Organização Brasileira
para o Desenvolvimento
da Certificação Aeronáutica

– Projeto de Difusão de Conhecimentos (PDC 01) –

Safety Assessment

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

Módulo II – O PROCESSO DE SAFETY ASSESSMENT– Parte 1

2ª. Edição (Revisada)

Eng. Jolan Eduardo Berquó

– Outubro 2017 –

SUMÁRIO

1. CONSIDERAÇÕES INICIAIS

Neste Módulo e no Módulo III, vamos apresentar o Processo de *Safety Assessment*[1], voltado para as aeronaves que cumprem os requisitos da FAA *CFR 14 Part 23*, *Section 23.1309*[2] e *CFR 14 Part 25, Section 25.1309*, adotados também pela nossa Agência Nacional de Aviação Civil (ANAC).

Este trabalho está baseado na metodologia inserida na AC[3] 23.1309 -1E – *System Safety Analysis and Assessment for Part 23 Airplanes*, da FAA (Ref. 5), que sugere[4] um método para a realização da *Safety Assessment.* A AC 25.1309-1A também está incluída, mas a AC 23.1309-1E, em nossa opinião, é mais rica e didática em suas orientações. Qualquer diferença significativa proporcionada pela metodologia da AC 25.1309-1A, se detectada, será comentada.

"Baseado" aqui significa que há, neste contexto, nosso toque interpretativo, fruto de estudos, discussões e experiências. Contudo, fique bem entendido: não faremos contrapontos com as AC; apenas colocaremos nossa interpretação.

Como sabemos, o objetivo do processo de *Safety Assessment* é demonstrar à Autoridade que os requisitos de segurança estão incorporados nos sistemas dessas aeronaves, por meio de um relatório denominado *System Safety Analysis* (SSA), apresentando os resultados do processo.

Seguido à risca, o processo é também uma valiosa metodologia de alocação (inserção) de requisitos de segurança no projeto de novos sistemas ou na escolha de sistemas já existentes no mercado (*off-the-shelf*), com ou sem um histórico de serviço conhecido.

Como coadjuvantes, incluímos alguns aspectos tratados pelos documentos SAE ARP 4754A e 4761[5], particularmente no tocante ao emprego de ferramentas *(FTA, DD, FMEA, etc.*)[6] utilizadas em *Safety Assessment* e contidas na ARP 4761 (Ref. 8) .

***Nota**: Neste ponto, recomenda-se que os especialistas de Safety Assessment do Aplicante tenham à disposição as AC 23.1309-1E/25.1309-1A e os documentos coadjuvantes SAE ARP 4754A e SAE ARP 4761, mais especificamente a ARP 4761.*

[1] Em geral, daremos preferência aos termos em inglês usados em *Safety Assessment*, por serem mais usuais entre os especialistas.
[2] O processo, com pequenas alterações, pode ser aplicado às aeronaves das Partes 25, 27 e 29.
[3] AC: *Advisory Circular.*
[4] "Sugere" significa ser apenas uma orientação, isto é, não se trata de requisito, mas de uma ajuda. O Aplicante pode usar o método que melhor lhe aprouver, desde que atinja o mesmo objetivo preconizado nas AC 23.1309-1E/25.1309-1A.
[5] Documentos considerados aceitáveis pela FAA.
[6] FTA: *Fault Tree Assessment*; DD: *Dependence Diagrams*; FMEA: *Failure Modes, and Effects Analysis*.

Em princípio, o trabalho focalizará, sem ressalvas, os sistemas elétricos e eletrônicos, em especial os sistemas aviônicos. Os sistemas eletromecânicos, mecânicos, pneumáticos, e hidráulicos[7] também estão incluídos na AC e nos documentos coadjuvantes, mas sua inclusão deve considerar as ressalvas inseridas no **Apêndice A** do Módulo I.

Como dissemos no Módulo I (item 3.1), existe uma polêmica quanto ao que seja um sistema aviônico. Há quem diga que um sistema aviônico seja aquele que só tem equipamentos e componentes eletrônicos (ex.: ADF, VOR, Transponder - TDR, etc.). Contudo, neste trabalho estamos seguindo a nova corrente de autores de obras de eletrônica da aviação civil, considerando como sistema aviônico, já registrado no Módulo I, qualquer sistema que dependa de equipamentos eletrônicos, tenham esses sistemas partes mecânicas ou não. Um exemplo é o sistema *Fly-By-Wire* (Fig. 1), que contém componentes mecânicos e eletromecânicos, mas que depende de um computador de controle de voo (*Flight Control Computer* – FCC) e unidades eletrônicas de controle de atuadores.

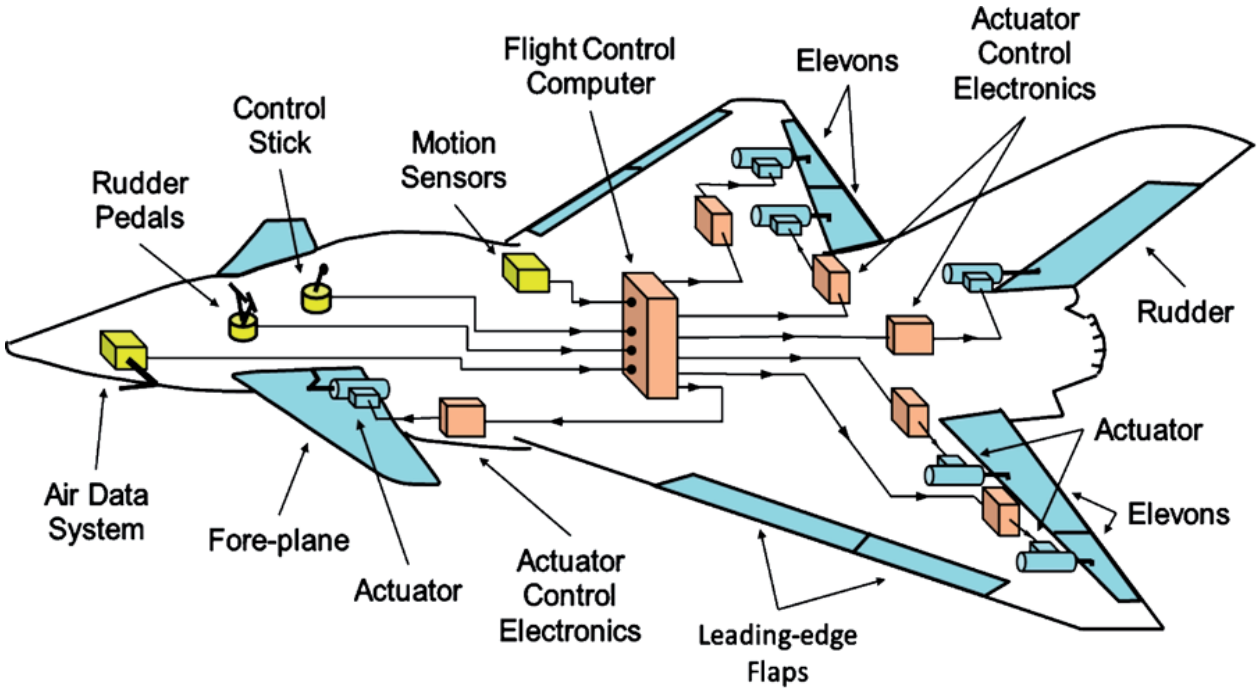


Fig. 1 – *Fly-By-Wire System* (Ref. 4)

[7] Há fabricantes que consideram os sistemas hidráulicos e pneumáticos como sendo mecânicos. Não vemos inconvenientes nisso; portanto, fica a critério da empresa.

Outro exemplo, também mencionado no Módulo I, é o sistema que executa a função de frenagem de uma aeronave, na movimentação no solo, no pré ou pós-voo. O documento SAE ARP 4761 (Ref. 8) descreve esse sistema, para exemplificar o processo de *Safety Assessment* completo de um sistema. Há muitos componentes (itens) mecânicos no sistema ali apresentado; mas, seu principal componente, seu cerne, é um computador, denominado *Braking System Control Unit* (BSCU).

Neste nosso trabalho, quando o sistema aviônico for híbrido, procuraremos deixar isso claro.

Como já mencionado no Módulo I, quando utilizarmos o termo “requisito”, neste Módulo e no Módulo III, sem especificar a que se refere o requisito, deve ficar subentendido que se trata de “requisito de segurança (*safety*)”.

2. ESPECIFICIDADES DO PROCESSO DE *SAFETY ASSE*SSMENT

Vamos, neste ponto, dar uma visão panorâmica, ou seja, um leque, sobre o que você verá neste Módulo.

Quando conseguimos sistematizar algum estudo, isso parece tornar mais leve nosso aprendizado.

Vamos tentar aqui fazer exatamente isso. A palavra “tentar” é bem adequada, querendo dizer que “pode ser que sim, mas pode ser que não”; até que ponto, só você, leitor, é que poderá dizer.

Procuramos, tanto quanto possível, usar os ensinamentos da boa escrita, quais sejam: Precisão (dizer o que tem de ser dito e só o que tem de ser dito); concisão (dizer o que tem de ser dito com o mínimo possível de palavras) e correção (usar palavras e frases, conforme a gramática da língua em que se está escrevendo). Dureza!

Pois bem, de um modo geral o que você vai ver neste Módulo já foi dito: o Processo de *Safety Assessment*.

A primeira coisa a fazer é entender o que a aeronave deve fazer, para transportar passageiros ou carga de um ponto a outro. Isso significa saber quais são as funções que a aeronave, por meio de seus sistemas, deve realizar, para atingir o intento desse transporte.

No entanto, como nós estamos preocupados com o voo e pouso seguros da aeronave, teremos de tratar de tudo que se enquadre nesse significado de segurança, que, daqui por diante, será resumido no termo inglês *Safety.*

Começaremos analisando as falhas no nível aeronave; depois, vamos ao nível de sistemas e, finalmente no nível de equipamento, procurando verificar se os sistemas integrados por esses equipamentos atendem aos requisitos de segurança. Ao final, temos de mostrar à Autoridade que todos os sistemas da aeronave estão enquadrados nos limites de *safety* traduzidos pelos requisitos dessa área, e que, portanto, a aeronave, em si, está nos limites aceitáveis da segurança. Simples assim, não? Pois é; não obstante, a jornada para realizar isso é longa; mas, é exatamente o que tentaremos mostrar aqui.

Queremos chamar a atenção, de pronto, para o fato de que, entre os sistemas existentes na aeronave, existe uma classe especial constituída pelos chamados sistemas aviônicos. Eles serão bem analisados (esperamos) e discutidos neste Módulo, em virtude da especificidade inerente aos mesmos.

Normalmente, analisamos os sistemas aviônicos, de um modo geral, sob o ponto de vista de *safety*, por meio de análises qualitativas, baseadas no conhecimento experiente da engenharia, e/ou, quantitativamente, por meio de alocação dos chamados requisitos numéricos de probabilidade de falha ou de mau funcionamento, comprovados por meio de análises quantitativas.

Entretanto, e é aqui que mora a peculiaridade dos sistemas aviônicos, quando se trata dos chamados sistemas aviônicos complexos (e isto será esmiuçado mais à frente), o processo pode prescindir dessas análises, simplesmente porque quase sempre não é possível realizá-las a contento, para demonstrar que o sistema cumpre os requisitos de *safety* que lhe são atribuídos. Então, alguma alternativa tem de ser utilizada. Mostraremos essa alternativa mais adiante (v. 5.4.1). Por enquanto, guarde isso: **sistemas aviônicos complexos.**

3. FUNDAMENTOS DO PROCESSO *DE SAFETY ASSESSMENT*[8]

Como acontece em qualquer estudo, a primeira coisa a fazer é apresentar os fundamentos, isto é, os conceitos que irão suportar o desenvolvimento do processo de *Safety Assessment.*

São eles:

- Função e Análise Funcional;
- *Failure Conditions* (Condições de Falha) das funções;
- Severidade de uma *Failure Condition*; e
- Requisitos qualitativos e quantitativos associados a cada *failure condition*.

3.1. Função e Análise Funcional

Como dissemos no Módulo I, uma função refere-se a uma ação realizada por um ser humano ou por um sistema, visando obter um resultado preestabelecido.

Outro conceito (Ref. 1 e 2): Função é uma tarefa, ação ou atividade realizada para obter um determinado objetivo (sem mencionar por quem ou pelo quê).

Num e noutro conceito, o resultado esperado define a função. Por ser uma ação, a função é enunciada por um verbo e, logicamente, no infinitivo impessoal, por exemplo: prover, anunciar, comparar, realizar, gerar. Todavia, tem sido de uso comum utilizar também expressões substantivas, tais como: provimento, anunciação, comparação, realização, geração, etc.

Para facilitar nosso raciocínio, vamos considerar que, rigorosamente, uma aeronave, em si, é um sistema[9]. Parece-nos óbvio que todo sistema tem de se movimentar para produzir algo (uma estátua não é um sistema, mas um produto de contemplação e, talvez, de "meditação"). O melhor exemplo dessa característica de movimento é o sistema denominado Ser Humano.

[8] Estaremos usando neste trabalho os termos ingleses pertinentes à atividade de *Safety Assessment,* por ser o mais usual entre os especialistas.

[9] Já tratamos desse conceito, de maneira especial, no item 1.2 do Módulo I. No nosso caso, a aeronave será considerada produto, sendo constituído por sistemas.

O movimento, enfim, é fundamental para prover resultados úteis. É essencial para um sistema produzir algo, mesmo que esse movimento não nos seja visível, como no caso dos sistemas eletrônicos, identificados apenas pelos seus resultados (*outputs*).

A aeronave, como qualquer sistema, não foge à regra, ou seja, tem de se movimentar, no solo e no ar, para realizar sua "missão"[10].

Identificam-se as seguintes fases de movimento global de uma aeronave: **Movimentação no Solo, Pré e Pós-voo, e Movimentação no Ar (voo).**

Muito bem, mas a pergunta agora é: Como as empresas identificam as funções que servirão de base para o desenvolvimento de suas aeronaves e, por tabela, também para o processo de *Safety Assessment*?

Para responder a essa pergunta, vamos tratar previamente de uma das metodologias que podem ser empregadas pelas empresas, para dispararem seus projetos de uma nova aeronave, seguindo o modelo da Engenharia de Sistemas (ES)[11].

Primeiro, ela faz uma pesquisa de mercado[12], para saber que tipo de aeronave certo segmento desse mercado pesquisado está desejando[13]. Em nosso caso, trata-se de obter os chamados requisitos médios de mercado de aeronáutica civil para o projeto de uma nova aeronave. Esses requisitos são denominados de "A voz do cliente" (*The Customer Voice*), porque são "desejos", amiúde não expressos numa linguagem técnica de engenharia.

De posse desses requisitos, a empresa vai para "A Voz da Engenharia", fazendo o translado dos requisitos médios de mercado para os requisitos formatados na linguagem de engenharia; tudo isso acontecendo na chamada Fase (Projeto) Conceitual, primeira do ciclo de vida da aeronave.

[10] "Missão"é um termo mais usado na aviação militar, onde uma aeronave pode ter várias missões. Entretanto, não vemos nada de errado usar o termo para a aviação civil, considerando, no entanto, que a aeronave civil só realiza um tipo de missão: transporte (de pessoas e cargas).
[11] As iniciais ES, designando Engenharia de Sistemas, serão utilizadas, ao longo de todo este trabalho.
[12] "Mercado" significa um conjunto de empresas operadoras de aeronaves civis.
[13] Há vários métodos para fazer isso. Um atual e que tem tido sucesso é o QFD (*Quality Function Deployment*).

Daí, a empresa dispara o primeiro passo, ou seja, realiza a indispensável Análise Funcional, um dos *outputs* da Fase Conceitual, com o objetivo de definir as funções da nova aeronave e de seus sistemas, que servirão de base para estabelecer a arquitetura final da aeronave, segundo o desejo médio do mercado.

Essa análise pode constituir-se num enorme esforço, por parte da empresa, quando se trata de um projeto muito diferente de projetos anteriores. Entretanto, a imensa maioria dos projetos de novas aeronaves, na área civil, é derivada de projetos anteriores, o que simplifica sobremaneira a tarefa da ES. Desse modo, com algumas variações, em geral se lida com as mesmas funções de projetos anteriores[14]. Um exemplo que contrariou essa habitualidade foi, por exemplo, o projeto da aeronave Concorde, desenvolvido nos anos 60, com um elenco de muitas funções novas, levando a ES a empregar uma razoável quantidade de homens-horas, em sua Análise Funcional.

A Análise Funcional é básica para a ES, mas é, e muito, também básica para o processo de *Safety Assessment*, que se desenvolve a partir das funções aeronave, para realizar sua primeira avaliação de segurança, a denominada *Functional Hazard Assessment - Aircraft Level* (AFHA), exigida pela Autoridade, para dar início à certificação.

Nosso interesse está nas funções relativas à operação da aeronave, que caracterizam o movimento da aeronave, conforme mostrada na Fig. 2 (Ref. 1).

[14] Lembramos que estamos tratando de projetos de aeronaves de transporte civil, cuja "missão" é sempre a mesma: transportar passageiros e/ou carga. Quando se trata de aeronaves militares, há diferentes funções, de projeto para projeto, dependendo das missões que a aeronave vai realizar.

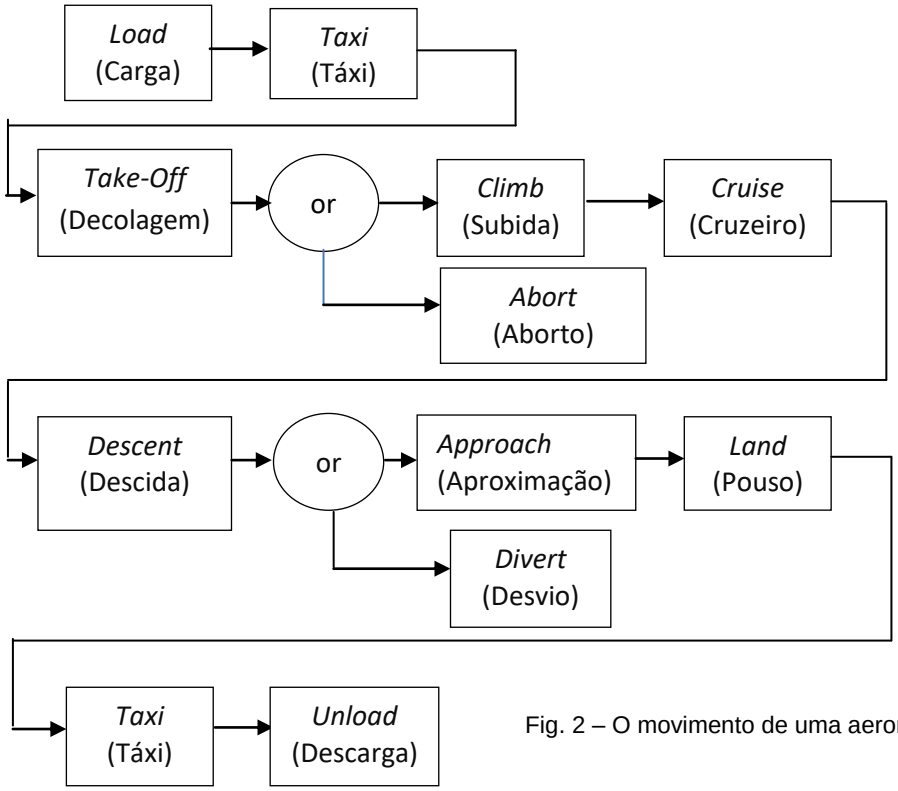


Fig. 2 – O movimento de uma aeronave

3.1.1. Identificação e Hierarquia das Funções

Vamos então identificar as funções da aeronave, "navegando" na Análise Funcional da ES da empresa. Primeiramente, devemos estabelecer critérios de hierarquia para os extensos grupos de funções que serão apresentados.

As funções são classificadas em níveis. No nível mais alto, elas são classificadas 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. É importante ter esse critério em mente, para não nos confundirmos. Desse modo, se, por exemplo, alguém nos disser que uma determinada função é de nível 2, sabemos, de imediato, que ela está ligada a um função superior de nível 1, e esta a uma função básica. Parece-nos simples e didático.

Pois bem, no caso de uma aeronave civil, as funções básicas ligadas à operação da aeronave são as seguintes:

- **(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).*

Observe que a ausência de qualquer função básica abortaria o ciclo completo de operação da aeronave. Contudo, vamos por etapas. Uma falha no grupo de funções **(B1)**, já "de cara" abortaria esse ciclo; mas, a análise, sob o ponto de vista da segurança, nos diz que as possíveis falhas que pudessem provocar esse aborto não implicariam em maiores preocupações com a segurança; a aeronave, mui provavelmente, permaneceria intacta e inerte no solo. Para demonstrar esse raciocínio, vamos considerar as funções **(N1)** do Grupo Básico **(B1):**

- Prover Propulsão (*Propulsion*);
- Prover Deslocamento (*Carriage*);
- Prover Frenagem (*Braking*) ou Desaceleração (*Deceleration*);
- Prover Direção (*Steering*); e
- Prover Comunicação (*Communication*).

Por outro lado, as outras duas funções básicas são realmente preocupantes, em termos de safety. É nelas, sim, que devemos nos concentrar (colocar mais energia). A preocupação já começa no início da Função **(B2),** exatamente na decolagem (*take-off*). Depois, já em voo, como teremos oportunidade de mostrar, há muitas funções ativas, e a perda ou mau funcionamento de várias pode levar a catástrofes.

Mas voltemos ao *take-off*. Se, na corrida para a decolagem, ocorrer uma repentina e não avisada (não anunciada) desaceleração depois de V1[15], o piloto, com considerável probabilidade, não conseguirá decolar, devido à aplicação da repentina frenagem, podendo então, com razoável probabilidade, ultrapassar o final da pista, indo, provavelmente, chocar-se com obstáculos sólidos, podendo aí até mesmo surgir uma catástrofe.

A função **(B2)** também possui várias funções **(N1)**. São elas:

- Gerar Forças Aerodinâmicas (*Aerodynamic Forces*)

[15] V1 – Velocidade máxima para a ação do piloto de rejeitar a decolagem (*Reject Take-OFF* – RTO).

- Prover Impulso Total (*Total Impulse*);
- Prover Guiagem[16] e Navegação (*Guidance* e *Navigation*);
- Prover Comunicação (*Communication*);
- Prover Potência (*Power*);
- Prover Controle Ambiental (*Environmental Control*);
- Gerenciar o Combustível (*Fuel*);
- Sensoriar Objetos Remotos (*Remote Objects*); e
- Comandar e Controlar a Aeronave (*Command* e *Control*);

As três últimas são atribuídas diretamente ao piloto.

A função **(N1) Gerar Forças Aerodinâmicas** possui ainda funções nível **(N2)**, quais sejam:

- Prover Desempenho em Ascenção (*Lift)*;
- Prover Desempenho em Arrasto (*Drag)*;
- Prover Estabilidade Aerodinâmica (*Aerodynamic Stability*); e
- Prover Controle Aerodinâmico (*Aerodynamic Control*).

A função **(N1) Prover Guiagem e Navegação**, extremamente importante para o controle da aeronave, por parte do piloto, admite as seguintes funções **(N2)**:

-
- Prover a posição da aeronave (*Location: location: altitude, longitude and latitude*);
- Prover a Atitude da Aeronave (*Attitude*);
- Prover a Velocidade da Aeronave *(Speed);*
- Prover a Direção da Aeronave (*Heading*); e
- Prover o Gerenciamento de Voo (*Flight Management*).

[16] Ato ou efeito de guiar projétil, míssil e nave (Dicionário Houaiss da Língua Portuguesa. 1ª. Ed. - 2009)

Com exceção da função relativa à posição e a função relativa ao Gerenciamento de voo, as demais (atitude, velocidade da aeronave e direção da aeronave), juntamente com a altitude, formam um conjunto funcional denominado “Primary Flight Information”[17]. Diz-se então: “Prover Primary Flight Information”.

A posição da aeronave inclui as seguintes informações ou parâmetros: Altitude, Latitude e Longitude, em relação a pontos no solo.

A Atitude é dada por variações angulares em *pitch* (arfagem), *roll* (rolagem) e *Yaw* (derrapagem ou guinada). A velocidade e a direção podem ser em relação ao ar ou em relação ao solo.

A função **(N1) Comandar e Controlar a Aeronave** provê comando tanto para o piloto quanto para o piloto automático, e deste para o piloto.

A função **(N1) Prover Comunicação** apresenta duas funções **(N2)**:

- Prover Comunicação Interna; e
- Prover Comunicação Externa.

A função **Prover Comunicação Interna** refere-se à troca de informações entre os membros da tripulação e às informações passadas aos passageiros.

Quanto à função **Prover Comunicação Externa** trata-se da comunicação do piloto com o controle de tráfego aéreo (Torre de Controle, por exemplo), com outras aeronaves em voo e com estações no solo.

Logicamente, a função **(N1) Prover Potência** é extremamente importante porque os sistemas aviônicos, elétricos, pneumáticos e hidráulicos dependem dessa função. Ela reúne quatro funções (**N2):**

- Prover Potência AC (*Alternating Current*);
- Prover Potência DC (*Direct Current*);
- Prover Potência Alternativa (*Backup)*; e
- Prover Distribuição de Cargas (*Load Distribution*).

[17] V. AC 23.1311-1C (Ref. 6).

Dada a importância da função **(N1) Prover Potência**, no aspecto ligado a safety, vamos tecer algumas considerações sobre essas quatro funções **(N2)**.

A maneira mais usual de se obter potência elétrica AC e DC é por meio de um gerador elétrico alimentado pelo torque mecânico de cada motor. O gerador produz corrente alternada (AC), que pode ser convertida em DC, para os equipamentos que dependem desse tipo de energia (a grande maioria). A potência DC é também usada para recarregar baterias, utilizadas para prover potência alternativa (*backup).* Além disso, a potência DC das baterias pode ser convertida em potência AC, por meio de equipamentos denominados Inversores, que são necessários durante a operação em emergência.

A distribuição de carga é obtida pela análise, durante a fase de síntese da ES. O objetivo dessa distribuição é assegurar o balanceamento das cargas elétricas, de modo que nenhum equipamento do sistema elétrico seja sobrecarregado, quando algum equipamento falhar.

Bem, na verdade poderíamos nos alongar muito mais com as funções do grupo **(B2)**, mas acreditamos que já seja o suficiente para se perceber a importância de uma Análise Funcional. Todas essas funções são consideradas numa FHA nível aeronave do processo de *Safety Assessment*.

Falemos agora sobre a função **(B3) Realizar Movimento no Solo, Pós-Voo,** Essa função tem as mesmas funções **(N1)** da função **(B1) Realizar Movimento no Solo, Pré-Voo**; no entanto, os sistemas que executam a função **(N1)** de frenagem ou desaceleração incluem recursos que, embora disponíveis nas funções **(N1) de B1** e **B3**, normalmente não são utilizados frequentemente na frenagem pré-voo, mas sim na frenagem pós-voo, como por exemplo o reverso. Parece-nos fácil ver que a perda da frenagem pós-voo pode levar a um acidente catastrófico, como temos visto acontecer. São, pois, detalhes para os quais o analista de *Safety Assessment* precisa estar atento, ou seja, ele vai ter que considerar, em termos de *safety*, o provimento dessas funções, levando em conta a diferença de utilização de recursos, numa e noutra fase (pré e pós-voo).

Como todo sistema, a aeronave necessita de outra função, com essa característica de movimento, para manter-se disponível (*available*), mas uma função de outro sistema externo à aeronave, porém agindo diretamente nela. Trata-se da função básica **B4**: **Prover Suporte Técnico Logístico**, com suas funções (N1):

- Prover Manutenção (*Maintenance*);

- Prover Manuais de Manutenção (*Technical Publications*)
- Prover Treinamento de Mecânicos (*Training*);
- Prover Equipamentos de Apoio no Solo (*Ground Spport Equipment)*; e
- Prover Suprimento de Peças de Reposição (*Spare Parts*).

A função **B4** é de importância equivalente à de movimento da aeronave, em termos de *safety*. Todavia, não vamos tratá-la aqui de maneira exaustiva. Ficará para outra oportunidade.

Achamos que já dá para perceber que a atividade de Análise Funcional é lógica e seu desenvolvimento é fascinante.

3.1.2. Modos de Falhas Funcionais (*Functional Failures Modes*)

Pedimos, mais uma vez, especial atenção, porque vamos tratar de um assunto controverso (aliás, mais um). Trata-se de discursar sobre a maneira como a falha funcional se apresenta. Vejamos.

- Perda total de função (anunciada ou não anunciada), como por exemplo o movimento do trem de pouso, na preparação para o pouso;
- Perda parcial de função (anunciada e não anunciada), tal como baixa pressão hidráulica ou perda parcial da alimentação elétrica;
- Função intempestiva, isto é, provida quando não requerida (anunciada e não anunciada), tal como uma ejeção não comandada de assento ejetável (caso militar) ou uma ação de controle de voo não comandada pelo piloto[18]; e
- Função com informações incorretas (anunciadas e não anunciadas), tais como uma informação de *altitude* ou *heading* incorretos no display.

Esses são os modos de falhas funcionais. Vamos, agora, associar-lhes as condições externas (VMC ou IMC)[19]. Entraremos em mais detalhes, quando tratando especificamente da FHA nível aeronave (AFHA).

[18] Um exemplo de ação de controle de voo não comandada pelo piloto é o acidente de uma aeronave Tornado, na Alemanha (anos 80), que foi "atacada" por ondas eletromagnéticas (EMI) oriundas de transmissores de broadcasting existentes no solo, que induziram pulsos elétricos no cabo de entrada do computador de controle de voo (FCC), promovendo, na saída, um não intencional comando de superfícies de controle de voo, levando a aeronave a precipitar-se.

Por exemplo, consideremos a perda da função “Prover a Altitude da Aeronave” (*Provide the Aircraft Altitude*). Se houver uma perda anunciada ou não anunciada ao piloto, voando condições IMC, em todas as fases do voo, o piloto poderá perder o controle da aeronave, conduzindo-a a um acidente fatal.

Se, no entanto, as condições forem VMC, o piloto ainda terá condições de controlar a aeronave, até o pouso em algum aeródromo.

3.1.3. *Failure Conditions,* Severidades e Requisitos

Vamos agora ao conceito central de uma *Safety Assessment*: *Failure Condition*. Uma *Failure Condition* é a expressão de uma falha funcional, em termos de potencial efeito na tríade: tripulação, aeronave e ocupantes (passageiros). A gravidade desse efeito é identificada pela severidade, numa escala de efeito mais grave (severo) para menos grave, ou seja:

- *Catastrophic* (Catastrofico);
- *Hazardous* (Perigosa);
- *Major* (Maior)
- *Minor* (Menor); e
- *No Safety Effect* (Nenhum efeito na segurança).

É importante entender que para associar à *failure condition* uma determinada severidade, é necessário fazer antes uma pergunta com o seguinte teor: *Qual é o potencial efeito da falha (perda da função ou mau funcionamento) sobre a tríade: tripulação, aeronave e ocupantes, fase por fase da operação, em condições IMC e VMC, considerando a falha anunciada ou não anunciada para o piloto*? Por exemplo: Perda da informação de atitude, em condições IMC, anunciada ou não anunciada. Quais os efeitos na tríade?

- **Fases da Operação <u>em Voo</u>**: todas;
- **Condições meteorológicas**: IMC;

[19] VMC: Visual Meteorological Conditions (Condições Meteorológicas Visuais) e IMC: Instrument Meteorological Conditions (Condições Meteorológicas por Instrumento). Por outro lado, VFR e IFR são regras para operar nas condições VMC e IMC, respectivamente.

- **Falha anunciada ou não anunciada**;

Efeitos na tríade:

- **Tripulação**: poderia exceder os limites da aeronave e perder o controle da mesma;
- **Aeronave**: possível perda;
- **Ocupantes**: possíveis ferimentos fatais ou incapacitação.

Severidade? *Catastrophic*.

Resumindo: Primeiro procura-se identificar o modo de falha funcional, com base nas possibilidades apresentadas em 3.1.2. Em seguida, verificar o potencial efeito da falha (*Failure Condition*) na tríade, em todas as fases da operação, nas condições VMC e IMC, considerando a falha anunciada ou não anunciada, para então identificar a severidade da *Failure Condition*. Esta é a regra.

Atenção! Para o desenvolvimento da SFHA, devemos considerar a pior severidade atribuída à *failure condition* nível aeronave. No exemplo acima, se a condição meteorológica fosse VMC, a condição de falha certamente não seria *Catastrophic.* Poderia ser, no máximo, de severidade *Hazardous* (a discutir). Contudo, a escolha da severidade dessa falha é a do pior caso, ou seja, *Catastrophic*.

Às vezes, a perda da função é menos grave que um mau funcionamento. Por exemplo, a perda anunciada do sistema *Ground Proximity Warning System - GPWS (*Sistema de Alerta de Proximidade de Terreno) é considerada de severidade Minor. Por outro lado, se a falha for um mau funcionamento do computador do sistema, resultando em alertas falsos, ou perda não anunciada da função, ou informação enganosa[20] (*misleading*), a *Failure Condition* pode ser considerada *Major*[21].

Convenhamos que é fácil perceber que a identificação da severidade de uma *Failure Condition* tem que ter a participação de pelo menos dois especialistas: piloto e engenheiro da área, ambos experientes.

[20] A severidade de um *misleading* depende do sistema, das condições meteorológicas, podendo ser a pior falha. A informação é enganosa, isto é, parece verdadeira, mas não é, podendo o piloto adotar atitudes fora dos limites permitidos.
[21] V. TSO-C151c: *Terrain Awareness and Warning System* (TAWS).

3.1.4. Requisitos Qualitativos e Quantitativos Associados a *Cada Failure Condition*

Conforme AC 23.1309-1E, *Figure 2 – Page 23*, a cada severidade se associa um requisito qualitativo e um quantitativo. Os requisitos quantitativos são expressos por faixas de probabilidades de falha por hora de voo, como mostra a Tabela 1, a seguir, que se refere às aeronaves da Classe IV *(Commuter*), a mais restritiva da Parte 23. Inserimos também a tabela 2, pertinente às aeronaves da parte 25.

Essa classificação é tratada também no item 15 da AC 23.1309-1E (*Four Certification Classes of Airplanes*). A figura 2 da página 23 dessa AC apresenta essas quatro classes, associadas às respectivas *Failure Conditions* e suas respectivas severidades, bem como os pertinentes requisitos qualitativos e quantitativos. É importante para o Aplicante entender bem o conteúdo daquela figura.

Tabela 1 – *Failure Conditions and Requirements*
*(*AC 23.1309-1E Aeronaves da Classe IV – *Commuter)*

Failure Condition Severity	*Requirements*	
	Qualitative	*Quantitative/hv*[22]
Catastrophic	*Extremely improbable*	$F<10^{-9}$
Hazardous	*Extremely Remote*	$F<10^{-7}$
Major	*Remote*	$F<10^{-5}$
Minor	*Probable*	$F<10^{-3}$
No Safety Effect[23]	*None*	None

A AC 23.1309-1A apresenta uma classificação diferente, conforme mostra a Tabela 2.

Tabela 2 – *Failure Conditions and Requirements*

(AC 25.1309-1A)

Failure Condition Severity	*Requirements*	
	Qualitative	*Quantitative/hv*
Catastrophic	*Extremely improbable*	$F<10^{-9}$
Major	*Improbable*	$10^{-5}>F>10^{-9}$
Minor	*Probable*	$F>10^{-5}$

[22] Hv: hora de voo.
[23] *No Safety Effect* poderia ser chamada de "ausência de severidade"

Como se vê, a Tabela 2, relativa às aeronaves da Parte 25, não especifica a *Failure Condition Hazardous*. Contudo, a AC 25.1309-1A, em seu item 6(h)(2), da página 6, estabelece dois níveis para a severidade *Major*: uma *Major* mais branda (equivalente àquela de mesmo nome da AC 23.1309-1E) e uma *Major* mais grave (*Severe Major*), que equivale à severidade *Hazardous* da AC 23.1301-1E.

Voltando à Tabela 1, para a *Failure Condition* de severidade *No Safety Effect* (que não é mencionada na AC 25.1309-1A), não se associa nenhum requisito quantitativo, por não haver nenhum potencial efeito na segurança da aeronave, ao longo de seu perfil de voo, sendo apenas um problema para a manutenção. No entanto, há que se tomar mínimos cuidados com essa "severidade", conforme mostraremos no item 5.5.2.

Como vimos no **Apêndice B** do Módulo I, os requisitos quantitativos são frutos de um extenso estudo estatístico, na década de 1970, com dados de acidentes coletados em países ocidentais, tomando como base o histórico de acidentes atribuíveis a sistemas[24].

Esses requisitos quantitativos, expressos por faixas de probabilidade de falha por hora de voo (taxa de falha), são utilizados, em *Safety Assessment*, nos casos em que o impacto de uma falha de sistema tiver que ser examinado por métodos quantitativos, como será discutido mais adiante.

Notem que, na mencionada figura 2 da AC 23.1309-1E, os requisitos mais restritivos são atribuídos à quarta classe, denominada *Commuter*, que comporta transporte de passageiros, razão pela qual são os mesmos das aeronaves da Parte 25, no que concerne às severidades *Catastrophic* e *Major* dessa Parte.

4. CONSIDERAÇÕES IMPORTANTES SOBRE OS SISTEMAS PARA O PROCESSO DE SAFETY ASSESSMENT

Os sistemas puramente eletrônicos ou elétricos não utilizam peças móveis. As taxas de falha (λ) desses sistemas são muito baixas e razoavelmente constantes, ao longo da fase operacional (que se inicia com a instalação do sistema na aeronave), dando, portanto, uma razoável previsibilidade temporal de funcionamento desses sistemas.

A filosofia de manutenção de um equipamento eletrônico é *On Condition*, ou seja, eles só são retirados da aeronave, para manutenção, se sofrerem falhas (perda da função) ou

[24] Só dez por cento do total de acidentes catastróficos.

mau funcionamento que os estejam impedindo de realizar a respectiva função. Quando isso ocorre, numa logística bem estruturada, o equipamento falhado (em pane)[25] é imediatamente substituído e submetido a reparos, ou, no limite, é descartado (situação rara).

A não ser em casos especiais[26], não se estabelece manutenção preventiva para equipamentos eletrônicos porque não há como fazê-lo. Se o equipamento, na última vez que foi desligado, estava funcionando bem, não há razão para suspeitar que, na próxima vez que for ligado, poderá não funcionar bem[27]. Além do mais, equipamento eletrônico de um sistema aviônico que execute uma função nível aeronave com *Failure Condition catastrophic* ou *hazardous*, certamente fará parte do *check-in* realizado pela tripulação, antes da próxima decolagem. Até onde sabemos, é o máximo que se pode fazer com esses equipamentos.

Mas os sistemas mecânicos e a parte mecânica dos sistemas aviônicos híbridos em geral têm manutenção preventiva. Como vimos no Apêndice A do Módulo I, os equipamentos ou componentes mecânicos não apresentam, na fase operacional, taxas de falha "mais ou menos constantes", como no caso da parte eletrônica; pelo contrário, a taxa de falha deles é sempre variável; decresce no início, como nos eletrônicos, passa por um mínimo e depois cresce e, às vezes, até vertiginosamente[28], ou seja, a taxa de falha é função do tempo ($\lambda = \lambda(t)$), durante toda a fase operacional. Por isso, em geral, não são, obviamente, *On Condition*, requerendo, quase sempre, a imposição de filosofia de manutenção preventiva.

Um tipo de manutenção preventiva para esses equipamentos, quando possível, como no caso do motor de uma aeronave, seria a manutenção dita preditiva, que, numa inspeção com equipamentos de teste adequados, analisa o estado do equipamento, permitindo decidir, segundo regras criteriosamente estabelecidas, se o mesmo poderá ou não continuar em operação, com alguma previsão de tempo de continuidade operacional,

[25] Do francês *Panne* e do inglês *fault*. Vide a norma ABNT 5462 – Confiabilidade e Mantenabilidade.

[26] Rarissimamente sucede que uma peça de um equipamento eletrônico esteja prematuramente falhando e com uma taxa de falha bem maior que a prevista (conhecemos vários casos práticos). Em virtude disso, a manutenção estabelece um tempo máximo de operação para aquela peça, removendo-a antes de completar o período em que a falha pode ocorrer. Esse procedimento é mantido até que o fabricante do equipamento emita um boletim técnico e de serviço, recomendando a instalação de um novo componente no equipamento (outro PN).

[27] V. item A1 do Apêndice A do Módulo I.

[28] Tivemos a oportunidade de constatar isso, quando nos dedicamos, por quase uma década, à manutenção de sistemas elétricos/eletrônicos e acompanhamos de perto a manutenção de sistemas mecânicos, eletromecânicos, hidráulicos e pneumáticos, tudo isso no Parque de Material Aeronáutico de São Paulo.

Outra característica importante dos equipamentos eletrônicos está no tratamento matemático probabilístico aplicado aos mesmos. Como vimos no **Apêndice B** do Módulo I, em termos de probabilidade de falhar, a Falibilidade (*Fallibility* ou *Unreliability*) é dada por:

$$\mathbf{F = \lambda t},^{29} \qquad \text{onde } \lambda = \text{constante.} \qquad (1)$$

Trata-se de uma expressão fundamental para o processo de Safety Assessment, que decorre da função de distribuição cumulativa de probabilidades complementar da função de distribuição exponencial negativa, qual seja:

$$\mathbf{F = 1 - e^{-\lambda t}}, \qquad \text{que para } \lambda t < 0{,}1, \text{ resulta na expressão (1).}$$

Como foi dito no **Apêndice B** do Módulo I, essa expressão rigorosamente não é adequada para sistemas mecânicos; contudo, ela tem sido utilizada para os sistemas aviônicos, tanto na parte eletrônica como na parte mecânica ou eletromecânica, de preferência com os cuidados mencionados no **Apêndice A** do Módulo I, em relação a equipamentos mecânicos. Na verdade, para esses equipamentos, uma função rigorosamente mais adequada seria, por exemplo, a função de Weibull (V. *Appendix* 3 da Ref. 5).

5. O PROCESSO DE *SAFETY ASSESSMENT* (Item 16 da AC 23.1309-1E)

5.1. Etapas e Ferramentas do Processo de *Safety Assessment*

O processo completo de Safety Assessment pode se estender ao longo de quatro avaliações: *Functional Hazard Assessment Nível Aeronave (AFHA), Functional Hazard Assessment Nível Sistemas (SFHA), Preliminary System Safety Assessment (PSSA) e System Safety Assessment (SSA).*

No entanto, nem sempre são desenvolvidas todas essas avaliações. O processo pode prescindir da PSSA. Tudo vai depender do tipo de sistema que se vislumbra, a partir dos

[29] Notem que se t=1 (uma hora de voo), F=λ.

resultados (*outputs*) da SFHA, que se desenvolve a partir dos resultados (*outputs*) da AFHA.

Algumas dessas etapas requerem a aplicação de ferramentas apropriadas. Na AFHA, não se vislumbra nenhuma ferramenta especial. Trata-se de uma avaliação das funções da aeronave, segundo os potenciais efeitos de uma perda dessas funções ou um mau funcionamento das mesmas, como teremos a oportunidade de ver, logo à frente.

Nas etapas seguintes, na SFHA e na PSSA (se incluída), vamos necessitar de ferramentas tais como FTA (*Fault Tree Analysis*) e, por parte dos fornecedores de sistemas, da FMEA (*Failure Modes, and Effects Analysis*) pertinentes a seus sistemas. Falaremos um pouco mais sobre essas ferramentas no item 6. Por ora, dizemos apenas que a FTA, por exemplo, é uma ferramenta *top-down*, isto é, uma ferramenta dedutiva; a ferramenta dos detetives, diríamos, que parte do crime consumado (falha) e vai identificar o(s) criminosos (causas). Ela poderia também ser largamente utilizada na Medicina (e em tantas outras áreas), que partiria de uma possível doença instalada para identificar as causas.

Em nosso caso, a FTA nos permite partir de uma failure condition (efeito) nível aeronave e identificar (deduzir) as causas que proveem dos sistemas que realizam as funções da aeronave.

Já a FMEA, é uma ferramenta *bottom-up*, isto é, uma ferramenta indutiva; ela parte das falhas dos componentes dos equipamentos dos sistemas, para chegar à taxa de falha desses sistemas.

5.2. Primeiro Contato com a Autoridade, Relativo ao Processo de *Safety Assessment*

Em seu item 16 (pág. 25), intitulado *Safety Assessment*, e, já de pronto, em seu subitem “a”, a AC 23.1309-1E passa a orientação de que o Aplicante é responsável pela identificação e classificação (*em relação à severidade*) de cada *Failure Condition,* afetando as funções nível aeronave, bem como pela escolha de um método aceitável (*como fazer*) para desenvolver o processo de *Safety Assessment.* Trata-se, portanto, de uma imposição da Autoridade.

A identificação das funções, como vimos em 3.1.1, é realizada pela ES da empresa, por meio da Análise Funcional. A atribuição da severidade da perda ou mau funcionamento dessas funções é feita no processo de Safety Assessment, por meio da *Functional Safety Assessment* (FHA), nível aeronave (AFHA), que identifica as *failure conditions* e respectivas severidades dessas funções, no nível aeronave. É essa AFHA que é apresentada à Autoridade, juntamente com a metodologia que o Aplicante pretende adotar no processo de *Safety Assessment*.

A entrega dessa documentação deverá ser feita logo no início (Fase Conceitual), para que a metodologia de *Safety Assessment*, aprovada pela Autoridade, seja logo depois introduzida no Plano de Certificação. Isso é importante para que ele, Aplicante, desenvolva, daí para frente, seu processo de *Safety Assessment*, tendo a certeza de que sua metodologia está no caminho certo, isto é, de acordo com a Autoridade, o que, talvez, lhe propicie evitar gastar custosos homens-horas.

Há autores que consideram a AFHA uma limitação, um desperdício de dinheiro. Isso nos parece paradoxal, ou seja, se ela praticamente já existe, decorrente de projetos anteriores, praticamente já está pronta para o novo projeto. Ademais, a empresa tem que entender que, como já dissemos, a Autoridade exige que lhe seja entregue uma AFHA, juntamente com uma proposta da metodologia de *Safety Assessment* que pretenda adotar. Portanto, ponto final à questão, a AFHA tem de ser (*must*) apresentada à Autoridade, seja ela difícil[30] ou não de ser feita.

Por outro lado, é muito importante, <u>mas importante mesmo</u>, que o Analista de *safety* entenda bem o espírito ou filosofia da AFHA, que apresentaremos mais adiante, quando trataremos especificamente desse tipo de avaliação.

Com relação à metodologia, as AC 23.1309-1E/AC 25.1309-1A e a ARP 4761 são métodos aceitáveis pela Autoridade. Todavia, estamos centrados aqui na adoção da metodologia das AC 23.1309-1E/25.1309-1A, por serem elas de própria lavra da Autoridade, sugerindo, no entanto, como coadjuvante, a ARP 4761, no que tange principalmente às ferramentas ali apresentadas, sobretudo para a análise quantitativa.

[30] No caso raro de um projeto com muitas novas funções.

5.3. O Passo a Passo do Processo de Safety Assessment – Informações Úteis para o Analista

A figura 3 apresenta o fluxograma do processo de *Safety Assessment*. Trata-se da figura 3 da AC 23.1309-1E (Pág. 26). Vamos, de modo geral, seguir esse fluxograma, complementando o processo ali estabelecido, passo a passo, com nossas considerações mescladas com aquelas das AC 23.1309-1E e AC 25.1309-1A.

Atenção! As avaliações e análises do processo são preliminares, isto é, à medida que o processo se desenvolve, elas vão sendo atualizadas com as alterações de configuração do projeto, até que o mesmo esteja congelado, tendo-se então avaliações definitivas. **Guardem isso.**

O processo é bastante extenso, quando se refere a um projeto novo no mercado, como acontece com aeronaves encomendadas por uma Força Aérea, uma vez que a configuração funcional das aeronaves depende das missões que lhe forem atribuídas.

Na Aviação Civil, no entanto, como já mencionamos, os projetos podem se diferenciar muito pouco, um em relação a outro, o que permite economizar um bom número de homens- horas dos analistas e participantes do processo de safety assessment.

5.3.1. Primeiro Passo: *Preliminary Functional Hazard Assessment* (FHA) Nível Aeronave (AFHA)

Como já alertado, a AFHA deve (*must*) ser feita logo no início do ciclo de vida da aeronave (*System Life Cycle*), isto é, na Fase Conceitual, quando, ainda nem teria sido apresentado o Plano de Certificação à Autoridade e, rigorosamente, nem se teria ainda o elenco dos sistemas que seriam instalados na aeronave, mas somente o elenco de funções decorrentes da Análise Funcional da ES. É básica porque por meio dela alocam-se os requisitos de segurança às funções da aeronave e, a partir destes, alocam-se, por meio de FHAs nível sistemas (SFHA), requisitos que serão aplicados aos meios que serão materializados nos sistemas que integrarão a aeronave, para a implementação de suas funções. Essa é a lógica.

A primeira coisa a fazer é identificar as *Failure Conditions* associadas à perda ou mau funcionamento das funções e suas respectivas severidades. Para fazer isso, devemos seguir a orientação contida no item 3.1.3.

Agora, vamos tratar da filosofia da AFHA. Por importante, sugerimos ao leitor especial atenção ao que será dito em seguida. Vamos inclusive colocar em itálico e em negrito, tentando assinalar a importância do assunto.

Nesta fase (Projeto Conceitual), temos de entender que a Autoridade não sabe nada (e de fato não sabe mesmo) a respeito do projeto da aeronave. Para ela, trata-se de um projeto novo de uma aeronave. A Autoridade não está interessada em saber quais são os sistemas, com suas características de fabricante, nomenclatura e Part Number (PN), que vão prover essas funções porque ela sabe que, nessa fase, essas informações ainda não existem; ela quer saber quais são as funções da aeronave e qual a severidade das failure conditions pertinentes à perda ou mau funcionamento de cada uma; só isso.

Obviamente, os experientes engenheiros da empresa já sabem quais são os sistemas mais prováveis para realizar as funções nível aeronave. Porém, esses sistemas surgirão ou começarão a surgir, em seguida, na FHA nível sistemas (SFHA), quando se tratará dos meios que deverão realizar as funções da aeronave.

Uma vez identificadas as funções nível aeronave e respectivas *Failure Conditions,* com suas associadas severidades, essas informações são inseridas numa tabela e apresentada como Apêndice de um relatório com o título, por exemplo, de *Technical Report SAR-1 – FHA Aircraft Level (AFHA): Functions, Failure Conditions and Severities Proposal.* Essa tabela apresenta as funções nível aeronave, as respectivas *Failure Conditions* (perda total da função ou mau funcionamento, anunciado ou não anunciado), a fase do voo, a condição meteorológica, os efeitos na tríade: tripulação, aeronave e ocupantes, e a severidade da *Failure Condition.* Esse quadro é suficiente para a apresentação à Autoridade.

Argumentamos, no entanto, que, nessa tríade, num primeiro momento das consequências de uma *Failure Condition*, está a tripulação, em especial os pilotos, que comandam e controlam a aeronave. No momento em que os pilotos perderem o comando e o controle, por indisponibilidade ou mau funcionamento de uma função, é que vão surgir as consequências que completam a tríade (aeronave e ocupantes). Desse modo, os pilotos são a prioridade, isto é, o foco.

No Módulo III, apresentaremos um exemplo de AFHA com o respectivo relatório, para servir de orientação ao leitor.

5.3.2. FHA Nível Sistemas (SFHA)

Concluída a AFHA, discutida e aceita pela Autoridade, juntamente com a metodologia do processo de *Safety Assessment*, prosseguem as atividades desse processo, agora com as FHA nível sistemas (SFHA).

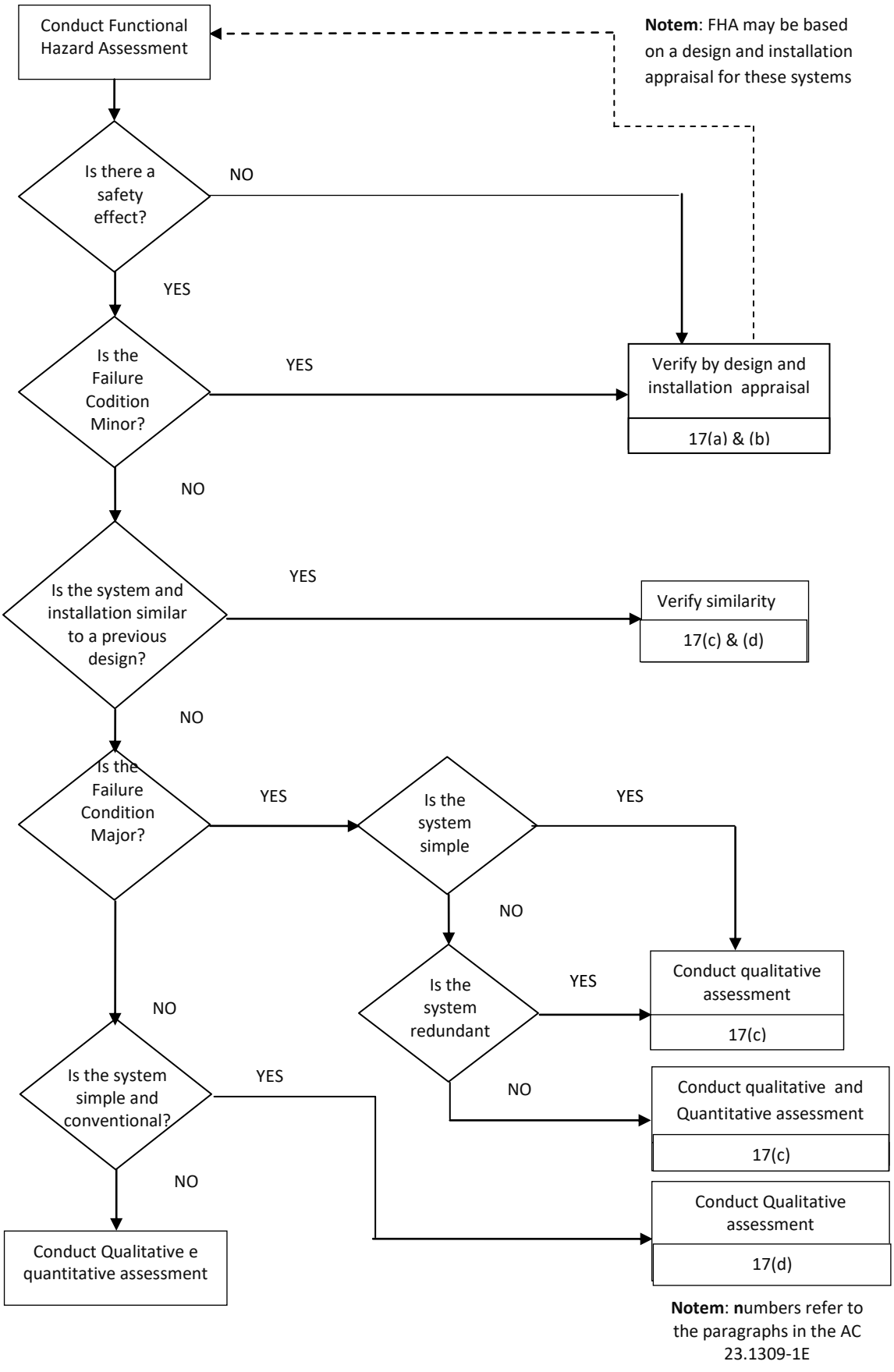
Reforçamos aqui que os sistemas são os meios que realizam as funções nível aeronave. Contudo, primeiro precisamos identificar esses meios, partindo da AFHA, e são as SFHA que, em princípio, caracterizarão os meios que serão configurados pelos sistemas. Trata-se de avaliações, por meio das quais se transladam requisitos de falibilidade (F) das funções da aeronave para esses meios, caracterizados fisicamente, a posteriori, pelos sistemas que realizarão as funções nível aeronave.

O translado dos requisitos nível aeronave para os respectivos meios é feito com a ajuda de uma FTA (*Fault Tree Analysis*), que já mencionamos, ou de uma *Dependence Diagram* (DD)[31]. Escolhemos, neste trabalho, a FTA, por dar uma visibilidade melhor do processo de alocação de requisitos; mas, isso é uma questão de opinião.

O exemplo apresentado no Módulo III deixará claro como se faz esse translado.

[31] V. Ref. 8.

Fig.3 (Figure 3 in AC) – DEPTH OF ANALYSIS FLOW CHART



Notem que, até aqui, não definimos fabricantes e *Part Number* (PN) dos possíveis sistemas que realizarão as funções nível aeronave; apenas alocamos requisitos de segurança a esses possíveis sistemas, que serão, a posteriori, definidos pela ES.

O primeiro passo na SFHA é verificar quais são as funções nível aeronave com severidades *No Safety Effect* e *Minor*, conforme o processo da Fig. 3. Essas funções não requerem nenhuma análise estruturada (como aquelas usando FTA, por exemplo). Bastará uma Avaliação de Projeto (*Design Appraisal*) e de Instalação (*Installation Appraisal*). No entanto, essas avaliações vão ter de demonstrar a existência de certas condições de projeto. É necessário demonstrar que essas funções são isoladas ou independentes, em termos de seus outputs serem inputs para funções cujas *Failure Conditions* sejam *Major, Hazardous* ou *Catastrophic*. Isso ficará claro quando tratarmos especificamente dessas *Failure Conditions* (itens 5.5.2 e 5.5.3).

Por outro lado, todas as funções nível aeronave com *Failure Conditions Major, Hazardous* e *Catastrophic* deverão ser objeto de SFHA.

O que o Aplicante deverá fazer, nas SFHA, é, como já assinalamos, definir, a partir da AFHA, os requisitos para os possíveis meios (futuros sistemas) que vão realizar as funções nível aeronave, procurando abrandar as *Failure Conditions* com severidades *catastrophic* e *hazardous*, identificadas no nível aeronave. Isso ficará claro no exemplo apresentado no Módulo III.

A alocação de requisitos, para cada meio considerado numa SFHA, considera o requisito atribuído à *Failure Condition* de mais elevada severidade da respectiva função nível aeronave, que, como já vimos, depende da fase do voo, das condições ambientais externas (VMC ou IMC) e dos efeitos na tríade Aeronave, Tripulação e Ocupantes.

Neste ponto, atenção! Talvez devêssemos até ter dito bem antes o que vamos dizer agora. Mas, vamos lá: se o Aplicante utilizar, por exemplo, apenas um sistema como meio para realizar uma função nível aeronave considerada crítica, isto é, indispensável para o voo e pouso seguros (potencial catastrófico), esse sistema não pode deixar de exercer sua função corretamente, em virtude de uma única falha. Veja a exceção decorrente da AC 25.1309-1A, no item 5.5.5(e).

Este é, entre nós da área de safety, o chamado conceito da falha simples ou singular (*Single Failure Concept*); na realidade, é um requisito de segurança[32].

Isso significa que não basta que o Aplicante demonstre que seu sistema satisfaz o requisito de extremamente improvável com $F < 10^{-9}$. É necessário demonstrar ainda, por meio de um meticuloso relatório de engenharia (*Design Appraisal*), por meio de uma rigorosa FMEA do fabricante, que o sistema, em consequência de uma única falha, não perde sua função ou entra em um mau funcionamento de consequências catastróficas. Depois, é conversar com a Autoridade.

Na verdade, esse requisito pode simplificar o processo de Safety Assessment. É que, para evitar esse inconveniente, o Aplicante, apesar dos custos adicionais, costuma utilizar a chamada redundância funcional, ou seja, utiliza dois sistemas: um deles é o denominado sistema principal (P), sendo aquele que o piloto normalmente usa, de pronto, e o outro, dito secundário (S), que servirá de alternativa ao piloto, em caso de falha do principal. Tem-se então, neste caso, um sistema dito duplo ou dual, ou um sistema redundante de dois canais.

Nesse contexto das SFHA, a AC chama a atenção para os sistemas que, individualmente, realizam várias funções nível aeronave, boa parte delas com *Failure Conditions* de severidade catastrófica, dependendo da fase de operação e das condições meteorológicas. Obviamente, a perda do inteiro sistema significa perda de todas as funções realizadas pelo mesmo, uma situação certamente mais crítica que a perda de uma única função. Aqui entra, de maneira contundente, o conceito de falha simples.

Para dar um exemplo, recorremos aos sistemas PFD (*Primary Flight Display)*, tratado na Seção 23.1311, com a orientação para mostrar sua conformidade com os requisitos de segurança apresentados não só nas AC 23-1309-1E/23.1309-1A, mas também na AC 23-1311-1C.

Esses sistemas realizam várias funções de apresentação de parâmetros importantes para o piloto, alguns críticos para o voo e pouso seguros (*Catastrophic Failure Conditions)* ou essenciais (*Hazardous/Major Failure Conditions*), tais como *speed, attitude, altitude e heading*, além de outras, como, por exemplo, parâmetros críticos do motor.

Para contornar esses problemas, em ambos os casos (falha total ou falha de uma das funções críticas), o Aplicante instala um sistema redundante de duplo canal ou sistema

[32] AC 23.1309-1E/25.1309-1A.

dual, ou seja, um conjunto de dois sistemas, um dito principal, que o piloto usa normalmente, e um secundário (o *backup*). O sistema *backup* pode ser idêntico ao principal ou diferente, desde que, no mínimo, realize as funções do principal e tenha uma diferente alimentação elétrica e sensor que o mantenham funcionando, na hipótese de perda de alimentação ou do sensor principal. Dito em outras palavras, os sistemas que constituem o sistema dual devem ser independentes.

Há outros aspectos a serem considerados, quando se trata de utilizar *displays* eletrônicos. Trataremos desses aspectos, quando apresentarmos o exemplo de uma SFHA, no Módulo III.

5.4. Tipos de Sistemas Considerados em Safety Assessment

Vamos agora tratar de alguns conceitos básicos, que a AC 23.1309-1E trata como “definições”. São os conceitos de Sistemas Convencionais, Sistemas Simples e Sistemas Complexos.

- **Sistemas Convencionais** - Um sistema é considerado convencional se sua função, os meios tecnológicos para implementar sua função e o pretendido uso são os mesmos ou muito similares aos daqueles sistemas previamente aprovados e que já são comumente usados. São sistemas que têm uma considerável história em serviço.
- **Sistemas Simples -** O sistema é considerado simples, quando sua operação para realizar suas funções, seus modos de falha ou efeitos de falha são relativamente fáceis de entender por meio de uma análise qualitativa e ensaios (testes) de laboratório.
- **Sistemas Complexos - O** sistema é complexo quando suas operações internas para realizar suas funções, seus modos de falha ou efeitos de falha são difíceis de entender sem ajuda de métodos de avaliação analíticos ou métodos de avaliação estruturados. Em geral, não se consegue ensaiar (testar) exaustivamente esses sistemas.

Poderíamos também dizer que o sistema é complexo quando ele não é simples (bem cômodo!). Note que um sistema convencional pode ser simples ou complexo.

Em geral, são complexos os sistemas que contêm circuitos lógicos inseridos em chips e/ou sistemas que não podem ser analisados exaustivamente por meio de ensaios. Isso significa, atualmente, a imensa maioria dos sistemas aviônicos. Por isso, consideramos que, praticamente, todo sistema aviônico, hoje, é complexo. Um computador de bordo, por exemplo, quando formando um sistema, torna-o complexo.

Não se deve perder de vista que não existe uma relação direta entre simplicidade ou complexidade do sistema e a severidade de suas *Failure Conditions*. Um sistema com *Failure Condition Major*, por exemplo, pode estar enquadrado como complexo, dependendo de sua arquitetura.

O fato é que, na hora de discutir isso com a Autoridade, pode ser que a interpretação do Aplicante não coincida com a da Autoridade. O remédio então é seguir, tanto quanto possível, a Autoridade.

5.4.1. Níveis de Garantia de Qualidade de Desenvolvimento (DALs) para Software e Hardware Complexo

Há pouco mais de quatro décadas, os equipamentos dos sistemas aviônicos eram constituídos principalmente por dispositivos discretos, já no estado sólido (semicondutores), tais como transistores, diodos, resistores, capacitores, etc. Hoje, esses dispositivos ainda existem, mas, em grande parte, são microdispositivos e estão inseridos nos chamados microcircuitos de uma “pastilha”, mais conhecida por *chip*.

O *chip*, atualmente, pode ter dezenas ou mais de uma centena de entradas (*inputs*) e saídas (*outputs*), com capacidade de realizar várias funções. Para complicar mais ainda, esses *chips* passaram a incorporar softwares, que são o “cérebro”, isto é, o comando e controle das funções nos *chips* residentes. Testar os equipamentos com esses dispositivos (SW e HW) não é tarefa fácil. Diante dessa realidade, a FAA classificou os sistemas com esses equipamentos como “complexos” e recomendou que os fabricantes, ao desenvolverem o SW para os mesmos, seguissem a DO-178, hoje na versão C, (Ref. 3), e para o hardware (HW) complexo recomendou a DO-254 (Ref. 7), documentos que primam pela qualidade do desenvolvimento do SW e do HW, ao compasso das severidades de falhas identificadas na AFHA.

Isso seria suficiente para demonstrar à Autoridade que os sistemas contendo esses equipamentos estão em conformidade com os requisitos de aeronavegabilidade, que incluem os requisitos de *safety* de sistemas.

A ideia é: "Já que não se consegue fazer testes exaustivos de sistemas eletrônicos complexos e nem FMEAS peça por peça, para determinar a taxa de falha dos equipamentos contidos nesses sistemas e, em consequência, a taxa de falha desses sistemas, vamos pelo menos de certa forma compelir os fabricantes a adotarem processos de desenvolvimento que redundem em uma boa qualidade do SW e do HW, com uma escala de níveis de qualidade decorrente da severidade da condição de falha resultante da AFHA".

Que fique bem entendido, no entanto, que a Autoridade não certifica SW, mas o sistema que o incorpora. Desse modo, a DO-178 e a DO-254, rigorosamente, "não são requisitos", mas padrões de *quality assurance* de desenvolvimento, recomendados pela FAA, para se atingir níveis de segurança aceitáveis; contudo, e aqui vem o melhor: **se o fabricante não seguir o processo global contido nesses documentos, o sistema não será aceito pela Autoridade**. Simples assim.

A DO-178 atribui ao SW um Nível de Garantia de Desenvolvimento (*Development Assurance Level* – DAL) que depende da severidade da *Failure Condition*, começando com o nível A, para sistemas com *Failure Conditions* que possam gerar falhas catastróficas da aeronave, decrescendo até o nível D, para a *Failure Condition Minor*[33]. O mesmo ocorre com o respectivo HW complexo, por meio da DO-254, que caracteriza o sistema físico. Desse modo, a fonte para essa classificação de SW e HW é a *FHA* nível aeronave (AFHA), que identifica a severidade das *Failure Conditions.*

A Fig. 4, extraída da Fig. 2 da AC 23.1309-1E (página 23), mostra as severidades, probabilidades (Falibilidade F) das *Failure Conditions* nível aeronave e os respectivos DALs para os sistemas da Classe IV (*Commuter*), da Parte 23.

Embora a AC 23.1309-1E não atribua nenhum requisito de DAL para a "severidade" *No Safety Effect*, os documentos DO-178C e DO-254 atribuem o DAL E para os sistemas cuja perda ou mau funcionamento não traga nenhum efeito adverso na segurança. Adotaremos essa estratégia.

[33] A AC não se assinala nenhum DAL para *Failure Condition No Safety Effect*.

Fig. 4 – Probabilidades (Falibilidades), Severidades de *Failures Conditions* e DAL de *Software* e *Hardware, para sistemas complexos, conforme a AC 23.1309-1E*

Failure Condition	No Safety Effect	Minor	Major	Hazardous	Catastrophic
Probability (F) and DAL	***No probability or SW and HW Development Assurance Level (DAL)*** **(34)**	$F < 10^{-3}$ ***P = D***	$F < 10^{-5}$ ***P = C, S = D***	$F < 10^{-7}$ ***P = B, S = C***	$F < 10^{-9}$ ***P = A, S = B***

***Notas**:*

(1) ***P** significa sistema principal, e **S**, sistema secundário, considerando configuração de sistema redundante de duplo canal ou dual. Observe que no caso de severidade Minor não se menciona um sistema redundante (**S**), porque, convenhamos, não faz sentido redundância para essa severidade.*

(2) *Note também que no caso das severidades Major, Hazardous e Catastrophic atribuem-se diferentes DAL para os sistemas principal e secundário. Para a severidade Major, por exemplo, temos o sistema principal com DAL C e a Falibilidade $F < 10^{-5}$, normalmente atribuída a Major; mas, para o sistema secundário, o DAL é D. Se o Aplicante utilizar, por exemplo, dois PFD iguais (mesmo fabricante e Part Number (PN)), tanto o principal como o secundário terão, obviamente, o mesmo DAL.*

5.5. Informações Úteis, Segundo as *Failure Conditions* Identificadas

No item 17 (pág. 29) da AC 23.1309-1E, são analisados vários aspectos das *failures conditions*, que podem conduzir o Aplicante a adotar posturas de análise qualitativas ou quantitativas, ou ambas. Trata-se de um ponto importante porque pode ajudar, e muito, o Aplicante a poupar homens-horas, na realização do processo *de Safety Assessment.*

Mas que fique bem claro: consiste apenas numa orientação; a última palavra é a da Autoridade. Seja como for, é recomendável estar tão perto quanto possível das orientações da Autoridade contidas nas AC.

5.5.1. Dois Importantes Atalhos: Critérios da Identidade e da Similaridade

Já, de pronto, devemos dizer que se o Aplicante pretende adquirir qualquer sistema sem passar pelo inteiro ciclo das análises de *Safety Assessment,* economizando uma boa

[34] DAL **E**, segundo a DO-178C e DO-254.

quantidade de homens-horas, poderá fazê-lo, em alguns casos, entre os quais, por importantes, citamos aqui dois deles, sob a forma de critérios: Critério da Identidade e Critério da Similaridade, lembrando sempre que a Autoridade vai ter que concordar com a argumentação do Aplicante, e é aí que pode estar o nó.

A AC 23.1309-1E não trata claramente do critério da identidade[35], mas a AC 25.1309-1A o faz no item 8(d)(2), da página 10 da AC. Ali se mencionam os sistemas idênticos e sistemas similares.

Parece-nos óbvio que o princípio da identidade seja mais forte que o da similaridade, porque identidade significa levar em conta a existência de sistemas idênticos instalados em aeronaves já certificadas de mesma classe da Parte 23 ou em aeronaves certificadas da Parte 25, já com uma experiência bem sucedida em serviço. Cabe ao Aplicante demonstrar à Autoridade a existência dessa identidade.

Não confundir com sistemas convencionais. Identidade significa mesmo fabricante, mesma nomenclatura, mesmo *part number* (PN), tendo seguido o mesmo manual de instalação do fabricante[36], como recomendado pela Autoridade, podendo ter na instalação pequenas diferenças, como, por exemplo, o comprimento de cabos e localização de antenas na fuselagem.

Outro critério a considerar é o da similaridade. Um sistema é similar a outro, quando realiza a mesma função desse outro, tem dimensões, projeto de instalação com pequenas diferenças, podendo ser de fabricante diferente e, portanto, com PN diferente. Pois bem, se um sistema for similar a outro, que esteja instalado numa aeronave certificada da mesma classe da Parte 23, ou similar a outro instalado numa aeronave certificada da Parte 25, já com experiência em serviço, isso seria suficiente para a aceitação, por parte da Autoridade, em se tratando de *Failure Conditions* de severidade até o nível *Major*. Basta que o Aplicante demonstre à Autoridade a existência dessa similaridade. No entanto, há algumas restrições adicionais, quando se trata de *Failure Conditions* de severidade *Hazardous* e *Catastrophic* (v. 5.5.5).

[35] Cremos que o critério da "Identidade" esteja incluído no critério da similaridade, tarado também na AC 23.1309-1E, no critério de similaridade, nos casos de "altíssima similaridade".

[36] A Autoridade espera que o Aplicante use o Manual de Instalação do Fabricante, por motivos óbvios: ele testou o projeto de instalação alhures, inicialmente em suas instalações e, posteriormente, em aeronaves, chegando à conclusão de que é um processo conveniente, a posteriori aceito pela Autoridade. No entanto, alguns detalhes adicionais decorrentes, por exemplo, de comprimentos de cabos, posicionamento de antenas na célula, podem divergir de projetos já certificados. Mas as possíveis consequências dessa pequenas diferenças podem ser verificadas em ensaios no solo e em voo.

5.5.2. *Failure Conditions* com Severidade *No Safety Effect*

Requisito: Nenhum (*none*). Mas, atenção! Apesar de não existir requisito de Severidade para essas *Failure Conditions*, a AC enfatiza que é necessário tomar certos cuidados. A função do sistema tem de ser independente de quaisquer outras funções críticas ou essenciais para a operação segura da aeronave. Em outras palavras, o *output* do sistema não pode ser um *input* importante para outro sistema que exerça uma função crítica (catastrófica) e essencial (*Hazardous*). Dá-se a essa característica a denominação de Independência Funcional.

Entretanto, em geral já é prática comum de projeto da ES isolar os sistemas daqueles que realizam funções críticas e/ou essenciais. O Aplicante pode mostrar essa independência por meio de uma FHA nível sistema, ou por meio de uma avaliação de projeto e instalação (*Design and Installation Appraisals*). Qualquer que seja o meio, tem de ser convincente.

Como já dito, o DAL para o SW e o HW de sistema complexo com *Failure Condition No Safety Effect* é E porque não há nenhum efeito na segurança. Contudo, aqui vai uma exceção a essa regra: os sistemas eletrônicos *Cockpit Voice Recorder* (CVR) e *Flight Data Recorder* (FDR), que são *No Safety Effect*, devem ter DAL nível D[37], isto é, o projeto deve ser feito com algum cuidado. Por que isso? Porque a Autoridade espera que esses sistemas tenham os projetos de SW e HW executados com certo esmero, uma vez que esses sistemas são importantes, numa possível investigação de acidentes.

5.5.3. *Failure Conditions* com Severidade *Minor*

Requisito: Provável (*Probable*) - $F < 10^{-3}/hv$. Também aqui, a análise deve considerar possíveis efeitos de falhas do sistema em outros sistemas que realizam funções nível aeronave consideradas críticas ou essenciais. O Aplicante pode mostrar essa independência por meio de uma FHA, ou por meio de uma avaliação de projeto e instalação (*Design Appraisal*). Se o sistema tiver SW e HW complexo, o DAL para SW e HW será D.

Como no caso anterior (*No Safety Effect*), em geral, a prática normal já é isolar o sistema daqueles que realizam funções essenciais e/ou críticas.

[37] A escala de DALs, do mais restritivo ao menos restritivo é A, B, C, D, E (vide DO-178B/C e DO-254, Ref. 3 e 6).

5.5.4. *Failure Conditions* com Severidade *Major*

Requisito: Remota (*Remote*) - F < 10^{-5}/hv. Se o sistema tiver SW e HW complexo, o DAL para SW e HW será P = C (sistema principal); se houver um sistema secundário, S = D.

A avaliação de segurança poderá ser baseada em um julgamento de engenharia, seguindo um dos vários métodos a seguir:

a) Quando pertinente, pode-se usar o argumento da identidade ou similaridade (5.5.1). Bastaria então uma avaliação de engenharia (*Design Appraisal*), comprovando essa identidade ou similaridade, seja o sistema simples ou complexo.

   Nota: *Só para lembrar, reforçamos que é responsabilidade do Aplicante fornecer dados que suportem suas reivindicações de identidade e/ou similaridade com uma instalação já certificada.*

b) Quando se tratar de um sistema simples (i.e, não complexo) e para o qual não possa ser usado o argumento de identidade ou similaridade, então a conformidade pode ser demostrada por meio de uma avaliação qualitativa que mostre que as condições de falha *Major* do sistema instalado são consistentes com a FHA pertinente (utilização de sistemas redundantes, por exemplo).

O parágrafo anterior é o que se depreende da AC (item 17c(2)), e pode confundir um pouco o analista. Vamos então colocar nosso comentário. Se o sistema é simples, não redundante, certamente será possível demonstrar quantitativamente, por meio de uma FMEA do fornecedor, que o sistema está em conformidade com o requisito. Isso nos parece suficiente. No entanto, se o Aplicante decide adotar um sistema dual, certamente fica fácil demonstrar a conformidade.

c) Para mostrar que mau funcionamento em sistemas de alta complexidade, sem redundância (por exemplo, um sistema com um microprocessador de auto-monitoramento), são de fato enquadrados no requisito Remoto, é necessário conduzir uma FTA qualitativa ou FMEA suportada por dados de taxas de falhas e análise de cobertura de detecção de falha (*fault*)[38].

O parágrafo anterior é o texto que se depreende do item 17c(3) da AC. Comparando esse texto com aquele do item 19(a), parece-nos haver um conflito. Aqui se admite um sistema

[38] A AC utilizou, uma única vez, o termo *fault*, em vez de falha. Esse termo é bastante controvertido no meio aeronáutico. A NBR 5462/1994, baseada na *International Electrotechnical Vocabulary - Cap 191 Dependability and Quality of Service*, da IEC, dá ao termo *fault* o significado de "pane", isto é, o estado que um sistema assume após ter sofrido uma falha. Nesse entendimento, ter-se-ia então *failure* como um evento e *fault* como um estado, que só se modificaria depois que o sistema fosse reparado, reassumindo seu estado ou condição operacional.

complexo sem redundância, impondo uma FTA qualitativa **ou** uma FMEA suportada por taxa de falha, ou seja, que é uma análise quantitativa, isto é, ou uma ou outra. Já o texto do item 19a da AC simplesmente impõe uma análise quantitativa para esses sistemas, para mostrar, é claro, que o sistema se enquadra em $F < 10^{-5}$.

Seja como for, sabemos, no entanto, que uma FMEA de sistemas complexos peça por peça (*piece-part*) pode ser inviável. Em última análise, se o sistema tiver DAL C (vide tabela da Fig. 4), isso hipoteticamente resolveria o problema. Quanto à cobertura de detecção de falha, entendemos que sejam avisos ou alertas anunciando a falha.

d) A análise de um sistema redundante (ou dual) na aeronave é usualmente completa se ela mostrar:

   (i) a isolação entre os canais funcionais de redundância; e

   (ii) uma satisfatória confiabilidade (ou Falibilidade) para cada canal.

   Para sistemas complexos, em que uma redundância seja requerida, pode ser necessária uma FMEA qualitativa ou uma FTA para determinar que a redundância realmente existe (por exemplo, que nenhuma falha simples afeta todos os canais funcionais).

O parágrafo anterior, salvo melhor juízo, é o texto que se depreende do item 17c(4) da AC, pág. 29. Ora, se os canais funcionais forem isolados, isto é, independentes, isso significa que uma falha simples num dos canais não vai refletir no outro canal, mesmo que os canais fossem idênticos. Em virtude dessa identidade dos canais, é claro que eles têm os mesmos modos de falha, mas é pouco provável que uma falha num dos canais vá acontecer ao mesmo tempo no outro canal. Nós não estamos diante de um ambiente determinístico, mas probabilístico. Temos de lembrar que os canais são independentes, em termos de instalação.

Lembramos que sendo o sistema complexo, como se menciona aqui, ele deve ser desenvolvido levando em conta o DAL C, para o sistema primário, e D, para o secundário.

5.5.5. *Failure Conditions* com Severidades *Hazardous* e *Catastrophic*

Requisitos: (a) *Hazardous*: *Extremely Remote*: $F < 10^{-7}/hv$; e

(b) *Catastrophic*: *Extremely Improbable*: $F < 10^{-9}$.

Essas *Failure Conditions* são as mais preocupantes para a segurança da aeronave, devendo, portanto, ter uma análise com máximo rigor.

Para essas *Failure Conditions*, normalmente é necessário realizar uma *Safety Assessment* mais completa. Essa avaliação usualmente consiste de uma combinação apropriada de análises qualitativa e quantitativa. No entanto, há casos em que não será necessário chegar a esse rigor. São os que apresentaremos a seguir.

a) Pode-se utilizar o Critério da Identidade (5.5.1), caso seja possível demonstrar cabalmente a existência dessa identidade com instalações em outras aeronaves já certificadas da mesma classe da Parte 23, ou ainda aeronaves certificadas da Parte 25. O julgamento de engenharia deverá ser bem fundamentado.

b) Para instalações simples e convencionais (i.é, com baixa complexidade e similaridade em seus atributos relevantes), pode ser possível avaliar uma *Failure Condition Hazardous* ou *Catastrophic* como sendo *extremely remote* ou *extremely improbable* (requisitos qualitativos) com base num julgamento de engenharia bem fundamentado, usando apenas uma análise qualitativa. A base para essa avaliação será:

   (i) existência de redundância;

   (ii) independência e isolação dos canais de redundância; e

   (iii) comprovação da confiabilidade da tecnologia envolvida[39].

c) Uma satisfatória experiência de serviço em sistemas similares, comumente usados em muitas outras aeronaves, pode ser suficiente, quando existir uma boa similaridade, tanto no projeto do sistema quanto nas condições de operação.

d) Para sistemas complexos, onde possa ser rigorosamente identificada uma verdadeira similaridade, em todos os atributos relevantes, incluindo atributos de instalação, pode ser possível avaliar uma *hazardous* ou *catastrophic Failure Condition* como sendo, respectivamente, *extremely remote* ou *extremely improbable,* a partir de um

[39] Certos fabricantes têm tecnologias de confiabilidade muito bem consolidada, comprovada pela excelência de seus produtos, ao longo do ciclo de vida dos mesmos.

experiente julgamento de engenharia, utilizando apenas uma análise qualitativa (*Design Appraisal* e *Installation Appraisal*), conforme apresentado em 6.2 e 6.3. É requerido um alto grau de similaridade no projeto e na aplicação.

e) Como já visto, nenhuma *Failure Condition* de severidade catastrófica deve resultar de uma falha única de um sistema. Isso, por si só, já recomendaria o uso de um sistema dual, isto é, redundante (*backup*). No entanto[40], admite-se que um julgamento experiente de engenharia e histórico de serviço possam demonstrar que uma *catastrophic Failure Condition,* a partir de um único modo de falha no sistema, não ocorre. A lógica e o raciocínio utilizados na avaliação devem ser diretos e muito óbvios, demonstrando cabalmente que um tal modo de falha simplesmente não ocorreria, a menos que esse modo de falha esteja associado com uma *Failure Condition* não identificada na avaliação do processo de *Safety Assessment*, que, por si só, seria catastrófica. É um risco incontrolável, porque qualquer análise tem vulnerabilidades que não são percebidas.

Na verdade, entendemos que, nesses casos, seria mais prudente existir uma redundância, com os argumentos de 5.5.4(d) ou 5.5.5(b). Um sistema dual apresentaria uma relação inversa excelente entre a severidade e a probabilidade de falha do sistema dual. Se uma falha ou mau funcionamento do sistema puder levar a aeronave a um acidente de severidade catastrófica, A AC 23.1309-1E recomenda que os sistemas tenham DALs A, para o sistema primário, e B, para o secundário. Todavia, nada impede que os sistemas que compõem o sistema dual sejam idênticos, o que requereria, obviamente, DAL A para os dois sistemas. Isso dá mais segurança, mas não exime o piloto de pedir à manutenção em terra para substituir o sistema falhado (em pane).

Esse tema, sem dúvida, poderia ser objeto de uma discussão motivada pela Autoridade.

5.6. Sistemas com Equipamentos TSOA (*Technical Standard Order Approval*)

Vamos interpretar aqui o item 21(f), pág. 36, da AC 23.1309-1E, que trata dos equipamentos com aprovação TSO (*TSO Approval*).

[40] V. AC 25.1309-1A, item 7g, pág. 8.

A TSO (*Technical Stander Order*), traduzida pela ANAC na expressão Ordem de Padrão Técnico (OTP), é um documento da Autoridade que estabelece padrões mínimos, conforme a finalidade dos equipamentos, inclusive os considerados complexos, para os quais é incluído o cumprimento da DO-178C (SW) e DO-254 (HW complexo), no que tange aos DALs a eles aplicáveis. Em outras palavras, equipamentos TSOA cumprem com os requisitos de desempenho funcional e de *safety* previstos nas TSO a eles pertinentes.

A Autoridade prefere os sistemas com equipamentos que têm aprovação TSO, isto é, que cumpram os requisitos mínimos inseridos na respectiva TSO. No entanto, não é obrigatório que os equipamentos tenham uma aprovação TSO. Se não tiverem essa aprovação, eles deverão cumprir padrões mínimos equivalentes e aceitáveis pela Autoridade. Há, portanto, que se discutir com a Autoridade. Neste caso, nos parece claro que os fabricantes vão ter de desenvolver seus *Safety Assessment* de maneira semelhante com o previsto na AC e demonstrar que o HW complexo e SW desses equipamentos foram desenvolvidos de acordo com os DALs previstos para os mesmos, conforme a Fig. 2 da AC. Simples assim.

6. MÉTODOS DE AVALIAÇÃO (Item 18 da AC 23.1309-1E)

6.1. Considerações Gerais

Há vários métodos disponíveis para a avaliação qualitativa e quantitativa de falhas, severidades e falibilidades de potenciais *Failure Conditions*, que podem auxiliar o Aplicante, na realização de um julgamento operacional e de engenharia. Alguns desses métodos são estruturados (métodos elaborados especificamente para essas análises).

Os vários tipos de análises são baseados tanto em enfoques indutivos (ex.: FMEA), isto é partindo das causas para os efeitos, quanto dedutivos (ex.: FTA), partindo dos efeitos para as causas (“método do detetive”). Cabe ao Aplicante selecionar as análises que julgar mais conveniente para realizar a *Safety Assessment* de um projeto particular. A ARP 4761 tem detalhes sobre os vários métodos usualmente empregados. Descrições de análises típicas que podem ser usadas são apresentadas a seguir.

6.2. Avaliação de Projeto (*Design Appraisal*)

Uma avaliação qualitativa da integridade e segurança do projeto do sistema. Requer julgamento de engenharia de profissionais experientes. A comprovação de identidade ou similaridade é um exemplo.

6.3. Avaliação de Instalação (*Installation Appraisal*)

Trata-se de uma avaliação da integridade e segurança da instalação do sistema. Qualquer desvio das práticas normais de instalação, aceitas pela indústria, deve ser avaliado. Essa avaliação requer também experiente julgamento de engenharia.

Nota *– Normalmente, as empresas utilizam o manual de instalação do fornecedor do sistema, prática inclusive recomendada pela Autoridade. Contudo, a empresa tem também suas práticas, em função da estrutura particular de seus projetos. Em princípio, é prudente seguir as recomendações do fabricante. Inovações praticadas pelo Aplicante devem ser justificadas à Autoridade, em termos de segurança e praticidade semelhantes àquelas propiciadas pelo manual de instalação.*

Recomenda-se que o Aplicante enfatize tudo isso, em sua avaliação, com profundidade, principalmente quando se tratar de sistemas cujas Failure Conditions tenham severidades Hazardous ou Catastrophic no nível aeronave.

6.4. *Failure Modes, and Effects Analysis* (FMEA)

Como já mencionamos, em termos de descrição, a FMEA é uma análise indutiva, que é utilizada para avaliar os efeitos no sistema e na aeronave de falhas de componentes em equipamentos do sistema. Quando propriamente formatada, ela deve ajudar até na identificação de falhas latentes e das possíveis causas de cada modo de falha. A FMEA pode ser de “componente por componente” (*piece-part*) ou funcional.

Com a tecnologia moderna baseada em microcircuitos, a FMEA “componente por componente” pode ser impraticável, razão pela qual considera-se mais racional utilizar a FMEA funcional. Uma FMEA funcional, por sua vez, pode conduzir a incertezas, nos aspectos qualitativos e quantitativos, que podem, talvez, serem compensados por avaliações mais conservativas, assumindo, por exemplo, que todos os modos de falhas resultem em *Failure Conditions* de interesse, escolhendo cuidadosamente a arquitetura de sistema e usando lições aprendidas de tecnologias similares.

Como já vimos, em se tratando de microcircuitos, estamos diante de sistemas complexos. Neste caso, o recurso é exigir que o sistema, se já existente, tenha sido desenvolvido conforme o DAL que lhe foi atribuído a partir da FHA. Para failure condition Catastrophic, conforme já vimos, o DAL correspondente é A, para um sistema primário, e B, para o secundário.

6.5. Análise por Árvore de Falhas ou Panes[41] (*Fault Tree Analysis – FTA)*

Como dissemos alhures, trata-se de uma análise *top-down.* É a famosa "análise dos detetives: veem o efeito (o morto) e procuram a causa (o assassino)". É utilizada para identificar falhas e eventos que causam as várias *Failure Conditions,* como no caso da FHA nível aeronave e nível sistema. Permite alocar requisitos de segurança quantitativos às funções e desencadear daí os requisitos de segurança dos sistemas. Quando tratarmos da SFHA, mostraremos o quanto são úteis.

6.6. Análise de Causa Comum (*Common Cause Analysis – CCA*)

Devemos ter em conta que um sistema, como os aviônicos, pode falhar (perder a função ou ter mau funcionamento) : (a) por um problema interno (falha de seus equipamentos); (b) ausência ou distorção de input provindo de outro sistema, indispensável para sua correta funcionalidade; (c) interferência eletromagnética interna (EMI); ações inadequadas de manutenção; ou (e) agressões provenientes do ambiente externo à aeronave.

O caso (a) é o que temos discutido, exceto no caso de *failure conditions No Safety Effect* e *Minor*, que a AC assinala minimamente a necessidade de demonstrar a independência, em relação a outros sistemas.

Todo esse contexto entra na chamada Análise de Causa Comum (CCA), que tem de ser feita para cada sistema.

A CCA é dividida em três áreas de estudos:

- Análise de Segurança Zonal (*Zonal Safety Analysis*);

[41] Vide ABNT NBR 5462 – Confiabilidade e Mantenabilidade, baseada no *International Electrotechnical Vocabulary – Chapter 191 – Dependability and Quality of Services,* da IEC (*International Electrotechnical Commission*).

- Análise de Riscos Específicos (*Particular Risk Analysis – PRA*); e
- Análise de Modo Comum (*Common Mode Analysis – CMA*).

6.6.1. Análise de Segurança Zonal (*Zonal Safety Analysis*)

Esta análise tem o objetivo de assegurar que a instalação de equipamentos dos sistemas, dentro de cada zona delimitada da aeronave, está adequada, com relação a padrões de instalação, como temperatura, interferência eletromagnética entre sistemas, e mantenabilidade.

***Nota**: Num projeto de instalação adequado, a maioria dos equipamentos eletrônicos de sistemas aviônicos é instalada na chamada Avionics Bay (Baia - pronúncia: Báia) da aeronave, espaço a eles destinados, com temperatura adequada a todos eles, com projeto de instalação e ensaios adequados, de modo a não haver interferências recíprocas (requisito assegurado por meio de ensaios EMC (Electromagnetic Compatibility), bem como projeto de suporte técnico logístico de Mantenabilidade (Maintainability) adequado, a fim de facilitar o acesso e a segurança, nas ações de manutenção de remoção e instalação. O Aplicante deve assegurar à Autoridade, por meio de Design Appraisal e/ou Installation Appraisal, que esse estado existe, no ambiente em que foram instalados equipamentos (LRU), ou, na hipótese de desvios, assegurar, no relatório, com evidências, que está dentro de limites de segurança esperados.*

6.6.2. Análise de Riscos Específicos (*Particular Risk Analysis – PRA*)

Riscos específicos são definidos como aqueles decorrentes de eventos ou influências externas ao sistema analisado; por exemplo: incêndio, vazamento de fluidos, colisão com aves, estouro de pneu, exposição a HIRF, raios *(lightining)*, falha incontida de máquinas rotativas de alta energia, etc.). Cada risco deve ser objeto de um estudo dedicado para analisar e documentar os possíveis efeitos simultâneos ou em cascata, ou influências que possam violar a independência.

***Nota**: Os mais prováveis riscos para sistemas aviônicos são Lightning e HIRF; porém, hoje os fabricantes adotam técnicas de projeto, análises e ensaios específicos com esses sistemas instalados, para assegurar que os mesmos estejam aceitavelmente protegidos contra essas agressões. Todavia, essas possibilidades têm de ser verificadas[42] e demonstradas à Autoridade.*

[42] Vide AC 20-136B – *Aircraft Electrical and Electronic System Lightning Protection* e AC 20-158A – *The certification of Aircraft Electrical and Electronic Systems for Operation in the High Intensity Radiated Fields (HIRF) Environment.*

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

Esta análise é realizada para confirmar a independência assumida dos eventos que foram considerados em combinação para uma determinada *Failure Condition*. Devem ser considerados os efeitos de erros de especificação, projeto com circuitos ocultos (*sneak circuits*), erros de instalação, procedimentos de manutenção, de fabricação e fatores ambientais diferentes daqueles já considerados na *Particular Risk Analysis* (PRA). Tudo isso, enfim tem de ser analisado e apresentado à Autoridade, em relatório dedicado.

Neste ponto, encerramos este Módulo. Continuaremos nosso estudo, no Módulo III, quando apresentaremos um Estudo de Caso.

Muito obrigado e até lá.

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.*