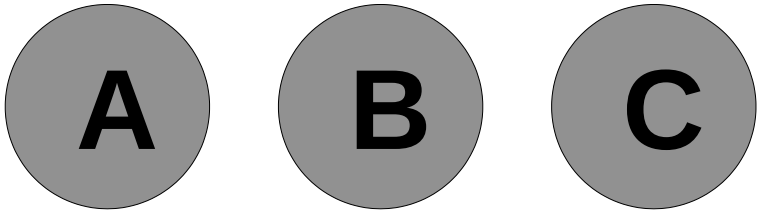

GUIDANCE MATERIAL

FHA Evaluation Activities

1 Introduction

This chapter gives guidance on verifying and validating a Functional Hazard Assessment (FHA).

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

2 Objectives of the FHA

The FHA process develops system Safety Objectives, defining the maximum frequency at which hazards can be accepted to occur.

3 How to Apply the Process

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

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

The accomplishment of objective evaluation is more likely to be ensured when the verification and validation processes are carried out by a person (or persons) other than those who performed the FHA process. However, such independence should only be necessary for the most critical systems – as determined during the FHA. The involvement of people with different skills (ATCO's, Pilots & Engineers) in a SAM process (e.g. brainstorming in FHA) 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.

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

- Conduct the verification and validation at varying FHA stages, especially for a large or complex FHA. This may identify gaps or issues in the FHA at an early stage and avoid repeating any of the FHA steps.
- Start the FHA validation when all the FHA verification is completed.

4 Scope of these guidelines

The activities described in this chapter are limited to the verification of FHA outputs and to the validation of Safety Objectives (and related assumptions).

5 FHA Verification

5.1 Objective

The objective of ***FHA Verification*** is to demonstrate that the set of Safety Objectives produced from the FHA meet your organisation's Safety Target, i.e. the overall acceptable level of risk.

The output of the FHA process is a set of system Safety Objectives. These define the maximum frequency at which hazards can be accepted to occur. In this sense verification is often described as "getting the output right". Verification can be seen as a series of steps that involve reviewing the process followed in the FHA as well as reviewing the final output. The verification process is summarised in **Figure 1**.

Verification activity can take place in phase with the development of the FHA or be carried out at the end when the FHA is complete. The verification process is outlined below.

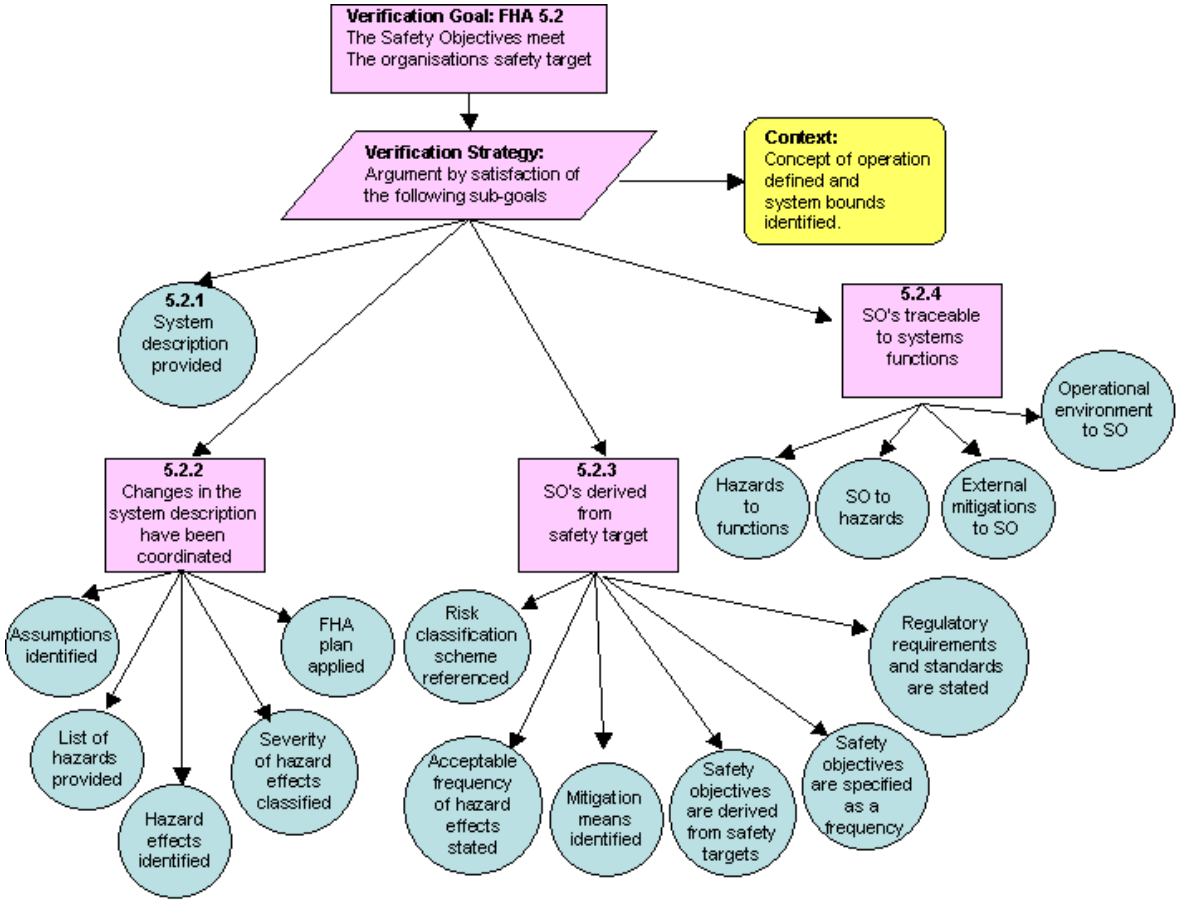

Figure 1: Verification goals

Note on GSN (Goal Structuring Notation) figures: The 'goal' of verification is symbolised as a rectangle and the verification 'strategy' as a parallelogram. The strategy relates to a number of facts to be verified during the verification process to establish the verification 'goal'. The round-cornered box symbolises the 'context' and relates to the context within which safety is to be assessed.

5.2 FHA Verification Process

To conduct the verification you will need the following:

- A description of the high level functions of the system;
- The FHA results, including the information collected during the various reviews of the FHA output.

It should be verified at the outset that the correct version of system description and FHA results are offered for verification. This is more likely if they have been placed under configuration management.

The following table may be used as a template for checking the availability of information and referencing it in the FHA you are verifying. The verification goals are labelled according to Figure 1.

Goal	Verification Item	Available (yes/no)	Reference in FHA (document, page)
FHA 5.2.1	**The System Description is documented** [Refer to FHA Chapter 1 Guidance Material OED]		
FHA 5.2.2	**Any changes in the system description as a result of the FHA have been coordinated between the safety team and project management team.**		
FHA 5.2.2.1	**Verify that assumptions are identified.**		
FHA 5.2.2.2	**List of hazards** [Refer to FHA Chapter 3 Guidance Material B1]		
FHA 5.2.2.3	**The hazard effects are documented.** [Refer to FHA Chapter 3 Guidance Material C]		
FHA 5.2.2.4	**The severity of the hazard effects and their classification are documented.** [Refer to FHA Chapter 3 Guidance Material D – Severity Classification Scheme, Table D2]		
FHA 5.2.2.5	**The FHA plan has been applied**. [Refer to FHA Chapter 2 Guidance Material A]		
FHA 5.2.3.1	**The Organisation Risk Classification Scheme is referenced.** [Ref FHA Chapter 3 GM E]		
FHA 5.2.3.2	**Statements of the acceptable frequency of hazard effects (Safety Objectives) are documented.** [Refer to FHA Guidance Material E –Risk Classification Scheme]		
FHA 5.2.3.3	**Mitigations means (external to the system under assessment) that are associated to Safety Objectives are identified**.		
FHA 5.2.3.4	**Safety Objectives are derived from Safety Targets.** [Refer to FHA Chapter 3 Guidance Material F – Safety Objective Classification Scheme]		
FHA 5.2.3.5	**Safety Objectives are specified as a frequency.** A unit should be given to specify the quantitative Safety Objective. (A Safety Objective is not a probability).		
FHA 5.2.3.6	**The applicable Regulatory requirements and standards are referenced.**		

Table 5.2A

Traceability:

The following items should be clearly traceable in the FHA.

Goal	Verification Item	Available (yes/no)	Reference in FHA (document, page)
FHA 5.2.4.1	**Hazards to System Functions (or to System scope when no function as such is associated)**		
FHA 5.2.4.2	**Safety Objectives to Hazards**		
FHA 5.2.4.3	**External mitigation means to Safety Objectives**		
FHA 5.2.4.4	**Operational environment to Safety Objectives**		

Table 5.2B

Note: The traceability between Safety Objectives and System Functions can be done directly or indirectly (using FHA-5.2.4.1 and FHA-5.2.4.2).

6 FHA Validation

6.1 Objective

The FHA-SOS (Safety Objectives Specification) should demonstrate how Safety Objectives are derived.

The objective of validating the FHA is to ensure that the outputs of the FHA process are correct and complete. In other words this can be referred to as "getting the right output", i.e. that the Safety Objectives are:

- complete – this is assured through a review of the process used in the FHA;
- correct - this is assured by reviewing the Safety Objectives themselves;
- credible - the safety-related assumptions are appropriately justified and documented.

The validation goals are summarised in the figures below. The numbers refer to the location of guidance on each goal in the tables which follow.

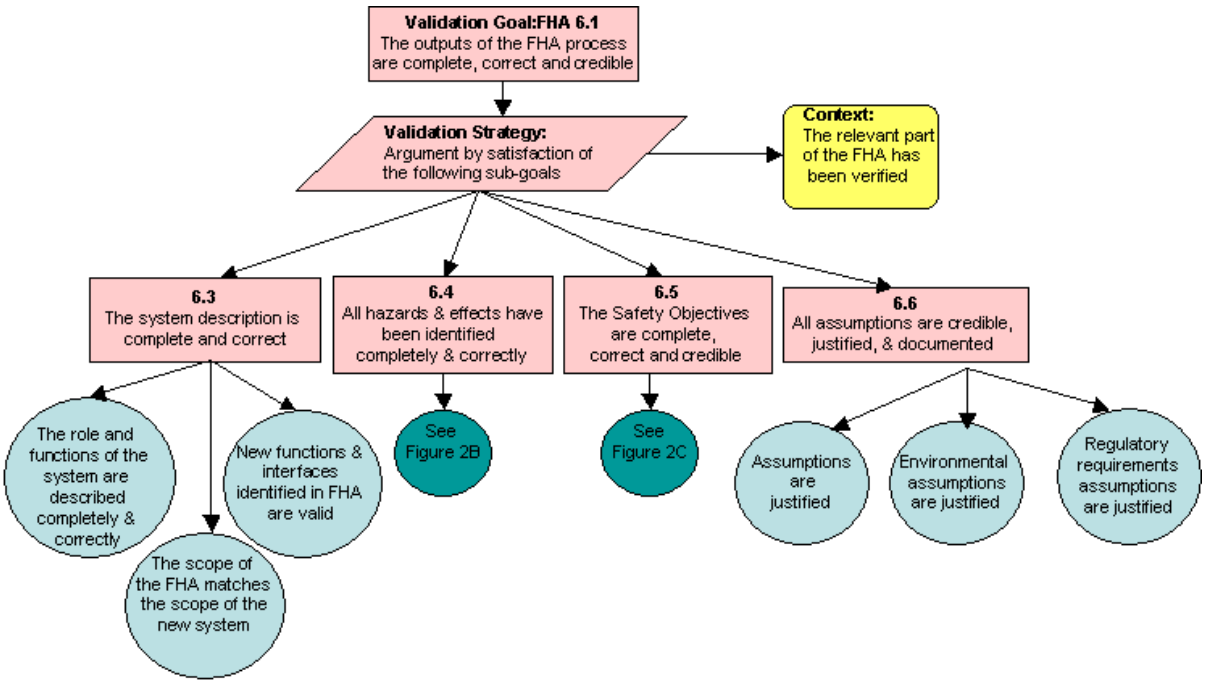

Figure 2A: Output of FHA Process Validation goals

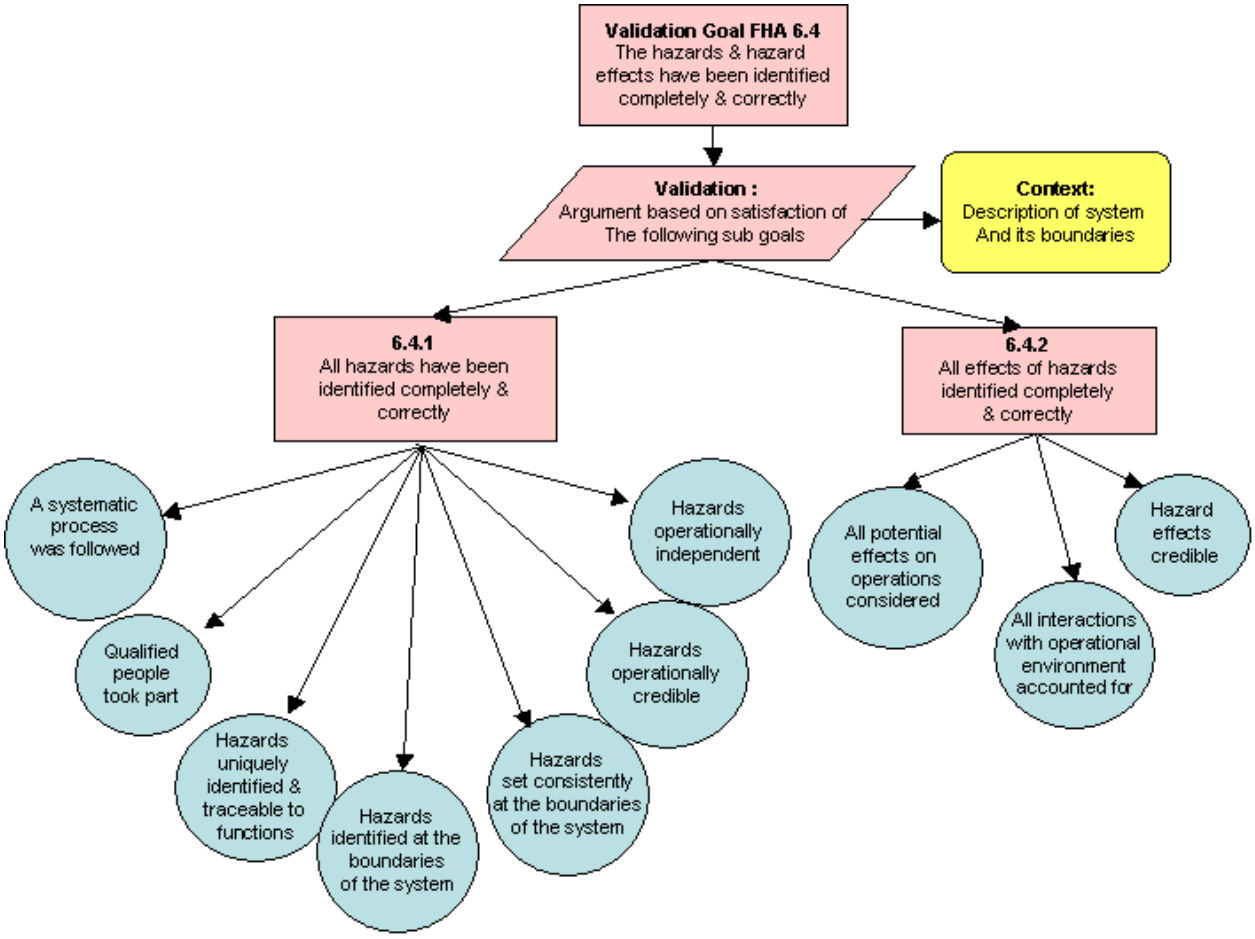

Figure 2B: Hazard and Hazard Effects Validation goals

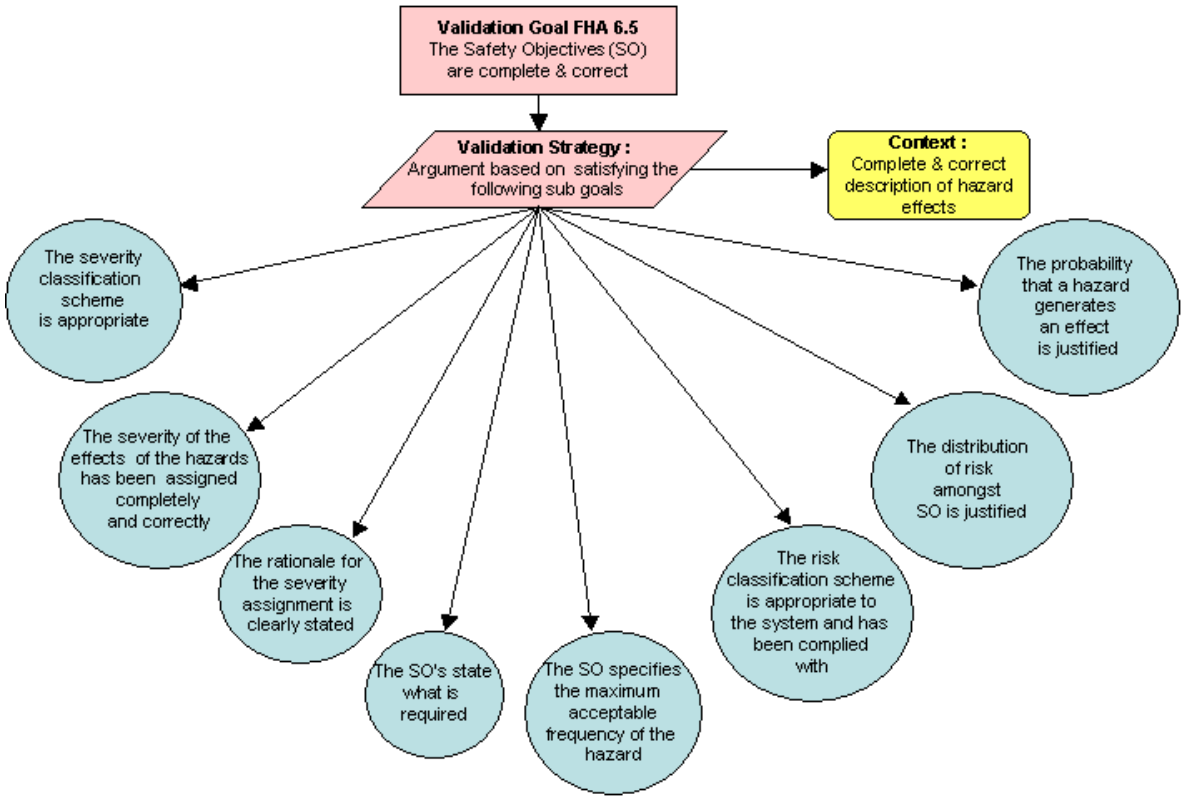

Figure 2C: Safety Objectives Validation goals

6.2 Validation Process

Before conducting this task you will first need to make sure of the following:

- That the verification of the FHA is complete.
- That you have a description of the high level functions of the system.
- That the Risk Classification Scheme is defined.
- That the hazard identification is documented.
- That the Safety Objectives have been documented.

The following tables list the validation items to be assessed for completeness and correctness. The validation goals are labelled according to Figures 2A, 2B & 2C above. The reviewer should signify by ticking the appropriate box whether the result is satisfactory i.e. conforming to the SAM methodology. The relevant FHA material should be referenced and qualifying comments made in the space provided, and amplified in the report as necessary.

6.3 The system description

The Reviewer shall confirm the following:

Goal	Validation Item:	Validation Result
FHA 6.3.1	**The system description provides sufficient detail to enable the reviewer to understand the functions of the system and how they interact internally and externally.** The first thing to confirm is that the system description itself is complete and correct. Refer to SAM Part 1, Chapter 1 - FHA Initiation and GM A– Operational Environment Definition which lists items to be considered. Most importantly, confirm that the role and functions of the system and its interactions are described. The functions of interest are the safety-related functions necessary for the planned operation. To further aid in understanding the system a configuration diagram showing the main functional elements should be included.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in FHA**	
FHA 6.3.2	**The scope of the FHA matches the scope of the new system or change to the existing system correctly and completely.** Review the description of the operational environment to confirm its completeness and correctness. The operational requirement and environment description is a useful tool for confirmation (assuming one is documented) otherwise make enquires to the relevant stakeholders.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in FHA**	
FHA 6.3.3	**Any new functions or interfaces identified in the FHA are valid.** Note that the FHA may develop new functions and interfaces as a result of the definition process and these should be coordinated with the project manager.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in FHA**	

Table 6.3

6.4 All hazards and hazard effects have been identified completely and correctly

6.4.1 All hazards have been identified completely and correctly

The primary concern here is that all the potential hazards have been identified including those arising from the system and the environment which could affect the safety of the planned operation.

The reviewer shall confirm the following:

Goal Item	Validation Item:	Validation Result
FHA 6.4.1.1	**A systematic process has been carried out:** Areas to be considered when conducting this activity are: • Functional hazard • Brainstorming • Databases • Other FHAs • Trials • Simulations • Operational data [Refer to FHA Chapter 3 Guidance Material B1 & B2]	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in FHA**	
FHA 6.4.1.2	**The process involved the people qualified to contribute ie ATCOs and / or aircrew.** Note, this includes confirming that the operational staffs are relevant to the operations, eg controllers validated and with appropriate ratings for the type of operation: approach, aerodrome and en-route, pilot flying in this airspace.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in FHA**	
FHA 6.4.1.3	**The Hazards identified are traceable to the functions of the subject system.** Ideally the hazards should be listed and labelled as described in Guidance Material B1, for example: *[failure mode]* of *[(sub)-function]* for more than *[exposure time]* in *[Operational Environment]* Note: For the non-functional hazards [Refer to FHA Chapter 3 Guidance Material B2], the traceability may be between the hazards and the scope of the system under assessment "as a whole" (not to a specific function).	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in FHA**	

Goal Item	Validation Item:	Validation Result
FHA 6.4.1.4	**Hazards are identified at the boundary of the system.** The system boundary may be a particular ATM function, a type of operation, a sector of operations or an area of operations etc. Cause and effect should be analysed within the declared boundary.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in FHA**	
Goal Item	**Validation Item:**	**Validation Result**
FHA 6.4.1.5	**Hazards are set consistently at the boundary of the system.** Example of inconsistent hazards (if scope = surveillance function, then radar failure = cause, hazard = loss of surveillance, effect = loss of separation)	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in FHA**	
FHA 6.4.1.6	**The hazards are operationally credible.** If some hazards are considered as not operationally credible, then there are listed but classified as “not credible” (so not to be further analysed) with a rationale sustaining that claim. , This will allow, later, challenging the rationale in case of change in the operational environment that could impact such rationale or in case of actual occurrence.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in FHA**	
FHA 6.4.1.7	**The hazards are independent.** The occurrence of a hazard should not infer the occurrence of another hazard of the same system under assessment. If so, then one new hazard (encompassing both) should replace the previously specified one**.**	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in FHA**	

Table 6.4A

6.4.2 The hazard effects have been identified completely and correctly

The Reviewer shall confirm the following:

Goal Item	Validation Item:	Validation Result
FHA 6.4.2.1	**All potential effects on operations have been considered.** FHA Guidance Material C identifies the effects on operations that need to be considered including the following criteria. • Effects on the ability to provide or maintain safe Air Navigation Service(s) • Effects on the functional capabilities of the airborne and ground parts of the ATM System • Effects on ATCO and/or Aircrew • Effects on the environmental mitigation means (not part of the system under assessment) [Refer to FHA Chapter 3 Guidance Material D]	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in FHA**	
FHA 6.4.2.2	**All interactions with the operational environment are accounted for.** For example, a hazard affecting the ability to provide or maintain safe Air Navigation Service(s) in one sector of operations may also have an adverse effect on adjacent sectors due to increased workload in those sectors while rerouting traffic from the affected sector.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in FHA**	
FHA 6.4.2.3	**All hazard effects are credible** If some effects are considered as not operationally credible, then there are listed but classified as “not credible” (so not to be further analysed) with a rationale sustaining that claim. , This will allow, later, challenging the rationale in case of change in the operational environment that could impact such rationale or in case of actual occurrence.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in FHA**	

Table 6.4B

6.5 The Safety Objectives are complete and correct

The Reviewer shall confirm the following:

Goal	Validation Item:	Validation Result
FHA 6.5.1	**The severity classification scheme is appropriate to the type of operations envisaged for the system under assessment.** [Refer to FHA Chapter 3 Guidance Material D]	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in FHA**	
FHA 6.5.2	**The reviewer shall confirm that the severity of the effects of hazards have been assigned completely and correctly.** The different effects of hazards are described in the Severity Classification Scheme Guidance Material D. Each class of hazard effect has a defined severity indicator which can be found in Table D-2. One or more sets of severity indicators may be used. There is some degree of overlap between them and the user should have chosen those which best suit their conceptual model of the system. Not all sets of indicators, or all indicators within a set, are necessarily relevant or meaningful for every assessment.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in FHA**	
FHA 6.5.3	**The rationale for the severity assignment is clearly stated.** A clear and complete description of the effects (especially what ATCO and/or aircrew have to do or can not do anymore) should be provided such that any reviewer that did not take part to the assessment can objectively understand and support the severity assignment.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in FHA**	

Goal Item	Validation Item:	Validation Result
FHA 6.5.4	**The Safety Objectives state what is required.** [See FHA Chapter 3 GM G §6]	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in FHA**	
FHA 6.5.5	**The Safety Objective specifies the maximum acceptable frequency of occurrence of the hazard.** e.g. A or many unit(s) (flight hour, operational hour, per sector, etc.) is(are) used to specify Safety Objectives. FHA Chapter 3 Guidance Material G explains the various methods of setting Safety Objectives. One approach (mainly for "Uncertain Starters" or "Willing Developers") consists in focusing on the Worst Credible case (not the Worst Case). 'Worst' means the most unfavourable conditions – e.g. extremely high levels of traffic or extreme weather disruption. 'Credible' implies that it is not unreasonable to expect to experience this combination of extreme conditions within the operational lifetime of the system; so that such a scenario leading to such an effect has to be considered. This approach (Worst Credible case) is not the only one acceptable and anyhow is not the most accurate and complete one (See Method 2 of FHA Chapter 3 GM G).	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in FHA**	
FHA 6.5.6	**The Risk Classification Scheme is complied with.** The Risk Classification Scheme (RCS) defined by the Organisation should be used. A RCS sets the maximum acceptable rate of occurrence of hazard effect (Safety Target ST) for a corresponding severity class of the hazard effect. [Ref: FHA Chapter 3 Guidance Material E]. Safety Objectives should be derived from the Safety Targets set in the RCS. The combination of Safety Objectives and mitigation means (external to the system under assessment) should satisfy the Safety Target per severity class.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in FHA**	

FHA 6.5.7	**Even or uneven distribution of risk amongst Safety Objectives is justified.** If the hazards having the same Worst Credible Consequence are allocated an even part of the risk associated to such effect severity, then such assumption shall be justified.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in FHA**	
FHA 6.5.8	**The probability that the hazard generates an effect (Pe) is justified.** A Pe different from 1 shall be justified and requirements set on the external mitigation means that contribute to set such Pe.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in FHA**	

Table 6.5

6.6 All safety related assumptions are credible, appropriately justified and documented

The reviewer shall confirm that the safety-related assumptions about the system its operational environment and its regulatory framework were valid at the outset of the FHA, taken into account during the FHA and remain valid at the end.

Goal	Validation Item:	Validation Result
FHA 6.6.1	**The system assumptions are justified.** Confirm that there is traceable evidence to support the justification. It may be claimed for example, that no change to existing ATC procedures will be required etc. Such assumptions may require assessment in their own right and involving the system element concerned to validate the completeness and correctness. Confirm assumptions about the boundary of the system coming within the scope of the FHA.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in FHA**	
FHA 6.6.2	**Environmental assumptions are justified.** Confirm that there is traceable evidence to support the justification. It may be claimed for example, that the Operational Environment will exclude certain type of traffic etc. Such assumptions may require a check for consistency and completeness.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in FHA**	
FHA 6.6.3	**Regulatory requirements assumptions are justified.** Confirm that there is traceable evidence to support the justification. It may be claimed for example, that the system will meet regulatory requirements etc. Such assumptions may require a check for consistency and completeness between the regulatory requirement and the system requirements.	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in FHA**	

Table 6.6

6.7 FHA report

The FHA report should support decision making about the safety acceptability of the system definition. The report should describe how the Safety Targets and/or risk acceptability criteria have been translated into Safety Objectives for the system. The FHA report should be clear, traceable and approved by stakeholders.

The FHA report should contain:

- a description of the system being assessed;
- a Risk Classification Scheme (with its Safety targets);
- a list of assumptions used to derive the Safety Objectives;
- justification material for external mitigation means;
- a list of hazards and their consequences;
- Safety Objectives.

The FHA 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
FHA 6.7.1	**The FHA facilitator and report writers are suitably qualified.** [See FHA Chapter 3 GM A on choosing an FHA facilitator]	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in FHA**	

FHA 6.7.2	**The reviewer shall comment on the quality of the process followed and whether, it is well documented, accessible and credible (the Safety Objectives appear to be appropriate).** To specify Safety Objectives, the following criteria have been appropriately covered (an acceptable rationale exists to sustain the choices made to address those criteria): • Consistency and correctness of hazard scope (6.4.1); • Completeness of hazard identification (6.4.1); • Probability that hazard lead to effects (Pe) (6.5.8); • Independence of hazards (6.4.1.7); • Distribution of Safety Objectives (e.g; Even-distribution or un-even) (6.5.7)	Satisfactory ☐ Requires Action ☐
	Comment / action: **Reference in FHA**	

Table 6.7