

O processo de Safety Assessment é aplicável a Sistemas/Itens Mecânicos?

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@gmail.com

MSC 67 A– 29Nov2018

Há quem diga que sim e há quem diga que não. Embora já tenhamos tratado do assunto no PDC-01, há ainda quem tenha dúvidas em relação à pergunta em epígrafe. Vamos então, neste MSC, tentar por fim a essas dúvidas. A base que usaremos será a CFR 14 Parte 23 §1309 e sua correspondente AC 23.1309-1E, considerando as aeronaves da Classe IV (Commuter). Essas aeronaves, em termos de Safety Assessment, cumprem os mesmos requisitos qualitativos e quantitativos das aeronaves regidas pela Seção 25.1309, no que tange às faixas toleráveis de probabilidade de ocorrência de falhas de severidades “catastrophic, Hazardous, Major e Minor”. Por outro lado, a AC 23.1309-1E, por ser bem mais recente que a AC 25.1309-1A, incorpora conceitos mais atualizados pertinentes a Safety Assessment.

Lembramos que a AC 23.1309-1E é o documento de orientação da FAA para demonstrar a conformidade com os requisitos da Seção 23.1309. Deste modo, ela será nosso guia. Para realizar essa tarefa, a AC define métodos qualitativos e quantitativos. Isso é básico para nossa análise.

Atentemos, a partir deste momento, que as aeronaves que estamos considerando apresentam, em geral, uma estrutura com os seguintes segmentos: Ambiental, Aviônico, Elétrico, Interiores, Mecânico, Propulsão, Auxiliar e Fuselagem¹.

Neste MSC, estamos interessados no Segmento Mecânico, que compreende os seguintes sistemas: **Controles de Voo (Flight Controls)**,

Potência Hidráulica e Trens de Pouso. Nossa discussão, é claro, se prende a esses itens².

Poderíamos então liquidar o assunto, considerando o seguinte trecho constante do item 5 (*Applicability*) da AC 23.1309-1E:

“...As estruturas de vôo, como asa, empenagem, superfícies de controle e seus sistemas simples; a fuselagem, o berço do motor e o trens de pouso (incluindo suas fixações primárias) estão excluídos (da Seção 23.1309)”.

Ora, as superfícies de controle e o trem de pouso são itens do segmento mecânico da aeronave, complementados pela potência hidráulica necessária para movimentar esses itens.

Isso já seria suficiente para parar por aqui; contudo, vamos continuar analisando o item 5 da AC, para verificar se há alguma aplicabilidade para itens mecânicos, quanto ao safety assessment, ainda que seja parcial. Este passa, agora, a ser o nosso problema.

Vamos então para o seguinte texto, logo no início do item 5 da AC:

“Além dos requisitos específicos de projeto da parte 23, os requisitos do § 23.1309, exceto conforme identificado abaixo, se aplicam a todos os sistemas instalados na aeronave”.

¹ V. Ref. 1.

² V. Ref. 1.

Comentários – Tendo em conta o parágrafo anterior, relativo ao segmento mecânico da aeronave, essa afirmação poderia nos parecer contraditória. A sutileza, acreditamos, talvez esteja na aplicabilidade pelo menos parcial aos itens mecânicos. Vasculemos.

Continuando, no que interessa, o texto registra:

“A nova tecnologia avançada em projetos de sistemas elétricos, eletrônicos e mecânicos, que incluem componentes eletrônicos complexos com software, hardware complexo, HIRF (Campos Irrradiados de alta intensidade) e/ou lightning (raios) requer uma análise do § 23.1309”. Uma SSA³ (System Safety Analysis) é necessária para determinar o nível de aderência aos processos contidos em documentos normativos e de orientação, como RTCA/DO-178B⁴, RTCA/DO-254, AC 20-136A e AC 20-158 ou equivalente”.

Comentários – Quando se fala de sistemas complexos (vide definição na AC), fala-se de sistemas que contêm os chamados equipamentos ou itens eletrônicos complexos (grande parte dos modernos equipamentos eletrônicos de hoje), mesmo tendo partes mecânicas, como no sistema *fly-by-wire* de aeronaves de certo porte. Nesses casos, a SSA não aplica métodos quantitativos. Para os equipamentos eletrônicos complexos, o fabricante se vê compelido a desenvolver seu projeto com base nas DO-178C, para software, e DO-254, para o hardware complexo. Nesses casos, o processo de SSA é qualitativo e consistiria numa auditoria de projeto, por parte da Autoridade de Certificação, junto ao fabricante, para verificar se o projeto desses equipamentos complexos está sendo desenvolvido de acordo com o previsto nas DO's e AC's mencionadas.

Continuando.

“A Seção 23.1309 deve ser usada para determinar a condição de falha, probabilidade de falha, Nível de Garantia de

Desenvolvimento de Software (DAL) e DALs de hardwares complexos mostrados na Figura 2”.

Comentários – A determinação da condição de falha (efeito da falha na tríade: passageiros, tripulação e aeronave) aplica-se a qualquer sistema (mecânicos, elétricos e eletrônicos), mas a determinação da probabilidade da condição de falha depende da taxa de falha λ fornecida pelo fabricante, que para itens elétricos e eletrônicos é considerada constante⁵ em toda a fase operacional. Contudo, isso não se aplica a partes mecânicas porque a taxa de falha dessas partes é função do tempo ($\lambda = \lambda(t)$), isto é, não se saberia, num momento qualquer da fase operacional, o valor dessa taxa.

Para equipamentos elétricos e eletrônicos, pode-se escrever $F = 1 - \text{Exp}(-\lambda t)$, onde F é a probabilidade do equipamento falhar num tempo t e λ é a taxa de falha constante.

Para afiançar essas considerações, a AC, em seu Apêndice 3, dedicado ao cálculo da probabilidade média por hora de voo (*Average Probability per Flight Hour*) incentiva o Requerente ou Aplicante (*Applicant*) a aplicar a função F com taxa de falha λ constante, caso dos elétricos e eletrônicos, ao longo da fase operacional. Seria então o caso da função $F = 1 - \text{Exp}(-\lambda t)$ ⁶, ou $F = \lambda t$, se λt for muito menor (10 ou mais vezes) que 0,1, como aliás ocorre, na imensa maioria dos itens elétricos e eletrônicos. Acrescenta ainda a AC que se a taxa de falha de alguma parte do sistema não for constante (caso dos itens mecânicos), pode-se aplicar-lhe, por exemplo, a função de distribuição cumulativa de probabilidades de Weibull.

Prossegue...

“Para sistemas eletromecânicos, mecânicos ou analógicos simples e convencionais, ou ambos, com processos de projeto e certificação bem estabelecidos (onde a instalação não seja complexa), a análise de segurança (*safety assessment*) pode ser satisfeita por uma avaliação qualitativa,

³ Parte do Processo de *Safety Assessment*.

⁴ Que foi substituída pela DO-178C.

⁵ Ou mui aproximadamente constante.

⁶ F é a Falibilidade ou Inconfiabilidade, ou seja, a probabilidade de um item falhar num determinado intervalo de tempo.

como o conceito de falha única e a experiência de projetos comprovados por serviços e julgamento de engenharia. Neste caso, uma FHA, uma avaliação de projeto e uma avaliação de instalação abordada nesta AC podem satisfazer o § 23.1309, conforme mostrado na Figura 3”.

Comentários – Claramente, admite-se uma análise qualitativa, inclusive para partes mecânicas.

Para finalizar nossos comentários. Devemos acrescentar que quando um fabricante de itens mecânicos passa uma taxa de falha à Autoridade, esse valor é o valor a ser considerado considerado no início da operação do item na aeronave, esperando-se que esse valor esteja ainda em fase decrescente (a curva da taxa de falha de itens mecânicos decresce até que passa por um valor mínimo e depois começa a crescer de maneira acentuada).

Isso é um dos motivos das partes mecânicas essenciais para o voo e pouso seguros serem objeto de manutenção preventiva, incluindo, onde necessário e possível, a manutenção preditiva (verificação da integridade do item de prosseguir em operação; caso positivo, volta-se a examinar o mesmo numa data futura, criteriosamente estabelecida). Os equipamentos elétricos e eletrônicos, por sua vez, não têm manutenção preventiva. Eles são *on condition*, isto é, só são submetidos à manutenção quando falham, e neste caso trata-se de manutenção corretiva.

Desse modo, concluímos que os sistemas ou equipamentos mecânicos são parcialmente passíveis de serem submetidos ao processo de *safety assessment*, mas só até a determinação da severidade da condição de falha dos mesmos (fase inicial do processo), não se lhes aplicando, pelas razões apresentadas, a determinação da probabilidade de ocorrência de suas condições de falha, ao longo de toda a fase operacional. Rigorosamente, só os elétricos e eletrônicos podem ter essa avaliação.

Vamos ficando por aqui. Até uma nova oportunidade.

Referências

(1) Jackson, Scott, *Systems Engineering for Commercial Aircraft – A Domain Specific Adaption*, 2nd Ed., 2016, University of

Southern California and Burhan Systems Consulting, EUA.

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

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