GUIA DE CERTIFICAÇÃO

SUPERINTENDÊNCIA DE AERONAVEGABILIDADE (SAR)

GERÊNCIA GERAL DE CERTIFICAÇÃO DE PRODUTO AERONÁUTICO (GGCP)

CERTIFICAÇÃO SUPLEMENTAR DE TIPO

GUIA DE ANÁLISE DE FALHAS (“SAFETY ASSESSMENT”) PARA GRANDES MODIFICAÇÕES

São José dos Campos-SP

Outubro de 2015

Sumário

1. Escopo

Este guia pode ser utilizado como forma de esclarecimento e auxílio quando for necessário realizar uma análise de falhas (“Safety Assessment”), relativa a sistemas, equipamentos e instalações em aeronaves, conforme preconizado nos requisitos de aeronavegabilidade pertinentes, RBAC/FAR 23.1309, 25.1309, 27.1309 e 29.1309.

Este material não é mandatório e nem possui caráter regulatório. Deve ser entendido apenas como um suporte para a elaboração da análise de falhas (“Safety Assessment”) em processos de aprovação de grandes modificações apresentados a esta gerência (ANAC/SAR/GGCP) para obtenção do Certificado Suplementar de Tipo (CST) ou SEGVOO 001. Por outro lado, este texto visa contribuir para a padronização dos relatórios apresentados pelos requerentes desses processos, bem como otimizar o tempo gasto nas análises feitas pelos especialistas do grupo PST.

2. Documentos e Regulamentos Relacionados

RBAC/FAR Part	23.1309, 25.1309, 27.1309 e 29.1309.
AC 20-136A	Protection of Aircraft Electrical/Electronic Systems Against the Indirect Effects on Lightning
AC 20-158	The Certification Aircraft Electrical and Electronic Systems for Operation in the High-Intensity Radiated Fields (HIRF)
AC 23.1309-1E	System Safety Analysis and Assessment for Part 23 Airplanes
AC 25.1309-1A	System Design and Analysis
AC 27-1B	Certification of Normal Category Rotorcraft
AC 29-2C	Certification of Transport Category Rotorcraft
RTCA/DO-160G	Environmental Conditions and Test Procedures for Airborne Equipment
RTCA/DO-178B	Software Considerations in Airborne Systems and Equipment Certification
RTCA/DO-254	Design Assurance Guidance for Airborne Electronic Hardware
ARP 4754A	Guidelines for Development of Civil Aircraft and Systems
ARP 4761	Guidelines and Methods for Conduction the Safety Assessment Process on Civil Airborne Systems and Equipment
AC 43.13-1B	Acceptable Methods, Techniques, and Practices - Aircraft Inspection and Repair
AC 43.13-2B	Acceptable Methods, Techniques, and Practices - Aircraft Alterations

3. Aplicabilidade

O requisito “Equipment, systems, and installations” (§ 23.1309 / 25.1309 / 27.1309 / 29.1309) é aplicável a qualquer instalação de equipamentos ou sistemas em aeronaves. Novas tecnologias nas áreas de projetos de sistemas elétricos, eletrônicos e mecânicos, que incluam eletrônica complexa com software, hardware complexo, HIRF (“High Intensity Radiated Fields**”**) e/ou “Lightning”, requerem análise para cumprimento com o requisito do §23/25/27/29.1309. Um SSA (“System Safety Assessment”) é requerido para se determinar o grau de confiabilidade para o processo, através dos documentos de referência, tais como RTCA/DO-178, RTCA/DO-254, AC 20-158, ou equivalentes. Por outro lado, a seção §23/25/27/29.1309 deve ser usada para determinar a condição de falha, probabilidade da condição de falha, “Development Assurance Level” (DAL) de software e hardware complexo. Além disso, o processo de “Safety Assessment” é utilizado para determinar a classificação da condição de falha, o que determina também o nível de proteção de HIRF e “Lightning”, caso aplicável. Cabe ressaltar que, para sistemas mecânicos ou analógicos eletromecânicos, simples e convencionais, com projeto e processo de certificação bem estabelecidos (onde a instalação não é complexa), o “Safety Assessment” pode ser realizado por uma avaliação qualitativa, baseado na experiência de serviço e julgamento de engenharia. Nesses casos, uma FHA (“Functional Hazard Assessment”) ou uma avaliação de projeto pode satisfazer o requisito de “safety”.

Contudo, a seção §23/25/27/29.1309 não se aplica a desempenho, características de voo requeridas na subparte B, e requisitos estruturais das subpartes C e D. Estão excluídos as estruturas de voo, como por exemplo, asa, empenagem, superfícies de controle, fuselagem, suporte do motor e trem de pouso. Deve-se aplicar um julgamento baseado em experiência em engenharia e operacional, ao determinar se um sistema é complexo ou não. Comparações com sistemas similares, previamente aprovados podem, muitas vezes, auxiliar nessa análise.

4. Acrônimos

AC	Advisory Circular
AFMS	Airplane Flight Manual Supplement
ARP	Aerospace Recommended Practice
CCA	Common Cause Analysis
CFR	Code of Federal Regulations
CMA	Common Mode Analysis
DAL	Development Assurance Level
FAA	Federal Aviation Administration
FHA	Functional Hazard Assessment
FMEA	Failure Modes and Effects Analysis
FTA	Fault Tree Analysis
GNSS	Global Navigation Satellite System
HIRF	High Intensity Radiated Fields
ICA	Instructions for Continued Airworthiness
IFR	Instrument Flight Rules
MFD	Multifunction Flight Display
MOC	Means of Compliance
MTBF	Mean Time Between Failures
PFD	Primary Flight Display

PRA	Particular Risk Analysis
PSSA	Preliminary System Safety Assessment
SSA	System Safety Assessment
TSO	Technical Standard Order
VFR	Visual Flight Rules
ZSA	Zonal Safety Analysis

5. Definições

a. Avaliação de projeto ("Design Appraisal"). É uma avaliação qualitativa da integridade e segurança do sistema projetado. Uma avaliação efetiva requer experiência nesse tipo de análise.

b. Avaliação da Instalação. Avaliação qualitativa da integridade e segurança da instalação. Quaisquer desvios das práticas de instalação normalmente aceitas pela indústria devem ser avaliados.

c. Carga essencial. São os equipamentos imprescindíveis utilizados para o voo seguro e que requerem uma fonte de alimentação para seu funcionamento adequado.

d. Condição de operação adversa. Trata-se de um conjunto de circunstâncias operacionais ou ambientais aplicáveis a uma aeronave que, combinadas com uma falha ou outra situação de emergência, resulta no aumento significativo da carga normal de trabalho da tripulação.

e. Continuação de voo e pouso seguros. Essa condição significa que, possivelmente usando procedimentos de emergências, a aeronave é capaz de continuar o voo de maneira controlada e segura, assim como pousar, sem que para isso seja requerido um piloto com habilidades ou força excepcionais.

f. Condições de falha prováveis. São as condições de falha que são presumidas de ocorrer uma ou mais vezes durante toda a vida em serviço de uma aeronave. Essas condições de falha podem ser determinadas com base na experiência em serviço com componentes similares em aeronaves semelhantes.

g. Condições de falha remota. São as condições de falha que são improváveis de ocorrer em cada aeronave durante toda a sua vida em serviço, mas que podem ocorrer algumas vezes quando considerada toda a vida operacional de diversas aeronaves desse Tipo.

h. Condições de falha extremamente remotas. São as condições de falha que não são previstas de ocorrer em cada aeronave durante toda a sua vida em serviço, mas que podem ocorrer algumas vezes quando considerada toda a vida operacional de todas as aeronaves desse Tipo.

i. Condições de falha improváveis. São as condições de falha que são improváveis de ocorrer em cada aeronave durante toda a sua vida em serviço, mas que podem ocorrer algumas vezes quando considerada toda a vida operacional de diversas aeronaves desse Tipo. Além disso, são as condições de falha que não são previstas de ocorrer em cada aeronave durante toda a sua vida em serviço, mas que podem ocorrer algumas vezes quando considerada toda a vida operacional de todas as aeronaves desse Tipo.

j. Condições de falha extremamente improváveis. Para as categorias de aeronaves commuter e transporte, são as condições de falha tão improváveis que não são previstas de ocorrer durante toda a vida em

serviço do conjunto de todas as aeronaves de um Tipo. Para aeronaves de categoria diferente de commuter ou transporte, a probabilidade de ocorrência pode ser maior.

k. Conceito de falha simples. O objetivo desse conceito de projeto é permitir que a aeronave continue o voo e o pouso de forma segura, após qualquer falha única.

l. Condições de falha. São condições que tem efeitos, tanto diretos quanto indiretos, na aeronave, nos ocupantes, ou em ambos, que são causadas ou contribuem para uma ou mais falhas ou erros, considerando-se: a fase do voo, efeitos relevantes na operação da aeronave, condições ambientais e eventos externos. As condições de falha são classificadas de acordo com a severidade, a saber:

(1) "No Safety Effect". São as condições de falhas que não degradam a capacidade operacional da aeronave e nem aumentam a carga de trabalho da tripulação.

(2) "Minor". São as condições de falha que não reduziriam significativamente a segurança da aeronave e nem envolveriam ações fora da capacidade da tripulação. As condições de falha "Minor" podem incluir uma pequena redução nas margens de segurança ou na capacidade funcional, um pequeno aumento da carga de trabalho da tripulação, ou algum desconforto físico para os passageiros ou para tripulação de cabine.

(3) "Major". São as condições de falha que reduziriam a capacidade da aeronave ou a habilidade da tripulação em lidar com condições operacionais adversas e que resultariam em significante redução das margens de segurança ou capacidade funcional. Ademais, dessa condição de falha também resulta um significante aumento da carga de trabalho da tripulação, condições que diminuem a capacidade da tripulação, desconforto na tripulação de voo ou estresse físico aos passageiros ou à tripulação de cabine, podendo até incluir ferimentos.

(4) "Hazardous". São as condições de falha que reduziriam a capacidade da aeronave ou a habilidade da tripulação em lidar com condições operacionais adversas que poderiam resultar em:

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

(b) Desgaste físico ou um grande aumento da carga de trabalho, de forma que a tripulação de voo não consiga desempenhar, de modo confiável, suas tarefas de maneira precisa ou completa; ou

(c) Ferimentos sérios ou fatais aos ocupantes distintos da tripulação de voo.

(5) "Catastrophic". São as condições de falha das quais se esperam múltiplas fatalidades dos ocupantes, incapacidade ou ferimento fatal da tripulação de voo, normalmente com a perda da aeronave.

Nota: A frase "das quais se esperam" não significa que 100% dos efeitos desse tipo de falha serão sempre catastróficos.

m. Confiabilidade. É a determinação que o sistema, subsistema, unidade ou parte, desempenhará sua função pretendida num intervalo específico, sob certas condições operacionais e ambientais.

n. Efeito adverso. Corresponde à resposta de um sistema que resulta em uma operação indesejável de um sistema ou subsistema da aeronave.

o. Equipamentos essenciais para operação segura. São os equipamentos instalados para cumprimento com os requisitos aplicáveis de aeronavegabilidade e operacionais.

p. Erro. É uma omissão ou ação incorreta tomada pela tripulação em comando ou pessoal de manutenção, ou ainda uma ação equivocada ou um engano em relação a requisitos, projeto e implementação.

q. Evento. É uma ocorrência interna ou externa que não tem sua origem na aeronave como, por exemplo: condições atmosféricas, rajadas, condições da pista, condições de navegação e comunicação, impacto de pássaros ("bird-strike"), HIRF e "Lightning", etc. O conceito de evento não inclui sabotagem.

r. Falha. É uma ocorrência que afeta a operação de um componente, parte ou elemento, de tal forma que impede o seu funcionamento adequado (essa definição inclui tanto a perda quanto o mau funcionamento de uma função).

Nota: Um erro, como definido neste documento, pode causar falhas, mas esse não é considerado uma falha.

s. Falha latente. Uma falha é latente até que ela se torne conhecida pela tripulação ou pela equipe de manutenção.

t. Função. Definida como o mais baixo nível relacionado a uma ação específica de um sistema, equipamento e desempenho da tripulação de voo a bordo da aeronave, que por si só, provê capacidade operacional completamente reconhecível (ex: a proa de uma aeronave é uma função). Um ou mais sistemas podem conter uma função específica ou um sistema pode conter várias funções.

u. Função crítica. Função crítica é toda e qualquer função que, quando perdida, impede a continuação do voo seguro e pouso da aeronave.

Nota: O termo "função crítica" é associada à uma condição de falha "Catastrophic".

v. Função essencial. É uma função cuja perda reduz a capacidade da aeronave ou a habilidade da tripulação em lidar com condições adversas de operação.

Nota: O termo função essencial é comumente associado com falhas entre "Major" e "Hazardous".

x. Função primária. É uma função instalada para cumprir com determinado regulamento aplicável a qual provê os controles relevantes ou informações de forma contínua ao piloto. Por exemplo, o PFD ("Primary Flight Display") é uma unidade física única que provê informações primárias de voo para cumprir com requisitos de: altitude, velocidade, proa e atitude da aeronave.

y. "Functional Hazard Assessment" (FHA). É um exame sistemático e abrangente das funções da aeronave e seus sistemas para identificar potenciais condições de falha "Minor", "Major", "Hazardous" e "Catastrophic", que podem surgir como resultado de uma falha ou mau funcionamento.

z. Hardware complexo. São todos os itens que não são considerados simples segundo a definição da RTCA/DO-254.

aa. "Hazard". É uma condição potencialmente insegura, resultante de uma falha, mau funcionamento, eventos externos, erros, ou suas combinações. Esse termo é voltado a maus funcionamentos

ou falhas simples que são considerados prováveis baseados tanto na experiência em serviço quanto em análise, considerando componentes similares em aplicações de aeronaves semelhantes. Não há análise quantitativa nesse caso.

bb. Indicação "Caution". É uma indicação clara e inequívoca para a tripulação de voo de que uma falha requer uma atenção imediata e uma possível ação subsequente.

cc. Indicação "Warning". É uma indicação clara e inequívoca para a tripulação de voo de que uma falha requer uma ação corretiva imediata.

dd. Mau funcionamento. Falha de um sistema, subsistema, unidade, ou parte em operar de maneira normal ou usual. É a ocorrência de uma condição fora dos limites especificados.

ee. "Development Assurance Level" (DAL). São todas as ações planejadas e sistematicamente utilizadas para substanciar um adequado nível de confiança, de modo que erros em requisitos, projeto e implementação sejam identificados e corrigidos para que o sistema satisfaça a base de certificação aplicável.

Nota: Para este guia o DAL também pode estar correlacionado com níveis de software e hardware, RTCA/DO-178 e RTCA DO-254, respectivamente.

ff. Probabilidade média por hora de voo. É uma representação do número de vezes que uma dada ocorrência de condição de falha é prevista durante a vida em serviço de todas as aeronaves de determinado Tipo, dividida pelo total antecipado do número de horas de voo de todas as aeronaves desse Tipo.

Nota: A probabilidade média por hora de voo é normalmente calculada como a probabilidade de uma condição de falha ocorrer durante um voo típico dividido pela duração média desse voo.

gg. "Preliminary System Safety Assessment" (PSSA). É uma avaliação sistemática de uma arquitetura de sistema e sua implementação proposta, baseada no FHA e na classificação de condição de falha para determinar requisitos de segurança para todos os itens.

hh. Qualitativa. São análises objetivas de sistemas de forma não numérica. (Ex: experiência de engenharia, descrição técnica, etc.)

ii. Quantitativa. São análises de sistemas que utilizam métodos matemáticos. (Ex: árvore de falhas, FMEA, etc.)

jj. Redundância. É a presença de mais de um meio independente, não necessariamente idênticos, para realizar uma determinada função.

kk. "Safety Assessment". É uma análise de falhas baseada em julgamento de engenharia.

ll. "System Safety Assessment" (SSA). Uma avaliação sistemática e abrangente do sistema implementado para demonstrar cumprimento com os requisitos afetados.

mm. "Final System Safety Assessment" (FSSA). Conforme uso neste guia, é um Relatório de Análise Final de Falhas baseado na PSSA para concluir se os meios de cumprimento com requisito ("Means of Compliance" - MOCs) aplicáveis, incluindo inspeção/ensaios, atendem aos requisitos de segurança/certificação.

nn. Similaridade. É um processo para mostrar que o tipo, função, projeto e instalação de um equipamento~~,~~ tem apenas pequenas diferenças em relação a um equipamento previamente aprovado. As características de segurança, operacionais ou outras da nova instalação proposta não devem ter nenhum efeito na aeronavegabilidade da aeronave.

oo. Sistema convencional. Um sistema é considerado convencional quando sua função, tecnologia e uso pretendido são os mesmos, ou similares, dos já aprovados e comumente utilizados. Os sistemas que tem um histórico de serviço adequado e meios de cumprimento para aprovação já consolidados são, geralmente, aceitos como convencionais. Ademais, um sistema convencional pode ser usualmente analisado de forma qualitativa.

pp. Sistema primário. Sistema que provê uma função primária.

qq. Sistema secundário. É um sistema redundante que provê a mesma funcionalidade de um sistema primário.

rr. Sistema simples. É usualmente um sistema que pode ser avaliado apenas por análise qualitativa e que não é complexo.

ss. Sistema complexo. Um sistema é complexo quando sua operação, modos de falha ou efeitos são difíceis de entendimento sem o auxílio de métodos analíticos ou de análise estruturada. FMEA e FTA são exemplos de tais métodos de análise estruturados. O aumento da complexidade de sistemas é frequentemente causado por itens muito sofisticados, de tecnologias avançadas e que possuem múltiplas interligações. Por exemplo, para esses tipos de sistemas, uma parcela do cumprimento pode ser demonstrada pelo uso de DALs, tal como nos processos descritos na RTCA DO-178 ou RTCA DO-254, em suas últimas versões, ou documentos equivalentes.

6. Demonstração do Cumprimento Conforme Emenda Adotada

Conforme a emenda do requisito § XX.1309 que for adotada, há diferenças no que deve ser cumprido e demonstrado. Mais informações sobre o assunto podem ser obtidas nas ACs correspondentes.

Contudo, pode ser necessário adotar uma emenda mais atual que a da base de certificação original, como, por exemplo, quando são instalados sistemas complexos pois, nesse caso, os requisitos da Emenda 23-14 podem não fornecer um nível adequado de segurança.

7. Safety Assessment

a. Análise de Falhas. O requerente é responsável por identificar e classificar cada condição de falha e escolher a metodologia adotada para o “Safety Assessment”. Após a realização de tais procedimentos, o requerente deve submeter à aceitação da ANAC as condições de falha encontradas, suas classificações e a escolha dos meios aceitáveis de cumprimento. O apêndice 2 ilustra um fluxograma geral de como conduzir um “Safety Assessment”. Essa figura é apenas para referência e não possui todas as informações fornecidas por este guia ou pelos documentos referenciados.

De acordo com esse fluxograma, o processo deverá iniciar pela elaboração de uma FHA, em que são descritos os detalhes do sistema, suas interligações, etc.; bem como identificar e caracterizar as falhas funcionais associadas, determinando por último o grau de severidade correspondente a cada falha. Depois disso, partindo do resultado dessa análise, caso a máxima condição de falha seja "Minor", o processo de avaliação da segurança se encerra com a realização dos ensaios aplicáveis. Caso contrário, o requerente deverá elaborar um relatório apresentando o SSA baseado no FHA (Ver exemplo no Apêndice 4). Além disso, deve-se verificar, através de uma avaliação do projeto e da instalação, as premissas relevantes pertinentes ao sistema, tais como: similaridade, redundância, simplicidade, tecnologia, meio de cumprimento com requisito, dentre outras aplicáveis. Em seguida, deve-se estabelecer se a modificação em questão degrada o nível de segurança ou não mantém as premissas atuais. Caso melhore o nível de segurança ou mantenha as premissas, o processo segue para a realização dos ensaios em solo e voo aplicáveis e concluí-se com algum acréscimo ao SSA, caso necessário.

Contudo, se a modificação em questão degradar o nível de segurança ou não mantiver as premissas atuais, o requerente deverá propor um PSSA baseado no SSA, indicando os meios de cumprimento aplicáveis, como por exemplo, FTA, FMEA, Análise Zonal ("Zonal Analysis"), etc. (atentar para as considerações no caso de "Major" e "Hazardous"/"Catastrophic"). Após, seguem-se os ensaios em solo e voo, se aplicáveis e, finalmente, é elaborado um FSSA baseado no PSSA, para concluir se os meios de cumprimento com requisito ("Means of Compliance" - MOCs), cumpriram com os requisitos de certificação elencados no Plano de Certificação, particularmente os mais relevantes em termos de "Safety Assessment".

b. "Functional Hazard Assessment" (FHA)

(1) Antes de realizar um "Safety Assessment" detalhado, deve ser elaborada uma FHA cobrindo os sistemas instalados e suas funções, para determinar a necessidade e o escopo das análises subsequentes. Essa avaliação pode ser realizada levando em conta:

(a) experiência em serviço, um julgamento de engenharia e um julgamento operacional; ou

(b) experiência em serviço e um exame qualitativo dedutivo "top-down" de cada função.

A FHA é uma análise sistemática e ampla dos sistemas instalados e suas funções, para identificar potenciais condições de falha e suas respectivas classificações ("No Safety Effect", "Minor", "Major", "Hazardous" e "Catastrophic"). Tais condições de falha podem surgir tanto de algum mau funcionamento ou de falhas das próprias funções, quanto de respostas a fatores externos não usuais ou anormais. A FHA é voltada às vulnerabilidades operacionais dos sistemas, não necessitando de uma análise detalhada da instalação.

(2) Cada função deve ser examinada considerando as demais funções realizadas pelo sistema, pois a perda ou mau funcionamento de todas as funções do sistema pode resultar em uma condição de falha mais severa que a perda de uma única função. Adicionalmente, também devem ser consideradas as funções realizadas por outros sistemas, pois a perda ou mau funcionamento de funções relacionadas, mesmo quando diferentes, pode afetar a severidade das condições de falha estipulada para um sistema em particular.

(3) A FHA é uma ferramenta de engenharia que deve ser utilizada no começo do projeto e atualizada conforme necessário. Ela é utilizada para definir as metas de segurança dos sistemas que devem ser consideradas em sua arquitetura proposta. Adicionalmente, ela deve ser utilizada como auxílio na definição

dos DALs para os sistemas. Para muitos sistemas, um exame simples de seu projeto pode ser suficiente para determinar a classificação de falhas.

(4) Diferentes enfoques podem ser adotados na FHA, dependendo da extensão das funções que serão examinadas e das relações entre funções e sistemas. Quando há uma correlação clara entre funções e sistemas, e quando a inter-relação entre sistemas e funções são relativamente simples, pode ser possível conduzir uma FHA separada para cada sistema. Contudo, para isso todos os aspectos das interfaces devem ser considerados e facilmente entendidos. Entretanto, quando as inter-relações entre sistemas e funções são mais complexas, a FHA deve ser planejada e conduzida em uma abordagem "top-down", considerando a aeronave como um todo.

(5) Após classificar cada condição de falha, para aeronaves RBAC/FAR 23, O Apêndice 1 pode ser utilizado para obter a probabilidade máxima aceitável da condição de falha e o DAL necessário para o software ou o hardware complexo. Por exemplo, a probabilidade para uma condição de falha "Hazardous" para um avião classe I precisa ser menor que 1×10^{-5}. Adicionalmente, o sistema primário de uma aeronave classe I precisa ter, para seu software e hardware complexo, um DAL C; o sistema secundário, se requerido, um DAL D.

(6) A classificação das condições de falha não depende de um sistema ou função serem requeridos por algum requisito específico. Alguns sistemas especificamente requeridos por requisitos, como transponder e luzes de posição, podem estar associados apenas a condições de falha "Minor". Da mesma forma, outros sistemas que não são requeridos por nenhum requisito, tais como sistemas de gerenciamento de voo e sistemas de pouso automático, podem estar associados a condições de falha "Major", "Hazardous" ou "Catastrophic".

(7) A classificação da condição de falha deve considerar todos os fatores relevantes. Entre os exemplos de tais fatores estão a natureza dos modos de falha, que inclui modos de falha comuns, degradação do sistema resultante de falhas, ações da tripulação de voo, carga de trabalho da tripulação de voo, degradação da performance, redução da capacidade operacional, efeitos na fuselagem, etc. É importante considerar fatores que podem aliviar ou intensificar a severidade de uma condição de falha. Um exemplo de fator que alivia a severidade é a continuidade do funcionamento de funções operacionais idênticas ou similares por outros sistemas não afetados pela condição de falha. Exemplo de fator que intensifica a severidade inclui condições não relacionadas que podem reduzir a habilidade da tripulação de lidar com a condição de falha, como as meteorológicas, ou outra condição operacional ou ambiental adversa. É desejável que o sistema tenha a capacidade de informar ao piloto sobre potenciais ou reais condições de falha, de forma que uma ação corretiva possa ser efetuada para reduzir os efeitos da combinação de eventos. Esse enfoque pode reduzir a severidade da condição de falha.

(8) Devido ao grande número de combinações de falhas, à variedade de fatores mitigatórios, às características de efeitos da aeronave e fatores similares, a FHA e o "Safety Assessment" podem ser significativamente diferentes para cada aeronave e configuração avaliada. Esses fatores impedem o fornecimento de um exemplo de FHA que se aplique genericamente a qualquer instalação. Contudo, exemplos genéricos podem ser fornecidos para ilustrar os conceitos envolvidos em uma FHA (ver o apêndice 4). É de fundamental importância compreender que o julgamento de engenharia e o bom senso são necessários para conseguir uma avaliação útil e aceitável da aeronave e de seus sistemas.

c. Considerações e Exemplos. O apêndice 1 da AC 23.1309-1E provê uma lista parcial da FHA para consideração em aviões part 23 IFR de classe I com funções típicas e, de modo geral, as condições de

falha relacionadas ocorrem no nível da aeronave. O critério no nível da aeronave é útil para obter a FHA do sistema. As condições de falha dos exemplos do apêndice 1 da AC 23.1309-1E não podem ser aplicadas indiscriminadamente para instalações em qualquer avião. Essa tabela é utilizada primariamente para reduzir a carga regulatória de requerentes que não tem familiaridade com os vários métodos e procedimentos geralmente utilizados na indústria para conduzir um "Safety Assessment". Essa lista é apenas um guia, não um "checklist" de certificação, já que ela não inclui toda informação necessária para uma FHA de uma aeronave específica com suas várias funções e usos pretendidos. As funções listadas na FHA parcial são um guia para a classificação das condições de falha quando essas funções estão instaladas. A lista de funções não tem a intenção de sugerir que essas são requeridas para aviões classe I. Mesmo que exista um guia informativo no apêndice 1 da AC 23.1309-1E, são os regulamentos aplicáveis que estipulam os requisitos para as funções nas instalações.

(1) Recomenda-se que o requerente utilize o apêndice 1 da AC 23.1309-1E como ponto de partida para a avaliação de um sistema específico. Ele pode ser utilizado para se chegar às condições de falha apropriadas para um sistema específico ou por similaridade, ou por interpolação entre os sistemas exemplificados. Ele não necessariamente provê, sozinho, uma resposta para um sistema, a não ser que esse sistema seja exatamente como o descrito. Seu único propósito é auxiliar o requerente ilustrando funções típicas e suas condições de falhas. Esse "apêndice" é de aplicabilidade geral, o que pode ser útil para determinar os DALs de software e hardware complexo, e não pode ser utilizado para substituir algum guia voltado a tipos específicos de equipamentos, sistemas ou instalações. O resultado da FHA depende das características da aeronave e da arquitetura do sistema. Os exemplos nesse apêndice são baseados em aeronaves e arquiteturas tradicionais. O RBAC 23.1309 contém requisitos gerais e não deve ser utilizado para suprimir qualquer outro requisito do RBAC 23.

(2) Em adição ao guia fornecido no apêndice 1 da AC 23.1309-1E, um exemplo de formatação para documentar os resultados da FHA é fornecido no apêndice 2 da AC 23.1309-1E. Essa formatação ilustra como fatores diversos dos representados no apêndice 1 da AC 23.1309-1E são pertinentes. Ele também ilustra que as condições de falha não se limitam aos três tipos gerais mostrados no apêndice 1 da AC 23.1309-1E. Os dados apresentados no apêndice 2 da AC 23.1309-1E são apenas para ilustrar um enfoque típico e não devem ser vistos como tecnicamente representativos de qualquer avião em particular. Uma FHA completa pode ser abrangida pelo leiaute mostrado no apêndice 2 da AC 23.1309-1E utilizando as considerações técnicas identificadas no apêndice 1 da AC 23.1309-1E, que devem ser modificadas e expandidas para refletir o projeto em consideração.

O RBAC 23 abrange uma grande variedade de tamanhos e capacidades de aviões. Esses aviões podem ser desde aeronaves monomotores, com assento único e de baixa performance a aviões complexos multimotores, de velocidade e performance elevadas. Nos aviões mais simples, há características que mitigam alguns dos efeitos de uma falha. Características como a maneabilidade suave, baixa velocidade de "stall", projeto resistente a "spin", menor probabilidade de operação em condições meteorológicas extremas e filosofias inerentes ao projeto de aviões monomotores, são exemplos específicos de características a se considerar em uma FHA. Geralmente o suporte do controle de tráfego não é um fator mitigante.

8. Condições de Falha

a. Condições de falha sem efeitos na segurança ("No Safety Effect"). Uma FHA, com o projeto e avaliação da instalação, é necessária para determinar a independência entre sistemas e suas condições

de falhas no SSA. Em geral, práticas comuns de projeto já estabelecem isolações físicas e funcionais de componentes essenciais à operação segura.

b. Análise das condições de falha "Minor". Uma análise deve considerar os efeitos das condições de falhas em outros sistemas e suas funções. Uma FHA, com o projeto e avaliação da instalação, é necessária para determinar a independência entre sistemas e suas condições de falhas no SSA. Em geral, práticas comuns de projeto já estabelecem isolações físicas e funcionais de componentes essenciais à operação segura.

c. Análise das condições de falha "Major". É uma análise baseada no julgamento de engenharia desenvolvida de forma qualitativa, conforme os métodos abaixo:

(1) A similaridade permite a validação de um requisito por comparação aos requisitos de sistema já certificado. O uso desse método torna-se mais eficiente conforme se aumenta a experiência de uso do sistema. Se o sistema é similar em seus atributos a outros instalados em outras aeronaves, e se as funções e modos de falhas são os mesmos, então uma avaliação do projeto e sua instalação, assim como histórico de serviço favorável, são geralmente aceitáveis para cumprimento de requisito. Informa-se que é de responsabilidade do requerente prover dados que substanciem qualquer pedido de similaridade.

(2) Para sistemas não complexos, quando a similaridade não pode ser usada como forma de cumprimento, o cumprimento pode ser evidenciado por meio de uma análise qualitativa, em que as condições de falha "Major" do sistema são consistentes com o FHA proposto (por exemplo, há a redundância de sistemas, etc.)

(3) Para mostrar que as ocorrências de mau funcionamento são realmente remotas nos sistemas de alta complexidade, em que não há redundância (por exemplo, um sistema microprocessado com "self-monitoring"), é necessária a condução de uma análise qualitativa funcional por meio de FTA ou FMEA, embasada por informações como taxas de falhas, detecção de falhas, etc.

(4) Uma análise da redundância de um sistema na aeronave é geralmente satisfatória quando ela demonstra que há isolação entre canais do sistema e suficiente confiabilidade de cada canal. Para sistemas complexos, quando a redundância é requerida, uma análise qualitativa funcional por meio de FTA ou FMEA pode ser necessária para determinar a existência de redundância.

d. Análise das condições de falha "Hazardous" ou "Catastrophic". Para essas condições de falha, uma análise completa de SSA é necessária. Essa avaliação usualmente consiste de apropriadas combinações de análises qualitativas e quantitativas. Para esses casos, sugere-se consultar a AC 23-1309 da FAA para aeronaves Parte 23 ou outros documentos pertinentes, para as aeronaves Partes 25, 27 e 29.

9. Métodos de Análise

a. Métodos de análise. Existem métodos para qualitativamente e quantitativamente avaliar as causas, severidades e probabilidades das condições de falha potenciais que podem ser utilizados para auxiliar no julgamento técnico de engenharia e operacional do sistema avaliado. O requerente deverá selecionar o método de análise apropriado para validar a segurança do seu projeto, baseando-se em fatores como a

arquitetura utilizada, complexidade, criticalidade das funções, etc. A norma ARP 4761 detalha os vários métodos possíveis de implementação, a saber:

(1) Avaliação de projeto. É uma avaliação qualitativa da integridade e segurança do projeto do sistema. Uma avaliação de projeto eficaz requer experiência na análise técnica de engenharia dos sistemas envolvidos.

(2) Avaliação da instalação. Trata-se da avaliação qualitativa da integridade e segurança da instalação proposta. Qualquer desvio das práticas normalmente aceitas deverá ser devidamente substanciado. Uma avaliação da instalação eficaz requer experiência na análise técnica de engenharia dos sistemas envolvidos.

(3) FMEA ("Failure Modes and Effects Analysis"). É uma avaliação estruturada, indutiva e de baixo para cima ("bottom-up") que busca identificar falhas de elementos ou componentes e respectivos efeitos no funcionamento de outros elementos e funções. A norma ARP 4761 detalha a metodologia a ser desenvolvida para esse método.

(4) FTA ("Fault Tree Analysis"). É uma análise gráfica estruturada, dedutiva e de cima para baixo ("top-down") que é usada para identificar todas as possíveis combinações de falhas, eventos e erros que podem causar cada condição de falha identificada. A norma ARP 4761 detalha a metodologia a ser desenvolvida nesse método.

(5) CCA ("Common Cause Analysis"). A determinação da probabilidade de condição de falha é geralmente derivada da análise de múltiplos sistemas assim como, em muitos casos, na premissa de que essas falhas são independentes. Contudo, na prática, nem sempre tal independência ocorre e, como resultado, estudos específicos são necessários para garantir que tal independência possa ser assegurada. O método "Common Cause Analysis" é dividido em três áreas de estudo:

a. ZSA ("Zonal Safety Analysis"). Essa análise tem o objetivo garantir que a instalação de equipamentos em determinada área da aeronave está de acordo com os padrões de segurança em relação ao projeto e instalação, interferência entre sistemas e erros de manutenção.

b. PRA ("Particular Risk Analysis"). É a análise de eventos ou influências exteriores à aeronave (por exemplo: condições atmosféricas, rajadas, condições da pista, condições de navegação e comunicação, impacto de pássaros ("bird-strike"), HIRF e "Lightning", etc. Cada risco deve ser sujeito a um estudo específico para determinar seus efeitos e influências.

c. CMA ("Common Mode Analysis"). Essa análise é realizada para confirmar a independência entre eventos que são considerados em conjunto para uma dada condição de falha. Falhas de Modo Comum ("Common Mode") tem a capacidade de anular redundâncias, provocando falhas simultâneas em diversos sistemas.

NOTA: Para o cálculo das probabilidades das condições de falha, usando os métodos quantitativos (FTA e FMEA), o requerente deverá usar a AC 23.1309, 25.1309, 27-1 e 29-2 e ARPs. Em geral esses métodos são aplicáveis às condições de falhas "Major" (quando for sistema complexo), "Hazardous" e "Catastrophic".

10. Considerações Operacionais e de Manutenção.

a. Alertas. Os alertas devem ser fornecidos em tempo hábil, quando for necessário que os pilotos tenham consciência situacional de uma condição insegura, para que possam executar as ações corretivas necessárias, imediatas ou posteriores. O método particular de indicação depende da urgência e da necessidade de conscientização da tripulação de voo ou das ações necessárias para a mitigação da falha.

Verificações pela tripulação ("flight crew checks") ou procedimentos periódicos de manutenção que visam detectar falhas latentes significativas, não devem ser utilizados no lugar de práticas confiáveis de monitorização e indicações de falha. O projeto de sistemas e controles, incluindo indicações e anúncios, deve ser concebido para minimizar os erros da tripulação que poderiam criar riscos adicionais, tais como reações inadequadas da tripulação em resposta à falha, ou aqueles que poderiam ocorrer após uma falha.

Nota: Os alertas podem incluir, por exemplo: sinais visuais, sonoros, vibração no manche ("shaker"), indicação em um display através de cores, símbolos ou texto, etc. Na concepção de alertas devem ser considerados: o correto posicionamento e as cores/indicações de anunciadores; volume e inteligibilidade dos alertas sonoros; o ajuste dos parâmetros de indicações nos displays; calibração de transdutores que vibram; etc.

b. Ações da tripulação de voo. Ao se avaliar a capacidade da tripulação de voo em lidar com uma condição de falha, devem ser consideradas as informações fornecidas à tripulação e a complexidade da ação necessária.

(1) Se essa avaliação indicar que uma condição de falha potencial pode ser aliviada ou superada em tempo hábil, sem prejuízo de outras atividades relacionadas à segurança da tripulação de voo e sem requerer habilidade ou força excepcionais do piloto, em ambas as avaliações, qualitativa e quantitativa, pode ser assumido que a tripulação irá agir de forma correta.

(2) Anúncios que requerem ações da tripulação de voo devem ser avaliados para se determinar se as ações necessárias podem ser realizadas em tempo hábil, sem habilidades excepcionais de pilotagem.

Se a avaliação indicar que uma condição de falha potencial pode ser aliviada ou superada em tempo hábil, sem prejuízo de outras atividades relacionadas à segurança da tripulação de voo e sem requerer habilidade ou força excepcionais do piloto, medidas corretivas corretas e apropriadas podem ser tomadas como crédito para avaliações qualitativa e quantitativa. Da mesma forma, pode ser tomado como crédito no "Safety Assessment" o correto desempenho da tripulação de voo, se a carga de trabalho global da tripulação durante o tempo disponível não é excessiva e se as tarefas não exigem habilidade ou força excepcionais do piloto.

(3) Se em decorrência do "Safety Assessment" forem necessárias algumas práticas de pilotagem ou ações não usuais da tripulação de voo, os procedimentos adequados devem ser incluídos em um adendo ao manual de voo ou um Suplemento ao Manual de Voo (AFMS), que deve conter: procedimentos para o funcionamento de sistemas complexos, tais como sistemas integrados de orientação de voo e controle; procedimentos para a resposta adequada dos pilotos às indicações na cabine; diagnóstico de falhas do sistema; a discussão de possíveis problemas no sistema de controle de voo induzidos pelo piloto e tudo o que for necessário acrescentar para utilização segura do sistema.

Nota: Para aeronaves cuja certificação de tipo não possui um manual de voo associado, placares ou outros meios de indicação (por exemplo, alertas visuais ou sonoros) podem ser necessários.

c. Ações de manutenção. Se as tarefas de manutenção forem avaliadas e consideradas razoáveis, pode ser tomado crédito da correta realização dessas tarefas nas avaliações qualitativas e quantitativas. Tarefas de manutenção necessárias, que mitigam riscos, devem ser fornecidas para uso em programas de manutenção aprovados pela ANAC, tais como a ICA. Falhas anunciadas devem ser corrigidas antes do próximo voo ou um prazo máximo deverá ser estabelecido antes de uma ação de manutenção necessária. Se esse prazo for aceitável, a análise deve estabelecer o intervalo máximo permitido necessário antes da ação de manutenção.

Tarefas de manutenção agendadas podem detectar falhas latentes. Se essa abordagem for seguida, e a condição de falha for "Hazardous" ou "Catastrophic", então deve ser estabelecida uma tarefa de manutenção. Algumas falhas latentes podem ser identificadas com base em um teste de retorno ao serviço do equipamento, após a sua remoção e reparo (onde o MTBF do componente deve ser a base para a verificação de tempo de intervalo).

11. DALs de Software e Hardware Complexo para Sistemas Embarcados e Aplicações

a. "Background". A AC 20-115B aborda como a RTCA / DO-178B fornece um meio aceitável para mostrar que o software está em conformidade com os requisitos de aeronavegabilidade pertinentes. A AC 20-152 e o Order 8.110.105 fornecem meios aceitáveis para mostrar que o hardware complexo cumpre com os requisitos de aeronavegabilidade pertinentes.

b. DALs de software e hardware complexo aceitáveis. É necessário considerar a possibilidade de requisitos, design, e erros de implementação, a fim de cumprir com os requisitos § 2X.1309. Os erros cometidos durante a concepção e desenvolvimento de sistemas têm sido tradicionalmente detectados e corrigidos por testes exaustivos realizados sobre o sistema e seus componentes. Esses testes utilizam inspeção direta e outros métodos de verificação direta capazes de caracterizar completamente o desempenho do sistema. Essas técnicas diretas podem ainda ser apropriadas para sistemas simples, os quais desempenham um número limitado de funções e que não são altamente integrados com outros sistemas da aeronave.

(1) Para sistemas mais complexos ou altamente integrados, testes exaustivos podem ser impossíveis, porque não poderiam ser determinados todos os estados desses sistemas, ou podem ser impraticáveis, devido ao número de testes que deveriam ser realizados. Para esses tipos de sistemas, a conformidade pode ser mostrada pelo uso de DALs de software e de hardware complexo. O DAL de software e hardware complexo deve ser determinado pela severidade dos potenciais efeitos para a aeronave em caso de mau funcionamento ou perda de funções do sistema.

c. Critérios de DALs de software e hardware complexo. Os critérios de DALs correlacionam-se com o nível de software na RTCA / DO-178B e o nível de segurança de projeto complexo na RTCA / DO-254. A classificação da condição de falha e a classe de aeronave devem ser determinadas para se determinar os níveis de DALs, ver Apêndice 1.

d. Equipamentos instalados que executam funções abrangidas pelos padrões TSO. Equipamentos instalados que executam funções abrangidas pelos padrões TSO devem cumprir as normas TSO aplicáveis. É preferível o uso de equipamentos com aprovação TSO. No entanto, não é obrigatório que um equipamento tenha aprovação TSO, mas é necessário que ele atenda outros padrões mínimos de desempenho equivalentes aceitáveis. Os dados TSO devem incluir os níveis de DALs de software e hardware complexo. Para ambos casos, equipamentos com TSO e sem TSO, o "Safety Assessment" (e o Apêndice 1 deste guia para

aeronaves Parte 23) devem ser utilizados para verificar os DAL de software e hardware complexo conforme os requisitos de instalação.

12. Proteção Eletromagnética para os Sistemas Elétricos e Eletrônicos.

A tendência atual é de um aumento da dependência de sistemas elétricos e eletrônicos para operações seguras. Efeitos eletromagnéticos, efeitos ambientais e qualificações ambientais devem ser considerados para sistemas que executam funções de voo, propulsão, navegação e instrumentação. Os DALs de software e hardware complexo, do Apêndice 1, não se aplicam aos níveis de HIRF e de proteção contra raios. Para obter orientação sobre a proteção contra esses efeitos, consulte a versão mais recente e aplicável à aeronave das AC 21-16F, AC 23-17C, AC 27-1B, AC 29-2C, AC 20-136A, e AC 20-158.

O apêndice 7 contém um exemplo de aplicação do uso da FHA para verificar requisitos de qualificação conforme a DO-160, quanto a HIRF, “Lightning” e EMI.

13. Referências

AC 20-136 - ***Aircraft Electrical and Electronic System Lightning Protection.*** Rev. B, FAA, 2011.

AC 20-158 - ***The Certification of Aircraft Electrical and Electronic Systems for Operation in the High-intensity Radiated Fields (HIRF) Environment.*** Rev. A, FAA, 2014.

AC 23-1309-1 - ***System Safety Analysis and Assessment for Part 23 Airplanes.*** Rev. E, FAA, 2011.

ARP 4761 - ***Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.*** Rev. -, SAE, 1996.

DO-178 - ***Software Considerations in Airborne Systems and Equipment Certification.*** Rev. C. RTCA, 2011.

DO-254 - ***Design Assurance Guidance for Airborne Electronic Hardware.*** Rev. -. RTCA, 2000.

RBAC nº 01 - **Regulamento Brasileiro da Aviação Civil - Definições, Regras de Redação e Unidades de Medida**. Rev. 01, ANAC, 2011.

APÊNDICE 1 – RELAÇÃO ENTRE CLASSES DE AVIÃO (RBAC 23), PROBABILIDADES, SEVERIDADE DAS CONDIÇÕES DE FALHA E DALS

Classificação das Condições de Falha	**NO SAFETY EFFECT**	**MINOR**	**MAJOR**	**HAZARDOUS**	**CATASTROPHIC**
Probabilidade Qualitativa Aceitável	**Sem exigência**	**Razoavelmente provável**	**Remoto**	**Extremamente Remoto**	**Extremamente Improvável**
Efeito no Avião	Sem efeito nas capacidades operacionais ou na segurança	Leve redução das capacidades funcionais ou das margens de segurança	Significante redução das capacidades funcionais ou das margens de segurança	Grande redução das capacidades funcionais ou das margens de segurança	Normalmente inclui perda da fuselagem
Efeito nos Ocupantes	Incômodo para os passageiros	Desconforto físico para os passageiros	Sofrimento físico aos passageiros, possivelmente incluindo ferimentos	Ferimento grave ou fatal a algum ocupante	Fatalidades Múltiplas
Efeito na Tripulação de Voo	Sem efeito na tripulação de voo	Leve aumento na carga de trabalho ou o uso de procedimentos de emergência	Desconforto físico ou um aumento significante na carga de trabalho	Sofrimento físico ou carga de trabalho excessiva prejudicando a habilidade de executar tarefas	Ferimento Fatal ou incapacitação
Classes de Aviões	**Probabilidade Quantitativa Aceitável e DALs necessários (Ver Nota 2)**				
Classe I	Sem exigência e não necessário	$<10^{-3}$ Nota 1 P=D	$<10^{-4}$ Notas 1 e 4 P=C, S=D	$<10^{-5}$ Nota 4 P=C, S=D	$<10^{-6}$ Nota 3 P=C, S=C
Classe II	Sem exigência e não necessário	$<10^{-3}$ Nota 1 P=D	$<10^{-5}$ Notas 1 e 4 P=C, S=D	$<10^{-6}$ Nota 4 P=C, S=C	$<10^{-7}$ Nota 3 P=C, S=C
Classe III	Sem exigência e não necessário	$<10^{-3}$ Nota 1 P=D	$<10^{-5}$ Notas 1 e 4 P=C, S=D	$<10^{-7}$ Nota 4 P=C, S=C	$<10^{-8}$ Nota 3 P=B, S=C
Classe IV	Sem exigência e não necessário	$<10^{-3}$ Nota 1 P=D	$<10^{-5}$ Notas 1 e 4 P=C, S=D	$<10^{-7}$ Nota 4 P=B, S=C	$<10^{-9}$ Nota 3 P=A, S=B

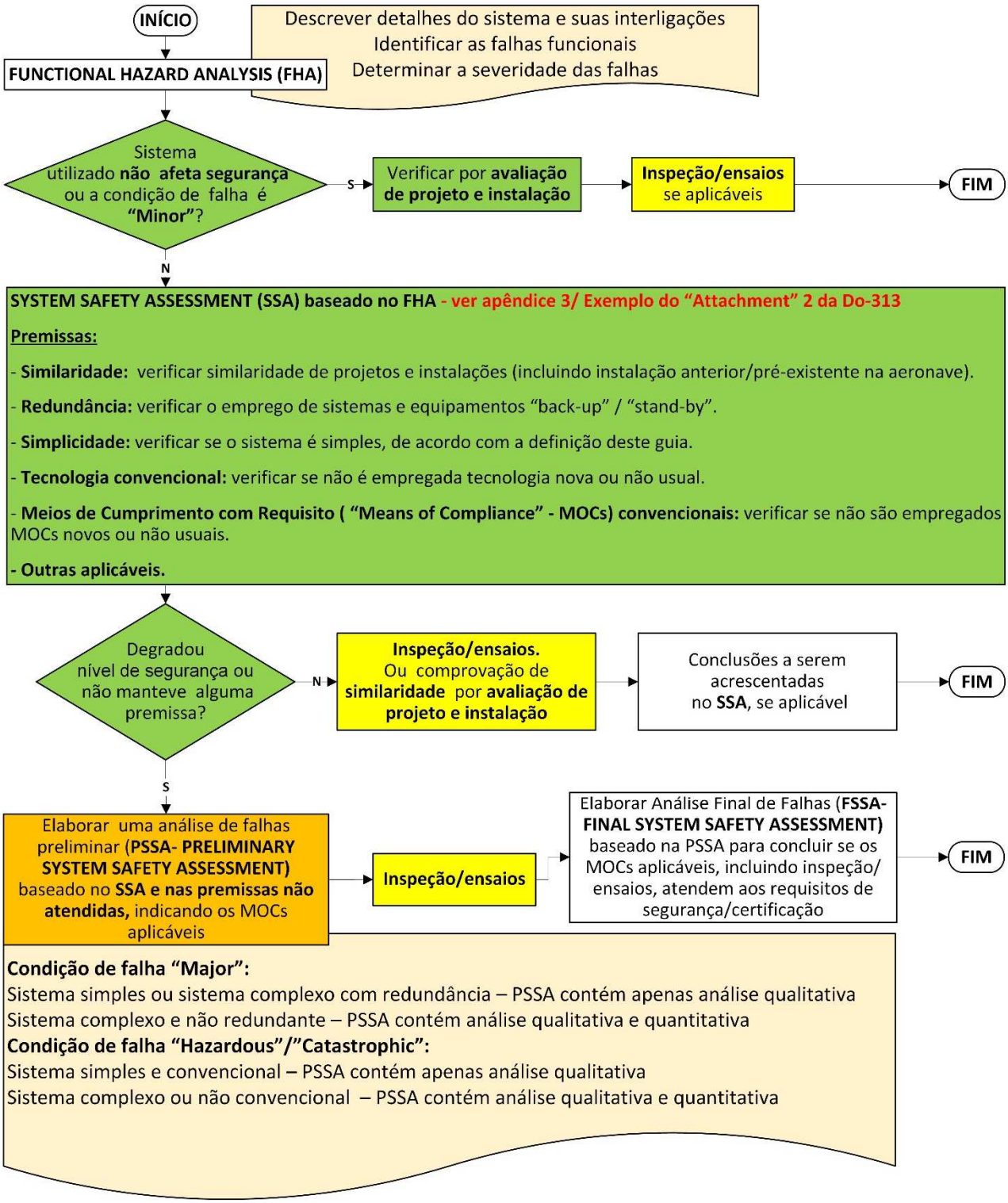
Nota 1: Os valores numéricos indicam uma faixa de ordem de probabilidade e são fornecidos apenas como referência.

Nota 2: As letras do alfabeto denotam o DAL típico para sistemas primários (P) e secundários (S). Por exemplo, DAL A em um sistema primário é representado como P=A.

Nota 3: No nível de função do avião, nenhuma falha simples resultará em uma condição de falha "Catastrophic".

Nota 4: Um sistema secundário (S) pode não ser necessário para atingir a probabilidade requerida. Se instalado, S precisa obedecer os critérios estabelecidos.

APÊNDICE 2 – FLUXOGRAMA DE PROFUNDIDADE DE ANÁLISE DE SAFETY ASSESSMENT



APÊNDICE 3 – EXEMPLO DE RELATÓRIO DE ANÁLISE DE FALHAS

ABX AERONAVES LTDA.

RELATÓRIO Nº ABX-SA-010

Aplicável a Aeronaves ABX modelo 505-A

<TÍTULO DA INSTALAÇÃO>

RELATÓRIO DE ANÁLISE DE FALHAS

Emissão Inicial - Data: 10 ago. 2015

Preparado por:_____ __/__/___

Aprovado por:_____ __/__/___
Engenheiro Aeronáutico
CREA Nº:_____
Registro ANAC Nº:_____

ABX Aeronaves Ltda.
<Endereço>
<Endereço>
<Telefone>

ABX Aeronaves Ltda.	Pág. Nº 2	Total págs. 10
<TÍTULO DA INSTALAÇÃO>	Aeronaves modelo 505-A	
RELATÓRIO DE ANÁLISE DE FALHAS	Relatório nº **ABX –SA-001** Revisão: **EI –** 10/08/15	

LISTA DE PÁGINAS EFETIVAS					
Pág.	Rev.	Pág.	Rev.	Pág.	Rev.
1	EI	7	EI		
2	EI	8	EI		
3	EI	9	EI		
4	EI	10	EI		
5	EI				

REVISÕES				
Rev.	Data	Páginas afetadas	Observações	Aprovação
EI	10 ago. 2015	Todas	Emissão Inicial	<Assinatura>

ABX Aeronaves Ltda.	Pág. Nº 3	Total págs. 10
<TÍTULO DA INSTALAÇÃO>	Aeronaves modelo 505-A	
RELATÓRIO DE ANÁLISE DE FALHAS	Relatório nº **ABX –SA-001** Revisão: **EI –** 10/08/15	

SUMÁRIO

ABX Aeronaves Ltda.	Pág. Nº 4	Total págs. 10
<TÍTULO DA INSTALAÇÃO>	Aeronaves modelo 505-A	
RELATÓRIO DE ANÁLISE DE FALHAS	Relatório nº **ABX –SA-001** Revisão: **EI –** 10/08/15	

1. OBJETIVO

Este documento apresenta uma análise de falhas relacionadas à instalação dos sistemas <**descrever sistemas a serem instalados**> na aeronave ABX modelo 505-A <**descrever fabricante e modelo da aeronave, conforme este modelo**> operando em <**descrever o tipo de operação desejado**>.

A análise de falhas aqui apresentada avalia as funções desses sistemas e sua instalação e são classificadas as condições de falhas prováveis/mau funcionamento de acordo com sua severidade, de forma a evitar que essas condições não coloquem em risco a operação segura da aeronave.

Requisitos RBAC/CFR FAR XX afetados:

Subpart F- Equipment – General

- 2X.1301 Function and installation.

- 2X.1309 Equipment, systems, and installations.

2. DESCRIÇÃO GERAL DA MODIFICAÇÃO

<Apresentar um descritivo da aeronave antes e após a modificação, indicando em formato de lista, tabela ou texto os sistemas mantidos, realocados ou novos, conforme os exemplos a seguir>

2.1. Painel antes da modificação

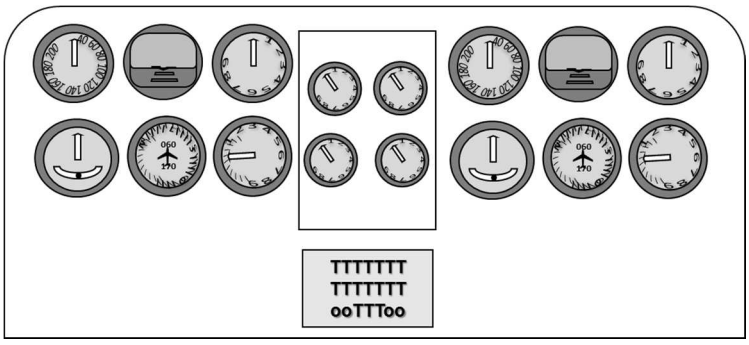


Figura 1 - Painel antes da modificação <exemplo para fins ilustrativos, somente>

<Incluir texto descrevendo o painel antes da modificação e o modo de operação da aeronave>

2.2. Painel após a modificação

<Incluir descrição do painel, conforme a seguir. Se aplicável, novo modo de operação>

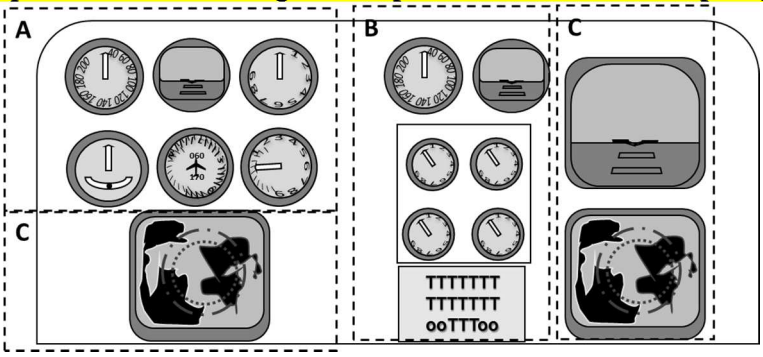


Figura 2 - Painel após a modificação <exemplo para fins ilustrativos, somente>

Legenda:

A. Instrumentos mantidos

<Incluir breve descrição de cada instrumento, indicando também instrumentos "back-up"/ "stand-by", se houver, para a instalação pretendida>

- Equipamento XYZ
  O equipamento XYZ apresenta as seguintes funções:
  <Incluir descrição das funções apresentadas>

- **[...]**

B. Instrumentos realocados

<Incluir breve descrição de cada instrumento, indicando também instrumentos "back-up"/ "stand-by", se houver, para a instalação pretendida>

- Anunciador ABCDE
  O anunciador ABCDE apresenta as seguintes funções:
- **[...]**

<Incluir descrição das funções apresentadas>

ABX Aeronaves Ltda.	Pág. Nº 6	Total págs. 10
<TÍTULO DA INSTALAÇÃO>	Aeronaves modelo 505-A	
RELATÓRIO DE ANÁLISE DE FALHAS	Relatório nº **ABX –SA-001** Revisão: **EI –** 10/08/15	

C. Novos instrumentos

<Incluir descrição detalhada de cada novo instrumento, indicando também instrumentos "back-up"/ "stand-by", se houver, para a instalação pretendida>

- Display primário PFD
  O sistema PFD apresenta as seguintes funções:
  <Descrever funções apresentadas>

- Display multifunção MFD#1
  O sistema MFD#1 apresenta as seguintes funções:
  < Descrever funções apresentadas >

- Display multifunção MFD#2
  O sistema MFD#2 apresenta as seguintes funções:
  <Incluir descrição das funções apresentadas>

- **[...]**

- Chave "MFD 1/MFD 2"
  A Chave "MFD 1/MFD 2" apresenta as seguintes funções:
  <Incluir descrição das funções apresentadas>

A Tabela 1 mostra os sistemas, equipamentos e componentes referentes à modificação proposta.

Sistemas, equipamentos e componentes	**Qt.**	**P/N**	**Fabricante**	**TSO/DO**	**Referência**
PFD **<modelo>**	1	**<Nº P/N>**	**<Nome>**	**<Citar, se houver>**	Novo
MFD **<modelo>**	2	**<Nº P/N>**	**<Nome>**	**<Citar, se houver>**	Novo
Equipamento XYZ	**<Qt.>**	**<Nº P/N>**	**<Nome>**	**<Citar, se houver>**	Mantido
...	**...**	**...**	**...**	**...**	**...**
Chave "MFD 1/MFD 2" **<modelo>**	**<Qt.>**	**<Nº P/N>**	**<Nome>**	**<Citar, se houver>**	Novo
...	**...**	**...**	**...**	**...**	**...**
Anunciador ABCDE	**<Qt.>**	**<Nº P/N>**	**<Nome>**	**<Citar, se houver>**	Realocado

Tabela 1 – sistemas, equipamentos e componentes da modificação

<exemplo para fins ilustrativos, somente>

ABX Aeronaves Ltda.	Pág. Nº 7	Total págs. 10
<TÍTULO DA INSTALAÇÃO>	Aeronaves modelo 505-A	
RELATÓRIO DE ANÁLISE DE FALHAS	Relatório nº **ABX –SA-001** Revisão: **EI –** 10/08/15	

3. CARACTERÍSTICAS DA ALIMENTAÇÃO E DO SISTEMA ELÉTRICO

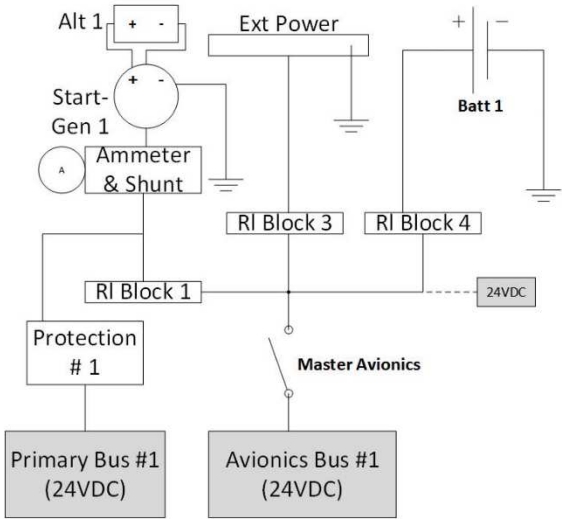


Figura 3 – Sistema elétrico # 1 <exemplo para fins ilustrativos, somente>

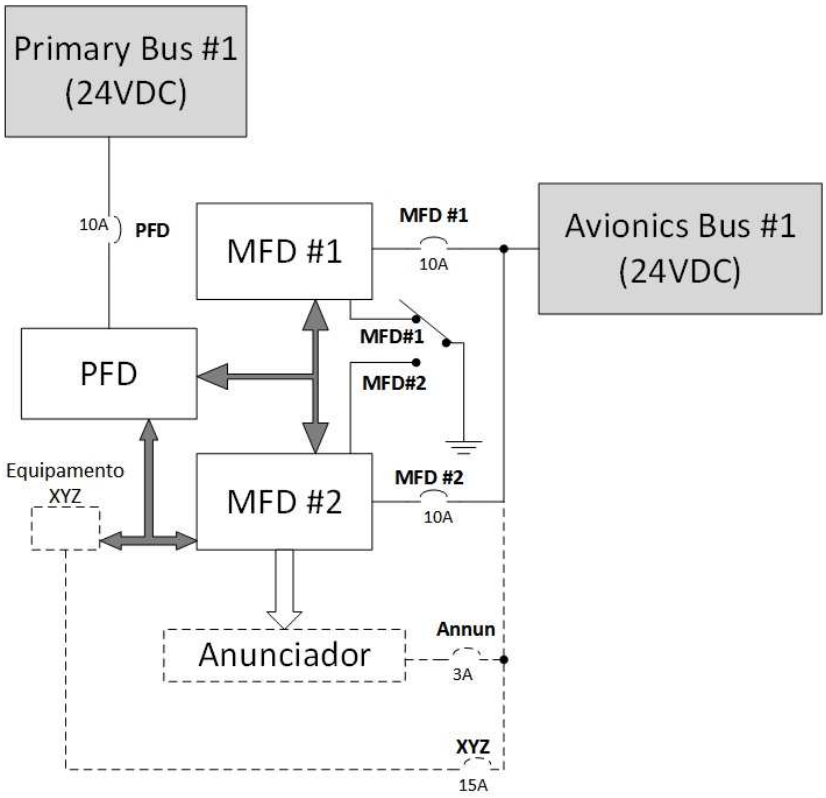


Figura X – Diagrama de Blocos <exemplo para fins ilustrativos, somente>

ABX Aeronaves Ltda.	Pág. Nº 8	Total págs. 10
<TÍTULO DA INSTALAÇÃO>	Aeronaves modelo 505-A	
RELATÓRIO DE ANÁLISE DE FALHAS	Relatório nº **ABX –SA-001** Revisão: **EI –** 10/08/15	

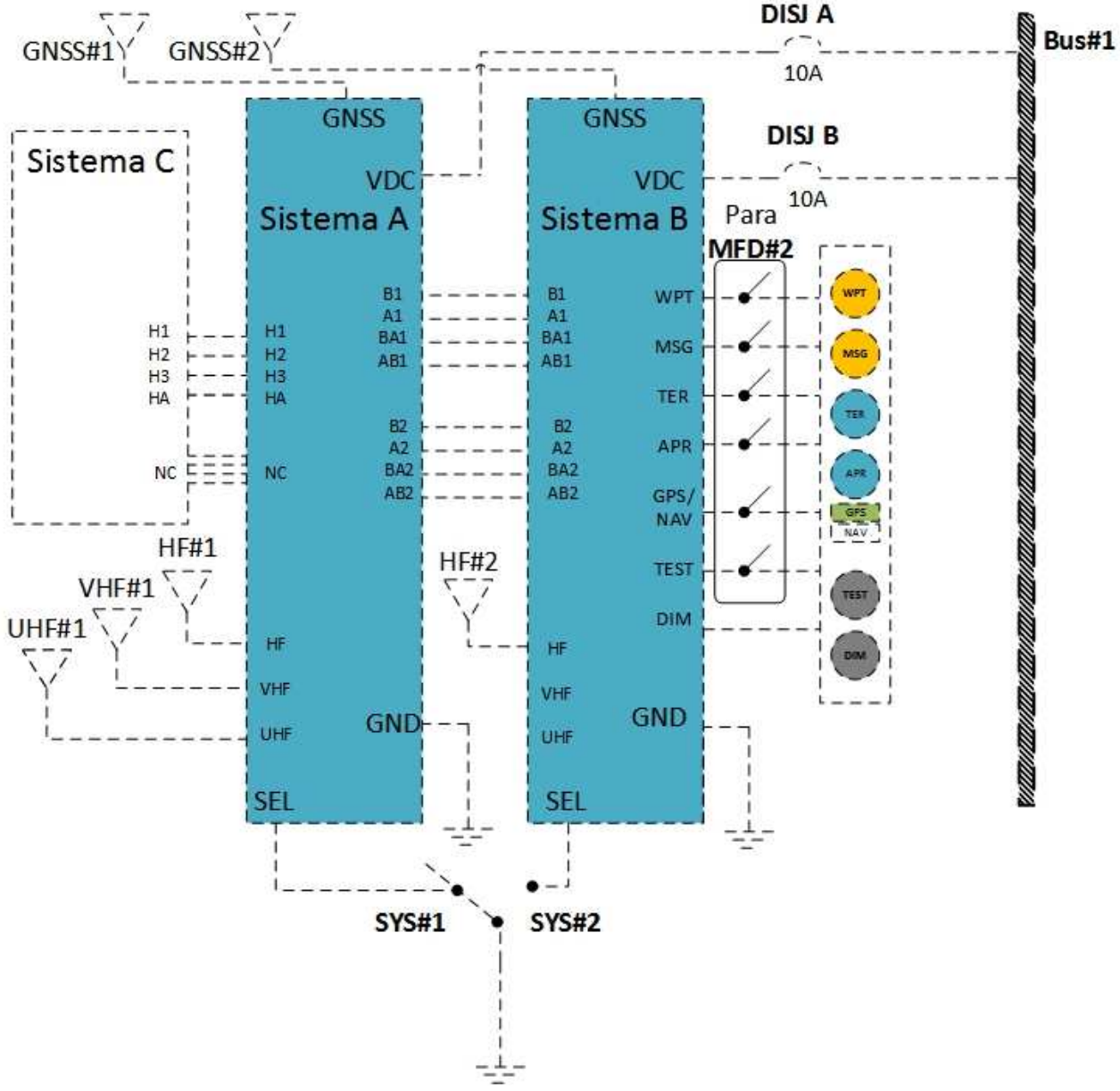


Figura Y – Diagrama de Blocos – conexão com MFD#2

<exemplo para fins ilustrativos, somente>

Nota: poderão ser citados os esquemas elétricos, ao invés de reproduzi-los em todo ou em parte, desde que a referência seja completa (desenho, nº página/folha e detalhe de linha coluna, se aplicável)

3.1. Instalação da Cablagem Considerando Aspectos de Análise Zonal ("Zonal Analysis")

A cablagem entre os barramentos da aeronave e as unidades instaladas será fixada e o roteamento da cablagem será separado de outros sistemas de acordo com as práticas aceitáveis, sendo utilizado padrões especificados pelo próprio fabricante da aeronave, as AC 43.13-1B e AC 43.13-2B, ou outra norma compatível que apresente o mesmo nível de segurança. Os cabos não serão roteados em regiões por onde passem fluidos inflamáveis, umidade ou vento excessivo. Será observado na instalação dos cabos a adequada separação e proteção em relação a:

a. Linhas de combustível e componentes associados.

b. Linhas hidráulicas e componentes associados.

c. Linhas de oxigênio e componentes associados.

d. Equipamentos aquecidos, dutos de ar quente e linhas associadas.

f. Cabos associados a sistemas de controle mecânico, cabos de comando e seus componentes associados, bem como outros objetos que se movem.

g. Superfícies e cantos pontiagudos.

h. Cablagem de sistemas essenciais.

i. e outros aplicáveis.

4. FUNCTIONAL HAZARD ASSESSMENT (FHA)

Ver exemplo no Apêndice 4 < Descrever funções apresentadas na tabela, critérios de classificação, documento utilizados come referência e demais tópicos aplicáveis>

Item	Função	Condição de falha	Fase do voo	Efeito da falha na aeronave / piloto	Meio de detecção da falha	Classificação da falha	Comentário	Método de validação
…		...	...	...	...	...	...	...

Tabela W – "Functional Hazard Assessment" (FHA) <exemplo para fins ilustrativos, somente>

5. PRIMARY SAFETY ASSESSMENT ANALYSIS (PSSA)

Ver exemplo no Apêndice 5 < Descrever funções apresentadas na tabela, critérios de classificação, documento utilizados come referência e demais tópicos aplicáveis>

Função	Falha
<nome da função>	<descrição da falha>

Tabela S: Falhas Classificadas como "Major", "Hazardous" ou "Catastrophic"
<exemplo para fins ilustrativos, somente>

ABX Aeronaves Ltda.	Pág. Nº 10	Total págs. 10
<TÍTULO DA INSTALAÇÃO>	Aeronaves modelo 505-A	
RELATÓRIO DE ANÁLISE DE FALHAS	Relatório nº **ABX –SA-001** Revisão: **EI –** 10/08/15	

6. REFERÊNCIAS

1- 505-A- Pilot Reference Handbook, Doc. PRH-505A, Rev. 4, de 05 de maio de 2005.

2- TrShPlane Switches and Annunciators Data Sheet Handbook, Doc. 123456789101112, Rev. 12, de 12 de dezembro de 1999.

3- TrShPlane Switches Detailed Hazard Analysis & Historical Airworthiness, Doc. 101112123456789, Rev. AB, de 10 de julho de 2013.

7. IMPACTOS NOS PROCEDIMENTOS OPERACIONAIS EXISTENTES

< Caso aplicável, apresentar possíveis procecimentos operacionais (normal / emergência) afetados pela instalação dos sistemas em questão e que sejam objetos do resultado do "Safety Assessment". Consolidar as informações pertinentes no AFMS, caso aplicável. >

8. CONCLUSÃO

< Apresentar concussão substanciando o que foi apresentado no relatório, comentando as condições de falhas, em especial as condições "Major" ou superiores, e referenciando/comentando as ações de mitigação necessárias e demais tópicos aplicáveis>

< Os dados apresentados nesta análise demonstra que o projeto de instalação dos sistemas cumpre com os requisitos RBAC XX.1309, XX.1431 (listar outros aplicáveis). Nenhuma falha simples resulta em uma condição insegura. Baseado nas práticas de projeto, separação e outros fatores de mitigação, e considerando separadamente, e em relação a outros sistemas, nenhuma combinação de falhas resulta em qualquer condição de falha mais severa que "no safety effect".>

9. ANEXO Z – DESENHOS DA INSTALAÇÃO

Desenho nº	Título
60000	Desenhos do Painel, Instalação e Fixação (10 págs.)
70100	Esquemas elétricos (7 págs.)
70101	Diagrama de Blocos (2 págs.)

APÊNDICE 4 – EXEMPLO DE FUNCTIONAL HAZARD ASSESSMENT (FHA)

Item	Função	Condição de falha	Fase do voo	Efeito da falha na aeronave / piloto	Meio de detecção da falha	Classificação da falha	Comentário	Método de validação
1	Suprir alimentação via Avionics BUS#1 e BUS #2	Perda da alimentação via Avionics BUS#1 e BUS #2	Todas	Perda total da função	Tela escura nos MFDs	"Major"	Análise complementar vide capitulo SSA- SAFETY ASSESSMENT ANALYSIS	• Ensaios no solo • MTBF x,xxxx EXP-9 • Equipamentos "Back-up" XXXXX, YYYYY, ZZZZ e Stand-by KKKKKK, LOLOLOL
2	Exibir GNSS	Perda da informação do GNSS #1	Todas	Perda do meio primário de providenciar navegação GNSS	Alerta "GNSS OFF" nos dois MFDs e no PFD	"Minor"	O sistema GNSS # 2 supre a navegação GNSS em caso de falha do sistema GNSS#1	• Ensaios em solo e voo • MTBF x,xxxx EXP-9
3	Exibir áudio do DVD aos passageiros	Perder áudio do DVD para os passageiros	Todas	Perda do áudio do DVD	Alerta "DVD OFF" no MFD #2	"No Safety Effect"	-	Função do entretenimento, não essencial ao voo
…		...	...	...	...	...	...	...

APÊNDICE 5 – EXEMPLO DE PRIMARY SAFETY ASSESSMENT ANALYSIS (PSSA)

Função	Falha
Suprir alimentação via Avionics BUS#1 e BUS #2	A perda da alimentação via Avionics BUS#1 e BUS #2 pode ser gerada pela falha da chave disjuntora "Master Avionics", segundo o manual do fabricante da aeronave [Ref. 1]. A possibilidade de falha dessa chave, original da aeronave, é classificada como extremamente remota, pois, de acordo com o Manual Do fabricante da chave [Ref. 2], pois possui MTBF inferior a 0,89 EXP-7. Em complemento, não existe histórico de falhas relatadas dessa chave pelo fabricante da aeronave ou pelo fabricante da chave, sendo essa empregada em centenas de modelos de aeronaves, conforme referência [Ref. 3].

APÊNDICE 6 – EXEMPLOS DE CLASSIFICAÇÃO DE SISTEMAS SEGUNDO A SEVERIDADE DE FALHA

Sistema	Classe (DO-254)	Classificação da falha	Documento que pode ser apresentado
Sistemas primários; PFD; FADEC e outros controles do motor; "Air Data"; Sistema Inercial; radio-altímetro para "autoland"	A*	"Catastrophic"	FHA/ PSSA/ SSA
Sistemas auxiliares; MFD; sistemas de comunicação e navegação; sistema elétrico	B/C*	"Hazardous"	FHA/ PSSA/ SSA
Sistemas de Pressurização	C*	"Major"	FHA como parte de SSA
Sistemas de Manutenção	D	"Minor"	FHA
Entretenimento, Equipamentos de "Galley"; CVR/FDR	E**	"No Safety Effect"	FHA

* **Nota 1:** Os efeitos ambientais, tais como HIRF e "Lightning" (verifique as AC 20-158 e AC 20-136, em suas revisões mais atuais), impacto de pássaros ("bird-strike"), entre outros, não devem ser considerados em combinação com outra falha única ou falha latente pré-existente.

** **Nota 2:** Considerando-se os casos mais comuns. Como exemplo de um caso comum, pode ser citada a falha de um equipamento de "Galley", como uma cafeteira deixando de funcionar. Desconsidera-se o caso da cafeteira entrar em curto e se incendiar pois, nesse caso, um curto é considerado como sendo falha do sistema elétrico e deve ser classificado como "Major" ou "Hazardous". A AC 23.1309 possui vários exemplos de classificação de falhas para aeronaves Part 23.

Nota 3: Para softwares, além de classificar sua função conforme a DO-254, a classificação da severidade da falha deve ser conforme os critérios da DO-178, em sua revisão mais atual.

Nota 4: Para uma análise quantitativa, deve ser considerada a classe da aeronave segundo a AC 23-1309-1E.

Nota 5: Na elaboração de FHA, a classificação de falha pode variar de acordo com o tipo de operação da aeronave (VFR/IFR, diurno/noturno, etc.)

APÊNDICE 7 – EXEMPLO DE USO DO FHA PARA VERIFICAR REQUSITOS DE QUALIFICAÇÃO CONFORME A DO-160, QUANTO A HIRF, LIGHTNING E EMI

<table>
<tr><th></th><th>HIRF
A, B e C</th><th colspan="2">LIGHTNING
A, B, C</th><th>EMI
Todos equipamentos</th></tr>
<tr><td>DO-160
ACs
ARPs</td><td>SEÇÃO 20 (*)
AC 20-158
ARP 5583A</td><td colspan="2">SEÇÃO 22 (**)
AC 20-136A
ARP 5415A</td><td>SEÇÃO 21 (**)
(Emissividade)</td></tr>
<tr><td>Severidade
<u>A controle</u></td><td>Deve ter medição direta na aeronave</td><td colspan="2">Deve ter medição direta na aeronave</td><td rowspan="5">Categoria M ou H
*simplifica ensaio de EMI (qualitativo).

- Não OK, executar teste mais severo de EMI.</td></tr>
<tr><td>Severidade
<u>A display</u></td><td>DO-160E
6dB W, F
ou
0dB Y, G</td><td>B</td><td>B</td></tr>
<tr><td>Severidade
<u>B</u></td><td>RR (“conducted”, “radiated”)</td><td>Sem interfaces externas
Nível 3
A3G33</td><td>Com interfaces externas
Nível 4
A4G44</td></tr>
<tr><td>Severidade
<u>C</u></td><td>TT (W, Y, R)</td><td>Nível 2
A2G22</td><td>Nível 3
A3G33</td></tr>
<tr><td>Outros</td><td>N/A</td><td colspan="2">N/A</td></tr>
</table>

A – “Catastrophic”. B – “Hazardous”. C – “Major”.

* Nota 1: Classificações dependem do tamanho da aeronave, considerando sistemas instalados na cabine do piloto. Consultar a DO-160 para outros casos e para verificar a aplicação específica.

** Nota 2: Considerando sistemas instalados na cabine do piloto. Consultar a DO-160 para outros casos.

*** Nota 3: As classificações acima podem mudar dependendo da versão da DO-160.