ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS DA AERONÁUTICA

DIVISÃO DE ENSINO

CURSO DE APERFEIÇOAMENTO DE OFICIAIS 1º/2024

RICARDO HENRIQUE RABELO **AMORIM**, Cap Av

Incorporação das Recomendações do Padrão DO-178C para o Desenvolvimento de *Software* Embarcado na Divisão de Eletrônica do IAE

Rio de Janeiro

2024

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS DA AERONÁUTICA
DIVISÃO DE ENSINO
CURSO DE APERFEIÇOAMENTO DE OFICIAIS 1º/2024

RICARDO HENRIQUE RABELO **AMORIM**, Cap Av

Incorporação das Recomendações do Padrão DO-178C para o Desenvolvimento de *Software* Embarcado na Divisão de Eletrônica do IAE

Trabalho de conclusão de curso apresentado no Curso de Aperfeiçoamento de Oficiais da Aeronáutica como requisito parcial para aprovação no Curso de Pós-graduação *Lato Sensu* em Liderança com Ênfase em Gestão no COMAER.
Linha de Pesquisa: Gestão Institucional
Orientador: Pedro Nolasco Duarte, Maj Av

Rio de Janeiro
2024

RICARDO HENRIQUE RABELO **AMORIM**, Cap Av

Incorporação das Recomendações do Padrão DO-178C para o Desenvolvimento de *Software* Embarcado na Divisão de Eletrônica do IAE

Trabalho de conclusão de curso apresentado no Curso de Aperfeiçoamento de Oficiais da Aeronáutica.

Aprovado por:

_____

Pedro **Nolasco** Duarte, Maj Av
EAOAR

_____

Rafael de Lima **Santana**, Maj Inf
EAOAR

Rio de Janeiro

2024

RESUMO

Desde o início desse século, o *software* embarcado tem exercido protagonismo crescente em sistemas aeroespaciais. O fenômeno também se verifica na FAB, nas suas mais diversas plataformas, com destaque para os veículos suborbitais VSB-30 e VS-50, desenvolvidos pelo Instituto de Aeronáutica e Espaço em parceria com a indústria e o Centro Espacial Alemão. Neste trabalho, propõe-se a incorporação das recomendações do padrão DO-178C aos processos de desenvolvimento de *software* da Divisão de Eletrônica do IAE, como forma de mitigar riscos à certificação dos veículos suborbitais ali desenvolvidos, por não conformação a normas aeroespaciais, e impedir que problemas de má comunicação prejudiquem o desenvolvimento bem-sucedido do *software* neles embarcado. Tais veículos são projetos complexos e multidisciplinares, resultantes da integração de diversos dispositivos e sistemas, dentre os quais se destacam os de controle. Esses sistemas demandam uma expressiva eletrônica embarcada, com o uso intensivo de *software* para torná-los versáteis e reutilizáveis. Dessa forma, seu desenvolvimento impõe não só desafios técnicos, de conformação aos estritos requisitos do setor, mas também gerenciais, relacionados à comunicação entre as partes envolvidas nos projetos. Assim, a incorporação do DO-178C promove o alinhamento da FAB com as melhores práticas do meio aeroespacial, aumentando a eficiência de seus processos de engenharia e facilitando o diálogo com a indústria, o que potencializa a criação de parcerias, uma fonte importante de financiamento alternativo de projetos do Programa Espacial Brasileiro e do Programa Estratégico de Sistemas Espaciais, num contexto de redução contínua do orçamento disponível para a pesquisa e o desenvolvimento na FAB.

Palavras-chave: Software embarcado. Padrão. Requisitos. DO-178C. Certificação.

1 **INTRODUÇÃO**

Segundo Hermann (2000), o *software* embarcado tem exercido grande protagonismo em sistemas eletrônicos desde o início desse século. Na FAB, ele pode ser encontrado em quase todas as plataformas, sendo as modernas aeronaves KC-390 e F-39 Gripen os exemplos mais óbvios. Contudo, também os veículos suborbitais VSB-30 e VS-50, desenvolvidos no Instituto de Aeronáutica e Espaço (IAE) em parceria com o *Deutsches Zentrum für Luft und Raumfahrt* (Centro Espacial Alemão, DLR), fazem uso desse tipo de *software*.

Tais veículos são projetos complexos, repletos de barreiras tecnológicas, cuja superação exige a aquisição de produtos e parcerias junto à indústria, o que, segundo Daw *et al.* (2023), impõe desafios de comunicação entre as partes envolvidas e requer processos de certificação para garantir a conformidade dos projetos com os requisitos estabelecidos, inclusive aqueles definidos em normas específicas.

Nesse sentido, o desenvolvimento de seu *software* requer atenção a aspectos técnicos e gerenciais, que assegurem sinergia e conformação aos estritos requisitos do setor aeroespacial. Na indústria, isso é obtido por meio de um conjunto de recomendações condensadas em documentos técnicos denominados “padrões”.

No caso específico do *software* embarcado em sistemas aeroespaciais, a norma DO-178C: *“Software Considerations in Airborne Systems and Equipment Certification”* (Considerações de *Software* em Sistemas Aerotransportados e Certificação de Equipamentos) converteu-se no padrão de fato do segmento e tem servido de referência de boas práticas desde 1985 (Hilderman, 2014).

Diante do exposto, defende-se a incorporação do padrão DO-178C aos processos de desenvolvimento de *software* da Divisão de Eletrônica do IAE, a fim de reduzir os riscos nos projetos dos veículos suborbitais ali desenvolvidos.

Argumenta-se que o uso de práticas consagradas no desenvolvimento de seu *software* embarcado reduz a probabilidade de fracasso na certificação final destes veículos. Sendo o DO-178C a referência do segmento, sua incorporação representa a institucionalização de tais práticas, com os ganhos associados.

Além disso, suas recomendações impedem que problemas decorrentes da má comunicação prejudiquem a interação entre as partes envolvidas nos projetos, pois estabelecem uma linguagem uniforme, criada por meio de uma estrutura documental clara e ordenada, focada no detalhamento e na rastreabilidade de requisitos.

2 **DESENVOLVIMENTO**

A partir dos anos 1980, a intensificação do uso de *software* em sistemas aeronáuticos levou representantes públicos e privados do setor, no mundo todo, a reunirem-se sob a coordenação da *Radio Technical Commission for Aeronautics* (RTCA), Comissão Radiotécnica para a Aeronáutica, a fim de produzir um documento de boas práticas para o segmento de *software* aeroembarcado (RTCA, 2011).

Como resultado, em 1985, foi publicada a versão DO-178A, fruto do consenso entre um variado grupo de profissionais de diferentes origens e nacionalidades. Ao longo dos anos, por solicitação da *Federal Aviation Administration* (Administração Federal de Aviação, FAA), o padrão sofreu duas grandes atualizações, a fim de incorporar os avanços ocorridos na engenharia de *software*, culminando na publicação do DO-178B, em 1992, e da versão de 2011, o DO-178C, cuja incorporação defende-se neste ensaio.

2.1 **O padrão como uma referência de práticas consagradas**

A elaboração do DO-178C é inspirada no entendimento, compartilhado por Rierson (2013), de que um bom *software* não é fruto do acaso, mas sim de um extenso processo de planejamento, que demanda o envolvimento de pessoal altamente qualificado e dedicado.

As recomendações do DO-178C são definidas a partir da avaliação das condições de falha às quais um sistema aeronáutico pode ser exposto em virtude de erros em seu *software*, classificando-o em um de cinco níveis distintos, aos quais estão associados objetivos específicos a serem perseguidos no processo de desenvolvimento, com o propósito de assegurar o cumprimento dos requisitos de segurança associados (RTCA, 2011).

Conforme Rierson (2013), isso é feito sem a vinculação a métodos específicos, conferindo alguma flexibilidade ao padrão, ainda que limitada. Essa flexibilidade é discutida por Hanssen, Wedzinga e Stuipa (2017), ao afirmarem ser possível incorporar métodos ágeis na estrutura proposta pelo DO-178C, graças à sua ênfase em objetivos, sem a vinculação a métodos específicos, o que ajuda a entender a alta adesão ao padrão entre as diversas organizações consultadas quando de sua pesquisa.

De fato, desde sua publicação original, em 1985, o DO-178 foi rapidamente assimilado (RTCA, 2011), consolidando-se como uma referência nos meios aeronáutico e espacial, por extensão. Para a FAA, a norma DO-178B é o meio usual de verificação de conformidade para aqueles que desenvolvem *software* embarcado (USA, 2018), o que é confirmado por Holloway (2012), segundo o qual o DO-178B foi o meio primário de obtenção de aprovação regulatória para o uso de *software* em sistemas aeronáuticos por mais de vinte anos.

No IAE, os sistemas de controle de veículos suborbitais demandam expressiva eletrônica embarcada, haja vista a elevada carga de automação que embutem. Tal eletrônica requer o uso intensivo de *software*, pois este confere versatilidade aos projetos, permitindo o reaproveitamento de sistemas entre veículos.

Considerando-se que o padrão DO-178C oferece um conjunto de recomendações customizadas para cada nível de criticidade de *software* avaliado, com flexibilidade de métodos para o alcance dos objetivos propostos, sua incorporação pelo IAE permite implementar uma filosofia de desenvolvimento dedicada ao alcance de requisitos essenciais, sem dispersão de foco pela equipe de projeto, o que reduz os riscos de fracasso por mau planejamento.

Além disso, Rierson (2013) sugere um alinhamento tácito entre o DO-178B e as normas ARP-4754 e ARP-4761, que definem diretrizes para o desenvolvimento de aeronaves e sistemas no meio aeronáutico. Tais normas são apontadas pela Sociedade de Engenheiros Automotivos (*Looking* [...], 2022), responsável por sua edição, como os pilares da segurança da aviação moderna. Como o padrão DO-178C é uma expansão do DO-178B, seu alinhamento com as normas ARP é uma consequência imediata, o que é confirmado por Hilderman (2014).

Nesse sentido, e considerando-se a sua história, o padrão DO-178C constitui-se um conjunto de práticas que, desde a origem, estão de acordo com procedimentos consagrados da indústria aeroespacial, o que se verifica por seu alinhamento tácito com as normas ARP e pela alta adesão conquistada desde a sua primeira versão em 1985.

Dada a criticidade do *software* a ser embarcado em veículos como o VSB-30 e o VS-50, no IAE, seu desenvolvimento demanda processos de engenharia que não apenas assegurem o cumprimento dos requisitos de projeto, mas também a conformidade dos sistemas de *software* destes veículos com os estritos requisitos de segurança do setor aeroespacial.

Isso pode ser conseguido com a implementação pelo IAE das recomendações contidas no DO-178C, que incorporam práticas de desenvolvimento de *software* crítico efetivamente testadas pela indústria, e reconhecidas pelas autoridades certificadoras, assegurando a conformação desses sistemas às normas do setor aeroespacial e reduzindo as chances de fracasso na sua certificação final.

2.2 **A ênfase na comunicação entre as partes envolvidas**

Segundo Rierson (2013), todo *software* é parte da implementação de um sistema mais amplo, cujos requisitos são construídos a partir de necessidades operacionais e outras considerações, dentre as quais aquelas relativas à segurança, segundo a RTCA (2011).

Tais considerações são feitas a partir da avaliação de segurança do sistema como um todo, originando os requisitos que devem ser atribuídos aos demais subsistemas, dentre os quais os de *software*. Esses requisitos podem abranger desde aspectos funcionais e de integridade, até requisitos de confiabilidade e restrições de projeto (RTCA, 2011).

De acordo com Rierson (2013), uma vez que os requisitos estabelecem a comunicação entre os clientes e os desenvolvedores, se mal definidos, dão causa ao desenvolvimento de produtos e sistemas problemáticos, evidenciando uma articulação deficiente entre as partes envolvidas nos projetos. De fato, Lempia e Miller (2009) apontam que erros de requisitos têm maior probabilidade de afetar a segurança de sistemas embarcados do que os erros introduzidos durante as fases de projeto ou de implementação.

Hilderman (2014) defende que o emprego do DO-178C aprimora a clareza sobre os requisitos, ao exigir que sejam completos e detalhados, o que força a busca antecipada por respostas e estimula a discussão para torná-los factíveis, reduzindo as suposições. Isso é confirmado por Rierson (2013), para quem os requisitos de *software* são fundamentais para a conformidade com o padrão DO-178C.

Dessa forma, o desenvolvimento de um *software* embarcado é dirigido pela arquitetura e pelos requisitos dos sistemas que integra, o que exige uma comunicação clara e antecipada entre as partes envolvidas nos projetos. Isso significa que os times técnicos e gerenciais devem interagir desde cedo, a fim de elaborar uma visão clara

do que pretendem desenvolver, permitindo a definição precisa dos requisitos de *software* decorrentes.

É o que acontece no caso dos projetos constantes do Programa Estratégico de Sistemas Espaciais (PESE) da FAB, ou do Programa Espacial Brasileiro, no qual se inserem os veículos suborbitais VSB-30 e VS-50 do IAE, que são de particular interesse para este ensaio.

Nesses veículos, o caráter multidisciplinar dos sistemas se traduz em uma eletrônica embarcada de elevada complexidade, o que se estende ao *software* associado, tornando desafiador o processo de levantamento e definição de requisitos. Com isso, elevam-se os riscos de má compreensão dos objetivos do *software*, e dos critérios operacionais e de segurança relevantes para a sua operação.

A interação e a clareza entre as partes envolvidas num projeto de *software* embarcado são favorecidas pela estrutura focada em objetivos e processos do DO-178C. É o que mostra Rierson (2013), ao afirmar que a conformidade com o padrão e a aprovação da autoridade certificadora requerem a elaboração de planos detalhados pela equipe de desenvolvimento, além de seu estrito cumprimento.

Analisando-se o padrão, verifica-se que a estrutura de trabalho proposta é composta por 6 processos principais: planejamento, desenvolvimento, verificação, gerenciamento de configuração, garantia de qualidade e certificação. Exceto pelo planejamento, cada um desses processos deve dispor de um plano que seja absolutamente coerente com os demais, o que garante a total rastreabilidade entre os requisitos e as escolhas técnicas e gerenciais (RTCA, 2011).

Dessa forma, a incorporação da estrutura de trabalho recomendada no DO-178C assegura que o desenvolvimento do *software* seja conduzido, técnica e gerencialmente, de maneira uniforme e cooperativa entre as partes, com foco na comunicação entre elas, o que é consistente com a natureza multidisciplinar dos projetos dos veículos suborbitais VSB-30 e VS-50 do IAE.

Assim, a ênfase no diálogo para o levantamento de requisitos, e a exigência de um planejamento completo e documentado que permita a plena rastreabilidade deles, são ganhos diretos associados à incorporação do padrão DO-178C pelo IAE, pois suas recomendações impedem suposições e formalizam as decisões, numa sequência lógica e temporal que facilita o trabalho dos times técnicos e favorece o desenvolvimento exitoso do *software* a ser embarcado nos veículos suborbitais do Instituto.

3 **CONCLUSÃO**

O grande protagonismo exercido pelo *software* embarcado desde o início deste século, fruto da intensificação de seu uso em sistemas aeronáuticos a partir de 1980, verifica-se também em sistemas da FAB, com destaque para os veículos suborbitais VSB-30 e VS-50, desenvolvidos no IAE em parceria com a indústria e o DLR.

Esses veículos têm forte dependência de *software* embarcado em seus sistemas de controle, o que gera desafios de conformação aos rigorosos requisitos do setor aeroespacial para a sua certificação final. Sendo o DO-178C um conjunto de recomendações específicas para cada nível de criticidade do sistema subjacente, pautadas em práticas consagradas na indústria de *software* aeroembarcado, sua adoção permite a incorporação de uma filosofia de desenvolvimento eficiente e dedicada ao alcance de tais requisitos.

Além disso, o caráter multidisciplinar dos projetos VSB-30 e VS-50 requer intensa coordenação entre as diferentes partes envolvidas, inclusive aquelas responsáveis pelo *software*. Isso é estimulado pelo DO-178C, por sua ênfase no diálogo formal e antecipado entre os times técnicos e gerenciais, focado no detalhamento exaustivo dos requisitos e em sua rastreabilidade. Dessa forma, sua adoção impede que a má comunicação comprometa o desenvolvimento bem-sucedido do *software* desses veículos.

Por todo o exposto, a incorporação do DO-178C aos processos de desenvolvimento de *software* da Divisão de Eletrônica do IAE proporciona não apenas a redução de riscos em seus projetos, mas também a modernização técnica do setor, alinhando-o com as melhores práticas do meio aeroespacial global.

Tal alinhamento promove ganhos de eficiência nos processos de engenharia de desenvolvimento da FAB e facilita o diálogo com a indústria, o que potencializa a formação de parcerias como a já existente com o DLR. Com a retomada da corrida espacial entre as nações e a contínua redução do orçamento disponível para pesquisa e desenvolvimento na FAB, a potencialização dessas parcerias revela-se fundamental, por disponibilizar formas alternativas de financiamento para projetos importantes do PESE e do Programa Espacial Brasileiro. Portanto, a incorporação do DO-178C representa uma oportunidade de expansão da capacidade do Brasil de desenvolver soluções científico-tecnológicas no campo do Poder Aeroespacial que lhe permitam consolidar a sua Soberania no espaço exterior.

REFERÊNCIAS

DANIELS, D. Thoughts from the DO-178C committee. *In*: IET INTERNATIONAL CONFERENCE ON SYSTEM SAFETY**,** 6., 2011, Birmingham. **Proceedings** […] Stevenage: IET, 2011.

DAW, Z. *et al*. AACE: Automated assurance case environment for aerospace certification. *In*: IEEE/AIAA DIGITAL AVIONICS SYSTEMS CONFERENCE (DASC), 42., 2023, Barcelona. **Proceedings** […] Piscataway: IEEE, 2023. p. 1-10.

UNITED STATES OF AMERICA. U.S. Department of Transportation. Federal Aviation Administration. **Order 8110.49A: Software Approval Guidelines**. Washington, D.C.: U.S. Department of Transportation, 29 mar. 2018. Disponível em: https://www.faa.gov/regulations_policies/orders_notices/index.cfm/go/document.information/documentid/1032976. Acesso em: 11 mar. 2024.

HANSSEN, G.; WEDZINGA, G.; STUIPA, M. An assessment of avionics software development practice: Justifications for an agile development process. *In*: INTERNATIONAL CONFERENCE ON AGILE PROCESSES IN SOFTWARE ENGINEERING AND EXTREME PROGRAMMING, 18., 2017, Cologne. **Proceedings** […] Berlin: Springer International Publishing, 2017. p. 217-231.

HERMANN, D. **Sofware Safety and Reliability: Techniques, Approaches, and Standards of Key Industrial Sectors**. 1. ed. Hoboken: Wiley - IEEE Computer Society, 2000.

HILDERMAN, V. Understanding DO-178C software certification: Benefits versus costs. *In*: IEEE INTERNATIONAL SYMPOSIUM ON SOFTWARE RELIABILITY ENGINEERING WORKSHOPS, 2014, Naples. **Proceedings** […] Piscataway: IEEE, 2014. p. 114-114.

HOLLOWAY, C. Michael. Towards understanding the DO-178C/ED-12C assurance case. *In*: IET INTERNATIONAL CONFERENCE ON SYSTEM SAFETY, INCORPORATING THE CYBER SECURITY CONFERENCE, 7., 2012, Edinburgh. **Proceedings** […] Stevenage: IET, 2012. p. 1-6.

LEMPIA, D. L.; MILLER, S. P. **Requirements engineering management findings report**. Cedar Rapids: Federal Aviation Administration, 2009.

RIERSON, L. **Developing safety-critical software: a practical guide for aviation software and DO-178C compliance**. 1. ed. Boca Raton: CRC Press, 2013.

RADIO TECHNICAL COMMISSION FOR AERONAUTICS. **RTCA DO-178C:** Software Considerations in Airborne Systems and Equipment Certification. Washington, D.C.: RTCA, 2011.

LOOKING at ARP4754 & ARP4761: A Case Study for The Twin Pillars of Aviation Safety. **Blog da Sociedade de Engenheiros Automotivos**, 2022. Disponível em: https://www.sae.org/blog/twin-pillars-case-study. Acesso em: 14 mar. 2024.