Melhore Seus Conhecimentos (MSC)

Hardware e Software na Certificação de Sistemas: Uma Resumida Opinião

***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 57 – 10 FEV 2016

Se tem um assunto que gera dúvidas em muita gente, na área de certificação de aeronaves, é o binômio Hardware (HW) e Software (SW). Neste MSC, falaremos brevemente sobre essa dupla, tomando por base recomendações da Autoridade de Aeronavegabilidade (FAA, EASA, ANAC, etc.), neste trabalho tratada simplesmente como Autoridade.

Antes de tudo, vamos estabelecer aqui que o que falaremos, neste MSC, refere-se a sistemas eletrônicos, os únicos passíveis de ter o binômio HW e SW.

Vamos nos focalizar na recomendação SAE ARP 4761 (Ref. 1)[1], recomendada pela Autoridade como uma metodologia aceitável (mas não a única) para o requerente demonstrar a conformidade de seu projeto com os requisitos de segurança (*safety*) dessa Autoridade[2].

O propósito da ARP 4761, como o próprio título indica, é passar, sugerir ao requerente uma maneira de realizar uma avaliação de segurança (*Safety Assessment*) do projeto da aeronave, de modo a atender aos requisitos de segurança da Autoridade.

No entanto, o mais importante, em nossa opinião, é que a metodologia da ARP é também um excelente instrumento de alocação ou inserção de requisitos de segurança.

Dito em outras palavras, a metodologia permite ao requerente inserir, no início do projeto (Fase Conceitual), os requisitos de segurança da Autoridade.

O processo começa com a alocação ou inserção desses requisitos às funções da aeronave, por meio da chamada Análise de Perigos Funcionais (*Functional Hazard Assessment* – FHA), utilizando, mais frequentemente, a ferramenta Análise por Árvore de Falhas[3] (*Fault Tree Analysis* – FTA)[4].

A partir dessa alocação, nível aeronave, outra FHA, mais comumente também feita com o recurso da ferramenta FTA, é utilizada para transladar esses requisitos nível aeronave para os sistemas que vão realizar as funções da aeronave. Trata-se, pois, neste caso, de uma FHA nível sistemas.

A translação dos requisitos nível sistemas para a arquitetura de cada um deles, ou seja, para os equipamentos que vão constitui-los, é feita por uma Análise de Segurança de Sistemas Preliminar (*Preliminary System Safety Analysis* – PSSA). Nessa translação de requisitos para os equipamentos, aparece, pela primeira vez, distintamente, o binômio HW e SW.

---

[1] A ARP 4761 é, na realidade, uma metodologia de *safety assessment*, prevista na SAE ARP 4754 (Ref. 2), documento este que trata da engenharia de sistemas - voltada para o processo de Certificação Aeronáutica, sendo também recomendada pela Autoridade.

[2] Porém, a ARP 4761, assim como a ARP 4754, não é um requisito, ou seja, o requerente pode, e o dizemos com ênfase, utilizar a metodologia que melhor lhe aprouver, desde que seja apta a demonstrar a conformidade do projeto com os requisitos de segurança da Autoridade. Esta é a filosofia.

[3] Adotamos aqui a tradução Árvore de Falhas, pelo uso, mas alertamos que a NBR 5462, da ABNT, entende que a tradução correta de *Fault Tree Analysis* é Análise de Árvore de Panes, por considerar que o termo *Fault* se traduz por Pane (o estado de um item após ter sofrido uma falha). Para essa norma, *Failure* é Falha, isto é, um evento, *e Fault* é Pane, ou seja, um estado posterior à falha.

[4] A ARP 4761 cita várias outras ferramentas; no entanto, a FTA é, disparadamente, a mais utilizada.

Este é um ponto importante. O equipamento é constituído de um HW (aquilo que se vê) e de um SW, embutido (*firmware*) em algum ou alguns componentes do HW. É como "Corpo e alma", digamos, mas guardando as devidas proporções.

Pois bem, a alocação de requisitos de segurança para os equipamentos, derivados da PSSA, inclui um limite máximo permissível de taxa de falha para cada um desses equipamentos (com ou sem SW embutido).

Mas essa taxa de falha refere-se apenas ao HW. Quanto ao SW, em si, de cada equipamento, convenhamos, não faz sentido estabelecer uma taxa de falha para o mesmo, por uma série de razões, tais como: (a) não há dispersão de características no SW, como no HW; (b) no SW, cada cópia é igual à original; (c) não há falhas devidas à variabilidade física (temperatura, rodagem, desgaste, fadiga, etc.), como no HW; (c) as "falhas" (erros) manifestam-se sem aviso prévio, ou seja, é inerente ao SW desenvolvido.

Acrescentemos também que não faz sentido falar em confiabilidade (R) de SW. Isso é claro, já que não se pode perder de vista, e aqui se enfatiza, que a Confiabilidade é uma função de distribuição de probabilidade contínua no tempo[5]. SW não se enquadra nisso. O tempo não tem a mínima influência no SW. Ele vai se comportar sempre do mesmo jeito, qualquer que seja o tempo de operação do sistema, onde esteja instalado. Num certo momento de seu processamento, ou ele funciona ou não funciona.

Há até mesmo quem diga, cremos que em tom de brincadeira, que em SW se tem R=1 (sem erro) ou R=0 (com um ou mais erros); mas, isso, em se tratando de confiabilidade, tal como assim definida, em nossa opinião, é pura pilhéria.

Muito bem, para o equipamento, como um todo, é estabelecida, como requisito de segurança, uma taxa de falha máxima. Mas, como dissemos, taxa de falha só se aplica ao HW, estendendo-se para o SW sob a forma de níveis de qualidade em seu desenvolvimento.

Aí, entra um documento da RTCA (*Radio Technical Commission for Aeronautics,* Ref. 3) conhecido como DO-178 (atualmente na versão C), recomendado pela ARP 4754.

Falemos só do essencial, na aplicação desse documento. Sabemos que essa aplicação parte dos cinco níveis de severidades para as condições de falhas de um equipamento, com ou sem SW: A, B, C, D e E, correspondendo, respectivamente, às seguintes severidades: Catastrófica, Maior Severa (*Hazardous*), Maior, Menor e Negligenciável (*No safety effect*).

O que se requer para o SW, repetimos, são níveis de esmero (qualidade), no seu desenvolvimento, considerando máxima qualidade para os equipamentos enquadrados na severidade A, decrescendo até o nível E; mas o nível E não requer nenhuma atenção além do normal para o desenvolvimento do SW.

Por sua vez, para um HW altamente complexo (*Very higly complex*), existe um documento, a DO-254 (Ref. 4), dedicado ao seu desenvolvimento[6]. Como na DO-178, aqui também há uma certa dose de esmero no projeto desse tipo de HW.

Assinalamos que a aplicação da DO-178, no desenvolvimento de SW, não é tarefa simples. Neste momento, existem poucos especialistas no Brasil capazes de aplicar com esmero esse documento.

Bem, ficamos por aqui. Longe de nós pensar que deixamos tudo inteiramente claro, mas cremos ter deixado os leitores com o que pensar e discutir, quando tratarem de HW e SW, na certificação. Leiam, com paciência, a DO-178 e DO-254.

A todos, um feliz ano de 2016, com muita saúde, porque, conforme um famoso jargão, saúde é o que interessa, o resto não tem pressa; poucas, mas sábias palavras, ditas, pela primeira vez, não sabemos por quem.

[5] No caso de aeronaves, a função de distribuição de probabilidades Confiabilidade é dada por $R = e^{-\lambda t}$, onde λ é uma constante denominada taxa de falha, e t é o tempo de operação.

[6] Numa outra ocasião, trataremos da DO-254, explorando esse conceito de *Very Higly Complex*.

Referências:

1. *SAE ARP 4761*, G*uidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, EUA, Nov/1996.*
2. *SAE-ARP-4754, Certification Considerations for Highly Integrated or Complex Systems, EUA, Nov 1996.*
3. *RTCA DO-178C, Software Considerations in Airborne Systems and Equipment Certification, EUA, Jan/2012.*
4. *DO-254, Design Assurance Guidance for Airborne Electronic Hardware, EUA, Abril/2000.*
5. *DoD: MIL-HDBK-217F, Reliability Prediction of Electronic Equipment, Departmente of Defense, Washington, D.C., 1991.*