Melhore Seus Conhecimentos (MSC)

Safety Assessment: Conversando com Requerentes e Certificadores – II

***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 55 – 15 JUL 2015

Neste MSC, vamos dar continuidade ao tema em epígrafe, procurando concluir a primeira parte da Safety Assessment (Avaliação da Segurança), focalizando a Hazard Assessment (HA) *e a Risk Assessment* (RA). *Estamos procurando ser cuidadosos nessa discussão porque é desta primeira parte que depende a eficácia da Safety Assessment* (SA).

Identificadas as funções da aeronave, o analista de *safety* focaliza, mas só mesmo, aquelas consideradas essenciais ou críticas para o comando e controle do piloto, ou seja, aquelas cuja perda (por falha ou mau funcionamento) são consideradas de severidade catastrófica (perda total de comando e controle por parte do piloto) ou severa maior (intenso trabalho do piloto, muita dificuldade de comandar e controlar a aeronave).

A realização do par HA e RA, com foco nas funções essenciais/críticas da aeronave e dos sistemas que a realizam denomina-se *Functional Hazard Assesssment* – FHA (Avaliação de Perigos Funcionais).

O fato de o foco estar nas funções essenciais/críticas não quer dizer que o analista deva desprezar as funções de severidade mais branda, como a Maior (*Major*) e Menor (*Minor*). A severidade Maior é analisada pelo analista de uma maneira mais simples e de forma qualitativa, apenas para chamar a atenção de quais sejam essas funções. Contudo, não há uma preocupação maior com essa severidade. As funções de severidade Menor simplesmente são elencadas, e nada mais.

Mas, neste ponto, cremos que dá para perceber que confiabilidade e segurança (*safety*) não são expressões sinônimas. Na confiabilidade, consideramos todas as funções da aeronave (essenciais/críticas e não essenciais/críticas) e todos os sistemas que realizam essas funções, ao passo que na segurança você só considera aquelas funções essenciais/críticas e apenas os sistemas que as realizam, os quais, é claro, são também considerados essenciais/críticos.

Na verdade, pode-se ter um projeto com alta confiabilidade, porém inseguro (Ref. 1).

Aliás, na regulamentação da Autoridade de Certificação, o termo confiabilidade é raramente citado. Praticamente só se fala de *Unreliability ou Falibility* (probabilidade de falhar), porque a Autoridade está preocupada com a segurança, isto é, com os efeitos de falhas e mau funcionamento. Confiabilidade, no entanto, não percamos de vista, é muito importante, principalmente para fatores do suporte técnico-logístico (manutenção, peças de reposição, equipamentos de apoio no solo) e, em consequência, para a disponibilidade operacional.

Voltando. Identificadas as funções da aeronave consideradas essenciais/críticas, o olho do analista focaliza os sistemas que tomam parte na realização dessas funções, e o processo continua até termos esses sistemas perfeitamente

definidos com as características de segurança desejáveis. A continuidade da *SA* não é assunto deste flash. O leitor poderá ter uma ideia razoável de seus passos seguintes no MSC 10 (Ref. 2).

A partir de agora, queremos focalizar um outro ponto. Gostaríamos de falar sobre sistemas utilizados no Controle de Tráfego Aéreo (*Air Traffic Control* – ATC). Mostrar que nesses sistemas, a FHA segue uma filosofia semelhante, mas com algumas nuances.

Há dois tipos de sistemas nessa área: aqueles que são utilizados como auxílios rádio à navegação e aqueles cujas informações são utilizados por um operador do ATC, para controlar as aeronaves. Ambos, é claro, instalados em terra.

Podemos citar como exemplos de sistemas de auxílio rádio o DME (*Distance Measuring Equipment* – Equipamento Medidor de Distância), NDB (*Non Directional Beacon* - Rádiofarol Não-Direcional), etc.

Esses sistemas não são submetidos a nenhum controle, isto é, após colocados em operação, continuam operando autonomamente. Trata-se de uma ajuda ao piloto, mas instalada no solo. A perda de um ou de outro pode ser contornada por outros meios disponíveis para o piloto.

Já aqueles utilizados por um operador do ATC[1] têm outra conotação. O "piloto", neste caso, é o operador, que utiliza as informações fornecidas pelo sistema para o controle das aeronaves; contudo, ele não se encontra no ambiente da aeronave; ele está no solo. A adrenalina, claro, é diferente daquela do piloto de uma aeronave.

Citemos, como exemplo, o sistema radar de vigilância, que envia sinais de interrogação à "nuvem" de aeronaves. Capta de volta os sinais de resposta dessas aeronaves propiciados pelo transponder existente em cada uma, processa esses sinais e encaminha um conjunto de informações ao operador do ATC. O operador utiliza essas informações para sua atividade de controle.

[1] Apenas por curiosidade, o ATC é reponsável por cerca de 5% dos acidentes catastróficos. Os sistemas das aeronaves, como já tivemos a oportunidade de apresentar no MSC 48, assume a culpa de 10% desses acidentes.

À semelhança da aeronave, as funções que produzem as informações ao operador são realizadas por subsistemas ou unidades ativas, isto é, que geram e processam os sinais de informação, encaminhando-os ao operador do ATC.

Desse modo, esses subsistemas ou unidades ativas é que são o alvo da FHA. O conjunto de todas as funções (inclusive as do interesse da FHA) interessa apenas à confiabilidade, visando uma boa disponibilidade operacional para o radar.

Não somos especialistas em sistemas utilizados no ATC, mas uma experiência recente, em que procuramos auxiliar um requerente de certificação, junto ao ente certificador dessa área, nos propiciou adquirir algum conhecimento a respeito. Assessoramos o cliente na produção dos documentos essenciais para a certificação do projeto do radar e, no trato com a segurança, trabalhamos também na assessoria para a realização de uma FHA.

Esse radar tem vários blocos funcionais, como por exemplo a antena rotativa, o motor e seu controle e uma unidade ativa que gera e processa os sinais que, ao final, serão encaminhados sob a forma de informações ao operador. Tudo isso, numa configuração redundante, o que eleva muito a segurança e a confiabilidade do sistema.

Como já enfatizamos, no caso de aeronaves, fixamo-nos, no radar, no subsistema ou unidade que produzia as informações para o operador do ATC e verificamos as severidades da falha ou de um mau funcionamento desses itens. Chegamos então ao final da FHA para o sistema.

Bem. Companheiros, procuramos, neste "flash", conversar um pouco mais sobre a FHA, tratando novamente de aeronaves e também de sistemas do Controle de Tráfego Aéreo, embora de maneira não tão exaustiva.

A ideia era mostrar que uma FHA não é tão complicada. O importante é entender a filosofia que envolve a metodologia. Numa enfatização final, afirmamos que, na SA, o importante é identificar bem as funções e trabalhar qualitativa e quantitativamente apenas com aquelas de

severidade catastrófica e maior severa (*hazardous*) para o piloto (ou operador do ATC),

Cremos, por outro lado, ter deixado claro que essas funções são realizadas por subsistemas ou unidades ativas, isto é, que geram e processam sinais. O objetivo é propiciar ao piloto meios para comandar e controlar a aeronave

Obrigado e até uma próxima oportunidade.

Referências:

1. Berquó, jolan Eduardo. **MSC 34 – Confiabilidade e Segurança *(Safety)***: **Curiosidades**. DCA-BR, São José dos Campos (SP): 06/3/2013.
2. Berquó, Jolan Eduardo. **MSC 10 - Avaliação de Segurança (*Safety Assessment- SA*).** DCA-BR, São José dos Campos (SP): 24/3/2012.