# - Safety Assessment- SA -
## Part Two: Talking About AC 25.1309 (III/V)

Berquó, Jolan Eduardo – Eng. Eletrônico (ITA)·.
Certificador de Produto Aeroespacial (DCTA/IFI)
Representante Governamental da Garantia da Qualidade – RGQ (DCTA/IFI)
jberquo@dcabr.org.br

IYK 08 – MAR 24 2012

We will discuss in this MSC the procedure to perform a SA (Safety Assessment), taking as a basis the AC 25.1309-1A (REF. 1).

In its documentation FAA considers the ARP 4761, where applicable to the certification, suitable for the verification of compliance with the requirements of the paragraph 25.1309.

We remember that the AC is a suggestion, namely, an attempt to assist the applicant in developing his SA for the purposes of certification, but unfortunately it is not a document sufficiently clear to allow an applicant can develop his SA with no difficulties.

The SAE (Society of Automotive Engineers) issued the document ARP 4761 (Ref 2), which helps the companies to perform a SA in order to identify safety requirements for the aircraft design. Part of this documentation may be used by the applicant for certification purposes, while the other part remains just as company's document, i.e. it is not submitted to the authority.

As a tool for generating of requirements, the SA begins in the so called Conceptual Phase (or Design) of the aircraft lifecycle. In this phase we just know the functions that the aircraft must carry out. So, the SA focuses just on these functions.

Once identified these functions, the company identifies the applicable requirements or attributes (or characteristics) for these functions, from the point of view of performance and safety. It is exactly on the safety aspect that we are interested.

In this phase, an efficient way to identify the safety requirements for these functions is through the application of a Functional Hazard Analysis (FHA).

This analysis identifies the failure conditions that affect the functions of the aircraft and its severity (Minor, Major, Severe Major and Catastrophic), imposing the probability for each severity, in accordance with the guidance set out in AC 25.1309-1A. It is not a question of calculating the probability of the conditions, but to impose the range of probabilities to the failure condition in the severity assigned to it.

These requirements or desirable attributes for the functions of the aircraft are registered in a technical specification, which will guide the designers in the design of the systems that will, ultimately, perform the aircraft functions. It is the so called system functional allocation.

The SA proceeds with the allocation of requirements in the level of the equipment which will constitute the systems.

Let's then follow the step by step of an SA.

**Step 1**: Perform an FHA in aircraft level.

**Goal**: To identify the severity of failure conditions on the aircraft, crew and passengers, defining the respective range of probability.

After identifying the aircraft level functions, the analyst proceeds and assess function by function, in terms of total or partial loss of each, identifying the consequences on the aircraft, crew and other occupants, in all phases of flight, defining the respective severity (Minor, Major, Severe Major and Catastrophic), according the AC.

We have a total loss of a function, when there is no other mean to perform such a function.

The loss is said to be partial, when it is still possible to run the function, using a different mean. It is the case of a function that is performed by a primary mean and, in his absence, by a secondary mean. But when we talk of total loss, we are talking of loss of the two means. The total loss could lead to a high severity gradation (Severe Major or Catastrophic), but when there is only the primary mean loss, the severity is not more than Major.

The phase of flight can also influence the severity of a failure because, sometimes, a function is not important in one or another phase, but is essential in others. For example, the deceleration of the aircraft on the ground obviously does not act on the cruise.

Failure conditions identified with Minor severity are not object of further analyses; it is enough to register them and justify the judgement of the Minor severity. But the failures conditions with severity classified in Major, Severe Major and catastrophic have to continue in analysis on the systems level.

Once completed the evaluation in the aircraft level, it is advisable to register the results in tabular form. As suggested by the AC 23.1309-1E (REF. 3), a satisfactory table could have the following columns:

1. Function;
2. Failure Condition (description);
3. Phase;
4. Effect of the failure on the aircraft, crew and passengers;
5. Severity;
6. Reference to supporting material; and
7. Verification.

Let us look at the concepts represented by these columns.

**Function** - For being an action, the function is often described by a verbal expression with the verb in the infinitive, e.g.: "Decelerate the aircraft on the ground.

**Failure Condition** –The failure condition is characterized by the effect of the failure or defect on the function, which can lead to a partial or total loss of the function. This effect is usually expressed through a noun expression, as for example: "Loss of deceleration capacity".

**Phase –** Phase of flight (e.g. Cruise, Approximation).

**Effect on Aircraft, Crew and Passengers** – The possible adverse consequences of failure condition on the aircraft, crew and passengers, i.e. the severity.

**Severity** – Minor, Major, Severe Major or Catastrophic.

**Reference to Supporting Material** – It can be a suggestion to the designer to be inserted, for example, in a procedure or a crew training program.

**Verification** – this is a process to establish, by an analysis of second-level functions (systems), the requirements of probabilities to be allocated to these systems, which ultimately will generate the aircraft level functions. All failure conditions classified as Severe Major and Catastrophic must be taken to this level of analysis. The Fault Tree Analysis-FTA is a good tool for this analysis.

We will return in the next MSC, to give continuity to the subject.

See you.

References


(1) **FAA**: AC 25.1309-1A, System Design and Analysis, USA, 06/21/1988.

(2) **SAE**: ARP 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, USA, 12/01/1996.

(3) **FAA**: CFR 14 Part 25 § 1309, Equipment, Systems, and Installations, Amendment 25-123, USA, 11/08/2007.

(4) **FAA**: AC 23.1309-1E, System Safety Analysis and assessment for Part 23 Airplanes, USA, 11/17/2011.