SAFETY OBJECTIVES SPECIFICATION

1 OBJECTIVES

The objectives of the FHA - ***Safety Objectives Specification*** step are:

- To identify all potential hazards associated with the system;
- To identify hazard effects on operations, including the effect on aircraft operations;
- To assess the severity of hazard effect(s);
- To derive Safety Objectives, i.e. to determine their acceptability in terms of hazard's maximum frequency of occurrence, derived from the severity and the maximum frequency of the hazard's effects.

Safety Objectives are qualitative or quantitative statements that define the maximum frequency at which a hazard can be accepted to occur.

Additionally, it is recommended to assess the intended aggregated risk (only if the method to set Safety Objectives does not make an explicit link to intended acceptable level of risk).

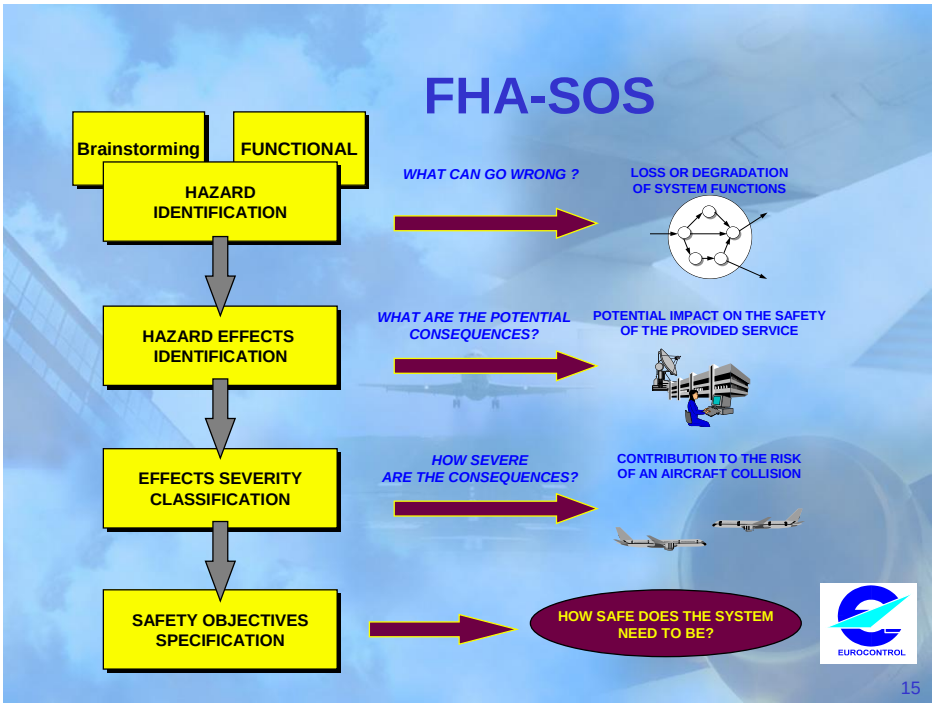


Figure 3.1: Safety Objective Specification (without "assess intended aggregated risk")

2 INPUT

- Information gathered or derived as an output of the FHA Initiation step.
- Severity Classification Scheme (refer to Guidance Material D)
- Risk Classification Scheme (refer to Guidance Material E)
- Safety Objective Classification Scheme (refer to Guidance Material F)

3 MAJOR TASKS

For each system function and combination of functions, the "four+one"-stage process illustrated in Figure 3-1 is conducted. This process aims at answering the following questions:

1. ***Identify Potential Hazards***: What could go wrong with the system and what could happen if it did?
2. ***Identify Hazard Effects***: How does it affect the safety of operations, including the safety of aircraft operations?
3. ***Assess Severity of Hazard Effects***: How severe would those effects be?
4. ***Specify Safety Objectives:*** How often can we accept hazard to occur?
5. ***Additionally, Assess the intended aggregated risk:*** What is the foreseen safety level aimed at?

Notes.

Tasks 1 and 2 require creative consideration of what can happen, informed by broad knowledge of the system functions and interfaces, within the specific environment of operation. For this reason it is usually best to undertake, or at least initiate, this process in a structured meeting between the various organisations involved – the users and developers of the system. Advice on the planning and conduct of such meetings (FHA sessions) is given in Guidance Material A and B of this Chapter 3.

Tasks 3 and 4 (and 5) involve making judgements about the intended risk associated with such sequence of events, and how often their occurrence can be accepted. These tasks can also be conducted in a group session where operational staff (ATCO, pilot) presence is mandatory (Guidance Material A of this Chapter 3 gives some advice). Where the system being assessed is complex, this may involve some more detailed analysis, which will generally be better done by a team outside the meeting.

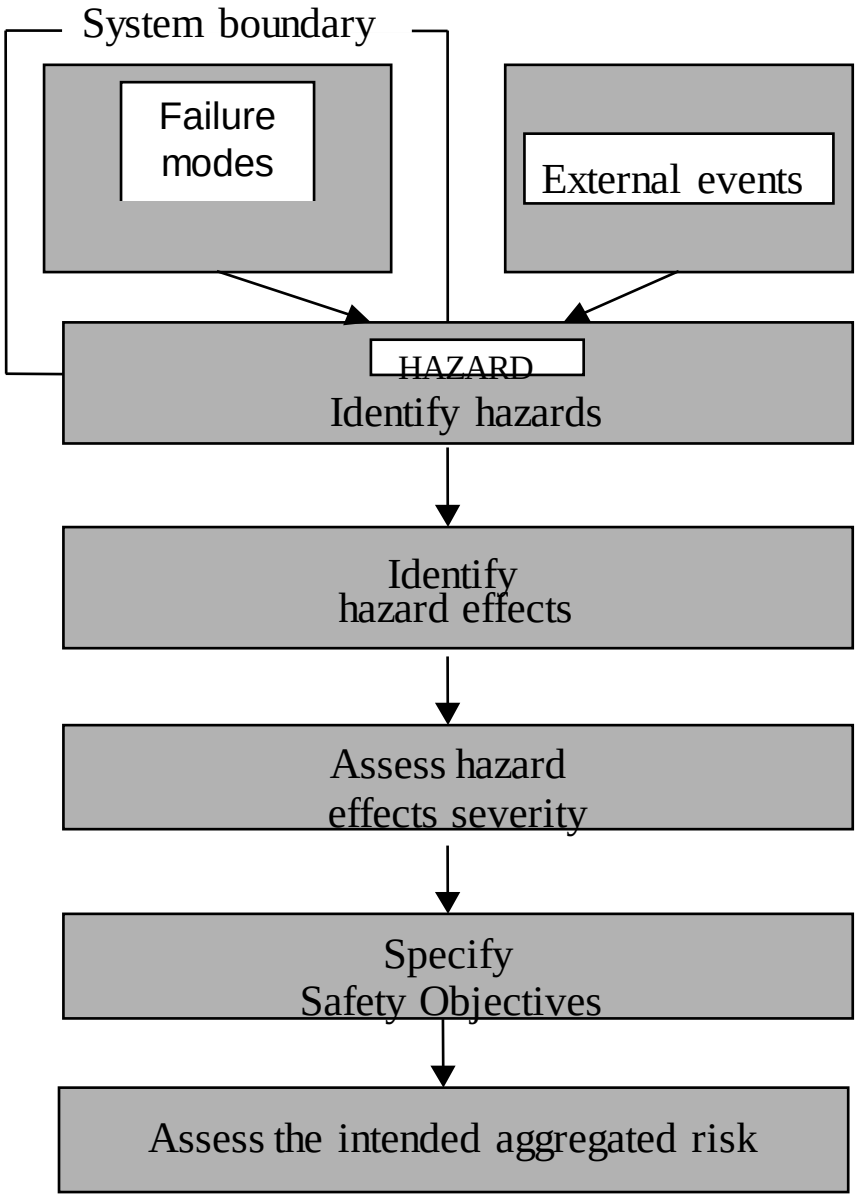


Figure 3-2. Overall FHA-SOS Process

3.1 Identify Potential Hazards

The purpose of this task is to identify potential hazards, resulting in the degradation of system function(s).

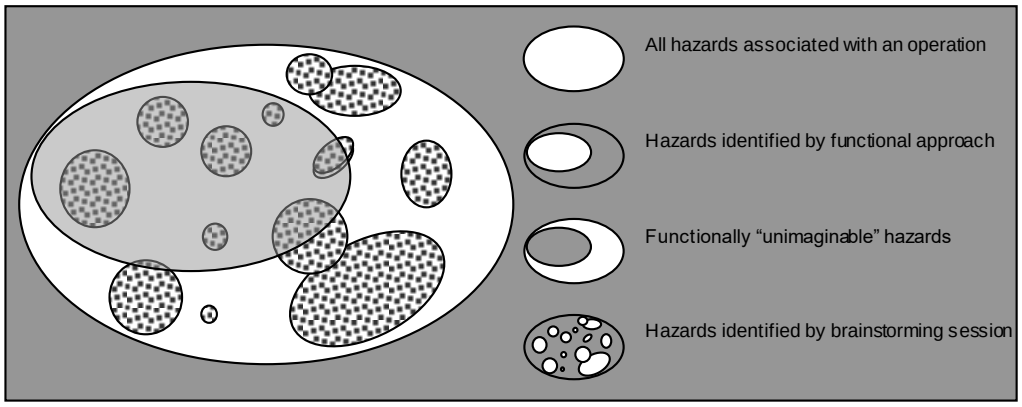
Hazards are the consequences of failures within the system, combination of failures and interactions with other systems and external events in the environment of operation. Hazards appear at the boundary of the system under assessment.

To identify potential hazards, it is necessary to consider the various ways each individual function of the system can fail (that is the failure mode).

FHA is limited to the selection of failure modes and does not address the identification of their causes (failures). These causes will be identified during PSSA when design is available.

The recommended method for identifying hazards is the combination of:

- **Systematic** application of a set of keywords to each function of the system under assessment. (Guidance Material B1 provides examples of suitable keywords for failure modes and external events);
- "**Brainstorming**" sessions aiming at finding "functionally unimaginable" hazards by assessing normal, abnormal and particular combinations of un-related events scenarii. (See Guidance Material A and B2 of this Chapter 3);
- Analysis of hazard database, accident/incident reports, other FHA, lessons learned.



The process of identifying hazards should take into account the following:

- The exposure time to the hazard;
- The ability to detect the hazard and the external event occurrence;
- The rate of development of the hazard (sudden or fast or slow).

Hazards are identified at the boundary of the system or service under assessment e.g. hazard at:

- Air Navigation System or Service level (e.g. total loss of ATM service for more than 30');
- Service level (e.g. datalink services: mis-direction of ATC Clearance);
- Functional level (e.g. surveillance: corruption of track position);
- System level (e.g. Air Traffic Control Centre: loss of adjacent centre connection);
- Sub-system level (e.g. FDP equipment: delay for more than 30' of Flight plan update).

(Refer to Guidance Material B1 of this Chapter 3).

An end-to-end (or total system) approach is needed for system safety assessment in order to assess the impact of the system hazards at the overall ANS level (so including the end user: aircraft, aircrew and passengers).

Some ANS/ATM-only hazards could be identified due to local ANS/ATM implementation of the system (e.g. Local ANSP HMI related hazards for Air-Ground data communications).

3.2 Identify Hazard Effects

The purpose of this task is to identify the possible consequences of hazards on operations, including the effects of hazards on aircraft operations.

In order to determine the effects of hazards on operations, various elements should be considered, such as:

- Effects on the ability to provide safe Air Navigation Service;
- Effects on ATCOs working conditions (e.g., workload, ability to perform his/her tasks);
- Effect on Air Crew working conditions (e.g., workload, ability to perform his/her tasks);
- Effects on Aircrew and ATCOs ability to cope with adverse operational and environmental conditions;
- Effect on the functional capabilities of the aircraft;
- Effect on the functional capabilities of the ground part of the Air Navigation System.

When the system under assessment is at a lower level than the Air Navigation Service Provision, it could appear difficult to assess the effect of such lower level hazards directly on aircraft operations. However, the aim is to assess effects also on aircraft operations (aircraft equipment or Flight crew), even if the immediate effects are on ATCOs workload or ability to maintain safe separation and/or on the functional capabilities of the ground part of the Air Navigation System.

In general, identification of the effects of hazards is best performed within the FHA session where operational staff (ATCO, pilot) presence is mandatory (See Guidance Material A).

Guidance Material C provides more detailed suggestions for the factors to take into account in determining the effects of hazards.

3.3 Assess Hazard Effects Severity

The purpose of this task is to classify the severity associated with each hazard effect. The Severity Classification Scheme is used for this purpose (refer to Guidance Material D).

The overall criterion to assess the severity of hazard effects is the effect on operations. It includes the effect on aircraft operations but also, especially in cases where the system to be changed/modified is at the lower level, additional criteria may be used, such as those described in Guidance material C.1 of this Chapter 3.

When assessing the severity of the hazard effects on operations, including aircraft operations, the following sets of indicators should be considered:

- Effects on Air Navigation Service: effects on ANS within the area of responsibility, ATCO and Flight Crew working conditions, ATCO and Air Crew ability to cope with adverse operational and environmental conditions;
- The exposure to the hazard: exposure time, number of aircraft exposed;
- Recovery indicators: annunciation, detection and diagnosis, contingency measures available, rate of development of the hazardous condition;
- The flight phase (effects may vary from flight phase to flight phase);

The rationale for the classification should be given: this could be engineering and/or operational judgement, relevant experience with similar system, etc.

Guidance Material D provides some advice on the practical use of a Severity Classification Scheme within the FHA.

3.4 Specify Safety Objectives

The purpose of this task is to specify system Safety Objectives in order that the system achieves an acceptable level of risk. Safety Objectives are derived from the Organisation Risk Classification Scheme (See Guidance Material E) or Safety Objective Classification Scheme (See Guidance Material F). Guidance Material G illustrates the process of Safety Objectives derivation.

Safety Objectives specify the maximum acceptable frequency for the occurrence of a hazard. Safety Objectives should be specified quantitatively.

In cases where it appears impracticable, qualitative Safety Objectives may be specified substantiated with a rationale explaining why.

Safety Objectives may be defined relative to those for some system, which is already accepted as safe enough (usually the current system) with a rationale explaining why Absolute Quantitative Safety Objectives were found impracticable.

Guidelines to choose the most appropriate form for the Safety Objectives and to set quantitative values where achievable are given in Guidance Material G of this Chapter 3.

3.5 Assess the intended aggregated risk (or effect on safety)

At the FHA level, "Intended risk" is used as only a goal for a level of risk or safety level can be specified (FHA is done during the system definition phase). The actual risk will be finally achieved only when operating the system and consequently actual risk will be assessed during SAM 3rd step: SSA (System Safety Assessment).

Note: This step has to be achieved only if Safety Objectives are set without an explicit link to an intended acceptable level of risk (so using Methods 2, 3 or 4 of SAM-FHA Guidance Material G as only Method 1 makes an explicit link to risk).

In order to make text more readable, here after "*change*" means "change(s) to the existing system or new system".

The impact of the *change* could be:

- **Positive Impact.** There are two scenarii for positive impact on safety.
  - Firstly – *change* mitigates risk for risk not created by the *change*.
  - Secondly – *change* mitigates risk for risk created by the *change* itself and achieves a lower risk than before the *change*.

  The list of potential risk reducing effects should be drawn to assess that impact.

- **Negative Impact.** To create additional risk and/or not to mitigate the risk the *change* is designed to mitigate.

  This negative impact can be acceptable only as long as the final system (including the *change*) intends to achieve an overall risk that remains acceptable (even though the *change* does not improve the level of safety).

Changes are usually introduced to improve performance while not impairing and where possible improving the level of safety. To assess the overall safety effect, both positive and negative effects of the *change* should be considered.

At the end of the FHA, the assessment should finally demonstrate that the system (including the *change*) intends to achieve an overall acceptable risk. A useful tool to achieve that is "Barrier Analysis" (See Guidance material I of this Chapter 3). It consists in assessing for all the barriers:

- Negative impact:
  - Decide on the level of barrier efficiency degradation because of any single hazardous scenario and overall hazardous scenarii identified;

- Decide on the overall effect on the risk due to the overall barriers efficiency degradation;

- Positive impact:
  - Decide on the level of barrier efficiency increase because of the *change*;
  - Decide on the overall effect on the risk due to the overall barriers efficiency increase;
- Net result:
  - Decide on the combined effects of barrier efficiency degradation and barrier efficiency increase.

4 OUTPUT

The outputs of this step are the lists of:

- Hazards, with the rationale for the severity classification of their effects;
- Safety Objectives;
- Assumptions.

Guidance Material H describes possible means for recording the outputs of FHA sessions.

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

List of Guidance Material of FHA Chapter 3:

A. Planning and conducting FHA session;
B. Identification of failure modes, external events and hazards;
C. Identification of Hazard effects;
D. Severity Classification Scheme;
E. Risk Classification Scheme;
F. Safety Objective Classification Scheme;
G. Methods for setting Safety Objectives;
H. Results records;
I. Barrier Analysis;
J. TLS (Target Level of Safety) apportionment method.

Other Guidance Material applying to this Chapter 3 (FHA - Safety Objectives Specification):

- SAM – Part IV Annex A: Acronym;
- SAM – Part IV Annex B: Glossary;
- SAM – Part IV Annex D: Safety Techniques Survey (report and technical annex).