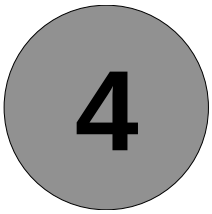

FHA EVALUATION

1 OBJECTIVES

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

- Verification;
- Validation;
- Process Assurance.

Note: The division into three major tasks (Verification, Validation and Process Assurance) is intended to help the Methodology's users ensuring correctness and completeness of the process.

It is recognised that there are areas of overlap between the activities suggested under each, and that the precise method of implementation will depend on the system considered and the user's current practices.

The guidance is not intended to specify the only way of meeting the FHA objectives.

Their relationships with the overall process are shown in Figure 4-1.

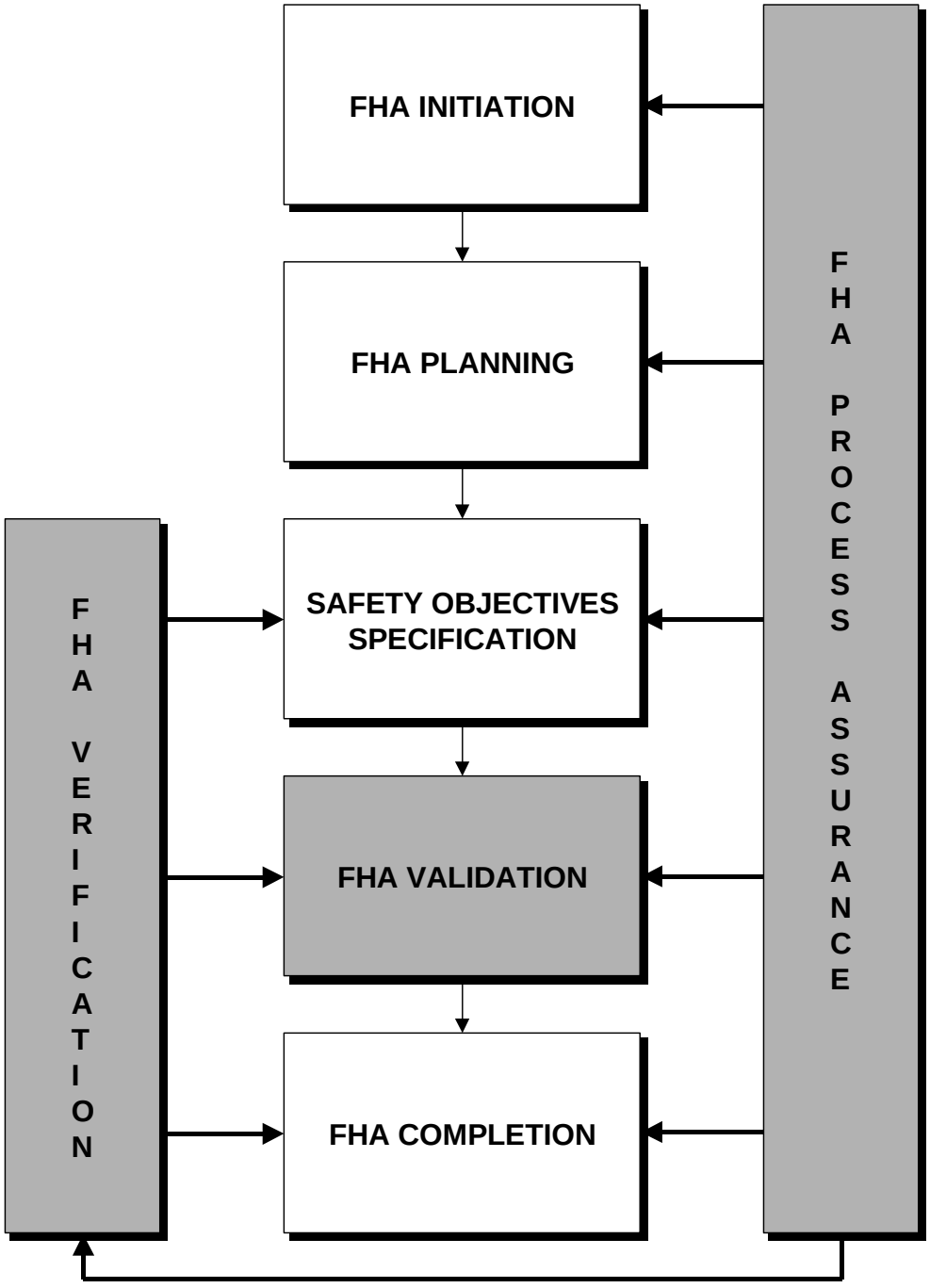

Figure 4-1 - Relationships between FHA Evaluation Activities and the Overall FHA Process

The objective of ***FHA Verification*** is to demonstrate that the set of Safety Objectives meet the Organisation Safety Target, i.e. the overall acceptable level of risk ("getting the output right").

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

- The Safety Objectives are (and remain) correct and complete;
- All safety-related assumptions are credible, appropriately justified and documented.

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

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

2 INPUT

- Information gathered or derived during the FHA steps.
- Initial Safety Plan and FHA Plan.
- Intermediate and final outputs of the FHA process.

3 MAJOR TASKS

Notes.

Relationships with overall System Verification and Validation activities. *The activities described in this chapter are limited to the verification of FHA outputs and to the validation of Safety Objectives (and related assumptions). These specific activities could be combined with or integrated into the overall system Definition Verification and Validation processes. It is essential to consider, in the overall Verification and Validation processes, other system specification errors (for example, operational, interoperability, security, engineering or environmental specifications),which could subsequently impact safety.*

Relationships with Quality Management activities*. As the tasks of Verification, Validation and Process Assurance are similar in intent with Quality Management activities, they could be combined with or integrated into the Quality Management process.*

Independence. *To ensure an independent view, all of these activities should, where possible, be conducted by one or more persons not involved in the performance of the assessment itself.*

For large and complex Projects/Programmes, these tasks could be performed by an independent department or organisation.

While there are benefits in independent checks, the findings should be fed back to those who were involved in the original work. The participants in the FHA session, for example, should have the opportunity to comment on whether their input has been correctly understood. They may also need to review their assumptions once the collated results are available, giving a clearer view of the implications than during the FHA session.

Such feedback will have the added benefit of contributing to future motivation to take part in such exercises (some useful output being seen to have emerged) and to 'organisational learning' – the breadth and depth of knowledge within the organisation.

3.1 FHA Verification Tasks

- Review and analyse the results of the FHA process.

Note: Verification is ongoing throughout the FHA. It also applies to FHA Validation.

Note: See Guidance Material A of this Chapter 4.

3.2 FHA Validation Tasks

- Review and analyse the Safety Objectives 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 safety-related assumptions about the system, its operational environment and its regulatory framework to ensure their completeness and correctness.
- Review and analyse traceability between functions, hazards, hazard's effects and Safety Objectives.
- Review and analyse the credibility and sensitivity of Safety Objectives with respect to assumptions and risk.

Note: See Guidance Material B of this Chapter 4.

3.3 FHA Process Assurance

The FHA Process assurance task should at least ensure in accordance with the FHA Plan that:

- The FHA steps are applied;
- Assessment approaches (e.g. use of safety methods and techniques) are applied;
- All outputs of the FHA steps, including FHA Verification, FHA Validation and FHA Process Assurance are formally placed under configuration management;
- Any deficiencies detected during FHA Verification or FHA Validation activities have been resolved;
- The FHA process would be repeatable by personnel other than the original analyst(s);
- The findings have been disseminated to interested parties;
- Outputs of the FHA process are not incorrect and/or incomplete due to deficiencies in the FHA process itself.

Note: *When changes are made to the specification, design, implementation or use of a system, process assurance should also ensure that the impacts of these changes on the current FHA results have been considered and that all required assessment, verification and validation activities have been performed.*

Note: See Guidance Material C of this Chapter 4.

4 OUTPUT

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

The FHA output comprises:

- Results of the FHA Verification task: including the information collected during the various reviews of FHA output, for assurance and evidence that Safety Objectives meet Organisation Safety Target;
- Results of the FHA Validation task: including the arguments for assurance and evidence of the completeness and correctness of Safety Objectives and assumptions;

- Results of the FHA Process Assurance task: including the information collected during the various activities for assurance and evidence that the FHA process as described in the FHA Plan has been conducted and that FHA process is correct and complete.