EUROPEAN ORGANISATION
FOR THE SAFETY OF AIR NAVIGATION

EUROCONTROL

Guidelines for the Safety Assessment of ATM Procedures (SAAP)

SAF.ET1.ST03.1000-SAAP-01-00

Edition Number:	**0.10**
Edition Date:	**25.04.06**
Status:	**Proposed Issue**
Intended for:	**General Public**

EUROPEAN AIR TRAFFIC MANAGEMENT

DOCUMENT CHARACTERISTICS

TITLE		
Guidelines for the Safety Assessment of ATM Procedures (SAAP)		
EATMP Infocentre Reference:		
Document Identifier	**Edition Number:**	0.10
	Edition Date:	25.04.06

Abstract

The present document supplements the ANS Safety Assessment Methodology (SAM) by providing specific guidelines relating to the performance of safety assessments of ATM procedures. The guidelines focus on the PSSA step of the SAM and provide guidance to elaborating safety requirements and allocating the procedures assurance level (PAL).

Keywords

SAM	ATM Procedure	Task Analysis
SAAP	Assurance Level	Deviation Analysis
Safety Assessment	PAL	Barrier Analysis

Contact Person(s)	Tel	Unit
Patrick MANA	93295	DAP/SAF
Tzvetomir BLAJEV	93965	DAP/SAF
Holger MATTHIESEN	93713	DAS/AFN

STATUS, AUDIENCE AND ACCESSIBILITY					
Status		**Intended for**		**Accessible via**	
Working Draft	☐	General Public	☑	Intranet	☐
Draft	☐	EATMP Stakeholders	☐	Extranet	☐
Proposed Issue	☑	Restricted Audience	☐	Internet (www.eurocontrol.int)	☐
Released Issue	☐	*Printed & electronic copies of the document can be obtained from the EATMP Infocentre (see page iii)*			

ELECTRONIC SOURCE		
H:\Private\safety methodology\ATM procedures		
Host System	Software	Size
Windows_NT	Microsoft Word 8.0b	4000 Kb

EATMP Infocentre
EUROCONTROL Headquarters
96 Rue de la Fusée
B-1130 BRUSSELS

Tel: +32 (0)2 729 51 51
Fax: +32 (0)2 729 99 84
E-mail: eatmp.infocentre@eurocontrol.int

Open on 08:00 - 15:00 UTC from Monday to Thursday, incl.

DOCUMENT APPROVAL

The following table identifies all management authorities who have successively approved the present issue of this document.

AUTHORITY	NAME AND SIGNATURE	DATE
Please make sure that the EATMP Infocentre Reference is present on page ii.		
Chairman of the Safety Assessment Methodology Task Force	P.MANA	
Chairman of the EATMP Safety Team	E. MERCKX	

DOCUMENT CHANGE RECORD

The following table records the complete history of the successive editions of the present document.

EDITION NUMBER	EDITION DATE	INFOCENTRE REFERENCE	REASON FOR CHANGE	PAGES AFFECTED
0.1	01/05/2002		Creation of the working draft	All
0.2	01/09/2002		SQS comments	All
0.3	19/11/2002		Safety Improvement Subgroup Comments	All
0.4	14/01/2003		Safety Assessment of ATM Procedures Task Force Comments	All
0.5	15/02/2003		APDSG Comments	All
0.6	05/10/2003		EUROCONTOL Agency consultation	All
0.7	05/05/04		SAMTF consultation	All
0.8	04/12/05		Radical revision of the document format	All
0.9	12/03/06		Comments following first review cycle	All
0.10	25/04/06		Final review	All

CONTENTS

SUMMARY

The present document provides guidelines relating to the performance of a safety assessment of an ATM procedure. Particular focus is on the PSSA step of the safety assessment process.

The guidelines try to provide the answers to the following main elements of the safety assessment / PSSA:

- What is an ATM procedure and when should a safety assessment of an ATM procedure take place?
- How do these guidelines fit into the Safety Assessment Methodology (SAM)?
- How do we plan and prepare the PSSA of the ATM procedure?
- How do we analyse causes and failure modes?
- How do we assure the procedure development process and minimise risks?
- How do we specify the final safety requirements?

Since the first edition of the SAAP, the theoretical part has been complemented with a real-life example illustrating the application of the contents of the guidelines. The real-life example deals with a safety assessment (FHA & PSSA) of a procedure for *Independent Parallel Approaches* designed for the parallel instrument runways in Helsinki-Vantaa Airport.

Each chapter / annex of the document is thus supplemented with illustrations from the safety assessment at Helsinki-Vantaa Airport which also is included in its whole in Appendix B.

1. INTRODUCTION

1.1. Purpose

This document constitutes a Level 2 document of the EUROCONTROL Safety Assessment Methodology (SAM) as illustrated in figure 1-1:

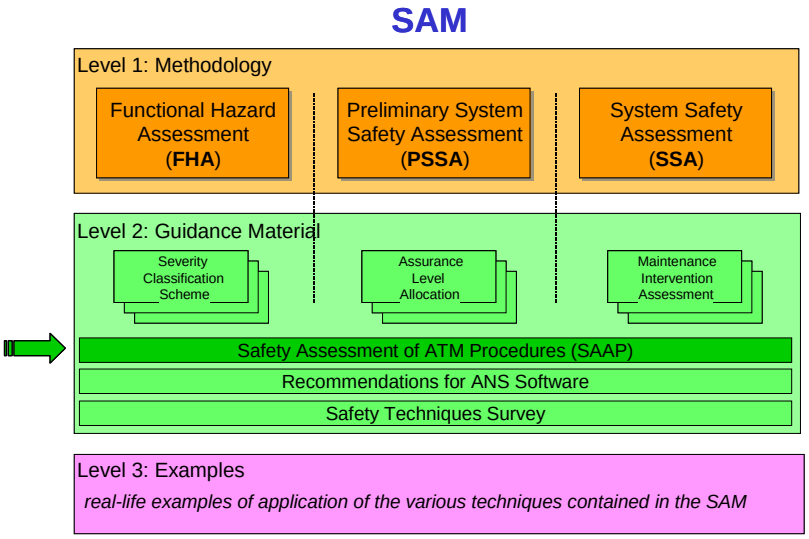


Figure 1-1: SAM structure (example)

Consequently, the document contains guidelines relating to the Safety Assessment of ATM Procedures. In particular, the guidelines are related to the PSSA step of the Safety Assessment. The document does not prescribe the only way of performing a safety assessment of ATM procedures. It rather provides one possible way to achieve such a task.

Therefore, the purpose of these guidelines is to provide more insight in the safety assessment of ATM Procedures by:

- Providing Guidance Material to the SAM for its application to the **PROCEDURE** system element (the other elements are Human and Equipment);
- Helping to rate the Procedure Assurance Level (PAL) by the level of risk associated with the procedure introduction into operations and procedure operations.

1.2. What is an ATM Procedure?

A procedure is a series of interrelated activities receiving inputs and transforming them into outputs (products).

Thus, to fulfil its objectives Air Navigation Systems have in place some tasks or processes (interrelated activities). Therefore, a procedure is a pre-specified way to carry out these tasks or a process of tasks. An example, which is a procedure, is the independent parallel approach procedure.

Figure 1-2 illustrates further some of the procedure types:

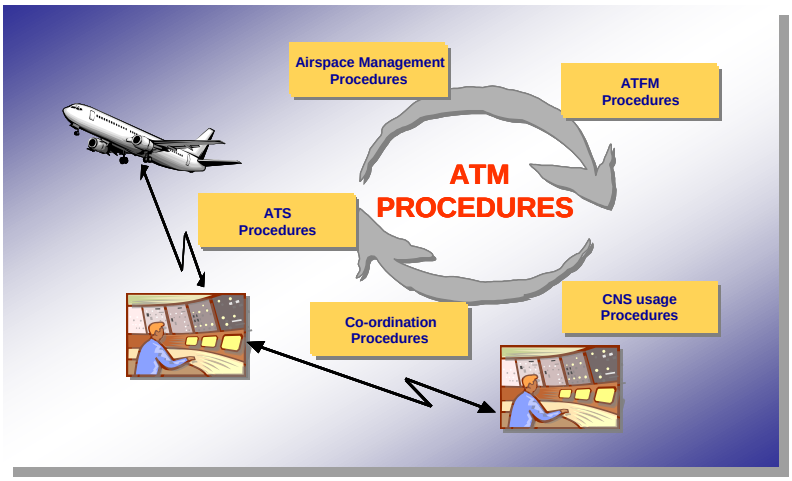


Figure 1-2: Procedures

Appendix A provides a taxonomy of the minimum level of ATM procedures which are covered by this document.

It is, however, in any case the responsibility of the Safety Organisation/Regulator that the SAAP is applied where applicable.

Note: Engineering procedures are not addressed here, but in the SAM-SSA Chapter 3 Guidance Material C.

1.3. When is an ATM Procedure Safety Assessment necessary?

A safety assessment of an ATM procedure is recommended (and required as per ESARR4) for any:

- Changes or modifications to existing ATM procedures;
- Introduction of new ATM procedures.

Note: Safety assessment of new ICAO procedures may not be required as already done by ICAO. However, the safety assessment of the local introduction of these ICAO procedures has to be done.

1.4. Who should participate in the Safety Assessment of an ATM Procedure?

A participation in the safety assessment process should be ensured of all the relevant and affected parties including ATCO, flight crew, flight operations staff, military personnel, aerodrome staff etc.

The procedure element should cover all the aspects relevant to ATM. In other words - all the issues for the safe movement of aircraft in the air or on the ground. Therefore, the procedure element covers both the ground and airborne part of the ATM. Some of the procedures are intended for the crew direct application – SID, STAR. Some of the procedures affect other parties – Civil-Military Co-ordination, Missed Approach.

Note: See SAM-FHA Chapter 3 Guidance A which helps to identify who should be part of the FHA.

1.5. Relationship between the Procedure Life Cycle and the Safety Assessment Process

Ideally, safety assessments should be performed as early as possible in the life cycle of the procedure as illustrated in Figure 1-3 below. This way, safety will evolve in parallel with the design maturation and it will enable more uncomplicated and cost-efficient risk mitigation.

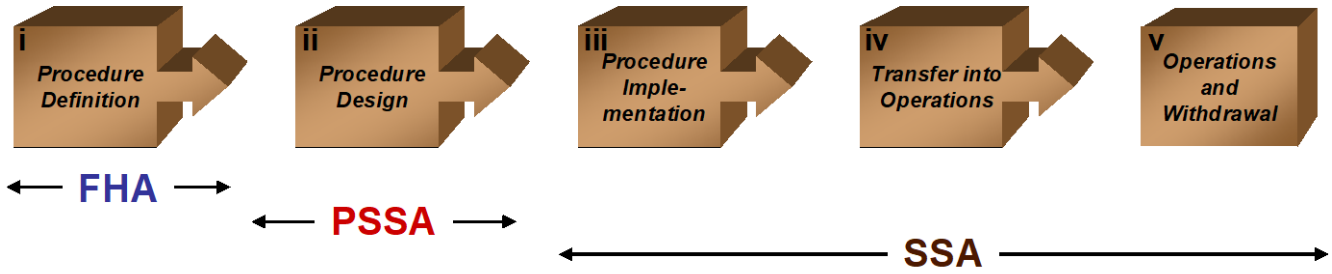


Figure 1-3: Ideal relationship between Procedure Life Cycle and the Safety Assessment Process

The ideal process is that the hazard identification is performed in connection with the definition phase whilst the risk mitigation is determined in connection with the design phase.

However, in reality the safety assessment process is often performed during later phases of the procedure life cycle as illustrated in Figure 1-4 below. This will not impair the quality of the safety assessment as such, but may in some cases imply that various constraints are put on risk mitigation (what is done cannot always be undone, e.g. construction or procurement).

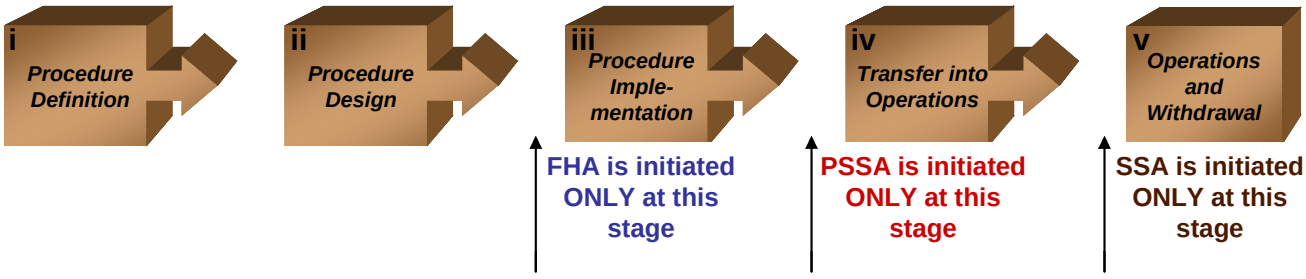


Figure 1-4: Example of Safety Assessment Process initiated too late in the Procedure Life Cycle

In general, the procedure development is a highly iterative process – especially the design and implementation phases. This should be utilised in the safety assessment process as it facilitates early implementation and validation of mitigation means, but the iterative aspect does also mean that the corresponding steps of the safety assessment process may have to be repeated (new design may lead to new hazards etc).

1.6. Structure of the Document

This document is composed of three main parts:

- Chapters, containing the present introduction (Chapter 1), the description of the SAAP process in relation to the SAM (Chapter 2) and a concise list of the activities to be performed when performing a Safety Assessment of an ATM procedure (Chapter 3);
- Annexes, which present specific Guidance Material related to each step (one Annex per step) of the process presented in Chapter 2;
- Appendices which provide background material and examples.

1.7. Target Audience

This document is specifically targeted at:

- ***ATM procedure designers***: Application in their domain of knowledge

The ATM procedure designers are responsible for the application of the safety assessment process (as it is defined by the safety practitioner) during the entire procedure life cycle.

Thus, ATM procedure designers are responsible for the performance of the FHA (what can go wrong?), the PSSA (how can we mitigate the hazards and which PAL shall be allocated?) and the SSA (does the mitigation means fulfil the objectives?).

- ***Safety practitioners:*** Correct process in a methodologically correct way

The safety practitioners are responsible for that the FHA, PSSA and SSA have been performed in accordance with the methodology. This includes that hazards are identified, that the hazard identification technique was correctly used, that a PAL is allocated and that mitigation means are verified and validated.

Thus, the safety practitioners are responsible for the link between the programme/project and the safety assessment process. They provide the methodological support to the different steps of the safety assessment process and the integration within the organisation Safety Management System (SMS).

- ***Other roles (Programme / Project Manager, Safety Manager, …):*** General understanding of the context

The other roles have no direct relation with the particular safety assessment, but a potential indirect role through the impact on their domain or work. Consequently, they need to have a general appreciation of the context of the SAAP.

1.8. Readership

The following table suggests a minimum reader's attention to this document.

	ATM Procedure Designer	Safety Practitioner	Other roles (Programme/ Project Manager, Safety Manager,...)
Chapter 1 – Introduction	✓	🕮	✓
Chapter 2 – Safety Assessment Process	🕮	🕮	✓.
Chapter 3 – Concise List of Activities to be Performed	🕮	🕮	✓
Annex A: PSSA Initiation – Transfer of FHA Output	🕮	✓	✓
Annex B: Analysis of Causes and Failure Modes - *Step 1*	✓	🕮	✓
Annex C: Analysis of Causes and Failure Modes - *Step 2*	✓	🕮	✓
Annex D: Safety Requirements Specification – *Step 1*	🕮	🕮	✓
Annex E: Safety Requirements Specification – *Step 2*	🕮	🕮	✓
Appendix A: Taxonomy of ATM procedures	✓	✓	N/A
Appendix B: Example of Assessment of Independent Parallel Approach Procedure at Helsinki-Vantaa Airport	✓	🕮	N/A

🕮: Detailed knowledge

✓: Aware

N/A: Not Applicable

2. SAM AND SAAP PROCESSES

2.1. Overall SAM Process Description

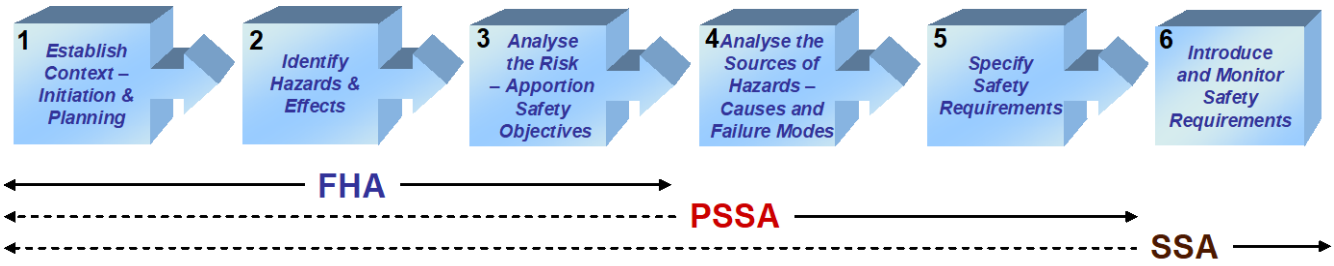


Figure 2-1: SAM process

The generic safety assessment process as described in the SAM level 1 documents is illustrated in broad outline in figure 2-1. As shown, the process includes the three steps: FHA, PSSA and SSA. The steps are illustrated with solid lines while the dotted lines illustrate that the process is iterative and findings during the PSSA may lead to re-initiation of the hazard identification or the Safety Objective specification. Similarly, findings during the SSA step may lead to re-iteration of the hazard identification and/or safety requirement specification (e.g. new causes or hazards identified, safety requirements insufficient).

When performing a safety assessment of an ***ATM procedure***, the FHA step shall be conducted as described in the SAM-FHA. Equally, the SSA step shall be conducted as described in the SAM-SSA. The present guidelines relate to the PSSA step and are adding particular guidance when performing an assessment of an ATM procedure.

As the safety assessment, as mentioned, is a highly iterative process, additional hazards may be identified during the PSSA step – in particular when the procedure goes though a functional breakdown (cf. Annex B4).

2.2. The FHA Process

Figure 2-2: FHA process

The objective of the **FHA** is:

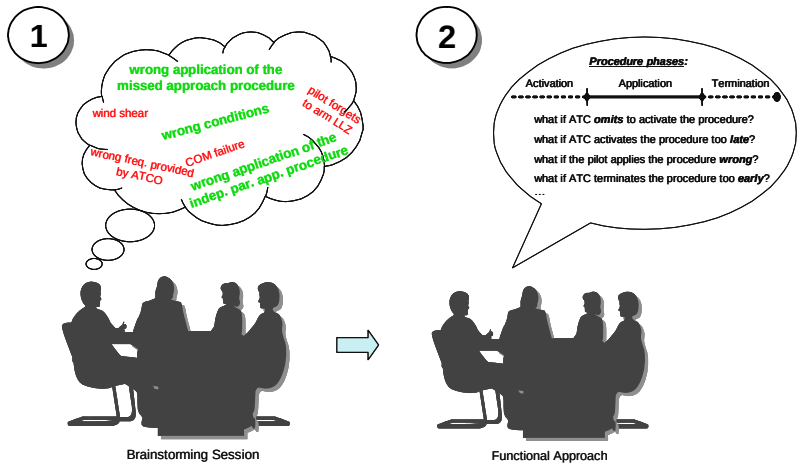
1. to identify hazards, i.e. what can go wrong?
2. to identify the associated effects on operations of the hazards
3. to assess the severities of these effects
4. to establish the safety objectives expressing the maximum acceptable frequency of the hazard's occurrence.

For the identification of hazards, brainstorming methods combined with a functional approach should be applied to ensure completeness.

For the identification of hazard effects, the consequences for the controllers'/pilots' ability to perform his/her tasks should be considered as well as the potential degradation of the ANS system as a whole and the potential functional degradation of the capabilities of the ground ATM or the Aircraft equipment.

For the establishment of safety objectives, an agreed safety objective classification scheme should be applied and the safety objectives be based upon severities allocated on each hazard effect.

Illustrations from safety assessment at Helsinki-Vantaa Airport (Appendix B):



The illustrations show the applied two steps of the hazard identification session.

1. *Brainstorming where the participating experts are asked to express any free-flowing safety issue they can think of.*
2. *Functional approach where key words (omit, wrong, late, early, …) in a structured way are aligned with the phases of the procedure to identify additional hazards, if any.*

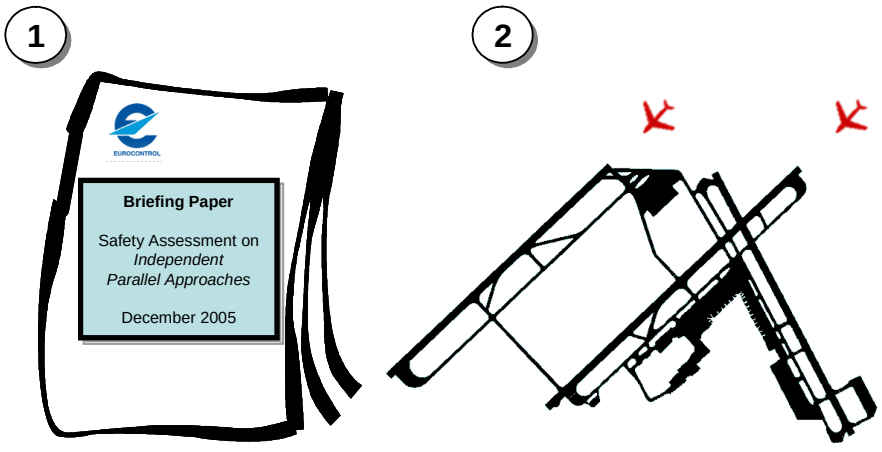
Table 2-1 below provides a brief overview of the five steps of the SAM-FHA process. Furthermore, the links to the relevant parts of the SAM-FHA documents and the safety assessment contained in Appendix B are provided.

SAM-FHA steps	Reference in SAM-FHA	Reference in Appendix B
1. Initiation - *develop a level of understanding of the ATM procedure*	SAM-FHA Chapter 1 Chapter 1 – Guidance Material A	Chapter 2 Chapter 4 Appendix A Appendix D Appendix R
2. Planning - *define the scope and objectives of the FHA*	SAM-FHA Chapter 2 Chapter 2 – Guidance Material A	Chapter 3.2.2 Appendix E
3. Safety Objectives Specification - *identify the hazard and the hazard effects, assess the severities per effect and specify the safety objectives*	SAM-FHA Chapter 3 Chapter 3 – Guidance Material A Chapter 3 – Guidance Material B1+B2 Chapter 3 – Guidance Material C Chapter 3 – Guidance Material D Chapter 3 – Guidance Material E Chapter 3 – Guidance Material F Chapter 3 – Guidance Material G Chapter 3 – Guidance Material H Chapter 3 – Guidance Material I Chapter 3 – Guidance Material J	Chapter 4 Appendix F Appendix H
4. Evaluation - *evaluate that safety objectives meet organisation safety targets, evaluate the assumptions, ensure completeness of process*	SAM-FHA Chapter 4 Chapter 4 – Guidance Material A Chapter 4 – Guidance Material B Chapter 4 – Guidance Material C	Chapter 4.3 Appendix L2
5. Completion - *document and disseminate the results*	SAM-FHA Chapter 5 Chapter 5 – Guidance Material A	The complete Appendix B constitutes the documentation of the results

Table 2-1: overview of FHA process

Note: For additional detail, refer to the SAM-FHA.

Illustrations from safety assessment at Helsinki-Vantaa Airport (Appendix B):



The illustrations present two important planning elements.

1. *Briefing material issued to all experts participating in the FHA and PSSA sessions for familiarisation purposes.*
2. *The scenario to be assessed – presenting the runway layout and the two parallel runways.*

2.3. The PSSA Process

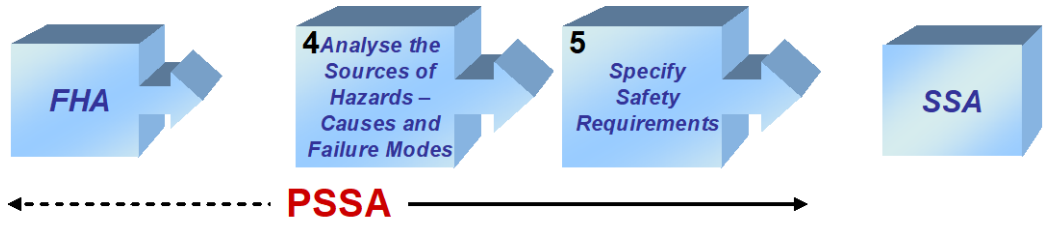


Figure 2-3: overall PSSA process

The objective of the **PSSA** is:

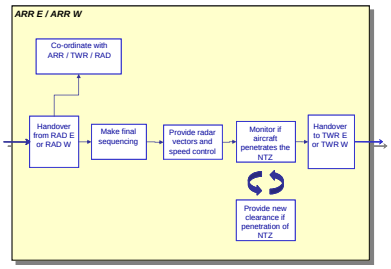
1. to identify the various causes and failure modes which may lead to the hazards identified during the FHA
2. to determine suitable risk mitigation means, which either eliminate, reduce or control the hazards and/or their effects, as well as set the development effort to be applied during the further procedure development.

For the identification of causes and failure modes, various identification methods and supplementary analyses should be applied (cf. Annex B and C). During these methods/analyses, further hazards may be identified leading to a re-iteration of the hazard assessment and thus the necessary determination of hazard effects and safety objectives.

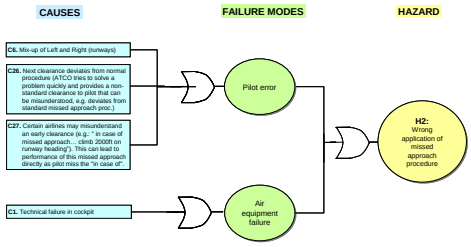
For the determination of the risk mitigation means, the specialist knowledge and the ideas of the experts at the PSSA session form input to further analyses leading to a final set of detailed safety requirements (cf. Annex D and E).

Illustrations from safety assessment at Helsinki-Vantaa Airport (Appendix B):

1



2



The illustrations present two elements of the PSSA process.

1. *Task decomposition - for the arrival controller - utilised in the task analysis for identification of causes.*
2. *Fault tree illustrating the relationship between causes, failure modes and hazards.*

An overall introduction to the PSSA process and the tasks to be performed is provided below. In addition, each separate PSSA step – illustrated in figure 2-4 below - is addressed in detail in the Annexes to these guidelines.

Figure 2-4: detailed SAM-PSSA process

This process is applied whether it is the people, procedure or equipment element of an ATM system being assessed.

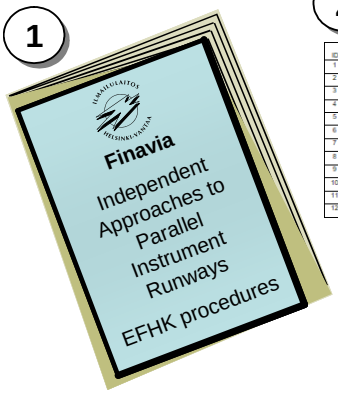
Table 2-1 provides a concise overview of the SAM-PSSA process with the focus on an ATM procedure. Furthermore, the links to the relevant subsequent annexes and the safety assessment at Helsinki-Vantaa contained in Appendix B are provided.

SAM-PSSA steps	Major tasks	Relevant Annex	Reference in Appendix B
1. Initiation - *develop a level of understanding of the ATM procedure* 	• Gather all necessary information describing the ATM procedure including the Description of the Procedure, the Operational Environment Description and the assumptions (from the FHA step). • Update the information as necessary.	Annex A	Chapter 2 Appendix D Appendix I
2. Planning - *define the scope and objectives of the PSSA* 	• Identify and describe the PSSA activities to be performed • Submit the plan for review as required • Disseminate the final PSSA plan	Annex A	Chapter 3.2.3 Appendix I

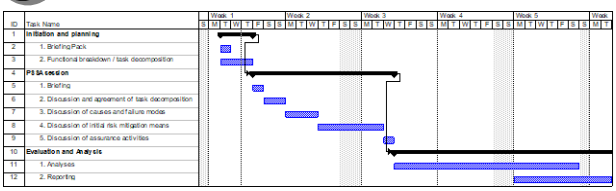
Table 2-2a: detailed PSSA process

Illustrations from safety assessment at Helsinki-Vantaa Airport (Appendix B):

1



2



The illustrations present two elements of the PSSA initiation and planning.

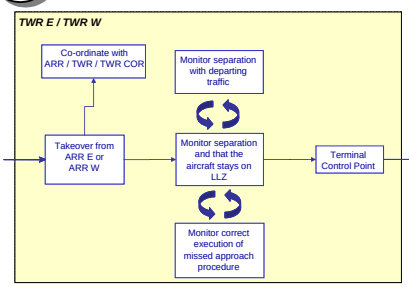
1. *The draft procedure description developed by Finavia (cf. Appendix R in Appendix C).*
2. *Gantt chart depicting all activities to be performed in relation with the PSSA.*

SAM-PSSA steps	Major tasks	Relevant Annex	Reference in Appendix B
3. Safety requirements specification - *derive the safety requirements* 	• Develop a functional breakdown by decomposing the ATM procedure into tasks • Identify causes and failure modes for each task • Apply risk mitigation strategies including allocation of PAL • Apportion safety objectives into safety requirements • Balance/reconcile safety requirements	Annex B Annex C Annex D Annex E	Chapter 5 Appendix J Appendix L1 Appendix M Appendix O

Table 2-2b: detailed PSSA process

Illustrations from safety assessment at Helsinki-Vantaa Airport (Appendix B):

1



2

PAL 3

Design and Validation	
ii1.	Establish an acceptable risk level (in qualitative terms)
ii2.	Ensure that HMI has been assessed
ii3.	Ensure suitably validation at different levels
ii4.	Ensure robustness

3

SR6: Aircraft operators shall examine the cockpit checklists in order to ensure that it as a minimum includes:

- checking of whether correct LLZ is armed
- re-checking if runway is changed

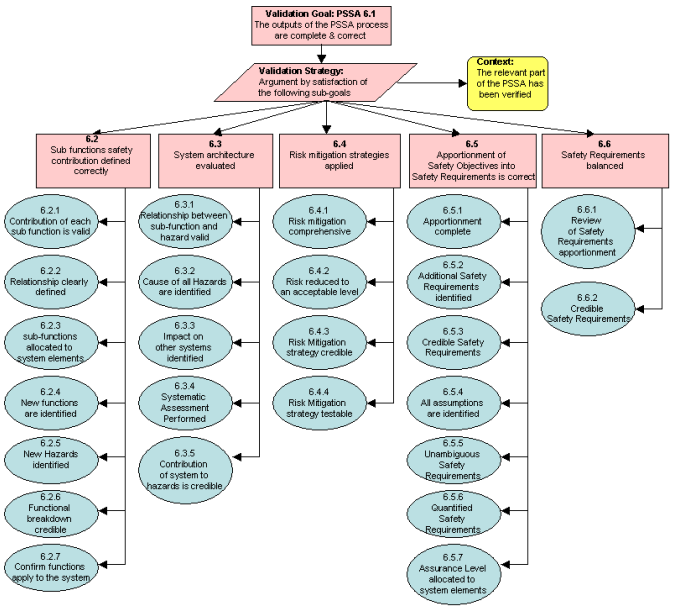
The illustrations reflect elements of the safety requirements specification.

1. *The functional breakdown is represented by the task decomposition used to identify causes and failure modes.*
2. *A PAL 3 has been allocated for which reason these listed objectives shall be fulfilled during the Design and Validation of the procedure.*
3. *30 safety requirements were developed. One requirement on the aircraft operator is exemplified.*

SAM-PSSA steps	Major tasks	Relevant Annex	Reference in Appendix B
4. Evaluation - *evaluate the results, the assumptions and the process* 	• Review and analyse whether the safety requirements can be expected to meet the safety objectives and that the identification of safety requirements is complete • Evaluate whether the assumptions remain correct and complete • Evaluate the PSSA process to ensure that the process is complete and in accordance with the plan	***Note: For additional detail, refer to the SAM-PSSA***	Chapter 5.3.3 Appendix L2

Table 2-2c: detailed PSSA process

Illustrations from safety assessment at Helsinki-Vantaa Airport (Appendix B):



The illustration presents a verification and validation means – by the use of a Goal Structured Notation - in relation to the evaluation of the PSSA process.

The real-life example in Appendix C does not contain this particular element.

Note: For additional detail, refer to the SAM-PSSA.

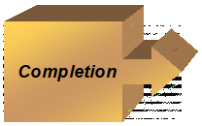
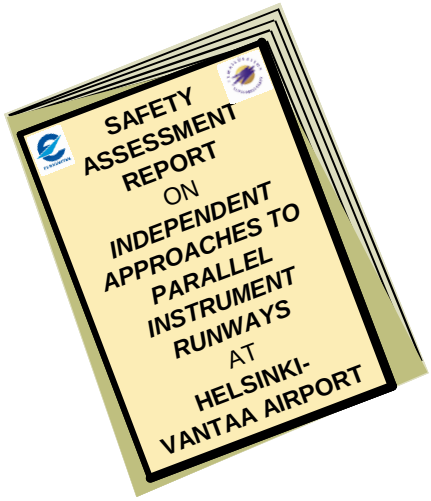
SAM-PSSA steps	Major tasks	Relevant Annex	Reference in Appendix B
5. Completion - *document and disseminate the results* 	• Document the results • Disseminate the results as required	***Note: For additional detail, refer to the SAM-PSSA***	*The complete Appendix B constitutes the documentation of the results*

Table 2-2d: detailed PSSA process

Illustrations from safety assessment at Helsinki-Vantaa Airport (Appendix B):



The illustration depicts the final output of the PSSA step: the Safety Assessment Report (Appendix B).

2.4. The SSA Process

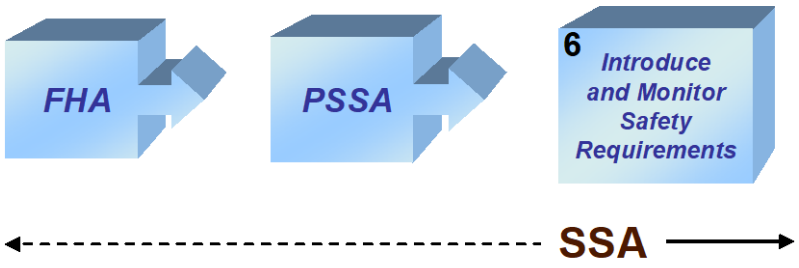


Figure 2-5: overall SSA process

The objective of the **SSA** is:

1. to validate whether the safety requirements stemming from the PSSA are sufficient and fulfil the safety objectives of the FHA

2. to discuss the PAL satisfaction.

For the validation of the safety objectives and requirements, various examination techniques, simulations, trial exercises, shadow-operations and other pre- and post-operational assessments should be utilised.

For the discussion of the PAL satisfaction, it shall be verified whether all PAL activities have been implemented suitably - not only relating to the activities relevant for the design & validation and implementation phases, but also those activities which are defined for the (upcoming) transfer into operations and operations phases.

Illustrations from safety assessment at Helsinki-Vantaa Airport (Appendix B):

During the SSA step, the results of the FHA and PSSA steps are validated and verified.

Thus, evidence shall be sought to demonstrate that the safety objectives are met through fulfilment of the safety requirements.

The safety assessment at Helsinki-Vantaa (Appendix C) does not include the SSA step. The illustration to the left is a tower simulator.

Note: For additional detail, refer to the SAM-SSA.

SAM-SSA steps	Reference in SAM-SSA	Reference in Appendix B
1. Initiation - *develop a level of understanding of the ATM procedure and the underlying framework*	SAM-SSA Chapter 1	None at present
2. Planning - *define the scope and objectives of the SSA*	SAM-SSA Chapter 2	None at present
3. Safety Assurance and Evidence Collection - *collect the evidence to demonstrate that the procedure - when implemented- meets an acceptable risk*	SAM-SSA Chapter 3	None at present
4. Evaluation - *ensure that the results are complete and properly recorded, evaluate the assumptions, ensure completeness of process*	SAM-SSA Chapter 4 Chapter 4 – Guidance Material A Chapter 4 – Guidance Material B Chapter 4 – Guidance Material C	None at present
5. Completion - *document and disseminate the results*	SAM-SSA Chapter 5 Chapter 5 – Guidance Material A	None at present

Table 2-3: overview of SSA process

Note: For additional detail, refer to the SAM-SSA.

3. CONCISE LIST OF ACTIVITIES TO BE PERFORMED

3.1. List of Activities

This Subchapter provides an incremental list of the activities to be performed as described in this SAAP. The list is concise by purpose and further detailing and rationales are found in the previous Chapter and the subsequent Annexes of this document.

FHA **Develop the FHA as described in the SAM-FHA**

PSSA **Plan the PSSA session including:**

1. set scope and contents for the session
2. prepare agenda for the session
3. invite experts to the session
4. revisit the operational environment definition and assumptions and refine if needed
5. prepare draft functional breakdown / task decompositions
6. prepare / update briefing paper
7. issue the briefing paper to the participating experts.

Perform the PSSA session including:

1. summarise the findings of the FHA
2. discuss and agree upon the task decompositions to be applied
3. identify causes and failure modes based upon the agreed task decompositions
4. identify initial risk mitigation means with outset in the identified set of causes and failure modes
5. discuss procedure assurance activities and allocate the PAL.

Perform the further analysis work including:

1. prepare traceability matrices (or apply other suitable tool) to correlate causes with initial risk mitigation means and ensure completeness
2. develop fault trees (or similar)
3. identify the complete set of risk mitigation means
4. develop the safety requirements
5. develop the safety assessment report documenting the results and disseminate to stakeholders.

SSA **Perform the SSA as described in the SAM-SSA**

3.2. List of Activities (Including References)

This Subchapter complements the incremental list of activities to be performed from Subchapter 3.1 with relevant references.

		reference
FHA	**Develop the FHA**	SAM-FHA, Appendix B (Chapters 2, 3, 4 + Appendices A, D, E, F, G, H, K)
PSSA	**Plan the PSSA session including:**	
	1. set scope and contents for the session	Appendix B (Chapt. 3)
	2. prepare agenda for the session	Appendix B (App. I)
	3. invite experts to the session	-
	4. revisit the operational environment definition & assumptions (refine if needed)	Annex A, Appendix B (App. D)
	5. prepare draft functional breakdown / task decompositions	Annex B4, Appendix B (App. D)
	6. prepare / update briefing paper	-
	7. issue the briefing paper to the participating experts.	-
	Perform the PSSA session including:	
	1. summarise the findings of the FHA	Appendix B (App. H)
	2. discuss and agree upon the task decompositions to be applied	Appendix B (App. B)
	3. identify causes and failure modes based upon the agreed task decompositions	Annex B, Appendix B (App. L1 & App. N)
	4. identify initial risk mitigation means with outset in the identified set of causes and failure modes	Annex D, Appendix B (App. N)
	5. discuss procedure assurance activities and allocate the PAL.	Annex E, Appendix B (Chapt. 5.3.2 & App. M)
	Perform the further analysis work including:	
	1. prepare traceability matrices (or apply other suitable tool) to correlate causes with initial risk mitigation means and ensure completeness	Appendix B (App. L1)
	2. develop fault trees (or similar)	Annex C, Appendix B (App. J)
	3. identify the complete set of risk mitigation means	Appendix B (App. L2)
	4. develop the safety requirements	Annex D, Appendix B (App. O)
	5. develop the safety assessment report documenting the results and disseminate to stakeholders.	Appendix B in its whole
SSA	**Perform the SSA**	SAM-SSA

ANNEX A

PSSA INITIATION

- TRANSFER OF FHA OUTPUT -

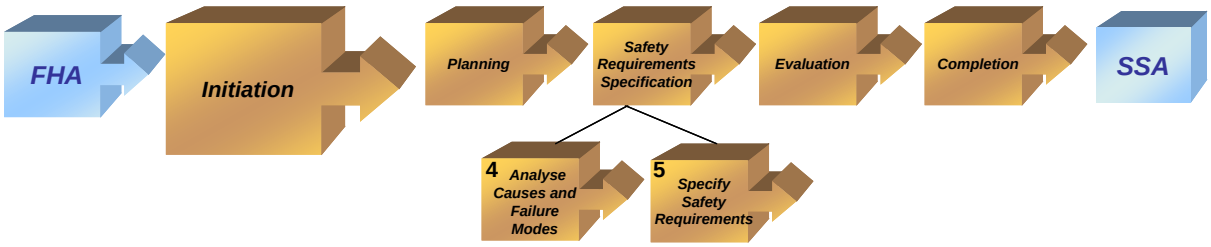


Figure A-1: PSSA process

Inputs

FROM THE FHA STEP

- Description of the procedure;
- Operational Environment Description;
- Assumptions.
-

OTHER INPUT

Other input is depending on the phase in the procedure life cycle, but could include:

- Design and validation constraints (if in design phase);
- Implementation constraints (if in implementation level);
- Transfer and operational constraints (if in transfer phase)
- Applicable legislation, rules, standards and procedures.

Note: See SAM-FHA Guidance material A of Chapter 1 for further detail.

Outputs

1. Refined description of the procedure, procedure's boundaries and interfaces;
2. Refined description of the Operational and Legislative Environment;
3. Revisited assumptions.

A.1 Procedure Description

The refined description of the procedure should contain at least:

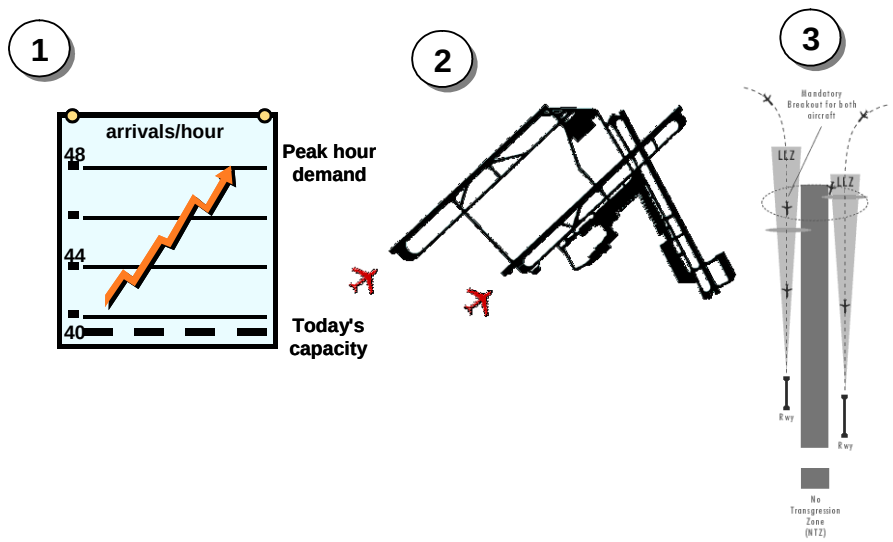
- ***Operational justification*** – why the procedure is needed - alternative means to achieve the same ANS functionality (cf. Appendix B: Section 2.4 + Appendix D)

- ***Functional description*** – this should be independent of the procedure realisation. For example the function "provide means for identification of potential conflicts" can be fulfilled by equipment (MTCD), procedure or combination of equipment and procedure (cf. Appendix B: Section 2.2 + Appendix D)

- ***Operational description*** – how the procedure will fulfil the functions. Which are the "actors" involved in the procedure use – ATM, Flight Crew, Aerodrome Services, military authorities etc. Description of the procedure elements – task scenarios for each of the actors (cf. Appendix B: Appendices A + B + R)

- ***Boundaries and Interfaces*** – logical (communication, control and feedback channels) - physical (spatial location of the controllers, other people, equipment and airspace) interfaces and timing boundaries (period of usage) (Appendix B: Appendix D + R).

Illustrations from safety assessment at Helsinki-Vantaa Airport (Appendix C):



The illustrations are all elements of the procedure description.

1. *The operational justification is the capacity increase achieved by using the parallel runways more efficiently.*
2. *The scenario with the two parallel runways forms part of the operational description.*
3. *The breakout representation is another element of the operational description.*

A.2 Operational and Legislative Environment Description

The refined operational and legislative environment description should contain at least:

- ***Operational environment –*** traffic volume, complexity and equipage, ATM equipment to be used/HMI, phase of flight, airspace organisation, ATFM constraints, prevailing and possible meteorological conditions, efficiency and environment constraints and risk trade-offs (cf. Appendix B: Section 2.5 + Appendix D)

- ***Legislative environment*** – relevant rules, standards, practices and procedures (cf. Appendix B: Section 2.6).

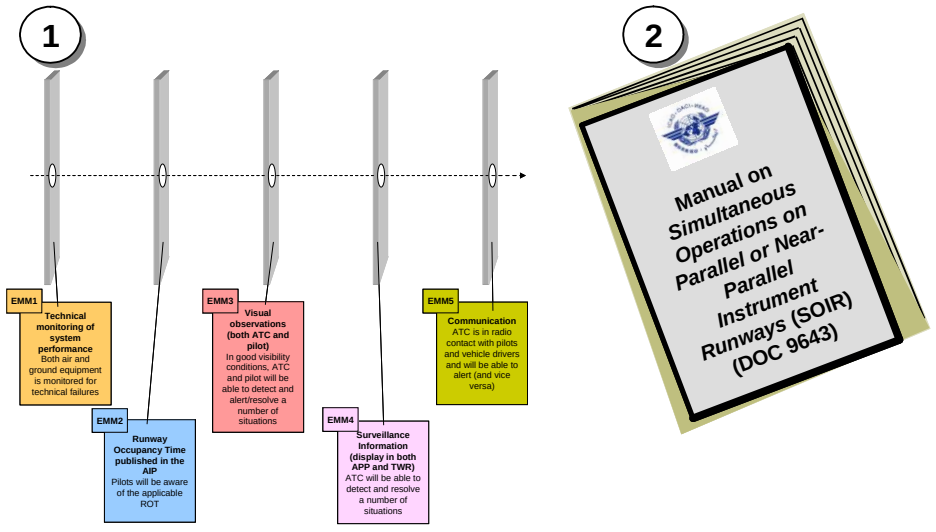
A.3 Assumptions

The revisited assumptions should contain at least:

- ***New identified assumptions*** – raised when designing the procedure (cf. Appendix B: Appendix D)

- ***Validation of existing assumptions*** – all assumptions carried on from the FHA initiation should be validated in relation to credibility and completeness (cf. Appendix B: Sections 2.3, 4 and 5).

Illustrations from safety assessment at Helsinki-Vantaa Airport (Appendix C):



The two illustrations relate to the operational and legislative environment.

1. *Five external mitigation means have been identified representing barriers - outside the system being assessed – which reduce the risk of an accident.*
2. *The ICAO manual on Simultaneous Operations on Parallel or Near-Parallel Instrument Runways forms part of the legislative environment.*

ANNEX B

- ANALYSIS OF

CAUSES AND FAILURE MODES -

STEP 1

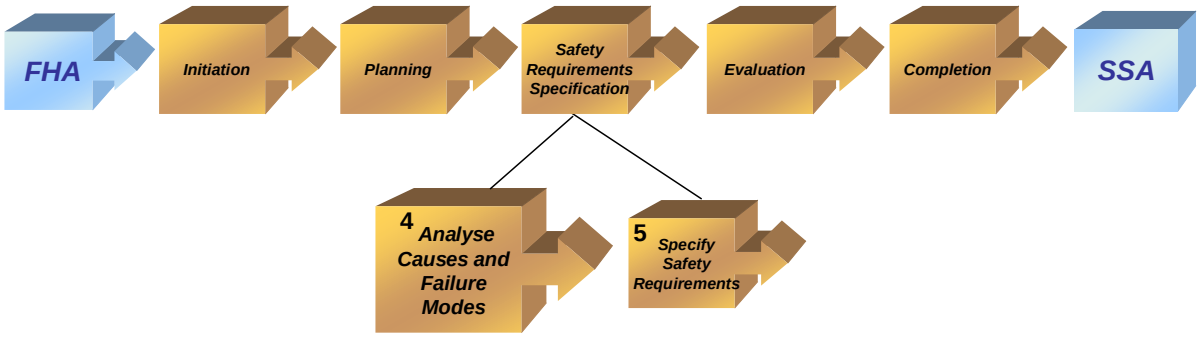


Figure B-1: PSSA process

Inputs

Refined description of the procedure, procedure's boundaries and interfaces;

Refined description of the Operational and Legislative Environment;

Revisited assumptions;

List of identified Hazards and Effects;

Initial list of causes and failure modes identified in connection with the brainstorming exercise in the FHA.

Outputs

1. List of causes and failure modes.

B.1 How Procedures Affect Safety

A procedure is a specified protocol for human activity. The reason to specify the human activity is to make it more efficient and standardised and ***less risky***. The safety impact of the procedure could be:

- ***Positive Impact ("Success Case"):*** There are two scenarios for positive impact on safety:
  1. Procedure as Risk Mitigation for risk not created by the procedure.
  2. Procedure as Risk Mitigation for the risk created by the procedure itself.

  The list of potential risk reducing effects is received from the performed Change Analysis, described further in B4.

- ***Negative Impact ("Failure Case"):*** There are two ways the procedure could negatively impair safety:
  1. Not to mitigate the risk to the required level. This is considering the main objective of the procedure – to reduce the risk, existing for some operational situations. This risk is normally not created by the procedure – for example the risk of low visibility operations at an airport. The procedures for low visibility operations are aimed at reducing this operational risk;
  2. To create additional risk. To be the reason of either a new hazard or to increase the risk of already existing hazards. This is both when the procedure is applied as specified, and when the procedure is failed to apply – human error.

Thus, the negative impact is either due to inefficiency of the procedure or from failure.

The latter aspect concerning the creation of additional risk is considered in the following section.

B.2 How the Procedure Could Create Additional Risk

The procedure could create additional risk because of:

- ***Procedure not followed:***

  Deliberate - non-adherence to procedure;

  Non-deliberate - error in performing the specified procedure. A controller (or other actor – pilot, airport vehicle driver etc.) failure to apply the specified procedure could be the source of the hazard such as slip, lapses, workload, …

- ***Procedure followed:***

  Human error induced by the procedure - but not in performing this procedure, in performing other procedure or process. A controller (or other actor – pilot, airport vehicle driver etc.) failure to apply other procedure or process because of complexity, workload, ...

  Wrong procedure design (procedure flaw) - even if the procedure is applied as specified the hazard may arise because of wrong procedure. A procedure can be wrong by being incorrect, incomplete, ...

Figure B-2 illustrates the principles of the negative impact.

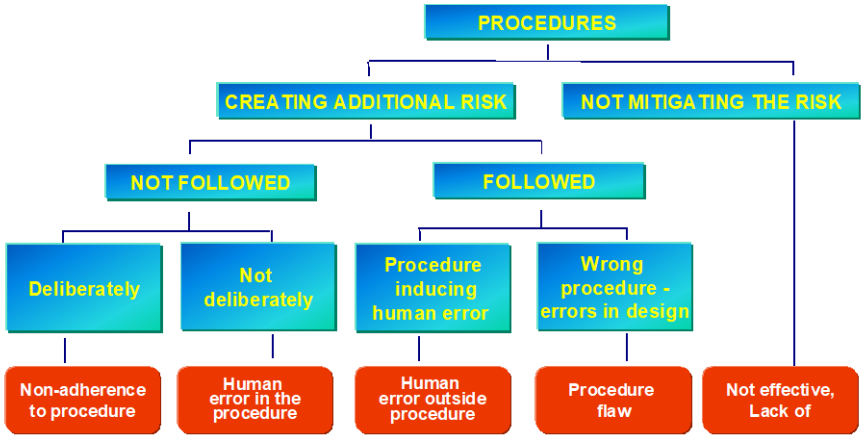


Figure B-2: additional risk created by the procedure

B.3 When Additional Hazards are Identified During PSSA

The sections above have highlighted how procedures may affect safety and how they could create additional risk. As previously mentioned, a safety assessment is an iterative process why hazards may be identified during the PSSA step as well even though the FHA is the step during which the hazards are identified. One of the reasons is that the ***functional breakdown*** made during the PSSA is even more detailed than the functional approach applied for the hazard identification during the FHA.

The functional breakdown and the identification of causes and failure modes are described in the following sections.

B.4 Causes and Failure Modes

There are three sources to the identification of causes and failure modes:

1. Results of the FHA – during the brainstorming and discussions performed in connection with the FHA, a variety of safety concerns have been identified covering both the actual hazards, but also causes, failure modes, effects etc. Thus, a number of the findings of the brainstorming constitute in reality a set of causes or failure modes to the hazards. These causes and failure modes shall be passed on to the PSSA step.

2. Task analysis – during a task analysis, the deviation from a specific task to be performed is identified, for example that the pilot omits to follow clearance or the ATCO fails to include the cleared level. Such deviation may lead to a hazard. The task analysis is described in more detail below.

3. Change analysis – during the change analysis, the changes in the system due to introduction of the procedure are identified, for example that the procedure introduces changes to the work routine of the controller. Such change may lead to a hazard, but may also have a reducing effect on the risk if the controller is considered to be a barrier. The change analysis is described in more detail below.

TASK ANALYSIS

Functional breakdown - the identification of deviation is performed by decomposing the procedure into tasks and subsequently list the possible failures of each task.

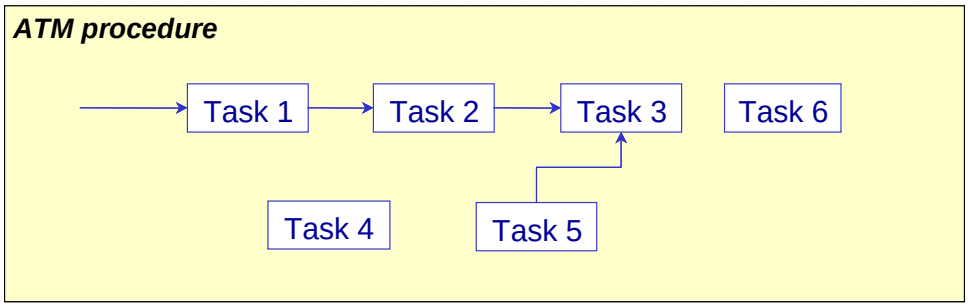
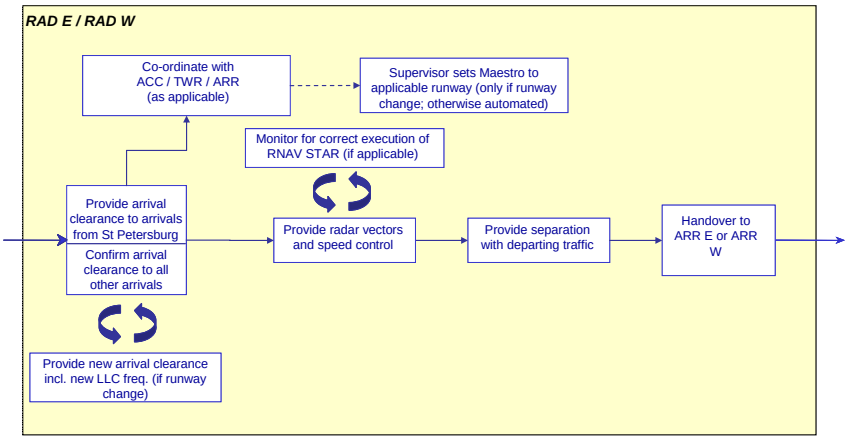


Figure B-3: tasks of a procedure, example

Illustrations from safety assessment at Helsinki-Vantaa Airport (Appendix C):



The task decomposition depicts the tasks of the approach controller in Helsinki-Vantaa airport.

The task scenario describes task by task the activity of the relevant actor: controller, pilot, military controller, military pilot, vehicle driver, maintenance staff, …

Thus, the task describes the visible part of the human behaviour, e.g. controller to identify the aircraft, pilot to start descent etc. This is different from a cognitive description of the activity.

List of causes and failure modes – for each identified task, series of checklist questions are applied (Table B-2). The purpose is to identify the different ways by which the task can fail. This is done in two steps:

- Identify basic task attributes like input, action, speed, output;
- For each attribute apply the checklist with the possible failure modes – like "omit the input", "speed not appropriate" etc. Table B-1 presents an example related to the task decompositions from the safety assessment of the procedure for Independent Parallel Approaches.

Task "provide arrival clearance					
omit	early	erroneous	late	out of sequence	out of range
✓	-	✓	✓	-	-
e.g. the ATCO failed to provide the ARR clr		*e.g. the ATCO provided a wrong ARR clr*	*e.g. the pilot confirmed the ARR clr late*		

Table B-1: coupling of tasks and checklist questions, example

In addition, the following list of key words may be used during the analysis of failure modes (***Note: See also SAM-FHA Chapter 3 Guidance Material B***):

Total loss of task	Failure to start
Partial loss of task	Failure to stop
Error of input/ output:	Failure to switch
- missing data (partial loss, total loss)	Delayed operation (too late)
- detected erroneous/corrupted data (credible error/corruption)	Premature operation (too early)
- undetected erroneous/corrupted data (incredible error/corruption)	Inadvertent operation
- spontaneous data	Intermittent or erratic operation
- out of sequence	Modified operation
- out of range	Misheard
Misdirection of data	Misunderstood
Inconsistent information	Used beyond intent
Erroneous updating	Out of time synchronisation

Table B-2: checklist questions

CHANGE ANALYSIS

The aim of the change analysis is to identify the changes that will happen in the system (people, procedure, equipment) no matter how "small" they appear.

The changes may be the cause of potential hazards, but also have a potential risk reducing effect.

The analyst should examine at least the following areas for possible changes:

- Human Factors;
- Equipment;
- Procedures within the scope of Appendix A;
- Context of the operations
- Physical location of the actors.

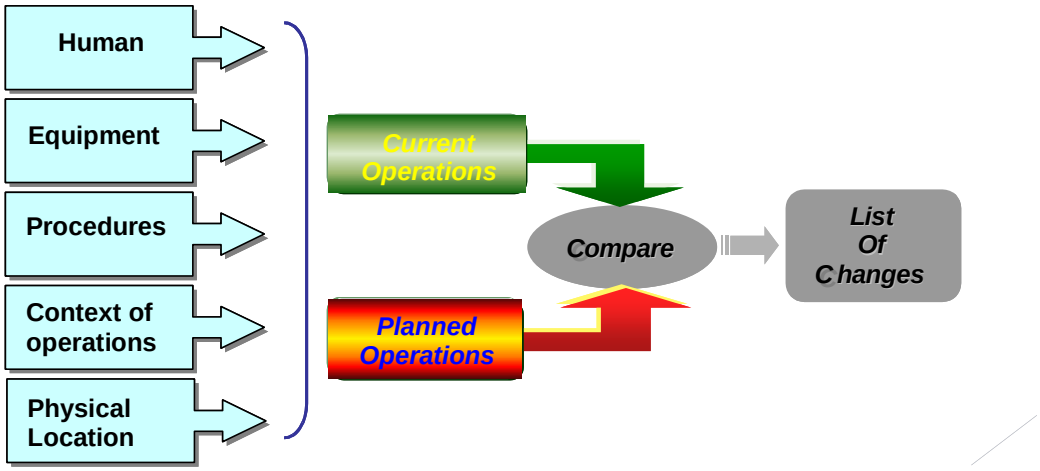


Figure B-4: change analysis

An important aspect relating to the change analysis is to include the interactions with other areas when identifying the changes. Consequently, the list of changes shall describe not only the change itself, but also the interactions with surroundings as this may be the cause to hazards as well. For example, often will a change in equipment affect the way the human uses the equipment etc.

When having derived the list of changes, apply the checklist in Table B-1 and B-2 to the list to identify the causes and failure modes.

ANNEX C

- ANALYSIS OF CAUSES AND FAILURE MODES -

STEP 2

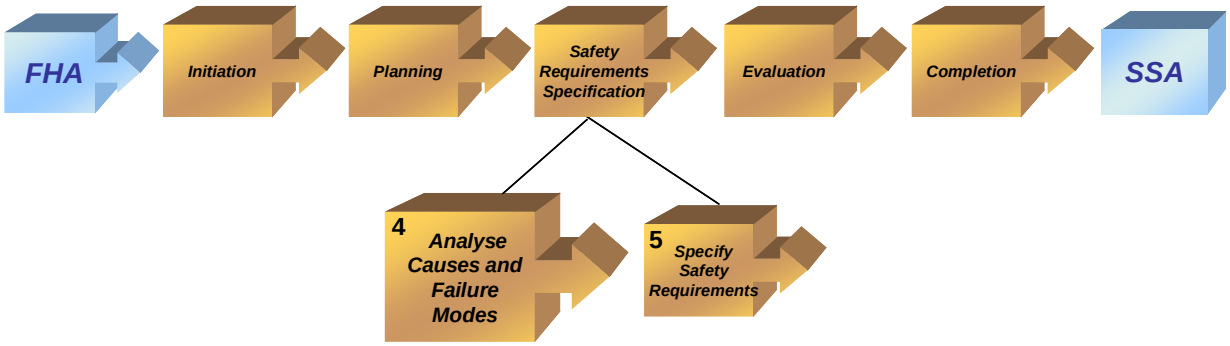


Figure C-1: PSSA process

Inputs

Refined description of the procedure, procedure's boundaries and interfaces;

Refined description of the Operational and Legislative Environment;

Revisited assumptions;

List of identified Hazards and Effects;

List of causes and failure modes developed in connection with the analyses described in Annex B.

Outputs

1. Refined list of causes and failure modes.

In some cases it may be found necessary to perform additional activities or further analysis of the causes and failure modes than the analyses described in the previous Annex. Such detailed analysis should be performed if it is felt that the already performed activities do no satisfactorily indicate that completeness is reached.

The possible more detailed analyses or activities include:

Collection of Good Practices – confidence in the completeness of the analysis of causes and failure modes can be achieved by examining how other organisations have handled comparable safety assessments as well as to investigate historical data such as incident reports etc.

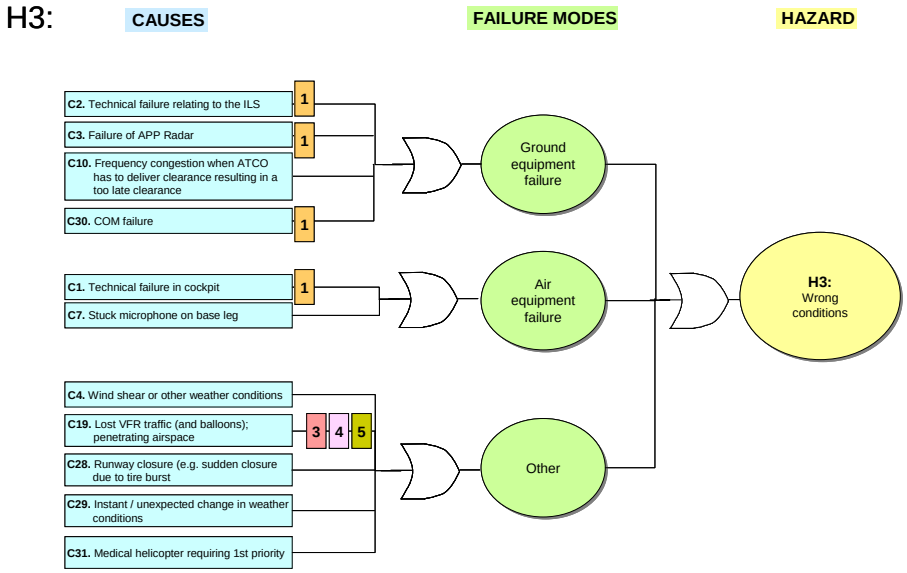
Fault Tree Analysis (FTA) – the FTA is a deductive analysis method that begins with the hazard and then attempts to determine the specific causes of this hazard. Based on a set of rules and logic symbols (AND and OR gates etc) from probability theory and Boolean algebra, FTA uses a top-down approach to generate a logic model that provides for a both qualitative and quantitative evaluation.

The FTA supports the Common Cause Analysis (CCA – see below).

In addition - since in connection with an ATM procedure a fault tree as such may not always provide an added value - the FTA can be used to allocate the impact of the individual external mitigation means on each cause. Thus, when combining with the impact of the external mitigation means, the fault trees provide an overview and clear picture of the importance of the various external mitigation means as well as illustrate the relationship between the causes and the external mitigation means.

Note: See also SAM PART IV Annex D Report / Annex K.

Illustrations from safety assessment at Helsinki-Vantaa Airport (Appendix C):



Fault tree illustrating the interrelations between hazards, causes, failure modes and external mitigation means.

The fault tree covers hazard#3 pertaining to "wrong conditions".

Time Sequence Diagram (TSD) – the purpose of the TSD is to depict the time-ordering of the procedure passing between interacting entities over its lifetime. Thus, the TSD displays the time sequence of the stakeholders affected by the procedure. It consists of the vertical dimension (time) and horizontal dimension (different stakeholders, e.g. pilot, ATCO).

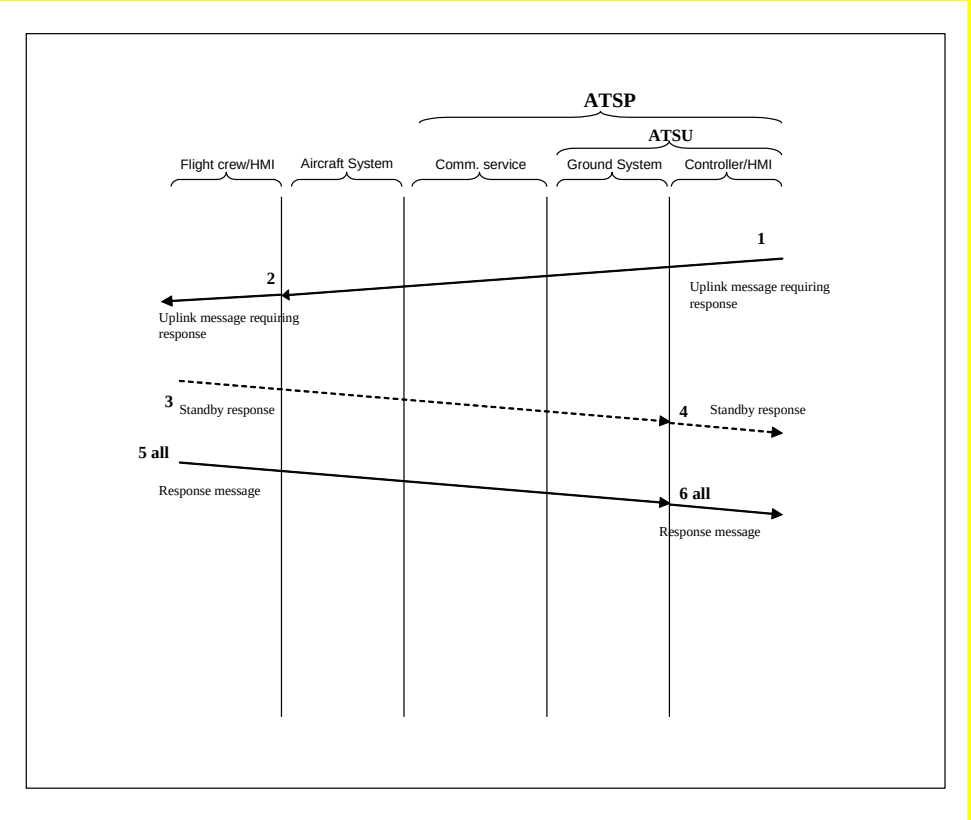


Figure C-2: Time Sequence Diagram

Common Cause Analysis (CCA) – the purpose of CCA is to identify any sequences in which two or more events could occur as the result of one common event. These common causes or events may result from a common process, manufacturing defect, a common human operator error, or some common external event. Common causes are present in almost any system where there is any commonality, such as human interface, common task, and common designs, anything that has a redundancy, from a part, component, sub-system or system. If the probability of a common cause is significantly greater than the probability of the two or more resulting events occurring independently, then the common cause could be an important risk contributor.

CCA is often subdivided into the following three areas:

- ***Common Mode Analysis (CMA)***
- ***Particular Risk Assessment***
- ***Zonal (Safety) Analysis***

Note: See also SAM PART IV Annex D Report.

ANNEX D

- SAFETY REQUIREMENTS SPECIFICATION -

STEP 1

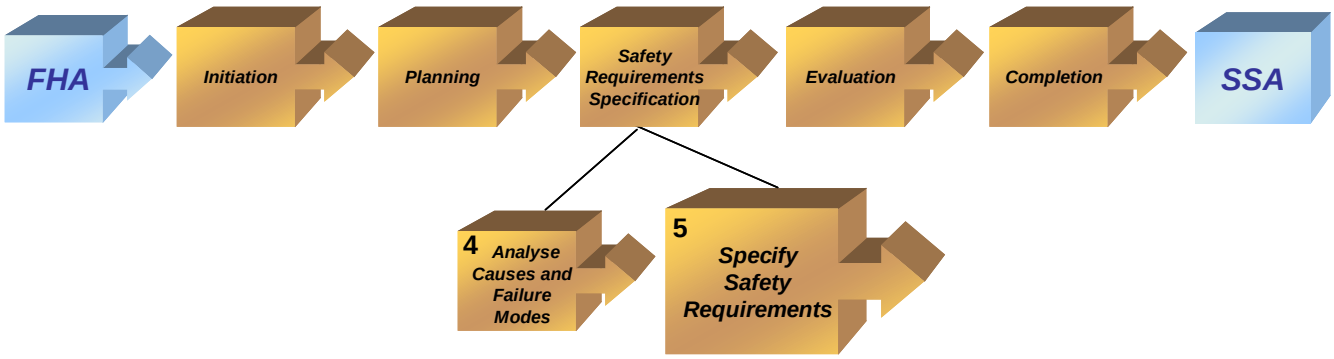


Figure D-1: PSSA process

Inputs

List of causes and failure modes (output from the analysis of causes and failure modes, see Annex B and C)

Safety objectives.

Outputs

1. List of safety requirements.

D.1 Introduction to Safety Requirements

Safety requirements specify risk mitigation and give the detailed objective and description of the safety action to be implemented to mitigate the risk as well as the responsibility (who is responsible for the implementation) and the timing (when to implement the requirement) if applicable.

The final list of safety requirements should, comprise the mitigation means expressed through the allocated PAL (see Annex E) as well as the safety requirements that have been identified as a reply to the causes and failure modes which have been identified (Annex B and C).

D.2 How to Identify Safety Requirements

Following the analyses of causes and failure modes, the following tasks should be completed:

- Apply Risk Mitigation Strategies: What can be done to eliminate, reduce or control hazards and their effect(s)? ***Note: See SAM-PSSA, Section 3.3.***
- Apportion Safety Objectives into Safety Requirements to System Elements: What is the part of the safety objectives to be allocated to tasks of the procedure? ***Note: See SAM-PSSA, Section 3.4.***
- Balance/Reconcile Safety Requirements: Are Safety Requirements credible? ***Note: See SAM-PSSA, Section 3.5.***

ANNEX E

- SAFETY REQUIREMENTS SPECIFICATION -

STEP 2

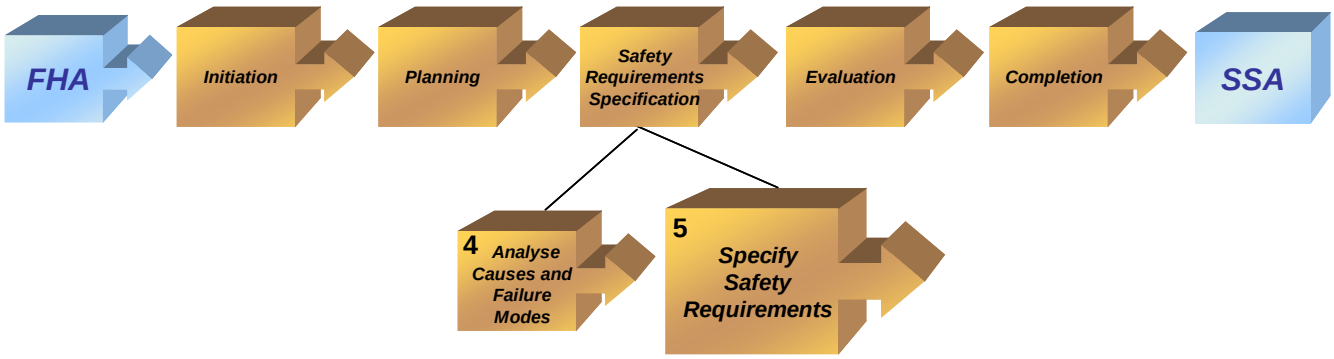


Figure E-1: PSSA process

Inputs

Risks associated with the identified hazardous scenarios.

Outputs

1. Procedure Assurance Levels (PALs).

E.1 Safety Requirements and Procedure Assurance Levels

Risk mitigation may be applied during all phases of a procedure life cycle, i.e. definition, design, implementation, etc. in order to eliminate, reduce or control the risks associated with the procedure.

The following Procedure Assurance Levels (PALs) express the *development effort* to be applied at the various phases of the procedure life cycle to ensure acceptable risk levels.

Hence, the PALs constitute generic potential mitigation means to be applied where required and applicable.

The final list of safety requirements should, therefore, comprise the mitigation means expressed through the allocated PAL as well as the safety requirements that have been identified as described in Annex D.

E.2 Introduction to Procedure Assurance Levels

Any procedure development effort should be proportional to the potential ***Risk*** associated with the ***Procedure***. To achieve this objective, a Procedure Assurance Level (PAL) should be determined and satisfied. Thus, the main aspect is that the higher the risk of the procedure is assessed to be (through the FHA), the more demanding shall the development effort be.

Thus, the PAL is setting some objectives to be met during the different phases of the procedure life cycle. See table E-1.

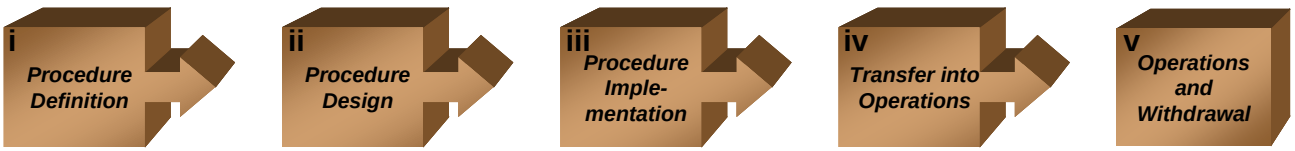


Figure E-2: procedure life cycle

PAL objectives are applicable to the entire Procedure, not only to some part of it.

E.3 Allocation of Procedure Assurance Levels

The following steps should be performed to allocate a PAL:

1. Identify the likelihood that, once the procedure fails, this procedure can generate an end-effect which has a certain severity (do that for each effect of a hazard);
2. Identify the PAL for that couple (severity, likelihood) using the matrix hereafter;
3. This has to be done for all the hazards due to the procedure.

The final PAL of an ATM procedure is the most stringent one.

Effect Severity / Likelihood of generating such an effect	1	2	3	4
Very Possible	PAL1	PAL2	PAL3	PAL4
Possible	PAL2	PAL3	PAL3	PAL4
Very Unlikely	PAL3	PAL3	PAL4	PAL4
Extremely Unlikely	PAL4	PAL4	PAL4	PAL4

Table E-1: PAL matrix

Very Possible: This effect will certainly occur due to a procedure failure.

Possible: This effect may happen (it is not unreasonable to expect such effect to happen due to a procedure failure).

Very Unlikely: It is not expected to have such an effect more than exceptionally and in some extreme cases throughout the system lifetime.

Extremely Unlikely: Such an effect is not expected to happen throughout the system lifetime.

Two examples of PAL allocation:

1st CASE: Safety Objectives were allocated using Method 1 or 3 (***Note: See SAM-FHA Chapter 3 Guidance Material G "Methods for Setting Safety Objectives***). As a result, ***all*** the hazard effects, due to ATM Procedure failure, are taken into consideration.

This Procedure will be allocated a PAL = PAL3 as it is the most stringent PAL.

Effect Severity / Likelihood of generating such an effect	1	2	3	4
Very Possible	PAL1	PAL2	PAL3	PAL4
Possible	PAL2	PAL3	PAL3	PAL4
Very Unlikely	PAL3	PAL3	PAL4	PAL4
Extremely Unlikely	PAL4	PAL4	PAL4	PAL4

Table E-2: PAL matrix, example 1

Procedure failure/cause leading to hazard 1:

Procedure failure/cause leading to hazard2:

2nd CASE: Safety Objectives were allocated using Method 2 or 4 (***Note: See SAM-FHA Chapter 3 Guidance Material G "Methods for Setting Safety Objectives***). As a result, the ***worst credible*** hazard effects, due to ATM Procedure failure, are taken into consideration.

This Procedure will be allocated a PAL = PAL3 as it is the most stringent PAL.

Effect Severity Likelihood of generating such an effect	1	2	3	4
Very Possible	PAL1	PAL2	PAL3	PAL4
Possible	PAL2	PAL3	PAL3	PAL4
Very Unlikely	PAL3	PAL3	PAL4	PAL4
Extremely Unlikely	PAL4	PAL4	PAL4	PAL4

Table E-3: PAL matrix, example 3

Procedure failure/cause leading to hazard 1:

Procedure failure/cause leading to hazard2:

Note: It should be noted that PAL1 is so stringent that it should nearly never be allocated for the following reasons:

1. PAL1 means somehow that the procedure “can directly kill once it fails” as having a Severity1 effect is “Probable” (very limited means to mitigate procedure failure(s)). This can only be tolerable in extremely exceptional circumstances;

2. PAL1 is so demanding to be satisfied. As the objectives and associated evidences are so stringent, the cost and development duration and effort are very high;

3. Allocating PAL1 means that an extremely low level of performance is accepted. The procedure will be requiring such separation minima, such safety margin, such operational checking that it will be acceptable to use it to expedite traffic only in extremely exceptional circumstances.

It could be the same for PAL2 with of course less stringency.

That is why an objective for PAL 1&2 requests to have the CEO signing it because this kind of procedure should not be the recommended practise.

PAL2 should be only allocated to highly risky procedures.

Consequently, mainly PAL3 and PAL4 will be allocated.

E.4 PAL Objectives (Standard)

Note: underlined objectives are those that are additional to the less demanding PAL just below.

Procedure Assurance Level	Objectives to be fulfilled during the Procedure Life Cycle Phases:				
	i Definition	ii Design and Validation	iii Implementation	iv Transfer into Operations	v Operation
PAL 1	*i1.* Ensure involvement of relevant operational expertise *i2.* Ensure a minimum set of quality assurance activities *i3.* Establish a proven and well-documented starting point for the definition phase *i4.* Ensure stakeholder acceptance *i5.* Ensure an approved and systematic specification	*ii1.* Establish an acceptable risk level (in quantitative terms) *ii2.* Ensure that HMI has been assessed *ii3.* Ensure suitable validation at different levels *ii4.* Ensure robustness *ii5.* Ensure external expert acceptance *ii6.* Ensure enhanced competence levels of designers *ii7.* Ensure stakeholder acceptance *ii8.* Ensure independency in design and validation	*iii1.* Establish an Implementation Plan which includes quality assurance activities *iii2.* Ensure a minimum set of acceptable quality assurance activities *iii3.* Ensure stakeholder acceptance *iii4.* Ensure training levels *iii5.* Ensure approval at the Corporate level of management *iii6.* Establish evidence of acceptable design maturity *iii7.* Ensure independent auditing of the procedure *iii8.* Ensure corporate level of approval by stakeholders	*iv1.* Ensure that feedback concerning the transfer process is provided to involved staff *iv2.* Ensure documented contingency measures *iv3.* Ensure dissemination of contingency measures *iv4.* Ensure enhanced competence levels of staff to perform the transfer *iv5.* Ensure incremental transfer *iv6.* Ensure approval of the Transfer Plan at management level *iv7.* Ensure stakeholder acceptance of the Transfer Plan *iv8.* Ensure application of an approved and systematic method to verify the transfer process	*v1.* Ensure documentation control *v2.* Establish a reporting system covering occurrences relating to the procedure *v3.* Ensure minimum proficiency levels *v4.* Ensure validity of assumptions *v5.* Ensure promulgation of related incident investigations *v6.* Ensure acceptable performance levels *v7.* Ensure minimum competency levels of staff to operate the procedure *v8.* Ensure that the application of the procedure is reduced to its minimum

Procedure Assurance Level	*Objectives to be fulfilled during the Procedure Life Cycle Phases:*				
	i Definition	**ii Design and Validation**	**iii Implementation**	**iv Transfer into Operations**	**v Operation**
PAL 2	*i1.* Ensure involvement of relevant operational expertise *i2.* Ensure a minimum set of quality assurance activities *i3.* Establish a proven and well-documented starting point for the definition phase *i4.* Ensure stakeholder acceptance	*ii1.* Establish an acceptable risk level (in qualitative terms) *ii2.* Ensure that HMI has been assessed *ii3.* Ensure suitable validation at different levels *ii4.* Ensure robustness *ii5.* Ensure external expert acceptance *ii6.* Ensure enhanced competence levels of designers *ii7.* Ensure stakeholder acceptance	*iii1.* Establish an Implementation Plan which includes quality assurance activities *iii2.* Ensure an acceptable quality assurance level *iii3.* Ensure stakeholder acceptance *iii4.* Ensure training levels *iii5.* Ensure approval at the Corporate level of management *iii6.* Establish evidence of acceptable design maturity	*iv1.* Ensure that feedback concerning the transfer process is provided to involved staff *iv2.* Ensure documented contingency measures *iv3.* Ensure dissemination of contingency measures *iv4.* Ensure enhanced competence levels of staff to perform the transfer *iv5.* Ensure incremental transfer *iv6.* Ensure approval of the Transfer Plan at management level *iv7.* Ensure stakeholder acceptance of the Transfer Plan	*v1.* Ensure documentation control *v2.* Establish a reporting system covering occurrences relating to the procedure *v3.* Ensure minimum proficiency levels *v4.* Ensure validity of assumptions *v5.* Ensure promulgation of related incident investigations *v6.* Ensure acceptable performance levels *v7.* Ensure minimum competency levels of staff to operate the procedure
PAL 3	*i1.* Ensure involvement of relevant operational expertise *i2.* Ensure a minimum set of quality assurance activities *i3.* Establish a proven and well-documented starting point for the definition phase	*ii1.* Establish an acceptable risk level (in qualitative terms) *ii2.* Ensure that HMI has been assessed *ii3.* Ensure suitable validation at different levels *ii4.* Ensure robustness	*iii1.* Establish an Implementation Plan which includes quality assurance activities *iii2.* Ensure an acceptable quality assurance level *iii3.* Ensure stakeholder acceptance *iii4.* Ensure training levels	*iv1.* Ensure that feedback concerning the transfer process is provided to involved staff *iv2.* Ensure documented contingency measures *iv3.* Ensure dissemination of contingency measures *iv4.* Ensure enhanced competence levels of staff to perform the transfer	*v1.* Ensure documentation control *v2.* Establish a reporting system covering occurrences relating to the procedure *v3.* Ensure minimum proficiency levels *v4.* Ensure validity of assumptions *v5.* Ensure promulgation of related incident investigations

Procedure Assurance Level	*Objectives to be fulfilled during the Procedure Life Cycle Phases:*				
	i Definition	**ii Design and Validation**	**iii Implementation**	**iv Transfer into Operations**	**v Operation**
PAL 4	*i1.* Ensure involvement of relevant operational expertise *i2.* Ensure a minimum set of quality assurance activities *i3.* Establish a proven and well-documented starting point for the definition phase	*ii1.* Establish an acceptable risk level (in qualitative terms) *ii2.* Ensure that HMI has been assessed *ii3.* Ensure suitable validation	*iii1.* Establish an Implementation Plan which includes quality assurance activities *iii2.* Ensure an acceptable quality assurance level	*iv1.* Ensure that feedback concerning the transfer process is provided to involved staff *iv2.* Ensure documented contingency measures *iv3.* Ensure dissemination of contingency measures	*v1.* Ensure documentation control *v2.* Establish a reporting system covering occurrences relating to the procedure *v3.* Ensure minimum proficiency levels

Table E-4: PAL objectives (standard)

E.5 PAL Objectives (Accumulated)

Procedure Assurance Level	Objectives to be fulfilled during the Procedure Life Cycle Phases:				
	i Definition	**ii Design and Validation**	**iii Implementation**	**iv Transfer into Operations**	**v Operation**
PAL 1	*i5* Ensure an approved and systematic specification	*ii8* Ensure independency in design and validation	*iii8* Ensure corporate level of approval by stakeholders *iii7* Ensure independent auditing of the procedure	*iv8* Ensure application of an approved and systematic method to verify the transfer process	*v8* Ensure that the application of the procedure is reduced to its minimum
PAL 2	*i4* Ensure stakeholder acceptance	*ii7* Ensure stakeholder acceptance *ii6* Ensure enhanced competence levels of designers *ii5* Ensure external expert acceptance	*iii6* Establish evidence of acceptable design maturity *iii5* Ensure approval at the Corporate level of management	*iv7* Ensure stakeholder acceptance of the Transfer Plan *iv6* Ensure approval of the Transfer Plan at management level *iv5* Ensure incremental transfer	*v7* Ensure minimum competency levels of staff to operate the procedure *v6* Ensure acceptable performance levels
PAL 3	*i3* Establish a proven and well-documented starting point for the definition phase *i2* Ensure a minimum set of quality assurance activities *i1* Ensure involvement of relevant operational expertise	*ii4* Ensure robustness *ii3* Ensure suitable validation at different levels	*iii4* Ensure training levels *iii3* Ensure stakeholder acceptance	*iv4* Ensure enhanced competence levels of staff to perform the transfer	*v5* Ensure promulgation of related incident investigations *v4* Ensure validity of assumptions
PAL 4		*ii3* Ensure suitable validation *ii2* Ensure that HMI has been assessed *ii1* Establish an acceptable risk level (in qualitative terms)	*iii2* Ensure an acceptable quality assurance level *iii1* Establish an Implementation Plan which includes quality assurance activities	*iv3* Ensure dissemination of contingency measures *iv2* Ensure documented contingency measures *iv1* Ensure that feedback concerning the transfer process is provided to involved staff	*v3* Ensure minimum proficiency levels *v2* Establish a reporting system covering occurrences relating to the procedure *v1* Ensure documentation control

Table E-5: PAL objectives (accumulated)

E.6 PAL Activities

A number of possible activities have been identified for fulfilling the objectives contained in Table E-4. The list is not exhaustive and not all activities may be equally applicable. The essential part is to fulfil the objectives – not how. The rationales for the activities are written in *italics*.

i. Definition	
Objective	**Activity / activities**
i1 **Ensure involvement of relevant operational expertise**	• Involve familiar operational expertise in the definition of the procedure *Air traffic controllers and pilots who are working in the concerned environment and have relevant experience should be involved in the definition of the procedure to ensure practicality and applicability.*
i2 **Ensure a minimum set of quality assurance activities**	• Apply a minimum set of quality assurance activities to validate the procedure definition *The activities may include:* - *has the organisation's standards for developing procedures been applied?* - *has a complete FHA been performed covering both the 'transfer into operations phase' and the 'operations phase'?* - *are the tasks of the procedure clearly identified and described?* - *are weather conditions considered (robustness to abnormal conditions)?* - *are specific traffic compositions (mixture of traffic) considered (overload tolerance)?* - *has a time sequence diagram been elaborated and considered?* *The evidence of the minimum set of quality assurance activities may be provided by references to the relevant documentation.*
i3 **Establish a proven and well-documented starting point for the definition phase**	• Collect relevant benchmarking results and/or perform own experience benchmarking *Benchmarking with organisations that have successfully implemented a similar procedure in order to identify the gaps and benefits compared to own environment - or benchmarking based upon experience and "best guesses" of experts (if no comparable organisations or procedures exist) - may provide a valuable input to the definition phase.* • Include best practice and lessons learnt *Learn from other's mistakes and successes.*

i. Definition	
Objective	**Activity / activities**
i4 **Ensure stakeholder acceptance**	• Perform relevant stakeholder consultations *The consultations should reach all stakeholders to support that as many risks as possible are anticipated (different stakeholders may have different risks).* • Involve stakeholders in the definition phase itself *Involvement will create confidence in the procedure.*
i5 **Ensure an approved and systematic specification**	• Apply a formal method for the definition specification *If possible a formal method should be applied. Such methods are principally designed to ensure that every scenario is considered in a systematic way.*

ii. Design and Validation	
Objective	**Activity / activities**
ii1 **Establish an acceptable risk level (in quantitative / qualitative terms)**	• Perform a quantitative / qualitative risk analysis *The results of the risk analysis shall provide the level of risk of the procedure and the required activities to ensure an acceptable risk level. Thus, the risk analysis activities include the performance of the PSSA, e.g. by applying the present SAAP.*
ii2 **Ensure that HMI has been assessed**	• Perform assessment of the HMI *All HMI, which are linked (e.g. specifically designed or modified) to the procedure, should be validated.* - *At PAL4 level a limited number of ATCOs should have played with the HMI.* - *At PAL3 level a representative number of ATCOs should have played with the HMI and validated the prototypes.* - *At PAL2 level large number of ATCOs should have played with the HMI and validated the prototypes during several rounds.* - *At PAL1 level a large number of ATCOs should have played with the HMI, validated the prototypes and subsequent versions, and approved the final version.*
ii3 **Ensure suitable validation … at different levels**	*Depending on the PAL and the feasibility of the validation (it is not possible to implement all types of procedures for trial in a real life environment)* • Perform pre-implementation trials covering e.g. shadow operations (PAL 1, 2, 3, 4) • Perform fast time simulations (PAL 1, 2, 3, 4) • Perform real time simulations (PAL 1, 2, 3) • Request aircraft operators to validate the procedure through own simulations (PAL 1, 2)

ii. Design and Validation	
Objective	**Activity / activities**
***ii4* Ensure robustness**	• Apply fail-safe measures *Proper fail-safe measures will automatically and safely compensate for failures.* • Apply error-tolerance measures *The procedure design should minimise the consequences of some unintended errors (e.g. human memory errors).* • Validate the procedure when under stress or when confronted with an invalid application *Warrant a certain resilience.*
***ii5* Ensure external expert acceptance**	• Perform independent review by external experts *External experts will provide neutrality and fresh viewpoints. The external experts should include both external ATM procedure designers and operational staff who have – if applicable - expertise in operating a similar procedure.*
***ii6* Ensure enhanced competence levels of designers**	• Collect evidence of designers' competence *Verify that the designer has the necessary level of experience and skills*
***ii7* Ensure stakeholder acceptance**	• Perform relevant stakeholder consultations *The consultations should reach all stakeholders to support that as many risks as possible are anticipated (different stakeholders may have different risks).* • Involve stakeholders in the design and validation phase itself *Involvement will create confidence in the procedure.*
***ii8* Ensure independency in design and validation**	• Perform independent parallel design and validation - *Independent to warrant that invalid design assumptions are not propagated into the validation process. The independence should be ensured by having two individuals involved in the design of the procedure. Thus, they should design independently and merge accordingly ultimately. The independence-factor is increased by having two individuals from different units involved in the design or even having two individuals from different companies involved.* - *Parallel to create an iterative and comparative process where validation may lead to re-design.*

iii. Implementation	
Objective	**Activity / activities**
iii1 **Establish an Implementation Plan which includes quality assurance activities**	• Develop an Implementation Plan *The Implementation Plan shall specify in a clear and transparent manner how the implementation is planned to be performed including the related quality assurance activities. The minimum content should include:* - *scope and goals* - *description of tasks of the implementation* - *quality assurance activities* - *resource requirements* - *time schedule* - *milestones.*
iii2 **Ensure an acceptable quality assurance level**	• Apply a minimum set of quality assurance activities / assessments to validate the procedure implementation *The activities may include:* - *has the organisation's standards for implementation been applied?* - *has a pre-SSA been performed covering both the 'transfer into operations phase' and the 'operations phase'?* - *are responsibilities during the implementation process allocated?* - *are the implementation process as described in the Implementation Plan considered to be correct and complete?* - *are critical paths of the implementation process considered?* *The evidence of the minimum set of quality assurance activities may be provided by references to the relevant documentation.*
iii3 **Ensure stakeholder acceptance**	• Perform relevant stakeholder consultations *The consultations should reach all stakeholders to support that as many risks as possible related to the implementation are anticipated (different stakeholders may have different risks).* • Implement awareness programmes *Ensure that all staff acknowledge the procedure and its implementation.*

iii. Implementation	
Objective	**Activity / activities**
iii4 **Ensure training levels**	• Develop a training plan setting the required training levels *Warrant that acceptable levels are achieved.* • Perform dedicated training of staff *Develop training programme(s) for the future users of the procedure which is devoted to ensure correct application of the procedure.* • Implement awareness programmes *The awareness programmes should reach not only the staff who will be directly affected by the procedure, but as well staff who indirectly are affected, in order to create a common understanding of the safety implications related to the procedure.*
iii5 **Ensure approval at the Corporate level of management**	• Perform consultation at the corporate level of management *A shared approval and acceptance - by management - of the procedure prior to implementation strengthens and facilitates the implementation process. Furthermore, it raises awareness of potential consequences of mis-application of the procedure.*
iii6 **Ensure evidence of acceptable design maturity**	• Collect design maturity argumentation *The evidence that the design has reached the maturity level, which is required for implementation, is essential – and any shortcomings should be corrected immediately or generate other mitigating actions such as re-design or implementation interruption.*
iii7 **Ensure independent auditing of the procedure**	• Audit the procedure by external experts *Warrant neutrality and objectivity.*
iii8 **Ensure corporate level of approval by stakeholders**	• Collect stakeholders' approval regularly through the implementation phase *Approval and acceptance by stakeholders are obtained by involving them at regular intervals in the implementation process for their acceptance of the performance.*

iv. Transfer into Operations	
Objective	**Activity / activities**
iv1 **Establish that feedback concerning the transfer process is provided to involved relevant staff**	• Implement feedback means *All relevant staff should be able to receive feedback on the transfer process and possible deviations from the Transfer Plan.*

iv. Transfer into Operations	
Objective	**Activity / activities**
iv2 **Ensure documented contingency measures**	• Develop a contingency plan *Ensure that all abnormal situations are considered.*
iv3 **Ensure dissemination of contingency measures**	• Disseminate the contingency plan *Ensure that all relevant controllers and pilots know what contingency measures to be taken and when.*
iv4 **Ensure enhanced competence levels of staff to perform the transfer**	• Establish competency argumentation for the staff to perform the transfer *It should be verified that the staff performing the transition has the necessary level of experience and skills in order to ensure a correct transfer into operations of the procedure.*
iv5 **Ensure incremental transfer**	• Implement an incremental transfer into operations process *An incremental process enables a smooth transition and allows for corrective actions to be continuously implemented (or implemented in the next step), decreases the number of risks and makes the transfer process easier to manage.*
iv6 **Ensure approval of the Transfer Plan at management level**	• Perform relevant management consultation *A shared approval and acceptance - by management - of the transfer plan strengthens and facilitates the transition process.*
iv7 **Ensure stakeholder acceptance of the Transfer Plan**	• Perform relevant stakeholder consultations *The consultations should reach all stakeholders to support that as many risks related to the transition as possible are anticipated (different stakeholders may have different risks).* • Involve stakeholders in the development of the Transfer Plan *Involvement of a representative number of stakeholders will create confidence concerning the transfer process.*
iv8 **Ensure application of an approved and systematic method to verify the transfer process**	• Apply a formal method for verifying the transfer process *If possible a formal method should be applied. Such methods are principally designed to ensure that every scenario is considered in a systematic way.*

v. Operation	
Objective	**Activity / activities**
v1 **Ensure documentation control**	• Strict document control should be applied *Ensure that correct version is always applied in operations.*

v. Operation	
Objective	**Activity / activities**
v2 **Ensure that means for collecting occurrences relating to the procedure are in place**	• The reporting system in compliance with ESARR2 should capture occurrences relating to the procedure *In order to implement corrective actions if required and disseminate lessons learnt.*
v3 **Ensure high-ranking proficiency levels**	• Implement a minimum set of activities to support minimum proficiency levels *The activities may include:* - *performing regular proficiency checks* - *implementing dedicated training as well as recurrence training* - *performing awareness campaigns.*
v4 **Ensure validity of assumptions**	• Perform dedicated assumptions monitoring *Periodical review of the assumptions should be performed to ensure that the assumptions are still valid.*
v5 **Ensure promulgation of related incident investigations**	• Implement feedback means and the associated means to implement corrective actions *Incident reports should be disseminated to relevant controllers and pilots if an incident relating to the procedure occurs, enabling them to pay extra attention.*
v6 **Ensure acceptable performance levels**	• Perform dedicated performance monitoring *Use the monitoring to evaluate the performance levels of the procedure. If the performance levels are not satisfied, the procedure needs to be re-assessed.*
v7 **Ensure minimum competency levels of staff to operate the procedure**	• Implement a minimum set of competency requirements for the staff that are envisaged to operate the procedure *Ensure that only the most experienced and professional staff is involved when operating the procedure.*
v8 **Ensure that the application of the procedure is reduced to its minimum**	• Reduce the application of the procedure to a minimum *Due to the critical contributions to various serious incidents or accidents, the procedure should only be used in extremely exceptional circumstances and other ways of working should be considered.* *Under extreme circumstances (e.g. unexpected closed runways, extreme weather conditions or extreme system degradation), it might be necessary to use a more risky procedure. It shall then be ensured that the duration of the procedure application is kept to an absolute minimum.* *Investigate / survey alternative or new additional mitigation means that will reduce the risk of operating such procedure.*

Table: E-6: PAL activities

E.7 PAL Compliance Matrix

Obj. no:	Objectives to be fulfilled during the Procedure Life Cycle Phases:	Procedure Assurance Level			
		PAL 1	PAL 2	PAL 3	PAL 4
i. Definition					
i1	Ensure involvement of relevant operational expertise	●	○	○	○
i2	Ensure a minimum set of quality assurance activities	●	○	○	○
i3	Establish a proven and well-documented starting point for the definition phase	●	○	○	○
i4	Ensure stakeholder acceptance	●	○		
i5	Ensure an approved and systematic specification	●			

		PAL 1	PAL 2	PAL 3	PAL 4
ii. Design and Validation					
ii1	Establish an acceptable risk level (in quantitative* / qualitative terms)	●	○	○	○
ii2	Ensure that HMI has been assessed	●	●	○	○
ii3	Ensure suitable validation … at different levels	●	○	○	○
ii4	Ensure robustness	●	○	○	
ii5	Ensure external expert acceptance	●	●		
ii6	Ensure enhanced competence levels of designers	●	○		
ii7	Ensure stakeholder acceptance	●	○		
ii8	Ensure independency in design and validation	●			

- ** PAL1 only*

		PAL 1	PAL 2	PAL 3	PAL 4
iii. Implementation					
iii1	Establish an Implementation Plan which includes quality assurance activities	●	○	○	○
iii2	Ensure an acceptable quality assurance level	●	○	○	○
iii3	Ensure stakeholder acceptance	●	○	○	
iii4	Ensure training levels	●	○	○	
iii5	Ensure approval at the Corporate level of management	●	○		

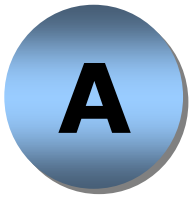
		PAL 1	PAL 2	PAL 3	PAL 4
iii. Implementation					
iii6	Ensure evidence of acceptable design maturity	●	○		
iii7	Ensure independent auditing of the procedure	●			
iii8	Ensure corporate level of approval by stakeholders	●			

		PAL 1	PAL 2	PAL 3	PAL 4
iv. Transfer into operations					
iv1	Establish that feedback concerning the transfer process is provided to involved staff	●	○	○	○
iv2	Ensure documented contingency measures	●	○	○	○
iv3	Ensure dissemination of contingency measures	●	○	○	○
iv4	Ensure enhanced competence levels of staff to perform the transfer	●	○	○	
iv5	Ensure incremental transfer	●	○		
iv6	Ensure approval of the Transfer Plan at management level	●	○		
iv7	Ensure stakeholder acceptance of the Transfer Plan	●	○		
iv8	Ensure application of an approved and systematic method to verify the transfer process	●			

		PAL 1	PAL 2	PAL 3	PAL 4
v. Operation					
v1	Ensure documentation control	●	○	○	○
v2	Establish a reporting system covering occurrences relating to the procedure	●	○	○	○
v3	Ensure high-ranking proficiency levels	●	○	○	○
v4	Ensure validity of assumptions	●	○	○	
v5	Ensure promulgation of related incident investigations	●	○	○	
v6	Ensure acceptable performance levels	●	○		
v7	Ensure minimum competency levels of staff to operate the procedure	●	○		
v8	Ensure that the application of the procedure is reduced to its minimum	●			

○ To Be Done

● To Be Done by independent party



APPENDIX A:

TAXONOMY OF ATM PROCEDURES

GENERAL

The application of the present document can be done to a variety of ATM procedures. In the perspective of ATM, the application of the procedure is considered to be most beneficial (to potentially have the greatest safety enhancement impact) on the following main groups of procedures/documentation:

- Operational ATM procedures, both national (ATS instructions) and at unit level (Local ATS instructions (LATSI), amendments to LATSI)
- Technical ATM procedures
- Training procedures (Operational and Technical)

At the **national level** (regulatory), depending on the method for transposing international ATM regulation (ICAO, Eurocontrol) into national procedures, it is always recommended to conduct safety assessment of the application of the procedure into “local” context.

At the **ANSP/unit level** the methodology can be applied to any change of the Operational and Technical ATM procedures/written instructions. This would include both permanent and temporary changes to these instructions.

Regarding **ATM training** it is considered beneficial to conduct a safety assessment of any change to the training procedures, both national and local, which affects the content of the training manual and the method for conducting practical ATM training (OJT).

In the following is a list relating to the above described areas to which the SAAP could be applied. The list is not exhaustive but meant as a “catalogue” of minimum areas to which the SAAP could be applied. Further “local” elaboration on topics to be included is considered valuable. The identification of areas of safety “concern” can best be done with local knowledge based on experience from practical use of existing procedures. Other valuable input could be from safety reports (known local safety critical areas), previous conducted safety assessments etc.

OPERATIONAL PROCEDURES

1. ATM PROCEDURES

1.1 Types of procedures according to type of ATS

- **Air Traffic Control Service**

→ **Aerodrome control service procedures:**

- Ground control service procedures;
- Ground surveillance procedures;
- Air control procedures;
- Radar procedures;
- Co-operation/co-ordination procedures
- SID/STAR
- Local ATS instructions
- Amendments to Local ATS instructions
- Any procedures regarding the handling of support systems(i.e. COM systems (incl. Radio, Intercom, Phone) ATIS, VOLMET, INFO systems, Aerodrome lighting/ILS etc)
- Contingency plans (radar, COM, Unit)
- Emergency procedures (operational and non-operational)
- Unit OJT plan

→ **Approach control service procedures:**

- Surveillance;
- Procedural;
- Co-operation/co-ordination procedures;
- Letters of Agreement
- SID/STAR
- Local ATS instructions
- Amendments to Local ATS instructions;
- Any procedures regarding the handling of technical support systems(i.e. COM systems incl. Radio, Intercom, Phone), ATIS, VOLMET, INFO systems))
- Contingency plans (radar, COM, Unit)
- Emergency procedures (operational and non-operational)
- Unit OJT plan

→ **Area control:**

- Surveillance;
- Procedural;
- Co-operation/co-ordination procedures
- Letters of Agreement;
- SID/STAR

- Local ATS instructions
- Amendments to Local ATS instructions;
- Any procedures regarding the handling of technical support systems (i.e. COM systems incl. Radio, Intercom, Phone), INFO systems etc.))
- Contingency plans (radar, COM, Unit)
- Emergency Procedures (operational and non-operational)
- Unit OJT plan

→ **Oceanic control procedures:**

- Radar, ADS;
- Procedural;
- Co-operation/co-ordination procedures;
- Letters of Agreement;
- Local ATS instructions
- Amendments to Local ATS instructions;
- Any procedures regarding the handling of technical support systems(I.e. COM systems (incl. Radio, Intercom, Phone INFO systems)
- Contingency plans (radar, COM, Unit)
- Emergency procedures ((operational and non-operational)
- Unit OJT plan

- **Flight information service:**

→ **Broadcast;**

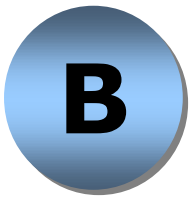
→ **Radar;**

→ **Air-ground radar;**

→ **Air traffic advisory service;**

- Contingency plans (radar, COM, Unit)
- Procedures (operational and non-operational)
- Unit OJT plan

- **Alerting service**
- **Airspace Management Procedures**
- **Strategic (interface with CFMU, Interface with local unit)**
- **Tactical (Unit adjustment of flow control (i.e. procedures regarding the use of sequencing tools etc.)**



APPENDIX B:
EXAMPLE OF ASSESSMENT OF INDEPENDENT PARALLEL APPROACH PROCEDURE

**** see separate document ****