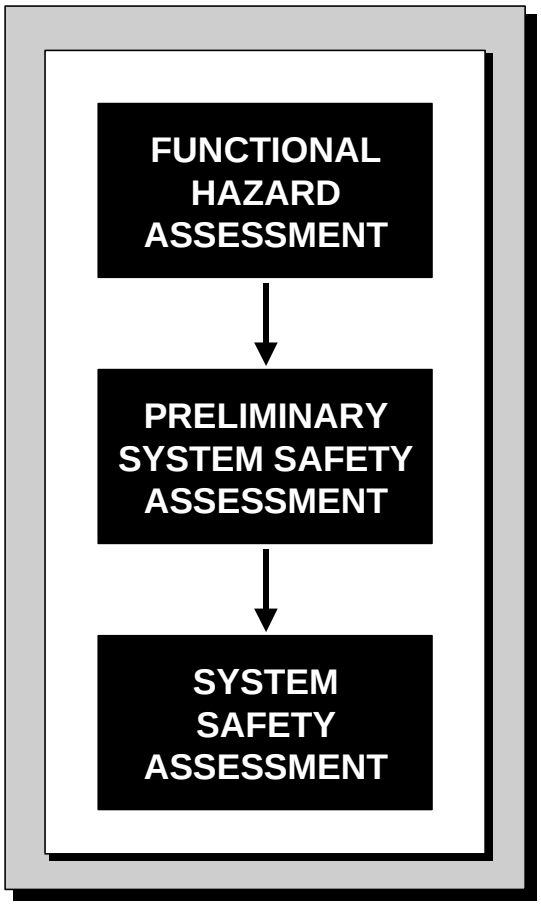
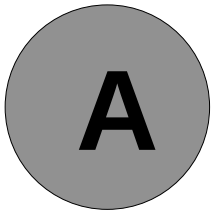
PART IV

ANNEXES



This page is left blank intentionally.

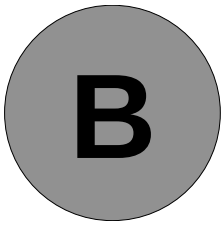


ACRONYMS

ANS	Air Navigation Service
ARP	Aerospace Recommended Practice
ATCO	Air Traffic Control Officer
ATM	Air Traffic Management
ATS	Air Traffic Service
CCA	Common Cause Analysis
CMA	Common Mode Analysis
CNS	Communications, Navigation and Surveillance
CPDLC	Controller/Pilot Data Communications
ESARR	EUROCONTROL Safety Regulatory Requirement
ETA	Event Tree Analysis
EUROCAE	European Organisation for Civil Aviation Equipment
FAA	Federal Aviation Authority

FAA	Federal Aviation Authority
FHA	Functional Hazard Assessment
FTA	Fault Tree Analysis
HWAL	HardWare Assurance Level
JAA	Joint Airworthiness Authorities
OCD	Operational Concept Document
OLDI	On-Line Data Interchange
PAL	Procedure Assurance Level
PRA	Particular Risk Analysis
PSSA	Preliminary System Safety Assessment
RCS	Risk Classification Scheme
SAM	Safety Assessment Methodology
SMGCS	Surface Movement Guidance and Control System
SOCS	Safety Objective Classification Scheme
SSA	System Safety Assessment
SWAL	SoftWare Assurance Level
TLS	Target Level of Safety
TMA	Terminal Manoeuvring Area
ZSA	Zonal Safety Analysis

This page is intentionally left blank.



GLOSSARY

The definition of any term useful to apply SAM should be found in ESARR4. This glossary includes only those terms for which a different definition was necessary.

1. Air Navigation System

The aggregate of organisations, people, infrastructure, equipment, procedures, rules and information used to provide the Airspace Users Air Navigation Services in order to ensure the safety, regularity and efficiency of air navigation.

2. Assessment

An evaluation based on engineering, operational judgement and/or analysis methods.

3. Safety Assurance

All planned and systematic actions necessary to provide adequate confidence that a product, a service, an organisation or a system achieves acceptable or tolerable safety.

4. External Event

An occurrence which has its origin distinct from the considered system.

5. Failure

The inability of an Air Navigation System to perform its intended function or to perform it correctly within specified limits.

6. Hazard

Any condition, event, or circumstance which could induce an accident.

7. Incident

An occurrence, other than an accident, associated with the operation of an aircraft, which affects or could affect the safety of operations.

8. Risk

The combination of the overall probability, or frequency of occurrence of a harmful effect induced by a hazard and the severity of that effect.

9. Safety

Freedom from unacceptable risk.

10. Safety Objective

Quantitative or qualitative statement that defines the maximum frequency or probability at which a hazard can be accepted to occur.

11. Severity

Level of effect/consequences of hazards on the safety of operations, including the aircraft operations.

12. Severity Class

Gradation, ranging from 1 (most severe) to 5 (least severe), as an expression of the magnitude of the effects of hazards on operations, including the aircraft operations.

13. Target Level of Safety

A level of how far safety is to be pursued in a given context, assessed with reference to an acceptable or tolerable risk.

14. Verification

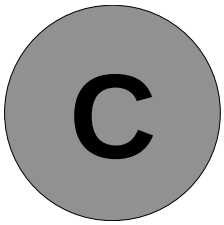
Confirmation by examination and provision of objective evidence that the requirements have been fulfilled. (ISO 8402)

15. Validation

Confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled. (ISO 8402)

16. Worst Credible

See FHA Chapter 3 Guidance Material G.



SAFETY PLANNING PRELIMINARY GUIDANCE MATERIAL

1 PRINCIPLES

A basic principle of Safety (and Project) Management is:

- To produce a plan describing the activities to be carried out,
- To submit the plan to review to provide assurance of its suitability,
- To follow the plan and finally,
- To show that the plan has been followed.

Assurance of safety is provided by demonstrating that the agreed Safety Plan has been followed.

The Safety Plan is necessarily an evolutionary document. It should be updated for each main phase of the Safety Assessment process or system life cycle.

The default Safety Planning process is:

- During the FHA, develop an Initial Safety Plan. It should describe the safety policy and justify the overall strategy adopted for the Project/Programme. It should also describe the major activities and deliverables identified for implementing the policy and strategy.

- During PSSA, update the initial Safety Plan to define the safety assessment activities to be carried out during the System Design Phase. It should in particular describe the approach adopted to ensure that the system architecture is expected to achieve the specified Safety Objectives.

- During SSA, update the Safety Plan to describe how the Safety Requirements are to be met. The Safety Plan should define the means for evaluating the fulfilment of Safety Requirements and the achievement of Safety Objectives. It should also specify specific procedures to be used during the operations and maintenance, and decommissioning of the System.

2 APPLICATION

2.1 Responsibilities

Generally, the Project or Programme Manager should be responsible for the preparation of a Safety Plan and for ensuring that safety activities are carried out by properly trained, qualified and competent personnel.

The Project or Programme Manager may delegate the preparation of the Safety Plan to suitably qualified and competent personnel, but should retain the overall responsibility.

The Safety Plan should be formally reviewed by all persons, departments and organisations concerned by its implementation. Agreement should be gained on the contents.

In particular, the Project/Programme Manager should establish if the Safety Plan requires a formal endorsement by the regulatory authority.

Finally the Project/Programme Manager should ensure that all those involved in implementing the Safety Plan are informed of responsibilities assigned to them under the Plan.

2.2 Size and Depth of the Safety Plan, Frequency of Updates

The size and depth of the Safety Plan will depend on the complexity and the safety criticality (risk level) presented by the Air Navigation System.

For simple Project or Programme, and systems presenting low risk, a simple Safety Plan defining the Project/Programme personnel and justifying the overall approach may be sufficient. The Safety Plan may be included in a section of the overall Project/Programme Plan.

For more complex Project/Programme and systems presenting higher levels of risks, a complete Safety Plan should be developed. Several documents may be developed, for example, one document for the overall system and one document for each major sub-systems.

More frequent updates may be required to reflect changes in, for example, the concept, the programme or the project organisation.

At any given time, the Safety Plan should give a valid overview of how the safety assessment process is being applied.

3 CONTENT OF AN INITIAL SAFETY PLAN

3.1 Defining the Overall Approach to Safety Assessment

This guidance material outlines the tasks involved in defining the overall approach to safety within a Project/Programme:

- Define the overall Safety Policy and Strategy for the Project/Programme.

> ***Note.***
>
> *To define the overall Safety Policy and Strategy for the Project/Programme, one could refer to the EATMP Safety Policy and describe how each policy statement and principle will be implemented in the Project/Programme.*

- Describe and justify the approach adopted for the safety assessment of the system.
- Describe the relationships between the safety assessment process and the system life cycle.
- Identify major safety deliverables and describe their relationships with the major milestones of the Project/Programme.
- Identify interfaces with other Projects/Programmes, if appropriate.
- Describe major assumptions on the system and/or its interfaces, that may have an impact on the safety of the system.

- Identify particular issues or features that may have an impact on the safety of the system (e.g., introduction of new technology).

- Identify persons, departments and organisations involved in the Safety Assessment process.

Note.

Individuals include, for example, the Project/Programme manager, system and safety experts. Internal departments concerned include the safety department and safety review panels. Organisations include suppliers, contractors and consultants, end user representatives and regulators. Interactions between these organisations, and responsibilities for development, review, authorisation, approval and acceptance of the Project/Programme safety deliverables will be defined.

3.2 Example of Initial Safety Plan Pro-Forma

The Plan should document the outcomes of all the safety planning activities. It should be concise and readily comprehensible, and should refer to, rather than repeat material which is adequately documented elsewhere. For example, it is only necessary to document *differences* from the generic FHA process.

The Plan should be an aid to the project team, not an additional burden. It should be distributed to, or at least accessible by, all the organisations, departments and individuals involved. It is therefore important that it should be written in a way intelligible to readers with a wide range of experience and involvement with the system.

A possible structure for a Safety Plan is shown in Table 1.

Version control information

Date of latest revision, approval status.

Introduction

- Aims and objectives of the Plan.
- A high-level description of the Programme/Project objectives.
- A high-level description of the system purpose, operational scenarios, functions, boundaries, interfaces and operational environment.
- Scope of the Plan – Phases of safety assessment process covered by the current issue of the Safety Plan.
- Structure of the Plan.

Safety Criteria

- The regulatory and organisational requirements, and standards to be met, justifying their selection or the choice of an alternative approach where necessary.
- A justified statement of the specific targets to be applied to the system (e.g., any quantified Safety Objectives used in the Risk Classification Scheme), or of the approach to setting such targets.

Safety Assessment Approach

- Definition of the safety policy and strategy adopted by the Project/Programme.

Roles and Responsibilities

- Responsibilities for safety assessment activities – by organisation, department, job title on the Project and individual name.

Inputs, Activities, Methods and Outputs

- General description of the safety assessment activities to be performed, their inputs and outputs, the methods to be used

Safety Assurance Activities

- General approach for the Safety Assurance activities.

Schedule and Resource Allocation

Plans for the next stage

- Outline of how the next stages of safety assessment are expected to progress.

Table 1 - A Typical Pro Forma for a Safety Plan

This page is intentionally left blank.