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

Segunda Parte: Discorrendo sobre a AC 25.1309-1A (IV/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 10 – 24 MAR 2012

Voltamos aqui, apresentando a maneira de alocar requisitos de segurança para as funções nível sistema, que isoladas ou associadas a outras conduzem às funções nível aeronave.

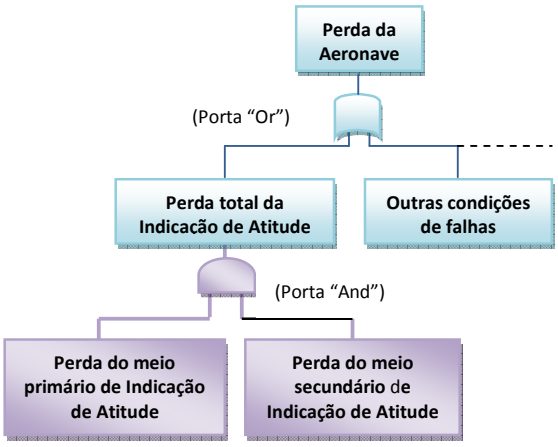
Dissemos que a FTA é uma boa ferramenta para realizar essa alocação. Entretanto, é necessário deixar claro que existem outras ferramentas (Ref. 2) que podem ser utilizadas com o mesmo objetivo. No entanto, a FTA é, disparadamente, a preferida pelos analistas de segurança.

A FTA utilizada na FHA nível aeronave é dita preliminar porque, mais adiante, na FHA nível sistemas, as condições de falha e os requisitos estabelecidos nível aeronave serão confirmados e/ou atualizados.

Vamos utilizar uma função nível aeronave tratada na AC 23.1309-1E, qual seja, a função "**Apresentar a informação de atitude, em rolagem (*roll*) e arfagem (*pitch*)**".

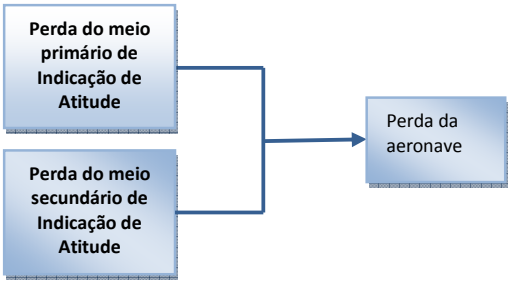
A pior condição de falha para essa função é "Perda total da informação de atitude, em rolagem e arfagem". Trata-se de uma condição catastrófica, para todas as fases do voo.

A FTA teria a seguinte estrutura:



Onde o evento "Perda da Aeronave" é o chamado Evento de Topo (ET) da FTA. A porta "AND", da Álgebra de Boole, é utilizada para expressar que é necessário que ocorra a perda de ambos os meios de indicação de atitude para que ocorra o ET.

Numa configuração de Diagrama de Blocos de Confiabilidade (DBC), o esquema seria como o de uma configuração paralela, conforme figura abaixo.



Ou seja, para que ocorra o ET (Perda da Aeronave), é necessário que ocorram as duas condições de falha.

No caso de um evento catastrófico, o requisito estabelece que a taxa de ocorrência deve ser menor que 1.10^{-9} por hora de voo. Supondo que o tempo médio de voo seja de 6 horas, temos uma Falibilidade[1] permitida $\lambda t < 6.10^{-9}$, por voo.

Tendo em conta que numa porta "AND" as probabilidades dos eventos de entrada se multiplicam, poderíamos estabelecer, por exemplo, para o sistema fornecedor do meio primário de indicação de atitude o requisito de

[1] **Falibilidade (F)** ou **Probabilidade de falhar até um instante t**. Considerando que $e^{-\lambda t} = 1 - \frac{\lambda t}{1!} + \frac{(\lambda t)^2}{2!} - \frac{(\lambda t)^3}{3!} + \ldots$ e que, para $\lambda t < 0{,}1$, a expressão constituída pelos dois primeiros termos da série $(1-\lambda t)$ é uma boa aproximação para $e^{-\lambda t}$, ou seja, para a Confiabilidade R, vem que a Falibilidade, que é dada por $F = 1 - R = 1 - (1 - \lambda t) = \lambda t$, é também uma boa aproximação para F, na condição de $\lambda t < 0.1$(Pág. 39 e *Appendix 2* da Ref.1).

probabilidade "menor que 3.10^{-6}", resultando um requisito de "menor que 2.10^{-3}", para o sistema fornecedor do meio secundário, porque "3.10^{-6}**.** $2.10^{-3} = 6.10^{-9}$".

Não é difícil obter a faixa "menor que 3.10^{-6}", usando uma plataforma estabilizada por giroscópios a laser, por exemplo. Mas a escolha dessas faixas de probabilidades para os sistemas é, sem dúvida, fortemente influenciada pela experiência dos projetistas.

Esse procedimento é repetido para todas as condições de falhas funcionais catastróficas ou maiores severa, nível aeronave.

Feita a análise funcional nível aeronave, passa-se para a análise funcional nível sistemas, que, enfim, serão responsáveis pela função nível aeronave. Trata-se do segundo passo da SA.

2º Passo: Realize uma FHA nível sistema.

A partir dos requisitos de segurança estabelecidos para os sistemas responsáveis pela função em análise, os projetistas deverão obter uma arquitetura para os mesmos, tal que a probabilidade de cada um, como um todo, fique dentro desses requisitos.

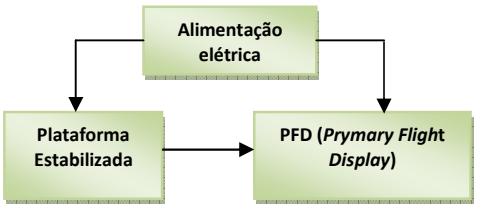
Observe que, com esse procedimento, os projetistas começam a configurar os sistemas, de acordo com os requisitos de segurança da Autoridade de Certificação.

Prosseguindo no exemplo, podemos então considerar que temos dois sistemas: um sistema principal (primário) de indicação de atitude e um sistema alternativo (secundário).

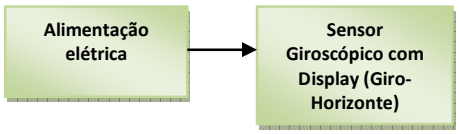
O sistema principal pode ser aquele fornecido num display principal de voo *(Prymary Flight Display)* e seu associado sensor giroscópico remoto, e o sistema secundário ou alternativo pode ser um giro horizonte instalado diretamente no painel da aeronave.

3º Passo: Realize uma Avaliação Preliminar de Segurança de Sistema (*Preliminary System Safety Assessment - PSSA*).

Os resultados da FHA nível sistemas são os inputs para a PSSA. Contudo, a decisão de levar a efeito uma PSSA depende da arquitetura do projeto, de sua complexidade, além de outras considerações. No presente caso, os sistemas são simples[2]. A arquitetura de cada um poderia ser como apresentado na figura abaixo.



(a) Sistema Primário de Indicação de atitude.



(b) Sistema Secundário de Indicação de Atitude

Os equipamentos disponíveis para constituírem os sistemas são provavelmente *Off-the-Shelf*, isto é, disponíveis no mercado e com taxas de falha especificadas.

Faremos as considerações finais no próximo MSC.

Até lá

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.*

[2] Para um exemplo de PSSA completo, sugere-se que o leitor consulte a Ref. 2.