A B C

GUIDANCE MATERIAL:

PSSA Evaluation Activities

1 Introduction

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

This guidance is 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.

The objective of these guidelines is to ensure that the PSSA is suitable for use during the System Safety Assessment (SSA).

2 Objectives of the PSSA

The PSSA apportions Safety Objectives (defined during the FHA) into Safety Requirements allocated to the system elements. Safety Requirements specify the risk level to be achieved by the system elements. The PSSA is conducted during the *System Design* phase of the system life cycle.

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

3 How to apply the process

Verification and validation processes are satisfied through a combination of reviews and analysis of the PSSA process and results. 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, in all probability, report to the project manager. Their role will be to give the project manager an objective assessment of the outputs of the PSSA and the process followed.

The same person (or persons) may carry out verification and validation. The decision is the responsibility of the project manager.

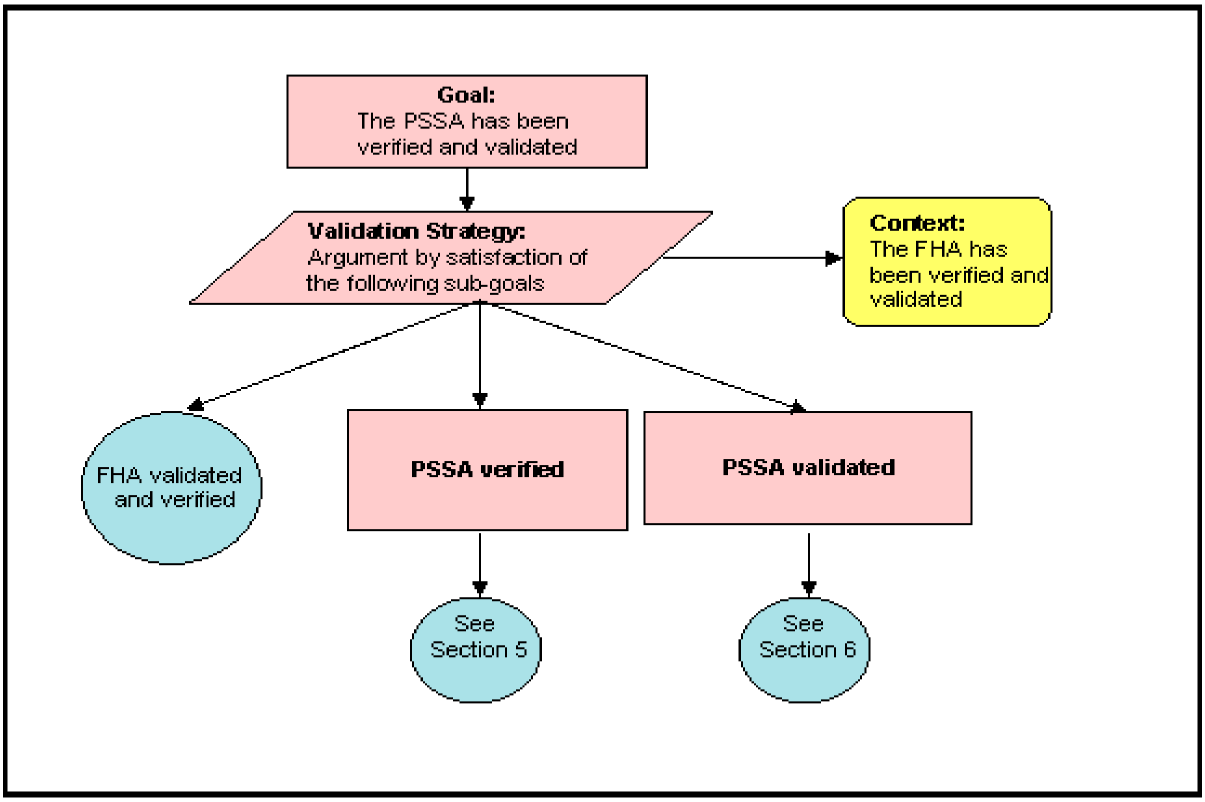
The accomplishment of objective evaluation is more likely to be ensured when the verification and validation processes are carried out by a person (or persons) other than those who performed the PSSA.

The involvement of people with different skills (ATCO’s, Pilots, Engineers and safety experts) in a SAM process (e.g. identification of causes in the PSSA) 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 PSSA verification and validation can only be applied when the Functional Hazard Assessment has been verified and validated.

A number of approaches can be followed for verification & validation:

- Conduct the verification and validation at varying PSSA stages, especially for a large or complex PSSA. This may reduce the risk of wasting effort by identifying gaps or issues in the PSSA at an early stage.
- Start the PSSA validation when all the verification is completed.


Goal:
The PSSA has been verified and validated
Validation Strategy:
Argument by satisfaction of the following sub-goals
Context:
The FHA has been verified and validated
FHA validated and verified
PSSA verified
PSSA validated
See Section 5
See Section 6

4 Scope of these guidelines

The activities described in this chapter are limited to the verification and validation of PSSA output (Safety Requirements and related assumptions).

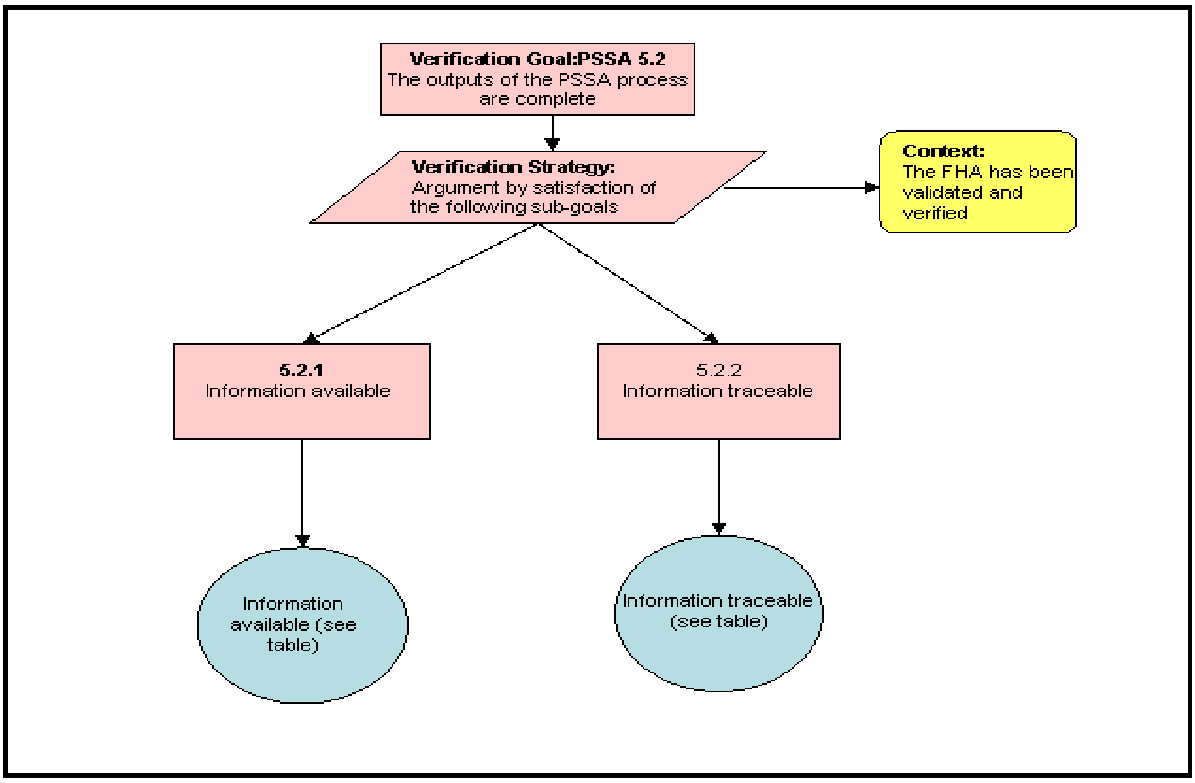
5 PSSA Verification

5.1 Introduction

The essential pre-requisite for conducting a PSSA is a Functional Hazard Assessment (FHA), which will provide a description of the high level functions of the system, a list of assumptions, hazards and their associated Safety Objectives.

Another essential pre-requisite for conducting a PSSA is a or multiple proposed system architecture(s) to be assessed.

5.2 Verification Process


Verification Goal:PSSA 5.2
The outputs of the PSSA process are complete
Verification Strategy:
Argument by satisfaction of the following sub-goals
Context:
The FHA has been validated and verified
5.2.1
Information available
5.2.2
Information traceable
Information available (see table)
Information traceable (see table)

The following information should be clearly identified in the FHA and/or PSSA.

Goal	Verification Item	Available (yes/no)	Reference in PSSA (document,page)
PSSA 5.2.1.1	**The description of system functions and sub-functions and the relationships between these (sub-)functions (e.g. messages and data exchanged) is documented** [Refer to PSSA Chapter 1 Guidance Material OED]		
PSSA 5.2.1.2	**Verify that assumptions are identified.**		
PSSA 5.2.1.3	**Updated list of Hazards** New hazards may have been identified during PSSA.		
PSSA 5.2.1.4	**Updated list of Safety Objectives** Safety Objectives may have been redefined during PSSA (e.g. common causes between internal and external mitigation means may have been found).		
PSSA 5.2.1.5	**The description of system architecture(s) and their rationale (justification material, supporting analyses) is documented.** [Refer to PSSA Chapter 1 Guidance Material OED]		
PSSA 5.2.1.6	**The design constraints are documented** e.g. maximum reuse of pre-existing equipment or COTS (Commercial Off The Shelf) Software or hardware.		
PSSA 5.2.1.7	**The System elements requirements and/or specification are documented.**		
PSSA 5.2.1.8	**The system Physical interfaces are documented.** [Refer to PSSA Chapter 1 Guidance Material OED]		
PSSA 5.2.1.9	**The applicable Regulatory requirements are referenced.**		
PSSA 5.2.1.10	**The Applicable standards are referenced.**		
PSSA 5.2.1.11	**The Risk Mitigation strategies are defined and documented in the PSSA plan.** [Refer to PSSA Chapter 2 Guidance Material A]		
PSSA 5.2.1.12	**Safety Requirements are derived from Safety Objectives.**		
PSSA 5.2.1.13	**The PSSA plan has been applied.** [Refer to PSSA Chapter 2 Guidance Material A]		

Traceability:

The following items should be clearly traceable in the PSSA.

Goal	Verification Item	Available (yes/no)	Reference in PSSA (document,page)
PSSA 5.2.2.1	**Safety Requirements to Safety Objectives**		
PSSA 5.2.2.2	**Sub-function/system elements to System Functions**		
PSSA 5.2.2.3	**Safety Requirements (including Assurance Level when applicable) to system elements**		

Note: The traceability between Safety Requirement and System Functions (as identified in the FHA) can be done either directly or indirectly (via the traceability to Safety Objectives, using PSSA-5.2.2.1 and FHA-5.2.4.1 and FHA-5.2.4.2).

6 PSSA Validation

6.1 Process assurance

The PSSA-SRS (Safety Requirements Specification) should demonstrate how Safety Requirements are derived for each individual system element (people, procedure and equipment).

Safety Requirements Specification is defined in five steps (reference Guidance Material Chapter 3) and should be clearly identified. They are:

1. Refine Sub-Functions Safety Contribution;
2. Evaluate System Architecture(s);
3. Apply Risk Mitigation Strategies;
4. Apportion Safety Objectives into Safety Requirements to System Elements;
5. Balance/Reconcile Safety Requirements.

The Reviewer shall confirm the following:

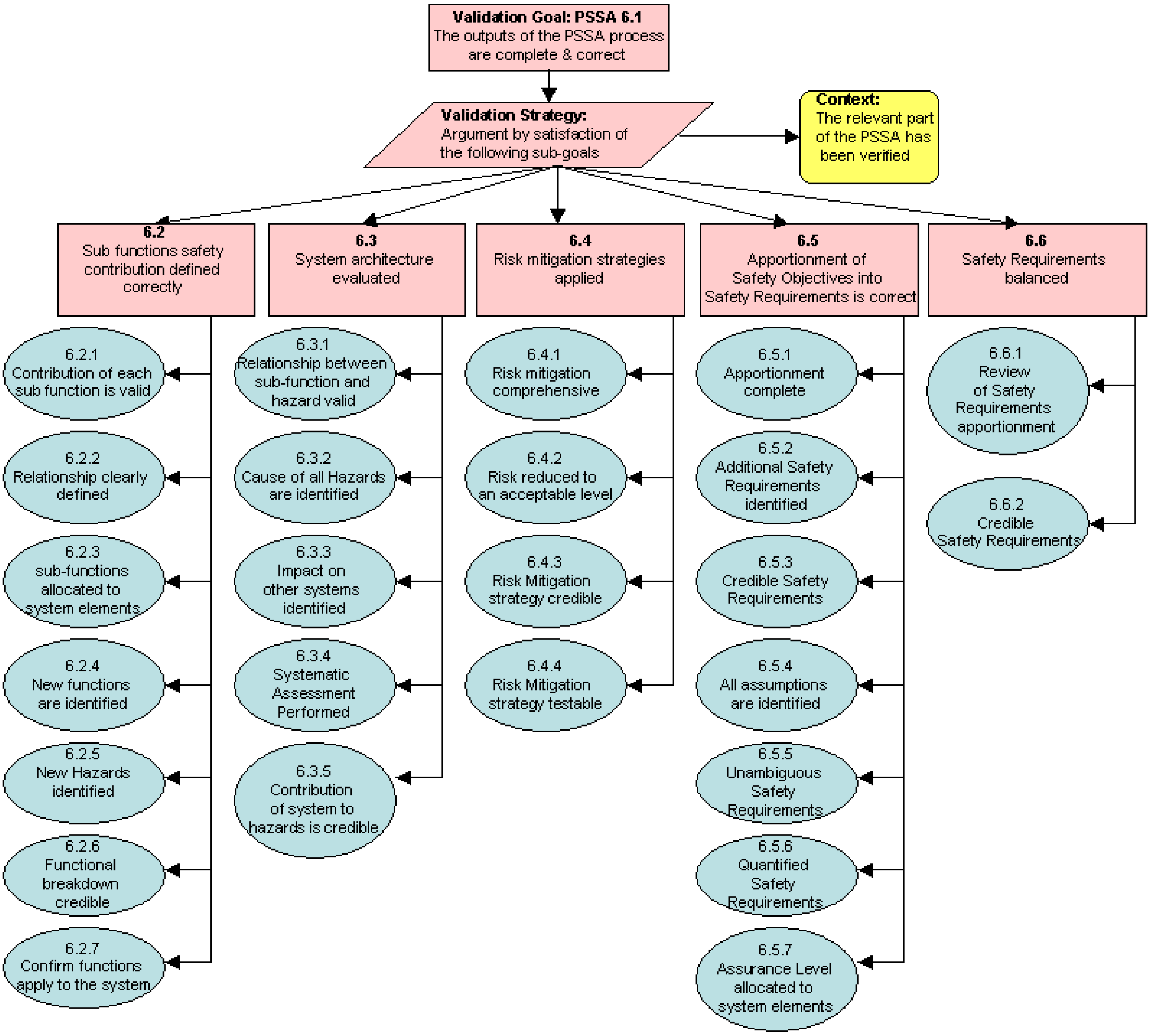
Goal	Validation Item	Validation Result
PSSA 6.1.1	**All five stages of the PSSA-SRS have been addressed**.	Satisfactory □ Requires Action □
	Comment / action: **Reference in PSSA:**	

The reviewer should address items:

- 1 - Refine Sub-Functions Safety Contribution and
- 2 - Evaluate System Architecture(s)

before moving to:

- 3 - Apply Risk Mitigation Strategies;
- 4 - Apportion Safety Objectives into Safety Requirements to System Elements and
- 5 - Balance/Reconcile Safety Requirements.


Validation Goal: PSSA 6.1
The outputs of the PSSA process are complete & correct
Validation Strategy:
Argument by satisfaction of the following sub-goals
Context:
The relevant part of the PSSA has been verified
6.2
Sub functions safety contribution defined correctly
6.3
System architecture evaluated
6.4
Risk mitigation strategies applied
6.5
Apportionment of Safety Objectives into Safety Requirements is correct
6.6
Safety Requirements balanced
6.2.1
Contribution of each sub function is valid
6.2.2
Relationship clearly defined
6.2.3
sub-functions allocated to system elements
6.2.4
New functions are identified
6.2.5
New Hazards identified
6.2.6
Functional breakdown credible
6.2.7
Confirm functions apply to the system
6.3.1
Relationship between sub-function and hazard valid
6.3.2
Cause of all Hazards are identified
6.3.3
Impact on other systems identified
6.3.4
Systematic Assessment Performed
6.3.5
Contribution of system to hazards is credible
6.4.1
Risk mitigation comprehensive
6.4.2
Risk reduced to an acceptable level
6.4.3
Risk Mitigation strategy credible
6.4.4
Risk Mitigation strategy testable
6.5.1
Apportionment complete
6.5.2
Additional Safety Requirements identified
6.5.3
Credible Safety Requirements
6.5.4
All assumptions are identified
6.5.5
Unambiguous Safety Requirements
6.5.6
Quantified Safety Requirements
6.5.7
Assurance Level allocated to system elements
6.6.1
Review of Safety Requirements apportionment
6.6.2
Credible Safety Requirements

6.2 Refine Sub-Functions Safety Contribution

The reviewer shall confirm that the system functional architecture from the FHA is decomposed into lower-level sub-functions.

The Reviewer shall confirm the following:

Goal	Validation Item	Validation Result
PSSA 6.2.1	**The contribution of each sub-function to a Safety Objective is valid.** The PSSA should illustrate the contribution of each sub-function to Safety Objectives, by associating each Safety Objective (not only the most stringent one) to individual sub-functions of the functional architecture that contribute to it.	Satisfactory □ Requires Action □
	Comment / action: **Reference in PSSA:**	
PSSA 6.2.2	**The relationship of sub-functions to high level functions is valid.** The PSSA should provide a clear mapping between high level functions and the sub-functions. All sub-functions should be allocated to a high level function.	Satisfactory □ Requires Action □
	Comment / action: **Reference in PSSA:**	
PSSA 6.2.3	**Sub-functions allocated to system elements are defined.** The PSSA should develop the functional breakdown until each sub-function becomes sufficiently defined to be allocated to a system element: people, procedure or equipment (hardware or software).	Satisfactory □ Requires Action □
	Comment / action: **Reference in PSSA:**	
PSSA 6.2.4	**Any new functions identified in the PSSA are valid.** The PSSA may develop new functions as a result of the design process. Validation of these new functions should be performed by the design team and approval for the new functions should be obtained from the project manager. The reviewer should ensure that the new functions do no impact on the hazards or Safety Objectives generated in the FHA (e.g. introduces new hazards, removes hazards or changes the consequence [severity] of the Safety Objectives). It may be necessary to re-perform part of the FHA to ensure that there is no safety impact.	Satisfactory □ Requires Action □
	Comment / action: **Reference in PSSA:**	
PSSA 6.2.5	**Any new hazards are valid.** The PSSA may identify additional hazards or Safety Objectives, by considering additional potential hazards and their effect(s) resulting from the failure of sub-functions. These should be recorded and 'fed-back' to the PSSA owner.	Satisfactory □ Requires Action □
	Comment / action: **Reference in PSSA:**	

Goal	Validation Item	Validation Result
PSSA 6.2.6	**The functional breakdown is credible.** The PSSA shall provide evidence that the functional breakdown is credible and acceptable. Typically this is proven by stakeholder endorsement of the process and conclusions.	Satisfactory □ Requires Action □
	Comment / action: **Reference in PSSA:**	
PSSA 6.2.7	**The sub-functions are applicable to the system under assessment.**	Satisfactory □ Requires Action □
	Comment / action: **Reference in PSSA:**	

6.3 Evaluate System Architecture(s)

> The reviewer shall confirm that the contribution of the proposed system design to hazards and the Safety Objectives is valid.

The Reviewer shall confirm the following:

Goal	Validation Item	Validation Result
PSSA 6.3.1	**The contribution of each system element to each hazard is valid.** The PSSA should illustrate how each system element contributes to each hazard. For example, during the PSSA process, experts in ATM design should have participated in identifying the contribution of each element to the hazard. In addition, the contribution (as a proportion of to the Safety Objective) should have been validated by experts.	Satisfactory □ Requires Action □
	Comment / action: **Reference in PSSA:**	
PSSA 6.3.2	**The causes of the hazards are stated and valid.** The PSSA should address how the system contributes to hazards in normal operations, failure of system elements, common cause failures and when the new system begins operation.	Satisfactory □ Requires Action □
	Comment / action: **Reference in PSSA:**	
PSSA 6.3.3	**The impact on other systems (outside the scope of the safety assessment) is identified.** The PSSA should identify the impact that the new system may have on other ATM elements (e.g. interference with other systems or changes in the operation of other equipment due to the introduction of new systems). These should have been identified by experts, validated by the owners and users of the outside system. In addition, the impact on the new systems should be documented and passed onto the project manager who should ensure that co-ordination (at the system or centre level) is performed.	Satisfactory □ Requires Action □
	Comment / action: **Reference in PSSA:**	
PSSA 6.3.4	**A systematic and structured approach has been applied to the evaluation of the cause of the hazards.** The PSSA should have a structured approach for evaluating the contribution of the system to hazards. Various techniques could be used to help the safety analyst to assess the hazardous scenarios and to identify causes. [Ref SAM-Part IV Annex D].	Satisfactory □ Requires Action □
	Comment / action: **Reference in PSSA:**	

Goal	Validation Item	Validation Result
PSSA 6.3.5	**The contribution of the system to the hazards is credible.** The PSSA should provide evidence that the contribution of the system to the hazards is credible. Credibility can be proven by stakeholder endorsement of the process and the conclusions	Satisfactory □ Requires Action □
	Comment / action: **Reference in PSSA:**	

6.4 Risk Mitigation Strategies

The reviewer shall confirm that the system design has been evaluated and possibly modified to make it able to mitigate the risk to an acceptable level. Risk Mitigation Strategies should be applied in accordance with the overall risk mitigation strategy as defined in the PSSA plan (See “PSSA Planning” Chapter 2)

The Reviewer shall confirm the following:

Goal	Validation Item	Validation Result
PSSA 6.4.1	**The risk mitigation strategy is comprehensive.** The PSSA should demonstrate that the risk mitigation strategy addresses both the potential causes of system failures and the potential consequences of system failures and hazards. [Ref PSSA Chapter 3.3].	Satisfactory □ Requires Action □
	Comment / action: **Reference in PSSA:**	
PSSA 6.4.2	**The application of mitigation strategies is able to reduce the risk to an acceptable level.** The PSSA should present detailed arguments to show that risk mitigation strategies have been applied to eliminate, reduce or control the risk [Ref PSSA Chapter 3.3].	Satisfactory □ Requires Action □
	Comment / action: **Reference in PSSA:**	
PSSA 6.4.3	**A credible risk mitigation strategy has been defined** The PSSA shall demonstrate that all risk mitigation strategies are credible. This can be proven by stakeholder endorsement of the process and conclusions. [Ref PSSA Chapter 2 Guidance Material A].	Satisfactory □ Requires Action □
	Comment / action: **Reference in PSSA:**	
PSSA 6.4.4	**A testable risk mitigation strategy has been defined.** The PSSA shall ensure that all risk mitigation strategies are testable when implemented. This is typically an expert judgement, supported through peer review. [Ref PSSA Chapter 2 Guidance Material A].	Satisfactory □ Requires Action □
	Comment / action: **Reference in PSSA:**	

6.5 Apportion Safety Objectives into Safety Requirements

The PSSA should apportion Safety Objectives to Safety Requirements specified for each individual system element.

The Reviewer shall confirm the following:

Goal	Validation Item	Validation Result
PSSA 6.5.1	**The apportionment of Safety Requirements is complete.** The PSSA should also demonstrate that all Safety Objectives are apportioned into Safety Requirements. The PSSA should demonstrate that all Safety Requirements have been identified for all system elements.	Satisfactory □ Requires Action □
	Comment / action: **Reference in PSSA:**	
PSSA 6.5.2	**Any additional Safety Requirements are identified.** Additional Safety Requirements may be set to meet regulations or standards.	Satisfactory □ Requires Action □
	Comment / action: **Reference in PSSA:**	
PSSA 6.5.3	**The Safety Requirements apportionment is credible.** The PSSA should demonstrate that the Safety Requirements apportionment is credible. A Fault-Tree Analysis (FTA) completed with a Common Cause Analysis (CCA) can contribute to his demonstration. This can be proven by stakeholder endorsement of the process and conclusions.	Satisfactory □ Requires Action □
	Comment / action: **Reference in PSSA:**	
PSSA 6.5.4	**All assumptions are listed.** The PSSA should identify all assumptions. These assumptions shall be credible and validated by stakeholders.	Satisfactory □ Requires Action □
	Comment / action: **Reference in PSSA:**	
PSSA 6.5.5	**The Safety Requirements are unambiguous.** The PSSA should ensure that all Safety Requirements are unambiguous. This typically means that the use of 'and' and 'or' are not included in Safety Requirements.	Satisfactory □ Requires Action □
	Comment / action: **Reference in PSSA:**	
PSSA 6.5.6	**Safety Requirements are quantified, when possible.** One purpose of the PSSA consists in specifying unambiguous Safety Requirements. One way to make Safety Requirements unambiguous is to quantify them. Quantitative Safety Requirements should be defined in one or many units applicable to the operations under assessment (typically in flight hours or operation hours). However, many Safety Requirements can not be quantified (Software, Procedure, Human maybe difficult also).	Satisfactory □ Requires Action □

Goal	Validation Item	Validation Result
	Comment / action: **Reference in PSSA:**	
PSSA 6.5.7	**Assurance Level of requirement satisfaction demonstration is allocated to the system element.** A PAL (Procedure Assurance Level) or SWAL (Software Assurance Level) has always to be allocated to a ATM procedure or a ATM Software. If necessary, a HWAL (Hardware Assurance Level) can be allocated. In the future (SAM V2 does not provide yet recommendation on this aspect yet) HAL (Human Assurance Level) will have to be allocated.	Satisfactory □ Requires Action □
	Comment / action: **Reference in PSSA:**	

6.6 Balance/Reconcile Safety Requirements

> The PSSA shall show that the Safety Requirements are balanced and achievable (to ensure that the Safety Requirements are not unnecessarily stringent or not credible).

The Reviewer shall confirm the following:

Goal	Validation Item	Validation Result
PSSA 6.6.1	**The overall set of Safety Requirements has been reviewed and maybe alternative strategies for apportionment were considered.** A global analysis (and not only one Safety Objective at a time or a group of Safety Objectives) of the type of Safety Requirement (e.g. always procedure or human mitigation means) or "complexity/stringency of Safety Requirement (e.g. too many new mitigation means or too many very stringent requirement). An analysis of Single Point of Failure is commensurate with the stringency of Safety Requirement, Safety Objective and risk (e.g. no single point of failure that can lead directly to a Severity 1 or 2). The PSSA may show that alternative apportionment of Safety Requirements has been evaluated and the decision making process for the approval or rejection of the Safety Requirements apportionment is described.	Satisfactory □ Requires Action □
	Comment / action: **Reference in PSSA:**	
PSSA 6.6.2	**The Safety Requirements are credible** The PSSA shall show that the Safety Requirements are deemed to be achievable and implemented by stakeholders. Past experience or state-of-the-art knowledge can be used. Usage of pre-existing equipment or COTS (Commercial Off the Shelf) software or hardware is compatible with the allocated Safety Requirements.	Satisfactory □ Requires Action □
	Comment / action: **Reference in PSSA:**	

7 PSSA report

The report should describe how Safety Objectives were translated to Safety Requirements for the system. The PSSA report shall be clear, traceable and approved by stakeholders. The purpose of the PSSA Report is to support the decision making process by providing assurance about the prospects of the system architecture being able to achieve an acceptable risk.

The PSSA report shall contain:

- An updated list of assumptions;
- An updated list of identified hazards and Safety Objectives (new hazards and/or effects may have been identified);
- Results of Safety analyses;
- Justification material for risk mitigation strategies application;
- Safety Requirements on individual system elements and their rationale;
- Assurance Level of satisfaction of Safety Requirements for system elements;
- A conclusion on the ability of the system architecture to achieve an acceptable risk.

The PSSA report should demonstrate that stakeholders have validated and approved the methodology, assumptions and conclusions.

The Reviewer shall confirm the following:

Goal	**Validation Item:**	Validation Result
PSSA 6.7.1	**PSSA report writers are suitably qualified.**	Satisfactory □ Requires Action □
	Comment / action: **Reference in FHA**	
PSSA 6.7.2	**The reviewer shall comment on the quality of the process followed and whether, it is well documented, accessible and credible (the Safety Requirements appear to be appropriate).** To specify Safety Requirements, the following criteria have been appropriately covered (an acceptable rationale exists to sustain the choices made to address those criteria): • Benefit from "AND" gates is explained; • Common cause analysis has been done; • Assurance Level of requirement satisfaction is allocated (per system element) • Usage of pre-existing equipment or COTS (Commercial Off The Shelf) software or hardware is considered.	Satisfactory □ Requires Action □
	Comment / action: **Reference in PSSA**	

Table 6.7