- Avaliação de Segurança (*Safety Assessment- SA*) -

Segunda Parte: Discorrendo sobre a AC 25.1309-1A (V/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 11 – 11 JUL 2012

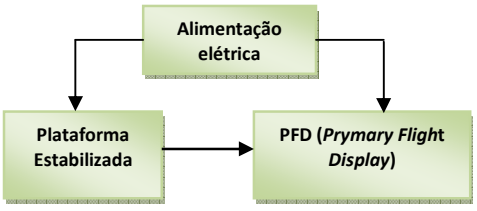
Retornamos aqui, neste trabalho da série "Avaliação de Segurança", apenas para dar um fecho a nossa proposta.

No MSC anterior, chegamos até a PSSA (*Preliminary System Safety Analysis*). Mas encaminhamos, propositadamente, a análise para sistemas simples, dado que o espaço estabelecido para esta seção é destinado a "flashes". Por assim ser, procura-se, neste espaço, dar apenas uma ideia ao leitor, ou seja, familiarizá-lo com o assunto tratado, tentando incentivá-lo a se aprofundar na matéria, por meio de consulta às referências assinaladas, nas quais encontrará também outras referências. É um estudo continuado.

Ortodoxamente, deveríamos passar de uma PSSA para uma SSA e ainda realizar outras análises, mas, conforme as circunstâncias apresentadas, vamos encerrar o assunto, considerando a arquitetura proposta para os sistemas primário e secundário de atitude.

Vamos levar em conta apenas o sistema primário de indicação de atitude. O Secundário tem análise semelhante, mas com números diferentes.

A estrutura apresentada no MSC 10 é a da figura a seguir.



A alimentação elétrica é geral, isto é, ela é dedicada a todos os sistemas da aeronave que necessitam de tal alimentação, sendo suas condições de falha um modo comum de falha, ou seja, entra em todos os sistemas que requeiram alimentação elétrica.

Desse modo, ficamos então apenas com o sistema dedicado à função em análise.

Assim, a configuração que nos interessa é a apresentada na figura a seguir.

Precisamos considerar que estamos usando a função de distribuição exponencial negativa. Já dissemos que quando adotamos tal função, para nosso sistema, significa que o mesmo se comporta sempre como novo (*v. MSC 05*), isto é, todas as vezes que for ligado, tudo se passa como se fosse ligado pela primeira vez (pelo menos enquanto a taxa de falha for aproximadamente constante). É a chamada Propriedade do Esquecimento ou da Perda de Memória. No presente caso, isso é muito próximo da realidade, considerando que o sistema que estamos analisando é preponderantemente eletrônico.

Sendo assim, enquanto o sistema estiver no patamar da taxa de falha constante, sempre teremos a seguinte probabilidade de falha para o voo médio de 6 horas: $6.\lambda$, para $\lambda t<0,1$. Para a plataforma estabilizada, teríamos $6.\lambda<3.10^{-6}$. Segue que

$$\lambda < \frac{3.10^{-6}}{6} = 3,3.10^{-7}.$$

O raciocínio seria semelhante para o PFD. O analista, no entanto, está livre para manusear essas taxas de falha, de acordo com as conveniências do projeto, sempre tendo em mente os valores de probabilidades estabelecidos como requisitos no nascedouro da SA, ou seja, na FHA nível aeronave.

Para finalizar, gostaríamos de tratar um pouco das chamadas condições de falha Maior.

Como vimos, a condição de falha Maior deve ser improvável. Isso significa que a taxa de ocorrência de falha deve estar no intervalo entre 1.10^{-7} e 1.10^{-5}.

Como já dissemos, em geral os equipamentos que constituem o sistema em análise têm uma taxa de falha definida, ficando fácil então verificar se a arquitetura do sistema de que fazem parte atende aos requisitos de segurança. Por uma questão de mais segurança, pode-se solicitar do fabricante relatórios de testes e/ou de análises que levaram à taxa apresentada. Em termos de análise, pode-se solicitar a FMEA (*Failure Mode, and Effects Analysis)* feita para o equipamento.

A similaridade com instalações em outras aeronaves certificadas também é uma demonstração considerada satisfatória pela Autoridade.

Encerramos aqui essa série de "flashes", sugerindo fortemente o leitor a consultar as referências listadas.

Nosso muito obrigado pela paciência de nos ler. Voltaremos com novos assuntos de interesse dos que participam do *mundo da aeronavegabilidade.*

Até breve

Referências

(1) ***O'CONNOR, P.D.T****. Practical Reliability Engineering. John Wiley & Sons, Inc., New York, 1991.*

(2) ***SAE****: ARP 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, EUA, 01/12/1996.*

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

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

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