Republika e Kosovës
Republika Kosovo - Republic of Kosovo

Autoriteti i Aviacionit Civil i Kosovës
Autoritet Civilnog Vazduhoplovstva Kosova
Civil Aviation Authority of Kosovo

Technical Publication – TP 15

SAM – System Safety Assessment

EUROCONTROL's Guidance Material for the application of SAM-SSA

Foreword

The purpose of this guidance material is to support the implementation of System Safety Assessment (SSA), one of the three phases of EUROCONTROL's Safety Assessment Methodology (SAM), which is one of the Acceptable Means of Compliance for the regulatory requirements on risk assessment and mitigation.

This document, taken from EUROCONTROL, covers the 5 steps of SSA, with all the corresponding guidance material made available by EUROCONTROL. This guidance material is part of a group of documents which aim at supporting the Air Navigation Service Providers (ANSPs) in fully and effectively applying the SAM Methodology when conducting risk assessments and mitigation with respect to changes to ATM systems. This group of documents consists of four Guidance Materials concerning SAM: an introductory material which explains the fundamental concepts of SAM, namely CAAK TP-12 and three supplementary guidance materials which address the three phases of SAM (FHA, PSSA and SSA), CAAK TP-13, TP-14 and TP-15 respectively.

CAAK considers that making this material available to the ANSPs in the Republic of Kosovo will contribute to the safety of air traffic in the Republic of Kosovo, by ensuring that ANSPs have the all the necessary support and guidance in properly addressing safety-related changes to ATM systems.

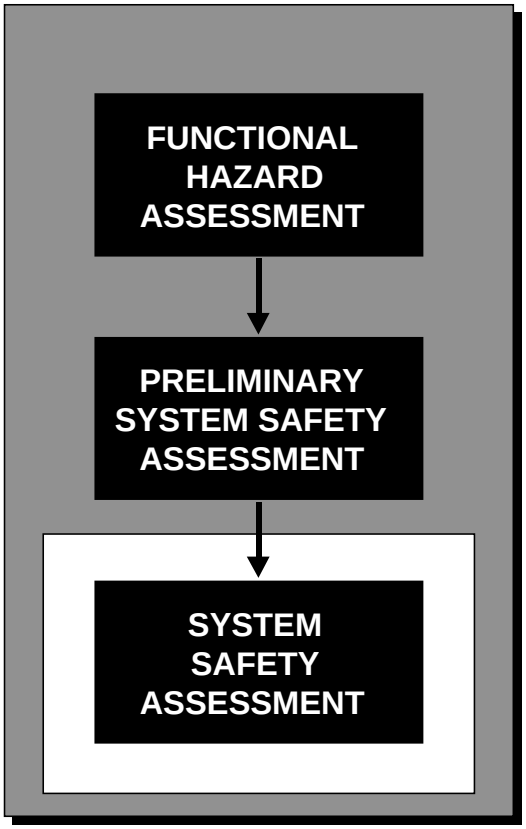
This Guidance Material should be applied taking into consideration the complementary Guidance Materials available for SAM, as well as ANSPs' own Safety Management Manuals. Furthermore, the content of this Guidance Material broadly addresses subject matter related to risk assessment and mitigation, therefore ANSPs should apply caution when using this material, since it is their responsibility to determine the exact requirements deriving from the Common Requirements and not simply refer to the guidance offered in this publication. ANSPs must also ensure that when used, this Guidance Material must be suitably adapted to the particular change.

Dritan Gjonbalaj
Director General
Civil Aviation Authority

Safety Assessment Methodology

PART III

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.

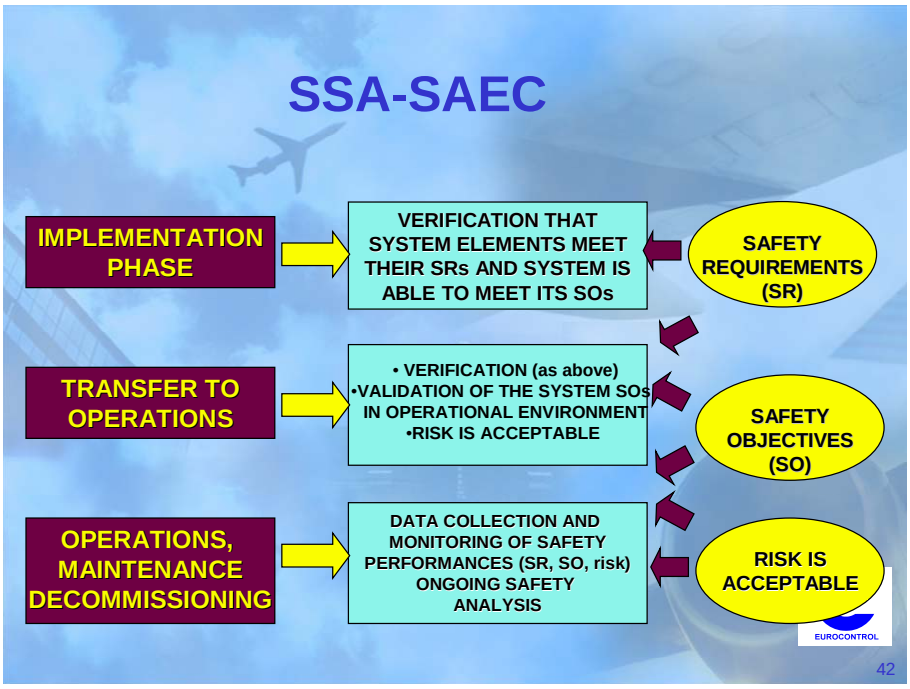


Figure 1 Role of the SSA

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.

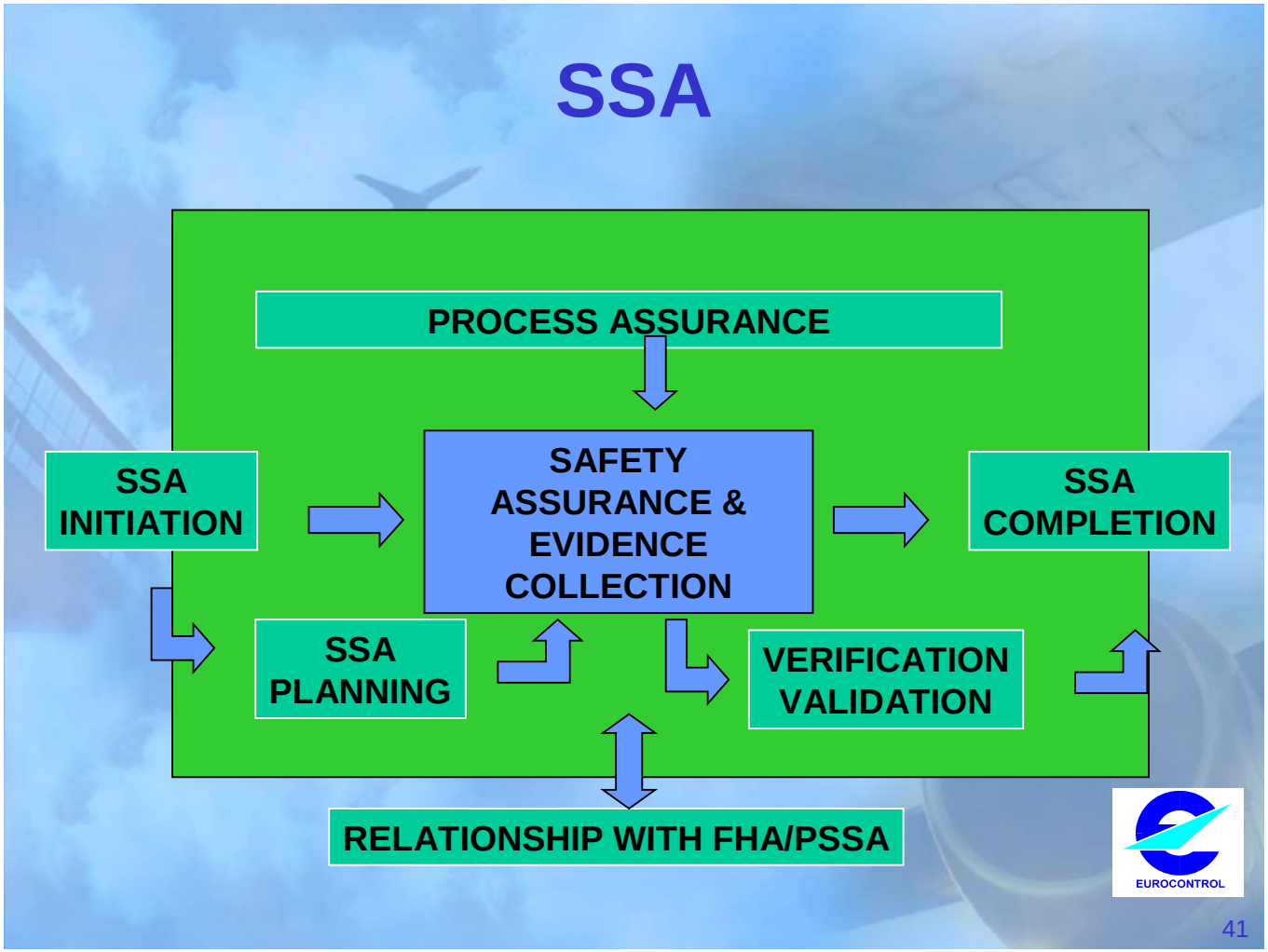


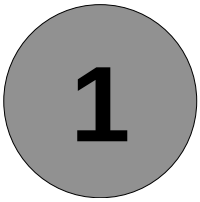
Figure 2: SSA Process

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



SSA INITIATION

1 OBJECTIVES

The objectives of the ***SSA Initiation*** step are:

- To develop a level of understanding of the system development, implementation, operation, maintenance and decommissioning and its rationale;
- To update the description of the operational environment;
- To identify, when appropriate, regulatory requirements and/or standards applicable to the system implementation, integration, transfer into operation, operation, maintenance and decommissioning.

2 INPUT

2.1 System Definition and Design

- Description of system architectures and their rationale (justification material, supporting analyses);
- List of assumptions (FHA and PSSA output);
- Safety Objectives and Safety Requirements (FHA and PSSA output);
- Design constraints (including risk mitigation strategies);
- System elements requirements and/or specification;

- Physical interfaces.

2.2 Operational Environment Description (OED)

The OED is a common part used for the FHA, PSSA and SSA processes. The OED needs to be refined before starting the SSA.

The AIP (Aeronautical Information Publication) and AIC (Aeronautical Information Circular) should be referenced.

See Guidance Material A of Chapter 1.

2.3 Regulatory Requirements

International and national safety regulatory objectives and requirements related to the system: (ICAO, EUROCONTROL, …).

2.4 Applicable Standards

Standards applicable to the system (e.g., EUROCONTROL Standards, standards internal to the organisations involved with the system).

As system means people, procedure and equipment, these standards can provide guidance on how to develop, integrate, transfer into operation, operate, maintain and decommission Software, Hardware, Procedures, Human factors, Human Machine Interface (HMI).

2.5 Others

- Organisation Risk Classification Scheme;
- FHA Report (not restricted to the list of Safety Objectives and assumptions);
- PSSA Report (not restricted to the list of Safety Requirements and the updated list of assumptions);
- Data coming from hazard databases, incident investigation reports, lessons learned, … providing feedback on the SSA process (the process itself as well as the assurance level allocation process, quantification issues, …) and previous applications of it (system element failures, contribution to hazard).

3 MAJOR TASKS

- Gather all necessary information describing the system implementation, transfer into operation, operation, maintenance and decommissioning, as outlined in Section 2 above;
- Review this information to establish that it is sufficient to carry out the SSA;

- Update the operational environment description of the system to add any system implementation, integration, transfer into operation, operation, maintenance and decommissioning related data;

- Identify and record assumptions made. Areas in which assumptions are commonly necessary relate to the operational scenarios, the system functions, architecture, implementation, transfer into operation, operation, maintenance, decommissioning and the system environment;

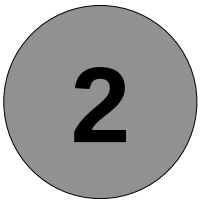
- Formally place all information under a documentation control scheme.

4 OUTPUT

- Input information describing the system implementation, as outlined in Section 2 above;

- Updated information (e.g., updated description of the operational environment, updated list of assumptions).

This page is intentionally left blank.



SSA PLANNING

1 OBJECTIVE

The objective of the ***SSA Planning*** step is to define the objectives and scope of the SSA, the activities to be carried out, their deliverables, their schedule and the required resources.

2 INPUT

- Overall Project/Programme plan(s);
- Project/programme Safety Plan;
- FHA and PSSA Reports.

3 MAJOR TASKS

- 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 SSA plan under a documentation control scheme;
- Disseminate SSA plan to all interested parties.

The SSA Plan should:

- Define and describe the safety aspects of development strategies to be used;
- Identify methods and techniques to be used in the SSA part of the safety assessment;
- Identify interdependencies with the development, implementation, transfer into operation, operation, maintenance and decommissioning phases;
- Define the schedule, transition criteria between SSA steps, resources, responsibilities and deliverables.

The SSA Plan should justify how the planned SSA activities will be conducted in the light of:

- The phases of the lifecycle (Implementation & integration, transfer into operation, operation, maintenance and decommissioning);
- The transition criteria to proceed to the next lifecycle phase including the criteria and steps to obtain approval for operation with regard to acceptability or tolerability of risk;
- The **safety impact** of the system: approaches appropriate to the level of risk, stringency of Safety Objectives, Safety Requirements and Assurance Levels;
- The degree of **complexity** of the system or its introduction into operation (e.g. number of stakeholders, number of ACCs,…);
- The **novelty** of the system: usage of new technology or of conventional technology not previously used for similar systems;
- Any other specific features of the system that could impact safety.

See Guidance Material A of Chapter 2.

4 OUTPUT

- Reviewed and approved SSA Plan.

SAFETY ASSURANCE & EVIDENCE COLLECTION

1 OBJECTIVE

The objective of the ***Safety Assurance & Evidence Collection*** step is 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);
- any **assumptions** made during the safety assessment process is correct;
- the system satisfies **users expectations** with respect to safety;
- the system achieves an acceptable **risk**.

2 INPUT

- Description of the system architecture and its rationale;
- The updated list of assumptions (on which Safety Objectives and Safety Requirements might be funded);
- The Operational Environment Description (OED);

- The list of hazards, with the rationale for their effects severity classification (FHA output);
- The Safety Objectives (FHA output);
- System element (People, Procedures, Equipment) Safety Requirements allocated by PSSA;
- Procedures and Equipment Assurance Levels allocated by PSSA;

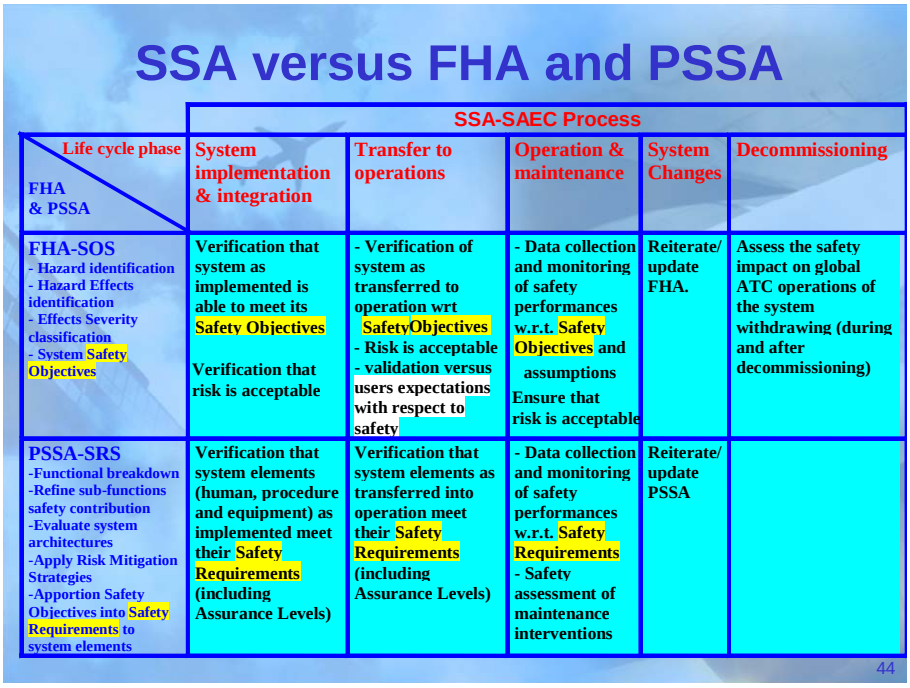
  PAL: Procedure Assurance Level;

  SWAL: SoftWare Assurance Level;

  HWAL: HardWare Assurance Level.

  Note: PAL, HWAL and SWAL are further explained in Guidance Material A of PSSA – Chapter 3.
- Safety evidence demands as specified by FHA and PSSA: safety-related specifications for verification activities (for example: tests, real-time simulations, specific analysis and studies, ..) and for validation activities (for example: trials, transition analysis, ..);
- FHA and PSSA analyses results (For example: FMEA, FTA, CCA, …).

3 MAJOR TASKS



An overview of Safety Assurance & Evidences Collection is provided hereafter for each of the lifecycle phases concerned:

- **SSA during Implementation & Integration (including Training)**
  - Re-assess FHA and PSSA output (process and assumptions) using the knowledge of the system acquired during its Implementation & Integration;
  - Verification that system elements (People, Procedures, Equipment) as implemented meet their Safety Requirements;
  - Verification that the 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 the system as transferred into operations meets its Safety Objectives, that system elements meet their Safety Requirements and that assumptions are correct;
  - Validation of the system as transferred into operations with respect to users' Safety expectations; (These users' Expectation with regards to safety are defined in the System Definition phase and collected during FHA.);
  - Validation that risk is acceptable.
- **SSA during Operations & Maintenance,**
  - Continuous data collection and monitoring of safety performances with respect to Safety Requirements, Safety Objectives, assumptions and risk acceptability;
  - Safety assessment of maintenance and/or planned interventions.
- **SSA during System Changes (People, Procedures, Equipment)**
  - Any change to the system and its elements (People, Procedures, Equipment) leads to the re-iteration of the overall Safety Assessment process, through: FHA, PSSA and SSA (thus no specific paragraph is dedicated to this item).
- **SSA during Decommissioning**
  - Assessment of the safety impact on ANS operations due to decommissioning (withdrawing) the system;
  - Safety assessment of the decommissioning phase.

If any of these tasks are not successfully achieved (so Safety Objectives and/or Safety Requirements are not met), then it leads to re-iterate FHA and /or PSSA in order to define new Safety Objectives and/or Safety requirements that can be met and finally achieve an acceptable risk.

This does not mean that during the re-iteration of the FHA and/or PSSA, less demanding Safety Objectives and/or Safety Requirements will be identified. It means that a new functional definition or new external mitigation means or a new architecture will have to be specified to set Safety Objectives and Safety Requirements that can be met while still achieving an overall acceptable risk.

All these tasks are further described in Guidance Material B of this Chapter 3. In addition, Guidance Material B also recommends activities, methods, techniques and means to actually conduct and achieve each of the tasks (as some techniques may apply to certain task(s)/phase(s) of the lifecycle but not to others).

3.1 SSA during Implementation & Integration

3.1.1 Re-assess FHA and PSSA output

This step of the process is recommended as:

- The domain maturity of the FHA and PSSA processes application is still to be increased;
- The major difficulty of a safety assessment lies in its completeness.

Using the deeper knowledge of the system and its operational environment acquired during its implementation and integration:

1. Re-assess the hazard analysis (hazard identification) output throughout the implementation and integration phase (check if there are some new or modified hazards);

2. Review the Safety Objectives allocation process by checking if quantitative frequencies and probabilities are still correct;

3. Check validity of assumptions on which Safety Objectives were funded along the FHA process.

   Then depending on results, Safety Objectives can be impacted. This can lead to redefine the system (and so redo a FHA of the new system).

4. Review the Safety Requirements apportionment process by checking the correctness of choices made during PSSA as well as the correctness of frequencies and probabilities.

5. Check validity of assumptions on which system element Safety Requirements were funded along the FHA and PSSA phases.

   Then depending on results, Safety Objectives and Safety Requirements can be impacted. This can lead to redesign the system (and so redo a PSSA of the new design or the change to the existing system) or even redefine the

system (and so redo a FHA of the new system or the change to the existing system).

3.1.2 Verification that system elements (People, Procedures, Equipment) as implemented meet their Safety Requirements

A. People and Procedure Elements:

1. Collect Human and Procedures element Safety Requirements derived during FHA and PSSA phases;

2. Complete them with additional Safety Requirements derived during Implementation & Integration;

3. Input all of these Safety Requirements to the:
   - training definition, organisation and validation process (for example: training courses and manual, training simulator);
   - licensing;
   - staff selection & management;
   - ATM operational & maintenance procedures development and validation processes.

4. Ensure that needs, means and planning for Human and Procedures element Safety Requirements verification and, as far as feasible, safety validation:
   - are captured by activities such as Simulations and pre-operational Trials;
   - or are expressed in terms of specific analysis to be performed (for example: Operating procedure analysis, Maintenance procedure analysis);
   - collect conclusions of those activities and analyses with respect to at least HMI interface design improvement, procedures design and training;
   - add, if necessary, new safety related requirements to cope with safety problems highlighted by those activities and analyses.

B. People Element:

1. See People and Procedure Elements;

2. Verify that Safety Requirements for Human element are met (for example by the Training, Licensing processes and Staff selection & management, by ensuring that training courses, manuals and simulators address specific training issues according to the Safety Requirements).

C. Procedure Element:

1. See People and Procedure Elements;

2. Verify that each ATM Procedure satisfies its PAL (Procedure Assurance Level);

3. Verify that each Maintenance Procedure satisfies its Safety Requirements (for example as defined in the Maintenance Manual and Training Programme).

D. Equipment Element:

1. Verify satisfaction of Quantitative Safety Requirements[1] for Hardware element(s);

2. Verify that each Hardware satisfies its HWAL (HardWare Assurance Level);

3. Verify satisfaction of Safety Requirements for Software element(s). The level of satisfaction of Safety Requirements for a SW element is specified by its SWAL;

4. Verify that each Software satisfies its SWAL (SoftWare Assurance Level).

3.1.3 Verification that system as implemented can meet its Safety Objectives

1. Verify if **Quantitative Safety Objectives** can be satisfied;

2. Verify if **Qualitative Safety Objectives** can be satisfied.

Note: During implementation & integration phase of the lifecycle, at least it can be verified that Safety Objectives are not unsatisfied. At this phase of the lifecycle, it can be difficult to verify that Safety Objectives are satisfied as Safety Objectives are associated to an appropriate operational environment and as limited evidence/feedback can be made available/collected in that appropriate operational environment.

3.1.4 Verification that risk is acceptable

1. As demonstration that Safety Requirements, Safety Objectives and assumptions can not always be fully made during this phase, risk acceptability should be verified using system knowledge and data available at that stage of the lifecycle (sensitivity analysis to certain remaining SRs or SOs not yet fully satisfied can be made).

3.2 SSA during Transfer into Operation

3.2.1 Safety assessment of the transfer into operations phase.

1. Conduct specific safety assessment of the transfer into operation phase (site installation, shadow operation, switch to operations processes ….); verify that transfer phase' Safety Requirements for the installation of different equipment, or change of procedure are met and ensure that risks induced by transfer phase on on-going ANS operations are acceptable;

[1] **Quantitative** Safety Requirements might be deterministic or probabilistic.
- **Deterministic**: time to switch-over, maximum acceptable time of service interruption, maximum acceptable time for a maintenance intervention, etc;
- **Probabilistic**: safety (free from accidents), reliability (mission success or continuity of proper service), availability (readiness for use), integrity (correctness of data), maintainability (ability to be maintained).

Note that quantitative Safety Objectives result, through allocation process, into Safety Requirements addressing reliability, availability, integrity, maintainability, dependability,...

2. Define safety performance indicators and monitor performance of the transfer into operation phase (These indicators are two fold: indicators derived from the safety assessment of the transfer into operation phase itself as well as indicators that will still be valid during operation).

3.2.2 Verification[2] that system elements meet their Safety Requirements, that system as transferred into operations meets its Safety Objectives and that assumptions are correct

1. Collect evidence that Safety Requirements, Safety Objectives and all assumptions are met in the actual operational environment (at least the one of the transfer into operation phase that, sometimes, could slightly differ from the final one and that could differ from the one initially provided to the Safety Assessment process);

2. If new safety related problems are highlighted by verification, then identify and document constraints when interfacing other systems (related to system integrity or to robustness of those interfacing systems), propose operational or maintenance limitations, or ultimately Element or System changes which lead to reiterate FHA and/or PSSA.

3.2.3 Validation of the system as transferred into operations with respect to users' Safety expectations.

1. Collect evidence resulting from validation activities (system evaluation with respect to Safety, as performed by its end users – for ex: Operational trials, Transition analysis, Operational Readiness Review);

2. If new safety related problems are highlighted by validation: propose operational or maintenance limitations or ultimately system changes (people, procedures and equipment) which could lead to reiterate FHA and/or PSSA.

3.2.4 Validation that risk is acceptable.

1. Assess actual risk by updating the initial (predictive) safety assessment performed before operation, with data fed-back during the Transfer into operation phase, in order to ensure risk acceptability with respect to Safety Requirements, Safety Objectives and assumptions on the operational environment and its external mitigation means and any assumptions made during the safety assessment process.

3.3 SSA during Operation & Maintenance

3.3.1 Continuous data collection and monitoring of safety performances

1. Perform continuous safety monitoring to ensure that Safety Requirements are met, Safety Objectives are satisfied and assumptions (on the operational environment and its external mitigation means and any assumptions made during the safety assessment process) are correct while the system is in

[2] Verification activities started during the Implementation & Integration will go on as assurance that system and its elements meet the associated Safety Objectives and Requirements can't be fully obtained during Implementation & Integration. Some essential evidence can be provided only in a context close to the operational one available during the Transfer into operation phase (for some Safety Requirements, satisfaction can not be demonstrated in a simulated environment).

operation. Safety Monitoring also allows identifying any trends in the evolution of the safety performance or any common factors that might be at the origin of safety problems;

2. Perform continuous safety occurrence reporting and assessment consisting of: events detection and notification, factual information gathering and event reconstruction, event analysis, issue of recommendations, assessment of their effectiveness by monitoring over time the effect of their implementation, and reporting and exchange;

3. Assess risk by updating the initial (predictive) safety assessment performed before operation, with data fed-back by the Reporting and Assessment process, in order to continuously monitor risk acceptability;

4. Use "lessons learned", which represent an informal feedback of safety-related experience, complementary to the formalised Safety Occurrence Reporting & Assessment;

5. Conduct safety surveys.

3.3.2 Safety assessment of maintenance or planned interventions

Perform safety assessment of maintenance and/or planned intervention: prepare and conduct planned and/or maintenance interventions to ensure that risks induced by any maintenance and/or planned intervention are acceptable.

See Guidance Material C of this Chapter 3.

3.4 SSA during System Changes

Any major change to the system and its elements (People, Procedures, Equipment) leads to the re-iteration of the overall Safety Assessment process, through: FHA, PSSA and SSA (thus no specific guidance is dedicated to this item in the SSA).

3.5 SSA during Decommissioning

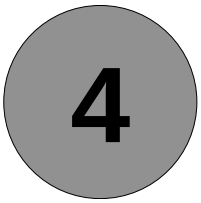
1. Assess safety impact on global ANS operations due to withdrawing the system from operations;

2. Perform safety assessment of the decommissioning process. That implies ensuring that risks induced on on-going ANS operations by the decommissioning operations (prepare and perform work to uninstall the system) are acceptable.

4 OUTPUT

- Updated list of assumptions;
- An updated list of identified hazards (new hazards may have been identified during the process and hazard scenarios may have been refined);
- The list of additional Safety Requirements defined during the Implementation & integration;
- The list of Safety Objectives and Safety requirements associated to the Transfer into Operation phase itself;
- The list of Safety Objectives and Safety requirements associated to the Decommissioning phase itself;
- Safety analyses results;
- Assurance & Evidence that assumptions are correct;
- Assurance & Evidence that Safety Requirements are met and Assurance Levels (HW, SW, ATM Procedure) are satisfied (including Safety Requirements specific to Transfer into Operation and Decommissioning);
- Assurance & Evidence that Safety Objectives are satisfied (including those specific to Transfer into Operation and Decommissioning);
- Assurance & Evidence that risk is acceptable (including those specific to Transfer into Operation and Decommissioning);
- The list of Safety Indicators to be monitored during transfer into operations, operation, maintenance and decommissioning;
- The list of remaining tolerable (but not acceptable) risks to be monitored and to be controlled during operations and the appropriate means to monitor and control them;
- The results and conclusions of the data collection (safety occurrence reporting and assessment, risk assessment based on occurrences reported, lessons learned, safety surveys) and safety monitoring activities, performed during system operation & maintenance;
- The results of the risk assessment and the appropriate justification demonstrating that safety impact of any major change to the system or its elements (People, Procedures, Equipment) is acceptable (concerns SSA if there is no impact, if any impact then re-iterate SAM);
- All the data of the safety assessment of:
    - The transfer into operation phase itself;
    - Maintenance and/or planned interventions;
    - Decommissioning phase itself.

This page is left blank intentionally.



SSA EVALUATION

1 OBJECTIVES

The objective of the SSA Evaluation stage is to demonstrate that the SSA process meets its overall objectives and requirements. This is carried out in three stages:

- Verification;
- Validation;
- Process Assurance.

The objective of ***SSA Verification*** is ("getting the output right") to ensure that the Safety Assurance & Evidence demonstrate that the Safety Requirements are met by a review and analysis of the results of the SSA.

The objective of ***SSA Validation*** is to ensure that the outputs of the SSA process are correct and complete ("getting the right output"), i.e. that:

- The Safety Assurance & Evidence are (and remain) correct and complete;
- All safety-related assumptions are (and remain) correct and complete.

The objectives of ***SSA Process Assurance*** are ("getting the process right and the right process"):

- To provide assurance and evidence that all SSA activities (including SSA Verification and SSA Validation tasks) have been conducted according to the SSA plan;

- To ensure that the SSA process as described in the SSA plan is correct and complete.

2 INPUT

- Information gathered or derived during the SSA steps;
- Safety Plan and SSA Plan;
- Outputs (including the final one) of the SSA process.

3 MAJOR TASKS

3.1 SSA Verification Task

The objective of ***SSA Verification*** is ("getting the output right") to ensure that the Safety Assurance & Evidence demonstrate that the Safety Requirements are met, Safety Objectives are satisfied, assumptions are correct and risk is acceptable by a review and analysis of the results of the SSA.

3.2 SSA Validation Task

The SSA validation tasks should include:

- Review and analyse the 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, its operational environment and its regulatory framework to ensure their completeness and correctness;
- Review and analyse traceability between Safety Assurance & Evidence and Safety Requirements, Safety Objectives, assumptions and risk;
- Review and analyse the credibility and sensitivity of Safety Assurance & Evidence with respect to Safety Requirements, Safety Objectives, assumptions and risk.

3.3 SSA Process Assurance Task

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.

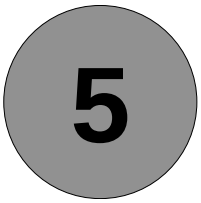
4 OUTPUT

The output of the SSA Evaluation is the assurance and evidence collected during the SSA Validation, SSA Verification and SSA Process Assurance tasks.

The SSA Evaluation output comprises:

- Results of the SSA Validation task: including the arguments for assurance and evidence of the completeness and correctness of Safety Assurance & Evidence and assumptions;
- Results of the SSA Verification task: including the information, collected during the various reviews of SSA output, for assurance and evidence that Safety Assurance & Evidence demonstrate that Safety Requirements are met;
- Results of the SSA Process Assurance task: including the information collected during the various activities for assurance and evidence that the SSA process as described in the SSA Plan has been conducted and that SSA process is correct and complete.

This page is intentionally left blank.



SSA COMPLETION

1 OBJECTIVE

The objectives of the ***SSA Completion*** step are:

- To record the results of the whole SSA process;
- To disseminate these results to all interested parties.

2 INPUTS

Outputs from all other SSA steps.

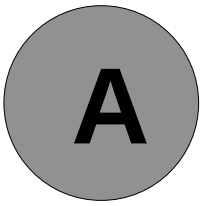
3 MAJOR TASKS

- Document the results of the SSA process (including Safety Assurance & Evidence, SSA Plan, including the results of SSA Validation, Verification and Process Assurance activities);
- Formally place the SSA results under a configuration management scheme;
- Disseminate the SSA documentation to all interested parties.

4 OUTPUT

- SSA results formally placed under a configuration management scheme.

Guidance material A of this Chapter 5 suggests possible format for documenting the SSA results.



CHAPTER 1
GUIDANCE MATERIAL:

OPERATIONAL ENVIRONMENT DEFINITION

1 INTRODUCTION

The purpose of this Guidance Material is to help further describing the Operational Environment so that SSA can be performed.

The OED was already made during FHA and PSSA. However during those two steps, the Operational Environment was specified to perform a certain way.

During SSA, the Operational Environment becomes a reality, so that FHA and PSSA descriptions of the Operational Environment could be impacted or confirmed.

Besides, some specific Operational Environments have to be specified:

- “Transfer into Operation” Operational Environment (that could differ from the Operational one;
-

1 OPERATIONAL ENVIRONMENT DEFINITION FOR SSA PURPOSE

System Safety Assessment can only be properly conducted when considering the Air Navigation System being assessed within the context of the Operational Environment in which it will be integrated.

The description of the Operational Environment should include all characteristics, which may be relevant when assessing the system and its ability to achieve an acceptable risk, to satisfy its Safety Objectives and meet its Safety Requirements.

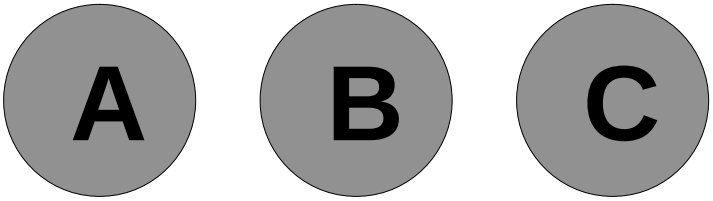
SSA aims at updating the description provided in FHA OED (see FHA Chapter 1 Guidance Material A) and PSSA OED (see PSSA Chapter 1 Guidance Material A) with actual, real and any additional data.

SSA Verification & Validation (SSA Chapter 4) includes verification and validation of the Operational Environment Definition.

2 OPERATIONAL ENVIRONMENT DEFINITION FOR TRANSFER INTO OPERATION PURPOSE

The nature and type information to describe the Operational Environment for the “Transfer into Operation” phase are the same as the one recommended in FHA-OED (see FHA Chapter 1 Guidance Material A) and in PSSA-OED (see PSSA Chapter 1 Guidance Material A).

This page is intentionally left blank.



CHAPTER 4
GUIDANCE MATERIAL

SSA Evaluation Activities

1 Introduction

This chapter gives practical guidance on verifying and validating a System Safety Assessment (SSA).

The guidance is meant to be used with the SAM and aims to avoid duplication. For the most part, the guidance gives references to specific parts of the SAM but there are occasional quotes to reduce the reader's time spent searching for information.

2 Objectives of the SSA

SSA is a process initiated at the beginning of the implementation of an Air Navigation System (ANS). 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 Functional Hazard Assessment (FHA) and the system elements meet their Safety Requirements specified in the Preliminary System Safety Assessment (PSSA).

The SSA process **collects evidences** and **provides assurance** from implementation to 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.

3 How to Apply the Evaluation Process

Verification and validation processes are satisfied through a combination of reviews and analysis of the SSA output. One distinction between reviews and analysis is that analysis provides repeatable evidence of correctness and reviews provide a qualitative assessment of correctness. A review may consist of an inspection of an output of a SAM process guided by a checklist or similar aid. An analysis may examine in detail the performance, results and traceability of the SAM process.

The person (or persons) carrying out verification and validation will report to the project manager. Their role will be to give the project manager an objective evaluation of the outputs of the SSA and the process followed.

The accomplishment of objective evaluation is more likely to be ensured when the verification and validation processes are carried out by a person (or persons) other than those who performed the SSA process. However, such independence should only be necessary for the most critical systems – as determined during the FHA. The involvement of people with different skills (ATCO's, Pilots & Engineers) in a SAM process (e.g. testing a system) will by itself ensure a degree of objectivity. Verification and validation may be carried out by the same person, something which the project manager will decide in accordance with the Safety Management System implemented within the organisation.

The verification and validation processes are split into five separate processes to match the life-cycle phases as there will be a significant time span between some of these phases, and different personnel will be involved. The processes are outlined in the following paragraphs covering:

- System Implementation and Integration;
- Transfer to Operations;
- Operations and Maintenance;
- System Change;
- Decommissioning.

Note that the verification and validation activities have to take place in phase with the development of the SSA

4 Scope of these Guidelines

The activities described are limited to the verification and validation of SSA outputs.

5 SSA Verification

5.1 Objective

The verification task reviews and analyses the results of the SSA ensuring that the information and output required from the SSA is available (e.g. "getting the output right"). The main focus of the task is the documented results of the Safety Assurance

and Evidence Collection (SAEC) carried out during the SSA. The SAEC activity itself involves a considerable amount of verification at each stage.

5.2 System implementation and integration verification process

The purpose of verification for this phase is to provide assurance that the system, as implemented, is able to achieve an acceptable level of risk, that is to meet its Safety Objectives and that the system elements (human, procedure and equipment) meet their Safety Requirements (including assurance levels).

The verification goals are summarised in the following figure. The numbers refer to the location of guidance (in this document) on each goal in the tables which follow.

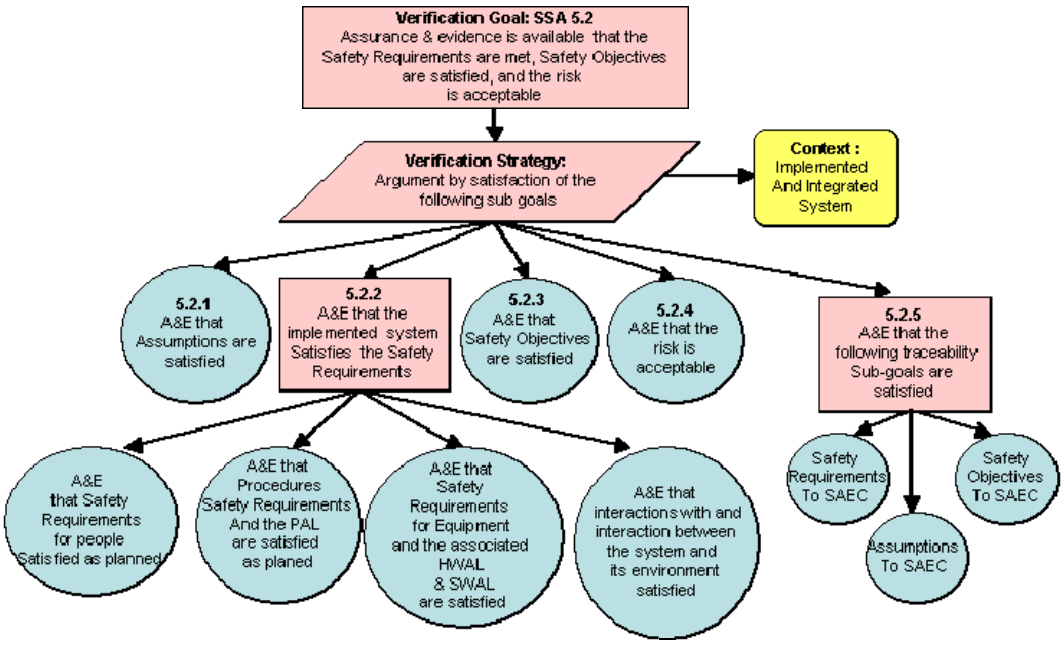


Figure 5.2 Verification goals

The reviewer will need the correct version of the following information for conducting the verification:

- 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. [Ref SSA Chapter 2]
- A description of the system architecture with the Safety Requirements allocated to system elements. All these come out of the PSSA. [Ref SSA Chapter 2]
- The results of the SAEC activity.
- SSA Chapter 3 Guidance Material A.

The reviewer should verify that the Assurance and Evidence for following verification items is clearly identified in the SSA results: [Ref SSA Chapter 3 §3.1]. A requirement is deemed to be 'satisfied' when there is evidence available to show that it has been met by the new system or the change to the existing system.

Goal	Verification Item	Available (yes/no)	Reference in SSA (document, page)
SSA 5.2.1	**Assumptions are satisfied** Is evidence available to show that assumptions are satisfied?		
SSA 5.2.2.1	**Safety Requirements for people are satisfied as planned.** Is evidence available to show that Safety Requirements (including HAL) allocated to Human are satisfied?		
SSA 5.2.2.2	**Safety Requirements for procedures are satisfied, and the associated PAL is satisfied as planned.** e.g. Is evidence available to show that the Safety Requirements allocated to procedures (including PAL) are satisfied?		
SSA 5.2.2.3	**Safety Requirements for equipment are satisfied and the associated HWAL and SWAL are satisfied as planned.** e.g. Is evidence available to show that the Safety Requirements allocated to hardware and software (including HWAL and SWAL) are satisfied?		
SSA 5.2.2.4	**The interactions within the system and interaction between the system and its environment are satisfied.** e.g. Is evidence available to show that changes to airspace design have been evaluated against the adjacent areas/sectors of operations? e.g. Is evidence to show that Safety Requirements about interactions with adjacent centres are satisfied?		
SSA 5.2.3	**Safety Objectives are satisfied as planned.** e.g. Is evidence available to show that the predicted/measured frequency of occurrence of hazards resulting from system failures meet the Safety Objectives?		
SSA 5.2.4	**The risk is acceptable.** e.g. Is evidence available to show that the risks have actually been assessed and a statement of acceptance (or otherwise) by the ANSP included?		

Table 5.2A System implementation & integration

Traceability:

The reviewer should verify that the following information is clearly traceable in the SSA:

Goal	Verification Item	Available (yes/no)	Reference in SSA (document, page)
SSA 5.2.5.1	**Safety Requirements to SAEC** e.g. Can the specific assurance activities and associated evidence indicating that the Safety Requirements are met, be clearly identified?		
SSA 5.2.5.2	**Safety Objectives to SAEC** e.g. Can the specific assurance activities and associated evidence indicating that the Safety Objectives are met, be clearly identified?		
SSA 5.2.5.3	**Assumptions to SAEC** e.g. Can the specific assurance activities and associated evidence indicating that the assumptions are met, be clearly identified?		

Table 5.2B System implementation & integration

5.3 Transfer to operations verification process

The purpose of verification for this phase is to provide assurance that the system continues to meet its Safety Objectives and Safety Requirements in operation.

Verification activities started during the implementation and integration will continue. This is to obtain assurance that the system and its elements meet the associated Safety Objectives and Safety Requirements – assurance that cannot be fully obtained during implementation and integration. Note that some essential evidence can be provided during the actual transfer into operation phase (for some Safety Requirements, satisfaction can not be demonstrated in a simulated environment). [Refer SSA Chapter 3, §3.3].

The reviewer should verify that the following information is clearly identified in the SSA results: [Ref SSA Chapter 3 § 3.2]. The following table refers to verification activities of the safety assessment of the transfer into operations phase itself.

Goal	Verification Item	Available (yes/no)	Reference in SSA (document, page)
SSA 5.3.1	**Assurance & Evidence available showing that transfer phase Safety Requirements for the installation of different equipment or change of procedure are met.**		
SSA 5.3.2	**Assurance & Evidence available showing that risks induced by transfer phase on on-going ANS operations are acceptable.** e.g. Has the operating authority been appraised of the risks and indicated acceptance?		

Goal	Verification Item	Available (yes/no)	Reference in SSA (document, page)
SSA 5.3.3	**Definition of safety performance indicators.** e.g. Has the operating authority been informed which system parameters need to be monitored for safety?		
SSA 5.3.4	**Monitoring of performance of the transfer into operation phase.** e.g. Have arrangements been made to ensure that the performance of the system is verified in the operational environment?		
SSA 5.3.5	**Constraints when interfacing other systems identified and documented.** e.g. Have arrangements been made to recover to the existing system should a problem occur with the new system during transfer to operations?		

Table 5.3A Transfer to operations

The following table refers to additional (complementary) verification of Table 5.2A to be gathered during the transfer into operations phase.

Goal	Verification Item	Available (yes/no)	Reference in SSA (document, page)
SSA 5.3.6	**Limitations proposed if new safety related problems are highlighted.** e.g. The operating range of a surveillance system may have to be curtailed if positional accuracy is affected by reflections.		
SSA 5.3.7	**Monitoring of performance of the transfer into operation phase.**		
SSA 5.3.8	**Safety Objectives are satisfied as planned.** Additional to 5.2.3		
SSA 5.3.9	**Safety Requirements for people are satisfied as planned.** Additional to 5.2.2.1.		
SSA 5.3.10	**Safety Requirements for procedures are satisfied, and PAL satisfied as planned** Additional to 5.2.2.2.		
SSA 5.3.11	**Safety Requirements for equipment are satisfied, and HWAL & SWAL satisfied as planned.** Additional to 5.2.2.3.		
SSA 5.3.12	**Assumptions satisfied.** Additional to 5.2.1.		
SSA 5.3.13	**The risk is acceptable.** Additional to 5.2.4.		

Table 5.3B Transfer to Operations

5.4 Operation and maintenance verification process

The reviewer will need the correct version of the following information for conducting the verification:

- SSA - results of safety assessment of operations and maintenance.
- SSA - Chapter 3 SAEC.

The reviewer should verify that Assurance & Evidence for the following verification items is clearly identified in the SSA results: [Ref SSA Chapter 3, § 3.3.]

Goal	Verification Item	Available (yes/no)	Reference in SSA (document, page)
SSA 5.4.1	**Continuous safety monitoring is performed to ensure that Safety Requirements are met, Safety Objectives are satisfied and assumptions are correct while the system is in operation.**		
SSA 5.4.2	**Continuous safety occurrence reporting and assessment is performed.**		
SSA 5.4.3	**The risk is continuously monitored for acceptability.**		
SSA 5.4.4	**Use is made of "lessons learned", to complement formal safety occurrence reporting & assessment.**		
SSA 5.4.5	**Safety surveys are conducted.**		
SSA 5.4.6	**Safety assessment of maintenance intervention is performed.**		

Table 5.4 Operation and Maintenance

5.5 System change verification process

Any change shall be assessed decide whether it deserves or not a safety assessment or only to revisit the existing safety assessment (See Part IV Guidance Material H)

As long as the to the system and its elements (people, procedures, equipment) change deserves a safety assessment, it leads to the re-iteration of the overall safety assessment process, through the FHA, PSSA and SSA (thus no specific guidance is dedicated to this item in the SSA verification).

5.6 Decommissioning verification process

The purpose of verification for this phase is to provide assurance that the risks associated with decommissioning the system are acceptable.

The reviewer will need the correct version of the following information for conducting the verification:

- SSA - results of safety assessment of the decommissioning process;
- SSA - Chapter 3 SAEC.

The reviewer should verify that Assurance & Evidence for the following verification items is clearly identified in the SSA results: [Ref SSA Chapter 3, § 3.5.]

Goal	Verification Item	Available (yes/no)	Reference in SSA (document, page)
SSA 5.6.1	**The safety impact on global ANS operations due to withdrawing the system from operations has been assessed.**		
SSA 5.6.2	**The safety assessment of the decommissioning process itself has been performed to ensure that that risks induced on on-going ANS operations by the decommissioning operations are acceptable**.		

Table 5.6 Decommissioning

6 SSA Validation

6.1 Objective

The validation task aims at reviewing and analysing the results of the SSA to confirm that the outputs of the SSA process are correct and complete ("getting the right output"), i.e. that:

- The safety Assurance & Evidence are (and remain) correct and complete;
- All safety-related assumptions are (and remain) correct and complete.

[Ref SSA Chapter 4 - SSA Evaluation]

Note: One major aspect of Validation consists in ensuring the credibility and sensitivity of Assurance & Evidence aiming at demonstrating a certain type of satisfaction.

Note: It is assumed that Safety Objectives completeness and correctness at the system definition phase is ensured in the FHA (Chapter 4).

Note: It is assumed that Safety Requirements completeness and correctness at the system design phase is ensured in the PSSA (Chapter 4)

6.2 System implementation & integration validation process

The purpose of validation for this phase is to provide assurance that the risk of operating the new system or the change to the existing system is acceptable.

The reviewer will need the correct version of the following information for conducting SSA validation:

- 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.
- A description of the system architecture with the Safety Requirements allocated to system elements. All these come out of the PSSA.
- Results of SSA verification.
- Results of Safety Assurance & Evidence Collection (SAEC).
- SSA Plan.
- SSA Generic Activities - Chapter 3 Guidance Material A.
- SSA Activities Along the Life-Cycle –Chapter 3 Guidance Material B.

The validation goals are summarised in Figure 6.2.

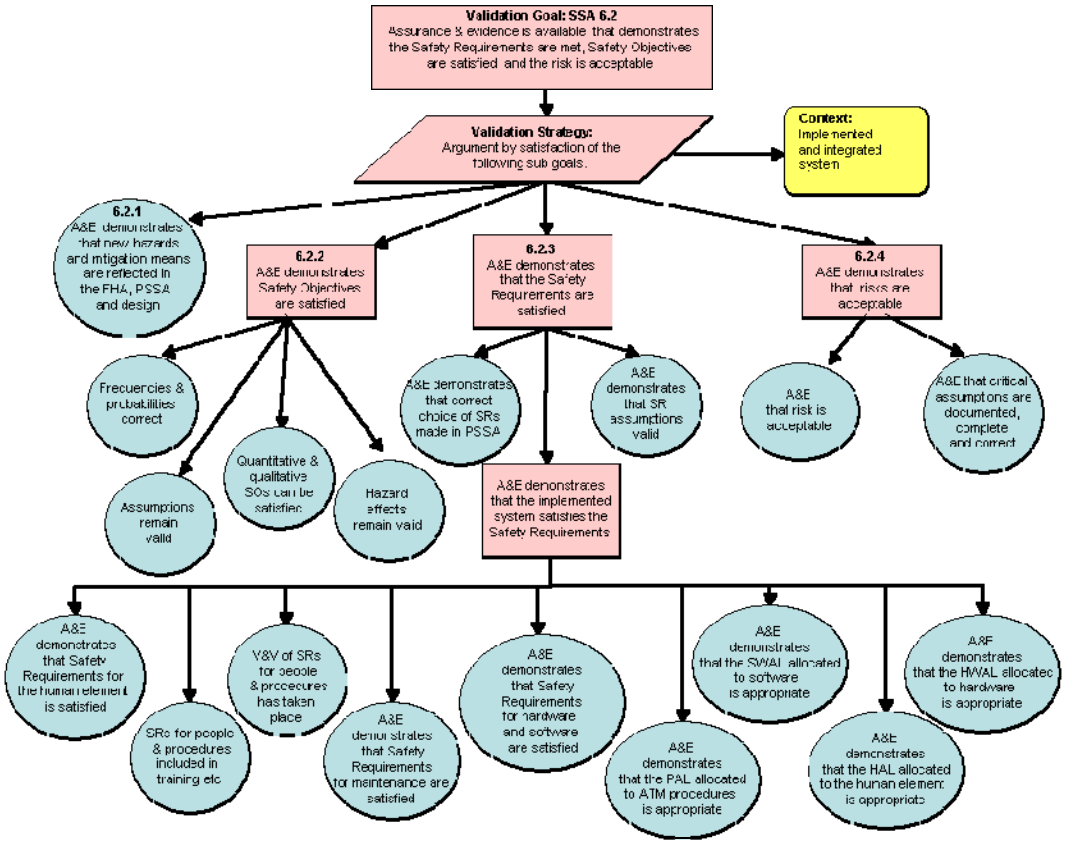


Figure 6.2: System implementation validation goals

6.2.1 New hazards and mitigation means.

The reviewer shall confirm that the assurance available demonstrates the following:

Goal	Validation Item:	Validation Result
SSA 6.2.1.1	**If any new hazards and mitigation means were identified during SSA then:** **(1) the necessary revision of the FHA and/or PSSA took place or is planned; and** **(2) the necessary reiteration of the design took place or is planned.** The primary concern is that all the potential hazards arising from the system implementation and integration are identified and that appropriate mitigation is applied. One specific source of new hazards can be the unintended implemented functions (functions being implemented but not required due to e.g. reuse of or configurable elements,. [Refer to SAM Part IV GM E "Recommendations for ANS SW" Objective 3.0.4]	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	

Table 6.2A System implementation

6.2.2 Safety Objectives are satisfied as planned.

The reviewer shall confirm that the assurance available demonstrates the following:

Goal	Validation Item:	Validation Result
SSA 6.2.2.1	**Assurance and Evidence are correct and complete to show that the quantitative frequencies and probabilities are still correct**. [Refer to SSA Chapter 3 Guidance Material B § 2.1] Reviewing analysis of the system low level design may reveal that the frequency of hazards occurring is higher than originally predicted.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in SSA**	
SSA 6.2.2.2	**The assumptions on which the Safety Objectives were founded remain valid, and if not that the necessary redefinition of the system took place, or is planned.** [Refer to SSA Chapter 3 Guidance Material B § 2.1]**.** Only documented assumptions are relevant – there should be no implicit assumptions.	Satisfactory ☐ Requires Action: ☐
	Comment / action: **Reference in SSA**	
SSA 6.2.2.3	**Assurance and Evidence are correct and complete* to show that the quantitative and qualitative Safety Objectives can be satisfied as required**. [Refer to SSA Chapter 3 Guidance Material B § 2.1.1] *: At this phase of the lifecycle, it can be difficult to confirm that Safety Objectives are satisfied as they relate to a particular operational environment and limited evidence/feedback may be available/collected about that operational environment. Some confidence can be gained in this regard by establishing that the assumptions made at the outset remain valid as planned.	Satisfactory ☐ Requires Action: ☐
	Comment / action: **Reference in SSA**	
SSA 6.2.2.2	**Assurance and Evidence are correct and complete to show that the specified probability that the hazard generates an effect (Pe) is satisfied.** Requirements set on the external mitigation means that contributed to set such Pe are satisfied. Depending on the approach chosen to set Safety Objectives either only the Pe of the Worst Credible effect has to be validated or the Pe of effect [See FHA Chapter Guidance Material G]	Satisfactory ☐ Requires Action: ☐
	Comment / action: **Reference in SSA**	

Table 6.2B System implementation

6.2.3 Safety Requirements are satisfied as planned.

The reviewer shall confirm that the assurance available demonstrates the following:

Goal	Validation Item:	Validation Result
SSA 6.2.3.1	**Assurance and Evidence are correct and complete to show that the correct choice of Safety Requirements was made during the PSSA including the correctness of the frequencies and the probabilities.** New Safety Requirements may be generated as a result of the better understanding of the system gained during the design phase.	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	
SSA 6.2.3.2	**The assumptions on which the Safety Requirements were founded remain valid, and if not that the necessary redesign of the system took place, or is planned.**	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	
SSA 6.2.3.3	People: **Assurance and Evidence are correct and complete to show that any Safety Requirements for the human element are satisfied as required.** [Refer to SSA Chapter 3 Guidance Material B § 2.1.2] Review of credibility and sensitivity of Assurance & Evidence showing that Human Safety Requirements are satisfied such as specific training, licensing, staff selection & management, and manuals. (including HAL[1] (Human Assurance Level) satisfaction means)	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	
SSA 6.2.3.4	ATM Procedures: **Assurance and Evidence are correct and complete to show that any the Safety Requirements for the people & procedures (including PAL) element are satisfied as required.** [Refer to SAM Part IV Annex G (SAAP) and SSA Chapter 3 Guidance Material B § 2.1.2] Review of credibility and sensitivity of Assurance & Evidence showing that ATM procedure Safety Requirements are satisfied such as procedure tasks analysis, deviation analysis, contingency plan, … Review of credibility and sensitivity of Assurance & Evidence showing that ATM procedure PAL (Procedure Assurance Level) is satisfied	Satisfactory ☐ Requires ☐ Action

[1] HAL (Human Assurance Level): At the time V2.1 of V&V Guidance Material was written, HAL definition was under development. Therefore, reference to SAM Guidance Material addressing HAL is not yet available.

Goal	Validation Item:	Validation Result
	Comment / action: **Reference in SSA**	
SSA 6.2.3.5	Maintenance Procedures: **Assurance and Evidence are correct and complete to show that any Safety Requirements relating to maintenance procedures are satisfied as required**. [Refer to SSA Chapter 3 – GM C & SSA Chapter 3 Guidance Material B § 2.1.3] Review of credibility and sensitivity of Assurance & Evidence showing that each maintenance procedure satisfies its safety requirements (for example as defined in the Maintenance Manual and Training Programme).	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	
SSA 6.2.3.6	Equipment**: Assurance and Evidence are correct and complete to show that any Safety Requirements relating to hardware (including HWAL) and software (including SWAL) are satisfied as required**. [Refer to SAM- Part IV Annex F & SSA Chapter 3 Guidance Material B § 2.1.4] Review of credibility and sensitivity of Assurance & Evidence showing that: The hardware satisfies its HWAL (Hardware Assurance Level); The software satisfies its SWAL (Software Assurance Level).	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	
SSA 6.2.3.7	**Assurance and Evidence are correct and complete to show that the PAL allocated to any ATM procedure is appropriate.** [Refer to SAM Part IV Annex G (SAAP) and PSSA Chapter 3 Guidance Material A] Review of the credibility and sensitivity of Assurance & Evidence sustaining the PAL allocation.	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	
SSA 6.2.3.8	**Assurance and Evidence are correct and complete to show that the SWAL allocated to any software is appropriate.** [Refer to SAM Part IV Annex F (Recommendations for ANS SW) and PSSA Chapter 3 Guidance Material A] Review of the credibility and sensitivity of Assurance & Evidence sustaining the SWAL allocation.	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	

Goal	Validation Item:	Validation Result
SSA 6.2.3.9	**Assurance and Evidence are correct and complete to show that the HWAL allocated to any hardware is appropriate.** Review of the credibility and sensitivity of Assurance & Evidence sustaining the HWAL allocation, if any.	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	
SSA 6.2.3.10	**Assurance and Evidence are correct and complete to show that the HAL allocated to any human element is appropriate.** [Refer to TBD] [2] At the time this V&V Guidance Material was written HAL was under development. Review of the credibility and sensitivity of Assurance & Evidence sustaining the HAL allocation.	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	

Table 6.2C System implementation

6.2.4 The risk is acceptable.

The reviewer shall confirm that the assurance available demonstrates the following:

Goal	Validation Item:	Validation Result
SSA 6.2.4.1	**Assurance and Evidence are correct and complete to show that the risk is acceptable.** Review of the credibility and sensitivity of Assurance & Evidence showing that risk is acceptable. The demonstration may have to rely on system knowledge and data available at that stage of the lifecycle [Refer to SSA Chapter 3 Guidance Material A § 2.3.1] Note: Demonstration that risk is acceptable can not always be fully made during this phase (sensitivity analysis to certain remaining SRs or SOs not yet fully satisfied can be made).	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in SSA**	
SSA 6.2.4.2	**Any critical assumptions about the system, its operational environment and its regulatory framework are justified, documented, complete and correct.** For example, if the system design required that data lines should have dual independent routing and the lines were supplied by a third party it would be insufficient just to assume that they complied with the requirement.	Satisfactory ☐ Requires Action: ☐
	Comment / action: **Reference in SSA**	

Table 6.2D System implementation

6.3 Transfer to operations validation process

The purpose of validation for this phase is to provide assurance that the transfer into operation risk is acceptable.

The reviewer will need the correct version of the following information for conducting the validation:

- SSA - verification results.
- SSA - Guidance Material along the life cycle.
- SSA - results of safety assessment of the transfer into operations.

The validation goals are summarised in Figure 6.3:

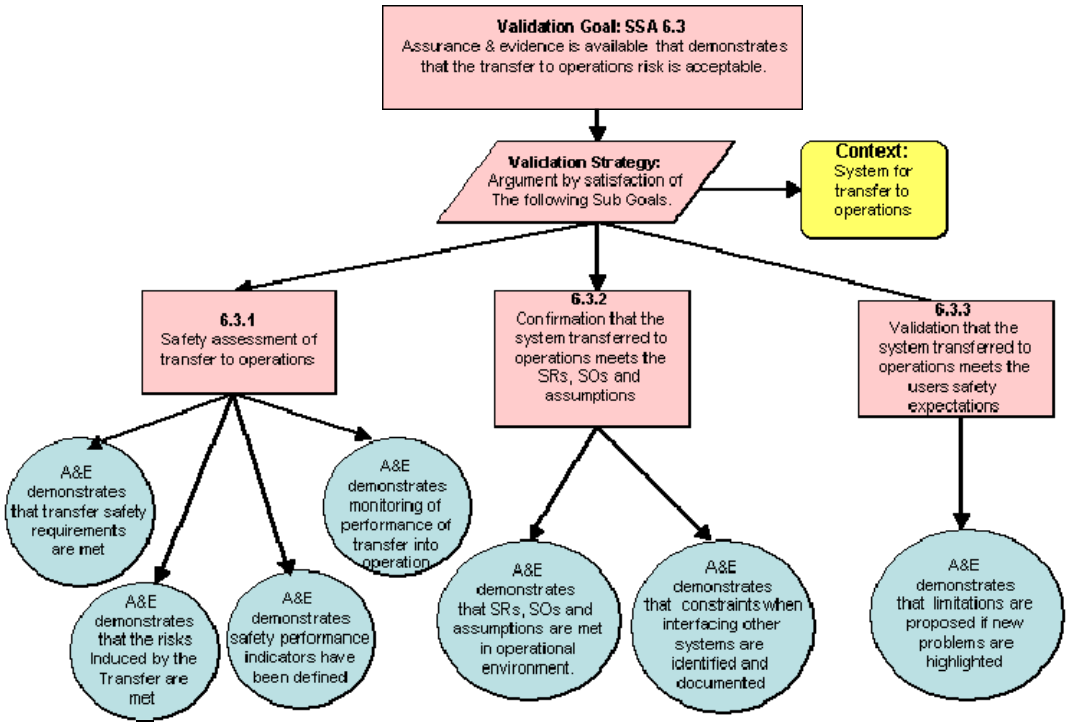


Figure 6.3 System transfer to operations validation goals

6.3.1 Safety assessment of transfer into operations.

The reviewer shall confirm that the assurance available demonstrates the following:

Goal	Validation Item:	Validation Result
SSA 6.3.1.1	**Assurance and Evidence are correct and complete to show that the transfer phase' Safety Requirements for the installation of different equipment or change of procedure are satisfied as required.** [Refer to Guidance Material B § 2.2.2] Review of the credibility and sensitivity of Assurance & Evidence showing that these Safety Requirements are met. It needs to be planned and managed by the ANSP, and there should be evidence to that affect.	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	
SSA 6.3.1.2	**Assurance and Evidence are correct and complete to show that the risks induced by transfer phase on on-going ANS operations are acceptable.** Review of the credibility and sensitivity of Assurance & Evidence showing that transfer into operation phase risk is acceptable. The ANSP should be fully aware of what the risks are. It needs to be planned and managed, and there should be evidence to that affect.	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	
SSA 6.3.1.3	**Safety performance indicators are credible, correct and have the appropriate coverage (representative system, traffic load and duration).** Safety performance indicators should be linked to Safety Objectives; safety is only meaningful in an operational context. Safety performance indicators should be usable in ongoing risk assessment.	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	
SSA 6.3.1.4	**Monitoring of performance of the transfer into operation phase.** The ANSP should be fully aware of what the performance requirements are. It needs to be planned and managed, and there should be evidence to that affect.	Satisfactory ☐ Requires ☐ Action
	Comment / action: **Reference in SSA**	

Table 6.3A Transfer to Operations phase itself

6.3.2 Confirmation that the system, as transferred into operation, meets the Safety Requirements, Safety Objectives and that the assumptions are correct.

The following table refers to additional (complementary) validation of Table 6.2B, C & D to be gathered during the transfer into operations phase.

The reviewer shall confirm that the assurance available demonstrates the following:

Goal	Validation Item:	Validation Result
SSA 6.3.2.1	**Assurance and Evidence are correct and complete to show that the Safety Requirements, Safety Objectives and all assumptions are met in the actual operational environment.** [Ref SSA Chapter 3 Guidance Material B § 2.2.2.] This is an ongoing process, requiring review of the system performance by the ANSP.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in SSA**	
SSA 6.3.2.2	**Constraints when interfacing other systems are identified and documented.** For example, if the facilities that the system depends on (Power Supply, Heating, Ventilation, etc) are managed by a third party under contract to the ANSP, then the principles and procedures by which the contractors operate the system need to be agreed and documented in order to minimise the risk of unscheduled impacts on the system.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in SSA**	

Table 6.3B Transfer to operations

6.3.3 Validation of the system as transferred into operations with respect to users' safety expectations.

The reviewer shall confirm that the assurance available demonstrates the following:

Goal	Validation Item:	Validation Result
SSA 6.3.3.1	**Limitations are proposed if new safety related problems are highlighted.** [Refer to SSA Chapter 3 Guidance Material B § 2.2.3.] For example, the operating range of a surveillance system may have to be curtailed if positional accuracy is affected by reflections in one sector of operations.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in SSA**	

Table 6.3C Transfer to operations

6.4 Operation & maintenance validation process

The purpose of validation for this phase is to provide assurance that the risk continues to be acceptable in operation as indicated by system performance.

The reviewer will need the correct version of the following information for conducting the validation:

- The results of the SAEC activity;
- SSA Chapter 3 Guidance Material B - SSA activities along the life cycle.

The validation goals are summarised in Figure 6.4:

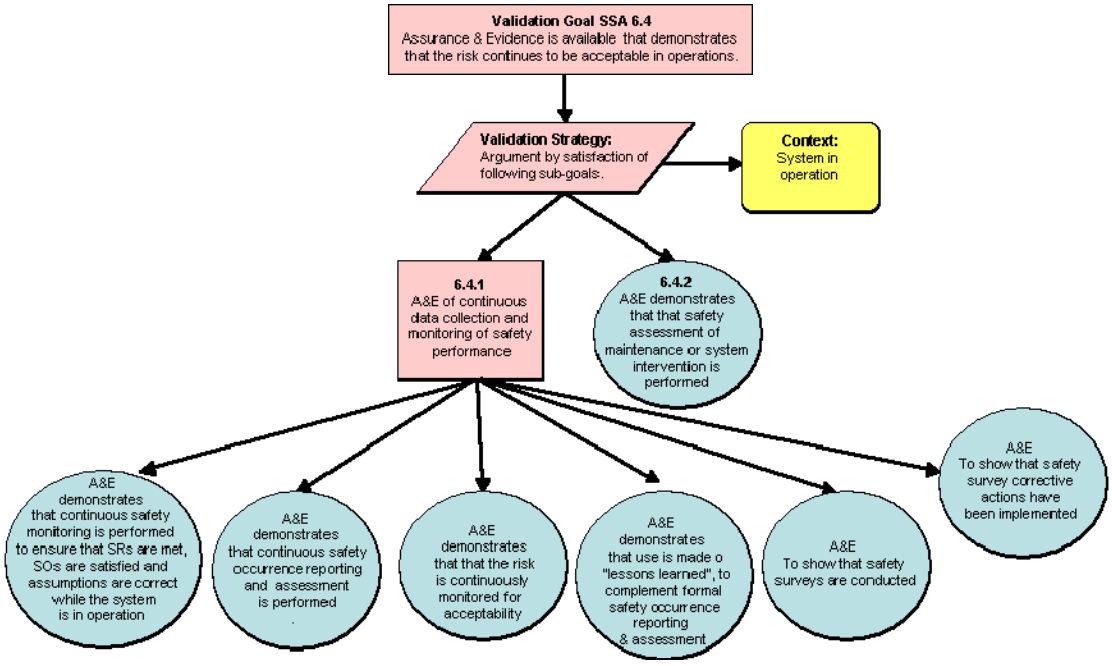


Figure 6.4 Operations and maintenance validation goals

6.4.1 Continuous data collection and monitoring of safety performance.

The reviewer shall confirm that the assurance available demonstrates the following:

Goal	Validation Item:	Validation Result
SSA 6.4.1.1	**Assurance and Evidence are correct and complete to show that continuous safety monitoring is performed to ensure that Safety Requirements are met, Safety Objectives are satisfied and assumptions are correct while the system is in operation.** [Refer to SSA Chapter 3 Guidance Material B § 2.3] Confirmed by establishing that formal monitoring arrangements and procedures are in place, and system performance records are maintained.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in SSA**	
SSA 6.4.1.2	**Assurance and Evidence are correct and complete to show that continuous safety occurrence reporting and assessment is performed.** [Refer to SSA Chapter 3 Guidance Material B § 2.3] Confirmed by establishing that incidents are recorded, formal analysis of results takes place, and remedial action is carried out.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in SSA**	
SSA 6.4.1.3	**Assurance and Evidence are correct and complete to show that the risk is continuously monitored for acceptability**. [Refer to SSA Chapter 3 Guidance Material B § 2.3] Judged by formal arrangements and procedures in place, to assess system performance against safety objectives.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in SSA**	
SSA 6.4.1.4	**Assurance and Evidence are correct and complete to show that use is made of "lessons learned", to complement formal safety occurrence reporting & assessment.** [Refer to SSA Chapter 3 Guidance Material B § 2.3] Refers to lessons learned from ANSP's own experience but also from the wider ATM community. Evidence would include publication/availability of local information sheets or digests of occurrences.	Satisfactory ☐ Requires Action ☐

	Comment / action: **Reference in SSA**	
SSA 6.4.1.5	**Assurance and Evidence are correct and complete to show that safety surveys are conducted**. [Refer to SSA Chapter 3 Guidance Material B § 2.3] Ideally, a schedule of surveys would be agreed and planned annually taking account of available resources. The selected items for survey need not be limited to those which may be a cause for concern, as potential issues to be addressed invariably result from surveys.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in SSA**	
SSA 6.4.1.6	**Assurance and Evidence are correct and complete to show that safety survey corrective actions follow-up (including their implementation and effectiveness) is conducted**.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in SSA**	

Table 6.4A Operation and maintenance

6.4.2 Safety assessment of maintenance and planned interventions.

The reviewer shall confirm that the assurance available demonstrates the following:

Goal	Validation Item:	Validation Result
SSA 6.4.2	**Assurance and Evidence are correct and complete to show that safety assessment of maintenance and/or planned intervention is performed**: [Refer to SSA Chapter 3 Guidance Material C] This is a critical area, common for human error resulting in system failures. The assessment should address the ongoing adherence to procedures, the procedures themselves, and the competency of the individuals involved.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in SSA**	

Table 6.4B Operation and maintenance

6.5 System change validation process

Any major change to the system and its elements (people, procedures, equipment) leads to the re-iteration of the overall safety assessment process, through the FHA, PSSA and SSA. Thus no specific guidance is dedicated to this item in the SSA validation.

6.6 Decommissioning validation process

The reviewer will need the correct version of the following information for conducting the validation:

- The results of the SAEC activity;
- SSA Chapter 3 Guidance Material B - SSA Activities along the life cycle.

The reviewer shall confirm that the assurance available demonstrates the following:

Goal	Validation Item:	Validation Result
SSA 6.6.1.1	**Assurance and Evidence are correct and complete to show that the safety assessment on global ANS operations due to withdrawing the system from operations has been performed**. [Refer to SSA Chapter 3 Guidance Material B § 2.5] Have all the Safety Requirements met by the withdrawn system been addressed by the new system, or shown to be no longer valid?	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in SSA**	
SSA 6.6.1.2	**Assurance and Evidence are correct and complete to show that the safety assessment of the decommissioning process itself has been performed to ensure that the risk induced on on-going ANS operations during the decommissioning operations is acceptable.** [Refer to SSA Chapter 3 Guidance Material B § 2.5] What steps have been taken to ring fence the operational system during the decommissioning? Responsibility for protecting the operational system should not be delegated to individuals outside the ANSP and a level of supervision should be in place appropriate to the safety significance of the system.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in SSA**	

Table 6.6 Decommissioning

6.7 SSA Report

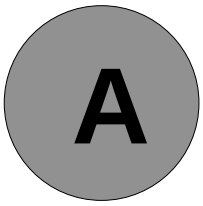
The purpose of the SSA Report is to support the decision making process by providing assurance about the prospects of the system achieving an acceptable risk.

The SSA report should contain a summary of the findings, supported by marked up V&V tables and commentary.

In addition the reviewer shall confirm the following:

Goal	Validation Item:	Validation Result
SSA 6.7.1	**Assurance and Evidence are correct and complete to show that Personnel conducting the safety assurance are suitably qualified.** They should be familiar with and understand the SAM recommendations.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in SSA**	
SSA 6.7.2	**The reviewer shall comment on the quality of the process followed and whether the safety assurance activities appear to be both adequate and appropriate**. This is for the information of the Safety Manager so that improvements can be made to the process as necessary. To review Safety Evidence, the following criteria have been appropriately covered (an acceptable rationale exists to sustain the choices made to address those criteria): • All Safety Requirements are continuously satisfied with the appropriate level of demonstration; • All Safety Objectives are continuously satisfied; • Risk is continuously acceptable; • Documentation and Evidence are up-to-date with regards actual operations.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in SSA**	

Table 6.7 SSA Report



CHAPTER 5
GUIDANCE MATERIAL:

SSA REPORT

The SSA documentation records the results of the SSA assessment process. This document will be updated through the complete system life cycle.

In order to make this document readable and conveying efficiently key messages and results of SSA, recommendations are:

- To keep the body of the document short (around 15 pages);

- To make this document conclusive: state whether the system achieves or not an acceptable risk and clearly and concisely list the main findings of the SSA such as where Assurance & Evidence is acceptable or insufficient ;
- To include an executive summary;
- To contain the results of detailed analyses in annexes.

A possible structure for the SSA report is given in Table 5.1.

Table 5.1. Structure of the SSA Report

Executive Summary It should focus on main messages delivered by SSA, such as: is system achieving an acceptable risk in its operational environment and where Assurance & Evidence is acceptable or insufficient. **Introduction** This section should describe: • The objectives of the document. • The scope of the SSA (What was addressed in the SSA process and what was not addressed). • The structure of the document. **System Description** This section should provide an overview of the system design and architecture. It will cover, or reference, documentation describing: • The system definition, architecture and design; • The purpose and boundaries of the system; • The system operational environment (if appropriate, the assumptions made about this operational environment); • The external interfaces (including technical data).

It will also identify whether the system is new, a replacement or a modification of an existing system.

Safety Criteria

This section should identify the specific safety criteria used to define the Safety Assurance & Evidence. For example,

- Applicable Safety Regulatory Requirements;
- (International) Standards
- Approach to collect and accept Safety Assurance & evidence, when appropriate.

Safety Assurance & Evidence Identification

The results are usually best presented in a tabular format.

If numerous, this part should focus on the main Safety Assurance & Evidence and make reference to the complete list in an annex.

Summary and Conclusions

This part should summarise the results of the SSA process. It should include:

- The phase of the lifecycle associated to this specific SSA report;
- The list of verified and validated: assumptions, most critical Safety Objectives/hazards, Safety Requirements;
- The main conclusions of the SSA validation, verification and process assurance activities;
- A statement whether the system achieves or not an acceptable risk.

This part should also identify any architectural elements or mitigation means or failures or hazards requiring additional analysis, and/or other priorities for further attention in the development/assessment cycle.

Annexes

- Detailed result tables;

- Cross-references to other documents produced within the SSA process, such as the SSA Plan (as described in SSA Chapter 2) and the Validation/ Verification and Process Assurance reports (as described in SSA Chapter 4);
- References to external documents – e.g. regulatory requirements, standards, documentation for systems interacting with the proposed system;
- Detailed results of analyses (FTA, FMEA, CCA, Sensitivity Analysis, …)
- Traceability matrices

  Evidence <> Safety Requirements
  Evidence <> System Elements
  Evidence <> Safety Objectives
  Evidence <> Assumptions (e.g. External Mitigation Means, Operational Environment, .. See FHA & PSSA)