- Safety Assessment- SA -
Part Two: Talking About AC 25.1309 (II/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 – JAN 18 2012

Continuing our discourse on AC 25.1309-1A, let's treat, in this opportunity, about the binomial: *the failure condition severity* and its *range of probability*.

First, it is necessary to keep in mind that there is no fatal accident-proof airplane. Zero probability of occurrence of a fatal accident is a mere chimera. You can use thousands of redundancies for one system and even so the probability of fatal accident will not be null. In addition, this practice can be prohibitive because of the probable high costs involved.

Therefore, it was necessary to establish an acceptable security level. This level, in civil aviation, came from an acceptable rate of accidents.

This rate was derived from the analysis of accident rate of occidental commercial aircraft for the period from 1970 to 1980. It was noted that, during that period, the catastrophic accident rate was slightly less than 1×10^{-6}, i.e. an accident every one million hours flown by any occidental commercial aircraft fleet.

In numbers: $\frac{N_C}{10^6} < 1 \times 10^{-6}$, where N_C is the total number of catastrophic accidents.

Considering the large amount of hours involved (10^6), the value above can be regarded as probability, obtained according to the empirical concept of probability, i.e:

$$P = \lim_{N \to \infty} \frac{n}{N}$$ (assuming 10^6 hours is a sufficiently large number)

where, n: number of failures observed; and
N: number of hours computed.

However, an analysis of the causes of these accidents showed that 10% were caused by failures of systems. In numbers:

$N_C = N_S + N_O$, ou seja: $\frac{N_C}{10^6} = \frac{N_S + N_O}{10^6} =$

$$= \frac{0{,}1(N_C) + 0{,}9(N_C)}{10^6},$$

where N_S is the number of accidents attributed to systems and No is the number of accidents attributed to other items.

Thus, the part allocated to systems was:

$$\frac{N_S}{10^6} = \frac{0{,}1\, N_C}{10^6} < 0{,}1\ (1 \times 10^{-6}) = 1 \times 10^{-7}.$$

This would be therefore the range of probability, in the empirical concept, of an accident occurs due to a catastrophic system failure condition, obtained from a sample in one million flight hours.

Starting from an arbitrary hypothesis, it was established that there are about 100 potential catastrophic failure conditions attributable to systems in large commercial aircraft. This way, we would have a subset **C** of events of the sample space $\mathbf{S_C}$ of catastrophic failure conditions consisting of 100 events, one for each condition of catastrophic failures attributable to systems. We could then represent such subset as follows:

$$\mathbf{C} = \{C_1, C_2, C_3, \ldots, C_{99}, C_{100}\},$$

where C_i is a generic catastrophic event.

Then we have $P(\mathbf{C}) = P(C_1) + P(C_2) + P(C_3) + \cdots + P(C_{99}) + P(C_{100}) < 1 \times 10^7$.

Admitting that **C** is a set with equally likely events[1], i.e. that each one of its 100 events has the same probability of occurrence, we have:

$P(C_1) = P(C_2) = P(C_3) = \cdots = P(C_{99}) = P(C_{100}) = P(C_i)$.

where C_i is any event in the space S_C

we have $P(C) = P(C_1) + P(C_2) + P(C_3) + \cdots + P(C_{99}) + P(C_{100}) = 100\ P(C_i)$.

Therefore, $100 \times P(C_i) < 1 \times 10^{-7} \Rightarrow P(C_i) < < \frac{1 \times 10^{-7}}{10^2}$ or **$P(C_i) < 1 \times 10^{-9}$**

Once established this maximum value for the open interval of probability for catastrophic failures, the limits for the other severities were also established. We have no information that these limits have been also based on historical data, as in the case of catastrophic failures. Thus, there is a doubt whether they were or not arbitrated.

Thus, the condition of catastrophic failure, that the item (b) (1) § 25.1309 requires that be **extremely unlikely**, is in the range $P(Ci) < 10^{-9}$, as established in the AC.

On the other hand, the Major failure condition, that the item (b) (2) § 25.1309 requires that must be **unlikely**, is in the open interval $10^{-9} < P(C_i) < 10^{-5}$, according the AC.

Finally, the Minor failure condition, for which the mentioned paragraph does not establish any requirement, was considered **probable** by the AC and inserted in the range $P(C_i) > 10^{-5}$.

It is important to note that the AC establishes two possibilities for the Major severity, one more serious than the other. Thus, one can speak of a severity **Normal Major**, or simply **Normal**, and a severity **Severe Major**. These two cases are inserted, without distinction, in the already mentioned range of probabilities $10^{-9} < P(C_i) < 10^{-5}$.

Just for information, noted that the AC 23.1309-1E, for small aircraft, and the AMC 25.1309, EASA, for large aircraft, divides the two possibilities of the severity Major in **Major** and **Hazardous**, characterizing them as follows:

- **Major**: Remote-10-$P(C_i)$ $9 < < 10^{-7}$.
- **Hazardous**: Extremely Remote $-10^{-7} < P(C_i) < 10^{-5}$.

We don't see any problem if the applicant wants to use this nomenclature.

It is interesting to present an example to see the logic of the numbers above. An aircraft can fly approximately 5×10^4 hours in its life. Then, a large fleet of 200 aircraft of the same type can accumulate a total of 10^7 hours. It is not expected, therefore, that a catastrophic failure occurs in that period.

But the Major failure condition ($10^{-9} < P(Ci)$ 10^{-5}) can happen once in a lifetime of an aircraft and several times in the life of the fleet.

Finally, the Minor failure condition can happen several times in the life of the aircraft.

Our next step is to present the procedure to perform an SA. With the objective to facilitate the task of the applicant, the AC presents a flow diagram (Figure 1 of the AC), looking for guiding the applicant in its assessment.

But such diagram will begin to be studied in detail in the next MSC of the SA series.

See you.

References

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

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

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

[1] Strictly, this is not true, but taking into account that for our analysis the interest is in the range assigned to each severity, we can consider a single and generic representative value of probability for each event of each range, which, in this case, is the range of catastrophic events.

(4) **EASA**: AMC 25.1309, System Design and Analysis. CS-125 - Book 2, Amendment 6, Cologne (Germany), 7/6/2009.

(5) **De Florio**, Filippo. Airworthiness – An Introduction to Aircraft Certification. 2nd. ed. USA: Elsevier Ltd, 2011.