- Avaliação de Segurança (*Safety Assessment- SA*) -
Segunda Parte: Discorrendo sobre a AC 25.1309-1A (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

MSC 08 – 18 JAN 2012

Dando continuidade ao nosso discurso sobre a AC 25.1309-1A, vamos tratar, nesta oportunidade, do binômio: *severidade da condição de falha* e *faixa de probabilidade permissível para a severidade.*

Primeiramente, é necessário ter em mente que não existe avião à prova de acidente fatal. Probabilidade zero de ocorrência desse tipo de acidente é mera quimera. Podem-se usar milhares de redundâncias para um sistema e, ainda assim, a probabilidade de acidente fatal não é nula, além de tal prática poder levar os custos de projeto às alturas.

Por isso, foi necessário estabelecer um aceitável nível de segurança (*Acceptable Safety level*). Esse nível, na aviação civil, decorreu do que se intitulou de taxa aceitável de acidentes (*Acceptable Accident Rate*).

Essa taxa derivou da análise da taxa de acidentes de toda a frota de aviões comerciais ocidentais, no período de 1970 a 1980. Observou-se que, nesse período, a taxa de acidentes catastróficos foi pouco menor que 1×10^{-6}.

Em números: $\frac{N_C}{10^6} < 1 \times 10^{-6}$, onde N_C é o número total de acidentes catastróficos.

Considerando a grande quantidade de horas envolvidas (10^6), o valor acima pode ser considerado como probabilidade, obtida segundo o conceito empírico de probabilidade, ou seja:

$P = \lim_{N\to\infty} \frac{n}{N}$ (supondo que 10^6 horas seja um número suficientemente grande)

onde, n: número de falhas observadas; e
N: número de horas computadas.

No entanto, a análise das causas desses acidentes evidenciou que apenas 10% foram causados por falhas de sistemas. Em números:

$$\frac{N_C}{10^6} = \frac{N_S + N_O}{10^6} = \frac{0{,}1N_C + 0{,}9N_C}{10^6},$$

onde N_S é o número de acidentes atribuídos a sistemas, e N_O é o número de acidentes atribuídos a outros itens.

Desse modo, a parte atribuída a sistemas foi:

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

Partindo de uma hipótese arbitrária, estabeleceu-se que uma aeronave poderia apresentar cerca de 100 potenciais condições de falhas catastróficas atribuíveis a sistemas, em grandes aeronaves comerciais. Desse modo, ter-se-ia um subconjunto de eventos do espaço amostral das condições de falhas catastróficas constituído por 100 eventos, um para cada condição de falha catastrófica atribuível a sistemas. Poder-se-ia então representar tal subconjunto por

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

onde C_i é um evento catastrófico genérico atribuível a sistemas.

Teríamos então $P(C) = P(C_1) + P(C_2) + P(C_3) + \cdots + P(C_{99}) + P(C_{100}) < 1 \times 10^{-7}$.

Admitindo-se que **C** seja um conjunto equiprovável[1], ou seja, que cada um de seus 100 eventos tenha a mesma probabilidade de ocorrência, teríamos:

[1] Rigorosamente, isso não é verdade, mas tendo em conta que para nossa análise o interesse está na faixa atribuída a cada severidade, podemos considerar um único e genérico valor representativo de probabilidade para cada evento de cada faixa, que, neste caso, é a faixa dos eventos catastróficos.

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

Resulta então que $P(C) = P(C_1) + P(C_2) + P(C_3) + \cdots + P(C_{99}) + P(C_{100}) = 100\ P(C_i)$.

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

ou $\boxed{P(C_i) < 1 \times 10^{-9}}$

Esta é a faixa registrada na AC, para as condições de falha Catastrófica**.**

Uma vez estabelecido esse valor máximo do intervalo aberto de probabilidade, para as condições de falhas catastróficas, foram estabelecidos também os outros limites máximos de intervalos para as demais severidades. Não temos informações de que esses limites tenham se baseado em dados históricos, como no caso das falhas catastróficas, ou se foram arbitrados.

Com base nos resultados numéricos acima, a AC estabelece então, para a condição de falha Catastrófica**,** a faixa de probabilidade $P<10^{-9}$. Em consequência, essa é a faixa de valores que o item (b)(1) do § 25.1309 diz que tem de ser **extremamente improvável.**

Já a condição de falha Maior, que o item (b)(2) do § 25.1309 estabelece que tem de ser **improvável**, a AC a situa no intervalo aberto de probabilidade $10^{-9}<P<10^{-5}$.

Finalmente, para a condição de falha Menor, a AC a situa na faixa $P>10^{-5}$, estabelecendo para os valores aí contidos o nível **provável**. Esta condição de falha não é enquadrada no § 25.1309 porque é aceitável que ocorra.

É importante observar que a AC estabelece também duas possibilidades para o enquadramento na severidade Maior, uma mais grave que a outra. Fala de uma severidade, digamos, **Maior Normal,** ou simplesmente **Normal,** e de uma severidade **Maior Severa**. Esses dois casos estão enquadrados, sem distinção na AC, na já mencionada faixa de probabilidades $10^{-9} <P< 10^{-5}$.

Com relação a esse detalhe da severidade Maior**,** registra-se que a AC 23.1309-1E, para pequenos aviões, e a AMC 25.1309, da EASA, para grandes aeronaves, denominam as duas condições de severidade Maior da AC 25.1309-1A de **Maior** e **Perigosa** (**Hazardous**), caracterizando-as da seguinte maneira:

- **Maior**: Remota - $10^{-9} <P< 10^{-7}$.
- **Perigosa (Hazardous)**: Extremamente Remota - $10^{-7} <P< 10^{-5}$.

Não vemos nenhum problema se o requerente quiser usar essa nomenclatura.

É interessante apresentar um exemplo para que se tenha uma ideia da lógica dos números acima. Uma aeronave pode voar cerca de 5×10^4 horas, em sua vida útil. Então, uma grande frota de 200 aeronaves do mesmo tipo pode acumular um total de 10^7 horas. Não se espera, portanto, que ocorra uma falha catastrófica ($P<10^{-9}$), nesse período.

Já a condição de falha Maior ($10^{-9}<P<10^{-5}$), pode acontecer uma vez na vida de uma aeronave e várias vezes na vida da frota.

Finalmente, a condição de falha Menor ($P>10^{-5}$) pode acontecer várias vezes na vida da aeronave.

Nosso próximo passo, agora, é dar uma ideia do procedimento para realizar uma SA. Com o objetivo de facilitar a tarefa do requerente, a AC apresenta um diagrama de fluxo (figura 1 da AC), procurando orientar o requerente em sua avaliação de segurança.

Mas esse diagrama será tratado, passo a passo, nos próximos MSC da série SA.

Até lá.

Referências:

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

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

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

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

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