UNIVERSIDADE DE SÃO PAULO
ESCOLA DE ENGENHARIA DE SÃO CARLOS

MATHEUS MACEDO

Título: Analise do acidente do avião N600XL sobre falha do transponder e estudo de caso sobre aplicação de ARP4754 e consequências

São Carlos
2025

MATHEUS MACEDO

Título: Analise do acidente do avião N600XL sobre falha do transponder e estudo de caso sobre aplicação de ARP4754 e consequências

Monografia apresentada ao Curso de Especialização em Sistemas Aeronáuticos da Escola de Engenharia de São Carlos da Universidade de São Paulo, como parte dos requisitos para obtenção do título de Especialista em Sistemas Aeronáuticos.

Orientador: Prof. Dr. Mateus Moreira de Souza

São Carlos

2025

Autorizo a reprodução e divulgação total ou parcial deste trabalho, por qualquer meio convencional ou eletrônico, para fins de estudo e pesquisa, desde que citada a fonte.

Ficha catalográfica elaborada pela Biblioteca Prof. Sérgio Rodrigues Fontes
e pelo Serviço de Comunicação e Marketing da EESC-USP,
com dados inseridos pelo(a) autor(a).

M134a

Macedo, Matheus

Analise do acidente do avião N600XL sobre falha do transponder e estudo de caso sobre aplicação de ARP4754 e consequências / Matheus Macedo ; orientador Mateus Souza. -- São Carlos, 2026.

48 p.

Trabalho de Conclusão de Curso - Especialização em Sistemas Aeronáuticos -- Escola de Engenharia de São Carlos da Universidade de São Paulo, 2026.

1. ARP4754. 2. Requisito FAR 25.1309. 3. Transponder (TCAS). 4. Desenvolvimento de Produto. 5. Desenvolvimento de Sistemas. I. Souza, Mateus, orient. II. Título.

Responsáveis pela estrutura de catalogação da publicação segundo a AACR2: Bibliotecários da EESC/USP.

FOLHA DE AVALIAÇÃO OU APROVAÇÃO

EESC · USP
Escola de Engenharia de São Carlos
Departamento de Engenharia Aeronáutica

ENGENHARIA AERONÁUTICA

FOLHA DE APROVAÇÃO

Candidato(a): **Matheus Macedo**

Título do Trabalho: **Analise do acidente do avião N600XL sobre falha do transponder e estudo de caso sobre aplicação de ARP4754 e consequências**

Data da defesa: **10/12/2025**

Comissão julgadora

Avaliador	Resultado (nota)
Mateus Moreira de Souza (orientador)	8,5
Jorge Henrique Bidinotto	8,5

Resultado final: **Aprovado**

Coordenador do Curso de Especialização em Sistemas Aeronáuticos
Prof. Associado **Jorge Henrique Bidinotto**

Vice-coordenador do Curso de Especialização em Sistemas Aeronáuticos
Prof. Associado **Hernán Darío Cerón Muñoz**

tel.: + 55 (16) 3373-9430
sistemasaeronauticos@eesc.usp.br – www.sistemasaeronauticos.eesc.usp.br

USP Universidade de São Paulo

AGRADECIMENTOS

Gostaria de agradecer inicialmente a Deus pela oportunidade e por me dar forças para mais essa etapa, agradecer a minha família e amigos por todo o apoio cotidiano e por sempre me incentivarem e acreditarem em mim mesmo quando eu mesmo não acredito.

Ao Prof. Dr. Jorge Henrique Bidinotto que contribuiu através da coordenação do Curso e lecionando de maneira magistral de forma a inspirar e contribui significativamente para meu conhecimento e crescimento acadêmico e profissional.

Ao Prof. Dr. Mateus Moreira de Souza, que muito me ensinou contribuindo para o meu crescimento através de sua orientação e paciência no desenvolvimento desse trabalho.

A USP de São Carlos bem como todos os seus professores e colaboradores que por meio dessa especialização me permitiram ter uma experiencia extremamente enriquecedora.

“A mente que se abre a uma nova ideia
jamais voltará ao seu tamanho original.”
(Albert Einstein)

RESUMO

MACEDO, M. **Analise do acidente do avião N600XL sobre falha do transponder e estudo de caso sobre aplicação de ARP4754 e consequências**. 2024. Monografia (Trabalho de Conclusão de Curso) – Escola de Engenharia de São Carlos, Universidade de São Paulo, São Carlos, 2025.

O objetivo desse trabalho foi desenvolver uma análise documental voltada para o desenvolvimento de produto, onde foi utilizado um caso bastante conhecido, o acidente do avião N600XL e as falhas no transponder que contribuíram para o evento. O componente do transponder foi analisado utilizando alguns documentos de base onde os principais foram a ARP4754 e o requisito FAR 25.1309 voltando-se principalmente para os processos contidos na ARP4754 para o desenvolvimento de produto e além disso foi analisado o impacto que teria no desenvolvimento do componente de o nível de garantia de desenvolvimento fosse alterado de Major para Hazardous, ou seja se o nível de criticidade fosse maior, quais seriam os impactos de desenvolvimento, onde os principais pontos afetados seriam relacionados ao desenvolvimento de hardware, software, além de sistemas de segurança atrelados ao componente que seriam necessários para o devido funcionamento de um componente de tal nível de criticidade. Por fim a conclusão da análise foi de que de fato o sistema caso fosse de um nível de criticidade mais elevado não seria susceptível a tal falha, dados os níveis de segurança exigidos para o nível analisado, entretanto é impossível chegar à conclusão de impacto de acidente uma vez que o estudo foi todo baseado no componente isolado e de acordo com o CENIPA a falha de operação no TCAS foi um dos eventos dentre muitos para a catástrofe do acidente.

Palavras-chave: b

ABSTRACT

MACEDO, M. **analysis of the PP-ZEZ aircraft accident regarding engine failure and case study on the application of ARP4754 and its consequences**: subtitle. 2024. Monografia (Trabalho de Conclusão de Curso) – Escola de Engenharia de São Carlos, Universidade de São Paulo, São Carlos, 2025.

The purpose of this study was to conduct a documentary analysis focused on product development, using a well-known case: the accident involving the N600XL aircraft and the transponder failures that contributed to the event. The transponder component was examined through reference documents, primarily ARP4754 and the FAR 25.1309 requirement, with emphasis on the processes outlined in ARP4754 for product development. Furthermore, the study assessed the potential impact on the component's development if the Development Assurance Level (DAL) were changed from Major to Hazardous. In other words, if the level of criticality were higher, what would be the implications for development? The main areas affected would include hardware and software design, as well as safety systems associated with the component, which would be required to ensure the proper functioning of a product with such a level of criticality. The analysis concluded that, indeed, if the system had been assigned a higher DAL, it would not have been susceptible to such a failure, given the safety requirements imposed at that level. However, it is not possible to determine the accident's overall impact, since the study was based solely on the isolated component. According to CENIPA, the operational failure of the TCAS was only one among several contributing factors to the catastrophe.

Keywords: ARP4754. FAR 25.1309 Requirement. Transponder (TCAS). Product Development.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ANAC	Agencia Nacional de Aviação Civil
ARP	Aerospace Recommended Pratice
ATC	Air Traffic Control
CENIPA	Centro de Investigação e Prevenção de Acidentes Aeronáuticos
CS	Certification Specifications
DAL	Development Assurance Level
DC	Decision Coverage
EASA	European Union Aviation Safety Agency
EGPWS	Enhanced Ground Proximity Warning System
ERJ	Embraer Regional Jet
FAA	Federal Aviation Administration
FAR	Federal Aviation Regulations
FHA	Functional Hazard Assessment
FMS	Flight Management System
HMI	Human-Machine Interface
MC	Modified Condition
NTSB	National Transportation Safety Board
OACI	Organização de Aviação Civil Internacional
PSAC	Plan for Software Aspects of Certification
PSSA	Preliminary System Safety Assessment
RA	Resolution Advisories
RTCA	Radio Technical Commission for Aeronautics
RVSM	Reduced Vertical Separation Minimum
SAE	Society of Automotive Engineers
SIPAER	Sistema de Investigação e Prevenção de Acidentes Aeronáuticos
SSA	System Safety Assessment
TCAS	Traffic Collision Avoidance System

Sumário

1 INTRODUÇÃO

A aviação é uma das indústrias mais rigorosamente regulamentadas e monitoradas do mundo, onde a segurança é a prioridade máxima. No entanto, acidentes aéreos, embora raros, ainda ocorrem e podem ter consequências devastadoras. Um exemplo notável é o acidente do avião X600XL, que levantou questões críticas sobre a confiabilidade dos transponders e a eficácia dos processos de operação, certificação e análise de risco. Este trabalho tem como objetivo analisar pontos de funcionamento do transponder junto com fatores humanos, que levaram ao acidente, bem como explorar a aplicação da norma ARP4754, que fornece diretrizes para o desenvolvimento de sistemas de aviação seguros e confiáveis. Através de uma análise detalhada, buscaremos entender as lições aprendidas e as implicações para a indústria da aviação, destacando a importância de uma abordagem sistemática na gestão de riscos e na garantia da segurança operacional.

2 REVISÃO BIBLIOGRÁFICA

2.1 CENIPA

O Centro de Investigação e Prevenção de Acidentes Aeronáuticos (CENIPA), órgão subordinado ao Comando da Aeronáutica, é a principal instituição brasileira responsável pela condução de investigações de ocorrências aeronáuticas civis e militares, com foco na prevenção de novos acidentes. Criado em 1982, o CENIPA atua de forma independente dos processos jurídicos ou punitivos, seguindo o princípio estabelecido pela Organização de Aviação Civil Internacional (OACI) de que a finalidade primária da investigação de acidentes é a prevenção, e não a atribuição de culpa.

Sua relevância na indústria aeronáutica nacional é expressiva, pois fornece dados essenciais para o aprimoramento contínuo da segurança operacional. Por meio de uma metodologia sistemática e baseada em evidências, o CENIPA conduz investigações técnicas que visam identificar os fatores contribuintes para as ocorrências, analisando aspectos humanos, operacionais, organizacionais, ambientais e técnicos.

Além das investigações em si, o CENIPA desempenha um papel central na formulação de recomendações de segurança, que são posteriormente encaminhadas a operadores aéreos,

fabricantes, órgãos reguladores e outras partes interessadas. Essas recomendações têm caráter proativo e visam a mitigação de riscos sistêmicos, contribuindo diretamente para a elevação dos níveis de segurança da aviação brasileira.

Outro aspecto relevante é a manutenção e o uso do Sistema de Investigação e Prevenção de Acidentes Aeronáuticos (SIPAER), uma estrutura institucional que promove a coleta, o tratamento e a disseminação de informações relacionadas à segurança de voo. Por meio do SIPAER, o CENIPA também promove treinamentos, publicações técnicas, campanhas educativas e programas de notificação voluntária de ocorrências, reforçando a cultura de segurança em todos os níveis da aviação.

2.2 CONTEXTUALIZAÇÂO

O acidente envolvendo a aeronave executiva Embraer Legacy 600, de prefixo N600XL, ocorrido em 29 de setembro de 2006, é considerado um dos eventos mais marcantes da história da aviação brasileira contemporânea. Segundo o CENIPA, 2020 no relatório do acidente o jato executivo, recém-saído da fábrica da Embraer em São José dos Campos, colidiu em pleno voo com um Boeing 737-800 da Gol Linhas Aéreas, voo 1907, que realizava a rota Manaus–Brasília–Rio de Janeiro.

A colisão ocorreu a cerca de 37.000 pés de altitude (FL370), na região de Mato Grosso, resultando na destruição total do Boeing e na morte dos 154 ocupantes a bordo. Já o Legacy, apesar dos danos estruturais significativos, conseguiu realizar um pouso de emergência na base aérea da Serra do Cachimbo, com todos os sete ocupantes ilesos.

Figura 1:Winglet N600XL danificado pós acidente

Figura 2: Profundor N600XL danificado pós acidente

Do ponto de vista técnico e investigativo, o acidente revelou falhas múltiplas de natureza sistêmica, envolvendo aspectos de gestão do tráfego aéreo, comunicação entre controladores e pilotos, e configuração inadequada dos sistemas de bordo, como o transponder e o TCAS (Traffic Collision Avoidance System), que ficaram inoperantes durante parte do voo. A investigação conduzida pelo CENIPA, em colaboração com o NTSB dos Estados Unidos, apontou que a interrupção inadvertida do transponder do Legacy impediu a detecção mútua das aeronaves pelo TCAS, o que poderia ter evitado a colisão.

O evento gerou grande repercussão internacional e destacou fragilidades nos procedimentos de controle de tráfego aéreo da época, além de levantar discussões sobre a responsabilidade compartilhada entre pilotos e controladores. Também impulsionou uma série de mudanças operacionais, incluindo melhorias nos protocolos de separação vertical e revisão dos sistemas de vigilância e comunicação na região amazônica.

Em termos acadêmicos e técnicos, o acidente do N600XL é amplamente utilizado como estudo de caso em segurança de voo, análise de risco operacional e interação homem-sistema. Ele evidencia a importância da aplicação rigorosa de práticas como as previstas na ARP4754A (para desenvolvimento seguro de sistemas aeronáuticos) e nos processos do SIPAER, que visam à identificação de falhas latentes e ao fortalecimento da cultura de segurança na aviação. [Centro de Investigação e Prevenção de Acidentes Aeronáuticos (2010)]

2.3 AERONAVE LEGACY 600

A aeronave envolvida no acidente era um Embraer Legacy 600, modelo de jato executivo derivado da plataforma regional ERJ-145, fabricado pela Embraer – Empresa Brasileira de Aeronáutica S.A.. Projetado para o mercado de aviação executiva de médio porte, o Legacy 600 possui alcance intercontinental, com capacidade para transportar até 13

passageiros em configuração de alta densidade. É equipado com dois motores turbofan Rolls-Royce AE 3007, sistema aviônico integrado e cockpit com arquitetura baseada em displays digitais (glass cockpit). A aeronave é certificada para operações em espaço aéreo controlado, com sistemas embarcados como TCAS II, EGPWS, FMS e transponder modo S. Sua robustez, confiabilidade e flexibilidade operacional tornaram o modelo uma escolha popular no segmento executivo desde seu lançamento, no início dos anos 2000.

2.4 O SISTEMA TCAS E A INTEGRAÇÃO DE SISTEMAS NA PREVENÇÃO DE COLISÕES

O TCAS (Traffic Collision Avoidance System) é um dos principais sistemas embarcados dedicados à prevenção de colisões entre aeronaves em voo. Sua função é monitorar o espaço aéreo ao redor da aeronave, detectando transponders ativos de outras aeronaves equipadas com sistema similar, com base em sinais de rádio secundário (modo S ou C). A partir dessas informações, o TCAS avalia possíveis trajetórias de conflito e, em caso de risco de colisão, emite alertas visuais e sonoros ao piloto, podendo inclusive sugerir manobras evasivas verticais — como subir ou descer — conhecidas como RA (Resolution Advisories). É importante ressaltar que o TCAS é considerado um radar secundário por conta de não emitir nenhuma onda de rádio e trabalhar baseando-se nas ondas emitidas pelos transponders de aeronaves próximas. Quando falamos em um radar primário esse por sua vez já emite a própria onda de rádio e trabalha com a detecção e análise do reflexo das ondas emitidas. [NOLAN, M. S (2010)].

Embora o TCAS opere de forma autônoma e independente do controle de tráfego aéreo, sua atuação está integrada ao ambiente cooperativo de vigilância. Quando uma manobra RA é executada, os pilotos devem informar imediatamente à torre de controle (ATC) sobre a ação tomada, permitindo que os controladores ajustem as separações e monitorem o tráfego envolvido. Essa comunicação é essencial para manter a consciência situacional do ATC e evitar instruções conflitantes.

Além disso, o funcionamento eficaz do TCAS depende da correta operação dos transponders das aeronaves próximas, cuja configuração e monitoramento são supervisionados pelas torres. Em situações de conflito entre comandos do TCAS e instruções do ATC, os procedimentos internacionais determinam que os comandos do TCAS têm prioridade, reforçando seu papel como última barreira contra colisões em voo.

Essa interação entre o TCAS e as torres de controle evidencia a importância da coordenação entre sistemas embarcados e infraestrutura terrestre para garantir a segurança operacional em ambientes de tráfego aéreo intenso.

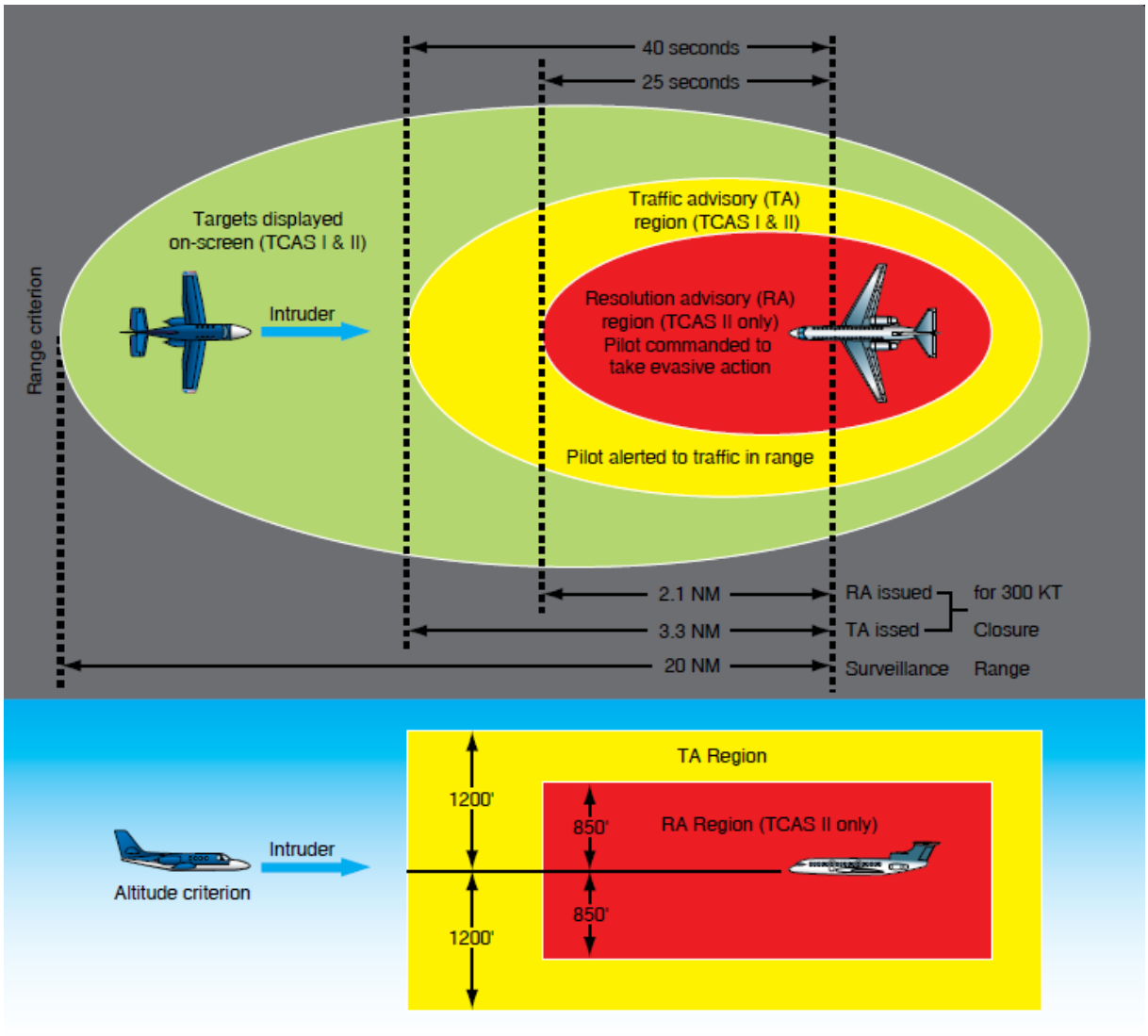

Figura 3: Interação TCAS recebendo informações de outras aeronaves

No contexto do acidente do Legacy N600XL, a falha crítica ocorreu justamente na inoperância do transponder, que impossibilitou a troca de sinais entre os dois sistemas TCAS — tanto da aeronave executiva quanto do Boeing 737 da Gol. Como consequência, nenhuma das tripulações recebeu alertas de tráfego ou comandos de evasão, impedindo qualquer tentativa de evitar a colisão.

Essa ocorrência evidencia a importância da integração segura e confiável entre sistemas aeronáuticos. O TCAS, embora seja um sistema independente no ponto de vista funcional,

depende de uma interligação eficiente com outros sistemas embarcados, como o transponder, sistema elétrico, interface de cockpit e navegação. Além disso, depende também da correta interação com sistemas externos, como o radar secundário dos órgãos de controle de tráfego aéreo (ATC).

Nesse sentido, a ARP4754A oferece uma abordagem estruturada para garantir que sistemas complexos como o TCAS sejam integrados ao projeto da aeronave de maneira segura, por meio da definição de requisitos, análise de funções críticas, rastreabilidade de falhas e testes de integração. Também está relacionada à ARP4761, que trata especificamente da análise de segurança e confiabilidade.

No caso do N600XL, a investigação identificou falhas tanto no projeto de interface homem-máquina (a tripulação não percebeu que o transponder estava desligado), quanto na comunicação com os sistemas de solo, revelando lacunas de integração entre homem, máquina e ambiente operacional. Tais falhas são típicas de sistemas sociotécnicos complexos e exigem, no desenvolvimento de aeronaves modernas, uma abordagem multidisciplinar que considere aspectos técnicos, humanos e organizacionais.

A integração entre sistemas não se limita ao funcionamento isolado de equipamentos, mas deve considerar o comportamento do sistema como um todo, incluindo eventos em cascata, dependências críticas, e a resposta do operador humano frente a diferentes modos de falha.

2.5 REQUISITO 25.1309 E SUA RELEVÂNCIA NO DESENVOLVIMENTO DE SISTEMAS AERONÁUTICOS

O requisito 25.1309 faz parte do regulamento FAR 25 (Federal Aviation Regulations, Parte 25), emitido pela FAA (Federal Aviation Administration), e encontra correspondência na CS-25 (Certification Specifications) da EASA. Ele é considerado um dos mais fundamentais no campo da certificação de sistemas aeronáuticos, pois estabelece os critérios gerais de segurança e confiabilidade operacional que os sistemas embarcados devem atender ao longo de todas as fases de voo.

O requisito 25.1309 (disponível no apêndice 1) estabelece os seguintes tópicos para equipamentos, sistemas e instalações:

De forma resumida, o §25.1309 determina que:

Os sistemas e equipamentos da aeronave devem ser projetados de forma que nenhuma falha isolada, nem qualquer combinação razoavelmente provável de falhas, resulte em uma condição catastrófica para a aeronave e seus ocupantes.”

O parágrafo também exige que:

- As falhas sejam analisadas sistematicamente;
- A probabilidade de falhas perigosas seja extremamente remota (10^{-9} por hora de voo para condições catastróficas);
- A função dos sistemas críticos seja mantida mesmo em caso de falhas parciais;
- E que exista mitigação suficiente para falhas previsíveis de natureza técnica, humana ou operacional.

No caso do acidente do Legacy 600 (N600XL), o requisito pode ser diretamente relacionado às condições que levaram à insuficiência de mitigação de falhas críticas envolvendo o sistema de prevenção de colisões (TCAS) e o transponder. A desativação inadvertida do transponder pela tripulação, sem qualquer alerta explícito ou redundância funcional perceptível, resultou na condição em que a aeronave se tornou "invisível" tanto para os sistemas TCAS das demais aeronaves quanto para o radar secundário do controle de tráfego aéreo.

À luz do FAR 25.1309, observa-se que o design do sistema estava em conformidade com o nível de segurança correspondente ao seu Development Assurance Level (DAL). Entretanto, a ocorrência da falha deve ser entendida como consequência da combinação entre o nível de criticidade atribuído ao equipamento e fatores operacionais externos. A interface homem-máquina, por exemplo, não forneceu feedback suficiente à tripulação sobre o status real do transponder, o que reduziu a capacidade de detecção e correção da falha. Assim, não se trata de um projeto intrinsecamente inseguro, mas de uma condição de falha emergente diante da interação entre o design, o nível de garantia estabelecido e circunstâncias adicionais que contribuíram para o evento.

Outro ponto é a falta de arquitetura redundante ou lógica de supervisão que garantisse a reativação automática do transponder em caso de desligamento não intencional — uma exigência implícita do §25.1309 para sistemas cuja falha pode resultar em uma condição catastrófica, como foi o caso.

Por fim, cabe destacar que o 25.1309 não atua isoladamente. Ele é suportado por normas como a ARP4754A e ARP4761, que orientam como os requisitos de segurança devem ser identificados, analisados e rastreados ao longo do desenvolvimento. O não atendimento adequado a esses requisitos e métodos, como se evidenciou no acidente, resulta em lacunas críticas de segurança e em falhas sistêmicas com potencial para causar eventos de grande magnitude.

2.6 ARP4754

A recomendação prática ARP4754A, emitida pela SAE International, estabelece diretrizes para o desenvolvimento seguro de sistemas aeronáuticos complexos, com foco na integração entre hardware, software, operadores humanos e seus ambientes operacionais. Ao enfatizar uma abordagem baseada em requisitos, análise funcional e segurança sistêmica, a norma busca garantir que os sistemas embarcados cumpram seus objetivos operacionais sob todas as condições previsíveis, inclusive em cenários de falhas.

No contexto do acidente envolvendo o Embraer Legacy 600 (N600XL), diversos aspectos da ARP4754A podem ser associados às falhas latentes de projeto e integração que contribuíram para o evento. Um dos principais pontos foi a inoperância do transponder, que resultou na desativação do TCAS e, por consequência, na ausência de alertas de tráfego e de manobras evasivas. Embora não tenha havido uma falha física do sistema, a investigação indicou que o transponder foi desligado inadvertidamente pela tripulação, possivelmente devido à interface de cockpit e à ausência de alertas explícitos sobre sua condição operacional.

De acordo com os princípios da ARP4754A, esse tipo de falha deveria ter sido identificado e mitigado durante a fase de Análise Funcional de Segurança (Functional Hazard Assessment – FHA), e tratado com maior rigor nas fases subsequentes de requisitos, design e testes de integração. A norma prevê que sistemas cuja falha possa contribuir para eventos catastróficos (como perda de separação de tráfego e colisão em voo) devem ser classificados com nível crítico, exigindo alto rigor em termos de redundância, validação de requisitos e proteção contra falhas humanas previsíveis.

Além disso, a falta de feedback visual ou sonoro adequado no cockpit sobre o estado do transponder é um indicativo de falha de projeto na interface homem-máquina (HMI) — outro ponto abordado pela ARP4754A, que exige que os requisitos de interação com o operador sejam claramente especificados, verificados e validados em condições realistas. A norma enfatiza que os operadores devem ser capazes de monitorar o estado do sistema de forma confiável e intuitiva, especialmente para funções críticas à segurança.

Outro aspecto relevante é a interação entre o TCAS e os sistemas de navegação e comunicação, cuja integração deficiente contribuiu para o isolamento da aeronave em uma região com cobertura limitada de radar e controle. A ARP4754A destaca que a integração entre sistemas deve considerar os modos de falha combinados e seu impacto na missão da aeronave, incluindo possíveis respostas incorretas do operador ou falhas em detectar condições anômalas.

Portanto, a aplicação mais rigorosa da ARP4754A poderia ter levado a um projeto mais resiliente à falha humana e a uma cadeia de eventos menos vulnerável a interrupções não intencionais de sistemas críticos. Esse caso realça a importância de se adotar uma abordagem sistêmica e estruturada no desenvolvimento de aeronaves, onde os riscos operacionais são tratados desde a concepção, e não apenas corrigidos reativamente após eventos trágicos.

2.7 DO-178

A DO-178, atualmente em sua versão mais utilizada DO-178C, é uma norma publicada pela RTCA (Radio Technical Commission for Aeronautics) que estabelece os requisitos para o desenvolvimento de software embarcado em sistemas aeronáuticos. Seu objetivo principal é garantir que o software crítico à segurança de voo seja desenvolvido, verificado e validado de forma sistemática, rastreável e conforme os níveis de integridade exigidos pela certificação aeronáutica.

A norma é adotada por autoridades reguladoras como FAA (Federal Aviation Administration) e EASA (European Union Aviation Safety Agency), sendo considerada um dos pilares para a certificação de sistemas embarcados em aeronaves civis.

Durante o desenvolvimento de software sob a DO-178C, os principais pontos de atenção incluem:

Níveis de Design Assurance (DAL): O software é classificado em cinco níveis (A a E), conforme o impacto potencial de uma falha. O nível A, por exemplo, é atribuído a funções cuja falha pode causar um acidente catastrófico, exigindo o mais alto rigor de desenvolvimento e verificação.

Planejamento do Ciclo de Vida: A norma exige a elaboração de planos formais como o Plan for Software Aspects of Certification (PSAC), Software Development Plan (SDP), Software Verification Plan (SVP), entre outros, que definem como o projeto será conduzido e auditado.

Requisitos e Rastreabilidade: A DO-178C enfatiza a definição clara de requisitos de alto e baixo nível, bem como a rastreabilidade bidirecional entre requisitos, código fonte e testes, garantindo que cada funcionalidade seja devidamente implementada e verificada.

Verificação e Validação: A norma exige atividades rigorosas de verificação, incluindo análise estática, revisão de código, testes estruturais e funcionais. Para níveis mais críticos (A e B), são requeridos critérios como cobertura de decisão e condição múltipla.

Independência nas Atividades de Verificação: Para os níveis mais altos, é necessário que as atividades de verificação sejam realizadas por equipes independentes daquelas que desenvolveram o software, assegurando imparcialidade na avaliação.

Suporte de Ferramentas e Suplementos Técnicos: A DO-178C introduziu suplementos como DO-330 (qualificação de ferramentas), DO-331 (model-based development), DO-332 (object-oriented technology) e DO-333 (formal methods), que ampliam a aplicabilidade da norma a abordagens modernas de engenharia de software.

A aplicação da DO-178C é essencial para garantir a confiabilidade, segurança e conformidade regulatória de sistemas embarcados em aeronaves, sendo um componente crítico no processo de certificação de software aeronáutico.

3 ANALISE DOCUMENTAL

O Traffic Collision Avoidance System (TCAS) é um sistema embarcado de vigilância ativa que auxilia os pilotos na prevenção de colisões em voo, emitindo alertas de tráfego e resoluções de manobra com base em sinais transponder de aeronaves próximas [Federal Aviation Administration. (2018)]. Embora seja um componente crítico para a consciência situacional, o TCAS não é classificado como um sistema catastrófico segundo os critérios de avaliação de falhas definidos pelas autoridades certificadoras.

Classificação de Falhas segundo FAR/CS 25.1309

De acordo com o regulamento FAR/CS 25.1309 [Veja apêndice 1], as falhas de sistemas são categorizadas em quatro níveis principais:

- Catastrófica: resulta em perda da aeronave ou fatalidades.
- Perigosa (Hazardous): causa ferimentos graves ou perda significativa de controle.
- Maior (Major): afeta a operação, mas com impacto gerenciável.
- Menor/Latente: impacto limitado ou não perceptível.

Para cada tipo de falha descrita no regulamento a descrição não é feita de maneira quantitativa, por essa razão o próprio órgão regulador criou uma AC que é para ser usada como um guia no cumprimento desse requisito (AC 25.1309 [Veja apêndice 1]). Nesse guia em questão é indicado o uso da ARP4754[SAE INTERNATIONAL (2010)] como guia para o

desenvolvimento de sistemas, cumprindo os itens desse regulamento no que diz respeito a classificação de Severidade.

Segundo a ARP4754A [SAE INTERNATIONAL (2010)], cinco níveis de severidade para condições de falha, que orientam o processo de desenvolvimento e verificação:

1. **Catastrophic (Catastrófico)**
    - Impacto: Pode resultar em perda da aeronave ou morte de seus ocupantes.
    - Exemplo: Falha total do sistema de controle de voo em condições críticas.
    - Probabilidade de falha: 10^-9
2. **Hazardous (Perigoso)**
    - Impacto: Pode causar ferimentos graves ou fatais a um número significativo de ocupantes; pode comprometer seriamente a segurança da aeronave.
    - Exemplo: Mau funcionamento do sistema de navegação que leva a uma rota incorreta em espaço aéreo restrito.
    - Probabilidade de falha: 10^-7
3. **Major (Importante)**
    - Impacto: Pode causar ferimentos a alguns ocupantes, redução significativa na segurança ou aumento da carga de trabalho da tripulação.
    - Probabilidade de falha: 10^-5
    - Exemplo: Falha parcial de um sistema de comunicação que exige procedimentos alternativos.
4. **Minor (Menor)**
    - Impacto: Pequeno efeito na segurança, possível aumento leve na carga de trabalho da tripulação ou inconveniência.
    - Exemplo: Falha de um sistema de entretenimento de bordo.
5. **No Safety Effect (Sem Efeito na Segurança)**
    - Impacto: Nenhum impacto na segurança da aeronave ou dos ocupantes.
    - Exemplo: Erro estético em uma interface de usuário que não afeta a operação.

Com base nessa classificação, o TCAS é normalmente considerado como tendo condições de falha do tipo Major ou Hazardous, dependendo do cenário operacional. Por exemplo:

- Uma falha total do TCAS em espaço aéreo de baixa densidade pode ser considerada Major, pois a separação visual e o ATC ainda são eficazes.
- Em áreas de tráfego intenso ou em operações RVSM, a falha pode ser Hazardous, devido à perda de uma camada crítica de proteção contra colisões.

Justificativas para a Classificação Não Catastrófica

- Sistema de apoio, não primário: O TCAS complementa a separação de tráfego gerenciada por controle de tráfego aéreo (ATC) e vigilância visual dos pilotos. Sua falha não implica perda de controle da aeronave. [UNITED STATES. Federal Aviation Administration (2023)]
- Redundância operacional: Em caso de falha do TCAS, os procedimentos de separação visual e comunicação com o ATC permanecem ativos e eficazes.
- Falha não resulta em evento imediato: A ausência de alertas TCAS pode aumentar o risco de proximidade, mas não gera uma condição de falha catastrófica por si só.

Implicações para Certificação

Durante o processo de certificação, o TCAS é avaliado quanto à sua confiabilidade, integridade de dados, e capacidade de alertar corretamente. No entanto, não é exigido que o sistema tenha tolerância a falhas múltiplas com probabilidade extremamente remota, como seria o caso de sistemas classificados como catastróficos (ex.: controle de voo, geração elétrica primária). [SAE INTERNATIONAL (2010)]

Além disso, os requisitos de manutenção para o TCAS são definidos com base em sua criticidade operacional, mas não exigem inclusão em limitações de aeronavegabilidade (ALS), a menos que estejam vinculados a outros sistemas críticos.

A Design Assurance Level (DAL) é atribuída com base na severidade da condição de falha associada ao sistema. Quanto maior o impacto na segurança, mais rigoroso é o processo de desenvolvimento, verificação e validação.

A tabela abaixo apresenta uma matriz proposta e desenvolvidaa de DAL para o TCAS, considerando diferentes cenários operacionais e classificações de falha:

Sistema/Função	Condição de falha	Severidade (ARP4754)	DAL (DO-178/DO-254)	Justificativa
TCAS (modo TA/RA ativo)	falha total em espaço aéreo de alta densidade	Hazardous/Severe-Major	DAL B	Perda de resolução de conflito pode levar a risco elevado de colisão
TCAS (modo TA/RA ativo)	falha total em espaço aéreo de baixa densidade	Major	DAL C	Impacto operacional gerenciavel, sem risco imediato
TCAS (modo TA apenas)	Perda de alerta de trafego	Major	DAL C	Redução da consciencia situacional, mas sem resolução automática
TCAS (modo standby ou inoperante)	Falha latente ou prolongada	Major	DAL D	Perda de resolução de conflito pode levar a risco elevado de colisão
Interfaçe TCAS com FMS ou EFIS	Dados incorretos ou ausentes	Major	DAL C	Pode afetar a apresentação de dados ou comandos

Figura 4: Matriz DAL para TCAS

A tabela apresentada foi desenvolvida com o intuito de demonstrar as principais condições de falha do TCAS com suas respectivas severidades baseadas na ARP 4754 e DO-178 e DO-254 e demonstrando suas justificativas para cada uma das severidades no que tipicamente é considerado para o TCAS.

Impacto da DAL na Certificação

- DAL B exige verificação rigorosa, incluindo análise de cobertura estrutural, testes de integração e independência na verificação.
- DAL C ainda requer testes robustos, mas com menor exigência de independência e cobertura.
- DAL D permite processos simplificados, com foco em testes funcionais.

De acordo com a ARP4754A, a severidade Catastrophic implica que uma falha no sistema pode levar à perda da aeronave e de vidas humanas. Embora o TCAS seja um sistema crítico para evitar colisões, ele normalmente é classificado como Hazardous ou Major, pois sua

falha não necessariamente leva à perda imediata da aeronave — os pilotos ainda podem tomar ações visuais ou baseadas em controle de tráfego.

Com o sistema considerado Catastrophic, os impactos seriam:

- DAL A (Design Assurance Level A): O software do TCAS teria que ser desenvolvido com o nível mais alto de integridade segundo a DO-178C. Isso inclui:
- Cobertura de código 100% (MC/DC – Modified Condition/Decision Coverage)
- Revisões formais de requisitos, design e código
- Testes de verificação independentes e rastreabilidade completa
- Processos de Engenharia de Sistemas mais rigorosos:
- Análises de segurança como FHA, PSSA e SSA teriam que demonstrar que o sistema não contribui para falhas catastróficas.
- Requisitos de redundância e tolerância a falhas seriam mandatórios.
- Hardware com DAL A (DO-254):
- O hardware embarcado (como processadores e sensores) teria que seguir processos de desenvolvimento e verificação equivalentes ao software.
- Verificação independente e certificação mais complexa:
- A autoridade certificadora (como FAA, EASA ou ANAC) exigiria evidências robustas de que o sistema não falha de forma catastrófica.

Impactos operacionais e econômicos

- Aumento de custo e tempo de desenvolvimento: Projetar com DAL A pode multiplicar o custo do projeto por 2 a 5 vezes. [MIRANDA, G. F (2017)]
- Redução de flexibilidade operacional: Atualizações e modificações no TCAS exigiriam revalidação completa.
- Possível sobreposição com outros sistemas: O TCAS teria que ser integrado com sistemas de navegação e controle de voo com lógica de prioridade e coordenação.

4 CONCLUSÃO

Na prática, classificar o TCAS como Catastrophic pode ser excessivo, pois ele é um sistema de suporte à decisão, não de controle direto da aeronave. A falha do TCAS não remove a capacidade do piloto de evitar colisões por outros meios. Por isso, ele é geralmente tratado como Hazardous, o que já impõe requisitos elevados sem exagerar na severidade.Podemos ver claramente através do acontecimento do acidente que a classificação de severidade pode ser considerada devidamente adequada ao nível atribuído uma vez que a falha acontecida resultou em uma fatalidade com meios adequados de redundância e capacidade de se evitar o acontecimento já que as falhas atribuídas ao acidente não foram exclusivamente atribuídas ao sistema do TCAS, mas sim ao conjunto de vários fatores, como fatores humanos, fatores psicológicos, controle de trafego e aspectos operacionais. [Centro de Investigação e Prevenção de Acidentes Aeronáuticos (2010)]

A partir dos resultados obtidos por meio da pesquisa documental dos requisitos e normas apresentados neste trabalho, bem como da análise realizada sobre o transponder, é possível afirmar que o objetivo proposto foi atingido. O estudo permitiu compreender, de forma consistente, a relação entre os processos de desenvolvimento de componentes estabelecidos pela ARP4754 e os requisitos de segurança previstos no FAR 25.1309, evidenciando seus impactos tanto no desenvolvimento do TCAS quanto nas falhas observadas no acidente da aeronave N600XL.

Todavia, é fundamental destacar que a investigação aqui conduzida se concentrou especificamente na falha associada ao transponder, não abrangendo a totalidade dos fatores que contribuíram para o acidente. Nesse sentido, torna-se inconclusivo afirmar que uma eventual alteração no nível de garantia de desenvolvimento do componente teria, por si só, modificado o desfecho da ocorrência. Conforme apontado por órgãos de investigação, a falha do transponder e do sistema TCAS representou apenas um dos diversos elementos que, em conjunto e dentro de um contexto operacional complexo, culminaram na fatalidade do caso.

Assim, a principal contribuição deste trabalho reside em demonstrar que, embora o design do transponder estivesse em conformidade com os requisitos normativos aplicáveis ao seu nível de criticidade, a interação entre fatores técnicos, humanos e operacionais pode gerar condições de falha que extrapolam o escopo de um único componente. Essa constatação reforça a importância de se considerar o sistema aeronáutico como um todo, em que cada elemento,

ainda que corretamente projetado, pode se tornar vulnerável diante da combinação de circunstâncias externas e da criticidade atribuída ao seu funcionamento.

REFERÊNCIAS

SAE INTERNATIONAL. *ARP4754A* – ***Guidelines for Development of Civil Aircraft and Systems*****.** : SAE Aerospace, 2010. Disponível em: https://www.sae.org/standards/content/arp4754a/. Acesso em: 14 jul. 2025.

SAE INTERNATIONAL. *ARP4761* – ***Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*****.** Warrendale: SAE Aerospace, 1996.

UNITED STATES. Federal Aviation Administration. *14 CFR Part 25* – ***Airworthiness Standards: Transport Category Airplanes*****. §25.1309 – Equipment, systems, and installations**. Washington, DC: FAA, 2023. Disponível em: https://www.ecfr.gov/current/title-14/chapter-I/subchapter-C/part-25. Acesso em: 14 jul. 2025.

UNITED STATES. **Federal Aviation Administration.** ***Aviation Maintenance Technician Handbook – Airframe, Volume 1 and 2*****. FAA-H-8083-31A**. Oklahoma City: U.S. Department of Transportation, 2018. Disponível em: https://www.faa.gov/regulations_policies/handbooks_manuals/aircraft/amt_airframe_handbook. Acesso em: 14 jul. 2025.

UNITED STATES. **Federal Aviation Administration.** ***Instrument Flying Handbook*****. FAA-H-8083-15B**. Oklahoma City: U.S. Department of Transportation, 2020. Disponível em: https://www.faa.gov/regulations_policies/handbooks_manuals/aviation/instrument_flying_handbook. Acesso em: 14 jul. 2025.

BRASIL. Centro de Investigação e Prevenção de Acidentes Aeronáuticos. ***Relatório Final – A-062/CENIPA/2006 – Ocorrência com as aeronaves PR-GTD e N600XL, em 29 de setembro de 2006***. Brasília: CENIPA, 2010. Disponível em: https://www.fab.mil.br/cenipa. Acesso em: 14 jul. 2025.

UNITED STATES. National Transportation Safety Board. ***Accident Report DCA06RA076 – Midair Collision Involving Embraer Legacy 600 and Gol Boeing 737-800***. Washington, DC: NTSB, 2007. Disponível em: https://www.ntsb.gov/. Acesso em: 14 jul. 2025.

NETO, A. F. et al. *TCAS e a Prevenção de Colisões Aéreas:* ***Lições do Acidente com o Legacy 600*****. Revista Conexão SIPAER, CENIPA**, Brasília, n. 5, p. 35–42, 2011.

SOUZA, M. C.; RAMOS, R. A. ***Falha Humana, Interação Homem-Máquina e Cultura Organizacional: Um Estudo de Caso sobre o Acidente Gol 1907*****. Revista Brasileira de Ciências Aeronáuticas**, São José dos Campos, v. 4, n. 1, p. 52–65, 2015. Disponível em: https://www4.fab.mil.br/rbca. Acesso em: 14 jul. 2025.

MIRANDA, G. F. ***Aplicação da ARP4754 e ARP4761 no Desenvolvimento de Sistemas Aeronáuticos Críticos*****. 2017. 124 f. Dissertação (Mestrado em Engenharia Aeronáutica) – Instituto Tecnológico de Aeronáutica**, São José dos Campos, 2017. Disponível em: https://www.biblioteca.ita.br/. Acesso em: 14 jul. 2025.

STUPP, E. *Sistemas Aeronáuticos:* ***Introdução à Aviação e à Engenharia de Sistemas Embarcados***. São Paulo: Érica, 2004.

HARRIS, D. (Ed.). ***Human Factors for Civil Flight Deck Design*****.** Boca Raton: CRC Press, 2011.

NOLAN, M. S. ***Fundamentals of Air Traffic Control*****.** 5. ed. Boston: Cengage Learning, 2010.

UNITED STATES. Federal Aviation Administration. *14 CFR Part 25* - **AC 25.1309-1A – System Design and Analysis**. Washington, DC: FAA, 2023

APÊNDICE

APÊNDICE 1: REQUISITO 25.1309

(a) Os equipamentos e sistemas da aeronave devem ser projetados e instalados de forma que:

1. Os equipamentos e sistemas exigidos para a certificação de tipo ou pelas regras operacionais, ou cujo funcionamento inadequado possa reduzir a segurança, desempenhem conforme o previsto nas condições operacionais e ambientais da aeronave; e
2. Outros equipamentos e sistemas, funcionando normalmente ou de forma anormal, não afetem adversamente a segurança da aeronave ou de seus ocupantes, nem o funcionamento adequado dos equipamentos e sistemas mencionados no parágrafo (a)(1) desta seção

(b) Os sistemas da aeronave e os componentes associados, avaliados separadamente e em relação a outros sistemas, devem ser projetados e instalados de forma que atendam a todos os seguintes requisitos:

1. Cada condição de falha catastrófica:

(i) Deve ser extremamente improvável; e

(ii) Não deve resultar de uma única falha.

2. Cada condição de falha perigosa deve ser extremamente remota.
3. Cada condição de falha significativa deve ser remota.
4. Cada falha latente significativa deve ser eliminada na medida do possível ou, se não for viável eliminá-la, sua latência deve ser minimizada. No entanto, os requisitos da frase anterior não se aplicam se o sistema associado atender aos requisitos dos parágrafos (b)(1) e (b)(2) desta seção, assumindo que a falha latente significativa tenha ocorrido.
5. Para cada condição de falha catastrófica que resulte de duas falhas, sendo que qualquer uma delas possa permanecer latente por mais de um voo, o requerente deve demonstrar que:

(i) É impraticável fornecer tolerância adicional a falhas; e

(ii) Considerando a ocorrência de qualquer falha latente única, a probabilidade média residual da condição de falha catastrófica devido a todas as falhas ativas subsequentes é remota; e

(iii) A soma das probabilidades das falhas latentes combinadas com cada falha ativa não excede 1/1000.

(c) A aeronave e seus sistemas devem fornecer informações sobre condições inseguras de operação dos sistemas à tripulação de voo, para que possam tomar as ações corretivas apropriadas de forma oportuna. Os sistemas e controles, incluindo informações, indicações e

alertas, devem ser projetados para minimizar erros da tripulação que possam criar riscos adicionais.

(d) [Reservado]

(e) O requerente deve estabelecer requisitos de manutenção para certificação conforme necessário para prevenir o desenvolvimento das condições de falha descritas no parágrafo (b) desta seção. Esses requisitos devem ser incluídos na seção de Limitações de Aeronavegabilidade das Instruções para Manutenção Continuada exigidas pelo § 25.1529.