Organização Brasileira
para o Desenvolvimento
da Certificação Aeronáutica

– Treinamento e Capacitação –

INTERPRETANDO A VISÃO DA AUTORIDADE DE AVIAÇÃO CIVIL NO PROCESSO DE *SAFETY ASSESSMENT*

Módulo III – O PROCESSO DE *SAFETY ASSESSMENT*– Parte 2

2ª. Edição (Revisada)

Eng. Jolan Eduardo Berquó

– Outubro 2017 –

SUMÁRIO

Apêndices

1. CONSIDERAÇÕES INICIAIS

Este é o nosso último Módulo do PDC-01. Com base nos Módulos I e II, podemos agora apresentar o que poderíamos chamar de Estudos de Caso, desenvolvendo avaliações de *Safety Assessment* importantes para a identificação dos sistemas que deverão realizar as funções nível aeronave, segundo os requisitos de segurança da Autoridade.

Lembramos que o processo completo de *Safety Assessment* (Ref. 8) compreende as seguintes avaliações:

- Avaliações Funcionais (*Functional Assessments*): **AFHA,** para a aeronave como um todo, e **SFHA**, para os respectivos sistemas;
- Avaliação Preliminar de Segurança de Sistemas (*Preliminary System Safety Assessment*): **PSSA**; e
- Avaliação de Segurança de Sistemas (*System Safety Assessment*): **SSA**.

A sequência de avaliações AFHA, SFHA e PSSA promove os *inputs* para a avaliação conclusiva do processo de *Safety Assessment*, ou seja, a SSA (*System Safety Assessment*), que vai demonstrar à Autoridade que os sistemas definidos e respectivas instalações cumprem os requisitos[1].

Rigorosamente, a AFHA (*Aircraft Functional Hazard Assessment*), como vimos, avalia as funções nível aeronave com relação à segurança da tripulação, da aeronave e dos ocupantes, em decorrência de perda ou mau funcionamento das funções nível aeronave; contudo, não podemos perder de vista que se trata de uma avaliação de alto nível, não se preocupando com os meios que serão materialmente caracterizados pelos sistemas, para a realização das funções nível aeronave.

Esse papel de avaliar os meios, identificando suas funções e analisando-as quanto a suas *Failure Conditions,* cabe à SFHA (*System Functional Hazard Assessment*), que fornecerá *inputs* para a PSSA, que, por sua vez, identificará, como *inputs* para a SSA, os requisitos aplicáveis aos sistemas que irão realizar as funções nível aeronave.

A atividade final, a SSA, demonstrará à Autoridade, como dissemos, que os sistemas da aeronave estão em conformidade com os requisitos estabelecidos.

[1]Sempre “requisitos de segurança”.

Antes de ir adiante, é oportuno lembrar que estamos considerando aeronaves Classe IV (*Commuter Category*)[2] e com autorização para voo IFR[3].

1.1. Duas Prévias e Importantes Recomendações

Como primeira recomendação, deve-se alertar o Analista de *Safety Assessment* para não se perder no emaranhado de documentos regulatórios da Autoridade.

Primeiro, tem de considerar que a Seção 1309 das Partes 23, 25, 27 e 29 é que estabelece os requisitos de segurança para os sistemas tratado em cada uma dessas Partes. As respectivas AC's (*Advisory Circulars*), ligadas a essas seções, sugerem uma metodologia para desenvolver o processo de *Safety Assessment*.

No entanto, não se pode perder de vista que quando estiver desenvolvendo o processo, para um determinado sistema, deverá ser analisada a Seção (p.ex., os requisitos da Seção 23.1309) específica para o sistema, bem como a respectiva AC, usando esta, se for o caso, em conjunção com a AC específica (p.ex., a AC 23.1309-1E) da metodologia para o desenvolvimento do processo de *Safety Assessment*. Trata-se de um par indissociável de documentos.

Os requisitos estabelecidos na seção específica para o sistema, em geral têm relação com o processo de *Safety Assessment* daquele sistema. É o caso, por exemplo, da Seção 1311 da Parte 23, que trata dos requisitos específicos para os displays eletrônicos, e o seu par, a AC 23.1311-1C, que apresenta uma metodologia para a comprovação dos requisitos contidos na Seção 1311, além de apresentar claramente vínculo com a AC 23.1309-1E, que é AC geral dedicada a *safety* dos sistemas da Parte 23.

Se o Analista entender bem isso, ele se poupará um bocado[4].

A segunda recomendação refere-se à língua que deverá ser utilizada em toda a documentação gerada, a partir do processo de *Safety Assessment*. Neste PDC, estamos utilizando nossa língua portuguesa, para facilitar o entendimento de nossos leitores, os quais, em princípio, são, na maioria, brasileiros. Mas, a documentação real enviada à Autoridade, pertinente ao *Safety Assessment*, prudentemente deve ser toda ela escrita na língua inglesa, não por exigência de nossa Autoridade (ANAC), mas para o caso de a

[2] V. Fig. 2 da AC 23.1309-1E (Ref. 5).
[3] IFR: *Instrument Flight Rules*: regras aplicáveis para voo em condições IMC (*Instrument Meteorological Conditions*).
[4] Caso haja dúvida, entre em contato com o autor, na DCA-BR, por meio do e-mail jberquo@dcabr.org.br.

aeronave ser vendida para usuários estrangeiros e ter de ter então sua certificação validada pela Autoridade a que está ligado o usuário. Neste caso, a língua inglesa é de aceitação universal.

2. DESENVOLVIMENTO COMENTADO DA AFHA

2.1. Considerações Preliminares

A AFHA, naturalmente, é feita para todas as funções da aeronave, derivadas da Análise Funcional da Engenharia de Sistemas (ES) da empresa. O objetivo é avaliar todas essas funções, em relação às *Failure Conditions* e suas associadas severidades, resultantes da falha, por perda da função ou por mau funcionamento de algum sistema da aeronave, associando a cada *Failure Condition* os respectivos requisitos previstos pela Autoridade.

Vamos repetir aqui o que já dissemos alhures: Na elaboração da AFHA, o analista deve esquecer (não pensar em) os sistemas que serão *a posteriori* definidos para realizar essas funções. É importante entender isso.

Não obstante, cremos ser também importante dizer, com ênfase, que os engenheiros, neste ponto, já elaboraram ou estão finalizando uma Especificação Técnica Preliminar para apresentar à Autoridade, no momento de dar início ao processo de certificação. Essa especificação, que é, em parte, fruto do levantamento dos requisitos gerais da maioria dos potenciais clientes da comunidade aeronáutica, já inclui os sistemas que irão realizar as funções da aeronave, sem identificar fabricantes. Os engenheiros até sabem, em muitos casos, quais serão os fabricantes desses sistemas e até mesmo o *Part Number* (PN) dos sistemas e de suas LRU's[5].

Em tese, eles só não saberiam, concretamente, quais são os requisitos[6] que devem ser alocados a esses sistemas. Essa importante tarefa é do processo de *Safety Assessment*.

Seja como for, o grupo (analista, piloto e engenheiros) que realizará a AFHA não está interessado em saber quais serão esses meios (sistemas), que serão providos para a realização das funções nível aeronave. É como se eles não existissem ainda.

[5] LRU: *Line- Replaceable Unit:* Unidade – ou Equipamento – Substituível em Linha (de manutenção).
[6] Requisitos de segurança (*safety*).

Por isso, enfaticamente asseveramos que o analista só deve se concentrar na severidade da *Failure Condition* correspondente à perda ou mau funcionamento das funções nível aeronave. Os meios materiais que serão disponibilizados para fazer isso, repetimos, não lhe interessam, nessa fase. Eles serão apresentados, na continuidade do Processo de *Safety Assessment*, na FHA nível sistemas (SFHA), prosseguindo com a PSSA, na alocação dos requisitos para os sistemas e seus equipamentos.

A maioria dos clientes do mercado pesquisado poderia dizer, por exemplo, que gostaria que as informações primárias de Guiagem e Navegação (*Guidance and Navigation*) fossem todas colocadas num *display* eletrônico, e que o sistema que incluísse esse *display* fosse de altíssima confiabilidade. Entretanto, uma boa parte desses clientes provavelmente não citaria necessariamente nenhum fabricante desse sistema. Os engenheiros, no entanto, já teriam, é claro, a solução praticamente pronta; já teriam até vislumbrado sistemas de vários fornecedores, já disponíveis no mercado[7], que poderiam satisfazer os clientes.

Pois bem, antes de prosseguir, permitam-nos assinalar uma reflexão importante: "*Sabemos que a aeronave, em si, é um corpo inerte, cheio de funções, mas que, sozinho, é uma "pata choca". No dizer de algumas gerações de outrora, isto significaria não fazer nada, por si só; mas, "ganha vida", quando ela está sob a batuta de pilotos, que a comandam e controlam. É exatamente por isso que enfatizamos, em Safety Assessment, serem os pilotos o foco. Na realidade, eles são um verdadeiro sistema que realiza a principal função na aeronave: comandar e controlar a aeronave, levando-a a se movimentar. No momento em que os pilotos perderem o comando e/ou o controle da aeronave, em virtude de perda ou mau funcionamento de uma função crítica[8], ou, pior ainda, por um problema neles próprios, não haverá mais o que fazer, e a precipitação da aeronave tornar-se-á extremamente provável".*

2.2. O Processo da AFHA

Vamos apresentar o processo de uma AFHA, considerando, como exemplo, não todas as funções, mas apenas algumas daquelas necessárias para a realização das operações de voo, que selecionamos a título de exemplo.

[7] COTS*: Commercial Off-The-Shelf,* isto é, sistema já disponível comercialmente, para aquisição e uso.
[8] Função cuja perda ou mau funcionamento pode gerar uma *Failure Condition* de severidade catastrófica.

Alertamos para o seguinte fato: a elaboração da AFHA não é obra de apenas um analista, mas de engenheiros e pilotos experientes. Mesmo com a ajuda desse pessoal, é fato normal que a AFHA desenvolvida por uma equipe, relativa a um determinado projeto, possa apresentar resultados diferentes da AFHA desenvolvida por outra equipe, relativa ao mesmo projeto. Isso é normal.

Para mitigar um pouco essas diferenças entre grupos, sugere-se muito cuidado na seleção da equipe que realizará a AFHA. Ainda que tendo alguma experiência profissional, é prudente que o Analista forme uma equipe com um piloto experiente, se possível no tipo de aeronave que está sendo desenvolvida, e também com um experiente engenheiro de sistemas (ou vários, dependendo do momento das avaliações), que irão ter participação importante, nas fases seguintes do processo de *Safety Assessment*.

Mesmo com esse cuidado, pode ocorrer, por exemplo, que para uma determinada *Failure Condition*, uma equipe considere sua severidade *Major*, enquanto outra equipe a considere *Hazardous*. Na verdade, a última palavra poderá envolver a discussão com a Autoridade, a quem será apresentada a AFHA, nos primeiros momentos da Certificação.

Tornamos a dizer que a AFHA do projeto de uma nova aeronave civil é, quase sempre, baseada em AFHA's de projetos de aeronaves similares anteriores, já em operação. Em suma, é um trabalho de retoques, retirando ou acrescentando algumas funções. Isso nem sempre ocorre com projetos de aeronaves militares, cujas funções podem mudar, de projeto para projeto, dependendo da missão.

É útil apresentar o elenco das funções nível aeronave numa configuração de árvore semelhante àquela apresentada na Fig. A1.2 do Apêndice 1, dando uma ideia geral das funções da aeronave, para o Analista e sua equipe conduzirem a avaliação e também para a Autoridade, no momento de apresentar-lhe a AFHA e a metodologia que será seguida no processo de *Safety Assessment*.

Seja como for, vamos considerar como gabarito no processo da AFHA os passos a seguir.

(1) Obter o elenco das funções da aeronave das três fases da operação (pré-voo, voo e pós-voo), resultante da Análise Funcional da ES da empresa – Item 3.1 do Módulo II;

(2) Descrever o modo de falha de cada função (perda ou mau funcionamento da função)[9]**;**

(3) Especificar a fase ou fases em que ocorreria a falha;

(4) Especificar as condições meteorológicas (IMC ou VMC)

(5) Especificar os potenciais efeitos (*Failure Condition*) na tríade: tripulação, aeronave e ocupantes;

(6) Identificar a severidade das *Failure Conditions*[10]; e

(7) Inserir essas informações numa tabela semelhante àquela que apresentamos na Fig. A1.3, constante do Apêndice 1.

***Nota**: Ao descrever o modo de falha (2), a não citação das informações "Anunciado(a) e/ou Não Anunciado(a)", significará que o efeito da falha será o mesmo nas duas condições. Caso haja diferença no efeito, numa ou noutra condição, a informação será citada.*

Vamos então considerar, a título de exemplo, apenas as seguintes funções **(N1)**[11], ligadas à função básica **(B2): Realizar as Operações de Voo** (v. item 3.1.1 do módulo II)

- Prover Guiagem e Navegação (*Guidance and Navigation*);
- Prover Comunicação (*Communication*); e
- Prover Potência (*Power*).

Embora possa parecer óbvio, consideramos importante enfatizar que se a perda de uma função **(N1)** de uma função básica (**BX)** for caracterizada como *Failure Condition* Catastrófica, a consequência, obviamente, é a perda da respectiva função básica **BX**. É o caso também da função básica (**B2),** a qual, como veremos, tem algumas funções **(N1)** com *Failure Conditions* catastróficas.

Da mesma forma, se ocorrer a perda de uma função **(N2)**, com *Failure Condition* catastrófica, ocorrerá a perda da respectiva função **(N1)**.

---

[9] Um mau funcionamento é qualquer ocorrência que modifique o output esperado de uma função. Uma ocorrência desse tipo que pode trazer resultados graves é o chamado *Misleading*, que consiste em se apresentar como uma informação enganosa, isto é, que parece ser verdadeira, mas não é. Em condição IMC (*Instrument Meteorological Conditions*), esse tipo de mau funcionamento pode implicar em acidentes graves, se não for incluído meios de detectar esse evento.

[10] Devemos levar em conta que um modo de falha pode ter várias *Failure Conditions* (efeitos), dependendo da fase da operação e das condições meteorológicas.

[11] A rigor, temos de considerar todas as funções identificadas pela ES da empresa, em especial aquelas da operação da aeronave, compreendendo movimento no solo (para a decolagem e pouso) e operação em voo.

Concentremo-nos agora na função **(N1)** Prover Guiagem e Navegação, que possui as seguintes funções **(N2)**:

(1) Prover a posição da aeronave (*Location: altitude, longitude and latitude*);

(2) Prover a Atitude da Aeronave (*Attitude*);

(3) Prover a Velocidade da Aeronave *(Speed);*

(4) Prover a Direção da Aeronave (*Heading*); e

(5) Prover o Gerenciamento de Voo (*Flight Management*).

Vamos nos deter nas quatro primeiras, que serão suficientes para apresentar o processo. Relembremos o que foi dito no Módulo II (item 3.1.1), quando inserimos em Nota o argumento de que as funções (2), (3), (4) e a Altitude, que fazem parte também da função **(N1)**, compõem uma função dita de síntese **(N1),** qual seja**: Prover as Informações Primárias de Voo** (*Provide Primary Flight Information).* Será esta a função que consideraremos, a partir da FHA nível sistema (SFHA), quando trataremos dos meios que serão materialmente caracterizados pelos sistemas que realizarão as funções identificadas na AFHA. Isso será devidamente explicado na SFHA.

Prosseguindo, vamos à função **(N2)**(1).

- Passo (1)

  Função: Prover a posição da aeronave (altitude, longitude e latitude).

- Passo (2)

  Perda da função ou mau funcionamento (p. ex., *misleading*),

- Passo (3).

  Fase: todas as fases do voo (*Flight*)

- Passo (4).

  Condições Meteorológicas: IMC.

- Passo (5).

  Failure Condition ou potencial efeito na Tríade: Tripulação, aeronave e ocupantes.

Tripulação – Possível perda de consciência da altitude, perdendo o controle da aeronave;

Aeronave – Perda.

Ocupantes – Ferimentos fatais ou incapacitações.

- Passo (6).

  Severidade: *Catastrophic*.

- Passo (7).

  Inserir os resultados numa tabela semelhante àquela da Fig. A1.3.

Pois bem, notem que consideramos o problema com o voo num espaço em condições IMC (voo IFR). A situação seria outra se a condição externa ambiental fosse VMC (voo VFR). Todavia, já dissemos algures que, na avaliação, temos de considerar a *Failure Condition* em seu efeito mais severo, que neste caso é aquele pertinente à condição IMC.

A função **Prover Comunicação (*Communication*)** tem duas funções **(N2)** :

(1) Prover Comunicação Interna; e

(2) Prover Comunicação Externa.

A função **Prover Comunicação Interna** refere-se à comunicação entre membros da tripulação ou da tripulação para os passageiros. A perda da função é de severidade *Minor*, mesmo em condições IMC, requerendo apenas manutenção, na próxima parada.

A perda da função **(N2) Prover Comunicação Externa**, em condições IMC, na fase de aproximação, pode trazer algum perigo, mas há pilotos que consideram a severidade da respectiva *Failure Condition* no máximo *Major,* e outros*, Hazardous*. É o que já dissemos alhures, isto é, um grupo que analisa a severidade de uma *Failure Condition* pode discordar da análise de outro grupo. Aí, de novo, não tem jeito, entra a Autoridade.

Muito bem, uma vez terminada essa avaliação, o Analista deve elaborar um quadro semelhante àquele inserido na Fig. A1.3 (Apêndice 1), que fará parte do relatório pertinente à AFHA.

3. DESENVOLVIMENTO COMENTADO DA SFHA/PSSA

3.1. O Sistema Configurado no Projeto Conceitual

É neste item que trataremos da análise dos meios e respectivas funções que serão caracterizados materialmente pelos sistemas, já pensados - na fase de projeto conceitual, que proverão as funções nível aeronave, alocando aos mesmos os requisitos[12] pertinentes, permitindo que os engenheiros de sistemas identifiquem, a partir desses requisitos, os sistemas adequados; aí, já em termos de fabricantes, nomenclatura e *part number*. Trata-se de um misto de SFHA e PSSA.

Esses resultados serão também inputs para a SSA System Safety Assessment, que será apresentada à Autoridade, mostrando a conformidade dos sistemas com os requisitos alocados ao smesmos.

Nos Apêndices 2 (Relatório de SFHA) e 3 (Relatório de PSSA), faremos uma distinção mais clara entre os dois tipos de avaliação.

Pois bem, prosseguindo, podemos dizer que, neste ponto, os engenheiros já sabem que a função **(N1) Prover Guiagem e Navegação**, em condições IMC, tem funções **(N2)** com *Failure Conditions* de potencial catastrófico. São aquelas funções que provêm os parâmetros *altitude, airspeed e attitude.*

Atualmente, o meio mais utilizado para prover essas informações é o chamado **Sistema de Informações Primárias de Voo,** constituído pelos já populares *displays* eletrônicos, conhecidos genericamente pelos chamados EFIS (*Electronic Flight Instrument System*), também configurados como *glass cockpit*, por causa de suas telas em LCD (*Liquid Crystal Display*) ou LED (*Light Emmiter Diode*).

Os engenheiros de sistemas sabem, sobejamente, que informações primárias de voo podem ser concentradas num EFIS, principalmente no conhecido PFD (*Primary Functions Display*), formando um sistema com sensores e respectivas interfaces de processamento.

[12] Só para lembrar: “Requisitos de segurança (*safety*)”.

Os sinais gerados pelos sensores são processados por interfaces (*Air Data Computers* – ADC, e *Attitude Heading Reference System* – AHRS) e encaminhados, por meio de *Data Buses* (DB)[13], para o PFD.

É fácil perceber que se houver uma falha ou mau funcionamento (*misleading*, por exemplo) nesse PFD, em condições IMC, a respectiva *Failure Condition* terá severidade catastrófica. Segue que o requisito qualitativo deve ser "extremamente improvável", e o quantitativo, $F < 10^{-9}$ phv[14] (taxa de falha).

Se houver também falha ou mau funcionamento de um qualquer dos sensores e/ou transdutores, uma ou mais informações serão perdidas, podendo, em condições IMC, conduzir a *Failure Conditions* catastróficas.

Por outro lado, como sabemos, o atendimento a esse requisito apenas com um display PFD não é aceitável pela Autoridade, em virtude do contundente e sábio critério da *single failure* (V. item 5.3.2, pág. 28 do Módulo II). Destarte, esse sistema com *display* tem de ser, no mínimo, dual[15], isto é, há que se ter pelo menos dois sistemas simples, formando um sistema redundante, tanto para o piloto quanto para o co-piloto, constituído por um display principal P (aquele que o piloto e o co-piloto miram de pronto) e um secundário S; isto, repetimos, é o mínimo.

Essa configuração inclusive é aceitável para demonstrar a conformidade com o requisito (b) do CFR 14 Part 23.1311, qual seja:

> *(b) The electronic display indicators, including their systems and installations, and considering other airplane systems, must be designed so that one display of information essential for continued safe flight and landing will be available within one second to the crew by a single pilot action or by automatic means for continued safe operation, after any single failure or probable combination of failures.*

O sistema secundário poderia ser outro PFD, mas, se possível com um outro PN e fabricante, para evitar falhas de modo comum, ou ser, por exemplo, um mais aconselhável, o *Navigation Display* (ND), um EFIS que além de propiciar as informações primárias de voo, ainda propicia outras informações, como aquelas referentes ao plano de voo.

---

[13] A mais usada hoje, na aviação comercial, é a DB ARINC 429.

[14] Phv: por hora de voo. Quando escrevemos F <... Phv, estamos falando da taxa de falha da LRU. Quando multiplicamos a taxa de falha por horas voadas, aí temos F como probabilidade de falha no período de horas de voo mencionado.

[15] Critério da *Single Failure*.

A título de exemplo, esse par (PFD e ND) está instalado no Airbus 380 (Ref. 1), formando dois pares, um para o piloto e outro para o co-piloto, conforme apresentado na Fig. 1 (Ref. 1), que mostra a cabine de um Airbus 380 com os dois pares de PFD e ND. A Fig. 2 e 3, a seguir, mostram um *close* dos *displays*.

Nessa configuração, quando o sistema PFD tem problemas (o do piloto ou o do co-piloto), o respectivo ND do par entra em ação, apresentando as informações primárias de voo. No entanto, se o ND falhar, o PFD não vai substituí-lo, mas vai apresentar, na parte inferior de sua tela, pelo menos o plano de voo, que normalmente é apresentado no ND.

Também poderiam ser usados um sistema PFD (P) e um sistema reversionário[16] MFD (S), este com página dedicada contendo as informações primárias de navegação.

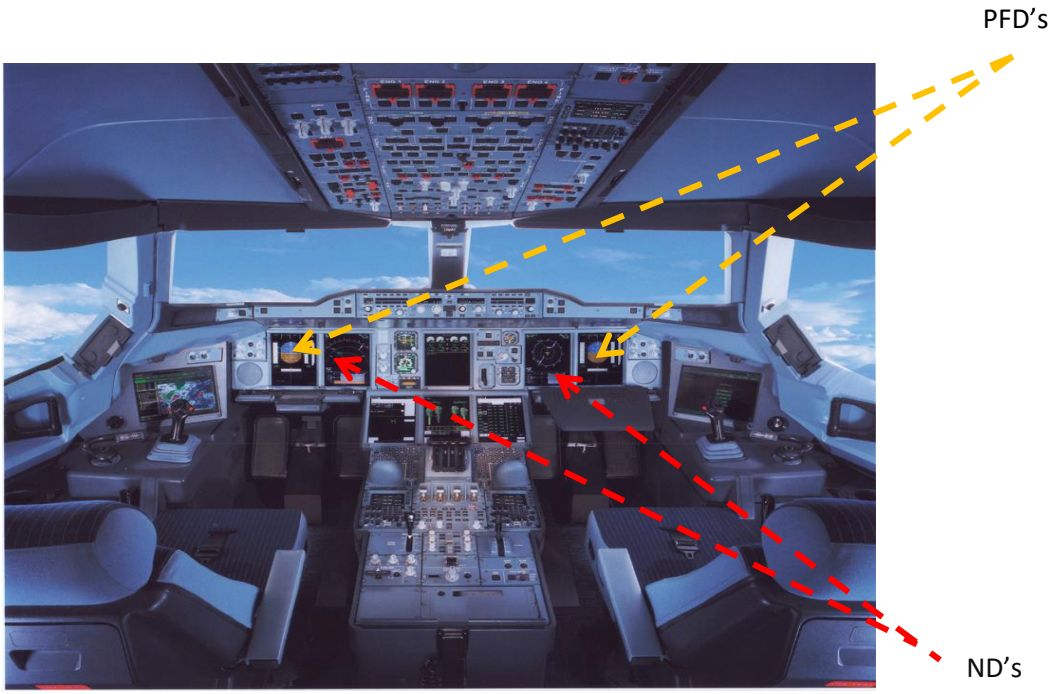

Fig. 1 - C*ockpit* do Airbus 380 (Ref. 4)

[16] Reversionário (*Reversionary*) – Um meio secundário para prover informação normalmente apresentada no PFD ou MFD. No caso, por exemplo, de se usar um PFD como meio primário, o MFD poderia ser usado como um meio reversionário, apresentando, em uma de suas páginas, as informações apresentadas no PFD.

Fig. 2 – *Primary Flight Display* - PFD (Ref. 4))

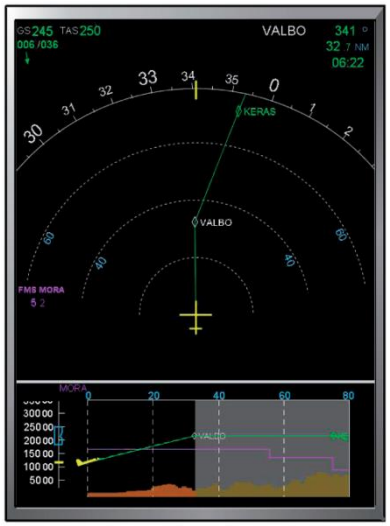

Fig. 3 – *Navigation Display* – ND (Ref. 4)

Costuma-se instalar ainda uma segunda redundância: os chamados *displays Standby Instrument System (SS)* - Fig. 4, para as *primary functions altitude, attitude* e *airspeed*, na hipótese de dupla falha (PFD e ND/MFD). Ele é praticamente autocontido, isto é, compreende, em seu interior, uma tríade de giroscópios e de acelerômetros, além de transdutores de pressão do estado sólido, junto com um microprocessador também de estado sólido. A única conexão comum com os outros displays é o sistema Pitot Estático,

Convenhamos que, com tal configuração, estamos diante de um sistema em si muito seguro (dupla redundância), ou seja, “quase à prova de falhas”. Na verdade, há muitas soluções disponíveis para os engenheiros de sistemas.

Esta é a configuração de displays (PFD, ND e SS) imaginada pelos engenheiros de sistemas da empresa, no projeto conceitual. **Esse conjunto de displays, sensores e processadores dos sinais provenientes desses sensores formam o já mencionado Sistema de Informações Primárias de Voo,** que será o sistema abordado como exemplo em nosso processo de Safety Assessment.

Vamos então apresentar uma FTA qualitativa (Fig. 5), procurando mostrar os vários eventos que podem levar à perda da aeronave, em consequência da perda desses meios críticos para a navegação, gerando, portanto requisitos para a procura (aquisição) do sistema.

Fig. 4 – *Standby Instrument System* (Ref. 4)

A configuração mostrada na FTA da figura 5, em dupla redundância (três displays), tem uma *Failure Condition* catastrófica com baixíssima probabilidade de falha por hora de voo (F), satisfazendo com sobra o requisito $F < 10^{-9}$ por hora de voo. Na verdade, "o céu é mais ou menos o limite". Só há um detalhe: os custos também sobem, e o espaço para a instalação torna-se mais difícil. Acrescente-se ainda que tornar a probabilidade de falha nula é utopia. Ter-se-ia que aplicar uma redundância com um número de sistemas tendendo ao infinito.

Em geral, os fornecedores desses sistemas, por sinais complexos, são desenvolvidos segundo uma TSO (*Technical Standard Order*) específica para esses sistemas[17], como tivemos a oportunidade de explicar no Módulo II, o que os credenciam a serem instalados numa aeronave[18], em termos de funcionalidade e segurança. São os chamados sistemas com TSOA (*Technical Standard Order Authorization).*

Para os sistemas que não são TSOA, em princípio deverá ser demonstrado que, de algum modo satisfazem os mesmos requisitos gerais estabelecidos na pertinente TSO; mas é melhor discutir isso com a Autoridade. Mas, uma coisa é certa: o Aplicante vai ter que, ainda que minimamente, comprovar que as LRU's do sistema foram desenvolvidas

[17] TSO (*Technical Standard Order*). Nossa Autoridade (ANAC) traduz o termo por Ordem Técnica Padrão (OTP).
[18] "Credencia", mas a efetiva instalação só acontecerá se o sistema passar nos ensaios, mostrando seu efetivo funcionamento e sua compatibilidade eletromagnética com o ambiente reinante na área de instalação.

de acordo com os princípios relativos aos DAL's (*Development Assurance Level*), contidos nos padrões de qualidade da DO-178C e DO-254, já comentados no Módulo II.

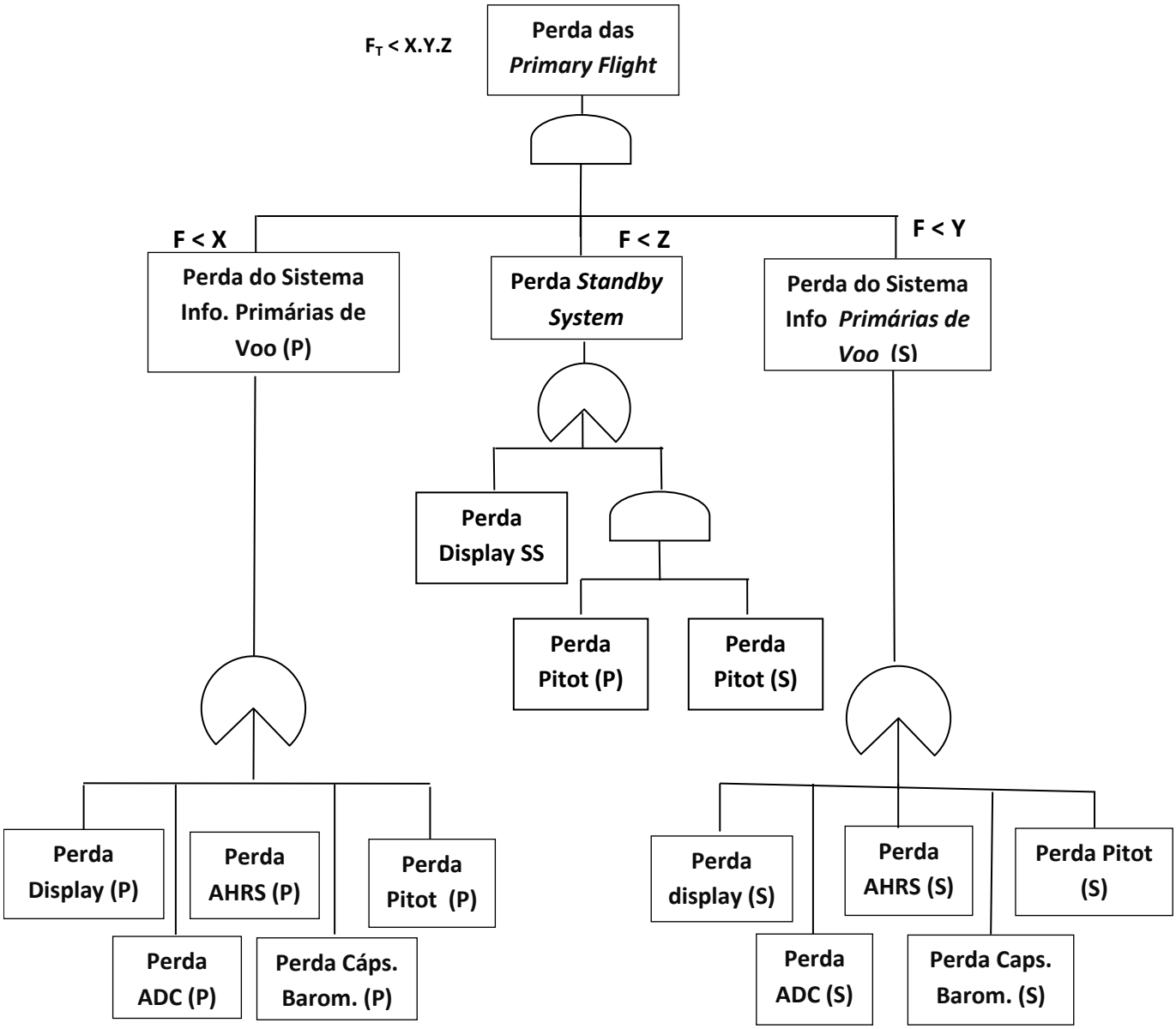

Fig. A3.1 - FTA do Sistema de Apresentação das Informações primárias

Pode-se estranhar que a FTA acima só apresente a perda do sensor de *Altitude* e *Airspeed e* não a perda dos sensores de *Attitude* e *Heading*. Pois bem, devemos dizer que estes sensores estão no próprio AHRS. São sensores inerciais, que captam as variações angulares de atitude e de deslocamento linear da aeronave, sem depender de informações externas à aeronave, como no caso do sensor de altitude.

Desse modo, sendo esses sensores internos ao AHRS, eles entram no cômputo da taxa de falha do AHRS.

Em se tratando de sistemas complexos, como sabemos ser o caso, com um *Hardware* (HW) com circuitos integrados *(chips),* dispositivos que, isoladamente, executam muitas funções sob a batuta de um SW incorporado, nem sempre se consegue obter dos fornecedores uma FMEA (*Failure Modes, And Effects Analysis*) e ensaios confiáveis, mostrando que os mesmos atendem aos requisitos quantitativos a eles alocados.

Em nosso exemplo, neste trabalho, vamos considerar que o fornecedor (ou fornecedores) consiga desenvolver uma FMEA e consiga também realizar ensaios suficientemente aceitáveis.

Deve-se, no entanto, informar que quando isso não é possível, e amiúde não é mesmo, o único jeito é aceitar apenas o enquadramento das LRU's do sistema nos padrões de garantia da qualidade de desenvolvimento, ou seja, os chamados DAL's (*Development Assurance Level*), estabelecidos, como já mencionado acima, na DO 178C (para o SW) e na DO-254 (para o HW complexo), ao compasso da severidade das *Failure Conditions* atribuídas a cada sistema simples que compõe o sistema redundante.

Os DAL's voltados para esses sistemas são A, para o SW e HW Complexo do sistema principal (PFD), e B, para o SW e HW Complexo dos sistemas redundantes (ND e *Standby Instrument System* - SS)[19].

Falemos um pouco dos sensores e interfaces sensores/displays.

Os sinais de *attitude e heading, que, como sabemos,* são gerados e processados no AHRS (*Attitude Heading Reference System*) e encaminhados na forma aceitável pelos *displays*, por meio de Barramentos de Dados (*Data Buses*). Como já dissemos – e não custa repetir, os sensores são do tipo inercial, isto é, não dependem de informações

[19] V. Fig. 2, pág. 23, da AC 23.13-09-1E

externas. Os sensores para a *attitude* são três giroscópios (*Ring Laser Gyroscopes*)[20] de altíssima confiabilidade, um para cada eixo ortogonal de um sistema de referência tridimensional. Para a informação do vetor deslocamento, adotam-se três acelerômetros (*Accelerometers*), um para cada eixo ortogonal (xyz), também de altíssima confiabilidade.

Por outro lado, as informações de *altitude* e *airspeed* são geradas a partir de dados do ar externo (*Air Data*), captados pelo Tubo de Pitot, tratados por sensores (transdutores) e encaminhados ao ADC (*Air Data Computer*), para processamento e encaminhamento, na forma conveniente, aos barramentos e daí para os displays. Portanto, as informações de *altitude* e *airspeed* dependem de dados externos à aeronave.

Resumindo, o ADC (*Air Data Computer*) é a interface entre o sensor barométrico e os displays, para a *Altitude* e *Airspeed*; para a *Attitude* e *Heading* é o AHRS (*Attitude Heading Reference System*), com seus próprios sensores inerciais e processador de sinais para os *displays*.

A alimentação elétrica dos sistemas principal e secundário vem de barramentos elétricos diferentes existentes na aeronave e, no caso de emergência, de uma bateria conectada à barra da bateria. Trata-se de uma configuração de distribuição de potência elétrica de altíssimo nível de confiabilidade. Contudo, devemos ter em conta que a alimentação elétrica é objeto de avaliação dedicada ao sistema que a provê, ou seja, ela tem sua FTA específica, em que se leva em consideração todos os outros sistemas, isto é, cargas (*loads*), que dependem de alimentação elétrica.

O que queremos dizer é que devemos nos preocupar apenas com o sistema objeto de nossa avaliação, ou seja, queremos identificar somente as *Failure Conditions* e respectivas severidades decorrentes das falhas ou maus funcionamentos do sistema do qual estamos tratando.

É importante deixar claro que o *Standby Instrument System* (SS) recebe alimentação elétrica comum aos outros *displays*; mas, além disso, está também conectado à barra da bateria, o último recurso, em termos de alimentação elétrica.

[20] Por muito tempo – e testemunhamos isso, até com uma certa nostalgia, as aeronaves tiveram que contar com instrumentos giroscópicos do tipo eletromecânicos, dispositivos de altíssima tecnologia eletro-mecânica, mas com baixíssima confiabilidade (altíssima falibilidade), em função principalmente do desgaste de rolamentos utilizados nesses instrumentos, que sustentavam uma rotação de até 25.000 RPM de uma massa girante. Num certo momento, surgiram os giroscópios *Ring Lasers* (e outros), cuja estrutura é inteiramente estática, isto é, não utilizam massas girantes. Em termos de confiabilidade, fo,i de fato, um gigantesco salto.

Lembramos novamente que facilita bastante para o Aplicante escolher PFD's, ND's, SS's e MFD's de fabricantes de reconhecida tecnologia, sobretudo aqueles cujas LRU's possuam TSOA (*Technical Standar Order Authorization*), o que, como já dissemos, os credencia para a instalação na Aeronave.

3.2. Evocando o Critério da Similaridade

Não podemos deixar de lembrar do importante item 5.5.5, do Módulo II, que trata da avaliação de *Failures Conditions Hazardous e Catastrophic.* Esse item refere-se aos casos em que não é necessário o rigor de avaliações de uma combinação de análises qualitativa e quantitativa, permitindo-se somente uma análise qualitativa.

Seu subitem (d) deixa claro que para sistemas complexos (como é o caso), onde possa ser rigorosamente identificada uma verdadeira similaridade, em todos os atributos relevantes, incluindo atributos de instalação, pode ser possível avaliar uma *Failure Condition Hazardous* ou *Catastrófica* como sendo respectivamente *extremely remote* ou *extremely improbable,* a partir de um julgamento experiente de engenheiros, utilizando apenas uma análise qualitativa, conforme os itens 6.2 e 6.3 do mencionado módulo, ou seja, por meio de uma avaliação de projeto (*Design Appraisal*) e avaliação de instalação (*Installation Appraisal*) do sistema a ser instalado na aeronave, mostrando a similaridade com sistemas instalados em outras aeronaves certificadas e em operação. Mas atenção: é requerido um alto grau de similaridade no projeto e na aplicação; ademais, alerta-se, o Aplicante terá o ônus da demonstração cabal dessa similaridade, junto à Autoridade.

Por importante, vamos inclusive registrar, a seguir, a definição de Similaridade constante da AC 23.1309-1E:

Similarity*. The process of showing that the equipment type, form, function, design, and installation have only minor differences to previously approved equipment. The safety and operational characteristics and other qualities of the new proposed installation should have no appreciable effects on the airworthiness of the airplane.*

Seja como for, como já dissemos algures, a Autoridade tem a última palavra. Cautela não faz mal a ninguém.

Acrescentamos também a possibilidade de adotar o critério da Identidade (V. item 5.5.1, pág. 32 do Módulo II); mas, a demonstração cabal dessa identidade pode ser um pouco mais complicada que a demonstração da similaridade.

No exemplo de sistema adotado neste trabalho, vamos supor que não haja nem identidade, nem similaridade.

4. ANÀLISE DE CAUSA COMUM (*COMMON CAUSE ANALYSIS* – CCA)

A tudo isso que falamos, temos de adicionar a chamada CCA (*Common Cause Analysis*), já mencionada no item 6.6 do Módulo II, que deverá fazer parte da avaliação de segurança dos sistemas. Voltamos aqui a tratar do assunto com algum acréscimo ao que dissemos no referido Módulo.

Devemos chamar a atenção para o fato de que a realização dessa análise (que está dividida em três outras, mencionadas abaixo) exige a participação ativa de engenheiros de sistemas.

Dependendo do sistema, por mais que nos esforcemos, é difícil realizá-la de maneira realmente exaustiva[21], ou seja, sempre há brechas perceptíveis ou não ao Analista. Desse modo, vamos procurar considerar aqui os principais aspectos, em termos de sistemas aviônicos.

Pois bem, um sistema aviônico pode falhar (perder a função ou ter um mau funcionamento), isto é, não apresentar a informação dele esperada, principalmente em virtude de:

(a) um problema interno (falha ou mau funcionamento de seus equipamentos);

(b) erros ocultos de projeto (*Sneak Circuits*), que se manifestam dependendo de certas condições não vislumbradas pelos projetistas (são falhas sistemáticas, ou seja, não aleatórias);

(c) ausência ou distorção de *inputs* provindo de outros sistemas, indispensáveis para sua correta funcionalidade;

(d) interferência eletromagnética interna (Compatibilidade Eletromagnética - EMC);

[21] V, ARP 4761.

(e) agressões provenientes do ambiente externo à aeronave (HIRF e Lightining, por exemplo);

(f) ações inadequadas de manutenção, provenientes de erros de procedimentos ou de ações inadequadas dos mecânicos.

Dissemos, naquele módulo, que a CCA é dividida em três áreas de estudos (análises):

- Análise de Segurança Zonal (*Zonal Safety Analysis* - ZSA);
- Análise de Riscos Específicos (*Particular Risk Analysis* - ORA); e
- Análise de Modo Comum (*Common Mode Analysis* – CMA).

Com certeza, não vamos esgotar essas análises aqui, mas vamos dar uma ideia desse processo, em se tratando do sistema que escolhemos para nosso processo de *Safety Assessment*.

4.1. Análise de Segurança Zonal (*Zonal Safety Analysis*)[22]

Em se tratando de sistemas aviônicos, devemos nos preocupar, minimamente, com os seguintes aspectos:

(1) temperatura do ambiente, onde as LRU's vão ser instaladas;

(2) interferência Eletromagnética (EMI) entre Sistemas;

(3) segurança das ações físicas de manutenção na inspeção, remoção e instalação de LRU's; e

(4) procedimentos corretos de manutenção, de modo a não introduzir circuitos ocultos (*sneak circuits*), numa possível ação de reparo de uma LRU (manutenção corretiva).

No aspecto (1), já existe uma preocupação com a temperatura, principalmente porque os especialistas sabem que a temperatura é a maior inimiga dos dispositivos eletrônicos do estado sólido (diodos, transistores, chips), que constituem todos os sistemas aviônicos da atualidade. Em geral, esses sistemas estão instalados na chamada *Avionics Bay*

[22] Poder-se-ia também traduzir para Análise Zonal de Segurança.

(conhecida como *Báia*), um espaço a eles destinado, com temperatura adequada às características físicas deles[23].

No aspecto (2), todo sistema, quando instalado, passa por ensaios de compatibilidade eletromagnética (EMC), procurando verificar se algum sistema interfere em outros sistemas ou é interferido por esses outros. Esses ensaios estão previstos no mapa MOC (*Means of Compliance*) que o fabricante apresenta à Autoridade, para informar quais são os meios (ensaios, inspeção, etc..) para a comprovação de todos os requisitos das Seções, no caso as da Parte 23. A cada meio de comprovação corresponde um relatório, apresentando o resultado obtido. A AC que trata desses ensaios de compatibilidade eletromagnética é a AC 23-8C.

Quanto ao aspecto (3), como requisito básico na Mantenabilidade, desenvolvida no projeto, o fabricante leva em consideração a facilidade e a segurança das ações de inspeção, remoção e instalação dos sistemas. Isso pode ser demonstrado por meio de uma Avaliação de Projeto (*Design Appraisal*) e Avaliação de Instalação (*Installation Appraisal*), mas também por meio de inspeção, utilizando o manual de procedimentos de remoção e instalação apresentados pela empresa.

No que tange ao aspecto (4), considerando possíveis inserções de circuitos ocultos no reparo de LRU's, não há como evitar totalmente essa possibilidade, a não ser recomendando que as regras existentes no manual de reparo da LRU sejam rigorosamente seguidas, com qualidade no trato do material usado na manutenção, sempre com o foco de não introduzir circuitos ocultos. Só para citar uma causa de circuitos ocultos, no reparo: soldagem inadvertida, deixando a solda ligar peças que podem trazer problemas funcionais, não percebido nos testes funcionais da oficina de manutenção, mas que poderão inesperadamente aparecer num momento do voo.

4.2. Análise de Riscos Específicos (*Particular Risk Analysis*)

Riscos específicos são aqueles pertinentes exclusivamente ao tipo de sistema que estamos avaliando, que no caso é um sistema aviônico.

O Módulo II cita, em particular, esses riscos relativos a sistemas aviônicos, evidenciando que os principais problemas para esses sistemas estão na exposição a raios (*Lightining*) e

[23] Lembrar que o inimigo número 1 de sistemas eletrônicos com componentes do estado s é a temperatura, que pode fazer variar características de dispositivos eletrônicos, mudando o comportamento funcional dos mesmos.

HIRF (*High Intensity Radiated Fields*). São ditos específicos porque os sistemas aviônicos são os mais vulneráveis a essas agressões.

Pois bem, hoje as empresas adotam técnicas de projeto, instalação, análises e ensaios dedicados para esses sistemas, seguindo sugestões apresentadas em AC's dedicadas, para mostrar que os sistemas podem, satisfatoriamente, suportar essas agressões e continuar operando normalmente.

As demonstrações (análises de projeto, ensaios no solo e em voo, etc.) são parte do mapa de MOC (*Means of Compliance*), desenvolvido para todos os requisitos das pertinentes Partes e Subpartes do CFR 14, para mostrar quais são os meios utilizados para demonstrar a conformidade com esses requisitos; em nosso caso, os requisitos na Parte 23, Subparte F – *Equipment*.

Portanto, de alguma forma será demonstrado à Autoridade, por meio de relatórios (*Design Appraisal* e *Installation Appraisal*) e/ou ensaios, que o sistema cumpre os requisitos atinentes aos problemas mencionados.

4.3. Análise de Modo Comum (*Common Mode Analysis* – CMA)

Esta, em nossa opinião, é, de fato, a parte mais complicada da CCA *(Common Cause Analysis)*. Trata-se da questão de independência entre os sistemas. Deve-se ter assegurado que a falha ou mau funcionamento de um sistema não afete outro sistema. Normalmente, os projetistas têm consciência do problema e procuram sempre evitar essa dependência, mas é necessário, de alguma forma, mostrar que a independência existe. Como fazer isso? Por exemplo, na análise da falha ou mau funcionamento de um sistema, verificar qual é a magnitude das consequências nos outros sistemas. Aqui, não entram a interferência eletromagnética (EMI) e HIRF, já considerados na PRA.

Enfim, tudo isso comentado acima há que ser demonstrado, no relatório de Análise de Causa Comum (*Common Cause Analysis*), podendo estar no texto do relatório de SSA ou ser um Apêndice do mesmo.

5. DESENVOLVIMENTO COMENTADO DA SYSTEM *SAFETY ANALYSIS* (SSA)

5.1. Introdução

Com os dados das avaliações anteriores, sobretudo da PSSA, podemos passar para a reta final do processo de *Safety Assessment*, ou seja, a Avaliação de Segurança de Sistema (*System Safety Assessment*). Nesse momento, estamos com o sistema definido, em sua arquitetura, e com todas as análises provenientes do fornecedor ou fornecedores.

O encadeamento do processo acontece mais ou menos como registramos a seguir.

Uma vez estabelecidos os requisitos do sistema em análise, apresentados na SFHA e PSSA, vai-se então verificar, no mercado, a disponibilidade dos sistemas que cumpram esses requisitos[24].

Rigorosamente, neste ponto, os possíveis fornecedores teriam de apresentar FMEAs pertinentes às LRU's do sistema e também do sistema completo que contêm essas LRU's, comparando a taxa de falha do sistema, obtida nessas análises, com a taxa de falha de requisitos estabelecida na PSSA.

Como mencionado, em se tratando de sistemas complexos, pode também acontecer que o fornecedor não tenha possibilidade de desenvolver uma FMEA minimamente confiável e nem condições de realizar testes ou ensaios exaustivos e convincentes, ficando sempre uma lacuna, se nesse mister insistir, que pode tornar sua avaliação não conclusiva. Nesses casos, repetimos que a única coisa que se pode exigir é que o fornecedor demonstre que desenvolveu o sistema, considerando os DAL's (*Development Assurance Level*), para SW e HW, conforme estabelecidos na PSSA.

Se o sistema não tiver uma TSOA, e a empresa considerar que tal sistema apresentado por um determinado fornecedor é o mais favorável, técnica e/ou financeiramente, vai ter de discutir com a Autoridade o melhor caminho a seguir e levar em conta os prazos. Consideraremos, no entanto, daqui por diante, que essa questão já esteja resolvida com a Autoridade e passamos então para o processo de SSA.

[24] Mas, atenção, não são apenas os requisitos quantitativos de segurança (taxas de falhas), mas outros como dimensões das LRU's, com base no padrão ARINC 600; potência elétrica, resultados de ensaios ambientais, de acordo com a DO-160, etc.

5.2. O Processo da SSA

Em nossa opinião, para o nosso sistema, os passos mínimos necessários e suficientes para o processo da SSA são os seguintes:

a. Verificação de que os requisitos estabelecidos na SFHA/PSSA foram atendidos pelo(s) fornecedor(es). Isso pode ser feito comparando os resultados da(s) FMEA(s) (quando existente, apesar de se tratar de sistema complexo) dos fabricantes das LRU's do sistema, com os resultados da SFHA/PSSA, inclusive com relatórios pertinentes à CCA.

b. Com os dados acima, atualizar a FTA nível sistema e, a partir desta, atualizar a FTA nível aeronave.

Ao final, deverá ser elaborado um relatório, tendo, entre seus Anexos, os relatórios relevantes ao sistema, fornecido pelo fornecedor (ou fornecedores).

6. CONCLUSÂO

Com este módulo, encerramos o PDC-01. No entanto, queremos acrescentar algumas considerações relativas a tudo que apresentamos neste PDC, em especial neste Módulo III.

Sabemos que não esgotamos o assunto aqui tratado, e que o trabalho, sem dúvida, tenha lacunas; mas, seja como for, acreditamos que o mesmo tenha sido útil para quem queira se familiarizar e prosseguir com estudos sobre o processo de *Safety Assessment*.

Trata-se de uma atividade fascinante, isto é, algo que nos ocupa bastante, nas discussões com companheiros igualmente interessados no assunto, bem como com a Autoridade. O necessário para isso são estudos e discussões desapaixonadas, ou seja, todos querendo aprender mais e mais.

Como viram, utilizamos como exemplo, para discutir o processo, um sistema bastante usual, tendo em conta sua importância para a tripulação, em termos de concentração, num só sistema, de informações de voo ditas primárias, para a condução da aeronave

com segurança, já que várias funções desse sistema possuem *Catastrophic Failure Conditions.*

É bom lembrar que os sistemas de displays eletrônicos, já de há algum tempo, vêm sendo instalados em muitas aeronaves, podendo assim até mesmo, arriscamos em dizer, serem considerados convencionais, a despeito de serem complexos. Isso, sem dúvida, dependendo do fabricante, facilita o trabalho no processo de *Safety Assessment*, no que tange à similaridade da instalação.

Considerado isoladamente, cremos que o processo aqui aplicado caberia também muito bem numa Certificação Suplementar de Tipo (CST).

No entanto, deve-se ter em mente que quando se trata de uma certificação de tipo (CT), o processo completo comporta muito mais trabalho, em virtude da quantidade razoável de funções que devem ser levadas em conta, no caso de perda ou mau funcionamento.

Mais um importante detalhe: Devemos considerar, não obstante, que todo esse processo de *Safety Assessment* refere-se somente a sistemas da aeronave, responsáveis por apenas 10% dos acidentes catastróficos, ficando os erros humanos, como sabemos, com cerca de 75% da responsabilidade por esses acidentes, atribuídos principalmente às tripulações. Por isso, sugerimos que estejam sempre atentos para qualquer metodologia que pretenda minimizar os problemas de segurança gerados pelos erros humanos.

Uma metodologia, nesse sentido, que vem sendo desenvolvida há uns 10 anos, é a *System-Theoretic Process Analysis,* mais conhecida pela sigla STPA[25]. Até onde temos conhecimento, a precursora dessa metodologia é Nancy G. Leveson, engenheira e professora doutora de Aeronáutica, Astronáutica e Engenharia de Sistemas, no *Massachusetts Institute of Technology* (MIT), nos Estados Unidos.

Sua proposta de metodologia vem encontrando espaço para se propagar. Ela procura, decisivamente, inserir o ser humano na interação com os processos que um sistema como um todo realiza, considerando também o meio ambiente que cerca o sistema, em sua operação. Diríamos que se trata de uma metodologia “de corpo inteiro”; um salto gigantesco, afirmamos, na segurança global do binômio aeronave/ser humano. No entanto, ainda haverá discussões, até que sua teoria seja aceita, mas, é claro, com a introdução de ideias de outrem.

[25] V. MSC 51 e 52: “Há Algo de Novo no Horizonte”, no item “Melhore Seus Conhecimentos”, do *site* da DCA-BR.

Concluímos, agradecendo a todos pela atenção. Queiram nos desculpar por eventuais erros ou equívocos. No entanto, apraz-nos, sinceramente, qualquer crítica construtiva, nesse sentido.

Em breve, estaremos trazendo mais um assunto de interesse, no PDC-02.

Apreciem, nas páginas seguintes, os exemplos de avaliações do processo de *Safety Assessment*, apresentados nos Apêndices 1, 2, 3 e 4.

Obrigado a todos e até breve.

REFERÊNCIAS:

1. *SCOTT, Jackson. System Engineering for Commercial Aircraft – A Domain – Especific Adaptation. Routledge, New York (EUA), 2016.*
2. *ROMLI, Franz I. Functional Analysis for Conceptual Aircraft Design. Journal of Advanced Management Science, Vol. No. 4, December 2013, India.*
3. *RTCA DO-178C, Software Considerations in Airborne Systems and Equipment Certification. RTCA, EUA, Jan/2012.*
4. *COLLINSON, R.P.G. Introduction to Electronics to Avionics. 3rd. Ed. Springer. 2011, United Kingdom (UK), 2011.*
5. *AC 23.1309-1E – System Safety Analysis and Assessment for Part 23 Airplanes, FAA, Nov, 2011; EUA.*
6. *AC 23.1311-1C – Installation of Electronic Display in Part 23 Airplanes, FAA, Nov., 2011; USA.*
7. *RTCA DO-254, Design Assurance Guidance for Airborne Electronic Hardware. RTCA, EUA, Abril/2000.*
8. *SAE ARP 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment. SAE, EUA, 1996.*

APÊNDICE 1

RELATÓRIO SAR-01

FUNCTIONAL HAZARD ASSESSMENT - AIRCRAFT LEVEL (AFHA) DA AERONAVE A-35

Notas do Autor

(1) Página de Rosto. Os dados inseridos nesta página são os considerados indispensáveis. Outros dados e arquitetura da página são de acordo com a sistemática adotada pela empresa.

(2) Sugere-se inserir na capa do relatório a equipe que participou da avaliação. Ex.:

"Profissionais que participaram da FHA nível aeronave:

Coordenador:** Eng. Eletrônico Joaquim Silvério**;

***Colaboradores:** Piloto Jarbas Passarinho; Eng. Eletrônico de Sistemas Antônio das Perdizes"*.

(3) Com relação ao conteúdo, repita-se, todas as funções nível aeronave devem ser consideradas. No entanto, em virtude do espaço demandante e do tempo necessário, vamos tratar neste estudo apenas da função (N1) Prover Guiagem (Guidance) e Navegação (Navigation) e suas funções (N2), bem como a função Prover Comunicação e Prover Potência).

SUMÁRIO

1. INTRODUÇÃO

Este relatório compreende a *Functional Hazard Assessment - Aircraft Level* (AFHA), pertinente à aeronave A-35.

1.1. Referências

(1) CFR 14 Part 23.1309 – *Equipment, Systems and Installations*.

(2) CFR 14 Part 25.1309 – *Equipment, Systems and Installations.*

(3) AC 23.1309-1E – *System Safety Analysis and Assessment for Part 23 Airplanes.*

(4) AC 25.1301-1A – *System, Design and Analysis.*

(5) AC 23.1311-1C – *Installation of Electronic Display in Part 23 Airplanes*.

(6) ARP 4754 – *Certification Considerations for Highly-Integrated or Complex Aircraft Systems.*

(7) ARP 4761 – *Guidelines and Method for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.*

2. DESCRIÇÃO SUMÁRIA

A aeronave S-35 é um bimotor de transporte comercial, projetada para transportar até 20 passageiros a uma distância de até 3.000 Km a 600 Km/h, com teto de serviço de aproximadamente 9.500 metros. Seu voo médio terá uma duração de 4 horas. A descrição de suas características e sistemas é apresentada na Especificação Técnica Preliminar da aeronave.

3. FUNÇÕES NÍVEL AERONAVE

As funções da aeronave estão classificadas em níveis. No nível mais alto, elas são agrupadas em conjuntos funcionais considerados como “Funções Básicas”, atribuindo-lhes a letra **B**, seguida de um número; por exemplo: **(B1)**. Funções de Nível 1 **(N1)** são aquelas ligadas diretamente a uma função básica. Funções de nível 2, simbolizadas por **(N2)**, são aquelas ligadas a uma função de nível 1, e assim por diante.

3.1. Funções Básicas

As funções básicas pertinentes a todas as fases de operação da aeronave, conforme mostradas na Fig. A1.1, distribuem-se em três conjuntos funcionais. São eles:

- **(B1): Realizar Movimento no Solo – Pré-Voo**, compreendendo as fases de *Load* e *Taxi*.
- **(B2): Realizar as Operações de Voo**, compreendendo as fases de *Take-Off, Climb (*ou *Abort), Cruise, Descent, Approach (*ou *Divert)* e *Land*; e

- **(B3): Realizar Movimento no Solo – Pós-Voo** (*Taxi e Unloading).*

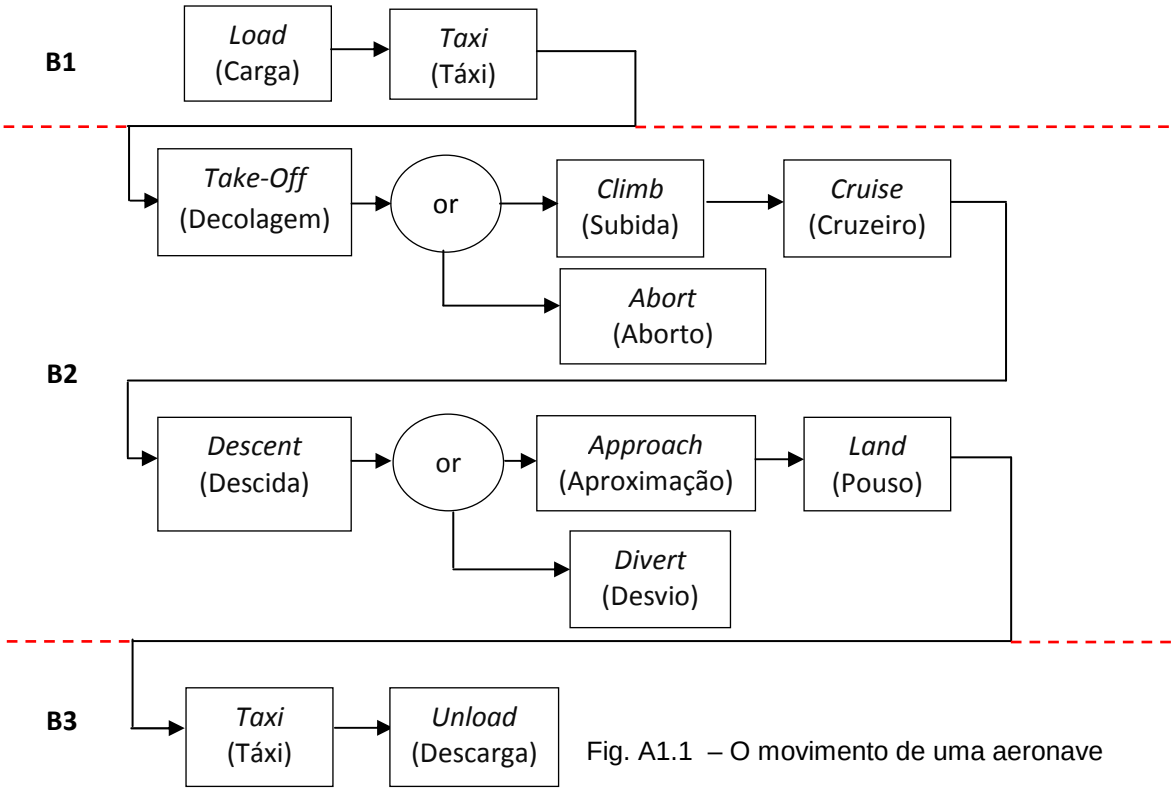

Fig. A1.1 – O movimento de uma aeronave

As funções básicas possuem subfunções de Nível **(N1),** e estas, subfunções de Nível **(N2)**.

> ***Nota do Autor:*** *A título de exemplo, vamos considerar apenas o ramo das funções (N2) da função (N1) Prover Guiagem e Navegação (Guidance and Navigation), (N2) da função (N1) Prover Comunicação (Communication) e a função (N1) Prover Potência (Power), apresentadas no quadro da Fig. A1.2).*

A Árvore de funções da aeronave, relativas a essas fases de operação, é apresentada na Fig. A1.2.

4. RESULTADOS DA AVALIAÇÃO

Os resultados da *AFHA* estão na Fig. A1.3, e a *Preliminary Fault Tree Analysis* (FTA), na Fig. A1.4.

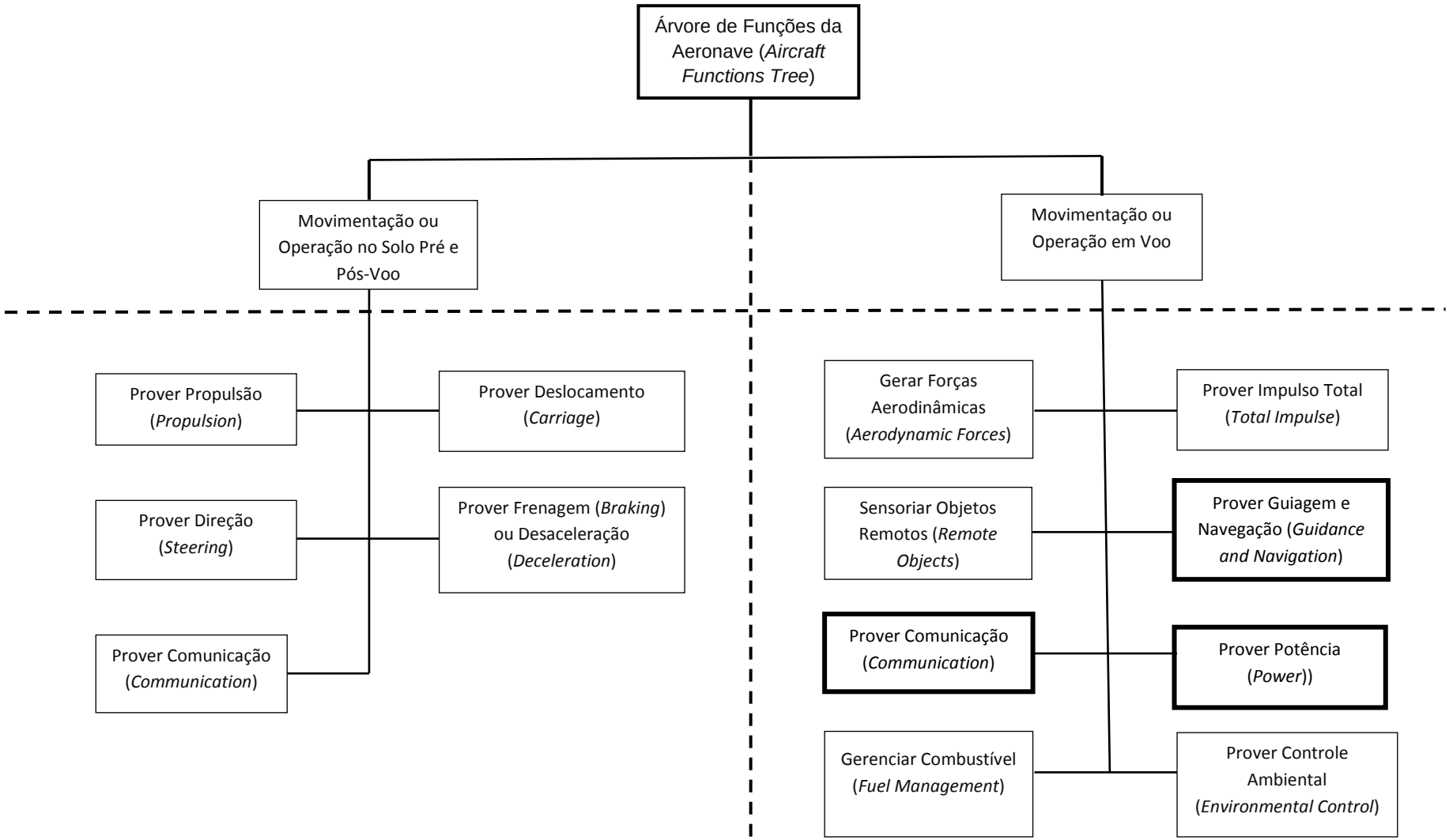

Fig. A1.2 – Árvore de Funções da Aeronave

Item	Função/Condição de Falha	Fase da Operação	Condição Meteorológica (IMC/VMC)	Efeito da Condição de Falha na Tripulação. Aeronave e Ocupantes	Severidade
1. Realizar Movimentação ou Operação no Solo - Pré e Pós-Voo					
2. Realizar Movimentação ou Operação em Voo					
2.1. Prover Guiagem e Navegação (*Guidance and Navigation*)					
AFHA-1	Perda das indicações de posição (*Location*) da aeronave (Altitude, Longitude e Latitude), ou *misleading.*	Voo	IMC	**Tripulação:** Possível perda de consciência da altitude, podendo perder o controle da aeronave; **Aeronave:** Perda. **Ocupantes:** Ferimentos fatais e/ou incapacitações.	*Catastrophic*, devido à perda da informação de altitude.
AFHA-2	Perda ou *misleading* (não anunciada) da indicação de velocidade (*Speed*) da aeronave.	Voo	IMC	**Tripulação:** Perda de controle da aeronave. **Aeronave:** Perda. **Ocupantes:** Ferimentos fatais e/ou incapacitações.	*Catastrophic*.
AFHA-3	Perda da indicação de atitude (*attitude*), ou *misleading*.	Voo	IMC	**Tripulação:** Provavelmente excederá os limites da aeronave e perderá o controle da aeronave. **Aeronave:** Perda **Ocupantes:** Ferimentos fatais e/ou incapacitações.	*Catastrophic*
AFHA-4	Perda (anunciada ou não anunciada) da indicação de direção *(heading).*	Voo	IMC	**Tripulação:** Seguirá seu curso com a bússola. **Aeronave:** Não será afetada. **Ocupantes:** Provavelmente algum desconforto e possíveis ferimentos.	*Hazardous*
2.2. Prover Comunicação					
AFHA-5	Perda da comunicação interna.	Voo	IMC/VMC	**Tripulação**: comunicação direta entre os membros da tripulação e destes com os passageiros. **Aeronave:** Não será afetada. Ocupantes: Não serão afetados.	*No Safety Effect*
AFHA-6	Perda da comunicação externa (anunciada ou não anunciada).	Voo	IMC	**Tripulação**: seguirá seu Plano de Voo. **Aeronave:** não será afetada. **Ocupantes**: não serão afetados.	*Minor*
2.3. Prover Potência					
AFHA-7	Perda da potência	Voo	IMC/VMC	**Tripulação:** Impossibilitada de realizar ações de comando e controle. **Aeronave**: Totalmente desgovernada. **Ocupantes**: Ferimentos fatais e/ou incapacitações.	*Catastrophic*

Fig. A1.3 – Resultados da AFHA

4.1. Outputs da AFHA

Com base na AFHA e nos requisitos da média dos clientes, já na fase (projeto) conceitual, os engenheiros de sistemas da empresa desenvolveram uma arquitetura genérica básica, para elaborar uma *Preliminary Fault Tree Analysis* da aeronave (PFTA) mostrada na Fig. A1.4, ligada aos resultados apresentados na Fig. A1.3.

Notem que a perda da função **(N1)** – Guiagem e Navegação pode ter *Failure Condition* catastrófica, isso porque três de suas funções **(N2)**, *Altitude, Attitude e Airspeed* têm *Failure Condition* com essa severidade.

Dessa maneira, a perda dessa função **(N1)** deve atender ao requisito $F < 10^{-9}$/phv[1] (taxa de falha), imposto à função, em virtude de três de suas funções **(N2)** terem também que atender a esse requisito. Cremos que a porta **OU**[2] da Fig. A1.4 deixe isso claro[3].

Pois bem, a função **(N1)** – Guiagem e Navegação é, como a imensa maioria das funções desse nível, dependente da alimentação elétrica, uma vez que os sistemas que vão realizar as respectivas funções **(N2)** são aviônicos, isto é, dependem da alimentação elétrica, tanto em corrente contínua como alternada. Por isso, a perda da função **(N1)** - Prover Potência tem *Failure Condition* catastrófica.

Entretanto, o nível de segurança dos sistemas de alimentação elétrica atuais, alocados para o provimento de potência é muito elevado, conforme será mostrado na PSSA do Sistema Elétrico, somando-se a isso a criteriosa distribuição das cargas dependentes da alimentação elétrica. Essas considerações vão ficar mais claras na SFHA.

[1] phv – por hora de voo.

[2] Relembrando: A probailidade apresentada na saída de uma porta OU é a soma das probabilidades das entradas da porta.

[3] Bastaria ocorrer a perda de uma função **(N2)** para ocasionar a perda da respectiva função **(N1)**.

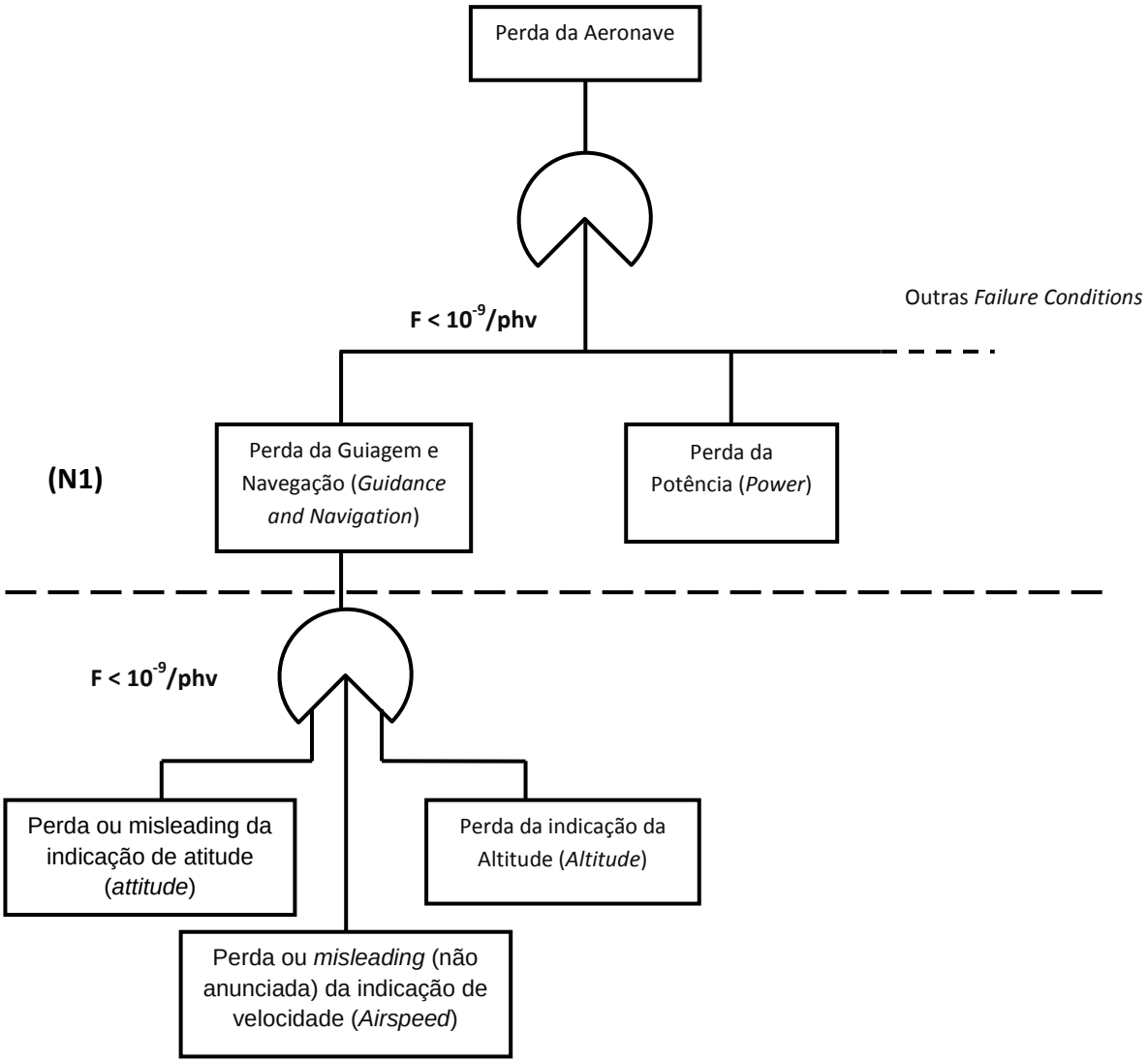

Fig. A1.4 - PFTA para as funções catastróficas

Observação

A porta OU significa que qualquer evento de falha na entrada da porta conduz ao evento de topo; no caso considerado, trata-se da perda da aeronave.

APÊNDICE 2

(Página de Rosto. Os dados inseridos nesta página são os considerados indispensáveis. Outros dados e arquitetura da página são de acordo com a sistemática adotada pela empresa)

RELATÓRIO SAR- 02

FUNCTIONAL HAZARD ASSESSMENT - SYSTEM LEVEL (SFHA) DO SISTEMA DE APRESENTAÇÃO DAS INFORMAÇÕES PRIMÁRIAS DE VOO

(Nota: Rigorosamente, todas as funções nível aeronave devem ser consideradas. No entanto, vamos considerar neste estudo apenas a função (N1) Prover Guiagem (Guidance) e Navegação (Navigation) e suas funções (N2)).

SUMÁRIO

1. INTRODUÇÃO

Este relatório compreende a *Functional Hazard Assessment* Nível Sistemas (SFHA), pertinente ao meio de provimento das seguintes informações, consideradas como Informações Primárias de Voo**:**

- Altitude da aeronave[1] (*Altitude*);
- Atitude da Aeronave (*Attitude*);
- Velocidade da Aeronave *(Airspeed);*
- Direção da Aeronave (*Heading*); e

Essas informações são supridas por funções de nível **(N2)** da função **(N1)** Prover Guiagem e Navegação (*Provide Guidance and Navigation*).

2. REFERÊNCIAS

(1) Especificação Técnica Preliminar da Aeronave S-35.

(2) Resultados da FHA Nível Aeronave (AFHA) da aeronave S-35.

(3) FTA Preliminar da AFHA.

(4) Requisitos de projeto da aeronave S-35, que incluem os requisitos da Comunidade Aeronáutica.

(5) AC 23.1309 -1E – *System Safety Analysis and Assessment for Part 23 Airplanes.*

(6) AC 23.1311-1C – *Installation of Electronic Display in Part 23 Airplanes*.

(7) SAE ARP 4754 – *Certification Considerations for Highly-Integrated or Complex Aircraft Systems.*

(8) SAE ARP 4761 – *Guidelines and Method for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.*

3. CONSIDERAÇÕES GERAIS

O meio utilizado para a apresentação das Informações Primárias de Voo[2] tem como principais componentes (LRUs) *displays* coloridos, atualmente em LCD (*Liquid Crystal Display*) ou em LED (*Light Emitter Diode*), conhecidos genericamente pela sigla EFIS (*Electronic Flight Instrument System*).

Esses *displays* atendem inclusive aos requisitos estabelecidos pela maioria dos clientes, que desejam ter tais informações em *displays* eletrônicos.

No entanto, a AFHA nos dá conta de que entre as funções **(N2),** apresentadas no item 1.0, existem funções cuja perda ou mau funcionamento apresentam *Catastrophic Failure Conditions*, em condições IMC. São elas: Altitude (*Altitude*), Atitude (*Attitude*) e Velocidade (*Airspeed*).

[1] Poderíamos escrever também “Determinar”, em vez de “Prover”; o importante é que o propósito fique claro.
[2] V. Item 2 do Texto.

Há ainda que se considerar a função realizada pelos próprios *displays*, qual seja: **Apresentar as Informações Primárias de Voo** (todas elas). A perda dessa função, em condições IMC[3], conduz a uma *Failure Condition* de severidade catastrófica, já que se perdem, de uma só vez, as três informações mencionadas, além do próprio *display.* As condições consideradas são.

3.1. Sumário

- Perda da informação de altitude da aeronave (*Altitude*). $\lambda < 1.10^{-9}$;
- Perda da Informação de Atitude da Aeronave (*Attitude*). $\lambda < 1.10^{-9}$;
- Perda da Informação de Velocidade da Aeronave *(Airspeed);* $\lambda < 1.10^{-9}$;
- Perda da Informação de Direção da Aeronave (*Heading*). $\lambda < 1.10^{-7}$; e
- Perda da Apresentação das Informações Primárias de Voo (Perda do *display*). $\lambda < 1.10^{-9}$;

Os valores acima são por hora de voo (phv), ou seja, trata-se de taxas de falha.

Com exceção da função primária de provimento de *Heading*, que possui *Failure Condition hazardous,* em condições IMC, todas as outras funções têm *Failure Conditions* de severidade catastrófica.

4. RESULTADOS DA AVALIAÇÃO

A tabela da Fig. A2.1 apresenta o resumo das considerações feitas nesta SFHA.

[3] IMC: *Instrument Meteorological Condition*.

Item	Função/Condição de Falha	Fase da Operação	Condição Meteorológica (IMC/VMC)	Efeito da Condição de Falha na Tripulação. Aeronave e Ocupantes	Severidade
1.	**Prover Funções Primárias de Voo (indicadas no *Display*)**				
SFHA-1	Perda ou misleading das indicações de posição (*Location*) da aeronave (*Altitude, Longitude e Latitude*).	Voo	IMC	**Tripulação:** Possível perda de consciência da altitude, podendo perder o controle da aeronave; **Aeronave:** Perda. **Ocupantes:** Ferimentos fatais e/ou incapacitações.	*Catastrophic*, devido à perda da informação de altitude.
SFHA-2	Perda ou *misleading* (não anunciada) da indicação de velocidade (*Airspeed*) da aeronave.	Voo	IMC	**Tripulação:** Perda de controle da aeronave. **Aeronave:** Perda. **Ocupantes:** Ferimentos fatais e/ou incapacitações.	*Catastrophic*.
SFHA-3	Perda ou misleading da indicação de atitude (*attitude*).	Voo	IMC	**Tripulação:** Provavelmente excederá os limites da aeronave e perderá o controle da aeronave. **Aeronave:** Perda **Ocupantes:** Ferimentos fatais e/ou incapacitações.	*Catastrophic*
SFHA-4	Perda (anunciada ou não anunciada) da indicação de direção *(heading).*	Voo	IMC	**Tripulação:** Seguirá seu curso com a bússola. **Aeronave:** Não será afetada. **Ocupantes:** Provavelmente algum desconforto.	*Hazardous*
2.	**Apresentar as Informações Primárias de Voo (*Display*)**				
SFHA-5	Perda do *display*.	Voo	IMC/VMC	**Tripulação**: comunicação direta entre os membros da tripulação e destes com os passageiros. **Aeronave:** Não será afetada. Ocupantes: Não serão afetados.	*Catastrophic*

Fig. A2.1 Resultados da SFHA

APÊNDICE 3

*(**Nota do autor**: Os dados inseridos nesta página de rosto são os considerados indispensáveis. Outros dados e arquitetura da página são de acordo com a sistemática adotada pela empresa)*

RELATÓRIO SAR- 3

PRELIMINARY SYSTEM SAFETY ASSESSMENT (PSSA) DO SISTEMA DE APRESENTAÇÃO DAS INFORMAÇÕES PRIMÁRIAS DE VOO

SUMÁRIO

1. INTRODUÇÃO

Este relatório compreende a *Preliminary System Safety Assessment* (PSSA) do Sistema de Apresentação das Informações Primárias de Voo da Aeronave S-35.

O objetivo é completar a lista de requisitos para o sistema.

2. REFERÊNCIAS

(1) Especificação Técnica Preliminar da Aeronave S-35.

(2) Resultados da FHA Nivel Aeronave (AFHA) da aeronave S-35;

(3) FTA Preliminar da AFHA;

(4) Resultados da FHA Nível Sistemas (SFHA);

(5) CFR 14 Part 23.1309 – *Equipment, Systems and Installations*;

(6) CFR 14 Part 25.1309 – *Equipment, Systems and Installations;*

(7) AC 23.1309-1E – *System Safety Analysis and Assessment for Part 23 Airplanes;*

(8) AC 25.1301-1A – *System, Design and Analysis;*

(9) AC 23.1311-1C – *Installation of Electronic Display in Part 23 Airplanes*.

(10) ARP 4754 – *Certification Considerations for Highly-Integrated or Complex Aircraft Systems.*

(11) ARP 4761 – *Guidelines and Method for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.*

3. DESCRIÇÃO RESUMIDA DO SISTEMA

O meio previsto, no projeto conceitual, para a apresentação das Informações Primárias de Voo é aquele dedicado a essas informações, ou seja, o *display* PFD (*Primary Flight Display*), com suas respectivas interfaces (ADC, para o processamento da informação de *altitude,* proveniente do sensor barométrico, e Airspeed; AHRS, para o processamento das informações de *attitude* e *heading*, provenientes dos sensores inerciais *Ring Gyroscopes* e *Accelerometers*).

Em face das restrições ditadas pelo critério da *single failure*[1], decidiu-se que o sistema a ser instalado teria de ser pelo menos do tipo dual, isto é, deveria ter minimamente uma redundância (dois *displays*), tanto para o piloto quanto para o co-piloto. O display que os pilotos dirigem de pronto sua visão é denominado principal (P), e o outro, secundário (S).

[1] Critério da *Single Failure* – Nenhuma *Failure Condition* catastrófica pode resultar de uma única falha de um sistema.

Tendo em conta a severidade das *Failure Conditions* (*catastrophic*), o sistema dual, como um todo, deve satisfazer o requisito quantitativo de $\lambda < 10^{-9}$ e Falibilidade $F < 4.10^{-9}$, considerando que o voo médio é de 4 horas.

Além disso, os requisitos de arquitetura do projeto conceitual estabeleceram a instalação de dois barramentos de dados (*Data Buses*), aos quais estarão integrados os displays e as interfaces entre os mesmos e os sensores.

Decidiu-se usar como sistema display secundário a LRU *Navigation Display* (ND), um display que entre outras informações apresenta também as informações primárias de voo.

Ainda no projeto conceitual, optou-se pela instalação de uma segunda redundância, configurada por um *Standby Instrument System* (SS). Trata-se de um sistema quase inteiramente autocontido, isto é, possui seus próprios sensores inerciais, isto é, *Ring Gyroscopes* (para a informação de atitude) e *Acelerommeters* (para a informação de deslocamento retilíneo). São três giroscópios e três acelerômetros, um para cada eixo ortogonal. Seu único sensor externo é o relativo à altitude, ou seja, um sensor barométrico do estado sólido conectada ao Pitot Estático.

Os sistemas principais serão alimentados por uma configuração do sistema de alimentação elétrica, e os secundários por outra configuração, de modo a evitar que a perda de uma configuração de alimentação tenha reflexo em ambos os sistemas.

O *Standby Instrument System* será conectado à barra da bateria.

3.1. FTA do Sistema

A FTA do sistema com dupla redundância, destinado a prover as informações primárias de voo, é mostrada a Fig. A3.1. A configuração é idêntica para piloto e co-piloto. Devemos lembrar que o evento de topo é a perda da aeronave, que deve ter uma taxa de falha $\boldsymbol{\lambda} = 1.10^{-9}$ e $F < 4.10^{-9}$, considerando que o voo médio é de 4 horas.

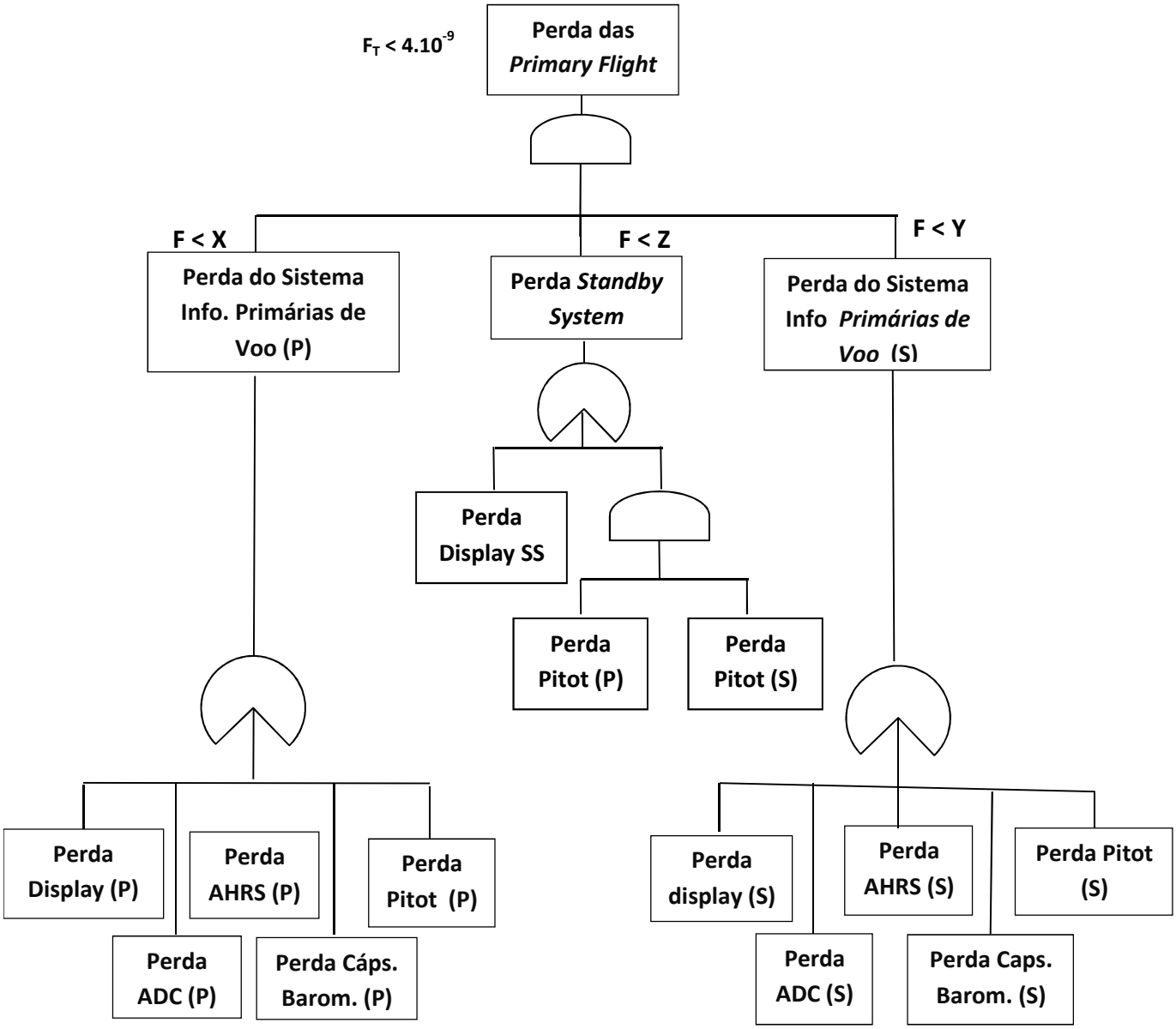

Fig. A3.1 - FTA do Sistema de Apresentação das Informações primárias

O sistema de interface para a altitude e a velocidade (*altitude* e *airspeed*) é o ADC (*Air Data Computer*), que processa a informação proveniente da cápsula barométrica. O *output* do ADC é endereçado ao *display*, por meio de um par de barramentos de dados (*Data Buses)*.

Por outro lado, a interface para a *attitude* e *heading* é o AHRS (*Attitude and Heading Reference System*), que contém os sensores inerciais *Gyroscope/Accelerometers* e o módulo de processamento dos sinais proveniente desses sensores. Também aqui o

output do AHRS é endereçado ao *display*, por meio do mencionado par de barramentos de dados (*Data Buses*).

4. RESULTADOS DA PSSA DO SISTEMA DE DISPLAY

O fato é que a Engenharia de sistema da empresa tem um leque enorme na escolha dos sistemas, em termos de requisitos de falibilidade. No entanto, registramos aqui as faixas de requisitos a serem respeitadas, considerando que a perda da função **(N1) *Provide Primary Flight Information*** tem por requisito quantitativo $\lambda < 10^{-9}$ ou $F < 4.10^{-9}$ (voo médio de 4 horas)**.** Reportemo-nos à Fig. A3.1.

(1) Perda do Sistema de Informações Primárias de Voo Principal (P): $\lambda_X < 1.10^{-4}$;

(2) Perda do Sistema de Informações Primárias de Voo Principal (P): $\lambda_Y < 1.10^{-3}$; e

(3) Perda do *Standby System* (SS): $\lambda_Z < 1.10^{-2}$.

Valores por hora de voo (phv).

Na realidade, na prática esses sistemas têm, no mercado, falibilidade menor que a estabelecida aqui.

Consideremos então o Sistema

- Perda do *Display* principal: $F_{DP} < 4.10^{-4}$;
- Perda do AHRS principal: $F_{AHP} < 4.10^{-4}$.
- Perda do ADC principal: $F_{ADP} < 4.10^{-4}$.
- Perda da Cápsula Barométrica (P): $F_{CBP} < 10^{-4}$
- Perda do Tubo de Pitot principal: $F_{S1} < 4.10^{-4}$.

Passemos ao Sistema de Informações Primárias de Voo Secundário (S).

- Perda do *Display* secundário: $F_{DPS} < 4.10^{-3}$;
- Perda do AHRS secundário: $F_{AHS} < 4.10^{-3}$.
- Perda do ADC secundário: $F_{ADS} < 4.10^{-3}$.
- Perda da Cápsula Barométrica (S): $F_{CBS} < 4.10^{-4}$.
- Perda do Tubo de Pitot secundário (S): $F_{S2} < 4.10^{-4}$.

Finalmente, vamos ao *Standby Instrument System* (SS), um sistema praticamente autocontido, isto é, com seus próprios sensores inerciais, só necessitando das informações de altitude do Pitot Estático. Repetindo:

- Perda do SS: $F_{SS} < 4.10^{-2}$.

Notemos que existem duas falhas de modo comum para os três displays: a perda do Pitot Estático e da Cápsula Barométrica. No entanto, os fornecedores de Pito Estático nos dão conta de que a taxa de falha desses sistemas é da ordem de 10^{-4}, o que satisfaz o requisito quantitativo da configuração escolhida. Da mesma forma, a taxa de falha da cápsula barométrica do estado sólido pode ser da ordem de 10^{-6}.

Os *displays* devem ser desenvolvidos com DAL A, para o principal, e DAL B para o secundário ND e o terciário SS.

APÊNDICE 4

RELATÓRIO SAR-4

SYSTEM SAFETY ASSESSMENT (SSA) DO SISTEMA DE APRESENTAÇÃO DAS INFORMAÇÕES PRIMÁRIAS DE VOO

SUMÁRIO

ANEXOS

(Nota do Autor: vamos citar apenas os títulos dos Anexos. O conteúdo dos mesmos pode variar, dependendo do fornecedor).

1. Requisitos Mínimos Estabelecidos no *Request For Proposal* (RFP) Para Fornecedores*, Outputs* da *Preliminary System Safety Assessment* (PSSA).
2. *Failure Modes & Efects Summary (*FMES*)* e *Failure Modes, And Effects Analysis (*FMEA'S*).*
3. FTA Final Nível Aeronave.
4. FTA Final Nível Sistema.
5. Procedimentos de Remoção e Instalação de LRU'S.

1. INTRODUÇÃO

Este relatório refere-se à *System Safety Assessment* (SSA) do Sistema de Apresentação das Informações Primárias de voo da Aeronave S-35, compreendendo:

(a) Sistema Principal (P)

- Display PFD;
- ADC;
- Cápsula Barométrica;
- AHRS; e
- Tubo de Pitot.

(b) Sistema Secundário (S)

- Display ND;
- ADC;
- Cápsula Barométrica;
- AHRS; e
- Tubo de Pitot.

(c) *Standby System*

- Display; e
- Tubo de Pitot.

O relatório foi realizado com base nas informações provenientes do provedor de cada sistema, escolhido a partir da proposta mais adequada à solicitação (*Request For Proposal* – RFP) desta empresa, em relação à especificação geral dos sistemas da Especificação Técnica Preliminar, incluindo os requisitos de segurança (taxas de falha) que cada sistema deveria atender.

Os possíveis provedores dos sistemas considerados n*a* procura foram aqueles já consagrados no mercado, que proveem sistemas de comprovada confiabilidade, já instalados em aeronaves com certificado de tipo obtido junto a essa Autoridade.

O sistema completo escolhido foi o (nomenclatura), PN (...) do fabricante (...)[1].

O material básico desse fornecedor é a FMEA constante do Anexo 2. pertinente a todas as LRU's do sistema, comprovando o atendimento aos requisitos qualitativos e quantitativos de segurança.

[1] Aqui, poderá haver um só provedor para todas as LRU's do sistema, ou, no limite, um provedor para cada LRU.

2. ANÁLISE DAS INFORMAÇÕES DOS ANEXOS 1 E 2

2.1. Do Atendimento aos Requisitos de Segurança de Sistemas da Autoridade

O RFP sinalizou os requisitos mínimos estabelecidos como *outputs* no relatório do Anexo 1. O Fornecedor X foi o que apresentou os melhores resultados, mostrando que o sistema ofertado estava dentro dos limites estabelecidos na PSSA constantes do mencionado RFP, conforme mostrado no Anexo 2.

A tabela da Fig. 1 mostra a comparação dos requisitos de segurança quantitativos, em termos de taxa de falha, estabelecidos para o sistema, na PSSA, com aqueles apresentados pelo Fornecedor.

LRU	Taxa de Falha (phv) (Principal)		Taxa de Falha (phv) (Secundário)		Observações
	Requisito	Fornecedor	Requisito	Fornecedor	
Display PFD	1.10^{-4}	1.10^{-5}	1.10^{-3}	1.10^{-4}	
Display ND	1.10^{-4}	1.10^{-5}	1.10^{-3}	1.10^{-4}	
Standby System (SS)	---	--	1.10^{-2}	1.10^{-4}	Só será instalado um SS
AHRS	1.10^{-4}	1.10^{-4}	1.10^{-3}	1.10^{-4}	
ADC	1.10^{-4}	1.10^{-4}	1.10^{-3}	1.10^{-4}	
Tubo de Pitot	1.10^{-4}	1.10^{-4}	1.10^{-3}	1.10^{-4}	
Transdutor Barométrico	1.10^{-4}	1.10^{-5}	1.10^{-4}	1.10^{-5}	O transdutor é do estado sólido

Fig.1 – Comparação dos requisitos da PSSA com os requisitos apresentados pelo Fornecedor

As FTA's finais nível aeronave e nível sistema são apresentadas respectivamente nos Anexos 3 e 4, com probabilidades máximas de falha dadas pelos requisitos, comparadas com as probabilidades de falha deduzidas das taxas de falhas apresentadas pelo fornecedor. Pode-se constatar que o sistema atende aos requisitos da Autoridade.

3. DA ANÁLISE DE CAUSA COMUM (CCA)

3.1. Análise de Segurança Zonal (*Zonal Safety Analysis* - ZSA)

Todas as LRU's do sistema estão instaladas em espaço com temperatura adequada a todas elas, conforme a Avaliação de Projeto (*Design Appraisal*) (...) e Avaliação de Instalação (*Installation Appraisal*) (...), apresentados à Autoridade, conforme previsto no mapa de MOC (*Means of Compliance*) relativo a todos os requisitos do CFR 14 Parte 23, Subparte F.

Os resultados dos ensaios de compatibilidade eletromagnética evidenciaram que a instalação final não apresenta nenhum efeito perceptível de interferência eletromagnética (EMI) entre as LRU's, conforme relatório de ensaio (...), apresentado à Autoridade pela empresa, conforme previsto no mapa de MOC (*Means of Compliance*).

A Mantenabilidade da instalação, no que tange ao acesso às LRU's está adequada, com espaços suficientes para a remoção e instalação das LRU's. conforme relatórios de inspeção (...), apresentado à Autoridade pela empresa, previsto no mapa de MOC (*Means of Compliance*).

Outro aspecto é o ligado à manutenção, isto é, à segurança das ações de inspeção, instalação e remoção de LRU's, características consideradas no desenvolvimento do suporte técnico-logístico da aeronave, que podem ser constatadas no relatório de inspeção, apresentado à Autoridade pela empresa, previsto no mapa de MOC (*Means of Compliance*). Adicionalmente, pode ser verificado nos procedimentos constantes do Anexo 5.

3.2. Análise de Riscos Específicos (*Particular Risk Analysis - PRA*)

Os principais riscos específicos dos sistemas aviônicos são, indubitavelmente, aqueles de exposição a raios (*Lightining*) e a bombardeio eletromagnético devido a *High Intensity Radiated Fields* (HIRF), provenientes principalmente de estações emissoras no solo.

A imunidade da configuração de aviônica da aeronave S-35 a esses riscos foi verificada e considerada satisfatória, conforme os relatórios pertinentes apresentados à Autoridade, previstos no mapa de MOC (*Means of Compliance*).

3.3. Análise de Modo Comum (*Common Mode Analysis* – CMA)

Trata-se da questão de independência entre os sistemas da dupla redundância.

Cada sistema (principal e secundário) possui um PFD e um ND, ambos de fato independentes, isto é, a falha de um deles não implica necessariamente na possibilidade de falha do outro porque são projetos diferentes e, além disso, não se pode perder de vista que falhas são aleatórias e não sistemáticas.

Para melhorar mais ainda essa independência, o *Standby System* (segunda redundância) é também totalmente independente do PFD e ND, em termos de projeto, tendo, ademais, até uma configuração de alimentação elétrica diferente dos mencionados displays, já que ele está ligado à barra da bateria.

O aqui afirmado pode ser verificado no relatório de projeto (*Design Appraisal*) e no relatório de instalação (*Installation Appraisal*) previstos no mapa de MOC (*Means of Compliance*).

4. CONCLUSÃO

Em vista dos resultados apresentados no item anterior, a empresa declara que os requisitos de segurança para o Sistema de Informações Primárias de Voo, instalado na aeronave S-35, foram atendidos.

ANEXO 1

Requisitos Mínimos Estabelecidos no Request For Proposal (RFP) para Fornecedores, Outputs da Preliminary System Safety Assessment (PSSA)

ANEXO 2

Failure Modes & Effects Summary

e

Failure Modes, and Effect Analysis (FMEAS) do Fornecedor do Sistema

(Nota do autor: A FMES é um resumo sobre os resultados das FMEAs)

ANEXO 3

FTA Final Nível Aeronave

(Nota do Autor: A FTA final nível aeronave deve ser comparada com a FTA Preliminar nível aeronave, para evidenciar o atendimento dos requisitos).

ANEXO 4

FTA Final Nível Sistema

(Nota do Autor: A FTA final nível sistema deve ser comparada com a FTA Preliminar nível sistema da PSSA, para evidenciar o atendimento dos requisitos).

ANEXO 5

Procedimentos de Remoção e Instalação de LRU’S

(Nota do Autor: se possível, inserir o próprio manual com fotos da instalação)