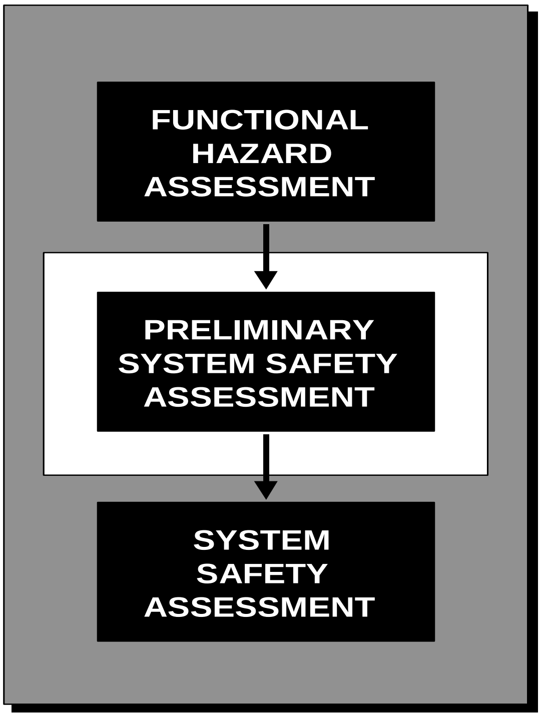
Safety Assessment Methodology

PART II

PRELIMINARY SYSTEM SAFETY ASSESSMENT


FUNCTIONAL HAZARD ASSESSMENT
PRELIMINARY SYSTEM SAFETY ASSESSMENT
SYSTEM SAFETY ASSESSMENT

This page is intentionally blank

TABLE OF CONTENTS

INTRODUCTION

CHAPTER 1 - PSSA INITIATION

CHAPTER 2 - PSSA SAFETY PLANNING

CHAPTER 3 – SAFETY REQUIREMENTS SPECIFICATION

CHAPTER 4 - PSSA EVALUATION

CHAPTER 5 - PSSA COMPLETION

INTRODUCTION

The ***Preliminary System Safety Assessment*** (PSSA) is the second of the three major steps in the generic process for the safety assessment of Air Navigation Systems. The PSSA seeks to answer the question "How Safe is the System Architecture?"

1. OBJECTIVE OF PSSA

Preliminary System Safety Assessment (PSSA) is a mainly top-down iterative process, initiated at the beginning of a new design or modification to an existing design of an Air Navigation System. The objective of performing a PSSA is to demonstrate whether the assessed system architecture can reasonably be expected to achieve the Safety Objectives specified in the FHA.

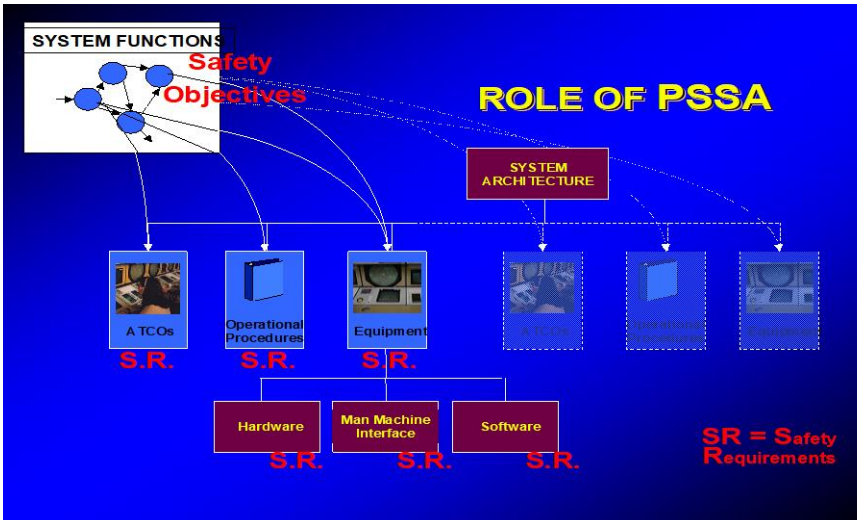
As a reminder, a **Safety Objective** [ESARR4] is a qualitative or quantitative statement that defines the maximum frequency or probability at which a hazard can be accepted to occur. ("Accepted" is underlined because this is the only difference with ESARR4 definition where "expected" is replaced with "accepted" as recommended by SRC DOC 20 Appendix C)

A **Safety Requirement** [ESARR4] is a risk mitigation means, defined from the risk mitigation strategy that achieves a particular safety objective. Safety requirements may take various forms, including organisational, operational, procedural, functional, performance, and interoperability requirements or environment characteristics.

The PSSA process apportions **Safety Objectives** into **Safety Requirements** allocated to the system elements, i.e. specifies the risk level to be achieved by the system elements. PSSA also identifies an Assurance Level per system element.

The system architecture can only achieve the Safety Objectives established during the FHA, provided the architecture elements meet their Safety Requirements.

Figure 1 Role of the PSSA



2. WHEN AND HOW PSSA IS APPLIED

PSSA is conducted during the ***System Design*** phase of the system life cycle.

A PSSA should be performed for a new system or each time there is a change to the design of an existing system. In the second case, the purpose of PSSA is to identify the impact of such a change on the architecture and to ensure the ability of the new architecture to meet either the same or new Safety Objectives.

The essential pre-requisite for conducting a PSSA is a description of the high level functions of the system, with a list of assumptions, hazards and their associated safety objectives. All these are outputs of the FHA (Functional Hazard Assessment). The list of hazards and Safety Objectives comes primarily from FHA and is further completed during PSSA.

The Safety Assessment Methodology aims at limiting the number of iterations between system development activities and safety assessment. Development and safety assessment usually proceed in parallel.

PSSA is therefore an iterative process, which should be reviewed, revised and refined as the derivation of safety requirements and the system design (for non-safety reasons e.g. performance, interoperability, security,..) evolve. It provides guidance on how to identify the extent of the re-analysis required. It may even show that meeting Safety Objectives as identified by FHA cannot be achieved and consequently lead to a re-iteration of the FHA.

3. STRUCTURE OF THE PSSA DESCRIPTION

The structure adopted for the description of the PSSA process is illustrated in Table 1 and Figure 2 in this chapter.

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

PSSA Initiation (Chapter 1);

Specification of Safety Requirements (Chapter 3);

PSSA Completion (Chapter 5).

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

PSSA Planning step (Chapter 2);

PSSA Evaluation step (Chapter 4).

Table 1 summarises the major activities conducted in each step of the PSSA, 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 TABLE

The following table suggests a minimum attention to PSSA Material:

PSSA Material	System (People, Procedure, Equipment) Designer	Safety Practitioner	Programme/project Manager	Programme/project Safety Manager
Introduction	✓	📖	📖	📖
Chapter 1 PSSA Initiation	N/A	📖	N/A	✓
Chapter 2 PSSA Planning	📖	✓	✓	✓
Chapter 3 SRS	✓	📖	✓	📖
Chapter 4 PSSA Evaluation	✓	📖	N/A	✓
Chapter 5 PSSA 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 PSSA process and the relationship between them.

6.1 Why?

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

The three important reasons are:

- To demonstrate to third parties (including the regulator) that risks have been reduced to an acceptable level;
- 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.

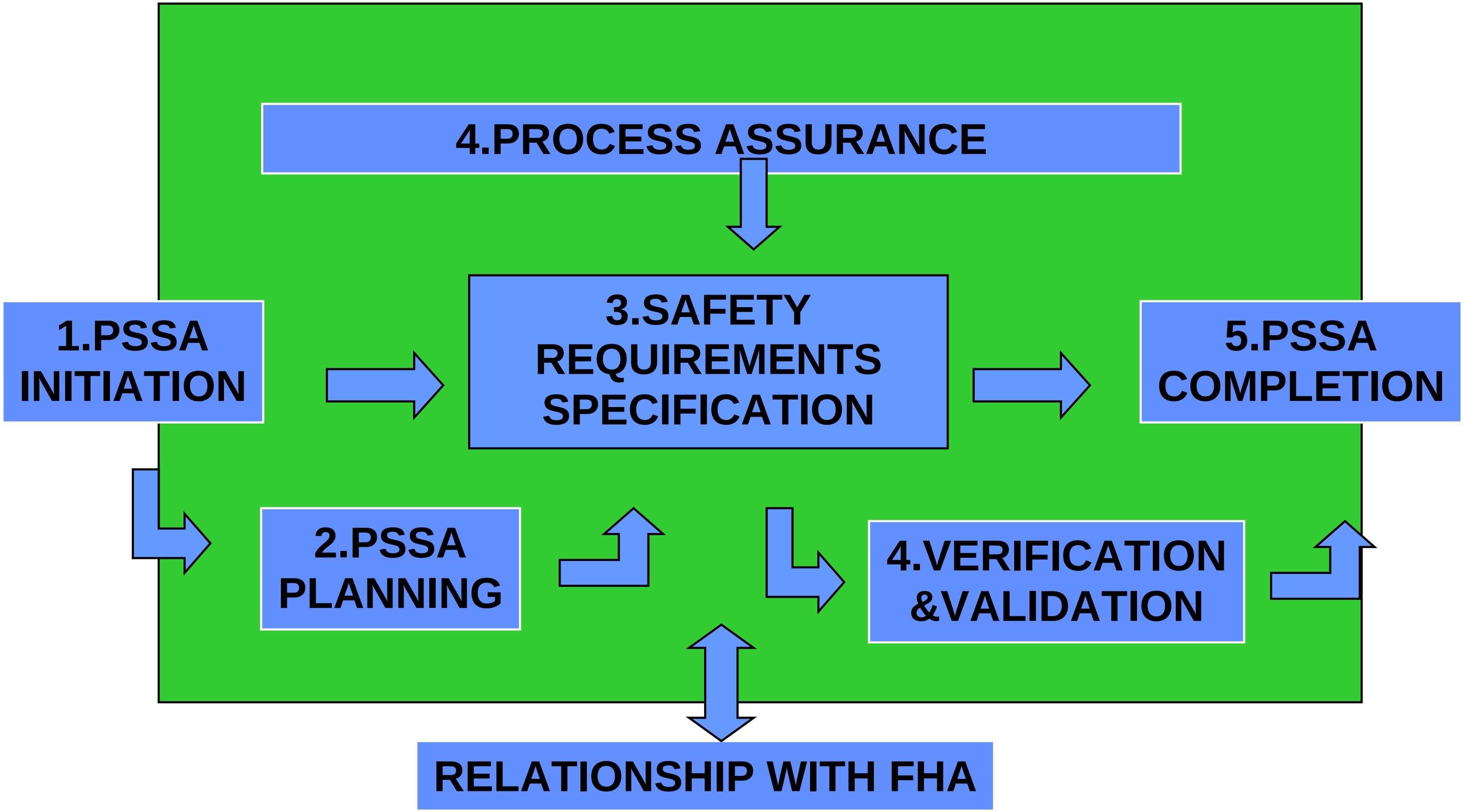


Figure 2: PSSA Process

PSSA STEP	OBJECTIVES	INPUT	MAJOR TASKS	OUTPUT

1
PSSA Initiation
	Develop a level of understanding of the system design framework, its operational environment and, if appropriate, its regulatory framework, sufficient to enable the safety assessment activities to be satisfactorily carried out.	System Definition & System Design;
		Operational Environment Description;
		Regulatory Requirements;
		Applicable Standards;
		FHA output;
		Other Inputs (e.g., other PSSA results, hazard databases, incident investigation reports, lessons learned, …).
			Gather all necessary information describing the system design;
			Review this information to establish that it is sufficient to carry out the PSSA;
			Update the Operational Environment Description (OED) of the system (add PSSA-related data to FHA-related data);
			Identify and record assumptions made;
			Formally place all information under a documentation control scheme.
				Input information describing the system design;
				Derived information (e.g., description of the operational environment, list of assumptions).

2
PSSA Planning
	Define the objectives and scope of the PSSA, the activities to be carried out, their deliverables, their schedule and the required resources.	Overall Project/Programme plans;
		Safety Plan;
		FHA Report.
			Identify and describe the more specific activities for each PSSA step in a PSSA Plan;
			Submit the PSSA plan to peer review to provide assurance of its suitability;
			Submit the PSSA plan for comment or approval to interested parties (including regulatory authorities), as appropriate;
			Formally place the PSSA plan under a documentation control scheme;
			Disseminate the PSSA plan to all interested parties.
				Reviewed and approved PSSA Plan.

3 **Safety Requirements Specification**	Derive Safety Requirements for each individual system element (People, Procedure and Equipment)	PSSA Initiation output, such as: Assumptions list; FHA output: Functions, hazards and their effects list, System Safety Objectives; System Architecture(s)…	For each function and combination of functions, • Refine the functional breakdown; • Evaluate system architecture(s); • Apply risk mitigation strategies; • Apportion Safety Objectives in to Safety Requirements; • Balance/Reconcile Safety Requirements.	Updated list of assumptions; Updated list of hazards and Safety Objectives; Safety analyses results; Justification material for risk mitigation strategies application; Safety Requirements.
4 **PSSA Evaluation**				
PSSA Verification	To ensure that Safety Requirements meet Safety Objectives.	Information gathered or derived in the PSSA steps; Safety Plan and PSSA Plan; Outputs (including the final one) of the PSSA process.	Review and analyse the results of the PSSA process.	PSSA Verification results.
PSSA Validation	To ensure that the Safety Requirements are (and remain) correct and complete; To ensure that safety-related assumptions are (and remain) correct and complete.	Information gathered or derived in the PSSA steps; Safety Plan and PSSA Plan; Outputs (including the final one) of the PSSA process.	Review and analyse Safety Requirements 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 critical assumptions about the system design, its operational environment and its regulatory framework to ensure their completeness and correctness; Review and analyse traceability between Safety Objectives and Safety Requirements; Review and analyse the credibility and sensitivity of Safety Requirements with respect to the Safety Objectives and the assumptions.	PSSA Validation results.
PSSA Process Assurance	To provide assurance and evidence that all PSSA activities (including PSSA Verification and PSSA Validation tasks) have been conducted according to the PSSA plan; To ensure that the PSSA process as described in the PSSA plan is correct and complete.	Information gathered or derived in the PSSA steps; Safety Plan and PSSA Plan; Outputs (including the final one) of the PSSA process.	The PSSA Process assurance tasks should at least ensure in accordance with the PSSA Plan that: • The PSSA steps are applied; • Assessment approaches (e.g. success approach, failure approach, use of safety methods and techniques such as Fault-Tree, FMEA, CCA, …) are applied; • All outputs of the PSSA steps (including PSSA Validation and Verification output) are formally placed under a configuration management scheme; • Any deficiencies detected during PSSA Verification or Validation activities have been resolved; • The PSSA process would be repeatable by personnel other than the original analyst(s); • The findings have been disseminated to interested parties; • Outputs of the PSSA process are not incorrect and/or incomplete due to deficiencies in the PSSA process itself.	PSSA Process Assurance results.
5 **PSSA Completion**	To document and formally place the results of the whole PSSA process under a configuration management scheme; To disseminate these results to all interested parties.	Outputs of all other PSSA steps	Document the results of the PSSA process (including the results of PSSA Validation, Verification and Process Assurance activities); Formally place the PSSA results under a configuration management scheme; Disseminate the PSSA documentation to all interested parties.	PSSA results formally placed under a configuration management scheme.

Table 1: PSSA Process: Input, Major Tasks and Output