DO-178: Software Assurance – Um papo com Certificadores

***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 58A – 15 JUL 2016

O documento RTCA DO-178B/C[1] nunca esteve tanto em voga como atualmente, em virtude do avanço de sistemas eletrônicos com funções baseadas em software (SW). O documento tem sido exigido em todas as áreas da aeronáutica, seja militar ou civil, e até para os produtos do Controle de Tráfego Aéreo, como radares, DME, etc. Aqui, naturalmente, vamos dar uma pincelada sobre o assunto.

A RTCA DO-178B/C, ou, por simplicidade, simplesmente DO-178, é um desenvolvimento conjunto da *Radio Technical Commission for Aeronautics* (RTCA), dos Estados Unidos, e da *European Organization for Civil Aviation Equipment* (EUROCAE). A versão equivalente da organização europeia é o EUROCAE/ED-12B/C[2].

De pronto e peremptoriamente, deve-se ter em mente que o documento não é um requisito de engenharia de desenvolvimento de SW da Autoridade, mas um padrão de garantia de esmero desse desenvolvimento.

Ficando apenas com a DO-178, por simplicidade, devemos deixar claro que a Autoridade não certifica SW, mas o sistema que o contém; contudo, o Aplicante terá que aplicar a DO-178, caso contrário não ocorrerá a certificação do sistema.

A empresa que desenvolve SW é livre para usar seus próprios métodos de engenharia de SW, desde que os resultados reflitam a inserção dos critérios de garantia da DO-178, nos processos de planejamento, definição de requisitos, projeto e codificação, integração, verificação, gerenciamento da configuração e garantia da qualidade.

O processo de garantia da qualidade está imerso em todos os outros processos, de modo a procurar garantir que esses processos sigam de perto a DO-178. Portanto, o profissional da área de *Quality Assurance* é peça fundamental para a aplicação completa da DO.

O ponto de partida para o emprego da DO-178 é a chamada *Functional Hazard Assessment* – FHA, a primeira avaliação da atividade de *Safety Assessment*[3].

Essa avaliação considera a severidade de cada condição de falha[4] (*failure condition*). A partir daí são então estabelecidos níveis (*levels*) de garantia da qualidade[5] para o desenvolvimento do SW, seguindo a seguinte gradação:

- **A** para as *failures conditions* de severidade catastrófica (*Catastrophic)*;
- **B** para as *failures conditions* de severidade perigosa (*Hazardous*);
- **C** para as *failures conditions* de severidade Maior (*Major*);
- **D** para as *failures conditions* de severidade Menor (*Minor*); e
- **E** para as *failures conditions* com nenhum efeito na segurança (*No Safety Effect*).

Um exemplo que conduz ao nível A é a perda da função que provê ao piloto a indicação de atitude

[1] *Software Considerations in Airborne Systems and Equipment Certification.*
[2] *Consideations sur le Logiciel en vue de la certificacion des Systemes et Equipments de Bord.*
[3] Veja a metodologia no documento SAE ARP 4761 – *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.*
[4] Costuma-se utilizar mais o termo inglês *Failure Condition.*
[5] Os chamados DAL's (*Development Assurance Levels*).

da aeronave em *roll* (rolagem) e *pitch* (arfagem), atualmente apresentada num EFIS[6] (*Electronic Flight Instrument System*), que funciona como Display de voo principal (*Primary Flight Display* - PFD).

No outro extremo, isto é, *level* E, estão, por exemplo, SW de funções de entretenimento de passageiros, uma vez que suas *failures condition*s não trazem nenhum efeito para a segurança.

Ora, diriam uns, então a função de prover dados de acidente (cumprida por um *Flight Data Recorder*- FDR) e a função de prover a conversação na cabine da aeronave (cumprida por um *Cockpit Voice Recorder* - CVR) também seriam *level* E, uma vez que a perda desses equipamentos não tem nenhum efeito na segurança. Errado. Na realidade, em virtude da importância desses sistemas, numa eventual investigação de acidente, o SW dos mesmos, por exigência da Autoridade, está enquadrado no *level* D.

Evidentemente, o certificador tem que ter uma boa ideia da parafernália de dados e documentos produzidos nos processos de desenvolvimento do SW, para discernir, juntamente com o Aplicante, quais os dados e documentos deverão ser apresentados pelo Aplicante.

Afinal, todas as informações de desenvolvimento do SW, previstas na DO-178, devem ser entregues à Autoridade? Claro que não porque seria muita coisa para descarregar na Autoridade. Em geral, o Aplicante do desenvolvimento do SW apresenta apenas um subconjunto de dados, a priori discutido e concordado com a Autoridade. No entanto, o Aplicante deverá reter e preservar todos os dados relevantes, conforme previstos na DO-178.

A Autoridade poderá então, a qualquer momento, examinar as facilidades do Aplicante aplicadas no processo de desenvolvimento do SW e quaisquer dados pertinentes que se encontram preservados pelo Aplicante.

Se tem uma coisa que preocupa as empresas é a questão do custo da aplicação da DO-178. Segundo alguns, já bem experientes no desenvolvimento de SW, a aplicação da DO-178 pode custar em média cerca de 30% do custo total do sistema que o incorpora; mas, dizem, pode custar mais ou menos até 6 vezes mais do que isso, se os especialistas não ficarem atentos às armadilhas que podem surgir na aplicação do documento.

Naturalmente, os custos são mais elevados para SW nível A, decrescendo até o nível E.

Para encerrar esse breve *flash*, vamos sumarizar as ideias centrais aqui inseridas.

(1) A DO-178 não é um requisito, mas um padrão de garantia da qualidade do desenvolvimento do SW.
(2) A empresa que desenvolve SW é livre para usar seus próprios métodos de engenharia de SW, desde que os resultados reflitam a inserção dos critérios de garantia da DO-178.
(3) SW não é certificado, mas sim o sistema que o contém; contudo, se a DO-178 não for seguida, não ocorrerá a certificação do sistema.
(4) O enquadramento do SW, num determinado nível de garantia da qualidade (DAL), depende dos resultados da *Functional Hazard Assessment* (FHA).
(5) Às vezes, a Autoridade estabelece um certo DAL para sistemas que não têm a mínima influência na segurança (Ex.: FDR e CVR).
(6) O certificador precisa estar bem informado quanto aos processos, dados e documentos produzidos, em função da aplicação da DO-178, principalmente para saber escolher aqueles que o Aplicante deverá repassar-lhe.

Ficamos por aqui. Até a próxima.

Referências

1. *Radio Technical Commission for Aeronautics (RTCA). DO-178C: Software Considerations on Airborne Systems and Equipment. RTCA (EUA), 2012.*
2. *Radio Technixcal Commission for Aeronautics (RTCA). DO-178B: Software*

[6] Denominação genérica para displays eletrônicos, como, por exemplo, *Primary Flight Displays* (PFD), *Multifunction Display* (MFCD), etc.

Considerations on Airborne Systems and Equipment. RTCA (EUA), 1992.

3. *HILDERMAN V., BAGHAI T. Avionics Certification – A Complete Guide to DO-178B (Software), DO-178C (Upgrade), DO-254 (Hardware). Avionics Communications Inc. (EUA), 2014.*