



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 14

SAM – Preliminary System Safety Assessment

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

Foreword

The purpose of this guidance material is to support the implementation of Preliminary System Safety Assessment (PSSA), 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 PSSA, 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.

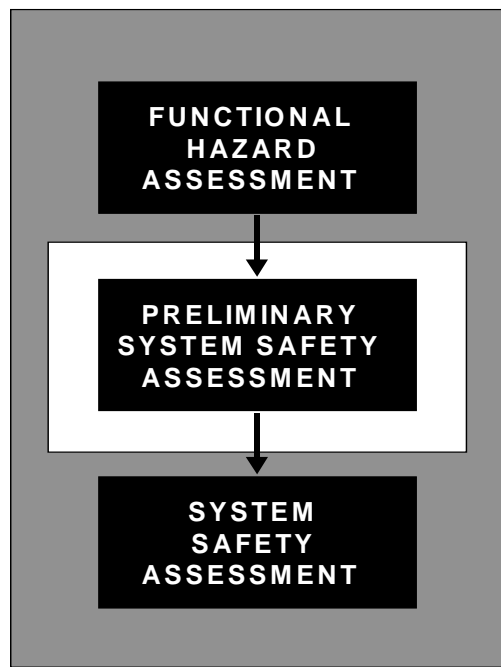
This Guidance Material should be applied taking into consideration the complementary Guidance Materials available for SAM, as well as ANSPs' own Safety Management Manuals. Furthermore, the content of this Guidance Material broadly addresses subject matter related to risk assessment and mitigation, therefore 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. ANSP's 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 II

PRELIMINARY SYSTEM SAFETY ASSESSMENT



This page is intentionally blank

TABLE OF CONTENTS

INTRODUCTION

1	OBJECTIVE OF PSSA.....	I-6
2	WHEN AND HOW PSSA IS APPLIED	I-7
3	STRUCTURE OF THE PSSA DESCRIPTION.....	I-7
4	STRUCTURE OF THIS DOCUMENT.....	I-8
5	READERSHIP TABLE	I-8
6	CONFIGURATION MANAGEMENT, DOCUMENTATION AND RECORDS	I-9
6.1	WHY?.....	I-9
6.2	HOW?	I-10

CHAPTER 1 - PSSA INITIATION

1	OBJECTIVE.....	I-13
2	INPUT	I-13

• 2.1	System Description.....	I-13
• 2.2	Operational Environment Description	I-14
• 2.3	Regulatory Framework	I-14
• 2.4	Applicable Standards	I-14
• 2.5	Other Inputs.....	I-14
3	MAJOR TASKS	I-15
4	OUTPUT	I-15

CHAPTER 2 - PSSA SAFETY PLANNING

1	OBJECTIVE.....	I-17
2	INPUT.....	I-17
3	MAJOR TASKS	I-17
4	OUTPUT	I-18

CHAPTER 3 – SAFETY REQUIREMENTS SPECIFICATION

1	OBJECTIVE.....	I-19
2	INPUT.....	I-20
3	MAJOR TASKS	I-20
3.1	Identify Potential Hazards	I-22
3.2	Identify Hazard Effects	I-23
3.3	Assess Hazard Effects Severity.....	I-24
3.4	Specify Safety Objectives	I-24
3.5	Assess the intended aggregated risk	I-25
4	OUTPUT	I-26

CHAPTER 4 - PSSA EVALUATION

1	OBJECTIVE.....	I-27
2	INPUT.....	I-29
3	MAJOR TASKS	I-29
• 3.1	PSSA Verification tasks.....	I-30
• 3.2	PSSA Validation tasks	I-30
• 3.3	PSSA Process Assurance	I-31

4 OUTPUTI-31

CHAPTER 5 - PSSA COMPLETION

1 OBJECTIVEI-33

2 INPUTI-33

3 MAJOR TASKSI-33

4 OUTPUTI-34

INTRODUCTION

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

1. OBJECTIVE OF PSSA

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

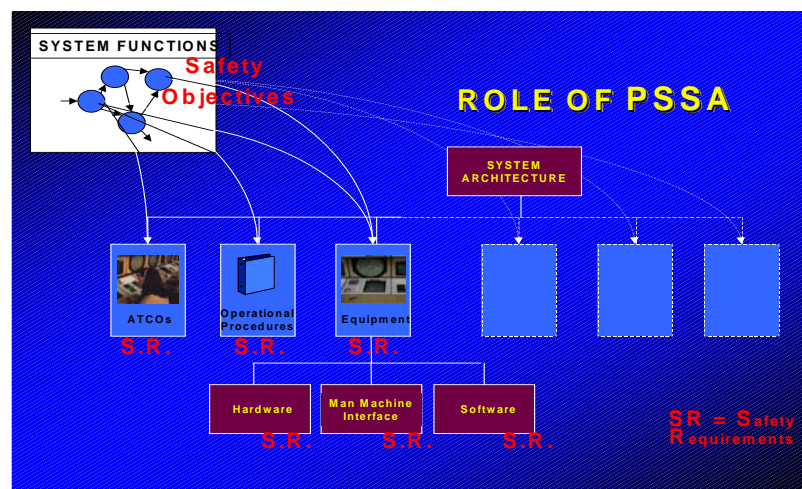
As a reminder, a **Safety Objective** [ESARR4] is a qualitative or quantitative statement that defines the maximum frequency or probability at which a hazard can be accepted to occur. ("Accepted" is underlined because this is the only difference with ESARR4 definition where "expected" is replaced with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

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

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

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

Figure 1 Role of the PSSA



2. WHEN AND HOW PSSA IS APPLIED

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

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

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

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

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

3. STRUCTURE OF THE PSSA DESCRIPTION

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

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

PSSA Initiation (Chapter 1);

Specification of Safety Requirements (Chapter 3);

PSSA Completion (Chapter 5).

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

PSSA Planning step (Chapter 2);

PSSA Evaluation step (Chapter 4).

Table 1 summarises the major activities conducted in each step of the PSSA, and their inputs and outputs.





4. STRUCTURE OF THIS DOCUMENT.

This document is in three main parts;

- **Chapters**, which describe the methodology and are printed on white paper;
- **Guidance Material**, which follows as annex each chapter for which it provides guidance and amplifies and explains the methodology, this is printed on colorA paper;
- **Appendixes**, which provide background material and examples and are printed on colorB paper.

5. READERSHIP TABLE

The following table suggests a minimum attention to PSSA Material:

PSSA Material	System (People, Procedure, Equipment) Designer	Safety Practitioner	Programme/project Manager	Programme/project Safety Manager
Introduction	✓			
Chapter 1 PSSA Initiation	N/A		N/A	✓
Chapter 2 PSSA Planning		✓	✓	✓
Chapter 3 SRS	✓		✓	
Chapter 4 PSSA Evaluation	✓		N/A	✓
Chapter 5 PSSA Completion	✓		N/A	✓
Guidance Material		✓	✓	✓
Examples	N/A	✓	N/A	✓

6. CONFIGURATION MANAGEMENT, DOCUMENTATION AND RECORDS.

A configuration management system should track the outputs of the PSSA process and the relationship between them.

6.1 Why?

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

The three important reasons are:

- To demonstrate to third parties (including the regulator) that risks have been reduced to an acceptable level;
- To maintain a record of why decisions were taken, to ensure that further change does not invalidate the assessment or does not lead to unnecessarily repeating it;
- To support the hand-over of safety responsibilities from one individual or organisation to another.

6.2 How?

An appropriate and useable control scheme that ensures the origin, version control, traceability and approval of all documentation is recommended.

The extent of safety records maintained by a project will depend on the complexity and levels of risk involved. Safety records are difficult to replace so there must be appropriate security and backup to ensure that records are preserved. Up-to-date records should be kept throughout the system lifetime (including decommissioning).

A number of people will contribute to and need access to safety documentation, typically project staff, engineering staff, operational staff, safety specialists, managers and regulators.

The configuration management and documentation control schemes should include procedures to:

- To develop a configuration management plan;
- To establish a consistent and complete set of baseline documents;
- To ensure there is a reliable method of version identification and control;
- To establish and monitor the change management process;
- To archive, retrieve and release documents.

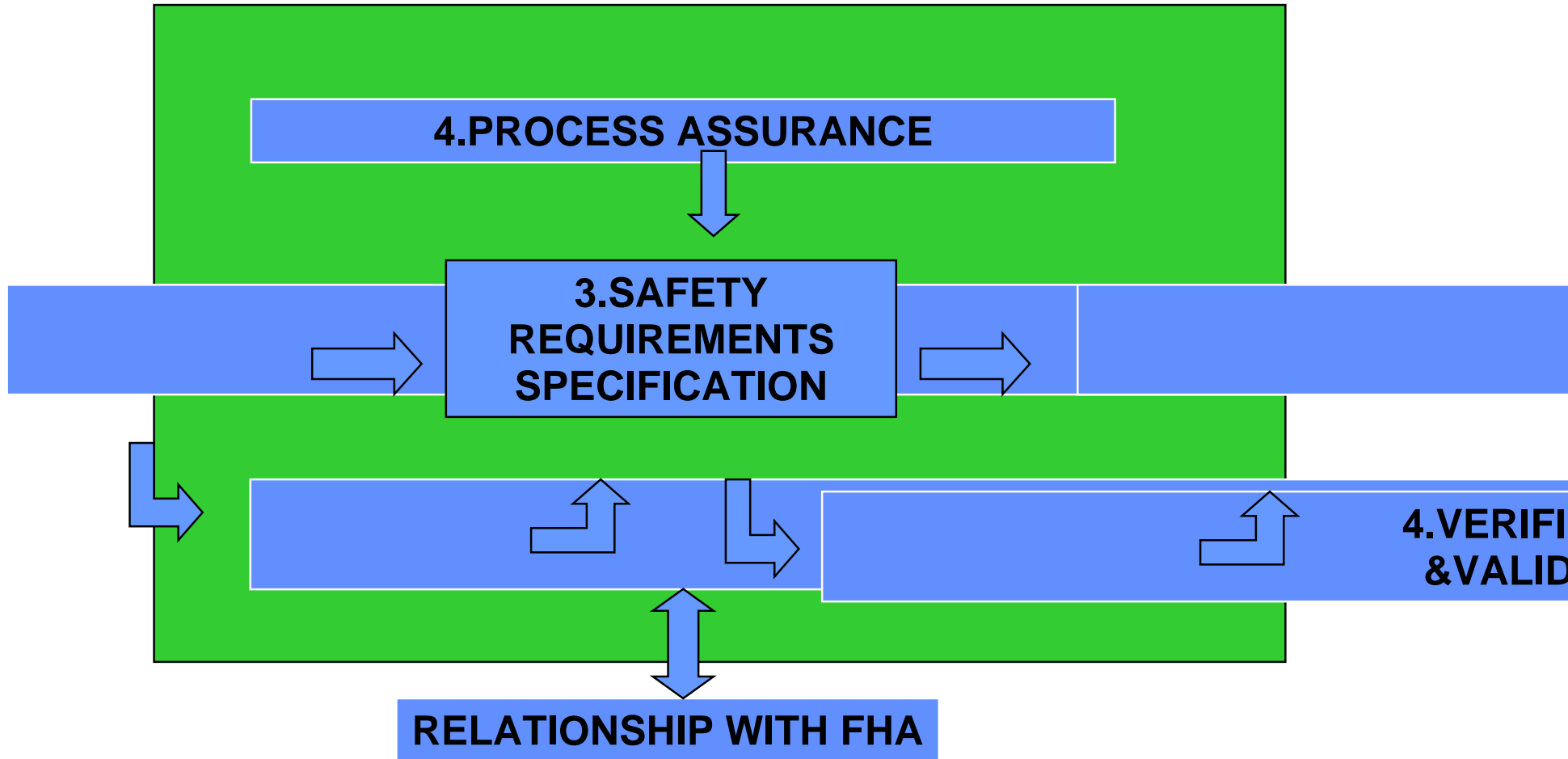
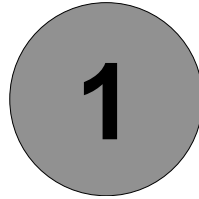


Figure 2: PSSA Process

PSSA STEP	OBJECTIVES	INPUT	MAJOR TASKS	OUTPUT
1 PSSA Initiation	Develop a level of understanding of the system design framework, its operational environment and, if appropriate, its regulatory framework, sufficient to enable the safety assessment activities to be satisfactorily carried out.	System Definition & System Design; Operational Environment Description; Regulatory Requirements; Applicable Standards; FHA output; Other Inputs (e.g., other PSSA results, hazard databases, incident investigation reports, lessons learned, ...).	Gather all necessary information describing the system design; Review this information to establish that it is sufficient to carry out the PSSA; Update the Operational Environment Description (OED) of the system (add PSSA-related data to FHA-related data); Identify and record assumptions made; Formally place all information under a documentation control scheme.	Input information describing the system design; Derived information (e.g., description of the operational environment, list of assumptions).
2 PSSA Planning	Define the objectives and scope of the PSSA, the activities to be carried out, their deliverables, their schedule and the required resources.	Overall Project/Programme plans; Safety Plan; FHA Report.	Identify and describe the more specific activities for each PSSA step in a PSSA Plan; Submit the PSSA plan to peer review to provide assurance of its suitability; Submit the PSSA plan for comment or approval to interested parties (including regulatory authorities), as appropriate; Formally place the PSSA plan under a documentation control scheme; Disseminate the PSSA plan to all interested parties.	Reviewed and approved PSSA Plan.
3 Safety Requirements Specification	Derive Safety Requirements for each individual system element (People, Procedure and Equipment)	PSSA Initiation output, such as: Assumptions list; FHA output: Functions, hazards and their effects list, System Safety Objectives; System Architecture(s)...	For each function and combination of functions, <ul style="list-style-type: none"> Refine the functional breakdown; Evaluate system architecture(s); Apply risk mitigation strategies; Apportion Safety Objectives in to Safety Requirements; Balance/Reconcile Safety Requirements. 	Updated list of assumptions; Updated list of hazards and Safety Objectives; Safety analyses results; Justification material for risk mitigation strategies application; Safety Requirements.
4 PSSA Evaluation				
PSSA Verification	To ensure that Safety Requirements meet Safety Objectives.	Information gathered or derived in the PSSA steps; Safety Plan and PSSA Plan; Outputs (including the final one) of the PSSA process.	Review and analyse the results of the PSSA process.	PSSA Verification results.
PSSA Validation	To ensure that the Safety Requirements are (and remain) correct and complete; To ensure that safety-related assumptions are (and remain) correct and complete.	Information gathered or derived in the PSSA steps; Safety Plan and PSSA Plan; Outputs (including the final one) of the PSSA process.	Review and analyse Safety Requirements to ensure their completeness and correctness; Review and analyse the description of the operational environment to ensure its completeness and correctness; Review, analyse, justify and document critical assumptions about the system design, its operational environment and its regulatory framework to ensure their completeness and correctness; Review and analyse traceability between Safety Objectives and Safety Requirements; Review and analyse the credibility and sensitivity of Safety Requirements with respect to the Safety Objectives and the assumptions.	PSSA Validation results.
PSSA Process Assurance	To provide assurance and evidence that all PSSA activities (including PSSA Verification and PSSA Validation tasks) have been conducted according to the PSSA plan; To ensure that the PSSA process as described in the PSSA plan is correct and complete.	Information gathered or derived in the PSSA steps; Safety Plan and PSSA Plan; Outputs (including the final one) of the PSSA process.	The PSSA Process assurance tasks should at least ensure in accordance with the PSSA Plan that: <ul style="list-style-type: none"> The PSSA steps are applied; Assessment approaches (e.g. success approach, failure approach, use of safety methods and techniques such as Fault-Tree, FMEA, CCA, ...) are applied; All outputs of the PSSA steps (including PSSA Validation and Verification output) are formally placed under a configuration management scheme; Any deficiencies detected during PSSA Verification or Validation activities have been resolved; The PSSA process would be repeatable by personnel other than the original analyst(s); The findings have been disseminated to interested parties; Outputs of the PSSA process are not incorrect and/or incomplete due to deficiencies in the PSSA process itself. 	PSSA Process Assurance results.
5 PSSA Completion	To document and formally place the results of the whole PSSA process under a configuration management scheme; To disseminate these results to all interested parties.	Outputs of all other PSSA steps	Document the results of the PSSA process (including the results of PSSA Validation, Verification and Process Assurance activities); Formally place the PSSA results under a configuration management scheme; Disseminate the PSSA documentation to all interested parties.	PSSA results formally placed under a configuration management scheme.

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



PSSA INITIATION

1 OBJECTIVES

The objectives of the *PSSA Initiation* step are:

- To develop a level of understanding of the system design and its rationale;
- To update the description of the operational environment;
- To identify, when appropriate, regulatory requirements and/or standards applicable to the system design.

2 INPUT

2.1 System Definition

- Description of system functions and the relationships between these functions (e.g. messages and data exchanged);
- Assumptions (FHA output);
- Hazards (FHA output);
- Safety Objectives (FHA output).

2.2 System Design

- Description of system architectures and their rationale (justification material, supporting analyses);
- Design constraints (e.g. maximum reuse of pre-existing equipment or COTS (Commercial Off the Shelf) Software or hardware);
- System elements requirements and/or specification;
- Physical interfaces...

2.3 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 PSSA. In particular, the system description used for the FHA may not be very detailed with respect to technical interfaces or legacy systems.

See Guidance Material A of Chapter 1.

2.4 Regulatory Requirements

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

2.5 Applicable Standards

Standards applicable to the system (e.g., EUROCONTROL Standards, organisation standards,...).

This includes the applicable standards for each kind of system element (people, procedure, equipment (HW, SW)).

2.6 Others

- FHA Report (not restricted to the list of hazards, assumptions and Safety Objectives, as identified in §2.1 of this chapter);
- Data coming from hazard databases, incident investigation reports, lessons learned, ... providing feedback on the PSSA process (the process itself as well as the assurance level allocation process, quantification issues, safety techniques and methods ...) and previous applications of it (system element failures, contribution to hazard).

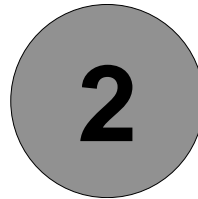
3 MAJOR TASKS

- Gather all necessary information describing the system design, as outlined in Section 2 above;
- Review this information to establish that it is sufficient to carry out the PSSA;
- Update the operational environment description of the system to add system design related data;
- Identify and record assumptions made (raised when designing the system). Areas in which assumptions are commonly necessary relate to the operational scenarios, the system functions, the system architecture and the system environment;
- Formally place all information under configuration management.

4 OUTPUT

- Input information describing the system design, as outlined in Section 2 above;
- Derived information (e.g., updated description of the operational environment, updated list of assumptions).

This page is intentionally left blank.



PSSA PLANNING

1 OBJECTIVE

The objective of the **PSSA Planning** step is to define the objectives and scope of the PSSA, 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 Report.

3 MAJOR TASKS

- Identify and describe the more specific activities for each PSSA step in a PSSA Plan;
- Submit the PSSA plan to peer review to provide assurance of its suitability;
- Submit the PSSA plan for comment or approval to interested parties (including regulatory authorities), as appropriate;
- Formally place the PSSA plan under configuration management;
- Disseminate the PSSA plan to all interested parties.

The PSSA Plan should:

- Define and describe the risk mitigation strategies to be used;
- Identify methods and techniques to be used in the PSSA part of the safety assessment;
- Identify interdependencies with the design phase;
- Define the schedule, transition criteria between PSSA steps, resources, responsibilities and deliverables.

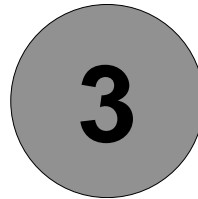
The PSSA Plan should justify how the planned PSSA activities will be conducted in the light of:

- The **safety impact** of the system: approaches appropriate to the severity of the effects and the probability of occurrence of these effects of the various identified hazards;
- The degree of **complexity** of the system;
- The **novelty** of the system: usage of new technologies or of conventional technologies 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 PSSA Plan.



SAFETY REQUIREMENTS SPECIFICATION

1 OBJECTIVE

The objective of the ***Safety Requirements Specification*** step is to derive Safety Requirements for each individual system element (People, Procedure and Equipment).

2 INPUT

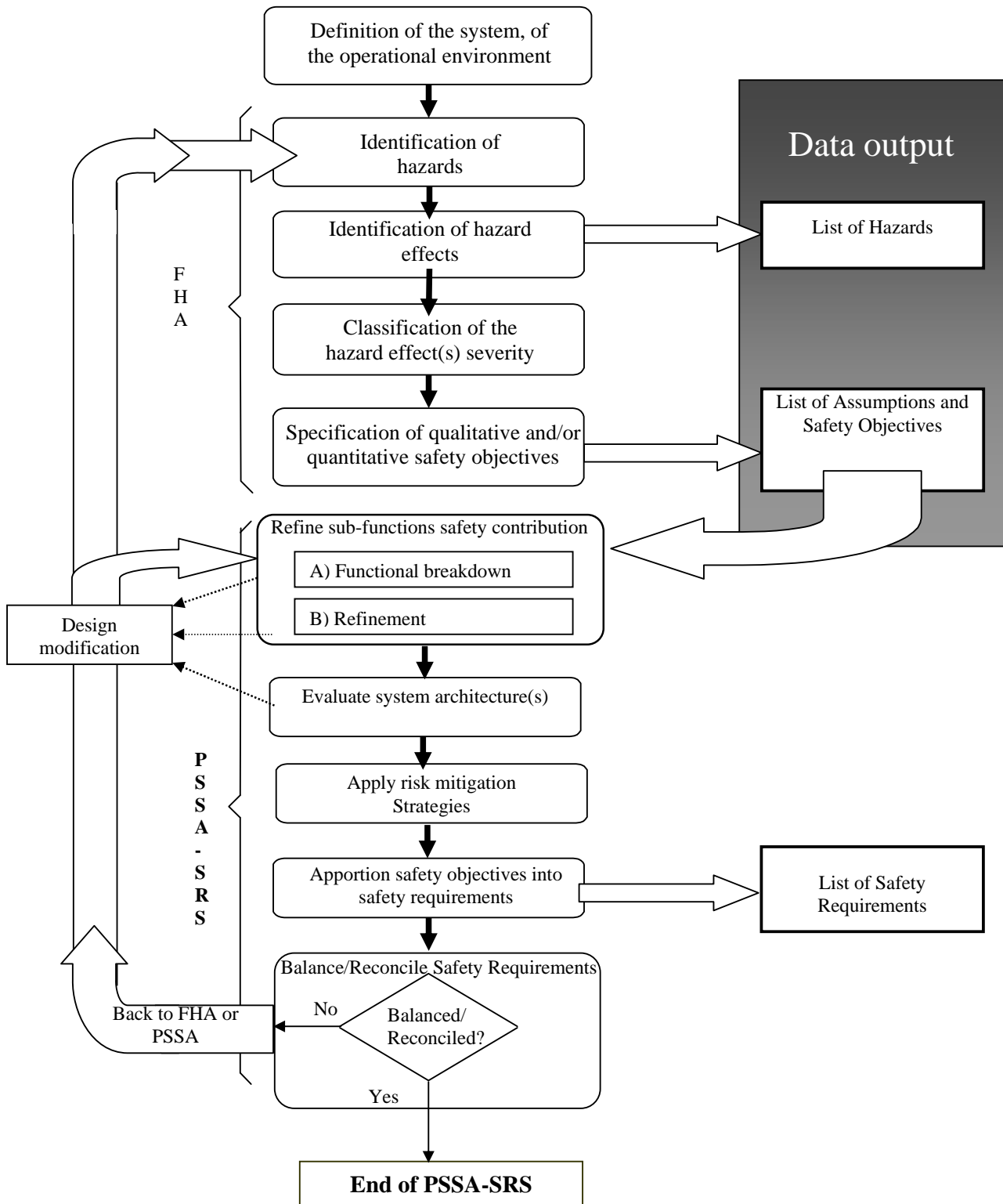
- PSSA Initiation output:
 - Description of the system architecture(s) and rationale;
 - The Operational Environment Description (OED);
 - The list of assumptions;
 - The list of hazards, with the rationale for the severity classification of their effects(s) (FHA output);
 - The Safety Objectives (FHA output);
- The risk mitigation strategies as stated in PSSA plan.

3 MAJOR TASKS

The five-stage process illustrated in Figure 3-1 is conducted as follows:

- Refine Sub-Functions Safety Contribution: What is the most stringent contribution of each sub-function to Safety Objectives_u (not only the most stringent Safety Objective)? See Section 3.1;
- Evaluate System Architecture(s): By evaluating alternative system architectures, PSSA determines: if and how the system can cause or contribute to the hazards and its effect(s) identified in the FHA? See Section 3.2;
- Apply Risk Mitigation Strategies: What can be done to eliminate, reduce or control hazards and their effect(s) by architectural means? See Section 3.3;
- Apportion Safety Objectives into Safety Requirements to System Elements: What is the part of the safety objectives to be allocated to architectural elements of the system? See Section 3.4;
- Balance/Reconcile Safety Requirements: Are Safety Requirements credible? See Section 3.5.

Figure 3.1: Safety Requirements Specification Process



3.1 Refine Sub-Functions Safety Contribution

The task is related to the definition (or refinement) of the system functional architecture: high level functions identified during the System Definition phase are successively decomposed into lower-level sub-functions.

Another way of asking the question: "What is the most stringent contribution of each sub-function to Safety Objectives (not only the most stringent Safety Objective)?" could be:

- "Are there some sub-functions, which are not part of the worst case? Then associate them with the relevant Safety Objective" or;
- "What is the most stringent Safety Objective dimensioning a sub-function?".

The functional breakdown is pursued until each sub-function becomes sufficiently defined to be allocated to a system element: Human, Procedure or Equipment (HW, SW). Moreover, new functions could be identified as a result of the design process. This functional breakdown allows identification of which sub-functions contribute (and the kind of contribution) to each safety objective.

The purpose of the task is:

- To refine 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 which contribute to it;
- To update the hazards and safety objectives lists established during FHA, by considering additional potential hazards and their effect(s) resulting from the failure of sub-functions.

3.2 Evaluate System Architecture(s)

The system architecture(s) evaluation consists of determining *if and how* architecture(s) and its elements could cause or contribute to identified hazards and assessing their effects in accordance with the Safety Objectives coming out of the FHA.

Hazards may arise as a result of:

	EXAMPLES
Normal System Operations	<ul style="list-style-type: none"> • Normal interactions between system elements; • System behaviour in response to extreme operational and environmental conditions; • Design characteristics of some system elements that may induce failures of other system elements. (i.e., automation design inducing ATCO errors).
Failures of System Elements	<ul style="list-style-type: none"> • Failures of individual system elements: latent and active failures; • Combination of latent and active failures, and external events; • Particular failure affecting other elements.

Common Cause of Failures	<ul style="list-style-type: none"> • Failure of common elements (i.e., failure of an operating system or a power supply); • Failure of physically adjacent systems (e.g. physical damage to telephone lines and power lines); • Failure resulting from a common design or implementation process (i.e., failure resulting from a compiler error).
Installation and Transition to Operations	<ul style="list-style-type: none"> • Hazards caused by the installation and transition into operations. (feasibility); • Hazards caused by means to revert to previous operations in case of a malfunctioning of the new system.

Various techniques could be used to help the safety analyst to assess the hazardous scenarios and to complement the FHA list. See SAM-Part IV Annex D.

3.3 Apply Risk Mitigation Strategies

Once the potential causes of hazards have been identified and associated risks evaluated, the system design may need to be modified to mitigate these risks.

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 §3).

Risk Mitigation Strategies address both:

- **Potential Causes of System Failures** By adopting a design approach that is aware of and minimises safety-related deficiencies in system elements.
- **Potential Consequences of System Failures and Hazards** By designing defensively and incorporating safeguards against the consequences of failure or hazard.

By adopting the following hierarchy of risk mitigation strategies, the aim is to reduce the risk to make it acceptable or at least as low as reasonably practicable while meeting the safety regulatory targets:

1. **Hazard Elimination** Hazards should, as far as it is consistent with operational objectives, be eliminated from the design, by the selection of the least hazardous design options and/or limiting operational usage.
2. **Hazard Reduction** If hazards cannot be eliminated, attempts should be made to reduce the frequency with which these hazards are expected to occur. This also includes the reduction of the frequency of failure to occur and the probability of failure(s) to become a hazard. Hazard reduction relies on design features such as fault tolerance for equipment element resistance or tolerance to human operational errors.
3. **Hazard Control** For remaining hazards (residual hazards), the design should ensure that, if a hazard does occur, it does not result in an unacceptable risk by reducing:
 - The probability of a hazard to become an accident or incident;
 - The severity of the hazard effect(s).

Hazard control requires, for example, the selection of recovery mechanisms and contingency procedures, or the implementation of design features for a timely detection of critical failure.

3.4 Apportion Safety Objectives into Safety Requirements

Once the architecture has been modified by applying risk mitigation strategies, final Safety Objectives apportionment can be performed and Safety Requirements can be specified for each individual system element.

This step includes allocation of Assurance Levels (to system elements: SW, Procedure, HW).

Additional Safety Requirements may be set to meet regulations or standards.

See Chapter 3 guidance material A.

Note: Apportioning Safety Objectives into Safety Requirements should be customised to the Operational Environment Description (e.g; en-route, TMA, tower, ...)

3.5 Balance/Reconcile Safety Requirements

The **Safety Requirements Specification** has been predominantly a top down approach. Interactions and overlaps within the overall system may have lead to some over stringent requirements.

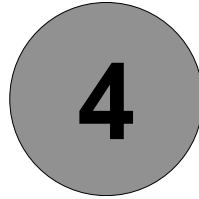
A bottom-up approach is therefore required from the low-level sub-functions to the high-level functions, in order to consolidate and adjust the requirements and to optimise the design. In this way the overlap of requirements, the over engineering and other constraints can be avoided.

As Safety Requirements may have been modified, PSSA needs to be re-iterated to ensure that these final Safety Requirements and this final architecture can reasonably be expected to achieve the Safety Objectives.

4 OUTPUT

- Updated list of assumptions;
- An updated list of identified hazards and safety objectives (new hazards may have been identified during the process and hazard scenarios (including their effect(s)) may have been refined);
- Safety analyses results;
- Justification material for risk mitigation strategies application;
- Safety Requirements on individual system elements and their rationale.

The output of the Safety Requirements Specification step should be formally placed under configuration management.



PSSA EVALUATION

1 OBJECTIVES

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

- Verification;
- Validation;
- Process Assurance.

The objective of **PSSA Verification** is to ensure that Safety Requirements meet Safety Objectives (“getting the output right”).

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

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

The objectives of **PSSA Process Assurance** are (“getting the process right and the right process”):

- To provide assurance and evidence that all PSSA activities (including PSSA Verification and PSSA Validation tasks) have been conducted according to the PSSA plan;
- To ensure that the PSSA process as described in the PSSA plan is correct and complete.

2 INPUT

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

3 MAJOR TASKS

3.1 PSSA Verification Task

The **PSSA Verification** tasks should include a review and analysis of the output of the PSSA (“getting the output right”).

3.2 PSSA Validation Task

The PSSA validation tasks should include:

- Review and analyse the Safety Requirements to ensure their completeness and correctness;
- Review and analyse the description of the operational environment to ensure its completeness and correctness;
- Review, analyse, justify and document critical assumptions about the system, its operational environment and its regulatory framework to ensure their completeness and correctness;
- Review and analyse traceability between Safety Objectives and Safety Requirements;
- Review and analyse the credibility and sensitivity of Safety Requirements with respect to the Safety Objectives and assumptions.

3.3 PSSA Process Assurance Task

The PSSA Process assurance tasks should at least ensure in accordance with the PSSA Plan that:

- The PSSA steps are applied;
- Assessment approaches (e.g. success approach, failure approach, use of safety methods and techniques such as Fault-Tree, FMEA, CCA, RBD...) are applied;
- All outputs of the PSSA steps (including PSSA Validation, PSSA Verification and PSSA Process Assurance) are formally placed under configuration management;

- Outcomes of PSSA Validation and PSSA Verification activities are formally placed under configuration management;
- Any deficiencies detected during PSSA Verification or PSSA Validation activities have been resolved;
- The PSSA process would be repeatable by personnel other than the original analyst(s);
- The findings have been disseminated to interested parties;
- Outputs of the PSSA process are not incorrect and/or incomplete due to deficiencies in the PSSA process itself.

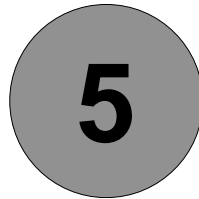
4 OUTPUT

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

The PSSA Evaluation output comprises:

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

This page is intentionally left blank.



PSSA COMPLETION

1 OBJECTIVE

The objectives of the *PSSA Completion* step are:

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

2 INPUTS

Outputs of all other PSSA steps.

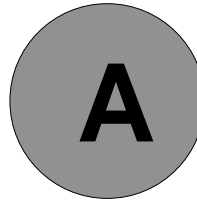
3 MAJOR TASKS

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

4 OUTPUT

- PSSA results formally placed under configuration management.

Guidance material-A of Chapter 5 suggests possible format for documenting the PSSA 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 PSSA can be performed.

The OED was already made during FHA, however some data have to be further detailed for the system design phase and its safety assessment (PSSA).

1 OPERATIONAL ENVIRONMENT DEFINITION FOR PSSA PURPOSE

Preliminary 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.

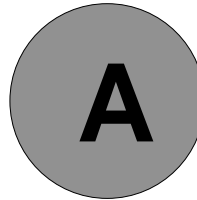
The description of the operational environment should include all characteristics, which may be relevant when assessing system architectures and their ability to meet safety objectives.

The minimum following information (additional to FHA'OED) should be provided:

- **Current ATM/CNS capabilities:** Detailed technical and operational performance and limitations of:
 - Equipment: technical specifications of the interface with the system being assessed:
 - either communication (Interface Requirement Specification) though Interface Control Document could be enough for FHA)
 - or Human Machine Interface (HMI): a user's manual or equivalent should be provided to start PSSA;
 - Navigation capability and performance (RNP, RNAV): PSSA-OED Should provide accuracy, precision, specifications;
 - Surveillance capability and performance (PSR, SSR, ADS): e.g. FHA-OED will say PSR+SSR though PSSA-OED will provide range coverage, exact area coverage (in case of obstacles, mountains), maximum number of tracks, accuracy, precision;
 - Communication capability and performance (voice and data-link): e.g. : FHA-OED will say "datalink", though PSSA-OED should say: datalink using VDL Mode 2 over ATN or using ACARS);
 - Proficiency of ATCOs;
 - Current procedures (operational, maintenance, etc.): procedures should be identified (decomposition into tasks, use of equipment, separation standards applied),
 - Use of safety nets (technical specification: algorithm, level of false alarms, time to react ,...);

- **Aircraft Performance and Equipment:**
 - aircraft technical requirements such as communication network, navigation performance, surveillance (transponder performance: Mode S, ...)
 - Aircraft operator specific performance: e.g. conformance to TCAS RA;
- **Adjacent Centre Capabilities:**
 - technical characteristics of ATC Unit with which traffic is exchanged (performances and limitations): FHA-OED will say coordination with adjacent centers, PSSA-OED should say “OLDI over X25” with a specified Quality of Service);
 - Detailed operational performance: Letter of Agreement specification (description of various roles, communication means, recovery, emergency aspects), specification of coordination procedure between centres (task decomposition, equipment interface specification, ...)
- **Airport Infrastructure:** e.g. detailed and technical specification of airport movement infrastructure (A-SMGCS, communication equipment, ..), specification of visual aids, airport movement procedure (decomposition into tasks, usage of equipment, emergency & recovery aspects, ..).

This page is intentionally left blank.



CHAPTER 2 GUIDANCE MATERIAL:

PLANNING PSSA ACTIVITIES

1 INTRODUCTION

The purpose of this annex is to provide guidance on how to plan PSSA activities. These recommendations aim at completing the part of the safety plan dealing with PSSA.

This guidance material outlines the tasks involved in defining the approach to safety within the PSSA itself.

A.1 PSSA Objectives and Scope

- Define the objectives of the Preliminary System Safety Assessment; and how these will contribute to overall safety assessment for the system.
- Define the scope and level of the PSSA. For example:
 - Different levels of PSSA could be conducted, dependent on whether certain functions have already been allocated to particular system elements;
 - A specific PSSA could be conducted to cover the transition between the current and future operations.

A.2 PSSA Process

- Identify the inputs to the PSSA process (drawing on the material gathered under the PSSA Initiation step, as described in Chapter 1).
- Define the methodology to be used for apportioning Safety Objectives into Safety Requirements. This should describe any necessary adaptations of the generic PSSA process for the specific application. For example:
 - Define the approach to be used when apportioning Safety Objectives into Safety Requirements (e.g., whether these are to be absolute or relative);
 - Outline methods used to identify risk mitigation means, drawing on information gathered in the Initiation stage regarding methods which were successful in past PSSA sessions.
 - Outline methods used to apportion Safety Objectives into Safety Requirements (namely: FMEA, Fault-Tree, Event-Tree, Bow-Tie, ...) drawing on information gathered in the Initiation stage regarding methods which were successful in past PSSA sessions.
- Specify the type and attributes of the information to be recorded in the PSSA process.
- Specify the structure of the required output of the PSSA process.

A.3 PSSA Evaluation Activities

- Define the PSSA validation, verification and process assurance activities to be performed (see Chapter 4 for further guidance).
- Identify specific methods to be applied.
- Specify information to be collected.
- Define the procedures to be applied if flaws are detected during any of the evaluation activities.

A.4 Roles and Responsibilities

- Define the roles and responsibilities of the persons, departments and organisations involved in the PSSA process in particular in order to ensure that adequate coordination is performed for Safety Requirements specification (apportionment and allocation) such as:
 - regulatory bodies for ATM, airworthiness and flight operations;
 - ANSPs (including ATCOs);
 - Airlines (including aircrew);
 - Aircraft and aircraft equipment manufacturers;
 - ANSP equipment manufacturers;
 - Any other required bodies (such as Communication Service Providers, ...).
- Specify the required competencies for the persons involved in the PSSA process, and any necessary training requirements.

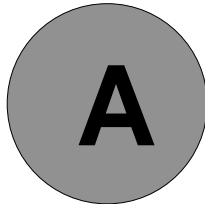
A.5 Schedule and Resource Allocation

- Define the time schedule and resources required.

A.6 Planning for Future Activities

Define the procedures to be applied when changes are made to Safety Requirements, system architecture, operational environment or system interfaces. Defining adequate lines of communication is particularly important – safety assessors need to be informed of such changes.

This page is intentionally left blank.



CHAPTER 3 GUIDANCE MATERIAL:

SAFETY REQUIREMENTS

1 INTRODUCTION

The purpose of this annex is to provide guidance material on the definition, content, phrasing, criteria of eligibility of safety requirements.

2 MORE DETAIL ABOUT SAFETY REQUIREMENTS

2.1 General

Safety requirements are derived from Safety Objectives. Generally, they specify the potential means to mitigate hazards, i.e. to:

- Prevent occurrence of hazards; associated means are:
 - Precautions for system & equipment design, development, procurement and validation
 - Precautions for procedures design and validation
 - Precautions for people training and licensing
- Reduce the severity of their consequences; associated means are addressing:
 - Detection,
 - Protection, (e.g. software barriers and checkings)
 - Recovery (automatic or human intervention; e.g. provide an automatic switch main/fall-back system or specify an operator manual procedure to activate the fall-back system),
 - Graceful degradation (deliver a reduced service in Degraded mode; e.g. specific procedures while in degraded mode, specific operator training for the degraded mode situations, ...),
 - Other.

The term "Safety Requirement" encompasses both:

- safety related requirements to be met by the system as a "product" and
- those safety related actions to be performed through the processes associated to that product.

Thus Safety Requirements include:

- System and element safety requirements derived from quantitative and qualitative Safety Objectives along the safety assessment process (mainly the FHA and PSSA phases), that have to be integrated in the System Specification and System Design documents

(for the HW and SW), in the Training manual (for Human element) or Operating manual (for Procedures element)

- Completion or modification of already existing system requirements (functional, performance, interoperability), in order to ensure compliance with Safety Objectives,
- Specific "safety evidence demands" (stemmed from the approved recommendations issued along the safety assessment process), to be satisfied in the different stages of the product life-cycle, inside the safety assessment process, or externally but correlated to it. Those "safety evidence demands" might concern:
 - Analysis activities to be addressed by the safety assessment itself (e.g. perform a detailed FMEA or perform a reliability prediction for a specific component in order to ensure that the occurrence rate associated to its failure is acceptable; perform a detailed Human Error analysis for a specific procedure) or
 - Analysis activities external to the safety assessment: Code inspection, Maintenance analysis, Operating Procedure analysis, Training analysis, Transition analysis, specific technical assessments (e.g. electromagnetic compatibility, system behaviour under overloaded conditions, R/F frequency interference and jamming, etc.). These activities are identified during FHA, PSSA or SSA phases and their safety related output is collected during those phases and consolidated by the SSA.
 - Assurance levels for SW and HW covering the different stages of the development process: (e.g. SW Development assurance levels), or specific development precautions to be applied for reducing the likelihood of the occurrence of certain failures,
 - Testing activities, defined for the verification of safety objectives and requirements and of assumptions on which certain safety objectives and requirements were founded. Tests have to be integrated in the Unit, System Integration or Factory acceptance tests plans. Safety related issues of those tests might be specified during the FHA and mostly during the PSSA phase, and then verified during Implementation & Integration, when SSA collects and interprets safety related results. Moreover, Site Acceptance tests might cover some safety validation aspects with respect to users expectations, additionally to verification. Safety related issues of these latter tests are specified during the FHA, PSSA and SSA phases and are verified and, as far as feasible, validated, during Transfer to operations, when SSA collects and interprets safety-related results.

- Simulation activities, defined for the verification of safety objectives and requirements, associated assumptions, and as far as feasible, for validation of those aspects with respect to users' expectations. Safety issues to be addressed by simulation might be specified during the FHA, PSSA and SSA phases, simulations might be performed any time before Transfer to operations, and SSA collects and interprets safety-related results,
- Demonstration activities, mainly represented by safety-related aspects addressed during trials, aimed at the system safety validation with respect to users' expectation and at the confirmation of some assumption validity. Safety issues to be addressed by trials might be specified during the FHA, PSSA and SSA phases, trials might be performed any time before Transfer to operations, and SSA collects and interprets safety-related results,
- Examination activities, represented by inspections, audits and reviews, can be performed all along the system lifecycle.

In conclusion, some Safety Requirements are intended to directly contribute to the reduction of the risk associated to specific hazards, whilst others represent safety evidence demands, which once satisfied, provide evidence that specific safety requirements are met or that associated assumptions are well founded.

Each Safety Requirement has to be recorded and made traceable to the Safety Objective (and consequently the hazard(s)) that justifies its definition.

The implementation of Safety Requirements has to be monitored along the safety assessment process and traced in SSA documents (usually the Hazard Log). Demands for Safety Evidence will have to be satisfied at different stages of the product life cycle, then their results will be collected and integrated by the SSA process.

2.2 People

People (human) element safety requirements address:

- The training process (specific safety-related aspects to be addressed by manuals, simulations, etc. or by the organisation of that process), including the competency and performance checking
- The licensing process,
- The staffing levels, rostering, call-out arrangements, specific skills/qualifications required for systems operation and maintenance, etc.

Note that HMI safety requirements concern the equipment, although their specification and verification & validation is strongly connected to the human element.

Generally, Safety Requirements for Human Element will take the form of training requirements for using the new automated system or procedure.

In a highly automated environment, the training of ATCO should address the functioning of the automated system as well as its limitations (to avoid over reliance on the automated system).

Hazard analysis results should be used also in ATCO training to point out potential hazards and how they are controlled in the design of the automated system or operational procedures.

2.3 Procedures

Procedure safety requirements address:

- Procedures design constraints and recommendations (e.g. provide a recovery action inside a safety related procedure, like "pilot should readback clearance"; design a specific fall-back procedure to cope with a system degradation, etc.),
- The procedures development and verification & validation process.

SAAP (Safety Assessment of ATM Procedures) is in charge of developing the Procedure Assurance Level.

The part of SAAP dealing with the allocation of PAL is the following:

The following steps should be performed to allocate a PAL:

1. Identify the likelihood that, once the procedure fails, this procedure failure can generate an end effect which has a certain severity (do that for each effect of a hazard) (See figure 2.3.1);
2. Identify the PAL for that couple (severity, likelihood) using the matrix here after;
3. This has to be done for all the hazards due to the procedure.

The final PAL of an ATM procedure is the most stringent one.

Effect Severity	1	2	3	4
Likelihood of generating such an effect				
Very Possible	PAL1	PAL2	PAL3	PAL4
Possible	PAL2	PAL3	PAL3	PAL4
Very Unlikely	PAL3	PAL3	PAL4	PAL4
Extremely Unlikely	PAL4	PAL4	PAL4	PAL4

Note: It should be noted that PAL1 is so stringent that it should nearly never be allocated for the following reasons:

1. PAL1 means somehow that the procedure “can directly kill once it fails” as having a Severity1 effect is “Very Possible” (very limited means to mitigate procedure failure(s). This can only be tolerable in extremely exceptional circumstances;
2. PAL1 is so demanding to be satisfied. As the objectives and associated evidences are so stringent, the cost and development duration and effort are very high;
3. Allocating PAL1 means that an extremely low level of performance is accepted. The procedure will be requiring such separation minima, such safety margin, such operational checking that it will be acceptable to use it to expedite traffic only in extremely exceptional circumstances.

It could be the same for PAL2 with of course less stringency. That is why an objective for PAL 1&2 requests to have the Senior Management signing it (CEO for PAL1 and Director of Operations for PAL2)... because this kind of procedure should not be the recommended practise.

This means that mainly PAL3 and PAL4 will be allocated.

Very Possible: This effect will certainly occur due to procedure failure.

Possible: This effect may happen (it is not unreasonable to expect such effect to happen due to procedure failure).

Very Unlikely: it is not expected to have such an effect more than exceptionally and in some extreme cases throughout the system lifetime.

Extremely Unlikely: Such an effect is not expected to happen throughout the system lifetime.

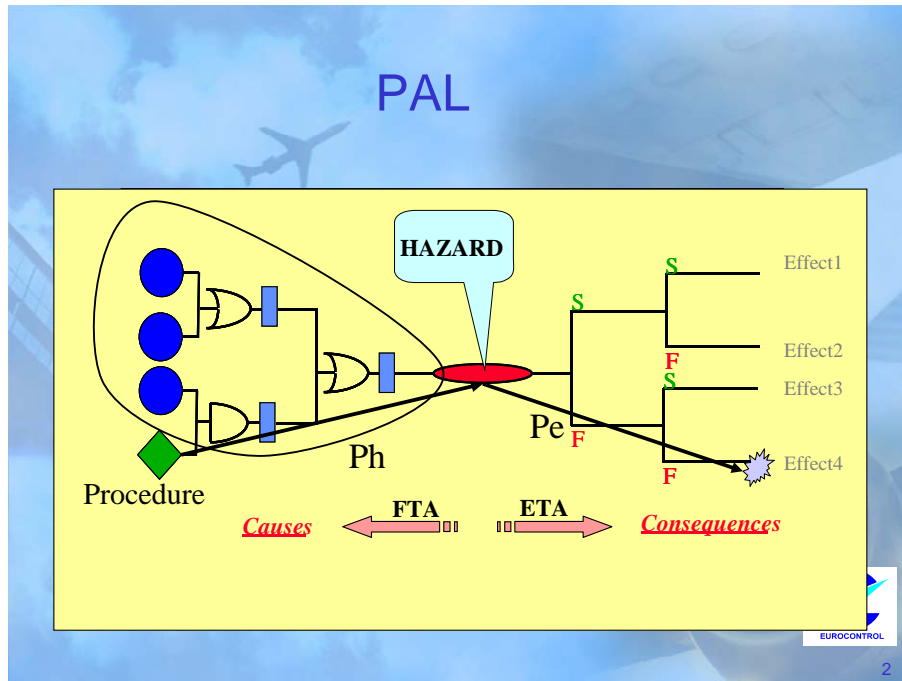



Figure 2.3.1: Relationship between Procedure failure, hazard and effects.


Example of PAL allocation: This procedure will be allocated a PAL = PAL3 as it the most stringent (for both hazards).

1st CASE: Safety Objectives were allocated using Method 1 or 3 (See FHA Chapter 3 Guidance Material G “Methods for Setting Safety Objectives). So all effects, due to ATM Procedure failure, are taken into consideration.

This Procedure will be allocated a PAL = PAL3 as it is the most stringent PAL (for both hazards).

Effect Severity	1	2	3	4
Likelihood of generating such an effect				
Very Possible	PAL1	PAL2	PAL3	PAL4
Possible	PAL2	PAL3	PAL3	PAL4
Very Unlikely	PAL3	PAL3	PAL4	PAL4
Extremely Unlikely	PAL4	PAL4	PAL4	PAL4

Procedure error leading to Hazard1: 

Procedure error leading to Hazard2: 

The way to read the table is the following:

For Hazard 1:

- If it is “Extremely Unlikely” that once the procedure fails, it generates Hazard1 and an effect having a severity 1, then this procedure should be allocated a PAL4;
- If it is “Possible” that once the procedure fails, it generates Hazard1 and an effect having a severity 2, then this procedure should be allocated a PAL3;
- If it is “Very Possible” that once the procedure fails, it generates Hazard1 and an effect having a severity 3, then this procedure should be allocated a PAL3;
- If it is “Very Possible” that once the procedure fails, it generates Hazard1 and an effect having a severity 4, then this procedure should be allocated a PAL4;


For Hazard 2:


- If it is “Extremely Unlikely” that once the procedure fails, it generates Hazard2 and an effect having a severity 1, then this procedure should be allocated a PAL4;
- If it is “Extremely Unlikely” that once the procedure fails, it generates Hazard2 and an effect having a severity 2, then this procedure should be allocated a PAL4;
- If it is “Very Unlikely” that once the procedure fails, it generates Hazard2 and an effect having a severity 3, then this procedure should be allocated a PAL4;
- If it is “Possible” that once the procedure fails, it generates Hazard2 and an effect having a severity 4, then this procedure should be allocated a PAL4.

2nd CASE: Safety Objectives were allocated using Method 2 or 4 (See FHA Chapter 3 Guidance Material G “Methods for Setting Safety Objectives). So only the worst credible scenario which has been used to set safety objectives is taken into consideration.

This ATM Procedure will be allocated a PAL = PAL3 as it is the most stringent PAL (for both hazards which have a worst credible hazard effect having a severity 3).

Effect Severity	1	2	3	4
Likelihood of generating such an effect				
Very Possible	PAL1	PAL2	PAL3	PAL4
Possible	PAL2	PAL3	PAL3	PAL4
Very Unlikely	PAL3	PAL3	PAL4	PAL4
Extremely Unlikely	PAL4	PAL4	PAL4	PAL4

Procedure error leading to Hazard1: 

Procedure error leading to Hazard2: 

The way to read the table is the following:

For Hazard 1: As the Worst Credible effect of Hazard 1 has a Severity 3 (FHA result), then

- If it is “Very Possible” that once the procedure fails, it generates Hazard1 and an effect having a severity 3, then this procedure should be allocated a PAL3;

For Hazard 2: As the Worst Credible effect of Hazard 1 has a Severity 3 (FHA result), then

- If it is “Very Unlikely” that once the procedure fails, it generates Hazard2 and an effect having a severity 3, then this procedure should be allocated a PAL4.

2.4 Equipment

Product safety requirements include system or component architecture constraints & recommendations (protection, detection, recovery, degraded mode strategy, type of fault tolerance mechanism), and operational contingencies (operational limitations, preventative and corrective maintenance).

Example of issues that might be subject to product safety-related requirements for a HW component:

- Power-up/Power-down,
- Input/output control,
- Operation at the limits,
- Error detection and processing,
- Main/fallback switch-over,
- System degraded modes and transition to/from nominal mode,
- HW watchdog,
- Etc.

Example of issues that might be subject to product safety-related requirements for a SW component:

- Initialisation/stop,
- Input/output control,
- Interface/control of the data flow,
- Data integrity,
- Data management,
- Operation at the limits,
- Error detection and processing,
- Master/slave switch-over,
- Main/fallback switch-over,
- System degraded modes and transition to/from nominal mode,
- HW support,
- Memory sizing and timing,
- FIFOs and buffers,
- Interruptions,
- SW watchdog,
- Etc.

Process safety requirements include specific actions and precautions to be taken during development, verification of implementation or testing (unit, integration, Factory acceptance or Site acceptance). For the Software, the Assurance levels associated to the design, development and verification & validation activities allow to systematically assign a set of process safety requirements to a component, in function of the level of severity associated to its failure (see [EUROCONTROL/Recommendations for ANS SW]).

Equipment safety requirements might be qualitative or quantitative.

Quantitative safety requirements might be deterministic or probabilistic.

- Deterministic: time to switch-over, maximum tolerable time of service interruption, maximum tolerable time for a maintenance intervention, etc;
- Probabilistic:
 - Safety (freedom of 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 and requirements, at a higher level, result into lower level requirements addressing reliability, availability, integrity, and maintainability through allocation process.

2.4.1 Hardware Safety Requirements

The safety requirements allocated to hardware elements of the architecture can be directly derived from the quantitative approach by applying Fault Tree Analysis for example and using the result of the decomposition of the safety objective.

Similar to the assurance levels for SW, HW Assurance Levels are being defined.

2.4.2 Software Assurance Level (SWAL)

2.4.2.1 SWAL Basics

A specific Safety Requirement for software consists in identifying a SoftWare Assurance Level (SWAL), which intends to provide the level of confidence that risks associated with the use of software in safety related ground-based ATM systems, are reduced to an acceptable level.

A SWAL establishes a level of confidence that the overall software lifecycle has been conducted in a sufficiently disciplined manner to limit the likelihood of development errors that could impact safety during operations.

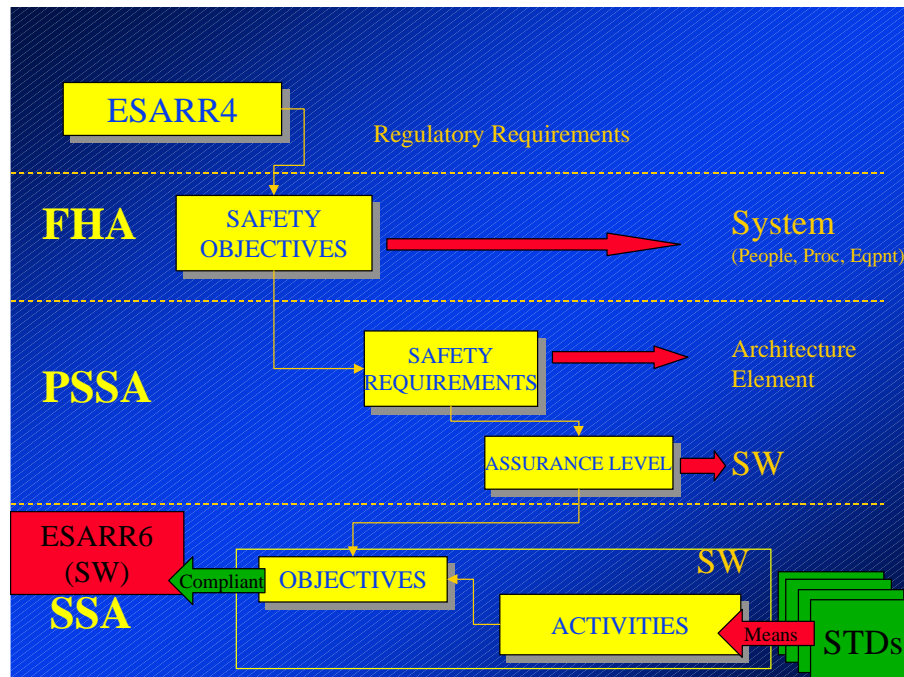


Figure 2.4.2.1: Software Assurance Level allocation

The first step to allocate a SWAL (SoftWare Assurance Level) consists in identifying the (sub-)function embedding/encapsulating this software and its associated safety requirements.

Basics of Mitigation Means Influence

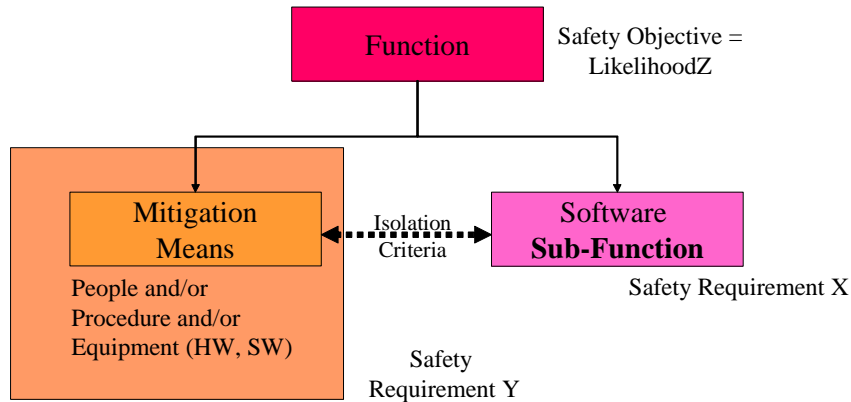


Figure 2.4.2.2: Basics of Mitigation Means Influence

As shown in Figure 2.4.2.2, “Mitigation means” are any kind of internal means (people and/or procedures and/or equipment) designed to control or prevent failures from causing harm and to reduce the expected effects of failures and hazards to a tolerable or acceptable level. In Figure 2.1.1, “Mitigation Means” encompass all the other sub-functions that are part of the function (that has a safety Objective “LikelihoodZ”) and complement the “SW sub-function” to which a SWAL is being allocated.

Figure 2.4.2.2 intends to show that the SWAL definition is commensurate with the Safety Requirements allocated to the software sub-function and not with the Safety Objective of the overall function.

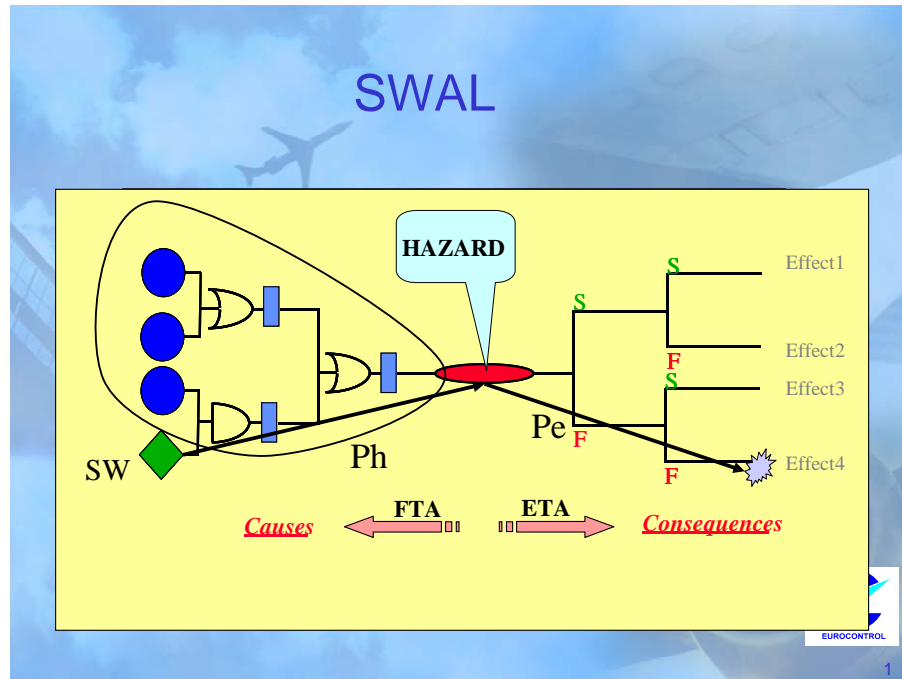


Figure 2.4.2.3: Relationship between SW failure, hazard and effects.

The likelihood ($Ph \times Pe$) that, once software fails, this software failure could generate a certain effect is illustrated in the above figure 2.4.2.3:

- Ph is the probability that, once software fails, this software failure generates a hazard. Ph is commensurate with the ability (probability) of the remaining part of the architecture to mitigate the software failure;
- Pe is the probability that the hazard generates an effect having a certain severity.

Depending on the method used to set Safety Objectives (See Sam-FHA Chapter 3 Guidance material G) there can be:

- Many Pe probabilities (one Pe per effect of the hazard), to be assessed for each individual effect (when using method 1 or 3 for setting Safety Objectives) or;
- Only one probability Pe (one for the worst credible effect when using method 2 & 4 for setting Safety Objectives).

As it can be difficult to quantify accurately and precisely these probabilities, expert judgement and other means (database, lessons learned, incidents reports) can be used to set those probabilities. Of course as part of the SAM-SSA, appropriate monitoring has to be put in place to ensure that these values are satisfied.

2.4.2.2 SWAL Allocation process

The following steps should be performed to allocate a SWAL (See Recommendations for ANS SW):

1. Identify the likelihood that, once Software fails, this software failure can generate an end effect which has a certain severity (do that for each effect of a hazard) (See figure 2.4.2.3) ;
2. Identify the SWAL for that couple (severity, likelihood) using the matrix here after;
3. This has to be done for all the hazards due to the software.

The final SWAL of software is the most stringent one.

Effect Severity	1	2	3	4
Likelihood of generating such an effect				
Very Possible	SWAL1	SWAL2	SWAL3	SWAL4
Possible	SWAL2	SWAL3	SWAL3	SWAL4
Very Unlikely	SWAL3	SWAL3	SWAL4	SWAL4
Extremely Unlikely	SWAL4	SWAL4	SWAL4	SWAL4

Very Possible: This effect will certainly occur due to software failure.

Possible: This effect may happen (it is not unreasonable to expect such effect to happen due to software failure).

Very Unlikely: it is not expected to have such an effect more than exceptionally and in some extreme cases throughout the system lifetime.

Extremely Unlikely: Such an effect is not expected to happen throughout the system lifetime.

Note: It should be noted that SWAL1 is so stringent that it should nearly never be allocated for the following reasons:


1. SWAL1 means somehow that software “can directly kill once it fails” as having a Severity1 effect is “Very Possible” (very limited means to mitigate SW failure(s). This can only be tolerable in extremely exceptional circumstances;
2. SWAL1 is so demanding to be satisfied. As the objectives and associated evidences are so stringent, the cost and development duration and effort are very high.


2.4.2.3 Example of SWAL allocation

1st CASE: Safety Objectives were allocated using Method 1 or 3 (See FHA Chapter 3 Guidance Material G “Methods for Setting Safety Objectives). So all effects due to Software failure are taken into consideration.

This Software will be allocated a SWAL = SWAL3 as it is the most stringent SWAL (for both hazards).

Effect Severity	1	2	3	4
Likelihood of generating such an effect				
Very Possible	SWAL1	SWAL2	SWAL3	SWAL4
Possible	SWAL2	SWAL3	SWAL3	SWAL4
Very Unlikely	SWAL3	SWAL3	SWAL4	SWAL4
Extremely Unlikely	SWAL4	SWAL4	SWAL4	SWAL4

SW failure leading to Hazard1: 

SW failure leading to Hazard2: 

The way to read the table is the following:

For Hazard 1:

- If it is “Extremely Unlikely” that once SW fails, it generates Hazard1 and an effect having a severity 1, then this SW should be allocated a SWAL4;
- If it is “Possible” that once SW fails, it generates Hazard1 and an effect having a severity 2, then this SW should be allocated a SWAL3;
- If it is “Very Unlikely” that once SW fails, it generates Hazard1 and an effect having a severity 3, then this SW should be allocated a SWAL3;
- If it is “Very Possible” that once SW fails, it generates Hazard1 and an effect having a severity 4, then this SW should be allocated a SWAL4;


For Hazard 2:


- If it is “Extremely Unlikely” that once SW fails, it generates Hazard2 and an effect having a severity 1, then this SW should be allocated a SWAL4;
- If it is “Extremely Unlikely” that once SW fails, it generates Hazard2 and an effect having a severity 2, then this SW should be allocated a SWAL4;
- If it is “Very Unlikely” that once SW fails, it generates Hazard2 and an effect having a severity 3, then this SW should be allocated a SWAL4;
- If it is “Possible” that once SW fails, it generates Hazard2 and an effect having a severity 4, then this SW should be allocated a SWAL4.

2nd CASE: Safety Objectives were allocated using Method 2 or 4 (See FHA Chapter 3 Guidance Material G “Methods for Setting Safety Objectives). So only the worst credible scenario which has been used to set safety objectives is taken into consideration.

This Software will be allocated a SWAL = SWAL3 as it is the most stringent SWAL (for both hazards which have a worst credible hazard effect having a severity 3).

Effect Severity	1	2	3	4
Likelihood of generating such an effect				
Very Possible	SWAL1	SWAL2	SWAL3	SWAL4
Possible	SWAL2	SWAL3	SWAL3	SWAL4
Very Unlikely	SWAL3	SWAL3	SWAL4	SWAL4
Extremely Unlikely	SWAL4	SWAL4	SWAL4	SWAL4

SW failure leading to Hazard1: 

SW failure leading to Hazard2: 

The way to read the table is the following:

For Hazard 1: As the Worst Credible effect of Hazard 1 has a Severity 3 (FHA result), then

- If it is “Very Possible” that once SW fails, it generates Hazard1 and an effect having a severity 3, then this SW should be allocated a SWAL3;

For Hazard 2: As the Worst Credible effect of Hazard 1 has a Severity 3 (FHA result), then

- If it is “Very Unlikely” that once SW fails, it generates Hazard2 and an effect having a severity 3, then this SW should be allocated a SWAL4.

Non-ATM example of allocation of SWAL

System: Navigation system (Hardware and software) in a car using GPS signal:

Assuming that the Severity Classification Scheme defines severity classes as following:

Severity Class 1: Accident

- Death (drivers and occupants and maybe other vehicle occupants or pedestrians);
- Vehicle(s) destroyed.

Severity Class 2: Serious Incident

- Serious injuries (maybe one death);
- Car destroyed.

Severity Class 3: Major Incident

- Major injuries;
- Car damaged.

Severity Class 4: Significant Incident

- Stress, increase of workload to recover the situation;
- Possibly minor car damages.

1°) Navigation system used for indication (as it is today)

OED (Operational Environment Definition): The following operational environment is assumed:

- Drivers have a driving license;
- Drivers have a good vision;
- Drivers have a situational awareness: other traffic, road signals (continuous line, one-way indication, priority signs, ...), direction indication;
- Drivers know their final destination and the navigation system is used only for indication (as described in the User's Manual);
- Road regulations exist and are known by drivers.

Assuming that operational environment, let's assess the following hazard:

- Hazard1: Undetected credible corruption of direction indication (provided by navigation system).

When looking at all effects to allocate a SWAL:

Effect Severity	1	2	3	4
Likelihood of generating such an effect				
Very Possible	SWAL1	SWAL2	SWAL3	SWAL4
Possible	SWAL2	SWAL3	SWAL3	SWAL4
Very Unlikely	SWAL3	SWAL3	SWAL4	SWAL4
Extremely Unlikely	SWAL4	SWAL4	SWAL4	SWAL4

- It is “Extremely Unlikely” that once SW fails, it generates Hazard1 and an effect having a severity 1, then this SW should be allocated a SWAL4 as:
 - The driver controls his/her car and has to assess the credibility of the indication before applying it and so will not apply it (See OED). Thus the probability of applying a credibly corrupted indication is “Extremely Unlikely”;
- It is “Extremely Unlikely” that once SW fails, it generates Hazard1 and an effect having a severity 2, then this SW should be allocated a SWAL4 as;
 - The driver controls his/her car and has to assess the credibility of the indication before applying it (See OED). Thus the probability of applying a credibly corrupted indication is “Extremely Unlikely”;
- It is “Extremely Unlikely” that once SW fails, it generates Hazard1 and an effect having a severity 3, then this SW should be allocated a SWAL4 as:
 - The driver controls his/her car and has to assess the credibility of the indication before applying it (See OED). Thus the probability of applying a credibly corrupted indication is “Extremely Unlikely”;
- It is “Very Possible” that once SW fails, it generates Hazard1 and an effect having a severity 4, then this SW should be allocated a SWAL4 as:
 - The driver spends some time assessing the indication applicability, so it increases driver workload, may stress him/her. Maybe the physical location of the car is not the expected one, but this is impacting performance not safety.

As a conclusion, as far as the hazard “credible corruption of navigation system indication” is concerned, the SWAL allocated to the Navigation system in the OED as described is:

- **SWAL4.**

2°) Navigation system in command (futuristic use)

OED (Operational Environment Definition): The following operational environment is assumed:

- Drivers have to apply navigation system command;

- Drivers are only monitoring the system;
- Drivers do not need a situational awareness: other traffic, road signals (continuous line, one-way indication, priority signs, ...), direction indication. Cars may not have windows!;
- Drivers have only to enter their final destination into the navigation system (as described in the User's Manual);
- Road regulations exist and are known by navigation system.

Assuming that operational environment, let's assess the following hazard:

- Hazard1: Undetected credible corruption of direction command (provided by navigation system).

When looking at all effects to allocate a SWAL:

Effect Severity	1	2	3	4
Likelihood of generating such an effect				
Very Possible	SWAL1	SWAL2	SWAL3	SWAL4
Possible	SWAL2	SWAL3	SWAL3	SWAL4
Very Unlikely	SWAL3	SWAL3	SWAL4	SWAL4
Extremely Unlikely	SWAL4	SWAL4	SWAL4	SWAL4

- It is "Very Possible" that once SW fails, it generates Hazard1 and an effect having a severity 1, then this SW should be allocated a SWAL1 as:
 - The driver applies the Navigation system command (See OED). Thus the probability of applying a credibly corrupted indication that can kill the driver (and other occupants and maybe other vehicle occupants) is "Very Possible";
- It is "Very Possible" that once SW fails, it generates Hazard1 and an effect having a severity 2, then this SW should be allocated a SWAL2 as:
 - The driver applies the Navigation system command (See OED). Thus the probability of applying a credibly corrupted indication that can seriously injure the driver (and other occupants and maybe other vehicle occupants) and destroys the car is "Very Possible";
- It is "Very Possible" that once SW fails, it generates Hazard1 and an effect having a severity 3, then this SW should be allocated a SWAL3 as:
 - The driver applies the Navigation system command (See OED). Thus the probability of applying a credibly corrupted indication that can seriously injure the driver (and other occupants and maybe other vehicle occupants) and destroys the car is "Very Possible";
- It is "Very Possible" that once SW fails, it generates Hazard1 and an effect having a severity 4, then this SW should be allocated a SWAL4 as:

- The driver applies the Navigation system command (See OED). Thus the probability of applying a credibly corrupted indication that can stress the driver (and other occupants and maybe other vehicle occupants) and damages the car is “Very Possible”.

As a conclusion, as far as the hazard “credible corruption of navigation system indication” is concerned, the SWAL allocated to the Navigation system in the OED as described is:

- **SWAL1.**

2.4.2.4 SWAL, Objectives, Activities & Evidences

These Software Assurance Levels (SWAL) are designed to provide a level of confidence that the software will be developed and can be integrated in the equipment and then in the system in order to manage risks due to software failure.

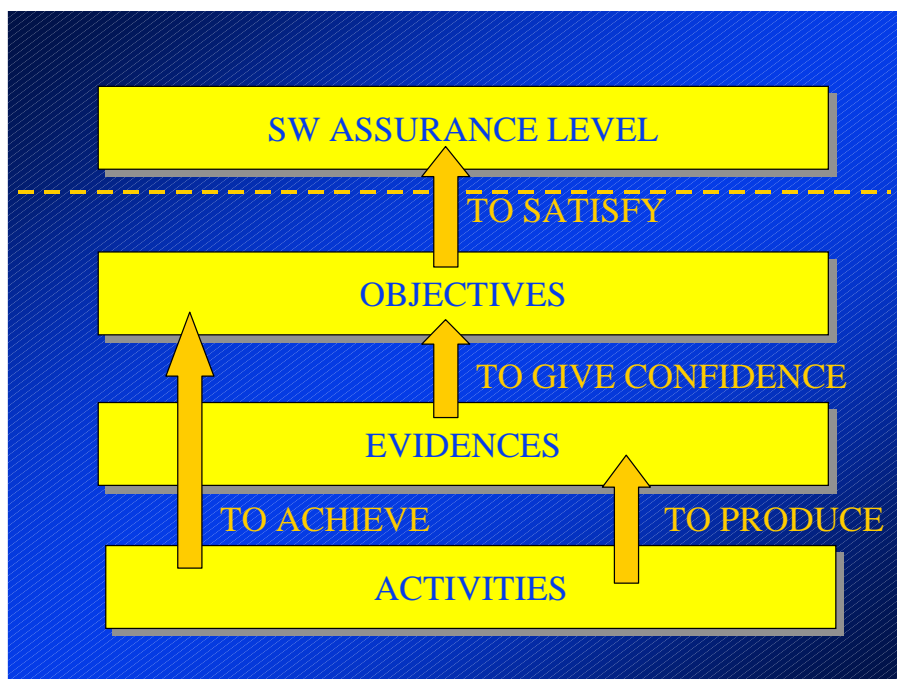
The way to provide this level of confidence and assurance is by defining some objectives that will satisfy this level of assurance.

These objectives address the software acquisition, development, integration, maintenance, operation, ... processes of the software lifecycle and identify what is to be done to satisfy a level of assurance;

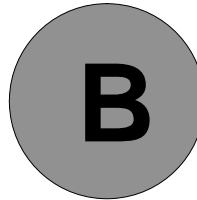
These objectives intend to give confidence that the assurance level is satisfied by showing evidences.

These evidences are produced by activities, which achieve these objectives. Different activities can produce different evidences, which are acceptable to satisfy objectives. However the same evidence can be produced by different activities. Activities define how to achieve objectives and to satisfy a level of assurance.

Figure 2.4.2.4: SW AL/Objectives/Evidences/Activities links



This page is intentionally left blank.



CHAPTER 3 GUIDANCE MATERIAL:

AUTOMATION

0 INTRODUCTION

The purpose of this annex is to provide recommendations on how to address automation especially when looking at its influence on the design and its safety-related aspects.

1 INTRODUCTORY MATERIAL

1.1 Definition

Automation is replacement of a human function, either manual or cognitive, with a machine function (usually a computer).

What is considered automation will therefore change with time. When the reallocation of a function from human to machine is complete and permanent, then the function will tend to be seen simply as a machine operation, not as automation.

1.2 Purpose of automation in ATM/CNS

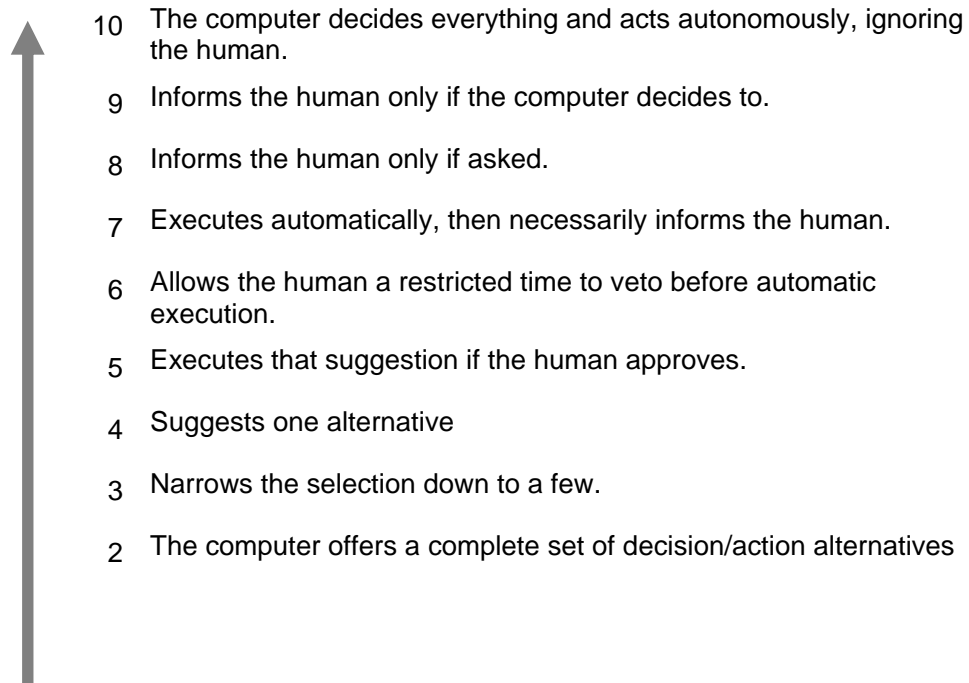
Automation is viewed as a viable and a requisite approach to comply with the demands for increased efficiency and improved safety.

Automation is introduced in ATM/CNS:

- To improve safety and to lessen the risk of a human error by reducing the ATCO's high mental workload;
- To increase efficiency, in order to accommodate the foreseen growth of traffic.

1.3 Levels of Automation

Levels of automation - decision and control action



- 1 The computer offers no assistance: the human must take all decisions and actions

1.4 Potential Problems

Automation does not supplant human activity; rather it changes the nature of the human work – often in a way that is not intended by the designers of automation.

Automation demands use of different resources - resources that in some areas require fundamentally different skills, procedures etc. - could be considered as a more demanding role.

While the positive impact of automation on safety and efficiency is undeniable, some new and potentially serious issues may arise as a consequence of the way humans interact with automation.

The following items are some of the problems to be aware of in an automated environment:

- If the human operator is not aware of the automation level, loss of system awareness will occur.
- If the human approach to system operation is not considered during system design, it reduces the operator's monitoring possibilities. The "cognitive level" required to manage the level of automation is too high.
- If the human is not involved in the system design, it may have influence on the attitude to automation.
- If the human operator's relationship to the management suffers it may have influence on the attitude to automation.
- If a system fails there is a tendency not to discard the automation and take over manually.
- If the mental workload is high, systematic decision errors, generated of the individual human bias, may occur.
- If humans become confident that the system performs "reliable", there is an obvious risk that they become more tolerant of errors.
- If humans do not rely on automated systems, they will remain reluctant to interfere with them.
- If the automated system behaves different than expected or if the system operates in a not intended mode, it may lead to distrust.
- If introduction of an automated system leads to interaction between the human and the machine only rather than between the humans in the group, it

may over time lead to isolating of the individual human experience to the human itself and the team function advantages may suffer.

2 HUMAN PERFORMANCES AND AUTOMATION

- *When, why and how does people decide whether to use automation or to disuse, misuse or abuse it?*
- *Do they make these decisions rationally or based on non-rational factors?*
- *Are automation usage decisions appropriate given the relative performances of operator and automation?*

2.1 Definitions

Use Of Automation

Use refers to the voluntary activation or disengagement of automation by human operators.

Misuse Of Automation

Misuse refers to over-reliance on automation and inadequate monitoring of automated systems.

Disuse Of Automation

Disuse refers to under-utilisation of automation.

Abuse of Automation

Abuse refers to an inappropriate application of automation by designers and managers or to inappropriate usage of automation by operators

2.2 Human and Automation

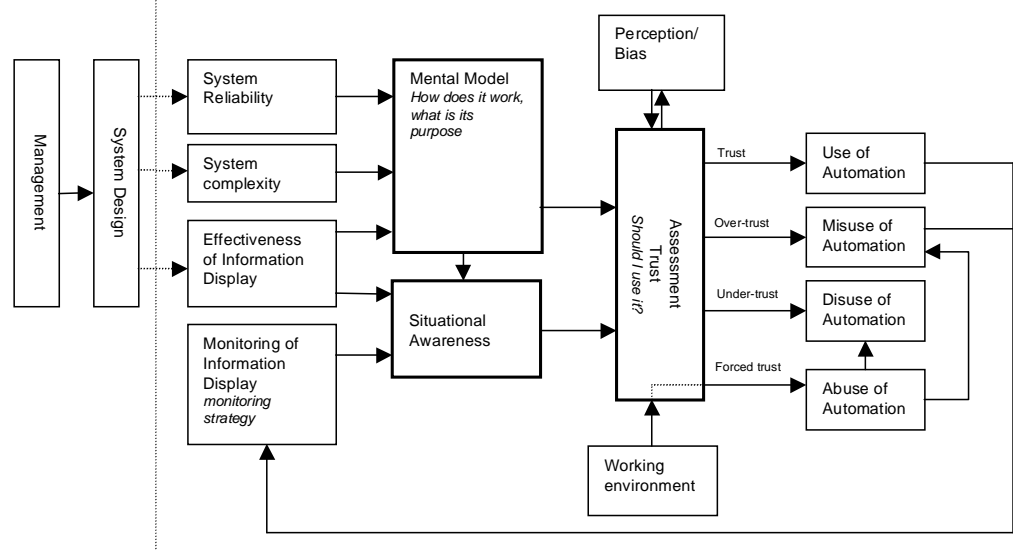
The figure below illustrates the relationship between the major elements of human interaction with automated systems:

- the mental model;
- the situational awareness and,
- the hence derived assessment.

Generally speaking, the mental model is the operator's understanding of how the automation works. The mental model is affected by the influence of the actual

automated system reliability, the system complexity and the effectiveness of the information presented for the operator.

The mental model contributes to the operator's situational awareness, which is also affected by the operators monitoring strategy and the value of the information provided by the automated system.



The assessment, the decision of using automation, is affected by the outcome of the mental model and the situational awareness, and furthermore, by the operator's perception and bias and the working environment.

Perception and bias are the subjectivity in the assessment process and, for example, it could be affected by the operator's attitude towards automation, skill or self-confidence.

The working environment includes the management limitations, workload, working procedures, ergonomics of the design, etc., have an effect on the assessment as well.

The outcome of the assessment process is a degree of trust or reliance on automation, which lead to a way to use automation: use, misuse, disuse or abuse of automation.

2.3 Why Automation is used, misused, disused or abused?

"Human use of automation is complex, subject to a wide range of influences, and capable of exhibiting a wide range of patterns and characteristics. That very complexity makes the study of automation a large undertaking, but the growing importance of automation in systems makes such study increasingly imperative."

Better understanding of why automation is used, misused, disused or abused will help future designers, managers and operators of systems avoid many of the errors that have plagued those of the past and present.

Application of this knowledge can lead to improved systems, the development of effective training curricula, and the formulation of judicious policies and procedures involving automation use."

Raja Pasuraman

2.3.1 Use of Automation

Automation use decisions are based on a complex interaction between many factors and subject to strongly divergent individual considerations. For example,

- **Attitude Towards Automation.** Automation use and attitude towards automation are correlated. Attitudes towards automation vary widely among individuals.
- **Workload.** As automation is introduced to lessen the likelihood of human error by reducing the operator's workload, one would expect that an operator is more likely to choose automation when his or her workload is high than when it is low or moderate.
- **Trust.** An important factor in the development of trust is automation reliability. If automation reliability is high, operators will rely on it. Another factor of trust is related to the ease to understand what automation is doing and why.
- **Cognitive Overhead.** The ease of automation usage and learning contributes to automation usage.
- **Skill, Confidence and other factors.** Skill and self confidence affect also automation usage. Fatigue could also a reason to rely on automation (with the danger to lead to over-reliance on automation).

2.3.2 Misuse of Automation

Automation may fail or behave unpredictably. Excessive trust on automation can lead to rely uncritically on automation without recognising its limitations or fail to monitor the automation's behaviour.

Over-reliance on automation represents an aspect of misuse that can result from several forms of human error, including decision biases and failures of monitoring.

- **Decision Biases.** Decision biases may result in omission errors, in which the operator fails to notice a problem (especially, when its occurrence is expected to be rare) or take an action because the automated aid fails to inform the operator.

- **Human Monitoring Errors.** Over-reliance on automation could also lead to poor monitoring of the automation performances, thus preventing the detection of occasional malfunctioning or failure of automation.

2.3.3 Disuse of Automation

When introduced into workplace, the operator may dislike, and even mistrust a new automated system.

As experience is gained with the new automated system, automation that is reliable and informative, will tend to earn the trust of operators.

An important cause of automation disuse is related to the propensity of false alarms for alerting systems. Operator disabling or ignoring of alerting systems has played a role in several accidents.

Trade-off should be made between the frequency of false alarms and the detection efficiency of real hazardous conditions.

2.3.4 Abuse of Automation

Automation abuse is the automation of functions by designers and implementation by management without due regard for the consequences for human (and hence system) performance and the operator's authority over the system.

This led to the concept of Technology Centred Automation. As the human operator is a major contributor of incidents and accidents, designers attempt to remove the source of error by automating functions carried out by human.

If designers tend to automate everything that leads to an economic benefit and leave the operator to manage the resulting system, several factors emerge:

- **Automation simply replaces the operator with the designer.** To the extent that a system is made less vulnerable to operator error through the application of automation, it is made more vulnerable to designer error.
- **The Technology Centred Automation may place the operator in a role which humans are not well suited.** Indiscriminate application of automation, without regard to the resulting roles and responsibilities of the operator, has led many of the current complaints about automation.
- Automation abuse may lead to misuse or disuse of automation.

2.4 Practical Implications

"Many of the problems of automation misuse, disuse and, abuse arise from differing expectations among the designers, managers, and operators of automated systems.

Our purpose is not to assign blame to designers, managers, or operators but to point out that the complexities of the operational environment and individual human operators may cause automation to be used in ways different from how designers and managers intend.

Discovering the root causes of these differences is a necessary step toward informing the expectations of designers and managers so that operators are provided with automation that better meets their needs and are given the authority and decision-making tools required to use the automation to its best effect."

Raja Pasuraman

The question of how automation should be implemented directly addresses the principal issue of all automation: who should be in control? The question also touches upon the issues of how the automation affects the human operator's tasks, how the automation should operate and be controlled (distribution of functions between man and machine).

The overall system may benefit more by having an operator who is aware of the environmental conditions the system is responding to and the status of the process being performed by virtue of active involvement in the process, than by having an operator who may not be capable of recognising problems and intervening effectively, even if it means that system performance may not be as good as it might be under entirely automated operations.

Human capabilities and limitations shall be considered from the very early stages in the design process and system design needs to be evaluated in a simulated or secured operational environment by a representative extract of operators to ensure that as many occurrences as possible are predicted and considered in the system design.

Designers and managers should consider all factors determining use, misuse, disuse or abuse of automation. For example,

- **Reliability.** If automation reliability is relatively high, then operators may rely on automation, and occasional failures do not substantially deteriorate trust in automation (unless the failures are sustained).
- **Complexity.** Automation should not be difficult or time consuming to turn on or off. Simple, easy to understand automation should encourage automation usage and reliance on automation.

- **Effectiveness and automation Status Information.** Automation should provide sufficient information to maintain situation awareness of the ATCO and to detect degradation or loss of automated function.
- **Mental Model.** Better operator knowledge of how the automation works results in more appropriate use of automation. Training should also highlight the importance of some factors when considering whether or not to use automation.
- **Perception and bias.** Over-reliance and under-reliance antecedent conditions and consequences should be recognised by designers and managers.
- **Working Environment.** Poor relationships with management or poor interface design could affect automation usage. For example, workload should not be such that the operator fails to monitor automation effectively.

3 HUMAN-CENTRED AUTOMATION CONCEPT

“The ability of humans to recognise and define the expected, to cope with the unexpected, to innovate and to reason by analogy when previous experience does not cover a new problem is what has made the aviation system robust, for there are still many circumstances that are neither directly controllable nor fully predictable. It is a compelling reason to retain the human and the central position.”

3.1 Why entering the human-centred concept?

Human errors have been identified as the primarily causal factor of incidents and accidents.

However, the experience shows that the so-called “human errors” are often induced by other aspects of the system.

By introducing the human factors from the design stage in system development, potential system induced human errors can be reduced.

Irrespective of the degree of automation, the operator is and will continue to be fully responsible.

As automated systems become more sophisticated, the risk of bypassing the operator increases. To oppose this trend the principles of Human-centred Automation must be implemented during the entire system life cycle.

A balance between the human and the automation shall be maintained and if compromises are needed it shall always be in the human favour – take into consideration the human characteristics – the weak points and the strong points.

3.2 Principles of Human - Centred Automation

The principles of Human-Centred Automation are given in the following Table.

The Human assumes the ultimate responsibility for the safety of the system.

Therefore:

- The Human must be in command.
- To command effectively, the Human must be involved.
- To be involved, the Human must be informed.
- Functions must be automated only if there is a good reason for doing so.
- The Human must be able to monitor the automated system.
- Automated system must, therefore, be predictable.
- Automated systems must be able to monitor the Human.
- Each element of the system must have knowledge of the other's intent.
- Automation must be designed to be simple to learn and operate.

3.2.1 The Human must be in command

- The responsibility for separation between controlled aircraft remains with the human.
- To assume responsibility for the safe separation of aircraft, the human must retain the authority to command and control those operations.

Potential Issues	Recommendations
<ul style="list-style-type: none"> • Managers and developers should recognise the essential unpredictability of how people will use automation in specific circumstances. • Training personnel should make operators aware of potential biases and influences in deciding to use or not to use automation. 	<ul style="list-style-type: none"> • Automation should be designed to assist the human in carrying out their responsibilities. • The human should be able to reverse to the pristine mode of non-automated functioning whenever needed. • The human should be able to detect failure of the automated system, to correct their

	<p>manifestations, to continue the operation safely until the automated system can resume their normal functions.</p>
--	---

3.2.2 To command Effectively, the ATCO must be involved

- The human should have an active role, whether that role is to actively monitor the automated system.
- Keeping the human involved provides substantial safety benefits by keeping him/her informed and able to intervene.

Potential Issues	Recommendations
<ul style="list-style-type: none"> • If the human is not involved, it is likely that he/she will be less efficient in reacting to critical situations. • High levels of automation could result in over-reliance on automation, when the operator believes that the automation is 100 % reliable. • High levels of automation could also result in skill degradation, when the operator has little opportunity to practice the skills involved in performing the automated tasks manually. 	<ul style="list-style-type: none"> • The decision to apply automation to a function should take into account the need for active human involvement, even if such involvement reduces system performances. • Adaptive tasks allocation may provide a means for involving the operator. Adaptive Task Allocation allocates functions between the operators and the automated system in a flexible way. For example, the operator can actively control a process during moderate workload, allocate this function during peak workload if necessary, and retake manual control when workload diminishes.

3.2.3 To be involved, the ATCO must be informed

- The human must have continuing flow of essential information to maintain situation awareness and to monitor the automation state.

Principle

- Over-reliance on automated solutions may reduce situation awareness. For example, advanced decision aids providing ATCOs with resolution advisories on potential conflicts, may lead to ATCOs accepting the proposed solutions as a matter of routine. This could lead to a loss of the "mental picture" in ATCOs, who tend to use automated conflict resolutions under conditions of high workload and time pressure.
- Monitoring studies indicate that automation failures are difficult to detect if the operator's attention is engaged elsewhere. These studies suggest that attentional rather than purely visual factors underlie poor monitoring.

Recommendations

- The provided information must be informative enough to enable the human to intervene effectively.
- Making automation state indicators more salient may enhance monitoring (e.g., integrated display).

3.2.4 Functions must be automated only if there is a good reason for doing so

- Automation can **amplify** human operator function, thereby allowing to the operator to be more efficient. When automation amplifies, its purpose is to aid the human operator in doing his or her job. When automation is used as amplification only, it leaves the human operator in control and makes the automation reversible, meaning that it should be possible for the human operator to reverse to the pristine mode of non-automated functioning whenever needed.
- Automation can **substitute**, by taking over functions, from the human operator when automation could perform a function more efficiently, reliably or accurately than the human operator. Substitution can lead to problems when automation fails.

Potential Issues	Recommendations
<ul style="list-style-type: none"> • In situations where the automation perform tasks autonomously, it could be difficult for the human to remain aware of exactly what the automation is doing and why. • Such situation may lead to 	<ul style="list-style-type: none"> • Automation should generally be used to amplify Human performances: except in pre-defined situations, automation should never assume command. • In those situations in which the

<p>extreme distrust of the automated system</p>	<p>automation performs tasks autonomously, it should be able to be countermanded easily.</p> <ul style="list-style-type: none"> • In contemplating where to introduce automation, it is necessary to analyse impact of any changes by all available means. One particular useful technique is to use dynamic simulations by using people in controlled conditions or interacting computer models.
---	--

3.2.5 The ATCO must be able to monitor the automated system

- The ability to monitor the automated system is necessary both to permit the human operator to remain on top of the situation and also because the automated systems are fallible.

Potential Issue	Recommendations
<ul style="list-style-type: none"> • Human monitoring tends to be poor in work environments that do not conform to well-established ergonomics design principle, in high workload situations, and in systems in which automation is highly autonomous and there is little experience with the automated tasks. 	<ul style="list-style-type: none"> • The operator must be able, from information available, to determine that automation performance is, and in all likelihood will continue to be. • Feedback about the automation states must be provided, and it must be salient enough to enable the operator to intervene effectively.

3.2.6 Automated systems must be predictable

- The ATCO must be able to evaluate the performance of automated system against an internal model formed through knowledge of the normal behaviour of the system.
- Only if automated system behaves in a predictable fashion can the human operator rapidly detect departure from normal behaviour and thus recognise failures in automated systems.

Potential Issues	Recommendations
<ul style="list-style-type: none"> • Unpredictable behaviour of 	<ul style="list-style-type: none"> • Better human knowledge of how

Potential Issues	Recommendations
<p>automated system may result in mistrust on automation and disuse of automation.</p>	<p>the automation works results in more appropriate use of automation</p> <ul style="list-style-type: none"> • The design of the automated system should include means for the detection of potential failures of the automated system. • Procedures should be designed to recover from automated system failures and to continue the operations safety until the automated system can resume normal functions. • Human should be trained on the safety consequences of specific failures of the automated system.

3.2.7

Automated systems must be able to monitor the human operator

- Human are fallible also and their failures may likewise be unpredictable.
- Because human operators are prone to errors, its is necessary that error detection, diagnosis and correction be integral parts of any automated systems.

Potential Issues	Recommendations
<ul style="list-style-type: none"> • False alarms may result on operator's under-reliance on automation. 	<ul style="list-style-type: none"> • The design of the automated system should integrate human error detection features (e.g., detection of wrong inputs). • The design of the automated system should be able to tolerate some human errors. • The design of alerting systems should take into account not only the detection threshold for these systems, but also the frequency of hazardous condition to be detected. • Alerting automated function should

	indicate when a dangerous situation is possible, rather than encouraging the operator to rely on the alarm for taking corrective action.
--	--

3.2.7 Each element of the system must have knowledge of the others' intent

- In highly automated operations, one way to keep the operator actively involved is to provide him or her with information concerning the intent of the automated system.
- Conversely, the automated system must be aware of the operator intent.

Potential Issues	Recommendations
<ul style="list-style-type: none"> • Lack of information of automated system intent may result in under-reliance on automation. • If the automated system cannot understand the human operator intent, it will be unable to monitor the human performance and to detect departure from normal behaviour. 	<ul style="list-style-type: none"> • When automation is granted a high level of authority over system functions, the operator requires a proportionately high level of feedback so that he or she can effectively monitor the intent of automation and intervene, if necessary. • The more removed of the operator is from the operations, the more feedback must compensate for this lack of involvement. • It must overcome the operator's complacency and demand attention, and it must compensate the lack of awareness once the attention is gained.

3.2.9 Automation must be designed to be simple to learn and to operate

- Automation must be simple to use.
- Automation must be simple to learn.

Potential Issues	Recommendations
<ul style="list-style-type: none"> • If the operator perceives that the advantages offered by automation is not sufficient to overcome the cognitive overhead involved, then he or she may simply choose not to use the automation and to do the task manually. • If an automated system cannot be made to appear reasonably simple to the human, the likelihood that it will be misunderstood and operated incorrectly increases significantly. 	<ul style="list-style-type: none"> • Better knowledge of how automation works results in more appropriate use of automation. • Knowledge of the automation design philosophy may also encourage more appropriate use. • The design should provide simple and intuitive automation that permit reversion in case of automated system failure

4 HUMAN FACTORS – RECOVERY FROM AUTOMATION FAILURES

Less than perfect reliability means that automation-related system failures can degrade system performance. System failures are both explicit and implicit and concern also failures introduced during system design; system fabrication, test, and certification; and during system maintenance.

Failure recovery in an automation perspective is the operator's ability in case of automation failure:

- to manage unexpected failures of the automation
- to continue the operation manually.

4.1 Potential Issues

Observation of the performance of automation have discovered a series of problems with human interaction with automation, with potentially serious consequences for system safety.

Most of them relate to human response when automation fails because implicitly, the automation assists the operator in maintaining the situational awareness and hence the operator's ability to manage higher traffic capacity, density and complexity.

As discussed in previous chapter, design and management influence on automation is an important factor. Poor design can have unfavourable influence on the system performance and contribute to failures, which require manual recovery and management decisions on operation; e.g. procedures and lack of authorisation to use or to disengage automation, may prevent the operator from using the automation effectively.

If automation fails it is reasonable to anticipate that manual take-over will be less efficient and with a safety impact on on-going operations. Automation will therefore require introduction of new procedures for recovery and as well for training and practice.

Several factors have influence on and are essential to an efficient failure recovery:

- the **time required** to respond to an unexpected failure;
- the **ability to intervene** with manual control skills (training aspects);
- how **noticeably** the failure is,

The time available is dependent on the current traffic load and the current traffic density – the human's situation awareness without assistance of automation.

How noticeable the failure is, is dependent on the failure characteristics according to the following example:

- abrupt: little time to prepare for intervention, but **noticeable**;
- graceful: degradation of system capabilities in a way that is **not noticeable**;
- intermittent: difficult to diagnose because of the difficulty in confirming the diagnosis.

The inability of operators to develop mental models (the operator's memory storage of experience, his basis when planning strategy – the basis for performing his job) appropriate to the system and task in order to maintain situation awareness is one of the most significant causes of unintended use of or reaction to automation.

Furthermore, it is likely to anticipate that the human's skills may degrade for most automated functions. As a result of the degradation human is likely to react more slowly to emergency situations if they require use of those manual skills during the recovery.

However, skill degradation has only impact on safety as far as it concerns automated advanced functions (i.e., decision-making and active control functions) and only if the human finds the new automation effective and reliable, their own skills may become degraded.

The combination of deteriorated situation awareness and skill degradation can result in the operator's inability to respond adequately to the failure of the automation.

4.2 Recommendations

Failure recovery in automation is the extent to which the human can act as a backup in the event of failure. The more helpful the automated assistance is when it is functioning normally, the more difficult it becomes for the human to compensate for it if it fails.

Each new automation feature should be evaluated for its impact on situation awareness.

Human should be trained to maintain proficiency in tasks that have been automated when they will be expected to be able to perform those tasks in response to automation failures.

The capability of human to manage the complexities permitted by automation should also be evaluated.

Neither traffic density, nor traffic complexity should be so high to preclude the safe performance of failure recovery tasks.

In order to maintain the operator's ability to separate traffic manually, *at least until all aircraft present in the sector have landed or left the area of responsibility*, it is necessary that:

- the traffic **density** is never so great that human cannot make decisions timely to ensure **separation**;
- traffic **complexity** is low enough so that the human can maintain **situational awareness**.

The system functionality should be designed so that failure recovery will not depend on skills that are likely to degrade. However, degradation of skills shall be considered together with the positive benefit of the actual automated function. The manual problem solving ability will decline but the automated elements will be more efficient from a safety point of view and cumulatively it will lead to a net gain in overall control ability.

5 VERIFICATION, VALIDATION AND EVALUATION

Verification, Validation and Evaluation of automation is critical and an important issue due to the serious impact any design failure can have. Special attention is needed because of the many different, and to a certain extent unpredictable variables contained in advanced automated functions.

Verification is the task of determining that the automated function is built according to its specifications: ***To confirm the automated function is built right.***

Validation is the process of determining that the automated function actually fulfils the purpose for which it was intended: ***To confirm that the right automated function were implemented.***

Evaluation reflects the acceptance of the automated function by the end users and its performance in the field: ***To confirm the usefulness of the automated function.***

5.1 Verification

As stated above, verification asks the question "is the automated function built right?"; verification is checking that all the predictable variables in the automated function are exposed and that the unpredictable variables will be managed properly during operation (i.e., alerts, decision-making and active control functions).

Issues addressed during verification of an automated function include:

- To be defined

5.2 Validation

Validation answers the question "is it the right automated function?", "are all the predictable variables exposed and will the unpredictable variables be managed correctly during operation?" or "is the automated function doing the job it was intended to do?"

It is practically impossible to test an automated function under all the rare events possible. Therefore during operation, it is important that the automated function can manage "lack of design" in the form of active self-monitoring (i.e., alerts, decision-making and active control functions).

Issues addressed during validation of automation:

- To be defined

5.3 Evaluation

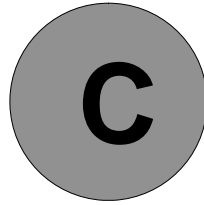
Evaluation addresses the issue "is the automated function valuable?" This is reflected by the acceptance of the automated function by its end users and the performance of the function in operation.

Relevant issues in evaluation are:

- Is the automated function user friendly, and do the users accept the function?
- Does the automated function offer the intended improvement?

Although the automated function is known to produce the correct result, it could fail the evaluation because it is too cumbersome to use, does not really save any effort, solves a problem rarely needed in practice, or produces a result not useful in operation.

This page is intentionally left blank.



CHAPTER 3 GUIDANCE MATERIAL:

SENSITIVITY ANALYSIS

1 FOREWORD

This paper aims at providing guidance for applying sensitivity analysis technique as part of the Preliminary System Safety Assessment (PSSA).

The purpose of this sensitivity analysis guidance material is not to focus on Safety Requirement quantification, but more to:

- enforce a thorough qualitative analysis of the system design weaknesses leading to identify complementary Safety requirements;
- challenge Safety Requirement credibility;

-
- assess the impact of divergence from nominal Safety Requirement specification;
 - and the identification of possible alternative solutions to balance Safety Requirements.

This Guidance Material is illustrated with an example extracted from a Preliminary System Safety Assessment (PSSA) performed in the framework of the MFF (Mediterranean Free Flight) Project for the ASAS Spacing application “Merge behind”.

PSSA aims at apportioning Safety Objectives into Safety Requirements to the main system elements as follows: aircraft system, ATSP provisions (ground ATC system, controllers), aircraft operator’s provisions (flight crew).

The Safety Requirements allocation process was based on the construction of Fault Trees for a selection of hazards to which quantitative Safety Objectives had been previously allocated and was driven by a sensitivity analysis performed on those fault trees.

The process involved both safety analysis done by engineers and validation of safety results and definition & justification of Safety Requirements in the framework of a workshop held with both operational experts (pilots, controllers) and technical experts (addressing airborne and ground systems supporting the ASAS applications).

2 WHEN TO PERFORM SUCH ANALYSIS

The sensitivity analysis is recommended to be conducted after the Top-Down apportionment of Safety Objectives into Safety requirements (PSSA-SRS Chapter 3 §3.4) was performed.

Such Top-Down apportionment phase is iteratively conducted while the system is design evolves, especially for an end-to-end system design when decisions have to be made to allocate certain Safety Requirements to a part of the end-to-end system (e.g. more on the aircraft equipment or on the pilot or on the ATCO or on the ground ATM equipment or on the Communication segment).

A sensitivity analysis can also be conducted at this level to identify the elements of the system design whose ability to satisfy their Safety Requirements influences greatly the Safety Objective satisfaction (PSSA-SRS Chapter 3 §3.5).

However, sometimes such Top-Down Safety Requirements specification proves difficult to apply down to the lowest architecture element due to lack of data to assess the credibility of certain apportionment or due to modification of an existing design (and not a totally new design).

Therefore, the recommended Top-Down approach can be complemented and completed by the approach described hereafter.

However, it is not recommended to directly start by applying such Bottom-Up approach without performing a Top-Down apportionment as the latter enforces a decision making process of preferred risk mitigation strategies.

3 DESCRIPTION OF THE PROCESS

Two ways of using this process exist:

1. Only steps 4 to 6 apply when the “top-down” apportionment of Safety Objectives into Safety Requirements was performed as recommended in PSSA-SRS Chapter 3 §3.4;
2. Steps 1 to 6 apply when such “top-down” apportionment of Safety Objectives into Safety Requirements was NOT performed as recommended in PSSA-SRS Chapter 3 §3.4.

Steps 2 & 3 of the process consist in a quantitative bottom-up allocation of probabilities combined with sensitivity analysis (steps 4 & 5) and with an expert validation driven by the sensitivity analysis results (step 6).

Note: This method requires using probability of basic event occurrence. Therefore, a conversion of frequency of occurrence of basic event into probability or a conversion from a unit to another unit (e.g. from /fh to /h) has to be performed. Such conversion requires conversion assumptions that will have to be further verified, validated and monitored.

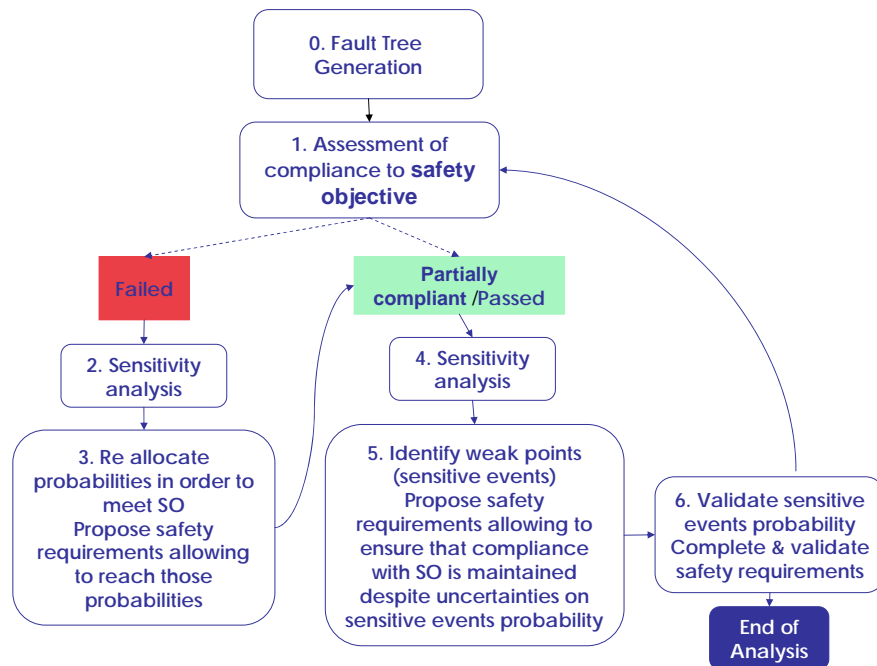


Figure 1 Safety Requirements allocation/balancing driven by sensitivity analysis

The process is iterative and its major steps are shown in Figure 1.

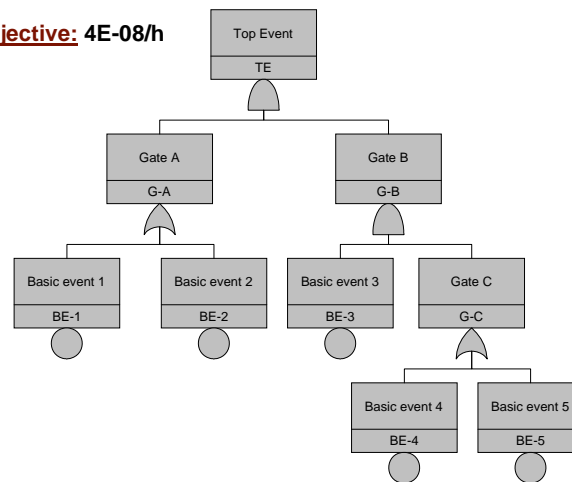
Step 0. Fault-Tree generation

A Fault-Tree has to be created (See SAM-Part IV annex K)

Step 0: Fault Tree Generation



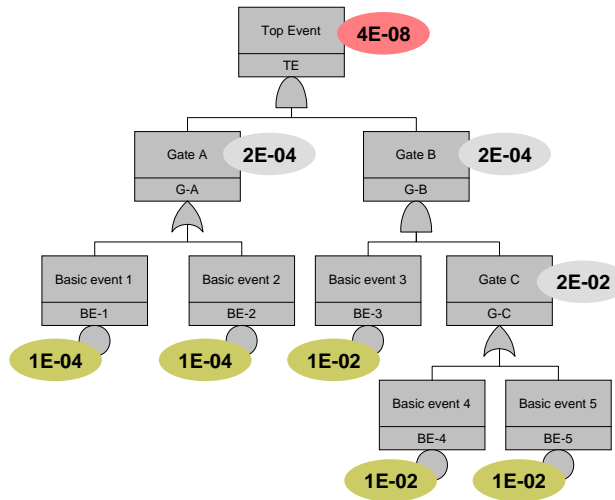
Safety Objective: 4E-08/h



Step 1. Assessment of compliance with Safety Objective (SO):

An initial probability is assigned to each basic event based on engineering judgement (achievable value). Then the probability of occurrence of the top event (operational hazard) is computed and compared with the quantitative Safety Objective (SO) assigned to that hazard.

Step 1: Probabilities assignment 



Initial Basic Causes probabilities 

SO achieved?	yes
Result on Top Event	4.E-08
Safety Objective	4.E-08

BC#	Basic Cause	Initial Value S1
BE-1	Basic event 1	1.00E-04
BE-2	Basic event 2	1.00E-04
BE-3	Basic event 3	1.00E-02
BE-4	Basic event 4	1.00E-02
BE-5	Basic event 5	1.00E-02

Step 2. Sensitivity analysis (aimed at re-allocation):

In case the top event result does not meet the SO, a sensitivity computation is launched to determine which causes (basic events) probability shall be modified (further decreased) to obtain the required Safety Objective.

Sensitivity analysis allows identification of causes which probabilities variation significantly impacts the resulting top event probability.

Sensitivity analysis is systematically performed on all basic events of the fault tree using certain fault tree dedicated software tools (e.g. ARALIA-SIMTREE or Fault-Tree+¹).

It consists in multiplying and dividing a basic event probability by some factors (e.g. divided by 100, then 10, multiplied by 10, then 100), only one event at a time, in order to assess the potential impact of its variation on the resulting top event probability.

Sensitivity results



		SO									
		4.E-08									
BE#	Values S2	(*0.001)	(*0.01)	(*0.1)	(*1)	(*10)	(*100)	(*1000)	Sen		
BE-1	1.00E-02	2.19E-08	3.98E-08	2.19E-07	2.02E-06	1.99E-05	1.99E-04	1.99E-04	D100		
BE-2	1.00E-04	1.99E-06	1.99E-06	1.99E-06	2.02E-06	2.19E-06	3.96E-06	2.17E-05	N		
BE-3	1.00E-02	2.01E-08	2.01E-08	2.01E-07	2.02E-06	2.01E-05	2.01E-04	2.01E-04	D100		
BE-4	1.00E-02	1.01E-06	1.02E-06	1.11E-06	2.02E-06	1.10E-05	1.01E-04	1.01E-04	N		
BE-5	1.00E-02	1.01E-06	1.02E-06	1.11E-06	2.02E-06	1.10E-05	1.01E-04	1.01E-04	N		

¹ EUROCONTROL has sponsored the inclusion of sensitivity analysis function in Fault-Tree+ since V11.

Step 3. Re allocate probabilities in order to meet SO and propose Safety Requirements allowing reaching those probabilities:

A Safety Requirement shall be proposed to ensure that satisfaction of the Safety Objective will be obtained and maintained with the new probabilities.

Safety Requirements take the following content:

- If intent is to mitigate human errors, then qualitative requirement is derived: it could be either a new procedure or the modification of an existing one, or the need to highlight during training the safety importance of a procedure (for example the read-back). Requirement that a specific human action be supported by specific features of a tool may be addressed as well.
- If intent is to mitigate equipment failures, then quantitative requirement is derived: in case of new systems failures, the safety requirement provides the maximal allowable probability of failure. In case of already-operated systems (e.g. failures affecting radar system), requirement stresses need to find out feedback field experience on these particular events in order to compare them with the ones considered as achievable, used as input in the allocation process.

Re-allocated BE probabilities



SO achieved?		no
Result on Top Event		2.01E-06
Safety Objective		4.E-08
BE#	BE	Old Value S2
BE-1	Basic event 1	1.00E-02
BE-2	Basic event 2	1.00E-04
BE-3	Basic event 3	1.00E-02
BE-4	Basic event 4	1.00E-02
BE-5	Basic event 5	1.00E-02

Step 4. Sensitivity analysis (aimed at weak point identification):

When the Safety Objective is met by the top event we have still to ensure that the latter probability will not change significantly through the variation of basic events probabilities (due to uncertainty related to those probabilities). A sensitivity analysis is performed for that effect to highlight the criticality of specific basic events which are identified as “weak points” of the system.

The column “Sensitivity conclusions” (when basic event probability is multiplied & divided by 10/100) the results of that sensitivity analysis are shown as follows:

- M100&D100 indicates that top event result is sensitive to the multiplication/division of that basic event probability by 2 orders of magnitude,
- M10&D10 indicates that result is sensitive to both the multiplication/division of that basic event probability by one order of magnitude.

Identification of weak points

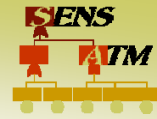
BE#	Values S2	(*)0.001	(*)0.01	(*)0.1	(*)1	(*)10	(*)100	(*)1000	Sen	(*)0.001	(*)0.01	(*)0.1	(*)10	(*)100	(*)1000
BE-1	1.00E-02	2.19E-10	3.98E-10	2.19E-09	2.01E-08	1.99E-07	1.99E-06	1.98E-06	M10	98.9%	98.0%	89.1%	981.1%	9802.0%	9802.0%
BE-2	1.00E-04	1.99E-08	1.99E-80	1.99E-08	2.01E-08	2.19E-08	3.98E-08	2.17E-07	N	1.0%	1.0%	0.9%	8.8%	97.0%	979.3%
BE-3	1.00E-04	2.01E-11	2.01E-10	2.01E-09	2.01E-08	2.01E-07	2.01E-06	2.01E-05	M10	99.9%	99.0%	90.0%	900.0%	9900.0%	9900.0%
BE-4	1.00E-02	1.01E-08	1.02E-08	1.11E-08	2.01E-08	1.10E-07	1.01E-06	1.01E-06	M10	49.7%	49.3%	44.8%	447.7%	4925.1%	4925.1%
BE-5	1.00E-02	1.01E-08	1.02E-08	1.11E-08	2.01E-08	1.10E-07	1.01E-06	1.01E-06	M10	49.7%	49.3%	44.8%	447.7%	4925.1%	4925.1%

SO 4.E-08

Step 5. Identify weak points (sensitive events) and propose Safety Requirements to ensure that compliance with SO is maintained:

Finally, once sensitive basic events (weak points) have been identified, safety requirements shall be proposed for the system elements displaying these failures, to ensure that despite the uncertainty affecting their probability, the Safety Objective will be satisfied. The advantage of this technique is to target the allocation of Safety Requirements on the weak points (failures with significant contribution to hazards associated to the Safety Objectives).

SR on weak points



BC#	BC	Initial Value	Final Value	SENS	SR#	Safety Requirements
BE-1	Basic event 1	1.00E-04	1.00E-02	M10	SR2	Safety Requirements to ensure Safety Objective compliance despite uncertainties on this weak point
BE-2	Basic event 2	1.00E-04	1.00E-04	N		Safety requirement no necessary because even if probability assigned is multiplied by 100, the Safety Objective is achieved.
BE-3	Basic event 3	1.00E-02	1.00E-04	M10	SR1	Safety Requirements to ensure that compliance with the Safety Objective will be obtained and maintained
BE-4	Basic event 4	1.00E-02	1.00E-02	M10	SR3	Safety Requirements to ensure Safety Objective compliance despite uncertainties on this weak point
BE-5	Basic event 5	1.00E-02	1.00E-02	M10	SR4	Safety Requirements to ensure Safety Objective compliance despite uncertainties on this weak point

Step 6. Validate sensitive events probability and complete & validated Safety Requirements:

A validation workshop involving operational (pilots, controllers) and technical experts is needed in order to validate the outcomes of the safety requirements allocation process. The following aspects are addressed:

- Credibility of the sensitive causes and validity of the achievable probability assumed for them (for the human factor related events, a qualitative ranking is used, from the most probable to the less probable one, addressing separately flight crew and controllers; that ranking is further translated in probability orders of magnitude in the next iteration of the allocation process²);

Note that the intent is not to assign an absolute probability value to a human error, but rather to allow inclusion of the relative contribution of the human errors in the fault trees. The final aim is the sensitivity analysis and not the absolute computation of the human error contribution to the probability of the hazard occurrence

- Safety requirements proposed for each sensitive basic event are validated or invalidated (in terms of credibility, feasibility and effectiveness). When needed and possible, alternative solutions are provided and Safety Requirements are defined in response to those weak points not yet covered by a requirement during the safety analysis allocation steps.

After the workshop the probability values that were modified are re-injected in the fault tree model and the previous steps are re iterated (new sensitivity analysis are performed). In case of major changes (significant changes in the list of sensitive causes), a second validation by experts might be necessary.

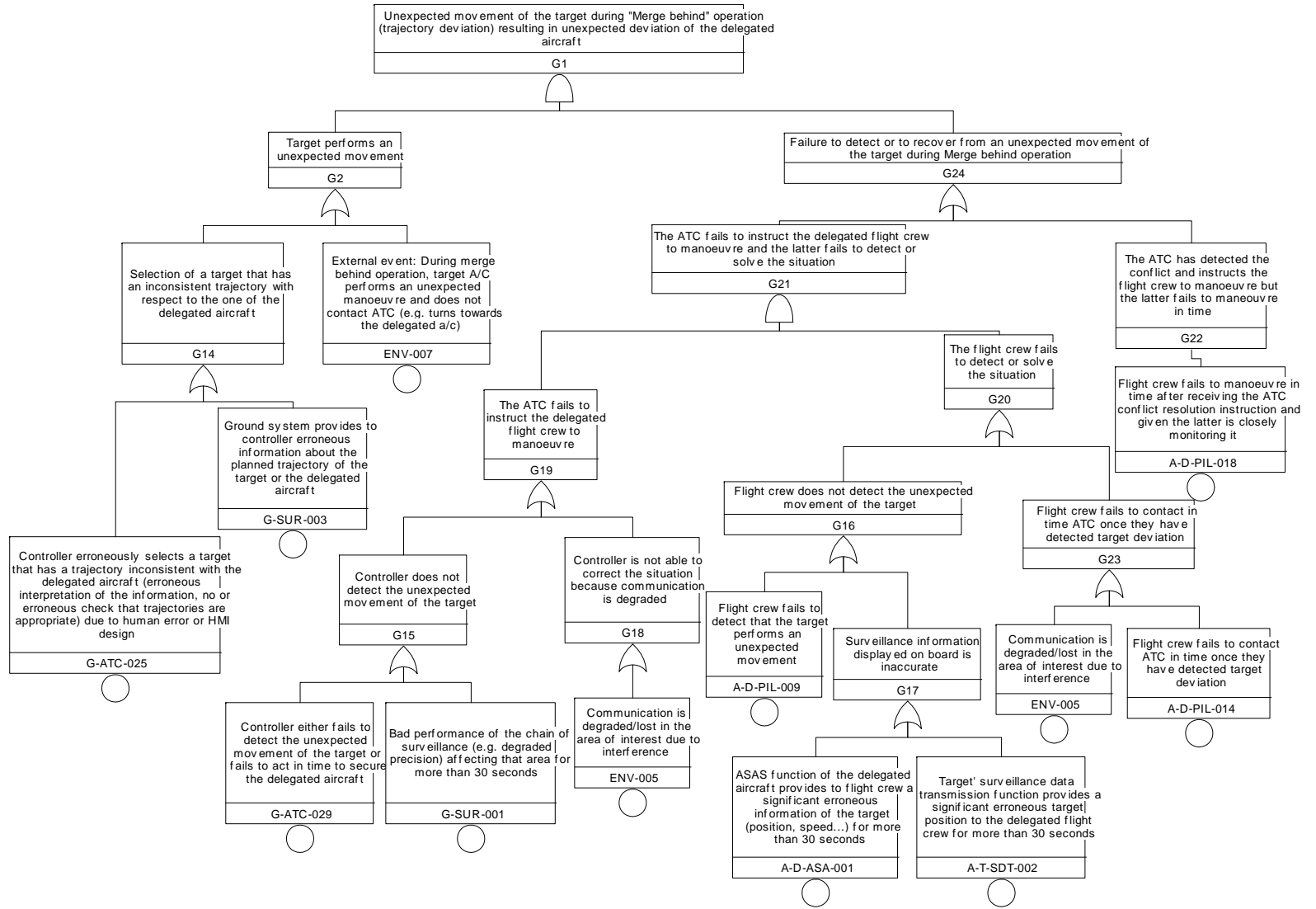
4 EXAMPLE: SENS-ATM APPLIED TO MFF

Step 0: Fault-Tree generation

Figure 2 presents the fault tree that was built for the operational hazard: “Unexpected movement of the target during “Merge behind” operation (trajectory deviation)”.

The Worst Credible effect of this hazard consists in an “unexpected deviation of the delegated aircraft” (Severity Class 2).

The Safety Objective (SO) associated to this hazard is “no more than 1E-07 occurrences per ASAS Spacing operation”.



Step 1. Assessment of compliance with Safety Objective (SO):

The following table provides the list of Safety Requirements allocated using a bottom-up approach for each basic event:

	SO achieved?	NO
	Top event (hazard) value	1E-06
	Safety Objective (SO)	1E-07
Event Label	Event Description	Basic Event achievable probability
A-D-ASA-001	ASAS function of the delegated aircraft provides to flight crew a significant erroneous information of the target (position, speed,,,) for more than 30 seconds	1E-06
A-D-PIL-009	Flight crew fails to detect that the target performs an unexpected movement	0.01
A-D-PIL-014	Flight crew fails to contact ATC in time once they have detected target deviation	1E-05
A-D-PIL-018	Flight crew fails to manoeuvre in time after receiving the ATC conflict resolution instruction and given the latter is closely monitoring it	0,001
A-T-SDT-002	Target' surveillance data transmission function provides a significant erroneous target position to the delegated flight crew for more than 30 seconds	1E-05
ENV-005	Communication is degraded/lost in the area of interest due to interference	1E-05
ENV-007	External event: During merge behind operation, target A/C performs an unexpected manoeuvre and does not contact ATC (e.g, turns towards the delegated a/c)	1E-04
G-ATC-025	Controller erroneously selects a target that has a trajectory inconsistent with the delegated aircraft (erroneous interpretation of information, no or erroneous check that trajectories are appropriate) due to human error or HMI design	0.001
G-ATC-029	Controller either fails to detect the unexpected movement of the target or fails to act in time to secure the delegated aircraft	0.001
G-SUR-001	Bad performance of the chain of surveillance (e.g, degraded precision) affecting that area for more than 30 s	1E-07
G-SUR-003	Ground system provides to controller erroneous information about the planned trajectory of the target or the delegated aircraft	1E-05

Table 1.1: MFF initial Safety Requirements definition

The achievable Safety Objective (Top event value) with such values is 1.13 E-6.

Step 2. Sensitivity analysis (aimed at re-allocation)

Table 2.1 provides the results of the sensitivity analysis aimed at re-allocating probabilities to obtain the required Safety Objective. The basic events A-D-PIL-018 and G-ATC-025 are the most sensitive with respect to a division by 10 of their respective probabilities and modification by that order of either of those events allows to reach the SO (top event probability passes from 1.2E-06 to 2.3E-07 which is judged acceptable³).

Evt Label	Evt Description	Basic Evt achievable probability	Top event probability - sensitivity computation				
			(*)0,01	(*)0,1	(*)1	(*)10	(*)100
A-D-ASA-001	ASAS function of the delegated aircraft provides to flight crew a significant erroneous information of the target (position, speed,...) for more than 30 seconds	1E-06	1.13e-6	1.13e-6	1.13e-6	1.13e-6	1.13e-6
A-D-PIL-009	Flight crew fails to detect that the target performs an unexpected movement	0.01	1.12e-6	1.12e-6	1.13e-6	1.23e-6	2.22e-6
A-D-PIL-014	Flight crew fails to contact ATC in time once they have detected target deviation	1E-05	1.13e-6	1.13e-6	1.13e-6	1.13e-6	1.13e-6
A-D-PIL-018	Flight crew fails to manoeuvre in time after receiving the ATC conflict resolution instruction and given the latter is closely monitoring it	0,001	3.33e-8	1.33e-7	1.13e-6	1.11e-5	1.11e-4
A-T-SDT-002	Target' surveillance data transmission function provides a significant erroneous target position to the delegated flight crew for more than 30 seconds	1E-05	1.13e-6	1.13e-6	1.13e-6	1.13e-6	1.13e-6
ENV-005	Communication is degraded/lost in the area of interest due to interference	1E-05	1.12e-6	1.12e-6	1.13e-6	1.23e-6	2.22e-6
ENV-007	External event: During merge behind operation, target A/C performs an unexpected manoeuvre and does not contact ATC (e.g, turns towards the delegated a/c)	1E-04	1.03e-6	1.04e-6	1.13e-6	2.04e-6	1.12e-5
G-ATC-025	Controller erroneously selects a target that has a trajectory inconsistent with the delegated aircraft (erroneous interpretation of information, no or erroneous check that trajectories are appropriate) due to human error or HMI design	0.001	1.22e-7	2.14e-7	1.13e-6	1.03e-5	1.02e-4
G-ATC-029	Controller either fails to detect the unexpected movement of the target or fails to act in time to secure the delegated aircraft	0.001	1.12e-6	1.12e-6	1.13e-6	1.23e-6	2.23e-6
G-SUR-001	Bad performance of the chain of surveillance (e.g, degraded precision) affecting that area for more than 30 s	1E-07	1.13e-6	1.13e-6	1.13e-6	1.13e-6	1.13e-6
G-SUR-003	Ground system provides to controller erroneous information about the planned trajectory of the target or the delegated aircraft	1E-05	1.12e-6	1.12e-6	1.13e-6	1.22e-6	2.14e-6

Table 2.1. Example of Safety Requirements re-allocation

³ To further decrease that value to 1E-07 the probability of G-ATC-025 shall be divided by 2. Nevertheless, given the uncertainty affecting the human errors occurrence, we accept to work with orders of magnitudes and define effective Safety Requirements to mitigate risk associated to those errors.

Step 3. Re-allocate probabilities in order to meet Safety Objectives and propose Safety Requirements allowing reaching those probabilities:

In the chosen example, both basic events A-D-PIL-018 and G-ATC-025 are candidates to be re-allocated a value of 1E-04 instead of the current 1E-03, but only one change would be enough.

Changing A-D-PIL-018 is chosen, given that a credible and effective Safety Requirement was found (see line corresponding to A-D-PIL-018 in Table 2.1).

Step 4. Sensitivity analysis (aimed at weak points identification):

As a result of the sensitivity analysis performed after the previous re-allocation, the events A-D-PIL-009, G-ATC-029 and ENV-005, ENV-007 were found sensitive as the multiplication by 10 of the former two and by 100 of the latter two involves a significant increase (one order of magnitude) of the top event probability (note that an updated table 1.1, not included here, is obtained).

Evt Label	Evt Description	Basic Evt achievable probability	Top event probability - sensitivity computation				
			(*)0,01	(*)0,1	(*)1	(*)10	(*)100
A-D-ASA-001	ASAS function of the delegated aircraft provides to flight crew a significant erroneous information of the target (position, speed,..) for more than 30 seconds	1E-06	1.13e-6	1.13e-6	1.13e-6	1.13e-6	1.13e-6
A-D-PIL-009	Flight crew fails to detect that the target performs an unexpected movement	0.01	1.12e-6	1.12e-6	1.13e-6	1.23e-6	2.22e-6
A-D-PIL-014	Flight crew fails to contact ATC in time once they have detected target deviation	1E-05	1.13e-6	1.13e-6	1.13e-6	1.13e-6	1.13e-6
A-D-PIL-018	Flight crew fails to manoeuvre in time after receiving the ATC conflict resolution instruction and given the latter is closely monitoring it	0,001	3.33e-8	1.33e-7	1.13e-6	1.11e-5	1.11e-4
A-T-SDT-002	Target' surveillance data transmission function provides a significant erroneous target position to the delegated flight crew for more than 30 seconds	1E-05	1.13e-6	1.13e-6	1.13e-6	1.13e-6	1.13e-6
ENV-005	Communication is degraded/lost in the area of interest due to interference	1E-05	1.12e-6	1.12e-6	1.13e-6	1.23e-6	2.22e-6
ENV-007	External event: During merge behind operation, target A/C performs an unexpected manoeuvre and does not contact ATC (e.g, turns towards the delegated a/c)	1E-04	1.03e-6	1.04e-6	1.13e-6	2.04e-6	1.12e-5
G-ATC-025	Controller erroneously selects a target that has a trajectory inconsistent with the delegated aircraft (erroneous interpretation of information, no or erroneous check that trajectories are appropriate) due to human error or HMI design	0.001	1.22e-7	2.14e-7	1.13e-6	1.03e-5	1.02e-4

Evt Label	Evt Description	Basic Evt achievable probability	Top event probability - sensitivity computation				
			(*)0,01	(*)0,1	(*)1	(*)10	(*)100
G-ATC-029	Controller either fails to detect the unexpected movement of the target or fails to act in time to secure the delegated aircraft	0.001	1.12e-6	1.12e-6	1.13e-6	1.23e-6	2.23e-6
G-SUR-001	Bad performance of the chain of surveillance (e.g, degraded precision) affecting that area for more than 30 s	1E-07	1.13e-6	1.13e-6	1.13e-6	1.13e-6	1.13e-6
G-SUR-003	Ground system provides to controller erroneous information about the planned trajectory of the target or the delegated aircraft	1E-05	1.12e-6	1.12e-6	1.13e-6	1.22e-6	2.14e-6

Table 4.1: Identification of weak points

Step 5. Identify weak points (sensitive events) and propose Safety Requirements to ensure that compliance with SO is maintained:

According to table 4.1, Safety Requirements were defined for each of the previously identified weak points.

Note that A-D-PIL-009, G-ATC-029 and G-ATC-025 display the highest sensitivity with respect to the increase of their probability and thus the Safety Requirements defined for mitigating them need particular attention when checking their effectiveness. Be aware that in the real process, some of these requirements are proposed at this step, others need to be amended or new ones added during the next step.

Step 6. Validate sensitive events probability and complete & validated Safety Requirements:

In Table 2, the last three columns reflect that iteration.

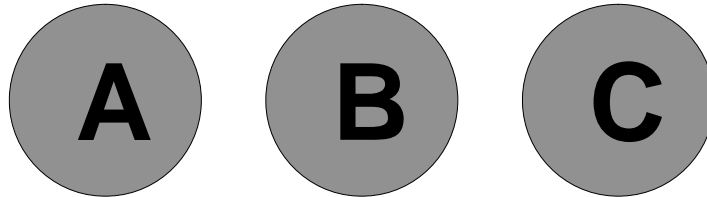
Note that following the workshop validation, the probability for G-ATC-029 was relaxed from 0.001 to 0.01. In the example neither the allocation nor the list of weak points were called into question following the validation step and the second iteration of sensitivity analysis.

Nevertheless the sensitivity of weak points A-D-PIL-009 and G-ATC-029 with respect to the increase of their probability becomes higher, and thus the Safety Requirements defined for mitigating them need particular attention when checking their effectiveness.

Cause Identifier	Cause (basic event) definition	Achievable probability (→ reallocated when necessary to meet SO)	Sensitivity conclusions after re-allocation (when basic event probability is multiplied & divided by 10/100)	Workshop validated/ allocated probability	Re-Sensitivity conclusions (based on validation outputs)	Validated Safety Requirement
A-D-PIL-009	Flight crew fails to detect that the target performs an unexpected movement	0.01	M100	Same	M10	To provide an appropriate HMI (e.g. visualisation precise enough or function allowing to highlight a significant target deviation) and sufficient training allowing the flight crew to easily/fastly detect an unexpected movement of the target
A-D-PIL-018	Flight crew fails to manoeuvre in time after receiving the ATC conflict resolution instruction and given the latter is closely monitoring it	0.001 → Changed to 1,00E-04 to meet the SO	D&M10	Same	M10	Use of ICAO phraseology that allows the controller to indicate to flight crew the emergency of the manoeuvre performance (e.g. essential traffic) shall be re-enforced for ASAS During the flight crews' training, it shall be highlighted that emergency situations are also applicable to ASAS
ENV-005	External event: Communication is degraded/lost in the area of interest due to interference	1E-05	M100	Same	M100	To be confronted with field feedback experience
ENV-007	External event: During merge behind operation, target A/C performs an unexpected manoeuvre and does not contact ATC (e.g. turns towards the delegated a/c)	1E-04	M100	Same, waiting for confrontation with field feedback experience	M100	In case the field feedback experience probability is of an order of magnitude of 1e-03 per ASAS delegation (or 3e-03 flight/hour) or worse, in areas where ASAS spacing is implemented (stipulated by AIP), the following safety requirement is proposed: "The normal procedure that states that aircraft shall contact controllers if they deviate from current trajectory shall be reinforced".
G-ATC-025	Controller erroneously selects a target that has a trajectory inconsistent with the delegated aircraft (erroneous interpretation of the information, no or erroneous check that trajectories are appropriate) due to human error or HMI design	0.001	D&M10	same	D&M10	A ground system shall be designed to help the controllers in selecting pairs of aircraft for ASAS spacing instruction having appropriate trajectories
G-ATC-029	Controller either fails to detect the unexpected movement of the target or fails to act in time to secure the delegated aircraft	0.001	M100	0.01 after validation workshop	M10	Two complementary requirements are issued: 1. Trajectory Change Points (TCP) shall be downlinked to the ground The controller shall be alerted of inconsistency between a/c trajectory selected on ground and the one selected on FMS. 2; Appropriate means on CWP shall be provided allowing controllers to correctly monitor the spacing (e.g. to provide an alert in case of predicted infringement of ASAS spacing on CWP)

(D = Division by; M = Multiplication by)

Table 6.1: Synthetic results of the allocation process driven by sensitivity analysis



CHAPTER 4 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.

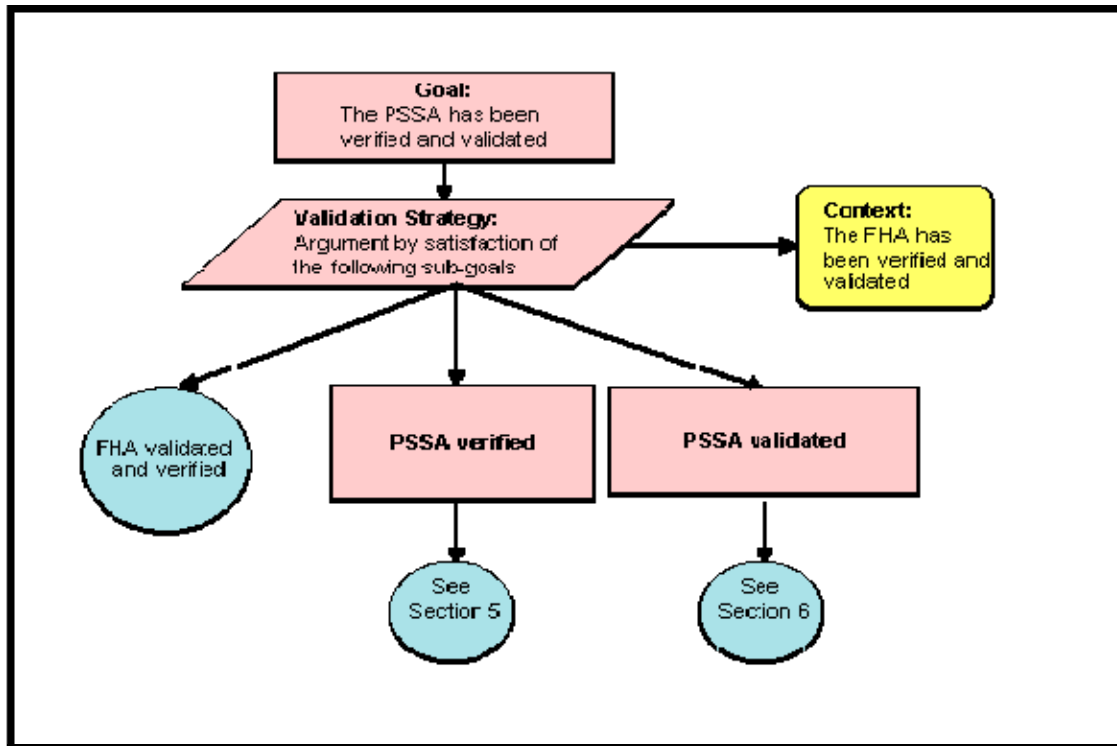
The accomplishment of objective evaluation is more likely to be ensured when the verification and validation processes are carried out by a person (or persons) other than those who performed the PSSA.

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.



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).

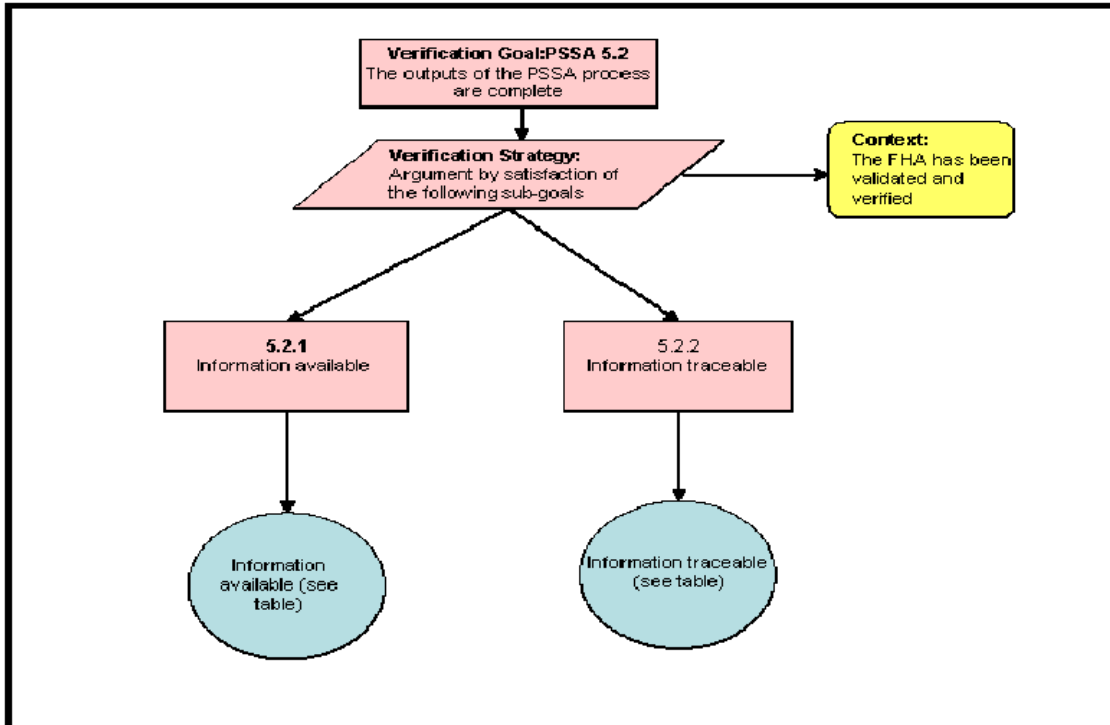
5 PSSA Verification

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



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:

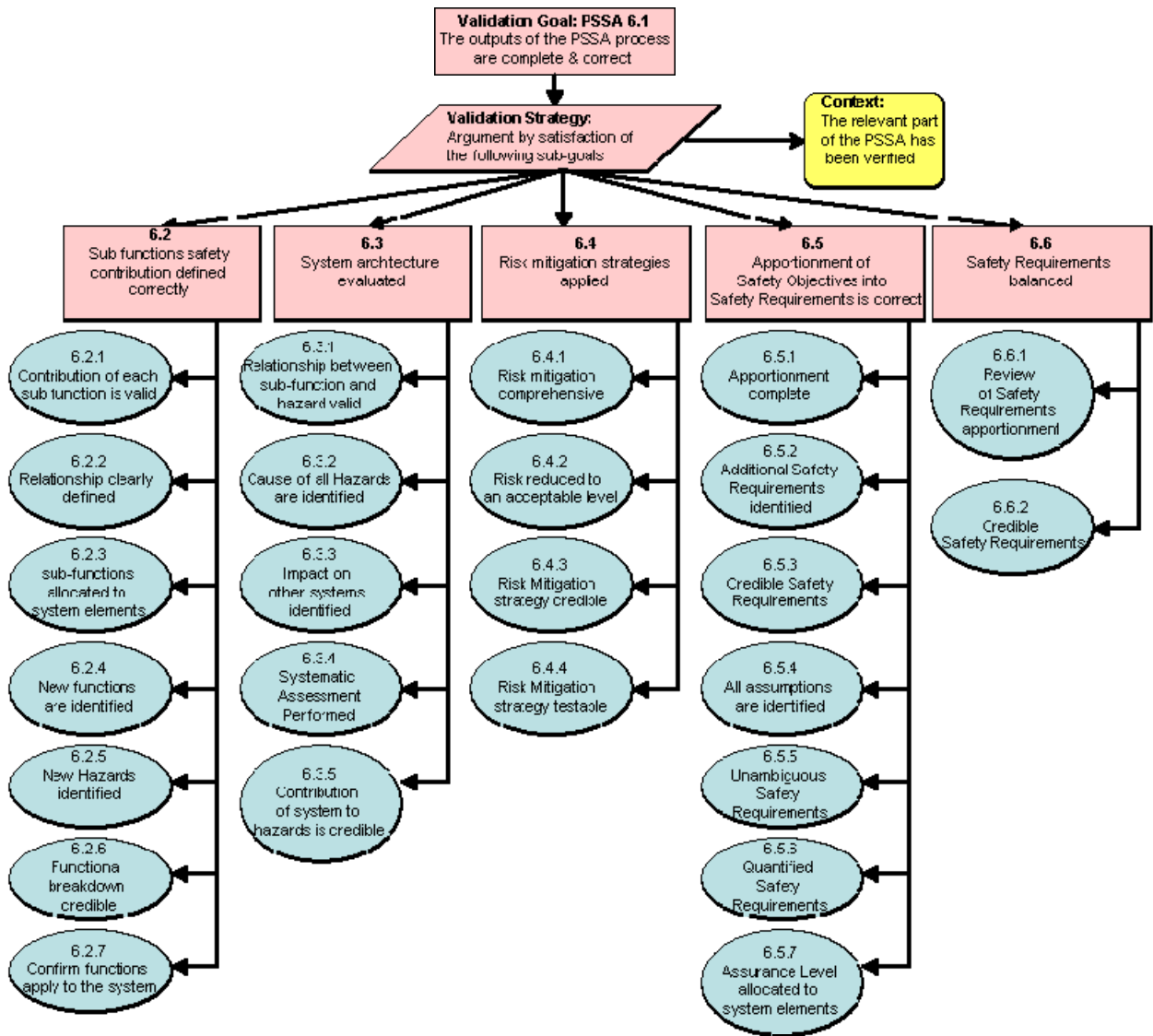
Goal	Validation Item	Validation Result
PSSA 6.1.1	All five stages of the PSSA-SRS have been addressed.	Satisfactory <input type="checkbox"/> Requires Action <input type="checkbox"/>
	Comment / action: Reference in PSSA:	

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.



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	<p>The contribution of each sub-function to a Safety Objective is valid.</p> <p>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.</p>	Satisfactory <input type="checkbox"/>	Requires Action <input type="checkbox"/>
<p>Comment / action: Reference in PSSA:</p>			
PSSA 6.2.2	<p>The relationship of sub-functions to high level functions is valid.</p> <p>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.</p>	Satisfactory <input type="checkbox"/>	Requires Action <input type="checkbox"/>
<p>Comment / action: Reference in PSSA:</p>			
PSSA 6.2.3	<p>Sub-functions allocated to system elements are defined.</p> <p>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).</p>	Satisfactory <input type="checkbox"/>	Requires Action <input type="checkbox"/>
<p>Comment / action: Reference in PSSA:</p>			
PSSA 6.2.4	<p>Any new functions identified in the PSSA are valid.</p> <p>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.</p> <p>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.</p>	Satisfactory <input type="checkbox"/>	Requires Action <input type="checkbox"/>
<p>Comment / action: Reference in PSSA:</p>			
PSSA 6.2.5	<p>Any new hazards are valid.</p> <p>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.</p>	Satisfactory <input type="checkbox"/>	Requires Action <input type="checkbox"/>
<p>Comment / action: Reference in PSSA:</p>			

Goal	Validation Item	Validation Result
PSSA 6.2.6	<p>The functional breakdown is credible.</p> <p>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.</p>	<p>Satisfactory <input type="checkbox"/></p> <p>Requires Action <input type="checkbox"/></p>
<p>Comment / action: Reference in PSSA:</p>		
PSSA 6.2.7	<p>The sub-functions are applicable to the system under assessment.</p>	<p>Satisfactory <input type="checkbox"/></p> <p>Requires Action <input type="checkbox"/></p>
<p>Comment / action: Reference in PSSA:</p>		

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	<p>The contribution of each system element to each hazard is valid.</p> <p>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.</p>	<p>Satisfactory <input type="checkbox"/></p> <p>Requires Action <input type="checkbox"/></p>
<p>Comment / action: Reference in PSSA:</p>		
PSSA 6.3.2	<p>The causes of the hazards are stated and valid.</p> <p>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.</p>	<p>Satisfactory <input type="checkbox"/></p> <p>Requires Action <input type="checkbox"/></p>
<p>Comment / action: Reference in PSSA:</p>		
PSSA 6.3.3	<p>The impact on other systems (outside the scope of the safety assessment) is identified.</p> <p>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.</p> <p>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.</p>	<p>Satisfactory <input type="checkbox"/></p> <p>Requires Action <input type="checkbox"/></p>
<p>Comment / action: Reference in PSSA:</p>		
PSSA 6.3.4	<p>A systematic and structured approach has been applied to the evaluation of the cause of the hazards.</p> <p>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].</p>	<p>Satisfactory <input type="checkbox"/></p> <p>Requires Action <input type="checkbox"/></p>
<p>Comment / action: Reference in PSSA:</p>		

Goal	Validation Item	Validation Result
PSSA 6.3.5	<p>The contribution of the system to the hazards is credible.</p> <p>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</p>	<p>Satisfactory <input type="checkbox"/></p> <p>Requires Action <input type="checkbox"/></p>
<p>Comment / action: Reference in PSSA:</p>		

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	<p>The risk mitigation strategy is comprehensive.</p> <p>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].</p>	<p>Satisfactory <input type="checkbox"/></p> <p>Requires Action <input type="checkbox"/></p>
<p>Comment / action: Reference in PSSA:</p>		
PSSA 6.4.2	<p>The application of mitigation strategies is able to reduce the risk to an acceptable level.</p> <p>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].</p>	<p>Satisfactory <input type="checkbox"/></p> <p>Requires Action <input type="checkbox"/></p>
<p>Comment / action: Reference in PSSA:</p>		
PSSA 6.4.3	<p>A credible risk mitigation strategy has been defined</p> <p>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].</p>	<p>Satisfactory <input type="checkbox"/></p> <p>Requires Action <input type="checkbox"/></p>
<p>Comment / action: Reference in PSSA:</p>		
PSSA 6.4.4	<p>A testable risk mitigation strategy has been defined.</p> <p>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].</p>	<p>Satisfactory <input type="checkbox"/></p> <p>Requires Action <input type="checkbox"/></p>
<p>Comment / action: Reference in PSSA:</p>		

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	<p>The apportionment of Safety Requirements is complete.</p> <p>The PSSA should also demonstrate that all Safety Objectives are apportioned into Safety Requirements.</p> <p>The PSSA should demonstrate that all Safety Requirements have been identified for all system elements.</p>	Satisfactory <input type="checkbox"/>	Requires Action <input type="checkbox"/>
<p>Comment / action:</p> <p>Reference in PSSA:</p>			
PSSA 6.5.2	<p>Any additional Safety Requirements are identified.</p> <p>Additional Safety Requirements may be set to meet regulations or standards.</p>	Satisfactory <input type="checkbox"/>	Requires Action <input type="checkbox"/>
<p>Comment / action:</p> <p>Reference in PSSA:</p>			
PSSA 6.5.3	<p>The Safety Requirements apportionment is credible.</p> <p>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.</p>	Satisfactory <input type="checkbox"/>	Requires Action <input type="checkbox"/>
<p>Comment / action:</p> <p>Reference in PSSA:</p>			
PSSA 6.5.4	<p>All assumptions are listed.</p> <p>The PSSA should identify all assumptions. These assumptions shall be credible and validated by stakeholders.</p>	Satisfactory <input type="checkbox"/>	Requires Action <input type="checkbox"/>
<p>Comment / action:</p> <p>Reference in PSSA:</p>			
PSSA 6.5.5	<p>The Safety Requirements are unambiguous.</p> <p>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.</p>	Satisfactory <input type="checkbox"/>	Requires Action <input type="checkbox"/>
<p>Comment / action:</p> <p>Reference in PSSA:</p>			
PSSA 6.5.6	<p>Safety Requirements are quantified, when possible.</p> <p>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).</p> <p>However, many Safety Requirements can not be quantified (Software, Procedure, Human maybe difficult also).</p>	Satisfactory <input type="checkbox"/>	Requires Action <input type="checkbox"/>

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 <input type="checkbox"/> Requires Action <input type="checkbox"/>
	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	<p>The overall set of Safety Requirements has been reviewed and maybe alternative strategies for apportionment were considered.</p> <p>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).</p> <p>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).</p> <p>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.</p>	<p>Satisfactory <input type="checkbox"/></p> <p>Requires Action <input type="checkbox"/></p>
<p>Comment / action: Reference in PSSA:</p>		
PSSA 6.6.2	<p>The Safety Requirements are credible</p> <p>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.</p>	<p>Satisfactory <input type="checkbox"/></p> <p>Requires Action <input type="checkbox"/></p>
<p>Comment / action: Reference in PSSA:</p>		

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:

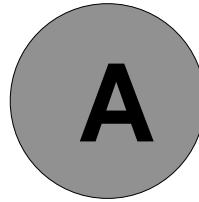
- An updated list of assumptions;
- An updated list of identified hazards and Safety Objectives (new hazards and/or effects may have been identified);
- Results of Safety analyses;
- Justification material for risk mitigation strategies application;
- Safety Requirements on individual system elements 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 <input type="checkbox"/> Requires Action <input type="checkbox"/>
	Comment / action: Reference in FHA	
PSSA 6.7.2	<p>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).</p> <p>To specify Safety Requirements, the following criteria have been appropriately covered (an acceptable rationale exists to sustain the choices made to address those criteria):</p> <ul style="list-style-type: none"> • 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 <input type="checkbox"/> Requires Action <input type="checkbox"/>
	Comment / action: Reference in PSSA	

Table 6.7



CHAPTER 5 GUIDANCE MATERIAL:

PSSA REPORT

The PSSA documentation records the results of the PSSA 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 PSSA, recommendations are:

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

- To make this document conclusive: state whether the proposed architecture is able or not to achieve an acceptable risk and clearly and concisely list the main findings of the PSSA such as main Safety Requirements (including Assurance Levels) and assumptions;
- To include an executive summary;
- To contain the results of detailed analyses in annexes.

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

Executive Summary

It should focus on main messages delivered by PSSA, such as: what are the main Safety Requirements, recommendations and conclusions.

Introduction

This section should describe:

- The objectives of the document.
- The scope of the PSSA (What was addressed in the PSSA process and what was not addressed).
- The structure of the document.

System Design Description

This section should provide an overview of the system design and architecture.

It will cover, or reference, documentation describing:

- The system 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 Requirements. For example,

- Applicable Safety Regulatory Requirements;
- (International) Standards
- Approach to derive quantitative Safety Objectives into Safety Requirements, when appropriate.

Safety Requirements Identification

The results are usually best presented in a tabular format.

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

Summary and Conclusions

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

- The updated list of assumptions;
- The list of most demanding Safety Requirements;
- The list of quantitative and/or qualitative Safety Requirements (including Assurance Levels);
- The main conclusions of the PSSA validation, verification and process assurance activities;
- A statement whether the proposed architecture is able or not to achieve an acceptable risk.

This part should also identify any architectural elements 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 PSSA process, such as the PSSA Plan (as described in PSSA Chapter 2) and the Validation/Verification and Process Assurance reports (as described in PSSA 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, ...)
- Traceability matrices:
 - Safety Objectives <> Safety Requirements
 - Safety Requirements <> System Elements
 - Safety Requirements <> Functions (This can be done via the Safety Objectives)
 - ALs (Assurance Level) <> System Elements

Table 5.1. Structure of the PSSA Report