Organização Brasileira
para o Desenvolvimento
da Certificação Aeronáutica

– Programa de Difusão de Conhecimentos (PDC 02) –

PRINCIPAIS FERRAMENTAS DE ANÁLISE UTILIZADAS NO PROCESSO DE SAFETY ASSESSMENT

Eng. Jolan Eduardo Berquó

– 2018 –

SUMÁRIO

Capítulo 1 INTRODUÇÃO

Neste capítulo você vai entender o propósito deste trabalho (PDC 02) e conhecerá os conceitos básicos que irão ajudá-lo, no desenvolvimento do assunto objeto deste PDC.

1.1. O PROPÓSITO DESTE TRABALHO

Primeiramente, vamos entender o significado de *Assessment*, cuja tradução para o português é “Avaliação”. A AC 23-1309-1D (*System Safety Analysis and Assessment for Part 23 Airplanes)*, em seu item 8 (*Definitions*), letra b, apresenta a diferença entre *Analysis* e *Assessment.* Numa tradução livre, lê-se:

“O termo análise e avaliação são utilizados em todas as partes (da AC). Cada um tem uma definição ampla e os termos são, até certo ponto, intercambiáveis. No entanto, o termo análise geralmente significa uma avaliação mais específica e mais detalhada, enquanto o termo avaliação pode ser uma avaliação mais geral ou mais ampla, podendo incluir um ou mais tipos de análise.

Por outro lado, o termo *safety* significa “segurança”, mas na acepção de proteção contra os perigos decorrentes de falhas não intencionais de um sistema, contrapondo-se ao termo *security*, que se refere a perigos criados intencionalmente, como, por exemplo, ataques terroristas.

Em português, temos um único termo “segurança” para as duas acepções (intencional e não intencional), sendo, por isso, necessário explicitar a acepção que estamos considerando.

O Processo de *Safety Assessment* (Avaliação de Segurança), na aviação civil, destina-se a demonstrar à Autoridade (FAA, EASA, ANAC, etc.) que os sistemas do projeto de uma aeronave, que realizam as funções da aeronave, estão em conformidade com os requisitos de segurança (*safety*) estabelecidos por essa Autoridade.

A etapa inicial desse processo é a alocação de requisitos de segurança (*safety requirements*) da Autoridade a todas as funções da aeronave identificadas pela Engenharia de Sistemas (ES) da empresa que desenvolve o projeto da aeronave, por

meio da chamada Análise Funcional, realizada na Fase ou Projeto Conceitual e, a partir dos resultados dessa primeira etapa, alocar também requisitos de segurança a todos os meios que vão ser fisicamente caracterizados pelos sistemas que realizarão as funções da aeronave. Esse processo compreende quatro etapas ou avaliações, quais sejam:

- *Functional Hazard Assessment* (FHA), nível aeronave (AFHA);
- *Functional Hazard Assessment* (FHA), nível sistemas (SFHA);
- *Preliminary System Safety Assessment* (PSSA); e
- *System Safety Assessment* (SSA).

Para desenvolver essas avaliações, os analistas têm à disposição várias ferramentas de análise[1]. As principais, isto é, as mais utilizadas, são as seguintes:

- *Fault Tree Analysis (FTA)* – Análise por Árvore de Falhas;
- *Dependence Diagrams Analysis (DDA)* – Análise por Diagramas de Dependência, que chega aos mesmos resultados da FTA;
- *Failure Modes, And Effects Analysis (FMEA)* - Análise de Modos de Falha e Seus Efeitos (numa tradução livre); e
- *Common Cause Analysis* (CCA) – Análise de Causa Comum.

A CCA se subdivide ainda em três tipos de análises:

- *Zonal Safety Analysis* (ZSA) – Análise de Segurança Zonal;
- *Particular Risks Analysis* (PRA) – Análise de Riscos Particulares; e
- *Common Mode Analysis* (CMA) – Análise de Modo Comum.

As FHA (AFHA e SFHA), PSSA, CCA e SSA são realizadas pela equipe da empresa responsável pelo Processo de Safety Assessment. A FMEA, por outro lado, é feita pelos fornecedores dos sistemas que serão implantados na aeronave, podendo ser fornecedores externos ou "internos"[2].

[1] Alertamos o leitor para ter o cuidado de não confundir as avaliações ou etapas do Processo de Safety Assessment com ferramentas destinadas à execução, que são instrumentos ou métodos para o desenvolvimento dessas avaliações ou etapas.

[2] Os fornecedores internos são os vários setores de ES da empresa, que podem também desenvolver sistemas para a aeronave por eles projetada.

Isto posto, podemos dizer que o propósito deste trabalho é exatamente *apresentar as* *principais ferramentas de análise, dando ao leitor condições de aplicá-las, nas várias etapas ou avaliações do Processo de Safety Assessment.* Mas, não vamos apresentar aqui um "Tratado" sobre essas ferramentas; passaremos ao leitor apenas o suficiente para que possa compreendê-las e começar a lidar com as mesmas. Caso o leitor deseje um aprofundamento maior no assunto, recomenda-se consultar as referências no final deste trabalho.

Como todos os nossos trabalhos, este também não é uma simples e ordenada coleta de informações de outros autores. Procuramos também acrescentar aqui nosso toque de interpretação, decorrente de nossa experiência profissional.

1.2. CONHECIMENTOS BÁSICOS

Antes de entrarmos no objeto propriamente dito deste trabalho, vamos ter de passar ao leitor alguns conhecimentos básicos pertinentes ao emprego das ferramentas de análise do Processo de *Safety Assessment*.

Primeiramente, devemos compreender a noção de "evento". Um evento é sempre o resultado de um experimento. Por exemplo, no experimento de atravessar uma rua há dois eventos possíveis: atravessar (sucesso) ou não atravessar (insucesso). Outro: o experimento de operação de um sistema, cujos eventos possíveis são não falhar (sucesso) ou falhar (insucesso). Estamos interessados aqui neste último tipo de experimento.

Quando falarmos de falha, estaremos mencionando um mau funcionamento ou perda da função de um item[3] que esteja sendo objeto de discussão. A propósito, muitas vezes o mau funcionamento de um item pode ser até pior que a perda de sua função.

Sabemos que quando um sistema está operando, não podemos afirmar categoricamente que ele vá operar como esperado, isto é, sem falhas, durante o tempo em que o colocarmos a operar. Sabemos, entretanto, que é possível prever a chance de o mesmo operar sem falha ou com falha nesse tempo, utilizando os recursos matemáticos da teoria clássica das probabilidades, partindo do conceito de Variáveis Aleatórias (*Random Variables* – RV), tratado a seguir.

- [3] Item, segundo a norma ABNT 5462, é qualquer coisa de um sistema ou quem com ele lida. Assim, um resistor, um equipamento, o próprio sistema, um ser humano (piloto, por exemplo) são itens.

1.2.1. Variáveis Aleatórias

Na teoria clássica das chamadas distribuições de probabilidades, o conceito de Variável Aleatória (*Random Variables* – R.V.)[4] é básico.

Consideremos então, de pronto, um experimento com um número possível de resultados governados pela chance de ocorrência (resultados aleatórios). Cada resultado é um evento. Ao conjunto dos resultados possíveis denominamos espaço amostral do experimento, representado pela letra S (do Ing. *Space*). Seguindo a notação da Teoria dos Conjuntos da Matemática (Álgebra de Boole), anotamos:

$$S = \{s_1, s_2, s_3, \ldots , s_{k-1}, s_k \}$$

onde, $s_1, s_2, s_3, \ldots , s_{k-1}, s_k$ são os eventos ou resultados possíveis do experimento.

Pois bem, o processo de atribuir a cada resultado possível do experimento um número é denominado R.V. Desse modo, a R.V. é uma função que atribui a cada resultado possível de um experimento um número, em geral real. O domínio da função é o conjunto de resultados do espaço amostral S do experimento. O contra-domínio é portanto um subconjunto dos números reais.

A R.V. pode ser uma função discreta ou contínua. Por exemplo, se observarmos um lote de lâmpadas funcionando durante um ano, e a R.V. contar o número de lâmpadas que tenham queimado em cada mês desse período, então a R.V. estará atribuindo a cada resultado possível um número inteiro. Neste caso, a R.V. é dita discreta. O espaço amostral seria denotado por um subconjunto de números inteiros.

Por outro lado, se acendermos várias lâmpadas e anotarmos o instante em que a cada lâmpada deixa de operar ("queima-se"), então os resultados possíveis são intervalos de tempo, isto é, um subconjunto de números reais. Desse modo, neste caso S é um subconjunto de números reais[5].

Pois bem, neste nosso trabalho estamos interessados em R.V. contínuas definidas no tempo. Por exemplo, estamos interessados no intervalo de tempo que um sistema instalado a bordo de uma aeronave opera, durante a missão da aeronave.

- [4] Daqui para frente, usaremos sempre a abreviação R.V. para as Variáveis Aleatórias.
- [5] Lembremos que o conjunto dos números reais inclue números inteiros positivos e negativos, números decimais, fracionários, etc., que em seu conjunto constituem os números reais.

Além disso, estamos interessados ainda em saber qual é a probabilidade de falha de um sistema, durante a realização de sua missão. Aí, entra uma teoria concentrada nas chamadas funções de distribuição de probabilidades, fundamentada em dois tipos de funções: a Função Densidade de Probabilidades (*Probability Density Function*- PDF), cujo exemplo mais conhecido de nossa área é a Confiabilidade (*Reliability*- R), que nos dá a probabilidade de o sistema não falhar num intervalo tempo t, e a Função de Distribuição Cumulativa de Probabilidades (*Probability Cumulative Distribution Function)*, ou simplesmente Função de Distribuição Cumulativa (*Cumulative Function Distribution* – CDF), cujo exemplo mais conhecido, em nossa área, é a Falibilidade (*Unreliability*), representada pela letra F, que nos dá a probabilidade do sistema falhar, num dado intervalo de tempo t.

A cada PDF (R) corresponde uma CDF (F). As duas são funções complementares, isto é R + F =1, como mostraremos a seguir.

1.2.2. Confiabilidade (Reliability) e Falibilidade[6] (*Unreliability*)

Como pode ser constatado, na extraordinária obra da Ref. 1, há várias PDF e a cada uma corresponde uma CDF. A utilização de uma ou outra PDF vai depender da natureza do sistema, isto é, vai depender de ser o sistema mecânico, hidráulico, eletrônico, elétrico, etc.

No caso de sistemas elétricos e eletrônicos, a PDF Confiabilidade mais adequada é a Exponencial Negativa, qual seja: $\mathbf{R} = e^{-\lambda t}$**,** onde λé uma constante denominada Taxa de Falha ou Falibilidade por hora de operação.

- [6] O termo *Reliability* tem em português a tradução Confiabilidade. Já o antônimo de *Reliability* , isto é, *Unreliability,* não tem, em nossos dicionários, um termo correspondente*.* Já vimos tentativas como "Não Confiabilidade" ou Inconfiabilidade, por parte de professores. O termo Inconfiabilidade também não existe em nossos dicionários, mas existe em nosso Vocabulario Ortográfico da Língua Portuguesa. Poderíamos então usar o termo Inconfiabilidade e simbolizá-lo nos cálculos com a letra "I"; mas, optamos, há muito tempo, pelo termo Falibilidade , como correspondente ao termo inglês *Unreliability*. Encontramos sentido por essa opção, consultando o Novo Dicionário da Língua Portuguesa – 3ª. Ed. (2004), do autor Aurélio Buarque de Holanda. Vemos lá que o termo Falibilidade significa "qualidade do falível". No mesmo dicionário, um dos significados do termo falível é: "aquilo que pode falhar". Desse modo, o termo Falibilidade nos parece uma boa escolha. Outra conveniência de usar esse termo é expressa na letra inicial "F", nos cálculos, que nos transmite a ideia de falha (*failure*).

R e F são funções complementares e mutuamente exclusivas porque ou o item falha ou não falha. É lógico então dizer que a probabilidade de o item falhar ou não falhar é 1 (100%). Desse modo, é válida a seguinte relação:

$$\mathbf{R + F = 1} \qquad (1.1)$$

Podemos então escrever:

$$\mathbf{F = 1 - R} \qquad (1.2)$$

Desse modo, em se tratando de sistemas eletrônico/elétricos, tem-se

$$\mathbf{F = 1 - e^{-\lambda t}} \qquad (1.3)$$

A figura 1.1 apresenta as curvas da Confiabilidade e da Falibilidade.

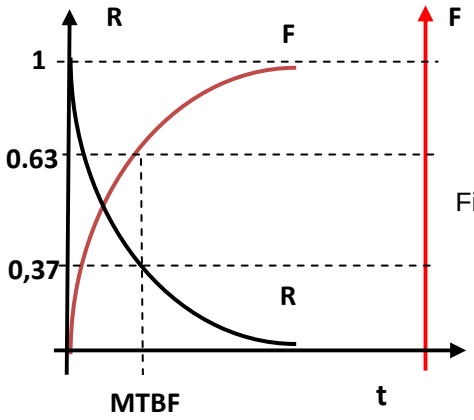


Fig. 1.1– Curvas de R e F

A Fig. 1.1 deixa clara a complementaridade de R e F, isto é, R + F = 1, qualquer que seja t.

O ponto assinalado por MTBF (= **1/λ**) corresponde ao instante cuja probabilidade de falhar (F) é 0,63 (63%), ou a probabilidade de não falhar (R) é 0,37 (37%).

É fácil ver que quando maximizamos F, minimizamos R.

A exponencial negativa tem uma propriedade curiosa, mas importantíssima, conhecida por Propriedade do “Esquecimento” ou da “Perda de Memória”. Com isso, queremos dizer que quando o item que segue essa função é desligado e depois ligado novamente, tudo se passa como se o item estivesse começando a operar pela primeira vez, ou seja, ele “não se lembra” de ter operado antes. A Ref. 1 demonstra essa propriedade matematicamente.

Trata-se de algo que, na prática, se observa com notável nitidez nos itens puramente eletrônicos e elétricos.

Por outro lado, alguém, de certa feita, lembrou, oportunamente, que a exponencial negativa $e^{-\lambda t}$ poderia ser escrita sob a forma de uma série matemática infinita de Taylor da seguinte maneira:

$$e^{-\lambda t} = 1 - \frac{\lambda t}{1!} + \frac{(-\lambda t)^2}{2!} - \frac{(-\lambda t)^3}{3!} + \ldots \qquad (1.4)$$

e percebeu que para $\lambda t < 0{,}1$, e isso ocorre amiúde com sistemas puramente eletrônicos/elétricos, pode-se considerar, como boa aproximação, apenas os dois primeiros termos da série. Portanto,

$$R = e^{-\lambda t} = 1 - \lambda t$$

Tendo em conta a expressão 1.3, podemos escrever para a Falibilidade: $F = 1 - (1 - \lambda t) = \lambda t$.

Destarte, $\mathbf{F = \lambda t}$ (1.5)

Trata-se, convenhamos, da equação mais simples que existe na matemática, ou seja, a equação de uma reta, com coeficiente angula igual a λ. Observe que se t = 1, $\mathbf{F = \lambda}$, que significa: “probabilidade de falhar por hora de operação”.

A (1.5) é fundamental para o Processo de *Safety Assessment*, sendo exaustivamente utilizada nessa atividade.

Nota *– Em Safety Assessment, não utilizamos o conceito de Confiabilidade, mas o de sua função complementar, a Falibilidade, porque, nos cálculos, é muito difícil fazer arredondamentos consistentes, utilizando a Confiabilidade.*

A taxa de falha λ de um item é a grandeza mais importante no Processo de *Safety Assessment*, principalmente para itens eletrônicos/elétricos, porque dada essa taxa, ficam definidas as funções Falibilidade e Confiabilidade desses itens.

1.2.3. Taxa de falha

Mostra a prática que a taxa de falha da equação (1.5), para qualquer tipo de sistema, não é rigorosamente constante. No entanto, em se tratando de itens puramente eletrônicos e elétricos, essa característica é mui aproximadamente constante, praticamente durante toda a vida operacional do sistema.

As figuras 1.2 e 1.3 dão uma ideia da variação da taxa de falha desses dois tipos de itens, numa mesma escala de tempo.

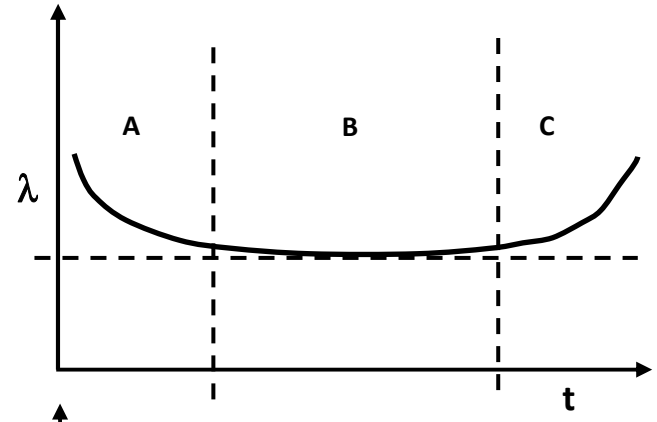


Fig. 1.2 Taxa de Falha típica de itens eletrônicos/elétricos

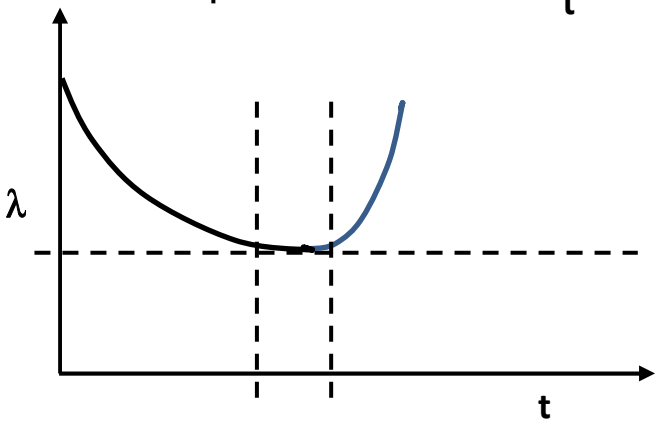


Fig. 1.3 Taxa de Falha típica de itens mecânicos

Na figura 1.2, a região denotada por A é denominada Região de *Debugging,* ou de Mortalidade Infantil, caracterizada por falhas iniciais atribuídas a equívocos no projeto e/ou nos processos de fabricação dos sistemas. A taxa de falha começa alta; mas, depois, as correções de engenharia de projetos e de processos de produção vão proporcionando a redução dessa taxa, até o ponto em que ela começa a ficar aproximadamente constante[7]. É a região B, a chamada fase de projeto maduro, Essa região é caracterizada por falhas aleatórias. É o trecho no qual se aplica a função exponencial negativa e, portanto, a Falibilidade da expressão 1.5. Já a região C é dita

- [7] É o momento em que o sistema é lançado no mercado.

região de desgaste (*wearout*), fase em que a taxa de falha assume uma derivada positiva, isto é, passa a ter valores crescentes.

Como dissemos, a equação $F = \lambda t$ rigorosamente só se aplica bem a sistemas eletrônicos e elétricos, na região de projeto e processos de produção maduros (período operacional), em virtude de terem esses itens, nessa região, taxa de falha aproximadamente constante.

Não é o caso dos sistemas mecânicos, como pode ser observado na figura 1.3, que apresentam apenas uma pequena região de taxa de falha aproximadamente constante. Na maior parte do tempo operacional, a taxa de falha é variável ($\lambda = \lambda(t)$), sendo decrescente na fase inicial, passando pela mencionada pequena região em que é aproximadamente constante, para depois se tornar crescente (fase de desgaste – *wearout*).

Contudo, no cálculo de probabilidades, utiliza-se para os sistemas mecânicos ou híbridos (com dispositivos mecânicos e eletrônicos) a mesma equação utilizada para equipamentos eletrônicos ($F = \lambda t$), mediante a adoção de um determinado artifício.

Trata-se de, uma vez atingida uma taxa de falha satisfatória ou de requisito, considerar que é a taxa de falha do item. O *debuggin*g, no entanto, deve continuar, até que se constate que a taxa de falha começa a parar de descrescer, anunciando que a região de desgaste (*wearout*) já está próxima. Nessas condições, o artifício é seguro. Mas, por uma questão de cautela, procura-se evitar os efeitos prematuros de desgaste, por meio de inspeções, para verificar o estado do sistema, ou estabelecer limites de vida (*life time*), na chamada manutenção preventiva preditiva, para o sistema ou para o equipamento responsável pela falha do sistema.

1.2.4. Operando com Probabilidades (Álgebra de Boole)

É imprescindível que saibamos como operar com probabilidades, em virtude de sua aplicabilidade nas ferramentas de análise quantitativas, como teremos a oportunidade de mostrar mais adiante.

Antes de tudo, devemos entender o que seja um evento, no Processo de Safety Assessment. Um evento é o sucesso de uma missão ou um insucesso (falha ou mau

funcionamento de um sistema). Desse modo, só há dois possíveis eventos de nosso interesse: falha e sucesso. Este é o nosso universo.

Começamos com os chamados axiomas da probabilidade. São eles (Ref. 1):

- $0 < P[A] < 1$;
- se A é um evento certo, P[A] = 1. Desse modo, P[S] = 1, i.e, a probabilidade de falhar ou não falhar é 1, uma vez que ou o item falha ou não falha;
- se ϕ é um evento de ocorrência impossível[8], então $P[\phi] = 0$;
- se A, B, C, ..., A_N são eventos independentes, então $P[A \cup B \cup C \cup ... \cup A_N] = P[A] + P[B] + P[C] + ... P[N]$;
- se A, B, C, ..., A_N são eventos independentes, então $P(A \cap B \cap C \cap ... \cap A_N) = P[A] . P[B] . P[C], ..., P[N]$;

Dois eventos A e B são independentes, quando a ocorrência de um deles não afeta a probabilidade de ocorrência do outro. Neste caso, escreve-se: P[A|B] = P[A], e lê-se: “a probabilidade de ocorrer A dado que ocorra B antes, é igual à probabilidade de ocorrer A, isto é, a ocorrência de B não interfere na ocorrência de A”.

Se a ocorrência de B provocar a ocorrência de A, então A e B não são independentes. Neste caso, escreve-se: $P[A \cup B] = P[A] + P[B] – P[A \cap B]$ e escreve-se P[A] + P[B] = P[A] + P[B] – P[A]. P[B].

[8] Exemplo de um evento impossível: Saltar de um lado a outro de uma avenida.

Capítulo 2 FERRAMENTAS DE ANÁLISE MAIS UTILIZADAS NO PROCESSO DE *SAFETY ASSESSMENT.*

Neste capítulo, você vai saber quais são as ferramentas de análise mais empregadas em cada etapa do Processo de Safety Assessment, servindo de introdução para o estudo propriamente dito dessas ferramentas, no Capítulo 3.

2.1. AS FERRAMENTAS DE ANÁLISE MAIS UTILIZADAS EM CADA ETAPA DO PROCESSO DE SAFETY ASSESSMENT

Preliminarmente, devemos deixar claro que as ferramentas que vamos apresentar neste capítulo não são de uso obrigatório. O Aplicante (requerente de certificação) pode usar a ferramenta que melhor lhe aprouver, desde que a Autoridade de Certificação concorde. É só isso. Todavia, as ferramentas aqui apresentadas já são historicamente aceitas pela Autoridade.

As ferramentas de análise já citadas no Capítulo 1 não se aplicam, necessariamente, a todas as fases ou etapas do Processo de Safety Assessment. Vamos mostrar, a seguir, quais são as etapas em que essas ferramentas são empregadas. Em seguida, ou seja, no Capítulo 3, trataremos especificamente do processo de cada ferramenta, mostrando como se trabalha com elas, por meio de exemplos. Acreditamos que, com esse roteiro, atinjamos o propósito deste trabalho.

Estaremos procurando, como sempre, ser eficazes, isto é, escrever só o que deve ser escrito (concisão), e eficientes, ou seja, além de escrever só o que tem de ser escrito, procurar, tanto quanto possível, escrever de maneira clara (precisão) e correta (correção). “Dureza!”.

Uma coisa que devemos deixar clara é que estaremos sempre utilizando a nomenclatura inglesa, quando tratarmos das ferramentas, mas sem deixar de esclarecer seu significado em português, na primeira oportunidade que citarmos a ferramenta. Essa atitude de usar a nomenclatura inglesa deve-se ao fato de que, na prática aeronáutica, usa-se mais a terminologia inglesa que a portuguesa, pelo simples fato de ser a nomenclatura técnica desse idioma quase universalmente utilizada.

2.1.1. Ferramentas Utilizadas na *Functional Hazard Assessment* (FHA) Nível Aeronave (AFHA);

A FHA Nível Aeronave (AFHA), como mencionado no Capítulo 1, é a primeira etapa ou avaliação do Processo de Safety Assessment. Ela é fundamental, isto é, imprescindível para o desencadeamento do inteiro processo; sendo mais enfático: o processo não vai adiante sem que se realize a etapa da AFHA, porque é nessa análise que se alocam os requisitos de *safety* da Autoridade às funções da aeronave, dos quais se derivam os requisitos que serão alocados aos sistemas que vão realizar essas funções.

Já podemos dizer de pronto, que, nessa etapa, não há obrigatoriedade de emprego de nenhuma das ferramentas tratadas neste trabalho. Deixaremos isso claro mais adiante.

Por outro lado, devemos ter sempre em mente que a base para a AFHA é a análise funcional realizada pela Engenharia de Sistemas (ES), logo no início do projeto da aeronave (Fase Conceitual). O resultado dessa análise é o elenco de todas as funções da aeronave.

A equipe que realiza a AFHA verifica o potencial efeito na tríade “tripulação, aeronave e passageiros”, em termos de *safety*, que possa resultar, na hipótese de perda ou mau funcionamento de cada função do elenco das funções identificadas pela ES.

A AFHA é desenvolvida por meio do seguinte questionamento e raciocínio:

“Qual seria o potencial efeito na tríade tripulação (principalmente os pilotos), aeronave e passageiros, se ocorrer uma perda ou mau funcionamento de uma função nível aeronave? O potencial efeito mais grave é o de **severidade *Catastrophic*** (catastrófica), que significa perda da aeronave e de seus ocupantes ou ferimentos graves. Se a perda da função ou mau funcionamento da mesma tiver um potencial efeito de gerar muito trabalho da tripulação para controlar a aeronave, podendo até haver ferimentos, mas ainda assim for possível conduzir a aeronave até o pouso, **a severidade seria *Hazardous*** (Perigosa)**.** Se o potencial efeito é dar mais trabalho que o habitual, mas ter ainda o piloto no controle da aeronave, e os ocupantes só sentirem algum desconforto, a severidade seria ***Major*** (Maior); e, por fim, se não houvesse nenhum efeito na segurança, a severidade ***No Safety Effect*** (Nenhum Efeito).

Para cada severidade, a Autoridade estabelece um requisito qualitativo e um correspondente requisito quantitativo (probabilístico) – (Ref.2). Esse processo é chamado de Alocação de Requisitos de Segurança às Funções Nível Aeronave.

Os resultados da AFHA são inseridos numa tabela com formato já bem estabelecido. Um exemplo é mostrado no Apêndice.

Apesar de não haver necessidade de utilizar ferramentas dedicadas, pode-se, no entanto, utilizar uma FTA ou uma DDA, para ajudar no trabalho do analista, mostrando as funções da aeronave cuja perda ou mau funcionamento conduzem ao evento de topo *catastrophic* “perda da aeronave”, ou a eventos de topo de severidade *Hazardous* ou *Major,* inseridos na mencionada tabela. Isso ajuda o analista, mas, como já dissemos, não é necessário apresentá-la à Autoridade. Portanto, a aplicação da FTA ou DDA, na AFHA, é facultativa.

2.1.2. Ferramentas Utilizadas na *Functional Hazard Assessment* (FHA) Nível Sistema (SFHA)

A SFHA parte dos resultados da AFHA, isto é, dos requisitos alocados a cada função nível aeronave, para definir os meios que irão realizar essas funções, alocando a cada um desses meios requisitos de segurança decorrentes daqueles alocados às funções da aeronave.

Para realizar isso, temos de aplicar a ferramenta *Fault Tree Analysis* (FTA), que permite, de maneira lógica, transladar os requisitos de segurança alocados às funções nível aeronave para esses meios que caracterizarão os sistemas.

Uma alternativa à FTA poderia ser a DDA; no entanto, a FTA é, de longe, a mais utilizada.

2.1.3. Ferramentas Utilizadas na *Preliminary System Safety Assessment* (PSSA)

Nesta etapa, são definidos os sistemas candidatos existentes no mercado, que caracterizarão os meios que realizarão as funções nível aeronave, de acordo com o conhecimento que a Engenharia de Sistemas da empresa tem a respeito de tais sistemas. Usando ainda a FTA ou a DDA, a PSSA estabelece, para cada candidato a sistema da aeronave, os requisitos decorrentes da SFHA, que servirão para a Engenharia de Sistemas encaminhar ao setor de procura e compra (*Procuring*) a lista

das empresas que poderão fornecer os referidos sistemas, apresentando àquele setor os requisitos de segurança decorrentes da PSSA, que deverão ser incorporados ao pedido de proposta (*Requirements for Proposal - RFP*) encaminhado a cada fornecedor indicado.

2.1.4. Ferramentas Utilizadas na *System Safety Assessment* (SSA)

Com base nos requisitos estabelecidos pela PSSA com os recursos da FTA (ou DD), o setor de procura e compras encaminha o chamado *Request for Proposal* (RFP) aos potenciais fornecedores dos sistemas, impondo-lhes, no caso do *Safety Assessment*, os requisitos estabelecidos pela FTA da PSSA, pertinente à taxa de falha máxima desses sistemas. Normalmente, o fornecedor demonstra o atendimento a esses requisitos por meio de uma *Failure Modes, And Effects Analysys* (FMEA).

Devemos, no entanto, ter em conta que uma FMEA para um sistema dito complexo[9], muitas vezes é impossível de ser realizada, ou, se realizada, apresenta-se inconclusiva. Falaremos mais sobre isso, quando tratarmos especificamente da FMEA.

O Processo de *Safety Assessment* encerra-se com a escolha do fornecedor que demonstre cumprir os requisitos de segurança, por meio da FMEA. Com as informações de cumprimento dos requisitos de segurança, o Aplicante ou Requerente (empresa que desenvolve a aeronave) atualiza a FTA da PSSA, que passa a ser a FTA definitiva do processo. Isto feito, encaminha à Autoridade o relatório da SSA com os resultados da FMEA e a FTA atualizada, encerrando então o Processo de *Safety Assessment*, se não houver contestação por parte da Autoridade.

- [9] Grande parte dos modernos sistemas aviônicos.

Capítulo 3 ESTUDO DAS PRINCIPAIS FERRAMENTAS UTILIZADAS NO PROCESSO *DE SAFETY ASSESSMENT*

Neste capítulo, você vai aprender a trabalhar com as ferramentas mais utilizadas no Processo de Safety Assessment, condição indispensável para participar de um Processo de Safety Assessment.

3.1. *FAULT TREE ANALYSIS* (FTA)

A FTA poderia perfeitamente denominar-se *Failure Tree Analysis*, uma vez que, na tradução habitual, a comunidade aeronáutica sempre diz “Análise por Árvore de Falhas”.

No entanto, é mister esclarecer que existe uma diferença entre os termos *failure* e *fault*. De fato, se consultarmos a norma ABNT 5462 (Confiabilidade e Mantenabilidade), vamos constatar que *failure* é um evento, isto é, ele acontece e pronto. Por outro lado, *fault* é um estado, ou seja, uma vez ocorrido o evento *failure*, o item entra no estado de *fault*, até ser reparado e retornar à operação, ou simplesmente ser descartado. Simples, não?

O termo *fault* é traduzido na norma para o termo português pane[10] e para o termo francês *panne*. Entretanto, neste trabalho, vamos nos associar à maioria que considera os dois termos como sinônimos e diremos simplesmente: “Análise por Árvore de Falhas (FTA)”, e ponto final.

A FTA é uma análise dedutiva, ou seja, postula-se um evento indesejável para um sistema, denominado Evento de Topo, e deduzem-se as possíveis causas desse evento. Costuma-se dizer que se trata do método dos detetives, isto é, que partem de um resultado indesejado (assassinato, por exemplo) e buscam os culpados (causas).

Nessa análise, incluem-se falhas de um sistema (perda da função ou mau funcionamento de algum equipamento desse sistema), ou até mesmo falha humana.

[10] De fato, em nossa longa experiência na manutenção de aeronaves, todo item que chegava falhado para a manutenção era dito estar em pane. O item só saia do estado de pane depois de reparado e colocado pronto para operar novamente.

E agora vem o mais importante sobre a FTA. A análise é uma representação gráfica dos vários eventos que podem conduzir ao evento de topo. A Fig.3.1 apresenta a simbologia utilizada, sintetizada em três grupos: Símbolos de Eventos Primários (*Primary Events Symbols*), Símbolos de Eventos Intermediários*(Intermediate Event Symbols*), Símbolos de Portas (*Gate Symbols*) e Símbolos de Transferência (*Transfer Symbols*).

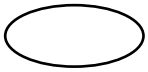
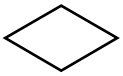
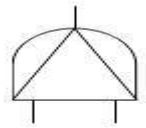
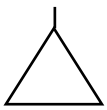
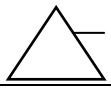
Símbolos de Eventos Primários	
	**Evento Básico** ou **Suficiente**– Evento ou modo de falha interna de um sistema, podendo ou não requerer ulterior investigação.
	**Evento Condicional** – Uma condição que é necessária para o modo de falha ocorrer.
	**Evento Não Desenvolvido** – Evento que não é ulteriormente desenvolvido porque tem impacto desprezível no nível superior ou porque não se tem informações disponíveis sobre ele.
Símbolo Intermediário	
	**Caixa de Descrição** – Descrição de um *output* (saída) de uma porta lógica.
Portas Lógicas	
	**AND (E)** – Porta lógica Booleana – O *output* de falha só ocorre se todos os *inputs*(entradas) de falha na entrada ocorrerem.
	**OR (OU)** – Porta lógica Booleana – O *output* de falha ocorre quando pelo menos um *input* de falha ocorrer.
	**OR Exclusivo** – Porta lógica Booleana – O *output* de falha ocorre se um determinado *input* de falha ocorrer.
	**AND de Prioridade** – Porta lógica booleana – O *output* de falha ocorre se os *inputs* de falhas ocorrerem em uma determinada sequência (a sequência é representada por um evento condicional desenhado à direita da porta).
Símbolos de Transferência	
	**Transferência de Entrada –** Entrada de um evento num ramo proveniente de outro ramo indicado pelo símbolo de Transferência de Saída.
	**Transferência de Saída –** Saída de um evento de um ramo da árvore para um outro ramo da árvore.

Fig. 3.1 – Simbologia adotada para a FTA

No que tange aos eventos primários, vamos, numa primeira etapa, concentrar-nos naqueles mais usados num Processo de *Safety Asse*ssment. São eles: o símbolo de Evento Básico, representado por um círculo, e o símbolo de Evento Não Desenvolvido, representado por um losango, repetidos na Fig. 3.2.

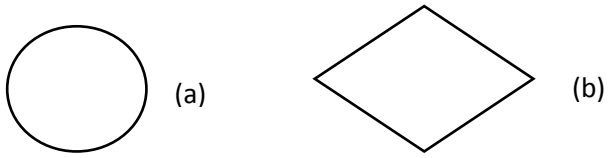


Fig 3.2 (a) – Evento Básico; (b) Evento não Desenvolvido

No Processo de *Safety Assessment*, a FTA é desenvolvida até chegar a um evento de falha de um sistema cuja responsabilidade de análise é do fornecedor desse sistema e não dos analistas do Processo de *Safety Assessment* da empresa integradora do sistema na aeronave (Aplicante ou Requerente do Processo de Certificação). A falha de cada um desses sistemas é chamada de **Evento Básico (a)** porque ele dá início ao desencadeamento de outros eventos de falha, que se propagam pela árvore com influência no evento de topo.

O **Evento Não Desenvolvido (b)**, por sua vez, simboliza um evento de falha que não tem nenhuma influência significativa para os ramos superiores na árvore de falhas.

No que tange aos símbolos de portas lógicas, eles representam o mecanismo de propagação de eventos de falhas, presentes nas entradas dessas portas, tendo na saída as consequências das falhas na entrada registradas em símbolos intermediários, os retângulos denominados **Caixa de Descrição** (v. Fig. 3.1).

As portas lógicas mais usadas são as portas **OU** e **E.** Normalmente, deveríamos representar essas portas com sua saída e com suas várias entradas, usando os seguintes símbolos (Fig. 3.3):

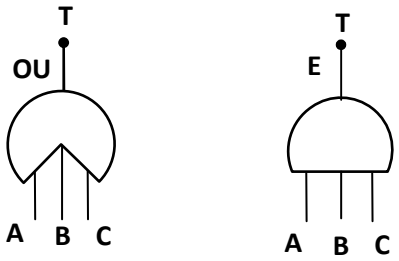


Fig.3.3 – Portas **OU** e **E**, no formato convencional

Todavia, por uma questão de clareza da figura, costuma-se usar o formato dito alternativo, mostrado na Fig. 3.4.

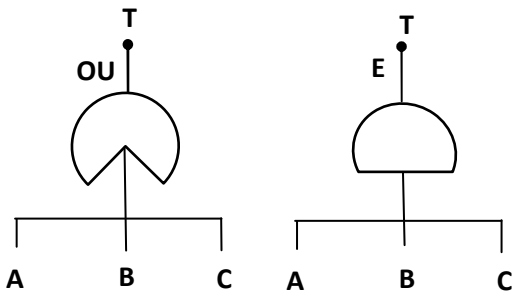


Fig.3.4 – Portas **OU** e **E**, no formato alternativo

Interessam-nos ainda os símbolos de transferência, mostrados na Fig. 3.5.

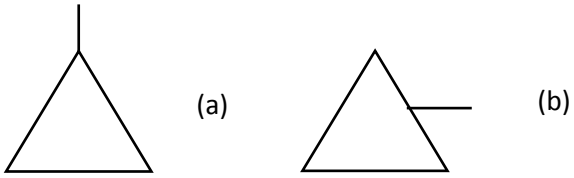


Fig. 3.5– (a) Transferência de Entrada; (b) Transferência de Saída

O símbolo de Transferência de Entrada (a) assinala a entrada num ramo da árvore de um evento que acontece também num outro ramo da árvore, com transferência evidenciada por um símbolo de Transferência de Saída (b). A cada símbolo de Transferência de Entrada corresponde um símbolo de Transferência de Saída. Por exemplo, o evento perda de alimentação elétrica, que normalmente se reflete em um ou mais ramos da árvore.

Voltemos nossa análise para as características de uma FTA. Ela pode ser qualitativa, isto é, mostrar apenas a conexão entre os eventos, a partir do evento de topo, ou quantitativa, isto é, considerando faixas de valores de probabilidades pertinentes à Falibilidade (F) de cada evento.

Vamos então nos deter na lógica de construção de uma FTA (qualitativa e quantitativa), por meio de exemplos, para o leitor se sentir seguro no desenvolvimento de uma ou outra etapa do processo às quais a FTA se refira.

Vamos apresentar dois exemplos, um relativo a um sistema de nosso cotidiano, isto é, não utilizados em aeronaves, mas nos prédios residenciais; o chamado Sistema de Bombeamento de Água. Em seguida, trataremos de um exemplo aplicado a um sistema aeronáutico, qual seja, o Sistema de Informações Primárias de Voo.

Exemplo 3.1 – Sistema de Bombeamento de água

O sistema é constituído de um reservatório d'água, no solo, bombas para o bombeamento de água para a caixa no topo do prédio e sensoriamento e controle do nível de água nessa caixa, muito comum nos prédios de apartamentos ou prédios comerciais.

Observa-se que se trata de um sistema de dois ramos de bombeamento de água, formando um sistema dual, ou seja, com uma redundância, e de um dispositivo de sensoriamento e controle (sensor/controle) do nível de água, na caixa d'água **C**. O sistema é constituído pelos componentes bombas (duas) e sensor/controle. O reservatório, a caixa C e a alimentação elétrica não fazem parte do sistema (já estavam instalados na edificação como parte do projeto).

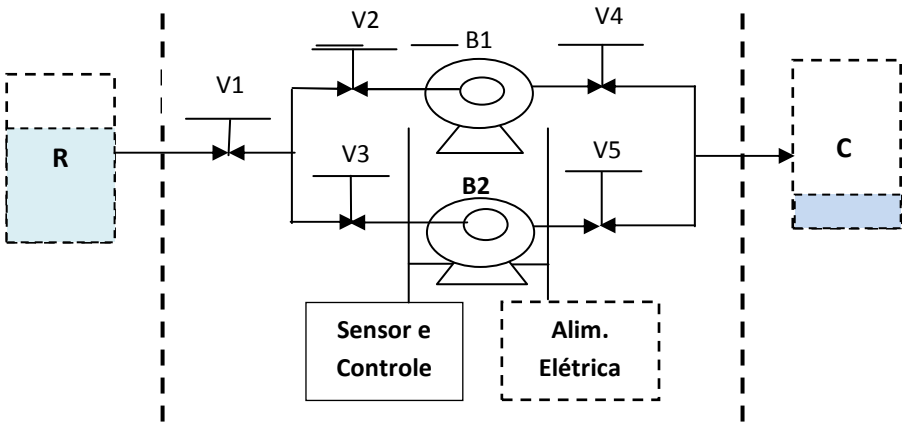


Fig. 3.6 – Diagrama Físico de um Sistema de Bombeamento de Água de um Edifício.

Para facilitar nosso raciocínio, consideremos que as válvulas (registros) V_x sejam ideais, isto é, que estejam sempre no estado necessário para liberar a passagem de água. Supomos também que sempre haja água no reservatório **R**.

Como se vê, o diagrama físico é desenhado com símbolos representativos dos componentes físicos do sistema, mostrando, claramente, a interligação desses componentes. É como deveria ser apresentado no manual de manutenção do sistema.

Para indicar que a alimentação elétrica, o reservatório e a caixa d'água não pertencem ao sistema de bombeamento, isto é, são providos pelo projeto de construção do prédio, os inserimos em retângulos tracejados na Fig. 3.6.

Antes de desenvolver uma FTA relativa a esse sistema, é imperioso que entendamos seu funcionamento físico.

O primeiro passo é a análise funcional, isto é, a identificação das funções, realizadas pela engenharia da empresa que desenvolve o projeto. As funções do sistema são:

(1) Prover sensoriamento do nível de água na caixa d'água **C**, realizada por meio de um sensor (boia);

(2) Prover controle do bombeamento de água, realizada por um dispositivo tipo relé, comandado pela bóia, que interrompe a continuidade da alimentação elétrica para as bombas de água, se o sensor indicar que o nível máximo da caixa **C** foi atingido; ou dando continuidade à alimentação elétrica para as bombas, quando o nível mínimo de água for "percebido" pelo sensor (boia).

(3) Prover bombeamento de água de um reservatório **R,** no solo, encaminhando-a para a caixa **C**.

Para construir a FTA, é prudente ter uma cópia da página 18 (Fig. 3.1) em mãos, para entendermos os símbolos que serão empregados.

Questionamento fundamental: Qual é o evento de topo? **Resposta**: Falta de água na caixa **C**.

- **Pergunta-se**: O que poderia impedir o envio de água para a caixa? **Resposta**: O não bombeamento por ambos os ramos de bombeamento de água.
- **Pergunta-se**: O que poderia impedir o funcionamento do bombeamento de ambos os ramos de bombeamento? **Respostas**:

  (a) Falha do sensor (boia) que verifica o nível de água ou do relé;

  (b) falha do dispositivo de controle (tipo relé);

(b) falha das bombas B1 **e** B2.

(c) ausência de alimentação elétrica, o que faria o sistema inteiro entrar em colapso.

A FTA qualitativa é mostrada na Fig.3.7.

Para verificar se estamos corretos na construção da árvore, devemos ter em mente que numa porta **OU** o evento de saída (neste caso o evento de topo) acontece quando pelo menos numa de suas entradas estiver presente uma falha.

Por exemplo, se falhar a alimentação elétrica, o sistema, mesmo íntegro (sem falha), não opera, não sendo, portanto, enviada água à caixa **C**, mesmo que as bombas **B1** e **B2** e o sensor/controle estejam operacionais.

Ainda, se o sensor ou o controle falharem, as bombas não serão acionadas, e não haverá então fluxo de água para a caixa **C**, mesmo que as bombas e a alimentação elétrica estejam normais.

Por outro lado, se uma das bombas falhar, a outra assumirá a função de bombeamento, e o sistema, como um todo, continuará operando, Mas se ambas as bombas falharem, não será enviada água à caixa **C**, mesmo que tudo o mais (alimentação elétrica e sensor/controle) esteja funcionando. Tecnicamente dizemos: se $\mathbf{B_1}$ **e** $\mathbf{B_2}$ falharem, haverá falha total de bombeamento. A porta lógica utilizada é então a porta **E** (B1 **E** B2 falham)

Vamos utilizar agora a álgebra booleana para apresentar a equação da Falibilidade do sistema. Consideremos, para isso, que as letras maiúsculas $\mathbf{F_T}$, $\mathbf{F_A}$, $\mathbf{F_B}$, $\mathbf{F_{B1}}$, $\mathbf{F_{B2}}$ **e** $\mathbf{F_C}$, são probabilidades de falha das funções.

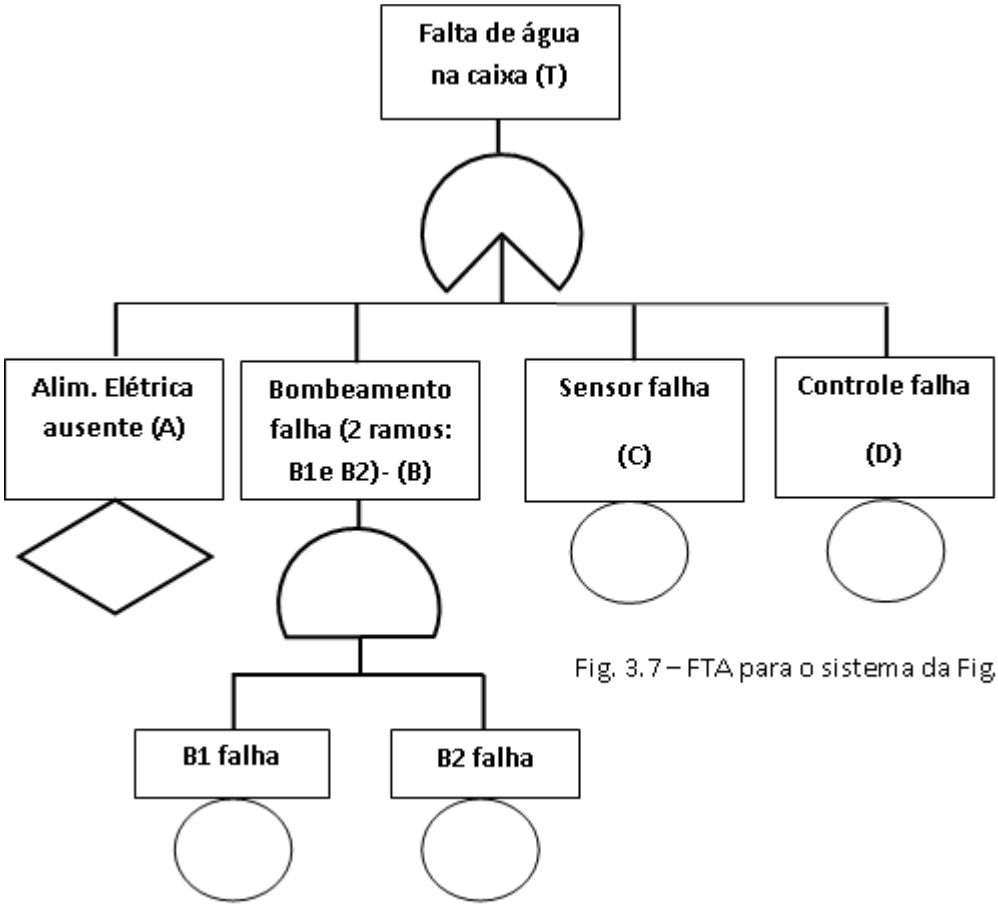


Fig. 3.7 – FTA para o sistema da Fig. 2.

Temos:

$F_T = F_A + F_B + F_C + F_D$ (porta **OU**). Por outro lado, **$F_B = F_{B1} . F_{B2}$(porta E)**. Portanto, **$F_T = F_A + (F_{B1}.F_{B2}) + F_C + F_D$.**

A análise está completa, mas resta ainda um esclarecimento: note os símbolos de Eventos Básicos (círculos), indicando que a responsabilidade para analisar os eventos aos quais se ligam esses símbolos é dos fabricantes das bombas e sensor/controle.

Observe também o triângulo, alocado antes do evento de falha da alimentação elétrica. Indica que não estamos interessados na análise de falha da alimentação elétrica, que é fornecida pela empresa responsável pelo seu fornecimento.

Acreditamos, enfim, que o exemplo tenha sido elucidativo, para um primeiro passo, visando o entendimento de construção de uma FTA; mas, agora, vamos a um exemplo de um sistema moderno instalado nas aeronaves (militares e civis) com o qual, sem dúvida, um analista no Processo de *Safety Assessm*ent de um projeto de uma aeronave vai ter de lidar.

Exemplo 3.2 – FTA de um Sistema de Informações Primárias de Voo

Trata-se um sistema muito utilizado em aeronaves modernas: **Sistema de Informações Primárias de Voo** *(Flight Primary Information System).* Entre outras informações, o sistema apresenta, num display eletrônico (*Primary Flight Display* – PFD), as chamadas informações primárias de voo, quais sejam: *altitude* (altitude), *attitude (*atitude), *airspeed* (velocidade) e *heading (*direção). A perda de uma das três primeiras tem potencial catastrófico em condições IMC (*Instrument Meteorological Conditions*), isto é, pode provocar a perda da aeronave e, consequentemente, dos seus ocupantes. Exatamente por isso, o sistema tem de ter, no mínimo, uma redundância, formando um sistema dual, tendo um sistema simples para o piloto - denominado Principal (P), e outro para o co-piloto - denominado Secundário (S).

Essa dualidade de sistemas P e S é uma imposição da Autoridade, baseada no chamado Critério da Falha Única (Ref. 2), ou seja: “Não pode ocorrer um evento catastrófico, em virtude de uma única falha no sistema”.

Cada sistema simples é constituído por sensores, transdutores e interfaces de processamento dos sinais provenientes dos sensores, dois Barramentos de Dados (*Data Bus*) e um *display* eletrônico (PFD).

Os sinais de *Attitude* e *Heading* são gerados e processados no AHRS (*Attitude, Heading Reference System*) e encaminhados ao PFD, por meio do Barramento de Dados, na forma aceitável por esse display. Os sensores, no interior do AHRS, são do tipo inercial, isto é, não dependem de informações externas. Estão ali sensores para a *Attitude,* ou seja*,* três giroscópios de *laser* (*Ring Laser Gyroscopes*) de altíssima confiabilidade, um para cada eixo ortogonal (xyz). Os sensores de deslocamento (*Heading*) são três acelerômetros (*accelerometers*), também de altíssima confiabilidade, um para cada eixo ortogonal. Tudo isso no interior do AHRS.

Por outro lado, as informações como *Altitude e Airspeed* são geradas a partir de dados do ar externo, captados por um Tubo de Pitot, tratados, em seguida, por um sensor barométrico, hoje do estado sólido, e encaminhados ao ADC (*Air Data Computer*), na forma conveniente, para processamento e encaminhamento aos barramentos e daí para o PFD.

Cada sistema simples (P e S) tem seus próprios sensores, transdutores, processadores e *display*, isto é, Tubo de Pitot, Sensor Barométrico, AHRS, ADC e PFD,

Vamos agora à FTA do sistema dual, apresentada na Fig. 3.8.

O evento de topo de nosso interesse é a falha na apresentação de uma ou mais das chamadas Informações Primárias de Voo (*Flight Primary Information*), caracterizando um evento de severidade catastrófica, razão pela qual a Falibilidade F do evento de topo deve ser menor que 4.10^{-9}, considerando um vôo com média de duração de 4 horas.

Para que ocorra o evento de topo, é necessário que ocorra a falha de cada sistema simples (P **e** S), daí a utilização da porta **E.** Sendo eventos que surgem na entrada de uma porta **E**, a Falibilidade de cada um deve ser menor que 2.10^{-5}, para esses sistemas satisfazerem o requisito, porque $F = F_P \cdot F_S = 2.10^{-5}. 2.10^{-5} = 4.10^{-10} < 4. 10^{-9}$.

Para que ocorra a falha do sistema P **ou** S, é necessário que ocorra a falha de seus respectivos PFD **ou** AHRS **ou** Tubo de Pitot **ou** ADC **ou** Sensor Barométrico; daí o uso da porta **OU** para ambos os subsistemas**.** Sejam então $\mathbf{F_D, F_A, F_T, F_C, F_B}$ as respectivas Falibilidades desses itens. Como eles estão na entrada de uma porta **OU**, as respectivas Falibilidades se somam, e a soma das mesmas tem de ser igual ou menor que 2.10^{-5}.

Observem os símbolos de eventos básicos representados pelos círculos, indicando que os eventos na saída deles são analisados pelos fabricantes ou fornecedores dos subsistemas[11], sensores, transdutores. Os eventos básicos são as falhas do PFD, AHRS, Tubo de Pitot, ADC e Sensor Barométrico.

Esses fornecedores é que deverão demonstrar que seus subsistemas, sensores e transdutores cumprem os requisitos de segurança estabelecidos pela empresa que está conduzindo o Processo de *Safety Assessment*.

[11] **Uma questão de nomenclatura** – Estamos utilizando pela primeira vez o termo "Subsistema", para caracterizar que se trata de parte de um sistema, que, no caso, é o Sistema de Apresentação de Informações Primárias de Voo. Esses subsistemas ainda poderão ter suas próprias partes, ou seja, equipamentos; e estes seus módulos com seus componentes (peças).

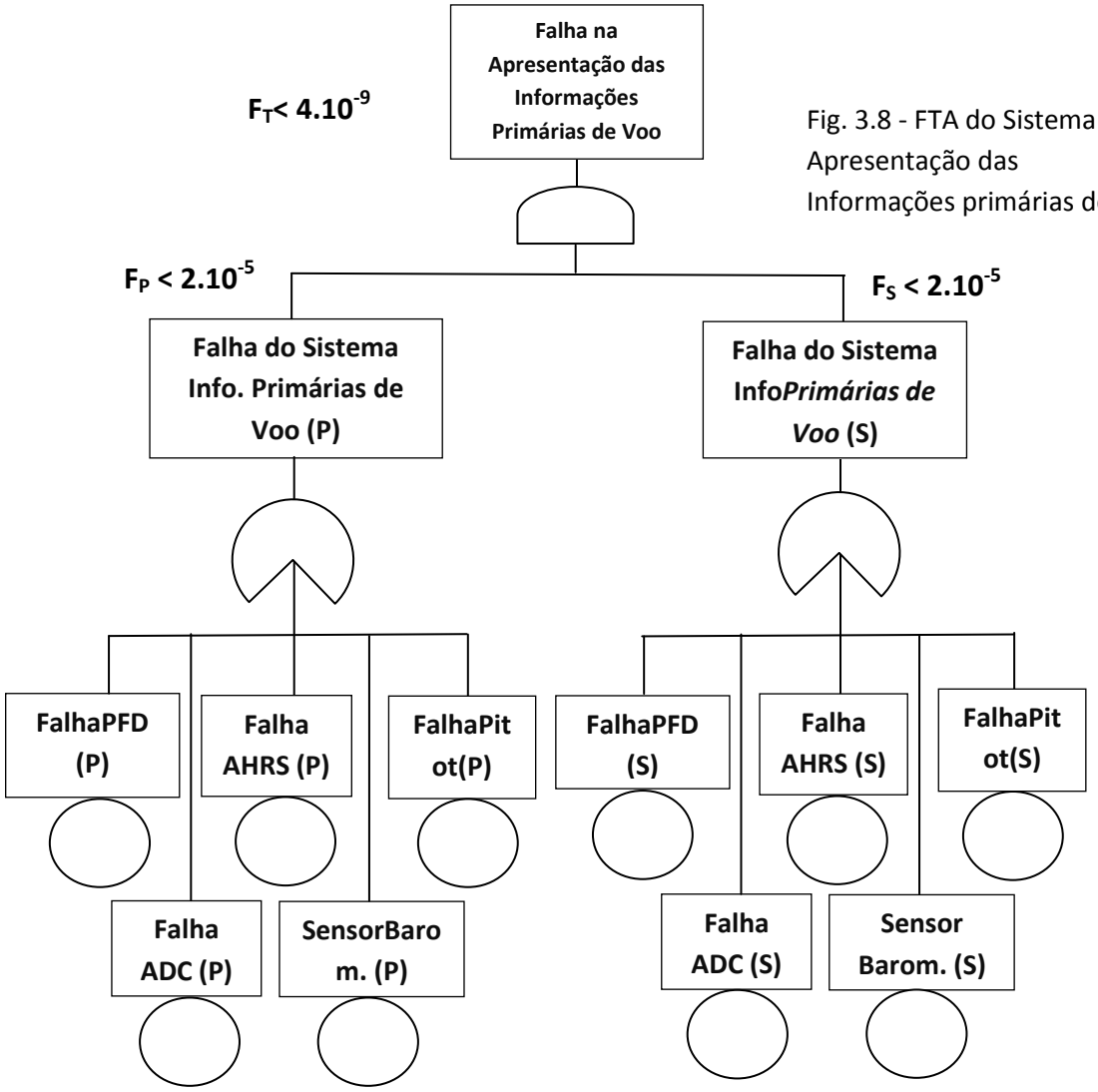


Fig. 3.8 - FTA do Sistema de Apresentação das Informações primárias de

3.2. *DEPENDENCE DIAGRAMS ANALYSIS* (DDA)

Como já dissemos, a FTA e a DDA são intercambiáveis, ficando a critério do analista usar uma ou outra. Particularmente, preferimos a FTA; mas, vamos agora tratar da DDA.

A DDA utiliza o RBD (*Reliability Blocks Diagram*) da Confiabilidade, mas aplicado à Falibilidade, isto é, em cada bloco se insere a Falibilidade, em vez da Confiabilidade[12], uma vez que no *Processo de Safety Assessment* estamos interessados na Falibilidade e não na Confiabilidade.

A DDA usa retângulos com os componentes do sistema em série ou em paralelo. A Fig.3.9 mostra a lógica geral da construção.

[12] Lembrando que **F = 1 – R.**

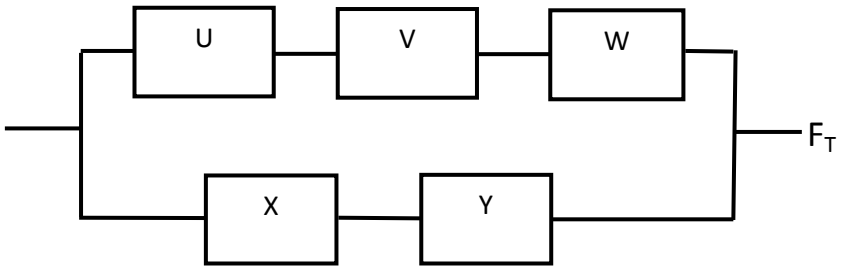


Fig. 3.9 – Lógica de construção de uma DDA

Importante assinalar que a ordem dos eventos de cada ramo não altera o resultado, ou seja, tanto faz colocar numa certa ordem de dependência funcional ou não. Desse modo, poderíamos ter inserido os blocos do ramo superior de seis maneiras diferentes, quais sejam: UVW, UWV, VUW, VWU, WUV e WVU. Da mesma forma, no ramo inferior: XY ou YX.

Porém, quando se trata de um diagrama funcional, como veremos na ferramenta FMEA, a ordem dos blocos funcionais tem uma relação de dependência funcional, isto é, a sequência dos blocos é única.

Pode-se, de pronto, mostrar como se relaciona a FTA com a DDA. Note que o ramo com os blocos U, V, W, em série na DDA, segue a lógica da porta **OU,** na FTA, isto é, basta estar presente uma falha em um dos blocos para falhar todo o ramo UVW. O mesmo se aplica aos blocos X e Y, no ramo XY.

Já os ramos UVW e XY, em seu conjunto, seguem a lógica da porta **E**, ou seja, é necessário que ambos os ramos falhem para ocorrer o evento de topo T. Desse modo, se passarmos para a FTA, o diagrama seria como na Fig. 3.10.

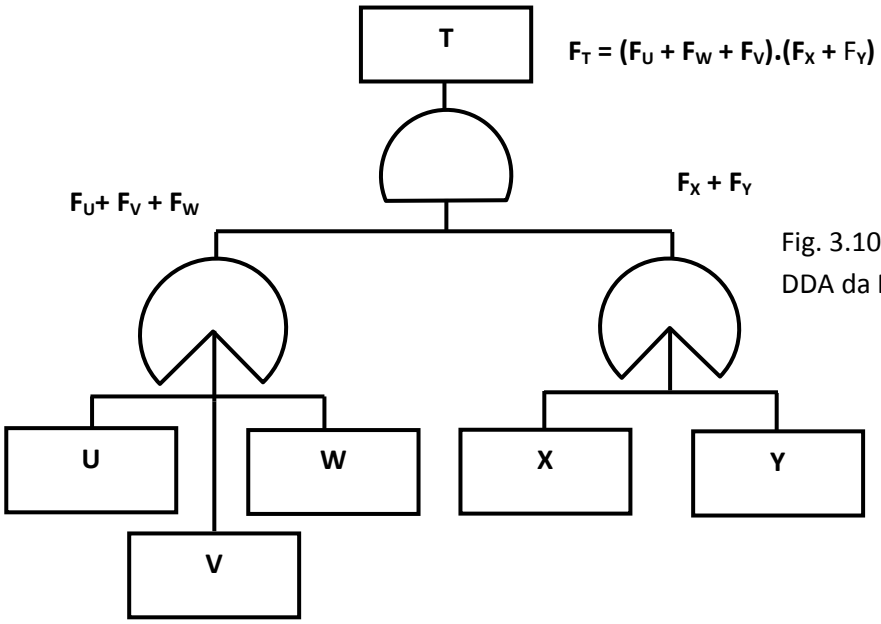


Fig. 3.10 – FTA correspondente à DDA da Fig. 3.9

Vamos agora passar da FTA do sistema de bombeamento da Fig. 3.2 para a DDA da Fig. 3.11.

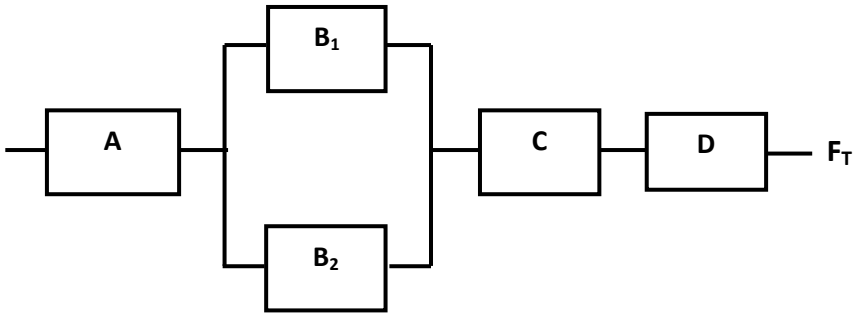


Fig. 3.11 – DDA correspondente à FTA da Fig. 3.2 (Sistema de

O diagrama deixa claro que o sistema falha se houver falha de **A ou B** (ambas as bombas B_1 e B_2) **ou C ou D**. A equação é $\mathbf{F_T = F_A + (F_{B1}.F_{B2}) + F_C + F_D}$, como já apresentado no exercício 3.2 da FTA.

Notem que a FTA traz uma informação adicional, mostrando a responsabilidade dos fornecedores dos subsistemas ou equipamentos que desencadeiam as falhas numa FTA, por meio de símbolos de Evento Básico (círculo). Isso até pode ser contornado na DDA, por meio de considerações a respeito dessa responsabilidade dos fornecedores.

Passemos à apresentação da DDA do sistema aviônico da Fig. 3.8. Para facilitar, repetimos aqui aquela figura.

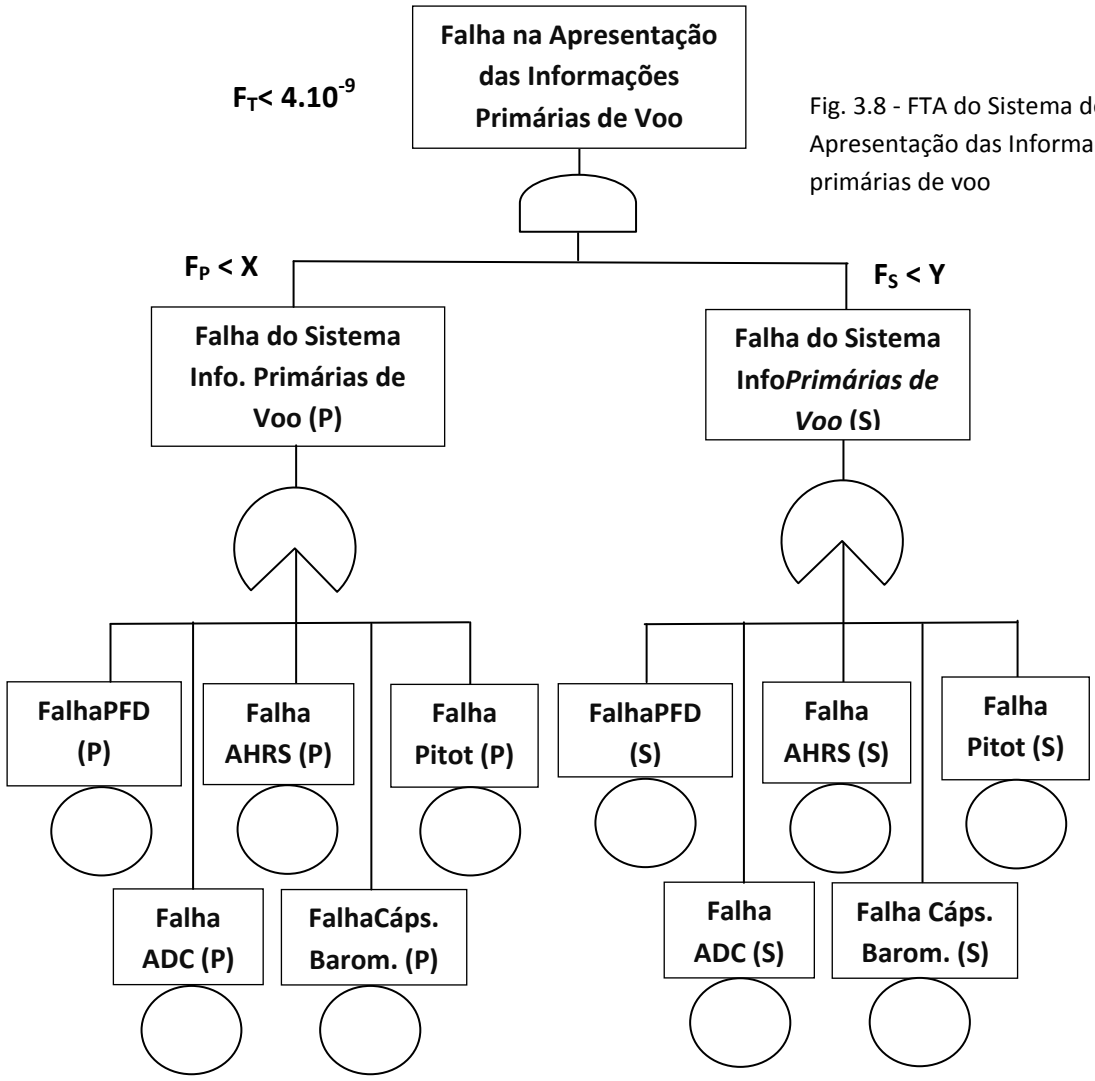


Fig. 3.8 - FTA do Sistema de Apresentação das Informações primárias de voo

A respectiva DDA é apresentada na Fig. 3.12.

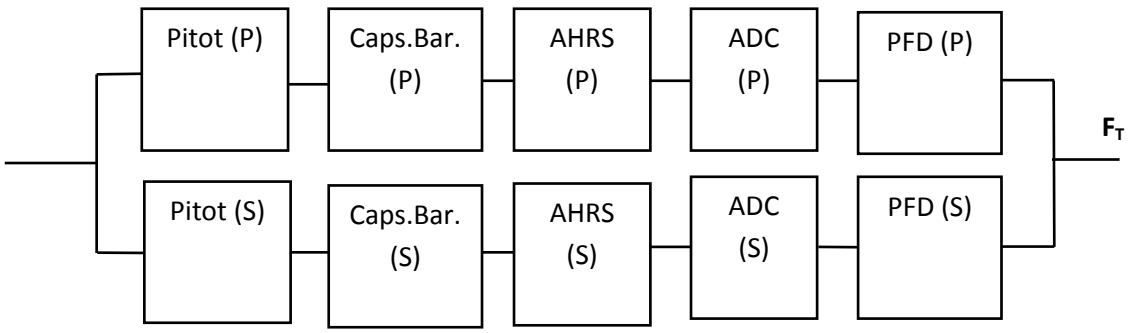


Fig. 3.12 – DDA do sistema de Apresentação das Informações Primárias de Voo

Note que são dois ramos em paralelo. Para que o sistema falhe ou tenha um mau funcionamento, é necessário que os dois ramos falhem ou tenham mau funcionamento (principalmente um *misleading*); Mas, basta haver uma falha ou mau funcionamento de qualquer subsistema ou item de um ou outro ramo para que o respectivo ramo falhe (pane). Isso está em absoluto acordo com a FTA de onde se gerou esta DDA.

3.3. *FAILURE MODE AND EFFECT ANALYSIS (FMEA)*

3.3.1. Considerações Iniciais Importantes

Vamos agora tratar da ferramenta que não é da competência da empresa que desenvolve o projeto do avião, mas dos fornecedores dos vários subsistemas que vão ser integrados na aeronave e para os quais foram estabelecidos, como requisitos, valores máximos de taxa de falha, na FTA da PSSA. A falha desses subsistemas está representada pelos eventos básicos (círculos) da mencionada FTA.

Neste ponto, é imperioso que enfatizemos o que de fato se quer dos fornecedores de subsistemas, como informação para o Processo de *Safety Assessment*, obtida por meio da FMEA. Isso é muito importante. Pois bem, o que se quer mesmo de cada fornecedor é que cada um demonstre que seu subsistema cumpre o requisito de taxa de falha máxima estabelecido na FTA da PSSA. Só isso. Repetimos: só isso.

Citemos então, como exemplo, incluído na mencionada FTA, o Sistema de Informações Primárias de Voo de uma aeronave, o qual provê a função de guiagem e navegação, adotando em sua configuração vários subsistemas cujos eventos de falha são representados por círculos, os chamados eventos básicos (V. Fig. 3.8). Um deles, por exemplo, é o subsistema ADC (*Air Data Computer*) que provê informações de navegação (*airspeed, altitude*, etc.), a partir de dados do ar externo à aeronave captados pelo Tubo de Pitot. Dois ADC compõem esse sistema; um para fornecer as informações para o piloto simbolizado pela letra P (Principal), e outro para fornecer as mesmas informações ao copiloto, simbolizado pela letra S (Secundário).

A taxa de falha do ADC (P) por perda de sua função ou por mau funcionamento imposta pela FTA da PSSA deve ser $\lambda_P < 10^{-4}$. Já para o ADC (S), impôs-se $\lambda_S < 10^{-3}$. Esses requisitos, como enfatizamos, constituem o foco da equipe que desenvolve o Processo

de Safety Assessment, na empresa integradora desses subsistemas; **não percamos isso de vista**.

Consideremos então que uma vez cumprida a etapa da PSSA, estabelecendo os requisitos de taxa de falha máxima para os vários subsistemas provenientes de fornecedores externos, o Setor de Procura e Compra - SPC (*Procuring)* da empresa que desenvolve o projeto do avião encaminha a esses possíveis fornecedores os requisitos gerais que seus subsistemas devem cumprir, mas em especial aqueles estabelecidos para os referidos eventos básicos da FTA (taxa de falha máxima). Essas informações, demonstrando o atendimento aos requisitos, serão inseridas no relatório SSA (*System Safety Analysis*), que será enviado à Autoridade de Certificação, demonstrando o atendimento aos requisitos de segurança por parte dos fornecedores de subsistemas.

Mas, atenção, não basta o fornecedor passar a taxa de falha ao SPC; é necessário demonstrar, por meio de um relatório de engenharia que, de fato, é aquela a taxa de falha máxima do subsistema em apreço, justificando a metodologia adotada para estabelecer tal afirmação.

Para demonstrarem que seus subsistemas cumprem os requisitos estabelecidos, os fornecedores provavelmente utilizarão a análise conhecida pela sigla FMEA (*Failure Modes, And Effects Analysis*).

3.3.2. Caracterizando a FMEA

A FMEA é um método adotado para identificar os modos de falha de itens[13] ou de funções de um subsistema, e determinar os efeitos desses modos de falha no subsistema e a correspondente taxa de falha (falhas por hora de vôo).

A introdução desse tipo de análise ocorreu efetivamente com o lançamento da norma militar MIL-STD-1629A (Ref. 3), que foi superada já na versão “A”, de 24/11/1980, continuando, no entanto, a ser considerada como a obra clássica desse tipo de análise.

Desse modo, ela surgiu para aplicação militar, mas logo foi adotada também para sistemas de aeronaves civis. Hoje, mesmo superada, ela continua a ser adotada por fornecedores de subsistemas da aviação militar e civil.

[13] Estabeleçamos aqui que “item” pode ser um equipamento ou uma parte dele (módulo ou peças desse módulo).

Para melhor caracterizar a FMEA, vamos compará-la com a FTA. Esta, como já sabemos, é um tipo de análise que vai do efeito para a causa (*top-down: de cima para baixo*), enquanto a FMEA vai da causa para o efeito (*bottom-up: de baixo para cima*).

Trata-se de uma análise essencialmente qualitativa, ou seja, em sua origem preocupa-se em identificar modos de falha e estabelecer seus efeitos e respectiva gravidade desses efeitos, sem, contudo entrar no trato probabilístico de ocorrência desses modos de falha.

Para complementar essa lacuna quantitativa, foi desenvolvida uma análise complementar desse gênero denominada Análise de Criticalidade (*Criticality Analysis* - CA) que, formando par com a FMEA, fez surgir a chamada FMECA (*Failure Modes, Effects and Criticality Analysis*). FMEA e FMECA são tratadas na MIL-STD-1629A.

Nós, no entanto, não trabalharemos com a CA neste trabalho, para chegar à taxa de falha do subsistema, que é o que nos interessa, no Processo de *Safety Assessment*. Consideraremos as taxas de falhas dos subsistemas obtidas por meios estatísticos, em ensaios de campo ou de laboratório, ou ainda por meio de documentos fontes de taxas de falhas, tais como MIL-HDBK-217A (Ref.4) do Departamento de Defesa dos Estados Unidos DoD), para itens (componentes) eletrônicos; além de outros documentos aceitáveis com a mesma finalidade, quais sejam: fontes da indústria de taxas de falhas, MIL-HDBK-338: “Dados de Confiabilidade de Peças Não Eletrônicas”; (NPRD) e GIDEP “Programa de Intercâmbio de Dados do Setor Público”; MIL-HDBK-978; e o “Kit de Ferramentas para Engenheiros de Confiabilidade” do Laboratório de Roma (EUA)[14].

3.3.3. Limitação da FMEA

Agora, vem o nó da FMEA, quando se trata de subsistemas aviônicos complexos. Esses subsistemas possuem equipamentos que utilizam circuitos integrados (CI) de última geração com uma ou mais centena de entradas e saídas, realizando ou participando de uma multitude de funções, tornando difícil a análise ou ensaios. A aplicação da FMEA a tais subsistemas pode ser inútil, ou no mínimo trazer resultados duvidosos.

Diante desse quadro, surgiram dois documentos adotados pela Autoridade de Certificação: a RTCA[15] /DO-254 (Ref.5), aplicada a projetos de desenvolvimento de *hardware*, formando par com a RTCA/DO-179 (Ref. 6), dedicada a projetos de desenvolvimento de *software*.

[14] O documento SAE ARP 4761 (Ref. 7) segue, em parte, metodologia similar.
[15] RTCA: *Radio Technical Commission for Aeronautics*.

São, enfim, documentos que sugerem [16] aos fornecedores desses subsistemas complexos a aplicação de processos de desenvolvimento acurados, em termos de qualidade, que, seguidos na íntegra, produzem sistemas de altíssima qualidade, que são então aceitos pela Autoridade sem outras exigências, tais como ensaios ou análises de segurança.

3.3.4. Enfoques da FMEA

A FMEA pode ser realizada segundo dois enfoques: funcional e peça-a-peça *(piece part).* O enfoque funcional ainda pode, até certo ponto, ser viável, para os já mencionados sistemas aviônicos complexos; mas, a FMEA peça-a-peça, infelizmente, não traz resultados confiáveis para tais sistemas, que congregam circuitos integrados (CI). Nesses casos, como já explicado, só tem um jeito: recorrer ao uso dos documentos RTCA/DO-254 (Ref. 5) e RTCA/DO-179 (Ref. 6).

Assim, vamos tratar aqui, com algum detalhe, apenas da FMEA funcional e tecer algumas considerações sobre a FMEA peça-a-peça, o suficiente, entretanto, para o leitor ter uma ideia do processo, mesmo porque, como já dissemos, tal análise é uma atribuição do fornecedor do sistema e não da equipe que desenvolve o Processo de *Safety Assessment*, parte integrante do esforço do projeto da aeronave.

Na realidade, esse grupo da empresa que desenvolve o Processo *de Safety Assessment* apenas tem de entender como a FMEA se processa no fornecedor, para poder ter conhecimento suficiente para aceitar ou não a FMEA relativa ao subsistema desse fornecedor.

3.3.5. FMEA Funcional

A FMEA funcional avalia os modos de falha funcionais, sendo por isso importante identificar os possíveis modos de falha de uma função. Dissemos no Módulo II do PDC 01[17] que os Modos de Falhas Funcionais (*Functional Failures Modes*) são os seguintes:

[16] "Sugerem"; mas, na realidade, são obrigatórios, uma vez que se não forem adotados, o subsistema não será aprovado pela Autoridade.

[17] PDC 01: "Interpretando a Visão da Autoridade de aviação civil no Processo de S*afety Assessment",* que está à disposição do leitor na página de entrada do site www.dcabr.org.br.

(a) Perda total de função (anunciada ou não anunciada) - como, por exemplo, o movimento do trem de pouso, na preparação para o pouso;

(b) Perda parcial de função (anunciada e não anunciada), tal como baixa pressão hidráulica ou perda parcial da alimentação elétrica;

(c) 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

(d) Função com informações incorretas ou *misleading* (parece correta mas não é) - tais como uma informação de *altitude* ou *heading* incorretos no display.

O modo de falha (a) é perda real da função, isto é, tem como efeito a ausência de qualquer informação (*output*). Os modos de falha (b), (c) são maus funcionamentos, porém em geral diretamente percebidos pelo piloto, ou indiretamente, por meio de sinais de advertência de dispositivos a bordo da aeronave, permitindo ao mesmo alguma reação. O modo de falha (d), o mencionado *misleading*, por sua vez, tem como efeito produzir um efeito enganoso, não anunciado, ou seja, a informação parece verdadeira, mas, na realidade, não é. Isso pode ser tão crítico ou mais crítico que a perda da função, principalmente se a aeronave estiver num voo IMC (*Instrument Meteorological Conditions*).

São esses os modos de falha que consideraremos neste trabalho, quando se tratar de análise funcional. Na FMEA peça-a-peça, os modos de falha terão uma contonação algo diferente, como será explicado, quando tratarmos desse enfoque.

Vamos agora ao Exercício 3.3 de uma FMEA funcional.

Exercício 3.3 – FMEA Funcional de um Sistema de Bombeamento de Água

***(Nota:** O sistema de bombeamento de água de uma edificação é por demais conhecido, na construção civil, e vários modelos estão disponíveis na praça. Entretanto, neste nosso exemplo, vamos supor que se trata de um sistema novo solicitado por um determinado cliente com requisitos que incluem um valor máximo de taxa de falha).*

[18] Um exemplo de ação de controle de voo não comandada pelo piloto foi o acidente de uma aeronave Tornado, na Alemanha (anos 80), que foi "atacada" por ondas eletromagnéticas (HIRF – *High Intensity Radiated Fields* - Campos Radiados de Alta Intensidade) 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.

Lembremos que no item 3.1 dissemos que esse sistema é constituído por duas bombas e um dispositivo de sensoriamento e controle (boia/contato). Dissemos também que a alimentação elétrica, o reservatório de água no solo e a caixa d'água, no topo da edificação, não fazem parte do sistema de bombeamento; quer dizer, esses itens já existiam na edificação, fazendo parte do projeto da mesma.

Como já vimos, existem apenas três funções realizadas por esse sistema:

(1) Prover sensoriamento do nível de água na caixa d'água **C**, realizada por meio de um sensor (boia);

(2) Prover controle do bombeamento de água, realizada por um dispositivo tipo relé, comandado pela boia, que interrompe a continuidade da alimentação elétrica para as bombas de água, se o sensor indicar que o nível máximo da caixa **C** foi atingido; ou dando continuidade à alimentação elétrica para as bombas, quando o nível mínimo de água for "percebido" pelo sensor (boia).

(3) Prover bombeamento de água de um reservatório **R,** no solo, encaminhando-a para a caixa **C**.

Consideremos então o diagrama funcional da Fig. 3.13.

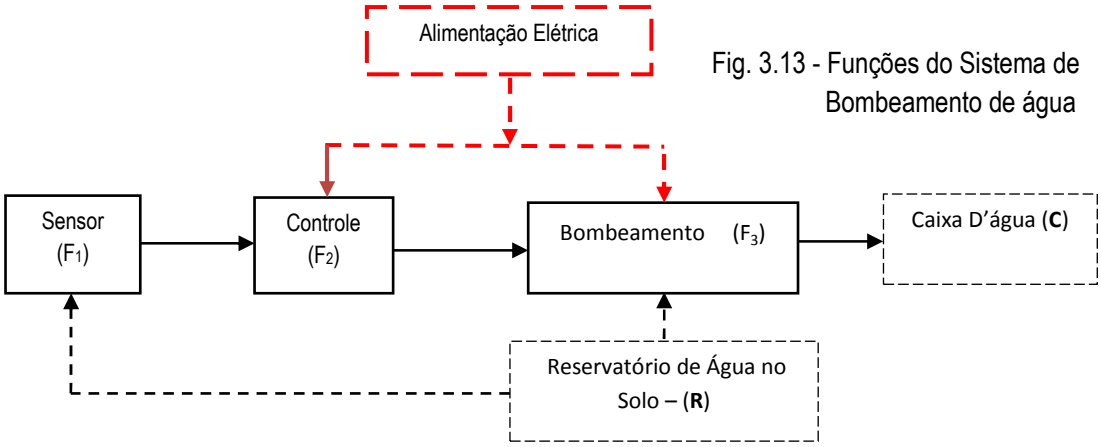


Fig. 3.13 - Funções do Sistema de Bombeamento de água

A função F_3 (Prover Bombeamento de Água), como sabemos, é provida por duas bombas, B1 e B2, numa configuração de redundância. Para deixar isso mais claro, podemos desmembrar a caixa (F_3) conforme a figura 3.14.

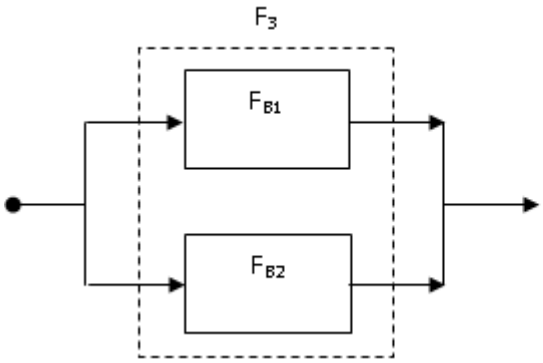


Fig. 3.14 – Desmembramento de F3

Como sabemos o provimento da alimentação elétrica não é uma função do sistema, mas é essencial para que o mesmo funcione. A empresa responsável pela instalação do sistema no prédio é claro, não analisa as falhas de alimentação elétrica porque não lhe cabe investigar algo pelo qual não tem qualquer responsabilidade. Só as funções F_1, F_2 e F_3 são objetos da FMEA.

Primeiramente, devemos fazer o seguinte questionamento:

(1) Quais são os modos de falha de cada função?

(2) Qual é a taxa de falha de cada função e do sistema como um todo?

Os modos de falha são perda da função ou mau funcionamento. O potencial efeito da perda funcional ou mau funcionamento do sistema é a falta de água na caixa ou insuficiência de bombeamento de água. É claro que, em tal sistema, não temos riscos à vida humana, como no caso de sistemas aeronáuticos; o pior efeito é a dor de cabeça por falta d'água por certo tempo.

Se for estabelecido que o sistema tenha de ter uma taxa de falha (ou Falibilidade/hora de operação) menor que um determinado valor λ, digamos $\lambda<10^{-4}$ por hora de operação, então a taxa de falha de cada uma das três funções (λ_1, λ_2 **e** λ_3) devem ser tais que sua soma seja menor que o requisito de 10^{-4}, ou seja, $(\lambda_1 + \lambda_2 + \lambda_3) < 10^{-4}$. Notemos que $\lambda_3 = \lambda_{B1}.\ \lambda_{B2}$. Assim, deve-se ter: $\lambda = [\lambda_1 + \lambda_2 + (\lambda_{B1}.\ \lambda_{B2})] < 10^{-4}$.

Pois bem, para verificar se isso acontece, o melhor é fazer ensaios de laboratório que componham o chamado *Debugging*, em se tratando de sistemas novos, verificando a taxa de falha de cada bloco funcional e somando essas taxas de falha[19], para obter a

[19] "Somando" porque o sistema falha (perde a função ou apresenta mau funcionamento) se qualquer um dos blocos funcionais falhar. Resulta, pois, um comportamento de entradas de uma porta "OU", tendo nas entradas as probabilidades de falha dos blocos funcionais, que, portanto, devem ser somadas para se ter a probabilidade de o sistema falhar.

taxa de falha do sistema. Se a taxa de falha do sistema for mais alta que o máximo de requisito, é preciso realizar uma FMEA peça-a-peça do bloco funcional mais crítico. Se ainda assim persistir uma taxa de falha maior do que a de requisito, deve-se procurar uma solução de projeto, como, por exemplo, redundância, de modo a, ao final, ter uma taxa de falha do sistema num valor aceitável.

Uma vez concluída a análise funcional e feitas as eventuais correções de projeto, deverá ser construída uma tabela ou planilha (*worksheet*), listando a função de cada bloco funcional, os modos de falha de cada função, as taxas de falha de cada modo de falha e o efeito de cada falha no sistema[20]. As taxas de falha dos modos de falha com o mesmo efeito devem ser somadas. Obtém-se assim a taxa de falha para cada efeito. Isso é o suficiente para o Processo de *Safety Assessment*.

A *worksheet* não tem um formato físico fixo; as informações nela contidas dependem dos requisitos do cliente, isto é, das informações que o cliente deseja que seja inserida na *worksheet*. Na presente análise, poderia ser como na tabela a seguir.

Quadro X - FMEA Funcional do Sistema de Bombeamento de Água XXXXX

Projeto e fabricação: YYYYY

Nome da Função	**Modo de Falha**	**Taxa de Falha**	**Efeito da Falha**
F1: Sensoriamento	Perda da função/Mau funcionamento	3,00E-6	Perda do Sistema
F2: Controle do bombeamento	Perda da função/Mau funcionamento	2,15E-6	Perda do Sistema
F3: Bombeamento	Perda da função/Mau funcionamento	5,15E-6	Perda do Sistema
Taxa de Falha Total do Sistema		1,03E-5	

Notem que os modos de falha das funções levam ao mesmo efeito no sistema, ficando evidente que devemos somar as taxas de falha desses modos de falha (é de fato como se fosse uma porta OU, ou seja, o sistema falha na hipótese de falha de F1 ou F2 ou F3). Observa-se então que o sistema satisfaz o requisito de taxa de falha porque sua taxa de falha enquadra-se no intervalo 1,03E-5 < 10^{-4}.

[20] No caso de sistemas de aeronaves, deve-se acrescentar ainda a "Fase do Voo" (ex.: decolagem, subida, cruzeiro, aproximação, descida e pouso).

Exercício 3.4 – FMEA Funcional de Um Sistema Simples de Alimentação Elétrica de Uma Aeronave de Pequeno Porte

(1) Descrição do sistema.

Consideremos o diagrama da Fig. 3.15. Trata-se de um sistema normalmente utilizado em aeronaves de pequeno porte[21].

(a) Componentes.

Temos os seguintes componentes, pela ordem de acionamento no sistema de partida:

- ***Master Switch*** (Chave Principal – Que liga o terminal negativo da bateria à massa ou terra, permitindo que a mesma forneça corrente elétrica aos vários dispositivos pelos quais fluirá a corrente para o Motor de Partida (*Starter*) – è o primeiro dispositivo a ser ligado na fase de decolagem, e o último a ser desligado após o pouso;
- ***Battery*** (Bateria) – Fornece corrente ao enrolamento da *Master Solenoide* (Solenoide Principal), que comanda o fechamento desse solenóide, permitindo que seus 24V sejam aplicados à *Main Bus* (Barramento Principal);
- ***Master Solenoide*** (Solenoide Principal) – Que, uma vez fechado, liga o terminal positivo da bateria ao terminal direito do *Starter Solenoide* e à Main Bus (Barra ou Barramento Principal);
- ***Starter Switch*** (Chave de Partida) – Que uma vez acionada (permite que os 24V da bateria, por meio da Main Bus, sejam aplicados ao enrolamento de campo do *Starter Solenoide* (Solenóide de Partida);
- ***Starter Solenoide*** (Solenoide de Partida) – Que uma vez fechado, permite que os 24V da bateria sejam aplicados ao *Starter* (Motor de Partida), que dá partida ao motor da aeronave;
- ***Alternator*** (Alternador ou Gerador) – Que é acionado pelo eixo do motor da aeronave.

[21] O diagrama da Fig. 3.1 consta do artigo *Aircraft Electrical System in Small Single Engine Aircraft (Part One)* da Flight Mechanic, que pode ser consultado na Internet.

Para facilitar nosso exemplo, não vamos considerar aqui a *External Power Jack* e seu *External Power Relay*, que fornecem energia para a partida, em caso de ser necessária uma fonte externa (*Ground Power Unit* – GPU) para esse fim.

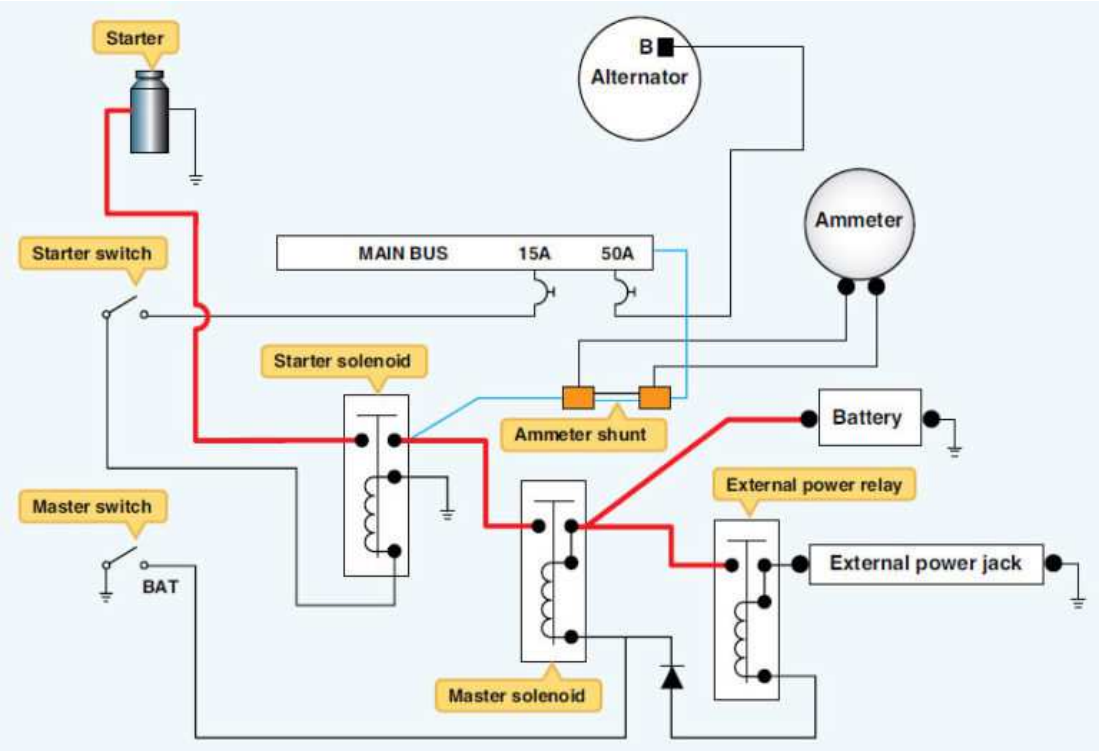


Fig. 3.15 – Sistema de Alimentação Elétrica de Uma Aeronave de Pequeno Porte

Para simplificar, vamos considerar as chaves *Master Switch* e *Starter Swich* (acionadas pelo piloto) como chaves ideais ou de baixíssima probabilidade de falharem. O diagrama funcional ficaria como na Fig. 3.16.

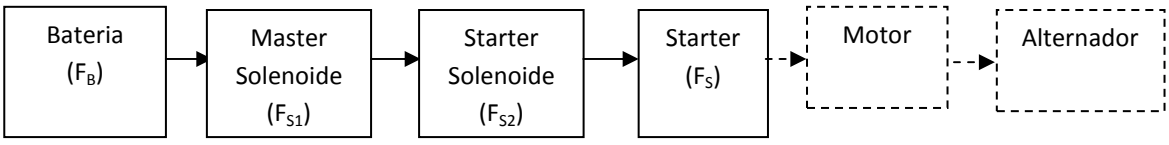


Fig. 3.16 – Diagrama funcional do sistema de partida da aeronave ("viagem" dos 24V da bateria até o motor de partida - *Starter*).

Digamos que o requisito para esse sistema, decorrente da FTA da PSSA, estabelece que a taxa de falha máxima λ, relativa à perda ou mau funcionamento do sistema, deve ser menor que 10^{-3}.

Temos então as seguintes funções:

- F_B – Prover tensão elétrica (voltagem) de 24VDC para o enrolamento do *Master Solenóide* (que então fecha a armadura desse solenóide, dando passagem aos 24V da bateria para um dos terminais do *Starter Solenóide)*;
- F_{S1} – Prover tensão da bateria para o *Starter Solenóide;*
- F_{S2} – Prover tensão da bateria para o motor de partida –*Starter* (depois que o piloto acionar a *starter switch*, fechando a armadura do *Starter Solenoide*, dando passagem para os 24V da bateria para o *Starter*);
- F_S – Prover torque para o motor da aeronave.

Notemos que os modos de falha perda ou mau funcionamento de qualquer uma das funções impedirá que seja provido o necessário torque para o motor da aeronave. Portanto, a perda ou mau funcionamento de qualquer função produzirá a perda ou mau funcionamento do sistema; são efeitos de mesma severidade. Assim, a taxa de falha do sistema será a soma das taxas de falha de cada função.

Por outro lado, os testes de campo ou de laboratório, justificados por análises de engenharia, nos dão conta de que as respectivas taxas de falha, a título de exemplo, seriam as seguintes:

- $\lambda_B < 10^{-4}$;
- $\lambda_{S1} < 10^{-5}$;
- $\lambda_{S2} < 10^{-5}$; e
- $\lambda_S < 10^{-4}$.

Assim, a taxa de falha do sistema, na perda ou mau funcionamento do mesmo, expressa e comprovada num relatório circunstanciado de engenharia, é:

$\boldsymbol{\lambda = \lambda_B + \lambda_{S1} + \lambda_{S2} + \lambda_S =}$ $2{,}2.10^{-4} < 10^{-3}$; faixa, portanto, que satisfaz o requisito de taxa de falha máxima para o sistema.

3.3.6. FMEA PEÇA-A-PEÇA (*Piece Part*)

Falemos, agora, sobre a FMEA peça-a-peça. Como dissemos a FMEA, em si, é qualitativa, mas podemos associar aos modos de falha taxas de falhas extraídas dos documentos fontes mencionadas no item 3.3.2[22]. Os resultados dos passos, que serão apresentados a seguir, são registrados numa planilha (*worksheet*). A configuração de colunas dessa planilha dependerá dos requisitos do cliente, isto é, das informações que ele, cliente, disser que quer receber. Vamos considerar então uma configuração de planilha que consideramos suficiente para os analistas do Processo de *Safety Assessment* da empresa integradora dos subsistemas na aeronave.

Não podemos perder de vista, de modo algum, que o que interessa ao Processo de *Safety Assessment* é a taxa de falha máxima do subsistema, na hipótese de perda ou mau funcionamento da função do mesmo, que deve ser aquela estabelecida pela FTA da PSSA.

(1) **Primeiro passo** – Procure entender o funcionamento do sistema em análise como um todo.

(2) **Segundo passo** – identifique os blocos funcionais do sistema, identificando também a função de cada bloco.

(3) **Terceiro passo** – Faça a análise por blocos, listando os componentes de cada um. Atribua, para cada componente listado, um identificador; ex.: 01A, para o primeiro componente da lista do bloco A.

(4) **Quarto passo** – Identifique os modos de falha de cada componente (ex.: ruptura, para um resistor).

(5) **Quinto passo –** identifique os efeitos dos modos de falha em cada bloco e deste no sistema como um todo.

(6) **Sexto passo** – Obtenha a taxa de falha para cada modo de falha. Para isso, consulte a taxa de falha para cada componente na MIL-HDBK-217F (Ref. 4).

[22] No caso de um desses documentos, a MIL-HDBK-217F (Ref. 4), é importante assinalar, neste momento, que a Indústria Aviônica considera que os valores de taxas de falha ali apresentados são muito conservativos, sugerindo taxas que, quase sempre, são maiores do que aquelas que a prática no campo operacional mostra. Isso trás problemas, pelo menos no processo de aquisição de peças de reposição, para uso nas oficinas de reparos dos sistemas, aumentando o estoque dessas peças para acima do razoável.

(7) **Sétimo passo** – Some as taxas de falha dos modos de falha que produzem o mesmo efeito no sistema.

(8) **Oitavo- passo** – Realizados os passos acima para cada bloco funcional, some as taxas de falha de cada bloco com o mesmo efeito no sistema como um todo.

(9) **Nono-passo** – Identifique a somatória das taxas de falhas do efeito mais grave (perda da função do sistema). Esta deverá ser a taxa de falha do sistema que deve satisfazer o requisito de máxima taxa de falha para o sistema (aquela estabelecida na FTA da PSSA).

(10) **Décimo passo** – Registrar tudo isso numa planilha (*worksheet*) e encaminhá-la ao cliente (empresa que desenvolve o projeto do avião) como parte de um relatório de engenharia. Faremos agora um exercício para deixar mais claro o processo.

A título de ajuda, os modos de falha típicos para a FMEA peça-a-peça a serem considerados incluem, mas não se limitam a, o seguinte[23]:

a. Aberto (resistores);

b. Curto (capacitores, diodos);

c. Desvios de parâmetros;

d. Ruptura de dielétrico (capacitor);

e. Operação Intermitente;

f. Inoperância;

g. Operação espúria;

h. Desgaste pelo uso;

i. Falha mecânica;

j. Engripagem (*Sticking*);

k. Fratura.

[23] Conforme o Anexo G do documento SAE ARP 4761 (Ref. 7)

Exercício 3.5 – FMEA Peça-a-Peça (Piece Part) de Um Sistema Simples de Fonte de Alimentação Elétrica de Corrente Contínua (DC)

Não vamos aqui dar uma aula de eletrônica, mas falar o suficiente para o entendimento de engenheiros ou técnicos não de eletrônica sobre o funcionamento do sistema de alimentação elétrica de equipamentos eletrônicos mostrado na Fig. XXXX. O sistema é considerado simples, porém elucidativo para nosso objetivo.

O circuito da figura 3.17 representa um sistema de alimentação elétrica utilizado para fazer funcionar circuitos eletrônicos que dependem de uma tensão (voltagem) de alimentação de corrente contínua, com tensão de saída simbolizada por V_{DC}, a partir de uma tensão de entrada de corrente alternada, simbolizada por V_{AC}.

Desse modo, temos:

V_{AC} : Tensão AC de entrada do sistema; e

V_{DC} : Tensão DC de saída do sistema.

Os componentes e respectivas funções são os seguintes:

(1) **Transformador (T)**, que rebaixa a tensão V_{AC} de entrada para um valor AC, definida conforme o projeto do sistema;

(2) **Diodos D_1** e **D_2**, que retificam a tensão AC, permitindo a passagem apenas dos pulsos positivos da tensão AC de entrada. Essa retificação é apresentada na figura 3.17. Esses pulsos positivos têm dois componentes: uma parte contínua (DC) e outra de corrente alternada (AC). O que nos interessa é só a a parte DC. Para conseguir isso, utiliza-se o componente denominado capacitor, no caso representado por C_1;

(3) **Capacitor C_1**, que tem a função de filtro, isto é deixa passar a parte AC para a terra e bloqueia a parte DC no ponto A. Desse ponto em diante a tensão é apenas DC;

(4) **Resistor R**, que reduz a tensão DC no ponto A para a tensão no Diodo Zener D_Z;

(5) **Diodo Zener D_Z**, que, uma vez alimentado, produz em sua saída uma tensão (DC) V_Z constante;

(6) **Transistor TR**, que dá passagem à corrente elétrica para a carga R_L colocada na saída B. R_L representa o sistema externo que está sendo alimentado pelo sistema em estudo; e

(7) **Capacitor C_2**, que elimina qualquer vestígio de componente AC.

A tensão (DC) V_O, na saída, é dada por V_O = -0,7 + V_Z . Digamos que supostamente tivéssemos V_Z = 7,7V. Desse modo, ter-se-ia: V_O = 7V.

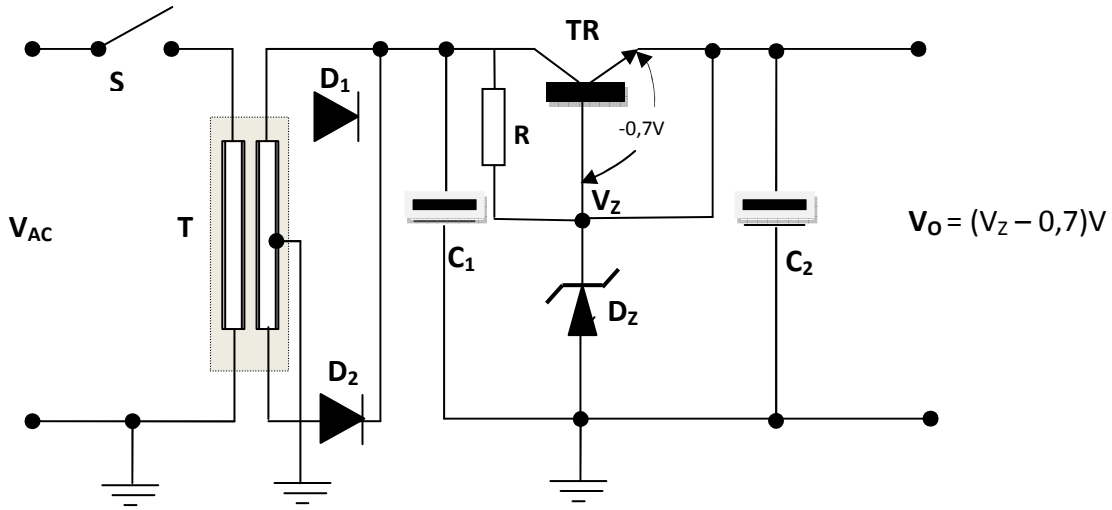


Fig. 3.17 – Sistema de Alimentação Elétrica DC

Consideremos a Tabela I, a seguir, para caracterizar os modos de falha dos componentes e seus efeitos.

Componente	Modo de Falha	Efeito na Saída do Sistema	Taxa de Falha
Transformador T	• Enrolamento primário ou secundário aberto. • Enrolamento primário ou secundário em curto.	• Perda da tensão de Saída V_O. • Perda da tensão de saída V_O.	λ_1
Diodos D_1 e D_2	• Abertos. • Em curto circuito.	• Perda da tensão de saída V_O. • Perda da tensão de saída V_O.	λ_2
Capacitor C_1	• Curto circuito. • Aberto.	• Perda da tensão V_O. • Perda da Tensão V_O.	λ_3
Resistor R	Ruptura	Perda da tensão de saída V_O, por falta de alimentação ao diodo Zener.	λ_4
Diodo Zener D_Z	• Aberto • Curto-circuito	Perda da tensão de saída	λ_5
Transistor TR	• Fora da especificação. • Curto circuito entre a base B e o emissor E	• Provável degradação da Tensão V_O. • Perda da tensão de saída V_O, por falta de continuidade de corrente no transistor TR.	λ_6
Capacitor C_2	• Curto circuito. • Aberto.	• Perda da tensão V_O. • Tensão V_O com algum espúrio de AC.	λ_7
		$\sum_{i}^{n} \lambda i$	λ_T

Tabela YYY– Modos de Falha, Efeitos e Taxas de Falha do sistema de Alimentação Elétrica da Fig. XXXXX

Observa-se que os modos de falha dos componentes levam à perda da tensão de saída $V_{O,}$ ou a uma tensão V_O com possíveis espúrios de corrente alternada, “mascarando” a tensão V_O. Ambos os efeitos são considerados de mesma severidade.

Sendo assim, como já orientado, temos de somar as taxas de falhas de cada componente para termos o valor final das dos modos de falha que produzem o mesmo efeito.

Finalmente, temos de comparar essa taxa de falha com aquela de requisito, ou seja, aquela taxa estabelecida como máxima para o sistema, na FTA da PSSA. Se estiver de acordo com o requisito, a análise é encaminhada à Autoridade como anexo do relatório da SSA.

Devemos apresentar tudo isso em uma planilha (*worksheet*), como mostrado a seguir.

Planilha (worksheet) da FMEA do Exemplo 3.5

Análise de Modos de Falha e Seus Efeitos (FMEA)

Sistema: Fonte de alimentação DC

Fabricante: xxxxyyyyyzzzzzz

Nível da análise: Peça-a-Peça (Piece Part)

Nr. Desenho: 8989898

Nº Identificação	Nomenclatura	Função	Modo de Falha	Efeito da Falha no Sistema	Taxa de Falha
1	Transformador	Rebaixar Tensão alternada de entrada da fonte	Enrolamento primário ou secundário aberto ou em curto	Perda da tensão de saída V_O	λ_1
2	Diodos D_1 ou D_2	Retificar a corrente alternada	Aberto ou em Curto	Perda da tensão de saída V_O	λ_2
3	Capacitor C_1	Filtrar a corrente alternada	Aberto ou em Curto	Perda da tensão de saída	λ_3
4	Resistor R	Limitar a corrente para o Diodo Zener	Ruptura	Perda da tensão de saída V_O	λ_4
5	Diodo Zener	Fornecer uma tensão constante	Aberto ou em Curto	Perda da tensão de saída V_O	λ_5
6	Transistor TR	Fornecer corrente contínua para a carga na saída	Fora de especificação ou curto entre base e emissor	Perda da tensão de saída V_O	λ_6
7	Capacitor C_2	Filtrar algum vestígio de corrente alternada	Aberto ou em curto	Perda da tensão de saída V_O	λ_7
				$\sum_i^n \lambda \mathbf{i}$	λ_T

Bem, caros leitores, encerramos por aqui a FMEA, acreditando ter sido suficiente pelo menos para o analista de Safety Assessment ter uma ideia do que seja esse tipo de análise. Para informações mais detalhadas, consulte a MIL-STD-1629A (Ref. 3).

3.4. ANÀLISE DE CAUSA COMUM (*COMMON CAUSE ANALYSIS* – CCA)[24]

Esta é a última análise do Processo de *Safety Assessment*, mais conhecida pela sigla CCA, do inglês *Common Cause Analysis*. Trata-se de uma análise qualitativa, realizada pela equipe da empresa que desenvolve a aeronave.

Devemos chamar a atenção para o fato de que a realização dessa análise (que está dividida em três outras, mencionadas abaixo), em alguns casos, pode ser um pouco complicada.

Dependendo do sistema, por mais que nos esforcemos, é difícil realizá-la de maneira realmente exaustiva[25], 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, como temos repetido, 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 de um seu subsistema ou equipamento);

(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);

[24] Já tratamos dessa análise no PDC-01; mas, resolvemos repeti-la no PDC-02, de modo a apresentar *in totum* as análises aplicadas ao Processo de *Safety Assessment*.
[25] V. Ref 7.

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

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

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

Com certeza, não vamos esgotar essas análises aqui, mas vamos dar uma ideia da filosofia adotada nesse processo, considerando as características do sistema que escolhemos para nosso processo de *Safety Assessment*: Sistema de Apresentação das Informações Primárias de Voo (Fig. 3.8).

3.4.1. Análise de Segurança Zonal (*Zonal Safety Analysis*)[26]

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

(1) temperatura do ambiente, onde a LRU vai ser instalada;

(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*

[26] 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[27].

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 deve apresentar 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[28], 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.

3.4.2. 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.

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

[28] Isso aconteceu com este autor, quando realizando soldagem de componentes do estado sólido num circuito impresso.

Os principais problemas para esses sistemas estão na exposição a raios (*Lightining*) e 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, 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 terá de ser 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.

3.4.3. 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 consideradas 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.

Conclusão

Bem, prezado leitor, concluímos este trabalho. Como já mencionamos, aqueles que estiverem interessados numa descrição detalhada da FMEA do tipo peça-a-peça podem consultar a MIL-STD-1629A (Ref. 3). Trata-se de um estudo que exige persistência e paciência. Também pode ser consultada a SAE ARP 4761[29] *(Ref. 7), não só para a FMEA, mas para todas as análises apresentadas aqui. Trata-se de um documento exaustivo, requerendo, da mesma forma, persistência e paciência para entendê-lo bem. Esta é a receita.*

Finalizando, nos despedimos, esperando ter acrescentado algo na vida profissional daqueles que nos lêem. Críticas serão sempre bem-vindas. Até uma próxima.

Referências

1. *Clarke, A.Bruce – Dysney, Ralph L., Probability and Random Process for Engineers and Scientists, John Wiley & Sons, Inc., New York, USA, 1970.*
2. *AC 25.1309-1A, System Design and Analysis, FAA, EUA, 21/06/1988.*
3. *MIL-STD-1629A, Procedures for Performing a Failure Mode, Effects, And Criticality Analysis (FMECA), DoD, EUA, 24/11/1980.*
4. *MIL-HDBK-217F, Reliability Prediction of Electronic Equipment, DoD, EUA, 02/12/1991.*
5. *DO-254, Design Assurance Guidance for Airborne Electronic Hardware, RTCA, EUA, Abril/2000.*
6. *RTCA DO-178C, Software Considerations in Airborne Systems and Equipment Certification. RTCA, EUA, Jan/2012.*
7. *SAE ARP 4761, Methods for Conducting the Safety Assessment Process in Civil Airborne Systems and Equipment, Pág. 137, EUA, 8/11/1996.*

[29] Nossa preferência.

APÊNDICE A

Exemplo de Quadro de Resultados de Uma *Funcional Hazard Assessment* Nível Aeronave (AFHA)

Exemplo de Quadro de Resultados de Uma *Funcional Hazard Assessment* Nível Aeronave (AFHA)

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 (*GuidanceandNavigation*)					
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*