Segurança de Sistemas: Qual é a abrangência da atividade de *Safety Assessment*?

***Berquó**, Jolan Eduardo –Eng. Eletrônico (ITA)·.*
Certificador de produto Aeroespacial (DCTA/IFI)
Representante Governamental da Garantia da Qualidade – RGQ (DCTA/IFI)
Pós-graduado em Engenharia de Confiabilidade e em Engenharia de Segurança de Sistemas (ITA)
Especialização em Engenharia e Análise de Sistemas (Itália).
jberquo@dcabr.org.br/jberquo@uol.com.br

MSC 48 – 25 JUL 2014

Quando se estabelece que uma condição de falha catastrófica de um sistema de uma aeronave deve ter uma probabilidade (P) de ocorrência menor que 10^{-9} (uma falha em cada bilhão de horas de voo), num voo de uma hora, o que de fato isso quer dizer? Significaria que esse é o intervalo da probabilidade permitido para a ocorrência de um acidente catastrófico? Vamos conversar sobre isso neste MSC.

Colocamos aqui o tema acima, exatamente porque um companheiro, conversando conosco, não conseguia entender porque os projetos das aeronaves não cumpriam esse requisito, muito embora a Autoridade de Aeronavegabilidade certificasse esses projetos, mas depois, na vida operacional, não era exatamente o que acontecia.

De fato, na realidade, essa probabilidade é maior.

Expliquemos.

O requisito de $P<10^{-9}$ refere-se somente a catástrofes decorrentes de condições de falhas dos sistemas da aeronave. No entanto, as catástrofes não são devidas apenas a falhas dos sistemas. Aliás, a parcela devida a sistemas é pequena.

Em verdade, só cerca de dez por cento (1/10) dos acidentes catastróficos são atribuídos a condições de falhas de sistemas.

Para mostrar isso, vamos recordar aqui algo que já tratamos no MSC 08.

Dissemos ali que a análise da taxa de acidentes catastróficos de toda a frota de aviões comerciais ocidentais, no período de 1970 a 1980, mostrou que, nesse período, a taxa global de acidentes catastróficos foi pouco menor que 1×10^{-6} (um em um milhão de horas).

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:

$$P = \lim_{N\to\infty} \frac{n}{N}$$

(admitindo-se que 10^6 horas seja um número suficientemente grande)

onde, n é o número de falhas observadas; N, o número de horas computadas.

No entanto, a análise das causas desses acidentes, como já dissemos, 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, mas conservativa, 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:

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

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

Muito bem, mas se só dez por cento dos acidentes catastróficos foram devidos a falhas de sistemas, quais são as outras causas? Diz a Estatística que o ser humano é a maior parcela dessas causas. Sabe-se que só a tripulação, em decorrência de seus erros, deve estar contribuindo com um percentual entre 75% e 80%.

Desse modo, quando alguém vai viajar e reza para não ocorrer um acidente, deveria fazê-lo focado na tripulação, rogando para que ela esteja bem treinada, que tenha tido uma boa noite de sono e entre no avião com a única preocupação de desempenhar bem seu papel.

Mas e os outros 20% ou 25% dos acidentes catastróficos, a quem ou a que atribuir?

Indo para as outras causas, citamos, de pronto, a manutenção como uma fonte significativa para os acidentes. As agressões ambientais, como, por exemplo, a interferência eletromagnética (EMI), fatores meteorológicos. Não se pode desprezar o controle de voo, em terra, com instruções erradas. Também panes em auxílios rádio à navegação, quando em rota, podem levar a aeronave a perder-se. Poderíamos até acrescentar, em menor dose, os atos terroristas.

Mas o objetivo aqui é deixar claro que a aeronave não se precipita apenas em decorrência de falhas de sistemas. A principal causa ainda está no ser humano.

E os Veículos Aéreos Não Tripulados (VANT)? — Bem, nesse caso, poderiam dizer alguns, o acidente é devido somente a falhas de sistemas. Será? E o ser humano que está na estação terrestre, dirigindo o VANT?

O fato é que o processo de *Safety Assessment*[2], previsto nas AC 1309 (Partes 23, 25, 27 e 29) e na SAE ARP 4761, que orienta os requerentes em suas análises, pelo menos por ora, cuida apenas de uma pequena parcela que pode causar acidentes catastróficos: os sistemas.

Alguns estudiosos, com os quais temos trocado ideias, estão continuadamente pensando numa expansão dessa abrangência, mas é assunto ainda incipiente.

Obrigado e até a próxima.

Referências

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

[1] Rigorosamente, isso não é verdade, mas tendo em conta que para nossa análise o interesse está na faixa atribuída a cada severidade, e não no valor exato, 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.

[2] Numa tradução livre: "Avaliação de Segurança".

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

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

(4) **De Florio**, Filippo, Airworthiness: An Introduction to Aircraft Certification. Elsevier. 2a.Ed., EUA, 2011.