

**AIR NAVIGATION SYSTEM  
SAFETY ASSESSMENT  
METHODOLOGY**

**SAF.ET1.ST03.1000-MAN-01**

**Edition : 2.1  
Edition Date : 03 October 2006  
Status : Released Issue  
Class : General Public**

# DOCUMENT IDENTIFICATION SHEET

## DOCUMENT DESCRIPTION

**Document Title**  
AIR NAVIGATION SYSTEM SAFETY ASSESSMENT METHODOLOGY

EWP DELIVERABLE REFERENCE NUMBER

**PROGRAMME REFERENCE INDEX**

SAF.ET1.ST03.1000-MAN-01

**EDITION :**

2.1

**EDITION DATE :**

03 October 2006

### Abstract

This document provides guidance material for conducting safety assessment of air navigation systems.

### Keywords

Safety assessment	Safety Assurance	Risk	PAL
FHA	Safety Objective	Hazard	HWAL
PSSA	Safety Requirement	Assurance	HAL
SSA	Evidence	SWAL	Safety Case

**CONTACT PERSON :** Patrick Mana

**TEL :** 93295

**DIVISION :** DAP/SSH

## DOCUMENT STATUS AND TYPE

STATUS	CATEGORY	CLASSIFICATION
Working Draft <input type="checkbox"/>	Executive Task <input type="checkbox"/>	General Public <input checked="" type="checkbox"/>
Draft <input type="checkbox"/>	Specialist Task <input checked="" type="checkbox"/>	EATM <input type="checkbox"/>
Proposed Issue <input type="checkbox"/>	Lower Layer Task <input type="checkbox"/>	Restricted <input type="checkbox"/>
Released Issue <input checked="" type="checkbox"/>		

## ELECTRONIC BACKUP

**INTERNAL REFERENCE NAME :**

**HOST SYSTEM**

Microsoft Windows

**MEDIA**

Type : Hard disk

Media Identification :

**SOFTWARE(S)**

---

**DOCUMENT APPROVAL**

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

<b>AUTHORITY</b>	<b>NAME AND SIGNATURE</b>	<b>DATE</b>
Chairman of the Safety Assessment Methodology Task Force	P.MANA	03 October 2006
Chairman of the Safety Team	E. MERCKX	03 October 2006
DAP Director	G.KERKHOFS	03 October 2006

---

**DOCUMENT CHANGE RECORD**

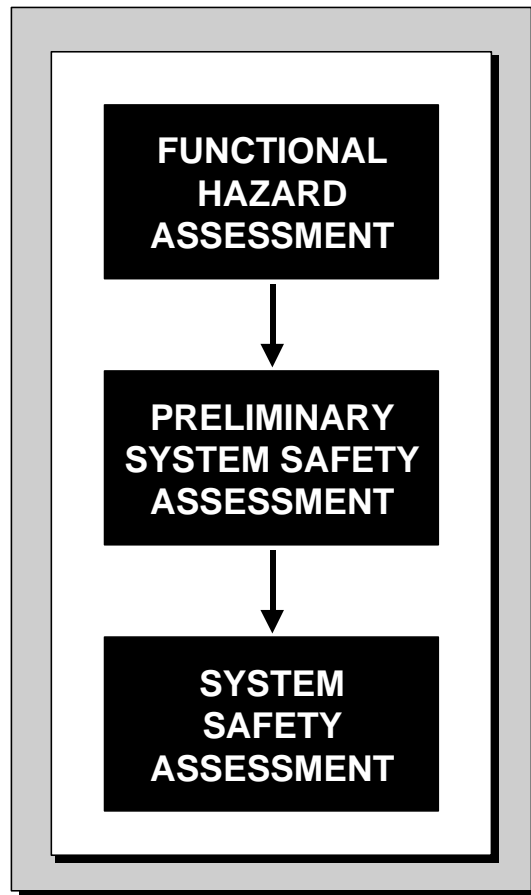
The following table records the complete history of the successive editions of the present document.

<b>EDITION</b>	<b>DATE</b>	<b>REASON FOR CHANGE</b>	<b>SECTIONS PAGES AFFECTED</b>
0.1	12 Mar. 1996	First Draft issue	All
0.2	10 Jul. 1996	Second Working Draft issue, after review by the Task Force	All
0.3	15 Sep. 1996	Third Working Draft issue, after review by the Task Force	All
0.4	27 Nov. 1996	Fourth Working Draft issue, after review by the Task Force	All
0.5	15 April 1999	Fifth Working Draft issue, after review by the Task Force	All
0.6	15 March 2000	Sixth Working Draft issue, last review by the Task Force	All
1.0	17 April 2000	First formal release of FHA material	
1.1	5 May 2003	SAMTF Comments and SRC DOC 12	All
1.2	07 August 2003	Comments by SAMTF	All
2.0	30 April 2004	Second formal release of SAM (First of complete issue of FHA, PSSA and SSA)	All
2.1	03 Oct. 2006	New Guidance Material and examples (No change to Level 1)	

## **FOREWORD**

This manual has been developed by the EUROCONTROL Safety Assessment Methodology Task Force (SAMTF), Sub-Group reporting to the Safety Team.

# GENERAL INTRODUCTION



This page is intentionally left blank.

## 1. PURPOSE

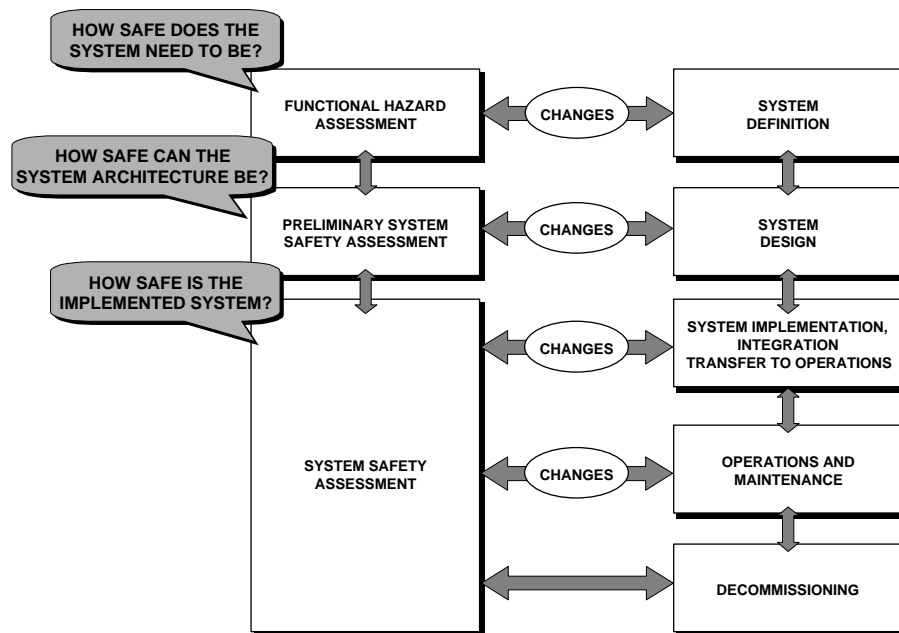
The ANS Safety Assessment Methodology (SAM) has been developed to reflect best practices for safety assessment of Air Navigation Systems and to provide guidance for their application.

SAM methodology describes a generic process for the safety assessment of Air Navigation Systems.

This process consists of three major steps:

- **Functional Hazard Assessment (FHA);**
- **Preliminary System Safety Assessment (PSSA);**
- **System Safety Assessment (SSA).**

Figure 1 shows the relationships between these major steps and the overall System Life Cycle.



**Figure 1 - Relationships between the Safety Assessment Process and the Overall System Life Cycle**

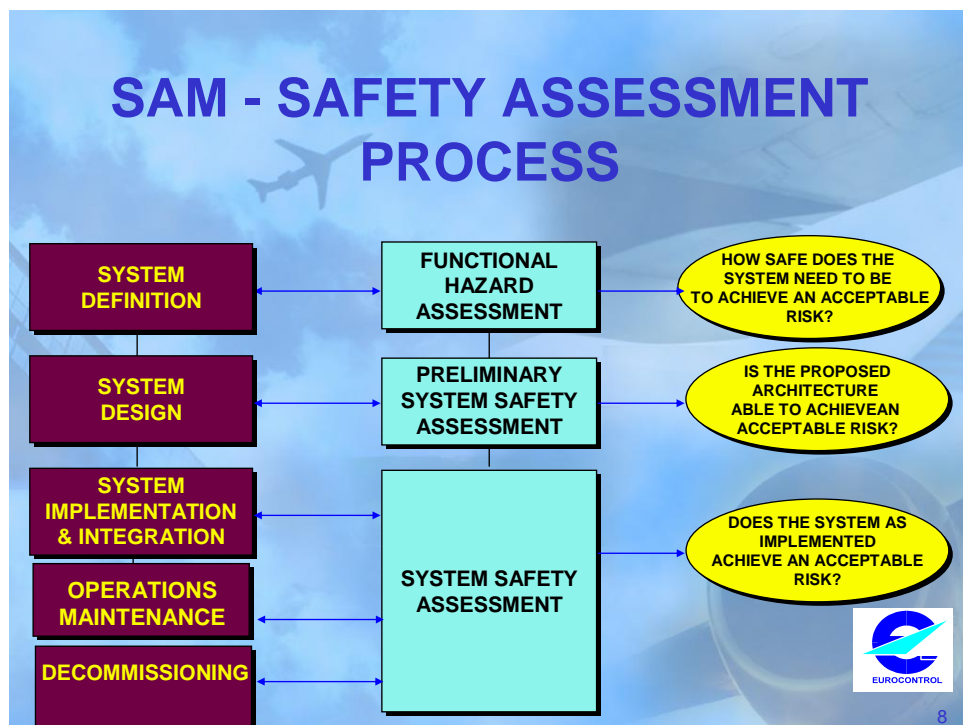


SAM methodology describes the underlying principles of the safety assessment process and leaves the details of applying these principles (or supplementing them if necessary) to be defined for each specific project.

The EATM Safety Assessment Methodology provides further guidance for developing the EATMP Safety Management Principles of the EATMP Safety Policy, in particular the following:

- 4.1.2 Risk Management Process;
- 4.1.4 Safety Objectives and Requirements;
- 4.1.5 System Safety Assessment Process and Documentation.

The ANS Safety Assessment Methodology should potentially support the demonstration that safety is being managed within safety levels meeting as a minimum those approved by the designated authority (“tolerable” risk). However, SAM aims at supporting ANSP to achieve an acceptable level of risk (See FHA chapter 3 GM E for explanations of “tolerable” and “acceptable”).



The ANS Safety Assessment Methodology V2.0 has been assessed as a Means of Compliance with ESARR 4. Results can be found in SRC DOC 12 V1.1

The compliance matrix is provided in SAM-Intro Annex B.

## 2 SCOPE OF THE METHODOLOGY

The safety assessment methodology described in this manual applies to Air Navigation Systems considering the three types of system elements: people, equipment and procedures and their interactions (within the system and with its environment) in a specific environment of operation.

An Air Navigation System may include ground-based (including space-based components) and air-based components.

It covers the complete life-cycle of the Air Navigation System, from initial planning and system definition to de-commissioning.

The methodology considers only the safety aspects of the Air Navigation System. Other attributes of the system, aiming, for example, to achieve capacity and/or efficiency objectives, are not addressed by the proposed methodology.

The ANS SAM provides guidelines on how to perform a Air Navigation System Safety Assessment.

SAM methodology does not address Air Navigation System “certification” issues. However, the application of the principles described in this manual could prepare to and support a certification process of Air Navigation Systems. (Cf. EUROCAE ED78A” Guidelines for approval of the provision and use of Air Traffic Services supported by data communication” may be used for approval purposes.)

SAM methodology does not address organisational and management aspects related to safety assessment. Acceptability of those changes should be assessed as part of the implementation of an organisation Safety Management System (refer to EATMP Safety Policy). For each project, organisational entities involved in the safety assessment process should be identified and their respective responsibilities specified.

ANS SAM methodology provides Guidance Material on how to assess what is a “change”, whether it deserves a safety assessment and what will be the extent of this safety assessment (See SAM Part IV – Annex H).

ANS SAM provides also Guidance Material to structure and document a safety argument: a safety case (See SAM Part IV – Annex I).

## 3 APPROACH FOR DEVELOPING THE METHODOLOGY

The basic approach for developing the methodology is to refer, as far as possible, to existing and well-established practices used in other domains of application, and to adapt them to the CNS/ATM environment.

The adaptation is necessary because the methodology needs to reflect the context in which it is applied and to incorporate specifics of the proposed

approach for Air Navigation System such as covering the three types of system elements.

Although the methodology (ARP4754/4761 or ED79) on which SAM was originally based is oriented towards the certification of civil aircraft systems and equipment, SAM now consists of well-established, dedicated and best practices for safety assessment in ANS added since early editions.

Moreover, in relationship to the integration of airborne and ground-based components of Air Navigation System, it is believed that SAM total aviation system approach and end-to-end safety assessment will ease the assessment of the new generation of Air Navigation Systems.

It is anticipated to revise periodically the material in order to incorporate necessary improvements.

#### 4 STRUCTURE OF THE MANUAL

The material presented in the manual is structured into three different parts:

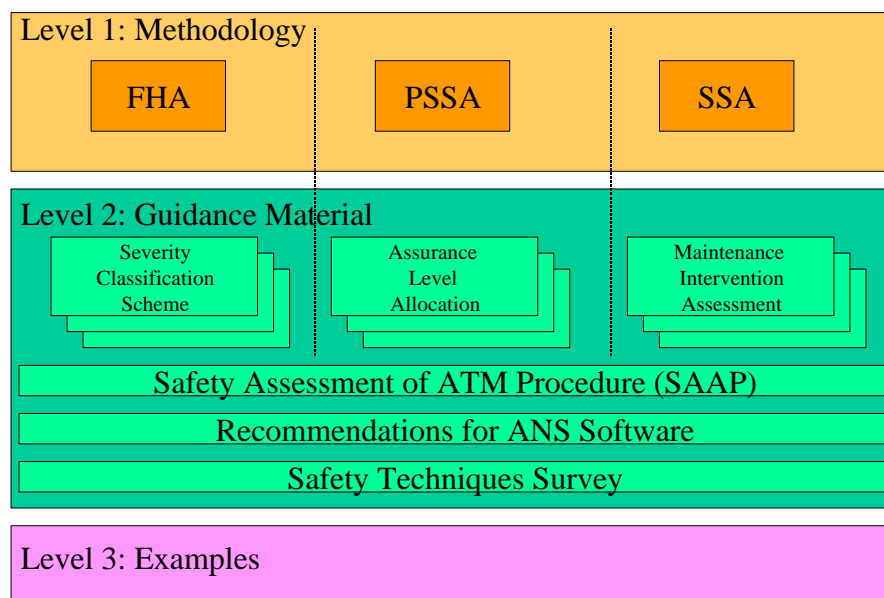
- ***Part I: Functional Hazard Assessment Process;***
- ***Part II: Preliminary System Safety Assessment Process;***
- ***Part III: System Safety Assessment Process;***
- ***Part IV: Annexes***

The ANS SAM is made of three levels of material:

- **Level 1:** The **methodology** following logically the steps:
  - FHA (Functional Hazard Assessment) (SAF.ET1.ST03.1000-MAN-01-01);
  - PSSA (Preliminary System Safety Assessment) (SAF.ET1.ST03.1000-MAN-01-02);
  - SSA (System Safety Assessment) (SAF.ET1.ST03.1000-MAN-01-03).
- **Level 2: Guidance Material (GM)** which are:
  - Providing further detailed information on the use of various techniques to achieve some parts of FHA or PSSA or SSA (then these GM are attached as annex to the chapter they refer to);

- Addressing specific system element throughout all the methodology steps such as ATM procedure or Software (then these GM are in PART IV such as “Safety Assessment of ATM Procedure” (SAAP) or “Recommendations for ANS SW”).
- **Level 3: Examples** of application of various techniques to real safety assessment (then these examples are attached as appendix to the SAM Step they refer to).

## SAM



The complete list of SAM material, including Level 1 (Methodology), Level 2 (Guidance Material) and Level 3 (Examples) documents, is provided in SAM-Intro Annex A.

An example of illustration of this SAM structure is (current status of Level 2 and Level 3 documents):

- **Level 1:** SAM Methodology
  - Part I – FHA:FHA methodology:
    - Chapter 1: Initiation;
    - Chapter 2: Planning;
    - Chapter 3: Safety Objectives Specification;
    - Chapter 4: FHA Evaluation;
    - Chapter 5: Completion;
  - Part II – PSSA: PSSA methodology:
    - Chapter 1: Initiation;
    - Chapter 2: Planning;
    - Chapter 3: Safety Requirements Specification;
    - Chapter 4: PSSA Evaluation;
    - Chapter 5: Completion;
  - Part III – SSA: SSA methodology:
    - Chapter 1: Initiation;
    - Chapter 2: Planning;
    - Chapter 3: Safety Assurance and Evidence Collection;
    - Chapter 4: SSA Evaluation;
    - Chapter 5: Completion;
- **Level 2:** Guidance Material (GM)
  - GM for SAM:
    - A: SAM content (Level 1, 2 & 3 material);
    - B: ESARR4 requirements compliance matrix;
    - C: SAM Awareness documentation (concepts and principles);
  - GM\_for FHA sub-steps:
    - GM for FHA - Chapter 1:
      - A: OED (Operational Environment Definition);
    - GM for FHA - Chapter 2:
      - A: Planning FHA activities;
    - GM for FHA - Chapter 3:
      - A. Planning and conducting FHA session;
      - B. Identification of failure modes, external events and hazards;
      - C. Identification of Hazards effects;
      - D. Severity Classification Scheme;
      - E. Risk Classification Scheme;
      - F. Safety Objective Classification Scheme;
      - G. Methods for setting Safety Objectives;
      - H. Results records;
      - I. Barrier Analysis;

- J. TLS (Target Level of Safety) apportionment method.
- GM for FHA - Chapter 4:
  - A-B-C: FHA Evaluation Activities;
- GM for Chapter 5:
  - A: FHA Report;
- GM for PSSA sub-steps:
  - GM for PSSA – Chapter 1;
  - GM for PSSA – Chapter 2;
  - GM for PSSA – Chapter 3:
    - A: Safety Requirement and Assurance Level Allocation (SWAL, PAL, ..);
    - B: Automation;
  - GM for PSSA - Chapter 4:
    - A-B-C: PSSA Evaluation Activities;
  - GM for PSSA – Chapter 5
    - A: PSSA Report
- GM for SSA sub-steps:
  - GM for SSA – Chapter 1;
  - GM for SSA – Chapter 2;
  - GM for SSA – Chapter 3:
    - A. SSA generic activities (testing, inspection, analysis, demonstration, ..);
    - B. SSA Activities along the lifecycle;
    - C. Maintenance intervention risk assessment;
  - GM for SSA - Chapter 4:
    - A-B-C: SSA Evaluation Activities;
  - GM for SSA – Chapter 5:
    - A: SSA Report;
- GM for SAM:
  - Part IV Annex A: Acronyms;
  - Part IV Annex B: Glossary;
  - Part IV Annex C: Initial Safety Plan;
  - Part IV Annex D: Safety Techniques Survey;
  - Part IV Annex E: ANS Software Lifecycle;
  - Part IV Annex F: Recommendations for ANS SW;
  - Part IV Annex G: Safety Assessment of ATM Procedures (SAAP);
  - Part IV Annex H: “what is a change”;

- Part IV Annex I: System X Safety Case Template;
- Part IV Annex J: HAZOP & TRACER;
- Part IV Annex K: Fault Tree Analysis;
- **Level 3:** Appendixes : Examples of application of methodology sub-steps and their Guidance Material:
  - FHA Appendixes:
    - A: FHA – Chapter 3 examples (Hazard assessment of OLDI, CPDLC, AGATE/A-ASMGCS); V2.0
    - B: TLS (Target Level of Safety) Apportionment method examples – En-Route airspace; V2.0
    - C: Safety Objective Classification Scheme (SOCS) examples; V2.0
    - D: ATCC Building FHA; V2.0.
    - E: Safety Targets for NAV application; V0.5 (Draft)
  - Part IV Appendixes:
    - A: Examples of “What is a change” processes; V1.0
      - A1: AVINOR 410 process (previously Part IV Annex H1);
      - A2: AVINOR 411 process (previously Part IV Annex H2);
      - A3: Czech ANS process (previously Part IV Annex H3);
      - A4: Swedish ANS process (previously Part IV Annex H4);
      - A5: French ANSP process (Word Document);
      - A6: French ANSP process (PowerPoint Document);





## 5 READERSHIP

These tables suggest a minimum reader’s attention to SAM.

A table is provided per part of the SAM step and even per Guidance Material when found necessary. The first row (type of readers) of each readership table is customised in accordance with the document to which it applies.

The table hereunder provides high-level guidelines of minimum reader’s attention. Of course, this high-level statement has to be refined per step of SAM and per material when specific. Some Guidance Material do not have necessarily to be “Detailed knowledge” for all “safety practitioners”. For example for the safety assessment of ATC procedure, safety practitioners

do not need to have a “Detailed knowledge” of Guidance Material on “Recommendations for ANS Software”.

	System (People, Procedure, Equipment) Designer	Safety Practitioner	Programme/project Manager	Programme/project Safety Manager
Level 1 Chapter 1 – 5 Of Methodology steps (FHA, PSSA, SSA)	N/A		✓	
Level 2 Guidance Material	✓		N/A	✓
Level 3 Examples	✓		N/A	✓

: Detailed knowledge;

✓ : Aware;

N/A: Not Applicable.

## 6 REFERENCES

- EATMP Safety Policy (Edition 2.0);
- ESARR 4, Risk Assessment and Mitigation in ATM, Edition 1.0 (05.04.2001);
- SRC DOC 12, Assessment of the EATMP Air Navigation System Safety Assessment Methodology (Edition 1.1) as a Means of Compliance with ESARR 4;
- EUROCAE ED78A, Guidelines for Approval of the Provision and Use of Air Traffic Services Supported by Data Communications (December 2000).



This page is left intentionally blank.