Improve Your Knowledgement

- Safety Assessment -
Part1: Introduction

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

MSC 06– Dec, 05 2011

There is much talk of safety assessment, in military and civil aeronautics community, but who has already done such assessments or worked as an analyst of these evaluations knows that the theme is not so simple, when an applicant has to perform this type of evaluation and when a certification analyst has to analyze it. Often, these assessments have to be discussed with the applicant and, sometimes, the technical knowledge on the part of the certification analyst, must be well established.

The civil requirements and procedures for SA can be suitable also for the military area, but the military certification authority may or may not accept such requirements and procedures, once the relevant military regulation not necessarily follows the regulation for civil aviation.

In particular, we address here the requirements contained in 14 CFR Part 25 § 1309-1A, the popular FAR 25.1309: Equipment, Systems, and Installations.

Like any other document establishing requirements, the FAR 25.1309 just registers what must be, but not how to do to verify compliance with the requirements.

Because of that, FAA has issued the so-called Advisory Circulars (AC) as a guide with suggestions to verify the compliance with the requirements. They are documents that suggest a methodology for carrying out this verification of conformity, but they are not mandatory for use by applicants. These documents try also to avoid that applicants interpret differently the requirements.

The AC corresponding to the FAR 25.1309 is the AC 25.1309-1A, 6/21/1988, but as we have said, the AC is just a suggestion. Thus, the applicant may use another methodology, since that can demonstrate compliance with the requirements. Thus, he can also use suggestions from other AC, as for example the AC 23.1309-1E (System Safety Analysis and Assessment for Part 23 Airplanes), dedicated to SA pertinent requirements of FAR 23.1309 (Light Aircraft).

At this point, we think it is appropriate to establish the difference between two terms: Safety Analysis and Safety Assessment, since some people consider that are expressions with a perfect synonymy. We reproduce here the explanation presented in the AC 23.1309-1C:

"Analysis and Assessment". The terms "Analisys" and "Assessment" are used throughout. Each has a broad definition and the two terms are, to some extent, interchangeable. However, the term "Analysis" generally implies a more specific and more detailed evaluation, while the term "Assessment" may be a more general or broader evaluation but may include one or more types of analysis. In practice, the meaning comes from the specific application (for example, FTA, Markov analysis, PSSA, etc.)".

It seems clear that Safety Assessment is a set whose elements are Safety Analyses, and this set, like any other set, can be a unitary set, i.e. can consist of a single Safety Analysis.

FAR 25.1309 establishes five requirements: (a), (b), (c), (d), (e) and (f). But the AC deals only with the means to demonstrate compliance with the requirements (b), (c) and (d), exactly those requirements that require an SA for this demonstration.

The requirements (a), (b), (c), (d) do apply to the installation of all equipment and systems (pneumatic, hydraulic, electrical/electronics, mechanical and propulsion – engines and propellers), but they do not apply to the structural elements.

The requirement (e) applies specifically to the design and installation of electrical and electronic equipment and emphasizes that in demonstrating compliance of such items with the requirements (a) and (b), must be considered the critical environmental conditions that can occur during the flight. Are excluded the items covered by TSO containing environmental test procedures. One of these tests is the electromagnetic compatibility (EMC). But the AC 25.1309-1A does not deal with these kind of tests. One way to accomplish EMC tests is suggested in AC 23.1309-1E to verify compatibility with the requirement (a) of § 23.1309[1].

With regard to requirement (f), the applicant should refer to paragraph 25.1709. But we explain here the meaning of the acronym EWIS: Electrical Wiring Interconnection Systems.

The requirement (b) refers to the conditions of catastrophic failure and failure conditions that can reduce the capacity of the aircraft or the ability of the crew to cope with these effects.

The verification of compliance with the requirement (b) is addressed in requirement (d) requiring that such demonstration be done by analysis (SA) and, when necessary, by ground tests, flight tests or on simulators. But the AC 25.1309-1A makes it clear that it is not required tests to verify failure conditions that are postulated to be catastrophic. This verification shall be only by analysis (SA).

The sequence of SA suggested by AC 25.1309-1A is not so complicated. Everything begins with a Safety Analysis called Functional Hazard Analysis (FHA). It is a qualitative analysis to verify the effects of the failure of a system on the functions of other systems in the aircraft.

This identification places the failure conditions in one of the following possibilities:

- *Minor;*
- *Major;*
- *Severe Major or Hazardous; and*
- *Catastrophic.*

Such grading takes into account the capacity of the aircraft to fly and land safely, the crew's ability to cope with failure conditions and the comfort of the occupants. At one extreme we have the Minor severity that does not carry significant problems; in another, is the catastrophic severity that would prevent the continued safe flight and landing with possible loss of the aircraft or lives.

AC 25.1309-1A establishes that the Minor severity must be probable, i.e. it can occur. The Major severity must be improbable and its probability situated between 1 x 10^{-7} and 10^{-5}. The Severe Major severity or Hazardous severity must be extremely remote and its probability situated in the interval between 1 x 10^{-9} and 10^{-7}. On the other hand, the Catastrophic severity must be extremely improbable and its probability cannot overcoming 10^{-9}.

In the next part of this theme, we will discuss the sequence of the SA, presenting the analyses that are suggested by the AC 25.1309-1A, according to the severity of the failure identified in the FHA above mentioned.

See you.

References:

(1) FAA: 14 CFR Part 23 §: 1309, Equipment, Systems, and Installations, Amendment 23-49, USA, 03/11/1996.

(2) FAA: 14 CFR Part 25 §: 1309, Equipment, Systems, and Installations, Amendment 25-123, USA, 11/8/2007.

(3) FAA: AC 23.1309-1E, System Safety Analysis and Assessment for Part 23 11/17/23, USA 11/17/2011.

(4) FAA: AC 25.1309-1A, System Design and Analysis, USA, 6/21/1988.

[1] It is interesting to note that although the AC 23.1309-1E applies the requirements of FAR 23.1309, dedicated to light aircraft, this AC, in our opinion, is more complex than the AC 25.1309-1A, applied to the requirements of FAR 25.1309, for large aircraft.