

**MINISTÉRIO DA DEFESA  
COMANDO DA AERONÁUTICA**



**AVIAÇÃO MILITAR**

**ICA 57-25**

**METODOLOGIA DE ACEITAÇÃO DE RISCO  
RESIDUAL EM PROJETOS MILITARES**

**2022**



**MINISTÉRIO DA DEFESA  
COMANDO DA AERONÁUTICA  
INSTITUTO DE FOMENTO E COORDENAÇÃO INDUSTRIAL**



**AVIAÇÃO MILITAR**

**ICA 57-25**

**METODOLOGIA DE ACEITAÇÃO DE RISCO  
RESIDUAL EM PROJETOS MILITARES**

**2022**





**MINISTÉRIO DA DEFESA**  
**COMANDO DA AERONÁUTICA**  
**DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA AEROESPACIAL**

PORTARIA DCTA Nº 83/DDO, DE 19 DE ABRIL DE 2022.  
Protocolo COMAER nº 67700.004768/2022-50

Aprova a edição da instrução que dispõe sobre a metodologia de aceitação de risco residual em projetos militares.

**O DIRETOR-GERAL DO DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA AEROESPACIAL**, no uso de suas atribuições concedidas pelo inciso IV do art. 10 do Regulamento do Departamento de Ciência e Tecnologia Aeroespacial, aprovado pela Portaria nº 581/GC3, de 12 de abril de 2019; e, considerando o que constam dos Processos nº 67050.002819/2022-19 e nº 67770.000895/2022-56, resolve:

Art. 1º Aprovar a edição da ICA 57-25 “Metodologia de Aceitação de Risco Residual em Projetos Militares”, no âmbito do Departamento de Ciência e Tecnologia Aeroespacial, que com esta baixa.

Art. 2º Esta Portaria entra em vigor em 2 de maio de 2022.

Ten Brig Ar MAURÍCIO AUGUSTO SILVEIRA DE MEDEIROS  
Diretor-Geral do DCTA

(Publicada no BCA nº 078, de 28 de abril de 2022)



## SUMÁRIO

<b>1 DISPOSIÇÕES PRELIMINARES</b> .....	9
<b>1.1 FINALIDADE</b> .....	9
<b>1.2 CONCEITUAÇÃO</b> .....	9
<b>1.3 ÂMBITO</b> .....	10
<b>2 CONTEXTUALIZAÇÃO</b> .....	11
<b>3 METODOLOGIA DE ANÁLISE DE RISCO PARA PROJETOS MILITARES</b> .....	15
<b>3.5 PROCESSO DE ANÁLISE DE SEGURANÇA DE SISTEMAS</b> .....	15
<b>4 PROCESSO DE ACEITAÇÃO DE RISCO RESIDUAL</b> .....	19
<b>5 DISPOSIÇÕES GERAIS</b> .....	22
<b>6 DISPOSIÇÕES TRANSITÓRIAS</b> .....	23
<b>7 DISPOSIÇÕES FINAIS</b> .....	24
<b>REFERÊNCIAS</b> .....	25



## PREFÁCIO

É responsabilidade do Comando da Aeronáutica (COMAER) garantir a segurança dos sistemas e produtos utilizados no cumprimento de suas missões. A busca pela segurança deve ser aspecto mandatário em todas as atribuições pertinentes a este Comando, eliminando riscos desnecessários ou injustificáveis que possam comprometê-la.

Ao se projetar um sistema, a *System Safety Analysis* (SSA) é uma parte importante das atividades de engenharia relacionadas à certificação inicial de aeronavegabilidade. Para projetos militares, a análise requer não apenas um processo para determinar se o sistema é seguro o suficiente, mas também para identificar um equilíbrio aceitável entre segurança, custo e capacidade militar.

Com o propósito de desenvolver uma metodologia que substancie a aceitação do risco residual para projetos militares, a Divisão de Certificação de Produto Aeroespacial (CPA) do IFI promoveu um estudo baseado no estado da arte das principais publicações de cunho técnico-científico na área de Análise de Risco.

Vale ressaltar que o produto final resultante da aplicação do método não é uma regra, mas sim um guia para uma avaliação fundamentada do risco de operações militares específicas. Dessa forma, o guia constitui uma excelente ferramenta para o suporte a decisões baseadas em avaliação de risco numa determinada operação militar.



## **1 DISPOSIÇÕES PRELIMINARES**

### **1.1 FINALIDADE**

A presente Instrução tem por finalidade detalhar a metodologia de aceitação do risco residual a ser aplicada nos projetos militares em certificação no âmbito do DCTA/IFI.

### **1.2 CONCEITUAÇÃO**

Para os propósitos desta Instrução, os termos técnicos devem seguir as definições previstas na DCA 800-2 “Garantia da Qualidade e da Segurança de Sistemas e Produtos no COMAER”, ICA 57-21 “Regulamento de Aeronavegabilidade Militar – procedimentos para Certificação de Produto Aeronáutico”, ICA 57-22 “Critérios para definição de Requisitos de Aeronavegabilidade de Produtos Aeronáuticos” e na ICA 57-23 “Metodologia de Análise de Risco para Aeronaves em Serviço”, em suas versões mais atuais, além dos termos a seguir, definidos de acordo com a norma MIL-STD-882E.

#### **1.2.1 ACIDENTE (*MISHAP*)**

Um evento não intencional (ou série de eventos) que resulta(m) em morte, ferimentos, doenças ocupacionais, dano ou perda de equipamento ou propriedade, ou danos ao meio ambiente.

#### **1.2.2 CICLO DE VIDA (*LIFE-CICLE*)**

Todas as fases de vida do sistema, sendo elas: concepção, pesquisa, desenvolvimento, teste, avaliação, produção, implantação, operação, suporte e desativação.

#### **1.2.3 PERIGO (*HAZARD*)**

Uma condição real ou potencial que pode culminar em um evento (ou série de eventos) não planejados, por exemplo um acidente, resultando em morte, ferimentos, doenças ocupacionais, dano ou perda de equipamento ou propriedade, ou danos ao meio ambiente.

#### **1.2.4 RISCO (*RISK*)**

A combinação da severidade do evento e a probabilidade deste ocorrer.

#### **1.2.5 RISCO ACEITÁVEL (*ACCEPTABLE RISK*)**

Risco que a Autoridade responsável está disposta a aceitar.

#### **1.2.6 SEGURANÇA (*SAFETY*)**

Ausência de condições que podem causar morte, ferimentos, doenças ocupacionais, dano ou perda de equipamento ou propriedade, ou danos ao meio ambiente.

#### **1.2.7 SEGURANÇA DE SISTEMAS (*SYSTEM SAFETY*)**

Aplicação de princípios, critérios e técnicas de engenharia e administração para alcançar o risco aceitável dentro das limitações de eficácia operacional, adequando tempo e custos ao longo de todas as fases do ciclo de vida do sistema.

### 1.2.8 SEVERIDADE (*SEVERITY*)

A magnitude das potenciais consequências de uma condição de falha ou de um perigo, incluindo morte, ferimentos, doenças ocupacionais, dano ou perda de equipamento ou propriedade, ou danos ao meio ambiente.

### 1.3 ÂMBITO

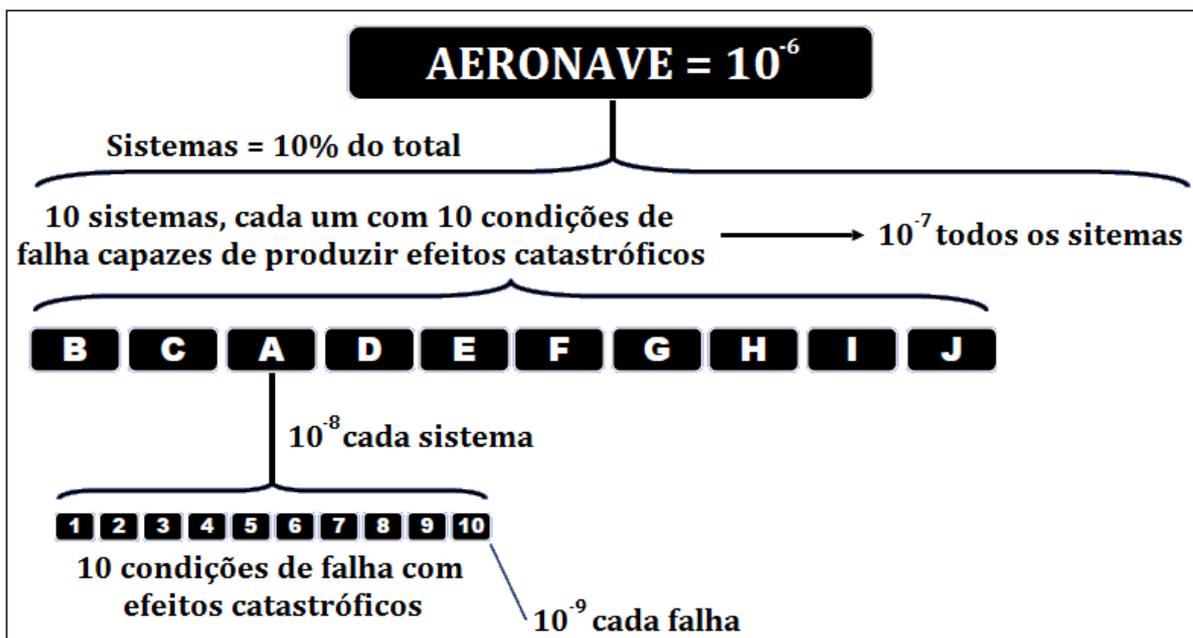
A presente Instrução aplica-se a todas os projetos militares, que sejam submetidos a um processo de certificação de projeto. A metodologia aqui definida é aplicável para compor a base de certificação de qualquer projeto militar para a qual será emitido um certificado de tipo militar.

## 2 CONTEXTUALIZAÇÃO

**2.1** O objetivo da certificação de aeronavegabilidade é atestar que a aeronave é segura e está em conformidade com os requisitos de segurança aplicáveis.

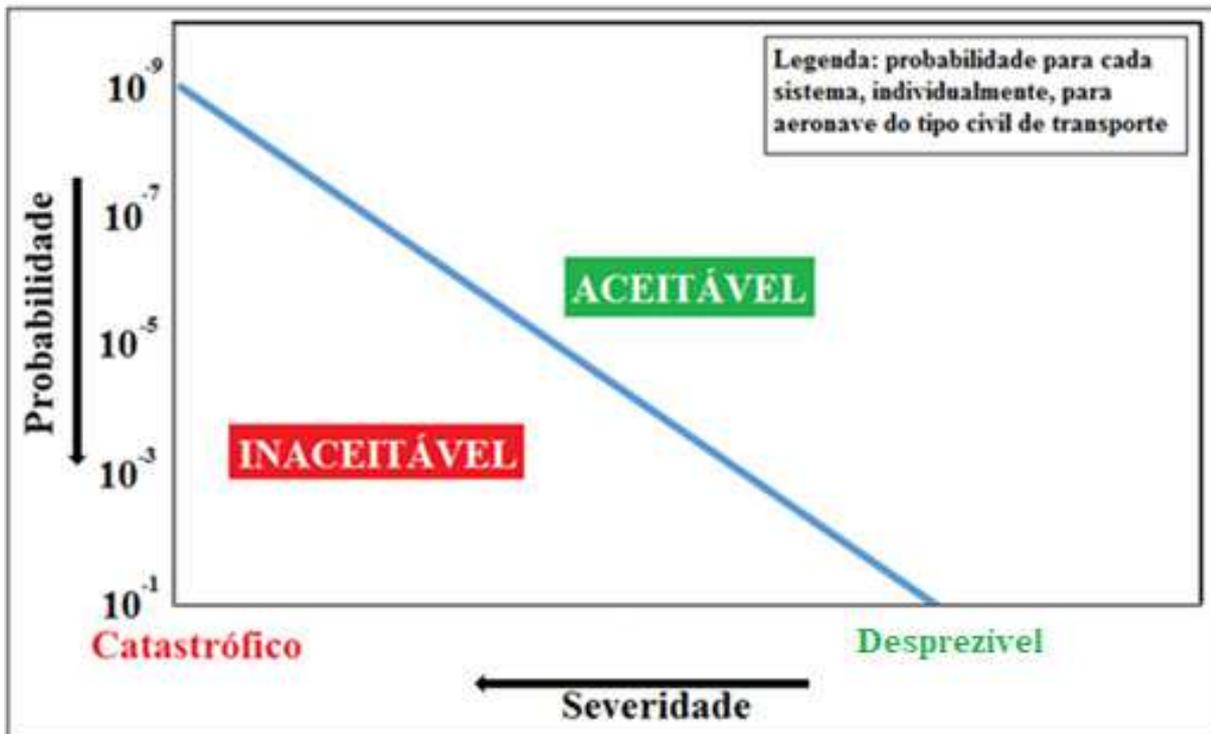
**2.2** Por muitos anos, os níveis de risco relacionados com aeronavegabilidade visados nos requisitos de certificação foram desenvolvidos com base em abordagens tradicionais. Nos últimos anos, esses níveis foram aprimorados por meio de comparações com os resultados já alcançados (julgados a partir de estatísticas de acidentes), das discussões e deliberações que buscavam requisitos mais racionais e por meio da influência de uma abordagem de Análise de Segurança na definição dos requisitos.

**2.3** Conforme o documento GM AMC 21.A.3B *Defect Correction - Sufficiency of proposed corrective action da European Aviation Safety Agency (EASA)*, os níveis de risco relacionados com aeronavegabilidade, ou objetivo de risco de aeronavegabilidade, são discutidos como um valor pontual: uma taxa de acidentes fatais de causa relacionada à aeronavegabilidade por hora de voo ou ciclo de voo. Para a aviação de transporte civil, por exemplo, o objetivo de segurança, considerando somente os acidentes ocorridos por falhas de sistemas da aeronave, geralmente é de não mais que 1 acidente catastrófico a cada 10.000.000 (dez milhões) de horas de voo, conforme diagrama a seguir. Entretanto, quando se particulariza para um determinado tipo de aeronave, os níveis de segurança atingidos variam numa faixa em torno do objetivo pontual.



**Figura 1:** Diagrama que ilustra a obtenção do valor  $10^{-9}$  de falha catastrófica por hora de voo. (fonte: *Advisory Circular (AC) 25.1309-1A: System Design and Analysis*)

**2.4** De uma maneira geral, tem-se que dada uma severidade e uma probabilidade de falhas, os riscos aceitável e inaceitável se fazem a partir de uma fronteira, como pode ser visto na Figura 2.



**Figura 2: Risco aceitável e inaceitável na aviação de transporte civil.**

2.5 Na aviação militar, existem algumas peculiaridades, quais são:

#### 2.5.1 AMBIENTE OPERACIONAL

Aeronaves militares inúmeras vezes operam sob condições climáticas adversas, devendo executar a missão sob condições muitas vezes extremas.

#### 2.5.2 ARMAMENTOS

As normas de aeronavegabilidade civis não possuem critérios ou requisitos que se referem a componentes equivalentes a armamentos.

#### 2.5.3 DIFERENTES REQUISITOS

Os requisitos de qualidade de voo para aeronaves civis, por exemplo, não consideram a missão das aeronaves militares no ambiente operacional a que se destinam.

#### 2.5.4 DISPOSITIVOS DE AUTODEFESA

Aeronaves militares operam em ambientes hostis que exigem o uso de *chaff*, *flares* e outras tecnologias de autodefesa.

#### 2.5.5 FUNÇÃO, MISSÃO E TAREFAS

Diversas funções, missões e tarefas militares são únicas e não possuem atividades equivalentes na aviação civil.

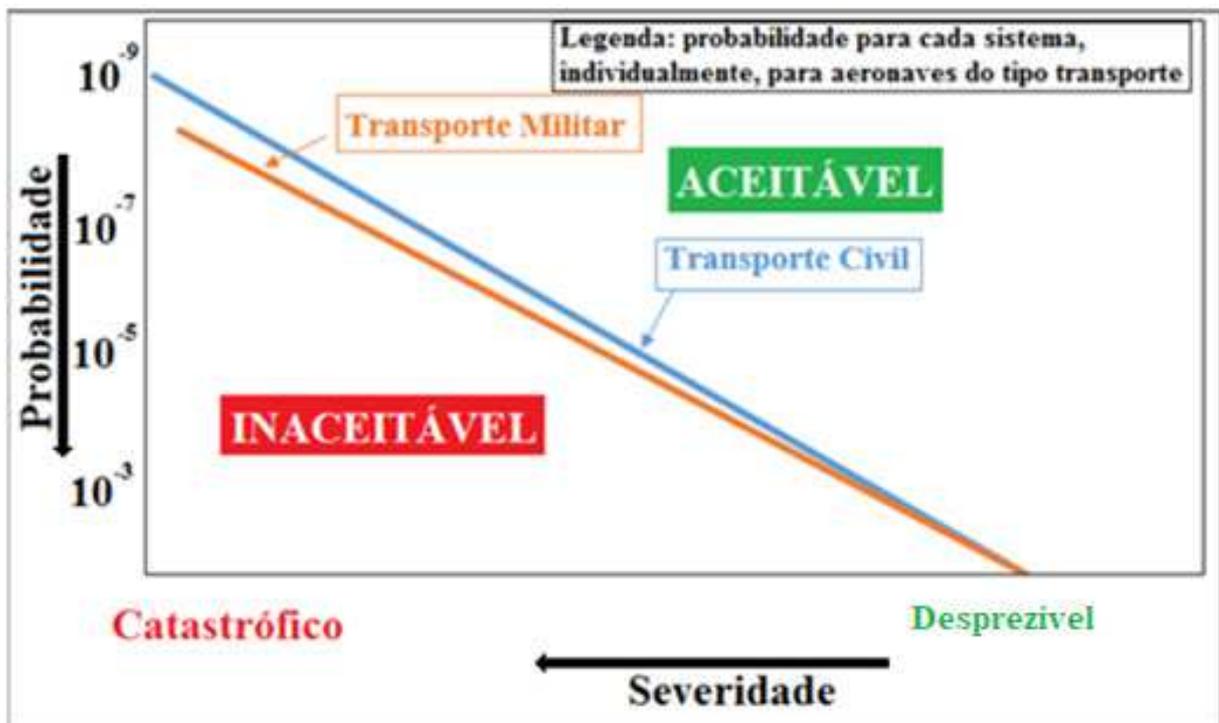
### 2.5.6 OPERAÇÕES EM CENÁRIO DE GUERRA

Operações relacionadas a guerras incluem missões extremamente perigosas em condições de necessidade operacional.

### 2.5.7 TECNOLOGIA MILITAR

Os requisitos técnicos para aeronaves militares demandam rápidos avanços tecnológicos que podem ser implementados antes de estarem maduros.

2.6 Conforme ICA 57-23/2019, tendo-se em vista todas as peculiaridades já citadas e considerando que a atividade-fim das Forças Armadas não é, de maneira geral, semelhante a atividade-fim das empresas aéreas civis, aceita-se um risco maior para as aeronaves militares, de maneira tal que o fator aceitável para a aviação civil multiplicado por um fator igual a 10 fornece o nível de aceitação militar para aeronaves de transporte, por exemplo, conforme ilustrado na Figura 3.



**Figura 3: Risco aceitável e inaceitável na aviação de transporte militar.**

2.7 Leva-se em consideração, também, as diferentes categorias das aeronaves militares, sendo que, em geral, os seguintes valores de probabilidade de ocorrência para uma condição de falha catastrófica, por hora de voo, podem ser adotados, conforme enunciado abaixo e representado na Figura 4.

- $10^{-8}$  para aeronaves militares de transporte;
- $10^{-7}$  para helicópteros militares; e
- $10^{-6}$  para aeronaves militares de caça.

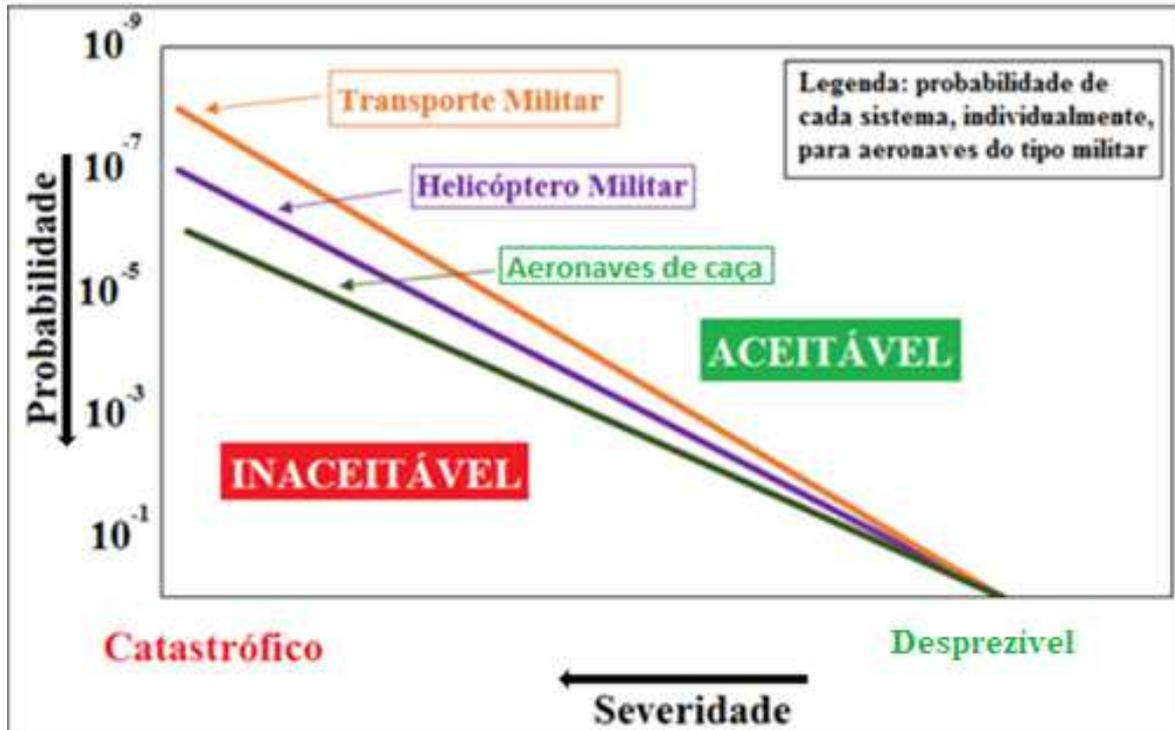


Figura 4: Níveis de aceitação para diferentes categorias de aeronaves militares.

2.8 Devido à sua peculiaridade, na aviação militar deve existir maior flexibilidade nos requisitos de níveis de segurança (*Safety*), entre aceitável e inaceitável. Para uma missão específica militar, o risco residual, considerando-se níveis de segurança abaixo dos referidos na Figura 4, pode ser aceito pela autoridade competente, visto que a atividade-fim pode exigir maior exposição a riscos, além de demandar urgência e prontidão. Tal fato pode ser ilustrado na Figura 5, como exemplo de uma aeronave de transporte militar:

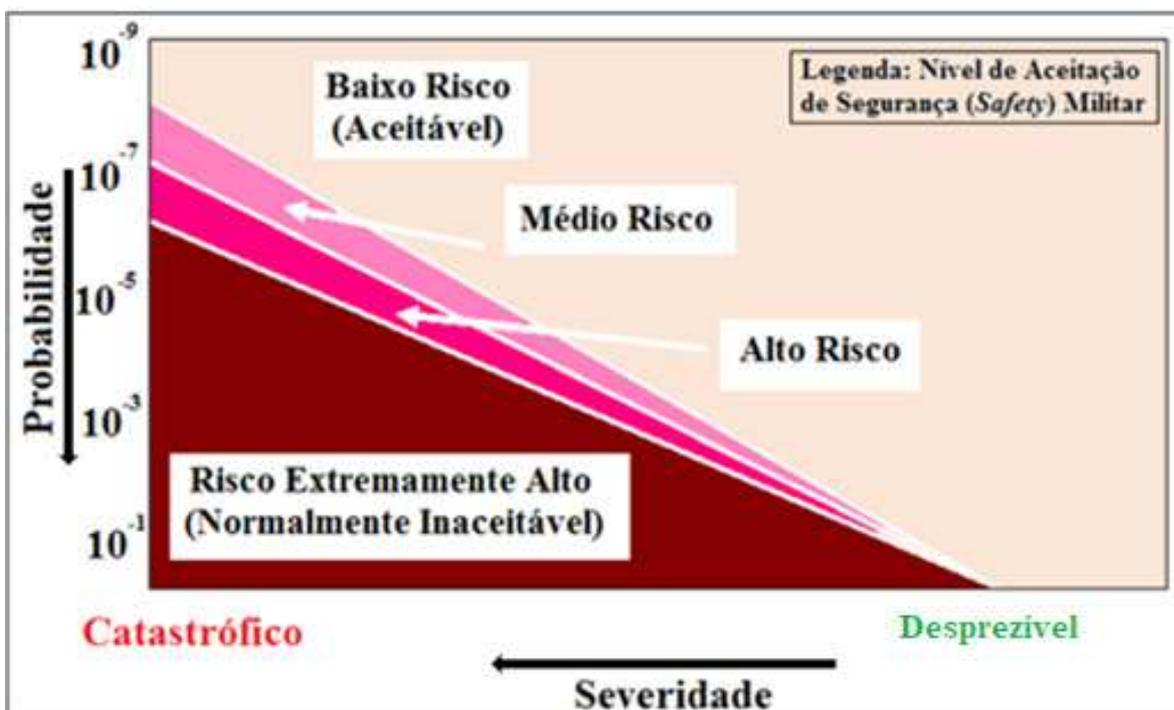


Figura 5: Exemplo de nível de aceitação de risco para uma aeronave militar.

### 3 METODOLOGIA DE ANÁLISE DE RISCO PARA PROJETOS MILITARES

**3.1** A norma MIL-STD-882E, divulgada pelo Departamento de Defesa (DoD) dos Estados Unidos da América, é um documento que discorre sobre a prática padrão de segurança de sistemas. A norma tem como objetivo eliminar os perigos, onde for possível, e minimizar os riscos onde os perigos não podem ser eliminados.

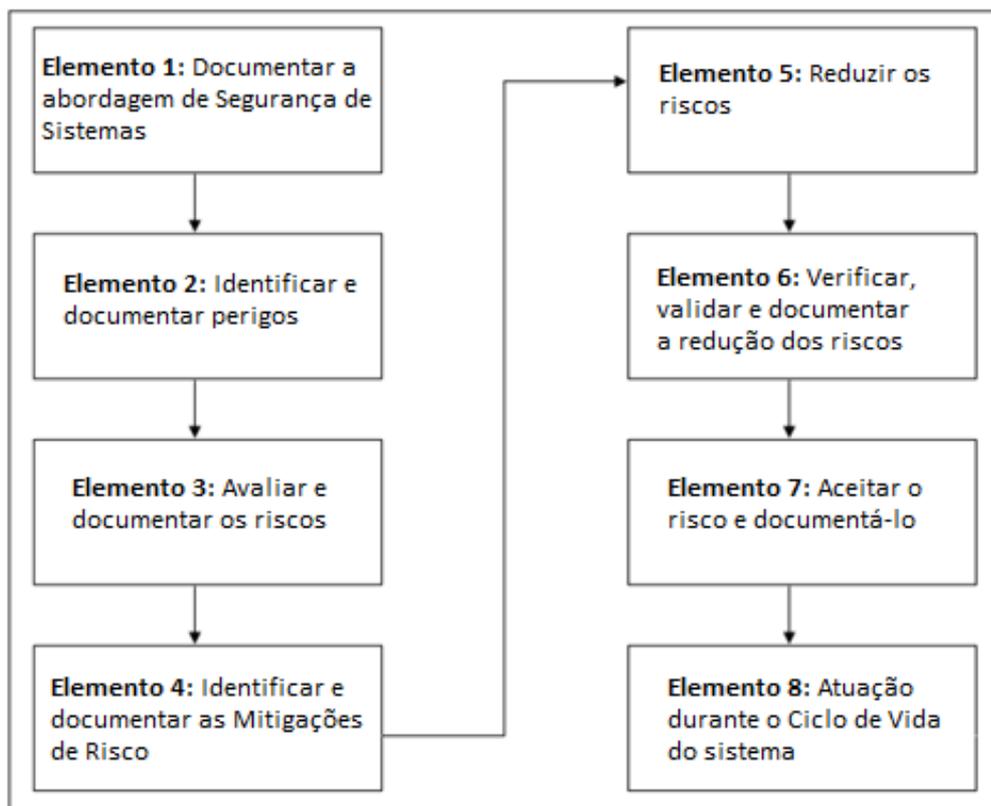
**3.2** Dessa forma, o documento abrange os perigos que se aplicam aos sistemas, produtos, equipamentos (incluindo *hardware* e *software*) ao longo do projeto, desenvolvimento, testes, produção, vida em serviço e desativação.

**3.3** A prática padrão de análise de segurança de sistemas contida na norma fornece uma metodologia, ou seja, uma padronização para a identificação, classificação e redução dos perigos. Ressalta-se que aquele documento tem cunho militar e foi produzido tendo como compromisso a proteção pessoal e material contra acidentes fatais, ferimentos, bem como salvaguardar os sistemas de defesa e o meio ambiente.

**3.4** A partir do momento em que um processo de certificação é solicitado junto ao DCTA/IFI, a MIL-STD-882E delinea as definições e requerimentos obrigatórios mínimos a serem cumpridos pela indústria para a segurança do sistema ser aceitável.

#### 3.5 PROCESSO DE ANÁLISE DE SEGURANÇA DE SISTEMAS

A partir desse momento, surge o processo de análise de segurança de sistemas que consiste em oito elementos dispostos numa sequência lógica a serem executados. Segue na Figura 6 uma exposição dos elementos supracitados e sua sequência de execução:



**Figura 6:** Sequência e elementos do processo de análise de segurança de sistemas.

### 3.5.1 ELEMENTO 1

Documentar o planejamento da Análise de Segurança de Sistemas: o requerente deve elaborar um Plano para gerenciar os perigos como uma parte integral do processo de Engenharia de Sistemas.

### 3.5.2 ELEMENTO 2

Identificar e documentar perigos: os perigos são identificados por meio de um processo sistemático de análise que inclui os sistemas de *hardware* e *software*, bem como o sistema de interface com o operador.

### 3.5.3 ELEMENTO 3

Avaliar e documentar os riscos: a partir das definições abaixo relacionadas é possível avaliar o risco:

#### 3.5.3.1 Categorias de severidade

Nessa classificação é levado em consideração mortes ou ferimentos, impactos ambientais, bem como perdas monetárias. Apenas a título de exemplo, o Manual Técnico de Aeronavegabilidade (*Technical Airworthiness Manual - TAM*) fornecido pelo *National Defence* (ND) do Canadá, define as categorias de severidade conforme definido na tabela 1.

**Tabela 1: Categorias de severidade de acordo com TAM.**

Descrição	Categoria da Severidade	Critério
<b>Catastrófico</b>	<b>A</b>	Todas as condições de perigo que impeçam a continuação do voo e pouso seguro. Pode resultar em morte dos tripulantes, normalmente com a perda da aeronave.
<b>Crítico</b>	<b>B</b>	Condições de perigo que resultam em grande redução das margens de segurança ou capacidades funcionais, maior carga de trabalho na tripulação, de maneira que a tripulação não seja capaz de executar suas tarefas. Pode resultar em morte ou ferimentos graves nos ocupantes da aeronave ou grandes danos aos sistemas da aeronave. Pode, ainda, resultar em morte ou ferimentos graves de pessoas em solo.
<b>Maior</b>	<b>C</b>	Condições de perigo que resultam em moderada redução das margens de segurança ou capacidades funcionais, incluindo aumento moderado na carga de trabalho da tripulação. É possível que haja feridos entre os ocupantes da aeronave, bem como dano leve nos sistemas da aeronave.
<b>Menor</b>	<b>D</b>	Condições de perigo que não irão reduzir significativamente a segurança da aeronave, mas que podem resultar em ligeira redução das margens de segurança e um ligeiro aumento na carga de trabalho da tripulação.
<b>Negligenciável</b>	<b>E</b>	Não há efeito sobre a segurança. Efeito negligenciável sobre as margens de segurança.

**3.5.3.2** Em conformidade com os critérios que definem a categoria da severidade, tem-se a definição do nível de probabilidade:

### 3.5.3.3 Níveis de Probabilidade

Avalia-se a probabilidade de ocorrência de uma condição de falha ou perigo. A título de exemplo, o TAM define a matriz de probabilidade conforme tabela 2:

**Tabela 2: Nível de probabilidade de acordo com TAM.**

Nível de Probabilidade	Aeronave militar carregando passageiros (FAR-25/29)	Aeronave Militar	Aeronave Militar Equipada com Assento Ejetável	SARP com Massa de Decolagem Superior a 150 kg
<b>Frequente</b>	$p > 10^{-3}$	$p > 10^{-3}$	$p > 10^{-3}$	$p > 10^{-2}$
<b>Provável</b>	$10^{-5} < p \leq 10^{-3}$	$10^{-5} < p \leq 10^{-3}$	$10^{-4} < p \leq 10^{-3}$	$10^{-3} < p \leq 10^{-2}$
<b>Remoto</b>	$10^{-7} < p \leq 10^{-5}$	$10^{-6} < p \leq 10^{-5}$	$10^{-5} < p \leq 10^{-4}$	$10^{-5} < p \leq 10^{-3}$
<b>Extremamente Remoto</b>	$10^{-9} < p \leq 10^{-7}$	$10^{-8} < p \leq 10^{-6}$	$10^{-7} < p \leq 10^{-5}$	$10^{-6} < p \leq 10^{-5}$
<b>Extremamente Improvável</b>	$p \leq 10^{-9}$	$p \leq 10^{-8}$	$p \leq 10^{-7}$	$p \leq 10^{-6}$

**3.5.3.4** A probabilidade “P” de ocorrência é a razão entre o número de eventos atuais ou esperados (numerador) durante uma específica exposição (denominador), no qual o denominador é baseado em características de vida para um item. O mais comumente utilizado são as horas de voo.

### 3.5.3.5 Matriz de Avaliação de Risco

A partir da severidade que um evento pode causar bem como o quão frequente o mesmo pode ocorrer, é possível determinar uma matriz de avaliação do risco. A título de exemplo, o TAM define sua matriz de avaliação do risco conforme tabela 3.

**Tabela 3: Matriz de Avaliação do Risco de acordo com o TAM.**

Severidade \ Probabilidade	Catastrófico (A)	Crítico (B)	Maior (C)	Menor (D)	Negligenciável (E)
<b>Frequente (1)</b>	Extremamente Alto	Extremamente Alto	Médio	Baixo	Baixo
<b>Provável (2)</b>	Extremamente Alto	Alto	Baixo	Baixo	Baixo
<b>Remoto (3)</b>	Alto	Médio	Baixo	Baixo	Baixo
<b>Extremamente Remoto (4)</b>	Médio	Baixo	Baixo	Baixo	Baixo
<b>Extremamente Improvável (5)</b>	Baixo	Baixo	Baixo	Baixo	Baixo

#### **3.5.4 ELEMENTO 4**

Identificar e documentar as Mitigações de Risco: a mitigação do risco potencial deve ser identificada, sendo que a redução esperada ou solução alternativa deve ser estimada e documentada no processo. O objetivo principal sempre é ELIMINAR o perigo, se possível. Entretanto, se não for possível, o risco associado pode ser reduzido ao menor nível aceitável com as limitações de custo, prazo e desempenho.

#### **3.5.5 ELEMENTO 5**

Reduzir o Risco: os riscos avaliados são selecionados e implementados para alcançar um nível aceitável de risco. Deve-se avaliar os custos, viabilidade e eficácia do método candidato à redução do risco.

#### **3.5.6 ELEMENTO 6**

Verificar, validar e documentar a Redução de Risco: deve-se verificar a implementação e validar a eficácia de todas as medidas de mitigação de risco selecionadas por meio de análise, teste, demonstração ou inspeção apropriados.

#### **3.5.7 ELEMENTO 7**

Aceitar o Risco e documentá-lo: uma medida a ser tomada anteriormente à exposição de pessoal, equipamento ou do meio-ambiente a um perigo conhecido do sistema é que o mesmo deve ser aceito pela autoridade responsável.

#### **3.5.8 ELEMENTO 8**

Atuação durante o Ciclo de Vida do Sistema: Após o sistema estar em operação, será utilizado o processo de avaliação de segurança de sistemas ao longo do ciclo de vida do sistema.

## 4 PROCESSO DE ACEITAÇÃO DE RISCO RESIDUAL

**4.1** Fica estabelecido, a seguir, o processo de aceitação do risco adotado no âmbito do DCTA/IFI para projetos militares em certificação, no que diz respeito aos sistemas, equipamentos e instalação.

**4.2** Conforme preconizado pela ICA 57-22/2019 e de acordo com os requisitos estabelecidos nos contratos de aquisição, uma aeronave militar, incluindo todos os seus sistemas, pode ser certificada pelo DCTA/IFI em uma versão básica “green” de acordo com os requisitos brasileiros de aeronavegabilidade (RBAC), exceto para as isenções acordadas entre COMAER e empresa.

**4.3** Entretanto, será considerado um ajuste (*tailoring*) em relação à seção RBAC 2X.1309 (25.1309, 27.1309, 29.1309), uma vez que o processo de análise de segurança subjacente à conformidade desse requisito é baseado em objetivos de segurança estabelecidos e em um perfil de voo civil. Essa consideração se apoia no princípio de que a abordagem civil é orientada para objetivos de segurança e que o nível aceitável de segurança já é definido e capturado no respectivo Código de Aeronavegabilidade Civil.

**4.4** No entanto, uma aeronave militar é orientada para realização da missão com o maior nível de segurança possível. Portanto, reconhece-se que o risco de uma missão militar envolve cenários operacionais que podem estar fora do controle do desenvolvedor de aeronaves. Logo, os aspectos críticos de segurança serão avaliados, à luz desta Instrução, em uma abordagem baseada em risco.

**4.5** As empresas são solicitadas a apresentar para o DCTA/IFI os níveis aceitáveis de segurança previstos para os sistemas, equipamentos e instalação e também os critérios de aceitação de risco, por meio do *System Safety Analysis* (SSA).

**4.6** A abordagem para se determinar o resultado da SSA pode ser uma abordagem baseada em objetivo de segurança ou uma abordagem baseada em risco ou, ainda, uma combinação deles. Uma abordagem baseada em objetivo define os objetivos de segurança de acordo com a severidade potencial, enquanto uma abordagem baseada em risco está argumentando que o risco é tão baixo quanto razoavelmente possível. A primeira tem um nível de segurança aceitável predeterminado com base em dados históricos e é usado na certificação de aeronaves civis. Um exemplo é o requisito RBAC 25.1309, que exige que todas as condições de falha identificadas como catastróficas sejam extremamente improváveis e não resultem de uma única falha. A última, não tem um nível predeterminado de segurança e requer uma análise de custo-benefício para determinar se o nível de segurança é aceitável ou não. Essas duas abordagens podem ser combinadas, principalmente usando uma abordagem baseada em objetivo, para se atender a um objetivo de segurança específico e se isso não for possível, usar-se-á uma abordagem baseada em risco e executar-se-á uma análise de custo-benefício para determinar se o risco pode ser aceito ou deve ser mitigado.

**4.7** De acordo com as estratégias estabelecidas para os diversos programas, a análise de segurança de sistema pode ser dividida em duas partes: um processo de análise de segurança civil e um processo de análise de segurança militar. O primeiro é baseado na seção 2X.1309 (Análise e Avaliação de Segurança de Sistemas) do RBAC e o segundo adota a MIL-STD-882E como referência. Ressalta-se que a metodologia abordada na MIL-STD-882 é utilizada como referência, porém a utilização das tabelas e tarefas contidas na norma devem ser discutidas caso a caso entre requerente e Organização Certificadora.

**4.8** Em geral, a aeronave “green” irá mostrar a conformidade com os requisitos §2X.1309 e outros requisitos de segurança relacionados que compreendem a “avaliação de segurança civil”, conforme preconizado pela ICA 57-22/2019.

**4.9** O projeto dos sistemas, equipamentos e instalações, cuja função é necessária para a realização segura das missões militares deve levar em consideração o cenário operacional militar.

**4.10** A avaliação de segurança para aviação militar é melhor referenciada como avaliação de risco. A avaliação de risco militar (MRA) é complementar à avaliação de segurança realizada para demonstrar o cumprimento do RBAC 2X.1309 para a plataforma “green” em um perfil de voo civil.

**4.11** O processo de avaliação de risco militar (*Military Risk Assessment* - MRA) é baseado na MIL-STD-882E e inclui as seguintes etapas já abordadas, ainda que com outra estrutura, no item 3 desta Instrução: Identificação de perigos; Avaliação de risco; Mitigação de risco e Revisão e aceitação do risco por nível apropriado.

**4.12** Basicamente, tem-se que:

#### **4.12.1 IDENTIFICAÇÃO DE PERIGOS**

Identificação e classificação de perigos, conforme item 3.5.3 desta Instrução.

#### **4.12.2 AVALIAÇÃO DE RISCO**

Categorias de risco (por exemplo, alto, sério, médio e baixo) são definidas de acordo com o item 3.5.3 desta Instrução.

#### **4.12.3 MITIGAÇÃO DE RISCO**

A mitigação de risco é realizada basicamente em dois níveis, que compreende precauções de projeto e/ou mitigação operacional. As precauções de projeto são medidas tomadas para mitigar os riscos associados às missões militares. Essas medidas são: seleção de projeto, dispositivos de segurança e avisos em sistemas. Por outro lado, mitigação operacional consiste em ações para criar e avaliar os procedimentos operacionais que fornecem mitigações ao risco envolvido. Todas as atividades de mitigação de risco são conduzidas com o objetivo de reduzir todas as categorias de risco para o menor nível possível.

#### **4.12.4 REVISÃO E ACEITAÇÃO DO RISCO RESIDUAL**

Se, após as atividades de mitigação serem concluídas, ainda houver riscos residuais maiores que o nível baixo, os riscos devem ser aceitos internamente no COMAER pelo nível apropriado. A aceitação dos riscos residuais pode se basear em comparação com outros modelos de aeronaves que operam em condições semelhantes e critérios adicionalmente definidos pela autoridade competente.

**4.13** Os contratos de aquisição e desenvolvimento de sistemas e produtos para o COMAER devem conter, conforme aplicável, cláusulas referentes às exigências de entrega e aprovação do Plano de Segurança de Sistemas (*System Safety Program Plan*), e as respectivas minutas devem ser previamente acordadas com a Organização Certificadora competente.

**4.14** Os referidos contratos devem conter ou referenciar os regulamentos e normas a serem considerados como referência para elaboração do Plano de Segurança de Sistemas.

**4.15** As autoridades competentes que aceitarão os respectivos níveis de risco residual serão definidas conforme a tabela 4, para cada processo de certificação, respeitando-se as peculiaridades de cada processo. Um meio alternativo de cumprimento pode ser proposto, caso aplicável, por meio de Ficha de Controle de Assunto Relevante Militar (FCAR-M) ou do Plano de Segurança de Sistemas (*System Safety Program Plan*). Ressalta-se que, em caso de meio alternativo de cumprimento, a definição de quem são as autoridades deverá ser submetida à aprovação das autoridades elencadas.

**4.16** O processo de aceitação de risco por nível de Autoridade se encontra na Tabela 4.

**Tabela 4: Aceitação de Risco.**

Categoria de risco	Nível de aceitação no COMAER
Alto	Comitê de Avaliação de Risco (CAR)
Sério	DCTA
Médio	IFI
Baixo	Especialista em Certificação

**4.17** Na tabela 4, o CAR é o Comitê permanente constituído por um ou mais membros do EMAER, COMGAP, COMPREP, COMAE, DCTA e CENIPA, coordenado pelo EMAER, que visa deliberar quanto à solução do tratamento de Dificuldades de Serviço com Potencial Limitante de Aeronavegabilidade e/ou quanto ao estabelecimento e/ou à manutenção de Limitações de Aeronavegabilidade decorrentes destas Dificuldades em Serviço, conforme estabelecido pela DCA 800-2/2019.

## **5 DISPOSIÇÕES GERAIS**

**5.1** O DCTA/IFI adota a metodologia descrita nesta Instrução como um dos critérios para o desenvolvimento e a aprovação da base de certificação.

**5.2** Adotam-se os procedimentos estabelecidos na norma MIL-STD-882 *System Safety*, em sua última versão, como obrigatórios em todos os processos de certificação a serem conduzidos junto ao DCTA/IFI, exceto para as plataformas derivativas de aeronaves civis.

## **6 DISPOSIÇÕES TRANSITÓRIAS**

**6.1** Os projetos militares que possuam base de certificação estabelecida em data anterior à publicação desta ICA podem manter a base já acordada.

**6.2** Os projetos militares que tenham sua base de certificação em fase de discussão devem procurar adotar as instruções desta ICA. Caso isso não seja possível, devem ser apresentadas as justificativas que permitam ao DCTA/IFI adotar uma outra metodologia para formação de uma base de certificação que garanta a segurança do sistema.

**6.3** Esta instrução não se aplica para sistemas que ainda estão em fase de estudo de concepção ou viabilidade, conforme termos da DCA 400-6/2007 “Ciclo de Vida de Sistemas e Materiais da Aeronáutica”.

## **7 DISPOSIÇÕES FINAIS**

Os casos não previstos nesta Instrução serão submetidos ao Diretor do IFI à apreciação do Diretor-Geral do DCTA.

## REFERÊNCIAS

BRASIL. Ministério da Defesa. Comando da Aeronáutica. *Portaria nº 2.190/GC3, de 19 de dezembro de 2019*. Aprova a reedição da Diretriz que dispõe sobre a Garantia da Qualidade e da Segurança de Sistemas e Produtos no COMAER. Brasília, 2019. (DCA 800-2)

BRASIL. Ministério da Defesa. Comando da Aeronáutica. Departamento de Ciência e Tecnologia Aeroespacial. *Portaria DCTA nº 214/DNO, de 22 de agosto de 2017*. Aprova a reedição da Instrução que dispõe sobre “Regulamento de Aeronavegabilidade Militar - Procedimentos para Certificação de Produto Aeronáutico”, no âmbito do Departamento de Ciência e Tecnologia Aeroespacial. São José dos Campos, 2017. (ICA 57-21)

\_\_\_\_\_. *Portaria DCTA nº 5/DNO, de 2 de outubro de 2019*. Aprova a edição da Instrução que dispõe sobre a metodologia de análise de risco para aeronaves em serviço. São José dos Campos, 2019. (ICA 57-23)

\_\_\_\_\_. *Portaria DCTA nº 13/DNO, de 9 de dezembro de 2019*. Aprova a edição da Instrução que dispõe sobre critérios para definição de requisitos de aeronavegabilidade de produtos aeronáuticos. São José dos Campos, 2019. (ICA 57-22)

BRASIL. Ministério da Defesa. Comando da Aeronáutica. Estado-Maior da Aeronáutica. *Portaria nº 129/GC4, de 5 de março de 2007*. Aprova a Diretriz que dispõe sobre Ciclo de Vida de Sistemas e Materiais da Aeronáutica. Brasília, 2007. (DCA 400-6)

CANADÁ. NATIONAL DEFENCE. Manual Técnico de Aeronavegabilidade (*Technical Airworthiness Manual - TAM*). 2015.

ESTADOS UNIDOS DA AMÉRICA. Department of Defense. *Standard Practice. System Safety. MIL-STD-882*. 2012.

ESTADOS UNIDOS DA AMÉRICA. FEDERAL AVIATION ADMINISTRATION (FAA). *Advisory Circular (AC) 25.1309-1A: System Design and Analysis*. Junho, 1988.

EUROPA. EUROPEAN AVIATION SAFETY AGENCY (EASA). *GM AMC 21.A.3B Defect Correction - Sufficiency of proposed corrective action, issue 2, amendment 13*. 2021.