MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

AVIAÇÃO MILITAR

ICA 57-23

METODOLOGIA DE ANÁLISE DE RISCO PARA AERONAVES EM SERVIÇO

2019

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

AVIAÇÃO MILITAR

ICA 57-23

METODOLOGIA DE ANÁLISE DE RISCO PARA AERONAVES EM SERVIÇO

2019

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

PORTARIA DCTA Nº 5/DNO, DE 2 DE OUTUBRO DE 2019.
Protocolo COMAER nº 67700.013050/2019-59

Aprova a edição da Instrução que dispõe sobre a metodologia de análise de risco para aeronaves em serviço.

O **DIRETOR-GERAL DO DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA AEROESPACIAL**, no uso das atribuições que lhe confere o 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; conforme item 2.3.23 da DCA 800-2 "Garantia da Qualidade e da Segurança de Sistemas e Produtos no COMAER", aprovada pela Portaria nº 1.164/GC3, de 19 de setembro de 2016; e, ainda, considerando o que consta do Processo nº 67770.003213/2019-61, resolve:

Art. 1º Aprovar a edição da ICA 57-23 "Metodologia de Análise de Risco para Aeronaves em Serviço", que com esta baixa.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

Ten Brig Ar LUIZ FERNANDO DE AGUIAR
Diretor-Geral do DCTA

(Publicada no BCA nº 180, de 7 de outubro de 2019)

SUMÁRIO

PREFÁCIO

O fomento à Indústria Nacional de Material de Defesa e a incorporação de novos vetores com crescente sofisticação tecnológica evidenciaram a necessidade de normatizar e detalhar as atividades de Certificação, Segurança e Garantia da Qualidade de produtos no setor aeroespacial.

O Comando da Aeronáutica (COMAER), em atendimento a essa necessidade, emitiu, em janeiro de 2014, a Diretriz do Comando da Aeronáutica (DCA) 800-2 "Garantia da Qualidade e da Segurança de Sistemas e Produtos no COMAER", com a finalidade de estabelecer normas e procedimentos, bem como atribuir competências a organizações do COMAER, para o exercício das atividades relativas à certificação de produtos aeronáuticos, espaciais, de infraestrutura e de controle do espaço aéreo, bem como de garantia governamental da qualidade desses produtos.

A DCA 800-2, reeditada em 2016, define Dificuldade em Serviço como todo e qualquer evento com potencial de diminuir o nível de segurança na operação ou da capacidade de execução da missão dos produtos aeronáuticos e de defesa de emprego aeronáutico, tais como acidentes, incidentes, erros em procedimentos e documentos de operação e manutenção, falhas, mau funcionamento e defeitos.

A mesma Diretriz atribui ao Departamento de Ciência e Tecnologia Aeroespacial (DCTA) a responsabilidade de gerenciar as Dificuldades em Serviço, sempre que houver indícios que a dificuldade está relacionada a problemas de projeto, ou de assessorar o Comando-Geral de Apoio (COMGAP), conforme disposto nos contratos de aquisição. O DCTA, por sua vez, delega ao Instituto de Fomento e Coordenação Industrial (IFI) esse papel.

Com a experiência em lidar com as Dificuldades em Serviço na Força Aérea Brasileira (FAB), o IFI percebeu a necessidade de estabelecer uma metodologia de controle de exposição ao risco. Em uma Dificuldade em Serviço cuja falha esteja relacionada ao projeto da aeronave, a correção de tal falha pode não ser imediata, necessitando-se de um tempo para que a fabricante possa desenvolver e implementar uma solução. Portanto, uma metodologia de controle de exposição ao risco pode auxiliar no julgamento de engenharia de qual o tempo adequado para que o produto continue a operar até a implementação da solução, sem que a segurança da operação seja afetada acima de um limite tolerável.

Com o propósito de desenvolver uma metodologia de análise de risco que se adequasse às particularidades da frota da FAB, o IFI, em parceria com a fabricante de aeronaves EMBRAER, promoveram um estudo baseado nas normas dos principais órgãos certificadores internacionais e em publicações técnico-científicas da área de segurança na aviação.

Foram analisadas três metodologias de controle de risco já aplicadas na aviação civil: o sistema TARAM da *Federal Aviation Administration* (FAA), o *Product Safety Monitoring* da EMBRAER e o GM AMC 21.A.3B *Defect Correction – Sufficiency of proposed corrective action* da *European Aviaton Safety Agency* (EASA). Das três metodologias estudadas, a que mais se mostrou adequada à frota da FAB foi a da EASA, a qual serviu de base para a criação da metodologia proposta para o COMAER.

Não obstante, como o guia da EASA foi desenvolvido com foco na aviação

civil, foram necessárias modificações no sentido de adaptar a metodologia às particularidades da aviação militar. Isto foi feito por meio de estudos e simulações realizados na parceria entre IFI e EMBRAER.

A metodologia que resultou ao final do processo se baseia no controle da exposição ao risco a que um produto estará sujeito durante toda sua vida em serviço. Por esse princípio, cada campanha de correção de falha pode tomar um tempo de reação tal que a exposição ao risco global das aeronaves se mantenha em um nível tolerável.

Vale ressaltar que o produto final resultante da aplicação do método não é uma regra, mas sim um guia para um valor de referência para a exposição ao risco. O tempo de reação resultado da metodologia deve ser submetido a análises de engenharia para que sejam avaliados aspectos particulares de cada campanha de correção. Assim, apesar do tempo de correção informado pela metodologia ser um excelente parâmetro, ele pode ser aumentado ou diminuído, justificadamente, pela equipe de analistas do DCTA.

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

1.1.1 Esta Instrução visa a detalhar a metodologia de controle de risco a ser aplicada nas Dificuldades em Serviço de produtos aeronáuticos da frota da Força Aérea Brasileira.

1.1.2 Os procedimentos descritos nesta Instrução servem como um guia para a aplicação da metodologia de controle de exposição ao risco. Os resultados gerados pela metodologia devem ser submetidos a análise de engenharia e podem ser ajustados, a critério justificado, pelos analistas responsáveis pelo processo de Dificuldade em Serviço em questão.

1.2 CONCEITUAÇÃO

Para os propósitos desta Instrução, os termos técnicos devem seguir as definições dos termos da ICA 57-21, em sua versão mais atual, bem como as definições abaixo discriminadas:

1.2.1 GERENCIAMENTO DO RISCO

O gerenciamento de risco é um termo genérico que engloba a avaliação e a mitigação dos riscos relativos aos perigos de um sistema e/ou de sua operação.

1.2.2 RISCO

A avaliação das consequências de um perigo, expresso em termos de probabilidade e severidade, tomando como referência a pior condição possível.

1.3 SIGLAS E ABREVIATURAS

SIGLA	DESCRIÇÃO
AC	*Advisory Circulars*
AMC	*Acceptable Means of Compliance*
ARP	*Aerospace Recommended Practice*
CFR	*Code of Federal Regulations*
CENIPA	Centro de Investigação e Prevenção de Acidentes Aeronáuticos
COMAER	Comando da Aeronáutica
COMGAP	Comando-Geral de Apoio
DCTA	Departamento de Ciência e Tecnologia Aeroespacial
DoD	*Department of Defense*
EASA	*European Aviation Safety Agency*
ER	Exposição ao Risco
FAA	*Federal Aviation Administration*
FAB	Força Aérea Brasileira

SIGLA	DESCRIÇÃO
FAR	*Federal Aviation Regulations*
IFI	Instituto de Fomento e Coordenação industrial
P	Probabilidade de ocorrência de um evento
RA	Objetivo de risco de aeronavegabilidade
RM	Risco Médio
SAE	*Society of Automotive Engineers*
T0(T zero)	Data do Início da Contagem do Tempo
TARAM	*Transport Airplane Risk Assessment Methodology*
TR	Tempo de Reação
VE	Valor Esperado
VU	Vida Útil da aeronave
Y	Percentual de alocação de exposição ao risco

1.4 ÂMBITO

Esta Instrução aplica-se a todas as Organizações Militares do Departamento de Ciência e Tecnologia Aeroespacial envolvidas em processos de desenvolvimento e certificação, bem como de segurança de sistemas e produtos aeronáuticos e de defesa.

1.5 NATUREZA

A presente Instrução é de natureza Ostensiva.

2 DESCRIÇÃO DA NORMA BASE (EASA)

2.1 CONTEXTUALIZAÇÃO

2.1.1 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 de performance mais racionais e por meio da influência de uma abordagem de *Safety Assessment* na definição dos requisitos.

2.1.2 Tradicionalmente, os níveis de risco relacionados com aeronavegabilidade, ou objetivo de risco de aeronavegabilidade, costumam ser 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 comercial, por exemplo, o objetivo geralmente é de não mais que 1 acidente catastrófico a cada 10.000.000 (dez milhões) de horas de voo. Entretanto, quando se particulariza para um determinado tipo de aeronave, os níveis de segurança atingidos variam numa faixa em torno do objetivo pontual.

2.1.3 Os níveis de risco relacionados com aeronavegabilidade alcançados podem variar de forma a estar abaixo do objetivo de risco definido, tornando a aeronave mais segura que o exigido, dada a impossibilidade de se projetar uma aeronave para atender apenas aos requisitos mínimos de segurança. Geralmente, na aviação civil, projeta-se uma aeronave para que ela seja mais segura que o requerido; uma aeronave não estará sempre operando em condições críticas de peso, posição do centro de gravidade, velocidade operacional e/ou condições ambientais (temperatura, humidade, nível de turbulência).

2.1.4 Por outro lado, os níveis de risco reais podem estar acima do objetivo pontual em virtude de variações nos parâmetros dos materiais ou dos processos de construção adotados, devido à deficiências de projeto, combinações não previstas de falhas ou por condições operacionais ou ambientais não previstas.

2.1.5 Por esses motivos, reconhece-se a necessidade de se monitorar as condições que tendem a elevar o nível de risco e de se tomar as medidas corretivas adequadas, quando aplicável, a fim de evitar que o nível de risco se eleve acima de um limite máximo aceitável.

2.1.6 Para a determinação do nível de risco máximo aceitável, devem ser levadas em conta as penalidades decorrentes de medidas corretivas a serem adotadas, que vão desde alguma restrição às capacidades operacionais de uma aeronave até à sua remoção de operação por meio de *grounding*.

2.1.7 Ao longo do tempo, vários parâmetros guiaram as decisões de questões relacionadas à segurança de voo. No passado, utilizou-se como medida a comparação entre o custo de se adotar uma determinada medida e o chamado “custo do risco”, ou seja, o custo de uma catástrofe multiplicado pela sua probabilidade de ocorrência. Esse tipo de avaliação foi substituído pelo controle dos níveis de exposição ao risco, isto é, o estabelecimento de objetivos de risco de aeronavegabilidade que determinado projeto de aeronave deve cumprir.

2.1.8 O objetivo de todos os envolvidos deve ser agir sem atrasos para minimizar os efeitos de qualquer situação com potencial de elevar significativamente a exposição ao risco. Entretanto, cabe aos órgãos certificadores deliberar sobre os programas mínimos de uma campanha de

correção, especialmente se o tempo solicitado pelos envolvidos para a correção das falhas é inviável ou inaceitável.

2.1.9 É justamente nesta parte que a metodologia de controle de exposição ao risco descrita nesta Instrução se aplica. Determinar, a partir de parâmetros específicos, um valor de referência para o julgamento do tempo de reação nas campanhas de correção.

2.2 METODOLOGIA EASA

2.2.1 A metodologia da EASA para controle de exposição ao risco na frota em operação é melhor compreendida assimilando-se a definição de risco como sendo a combinação da probabilidade de ocorrência de um evento indesejado (que resulta de uma condição de falha) com a severidade das consequências desse evento.

2.2.2 Por sua vez, o controle da exposição ao risco é feito prioritariamente com medidas que diminuam o risco da operação, sejam elas modificações na aeronave, nos perfis de operação, nos procedimentos de manutenção e na frequência e detalhamento de inspeções. Tomadas tais medidas, caso elas não sejam suficientes para restabelecer um nível de segurança adequado, a segunda linha de ação seria controlar o tempo da campanha de correção, ou seja, o tempo que a fabricante pode dispor para desenvolver e implementar as soluções de engenharia definitivas para o problema.

2.2.3 A metodologia se baseia em respeitar um objetivo de risco de aeronavegabilidade, um nível máximo do risco que deve ser respeitado pelo projeto da aeronave. Este parâmetro deve refletir o quanto de risco de aeronavegabilidade a sociedade e, no caso da operação militar, o COMAER estão dispostos a conviver. Ressalta-se que risco de aeronavegabilidade está relacionado com qualquer falha oriunda dos sistemas da aeronave e que afete sua capacidade de cumprir a missão com segurança. Por exemplo, falhas de projeto, mau funcionamento de equipamentos, erros na definição dos procedimentos de emergência ou de manutenção, etc. Excluem-se falhas na execução dos procedimentos de emergência ou de manutenção, falhas causadas por fatores humanos, condições meteorológicas, etc.

2.2.4 Em geral, conforme 2.1.3, na operação normal das aeronaves, as mesmas se encontram em um nível de risco abaixo do objetivo de risco de aeronavegabilidade, uma vez que no projeto e desenvolvimento da aeronave são extrapolados os valores mínimos de segurança e a aeronave, nem sempre, operará em condições críticas.

2.2.5 Entretanto, durante uma campanha de correção, a aeronave voará com alguma condição que degrada a sua segurança e, por consequência, eleva o nível de risco de sua operação. Por vezes, esse risco é tal que supera o valor definido como objetivo de risco de aeronavegabilidade.

2.2.6 Durante tais campanhas é que a metodologia de controle de exposição ao risco torna-se efetiva, pois, ao limitar o tempo em que as aeronaves conviverão com a falha que degrade sua segurança, espera-se que, ao final de sua vida útil, o risco médio ao qual a aeronave tenha sido exposta respeite o objetivo de risco de aeronavegabilidade.

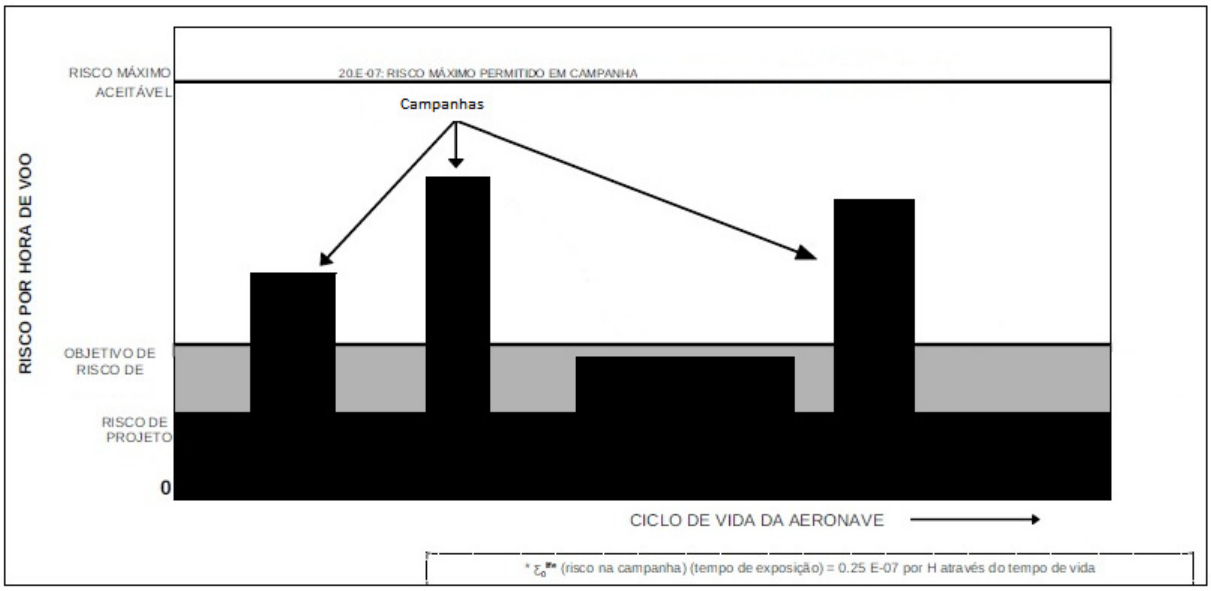


Figura 1: Exposição ao risco ao longo da vida da aeronave. (fonte: GM AMC 21.A.3B *Defect Correction – Sufficiency of proposed corrective action* da *European Aviaton Safety Agency* (EASA), adaptado pelo autor)

2.2.7 A Figura 1 ilustra o princípio da metodologia. A linha horizontal do objetivo de risco de aeronavegabilidade reflete o valor estabelecido durante o processo de certificação do projeto da aeronave. Durante a operação normal da aeronave, o risco a que ela estará sujeito é o risco de projeto, visualmente abaixo do objetivo de risco de aeronavegabilidade. Nesses casos, a parte "em cinza" representa a margem de risco entre esses dois valores. Quando há um fator que degrade a segurança, que demande uma campanha de correção, o risco se eleva, o que é representado pelos retângulos acima do risco de projeto.

2.2.8 A metodologia se baseia em limitar a largura dos retângulos (tempo de exposição) para que, ao final do ciclo de vida, o risco médio ao qual a aeronave tenha sido exposta durante a operação fique abaixo da área definida pelo objetivo de risco de aeronavegabilidade.

2.2.9 É importante que se estabeleça um limite superior de risco, representado na figura pelo risco máximo permissível, acima do qual as aeronaves não poderão operar, pois o risco seria muito alto, ainda que por um curto período de operação.

2.2.10 Para ilustrar o método da EASA, tomemos um exemplo de aplicação da metodologia para a aviação civil contido no documento da referência (GM AMC 21.A.3B *Defect Correction – Sufficiency of proposed corrective action da European Aviation Safety Agency* (EASA)). O histórico da aviação comercial de aeronaves de transporte revela uma média de um acidente catastrófico, de causa relacionada a sistemas, a cada 10 milhões de horas de voo. Desse valor foi definido o objetivo de risco de aeronavegabilidade, ou seja, 10^{-7} eventos/hora de voo.

2.2.11 O limite superior para a probabilidade de ocorrência de um evento catastrófico é definido como 20 vezes o objetivo de risco de aeronavegabilidade. Qualquer falha que ofereça um risco maior que este, contribuirá mais para a ocorrência de uma catastrófe que todas as outras causas (operacionais e ambientais) juntas. Nesses casos, a aeronave não deve ser operada, permitindo-se no máximo o retorno à base de manutenção.

2.2.12 Por outro lado, qualquer condição de falha de severidade catastrófica que apresente probabilidade menor que 10^{-9} eventos por hora de voo, é considerada aceitável, de acordo

com a *Advisory Circular* (AC) 25.1309–1A: *System Design and Analysis*. Este é definido como um limite inferior para a probabilidade, e caso a condição de falha apresente probabilidade de ocorrência menor que esta, nenhuma ação será necessária.

2.2.13 Para condições de falha que ofereçam um risco intermediário entre os dois limites impostos, devem ser tomadas providências para sua mitigação, o que poderá configurar uma campanha de correção. A metodologia de controle de exposição ao risco oferecerá uma referência de tempo que os fabricantes podem dispor para resolver o problema.

2.2.14 As estimativas da EASA são de que na operação normal da aeronave, o risco a que ela estará sujeita, ou seja, risco básico de projeto, corresponda a 3/4 do objetivo de risco de aeronavegabilidade, restando 1/4 de margem de risco para ser alocado para as campanhas de correção. Estima-se ainda que, ao longo da vida útil da aeronave, haverá da ordem de 10 campanhas de correção. Assim sendo, para que ao fim da vida útil da aeronave tenha-se um risco médio inferior ao objetivo de risco de aeronavegabilidade, cada campanha de correção deve acrescentar não mais que 1/40, ou 2,5%, do risco médio, ou seja, o produto entre a vida útil da aeronave e o objetivo de risco de aeronavegabilidade.

2.2.15 A restrição definida será respeitada, matematicamente, quando o produto entre a taxa de falha real e o tempo de reação para a campanha de correção se igualarem a 2,5% do risco médio.

A figura 2 ilustra esta alocação de exposição ao risco de 2,5% do valor global.

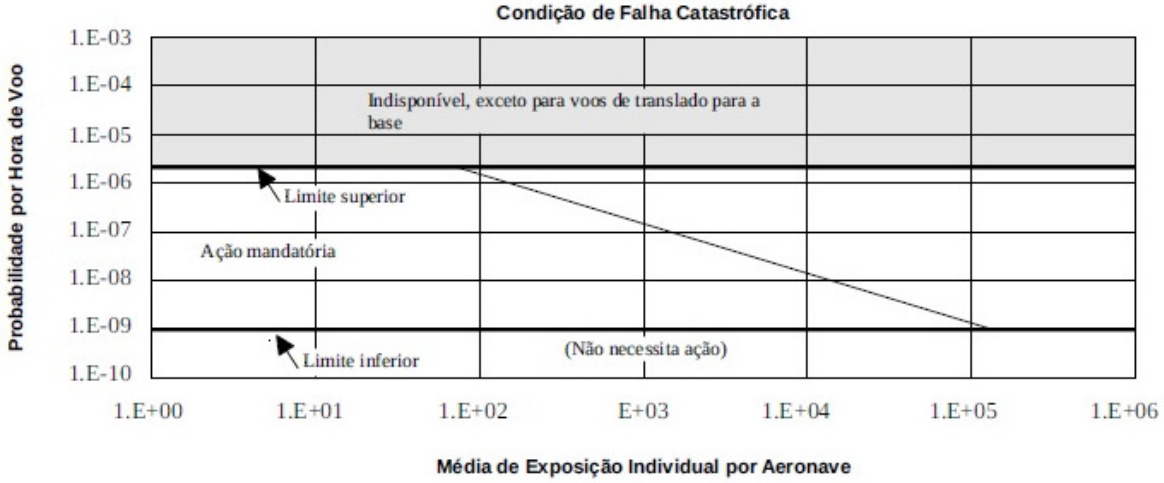


Figura 2: Exposição ao risco admissível para uma aeronave comercial (exemplo da EASA fonte: GM AMC 21.A.3B *Defect Correction – Sufficiency of proposed corrective action* da *European Aviaton Safety Agency*, adaptado pelo autor).

2.2.16 As linhas horizontais representam os limites inferior e superior de probabilidade. A linha inclinada representa a restrição de 2,5% da exposição ao risco. Por essa linha, a cada valor de probabilidade real da condição de falha que motiva a campanha de correção, corresponderá um valor de tempo de reação. Mais ainda, quanto maior a taxa de falha real, menor será o tempo de reação.

2.2.17 Para exemplificar, suponhamos uma aeronave comercial com vida útil estimada em 60.000 horas de voo. Considerando-se um objetivo de risco de aeronavegabilidade de 10^{-7} eventos por hora de voo, o Risco Médio (RM) será de:

$$RM = 2{,}5\% \times 10^{-7} \times 60.000 = 1500 \times 10^{-7}$$

O Tempo de Reação (TR) para cada nível de probabilidade (P) deve obedecer a:

$$TR \times P = RM = 1500 \times 10^{-7}$$

2.2.18 Considerando-se um consumo de esforço aéreo de cerca de 3.000 horas por ano por aeronave, a tabela 1 ilustra a distribuição de tempo de acordo com a probabilidade.

Taxa de eventos catastróficos (por horas de voo)	Tempo médio de reação para aeronaves em risco (em horas de voo)	Tempo baseado em calendário
4×10^{-8}	3 750	15 meses
5×10^{-8}	3 000	12 meses
1×10^{-7}	1 500	6 meses
2×10^{-7}	750	3 meses
5×10^{-7}	300	6 semanas
1×10^{-6}	150	3 semanas
1×10^{-5}	15	Retorno à base

Tabela 1: Distribuição de tempo de reação por nível de probabilidade do evento

2.2.19 O tempo de reação determinado se aplica a cada aeronave da frota. Deve ser imposta uma limitação adicional para que em frotas grandes, ou em valores de probabilidade elevados, o tempo de reação não conduza a uma certeza de catástrofe quando considerada toda a frota sujeita á falha. Para isso, a EASA impõe que o valor esperado dos eventos de severidade catastrófica, considerando-se a operação de toda a frota, não seja maior que 0,1, o que corresponde a uma expectativa de catástrofe não maior que 10%.

2.2.20 A metodologia descrita pela EASA foi desenvolvida com foco na aviação civil e não atende a todas as particularidades da aviação militar. Foram necessárias adaptações nesse método para corresponder às necessidades da FAB. O procedimento final, produto dos estudos do grupo de trabalho do IFI e da EMBRAER, segue descrito no item 4.

3 PROCEDIMENTOS PARA APLICAÇÃO DA METODOLOGIA DE CONTROLE DE EXPOSIÇÃO AO RISCO

3.1 SEVERIDADE E PROBABILIDADE DE FALHA

A determinação da severidade e a estimativa da probabilidade de ocorrência da condição de falha devem ser feitas caso a caso e não são objetos dessa metodologia. Para a determinação da severidade, recomenda-se a leitura da *AC* 25.1309–1A, ou *ARP 4761 – Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment* ou outro documento que tenha sido referência durante a certificação ou qualificação da aeronave em questão. Para uma estimativa de probabilidade, recomenda-se a leitura da norma (*ARP) 5150 – Safety Assessment of Transport Airplanes in Commercial Service*.

3.2 ANÁLISE QUALITATIVA DA PROBABILIDADE

3.2.1 Quando uma estimativa puramente quantitativa da probabilidade de ocorrência da condição de falha não for possível, recomenda-se adotar valores intermediários de probabilidade por hora de voo, utilizando-se a média geométrica dos limites de cada um dos intervalos do nível de probabilidade que definem as taxas aceitáveis para cada nível de severidade.

3.2.2 Exemplificando, para aeronaves comerciais, certificadas de acordo com o CFR 14 Part 25 da FAA, a AC 25.1309–1A define 5 níveis de probabilidade: *frequent* (probabilidade maior que 10^{-3}), *probable* (probabilidade entre 10^{-3} e 10^{-5}), *remote* (probabilidade entre 10^{-5} e 10^{-7}), *extremely remote* (entre 10^{-7} e 10^{-9}) e *extremely improbable* (probabilidade menor que 10^{-9}). Para cada um desses níveis de probabilidade está associada uma descrição de sua frequência. O nível *extremely remote*, por exemplo, se aplica a condições de falha que não se espera que ocorra várias vezes mas que é possível que ocorra ao menos uma vez na vida operacional da frota. Se for identificado que uma falha se encaixa nessa descrição, e não for possível estimar numericamente sua probabilidade de ocorrência, recomenda-se tomar por referência o valor de probabilidade igual à média geométrica do intervalo definido para o *extremely remote*, ou seja (raiz) (10^{-7} x 10^{-9}) = 10^{-8}. Por extensão das faixas de valores definidas na AC 25.1309–1A, para falhas de probabilidade *frequent* pode-se adotar a média entre 10^{-3} e 1 (~3,16 x 10^{-2}). Para falhas *extremely improbable* não há necessidade de realizar este cálculo, uma vez que a probabilidade por hora de voo estará abaixo do limite inferior aceitável.

3.3 LIMITE INFERIOR PARA O CONTROLE DE RISCO

3.3.1 Trata-se de um nível de risco que é baixo o bastante para não afetar de maneira significativa o risco total em que a aeronave estará sujeita durante toda sua operação. Caso o nível do risco em estudo seja igual ou menor que esse limite, entende-se que é seguro manter a operação mesmo com esse acréscimo no risco total e nenhuma ação precisa ser tomada.

3.3.2 Na etapa de projeto da aeronave, são definidas taxas de falha máximas aceitáveis para cada nível de severidade das possíveis condições de falha. Por exemplo, para aeronaves certificadas de acordo com o CFR 14 *Part* 25 da FAA, AC 25.1309–1A determina que qualquer condição de falha de severidade catastrófica não pode ter probabilidade de ocorrência maior que 10^{-9} eventos por hora de voo. Para um modo de falha de severidade *hazardous* esse valor não deve superar 10^{-7} eventos por hora de voo.

3.3.3 A Tabela do Anexo B traz os valores de limites inferiores para o controle de risco, abaixo dos quais nenhuma ação é requerida, definidos para algumas aeronaves da frota da Força Aérea Brasileira. Para as demais aeronaves, um estudo caso a caso deverá ser realizado durante a análise de risco.

3.4 LIMITE SUPERIOR PARA CONTROLE DO RISCO

3.4.1 Deve ser imposto também um limite superior para o risco, acima do qual não se pode tolerar que a aeronave opere. Não se pode permitir que o risco atinja níveis excessivamente altos para uma determinada quantidade de horas de voo, mesmo sendo pequeno o seu efeito sobre o risco global da operação, ou seja, em toda a vida útil da aeronave. Se isso fosse aceito, uma operação poderia ter seu nível de risco demasiadamente alto.

3.4.2 Adotando-se o parâmetro de referência mencionado pela EASA em seu guia, recomenda-se que seja estipulado um limite superior no valor de 20 vezes o objetivo de risco de aeronavegabilidade. Qualquer fator que ofereça um risco acima desse, passa a ter uma contribuição, para a ocorrência de uma catástrofe, maior que todas as outras causas, inclusive as não relacionadas com aeronavegabilidade (erros humanos, meteorologia, falhas de manutenção, etc.).

3.5 OBJETIVO DE RISCO DE AERONAVEGABILIDADE

3.5.1 Esse parâmetro, expresso em termos de uma taxa de acidentes causados por falhas de aeronavegabilidade (falhas de sistemas, erros nos manuais de manutenção ou nos procedimentos de emergência, etc.) por hora ou ciclo de voo, deve refletir o quanto de risco de aeronavegabilidade a sociedade e o COMAER estão dispostos a aceitar na operação dos produtos aeronáuticos operados pela Força Aérea Brasileira.

3.5.2 Uma referência histórica para esse parâmetro pode ser determinada pela combinação da taxa de acidentes daquele produto específico ou de uma classe de produtos semelhantes, com uma estimativa do percentual dos acidentes que são de origem sistêmica. A Tabela do Anexo B traz valores de referência para a taxa de acidentes de algumas aeronaves da frota da Força Aérea Brasileira. Para as demais aeronaves, um estudo caso a caso deverá ser realizado durante a análise de risco.

3.5.3 Para o percentual de acidentes que é devido a razões de aeronavegabilidade, a EASA recomenda para a aviação civil comercial, que seja considerado algo em torno de 10% dos acidentes totais. Na pesquisa feita durante a elaboração desta ICA, observou-se que a base de dados do CENIPA, à época, não dispunha de informação suficiente para substituição desse valor de forma consistente. Além disso, os mesmos 10% também encontram embasamento no documento *Military Aviation Safety, US Air Force Center Annual Report 2012*.

3.5.4 Por tais motivos, recomenda-se utilizar como referência para o objetivo de risco de aeronavegabilidade o valor 10% da taxa histórica de acidentes catastróficos do produto aeronáutico ou de uma classe semelhante.

3.6 PERCENTUAL DA EXPOSIÇÃO AO RISCO ALOCADO PARA A CAMPANHA DE CORREÇÃO.

3.6.1 Para se chegar a uma recomendação sobre qual o percentual do total da exposição ao risco da operação de um produto aeronáutico poderia ser alocado para uma campanha de correção, combinou-se o valor de referência indicado no guia da EASA com algumas

simulações numéricas aplicadas à frota de aeronaves de defesa.

3.6.2 Para o caso de aeronaves civis de transporte, o objetivo de segurança de cada sistema é igual a (10^{-9}) e o objetivo de risco de aeronavegabilidade é igual a (10^{-7}). A EASA recomenda que se use um percentual de 2,5% de alocação de risco por campanha (25% dividido em 10 campanhas). Em aeronaves militares semelhantes às aeronaves civis de transporte, como é o caso do KC-390, decidiu-se por adotar o mesmo percentual de alocação de risco por campanha, pois o tempo de resposta decorrente dessa alocação de risco é razoável.

3.6.3 Já para as aeronaves menores, em que se observa uma diferença entre objetivo de segurança e objetivo de risco de aeronavegabilidade de apenas uma ordem de grandeza (10^{-6} e 10^{-5}, por exemplo), os estudos revelaram que manter um percentual de alocação de risco de apenas 2,5% resultaria num tempo de campanha muito curto. Portanto, decidiu-se por adotar valores diferentes para aeronaves que se encaixam nessa situação.

3.6.4 Definiu-se um tempo de correção que passou a ser o parâmetro norteador para determinar o percentual de alocação de risco adequado. Caso a probabilidade do evento esteja no nível do objetivo de segurança para condições de falha com severidade catastrófica definido para o sistema, o percentual de alocação de risco deve ser tal que permita um tempo de correção correspondente a 250% da vida útil da aeronave (similarmente ao que ocorre no guia da EASA). Caso a probabilidade esteja no nível do objetivo de risco de aeronavegabilidade, o percentual de alocação de risco deve ser de 10%, o que permitiria um tempo de correção de também 10% da vida útil da aeronave.

3.6.5 Para valores intermediários, deve ser feita uma interpolação linear para calcular o percentual de alocação de risco. Caso o nível de probabilidade seja maior que o do objetivo de risco de aeronavegabilidade, o percentual de alocação de risco deve ser mantido em 10%. Nos estudos que levaram a esta metodologia, foram testados outros tipos de interpolação, como a logarítmica e as polinomiais de ordens 3 e 4, entretanto, dada a semelhança entre os resultados e para simplificar os cálculos, optou-se por manter a interpolação linear.

3.6.6 Com relação à estimativa do número de campanhas de correção ao longo da vida útil da aeronave, foi mantida uma estimativa de 10 campanhas para aeronaves semelhantes às aeronaves civis de transporte e de 1 campanha para aeronaves cujos objetivo de segurança e objetivo de risco possuem uma ordem de grandeza de diferença, por exemplo, de 10^{-6} e 10^{-5} respectivamente.

3.6.7 Considerou-se que as aeronaves com um padrão de objetivo de segurança e objetivo de risco de 10^{-6} e 10^{-5}, respectivamente, têm uma quantidade menor de sistemas críticos que apresentam condições de falha que podem levar a evento catastrófico (baseado na AC 23.1309–1E: *System Safety Analysis and Assessment for Part 23 Airplanes*, em que aviões nessa categoria tem por volta de 10 condições de falhas potencialmente catastróficas, diferentemente de uma aeronave comercial de transporte de passageiros, onde é considerado por volta de 100). Com uma menor quantidade desses sistemas, espera-se uma menor quantidade de condições de falha não previstos durante o projeto, os quais demandariam campanhas de correção. Justifica-se, assim, a redução da ordem de grandeza da expectativa de campanhas de correção.

3.7 CÁLCULO DO TEMPO DE REAÇÃO

O tempo de reação, determinado pelo critério de alocação de risco, deve ser tal

que a exposição ao risco durante a campanha de correção se iguale ao percentual de exposição ao risco alocado para ela conforme o procedimento descrito anteriormente. Em outras palavras, o produto entre o tempo de reação e a probabilidade de ocorrência do evento deve ser igual ao produto entre o percentual de alocação de exposição ao risco, o objetivo de risco de aeronavegabilidade e a vida útil da aeronave.

Para esse cálculo definamos as seguintes variáveis:

- P = Probabilidade de ocorrência de um evento;
- TR = Tempo de Reação;
- RA = Objetivo de risco de aeronavegabilidade;
- Y = Percentual de alocação de exposição ao risco;
- VU = Vida útil da aeronave.

A expressão matemática para essa sentença é:

$$TR \times P = VU \times Y \times RA$$

Em que TR é a variável desconhecida.

3.8 DEFINIÇÃO DA DATA DE INÍCIO DA CONTAGEM DO TEMPO DE EXPOSIÇÃO (T0)

3.8.1 De uma forma geral, o T0 será a data da emissão de um documento do IFI sobre o problema em questão, após a realização de uma análise de risco, mesmo que preliminar. Caso a fabricante valide internamente uma análise antes do pronunciamento do IFI e este Instituto endosse a classificação de severidade e probabilidade da análise, o T0 fica definido como a data da validação da análise realizada pela fabricante.

3.8.2 Na possibilidade de haver duas análises de risco, uma pela fabricante e outra pelo IFI, o T0 oficial será o definido pelo IFI, e caso o IFI não endosse a classificação de severidade e probabilidade da fabricante, o T0 oficial será a data da emissão de um documento do IFI sobre o problema.

3.9 LIMITAÇÃO PELO CRITÉRIO DO VALOR ESPERADO (VE)

3.9.1 Além da limitação individual por aeronave, determinada pelo critério de alocação de risco e descrita nos itens anteriores, deve ser considerada também uma limitação para a operação da frota de aeronaves que estarão sujeitas à falha em questão. Isso evita que, mesmo que haja controle sobre o risco individual de cada aeronave, a frota seja tão grande, ou a probabilidade seja tão alta que, considerando-se o conjunto de aeronaves, tenha-se a iminência de um evento catastrófico.

$$VE = P \times TR$$

3.9.2 Para essa limitação adicional, usa-se como parâmetro o valor esperado de eventos, calculado como o produto entre a probabilidade da condição de falha e o número de horas de voo (ou ciclos de voo) a ser executado pela frota.

3.9.3 Para falhas de severidade catastrófica, o valor esperado dos eventos não deve superar 0,1. Isto se traduz em uma expectativa não maior que 10% de que uma catástrofe venha a ocorrer durante a campanha de correção.

4 DISPOSIÇÕES TRANSITÓRIAS

4.1 O IFI e as demais Organizações Militares que desempenham funções relacionadas a Dificuldades em Serviço que venham a utilizar a Metodologia de Análise de Risco, podem consultar esta instrução a partir da data de sua publicação.

5 DISPOSIÇÕES FINAIS

5.1 A presente instrução entrará em vigor na data de sua publicação de acordo com sua respectiva Portaria de Aprovação.

5.2 Os casos não previstos nesta Instrução devem ser submetidos à apreciação do Diretor-Geral do DCTA, por intermédio do Diretor do IFI.

REFERÊNCIAS

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)

BRASIL. Ministério da Defesa. Comando da Aeronáutica. Estado-Maior da Aeronáutica. *Portaria n° 1.164/GC3, de 19 de setembro de 2016*. Aprova a reedição da Diretriz que dispõe sobre a Garantia da Qualidade e da Segurança de Sistemas e Produtos no COMAER. Brasília, 2016. (DCA 800-2)

BRASIL. Ministério da Infraestrutura. Agência Nacional de Aviação Civil (ANAC). *Resolução nº 303, de 5 de Fevereiro de 2014.* Aprova o Regulamento Brasileiro de Aviação Civil (RBAC) nº 25, emenda nº 136 que define Requisitos de Aeronavegabilidade para Aviões Cateroria Transporte. Brasília, 2014.

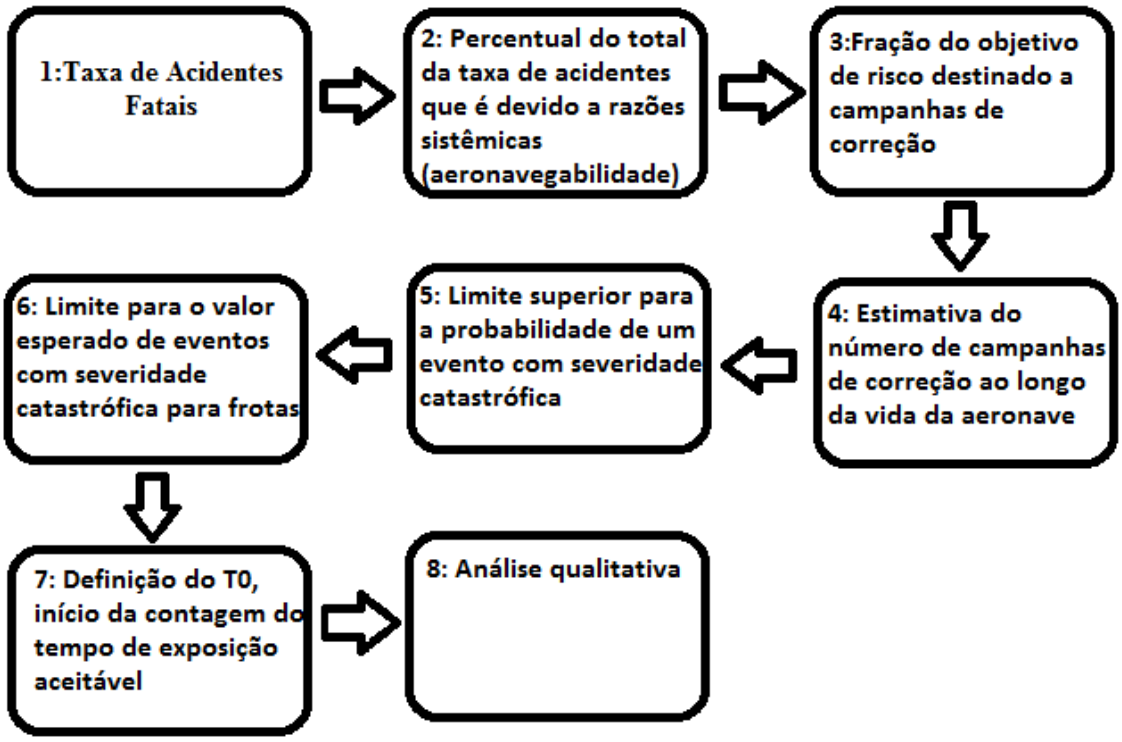
ESTADOS UNIDOS DA AMÉRICA. FEDERAL AVIATION ADMINISTRATION (FAA). *Advisory Circular (AC) 25.1309–1A: System Design and Analysis*. Junho, 1988.

ESTADOS UNIDOS DA AMÉRICA. FEDERAL AVIATION ADMINISTRATION (FAA). *Advisory Circular (AC)* 23.1309–1E*: System Safety Analysis and Assessment for Part 23 Airplanes.* Novembro, 2011.

SOCIETY OF AUTOMOTIVE ENGINEERS INTERNATIONAL (SAE). *Aerospace Recommended Practice* (*ARP) 4761 – Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.* Dezembro, 1996.

SOCIETY OF AUTOMOTIVE ENGINEERS INTERNATIONAL (SAE). *Aerospace Recommended Practice (ARP) 5150 – Safety Assessment of Transport Airplanes in Commercial Service*. Novembro, 2003

Anexo A – Sequência de Atividades



Anexo B – Tabela de Exposição ao Risco

Parâmetro/Programa	Guia EASA	KC-390 (Militar)	Super Tucano A-29	Tucano T-27	AMX/ A-1M	F-5M
Vida do avião	60000 FH (ex.)	45000 FH ou 15000 FC	FAB/FARD: 12000 FH FAC/EPA: 8000 FH FOM: 12000 FH LAS: 11500 FH	6000 FH	4000 FH	8000 FH
Taxa total de acidentes	1.00E-06	1.00E-05	1.00E-05	1.00E-04	1.00E-04	1.00E-04
Taxa acidentes sistêmicos	1.00E-07	1.00E-06	1.00E-06	1.00E-05	1.00E-05	1.00E-05
Limite Inferior Catastrófico	1.00E-09	1.00E-08	1.00E-07	1.00E-06	1.00E-06	1.00E-06
Limite Inferior *Hazardous*	1.00E-07	1.00E-06	1.00E-05	1.00E-05	1.00E-05	1.00E-05
Porcentagem *Unforeseen Situations*	25%	25%	Linearmente de 25% (para 1E-7) a 10% (para 1E-6)	Linearmente de 25% (para 1E-6) a 10% (para 1E-5)		
Número de *Unforeseen Campaign*	10	10				
Limite Superior Catastrófico	2.00E-06	2.00E-05	2.00E-05	2.00E-04	2.00E-04	2.00E-04
Limite Superior *Hazardous*	2.00E-04	2.00E-03	2.00E-03	2.00E-03	2.00E-03	2.00E-03
Prob evento CAT durante retificação	0.1	0.1	0.1	0.1	0.1	0.1
Prob evento HAZ durante retificação	0.5	0.5	0.5	0.5	0.5	0.5