



GUIDANCE MATERIAL:

SSA REPORT

The SSA documentation records the results of the SSA assessment process. This document will be updated through the complete system life cycle.

In order to make this document readable and conveying efficiently key messages and results of SSA, recommendations are:

- To keep the body of the document short (around 15 pages);
- To make this document conclusive: state whether the system achieves or not an acceptable risk and clearly and concisely list the main findings

of the SSA such as where Assurance & Evidence is acceptable or insufficient ;

- To include an executive summary;
- To contain the results of detailed analyses in annexes.

A possible structure for the SSA report is given in Table 5.1.

Table 5.1. Structure of the SSA Report

Executive Summary

It should focus on main messages delivered by SSA, such as: is system achieving an acceptable risk in its operational environment and where Assurance & Evidence is acceptable or insufficient.

Introduction

This section should describe:

- The objectives of the document.
- The scope of the SSA (What was addressed in the SSA process and what was not addressed).
- The structure of the document.

System Description

This section should provide an overview of the system design and architecture.

It will cover, or reference, documentation describing:

- The system definition, architecture and design;
- The purpose and boundaries of the system;
- The system operational environment (if appropriate, the assumptions made about this operational environment);
- The external interfaces (including technical data).

It will also identify whether the system is new, a replacement or a modification of an existing system.

Safety Criteria

This section should identify the specific safety criteria used to define the Safety Assurance & Evidence. For example,

- Applicable Safety Regulatory Requirements;
- (International) Standards
- Approach to collect and accept Safety Assurance & evidence, when appropriate.

Safety Assurance & Evidence Identification

The results are usually best presented in a tabular format.

If numerous, this part should focus on the main Safety Assurance & Evidence and make reference to the complete list in an annex.

Summary and Conclusions

This part should summarise the results of the SSA process. It should include:

- The phase of the lifecycle associated to this specific SSA report;
- The list of verified and validated: assumptions, most critical Safety Objectives/hazards, Safety Requirements;
- The main conclusions of the SSA validation, verification and process assurance activities;
- A statement whether the system achieves or not an acceptable risk.

This part should also identify any architectural elements or mitigation means or failures or hazards requiring additional analysis, and/or other priorities for further attention in the development/assessment cycle.

Annexes

- Detailed result tables;

- Cross-references to other documents produced within the SSA process, such as the SSA Plan (as described in SSA Chapter 2) and the Validation/Verification and Process Assurance reports (as described in SSA Chapter 4);
- References to external documents – e.g. regulatory requirements, standards, documentation for systems interacting with the proposed system;
- Detailed results of analyses (FTA, FMEA, CCA, Sensitivity Analysis, ...)
- Traceability matrices

Evidence <> Safety Requirements

Evidence <> System Elements

Evidence <> Safety Objectives

Evidence <> Assumptions (e.g. External Mitigation Means,

Operational

Environment, .. See FHA & PSSA)