1

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.