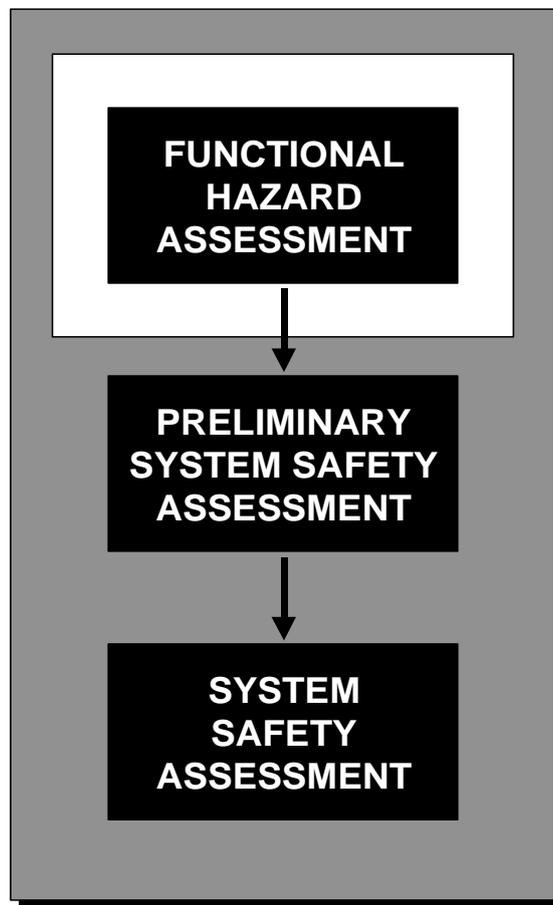


Safety Assessment Methodology

PART I

FUNCTIONAL HAZARD ASSESSMENT



This page is intentionally left blank.

TABLE OF CONTENTS

INTRODUCTION

1	OBJECTIVE OF FHA	I-6
2	WHEN AND HOW FHA IS APPLIED.....	I-7
3	STRUCTURE OF THE FHA DESCRIPTION	I-7
4	STRUCTURE OF THIS DOCUMENT	I-8
5	READERSHIP TABLE.....	I-8
6	CONFIGURATION MANAGEMENT, DOCUMENTATION AND RECORDS	I-9
6.1	WHY?	I-9
6.2	HOW?.....	I-10

CHAPTER 1 - FHA INITIATION

1	OBJECTIVE.....	I-13
2	INPUT.....	I-13
	• 2.1 System Description	I-13
	• 2.2 Operational Environment Description	I-14
	• 2.3 Regulatory Framework.....	I-14
	• 2.4 Applicable Standards	I-14
	• 2.5 Other Inputs	I-14
3	MAJOR TASKS	I-15
4	OUTPUT	I-15

CHAPTER 2 - FHA SAFETY PLANNING

1	OBJECTIVE.....	I-17
2	INPUT.....	I-17
3	MAJOR TASKS	I-17
4	OUTPUT	I-18

CHAPTER 3 – SAFETY OBJECTIVES SPECIFICATION

1	OBJECTIVE.....	I-19
2	INPUT.....	I-20
3	MAJOR TASKS	I-20
3.1	Identify Potential Hazards.....	I-22
3.2	Identify Hazard Effects	I-23
3.3	Assess Hazard Effects Severity.....	I-24
3.4	Specify Safety Objectives.....	I-24
3.5	Assess the intended aggregated risk	I-25

4 **OUTPUT** I-26

CHAPTER 4 - FHA EVALUATION

1 **OBJECTIVE** I-27

2 **INPUT** I-29

3 **MAJOR TASKS** I-29

- 3.1 **FHA Verification tasks** I-30
- 3.2 **FHA Validation tasks** I-30
- 3.3 **FHA Process Assurance** I-31

4 **OUTPUT** I-31

CHAPTER 5 - FHA COMPLETION

1 **OBJECTIVE** I-33

2 **INPUT** I-33

3 **MAJOR TASKS** I-33

4 **OUTPUT** I-34

INTRODUCTION

1 OBJECTIVE OF FHA

Functional Hazard Assessment (FHA) is a top-down iterative process, initiated at the beginning of the development or modification of an Air Navigation System. The objective of the FHA process is to determine: how safe does the system need to be.

The process identifies potential failures modes and hazards. It assesses the consequences of their occurrences on the safety of operations, including aircraft operations, within a specified operational environment.

The FHA process specifies overall **Safety Objectives** of the system, i.e. specifies the safety level to be achieved by the system.

2 WHEN AND HOW FHA IS APPLIED

The essential pre-requisite for conducting an FHA is a description of the high level functions of the system – such as would typically be specified in an operational concept document.

FHA is therefore first conducted during the **System Definition** phase of the system life cycle.

The purposes of the System Definition phase are to establish basic operational objectives for the system within its specified operational environment, to identify the functions required to achieve these objectives, and to specify system and interfaces (between functions and with the environment) requirements.

FHA is performed before the functions have been allocated to equipment, procedures or people elements: it considers what the proposed system will do, rather than how these elements should implement the functions. Indeed, FHA results will be used to support the process of function allocation.

In practice, however, development and assessment usually proceed in parallel, and some allocation of functions may already have been determined by practical constraints – especially where an existing system is being modified.

FHA can be applied at different levels. Ideally, FHA should be done at the overall Air Navigation Service or System level so that Safety Objectives are specified at this ANS level. Ideally Safety Requirements should be derived on sub-system elements during PSSA of this overall Air Navigation Service or System. So ideally there should be no need for FHA at sub-system level.

However, as of today, FHA is generally done at sub-system level and not at ANS level. Consequently, this methodology provides Guidance Material which addresses both ways of applying it.

FHA is an iterative process, which should be reviewed, revised and refined to cover lower level functions as the allocation of function is decided and the system design evolves.

3 STRUCTURE OF THE FHA DESCRIPTION

The structure adopted for the description of the FHA process is illustrated in Figure I-1 and Table I-1 in this chapter.

There are three key steps that have to be conducted whatever the size, complexity or organisational structure of the Programme/Project:

FHA Initiation (Chapter 1);

Specification of Safety Objectives (Chapter 3);

FHA Completion (Chapter 5).

The remaining two steps should be tailored to the size, complexity and organisational structure of the Programme/Project:

FHA Planning step (Chapter 2);

FHA Evaluation step (Chapter 4).

Table I-1 summarises the major activities conducted in each step of the FHA, and their inputs and outputs.

4. STRUCTURE OF THIS DOCUMENT.

This document is in three main parts;

- **Chapters**, which describe the methodology and are printed on white paper;
- **Guidance Material**, which follows as annex each chapter for which it provides guidance and amplifies and explains the methodology, this is printed on colorA paper;
- **Appendixes**, which provide background material and examples and are printed on colorB paper.

5. READERSHIP OF FHA

The following table suggests a minimum attention to FHA material:

FHA Material	System (People, Procedure, Equipment) Designer	Safety Practitioner	Programme/project Manager	Programme/project Safety Manager
Introduction	✓			
Chapter 1 FHA Initiation	N/A		N/A	✓

FHA Material	System (People, Procedure, Equipment) Designer	Safety Practitioner	Programme/project Manager	Programme/project Safety Manager
Chapter 2 FHA Planning		✓	✓	✓
Chapter 3 SOS	✓		✓	
Chapter 4 FHA Evaluation	✓		N/A	✓
Chapter 5 FHA Completion	✓		N/A	✓
Guidance Material		✓	✓	✓
Examples	N/A	✓	N/A	✓

6. CONFIGURATION MANAGEMENT, DOCUMENTATION AND RECORDS.

A configuration management system should track the outputs of the FHA process and the relationship between them.

6.1 Why?

Not only is it important that the FHA process is carried out correctly and completely, it is also important that the FHA process should be clear and auditable.

The three important reasons are:

- To demonstrate to second and third parties (including the regulator) that, at this stage of the lifecycle: system definition, the

system aims at having a safety level where risk is expected to be reduced to an acceptable level once the system is in operation;

- To maintain a record of why decisions were taken, to ensure that further change does not invalidate the assessment or does not lead to unnecessarily repeating it;
- To support the hand-over of safety responsibilities from one individual or organisation to another.

6.2 How?

An appropriate and useable control scheme that ensures the origin, version control, traceability and approval of all documentation is recommended.

The extent of safety records maintained by a project will depend on the complexity and levels of risk involved. Safety records are difficult to replace so there must be appropriate security and backup to ensure that records are preserved. Up-to-date records should be kept throughout the system lifetime (including decommissioning).

A number of people will contribute to and need access to safety documentation, typically project staff, engineering staff, operational staff, safety specialists, managers and regulators.

The configuration management and documentation control schemes should include procedures to:

- To develop a configuration management plan;
- To establish a consistent and complete set of baseline documents;
- To ensure there is a reliable method of version identification and control;
- To establish and monitor the change management process;
- To archive, retrieve and release documents.

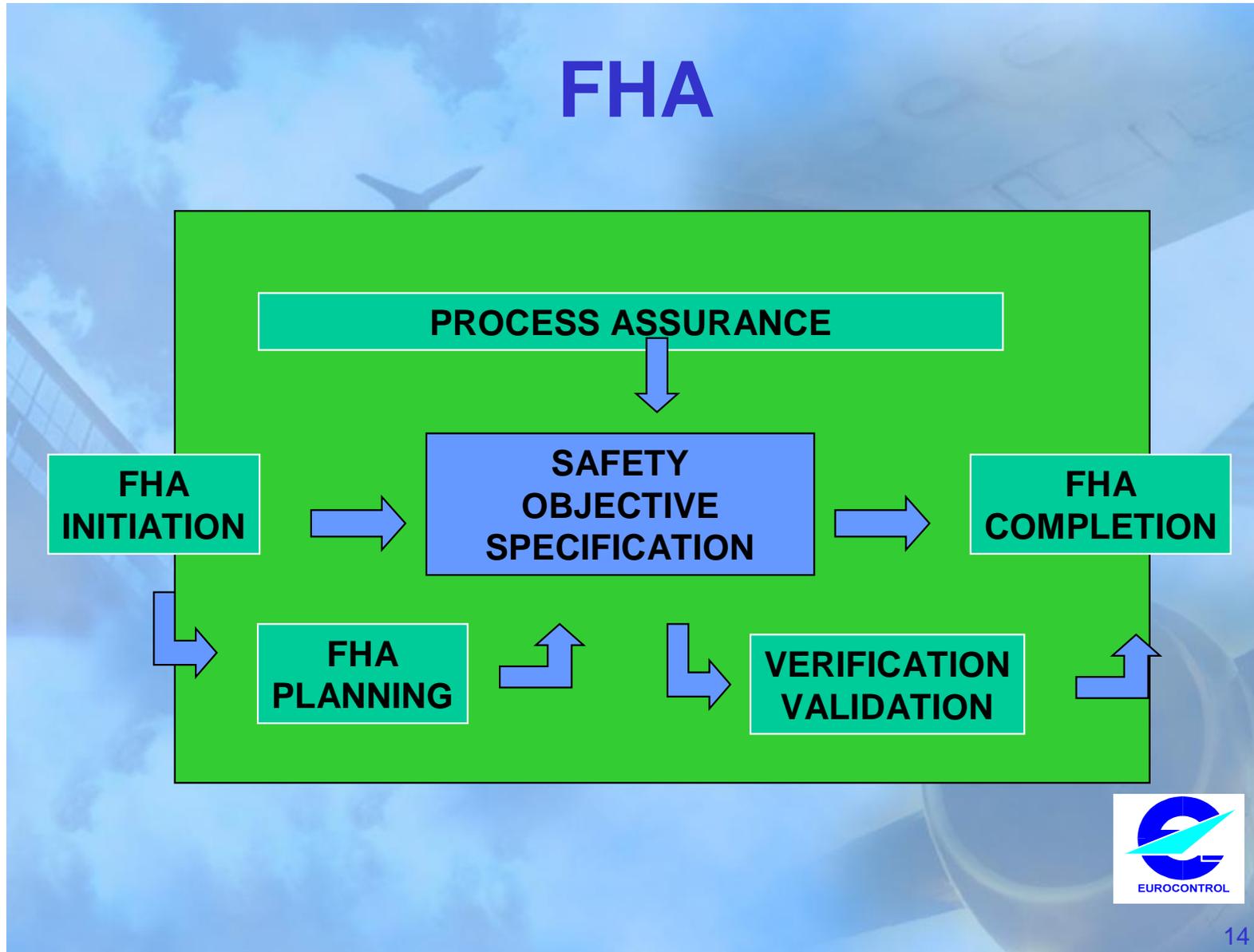


Figure I-1 – Overall FHA Process

This page is intentionally left blank.

FHA STEP	OBJECTIVES	INPUT	MAJOR TASKS	OUTPUT
1 FHA Initiation	<ul style="list-style-type: none"> Develop a level of understanding of the system, its operational environment and, if appropriate, its regulatory framework, sufficient to enable the safety assessment activities to be satisfactorily carried out. 	<ul style="list-style-type: none"> System Description Operational Environment Description Regulatory Framework Applicable Standards Other Inputs (e.g., other FHA results, hazard database, incident investigation reports, lessons learned, etc.) 	<ul style="list-style-type: none"> Gather all necessary information describing the system. Review this information to establish that it is sufficient to carry out the FHA. If not available, describe the operational environment of the system. Identify and record assumptions made. Formally place the input information under configuration management. 	<ul style="list-style-type: none"> Gathered input information describing the system under configuration management. Derived information (e.g., description of the operational environment, of the external interfaces, list of functions, list of assumptions) under configuration management.
2 FHA Planning	<ul style="list-style-type: none"> Define the objectives and scope of the FHA, the activities to be carried out, their deliverables, their schedule and the required resources. 	<ul style="list-style-type: none"> Overall Project/Programme plans Initial Safety Plan 	<ul style="list-style-type: none"> Identify and describe the more specific activities for each FHA step. Submit the FHA plan to peer review to provide assurance of its suitability. Submit the FHA plan for comment or approval to interested parties (including regulatory authorities), as appropriate. Formally place the FHA plan under configuration management. Disseminate the plan to all interested parties. 	<ul style="list-style-type: none"> Reviewed and approved FHA Plan.
3 Safety Objectives Specification	<ul style="list-style-type: none"> To identify all potential hazards associated with the system; To identify hazard effects on operations, including the effect on aircraft operations; To assess the severity of each hazard effect; To specify Safety Objectives, i.e. to determine the maximum frequency of hazard's occurrence; To assess the overall foreseen (future) risk associated to introducing the change or new system. 	<ul style="list-style-type: none"> Information gathered or derived in the FHA Initiation step Severity Classification Scheme Organisation Risk Classification Scheme Safety Objective Classification Scheme 	<p>For each system function and combination of functions:</p> <ul style="list-style-type: none"> Identify potential hazards Identify hazard effects Assess the severity of hazard effects. Specify Safety Objectives. Assess intended aggregated risk. 	<ul style="list-style-type: none"> List of hazards, with the rationale for the severity classification of their effects System Safety Objectives Assumptions <p>The output of this step should be formally placed under configuration management.</p>
4 FHA Evaluation				
FHA Verification	<ul style="list-style-type: none"> To demonstrate that the set of Safety Objectives meet the Organisation Safety Target, i.e. the overall acceptable level of risk. 	<ul style="list-style-type: none"> Information gathered or derived during the FHA steps; Initial Safety Plan and FHA Plan; Intermediate and final outputs of the FHA process. 	<ul style="list-style-type: none"> Review and analyse the results of the FHA process. 	Results of the FHA Verification task
FHA Validation	<ul style="list-style-type: none"> To ensure that the Safety Objectives are (and remain) correct and complete; To ensure that all safety-related assumptions are credible, appropriately justified and documented. 	<ul style="list-style-type: none"> Information gathered or derived during the FHA steps; Initial Safety Plan and FHA Plan; Intermediate and final outputs of the FHA process. 	<ul style="list-style-type: none"> Review and analyse the Safety Objectives to ensure their completeness and correctness; Review and analyse the description of the operational environment to ensure its completeness and correctness; Review, analyse, justify and document safety-related assumptions about the system, its operational environment and its regulatory framework to ensure their completeness and correctness. Review and analyse traceability between functions, failures, hazards, hazard's effects and Safety Objectives. Review and analyse the credibility and sensitivity of derived Safety Objectives to assumptions and risk. 	Results of the FHA Validation task
FHA Assurance Process	<ul style="list-style-type: none"> To provide assurance and evidence that all FHA activities (including FHA Verification and FHA Validation) have been conducted according to the plan; To ensure that the FHA process as described in the FHA Plan is correct and complete. 	<ul style="list-style-type: none"> Information gathered or derived during the FHA steps; Initial Safety Plan and FHA Plan; Intermediate and final outputs of the FHA process. 	<ul style="list-style-type: none"> Ensure that FHA steps are applied; Ensure that assessment approaches are applied; Ensure that all outputs of the FHA steps, including FHA Verification, FHA Validation and FHA Process Assurance are formally placed under configuration management; Ensure that any deficiencies detected during FHA Verification or FHA Validation activities have been resolved; Ensure that the FHA process would be repeatable by personnel other than the original analyst(s); Ensure that the findings have been disseminated to interested parties; Ensure that the outputs of the FHA process are not incorrect and/or incomplete due to deficiencies in the FHA process itself. 	Results of the FHA Process Assurance task
5 FHA Completion	<ul style="list-style-type: none"> To record the results of the complete FHA process; To disseminate these results to all interested parties 	<ul style="list-style-type: none"> Outputs from all previous steps 	<ul style="list-style-type: none"> Document the results of the FHA process (including the results of FHA Verification, FHA Validation and FHA Process Assurance activities); Formally place the FHA documentation under configuration management; Disseminate the FHA documentation to all interested parties. 	<ul style="list-style-type: none"> FHA results, under configuration management.

Table I-1. FHA Process Description