UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
FACULDADE DE ENGENHARIA DE SÃO JOÃO DA BOA VISTA

WILLIAN KATUMATA DO NASCIMENTO

AVALIAÇÃO DE PERIGOS FUNCIONAIS DE UM SISTEMA DE 'DETECT AND AVOID' PARA UMA AERONAVE VOLTADA PARA MOBILIDADE AÉREA URBANA

São João da Boa Vista
2025

Willian Katumata do Nascimento

AVALIAÇÃO DE PERIGOS FUNCIONAIS DE UM SISTEMA DE 'DETECT AND AVOID' PARA UMA AERONAVE VOLTADA PARA MOBILIDADE AÉREA URBANA

Trabalho de Graduação apresentado ao Conselho de Curso de Graduação em Engenharia Aeronáutica da Faculdade de Engenharia de São João da Boa Vista, Universidade Estadual Paulista, como parte dos requisitos para obtenção do diploma de Graduação em Engenharia Aeronáutica .

Orientador: Profº Dr. Julian Arnaldo Avila Diaz

São João da Boa Vista
2025

K19a

Katumata do Nascimento, Willian
Avaliação de perigos funcionais de um sistema de 'detect and avoid' para uma aeronave voltada para mobilidade aérea urbana / Willian Katumata do Nascimento. -- São João da Boa Vista, 2025
81 p. : il., tabs.

Trabalho de conclusão de curso (Bacharelado - Engenharia Aeronáutica) - Universidade Estadual Paulista (UNESP), Faculdade de Engenharia, São João da Boa Vista
Orientador: Julian Arnaldo Avila Diaz

1. Engenharia de sistemas. 2. Segurança de sistemas. 3. Auxilio a navegação aérea. 4. Mobilidade urbana. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Dados fornecidos pelo autor(a).

UNIVERSIDADE ESTADUAL PAULISTA "JÚLIO DE MESQUITA FILHO"
FACULDADE DE ENGENHARIA - CÂMPUS DE SÃO JOÃO DA BOA VISTA
GRADUAÇÃO EM ENGENHARIA AERONÁUTICA

TRABALHO DE CONCLUSÃO DE CURSO

AVALIAÇÃO DE PERIGOS FUNCIONAIS DE UM SISTEMA DE 'DETECT AND AVOID' PARA UMA AERONAVE VOLTADA PARA MOBILIDADE AÉREA URBANA

Aluno: Willian Katumata Do Nascimento
Orientador: Prof. Dr. Julian Arnaldo Avila Diaz

Banca Examinadora:

- Julian Arnaldo Avila Diaz (Orientador)
- Leandra Isabel De Abreu (Examinadora)
- Wilian Miranda Dos Santos (Examinador)

Os formulários de avaliação e a ata da defesa, na qual consta a aprovação do trabalho, devidamente assinados pela banca encontram-se no prontuário eletrônico do aluno.

São João da Boa Vista, 09 de dezembro de 2025

Dedico este trabalho a todos que buscam melhorar o coletivo ao seu redor.

AGRADECIMENTOS

Aos meus pais, cuja dedicação, valores e amor incondicional formaram o meu alicerce.
Aos meus amigos, cujo apoio, incentivo e companhia deram sentido a esse percurso.
Aos meus professores, cuja orientação, conhecimento e inspiração indicaram a direção.

“Tudo o que estabiliza a vida humana demanda dedicação de tempo prolongada“
(Byung-Chul Han, Não-coisas: Reviravoltas do mundo da vida.)

RESUMO

Este trabalho apresenta o desenvolvimento inicial e a avaliação de perigos funcionais (*Functional Hazard Assessment* - FHA) de um sistema de *Detect and Avoid* (DAA) dentro do escopo de uma aeronave eVTOL operando no Nível 4 de Maturidade da Mobilidade Aérea Urbana (UML-4). Considerando a complexidade prevista para as operações em ambientes urbanos para mobilidade aérea, o estudo aplica metodologias de engenharia de sistemas definidas pelas normas SAE ARP4754 e ARP4761, incorporando também requisitos regulatórios da base SC-VTOL da EASA, da concepção operacional PCA 351-7 do DECEA e da referência funcional da ASTM F3442. A metodologia envolve a definição do conceito operacional, a derivação dos requisitos do sistema, a proposição de uma arquitetura inicial em alto nível e a avaliação sistemática das condições de falha, classificando sua severidade e identificando estratégias de mitigação. O trabalho explora os desafios relacionados à vigilância cooperativa e não cooperativa, disponibilidade, integridade e necessidades de redundância desse tipo de sistema. Os resultados incluem uma arquitetura conceitual resultante do primeiro ciclo de análise e desenvolvimento, bem como a identificação de perigos funcionais que podem impactar a segurança do sistema. São propostas abordagens de mitigação que apoiam o desenvolvimento de sistemas robustos e futuros esforços de certificação. Em suma, o estudo contribui para o entendimento dos requisitos de *safety* em aeronaves eVTOL e testa um caminho inicial para a implementação de sistemas de DAA voltados à mobilidade aérea urbana avançada.

PALAVRAS-CHAVE: análise de perigos funcionais; sistema de detecção e desvio; engenharia de sistemas; mobilidade aérea urbana.

ABSTRACT

This work presents the initial development and the Functional Hazard Assessment (FHA) of a Detect and Avoid (DAA) system within the scope of an eVTOL aircraft operating at Level 4 of Urban Air Mobility Maturity (UML-4). Considering the expected complexity of operations in urban environments for air mobility, the study applies systems engineering methodologies defined by SAE ARP4754 and ARP4761, also incorporating regulatory requirements from EASA's SC-VTOL framework, DECEA's PCA 351-7 operational concept, and the functional reference ASTM F3442. The methodology involves defining the operational concept, deriving system requirements, proposing an initial high-level architecture, and systematically assessing failure conditions, classifying their severity and identifying mitigation strategies. The work explores challenges related to cooperative and non-cooperative surveillance, availability, integrity, and redundancy needs for this type of system. The results include a conceptual architecture resulting from the first analysis and development cycle, as well as the identification of functional hazards that may impact system safety. Mitigation approaches are proposed to support the development of robust systems and future certification efforts. In summary, the study contributes to understanding safety requirements in eVTOL aircraft and tests an initial path toward implementing DAA systems aimed at advanced urban air mobility.

KEYWORDS: functional hazard assessment; detect and avoid system; systems engineering; urban aerial mobility.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ACAS	Airborne Collision Avoidance System
ANAC	Agência Nacional de Aviação Civil
ADS-B	Automatic Dependent Surveillance–Broadcast
AGL	Above Ground Level
ARP	Aerospace Recommended Practice
ATC	Air Traffic Controller
ATM	Air Traffic Management
BIT	Built-in Test
BVLOS	Beyond Visual Line of Sight
CEL	Controlled Emergency Landing
CNS	Comunicação Navegação e Vigilância
CONOPS	Concept of Operations
CSFL	Continued Safe Flight and Landing
DAA	Detect and Avoid
DAL	Design Assurance Level
DECEA	Departamento de Controle do Espaço Aéreo
DFR	Digital Flight Rules
DSM	Digital Surface Model
EASA	European Union Aviation Safety Agency
EO	Electro-optical
ESC	Electronic Speed Controller
FAA	Federal Aviation Administration
FHA	Functional Hazard Assessment
FOV	Field of View
FTA	Fault Tree Analysis

GNSS	Global Navigation Satellite System
HMI	Human Machine Interface
IFR	Instrumental Flight Rules
IMC	Instrument Meteorological Conditions
IMU	Inertial Measurement Unit
IR	Infrared
LOAM	Laser Obstacle Avoidance and Monitoring
MOC	Mean of Compliance
MTOM	Maximum Take-Off Mass
NASA	National Aeronautics and Space Administration
NFZ	No Flight Zone
PCA	Plano do Comando da Aeronáutica
PSSA	Preliminary System Safety Assessment
PSU	Provedor de Serviço UAM
FAA	Federal Aviation Administration
UAM	Urban Aerial Mobility
UML	UAM Maturity Level
VFR	Visual Flight Rules
VMC	Visual Meteorological Conditions
VTOL	Vertical Take-Off and Landing

SUMÁRIO

1 INTRODUÇÃO

Quando se desenvolve um produto em áreas de alto risco associadas, uma das principais considerações de *design* que devem ser feitas é quanto à segurança. Logo, é importante entender o que é pensar em segurança quando falamos no design de um produto. É possível realizar uma separação em duas vertentes que acabam se misturando no português, *safety* e *security*. Ou seja, como evitar que o sistema ofereça riscos por falhas ou mau funcionamento (*safety*) e como proteger o sistema contra ataques ou uso malicioso (*security*).

Problemas em relação a *safety* são abordados e solucionados principalmente por meio do uso de redundância, que também necessita de uma melhor definição. De forma direta, adicionar uma redundância pode ser entendida como a inclusão deliberada para se aumentar a integridade ou disponibilidade de um sistema. Sendo que, garantir disponibilidade seria assegurar a continuidade do funcionamento do sistema, mesmo após uma ou mais falhas, e garantir integridade visaria minimizar o risco de uma função desempenhar de forma incorreta quando demandada (MOIR; SEABRIDGE; JUKES, 2013).

Com base nesses entendimentos, este trabalho gerará uma avaliação de perigos funcionais (Functional Hazard Assessment – FHA), e se voltará para considerações de *safety* e aplicação de redundâncias, em um sistema de DAA, ou "*Detect and Avoid*", pensando numa aeronave eVTOL de transporte de passageiros. No trabalho o FHA será desenvolvido conforme a norma SAE ARP4761 em conjunto com a ARP4754, pensando em uma arquitetura inicial do sistema em nível conceitual - apenas em alto nível, para se obter uma arquitetura direcionada às necessidades do transporte de passageiros no contexto de Mobilidade Aérea Urbana (UAM).

Dentro do FHA serão classificadas as severidades e propostas formas de mitigação dos perigos observados. Para os requisitos funcionais do sistema de DAA, será usado como referência a ASTM F3442-25, baseline que surgiu no mercado de drones. É de conhecimento que normas mais adequadas seriam as RTCA DO-365 ou DO-396, que não consideram apenas operações de baixo e médio risco, mas já avaliam a integração com o espaço aéreo controlado, se adequando mais facilmente com a base de certificação publicada pela EASA, SC-VTOL, e seu MOC (*Mean of Compliance*) de referência. Contudo, entende-se que é um documento com integrações fora do escopo desse trabalho e, por isso, é considerado um ponto de melhoria do mesmo. Em suma, escolheu-se de forma arbitrária a publicação feita pela ASTM e considera-se uma extrapolação da mesma para o desenvolvimento da arquitetura.

Além disso, quanto ao ambiente operacional o estudo se insere no cenário de aeronaves eVTOL dentro do nível UML-4 (*UAM Maturity Level* 4), conforme conjecturado pela NASA, que o caracteriza como um estágio intermediário da mobilidade aérea urbana. Nesse nível, as operações ocorrem com densidade e complexidade médias, utilizando sistemas colaborativos e automatizados para a gestão da segurança operacional. A a chegada a esse nível representa um marco significativo rumo a uma maior autonomia de decisões através de sistemas, sendo um marco justamente pela tentativa de alcançar a aceitação pública e viabilidade operacional das aeronaves em ambientes dependentes de sistemas decisórios automáticos, como o DAA (GOODRICH; THEODORE, 2021).

Dessa forma, este trabalho tem a intenção de explorar as necessidades quanto à segurança e viabilidade da Mobilidade Aérea Urbana levantando uma avaliação sistêmica dos perigos funcionais relacionados à operação dessas aeronaves com sistemas de DAA, que serão altamente integrados com todo o ecossistema de operação da aeronave. A análise permitirá identificar pontos de segurança e buscar embasamento para o desenvolvimento de estratégias de mitigação, alinhadas com os requisitos regulatórios, operacionais e de aceitação pública.

2 OBJETIVO

Este trabalho tem como objetivo principal realizar o ciclo inicial de desenvolvimento de um sistema de DAA aplicável a operações de mobilidade aérea urbana no nível UML-4, utilizando modelagem em arquitetura de sistemas e incorporando, desde as fases conceituais, requisitos funcionais derivados da ASTM F3442 e considerações de safety, de modo a propor uma arquitetura de alto nível consistente com o cenário operacional e capaz de orientar estratégias de mitigação e robustez para aplicações futuras. Para atingir esse objetivo, estabeleceu-se como metas intermediárias:

1. Definir o CONOPS da aeronave e do sistema DAA para o contexto UML-4, alinhando o ambiente operacional e as premissas de operação necessárias para a derivação de requisitos;
2. Derivar e organizar requisitos funcionais e de certificação aplicáveis ao DAA, usando a ASTM F3442 como *baseline* funcional e relacionando-os com o contexto regulatório adotado no trabalho;
3. Elaborar uma arquitetura conceitual de alto nível para o sistema DAA e realizar uma avaliação qualitativa de safety via FHA, classificando perigos funcionais e propondo mitigações (por exemplo, redundância, integridade, monitoramento e alternativas de intervenção humana) compatíveis com o nível de severidade.

3 FUNDAMENTAÇÃO TEÓRICA

3.1 ANÁLISE E ENGENHARIA DE SISTEMAS

3.1.1 ARP4754

Para iniciar as ideias utilizadas na construção do trabalho, o ponto de partida será o entendimento de um dos norteadores adotados na indústria. A ARP 4754, denominada como "Diretrizes para o desenvolvimento de aeronaves e sistemas de aeronaves civis", estabelece procedimentos de engenharia de sistemas para o desenvolvimento de aeronaves e sistemas aeronáuticos civis ao longo de todo o ciclo de vida, integrando requisitos, verificações/validações e níveis de garantia de desenvolvimento (DAL). Ela é publicada pela SAE International, e foi inicialmente criada no contexto de certificação para estabelecer uma padronização no desenvolvimento de sistemas aeronáuticos civis, com foco na segurança, rastreabilidade e integração entre sistemas(SAE INTERNATIONAL, 1996a).

O documento é usado como base metodológica para o processo de desenvolvimento de sistemas aeronáuticos, estabelecendo uma abordagem orientada ao ciclo de vida do produto. Dentro do trabalho aqui feito será utilizada a sua versão publicada de 1996, ARP 4754 "Considerações de Certificação para Sistemas Aeronáuticos Altamente Integrados ou Complexos", que apesar de não ser a atual, foi possível de ser acessada. Portanto, direcionado pelos processos definidos no anexo A do documento supracitado, o desenvolvimento desse trabalho seguirá os seguintes passos:

1. Definição do conceito operacional;
2. Levantamento das funções da aeronave e seus requisitos;
3. Definição de interface entre os sistemas;
4. Aplicação inicial do FHA;
5. Divisão hierárquica dos sistemas com alocação das funções identificadas;
6. Desenvolvimento da arquitetura;
7. Indicação de atendimento aos requisitos com base na arquitetura definida;

Nesse sentido, o levantamento funcional forma a base para estabelecer a arquitetura. No processo íntegro, ao selecionar uma arquitetura em alto nível, define-se a decomposição em funções e requisitos necessários para o sistema de nível abaixo, e a cada derivação inicia-se um ciclo de definição de arquitetura e levantamento de requisitos detalhados e novos que sejam identificados. Conforme são tomadas as decisões de projeto, novos problemas são encontrados que podem levar à definição de

novos subsistemas com requisitos adicionais. Esse processo é realizado continuamente durante o desenvolvimento do produto, sendo que no escopo desse trabalho não se pretende chegar ao mais baixo nível de sistema, fechando seu contorno apenas em níveis mais altos (SAE INTERNATIONAL, 1996a).

Em suma, o processo iterativo utilizado neste trabalho para a criação da arquitetura conceitual do sistema de DAA se dará a partir da definição do problema a ser solucionado, que determinará um conceito operacional e definirá os requisitos funcionais necessários para o cumprimento dos objetivos definidos. Com as funções, será realizada a decomposição em subsistemas necessários para o funcionamento do DAA, aplicação do FHA e criação de uma nova arquitetura do sistema analisado.

3.1.2 ARP4761

Em complemento com a norma anterior, a ARP 4761 descreve procedimentos para a avaliação da segurança de sistemas aeronáuticos civis. Inicialmente, foi criada para se demonstrar o cumprimento em processos de certificação aeronáutica e, por isso, seu foco é identificar, analisar e mitigar riscos associados a falhas de sistemas. A norma fornece uma estrutura sistêmica para integrar a segurança do produto desde as fases iniciais de concepção até a operação, garantindo que os níveis de integridade e confiabilidade exigidos sejam devidamente alcançados (SAE INTERNATIONAL, 1996b).

Vale ressaltar que, assim como a anterior, será utilizada como referência sua versão publicada em 1996, ARP 4761 "Diretrizes e Métodos para Conduzir o Processo de Avaliação de Segurança em Sistemas e Equipamentos Aerotransportados Civis", devido a ela ser a qual foi possível ser acessada para confecção do trabalho.

3.1.2.1 *Functional Hazard Assessment (FHA)*

A primeira das ferramentas apresentadas no documento de referência é chamada de avaliação de perigos funcionais, e é foco do trabalho. De acordo com a ARP 4761, é uma avaliação sistemática e qualitativa das funções a fim de se identificar e classificar condições de falha de acordo com sua severidade. É válido se ressaltar que, nesse âmbito, chama-se sistema tudo aquilo que desempenha uma função cujas partes sozinhas não desempenhariam. Portanto, como exemplo, o sistema VTOL é um subsistema do sistema de aeronave, mas também tem seus subsistemas, como rotor, ESC (*Electronic Speed Controller*), bateria etc, que também funcionam através do conjunto de seus subsistemas ou componentes. Além disso, após se realizar a análise de segurança, podem surgir novos subsistemas voltados para a segurança dos iniciais, que também deverão passar por uma avaliação de perigo até que se garanta que nenhum ponto de falha único possa gerar falhas catastróficas - pensando em aeronaves

civis para transporte de pessoas.

Entretanto, faz parte da ferramenta não apenas o exercício de classificação, mas de predição das possíveis consequências e justificativas da severidade. A construção do FHA é um processo iterativo que evolui junto com o desenvolvimento do produto e serve de entrada para as análises e, em conjunto com uma árvore de falhas, pode determinar se os sistemas alcançam ou não as probabilidades exigidas em um nível aceito pelas agências reguladoras, e, consequentemente, pela sociedade. Aqui não serão feitas análises quantitativas pois essas análises exigem definição a nível de componente, o que ainda não se pretende chegar. O processo segue, mesmo que não direta e explicitamente, os seguintes passos:

1. Identificação de todas as funções associadas ao sistema em estudo;
2. Identificação e descrição das condições de falha associadas a essas funções, considerando falhas simples e múltiplas em ambientes normais e degradados;
3. Determinação dos efeitos da condição de falha;
4. Classificação da severidade da condição de falha;
5. Atribuição de requisitos às condições de falha a serem consideradas no nível inferior;
6. Identificação do material de apoio necessário para justificar a classificação dos efeitos da condição de falha;
7. Identificação do método utilizado para verificar a conformidade com os requisitos da condição de falha.

Para isso, é necessário como entrada na FHA as funções de mais alto nível da aeronave (por exemplo, sustentação, propulsão etc.), os objetivos da aeronave e os requisitos do cliente (por exemplo, número de passageiros, alcance etc.), e decisões iniciais de projeto (por exemplo, número de motores, empenagem convencional etc.); ou, pensando em sistemas as funções principais a serem consideradas, diagrama funcional mostrando as interfaces entre sistemas (por exemplo, diagrama temporal, caminho da informação), a lista de funções criadas nas FHAs de níveis superiores, as condições de falha identificadas nas FHAs de níveis superiores, e todas as decisões tomadas no nível superior considerando suas justificativas.

Todo o processo de utilização da ferramenta obriga o sistema a passar por uma avaliação das consequências de se perder uma determinada função seja de forma anunciada e não anunciada, funcionamento errôneo, ativação inadvertida, qualquer causa-raiz que resulte em uma ação indesejada. Tudo isso com o objetivo de que exista um preparo prévio de como impedir ou agir quando eventualmente cada falha ocorrer.

3.1.3 Severidade e probabilidade de falha

Primeiramente, para a classificação de severidade devemos sustentar o racional construído em alguma definição de uma autoridade. Considerando que esse mercado é incipiente, ainda não existe uma definição padronizada para aeronaves voltadas para a mobilidade aérea urbana. Sendo assim, no trabalho apresentado nos basearemos no que define a EASA dentro do contexto atual deste trabalho, voltadas para aeronaves de pequeno porte com capacidade de VTOL para até 9 passageiros e MTOM igual ou inferior a 5,700 kg.

Ainda, para entendimento da classificação da severidade, é necessário entender a divisão de categoria dentro da publicação e a definição da autoridade quanto a o que é um voo e pouso seguro e contínuo (CSFL) e o que é um pouso de emergência controlado (CEL). A EASA dividiu as aeronaves na categoria avançada - àquelas destinadas a operações sobre áreas congestionadas ou de transporte comercial, sendo necessário garantir o CSFL, e básica - aeronaves que não se enquadram na definição e apenas garantem o CEL. Para a autoridade civil, o CSFL significa ser capaz de manter voo controlado e realizar o pouso em um vertiporto, mesmo que utilizando procedimentos de emergência, e que não exija habilidade ou força excepcional do piloto; já o CEL seria a capacidade de realizar um pouso controlado, utilizando procedimentos de emergência, também sem exigir habilidade ou força excepcional do piloto, mas considerando que possa ocorrer algum dano à aeronave e sem a necessidade de realizá-lo em um vertiporto.

Sendo assim, partindo dessa premissa, a classificação de falhas será realizada da seguinte forma. A severidade refere-se às consequências de uma condição de falha sobre a segurança da aeronave, dos ocupantes e de terceiros no solo, e são categorizadas em níveis como *No Safety Effect, Minor, Major, Hazardous e Catastrophic*, definido mais precisamente abaixo. Cada nível é diretamente ligado a uma probabilidade permitida, referindo-se à frequência esperada com que essa condição de falha pode ocorrer durante todo ciclo de operação do modelo de aeronave, sendo, exceto para àquelas classificadas como *No Safety Effect*, respectivamente, *Probable, Remote, Extremely Remote e Extremely Improbable*. A relação entre esses dois conceitos é o que define a criação de redundâncias através da FHA e é o que, de fato, orienta decisões de projeto. Essas probabilidades podem ser avaliadas de forma qualitativa ou quantitativa, sendo que, por definição, temos:

- *Probable*: São aquelas cuja ocorrência é esperada uma ou mais vezes durante toda a vida operacional de cada aeronave (ocorrência menor ou igual a 10^{-3} para categoria avançada).
- *Remote*: São aquelas improváveis de ocorrer em cada aeronave individualmente durante sua vida total, mas que podem ocorrer diversas vezes ao se considerar a vida operacional total de várias aeronaves do mesmo tipo (ocorrência menor ou igual a 10^{-5} para categoria avançada).
- *Extremely Remote*: São aquelas que não se espera que ocorram em cada aeronave durante toda a sua vida útil, mas que podem ocorrer algumas vezes ao se considerar a vida operacional total de todas as aeronaves do mesmo tipo (ocorrência menor ou igual a 10^{-7} para categoria avançada).

- *Extremely Improbable*: São aquelas tão improváveis que não se espera que ocorram durante toda a vida operacional de todas as aeronaves de um determinado tipo (ocorrência menor ou igual a 10^{-9} para categoria avançada).

No entanto, será frisado que no escopo desse trabalho serão considerados apenas pontos de falha únicos para criação de redundâncias, sendo simplificadas as análises de falhas combinadas. Ou seja, o objetivo é manter o voo e pouso seguro após uma falha única, a proteção contra múltiplas falhas será abordada considerando que haverá mitigações através de detecções durante as operações normais da aeronave, o que inclui as verificações pré-voo, ou, caso identificada que uma primeira falha cause outros mau funcionamentos, que a sua forma de monitoramento seja desconsiderada como ponto de falha.

Então, considerando a primeira edição do MOC SC-VTOL ou Meios de Cumprimento do SC-VTOL, que define uma falha como "ocorrência que afeta a operação de um componente, parte ou elemento de forma que ele não possa mais funcionar conforme o previsto", nesse trabalho elas serão categorizadas de acordo com as severidades definidas como:

- *No safety effect*: Condições de falha que não teriam nenhum impacto na segurança (ou seja, falhas que não afetariam a capacidade operacional da aeronave nem aumentariam a carga de trabalho da tripulação).

- *Minor*: Condições de falha que não reduziriam significativamente a segurança da aeronave e envolveriam ações da tripulação dentro de suas capacidades. Podem incluir:

  (a) Uma leve redução nas margens de segurança ou nas capacidades funcionais,

  (b) Um leve aumento na carga de trabalho da tripulação como alterações rotineiras no plano de voo,

  (c) Algum desconforto físico para os passageiros ou a tripulação de cabine.

- *Major*: Condições de falha que reduziriam a capacidade da aeronave ou a habilidade da tripulação de lidar com condições operacionais adversas, a ponto de haver:

  (a) Uma redução significativa nas margens de segurança ou nas capacidades funcionais,

  (b) Um aumento considerável na carga de trabalho da tripulação ou que prejudiquem sua eficiência,

  (c) Desconforto à tripulação de voo, sofrimento físico aos passageiros, possivelmente incluindo ferimentos.

- *Hazardous*: Condições de falha que reduziriam a capacidade da aeronave ou a habilidade da tripulação de lidar com condições adversas a tal ponto que haveria:

  (a) Uma grande redução nas margens de segurança ou nas capacidades funcionais;

  (b) Sofrimento físico ou carga de trabalho tão elevada que a tripulação de voo não poderia mais ser considerada confiável para executar suas tarefas de forma precisa ou completa;

(c) para Categoria Avançada, possível ferimento grave a um ocupante que não seja da tripulação de voo, mas sem expectativa razoável de fatalidades, ou

(d) para Categoria Básica, ferimento grave ou fatal a um ocupante que não seja da tripulação de voo.

- *Catastrophic*:

(a) Para Categoria Avançada: condições de falha que se espera como resultado uma ou mais fatalidades ou incapacitação de um membro da tripulação de voo, geralmente acompanhadas da perda da aeronave e condições de falha que impediriam o CSFL da aeronave.

(b) Para Categoria Básica: condições de falha que se espera resultar em múltiplas fatalidades ou em incapacitação ou ferimento fatal de um membro da tripulação de voo, normalmente com perda da aeronave e condições de falha que impediriam o CEL da aeronave.

Abaixo, na 1, podemos ver de forma mais visual a correlação de severidade e probabilidade conforme define o MOC (*Means of Compliance*) da base de certificação SC-VTOL.

Figura 1 – Objetivos de *Safety* com base na SC-VTOL

		Failure Condition Classifications			
	Maximum Passenger Seating Configuration	Minor	Major	Hazardous	Catastrophic
		Allowable Qualitative Probability			
		Probable	Remote	Extremely Remote	Extremely Improbable
		Allowable Quantitative Probability (Note C and D) Development Assurance Level			
Category Enhanced	-	$\leq 10^{-3}$ FDAL D (see Note B)	$\leq 10^{-5}$ FDAL C	$\leq 10^{-7}$ FDAL B	$\leq 10^{-9}$ FDAL A
Category Basic	7 to 9 passengers (Basic 3)	$\leq 10^{-3}$ FDAL D (see Note B)	$\leq 10^{-5}$ FDAL C	$\leq 10^{-7}$ FDAL B	$\leq 10^{-9}$ FDAL A
	2 to 6 passengers (Basic 2)	$\leq 10^{-3}$ FDAL D (see Note B)	$\leq 10^{-5}$ FDAL C	$\leq 10^{-7}$ FDAL C (see Note A)	$\leq 10^{-8}$ FDAL B (see Note A)
	0 to 1 passenger (Basic 1)	$\leq 10^{-3}$ FDAL D (see Note B)	$\leq 10^{-5}$ FDAL C	$\leq 10^{-6}$ FDAL C (see Note A)	$\leq 10^{-7}$ FDAL C (see Note A)

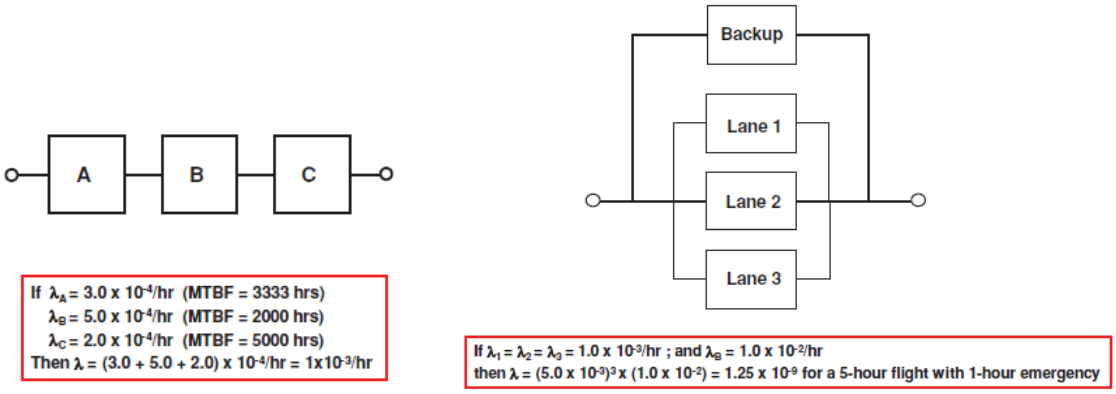
[Quantitative safety objectives are expressed per flight hour]

Fonte: (EUROPEAN UNION AVIATION SAFETY AGENCY (EASA), 2023)

3.1.4 Redundância, disponibilidade e integridade

Antes de iniciar outros assuntos, ainda é importante definir para o leitor o que seriam alguns pilares quanto a *safety* de sistemas. Nessa seção, definiremos o entendimento de redundância, disponibilidade e integridade para sistemas. Primeiramente, partiremos da premissa da ARP 4764 de que a garantia de

Figura 2 – Comparação de Arquiteturas



(a) Arquitetura Simplex (b) Arquitetura Triplex com Backup

Fonte: (MOIR; SEABRIDGE; JUKES, 2013)

safety se dá quando o risco é menor que o aceito. Ou seja, por existir subjetividade na definição, é necessário ter embasamento em publicações de autoridades que consigam representar o interesse da sociedade. Com essa definição em mente, podemos entender as análises de *safety* como a tentativa de garantir que a probabilidade de uma falha acontecer seja equivalente à severidade das consequências dela. Então, dentro de uma visão booleana, podemos visualizar redundâncias em um sistema como a tentativa de adicionar eventos condicionais “E” para alcançar as probabilidades de falha com aceitação.

Por exemplo, utilizando como referência o livro “Civil Avionics Systems”, um sistema que seja composto pelos subsistemas A, B e C, falham por hora-voo λ_A, λ_B e λ_C. A probabilidade de falha total do sistema será a soma dos três sistema, já que se subsistema A, B "OU"C falham, o sistema inteiro perderia sua função. Agora, quando pensamos numa arquitetura de tripla redundância e adicionamos um sistema de *backup* conseguimos atingir níveis de probabilidade aceitáveis até para falhas catastróficas, como exemplificado na 2 retirada da referência. Cada redundância adicionada visa principalmente dois objetivo, aumentar a disponibilidade ou integridade do sistemas.

A disponibilidade mede a probabilidade de um sistema estar operacional quando necessário. Em termos probabilísticos, ela é fortemente dependente da quantidade de canais redundantes, com a disponibilidade crescendo de forma exponencial com o número de canais. Agora, a integridade refere-se à confiança de que o sistema está fornecendo informações corretas. Nesse caso, não basta estar disponível, é preciso funcionar corretamente. Uma informação errada pode ser mais perigosa que a ausência dela, sendo necessário determinar alguma forma de monitoramento. Por exemplo, a perda de dados de altitude ou velocidade pode ser “hazardous”, mas dados incorretos apresentados como corretos podem ser “catastrophic”, pois induzem sistemas e o piloto ao erro. Ela será assegurada por técnicas como *Built-in Test* (BIT), testes automáticos contínuos ou periódicos que verificam se cada canal funciona corretamente, e *Cross-Monitoring*, em que cada canal verifica a si mesmo e compara seus resultados com outros canais para detectar discrepâncias (MOIR; SEABRIDGE; JUKES, 2013).

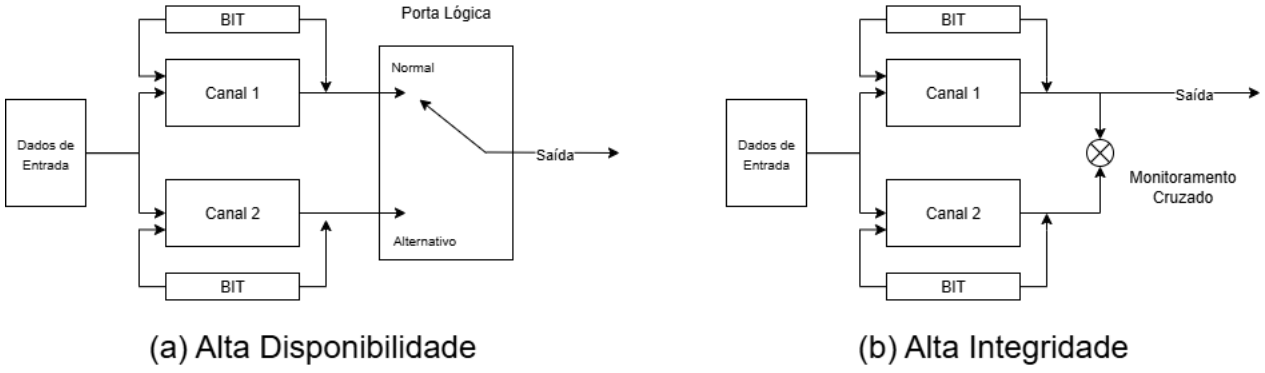
Por fim, podemos entender o que seria de fato uma redundância, um mecanismo que assegura tanto disponibilidade quanto integridade por meio da replicação de sensores, processadores, atuadores etc. Sendo, conforme a classificação dos autores, os principais tipos:

- Simplex (×1): único canal de controle e sensor, a falha implica na perda total da função, embora possa haver *fallback* para um estado seguro;

  Exemplo: sistemas economicamente e tecnicamente não críticos como o controle de iluminação da cabine.

- Duplex (×2): dois canais idênticos operando em paralelo. Pode priorizar alta disponibilidade (um canal assume se o outro falhar) ou alta integridade (ambos devem concordar para emitir o comando) como mostra a 3;

Figura 3 – Exemplos de Arquiteturas Duplex voltadas a Integridade e Disponibilidade



Fonte: (MOIR; SEABRIDGE; JUKES, 2013)
Adaptação: Autor.

  Exemplo: sistemas de trem de pouso ou freios, em que falhas são inaceitáveis.

- Triplex (×3): três canais independentes com um sistema selecionador ou comparador, que adota a média ou o valor majoritário. Assim, é possível permitir a falha operacional no primeiro defeito (mantém função) e o “fail safe” no segundo;

  Exemplo: sistemas fly-by-wire de aeronaves comerciais.

- Quadruplex (×4): quatro canais redundantes, usados em sistemas instáveis por projeto;

  Exemplo: sistema de controle para manter estabilidade do Northrop B-2 Spirit stealth bomber (MOIR; SEABRIDGE; JUKES, 2013).

Em suma, a escolha entre arquiteturas simplex, duplex, triplex ou quadruplex deriva da análise de risco e da classificação de severidade da falha. Além disso, podemos dizer que confiabilidade trata da frequência de falhas (“Com que frequência o sistema falha?”) e integridade trata da qualidade na identificação das falhas ("O sistema é capaz de identificar que falhou?”), sendo ambos importantes na determinação do nível de redundância. Em sistemas de segurança crítica, como aviônica, alta integridade é prioritária em relação à alta confiabilidade, pois a detecção e isolamento corretos de uma falha são mais importantes do que a simples redução da sua frequência, sendo essa a lógica que será seguida no trabalho.

3.2 EVTOL PARA MOBILIDADE AÉREA

3.2.1 Conceito de eVTOL pelas autoridades

Antes de iniciar o desenvolvimento do sistema de DAA, é importante entender a importância dele para o seu mercado, e principalmente, o novo cenário operacional que ele será inserido. Ressalta-se que os eVTOLs são uma nova categoria de veículos aéreos, não veículos de asas rotativas elétricos. Essa categoria tem suas missões típicas próprias e objetivos diferentes, sendo que seu foco principal é garantir uma escalabilidade de operação em cenário urbano. Todas as suas características advêm dessa premissa, seja o fato de serem elétricas, autônomas (no longo prazo), com decolagem e pouso vertical, com baixo ruído acústico etc.

Essa afirmação se baseia justamente em como as autoridades de aviação civil tratam essa nova categoria. Na EASA, eVTOLs entram com base regulamentar própria sob a SC-VTOL, um enquadramento distinto de aeronaves convencionais, sendo definidas principalmente por seus sistemas de sustentação para decolagem e pouso vertical.

Já a FAA, enquadra essas aeronaves numa categoria denominada como *powered-lift* e atualmente estão sendo certificados via 14 CFR 21 para processos com aeronaves de condição especial, com a unificação de requisitos de diversas bases e regras complementares voltadas a cada produto em específico, semelhante à construção da base da EASA. Ainda, é também a mesma forma que a ANAC está tratando o projeto EVE, com publicação de base de requisitos de certificação própria através da unificação de diversas bases existentes e novos requisitos apresentados em chamada pública para comentários (FEDERAL AVIATION ADMINISTRATION, 2023b).

Portanto, com base na 14 CFR 1, aeronaves *Powered-lift* foram definidas como aeronaves mais pesadas que o ar, capazes de decolagem e pouso vertical e voo em baixa velocidade, que dependem principalmente de dispositivos de sustentação acionados por motor ou do empuxo do motor para gerar sustentação durante esses regimes de voo, e de superfícies aerodinâmicas não rotativas para gerar sustentação durante o voo horizontal (FEDERAL AVIATION ADMINISTRATION, 2023a).

Como se pretende operar milhares dessas aeronaves compartilhando um mesmo espaço aéreo de baixa altitude, é necessário que o espaço de operação seja menor, que poluam menos, que gerem menos ruído, que suportem um controle do espaço aéreo integrado e automático, que o custo para treinamento da tripulação não seja exorbitante, que garantam alta confiabilidade e integridade, todas essas características advêm da premissa inicial que as diferenciam das aeronaves atuais. Essas aeronaves convencionais não foram pensadas para operarem em escala de milhares compartilhando um único espaço aéreo controlado, e portanto é preciso disrupção na tecnologia.

E, do ponto de vista do autor, justamente por serem aeronaves disruptivas, elas diferem tanto entre si. Os diversos *designs* levam em conta pontos como complexidade de implementação, peso final dos sistemas e dificuldades com a certificação. Ainda não se chegou na configuração com o melhor *trade-off* entre todas as características citadas, entretanto, atualmente as principais configurações

utilizadas são *lift+cruise* - sistemas de cruzeiro e decolagem separados, e *tilt-rotor* - rotores que são utilizados tanto em cruzeiro quanto na decolagem, sendo algumas das principais concorrentes as aeronaves da Joby, Archer, EVE e Vertical Aerospace.

3.2.2 UML (*UAM Maturity Level*)

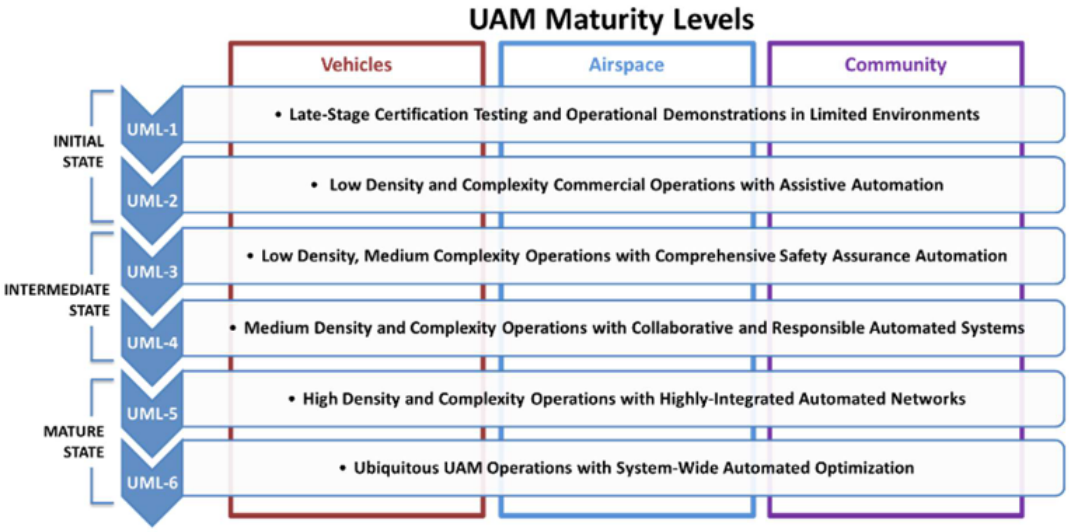
Inserido dentro de um contexto de preparação regulamentar, a NASA publicou um *roadmap* para padronização do entendimento quanto à evolução do novo espaço aéreo que surgirá com a mobilidade aérea urbana. O órgão entende que o espaço evoluirá de formas diferentes e simultaneamente; por exemplo, metrópoles como São Paulo atingiriam um nível de maturidade maior e mais rapidamente devido à necessidade local do serviço, enquanto que cidades mais interioranas poderiam estar em níveis anteriores. Como será necessário um ecossistema inteiro para manter o funcionamento seguro desse novo mercado, esses diferentes níveis de maturidade abordariam os riscos associados de forma adequada para a sua complexidade.

Não faria sentido exigir sistemas de DAA e integração com sistemas de controle do espaço aéreo automático para aeronaves que tenham pretensão de voar regiões com baixa densidade de tráfego, que não sobrevoam pessoas e nem demonstrem riscos em solo. Assim como não seria apropriado permitir que uma aeronave sem esses sistemas integrasse um espaço aéreo que seguisse regras de voo digital ou baseadas em trajetórias 4D (espaço e tempo), como idealiza o órgão em níveis de maturidade mais elevados.

Tendo esse contexto em vista, a 4 foi retirada do relatório técnico publicado (GOODRICH; THEODORE, 2021). Nela podemos ver a divisão em 6 níveis que aumentam em complexidade de operação e atravessam três frentes de maturidade, a do veículo, do espaço aéreo e da comunidade, que pode ser entendida como a junção da percepção da sociedade, mercado e autoridades. Portanto, as divisões do *framework* tentam avaliar os requisitos tecnológicos e regulatórios gerados desse processo de maturação, sendo que um sistema de DAA robusto torna-se condição necessária para segurança, escalabilidade e aceitação pública.

Com isso, chegamos à definição do escopo deste trabalho, que irá utilizar as ferramentas de avaliação de *safety*, já citadas, no contexto de uma aeronave fictícia que surgirá com a intenção de atender o quarto nível de maturidade descrito, com operações de média densidade e complexidade, baseando-se em sistemas automatizados colaborativos e responsáveis, ou seja, espera-se que, nesse nível, já se tenha reduzido o nível de especialização necessário para pilotos e controladores, entendendo que os sistemas já garantem alta confiabilidade na tomada de decisão, justamente o foco do trabalho, entender o que é necessário a nível de sistema para se conquistar essa maturidade.

Figura 4 – Escala de Nível de Maturidade UAM (UML)



Fonte: (GOODRICH; THEODORE, 2021)

3.2.3 Concepção Operacional UAM Nacional

3.2.3.1 *Visão Geral*

No ano de 2024, o DECEA publicou o seu Plano do Comando da Aeronáutica 351-7 que dispõe sobre a concepção operacional do UAM nacional. A publicação define parâmetros operacionais, tecnológicos e regulatórios para orientação dos projetos de mobilidade aérea urbana no Brasil. Na publicação define-se esse ecossistema como um subconjunto do Sistema ATM, com o objetivo de proporcionar o Gerenciamento de Tráfego Aéreo em ambientes urbanos e suburbanos considerando a integração colaborativa de informações e serviços. É previsto que nesse ambiente poderão operar aeronaves eVTOL, helicópteros, aeronaves remotamente pilotadas ou da aviação geral, desde que cumpram os requisitos mínimos para acesso a esse espaço aéreo.

O objetivo principal da concepção operacional é orientar a forma como as operações de aeronaves eVTOL deverão ser gerenciadas, considerando novas regras de voo e métodos de gerenciamento de tráfego aéreo, partindo da premissa que não se reduza o nível de segurança nem a capacidade das operações aéreas atuais. O espaço aéreo UAM será definido por volumes 4D (três dimensões espaciais e uma temporal) dentro dos quais as operações serão geridas por um Provedor de Serviço UAM (PSU). Esses volumes serão parametrizados conforme a dinâmica local de tráfego e as rotas existentes. Vislumbra-se a criação de uma nova classificação de regras de voo dentro desse contexto, o DFR (*Digital Flight Rules*). Com esse novo paradigma, o gerenciamento será progressivamente automatizado e apoiado em sistemas de tomada de decisão colaborativa e operações baseadas em trajetória.

Do ponto de vista da própria publicação, a introdução de um novo tipo de regra de voo será fundamental a partir do UML-4, escopo desse trabalho, sustentando essa conclusão com base no nível de escalabilidade esperado em conjunto da utilização de dados para complementar a navegação aérea. Por fim, será tomado como necessidades dos *stakeholders* as definições da publicação, sendo essas necessidades exploradas abaixo.

3.2.3.2 *Necessidades UAM Nacional*

No desenvolvimento de um novo sistema, parte dos *stakeholders* considerados são justamente as autoridades de aviação civil que representam os interesses e aceitação da sociedade a essa nova tecnologia. Como referência para os primeiros requisitos serão consideradas as indicações realizadas pelo documento. Por exemplo, do ponto de vista do plano publicado entende-se que poderá ser requerido ADS-B para suporte no gerenciamento de todo o tráfego aéreo cooperativo. Fora isso, requisitos específicos de capacidade e performance foram mais explorados com base em cada nível de UML. No entanto, do ponto de vista da análise desse trabalho, eles foram definidos ainda de forma abrangente. Para absorção no desenvolvimento aqui realizado, abaixo será definido de forma explícita o que se interpretará como influente para aeronaves dentro do UML 4, e àqueles que de alguma forma também influenciam o sistema de DAA.

Antes dessa definição, é importante conceitualizar as soluções de desconflito em dois âmbitos, estratégico e tático. Para o primeiro, considerando a definição do próprio plano, são ações e planejamentos realizados anteriormente ao inicio da operação, e não te relação direta com um sistema de DAA. E o segundo, são as ações de lógicas utilizadas para realizar o desconflito durante a operação. Assim sendo, o primeiro é de maior responsabilidade das próprias tecnologias voltadas ao gerenciamento e otimização do uso do espaço aéreo, e o segundo de fato envolveria a identificação de obstáculos em tempo real e o replanejamento da rota para desvio.

Postuladas essas definições, entende-se que, como requisitos influentes da norma pois afetam o desenvolvimento do sistema de DAA os seguintes:

- **Do Capítulo III, Seção VI - Requisitos de Capacidade e Performance:**

  - O ADS-B é obrigatório em ambientes congestionados,

  - Existe a possibilidade de uso apenas de ADS-B OUT em baixa demanda, sendo que o DAA deve funcionar mesmo quando não houver ADS-B IN de outros veículos.

- **Do Capítulo IV, Seção II - Serviços CNS (Comunicação, Navegação e Vigilância):**

  - A aeronave não poderá depender exclusivamente de GNSS devido a não garantia de visibilidade dos satélites perto de edifícios, torres, estruturas que bloqueia o sinal;

  - Os sistemas deverão ter comunicações de alta taxa e baixa latência (Ex.: 5G)

  - As aeronaves deverão compartilhar a posição e receber posições de outras aeronaves;

- Os usuários precisarão ser constantemente informados sobre o status do tráfego aéreo, condições meteorológicas e quaisquer eventos inesperados;

- Deverão ser usadas diferentes bandas de frequência (entende-se como parte de uma solução *anti-jamming* e *anti-spoofing*).

- Necessidade de vigilância aérea independente de radar pois o controle de tráfego aéreo é incapaz de rastrear aeronaves em voos de baixa altitude

- **Do Capítulo IV, Seção VI - Serviço de Cartografia:**

  - As aeronaves deverão ser alimentadas com modelos digitais de elevação e os obstáculos na região em estudo (naturais e artificiais).

  - Será tomado crédito que das funções esperadas para o PSU, o mapeamento do solo já estará sendo oferecido em UML 4. Sendo assim, poderá ser considerado como entrada do sistema cooperativo a existência de modelos digitais do terreno

- **Do Capítulo IV, Seção X - Serviço de Gerenciamento de Tráfego Aéreo – ATM:**

  - O gerenciamento de tráfego, em nível estratégico, aprovará a intenção de voo de forma a viabilizar a separação estratégica, permitir a identificação e informar as restrições de espaço aéreo; e definir horários de decolagem e pouso.

- **Do Capítulo VI, Seção IV - Requisitos Iniciais:**

  - Comunicação por Datalink e VHF para situações emergenciais

  - Coordenação realizada pela piloto com regras de voo DFR

  - Voos apenas em condições meteorológicas IMC e VMC

  - Separação realizada pelo conjunto de sistemas embarcados e serviços do PSU

  - Performance de navegação requerida de 0.3 NM ou melhor para separação entre intenções de voo das aeronaves

  - Existência de ADS-B, ACAS (*Airborne Collision Avoidance System*) e DAA

3.3 SISTEMAS DE DAA (*DETECT AND AVOID*)

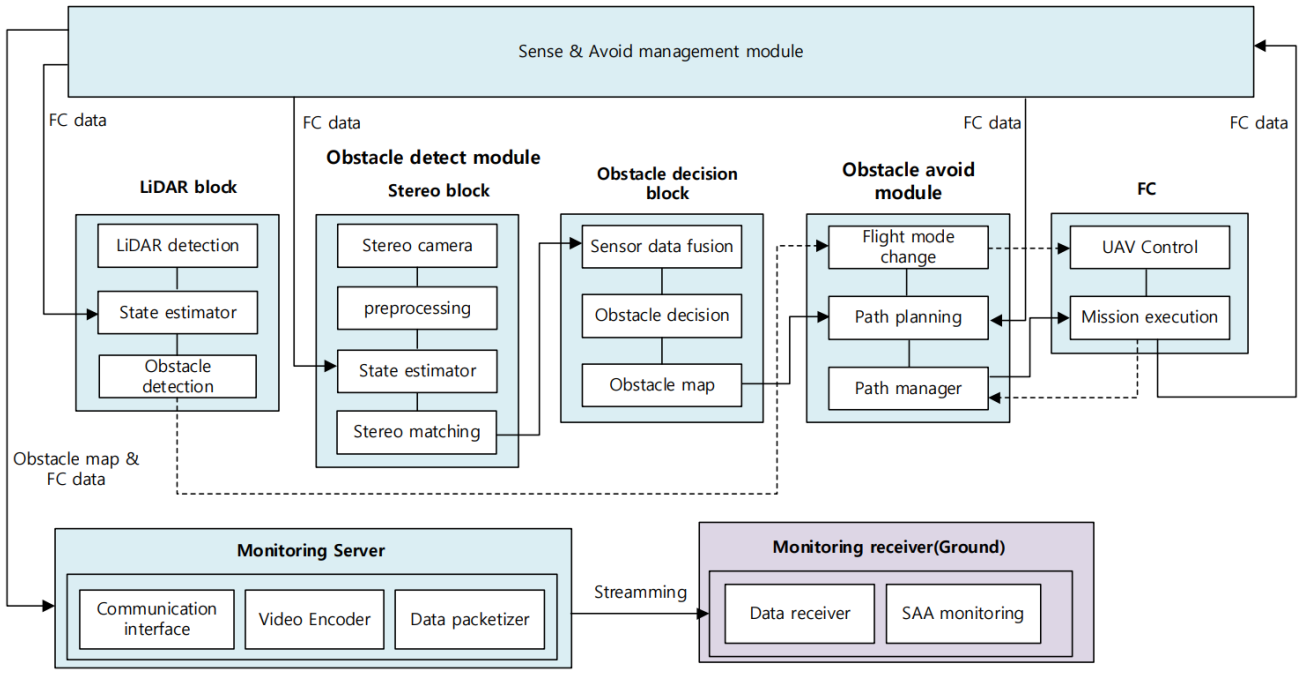
3.3.1 Revisão sobre o sistema

A detecção e o desvio de obstáculos são funções de grande importância quando se estuda a viabilidade de sistemas de aeronave autônomos. Pensando em um extremo, eles seriam capazes de garantir a segurança operacional mesmo em ambientes não controlados ou com agentes não

colaborativos. No entanto, existem diferentes abordagens para se implementar essa função através de um sistema. Aqui será feita a revisão de alguns trabalhos publicados para servir de base na avaliação de qual arquitetura inicial será proposta.

Utilizando a combinação de um LiDAR *Sweeper* 2D e uma câmera estéreo é possível conseguir resultados satisfatórios em ambiente controlado, segundo suas simulações e testes. Ki, Cha e Lyu concluem em seu trabalho que a combinação de diferentes sensores é muito mais eficiente em performance. Com a mistura do LiDAR com a câmera eles conseguiram uma precisão em curta distância através do primeiro, mesmo restringindo seu FOV (*Field of View*) a ±30°, para reduzir o processamento necessário. Como a câmera depende da iluminação externa e é influenciada pelo movimento, a detecção em curto alcance pode ser insuficiente.

Figura 5 – Arquitetura do Sistema de Ki, Cha e Lyu (2018)



Fonte: (KI; CHA; LYU, 2018)

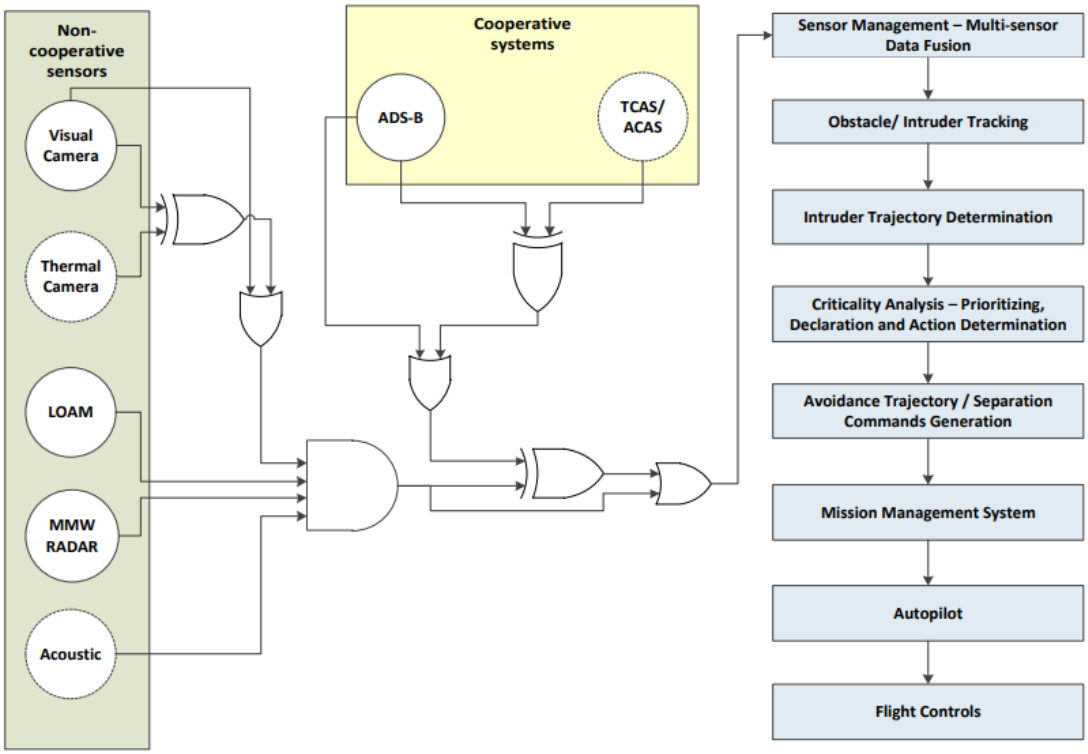
No entanto, isso não é um problema para o LiDAR, que é limitado por outras variáveis, como poder de processamento, gasto energético e dispersão com a distância. Como o LiDAR é um sensor ativo, emite luz e detecta sua reflexão, ele precisa de muita potência para alcançar distâncias maiores, diferente da câmera que só precisa receber a luz de forma passiva. Com isso, utilizando ambos, os sensores conseguem se complementar em seus défices, sendo muito mais eficiente do que uma solução centrada em um ou no outro. Por fim, o algoritmo de evasão foi baseado em campo potencial e executado em um computador embarcado (NVIDIA TX2).

Além disso, alguns pontos para discussão, no trabalho foi utilizada uma aeronave multicóptero pequena, que trazia em si limitações quanto ao tamanho e consequente capacidade computacional. Tais limitações podem ser parcialmente mitigadas em aeronaves eVTOL de maior porte, que dispõem de maior capacidade energética e computacional. Contudo, requisitos de certificação e redundância impõem restrições próprias de segurança e custo que não devem ser desconsideradas. Ainda, a variação de ângulo de visada devido a inclinação seriam também um problema para aeronaves de asa fixa, no

entanto, com maior poder de processamento, o FOV não precisaria ser limitado ou o LiDAR sendo bidimensional, não sendo considerada uma limitação como no caso do trabalho discutido.

Com base na arquitetura mostrada na 5, quando o LiDAR detecta um obstáculo, o módulo de evasão é acionado, alterando o modo de voo e recalculando a rota a partir do mapa de obstáculos e das estimativas de estado, até retomar a trajetória planejada. Quando o sentido é determinado, um novo destino é posto e o ciclo de avaliação reinicia até voltar ao modo de seguir a trajetória definida no planejamento do voo (KI; CHA; LYU, 2018).

Figura 6 – Arquitetura do Sistema de Ramasamy, Gardi e Sabatini (2015)



Fonte: (RAMASAMY; GARDI; SABATINI, 2015)

Fora a arquitetura descrita acima, Ramasamy, Gardi e Sabatini testam uma adaptação de um sistema LOAM (*Laser Obstacle Avoidance and Monitoring*), voltado para aeronaves de asa rotativa usuais, mas integrado a um sistema de aeronave remotamente pilotada com outros sistemas para formar o DAA (11). Ele separa a capacidade de detectar e desviar entre cooperativo e não cooperativo, sendo que a função é separada em três passos, predição da trajetória futura da plataforma, cálculo das potenciais colisões com os obstáculos detectados e a geração de uma serie de trajetórias para desvio.

Do ponto de vista do sistema, o avião é representado como corpo rígido com controle de rolagem até um ângulo máximo de inclinação, e com base na identificação dos obstáculos são modelados volumes de incerteza nesse mapa tridimensional no qual cada obstáculo é envolvido por um volume elipsoidal que representa erros de detecção e rastreamento com margem de segurança. Para selecionar a melhor das trajetórias geradas, o algoritmo tenta otimizar uma função de custo que é dependente do tempo de evasão, consumo de combustível e a distância até a elipse de desvio e os pesos de cada uma das variáveis, que mudam conforme o comportamento do obstáculo detectado

Por fim, embora o trabalho de Ramasamy, Gardi e Sabatini inclua análises de otimização de trajetórias e incerteza por meio de formulações tensoriais, o presente estudo restringe-se à revisão das arquiteturas e análise de seus perigos funcionais, sem abordar formalmente os aspectos de otimização matemática. Em suma, interpreta-se que a arquitetura aqui proposta é um passo a mais quando comparado com a análise do sistema anterior. A quantidade de sensores e o auxilio de um sistema colaborativo preenche os gaps que unicamente uma câmera e um LiDAR não conseguiriam, como o uso de radares, sensores acústicos e câmeras termais para se ter visão mesmo fora de condições VMC ou em maiores distâncias (RAMASAMY; GARDI; SABATINI, 2015).

Ainda na literatura apresentada por Sabatini, mas agora com Moore e Hill, o terceiro trabalho revisado discute como aumentar a segurança da navegação por GNSS em aeronaves remotamente pilotadas por meio de um sistema embarcado capaz de identificar com antecedência quando o sinal de navegação está se degradando para função de DAA. Em vez de depender apenas de sistemas de correção baseados em solo ou satélite, os autores propõem o uso de informações dos próprios sensores da aeronave para gerar alertas preventivos e avisar o piloto remoto ou o piloto automático de que a navegação pode estar prestes a falhar (SABATINI; MOORE; HILL, 2014).

A arquitetura do DAA apresentado é muito semelhante ao trabalho avaliado anteriormente, também de Sabatini. Ele combina diferentes sensores e técnicas de rastreamento para prever conflitos e gerar manobras de desvio. A contribuição central do artigo é mostrar que, ao combinar o DAA com o sistema de integridade do GNSS, é possível escolher manobras que não apenas evitem a colisão, mas que também garantam que a aeronave mantenha navegação confiável durante toda a manobra, algo essencial para aeronaves que dependem do GNSS.

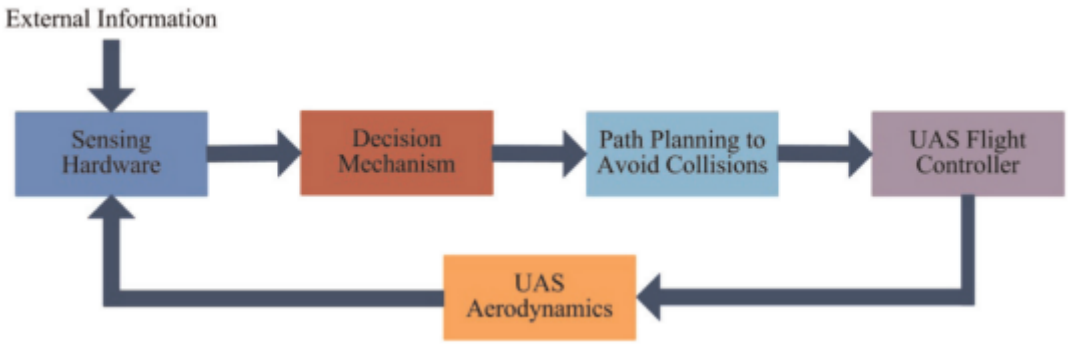
Por fim, os autores apresentam simulações com diferentes cenários de tráfego aéreo, mostrando que a integração dos dois sistemas possibilita respostas seguras e eficientes mesmo em situações complexas. O sistema integrado consegue identificar riscos a tempo, propor rotas alternativas e manter a qualidade da navegação, reforçando seu potencial para permitir que aeronaves remotamente pilotadas operem de forma mais segura em espaços aéreos compartilhados com aviação tripulada (SABATINI; MOORE; HILL, 2014).

Agora, seguindo para trabalhos de revisão de sistemas de DAA, a revisão conduzida por Yu e Zhang em 2015 apresenta um panorama amplo sobre tecnologias de DAA. Eles destacam que, a medida que drones passam a dividir o espaço aéreo com aeronaves tripuladas, torna-se indispensável que as aeronaves possuam sistemas capazes de perceber o ambiente, identificar riscos e reagir de forma autônoma — funções tradicionalmente desempenhadas por pilotos humanos. A publicação também resume as principais tecnologias disponíveis para detectar outras aeronaves e obstáculos, dividindo-as entre soluções cooperativas (como ADS-B e transponders) e não cooperativas (como câmeras, radares, sensores infravermelhos e LIDAR).

De maneira geral, os autores explicam que cada tecnologia apresenta vantagens e limitações em custo, alcance, condições climáticas e tipo de objeto detectável, reforçando que sistemas de DAA normalmente combinam múltiplos sensores. Além disso, o artigo apresenta, de forma acessível, as estratégias usadas para tomar decisões e planejar rotas seguras, mostrando que há diversos métodos capazes de calcular desvios seguros, desde regras lógicas até técnicas de otimização e algoritmos.

No final, os autores discutem desafios ainda abertos, como operar com confiabilidade em condições climáticas adversas, lidar com incertezas do ambiente e garantir respostas rápidas o suficiente para evitar colisões. Eles apontam também direções futuras, incluindo maior integração entre sensores, algoritmos mais robustos e sistemas totalmente autônomos capazes de atuar com um nível de segurança equivalente ao da aviação tripulada. Assim, o artigo funciona como uma síntese atualizada do estado da arte em DAA, servindo como referência introdutória para essa tecnologia (YU; ZHANG, 2015).

Figura 7 – Diagrama Funcional Genérico de Yu e Zhang (2015)



Fonte: (YU; ZHANG, 2015)

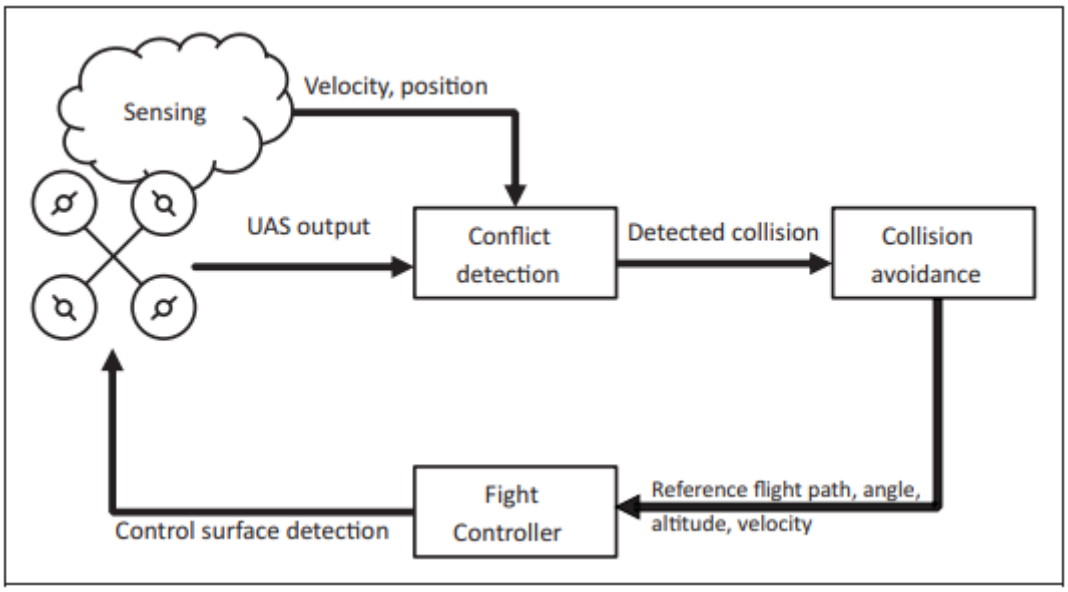
A revisão apresentada por Skowron et al, também oferece um panorama abrangente e acessível sobre o estado da arte em sistemas de DAA. Sua revisão destaca como o uso de drones se expandiu rapidamente em aplicações como inspeções, agricultura de precisão, mapeamento e busca e salvamento, e que a maior parte dessas operações ocorrem em cenário BVLOS. Para que se mantenha a segurança, do ponto de vista dos autores, é indispensável que os drones desenvolvam a capacidade de "ver e evitar" obstáculos de forma semelhante ao que pilotos humanos fazem na aviação tripulada.

A revisão apresenta, de forma geral, as principais tecnologias de detecção disponíveis. Os autores também distinguem entre métodos cooperativos, que dependem que outras aeronaves transmitam sua posição (como ADS-B), e métodos não cooperativos, que usam sensores próprios do drone, como câmeras, radares, LiDAR, sensores acústicos ou infravermelho. Para cada tecnologia são apresentadas vantagens e limitações em alcance, custo, peso, consumo de energia e desempenho em diferentes condições climáticas. O artigo mostra ainda que não existe um sensor único capaz de atender todas as necessidades; por isso, as soluções tendem a combinar várias tecnologias, conclusão semelhante do trabalho de Yu e Zhang.

Por fim, o texto analisa tendências e desafios do setor, observando que ainda não existe um sistema comercial totalmente autônomo e universal para DAA. Limitações de sensores, custos, requisitos regulatórios e necessidade de grande poder computacional ainda são barreiras importantes. Mesmo assim, os autores destacam avanços promissores na miniaturização de hardware, no desenvolvimento de algoritmos e na adoção de plataformas embarcadas mais potentes, sugerindo um futuro no qual drones possam operar com maior autonomia e segurança em espaços aéreos compartilhados (SKOWRON et al., 2019).

A última revisão, apresentada por Merei et al, descreve o avanço das técnicas de DAA para drones. Nela, é apresentada diferentes abordagens existentes, classificando métodos segundo o tipo de sensor

Figura 8 – Diagrama Funcional Genérico de Skowron et al (2019)

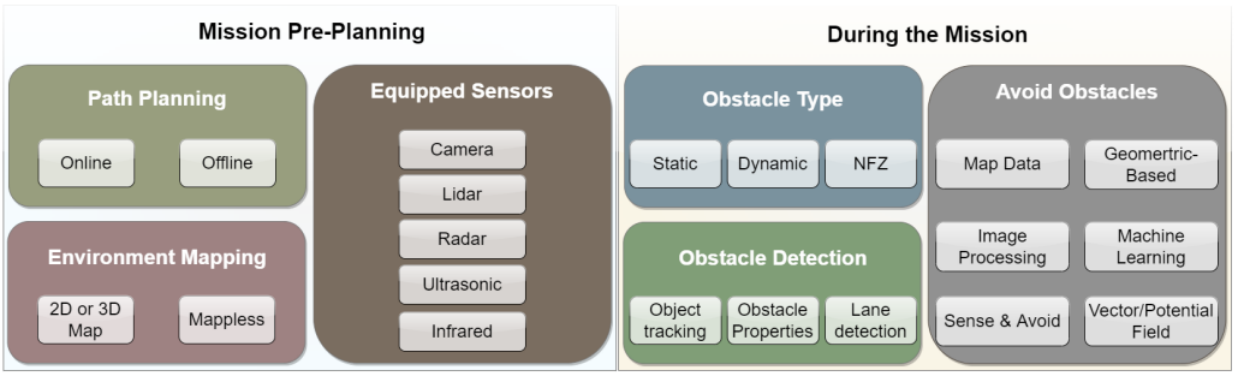


Fonte: (SKOWRON et al., 2019)

utilizado, o modo como o drone percebe o ambiente e as estratégias empregadas para gerar caminhos seguros. Novamente são exemplificados sensores como câmeras, LiDAR, radares, ultrassônicos e sistemas de visão estereoscópica. De maneira geral, a literatura mostra que nenhum sensor isolado é capaz de lidar com todos os cenários, reforçando a necessidade do sistema ser multissensorial. Além disso, o artigo apresenta métodos de planejamento que vão desde soluções geométricas simples até estratégias baseadas em inteligência artificial, reforçando que diferentes missões demandam combinações distintas de técnicas.

Ao final, os autores apontam como desafios ainda existentes operar em ambientes dinâmicos, lidar com múltiplos obstáculos simultaneamente, reduzir o consumo de energia e integrar NFZs de forma eficiente no planejamento. O estudo conclui que, embora haja grandes avanços tecnológicos, ainda existe espaço para melhorar a robustez e a adaptabilidade desses sistemas, especialmente para permitir voos totalmente autônomos e seguros em cenários complexos(MEREI et al., 2025).

Figura 9 – Componentes de Missão Generalizados para um DAA de acordo com Merei et al (2025)



Fonte: (MEREI et al., 2025)

4 MATERIAIS E MÉTODOS

4.1 PROCESSO

Como o trabalho tem como objetivo simular um ciclo inicial de desenvolvimento de um sistema foi utilizado como referência um sistema de DAA de uma aeronave voltada para mobilidade aérea urbana. Para isso, foi utilizado o contexto em nível de maturidade 4 de acordo com a visão de Goodrich e Theodore ((GOODRICH; THEODORE, 2021)), e publicado pela NASA, no qual o processo de tomada de decisão passa a ter maior efetivo dos sistemas automáticos como suporte para tomada de decisão do piloto. Além disso, para definir o objetivo de *safety* com o ambiente regulatório, absorveu-se a base de requisitos publicada pela EASA e a concepção operacional do UAM Nacional publicada pelo DECEA.

Além do mais, a metodologia seguiu principalmente como base o processo de desenvolvimento conforme definido na ARP 4754, para desenvolvimento do sistema, e ARP 4761, para análise de *safety* do sistema. Conforme definido nas normas, foram embasados os requisitos do sistema na forma de operação definida pelo DECEA do documento PCA 351-7 considerando UML-4, requisitos de certificação com base na SC-VTOL publicada pela EASA, e para requisitos funcionais, a ASTM F3442-25. No geral, com base na definição para desenvolvimento de sistemas da ARP4754, o processo para criação da arquitetura final com a aplicação do FHA será:

1. Definição do CONOPS da Aeronave (UML-4 / PCA 351-7)
2. Definição do CONOPS do Sistema (ASTM F3442-25)
3. Derivação dos requisitos regulatórios e funcionais do sistema
4. Criação da arquitetura do sistema
5. Aplicação do FHA (ARP 4761)
6. Proposta de arquitetura do sistema com as considerações de *safety*

E, para aplicar o FHA com a metodologia apresentada na ARP 4761 para a realização do mesmo será utilizado o seguinte roteiro de questionamentos.

1. Quais são as funções primárias do sistema?
2. Quais são as funções decompostas das funções primárias?
3. O que pode resultar caso ocorra perda de função anunciada, perda de função não anunciada, desempenho enganoso ou atraso na função?
4. Qual o nível de severidade do risco?
5. Como podemos mitigar o risco associado à essa condição de falha?

4.2 LIMITAÇÕES

Em suma, como já citado ao longo da fundamentação teórica, existem extrapolações de conceitos e limitações dentro do escopo desse trabalho. Do ponto vista regulatório, o principal é que o arcabouço SC-VTOL não foi criado para UAM em larga escala. Está sendo usado como o início da base de requisitos de certificação para aeronaves de pequeno porte com capacidade de VTOL para até 9 passageiros e MTOM igual ou inferior a 5,700 kg, o que limita aderência total ao contexto UML-4. No entanto, por ser um mercado em formação, a utilização como referência inicial é apropriada, já que há diversas incertezas em relação a esse novo ambiente.

Também destaca-se novamente que o uso da ASTM F3442-25 como início para a avaliação de requisitos para eVTOL/UAM, ao invés da DO-365/396, é uma extrapolação da norma ASTM, voltada para aeronaves pequenas e sem a função de transporte de pessoas. Como dito no documento, ela é aplicada para aeronaves remotamente pilotadas com máxima dimensão de 8 m e velocidade menor que 185,2 km/h inseridas num ambiente de médio risco. Ou seja, não se aplicaria para locais onde aeronaves tripuladas voam de forma predominante com taxa de encontro frequente.

Ainda, por se tratar de um primeiro ciclo iterativo do desenvolvimento do sistema, a consideração apenas de falhas simples no FHA, ignorando combinações, é uma lacuna que deve ser avaliada dentro de um desenvolvimento real, que seguiria ciclos iterativos de anos de desenvolvimento até a implementação de software/hardware. Dentro desse mesmo escopo, ressalta-se que não foi analisado nenhum requisito de performance por não ser o escopo desse trabalho, já que o atendimento dos mesmos necessitaria de ensaios para se determinar as probabilidades de encontro dentro das regiões de análise, e necessitaria de diversos ciclos de desenvolvimento para sua validação. No geral, foram desenvolvidos os sistemas em alto nível olhando para funcionalidade, e não performance.

Sendo assim, análises mais quantitativas (PSSA, FTA etc.) para mostrar que os objetivos de probabilidade de falha são atendidos não foram aplicados nesse nível de desenvolvimento do sistema. Entretanto, em um ciclo de desenvolvimento real, é necessário aprofundar o desenvolvimento do sistema a fim de realizar essas análises para a definição dos componentes apropriado. Em suma, aqui o trabalho se voltará para a parte qualitativa do ciclo de desenvolvimento.

5 DESENVOLVIMENTO

5.1 CONOPS NO ESCOPO DE AERONAVE

Para iniciar o desenvolvimento, nesta seção será descrito o conceito de operação da aeronave eVTOL no contexto da Mobilidade Aérea Urbana (UAM), enquadrada em UML-4 conforme previsto na PCA 351-7. Nela adota-se o emprego de rotas aéreas entre vertiportos, em ambiente controlado por serviços UAM dedicados e oferecidos pelo PSU. O objetivo é definir como a aeronave realizaria a separação entre tráfegos cooperativos e não cooperativos e de que forma o sistema de DAA atuaria nesse contexto.

Considerando a publicação PCA 351-7, a aeronave opera em um volume de espaço aéreo dedicado à UAM, delimitado horizontalmente por geofences que definem as áreas reservadas para UAM e suas interfaces com outros espaços aéreos. Esse volume é definido como de risco médio conforme a ASTM F3442-25, para que assim possa se manter aplicável ao desenvolvimento, ou seja, uma região em que aeronaves tripuladas convencionais tendem a não operar de forma predominante, com exceção de helicópteros, aeronaves agrícolas ou operações específicas de baixa altura. Trata-se, em geral, de espaço aéreo sem ATC acima de uma altitude mínima típica de 500 ft AGL.

Dentro desse volume, são estabelecidas rotas aéreas entre vertiportos, com fluxos predominantemente estruturados (origens e destinos recorrentes) e procedimentos padronizados de decolagem, cruzeiro e aproximação. A altitude de operação é definida de forma flexível em função das trajetórias, da ocupação do espaço aéreo e dos requisitos de desconflito, não sendo tratada aqui como limite fixo do conceito de operação, mas como parâmetro gerenciado pela personalização daquele serviço de tráfego UAM.

A aeronave se enquadra na categoria SC-VTOL (básica ou avançada, conforme a missão considerada), com porte compatível com o transporte de passageiros em rotas urbanas ou interurbanas. O perfil típico de missão é a ligação entre dois vertiportos em ambiente interurbano, com baixa rotatividade de movimentos entre rotas. Diferentemente da aviação convencional, em que a separação entre aeronaves é provida:

- Diretamente pelo piloto, que mantém separação visual em condições VMC sob regras de voo visual (VFR); ou
- Pelo órgão ATC, responsável por prover a separação em voo por instrumentos (IFR),

No contexto UML-4, conforme a PCA 351-7, adota-se o conceito de Digital Flight Rules (DFR). Nestas regras:

- Não há dependência da garantia contínua de condições VMC ou IMC como pré-requisito para a operação, desde que os requisitos de consciência situacional e de separação estejam atendidos por meio de sistemas e serviços digitais;

- A consciência situacional do operador (piloto remoto ou tripulação a bordo) é suportada por sistemas automáticos de acompanhamento digital do tráfego e do espaço aéreo;
- A separação estratégica e tática é realizada de forma cooperativa por meio da troca de informações digitais padronizadas, reduzindo a necessidade de prestação de serviço de separação tradicional pelo ATC dentro do volume UAM.

Assim, o operador da aeronave deixa de depender exclusivamente da visão natural ou de instruções de um controlador para manter separação, passando a atuar em coordenação com um provedor de serviços UAM (PSU), responsável por consolidar e analisar as intenções de voo e estados de múltiplas aeronaves, de um o sistema de DAA, encarregado da detecção e mitigação de conflitos táticos, especialmente frente a tráfegos não cooperativos e de um sistema ACAS (*Airborne Colision Avoidance System*), como última barreira de segurança em caso de iminência de colisão.

No ambiente UAM, a mitigação do risco de colisão com outros usuários do espaço aéreo é estruturada em duas camadas complementares: desconflito em nível estratégico e nível tático. O primeiro ocorre antes da decolagem, a partir do compartilhamento e análise das intenções de voo de todas as aeronaves que pretendem operar no volume UAM. O PSU consolida essas intenções, gera reserva de intenção operacional (Operational Intent Reservation - OIR) e verifica conflitos potenciais, considerando desvios espaciais e temporais esperados. Ou seja, casos de aeronaves com mesma origem e destino no mesmo tempo; aeronaves com origens e destinos distintos, mas com interseções previstas de trajetória; aeronaves com origens distintas e mesmo destino, com convergência em um vertiporto no mesmo tempo; entre outros casos, seriam solucionados já em nível estratégico.

No entanto, a presença provável de objetos voadores não cooperativos (aeronaves que não aderem às regras UAM, pilotos maliciosos, aves, drones recreativos, etc.); obstáculos como postes, linhas de transmissão e outros que não seriam pegos no DSM, ficam como responsabilidade de desconflito a nível tático do sistema de DAA e do ACAS. Prevendo um conflito, o DAA emite correções prévias ao plano de voo, tais como ajustes de velocidade de cruzeiro, perfil de trajetória (rota, nível de voo, procedimentos de subida/descida), altitudes de passagem em pontos de navegação, ou horários de decolagem, chegada ou passagem por waypoints. Essas correções são implementadas pelo piloto, que aceita e executa o plano revisado antes do início do voo, reduzindo a probabilidade de encontros perigosos durante a missão.

Por fim, aqui será frisado que não é papel do sistema de DAA impedir uma atuação maliciosa do próprio piloto, mas aumentar a segurança operacional realizando desconflitos de trajetória em nível tático. Também não é sua responsabilidade realizar o desconflito quando há a iminência de colisão, sendo esse o papel do ACAS. O DAA atua quando ainda é possível realizar desvios de trajetória para manutenção da segurança operacional. Uma vez identificado o risco de conflito, o DAA computa e apresenta manobras de desconflito (variação de velocidade, alteração de trajetória lateral ou vertical, ajuste de tempo de passagem em pontos específicos), auxiliando o piloto a restaurar margens seguras de separação. De forma resumida:

- O PSU é responsável pela camada de desconflito preventivo estratégico, garantindo que, na medida do possível, o plano de voo submetido pela aeronave seja compatível com os demais

tráfegos e restrições do espaço aéreo UAM.

- O DAA atua na camada de desconflito tático, tratando conflitos residuais ou inesperados, especialmente com tráfegos não cooperativos, e fornecendo ao operador alertas e recomendações de manobra em tempo hábil para evitar a perda de separação.
- O ACAS representa a última barreira, acionada em caso de iminência de colisão, emitindo avisos de resolução (RA) que orientam manobras evasivas imediatas, devendo ser obedecidos pelo operador mesmo que em detrimento do plano de voo nominal.

Portanto, o CONOPS prevê que o operador irá interagir com essas três camadas por meio da cabine ou estação de controle remoto no longo prazo, mantendo responsabilidade final pela condução segura do voo em UML-4, mas fortemente apoiado por mecanismos automáticos de detecção, previsão e mitigação de conflitos.

5.2 CONOPS NO ESCOPO DE SISTEMA

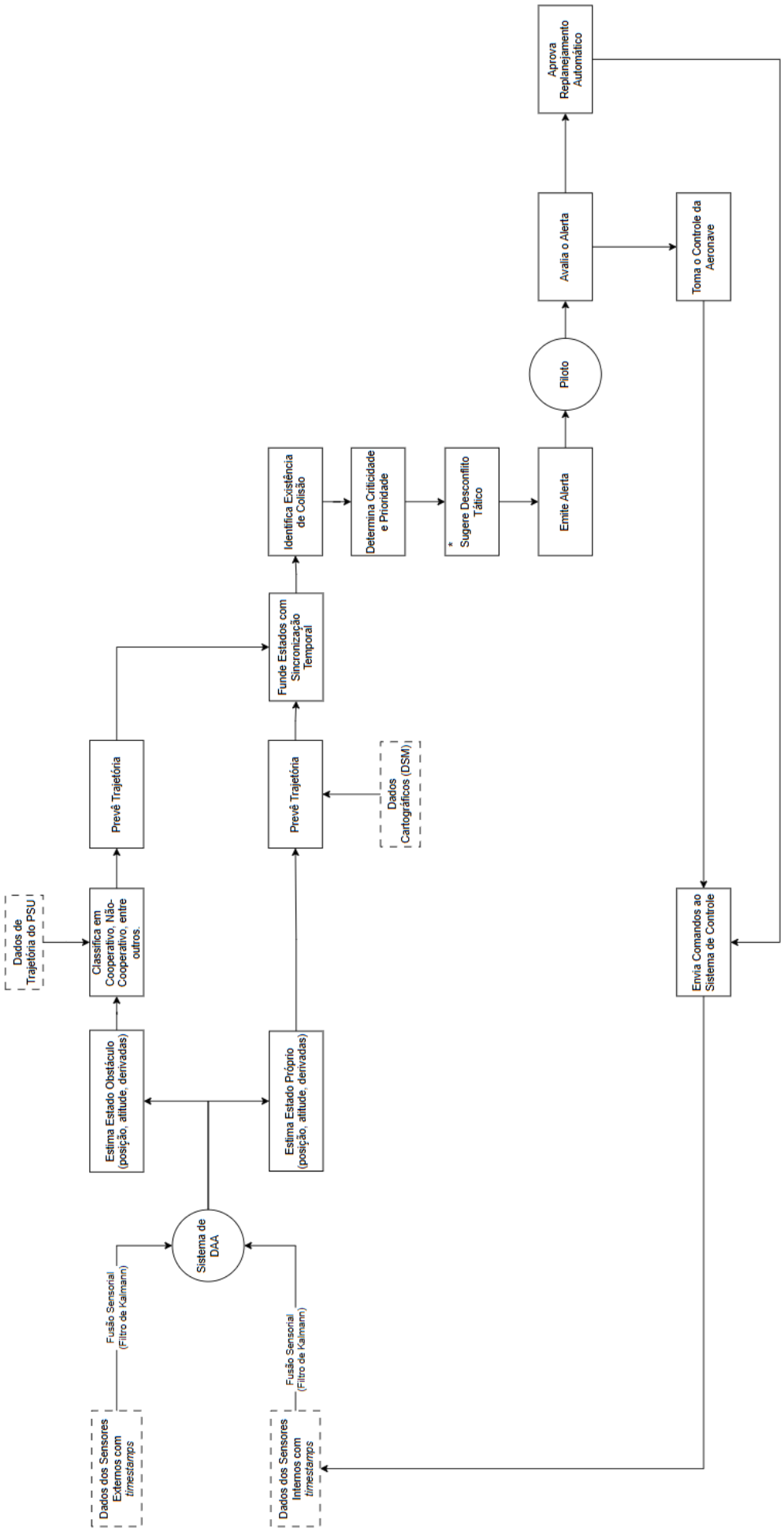
Dando continuidade ao processo de desenvolvimento, em resumo, do CONOPS no escopo de aeronave foi considerado o PCA 351-7 em UML 4, absorvendo a utilização de rotas aéreas entre vertiportos e o conceito de DFR para operação. Nesse caso, perde-se a restrição de garantia de condições VMC ou IMC e opera-se garantindo a consciência situacional dos pilotos através de sistemas automáticos de acompanhamento digital, com separação estratégica e tática, evitando a necessidade de segregação do espaço aéreo para operações dentro do ambiente UAM, apenas de outros ambientes (ex.: ATM e UTM). O operador da aeronave fará a separação de forma cooperativa através da troca de informações digitais, em substituição a procedimentos visuais baseados exclusivamente na visão ou na prestação de serviços de separação pelo ATC.

Com essa recapitulação em mente, agora será definida a concepção operacional do sistema de DAA embarcado nessa aeronave cuja forma de operação seguirá o que foi supracitado. Ela servirá de entrada para definir as funções necessárias para o sistema realizar a garantia de separação tática entre tráfegos cooperativos e não cooperativos, função de alto nível do sistema. Além disso, o sistema opera como camada intermediária entre o desconflito estratégico provido pelo PSU e a mitigação de colisão iminente de responsabilidade do ACAS. No geral, o sistema deverá assegurar consciência situacional contínua da aeronave, detectar riscos de perda de separação e propor ou executar manobras táticas baseado em mudança de trajetória, considerando restrições operacionais, ambientais e de desempenho, com referência as regras definidas pela PCA 351-7. Nesse contexto, o DAA representa a camada tática de mitigação e será responsável por:

- Monitorar continuamente o espaço aéreo ao redor da aeronave;
- Detectar tráfego cooperativo e não cooperativo;

- Detectar obstáculos fixos e móveis;
- Prever trajetórias e avaliar conflitos;
- Avaliar nível de risco de colisão;
- Gerar alertas e recomendações ao operador; e

Figura 10 – Diagrama Funcional do Sistema de DAA



Fonte: Elaborado pelo Autor

- Executar o replanejamento da trajetória, caso necessário.

A arquitetura funcional utilizada como base para este CONOPS está representada na 10. Essa arquitetura foi elaborada com base no entendimento da concepção operacional no nível da aeronave e podemos organizá-lo em seis grandes blocos funcionais que atendem as responsabilidades definidas para o sistema:

1. Aquisição e fusão sensorial (estado próprio e obstáculos).
2. Classificação e avaliação do ambiente (cooperativo, não cooperativo, estático e dinâmico).
3. Previsão de trajetórias e sincronização temporal.
4. Detecção e avaliação de conflitos (perda de separação e colisão).
5. Geração de resolução tática (manobras, replanejamento, prioridades).
6. Interação com piloto, ACAS e sistemas de controle.

Nas próximas seções, esses grandes grupos funcionais serão melhor desenvolvidos, sendo descrita cada etapa conforme essa separação em blocos funcionais.

5.2.1 Aquisição e Fusão de Dados Sensoriais

O DAA integra dados de sensores internos (ex.: GNSS, inercial, altímetro, câmeras, radar/lidar embarcado) e externos (ex.: ADS-B IN, radar terrestre, geofences, DSM, dados meteorológicos). Todos os dados deverão estar vinculados a um *timestamp*, permitindo uma fusão temporalmente coerente pelo filtro de Kalman. Por exemplo, o estimador pode combinar previsões do modelo dinâmico da aeronave com medições diretas do GNSS para obter a melhor estimativa possível do estado (posição, atitude e derivadas) minimizando incertezas vindo de ruído ou viés dos sensores. E, portanto, para que essa fusão seja confiável, o uso de *timestamps* é necessário. Cada dado deve ser alinhado temporalmente para refletir o instante exato em que foi medido, e assim propagar nas novas estimativas.

No caso de um sistema de DAA, no qual múltiplos sensores possuem diferentes frequências, latências e tempos de processamento, essa marcação temporal torna-se essencial para essa sincronização e compensação dos atrasos, evitando erros que poderiam distorcer a estimativa do estado próprio e do obstáculo, e, consequentemente, da previsão das trajetórias e detecção de colisão. Portanto, de modo geral, o sistema realiza a:

1. Estimativa do estado próprio (posição, velocidade, atitude e derivadas);
2. Medição direta e correção do estado próprio;
3. Percebimento de um obstáculo na sua visada;

4. Estimativa do estado de obstáculos (aeronaves cooperativas, não cooperativas, aves, drones, objetos móveis urbanos).
5. Correção do estado do obstáculo caso possível;

5.2.2 Classificação e Avaliação do Ambiente

Com base na aquisição dos dados anteriores e a estimativa do estado, o DAA classifica objetos percebidos em:

- Obstáculos fixos: edificações, torres, linhas de transmissão, relevo.
- Obstáculos móveis: aeronaves de baixa altitude, helicópteros, drones recreativos.
  - Cooperativos: aeronaves com ADS-B OUT, mensagens PSU válidas, considerações que permitem uma coordenação para o desconflito.
  - Não cooperativos: objetos detectados apenas pelos sensores cuja trajetória será apenas uma projeção, dependendo totalmente do "eu"para realizar o desconflito.

Isso ocorrerá através da retirada de características visual através de algoritmos de visão computacional, como deep learning, embarcados no sistema (TANG et al., 2023).

5.2.3 Previsão de Trajetórias e Sincronização Temporal

Para realizar o desconflito, o DAA deverá prever as trajetórias com base na estimativa dos estados. Essa trajetória deverá ser periodicamente atualizada conforme a proximidade de um obstáculo detectado. Portanto, com os dados da:

- Aeronave própria;
- Tráfegos cooperativos próximos detectados;
- Obstáculos móveis não cooperativos;
- Rotas e volumes autorizados pelo PSU.
- Geofences;
- Relevos e DSM;

O sistema de DAA deverá indicar trajetórias considerando um espaço tridimensional. Para isso, esses estados são inseridos em uma mapa de voxels ou malhas volumétricas, no qual um planejador de trajetória (como A*, D*, RRT*, entre outros) opera sobre para gerar caminhos viáveis. Além disso, também seria possível dar peso aos possíveis caminhos considerando as equações de movimento da aeronave, limites de aceleração, gradiente de subida e envelopes operacionais. A cada ciclo, previsões de movimento de tráfegos e obstáculos são atualizados permitindo ao planejador recalcular as trajetórias continuamente (YANG; XIONG; YAN, 2023).

5.2.4 Detecção e Avaliação de Conflitos

Com base nos dados percebidos pelos sensores, a classificação dos obstáculos e a projeção das trajetórias, o sistema será capaz de determinar como resultado a:

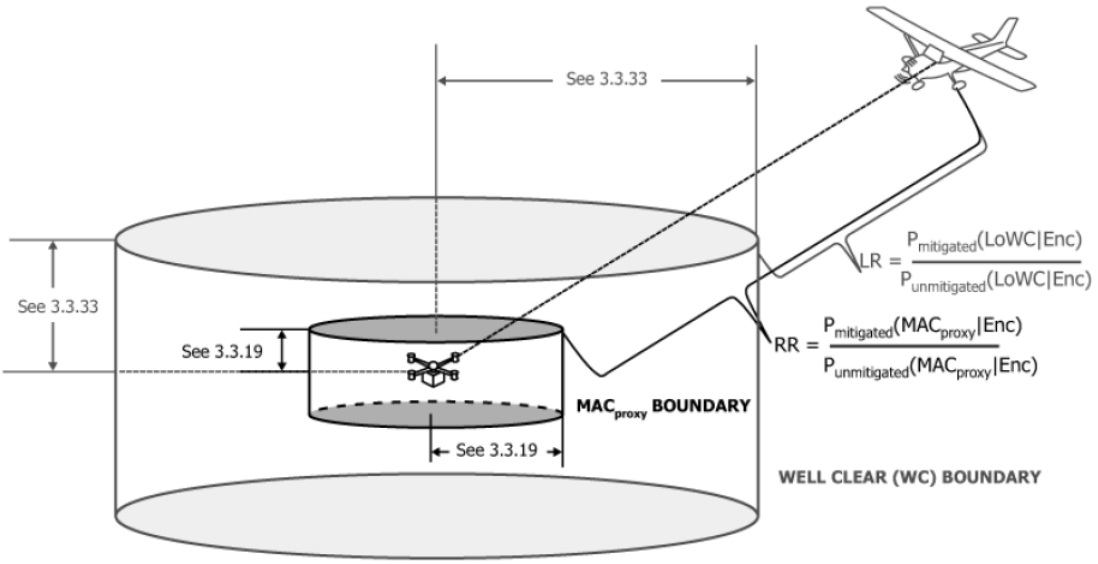
- Violação de geofences;
- Invasão iminente do "*well clear boundary*";
- Invasão iminente do "*MACproxy boundary*";
- Possibilidade de colisão com obstáculos fixos;
- Desvios próprios ou alheios do plano autorizado;

E, para manter a consciência situacional do piloto, deverá para cada conflito classificar segundo:

- **Tipo:** Cruzamento, colisão vertical, colisão lateral e limites espaciais excedido;
- **Criticidade:** Distância, tempo até colisão e incerteza da estimativa.

As considerações do “*well clear boundary*” e "*MACproxy boundary*"advêm da ASTM F3442. O primeiro é um cilindro tridimensional de proteção que define a margem mínima de separação entre o "eu"e qualquer outra aeronave. Segundo a ASTM, esse volume é escolhido para garantir que, sempre que as aeronaves estiverem fora dele, a probabilidade de colisão é suficientemente baixa. Internamente ao volume de “*well clear boundary*”, temos o "*MACproxy boundary*". Ele seria o limite de proximidade usado como proxy para risco de colisão, é onde se limita a atuação do DAA e do ACAS. Os valores físicos para ambos os limites não serão discutidos no escopo deste trabalho, pois como citado nas limitações, aqui não será discutido performance. Por fim, para melhor visualização abaixo é apresentada a 11 , que representa os conceitos citados.

Figura 11 – Limites de detecção para alertas (ASTM F3442)



Fonte: (ASTM INTERNATIONAL, 2021)

5.2.5 Geração de Resolução Tática

E, como última função automática do sistema, identificado um risco, o DAA gera opções de resolução para tomada de decisão do piloto. Essas resoluções podem variar de indicações de alteração na velocidade, trajetória lateral (desvio horizontal) ou altitude de operação. Todas as sugestões serão compatíveis com algumas restrições que irão variar conforme o nível do risco identificado. Essas restrições podem ser:

- Obstáculos fixos identificados
- Trajetórias de obstáculos móveis identificados
- Envelope de voo de segurança da aeronave
- Espaço aéreo definido (rotas e limites operacionais daquele espaço aéreo) e restrições de segurança do uso do espaço aéreo
- Geofences e restrições de otimização do uso do espaço aéreo

5.2.6 Interação com Piloto

Por fim, como dito anteriormente, em UML 4 as decisões são tomadas ainda pelo piloto, sendo que sistemas como DAA devem auxiliar na troca de informações entre aeronaves e no suporte à tomada de decisões assertivas. Portanto, as resoluções táticas são apresentadas ao operador com a criticidade

do conflito (distância, tempo até colisão, incerteza da estimativa) a recomendação de manobra e o prazo para execução. Com isso, o operador pode aprovar a sugestão replanejamento automático (modo colaborativo), ou assumir o controle manual, seguindo as orientações do DAA ou alterando para as regras de voo em VFR/IFR.

5.3 DEFINIÇÃO DE REQUISITOS

5.3.1 Requisitos de Certificação

Definida a forma de operação, agora levantaremos os pontos que devem ser levados em conta pelo viés da autoridade certificadora. Para essa análise foi usada como referência as requisitos publicados na base SC-VTOL, por ser uma análise multidisciplinar, é possível que existam mais correlações do que as aqui presente. Portanto, para retirar essa dúvida, abaixo serão apresentados explicitamente os requisitos que entendeu-se como relevantes para o desenvolvimento, sendo possível que novas necessidades apareçam conforme o aprofundamento do sistema.

Antes de finalizar, é válido levantar que existem requisitos referente a proteção contra descargas de alta tensão (VTOL.2515) e exposição a campos irradiados de alta intensidade (VTOL.2520). No entanto, são análises específicas e que exigem conhecimento especializado, fugindo da construção em alto nível do sistema, mas que deve ser levado em conta no desenvolvimento do sistema em níveis mais baixos.

5.3.2 Requisitos Funcionais

Seguindo o processo de desenvolvimento do sistema, com a definição do CONOPS agora é possível derivar os requisitos do sistema. Nesta seção serão apresentados o conjunto de requisitos funcionais que orientam o desenvolvimento do DAA aqui considerado. O objetivo deste levantamento é estruturar de forma explícita as capacidades que o sistema deve possuir para garantir todas as suas funções.

Além das funções centrais de percepção e previsão, os requisitos incluirão aspectos de avaliação de conflito, determinação de manobras de evasão, comunicação com o piloto e integração com outros sistemas aeronáuticos, como o PSU e o ACAS.

Por último, reforça-se que não serão discutidos requisitos de performance, já que o objetivo do trabalho é realizar um primeiro ciclo de desenvolvimento do sistema, definindo a lógica de operação do sistema. Entende-se que requisitos de performance aparecerão quando for necessário escolher modelos e números de série de componentes, em níveis mais baixos do desenvolvimento.

Tabela 1 – Requisitos SC-VTOL

ID	Interpretação
VTOL.2110	Define a necessidade de determinação dos envelopes de voo normal, operacional e limite.
VTOL.2135.a)	Define a necessidade da manobrabilidade da aeronave não exigir habilidade, nível de alerta ou força excepcional do piloto. Esse requisito só poderá ser avaliado em níveis mais baixos do desenvolvimento, mas é entendido como influente no DAA.
VTOL.2500.b)	Define a necessidade de adequação de forma que desempenhe sua função prevista dentro dos limites operacionais e ambientais para os quais a aeronave é certificada. Esse requisito só poderá ser avaliado em níveis mais baixos do desenvolvimento, mas é entendido como influente no DAA.
VTOL.2510.a)	Define a necessidade de se garantir que (1) cada condição de falha "*catastrophic*"seja extremamente improvável e não resulte de uma única falha; (2) cada condição de falha "*hazardous*"seja extremamente remota; e (3) cada condição de falha "*major*"seja remota. Esse requisito só poderá ser avaliado em níveis mais baixos do desenvolvimento, mas é entendido como influente no DAA.
VTOL.2510.c)	Define que para a categoria Avançada devem ser estabelecidas disposições para o monitoramento em serviço de equipamentos cuja falha possa ter consequências "*hazardous*"ou "*catastrophic*".
VTOL.2600.b)	Define que uma tripulação de voo qualificada deve conseguir monitorar as tarefas definidas e associadas às funções previstas e deve considerar erros da tripulação de voo que possam resultar em perigos adicionais.
VTOL.2605.c)	Define que informações sobre uma condição insegura de operação do sistema devem ser fornecidas ao membro da tripulação responsável por tomar a ação corretiva.
VTOL.2615.a)	Define que os sistemas instalados que fornecem ao membro da tripulação parâmetros de voo, navegação e do sistema de sustentação/propulsão devem fazê-lo: (1) apresentando de maneira que os membros da tripulação possam monitorar os parâmetros e suas tendências.

Fonte: (EUROPEAN UNION AVIATION SAFETY AGENCY (EASA), 2023)

Tabela 2 – Requisitos do Sistema

ID	Interpretação
DAA.001	O sistema deve detectar obstáculos estáticos com informações advindas dos sistemas de PSU
DAA.002	O sistema deve classificar obstáculos estáticos detectados através de visão computacional
DAA.003	O sistema deve interfacear com os sistemas de PSU para recebimento de dados do DSM e de aeronaves cooperativas
DAA.004	O sistema deve gerar um mapa de voxels com base nos obstáculos estáticos identificados e o DSM
DAA.005	O sistema deve detectar aeronaves cooperativas (ou seja, que transmitem posição/identificação) com informações advindas dos sistemas de PSU
DAA.006	O sistema deve detectar obstáculos móveis não-cooperativas com informações sensoriais
DAA.007	O sistema deve classificar obstáculos móveis cooperativos e não-cooperativos detectados através de visão computacional
DAA.008	O sistema deve acompanhar obstáculos que tenham atravessado a fronteira de "*well clear*"
DAA.009	O sistema deve estimar a trajetória de si próprio e das aeronaves sendo acompanhadas.
DAA.010	O sistema deve estimar o estado de aeronaves cooperativas (ou seja, que transmitem posição/identificação) com informações advindas dos sistemas de PSU e que tenham atravessado a fronteira de "*well clear*"
DAA.011	O sistema deve estimar o estado de obstáculos móveis não-cooperativas com informações sensoriais e que tenham atravessado a fronteira de "*well clear*"
DAA.012	O sistema deve determinar a possibilidade de conflito com uma probabilidade relacionada
DAA.013	O sistema deve identificar tipo de conflito (colisão lateral, colisão vertical, cruzamentos de rota, etc).
DAA.014	O sistema deve determinar uma manobra de evasão com base no tipo de conflito (colisão lateral, colisão vertical, cruzamentos de rota, etc) e no mapa de voxel gerado.
DAA.015	O sistema deve gerar alerta com a manobra de evasão para tomada de decisão do piloto com indicação de criticidade.
DAA.016	O sistema deve notificar o piloto com aviso visual e sonoro com indicação de criticidade.
DAA.017	O sistema deve ter interface com o sistema de controle para caso seja realizada uma manobra de evasão automaticamente.
DAA.018	O sistema deve associar o timestamp de todas as variáveis percebidas através dos sensores.
DAA.019	O sistema deve identificar caso um obstáculo tenha atravessado a fronteira de "MAC_{proxy}"
DAA.020	O sistema deve ter interface com o sistema ACAS para casos de conflito iminente.

Fonte: Elaborado pelo Autor

5.4 DESCRIÇÃO DO SISTEMA INICIAL

Com base nas discussões anteriores podemos definir então a seguinte arquitetura. O sistema deverá receber informações de posição e trajetória de outras aeronaves colaborativas e o DSM (Modelo Digital de Superfície) dos sistemas de gerenciamento de tráfego baseado em regras digitais de voo (DFR). Para receber informações de aeronaves cooperativas, mas participantes de outro espaço aéreo, o sistema também terá em sua composição um ADS-B IN, para receber informações de transponders de outras aeronaves. Para a função de percepção, o sistema terá uma IMU (Inertial Measurement Unit), que pode ser alguma outra já dentro dos sistemas da aeronave. Essa unidade é responsável por dar as entradas do estado da própria aeronave, posição, atitude e derivadas. No entanto, como IMUs geralmente medem aceleração e velocidade angular, para obter os valores de velocidade, posição e atitude, o sinal desses sensores são integrados. Por conta disso, devido ao próprio viés do sensor, a integração do sinal para realizar as inferências devem ser corrigidas por uma medida direta. Portanto, isso justifica a utilização do magnetômetro, que apesar de uma precisão ruim, pode servir para avaliar o desvio das estimativas da IMU em relação à atitude, e do GNSS, que ocupa a mesma função do magnetômetro para a posição.

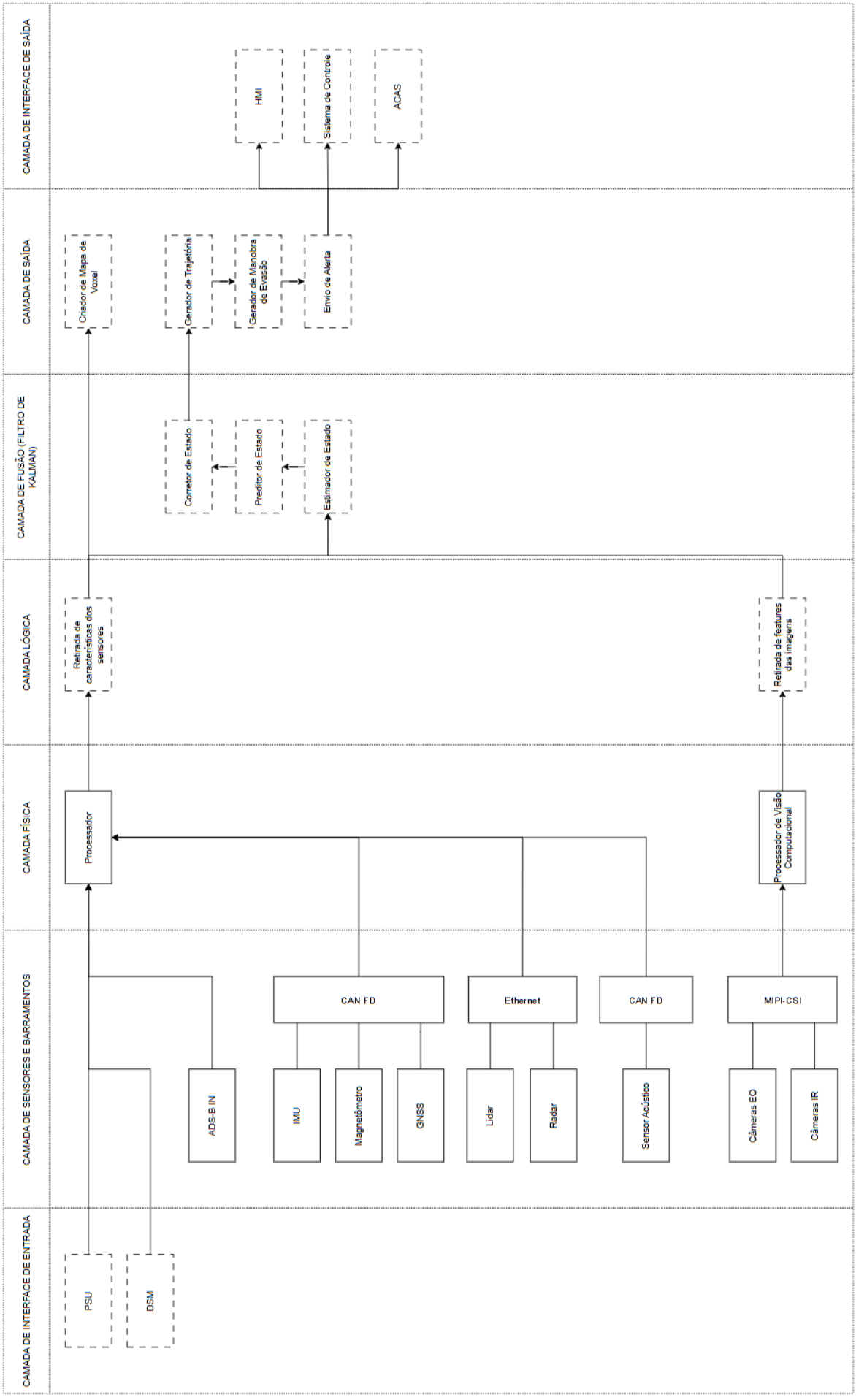
Para o sensoriamento do exterior, foi escolhido o conjunto de Lidar, Radar e sensor acústico para conseguir coletar diversas características do ambiente. Essa decisão foi arbitrária baseada na aborção das revisões realizadas para esses sistemas. Para classificação dos obstáculos, pretende-se utilizar um conjunto de câmeras eletro-ópticas e infravermelho, assim o sistema consegue a resolução oferecida pelo primeiro tipo, e o alcance e a independência de condições visuais do segundo. Além disso, as câmeras também conseguiram emitir alertas de aproximação, mesmo que mais imprecisos. Selecionados esses sensores, foi definido também o tipo de barramento para transmissão dos dados de cada um. Entende-se que para essa arquitetura é necessário garantir uma baixa latência e que seja possível ter um determinismo temporal. Sensores como IMU, câmeras e radares operam com taxas elevadas e exigem jitter mínimo, variação da latência, para evitar desalinhamento temporal durante a fusão e degradação da predição para assegurar precisão na propagação do estado e nas correções de atitude e posição. Além disso, é preciso uma largura de banda elevada, especialmente no caso de câmeras e Lidar. Por fim, mesmo antes de uma análise de *safety*, é importante já garantir que não haverá problemas na transmissão dos dados com detecção de erros (CRC, frame checking) e tolerância a ruídos, que serão solucionados por essas formas de barramento.

Sendo assim, foi avaliada a possibilidade de se utilização de CAN FD, Ethernet e MIPI-CSI. O primeiro é utilizado em aplicações aeronáuticas e tem prioridade determinística de mensagens e elevada imunidade a ruídos. Mesmo que a largura de banda seja limitada, é suficiente para sensores de navegação como IMUs, GNSS, etc. Sua principal limitação reside na incapacidade de transportar fluxos de alta resolução, como dados de câmeras. Já o Ethernet foi estabelecido pela capacidade de transmissão de grande volume de dados (1 Gbps), como câmeras EO/IR, Lidar e radares. Ele garante entrega temporal com jitter pequeno e sincronização, mas seu maior diferencial é a capacidade de banda. Por fim, o MIPI-CSI é empregado em câmeras, permitindo taxas de transmissão da ordem de gigabits por segundo com latência extremamente baixa. Entretanto, é suscetível a ruído eletromagnético

e limitado em distância, sendo necessário estar próximo do processador. No entanto, isso pode ser solucionado na arquitetura com um processador dedicado às imagens, que também garante a possibilidade de processamento do grande volume de dados que todo o conjunto de câmeras exigiria, sendo esse o caminho seguido no trabalho.

Em suma, para IMU, Magnetômetro, GNSS e o sensor acústico, determinou-se o CAN FD como barramento. Para Lidar e Radar, devido ao maior volume de dados, escolheu-se o Ethernet como barramento. E, para as câmeras, optou-se pelo MIPI-CSI por ser um barramento próprio para processamento de imagens, garantindo que não se perca resolução, sendo necessária apenas a provisão de um processador dedicado por conta da susceptibilidade a ruídos com a distância. Dessa forma, já se garante a segurança na transmissão de dados dos sensores para os processadores. Neles, ocorrerão todas as fases de camada lógica, de fusão e de saída, com as interfaces com outros sistemas e com o piloto pelo HMI (*Human Machine Interface*). Para diferenciar as camadas de hardware e software, foi utilizada a legenda de linha contínua para o primeiro, e linha tracejada para o segundo. Abaixo, na 12, temos a representação da arquitetura descrita.

Figura 12 – Arquitetura Inicial do Sistema de DAA



Fonte: Elaborado pelo Autor

5.5 AVALIAÇÃO DOS PERIGOS FUNCIONAIS

Usualmente o FHA é apresentado em forma de tabela, contudo, uma tabela única não seria o formato mais adequado para apresentação aqui neste trabalho. Tendo em vista que o desenvolvimento em si é sua confecção, e o formato de tabela é benéfico para facilitar a visualização e correlação entre as informações, aqui será apresentado dividindo-a em partes separadas. Com isso em mente, o FHA será apresentado separando as funções em primárias e decompostas, das funções decompostas serão apresentados as consequências de cada um dos tipos de falha e, por último, a severidade atrelada a cada uma dessas falhas com a forma de mitigação desses riscos em relação a alterações na arquitetura. Ainda, devido a extensão, optou-se pela apresentação das tabelas de falhas e de severidade com forma de mitigação nos apendices A e B, respectivamente. Sendo assim, as funções primárias do sistema, derivadas do diagrama funcional e consideradas para a análise são apresentadas abaixo.

Tabela 3 – Funções Primárias

ID	Função
F1	Detectar obstáculos
F2	Prever conflito futuro
F3	Gerar forma de resolução do conflito
F4	Alertar o piloto

Fonte: Elaborado pelo Autor

E, as funções decompostas das primárias são:

Antes de prosseguir, é necessário explicar que, para padronizar a identificação das falhas avaliadas no FHA, adotou-se uma codificação composta pelo tipo de falha, o prefixo da função afetada e o identificador específico da função decomposta. Assim, a codificação segue o formato T-FX.Y, em que T representa o tipo de falha, sendo PF-A (Perda de Função Anunciada), PF-NA (Perda de Função Não Anunciada), DE (Desempenho Enganoso) ou AT (Atraso na Função), e FX.Y indica a função decomposta correspondente.

Por exemplo, o identificador PF-NA-F1.1 refere-se à perda não anunciada da função de classificação de obstáculos, enquanto DE-F2.6 representa um desempenho enganoso na função de estimação do estado de obstáculos móveis. Essa padronização garante rastreabilidade, consistência documental e clareza ao longo das diversas etapas do processo respeitando a ARP-4761. Em suma, a associação direta de cada falha ao elemento funcional onde ocorre facilitará a correlação dos perigos com a identificação da severidade e forma de mitigação. Portanto, no apêndice A são apresentadas as falhas, perigos e seus efeitos no sistema na aeronave e na tripulação, caso existam.

Após a indicação das falhas, perigos e efeitos, é possível ter clareza da severidade do que pode ocorrer. Por ser uma classificação subjetiva, mesmo que baseada no entendimento da autoridade reguladora, é esperado que a classificação seja constantemente discutida e atualizada. No escopo do trabalho não houve discussão dentro de um grande grupo multidisciplinar, sendo a visão exclusiva do autor. Nesse contexto, tentou-se seguir uma lógica nas formas de mitigação considerando três tipos, mudanças no hardware, adição de procedimentos e mudanças no software. Dessa forma foi possível

Tabela 4 – Funções Decompostas

ID	Função
F1.1	Classificar obstáculos
F1.2	Detectar aeronaves cooperativas
F1.3	Detectar aeronaves não cooperativas
F1.4	Detectar outros obstáculos móveis
F1.5	Detectar obstáculos estáticos
F2.1	Aquisição de dados sensoriais
F2.2	Sincronização de dados sensoriais
F2.3	Fusão de dados sensoriais
F2.4	Estimar estado de si próprio
F2.5	Estimar trajetória de si próprio
F2.6	Estimar estado dos obstáculos móveis
F2.7	Estimar trajetória dos obstáculos móveis
F2.8	Gerar mapa com obstáculos estáticos
F2.9	Identificar probabilidade de conflito
F2.10	Identificar invasão na fronteira de "*well clear*"
F2.11	Identificar invasão na fronteira de "MAC_{proxy}"
F3.1	Classificar tipo de conflito
F3.2	Determinar manobra de resolução do conflito
F3.3	Gerar comandos necessários para realizar manobra de resolução do conflito
F4.1	Apresentação das informações no display do HMI

Fonte: Elaborado pelo Autor

alinhar as expectativas de alteração na arquitetura sem uma análise quantitativa da probabilidade de falha. Para aquelas falhas cuja severidade foi declarada como Hazardous ou Catastrophic presou-se pela adição de redundâncias que aumentassem a integridade ou disponibilidade da função. Caso fossem falhas cuja severidade é Minor ou Major, apenas foram adicionados procedimentos e mudanças no software. No apêndice B são apresentadas as relações de falha, severidade e forma de mitigação.

6 RESULTADO

A análise de perigos funcionais do sistema de DAA resultou em um total de setenta e seis eventos com severidade relevante, distribuídos conforme a classificação estabelecida pela SC-VTOL. Desses, sete perigos foram classificados como Minor e trinta e seis como Major, refletindo condições que podem degradar levemente a operação e demandam ações procedimentais por parte da tripulação ou modos degradados de funcionamento do sistema. Outros dezessete perigos receberam classificação Hazardous, indicando eventos capazes de comprometer a segurança de forma relevante, exigindo mitigação por meio de mecanismos independentes de alerta e aprimoramentos nas interfaces homem-máquina.

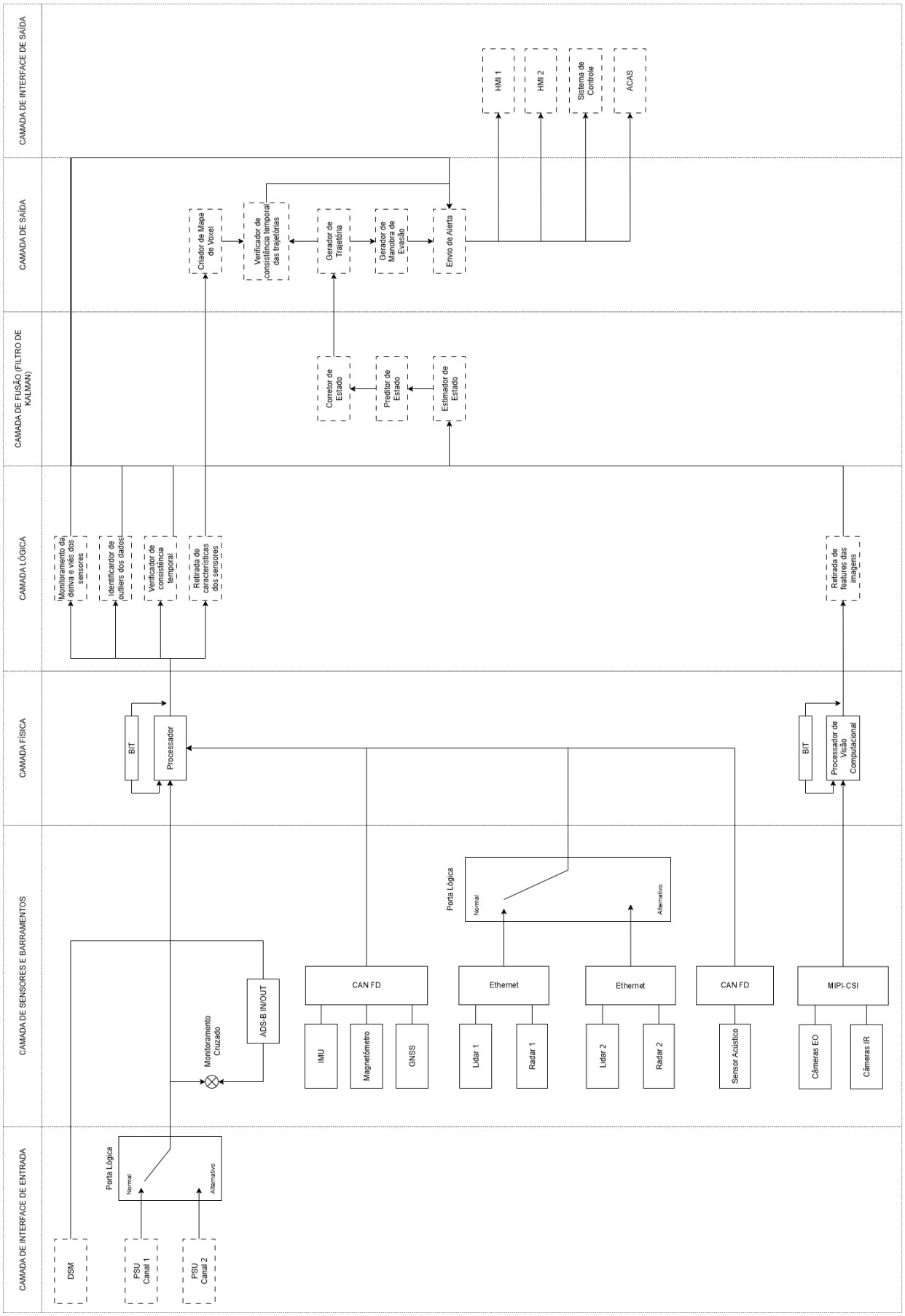
Por fim, dezesseis perigos foram classificado como Catastrophic, associado à possibilidade de comandos inadequados de resolução, cuja falha pode levar à perda da aeronave caso não mitigada; esse caso demandou mudanças de hardware na arquitetura e monitoramento de função. Esse conjunto de classificações orientou diretamente as modificações implementadas na arquitetura final do sistema, assegurando que os riscos identificados fossem reduzidos a níveis aceitáveis dentro do processo de safety.

Com a definição de severidade e forma de mitigação, agora é possível reavaliar a arquitetura inicialmente definida. Para facilitar o entendimento da análise realizada, abaixo serão enumeradas as modificações surgidas da análise de perigos funcionais relacionados a Hardware e Software. Para software, serão focadas as novas funções surgidas do FHA, portanto, não será representado limitações ou outras alterações no Software que não as supracitadas. Portanto, as formas de mitigação que resultaram em alteração da arquitetura são:

- **Hardware**
    1. Adição de ADS-B OUT para outras aeronaves conseguirem identificar a aeronave.
    2. Redundância de comunicação com PSU.
    3. Monitoramento cruzado entre PSU e ADB-B IN;
    4. Redundância dos sensores externos que coletam características do ambiente;
    5. Monitoramento cruzado entre detecção on-board e base externa (DSM vinda do PSU)
    6. HMI redundante (displays independentes)
- **Software**
    1. Monitoramento de deriva e viés dos sensores.
    2. Monitoramento cruzado entre diversos sensores que percebem diferentes características do ambiente;
    3. Verificação de consistência entre carimbos de tempo
    4. Monitoramento de consistência das trajetórias geradas.

Sendo assim, após realizar essas modificações na arquitetura inicial do sistema de DAA, obtemos a nossa arquitetura final como na 13.

Figura 13 – Arquitetura Final do Sistema de DAA



Fonte: Elaborado pelo Autor

Dessa forma, pode-se avaliar que as principais mudanças de sistemas foram:

- A adição de um segundo canal de comunicação com o PSU e uma porta lógica para aumento de disponibilidade
- Monitoramento cruzado entre dados recebidos do PSU com os detectados pela ADS-B IN
- Arquitetura dupla para radar e lidar com porta lógica para aumento de disponibilidade
- BIT nos processadores para rotinas de verificação do funcionamento das funções de software
- Adição das funções de identificação de outliers nos dados, verificação de consistência temporal dos dados e monitoramento da deriva e viés dos dados dos sensores sensores na camada lógica
- Função de verificação de consistência temporal das trajetórias geradas para alertas de perda da função
- HMI redundante para apresentação dos dados ao piloto

Com isso, podemos voltar para os requisitos definidos para o sistemas e indicar a forma de cumprimento dos mesmos, como mostrada na tabela abaixo.

Tabela 5 – Demonstração de Meio de Cumprimento dos Requisitos

ID	Meio de Cumprimento
VTOL.2110	Os envelopes exigidor por esse requisito serão integrados na função de geração de trajetória.
VTOL.2510.c)	Função de monitoramento adicionada na camada lógica da arquitetura para todas as funções.
VTOL.2600.b)	Indicação de alertas e apresentação de informações no HMI para garantia do cumprimento do requisito.
VTOL.2605.c)	Indicação de alertas e apresentação de informações no HMI para garantia do cumprimento do requisito.
VTOL.2615.a)	Indicação de alertas e apresentação de informações no HMI para garantia do cumprimento do requisito.
DAA.001	O sistema recebe as informações do PSU através de dois canais redundantes
DAA.002	O sistema terá processamento embarcado baseado em deep learning para classificação de objetos nas imagens do conjunto de câmeras EO/IR na aeronave.
DAA.003	O sistema recebe as informações do PSU através de dois canais redundantes
DAA.004	Indicado na camada lógica a geração de mapa de voxels com base nos obstáculos estáticos identificados pelos sensores e o DSM recebido pelo PSU
DAA.005	O sistema recebe as informações do PSU através de dois canais redundantes

ID	Meio de Cumprimento
DAA.006	O sistema tem integrado um conjunto de sensores para detecção de características do ambiente sendo eles um Radar, um Lidar e um sensor acústico que são processados na camada lógica para retirada de características do ambiente.
DAA.007	O sistema terá processamento embarcado baseado em deep learning para classificação de objetos nas imagens do conjunto de câmeras EO/IR na aeronave.
DAA.008	O sistema tem integrado um conjunto de sensores para detecção de características do ambiente sendo eles um Radar, um Lidar e um sensor acústico que são processados na camada lógica para retirada de características do ambiente.
DAA.009	O sistema gerará um mapa de voxels aplicando metodologias de identificação de rotas baseado nesse mapa. Não foi definido um algoritmo específico podendo ser explorada essa ideia futuramente.
DAA.010	O sistema terá implementado na camada lógica um filtro de Kalman que fará a função de fundir os dados para melhor identificação dos estados e consequente predição das trajetórias
DAA.011	O sistema terá implementado na camada lógica um filtro de Kalman que fará a função de fundir os dados para melhor identificação dos estados e consequente predição das trajetórias
DAA.012	O sistema determinará a colisão através da posição da aeronave com um buffer de separação associado à precisão da medida. Essa precisão levará em conta o monitoramento da deriva e do viés dos dados coletados. Quanto mais longe do centro da esfera probabilística da posição, maior a probabilidade do conflito
DAA.013	A função será implementada na camada lógica do sistema, tendo como entrada a trajetória do obstáculo e a predição da sua própria, indicando como o conflito poderia ocorrer dependendo de como essas trajetórias se cruzam no mapa de voxels
DAA.014	Tendo o envelop de operação da aeronave como entrada e o seu modelo dinâmico, o sistema determinará como realizar as manobras para desconflito das trajetórias. Como são funções simples como alterar a velocidade, altitude de voo, ou direção, entende-se que a tecnologia seria o equivalente a sistemas de piloto automático atuais.
DAA.015	Todos os eventos indicados no FHA serão monitorados, seja em nível de hardware ou software, e deverão aparecer no HMI 1 e HMI 2.
DAA.016	Todos os eventos indicados no FHA serão monitorados, seja em nível de hardware ou software, e deverão aparecer no HMI 1 e HMI 2.
DAA.017	A interface com o sistema de controle é prevista na arquitetura mas não definida nesse estudo.
DAA.018	A captura do timestamp deve ser feita considerando o relógio interno dos sensores. O processamento desses dados são considerados na camada lógica da arquitetura.

ID	Meio de Cumprimento
DAA.019	O sistema tem integrado um conjunto de sensores para detecção de características do ambiente sendo eles um Radar, um Lidar e um sensor acústico que são processados na camada lógica para retirada de características do ambiente.
DAA.020	A interface com o ACAS é prevista na arquitetura mas não definida nesse estudo.

Fonte: Elaborado pelo Autor

7 CONCLUSÃO

A realização deste trabalho permitiu simular um ciclo inicial de desenvolvimento de um sistema de Detect and Avoid (DAA) para aplicação em aeronaves eVTOL operando no nível UML-4 de maturidade UAM. Foram utilizados princípios de engenharia de sistemas com a ARP4754 e a ARP4761 para estruturar uma arquitetura conceitual, identificar perigos funcionais e propor mitigações compatíveis com os requisitos regulamentares e funcionais de sistemas críticos.

Partindo do CONOPS definido pelo PCA 351-7 e dos requisitos funcionais extrapolados da ASTM F3442, desenvolveu-se um conjunto de funções, resultando em uma arquitetura inicial que consegue sustentar a função de DAA em ambiente urbano. A aplicação do FHA revelou os perigos funcionais associados às funções do sistema e permitiu classificá-los conforme os níveis de severidade estabelecidos pela SC-VTOL. Com base nessa análise, estratégias de mitigação foram propostas, incluindo redundâncias, monitoramento contínuo, mecanismos de integridade e alternativas de intervenção humana.

Os resultados reforçam que operações UAM em nível UML-4 exigem sistemas de DAA para possibilitar esse cenário de operação, com forte ênfase em integridade e disponibilidade. A análise demonstrou que a combinação de múltiplos sensores, fusão de dados, mecanismos de monitoramento cruzado e previsões de trajetória são elementos essenciais para compor soluções aptas nos quais tráfegos cooperativos e não cooperativos coexistem sem um controlador centralizado.

Reforça-se que mesmo assim, algumas limitações do trabalho devem ser reconhecidas. A utilização da ASTM F3442-25 como base para requisitos funcionais demonstrou-se apropriada para uma atuação de cenários com densidade de tráfego média, como UML-4. No entanto, para ter uma solução escalável, ainda se enxerga como necessáia a utilização de normas mais apropriadas para aeronaves tripuladas, como a DO-365/396. O FHA foi limitado a falhas simples, sem contemplar falhas múltiplas ou combinações de falhas dependentes, baseando-se na premissa de que se deve evitar pontos de falha únicos.

Por fim, não foram realizadas análises quantitativas, como FTA ou PSSA. Sendo ambas apropriadas para futuros trabalhos relacionados, uma vez que isso demandaria ensaios, simulações e dados de operação. Com essas análises, possibilitaria-se a determinação de performance do sistema, e, com o amadurecimento do desenvolvimento do sistema, seria possível garantir o atendimento das probabilidades exigidas para cada severidade de falha. A arquitetura deste trabalho foi desenvolvida apenas em alto nível, sem derivação para níveis inferiores ou avaliações de integração com outros sistemas. Portanto, recomenda-se como próximos passos:

- Prosseguir com análises quantitativas, incluindo PSSA, FTA e cálculos probabilísticos.
- Expandir o FHA para considerar falhas combinadas.
- Avaliar arquiteturas alternativas, com foco na relação entre custo, peso e confiabilidade.
- Explorar a interface do DAA com sistemas cooperativos, como ACAS e serviços PSU.

- Derivar requisitos de níveis inferiores, incluindo DAL, interfaces físicas e requisitos de *security*.

Em suma, a arquitetura que emergiu do processo demonstrou-se coerente com as exigências inicialmente definidas, oferecendo uma base sólida para iterações futuras. Embora limitada ao escopo conceitual, a análise permitiu compreender os desafios associados à certificação e operação segura de eVTOLs no contexto UML-4, contribuindo para o entendimento sistêmico das necessidades de segurança, redundância e desempenho em ambientes aéreos altamente integrados, alcançando seus objetivos.

REFERÊNCIAS

ASTM INTERNATIONAL. **Standard Specification for Detect and Avoid System Performance Requirements**. West Conshohocken: ASTM, 2021.

EUROPEAN UNION AVIATION SAFETY AGENCY (EASA). **Special condition for VTOL aircraft (SC-VTOL)**. Cologne: EASA, 2023.

FEDERAL AVIATION ADMINISTRATION. **14 CFR Part 1 – Definitions and abbreviations**. Washington, DC: U.S. Government Publishing Office, 2023.

FEDERAL AVIATION ADMINISTRATION. **14 CFR Part 21 – Certification procedures for products and articles**. Washington, DC: U.S. Government Publishing Office, 2023.

GOODRICH, K. H.; THEODORE, C. R. Description of the NASA urban air mobility maturity level (UML) scale. Langley Research Center, 2021.

KI, M.; CHA, J.; LYU, H. Detect and avoid system based on multi sensor fusion for uav. In: **2018 INTERNATIONAL CONFERENCE ON INFORMATION AND COMMUNICATION TECHNOLOGY CONVERGENCE (ICTC)**. [S.l.: s.n.], 2018. p. 1107–1109. ISSN 2162-1233.

MEREI, A. et al. A survey on obstacle detection and avoidance methods for uavs. **Drones 2025**, MDPI, v. 9, n. 203, 2025.

MOIR, I.; SEABRIDGE, A.; JUKES, M. **Civil Avionics Systems**. Chichester, West Sussex - Inglaterra: John Wiley Sons, Ltd, 2013.

RAMASAMY, S.; GARDI, A.; SABATINI, R. A laser obstacle avoidance system for manned and unmanned aircraft detect-and-avoid. In: **16th AUSTRALIAN INTERNATIONAL AEROSPACE CONGRESS – AIAC 16**. [S.l.: s.n.], 2015.

SABATINI, R.; MOORE, T.; HILL, C. Gnss avionics-based integrity augmentation for rpas detect-and-avoid applications. In: **4th Australasian Unmanned Systems Conference - ACUS 2014**. [S.l.: s.n.], 2014.

SAE INTERNATIONAL. **CERTIFICATION CONSIDERATIONS FOR HIGHLY-INTEGRATED OR COMPLEX AIRCRAFT SYSTEMS**. Warrendale: SAE, 1996.

SAE INTERNATIONAL. **GUIDELINES AND METHODS FOR CONDUCTING THE SAFETY ASSESSMENT PROCESS ON CIVIL AIRBORNE SYSTEMS AND EQUIPMENT**. Warrendale: SAE, 1996.

SKOWRON, M. et al. Sense and avoid for small unmanned aircraft systems: Research on methods and best practices. **Journal of Aerospace Engineering**, Sage Journals, v. 233, n. 16, 2019.

TANG, G. et al. A survey of object detection for uavs based on deep learning. **Remote Sensing 2023**, MDPI, v. 16, n. 149, 2023.

YANG, Y.; XIONG, X.; YAN, Y. Uav formation trajectory planning algorithms: A review. **Drone 2023**, MDPI, v. 7, n. 62, 2023.

YU, X.; ZHANG, Y. Sense and avoid technologies with applications to unmanned aircraft systems: Review and prospects. **Progress in Aerospace Sciences**, Elsevier, v. 74, p. 152–166, 2015.

APÊNDICE A – FALHAS, PERIGOS E EFEITOS

Tabela 6 – Falhas, perigos e efeitos

ID da Falha	Perigo	Efeito na Aeronave	Efeito na Tripulação
PF-A-F1.1	Perda da classificação de obstáculos.	Função de classificação desativada; DAA opera apenas com detecção bruta; Manobras de resolução menos otimizadas.	Maior carga de interpretação de alertas.
PF-NA-F1.1	Perda da classificação de obstáculos.	Função de classificação desativada; DAA opera apenas com detecção bruta; Manobras de resolução menos otimizadas.	Identificação tardia do aumento de carga na interpretação dos alertas.
DE-F1.1	Classificação enganosa de obstáculos.	Indicação de resoluções plausíveis porém erradas; Lógica de priorização distorcida.	Tripulação deve realizar o desconflito de forma manual, aumentando a carga de trabalho.
AT-F1.1	Classificação tardia de obstáculos.	Sem efeito na segurança	Sem efeito na segurança.
PF-A-F1.2	Perda de detecção de aeronaves cooperativas.	Módulo cooperativo é desativado; Sistema usa apenas sensores não cooperativos; Menor antecipação de conflitos com tráfego cooperativo.	Tripulação depende mais de informações sensoriais.
PF-NA-F1.2	Falha silenciosa na detecção de aeronaves cooperativas.	Módulo cooperativo é desativado; Sistema usa apenas sensores não cooperativos; Aeronave pode cruzar rotas de outros tráfegos sem alerta; Menor antecipação de conflitos com tráfego cooperativo.	Tripulação depende mais de informações sensoriais.

ID da Falha	Perigo	Efeito na Aeronave	Efeito na Tripulação
DE-F1.2	Dados cooperativos enganoso.	Posições/velocidades cooperativas distorcidas; aeronave cooperativa identificada de forma diferente entre sensores e PSU; Manobras indicadas contra tráfego inexistente ou em direção a tráfego real.	Sobrecarga cognitiva e perda de confiança no sistema.
AT-F1.2	Atraso em dados cooperativos.	Atualizações cooperativas chegam defasadas; Aeronave cooperativa identificada de forma diferente entre sensores e PSU; Aeronave reage a posição "antiga" do tráfego.	Sobrecarga cognitiva e perda de confiança no sistema.
PF-A-F1.3	Perda de detecção de aeronaves não cooperativas.	Intrusos não cooperativos podem se aproximar sem qualquer alerta.	Tripulação deverá realizar manobras de emergência
PF-NA-F1.3	Falha silenciosa na detecção de não cooperativos.	Intrusos não cooperativos podem se aproximar sem qualquer alerta.	Possível surpresa em encontro visual de última hora com alto risco de colisão.
DE-F1.3	Detecção enganosa de intrusos.	Gera alvos falsos ou omite alvos reais; Manobras desnecessárias ou ausência de manobra em conflito real.	Sobrecarga cognitiva e perda de confiança no sistema.
AT-F1.3	Detecção tardia de não cooperativos.	Alvos reais são detectados tardiamente; Distância para iniciar evasão é reduzida.	Tripulação recebe alertas com menos tempo para reagir.
PF-A-F1.4	Perda de detecção de outros obstáculos móveis.	Intrusos não cooperativos podem se aproximar sem qualquer alerta.	Tripulação deverá realizar manobras de emergência
PF-NA-F1.4	Falha silenciosa na detecção de outros móveis.	Intrusos não cooperativos podem se aproximar sem qualquer alerta.	Possível surpresa em encontro visual de última hora com alto risco de colisão.

ID da Falha	Perigo	Efeito na Aeronave	Efeito na Tripulação
DE-F1.4	Detecção enganosa de outros obstáculos móveis.	Gera alvos falsos ou omite alvos reais; Manobras desnecessárias ou ausência de manobra em conflito real.	Sobrecarga cognitiva e perda de confiança no sistema.
AT-F1.4	Atraso na detecção de outros móveis.	Alvos reais são detectados tardiamente; Distância para iniciar evasão é reduzida.	Tripulação recebe alertas com menos tempo para reagir.
PF-A-F1.5	Perda de detecção de obstáculos estáticos.	Mapa estático fica incompleto; Rota pode cruzar edificações, torres e estruturas não mapeadas.	Tripulação deve tomar o controle da operação assim que anunciado
PF-NA-F1.5	Falha silenciosa na detecção de estáticos.	Mapa estático fica incompleto; Rota pode cruzar edificações, torres e estruturas não mapeadas.	Surpresa e falta de tempo para procedimentos de emergência.
DE-F1.5	Mapa estático enganoso.	Estruturas são mostradas em posições erradas ou omitidas; Trajetórias supostamente seguras levam a colisão com obstáculos.	sobrecarga cognitiva e perda de confiança no sistema.
AT-F1.5	Atraso na atualização de estáticos.	Mapa demora a refletir obstáculos detectados; Rota é planejada com base em ambiente defasado.	Percepção tardia de alterações em rotas e procedimentos.
PF-A-F2.1	Perda anunciada de aquisição sensorial.	Canais sensoriais são desligados; sistema entra em modo degradado.	Tripulação informada de degradação e reverte para procedimentos alternativos.
PF-NA-F2.1	Falha silenciosa na aquisição sensorial.	Dados nulos ou corrompidos alimentam fusão e estimadores.	Tripulação guiada por informações erradas.
DE-F2.1	Desempenho enganoso na aquisição.	Dados enviesados são fornecidos; Erros sistemáticos em todas as funções subsequentes.	Dificuldade em perceber incoerência sem indicação de falha.

ID da Falha	Perigo	Efeito na Aeronave	Efeito na Tripulação
AT-F2.1	Atraso na aquisição de dados.	Amostras chegam com jitter significativo; Estimativas dinâmicas inconsistentes no tempo.	Alertas intermitentes confundindo a tripulação.
PF-A-F2.2	Perda de sincronização anunciada.	Módulo de fusão é desabilitado por falta de sincronismo; Sistema perde benefícios de fusão multisensor.	Tripulação recebe apenas informações parciais.
PF-NA-F2.2	Falha silenciosa na sincronização.	Dados defasados são combinados como se estivessem alinhados; Trajetórias estimadas apresentam desvios significativos.	Tripulação recebe indicação de conflitos incoerentes com o visual.
DE-F2.2	Sincronização enganosa.	Timestamps errados parecem válidos; Posições/velocidades calculadas com base em instantes incorretos.	Tripulação recebe indicação de conflitos incoerentes com o visual.
AT-F2.2	Atraso na sincronização.	Timestamps errados parecem válidos; Posições/velocidades calculadas com base em instantes incorretos.	Tripulação recebe indicação de conflitos incoerentes com o visual.
PF-A-F2.3	Perda anunciada de fusão sensorial.	Erros sistemáticos em todas as funções subsequentes.	Tripulação deve iniciar procedimentos alternativos.
PF-NA-F2.3	Falha silenciosa de fusão.	Fusão gera resultados inconsistentes sem sinalizar falha; Cenário sintético não condiz com ambiente real.	Tripulação é levada a interpretar cenário enganoso.
DE-F2.3	Fusão enganosa.	Fusão gera resultados inconsistentes sem sinalizar falha; Cenário sintético não condiz com ambiente real.	Tripulação é levada a interpretar cenário enganoso.

ID da Falha	Perigo	Efeito na Aeronave	Efeito na Tripulação
AT-F2.3	Atraso na fusão.	Fusão gera resultados inconsistentes sem sinalizar falha; Cenário sintético não condiz com ambiente real.	Tripulação é levada a interpretar cenário enganoso.
PF-A-F2.4	Perda anunciada de estimação de "si".	Estimador próprio é desativado; sistema depende de dados menos precisos do GNSS; Previsão de conflitos perde base confiável.	Tripulação informada de degradação; pode aumentar vigilância.
PF-NA-F2.4	Falha silenciosa na estimação do próprio.	Estado próprio errado é propagado para todo o sistema; Trajetórias relativas são avaliações erradas.	Tripulação é levada a interpretar cenário enganoso.
DE-F2.4	Estimação enganosa do próprio.	Estado próprio errado é propagado para todo o sistema; Trajetórias relativas são avaliações erradas.	Tripulação é levada a interpretar cenário enganoso.
AT-F2.4	Atraso na estimação do próprio.	Estado próprio errado é propagado para todo o sistema; Trajetórias relativas são avaliações erradas.	Tripulação é levada a interpretar cenário enganoso.
PF-A-F2.5	Perda anunciada de previsão de trajetória própria.	Função de predição do próprio é desativada; Sistema age menos preditivo e mais reativo.	Tripulação recebe menos apoio na antecipação de conflitos.
PF-NA-F2.5	Falha silenciosa na previsão do próprio.	Sistema assume implicitamente que trajetória futura não é relevante; Conflitos que dependem da projeção não são antecipados.	Tripulação não é alertada com antecedência.
DE-F2.5	Predição enganosa da trajetória própria.	Trajetórias futuras são calculadas incorretamente; Manobras de resolução baseadas em projeções erradas.	Tripulação executa comandos acreditando em rota segura.
AT-F2.5	Atraso na predição da trajetória própria.	Predição é gerada com atraso; Janela temporal de decisão é encurtada.	Tripulação é pressionada a tomar decisões mais rápidas.

ID da Falha	Perigo	Efeito na Aeronave	Efeito na Tripulação
PF-A-F2.6	Perda anunciada da estimação do estado externo	Função de acompanhar alvos móveis é desligada; Sistema só tem informações instantâneas dos obstáculos.	Dificuldade em prever cruzamentos e aproximações.
PF-NA-F2.6	Perda não anunciada da estimação do estado externo	Função de acompanhar alvos móveis é desligada; Sistema só tem informações instantâneas dos obstáculos.	Dificuldade em prever cruzamentos e aproximações.
DE-F2.6	Estimativa enganosa de obstáculos móveis.	Velocidades/direções estimadas incorretamente; Sistema indica afastamento quando há aproximação (ou vice-versa).	Dificuldade em prever cruzamentos e aproximações.
AT-F2.6	Atraso na estimativa de obstáculos móveis.	Atualizações do estado de alvos são lentas; Posição/velocidade usadas nas decisões estão defasadas.	Dificuldade em prever cruzamentos e aproximações.
PF-A-F2.7	Perda anunciada de predição de trajetória dos obstáculos móveis.	Preditivo de obstáculos móveis é desativado; Sistema não antecipa cruzamentos futuros, apenas situação atual.	Tripulação recebe apenas indicação “instantânea” de proximidade.
PF-NA-F2.7	Falha silenciosa na predição de obstáculos móveis.	Preditivo de obstáculos móveis é desativado; Sistema não antecipa cruzamentos futuros, apenas situação atual.	Tripulação é surpreendida por alertas tardios.
DE-F2.7	Predição enganosa de trajetória de obstáculos móveis.	Projeções erram posição futuro do obstáculo; Evasões podem ser adiadas ou não executadas.	Tripulação é surpreendida por alertas tardios.
AT-F2.7	Atraso na predição de móveis.	Trajetórias futuras são computadas tardiamente; Margem de tempo para manobra diminui.	Tripulação precisa reagir com urgência.

ID da Falha	Perigo	Efeito na Aeronave	Efeito na Tripulação
PF-A-F2.8	Perda anunciada de geração de mapa estático.	Mapa de voxels não é gerado/atualizado; DAA não usa representação de obstáculos estáticos.	Tripulação não conta com representação confiável do ambiente.
PF-NA-F2.8	Falha silenciosa na geração do mapa.	Mapa incompleto é usado como se estivesse correto; Trajetórias passam por áreas perigosas não representadas.	Perigos locais não são evidentes na HMI.
DE-F2.8	Mapa de voxels enganoso.	Mapa incompleto é usado como se estivesse correto; Trajetórias passam por áreas perigosas não representadas.	Perigos locais não são evidentes na HMI.
AT-F2.8	Atraso na geração do mapa.	Mapa incompleto é usado como se estivesse correto; Trajetórias passam por áreas perigosas não representadas.	Perigos locais não são evidentes na HMI.
PF-A-F2.9	Perda anunciada de identificação de probabilidade de conflito.	Sistema não calcula probabilidade ou determina possibilidade de conflito	Tripulação recebe alertas menos claros quanto à urgência.
PF-NA-F2.9	Falha silenciosa na probabilidade de conflito.	—	—
DE-F2.9	Probabilidade de conflito enganosa.	Valores sub ou superestimados são apresentados; Manobras podem ser disparadas por falsos conflitos ou omitidas em conflitos reais.	Tripulação reage a criticidades equivocadas.
AT-F2.9	Atraso na identificação da probabilidade.	Valores sub ou superestimados são apresentados; Manobras podem ser disparadas por falsos conflitos ou omitidas em conflitos reais.	Tripulação reage a criticidades equivocadas.

ID da Falha	Perigo	Efeito na Aeronave	Efeito na Tripulação
PF-A-F2.10	Falha na detecção de well clear.	Sistema não gera gatilho para mudança de modo.	Tripulação não é avisada que separação mínima foi infringida.
PF-NA-F2.10	Falha silenciosa na detecção de well clear.	Sistema não gera gatilho para mudança de modo.	Tripulação não é avisada que separação mínima foi infringida.
DE-F2.10	Detecção enganosa de well clear.	Sistema não gera gatilho para mudança de modo.	Tripulação não é avisada que separação mínima foi infringida.
AT-F2.10	Atraso na detecção de well clear.	Sistema não gera gatilho para mudança de modo.	Tripulação não é avisada que separação mínima foi infringida.
PF-A-F2.11	Falha na detecção de MAC	Sistema não gera gatilho para mudança de modo.	Tripulação não é avisada que separação mínima foi infringida.
PF-NA-F2.11	Falha silenciosa na detecção de MAC.	Condição iminente de colisão não é reconhecida.	Tripulação dependente da atenção para resolução do conflito.
DE-F2.11	Alerta de MAC enganoso.	Geração de alertas críticos falsos ou errados; Condição iminente de colisão não é reconhecida.	Tripulação dependente da atenção para resolução do conflito.
AT-F2.11	Atraso na detecção de MAC.	Condição iminente de colisão não é reconhecida.	Tripulação dependente da atenção para resolução do conflito.
PF-A-F3.1	Perda anunciada da classificação do tipo de conflito.	Sistema não distingue entre conflitos laterais, verticais etc; Resolução não é gerada para o tipo de conflito.	Tripulação recebe apenas indicação genérica de conflito.
PF-NA-F3.1	Essa função não falharia de forma não anunciada	—	—
DE-F3.1	Classificação enganosa do tipo de conflito.	Sistema informa tipo errado de conflito; Pode realizar manobra que piora ou não resolve o conflito	Tripulação é levada a executar ação inadequada.

ID da Falha	Perigo	Efeito na Aeronave	Efeito na Tripulação
AT-F3.1	Atraso na classificação do tipo de conflito.	Sistema informa tipo errado de conflito; Pode realizar manobra que piora ou não resolve o conflito	Tripulação é levada a executar ação inadequada.
PF-A-F3.2	Perda anunciada de determinação da manobra.	Conflito é reconhecido, mas nenhuma manobra é proposta; DAA não oferece comando ou sugestão de resolução.	Tripulação precisa decidir manobra sem apoio do sistema.
PF-NA-F3.2	Essa função não falharia de forma não anunciada	—	—
DE-F3.2	Manobra de resolução enganosa.	Manobra calculada é incorreta ou insegura; Aeronave é guiada para rota que piora ou não resolve o conflito.	Tripulação é levada a executar ação inadequada.
AT-F3.2	Atraso na determinação da manobra.	Manobra calculada é incorreta ou insegura; Aeronave é guiada para rota que piora ou não resolve o conflito.	Tripulação é levada a executar ação inadequada.
PF-A-F3.3	Perda anunciada de geração de comando de manobra.	Comandos não são enviados ao controle automático; Sistema não executa automaticamente a manobra proposta.	Tripulação precisa intervir manualmente.
PF-NA-F3.3	Falha silenciosa na geração de comandos.	Comandos não são enviados ao controle automático; Sistema não executa automaticamente a manobra proposta.	Tripulação precisa intervir manualmente.
DE-F3.3	Comandos de manobra enganosos.	Comandos errados são enviados (direção/valor); Aeronave executa manobra errônea.	Tripulação pode perder controle situacional diante de reação inesperada.

ID da Falha	Perigo	Efeito na Aeronave	Efeito na Tripulação
AT-F3.3	Atraso na geração de comandos.	Comandos chegam tardiamente ao controle; Manobra ocorre fora do momento ideal.	Tripulação percebe resposta atrasada e pode tentar compensar.
PF-A-F4.1	Perda anunciada de apresentação da manobra ao piloto.	Manobra não é exibida, apesar de calculada; Interface HMI deixa de apresentar orientação.	Piloto não recebe indicação de manobra recomendada.
PF-NA-F4.1	Falha silenciosa na apresentação da manobra.	Manobra não é exibida, apesar de calculada; Interface HMI deixa de apresentar orientação.	Piloto não recebe indicação de manobra recomendada.
DE-F4.1	Apresentação enganosa da manobra.	HMI mostra manobra diferente da calculada ou necessária;	Piloto pode tomar decisão errada confiando na HMI.
AT-F4.1	Atraso na apresentação da manobra.	Manobra é mostrada ao piloto com atraso.	Piloto precisa reagir rapidamente, com maior carga de trabalho.

Fonte: Elaborado pelo Autor

APÊNDICE B – CLASSIFICAÇÃO DE SEVERIDADE E FORMAS DE MITIGAÇÃO DAS FALHAS DE DAA

Tabela 7 – Classificação de severidade e formas de mitigação das falhas de DAA

ID da Falha	Severidade	Tipo da Mitigação	Forma de Mitigação
PF-A-F1.1	Minor	Procedimento, Software	Procedimento para preparar a tripulação a manter a consciência situacional sem a classificação do obstáculo; Verificação em nível de software para testar o funcionamento da função.
PF-NA-F1.1	Major	Procedimento	Procedimentos para operação em modo degradado com maior separação mínima; Treinamento para constante atenção do piloto mesmo sem o auxílio do sistema.
DE-F1.1	Major	Procedimentos	Treinamento da tripulação para priorizar informação bruta em caso de dúvida.
AT-F1.1	Sem efeito na segurança	—	—
PF-A-F1.2	Minor	Procedimento, Software	Procedimentos de aumento de vigilância visual e separações; Indicação clara de perda do canal cooperativo no HMI
PF-NA-F1.2	Hazardous	Hardware, Procedimento	Adição de ADS-B OUT para outras aeronaves conseguirem identificar; Redundância de comunicação com PSU; Canal de comunicação direta com outras aeronaves cooperativas através do PSU.
DE-F1.2	Hazardous	Hardware, Procedimentos	Adição de ADS-B OUT para outras aeronaves conseguirem identificar; Redundância de comunicação com PSU; Monitoramento cruzado entre PSU e ADB-B IN; Canal de comunicação direta com outras aeronaves cooperativas através do PSU.
AT-F1.2	Major	Software	Limitação máxima de atraso aceitável com descarte de mensagens muito defasadas; Monitoramento de latência com aviso de operação degradada no HMI.

ID da Falha	Severidade	Tipo da Mitigação	Forma de Mitigação
PF-A-F1.3	Major	Procedimentos, Software	Procedimentos de limitação de operação e mudança para regra de voo visual ou instrumental; Indicação de saúde de cada sensor no HMI;
PF-NA-F1.3	Catastrophic	Hardware, Procedimento	Redundância dos sensores externos que coletam características do ambiente; Detecção redundante com o ACAS; Piloto deve manter condição visual durante todo o voo para casos de emergência;
DE-F1.3	Catastrophic	Hardware, Procedimentos	Monitoramento cruzado entre sensores que percebem características do ambiente; Treinamento para decisão de recusar manobras "não plausíveis".
AT-F1.3	Hazardous	Procedimento, Software	Buffer de separação do voo leva em conta a maior latência do sistema;
PF-A-F1.4	Major	Procedimentos, Software	Procedimentos de limitação de operação e mudança para regra de voo visual ou instrumental; Indicação de saúde de cada sensor no HMI.
PF-NA-F1.4	Catastrophic	Hardware, Procedimento	Redundância dos sensores externos que coletam características do ambiente; Detecção redundante com o ACAS; Piloto deve manter condição visual durante todo o voo para casos de emergência;
DE-F1.4	Catastrophic	Hardware, Procedimentos	Monitoramento cruzado entre sensores que percebem características do ambiente; Treinamento para decisão de recusar manobras "não plausíveis".
AT-F1.4	Major	Procedimento, Software	Buffer de separação do voo leva em conta a maior latência do sistema;
PF-A-F1.5	Major	Procedimentos	Bases de dados estáticas redundantes e verificadas (terrain, DSM, geofences); indicação clara de indisponibilidade; procedimentos de altitudes mínimas conservadoras.

ID da Falha	Severidade	Tipo da Mitigação	Forma de Mitigação
PF-NA-F1.5	Catastrophic	Hardware, Procedimento	Monitoramento cruzado entre detecção on-board e base externa (DSM vinda do PSU) para determinar funcionamento; Procedimentos de aproximação/voo baixo como auxílio do DAA apenas se verificado seu funcionamento pelo piloto.
DE-F1.5	Catastrophic	Hardware, Procedimentos	Monitoramento cruzado entre detecção on-board e base externa (DSM vinda do PSU) para determinar coerência; Instruções para abortar manobra em caso de discrepância com cenário visual.
AT-F1.5	Major	Procedimento, Software	Garantia de atualização com janela segura antes de iniciar uma aproximação ou voo em baixa altitude; Indicação de atualização do mapa; Confirmação do piloto em relação a indicação de manobras para desconflito.
PF-A-F2.1	Major	Procedimentos, Software	Detecção e sinalização de perda com modo degradado explicitamente indicado; procedimentos de reconfiguração e eventual término de missão.
PF-NA-F2.1	Hazardous	Hardware, Procedimento, Software	Redundância para garantia de disponibilidade; Procedimentos pré-voo para verificar obstrução nos sensores; Alerta para o piloto de perda de função.
DE-F2.1	Catastrophic	Hardware, Procedimento, Software	Monitoramento cruzado entre os sensores para verificação da integridade; Calibração periódica; Monitoramento de deriva e viés.
AT-F2.1	Major	Software	Time-stamping nos dados dos sensores; Monitoramento de jitter.
PF-A-F2.2	Major	Procedimentos	Procedimento claro de operação “sem sincronismo sem fusão sem predição de trajetória” ; Procedimentos de operação com dados não fundidos (informações apresentadas por sensor).

ID da Falha	Severidade	Tipo da Mitigação	Forma de Mitigação
PF-NA-F2.2	Hazardous	Software	Verifiação de consistência entre carimbos de tempo; Desligamento da fusão em caso de desvio excessivo.
DE-F2.2	Hazardous	Software	Verifiação de consistência entre carimbos de tempo; Alarmes de falha de sincronização.
AT-F2.2	Major	Software	Limites de atraso máximo para entrada dos dados no filtro de Kalman.
PF-A-F2.3	Major	Procedimentos	Procedimentos de operação com dados não fundidos (informações apresentadas por sensor).
PF-NA-F2.3	Hazardous	Software	Verificadores de consistência entre sensores antes e depois da fusão; Desligamento automático para modo não fundido quando inconsistências são detectadas.
DE-F2.3	Hazardous	Procedimentos, Software	Treinamento da tripulação para avaliar coerência do cenário; Monitoramento cruzado com outras formas de estimativas de estados.
AT-F2.3	Major	Software	Limites de atraso máximo para entrada dos dados no filtro de Kalman.
PF-A-F2.4	Major	Procedimentos, Software	Procedimentos de limitação de envelope; Monitoramento cruzado com outras formas de estimativas do estado.
PF-NA-F2.4	Hazardous	Software	Monitoramento cruzado com outras formas de estimativas do estado; Lógica de votação ou seleção de melhor fonte.
DE-F2.4	Hazardous	Software	Monitoração de deriva de sensores; Alarmes de inconsistência.
AT-F2.4	Major	Software	Preditor de estado próprio com compensação de atraso; Time-stamping dos sensores; Monitoramento de latência e jitter.
PF-A-F2.5	Major	Procedimentos	Procedimentos para operação com maior margem de separação; Limitação de envelope de operação.
PF-NA-F2.5	Major	Procedimento	Piloto decide a forma de desconflito com base nas informações oferecidas.

ID da Falha	Severidade	Tipo da Mitigação	Forma de Mitigação
DE-F2.5	Catastrophic	Procedimentos, Software	Treinamento para o piloto questionar resoluções “não plausíveis” para o perfil de missão; Monitoramento de consistência da trajetórias geradas.
AT-F2.5	Major	Software	Atualização em taxa mínima de latência; Bloqueio de trajetórias de latência alta; Exibição apenas de um horizonte temporal válido na HMI.
PF-A-F2.6	Major	Procedimentos, Software	Procedimentos de incremento de margem de separação e limitação de velocidade; Mudança de regra de voo ao se identificar esse modo degradado; Apresentação de posições instantâneas sem predição com indicação do modo degradado no HMI.
PF-NA-F2.6	Hazardous	Software	Verificação de coerência temporal entre medidas; Alarmes quando apenas detecções “instantâneas” persistirem sem rastreamento consistente.
DE-F2.6	Catastrophic	Procedimentos, Software	Treinamento para a tripulação reconhecer comportamentos de alvo “estranhos” na HMI; Verificação de coerência temporal entre estimativas.
AT-F2.6	Major	Software	Preditor de estado próprio com compensação de atraso; Time-stamping dos sensores; Monitoramento de latência e jitter.
PF-A-F2.7	Major	Procedimentos	Indicação de operação sem horizonte preditivo; Procedimentos para operação com maior margem de separação; Limitação de envelope de operação.
PF-NA-F2.7	Hazardous	Software	Verificação de coerência temporal entre medidas; Alarmes quando apenas detecções “instantâneas” persistirem sem rastreamento consistente.
DE-F2.7	Catastrophic	Procedimentos, Software	Treinamento para o piloto questionar resoluções “não plausíveis” para o perfil de missão; Monitoramento de consistência da trajetórias geradas.

ID da Falha	Severidade	Tipo da Mitigação	Forma de Mitigação
AT-F2.7	Major	Software	Atualização em taxa mínima de latência; Bloqueio de trajetórias de latência alta; Exibição apenas de um horizonte temporal válido na HMI.
PF-A-F2.8	Minor	Procedimentos, Software	Envelopes conservadores de trajetórias em baixa altitude; Realização de manobras de pouso com regras de voo diferente da DFR; Indicação de ausência de mapa; Uso do DSM enviado pelo PSU.
PF-NA-F2.8	Major	Procedimento, Software	Monitoramento cruzado entre DSM e detecção do terreno; Travas para impedir planeamento por regiões “desconhecidas”.
DE-F2.8	Catastrophic	Procedimentos, Software	Treinamento para abortar trajetória quando mapa/HMI conflitam com ambiente real; Checagem periódica de coerência com os múltiplos sensores.
AT-F2.8	Major	Software	Geração incremental de mapa com níveis de detalhe; Descarte de regiões com tempo de atualização excessivo; Travas para impedir planeamento por regiões “desconhecidas”.
PF-A-F2.9	Minor	Procedimentos	Indicação de perda do cálculo probabilístico; Avaliação da criticidade deverá ser validada pelo piloto com base nas informações apresentadas no HMI.
PF-NA-F2.9	—	—	Não aplicável.
DE-F2.9	Major	Procedimentos	Avaliação da criticidade deverá ser validada pelo piloto com base nas informações apresentadas no HMI.
AT-F2.9	Minor	Software	Indicação de perda do cálculo probabilístico; Avaliação da criticidade deverá ser validada pelo piloto com base nas informações apresentadas no HMI.
PF-A-F2.10	Major	Procedimento	Envelopes com buffers de separação apropriados para as trajetórias; Mudança para regras de voo diferente da DFR.

ID da Falha	Severidade	Tipo da Mitigação	Forma de Mitigação
PF-NA-F2.10	Hazardous	Procedimentos, Software	Envelopes conservadores com buffers de separação apropriados para as trajetórias.
DE-F2.10	Catastrophic	Hardware	Redundância e monitoramento cruzado dos sensores que percebem o ambiente;.
AT-F2.10	Major	Software	Envelopes conservadores com buffers de separação apropriados para as trajetórias.
PF-A-F2.11	Major	Procedimento	Envelopes com buffers de separação apropriados para as trajetórias; Mudança para regras de voo diferente da DFR.
PF-NA-F2.11	Catastrophic	Hardware, Procedimentos, Software	Lógica de separação do ACAS em paralelo e separado do DAA; Envelopes com buffers de separação apropriados para as trajetórias; Piloto mantém-se atento nos arredores; Alertas independentes entre sensores.
DE-F2.11	Catastrophic	Hardware, Procedimentos, Software	Lógica de separação do ACAS em paralelo e separado do DAA; Envelopes com buffers de separação apropriados para as trajetórias; Piloto mantém-se atento nos arredores; Alertas independentes entre sensores.
AT-F2.11	Catastrophic	Hardware, Software	Lógica de separação do ACAS em paralelo e separado do DAA; Envelopes com buffers de separação apropriados para as trajetórias; Piloto mantém-se atento nos arredores; Alertas independentes entre sensores.
PF-A-F3.1	Minor	Procedimentos	Procedimentos para que piloto escolha manobra com base em geometria apresentada.
PF-NA-F3.1	—	—	Não aplicável.
DE-F3.1	Major	Procedimentos	Treinamento para o piloto validar rapidamente se o tipo proposto faz sentido.
AT-F3.1	Minor	Procedimentos	Procedimentos para que piloto escolha manobra com base em geometria apresentada.

ID da Falha	Severidade	Tipo da Mitigação	Forma de Mitigação
PF-A-F3.2	Major	Procedimentos	Procedimentos para que piloto escolha manobra com base em geometria apresentada.
PF-NA-F3.2	—	—	Não aplicável.
DE-F3.2	Major	Procedimentos	Treinamento para o piloto validar rapidamente se o tipo proposto faz sentido.
AT-F3.2	Major	Procedimentos	Procedimentos para que piloto escolha manobra com base em geometria apresentada.
PF-A-F3.3	Major	Procedimentos	Procedimentos para que piloto escolha manobra com base em geometria apresentada.
PF-NA-F3.3	Major	Procedimentos	Procedimentos para que piloto escolha manobra com base em geometria apresentada.
DE-F3.3	Catastrophic	Procedimentos, Software	Checagem de plausibilidade do comando pelo piloto; Limitação de autoridade do DAA sobre o controle de voo; Possibilidade de "override" rápido pelo piloto.
AT-F3.3	Major	Procedimentos	Procedimentos para que piloto escolha manobra com base em geometria apresentada.
PF-A-F4.1	Hazardous	Hardware, Procedimentos	HMI redundante (displays independentes); Aviso sonoro com os alertas independente do display; Procedimentos para que piloto tome o controle da aeronave e mude para VFR/IFR.
PF-NA-F4.1	Hazardous	Hardware, Procedimentos	HMI redundante (displays independentes); Aviso sonoro com os alertas independente do display; Procedimentos para que piloto tome o controle da aeronave e mude para VFR/IFR.
DE-F4.1	Hazardous	Hardware, Procedimentos	HMI redundante (displays independentes); Aviso sonoro com os alertas independente do display; Procedimentos para que piloto tome o controle da aeronave e mude para VFR/IFR.

ID da Falha	Severidade	Tipo da Mitigação	Forma de Mitigação
AT-F4.1	Hazardous	Hardware, Procedimentos	HMI redundante (displays independentes); Aviso sonoro com os alertas independente do display; Procedimentos para que piloto tome o controle da aeronave e mude para VFR/IFR.

Fonte: Elaborado pelo Autor