the Safety Plan.

V2: Safety Objectives (SOs) and initial Safety Requirements (SRs) are developed—SOs define what needs to occur to meet the SAC (success approach), while SRs ensure those objectives are technically achievable, also including tolerable failure thresholds from operational hazard analysis (failure approach). The Safety Requirements (from the failure approach) are derived as a result of the application of the PSSA equivalent activities.

V3: Refines the Safety Requirements further in line with the evolving system design (e.g. lower level human tasks, technical systems, functional blocks, functions and services etc.). All safety elements must be traceable to the original SAC, and feasibility must be assessed.

The relationship between the key SESAR formal deliverables and the Safety Requirements is represented in Figure 12, which provides a top-level view of the System Engineering/development process which is an iterative one.

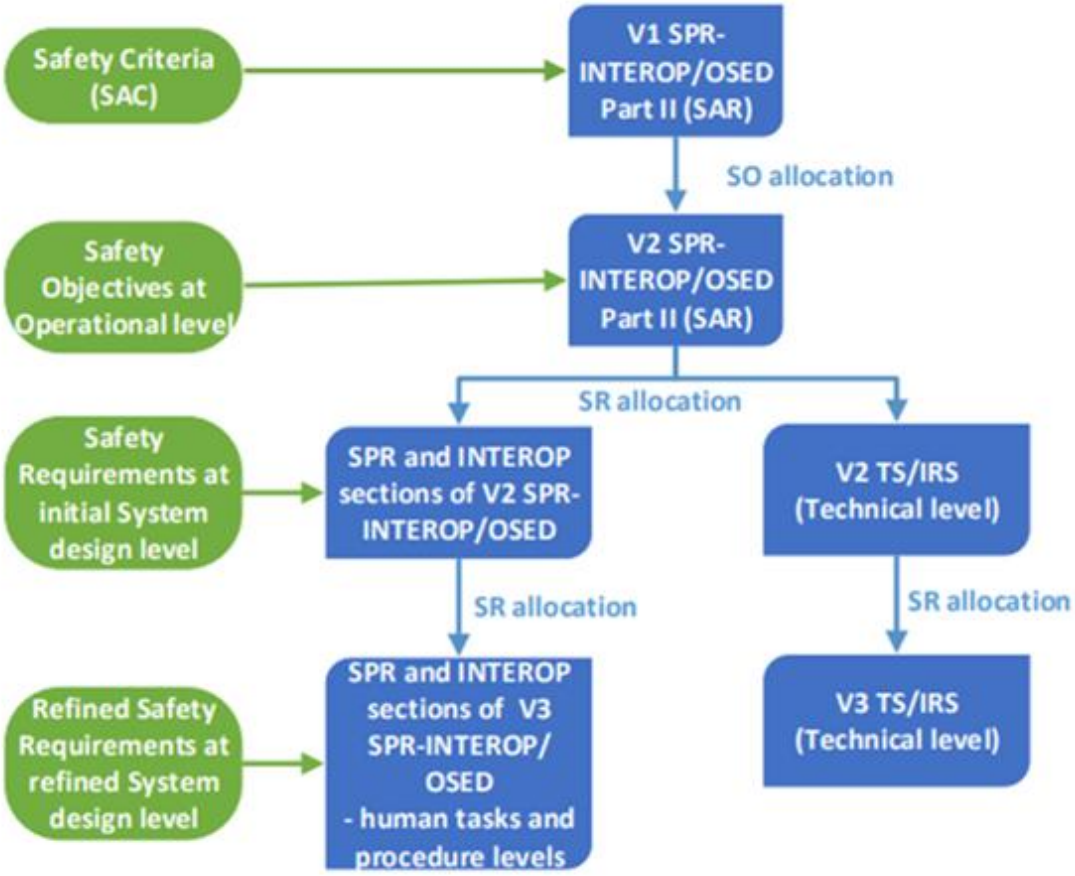

Figure 18. Safety Requirements and the Solution SPR-INTEROP/OSED and TS/IRS

The safety assessment must cover all foreseeable conditions, both normal and abnormal, and provide traceable justification through deliverables such as SPR-INTEROP/OSED and TS documents. Safety Objectives are operationally oriented ("what must happen"), while Safety Requirements are system-design oriented ("how it must be achieved").

Additionally, safety planning activities must define the operational environment, identify inherent aviation hazards, and specify the operational services affected. A Safety Plan Template guides teams in defining assurance activities. Though SESAR focuses on system-wide ATM safety, it may integrate detailed standards like ARP4754B when airborne systems are involved—ensuring compatibility between system-level and subsystem-level safety requirements.

The overarching safety goal of SESAR is to ensure no increase in the expected annual number of fatal accidents with ATM contribution, even as airspace and airport capacity increase.

Key Differences – Overlaps

Safety Assessment – Purpose and Objectives – Key Differences
Item #1 – Purpose of safety assessment framework **EASA –** Establishes a safety assessment framework specifically aimed at ensuring that AI/ML-based aviation systems are at least as safe as their traditional counterparts. Its main purpose is regulatory: to demonstrate that the introduction of AI does not increase risk within safety-critical aviation domains. **SESAR –** Designed to guide the safe development and integration of innovative ATM/ANS concepts and technologies into the aviation system. Its purpose is broader and more strategic, focusing not only on preventing added risk but also on ensuring that future ATM/ANS solutions positively contribute to overall system safety. **Note –** While both frameworks aim to ensure aviation safety, the EASA AI approach is more focused on regulatory assurance for AI systems, emphasizing risk neutrality and lifecycle monitoring, whereas the SESAR framework supports strategic safety gains across the ATM system, embedding safety assessment throughout the iterative development of new solutions.
Item #2 –Risk levels **EASA –** The paper does not define new risk levels specifically for AI but builds on existing aviation safety assessment practices, such as those in ARP4754B and ARP4761, where risk levels are typically expressed in terms of Failure Conditions (e.g., Minor, Major, Hazardous, Catastrophic) and their associated acceptable probabilities. **SESAR –** The failure approach involves Operational Hazard Assessment (OHA) and Functional Hazard Assessment (FHA), which classify the severity of hazards and assign maximum acceptable frequencies (i.e., risk levels). The AIM (Accident Incident Model) also supports risk classification by mapping SESAR Solutions to historical accident types, helping identify which types of failures or deviations would carry significant risk. **Note –** The EASA paper uses existing aviation safety risk levels (severity/probability), but with a focus on ensuring AI doesn't increase risk. No new classification scheme introduced. Whereas SESAR defines and applies explicit risk levels through Safety Criteria, derived from accident models and quantitative assessments, assigning maximum acceptable frequencies for different types of failures.

Item #3 – Approach for Safety Assessment

EASA – Proposes a two-tiered safety assessment approach tailored to the unique characteristics of AI—first, an initial safety assessment is conducted during development to analyse AI-specific risks, and second, a continuous safety assessment is required throughout the operational life of the system, focusing on data-driven monitoring and adaptation of in-service processes. This approach reflects the unique characteristics of AI, such as unpredictability and data dependency. The framework further refines this approach depending on the AI system's domain of application, providing specific guidance for both the initial and continuous safety assessment phases.

SESAR – Uses a dual perspective: a "success" approach assesses the safety benefits when systems function as intended, while a "failure" approach evaluates risks introduced by potential malfunctions. The framework is tightly integrated into SESAR's R&D lifecycle, from early validation to refined system design, where Safety Criteria evolve into operational Safety Objectives and eventually into specific Safety Requirements.

Note – EASA treats safety as a lifecycle responsibility, where the introduction of AI demands both a proactive assessment during design and an ongoing oversight once deployed. Its approach reflects the regulatory mindset: domain-specific, risk-averse, and focused on ensuring AI does not degrade existing safety levels. The structure separates responsibilities by aviation domains, acknowledging that AI's impact and the applicable regulatory frameworks differ between domains. On the other hand, SESAR's safety assessment is rooted in innovation-driven system evolution. It frames safety as both an opportunity and a risk — aiming not just to preserve safety but to enhance it through operational improvements. SESAR's approach is more function-oriented than domain-bound, integrating safety thinking into the entire research and design pipeline.

Item #4 – Impact areas

EASA – Safety assessment focuses on regulatory domains and how AI affects compliance and operational safety across them (Airworthiness, Air Operations, ATM/ANS, Maintenance and Training, Aerodromes etc.)

SESAR – SESAR focuses on the functional and operational transformation of the ATM system (ATM/ANS, Operational Environment, Human-in-the-loop systems e.g. ATCOs, pilots, Phases of Flight)

Note – SESAR does not differentiate its safety assessment approach by aviation domains (like EASA does); instead, it applies a system-wide ATM/ANS focus, treating the air traffic management environment as a whole. While this "system-wide" perspective suggests a comprehensive scope, it could also be argued that SESAR's approach is, in another sense, narrower than EASA's overall remit, as it "only" concerns ATM systems rather than the full spectrum of aviation domains. The assessment is structured around operational changes, not domain-specific boundaries, and is supported by the Accident Incident Model (AIM) to ensure consistency across different SESAR Solutions.

SESAR targets system transformation and performance-driven safety gains

Item #5 – Objectives vs TRL
EASA – EASA doesn't certify "experimental" technologies in the sense of TRLs. They certify products that are ready and proven for operational use.
SESAR – System Maturity (TRL): As solutions evolve from concept to deployment, safety requirements become more detailed and technically grounded.
Note – EASA's safety assessment framework does not use TRLs like SESAR does. Instead, it follows a development-assurance approach rooted in aviation standards (V-model) (e.g., ARP4754, DO-178C for software, DO-254 for hardware), which define the development and verification processes for airborne systems. In contrast, SESAR ties its safety assurance process to TRLs — as part of its R&D lifecycle — where safety assessments evolve in depth and detail as the system matures (from V1 to V3 phases). To conclude, while SESAR links safety with system maturity, EASA focuses on systematic assurance regardless of TRL, based on function-criticality and compliance with certification standards.

Table 21. Key Differences for Safety Assessment subprocess - Purpose and Objectives

Safety Assessment – Purpose and Objectives – Overlaps
Item #1 – Objectives related to Safety Assessment
Note – Both EASA's Functional Hazard Assessment (FHA) and SESAR's Safety Assessment share a common failure-focused approach when it comes to identifying, analysing, and mitigating risks associated with system failures.

Table 22. Overlaps for Safety Assessment – Purpose and Objectives

B.2 Target Audience

EASA

The target audience of the guidance are the applicants in demonstrating that systems embedding AI/ML constituents operate at least as safely as traditional systems developed. In this respect, this guidance should benefit all aviation stakeholders, end users, applicants, certification or approval authorities. Note: the term "applicant" is not further explained.

SESAR

SESAR aims mainly at safety practitioners in R&I and VLD projects of SESAR 2020.

The intended audience also includes SESAR JU and SJU members, SESAR 2020 Transversal Area and Master Plan projects, National Supervisory Authorities (NSAs) as well as EASA within the scope of the rulemaking activities in the field of aerodromes, air traffic management and air navigation services.

Key Differences – Overlaps

Safety Subprocess – Target Audience – Key Differences
Item #1 – Main goal of the target audience
EASA – The target audience is defined broadly as the applicants who need to demonstrate the safety of the ML/AI system they propose. They are supposed to get guidance from the document in how to ensure overall safety of the system.
SESAR – The target audience constitutes the safety experts who are expected to carry out the safety studies and safety assessments. These are closely related to the system developers.
Note – EASA describes in more general terms the need and processes to carry out for safety; SESAR provides more details on the safety assessment itself.

Table 23. Key differences for safety subprocess – Target Audience

Safety Subprocess – Target Audience – Overlaps
Item #1 – Safety Expertise
Both target audiences will require significant knowledge on safety aspects of ML/AI systems.

Table 24. Overlaps for safety subprocess – Target Audience

B.3 Scope

EASA

The scope of the EASA safety process covers all aviation systems in the development and deployment phases. This includes ATM/ANS systems, on-board systems, on-ground support systems, maintenance and training.

The main activities recommended by EASA are set up through a series of phases.

During the *development phase*, the main activities are

- Perform functional hazard assessment in the context of the ConOps
- Safety assessment activities supporting design and validation phases

Next, in the verification phase,

- Perform the final safety assessment
- Consolidate the safety assessment to verify that the implementation satisfies the safety objectives

The applicant should perform a safety (support) assessment for all AI-based (sub)systems, identifying and addressing specificities introduced by AI/ML usage.

In the airworthiness domain, activities to ensure continuing airworthiness of the type design are required by Part 21 and follow the steps described there. To ensure safe operations of AI-based systems, the applicant should identify which data needs to be recorded for the purpose of supporting the continuous safety assessment. For this, metrics, target values, thresholds and evaluation periods to guarantee that design assumptions hold, should be defined.

SESAR

The scope of the SESAR safety process covers ATM/ANS systems in the development phases.

SESAR encompasses a dual approach considering safety from two perspectives:

- Firstly, *a success approach* in which the new concepts and technologies are assessed to check what the effectiveness would be when they are working as intended – i.e. how much the pre-existing risks that are inherent to aviation will be reduced by the ATM/ANS changes. The success approach is closely aligned with the SESAR Validation Exercises
- Secondly, *a failure approach* in which the ATM/ANS system generated risks are assessed – i.e. induced by the ATM/ANS changes failing.

Further safety material is available in e.g. the Final Resilience Guidance Material for Safety Assessment (SRM) and Design'.

The SESAR safety assessment includes Human Factors Integration = show that for tasks which are critical in terms of safety impact, an appropriately thorough HF analysis has been undertaken.

The safety assessment is embedded in the SESAR EOCVM Phases V1 to V3, where requirements at different levels are linked to those and documented in the required parts (usually, this is Part II) of the SESAR documents, as indicated in Figure 12.

SESAR does not prescribe a certain method to be used for performing the safety analysis, but gives guidance towards the application of safety activities that must be performed as formal analysis or through workshops, see figure below.

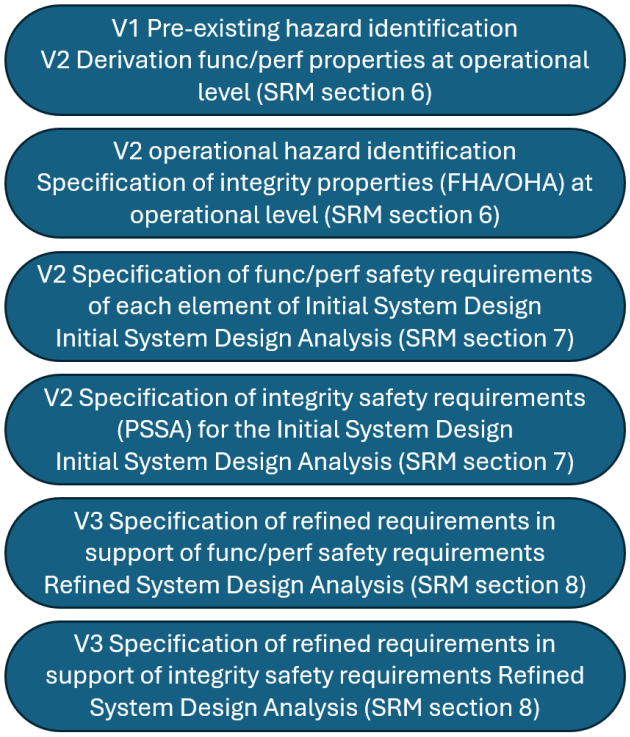

Figure 19. Activities to perform a Safety Analysis

The scope of the SESAR Safety activities concerns the Initial System Design Level and the Refined System Design Level. Furthermore, the Guidance Material gives information on how to apply safety management at project level, such as the Very Large-scale Demonstrations.

Safety Subprocess – Scope – Key Differences
Item #1 – Aviation system scope **EASA –** The scope of the safety work in EASA is the complete aviation system, which includes the on-board system, ground system, ATM/ANS system, maintenance and training. **SESAR –** The scope of SESAR is concerned with the ATM/ANS system, both on-ground and on-board.
Item #2 – Operational scope **EASA –** EASA is concerned with the full life cycle of the aviation systems, i.e. from system design to operational use, including maintenance. **SESAR –** The scope of SESAR is system development and support to specific types of SESAR projects, such as VLDs, according to a predefined Validation level (V1 to V3).
Item #3 – Technical scope **EASA –** The EASA Guidance Material concerns the application of ML/AI and gives specific guidance for this type of systems. **SESAR –** SESAR is concerned with the full system development process, which may include ML/AI though most of the time does not.

Table 25. Key differences for Safety subprocess – Scope

Safety Subprocess – Scope – Overlaps
Item #1 – Scope
Both EASA and SESAR propose a structured approach towards ensuring safety of the system that needs to be developed.

Table 26. Overlaps for Safety subprocess – Scope

B.4 Terminology and Definitions

SESAR

SESAR provides a long list of definitions that concern safety related terms and general SESAR-related terms

EASA

EASA describes different AI-techniques in the section on terminology and with this provides a clear scope to the applicable techniques for the current document

Safety Subprocess – Terminology – Key Differences
Item #1 – Prescribed documentation
EASA – Considers knowledge of safety processes as basics and describes here terms on AI.
SESAR – Considers all safety terms and SESAR-related definitions.

Table 27. Key differences for Safety subprocess – Terminology

B.5 Inputs

SESAR

Documentation within SESAR is based on the existing Solution Safety Plan (V1, V2, V3). Any documentation that is produced before the Safety Plan is set up, is considered to be input to the plan. These can be the OSED, SPR, etc.

EASA

EASA considers aviation standards as major inputs to the certification process:

- for airborne systems, ARP4761 defines a system as ‘combination of inter-related items arranged to perform a specific function(s);
- for the ATM/ANS domain (ATS and non-ATS), Regulation (EU) 2017/373 defines a functional system as ‘a combination of procedures, human resources and equipment, including hardware and software, organised to perform a function within the context of ATM/ANS and other ATM network functions’.

Safety Subprocess – Inputs – Key Differences
Item #1 – Prescribed documentation
EASA – Considers mostly aviation standards as inputs to the safety process.
SESAR – Considers all existing project documentation to be inputs.

Table 28. Key differences for Safety subprocess – Inputs

B.6 Outcomes

SESAR

Documentation in SESAR is based on the Solution Safety Plan (V1, V2, V3).

- VALP/DEMOP Annex II: Safety Plan Contains the link to the SESAR-program (link to the SESAR solutions) and all planning activities towards the safety assessment for a project Objectives, scope, safety argument and everything on planning (timing and resources).
- VALR/DEMOR Annex II: Safety Report Safety Criteria (SAC) are derived during V1 through the analysis of AIM and are presented in the V1 Solution Validation Plan – Part II: Safety Plan. As the Solution progresses to V2 and the Solution concept is further refined, the safety assessment at the operational level will establish the Safety Objectives to deliver the Safety Criteria, and the safety assessment at initial system design level will establish the Safety Requirements to satisfy the Safety Objectives.
- For Human Performance, the tasks and the environment must be documented. Identify all interfaces between humans and technical equipment. Then: “show that for tasks which are critical in terms of safety impact that an appropriately thorough HF analysis has been undertaken.” (Safety Reference Material).
- With respect to the formal SESAR deliverables, the SESAR 2020 Solution SPR-INTEROP/OSED and TS formally capture, from a safety perspective, the safety requirement hierarchy11 within a Solution. The Safety Criteria define what is considered tolerably safe for the change being introduced by operations within the scope of the Solution.

EASA

A safety assessment, and, if necessary, appropriate safety requirements should be defined and verified. This may include independence requirements to guarantee an appropriate level of independence of the safety risk mitigation architectural mitigations from the AI/ML constituent.

The EASA AI Concept Paper does not prescribe any formal deliverables. It does note that all outcomes of the safety assessment must be documented. The applicant should also document how end users’ inputs are collected and accounted for in the development of the AI-based system.

Documented are the Means of Compliance (MOC). The goal of this document is twofold:

- to allow applicants proposing to use AI/ML solutions in their projects to have an early visibility on the possible expectations of EASA in view of an approval. This material may be referred to by EASA through dedicated project means (e.g. a Certification Review Item (CRI) for certification projects);
- to establish a baseline for Level 1 and Level 2 AI applications that will be further refined for Level 3 AI applications (‘advanced automation’).

Safety Subprocess – Outcomes – Key Differences
Item #1 – Prescribed documentation
EASA – Describes in general terms the required documentation, like Means of Compliance and to document all users' inputs.
SESAR – Follows a strict documentation approach with a Validation Plan and Validation Report of which part II concern the safety documentation.

Table 29. Key differences for Safety subprocess – Outcomes

Safety Subprocess – Outcomes– Overlaps
Item #1 – Scope
Both EASA and SESAR require documentation to the level applicable of the application that is developed.

Table 30. Overlaps for Safety subprocess – Outcomes

B.7 Assessment Methodology

SESAR

SESAR prescribes a structured safety assessment methodology for all its solutions, known as the Safety Reference Material (SRM) and its extended version, the Expanded Safety Reference Material (E-SRM). This methodology provides a harmonised framework for identifying hazards, assessing risks, and defining safety requirements throughout the lifecycle of SESAR solutions. By mandating the use of SRM/E-SRM, SESAR ensures consistency, traceability, and regulatory alignment in safety assurance activities across all projects. Expert judgement is used by the ANSP Safety Manager to decide the significance of safety on any proposed change in the system. Guidance can be provided that is supposed to be practical and provide support at the right level of safety.

EASA

EASA's AI Concept Paper outlines clear safety assessment objectives through anticipated Measures of Compliance (MOC-SA), but does not prescribe specific methods for compliance. Applicants are required to identify, assess, and mitigate uncertainties; establish a taxonomy of AI/ML constituent failure modes and evaluate associated detection methods; and quantitatively link generalisation performance to safety requirements. While the concept paper allows flexibility in how these objectives are met, all methods must be justified and aligned with established aviation safety standards. Further guidance is expected through future AMC/GM under Rulemaking Task RMT.0742.

Safety Subprocess – Assessment methodology – Key Differences
Item #1 – Level of guidance
EASA – Provides extensive guidance towards compliance of the proposed system towards several topics and identifies standards from recognised standardisation bodies.
SESAR – Defines a formal safety assessment methodology, providing a repeatable and consistent process for safety assurance within SESAR projects.

Table 31. Key differences for Safety subprocess – Assessment Methodology

B.8 Performance Indicators

SESAR

The SESAR program is built around a number of Key Performance Areas (KPA) that each constitute a number of Key Performance Indicators (KPI). Each SESAR project must start with an assessment of the major KPIs and must indicate how it will contribute to the establishment of improving these. Importantly, none of the KPIs should degrade as a result of project implementation. SESAR's Accident Incident Model (AIM) underpins this process by systematically linking safety occurrences to operational risks, providing a robust framework for safety performance assessment in ATM.

EASA

For each application, metrics must be defined to evaluate the AI/ML constituent performance. No a-priory indicators are given; these are left to be defined within the project.

Safety Subprocess – Performance indicators – Key Differences
Item #1 – Pre-existence of performance indicators
EASA – Leaves it to the system developer or manufacturer to define relevant performance indicators to the proposed system.
SESAR – Already identifies at solution-level a large number of KPAs and KPIs and in this way guides the system developer in choosing performance indicators.

Table 32. Key differences for Safety subprocess – Performance Indicators

Safety Subprocess – Performance indicators – Overlaps
Item #1 – Output
Both EASA and SESAR consider the use of performance indicators to prove system compliance with a defined safety level.

Table 33. Overlaps for Safety subprocess – Performance Indicators

B.9 Support and Resources

SESAR

The SESAR programme provides extensive templates for each deliverable, thus ensuring an overall consistency throughout the projects running in the programme. Templates for the Safety Plan and Safety Report are provided.

SESAR organised different courses, e.g. on how to deal with safety issues in a project.

EASA

The EASA Concept Paper is a recently published document that is not yet supported with tools or other materials.

Safety Subprocess – Support and resources– Key Differences
Item #1 – Templates **EASA –** Not provided. **SESAR –** Follows a strict documentation approach with a Validation Plan and Validation Report of which part II concerns the safety documentation. For each deliverable an extensive template is provided.

Table 34. Key differences for Safety subprocess – Support and Resources

Appendix C Security Subprocess Analysis

C.1 Purpose and Objectives

EASA

With Decision 2020/006/R [3], EASA has amended the Certification Specifications (CSs) for large aircraft and rotorcraft, as well as the relevant Acceptable Means of Compliance (AMC) and Guidance Material (GM), introducing specific objectives for assessing and controlling safety risks posed by information security threats. Such threats could be the consequences of intentional unauthorised electronic interaction (IUEI) with systems on the ground and on board of the aircraft [1]. These amendments are used as a base for the guidelines about the information security of systems and equipment based on AI/ML applications.

The main goal of the EASA subprocess for information security concerns the realization of the following key aspects for each AI-based (sub)system and its data sets [1]:

- the **identification of vulnerabilities and security risks** that **have an impact on safety**, through a product information security risk assessment (PISRA) or, more in general, an information security risk assessment.
- the **implementation of the necessary mitigations** to reduce the aforementioned risks to an acceptable level (acceptability is defined in the relevant CS for the product).
- the **verification of effectiveness of the implemented mitigations**, entailing a combination of analysis, security-oriented robustness testing and reviews.

The aforementioned three key aspects are associated to specific information-security objectives.

The concept paper recognizes that the management of identified risks is an iterative process that requires assessment and implementation of mitigation means until the residual risk is acceptable (acceptability criteria depend on the context that is considered for the certification of the affected product or part).

For the management of information security risks, EASA concept paper addresses both on-ground and on-board (airborne) systems, based on AI. It does not directly cover the organisation processes such as design, maintenance or production processes, which should anyway be adequately managed since they represent another source of information security risk. For these parts, Commission Delegated Regulation (EU) 2022/1645 (applicable as of 16 October 2025) [4] and Commission Implementing Regulation (EU) 2023/203 [5] have introduced a set of information security requirements for approved organisations, that should be also taken into account.

As a main limitation, EASA concept paper recognizes that security aspects of AI/ML applications are still an object of study, and that there are no commonly recognised protection measures that have been proved to be effective in all cases. Therefore, we have to consider that the initial level of protection of an AI/ML application may degrade more rapidly if compared to a standard aviation technology. In light of this, systems embedding an AI/ML constituent should be designed with the objective of being resilient and capable of failing safely and securely if attacked by unforeseen and novel information security threats [1].

SESAR

To demonstrate SESAR solutions are secure and cyber-resilient (up to maturity level TRL8), it is strongly recommended to perform a security risk assessment (SecRA), based on the SESAR security risk assessment methodology (SecRAM) [18]

SecRAM document [6] provides the methodology and practical guidance for SESAR solution projects when building their cybersecurity risk assessment. It presents the requirements for demonstrating that a SESAR solution has adequately addressed ATM security in the research and development phase of SESAR, thus ensuring that the outcome is a secure and cyber-resilient SESAR solution.

In general, SecRAM is not limited to cyber aspects, but it also considers physical security properties. Indeed, the main SecRAM objective is to not confine SESAR (cyber)security context to attacks delivered through Information Technology (IT) and Operational Technology (OT), including all causes of impact.

SecRAM assessment is conceived as an iterative process, that needs to be iterated by adding controls until the residual risks meet the cybersecurity objectives. The steps are explained in section 3.3 [6]. At the end of each iteration, the process determines whether the residual security risk is within the acceptable level set by the cybersecurity objectives.

SecRAM risk levels are reported in Table 35. The current cybersecurity objectives of a SESAR solution (defined at SESAR programme level) prescribe that:

- a **high-level residual risk is not acceptable**;
- a **medium-level residual risk shall be justified** in a security annex.

	Impact				
Likelihood	**1**	**2**	**3**	**4**	**5**
5	Low	High	High	High	High
4	Low	Medium	High	High	High
3	Low	Low	Medium	High	High
2	Low	Low	Low	Medium	High
1	Low	Low	Low	Medium	Medium

Table 35. SecRAM security risk levels [6].

In regard to the boundaries, SecRAM follows a **service-oriented approach**: it is recommended to apply the methodology to the service level of the SESAR solution, to distinguish between information flows, data flows, data elements and interfaces to other services.

In addition, impacts are evaluated as the extent to which a **loss of Confidentiality, Availability or Integrity (CIA)** of a primary asset, as a result of a security incident, affects the achievement of business objectives. Impacts are assessed for the following areas:

- people;
- capacity;
- performance;
- economic;

Co-funded by the European Union

- branding;
- regulatory;
- environment.

Since the DES programme covers TRLs from 2 to 8, SecRAM requires different evidences for security assessment, based on the current TRL of the solution. Even though many aspects of security will only be implemented during industrialisation and deployment (TRL8), the majority of the security controls has to be anticipated during the security risk assessment in R&D and captured as security requirements of the SESAR solution pack, starting from TRL2 and with incremental updates according to the TRL, as shown in Table 36. At TRL8, the security controls, previously identified and captured as security requirements, shall be properly implemented and effectively functioning effectively. Here, the verification and validation of security controls could be carried out with dedicated (cyber)security scenarios within validation exercises, and penetration testing of key supporting assets.

	TRL2	TRL4	TRL6	TRL7	TRL8
Capturing controls as security requirements	Initialise	Update	Update	Update	Ensure that previous requirements have been deployed as security controls and update them.

Table 36. SESAR security requirements vs TRL.

Key Differences – Overlaps

Security Subprocess – Purpose and Objectives – Key Differences
Item #1 – Purpose of security risk assessment **EASA –** An information security risk assessment is recommended, intended as a comprehensive assessment of security risk across all forms of information and its protection, especially from a digital or data perspective. In the specific case, security risks shall be assessed in regard to the design, production and operation phases of AI/ML constituents. **SESAR –** Even if a special focus is put on cybersecurity perspective, SecRAM addresses a general security risk assessment, which encompasses all types of security risks, including information security, but also physical and operational risks. **Note –** Even if this difference may be conceived as a more general view of SecRAM assessment, it potentially contributes to an inconsistency of the levels of detail of the two assessments.
Item #1 – Security risk levels **EASA –** The concept paper does not prescribe specific constraints about mandatory security risk levels. Acceptability criteria for residual risk depend on the context that is considered for the certification of the affected product or part. **SESAR –** A high-level residual risk is not acceptable. A medium-level residual risk shall be justified in a security annex. **Note –** This difference may be conceived as a SESAR specific requirement for the cybersecurity objectives of its programme.

Security Subprocess – Purpose and Objectives – Key Differences
Item #2 – Approach for security risk assessment **EASA –** The concept paper does not recommend a specific approach for the information security risk assessment. **SESAR –** SecRAM follows a service-oriented approach: it is recommended to apply the methodology to the service level of the SESAR solution, to distinguish between information flows, data flows, data elements and interfaces to other services. **Note –** Being focused on AI-based (sub)systems and their data sets, EASA addresses a (sub)system-level assessment, which could represent a different view of the security risk assessment with respect to the service-level of SecRAM. In a way, this difference is related to item #1.
Item #3 – Impact areas **EASA –** The risk assessment shall include the identification of vulnerabilities and security risks that have an impact on safety. **SESAR –** In SecRAM, impacts are assessed for several areas: people, capacity, performance, economic, branding, regulatory, and environment. **Note –** Even if this represents a difference, the SecRAM impact area about people coincides with the safety impact area. Thus, SecRAM provides a more general evaluation of the impacts of security incidents.
Item #4 – Objectives vs TRL **EASA –** There are no specific objectives based on the TRL of the reference AI/ML constituent. **SESAR –** In SecRAM, there are general TRL-driven considerations for the required evidences (e.g., security requirements) to prove that the reference ATM solution is securable and resilient. Even though many aspects of security will only be implemented during industrialisation and deployment (TRL8), the majority of the security controls has to be anticipated, starting from TRL2 and with incremental updates according to the TRL. **Note –** SecRAM introduces an incremental view of security assessment and its evidences, based on the TRL.
Item #5 – Validation and Verification of Security Controls **EASA –** A specific information-security objective is present to validate and verify the effectiveness of the security controls targeting identified AI/ML-specific information security risks **SESAR –** In SecRAM, only for SESAR solutions at TRL8, the residual risk after implementation of controls could be assessed also through dedicated security-related scenarios during validation exercises and/or penetration testing of relevant assets. **Note –** Even if SecRAM does not directly require the validation of security controls at low and intermediate TRLs, there are general TRL-driven considerations for the required evidences, in terms of security requirements, to prove that the reference ATM solution is securable and resilient. Such security requirements should be subject to verification activities.

Table 37. Key differences for security subprocess – purpose and objectives.

Security Subprocess – Purpose and Objectives – Overlaps
Item #1 – Objectives related to security risk assessment Both EASA and SESAR (SecRAM) require a security risk assessment in terms of security risk analysis (including identification of vulnerabilities and threat scenarios, and evaluation of risks) and security risk treatment. They both apply an iterative concept for the management of security risks: the assessment is an iterative process to be repeated until the residual risk is acceptable. **Note –** This overlap establishes a basic commonality in the objectives of the security subprocesses.

Table 38. Overlaps for security subprocess – purpose and objectives.

C.2 Target Audience

EASA

The target audience is represented by:

- (Cyber)Security Analysists and Architects;
- AI/ML Software Engineers/Developers.

The main levels of expertise concern both:

- for (Cyber)Security, the implementation of methodologies and processes for information security risk assessment;
- for AI/ML, a specific knowledge of the reference solution (e.g., dataset features, model, etc.), to assess threats and threat scenarios and to evaluate the effectiveness of countermeasures.

SESAR

The target audience is represented by (Cyber)Security Analysists and Architects.

The main levels of expertise concern the implementation of methodologies and processes for (cyber)security risk assessment. For the process execution, specialist operational or design knowledge of the system is required.

Key Differences – Overlaps

Security Subprocess – Target Audience – Key Differences
Item #1 – Solution Expertise **EASA –** For AI/ML, a specific knowledge of the reference solution (e.g., dataset features, model, etc.) is required to assess threats and threat scenarios and to evaluate the effectiveness of countermeasures. **SESAR –** For the process execution, specialist operational or design knowledge of the system is required. **Note –** SecRAM is deemed to require a generic knowledge of the solution design, in addition to the operational knowledge. Instead, EASA is deemed to require a detailed knowledge of the AI/ML solution (including the features of the adopted datasets), especially concerning its potential cybersecurity implications.

Table 39. Key differences for security subprocess – target audience.

Security Subprocess – Target Audience – Overlaps
Item #1 – Security Expertise Both EASA and SESAR (SecRAM) require security expertise, especially regarding security risk assessment. **Note –** This overlap establishes a basic commonality in the expertise required to carry out the subprocess.

Table 40. Overlaps for security subprocess – target audience.

C.3 Scope

EASA

The main activities and steps recommended by EASA are those related to typical methodologies for information security risk assessment, i.e.:

- vulnerability and risk identification and evaluation;
- security control identification for risk treatment;
- residual risk evaluation.

For the threat and attack scope, EASA recommends to consider at least the following ML threats/attacks highlighted by ENISA [7]:

- evasion attacks, in which the attacker works on the ML algorithm's inputs to find small perturbations leading to large modification of its outputs (e.g., decision errors);
- poisoning attacks, in which the attacker alters data to modify the behaviour of the algorithm in a chosen direction;
- oracle attacks, in which the attacker explores a model by providing a series of carefully crafted inputs and observing outputs (these attacks can be predecessors to more harmful types, such evasion and poisoning).

The reference threat scope in illustrated in Figure 20 and Figure 21shows also some suggested defensive techniques for the mitigation, with respect to the scope. Such figure is included in EASA concept paper for the ATM/ANS use case.

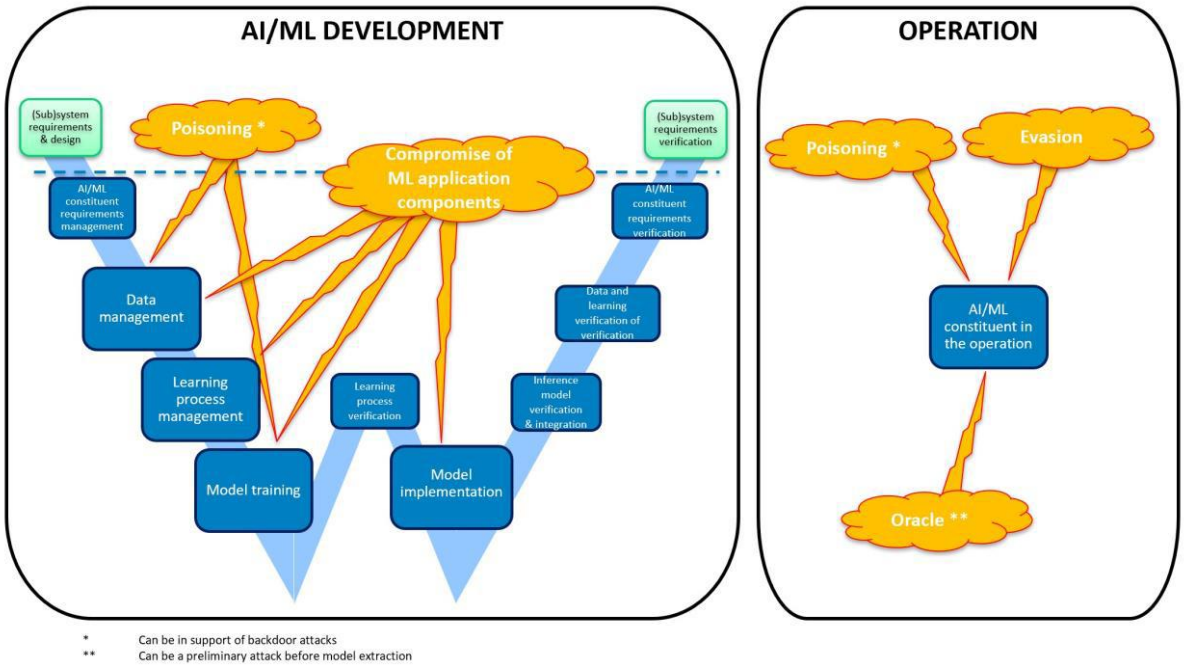

Figure 20. Threat scope to be used as a reference for the information security risk assessment of AI/ML constituents according to EASA [1].

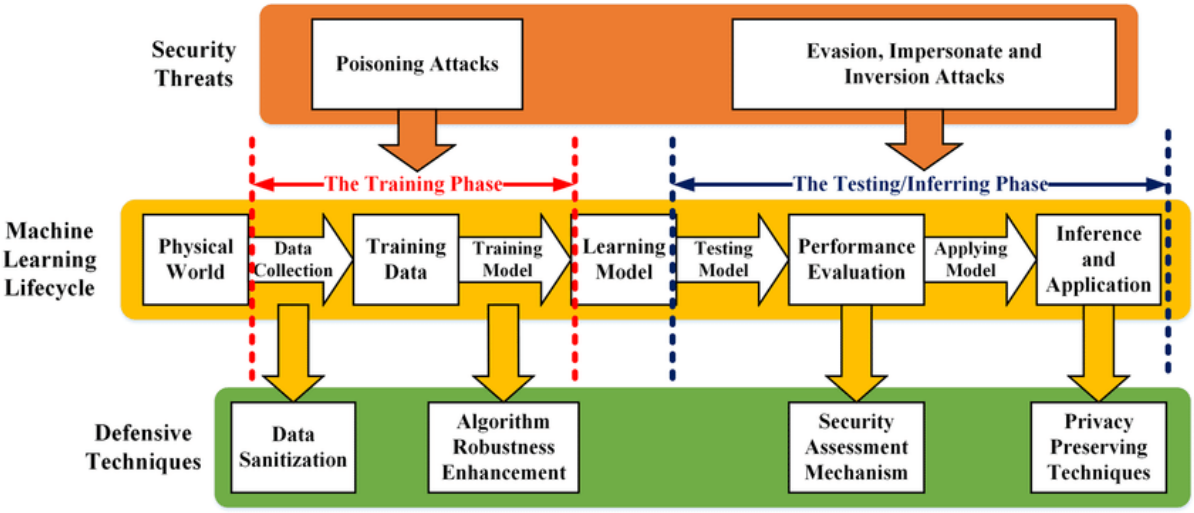

Figure 21. Threat scope and defensive techniques suggested by EASA for the ATM/ANS use case [1] [8]

SESAR

SecRAM assessment is conceived as an iterative process, that needs to be iterated by adding controls until the residual risks meet the cybersecurity objectives. The steps are the following:

- **scope definition**, to describe involved roles, equipment, and systems, and to identify dependencies of the reference system on other systems and infrastructure;

- **asset identification**, to identify possible targets of security attacks in terms of **primary assets** and **supporting targets**;
- **impact evaluation**, to evaluate the possible impacts concerning the harm resulting from each primary asset being compromised by an attack;
- **identification of vulnerabilities, threats and likely threat combinations**, to identify the vulnerabilities of supporting assets that may be exploited by an attacker, jointly with the associated threat sources and threat scenarios;
- **security control identification**, to identify the available protections acting upon the supporting assets, that will reduce the impact on primary assets or attack likelihoods;
- **attack likelihood estimation**, to evaluate the likelihoods of attacks and related threat scenarios;
- **security (residual) risk evaluation**, to assess the levels of each security risk (or residual security risk in case of iterated cycle).

At the end of each iteration, the process determines whether the residual security risk is within the acceptable level set by the cybersecurity objectives. If this is not the case, the process goes back to a previous step to identify how non-acceptable residual risks may be reduced, e.g., inserting additional security controls. SecRAM process is depicted in Figure 22.

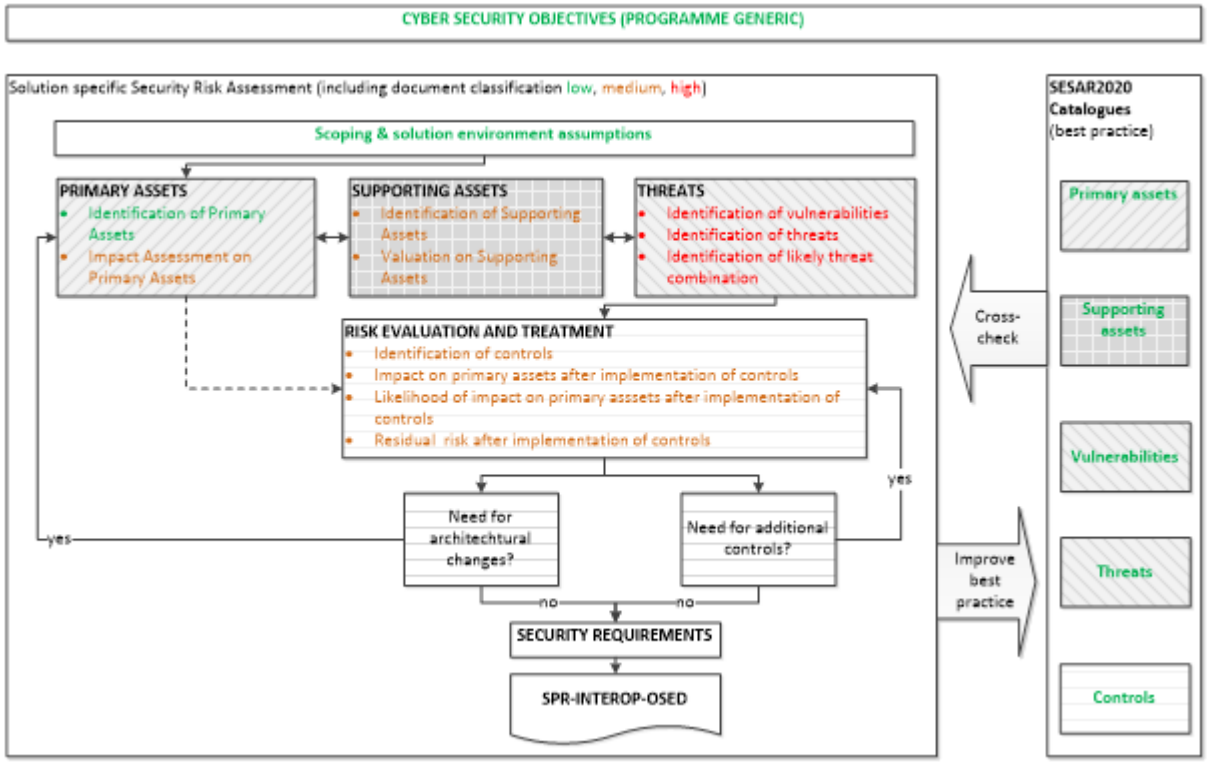

Figure 22. SecRAM process [6].

Key Differences – Overlaps

Security Subprocess – Scope – Key Differences
Item #1 – Threat Scope **EASA –** For the threat and attack scope, EASA recommends to consider at least specific threats/attacks targeting AI/ML constituents (evasion, poisoning, oracle), as highlighted by ENISA. **SESAR –** SecRAM considers generic IT and OT threats. **Note –** Even if this difference may be conceived as a more general view of SecRAM assessment, it potentially contributes to an inconsistency of the levels of detail of the two assessments, especially concerning the supporting assets (i.e., the targets of possible attacks) that are required to be considered in SecRAM. Indeed, these could be more related to a service level (in lined with SecRAM service-oriented approach), in contrast with the (sub)system-level focus of EASA for the assessment of AI/ML-related security risks.

Table 41. Key differences for security subprocess – scope.

Security Subprocess – Scope – Overlaps
Item #1 – Activities and Steps Both EASA and SESAR (SecRAM) assume the execution of an iterative process, with the same basic steps (risk analysis, security control design, risk residual evaluation). **Note –** This overlap establishes a basic commonality in the activities and steps required to carry out the subprocess.

Table 42. Overlaps for security subprocess – scope.

C.4 Terminology and Definitions

Key Differences – Overlaps

Security Subprocess – Terminology and Definitions – Overlaps
Item #1 – Main Concepts Both EASA and SESAR (SecRAM) address the same basic concepts for (information) security risk assessment and the related objectives.

Table 43. Overlaps for security subprocess – terminology and definitions.

C.5 Inputs

EASA

The following main references inputs are envisaged [1]:

- For the initial and continuing airworthiness of airborne systems embedding AI/ML applications, the guidance from AMC 20-42 “Airworthiness information security risk assessment” [9] is applicable, although contextualised to take into account the peculiarities of the AI/ML techniques.
- ENISA report [7] is directly applied for the objectives concerning: vulnerability and risk identification (IS-01); security control identification (IS-02).

SESAR

SecRAM applies the ISO 27002:2013 catalogue for addressing applicable security controls for SESAR solutions.

Key Differences – Overlaps

Security Subprocess – Inputs – Key Differences
Item #1 – Reference Inputs
EASA – AMC 20-42 and ENISA reports are used as main reference inputs for the guidelines about information security risk assessment of AI/ML constituents.
SESAR – ISO 27002:2013 catalogue is used in SecRAM for addressing applicable security controls for SESAR solutions.
Note – This difference is related to the different scopes of the security assessments in EASA and SESAR.

Table 44. Key differences for security subprocess – inputs.

C.6 Outcomes

EASA

For the compliance analysis with respect to the certification objectives for information security risk management, the outcomes to be produced shall address the following elements for AI/ML constituents [1]:

- the PISRA or, more generally, the information security risk assessment;
- the design of mitigation measures (security controls) for non-acceptable security risks, as identified in the assessment;
- security-oriented analysis, robustness testing and review focussing on the verification of the effectiveness of mitigation measures.

SESAR

For the security subprocess, a SESAR solution project shall provide only two formal deliverables:

- the Security Assessment Plan (SecAP);
- security requirements, to be documented in SPR-Interop/OSED and/or TS-IRS and/or DEMOR as applicable.

There is no mandatory template to document the results of a SESAR solution's security risk assessment and no security risk assessment report shall be stored in STELLAR due to the sensitive nature of such documents. The SESAR solution teams are free to use any document/tool to document this step of security risk assessment.

Anyway, for SESAR solutions at TRL8, it is important to ensure requirement traceability and show how security requirements captured at lower maturity levels have been properly implemented as security controls in the SESAR solution.

Key Differences – Overlaps

Security Subprocess – Outcomes – Key Differences
Item #1 – Security Assessment Plan **EASA –** The concept paper does not require any specific plan of security assessment activities. **SESAR –** The SecAP is a formal deliverable of every SESAR solution.
Item #2 – Security-oriented Verification **EASA –** The verification of the effectiveness of the security controls shall typically take place as part of any verification step during the development cycle, taking into account the specific threat under consideration. Security-oriented analysis, robustness testing and review shall occur focussing on the verification of the effectiveness of mitigation measures **SESAR –** For TRL8, SecRAM suggests traceability with security requirements to show how they have been implemented as final security controls. However, there is no formal deliverable providing evidences of the results achieved for the verification of effectiveness of security controls. Instead, for the validation, the DEMOR could include validation exercises about security aspects.

Table 45. Key differences for security subprocess – outcomes.

Security Subprocess – Outcomes – Overlaps
Item #1 – Security Requirements Both EASA and SESAR introduces security mitigation as a formal outcome. On the one hand, EASA concept paper requires to document a mitigation approach (security controls) to address the identified AI/ML-specific information security risks. On the other hand, for every SESAR solution (from TRL2 to TRL8), security requirements shall be documented in SPR-Interop/OSED and/or TS-IRS and/or DEMOR as applicable.

Table 46. Overlaps for security subprocess – outcomes.

C.7 Assessment Methodology

EASA

For the compliance analysis with respect to the certification objectives for information security risk management, the following methods are possibly envisaged [1]:

- security risk assessment – analysis, review;
- design of mitigation measures – analysis, review;
- verification of mitigation measures – analysis, review, testing (security-oriented robustness testing).

SESAR

Analysis and review activities are expected for all the steps of SecRAM process. For SESAR solutions at TRL8, testing activities, in the form of dedicated (cyber)security validation scenarios and penetration testing, shall be executed for the validation of security requirements.

Key Differences – Overlaps

Security Subprocess – Assessment Methods – Overlaps
Item #1 – Main Assessment Methods
Although SESAR recommends a specific methodology (SecRAM), both EASA and SESAR require the same main basic methods for security risk assessment, i.e., analysis, review, and security-oriented testing.

Table 47. Overlaps for security subprocess – assessment methods.

C.8 Performance Indicators

EASA

Even if EASA concept paper does not specify explicitly security-related indicators or metrics, the following KPIs have been identified in D4.2 [28] as indicators that can be used by the applicant to measure whether the information security objectives have been satisfied in [1]:

- List of information security risks with an impact on safety.
- The effectiveness of the security controls introduced to mitigate the identified AI/ML-specific information security risks to an acceptable level.

SESAR

Some indicators are suggested to track the need of architectural changes in a SESAR solution due to security issues, as derived within SecRAM assessment, such as:

- Unacceptably high residual risks, i.e., a failure to meet security objectives.
- A high cost of recommended controls.
- The identification of new threats or vulnerabilities.

Thus, potential security-related KPIs of a SESAR solution are the following:

- number of unacceptable residual security risks;
- cost of recommended security controls;
- number of new threats or vulnerabilities discovered in the last assessment iteration.

Key Differences – Overlaps

Security Subprocess – Performance Indicators – Key Differences
Item #1 – Scope of Security-related Performance Indicators
EASA – The concept paper does not suggest specific security-related performance indicators. Some KPIs may be derived in regard to the list of information security risks with an impact on safety, and to the effectiveness of the security controls for AI/ML-specific information security risks to an acceptable level.
SESAR – Potential security-related KPIs of a SESAR solution are the following: number of unacceptable residual security risks; cost of recommended security controls; number of new threats or vulnerabilities discovered in the last assessment iteration. These may track the need of architectural changes in a SESAR solution due to security issues.
Note – SecRAM indicators are strictly focused on the scope of security risk assessment, in order to track the need of architectural changes to cope with security issues. Instead, EASA does not explicitly recommend security-related performance indicators to manage security issues affecting AI/ML-based systems.

Table 48. Key differences for security subprocess – performance indicators.

C.9 Support and Resources

EASA

The following additional reference inputs are listed for the ATM/ANS use case and may be considered as a support for the information security risk assessment of AI/ML [1]:

- Microsoft AI/ML Pivots to the Security Development Lifecycle Bug Bar [10];
- Microsoft Threat Modeling AI/ML Systems and Dependencies [11];
- Microsoft Failure Modes in Machine Learning [12];
- the survey paper on security threats and defensive techniques of ML [8];
- MITRE Adversarial ML Threat Matrix [13].

SESAR

SecRAM does not prescribe a specific tool support for the activities included within the security risk assessment of a SESAR solution.

The use of a specific SecRAM catalogue is not restrictive but should be considered as guidance material. Such catalogue includes a list of primary assets, supporting assets, threats, vulnerabilities, and security controls, to be used as a reference in the different steps of security risk assessment. To improve best practice in DES, after SESAR solution level brainstorming, new elements for re-use by other projects can be proposed to the transversal performance team for inclusion.

Key Differences – Overlaps

Security Subprocess – Support and Resources – Key Differences
Item #1 – Scope of Security-related Performance Indicators
EASA – EASA concept paper suggests some optional references as a support for the information security risk assessment of AI/ML constituents.
SESAR – SecRAM recommends the adoption of SecRAM catalogue as guidance material.
Note – SecRAM catalogue does not include any specific element (especially supporting assets, threats, vulnerabilities security controls) that is directly applicable for AI/ML-based SESAR solutions. This key difference is also related to the different threat scope of EASA and SESAR.

Table 49. Key differences for security subprocess – support and resources.

Appendix D Ethics Subprocess

D.1 Purpose and Objectives

Moving to the ethics subprocess from the perspective of EASA, this analysis relies on the EASA Artificial Intelligence Concept Paper Issue 2 (Guidance for Level 1 & 2 machine-learning applications), following the EASA AI Roadmap 2.0, as its main documentation source.

The guidelines contained within the Concept Paper cover ethics objectives and anticipated means of compliance for data-driven AI approaches, limiting themselves to Level 1 and Level 2 AI applications, as laid down by the AI Roadmap and subsequently specified by the Concept Paper, focusing on supervised learning and\or unsupervised learning approaches. In this context, the ethics subprocess is part of the trustworthiness assessment building block as a dedicated evaluation step, anticipating future means of ethics compliance and laying down corresponding objectives based on the work of the EU Commission AI High-Level Expert Group (HLEG) on Artificial Intelligence. Specifically, the ethics assessment adapts and builds on the questions initially developed in the Assessment List for Trustworthy AI (ALTAI) [15], tailoring them to the specificities of the aviation domain. The result is a list of *Gears* which reference key ethical concepts, such as human agency and oversight, technical robustness and safety, privacy, data protection and data governance, transparency, accountability and environmental well-being, laying down objectives and anticipated means of compliance under the trustworthiness block for each one.

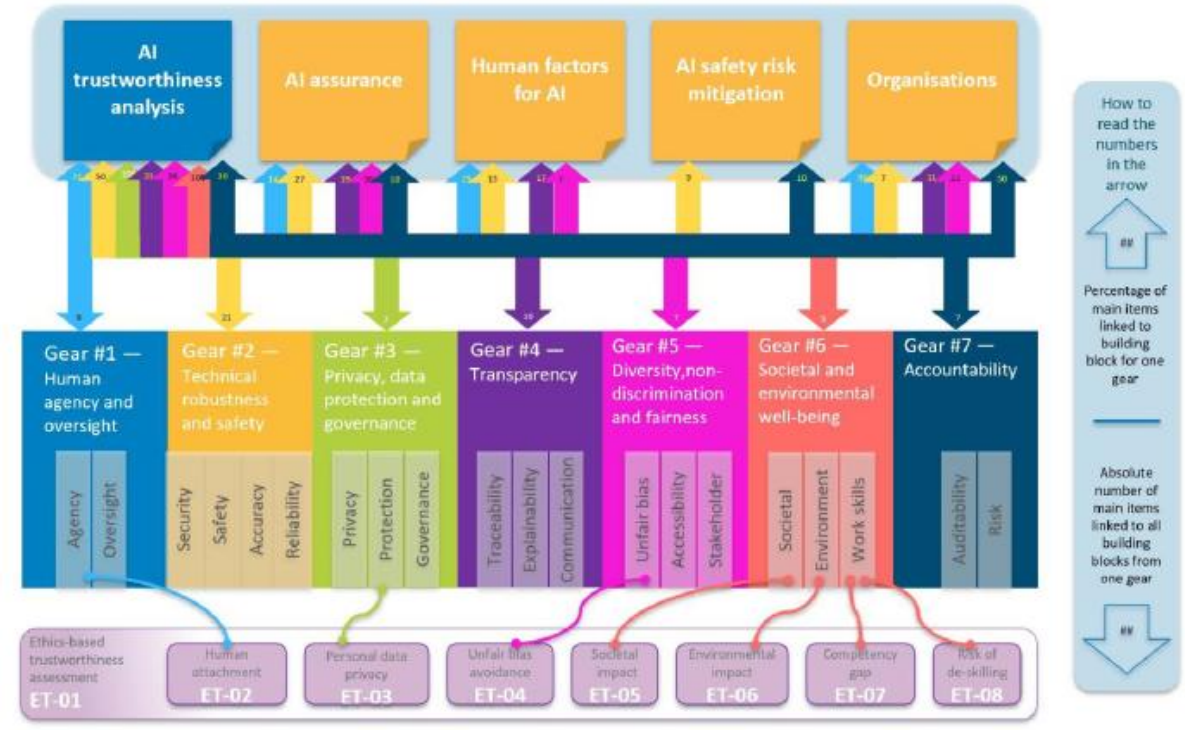

Figure 23. Mapping of 7 gears to the AI trustworthiness building blocks

Boundaries. Considering the structure, scope and purpose of the ethics-based assessment and its relationship with the ALTAI, a boundary of the EASA ethics assessment emerges, as the document

clarifies that not all the key ethical dimensions of AI can be easily adapted, nor substantially implemented, for the purposes of the aviation domain. Specifically, under the **societal and environmental well-being** *Gear*, the document clarifies under "*Impact on work and skills and on society at large or democracy*" that the criteria may not apply to all solutions and use cases for the aviation domain. The same clarification is present for the **diversity, non-discrimination and fairness** *Gear*, where the document nevertheless specifies the need to use and interpret it by focusing on persons, either as individuals or groups. This boundary stems from the adaptation of general ethics guidelines for AI to the specificity of the aviation domain and could suggest the development of alternate ethics criteria of assessment native to the field, also considering how both objectives and anticipated means of compliance are nevertheless laid down for all *Gears*, including those mentioned above.

However, overall, no significant or critical limitations or gaps emerge considering the guidelines objectives and purpose relating to the ethics subprocess, which adopts a well-established set of definitions, priorities and criteria already laid down at the EU level, adapted for the aviation domain and the trustworthiness framework.

Relying on the documentation available on STELLAR Program Library, the main reference on ethics within the SESAR framework consists in the Horizon Europe Ethics Guidelines [19]. In addition to these specific guidelines, the general references for compliance are European Commission notes on Ethics and Data Protection (2021) [20] and Ethics By Design and Ethics of Use Approaches for Artificial Intelligence (2021) [21].

Accordingly, as a specialised branch of the Horizon Programme, for SESAR funded initiatives ethics of research is an essential legal requirement (Reg. (EU) 2021/695 [22], Articles 18 and 19 and Grant Agreement [23], Article 14 and Annex 5). The ultimate goal of this objective is to ensure that EU-funded research initiatives—both in terms of methodology and outcomes—are fully aligned with core European values. Actions carried out under the Programme thus must comply with ethical principles and relevant Union, national, and international law, including the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights and its Supplementary Protocols. Particular attention must be given to key principles such as proportionality, the right to privacy and personal data protection, the physical and mental integrity of individuals, non-discrimination, as well as the safeguarding of the environment and the promotion of high standards of human health protection (Reg. (EU) 2021/695, Article 18 and Recital 71).

From a procedural point of view, this is a comprehensive duty that encompasses all the project management phases, from the proposal to the implementation of the research activities. Beneficiaries are responsible for ensuring that all ethical aspects of the activities carried out under the grant(s) are handled in accordance with ethical principles, relevant international and national laws, and the terms outlined in the Grant Agreement(s). Should any significant new ethical issues emerge, beneficiaries are required to notify the granting authority without delay. On its side, the European Commission and/or SESAR, as granting authorities, conduct systematic ethics reviews of all Horizon Europe proposals to identify activities that may raise ethical concerns. Based on the outcomes of these reviews, specific recommendations and requirements may be issued to ensure ethical compliance. These can include the submission of targeted Ethics Deliverables and supporting documentation at any time during the project, the appointment of an external and independent Ethics Advisor or Ethics Board, and the implementation of periodic Ethics Checks or Reviews.

In terms of substance, the SESAR guidelines highlight the critical importance of ensuring data protection and adherence to AI ethical standards. In this regard, the primary references are the provisions of the General Data Protection Regulation (GDPR - Reg. (EU) 2016/679) as well as the work of the EC Independent High-Level Expert Group on AI. It is strongly recommended to monitor potential ethical risks—both in the early stages (research proposal phase) and throughout the operational phase (project management)—that may emerge or intensify during the development and deployment of AI-based solutions.

For the purposes of ethics compliance, beyond safety and robustness requirements, AI-based systems and applications should be designed to uphold and promote the following key values:

- Respect for human agency
- Privacy, personal data protection, and data governance
- Fairness
- Individual, social, and environmental well-being
- Transparency
- Accountability and oversight

Accordingly, SESAR embraces an approach to compliance by design. Ethics by Design aims to prevent ethical issues from arising by integrating ethical considerations from the very beginning of the development process, rather than addressing them retrospectively. This is achieved by proactively incorporating ethical principles as system-level requirements, outlining specific tasks and measures to ensure that AI systems embody these principles [25].

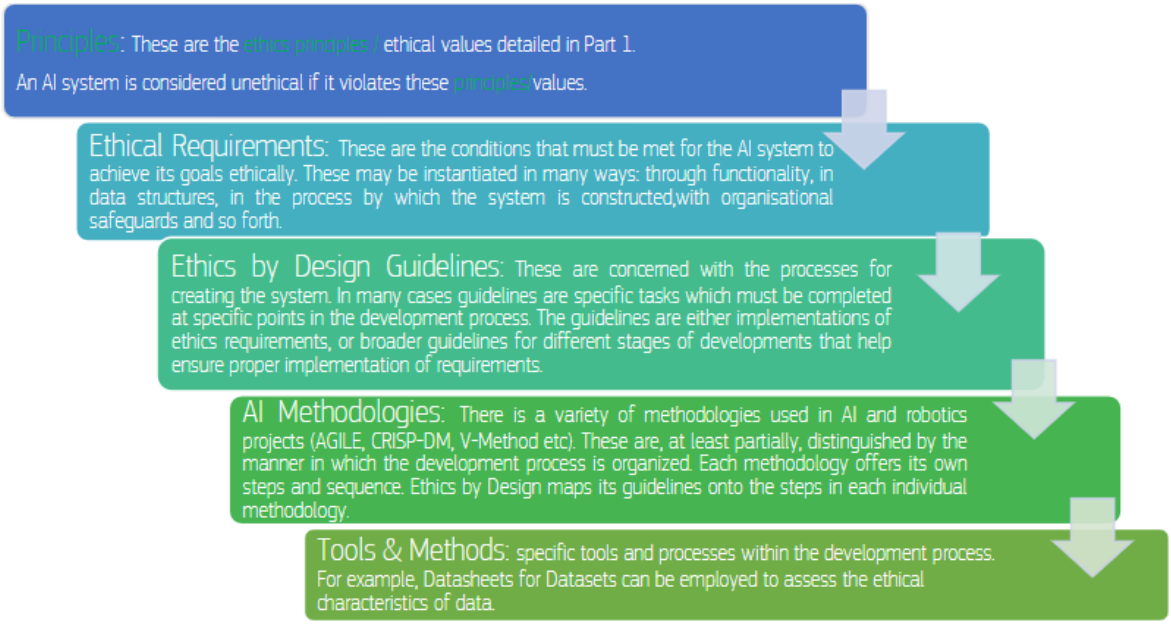

Figure 24. The 5-layer Model of Ethics by Design

In principle, these practices can be integrated into any development methodology, including AGILE, the V-Model, or CRISP-DM. Moreover, Ethics by Design and AI Ethics should encompass the four core phases of AI system use within research projects: project management, acquisition, implementation,

and monitoring. By addressing all these stages, the ethical framework also seeks to prevent *function creep*—the unintended or unauthorized expansion of AI system functions—especially after the project's conclusion.

Figure 25. The generic model for AI Development

Ethics Subprocess – Goals - Key differences
Item #1 – Scope and purpose
EASA – The primary goal is to evaluate the trustworthiness of AI applications—specifically Level 1 and Level 2 machine-learning solutions in the aviation domain. On a long term perspective, this subprocess is aimed at ensuring ethics compliance for certification purposes and through certification.
SESAR – The main aim is to ensure that EU-funded research projects comply with ethical principles and core European values throughout their life cycle. So far, the references to AI ethics should be valid for any solution, regardless of the AI techniques used and the level of automation targeted or achieved.

Table 50. Key differences for ethics subprocess – goals

Ethics Subprocess – Goals - Overlaps
Item #1 – AI Ethics by design
Both EASA and SESAR promote an ethics-by-design approach in the development of AI-based solutions for aviation. While EASA provides general guidelines to support the integration of ethical principles in AI for aviation, SESAR builds on this by offering more specific instructions and references tailored to EU-funded research, particularly focused on innovative, AI-driven solutions.

Table 51. Overlaps for security subprocess – goals

Considering the procedural strategy provided to promote and ensure ethics of research within the SESAR framework, there are no evident limitations. The provided guidelines define a general and consolidated strategies for risk management and impact assessment (e.g., preliminary and periodic systematic ethics review of proposals and projects, definition of specific ethics requirements where needed, internal or external support by advisors with specialist expertise). Moreover, these ensure the alignment of research initiatives on innovative technologies in aviation as well as in other domains with consistent research ethics practices.

In terms of substances, on the one hand, privacy and data protection compliance is a cornerstone of the EU digital strategy and the related requirements are usually proficiently addressed. The guidelines rightly emphasize that EU-funded research projects involving the processing of personal data are not only bound by legal compliance with EU and national data protection laws, but must also be guided by

ethical responsibility. For this reason, particular attention must be given to projects that may present a high ethical risk, where legal compliance alone may not be sufficient to address all potential concerns. In this context, certain indicators can signal a higher ethical risk in personal data processing—*inter alia*, the handling of sensitive data (such as biometric information), the use or reuse of data for research purposes beyond the scope of the original consent, large-scale data processing, the involvement of multiple datasets and/or external service providers, or the combination and analysis of diverse datasets, especially when supported by AI technologies. Consequently, research projects within the SESAR framework that focus on advanced automation or AI-based solutions must carefully consider these aspects and integrate both legal and ethical safeguards throughout their design and implementation.

On the other hand, with regard to the guidance on ethics by design and AI ethics, it should be noted that the references provided are largely drawn from general principles that are not specifically tailored to the needs of the aviation sector. While this approach may serve a systematic purpose by promoting consistency within a unified ethical framework, as several commentators have pointed out, it is essential that these principles and requirements be interpreted in light of the particular characteristics of the aviation context—both in terms of the broader domain and specific operational scenarios. Such an approach is necessary to ensure a coherent and integrated understanding of ethical standards, aligned with the specific ethical needs and challenges inherent in this domain (HLEG-AI, 2019, p. 3) [26].

Ethics Subprocess – Boundaries - Key differences
Item #1 – Coverage of ethical dimensions
EASA – Not all the ethical requirements identified by ALTAI can be easily adapted, nor substantially implemented, for the purposes of the aviation domain. The majority remain relevant with design consequences.
SESAR – The references provided, in principle, suggest that research projects should be compliant with all the AI ethics requirements (ethics by design).

Table 52. Key differences for ethics subprocess – boundaries

Ethics Subprocess – Boundaries - Overlaps
Item #1 – Level of detail
Both EASA and SESAR address ethics in AI through high-level principles, but their guidance often lacks the specificity needed for practical implementation in the aviation sector. EASA's objectives and Anticipated Means of Compliance related to ethics tend to be generic and less actionable compared to more technical KPAs, while SESAR's references are largely based on broad principles that are not specifically tailored to the unique requirements of aviation.

Table 53. Overlaps for ethics subprocess – boundaries

D.2 Target Audience

The EASA Concept Paper targets applicants and developers of AI/ML technologies in aviation, as well as certification authorities, regulatory bodies, and organisations across domains like airworthiness, operations, maintenance, and training. Its main stakeholders include EASA, industry players introducing AI, regulatory and approval bodies, technical developers, human factors experts, end users such as pilots and air traffic controllers, and research and standardisation organisations.

Considering the ethics subprocess specifically, it refers to all stakeholders involved in carrying out the ethics assessment under the trustworthiness framework, primarily organizations and applicants presenting solutions as technology developers and providers.

The target audience for this document is the SESAR research community as a whole, encompassing a wide range of expertise.

Particular attention to these references should be paid by SESAR programme managers, project coordinators and project managers within the participating organisations; data protection officers of both the research consortia and the individual entities involved; as well as researchers directly responsible for managing practical issues related to research ethics and technology ethics in specific activities. This also applies to project ethics officers, ethics advisors, and ethics boards.

The target audience of the two subprocesses does not perfectly overlap from a formal perspective. However, regarding the research ethics aspects that may also impact AI ethics, there are significant connections from a substantive standpoint. In principle, it would be reasonable to assume that the axiological component of the Ethics by Design methodology, when SESAR solutions involve AI technologies or components, should reference ALTAI, taking into account the specifications provided by EASA for the aviation sector.

D.3 Scope

This subprocess within the EASA framework requires the implementation of the following activities, in line with the ALTAI requirements and the concept paper approach:

- **Ethics-based trustworthiness assessment:** perform an ethics-based assessment (Objective ET-01) for any AI-based system. This assessment must align with the 7 ethical gears adapted from the EU Commission ALTAI framework, concerning: human agency and oversight; technical robustness and safety; privacy, data protection, and data governance; transparency; diversity, non-discrimination, and fairness; societal and environmental well-being; and finally accountability. This assessment must be revisited iteratively throughout the system life cycle, mitigating unforeseen ethical issues arising after deployment.
- **Data management and compliance**: compliance is required with EU and national data protection laws (Objective ET-03), including the drafting and updating of Data Protection Impact Assessments (DPIA) as necessary.
- **Environmental and societal impact analysis**: assess the environmental and societal impacts (Objective ET-06), including emissions, energy use, noise, rebound effects, and implications for human health.
- **Training and deskilling risk mitigation**: identify and address any new skill requirements for users and mitigate de-skilling risks through structured training (Objectives ET-07 and ET-08).
- **Documentation and reporting:** all assessments and their outcomes should be well-documented. EASA requires transparency and self-evaluation, with applicants expected to consult the adapted ALTAI list in Annex 5 for guidance.

This subprocess within the SESAR framework requires the implementation of the following activities, in line with the operational guidelines provided by the European Commission and the granting authority:

- A preliminary ethics self-assessment, which may need to be updated iteratively throughout the project. The drafting of a Data Management Plan at the start of and iteratively during the project, including ethical aspects related to data.
- The implementation of an ethics by design strategy for research activities with potential ethical risks (if present) consistently with the adopted research and development methodologies.
- Timely communication with the granting authority if unforeseen ethical issues emerge during the course of the project and the concerted development of a mitigation strategy, if necessary.
- The reporting of any iterative ethics assessments, if required by the granting authority.

Ethics Subprocess – Activities and steps - Key differences
Item #1 – Official Approach
EASA – Applicants may refer to the list of questions from ALTAI, adapted to the aviation sector. However, an official methodology (activities and steps) for ethics compliance has not been finally defined. Given that some of the Gears are connected to other KPAs, the methodologies used there may be applicable to these. However, for others, there remains flexibility in the approach.
SESAR – The official approach to ethics is structured through the guidelines, procedures, tools, and templates provided by the European Commission, as implemented within SESAR.

Table 54. Key differences for ethics subprocess – activities and steps

D.4 Inputs

With a similar process [to the once embraced by SESAR], the inputs required according to the EASA guidelines under the ethics assessment follow the implementation of the activities and objectives based on the anticipated means of compliance gathered from the HLEG assessment list, and referencing chapter C of the Concept Paper:

- **Comply with the AI trustworthiness framework in Chapter C.** Align with safety, robustness, and risk mitigation guidelines defined in the trustworthiness objectives.
- **Comply with GDPR, EU Data Governance, and national rules.** Address both personal and non-personal data protection and integrity across the system lifecycle.
- **Involve the Data Protection Officer (DPO).** Appoint and include the DPO early in system development and ensure independence.
- **Conduct and document a DPIA.** Required if AI processes personal or sensitive data or uses profiling/monitoring.
- **Ensure operational and developmental explainability.** Provide meaningful, role-appropriate explanations of AI behaviour at design and post-ops stages.
- **Use explainability to detect residual bias and unintended behaviors.** Explainability should support model transparency and safety assurance activities.
- **Assess whether AI may impact fairness or discrimination.** If no impact, document this explicitly in the ethics assessment.
- **Create procedures to mitigate bias in both data and model.** Implement systematic controls across the AI lifecycle for safety-relevant fairness issues.
- **Train developers on fairness and bias.** Run awareness programs to prevent unintended bias during AI system design.
- **Inform users they are interacting with AI.** Clearly indicate AI presence and whether personal data is recorded, via UI or manuals.

- **Conduct an environmental impact assessment.** Evaluate lifecycle effects (development to disposal), emissions, energy, and noise.
- **Use environmental standards like EMAS or ISO 14001.** Align mitigation measures with Plan-Do-Check-Act environmental management frameworks.
- **Provide theoretical and practical training (ET-07).** Identify new skills needed and train with theory, practice, and on-the-job mentoring.
- **Assess and mitigate de-skilling risks (ET-08).** Perform a skills gap analysis and maintain proficiency through evaluated retraining.
- **Match training effort to AI Level (e.g., stricter for Level 2B).** Tailor stringency of training and skill retention programs to system autonomy level.
- **Ensure auditability and risk management.** Maintain traceability and align with objectives under the trustworthiness framework.

The inputs required for these subprocesses are, in general, those currently needed for completing the **ethics self-assessment** and the **data management plan**.

For AI ethics and ethics by design, the necessary inputs include those required to complete the **Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment**, which supports the implementation of the Guidelines for Trustworthy AI promoted by the HLEG-AI.

To provide a clearer overview, the key inputs can be summarized as follows:

- Description of the **research activities that may involve human subjects** (excluding personnel) and the applicable research methods/protocols.
- Definition of the **project privacy policy**, identifying high-risk practices (e.g., profiling, monitoring, tracking, surveillance, data reuse, transfer outside the EU) especially for data concerning volunteers.
- Identification and preliminary analysis of **activities conducted in non-EU countries** (if any), including potential ethical issues, risks to participants, and the use or import of local resources that may raise ethical concerns.
- Identification of **substances, processes, or technologies** (if any) used in the research **that may harm the environment**, and clarification on whether the research involves endangered fauna/flora or activities within protected areas.
- Identification of **research activities or results vulnerable to misuse** (e.g., surveillance technologies, profiling tools, and materials or technologies that could be misused for creation of CBRN weapons or adapted for criminal or terrorist activities).
- Description of the **AI-based system (if any) and its concept of operations**, followed by the identification of data used for training and research activities involving the development, deployment, and/or use of the solution.

Ethics Subprocess – Inputs - Key differences
Item #1 – Scope of inputs
EASA – The inputs should come from the previous steps of the AI trustworthiness analysis, particularly from the ConOps outline, the solution characterization, the safety and security assessments, as well as from the outcomes of the ALTAI questions adapted to aviation.
SESAR – In general, the inputs related to research ethics come from the PMP, the DMP, and, if applicable, the requirements and duties prescribed following the ethics review by the EC or the granting authority. If there are specific tasks related to technology ethics (e.g., AI ethics), these can be used both for compliance with research ethics and as inputs for Ethics by Design.

Table 55. Key differences for ethics subprocess – inputs

Ethics Subprocess – Inputs – Overlaps
Item #1 – Use of inputs from the ConOps
EASA – The inputs from the ConOps are aimed at supporting Ethics by Design for certification purposes.
SESAR – If there are specific tasks related to technology ethics (e.g., AI ethics), the analysis of the ConOps can be used both for compliance with research ethics and as inputs for Ethics by Design.

Table 56. Overlaps for ethics subprocess – inputs

D.5 Outcomes

The main outcomes of this subprocess under EASA, which reference the Gears from the ALTAI, include:

- **Requirements-based tests.** Referenced under Objective ET-02, these tests are used to verify that end users interacting with the AI-based system can perform oversight and that the system does not create overreliance, attachment, or manipulative behaviour.
- **Ethics-based assessment.** Required under Objective ET-01, this assessment documents how the AI-based system addresses the seven ethical Gears, including transparency, fairness, environmental impact, and human oversight.
- **Data Protection Impact Assessment (DPIA).** Required under Objective ET-03 when personal data is processed, to ensure compliance with GDPR and national data protection regulations.
- **Training needs analysis and training activity.** Required under Objectives ET-07 and ET-08, these identify necessary new skills and ensure skill retention through training, particularly to mitigate risks of deskilling.
- **Environmental impact analysis.** Required under Objective ET-06, this analysis assesses negative environmental and human health impacts of the AI system throughout its lifecycle.
- **Documentation of absence or presence of impact.** For objectives like ET-04 (fairness) and the societal aspects of Gear #6, the applicant must document whether impacts exist and address them accordingly in the ethics-based assessment.
- **Development and design** to minimize automation bias, overreliance, emotional attachment and human-AI interactions undermining oversight. Identify and implement technical and organizational requirements to monitor human oversight on AI.

The main outcomes of this subprocess in SESAR include:

- **Ethics self-assessment report** (mandatory for the proposal; if requested over the project)
- **Ethics review** by the granting authority, including potential clearances for risk mitigation
- **Data management plan** (mandatory) and the project privacy policy (if required)
- **Ethics-by-design initiatives** (if required; e.g., specific activities or assessment)

Ethics Subprocess – Outputs - Key differences
Item #8 – Ethics Impact Documentation
EASA – The outcome of the subprocess should be, at a minimum, a documentation of the presence or absence of impact, based on the results of the ALTAI questions adapted for aviation. Ideally, it should take the form of a report outlining the initiatives and technical choices undertaken to meet the ethics objectives, in relation to the risks previously identified.
SESAR – The output is a report or another form of supporting documentation that demonstrates that the research carried out (and its applications) has been conducted in compliance with the principles, requirements, and procedures outlined by the EC and the granting authority.

Table 57. Key differences for ethics subprocess – outputs

D.6 Assessment Methodology

To carry out this subprocess under EASA guidelines, the following methods are relevant or required:

- **Ethics assessment.** A structured report recording the analysis of the system against the Gear assessment areas. The report is the primary outcome and supports compliance documentation for certification, and it includes the justification of impact (or lack thereof) and applied mitigation strategies.
- **Test reports.** Tests verifying system behavior (e.g. meaningful user oversight, lack of manipulation, presence of explainability), which is linked to objective ET-02 and IMP-09 and demonstrates compliance through practical human-machine interaction.
- **Data protection compliance documentation**. Required under data protection and management law, particularly when processing personal data, and it must involve the data protection officer and national competent authorities. Formal records must be kept to comply with privacy and data governance pursuant to objective ET-03, with the data protection impact assessment being a potential example.
- **Environmental impact analysis**. Assesses system-wide environmental risks (e.g. emissions, noise, rebound effects), also includes lifecycle analysis and mitigation strategies (using EMAS or ISO 14001 frameworks).
- **Training plan.** Documentation identifying required skills and training needs (ET-07, ET-08), with the guidelines suggesting theoretical and practical training plans, plus performance evaluation.
- **User documentation.** Discloses information and explanations about the system interacting with the user, also clarifying whether personal data is being recorded (ET-05)

In general, the main methods that may be useful for carrying out this subprocess within the SESAR context include:

- **Analysis of research activities and outcomes**, particularly in terms of research impact, project management, data governance and information security management
- **Ethics assessment approaches**, as recommended by the EC for Horizon Europe initiatives
- **Data Protection Risk Assessment**, if applicable
- **Assessment List for Trustworthy AI (ALTAI) for self-assessment**, if applicable
- **Fundamental Rights Risk Assessment,** if needed
- **Interactive review of the ethical risks** over the project, if required

Ethics Subprocess – Methods - Key differences
Item #1 – Solutions-focused vs process-focused **EASA –** Certification-focused, aiming to support compliance through structured documentation (e.g. ethics reports, test reports, training plans). EASA requires formal documentation and test results directly tied to certification and legal compliance. EASA integrates ethics into system validation (e.g. user oversight, explainability, data governance). **SESAR –** In contrast, SESAR emphasizes research project oversight and ethical foresight, aligning with EU research governance (e.g. Horizon Europe). SESAR relies more on flexible tools like ALTAI and optional risk assessments, geared toward project lifecycle ethics rather than system-level certification. SESAR's approach is higher-level, focusing on ethical governance of the research and innovation process.

Table 58. Key differences for ethics subprocess – methods

Ethics Subprocess – Methods - Overlaps
Item #1 – Ethical assessment **Note –** Both EASA and SESAR use structured ethics assessments to analyze the ethical dimensions of AI systems or projects. Both require Data Protection Impact Assessments (DPIAs) where personal data is involved. Both align with EU frameworks—EASA with operational certification (e.g. EMAS, ISO), SESAR with Horizon Europe ethical guidelines and tools like ALTAI.

Table 59. Overlaps for ethics subprocess – methods

D.7 Support and Resources

- SESAR. Horizon Europe Ethics Guidelines. 26 June 2024.
  Available on STELLAR at this link:
  https://stellar.SESARju.eu/servlet/dl/ShowDocumentContent?doc_id=38025009.13&att=attachment&statEvent=Download

- EC. EU Grants - How to complete your ethics self-assessment. Version 2.0. 13 July 2021.
  Available on at this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/guidance/how-to-complete-your-ethics-self-assessment_en.pdf

- EC. Ethics and data protection. 5 July 2021.
  Available at this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-and-data-protection_he_en.pdf

- EC. Identifying serious and complex ethics issues in EU-funded research. 05 July 2021

Available at this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/guidelines-on-serious-and-complex-cases_he_en.pdf

- EC. Ethics By Design and Ethics of Use Approaches for Artificial Intelligence. Version 1.0. 25 November 2021
  Available at this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-by-design-and-ethics-of-use-approaches-for-artificial-intelligence_he_en.pdf

- EASA Artificial Intelligence Concept Paper Issue 2: Guidance for Level 1 & 2 machine-learning applications; https://www.easa.europa.eu/en/document-library/general-publications/easa-artificial-intelligence-concept-paper-issue-2

- EASA Artificial Intelligence Roadmap 2.0: Human-centric approach to AI in aviation; https://www.easa.europa.eu/en/domains/research-innovation/ai

- EC, HLEG-AI. Assessment List for Trustworthy AI (ALTAI) for self-assessment. 17 July 2020
  Document available at this link:
  https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68342
  Tool available on the ALTAI portal at this link: https://altai.insight-centre.org/

Appendix E Human-Factors Subprocess

[This chapter shall report the comparison analysis between EASA and SESAR for the operational concept subprocess. At least HF- objectives in [1] shall be used as a reference for EASA.

In regard to the questions about the key EASA-SESAR differences and overlaps within the reference topics of the next sections, the analysis shall highlight potential gaps and/or common aspects with respect to a harmonization between EASA and SESAR for such specific subprocess. For example, common aspects may help stakeholders avoid duplications. Instead, potential gaps may represent relevant deviations to be possibly faced by the harmonization process.]

E.1 Purpose and Objectives

EASA

Regulation (EU) 2017/373 lays down the common requirements for air traffic management and air navigation services. Yet, there are no requirements that specify the incorporation of human factors within the scope of equipment design or the introduction of new technology.

According to Regulation (EU) 2017/373, the scope of the safety assessment for a system change includes the 'equipment, procedural and human elements being changed'. By definition, therefore, any change impacting the functional ATM system should include an assessment of the impact on the human, but from a safety perspective, not necessarily from a human factors perspective. There are therefore currently no existing requirements that cover the entire ATM domain to which human factors requirements for AI could be attached.

In the absence of regulatory requirements on human factors in ATM/ANS, the existing material taken into account for the definition of the EASA guidelines are the SESAR Human Performance Assessment Process (SESAR JU, 2018), and the SESAR and/or Eurocontrol - Human Factors Case version 2. Although EASA acknowledges that such existing human factors requirements and guidance are applicable to AI-based installed systems and equipment used by end users, it has also highlighted the need to complement and/or adapt them to address the specific challenges associated with the introduction of AI. To this end EASA introduced a few dedicated objectives, focussed on:

- AI operational explainability
- Human-AI teaming
- Modality of interaction and style of interface
- Error management
- Workload management
- Failure management and alerting system
- Customisation of human-AI interface

SESAR

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. Therefore, adequate considerations of HF and HP in all phases of development and implementation are critical to reach the objectives of SESAR, in terms of achieving the benefits related to the KPAs.

In this framework, the purpose of the HP assessment process is to provide assurance that HP aspects related to SESAR technical and operational developments are systematically identified and managed; all the actions necessary to provide adequate confidence that a product, a service or a system is compatible with human capabilities are conducted.

To achieve this, the HP assessment process:

- describes arguments and necessary evidence to show that airborne and ground ATM actors will contribute to the SESAR expected performance benefits;
- describes arguments and necessary evidence to show that the roles, responsibilities and tasks of airborne and ground ATM actors as developed in SESAR are within the scope of human capabilities and limitations;
- defines the process to ensure HP proactively contributes to building the operational concept and system architecture and describes how results from HP activities should be used in the development process, with the aim of improving the concept and technology;
- defines HP transition criteria for progression from one V-phase to the next V-phase;
- has a clear link with validation by (a) providing an input to the validation plan and (b) using the results of the validation activities in support of the HP arguments;
- is aligned with the other Transversal Area (TA) assessment processes, by (a) using a shared description of the reference, the solution and the assumptions and (b) by identifying overlaps and synergies between HP and other TAs;
- defines interactions and uses synergies with the other TA assessment processes, in particular, the safety assessment process;
- provides data that can feed the SESAR Business Case.

HP assessment processes may be conducted in any V-phase. However, the scope of the SESAR HP assessment process is the SESAR V-phases (V1-V3).

Key differences - Overlaps

HF Subprocess – Purpose and Objectives – Key Differences
Item #1 – Purpose of HF assessment
EASA – The purpose is to ensure that all aspects deemed critical from a human factors perspective have been adequately addressed in the design of the solution, thus the solution demonstrates acceptable levels of performance across all these relevant factors. Requirements are formulated differently depending on the level of automation.
SESAR – The purpose is to progressively and iteratively support the design of new solutions, irrespective of their level of automation or the technological means through which they are implemented.

HF Subprocess – Purpose and Objectives – Key Differences
Item #2 – Focus of the HF assessment **EASA –** Being focused on AI-based systems, EASA focuses the assessment on specific themes, corresponding to challenges of interaction associated with the introduction of AI, namely AI operational explainability, Human-AI teaming, Modality of interaction and style of interface, Error management, Workload management, Failure management and alerting system and Customisation of human-AI interface. **SESAR –** The focus is broad and covers all the HF aspects that may affect the adoption and use of a system or a service in a specific context of use, namely 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.
Item #3 – Level of AI vs level of automation **EASA –** The concept paper grounds the assessment on levels of AI, that are considered as static attributions of the system or sub-system being analysed. It recognised that different levels of AI may affect differently specific themes, such as explainability, thus requiring a modular approach. **SESAR –** The HP Assessment process does not specifically refer to the levels of automation and does not present differences in its application depending on the level of automation of the solution being analysed.
Item #4 – Objectives vs Technology Readiness Levels (TRLs) **EASA –** Although the concept paper recommends taking into account the objectives of the human factors assessment during system design, this aspect is ultimately irrelevant for the assessment itself. In general, a high TRL is assumed. **SESAR –** Consistent with its objective of supporting solution design, the arguments within the Human Performance assessment are articulated differently depending on the maturity level of the solution. In this context, the reference framework for the maturity of the solution is the validation phases (V1 - V2 - V3), which are directly aligned with the corresponding TRLs. **Note –** The HP Assessment Process introduces an incremental view of HP assessment and its evidences, based on the TRL.

Table 60. Key differences for HF subprocess - purpose and objectives

HF Subprocess – Purpose and Objectives – Overlaps
Item #1 – Objectives related to security risk assessment Both EASA and SESAR require an HF assessment focussed on the interaction between the human operator and the system. They both apply an iterative approach for the management of HF assessment, that shall be repeated until the objectives are satisfied. **Note –** This overlap establishes a basic commonality in the objectives of the HF subprocesses.

Table 61. Overlaps for HF subprocess - purpose and objectives

E.2 Target Audience

Given EASA's remit, the Human Factors (HF) subprocess typically involves experts who are involved in developing solutions and in the certification process. As HF is an integral part of safety assessment, the target audience potentially includes a wide range of professionals. These professionals may specialise

in safety, security and HF, given the mutual correlation among these KPAs. However, more specifically, the intended stakeholders may include engineers, psychologists, communication scientists and ergonomists with specialised HF expertise.

Relevant areas of expertise include human behaviour, design philosophy, human performance modelling, organisational and human performance, and HF training, particularly in light of current advancements in human–AI interaction in these fields.

Considering the role of SESAR, the target audience of its processes and subprocesses consists of the research and development communities involved in or impacted by the funding programme. Within this framework, Human Factors (HF) are addressed through dedicated methods, such as the HP Case. Accordingly, the main recipients of the programme's guidelines are professionals engaged in HF-related aspects of the research projects.

As in similar contexts, the intended stakeholders may include engineers, psychologists, communication scientists, and ergonomists with specialised expertise in HF. Relevant areas of expertise include human behaviour, design philosophy, human performance modelling, organisational and human performance, and HF training. However, to date, SESAR has not provided specific guidelines or methodological developments regarding human–AI interaction within these domains.

HF Subprocess – Target Audience – Key Differences
Item #1 – AI-specific approaches **EASA –** EASA is developing and consolidating objectives and anticipated means of compliance specifically for AI. This implies that the target audience is expected to have specific competencies related to HF for AI, at least within the scope of the areas addressed so far. **SESAR –** SESAR has not yet developed dedicated objectives and subprocesses for HF and AI. As a result, its target audience operates with a considerable degree of autonomy in research activities, while still referring to EASA guidance as a point of reference.
Item #2 – Objectives **EASA –** EASA addresses its guidelines to a target audience concerned with the certification and certifiability of solutions. **SESAR –** SESAR, in contrast, directs its subprocesses towards a target audience focused on the research and development of new solutions, including exploratory research. Accordingly, a more nuanced approach is favoured.

Table 62. Key differences for HF subprocess – target audience

Security Subprocess – Target Audience – Overlaps
Item #1 – Areas of expertise **Note –** Both EASA and SESAR address a target audience that shares a common area of expertise in Human Factors.

Table 63. Overlaps for HF subprocess – target audience

E.3 Scope

As mentioned above, according to EASA guidelines, the Human Factors (HF) subprocess is based on the SESAR Human Performance Assessment Process (SESAR JU, 2018), and the SESAR and/or Eurocontrol Human Factors Case, version 2. This framework is further integrated with the new AI-specific objectives and anticipated Means of Compliance (MoCs) on HF for AI, as outlined in the EASA Artificial Intelligence Concept Paper Issue 2 – *Guidance for Level 1 & 2 Machine Learning Applications*. The detailed description of the main activities and steps is therefore not provided here, but will be presented in the following section, which is specifically dedicated to the SESAR methodology.

The main activities and steps outlined in the SESAR Human Performance Assessment Process (SESAR JU, 2018) consist of four key phases, supported by operational guidelines. In summary, the subprocess is structured as follows:

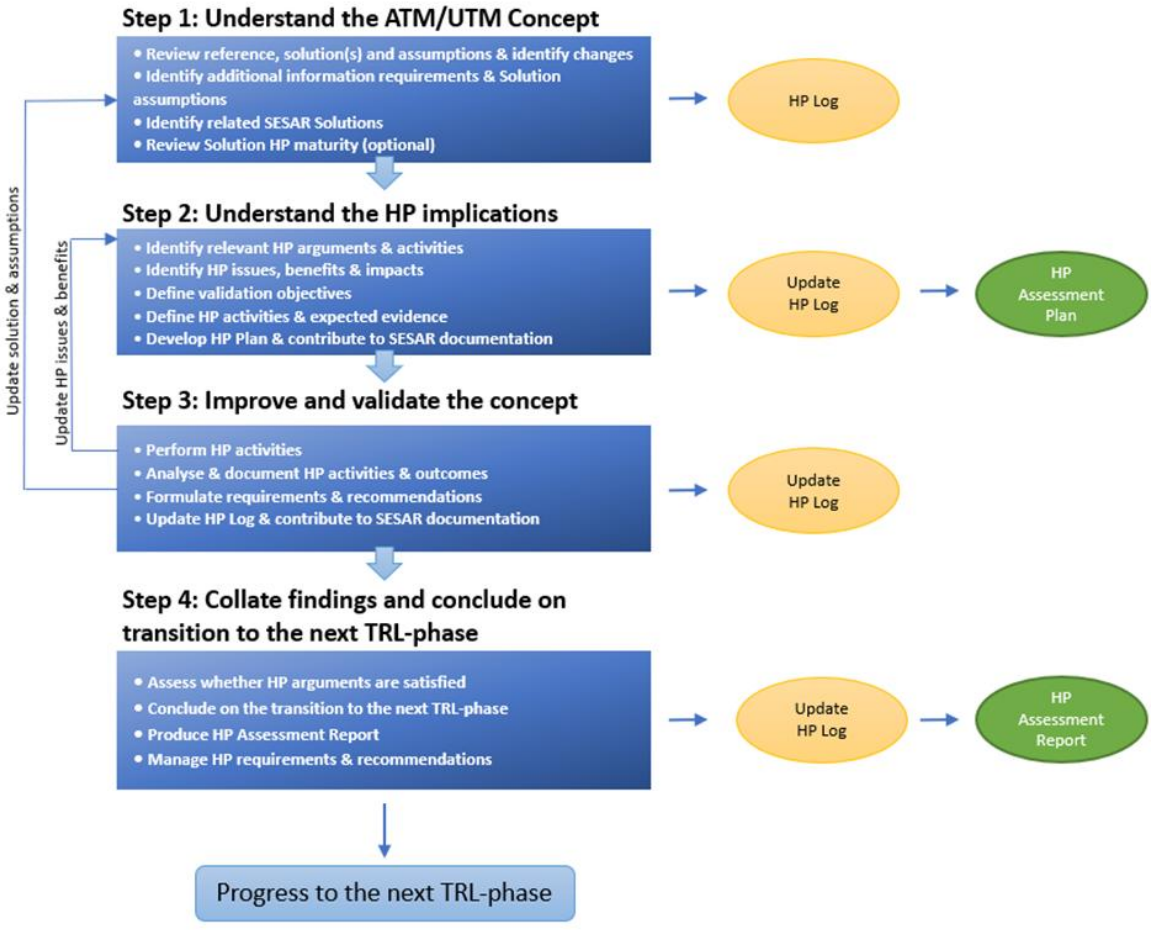

Figure 26. Steps of the HP assessment process

HF Subprocess – Scope – Key Differences
Item #1 – Integration AI-specific objectives **EASA –** The EASA approach assumes that AI-specific objectives and anticipated Means of Compliance (MoCs) can be integrated into the existing process. For example, in Step 1, it is reasonable to position the objectives and related anticipated MoCs concerning the Characterisation and Classification of AI applications (CO/CL). In Step 2, the Human Factors (HF) objectives could find their appropriate placement. **SESAR –** So far, SESAR has not yet provided this type of AI-specific adjustment.

Table 64. Key differences for HF subprocess - scope

Security Subprocess – Scope – Overlaps
Item #1 – Structures and activities **Note –** Both EASA and SESAR refer to the same procedure and tasks, as well as share the same operational objectives.

Table 65. Overlaps for HF subprocess – scope

E.4 Terminology and Definitions

In general terms, regarding Human Factors (HF), it is reasonable to assume that EASA and SESAR use similar terminology. However, it should be noted that, in the context of solution classification based on different levels of automation, EASA has developed an AI-specific approach within its Roadmap and complementary Concept Papers, identifying specific AI Levels. Initially, this approach partially diverged from the Level of Automation Taxonomy (LOAT) adopted by SESAR, which focuses on the automation of cognitive and operational functions regardless of the nature of the enabling technology. This divergence has been partially reconciled with the integrated taxonomy proposed by SESAR in the European ATM Master Plan 2025 [14], where the two taxonomies (AI Levels and LOAT) have been combined.

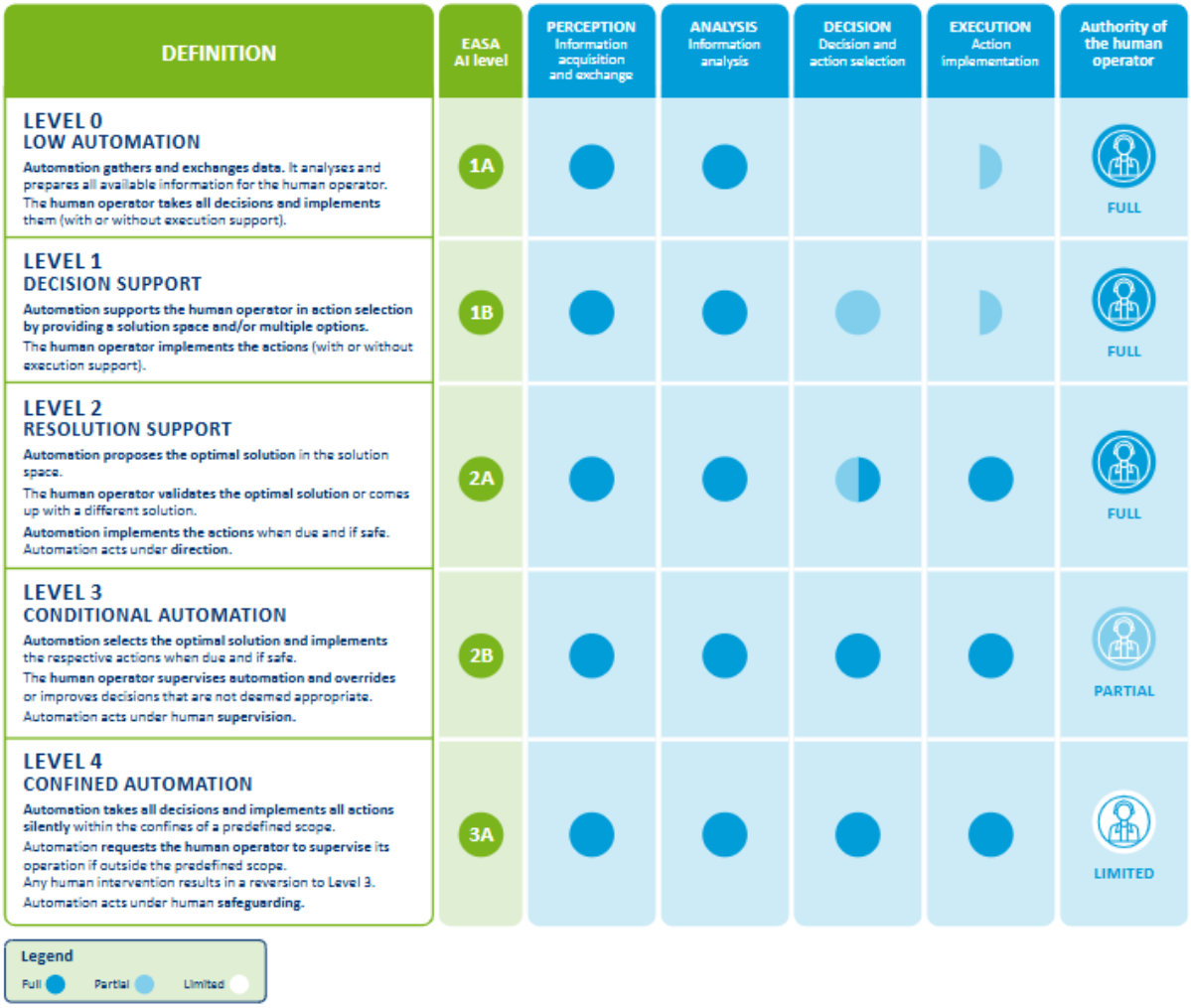

Figure 27. Levels of automation - taxonomy and correspondence to EASA AI levels

E.5 Inputs

The key inputs for the EASA subprocess are the description of the solution proposed by the applicant and the explanation of its AI level. The latter is particularly important, as the classification of the AI level forms the basis for understanding the degree of support or cooperation provided by the system to the human operation/s. At the same time, this aspect can be currently identified as challenging, as the current guidelines for classification are not sufficiently detailed or explanatory to guarantee an homogenous classification of the different solutions.

The key inputs for the SESAR subprocess is the information necessary to understand the proposed solution and changes it implies in the dimensions covered by the HP arguments, namely roles, working methods and procedures, human machine interaction, team structure and communication, and transitional factors. In this case the process of input collection is detailed and supported by dedicated SPR-INTEROP/OSED, VALP and VALR templates, tailored to the level of maturity of the solution analysed.

The necessary inputs for the performance of the four steps identified above can be summarized as follows:

HF subprocess - STEP(s)	INPUT(s)
Step 1 - Understand the ATM/UTM Concept	1. If available, review the needs, constraints and opportunities identified in the previous TRL level and use the input to start the concept design and evaluation process. 2. Description of the reference scenario (from SESAR project documentation e.g. SPR-INTEROP/OSED). 3. Initial list of Solution assumptions (from SESAR project documentation e.g. SPR-INTEROP/OSED). 4. Description of the solution(s) (from SESAR project documentation e.g. SPR-INTEROP/OSED). 5. Information on related SESAR Solutions (from SESAR project documentation).
Step 2 - Understand the HP implications	1. HP reviewed description of reference and solution and/or description of potential changes and ATM/UTM actors impacted (from Step1) 2. Consolidated list of Solution assumptions (from Step 1). 3. Project Benefit Mechanisms (from SESAR project documentation). 4. Existing previous HP assessment report(s). 5. Existing previous Validation report(s). 6. Existing HP Log. 7. Documentation related to solution (from SESAR project documentation). 8. List of SESAR Solutions to be considered in the project HP assessment (from Step 1). 9. Project planning documents: Project Management Plan, and Safety Plan (from SESAR project documentation). 10. P16.4.2 Repository of HF methods and tools (external input).[4]
Step 3 - Improve and validate the concept	1. List or register of HP issues/benefits & impacts and recommended HP activities, i.e. HP Log/HP assessment plan, (from Step 2); 2. VALP (SESAR project documentation).

[4] https://www.eurocontrol.int/ehp/

HF subprocess - STEP(s)	INPUT(s)
Step 4: Collate findings and conclude on transition to next TRL-phase	1. List of planned HP activities/HP assessment plan (from Step2). 2. Description of HP activities conducted (VALR or HP specific deliverable relating to an HP activity conducted by the HP specialist (from Step 3)). 3. Updated HP arguments, issues/benefits & impacts (including newly identified argument, issues & benefits, outcomes of the HP activities) (i.e. the updated HP Log from Step 3). 4. Register of HP recommendations and requirements (i.e. the updated HP Log (from Step 3)).

Table 66. Steps of the HP assessment process

HF Subprocess – Inputs – Key Differences
Item #1 – HOW TO UNDERSTAND THE SOLUTION **EASA –** The inputs collected in the EASA subprocess tend to focus on a narrow view of the solution proposed, limited to understanding its behaviours and its interactions with the human operator/s with reference to particular AI aspects such as AI operational explainability, Human-AI teaming, Modality of interaction and style of interface, Error management, Workload management, Failure management and alerting system, Customisation of human-AI interface **SESAR –** The input collected in the SESAR subprocess is more broadly focused on understanding the impact of the solution on the current working environment, exploring in particular the impact on roles, working methods and procedures of the concerned human actors, the impact on human machine interaction and on team structures and communication. It also explores the transitional aspects to be taken into account for a safe introduction of the solution in the working environment. All the aspects covered by the EASA subprocess are covered, although with a broader perspective and a more technology agnostic approach.
Item #1 – DIFFERENT LEVEL OF SUPPORT **EASA –** EASA offers some guidelines for the analysis of the solution and the classification of the level of AI in the HF perspective. Nevertheless, the guidelines are still quite vague and difficult to apply in a homogenous way. **SESAR –** SESAR offers a structured approach to input collection, supported by dedicated templates to be used at different stages of the process and at different maturity levels.

Table 67. Key differences for HF subprocess – inputs

HF Subprocess – Inputs – Overlaps
Item #1 – CONSISTENCY OF ARGUMENTS Notwithstanding the differences of approach highlighted above, the is an overall consistency in the arguments considered by the two subprocesses.

Table 68. Overlaps for HF subprocess – inputs

E.6 Outcomes

The intended outcome of the EASA HF for AI subprocess is to ensure the HF anticipated means of compliance are met. However, for Level 1A, existing guidelines and requirements for interface design should be used. For Level 1B, an initial set of design principles are proposed for the concept of operational explainability. For Level 2A and Level 2B, new objectives have been developed and others from existing human factors certification requirements and associated guidance have been adapted to account for the specific end-user needs linked to the introduction of AI-based systems.

The outputs for the performance of the four steps identified above can be summarized as follows:

HF subprocess - STEP(s)	OUTCOME(s)
Step 1 - Understand the ATM/UTM Concept	Reviewed and, potentially, amended description of the reference and solution scenario(s) (input to SPR-INTEROP/OSED and VALP). Description of ATM/UTM actors impacted and the potential changes to their work. Consolidated list of Solution assumptions (input to SPR-INTEROP/OSED and VALP), as well as constraints according to the characteristics of the current TRL-phase. List of SESAR Solutions to be considered in the HP assessment HP maturity of the Solution (optional)
Step 2 - Understand the HP implications	Identification of relevant HP arguments. List of Solution-specific HP issues and benefits together with their impact on HP and KPAs. List of HP validation objectives. List of activities and expected evidence. HP assessment plan and/or input to VALP

HF subprocess - STEP(s)	OUTCOME(s)
Step 3 - Improve and validate the concept	Description of all HP activities conducted and their outcomes (i.e. for SESAR exercises -input into VALR, for non-SESAR exercises (e.g. T A, CTA, stakeholder workshops etc. - reports documenting HP activity conducted and their output). Updated list/register of HP arguments, issues and benefits, validation objectives, with findings from activities conducted (Updated HP Log). Register of HP recommendations & requirements (Updated HP Log).
Step 4: Collate findings and conclude on transition to next TRL-phase	Completed maturity checklist for the appropriate TRL-phase (can be found in the HP Log in the dedicated tabs for each TRL-phase) to document and determine whether the HP assessment for a given TRL-phase can be finalised and closed. HP assessment report for a given TRL-phase. Updated HP recommendations and requirements in the HP Log.

Table 69. Outcomes of the HP process

HF Subprocess – Outcomes – Key Differences
Item #1 – COMPLIANCE VS IMPACT **EASA –** The output of the EASA subprocess provides information about the current conformity of the solution to the requirements described in the anticipated means of compliance and suggestions on how to cover the gaps that have been identified. **SESAR –** The output of the SESAR subprocess explores the impact of the proposed solution on the working environments highlighting possible issues that may concern the areas covered by the arguments. Recommendations are also provided to be considered in later stages of the design and validation process.

Table 70. Key differences for HF subprocess – outcomes

HF Subprocess – Outcomes – Overlaps
Item #1 – CONSISTENCY IN THE FOCUS Notwithstanding the differences highlighted above the two approaches maintain a common focus on human factors aspects.

Table 71. Overlaps for HF subprocess – outcomes

E.7 Assessment Methodology

EASA has not defined its own assessment methodology system, not even for the AI-specific objectives proposed in the AI Roadmap 2.0 and the Concept Papers. For this reason, it is reasonable to refer to established practices, such as those proposed by SESAR and EUROCONTROL methodologies. See above.

The assessment methodology proposed by SESAR is detailed in [27] and presupposes the use of the Arguments and activities outlined in Appendices A, B, C, and D. These latter specifically cover “HP Arguments, HP Activities and Required evidence for TRL0-TRL8” (Appendix A); “HP Log and document templates” (Appendix B); “HP Maturity criteria checklist for each TRL-phase (TRL0-TRL8)” (Appendix C) and “Guidance for writing HP benefits, issues and objectives” (Appendix D).

E.8 Performance Indicators

EASA has not defined its own KPIs, not even for the AI-specific objectives proposed in the AI Roadmap 2.0 and the Concept Papers. For this reason, it is reasonable to refer to established practices, such as those proposed by SESAR and EUROCONTROL methodologies. See below.

Within SESAR, KPIs are represented in terms of evidence or success criteria. For each argument and sub-argument, specific evidence is defined, tailored according to the relevant TRL thresholds.