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

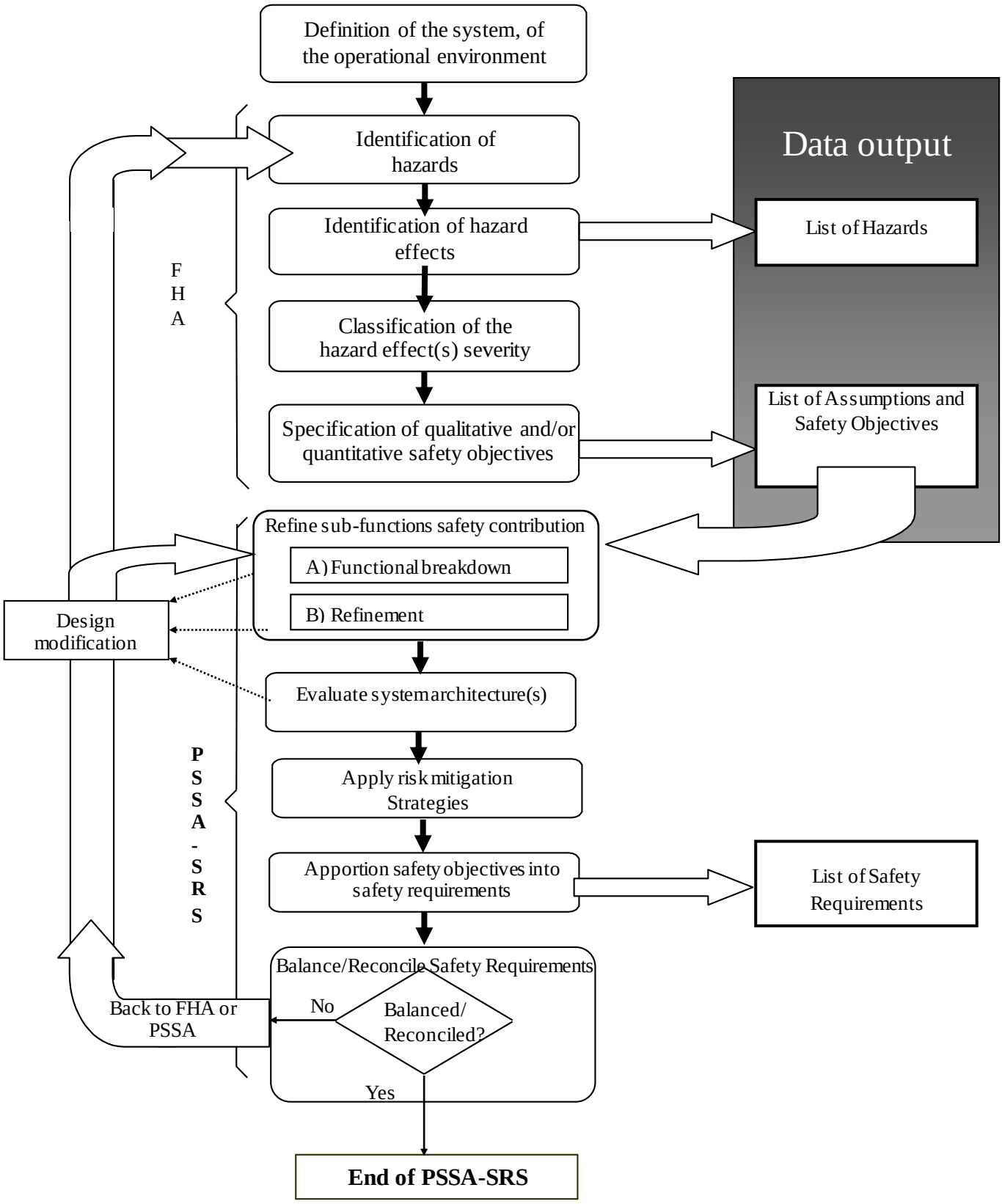
- PSSA Initiation output:
  - Description of the system architecture(s) and rationale;
  - The Operational Environment Description (OED);
  - The list of assumptions;
  - The list of hazards, with the rationale for the severity classification of their effects(s) (FHA output);
  - The Safety Objectives (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 Objective**s** (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 Objective**s** (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 objective**s,** 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	• 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	• 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	• 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	• 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.