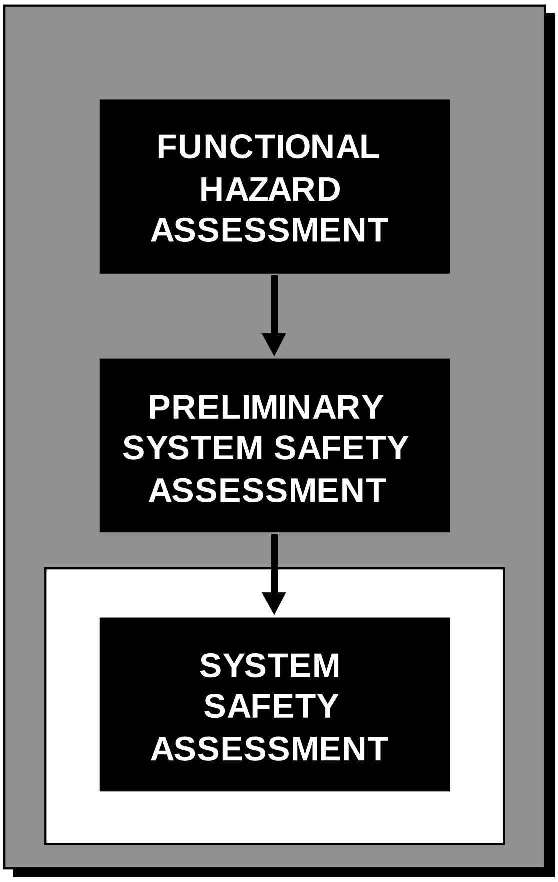
Safety Assessment Methodology

PART III

SYSTEM SAFETY ASSESSMENT


FUNCTIONAL HAZARD ASSESSMENT
PRELIMINARY SYSTEM SAFETY ASSESSMENT
SYSTEM SAFETY ASSESSMENT

This page is intentionally blank

TABLE OF CONTENTS

INTRODUCTION

CHAPTER 1 - SSA INITIATION

CHAPTER 2 - SSA SAFETY PLANNING

CHAPTER 3 – SAFETY ASSURANCE & EVIDENCE COLLECTION

CHAPTER 4 - SSA EVALUATION

CHAPTER 5 - SSA COMPLETION

INTRODUCTION

The ***System Safety Assessment*** (SSA) is the third of the three major steps in the generic process for the safety assessment of Air Navigation Systems. The SSA seeks to answer the question "Does the System as implemented achieve an acceptable risk?"

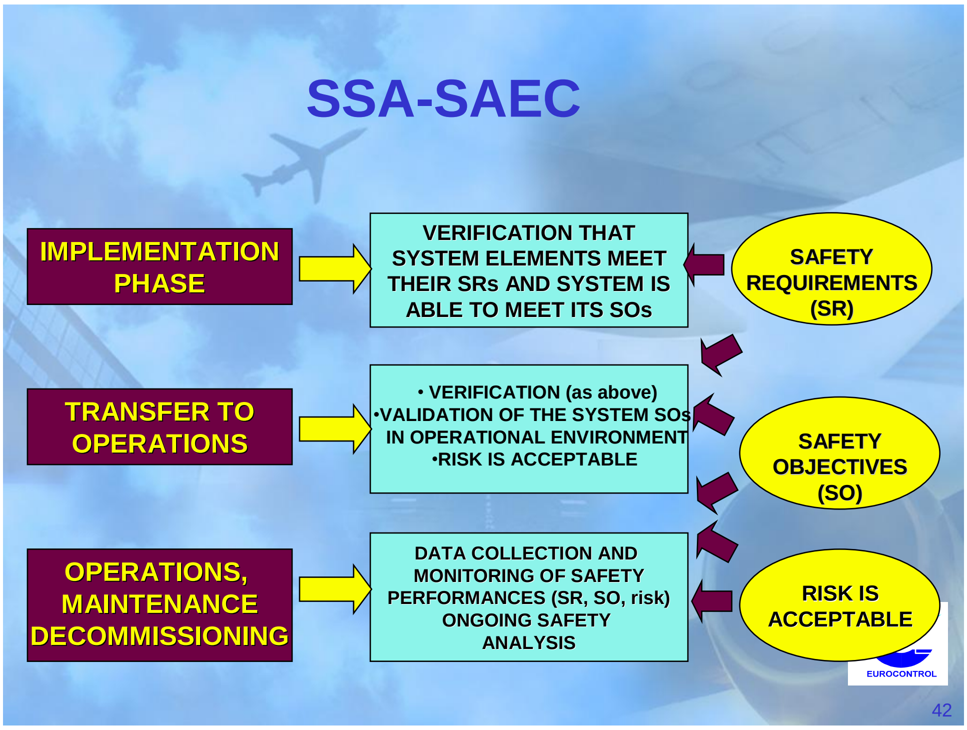
1. OBJECTIVE OF SSA

System Safety Assessment (SSA) is a process initiated at the beginning of the implementation of an Air Navigation System.

The objective of performing a SSA is to demonstrate that the system as implemented achieves an acceptable (or at least a tolerable) risk and consequently satisfies its Safety Objectives specified in the FHA and the system elements meet their Safety Requirements specified in the PSSA.

The SSA process **collects evidences** and **provides assurance** from implementation till decommissioning that the system achieves an acceptable (or at least a tolerable) risk and consequently satisfies its Safety Objectives and that the system elements meet their Safety Requirements and their Assurance Level.

SSA monitors the safety performances of the system during its operational lifetime.



SSA-SAEC

IMPLEMENTATION PHASE

VERIFICATION THAT SYSTEM ELEMENTS MEET THEIR SRs AND SYSTEM IS ABLE TO MEET ITS SOs

SAFETY REQUIREMENTS (SR)

TRANSFER TO OPERATIONS

• VERIFICATION (as above)
•VALIDATION OF THE SYSTEM SOs IN OPERATIONAL ENVIRONMENT
•RISK IS ACCEPTABLE

SAFETY OBJECTIVES (SO)

OPERATIONS, MAINTENANCE DECOMMISSIONING

DATA COLLECTION AND MONITORING OF SAFETY PERFORMANCES (SR, SO, risk) ONGOING SAFETY ANALYSIS

RISK IS ACCEPTABLE

Figure 1 Role of the SSA

2. WHEN AND HOW SSA IS APPLIED

SSA is conducted during the ***System Implementation & Integration, Transfer into operation, Operation, Maintenance and Decommissioning*** phases of the system life cycle.

The essential pre-requisites for conducting a SSA are:

- a description of the high level functions of the system, with their associated Safety Objectives and a list of hazards and assumptions. All these come out of the FHA (Functional Hazard Assessment);

- A description of the system architecture with the Safety Requirements allocated to system elements. All these come out of the PSSA (Preliminary System Safety Assessment).

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

SSA is an iterative process, which should be reviewed, revised and refined as the process of collecting safety assurance & evidences evolves. It provides guidance on how to identify the extent of the re-analysis required. It may even show that meeting Safety Objectives as specified by FHA and/or meeting Safety Requirements as specified by PSSA could not be achieved and consequently lead to a re-iteration of the FHA and /or PSSA.

3. STRUCTURE OF THE SSA DESCRIPTION

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

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

SSA Initiation (Chapter 1);

SAEC-Safety Assurance & Evidence Collection (Chapter 3);

SSA Completion (Chapter 5).

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

SSA Planning step (Chapter 2);

SSA Evaluation step (Chapter 4).

Table 1 summarises the major activities conducted in each step of the SSA, 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 annexe each chapter for which it provides guidance and amplifies and explains the methodology, this is printed on colorA paper;
- **Annexes**, which provide background material and examples and are printed on colorB paper.

5. READERSHIP TABLE

The following table suggests a minimum attention to SSA Material:

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

6.1 Why?

Not only is it important that the SSA process is carried out correctly and completely, it is also important that SSA 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 repeat 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.

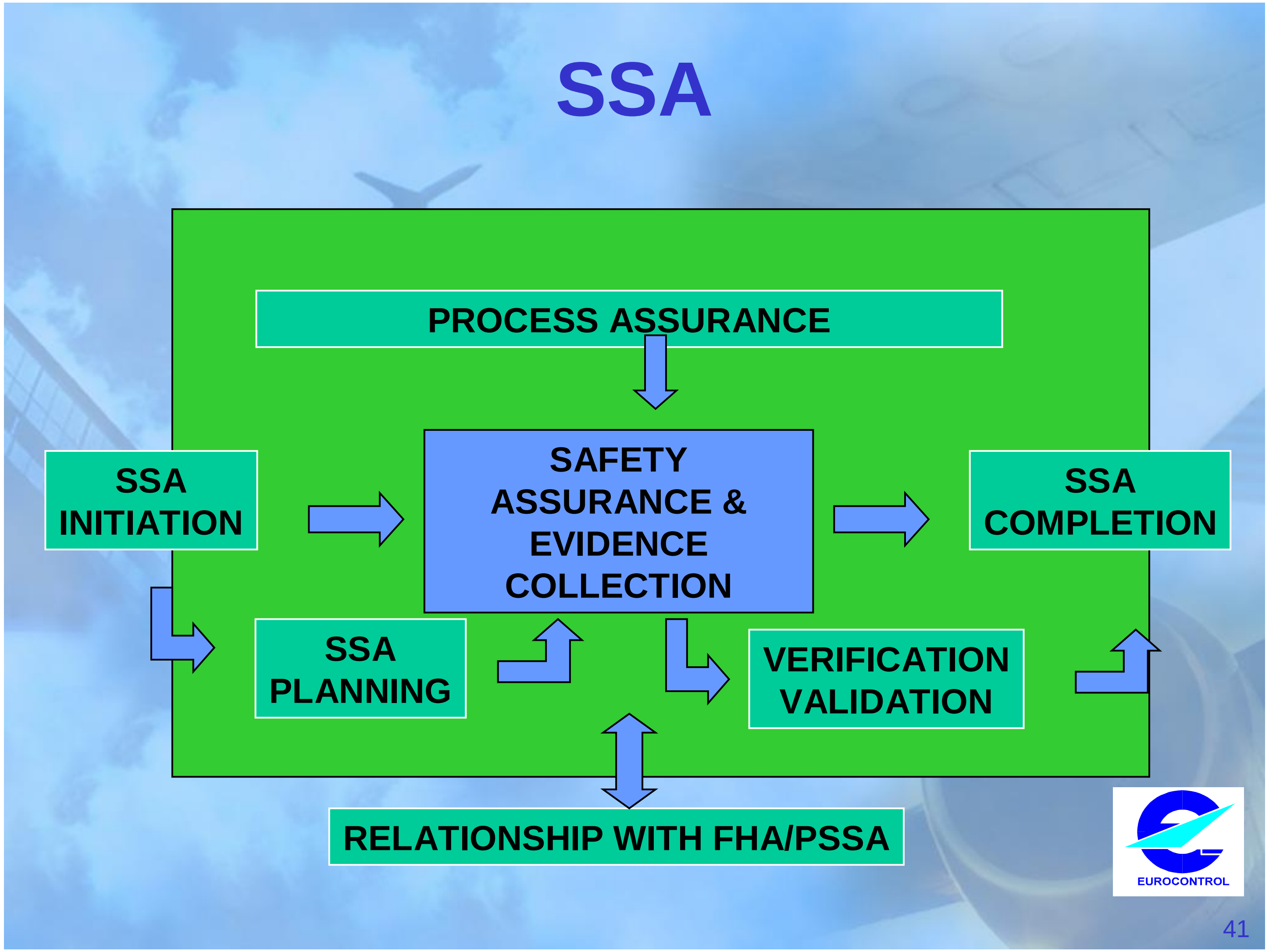


Figure 2: SSA Process

SSA STEP	OBJECTIVES	INPUT	MAJOR TASKS	OUTPUT

1
SSA 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 & Design;
		Operational Environment Description;
		Regulatory Framework;
		Applicable Standards;
		FHA & PSSA output;
		Other Inputs (e.g., other SSA results, hazard databases, incident investigation reports, lessons learned, …).
			Gather all necessary information describing the system implementation, transfer into operation, operation, maintenance and decommissioning;
			Review this information to establish that it is sufficient to carry out the SSA;
			Update the operational environment description (OED) of the system (add SSA-related OED data to FHA & PSSA-related data);
			Identify and record assumptions made;
			Formally place all input information under a documentation control scheme.
				Input information describing the system implementation;
				Updated information (e.g., description of the operational environment, list of assumptions).

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

3
Safety Assurance & Evidence Collection
	To collect evidences and to provide assurance that:
	• each system (people, procedure, equipment) element as implemented meets its Safety Requirements;
	• the system as implemented satisfies its Safety Objectives throughout its operational lifetime (till decommissioning);
	• the system satisfies users expectations with respect to safety;
	• The risk is acceptable.
		Information gathered or derived in the SSA Initiation step;
		Assumptions;
		Functions and hazards list (FHA output);
		Safety Objectives (FHA output);
		System Architecture (PSSA output);
		Safety Requirements (PSSA output).
			• SSA during Implementation & Integration (including Training):
			  • Re-assess FHA & PSSA output (process and assumptions);
			  • Verification that system elements (People, Procedures, Equipment) as implemented meet their SRs;
			  • Verification that system as implemented can meet its Safety Objectives;
			  • Verification that risk is acceptable.
			• SSA during Transfer into Operations:
			  • Safety assessment of the transfer into operations phase;
			  • Verification that system elements meet their SRs and that system as transferred into operations meets its Safety Objectives;
			  • Validation of the system as transferred to operations with respect to users' Safety expectations;
			  • Validation that risk is acceptable.
			• SSA during Operations & Maintenance:
			  • Continuous data collection and monitoring of safety performances with respect to SRs, SOs, assumptions and risk;
			  • Safety assessment of maintenance and/or planned interventions.
			• SSA during Decommissioning:
			  • Assessment of the safety impact on global ANS operations of the system withdrawing;
			  • Safety assessment of the decommissioning process.
				Safety Assurance & Evidence that:
				- Assumptions are true;
				- Safety Requirements (and Assurance Level) are met;
				- Safety Objectives are satisfied;
				- Risk is acceptable.
				Safety Indicators to be monitored;
				Data collection (ATM occurrences report, lessons learned, safety surveys);
				Change impact assessment results;
				Safety assessment data of:
				- Transfer into operation;
				- Maintenance interventions;
				- Decommissioning.

4 **SSA Evaluation**				
SSA Verification	To demonstrate that the process followed in collecting the Safety Assurance & Evidence is technically correct.	Information gathered or derived in the SSA steps; Safety Plan and SSA Plan; Outputs (including the final one) of the SSA process.	Review and analyse the results of the SSA process.	SSA Verification results.
SSA Validation	To ensure that the Safety Assurance & Evidence are (and remain) correct and complete; To ensure that all critical assumptions are credible, appropriately justified and documented.	Information gathered or derived in the SSA steps; Safety Plan and SSA Plan; Outputs (including the final one) of the SSA process.	Review and analyse Safety Assurance & Evidence 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 SOs/SRs/assumptions/risk and Safety Assurance & Evidence; Review and analyse the credibility and sensitivity of Safety Assurance & Evidence wrt to SOs/SRs/assumptions/risk.	SSA Validation results.
SSA Process Assurance	To provide evidence that all SSA activities (including Safety Verification and Safety Validation) have been conducted according to the plan; To ensure that the results – and the assumptions on which they depend - are properly recorded and disseminated for use by those involved in later stages of the development/assessment cycle, and to future system users.	Information gathered or derived in the SSA steps; Safety Plan and SSA Plan; Outputs (including the final one) of the SSA process.	The SSA Process assurance tasks should at least ensure in accordance with the SSA Plan that: • The SSA steps are applied; • Assessment approaches (e.g. success approach, failure approach, use of safety methods and techniques) are applied; • All outputs of the SSA steps are formally placed under a configuration management scheme; • Outcomes of SSA Validation and Verification activities are formally placed under configuration management; • Any deficiencies detected during SSA Verification or Validation activities have been resolved; • The SSA process would be repeatable by personnel other than the original analyst(s); • The findings have been disseminated; • Outputs of the SSA process are not incorrect and/or incomplete due to deficiencies in the SSA process itself.	SSA Process Assurance results.
5 **SSA Completion**	To record the results of the whole SSA process; To disseminate these results to all interested parties.	Outputs from all other SSA steps.	Document the results of the SSA process (including the results of SSA Validation, Verification and Process Assurance activities); Formally place the SSA results under a configuration management scheme; Disseminate the SSA result to all interested parties.	SSA results formally placed under a configuration management scheme.

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