Melhore Seus Conhecimentos

- Avaliação de Segurança (*Safety Assessment*) -
Primeira Parte: Introdução

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 – 20 DEZ 2011

Fala-se muito em avaliação de segurança (do Ing.: *Safety Assessment*), na comunidade aeronáutica civil e militar, mas quem já realizou avaliações dessa natureza ou trabalhou como analista dessas avaliações, em um organismo de certificação civil ou militar, sabe que o tema não é tão simples, quando se parte para a prática, ou seja, quando um requerente tem de realizar esse tipo de avaliação e o analista certificador tem que analisá-las. Não raro, essas avaliações têm de ser discutidas com o requerente e, às vezes, o conhecimento técnico, por parte do analista certificador, precisa estar bem consolidado.

A avaliação de segurança é mais conhecida por requerentes e organismos certificadores pelo termo inglês *Safety Assessment (SA)*. Da mesma forma, assim será tratada neste trabalho.

As normas e procedimentos civis para SA são apropriadas também para o meio militar, mas a autoridade de certificação militar pode ou não aceitar essas normas e procedimentos civis, uma vez que a regulamentação militar pertinente não se submete obrigatoriamente à regulamentação da aeronáutica civil.

Vamos tratar aqui, em especial, dos requisitos contidos em CFR 14 Part 25 § 1309-1A, o popular FAR 25.1309: *Equipment, Systems, and Installations.*

Como qualquer outro documento que estabelece requisitos, só se registra ali o que tem de ser, mas não como fazer para verificar a conformidade com esses requisitos.

Por isso, a FAA criou as chamadas *Advisory Circulars* (AC), procurando orientar com sugestões a maneira de verificar essa conformidade. São documentos que sugerem uma metodologia para realizar essa verificação de conformidade, mas não são de utilização obrigatória pelos requerentes. Procuram também evitar que os requerentes interpretem diferentemente os requisitos.

A AC correspondente ao FAR 25.1309 é a AC 25.1309-1A, de 21/6/1988, mas como foi dito, a AC é apenas uma sugestão. Desse modo, o requerente pode usar outra metodologia, desde que consiga demonstrar a conformidade com os requisitos. Assim, ele pode usar também sugestões de outras AC, como por exemplo a AC 23.1309-1E (*System Safety Analysis and Assessment for Part 23 Airplanes*), dedicada a SA pertinente aos requisitos do FAR 23.1309 (Aviões Leves) e até mesmo versões anteriores de uma mesma AC.

Neste ponto, julgamos conveniente estabelecer a diferença entre dois termos: *Safety Analysis* e *Safety Assessment*, uma vez que alguns consideram que são expressões com sinonímia perfeita. Para isso, vamos transcrever, a seguir, em tradução livre, a explicação contida na AC 23.1309-1D:

Análise e Avaliação (Analysis and Assessment) – *Os termos "analysis" e "assessment" são usados, ao longo da AC. Cada um tem uma conotação ampla e os dois termos são, até certo ponto, intercambiáveis. No entanto, o termo "analisys" geralmente implica em uma abordagem mais específica e detalhada, enquanto o termo "assessment" pode ser tratado como uma avaliação mais geral ou ampla, podendo incluir um ou mais tipos de análises[1]. Na prática, o significado vem da aplicação específica (por exemplo, Análise por Árvore de Panes ("Fault Tree Analysis – FTA"), Análise de Markov, AMPS, etc.).*

[1] Vide item 14 da AC, que em seu parágrafo (a) informa que o requerente é responsável pela escolha dos vários métodos (tipos de análises) para a SSA. Vide também o item 16, que descreve os vários tipos de análises utilizados na SSA.

Parece-nos claro, a partir desse conceito, que *Safety Assessment* é um conjunto cujos elementos são *Safety Analyses*, podendo esse conjunto, como qualquer outro conjunto, ser unitário, isto é, ser constituído de uma só *Safety Analysis*.

O FAR 25.1309 estabelece cinco requisitos: (a), (b), (c), (d), (e) e (f). Mas a AC trata apenas dos meios para demonstrar a conformidade com os requisitos (b), (c) e (d), exatamente aqueles requisitos que, de alguma forma, requerem uma SA.

Os requisitos (a), (b), (c), (d) são aplicáveis à instalação de todos os equipamentos e sistemas (pneumáticos, hidráulicos, elétrico/eletrônicos, mecânicos e de propulsão – motores e hélices), mas não se aplicam a elementos estruturais.

O requisito (e) é aplicável especificamente ao projeto e instalação de equipamentos elétricos e eletrônicos e enfatiza que na demonstração de conformidade desses itens com os requisitos (a) e (b) devem ser consideradas as condições ambientais críticas que podem ocorrer durante o voo. Estão excluídos os itens TSO que tenham passado por ensaios ambientais compatíveis com as condições ambientais críticas. Um desses ensaios é o de compatibilidade eletromagnética. Mas a AC 25.1309-1A não trata desses ensaios. Uma maneira de realizar o ensaio de EMC é sugerida na AC 23.1309-1E para verificar a compatibilidade com o requisito (a) do § 23.1309[2].

Com relação ao requisito (f), o requerente deverá reportar-se ao parágrafo 25.1709. Mas deixamos aqui o significado da sigla EWIS: *Electrical Wiring Interconnection Systems.* Numa tradução livre: Sistemas de Interconexão de Fiação Elétrica.

O requisito (b) trata das condições de falha catastrófica e das condições de falha que, de alguma forma, reduzem a capacidade da aeronave ou da tripulação de lidar com esses efeitos.

A verificação da conformidade com o requisito (b) é tratada no requisito (d), que exige que tal demonstração de conformidade seja feita por análise (SA) e, quando necessário, por ensaios no solo, em voo ou em simuladores. Mas a AC 25.1309-1A deixa bem claro que não se requer ensaios para verificar condições de falha catastróficas. Essa verificação deve ser só por análise (SA).

A sequência da SA, na AC 25.1309-1A, não é tão complicada. Tudo começa com uma *Safety Analysis* denominada *Functional Hazard Assessment* (Análise de Perigo Funcional), mais conhecida pela sigla FHA. Trata-se de uma análise qualitativa para verificar os efeitos da falha de um sistema nas funções de outros sistemas da aeronave.

Essa identificação enquadra as condições de falha em uma das seguintes possibilidades:

- Menor (*Minor*);
- Maior (*Major*);
- Maior severa (*Severe Major*) ou Perigosa (Hazardous); e
- Catastrófica (*Catastrophic*).

Tal gradação leva em consideração a capacidade da aeronave de voar e pousar com segurança, a capacidade da tripulação em lidar com as condições de falha e o conforto dos ocupantes. Num extremo está a severidade Menor, que não traria problemas preocupantes; noutro, está a catastrófica, que não permitiria a continuidade do voo e o pouso seguros, podendo resultar em perda da aeronave e de vidas.

A AC 25.1309-1A admite que a severidade Menor seja provável, ou seja, que possa ocorrer. A condição Maior deve ser improvável, enquadrando-se sua probabilidade entre 1×10^{-7} e 10^{-5}. A Maior Severa ou Perigosa (*Hazardous*) deve ser extremamente remota e sua probabilidade deve situar-se entre 1×10^{-9} e 10^{-7}. Já a catastrófica deve ser extremamente improvável, com probabilidade não superando 10^{-9}.

Na próxima parte deste tema, trataremos da continuidade da SA, apresentando as análises que são sugeridas pela AC 25.1309-1A, de acordo com a severidade da falha apurada na aplicação da FHA mencionada acima.

Até lá.

[2] Embora a AC 23.1309-1E se aplique aos requisitos do FAR 23.1309, dedicados a aeronaves leves, essa AC, em nossa opinião, é mais complexa que a AC 25.1309-1A, aplicada aos requisitos do FAR 25.1309, relativos a grandes aeronaves.

Referências:

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

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

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

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