3

SAFETY ASSURANCE & EVIDENCE COLLECTION

1 OBJECTIVE

The objective of the ***Safety Assurance & Evidence Collection*** step is to collect evidences and to provide assurance that:

- each system (people, procedure, equipment) element as implemented meets its **Safety Requirements**;
- the system as implemented satisfies its **Safety Objectives** throughout its operational lifetime (till decommissioning);
- any **assumptions** made during the safety assessment process is correct;
- the system satisfies **users expectations** with respect to safety;
- the system achieves an acceptable **risk**.

2 INPUT

- Description of the system architecture and its rationale;
- The updated list of assumptions (on which Safety Objectives and Safety Requirements might be funded);
- The Operational Environment Description (OED);

- The list of hazards, with the rationale for their effects severity classification (FHA output);
- The Safety Objectives (FHA output);
- System element (People, Procedures, Equipment) Safety Requirements allocated by PSSA;
- Procedures and Equipment Assurance Levels allocated by PSSA;

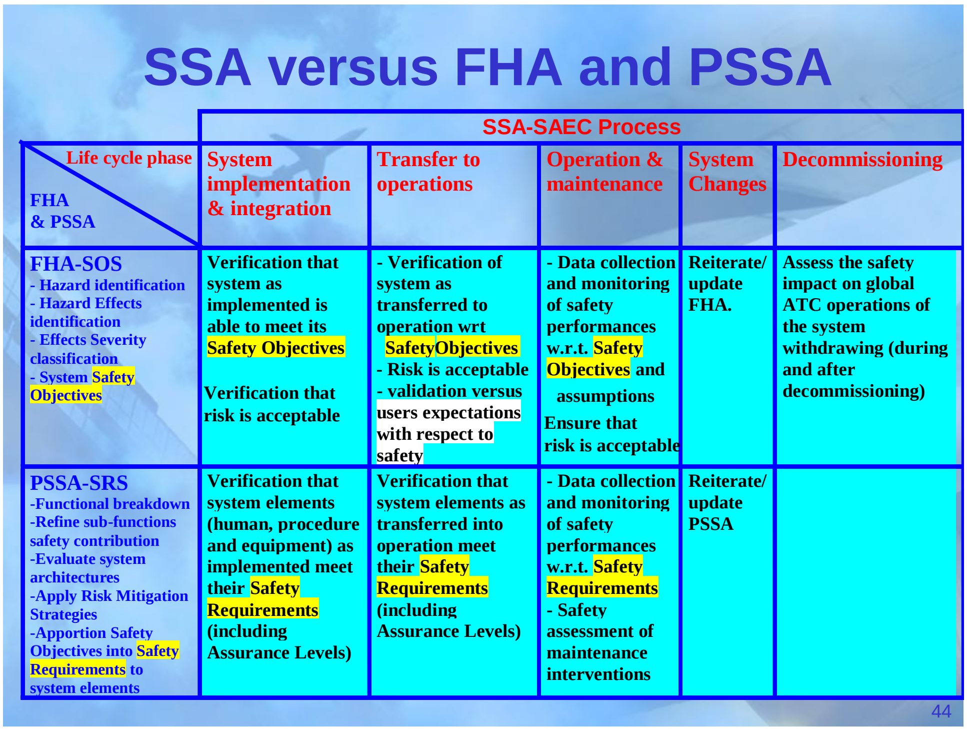
  PAL: Procedure Assurance Level;

  SWAL: SoftWare Assurance Level;

  HWAL: HardWare Assurance Level.

  Note: PAL, HWAL and SWAL are further explained in Guidance Material A of PSSA – Chapter 3.
- Safety evidence demands as specified by FHA and PSSA: safety-related specifications for verification activities (for example: tests, real-time simulations, specific analysis and studies, ..) and for validation activities (for example: trials, transition analysis, ..);
- FHA and PSSA analyses results (For example: FMEA, FTA, CCA, …).

3 MAJOR TASKS



SSA versus FHA and PSSA

Life cycle phase / FHA & PSSA	SSA-SAEC Process				
	System implementation & integration	Transfer to operations	Operation & maintenance	System Changes	Decommissioning
FHA-SOS - Hazard identification - Hazard Effects identification - Effects Severity classification - System Safety Objectives	Verification that system as implemented is able to meet its Safety Objectives Verification that risk is acceptable	- Verification of system as transferred to operation wrt SafetyObjectives - Risk is acceptable - validation versus users expectations with respect to safety	- Data collection and monitoring of safety performances w.r.t. Safety Objectives and assumptions Ensure that risk is acceptable	Reiterate/ update FHA.	Assess the safety impact on global ATC operations of the system withdrawing (during and after decommissioning)
PSSA-SRS -Functional breakdown -Refine sub-functions safety contribution -Evaluate system architectures -Apply Risk Mitigation Strategies -Apportion Safety Objectives into Safety Requirements to system elements	Verification that system elements (human, procedure and equipment) as implemented meet their Safety Requirements (including Assurance Levels)	Verification that system elements as transferred into operation meet their Safety Requirements (including Assurance Levels)	- Data collection and monitoring of safety performances w.r.t. Safety Requirements - Safety assessment of maintenance interventions	Reiterate/ update PSSA	

44

An overview of Safety Assurance & Evidences Collection is provided hereafter for each of the lifecycle phases concerned:

- **SSA during Implementation & Integration (including Training)**
    - Re-assess FHA and PSSA output (process and assumptions) using the knowledge of the system acquired during its Implementation & Integration;
    - Verification that system elements (People, Procedures, Equipment) as implemented meet their Safety Requirements;
    - Verification that the system as implemented can meet its Safety Objectives;
    - Verification that risk is acceptable.
- **SSA during Transfer into Operations,**
    - Safety assessment of the transfer into operations phase;
    - Verification that the system as transferred into operations meets its Safety Objectives, that system elements meet their Safety Requirements and that assumptions are correct;
    - Validation of the system as transferred into operations with respect to users' Safety expectations; (These users' Expectation with regards to safety are defined in the System Definition phase and collected during FHA.);
    - Validation that risk is acceptable.
- **SSA during Operations & Maintenance,**
    - Continuous data collection and monitoring of safety performances with respect to Safety Requirements, Safety Objectives, assumptions and risk acceptability;
    - Safety assessment of maintenance and/or planned interventions.
- **SSA during System Changes (People, Procedures, Equipment)**
    - Any change to the system and its elements (People, Procedures, Equipment) leads to the re-iteration of the overall Safety Assessment process, through: FHA, PSSA and SSA (thus no specific paragraph is dedicated to this item).
- **SSA during Decommissioning**
    - Assessment of the safety impact on ANS operations due to decommissioning (withdrawing) the system;
    - Safety assessment of the decommissioning phase.

If any of these tasks are not successfully achieved (so Safety Objectives and/or Safety Requirements are not met), then it leads to re-iterate FHA and /or PSSA in order to define new Safety Objectives and/or Safety requirements that can be met and finally achieve an acceptable risk.

This does not mean that during the re-iteration of the FHA and/or PSSA, less demanding Safety Objectives and/or Safety Requirements will be identified. It means that a new functional definition or new external mitigation means or a new architecture will have to be specified to set Safety Objectives and Safety Requirements that can be met while still achieving an overall acceptable risk.

All these tasks are further described in Guidance Material B of this Chapter 3. In addition, Guidance Material B also recommends activities, methods, techniques and means to actually conduct and achieve each of the tasks (as some techniques may apply to certain task(s)/phase(s) of the lifecycle but not to others).

3.1 SSA during Implementation & Integration

3.1.1 Re-assess FHA and PSSA output

This step of the process is recommended as:

- The domain maturity of the FHA and PSSA processes application is still to be increased;
- The major difficulty of a safety assessment lies in its completeness.

Using the deeper knowledge of the system and its operational environment acquired during its implementation and integration:

1. Re-assess the hazard analysis (hazard identification) output throughout the implementation and integration phase (check if there are some new or modified hazards);

2. Review the Safety Objectives allocation process by checking if quantitative frequencies and probabilities are still correct;

3. Check validity of assumptions on which Safety Objectives were funded along the FHA process.

   Then depending on results, Safety Objectives can be impacted. This can lead to redefine the system (and so redo a FHA of the new system).

4. Review the Safety Requirements apportionment process by checking the correctness of choices made during PSSA as well as the correctness of frequencies and probabilities.

5. Check validity of assumptions on which system element Safety Requirements were funded along the FHA and PSSA phases.

   Then depending on results, Safety Objectives and Safety Requirements can be impacted. This can lead to redesign the system (and so redo a PSSA of the new design or the change to the existing system) or even redefine the system (and so redo a FHA of the new system or the change to the existing system).

3.1.2 Verification that system elements (People, Procedures, Equipment) as implemented meet their Safety Requirements

A. <u>People and Procedure Elements:</u>

1. Collect Human and Procedures element Safety Requirements derived during FHA and PSSA phases;

2. Complete them with additional Safety Requirements derived during Implementation & Integration;

3. Input all of these Safety Requirements to the:

   - training definition, organisation and validation process (for example: training courses and manual, training simulator);
   - licensing;
   - staff selection & management;
   - ATM operational & maintenance procedures development and validation processes.

4. Ensure that needs, means and planning for Human and Procedures element Safety Requirements verification and, as far as feasible, safety validation:

   - are captured by activities such as Simulations and pre-operational Trials;

   - or are expressed in terms of specific analysis to be performed (for example: Operating procedure analysis, Maintenance procedure analysis);

   - collect conclusions of those activities and analyses with respect to at least HMI interface design improvement, procedures design and training;

   - add, if necessary, new safety related requirements to cope with safety problems highlighted by those activities and analyses.

B. <u>People Element:</u>

1. See People and Procedure Elements;

2. Verify that Safety Requirements for Human element are met (for example by the Training, Licensing processes and Staff selection & management, by ensuring that training courses, manuals and simulators address specific training issues according to the Safety Requirements).

C. <u>Procedure Element:</u>

1. See People and Procedure Elements;

2. Verify that each ATM Procedure satisfies its PAL (Procedure Assurance Level);

3. Verify that each Maintenance Procedure satisfies its Safety Requirements (for example as defined in the Maintenance Manual and Training Programme).

D. Equipment Element:

1. Verify satisfaction of Quantitative Safety Requirements[1] for Hardware element(s);

2. Verify that each Hardware satisfies its HWAL (HardWare Assurance Level);

3. Verify satisfaction of Safety Requirements for Software element(s). The level of satisfaction of Safety Requirements for a SW element is specified by its SWAL;

4. Verify that each Software satisfies its SWAL (SoftWare Assurance Level).

3.1.3 Verification that system as implemented can meet its Safety Objectives

1. Verify if **Quantitative Safety Objectives** can be satisfied;

2. Verify if **Qualitative Safety Objectives** can be satisfied.

Note: During implementation & integration phase of the lifecycle, at least it can be verified that Safety Objectives are not unsatisfied. At this phase of the lifecycle, it can be difficult to verify that Safety Objectives are satisfied as Safety Objectives are associated to an appropriate operational environment and as limited evidence/feedback can be made available/collected in that appropriate operational environment.

3.1.4 Verification that risk is acceptable

1. As demonstration that Safety Requirements, Safety Objectives and assumptions can not always be fully made during this phase, risk acceptability should be verified using system knowledge and data available at that stage of the lifecycle (sensitivity analysis to certain remaining SRs or SOs not yet fully satisfied can be made).

3.2 SSA during Transfer into Operation

3.2.1 Safety assessment of the transfer into operations phase.

1. Conduct specific safety assessment of the transfer into operation phase (site installation, shadow operation, switch to operations processes ….); verify that transfer phase' Safety Requirements for the installation of different equipment, or change of procedure are met and ensure that risks induced by transfer phase on on-going ANS operations are acceptable;

[1] **Quantitative** Safety Requirements might be deterministic or probabilistic.
- **Deterministic**: time to switch-over, maximum acceptable time of service interruption, maximum acceptable time for a maintenance intervention, etc;
- **Probabilistic**: safety (free from accidents), reliability (mission success or continuity of proper service), availability (readiness for use), integrity (correctness of data), maintainability (ability to be maintained).

Note that quantitative Safety Objectives result, through allocation process, into Safety Requirements addressing reliability, availability, integrity, maintainability, dependability,...

2. Define safety performance indicators and monitor performance of the transfer into operation phase (These indicators are two fold: indicators derived from the safety assessment of the transfer into operation phase itself as well as indicators that will still be valid during operation).

3.2.2 Verification[2] that system elements meet their Safety Requirements, that system as transferred into operations meets its Safety Objectives and that assumptions are correct

1. Collect evidence that Safety Requirements, Safety Objectives and all assumptions are met in the actual operational environment (at least the one of the transfer into operation phase that, sometimes, could slightly differ from the final one and that could differ from the one initially provided to the Safety Assessment process);

2. If new safety related problems are highlighted by verification, then identify and document constraints when interfacing other systems (related to system integrity or to robustness of those interfacing systems), propose operational or maintenance limitations, or ultimately Element or System changes which lead to reiterate FHA and/or PSSA.

3.2.3 Validation of the system as transferred into operations with respect to users' Safety expectations.

1. Collect evidence resulting from validation activities (system evaluation with respect to Safety, as performed by its end users – for ex: Operational trials, Transition analysis, Operational Readiness Review);

2. If new safety related problems are highlighted by validation: propose operational or maintenance limitations or ultimately system changes (people, procedures and equipment) which could lead to reiterate FHA and/or PSSA.

3.2.4 Validation that risk is acceptable.

1. Assess actual risk by updating the initial (predictive) safety assessment performed before operation, with data fed-back during the Transfer into operation phase, in order to ensure risk acceptability with respect to Safety Requirements, Safety Objectives and assumptions on the operational environment and its external mitigation means and any assumptions made during the safety assessment process.

3.3 SSA during Operation & Maintenance

3.3.1 Continuous data collection and monitoring of safety performances

1. Perform continuous safety monitoring to ensure that Safety Requirements are met, Safety Objectives are satisfied and assumptions (on the operational environment and its external mitigation means and any assumptions made during the safety assessment process) are correct while the system is in

[2] Verification activities started during the Implementation & Integration will go on as assurance that system and its elements meet the associated Safety Objectives and Requirements can't be fully obtained during Implementation & Integration. Some essential evidence can be provided only in a context close to the operational one available during the Transfer into operation phase (for some Safety Requirements, satisfaction can not be demonstrated in a simulated environment).

operation. Safety Monitoring also allows identifying any trends in the evolution of the safety performance or any common factors that might be at the origin of safety problems;

2. Perform continuous safety occurrence reporting and assessment consisting of: events detection and notification, factual information gathering and event reconstruction, event analysis, issue of recommendations, assessment of their effectiveness by monitoring over time the effect of their implementation, and reporting and exchange;

3. Assess risk by updating the initial (predictive) safety assessment performed before operation, with data fed-back by the Reporting and Assessment process, in order to continuously monitor risk acceptability;

4. Use "lessons learned", which represent an informal feedback of safety-related experience, complementary to the formalised Safety Occurrence Reporting & Assessment;

5. Conduct safety surveys.

3.3.2 Safety assessment of maintenance or planned interventions

Perform safety assessment of maintenance and/or planned intervention: prepare and conduct planned and/or maintenance interventions to ensure that risks induced by any maintenance and/or planned intervention are acceptable.

See Guidance Material C of this Chapter 3.

3.4 SSA during System Changes

Any major change to the system and its elements (People, Procedures, Equipment) leads to the re-iteration of the overall Safety Assessment process, through: FHA, PSSA and SSA (thus no specific guidance is dedicated to this item in the SSA).

3.5 SSA during Decommissioning

1. Assess safety impact on global ANS operations due to withdrawing the system from operations;

2. Perform safety assessment of the decommissioning process. That implies ensuring that risks induced on on-going ANS operations by the decommissioning operations (prepare and perform work to uninstall the system) are acceptable.

4 OUTPUT

- Updated list of assumptions;
- An updated list of identified hazards (new hazards may have been identified during the process and hazard scenarios may have been refined);
- The list of additional Safety Requirements defined during the Implementation & integration;
- The list of Safety Objectives and Safety requirements associated to the Transfer into Operation phase itself;
- The list of Safety Objectives and Safety requirements associated to the Decommissioning phase itself;
- Safety analyses results;
- Assurance & Evidence that assumptions are correct;
- Assurance & Evidence that Safety Requirements are met and Assurance Levels (HW, SW, ATM Procedure) are satisfied (including Safety Requirements specific to Transfer into Operation and Decommissioning);
- Assurance & Evidence that Safety Objectives are satisfied (including those specific to Transfer into Operation and Decommissioning);
- Assurance & Evidence that risk is acceptable (including those specific to Transfer into Operation and Decommissioning);
- The list of Safety Indicators to be monitored during transfer into operations, operation, maintenance and decommissioning;
- The list of remaining tolerable (but not acceptable) risks to be monitored and to be controlled during operations and the appropriate means to monitor and control them;
- The results and conclusions of the data collection (safety occurrence reporting and assessment, risk assessment based on occurrences reported, lessons learned, safety surveys) and safety monitoring activities, performed during system operation & maintenance;
- The results of the risk assessment and the appropriate justification demonstrating that safety impact of any major change to the system or its elements (People, Procedures, Equipment) is acceptable (concerns SSA if there is no impact, if any impact then re-iterate SAM);
- All the data of the safety assessment of:
  - The transfer into operation phase itself;
  - Maintenance and/or planned interventions;
  - Decommissioning phase itself.

This page is left blank intentionally.