Melhore Seus Conhecimentos (MSC)

System Safety Assessment (Avaliação de Segurança de Sistemas) dos Maravilhosos Displays Eletrônicos de Aeronaves Civis

***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 60 – 25SET2016

Deslumbrante apreciar o painel de uma aeronave civil com seus maravilhosos displays eletrônicos, obras de arte da tecnologia eletrônica. Fascinantes, sem dúvida, mas você conhece as exigências da Autoridade de Aeronavegabilidade para aceitá-los, numa certificação de tipo de uma aeronave que os contêm? Este é o nosso assunto de hoje. Siga-nos.

Sem dúvida, é lindo demais ver um display eletrônico de uma aeronave civil[1]. No entanto, para aquele *display* estar ali, aceito pela Autoridade, há que se percorrer um caminho razoavelmente longo, no ciclo da certificação *aeronáutica.*

Os *displays* eletrônicos instalados nas aeronaves têm Aprovação TSO (TSOA), cumprindo os requisitos constantes da TSO-C113a: *Airborne Multipurpose Electronic Displays*. Essa aprovação lhes propicia a condição necessária para a instalação, porém a suficiência só será reconhecida após os ensaios dedicados nas aeronaves.

Como qualquer sistema de uma aeronave, esses displays passam pelo rigoroso crivo da Autoridade, seja na aceitabilidade operacional e aceitabilidade de instalação na aeronave, seja pela sua admissibilidade, sob o ponto de vista da segurança (*safety*), assegurada pela atividade de *Safety Assessment*[2]. É neste segundo enfoque que nos concentraremos neste MSC.

A partir deste ponto, vamos abreviar o termo *Safety Assessment* para suas iniciais SA, por economia de espaço.

Consideraremos aqui o caso da certificação de tipo de aeronaves enquadradas no CFR 14 Part 23, na categoria Commuter, cujos requisitos de segurança de sistemas são os mesmos da Part 25.

A AC 23.1311-1C (*Installation of Electronic Display in Part 23 Airplanes*) trata da instalação desses sistemas e faz considerações sobre a atividade de SA pertinente aos mesmos, vinculando-a, no entanto, à AC 23.1309-1E, que é o documento que contém as sugestões para os Aplicantes realizarem tal atividade.

Iniciamos, dizendo que os requisitos de segurança (*safety*) de sistemas são estabelecidos de acordo com o potencial efeito de falhas nas funções nível aeronave. Por outro lado, as falhas que ocorrem no nível aeronave são reflexos das falhas que ocorrem no nível sistemas, que são os meios que realizam as funções nível aeronave.

O potencial efeito de uma falha[3] de uma função nível aeronave é denominado *failure condition* - FC (condição de falha)[4]. As FC têm uma gradação de gravidade conhecida por "severidade" (*severity)*, que enquadra as FC da menos grave à mais grave, na seguinte escala: *No Safety Effect*, *Minor*, *Major*, *Hazardous* e *Catastrophic*[5].

[1] O display de aeronave militar também é uma beleza.
[2] É mais frequente o uso do termo em inglês.
[3] Falha pode ser a perda da função ou sua degradação, causando o que chamamos de *misleading* (informação enganosa).
[4] É mais frequente o uso do termo em inglês.
[5] Vide AC 23.1309-1E.

A grande preocupação, sem dúvida, é com as FC *Hazardous e Catastrophic*. A primeira porque, em ocorrendo, exige um trabalho intenso da tripulação, para manter a aeronave sob controle, podendo, não obstante os esforços da tripulação, gerar ferimentos graves a bordo. A segunda porque representa a catástrofe, ou seja, o ponto final, a precipitação da aeronave, com as consequências já bem conhecidas.

As FC nível aeronave são identificadas pela chamada *Aircraft Functional Hazard Analysis* – AFHA (Análise de Perigo Funcional Nível Aeronave), a primeira análise a ser realizada na atividade de SA.

Nessa análise, primeiramente se identificam as funções nível aeronave e suas respectivas FC. A identificação é feita com o verbo no infinitivo, por exemplo: "Prover a informação de atitude da aeronave, prover a informação de altitude da aeronave", etc.

Mas prover a quem? Bolas, ao piloto, naturalmente, para que ele possa comandar e controlar a aeronave. É ele, sem dúvida, o foco, razão pela qual esperamos estar ele bem disposto e feliz, sempre que for exercer sua atividade. Como engenheiros da área de risco, feliz ou infelizmente, não temos controle sobre o temperamento deles (pelo menos, por enquanto).

As funções nível aeronave são providas pelos sistemas da aeronave. Antigamente, elas eram funções providas por sistemas discretos, mas hoje, muitas delas foram integradas, sendo providas visualmente pelos notáveis *displays* eletrônicos, sobretudo aquelas de navegação e controle de voo.

As aeronaves modernas têm no painel os chamados PFD (*Primary Flight Display*), que proveem ao piloto as principais informações de voo (*Primary Flight Informations* – PFI), quais sejam: *Attitude, Altitude, Airspeed e heading (direção),* além de outras, por exemplo, aquelas relativas ao desempenho do motor.

O termo *Primary* significa que se trata do principal display, isto é, aquele que o piloto visualiza em primeiro lugar.

É preciso entender que, na realidade, o *display* apenas apresenta as informações geradas pelos sistemas que as produzem, a partir de sensores dedicados. Dito em outras palavras, o display é um componente que faz parte de vários sistemas, agindo apenas como um "anunciante" das informações geradas por tais sistemas.

Quando uma dessas informações desaparece do *display*, entende-se, em princípio, que o sistema gerador tenha falhado, em algum ponto, inclusive, porque não, o próprio *display*, parte visual (*pictorial)* desses sistemas.

Sucede, no entanto, que a perda das funções de provimento das PFI *attitude, altitude* e *airspeed* são consideradas *failure conditions* de potencial catastrófico, enquanto a perda da informação de *heading (direção)* é de severidade *hazardous*.

Se o *display* falhar como um todo, a situação poderia ser considerada de altíssimo perigo, ou seja, de potencial "triplamente" catastrófico.

Ai entra o chamado princípio da intolerância à falha única (*single failure*) da Autoridade, segundo o qual um sistema que possui função com FC de severidade catastrófica não pode perdê-la, em virtude de uma falha singular (única).

Desse modo, para se enquadrar com certeza nesse princípio, não se pode ter um único *display* instalado na aeronave. É necessário que exista outro, no mínimo com as mesmas funções, podendo ser idêntico ao primeiro (mesmo fabricante e mesmo PN) ou diferente, mas independente do principal, em termos de sensores e alimentação elétrica.

Por isso, é imperioso que sejam instalados nas aeronaves dois *displays* executando as mesmas funções, cujas FC são catastróficas ou *hazardous*. São os chamados sistemas duais ou redundantes.

Quando os *displays* são idênticos, há quem diga ser isso um inconveniente porque ambos têm os mesmos modos de falha. Todavia, essas pessoas hão de entender que a ocorrência de falhas, principalmente em sistemas eletrônicos, é um evento aleatório, ou seja, não acontecem necessariamente no mesmo momento, nos dois *displays*, a despeito de serem "idênticos".

Em vez desses displays duais ou em *standby*, pode-se utilizar também os chamados *Reversionary Flight Displays (*Displays de Voo Reversíveis*),* tais como o *Multifunction Display*

(MFD). A função primordial do MFD é prover ao piloto acesso a vários dados, ou combinação de dados, usados para voar a aeronave, navegar, comunicar e/ou gerenciar sistemas da aeronave.

Mas o MFD pode ter uma outra página de *display*, ou seja, tem um *display* reversível, para apresentar as PFI, agindo como um meio alternativo, em caso de falha do PFD.

Bem, amigos, paramos por aqui, no espaço disponível para os MSC. Dentro em breve, traremos mais informações mais detalhadas sobre o tema tratado neste *flash*, num novo projeto de difusão de conhecimentos da DCA-BR.

Fiquem atentos, obrigado e até mais.

Referências:

1. *CFR 14 Part 23 § 1309 – Equipment, System and Installation, Amdt 23-62, FAA, Dec. 2, 2011; USA.*
2. *CFR 14 Part 23 § 1311 – Electronic Display Instrument Systems, Amdt 23-62, FAA, Dec. 2, 2011; USA.*
3. *AC 23.1311-1E – System Safety Analysis and Assessment for Part 23 Airplanes, FAA, Nov, 2011; USA.*
4. *AC 23.1311-1C – Installation of Electronic Display in Part 23 Airplanes, FAA, Nov., 2011; USA.*