Organização Brasileira
para o Desenvolvimento
da Certificação Aeronáutica

– Programa de Difusão de Conhecimentos (PDC 01) –

Safety Assessment

INTERPRETANDO A VISÃO DA AUTORIDADE DE AERONÁUTICA CIVIL NO PROCESSO DE SAFETY ASSESSMENT

Módulo I – CONSIDERAÇÕES BÁSICAS

2ª. Edição (Revisada)

Eng. Jolan Eduardo Berquó

– Outubro 2017 –

APRESENTAÇÃO

Estamos apresentando nossa Segunda Edição (2ª. Ed.) do PDC-01 com a introdução no texto das erratas já distribuídas e aperfeiçoamento do texto e de figuras.

Como dissemos na 1ª. Ed., vamos desenvolver esse tema, procurando interpretar a visão da Autoridade Civil, nesse campo, inserida nas AC 23.1309-1E/25.1309-1A. O objetivo é facilitar, principalmente aos que se iniciam no mundo da aeronavegabilidade, sua participação no desenvolvimento dessa importante atividade, aplicada aos sistemas de uma aeronave civil, como parte da atividade global da certificação de tipo (CT) e Certificação Suplementar de Tipo (CST), voltadas para o projeto das aeronaves da Parte 23 (*CFR 14 Part 23.1309*) da classe *Commuter* e Parte 23 (*CFR 14 Part 25.1309*)

Os *flashes* “Melhore Seus Conhecimentos (MSC)”, que de há muito têm sido publicados em nosso *site*, continuarão a ser apresentados com suas habituais informações pontuais e céleres sobre os incontáveis assuntos da área de aeronavegabilidade.

Nosso projeto é sempre apresentar uma base de conhecimento, no nível de familiarização e um passo acima desse nível, ou seja, algo que, acreditamos, permitirá ao leitor, *a posteriori*, participar da atividade de Safety Assessment, bem como aprofundar-se no estudo do tema, seguindo as recomendações contidas nos documentos referenciados no final deste módulo e seguintes.

Em princípio, conforme anunciamos, os temas que serão apresentados no PDC serão, a posteriori, objeto de cursos na DCA-BR, oportunidade em que serão debatidos os temas propostos, podendo gerar resultados talvez úteis para a nossa Autoridade (ANAC).

Devemos deixar claro que não vamos repetir aqui, *ipsis litteris*, o conteúdo dos mencionados documentos. Também não vamos divulgar uma nova teoria a respeito do tema. Vamos apresentar um processo global, baseado nas recomendações existentes, que, a nosso ver, é “um pouco mais palatável” que o recomendado nos documentos pertinentes da Autoridade, permitindo, da mesma forma, no entanto, comprovar, ao final do processo, a inserção, no projeto dos sistemas da aeronave, dos requisitos de segurança.

Essa postura de apresentar algo, em nossa opinião um pouco mais palatável, não é conflitante com a orientação da Autoridade, que aceita a metodologia que melhor aprouver ao Aplicante, desde que ela, a critério da Autoridade, atinja o objetivo de

demonstrar que os requisitos de segurança estão de fato incorporados ao projeto dos sistemas da aeronave.

Ao final, cremos, nossos leitores estarão em condições de iniciar a prática de *Safety Assessment* e de partir para um estudo mais aprofundado dos mencionados documentos, que serão aqui referenciados, ao final de cada módulo, quando pertinentes.

O PDC 01 prevê três (3) módulos:

I. Considerações Básicas;

II. O Processo de *Safety Assessment Assessment* - Parte 1.

III. O Processo de *Safety Assessment Assessment* - Parte 2.

Apreciem

SUMÁRIO

APÊNDICES

1. CONSIDERAÇÕES PRELIMINARES

Qualquer projeto de sistemas tem de se preocupar com a eficácia e a eficiência da função ou funções que esses sistemas realizam; mas, com intensa preocupação concentrada na segurança de seus usuários e alvos alhures.

Há sistemas que o próprio usuário comanda e controla para seu proveito. Outros há que os usuários não podem fazê-lo, isto é, dependem de outros seres humanos para poderem tirar proveito desses sistemas. É o caso do sistema aeronave, ou seja, os usuários dependem do acerto dos projetistas, da manutenção, da tripulação e do controle de tráfego aéreo, para tirarem o almejado proveito.

Fixando-nos em nosso caso, isto é, em aeronaves, os projetistas sabem que têm de se preocupar com o projeto, procurando satisfazer o desejo do usuário de ter um transporte eficaz (que faça o que tem de ser feito), eficiente (que faça bem feito o que tem de ser feito) e seguro, ou seja, que dê ao usuário a certeza de que todo o possível foi feito para a aeronave conduzi-lo de maneira segura até seu destino.

Para tentar dar certa garantia de atingimento desse objetivo, existem órgãos governamentais reguladores que impõem requisitos de segurança. São as chamadas Autoridades. Nos Estados Unidos, temos a FAA (*Federal Aviation Administration*); no Brasil, a ANAC (Agência Nacional de Aviação Civil), e na Europa, a EASA.

Décadas atrás, a segurança de sistemas de uma aeronave era voltada para aspectos pontuais, concentrados praticamente nos equipamentos das aeronaves, mediante o uso intensivo das chamadas FMEAs (*Failures Modes, and Effects Analysis)*. Posteriormente, uma nova geração de aeronaves, diríamos que, talvez a partir do projeto *Concorde*, mudou do pontual para um inter-relacionamento funcional. Parece-nos que foi um grande salto de melhoria. Esse é o estado em que nos encontramos hoje.

A questão do sistema, no caso a aeronave, está hoje num patamar bastante aceitável, em termos de segurança (*safety*). Entretanto, há um outro fator que deve ainda ser continuamente considerado. Trata-se do Fator Humano (FH). Há correntes preocupadas com esse fator, mas como tudo que significa inovação, padece da lentidão própria da cautela a uma inovação.

Nosso trabalho está focalizado nos sistemas da aeronave, que têm 10% de responsabilidade pelos acidentes catastróficos, como iremos mostrar.

2. PROPÓSITO DESTE TRABALHO

Neste módulo, serão apresentadas as considerações, em nossa opinião minimamente necessárias para desenvolver o tema proposto neste módulo e nos módulos seguintes, relativo a *Safety Assessment,* iniciando pelo ambiente (aeronave e sistemas), onde se insere o processo de *Safety Assessment*. Trataremos dos conceitos de segurança (*safety*) de sistemas, mas só no campo da aviação civil. Apresentaremos o conceito de *Safety Assessment*, sua abrangência, em relação à aeronave como um todo, e finalizaremos com a apresentação de comentários sobre a participação estatística dos sistemas da aeronave nos acidentes catastróficos.

Salientamos que as autoridades de aeronavegabilidade que estaremos considerando aqui são a FAA (*Federal Aviation Administration*) e nossa ANAC (Agência Nacional de Aviação Civil), esta com requisitos e recomendações muito de perto similares àqueles da FAA. Por esse motivo, vamos nos concentrar na FAA, em face de sua documentação estar disseminada e servir de base para várias autoridades de aeronavegabilidade. Mas, em geral, que fique claro, a cada documento da FAA corresponde algo similar na nossa ANAC. Mas, neste trabalho, não nos preocuparemos com qualquer dessemelhança porventura existente entre essas autoridades. Por isso, vamos aqui tratar a Autoridade de aeronavegabilidade simplesmente por Autoridade.

Por importante, reforçamos que consideraremos somente as aeronaves civis. As aeronaves militares têm aspectos de segurança, ligados às missões militares, bem divergentes daqueles das aeronaves civis. Numa outra oportunidade, quem sabe, falaremos sobre isso. No entanto, registramos aqui que, em certos aspectos, as aeronaves militares podem ter alguns de seus sistemas comuns com os da área civil (caso dos sistemas aviônicos) convenientemente certificados com base nos requisitos civis, considerando que aeronaves militares também ocupam o espaço aéreo (RVSM, por exemplo) ocupado pelas aeronaves civis.

3. A AERONAVE E SEUS SISTEMAS

Antes de tudo, vamos nos entender sobre o que seja um sistema. Rigorosamente, na conceituação da Engenharia de Sistemas (ES), a aeronave é um sistema constituído pelos seus subsistemas e estes com seus respectivos equipamentos ou unidades com seus componentes (peças). No entanto, a Autoridade não atribui à aeronave, em si, a designação de sistema, adotando essa designação apenas para os seus subsistemas. Pois bem, para não contrariar essa conduta e causar confusões com a documentação da Autoridade, seguiremos essa sistemática, ou seja, consideraremos a aeronave simplesmente como um produto com seus sistemas e seus respectivos equipamentos. Assim, falaremos, por exemplo, de sistema aviônico, em vez de subsistema aviônico. Os sistemas, por sua vez, serão considerados como constituídos por equipamentos e suas interligações.

3.1 Classificação dos Sistemas de Uma Aeronave – Os Sistemas Aviônicos

A classificação dos sistemas da aeronave tem pontos polêmicos. Fala-se de sistemas mecânicos, sistemas elétricos, sistemas aviônicos e até mesmo em sistemas hidráulicos e pneumáticos, além dos híbridos, como os sistemas eletromecânicos (eletricidade e mecânica).

Um ponto polêmico é aquele relativo ao termo “sistema aviônico”. Os principais sistemas chamados aviônicos da Parte 23 estão relacionados na AC 23-8C (*Flight Test Guide for Certification of Part 23 Airplanes, página 138 e seguintes*). Percebe-se ali que são sistemas puramente eletrônicos, isto é, sistemas com unidades ou equipamentos eletrônicos. Exemplos:

- Transceptor de VHF;
- Transceptor de HF;
- Transponder;
- VOR; etc.

De fato, num passado não muito remoto, tais sistemas eram os únicos denominados aviônicos. Contudo, com a vertiginosa evolução dos equipamentos eletrônicos, estes passaram a participar também de sistemas híbridos (eletrônicos-mecânicos), e autores

mais recentes[1] passaram a considerar também aviônicos os sistemas híbridos que dependam de subsistemas ou equipamentos eletrônicos para realizarem suas funções de sistemas.

Este é o conceito de sistema aviônico utilizado neste trabalho voltado para Safety Assessment, isto é, qualquer sistema que dependa de um subsistema ou equipamento eletrônico, para realizar sua função, é aqui considerado sistema aviônico.

Um exemplo é o sistema *Fly-By-Wire,* que contém componentes mecânicos e eletromecânicos, mas que depende de um computador de controle de voo (*Flight Control Computer* – FCC) para realizar sua função.

Outro exemplo é o sistema que executa a função de frenagem da aeronave, na movimentação no solo, no pré ou pós-voo. O documento SAE ARP 4761 (Ref. 4) descreve esse sistema, para exemplificar o processo de *Safety Assessment* completo. Seu principal componente é um computador, denominado *Braking System Control Unit* (BSCU).

A propósito, o avanço dos sistemas aviônicos e suas inúmeras aplicações na aeronave são impressionantes. Para se ter uma ideia, temos informações de que mais de 30% do custo total da aeronave civil está na aviônica. Na aviação militar, essa participação é maior ainda. No caso de aviões de patrulha marítima chega a 40%. Mas pode superar os 75%, como no caso de aeronaves de vigilância e alerta, aquelas conhecidas por AWACS (*Airborne Warning And Control System).*

4. CICLO DE VIDA DA AERONAVEGABILIDADE

Qualquer atividade pertinente à Engenharia, ao longo da vida de uma aeronave, desde a constatação da necessidade de desenvolvê-la, é uma parte integrante das fases que, em seu conjunto, chamamos de Ciclo de Vida de um Sistema (CVS) Esse ciclo é básico para a metodologia de ES, sendo dividido em fases[2], tais como: Fase Conceitual, Fase de Projeto Preliminar, Fase de Projeto Avançado, Fase de Preparação da Produção/Produção propriamente dita e Fase Operacional. Se quisermos comparar, guardando as devidas proporções, há semelhanças com o ciclo de vida dos seres humanos; mas, este é um outro discurso.

[1] V. Ref. 4.

[2] As fases do CVS podem diferir de autor para autor; porém, basicamente conduzem aos mesmos objetivos.

Todas as atividades da empresa ligadas ao CVS são objeto da Engenharia de Sistemas (ES).

Paralelamente a esse conceito, há outro que segue par e passo o CVS. É o chamado Ciclo de Vida da Aeronavegabilidade (CVA), cujas atividades interagem com aquelas do CVS. O grande objetivo das atividades do CVA é a segurança de voo, no sentido de manter, durante o CVS, uma alta probabilidade de a aeronave se deslocar, de um ponto para outro, sem riscos de monta, atendendo aos requisitos de segurança estabelecidos pela Autoridade.

Nossa preocupação, neste trabalho, é com o CVA, mas sempre em conjunção com o CVS. É aí que se insere o processo de *Safety Assessment*.

5. CONCEITO DE SEGURANÇA (*SAFETY*) DE SISTEMAS

Num sentido amplo, há quem defina segurança como “Ausência de Perigos”. Contudo, isso é uma quimera, isto é, rigorosamente não existe. O perigo sempre existirá, ou seja, é sempre possível encontrar perigos em nossas atividades, em nossos veículos, em nossas casas (onde, aliás, revelam-nos as estatísticas, ocorre a maior parte dos acidentes), em aviões, etc. Até em templos religiosos, convenhamos, há perigos.

Contudo, em aeronáutica, o termo é mais restrito. O que queremos proteger contra perigos, na área civil, são tripulações e passageiros de uma aeronave e, num segundo momento, propriedades e meio ambiente, no solo. Já na área militar, segundo a MIL-STD-882, do Departamento de Defesa dos Estados Unidos (DoD), o que se quer primordialmente proteger são os recursos para a missão fim da Arma, por exemplo os da Força Aérea. Mas, este assunto não será objeto deste PDC.

Quando alguém nos fala em segurança, no Brasil, sem maiores explicações, podemos ficar na dúvida, ainda que momentaneamente, sobre o que nosso interlocutor esteja falando. Isso porque o termo “segurança” pode significar segurança contra atentados (assaltos, terrorismo), ou segurança com relação a efeitos de falhas não intencionais de seres humanos ou de sistemas físicos construídos por eles, que podem provocar ferimentos ou até mesmo morte. [3]

[3] Insere-se também, neste caso, a segurança de prédios e instalações, voltadas para a preservação física de seus usuários, no trato, por exemplo, de substâncias e das condições de trabalho de empresas

Já nos países de língua inglesa, são adotados dois termos, um para cada uma das acepções acima. Utiliza-se o termo *Security* para a primeira acepção (assaltos, terrorismo, etc.) e *Safety*, para a segunda (voltada para falhas não intencionais).

Nosso foco aqui se concentra na segunda acepção e volta-se para os perigos decorrentes da perda ou mau funcionamento dos sistemas das aeronaves, quaisquer que sejam suas causas.

6. FUNÇÕES DAS AERONAVES E DE SEUS SISTEMAS

O termo função é básico em *Safety Assessment*. "Básico" significa que é um conceito que tem de ser muito bem entendido pelos engenheiros que atuam no lado da empresa e da Autoridade. Falaremos sobre ele com mais profundidade no módulo II. Por enquanto, fique aqui registrado apenas um conceito muito restrito sobre seu significado, qual seja: "função é uma ação realizada por um ser humano ou por um sistema, visando obter resultados preestabelecidos". Em *Safety Assessment*, tratamos, logo no início, de funções nível aeronave, que são aquelas que movimentam a aeronave, no solo e no ar, e das funções nível sistemas, que realizam as funções nível aeronave.

Naturalmente, os equipamentos dos sistemas têm também suas funções, que vão propiciar as funções nível sistemas. Enfim, os itens (módulos e peças) de um equipamento também têm suas funções, que vão proporcionar as funções nível equipamento.

Por ser uma ação, a função é representada por um verbo e no infinitivo impessoal, por exemplo: prover, anunciar, comparar, gerar, determinar..., etc . Todavia, tem sido uso comum utilizar também expressões substantivas, tais como: provimento, anunciação, comparação, geração, determinação, etc.

Na aeronave, existem as chamadas funções de alto nível, aquelas pertinentes à aeronave, funções decorrentes dessas de alto nível e, até mesmo funções decorrentes destas últimas. Fala-se então de níveis de funções ou de subfunções.

(insalubridade, procedimentos, etc.), cuja preocupação se assinala à Justiça do Trabalho e ao Corpo de Bombeiros das Polícias Militares de nossos Estados.

A identificação das funções nível aeronave é obtida por meio de uma criteriosa atividade de ES denominada Análise Funcional[4], que é realizada logo no início do projeto, ou seja, na fase conceitual. O objetivo é disponibilizar as funções nível aeronaves identificadas para a engenharia de sistemas ir avante no projeto da aeronave, definindo os meios (*sistemas*) que irão realizar essas funções. Por outro lado, o processo de *Safety Assessment*, nossa preocupação, também utiliza os *outputs* (funções e subfunções) da Análise Funcional como inputs para a FHA (*Functional Hazard Assessment*), a primeira atividade de *Safety Assessment*.

A Análise Funcional será tratada com mais profundidade no módulo II deste PDC 01.

7. CONCEITO DE *SAFETY ASSESSMENT*

O termo Safety *Assessment* é a expressão atribuída a uma avaliação de engenharia, qualitativa e/ou quantitativa, para demonstrar à Autoridade que os sistemas que realizam as funções da aeronave incorporam os requisitos decorrentes daqueles atribuídos às funções da aeronave pela Autoridade.

Trata-se de uma avaliação *top-down*, ou seja, inicia-se com a alocação (inserção) dos requisitos qualitativos e quantitativos (faixas de probabilidades de falha) da Autoridade às funções da aeronave, com foco naquelas essenciais e críticas para o voo e pouso seguros, gerando, a partir desses requisitos, os requisitos dos sistemas, isto é, dos meios que proporcionarão as funções da aeronave.

Ao final, por meio de um relatório circunstanciado, demonstra-se à Autoridade que os sistemas instalados de fato incorporam os requisitos de segurança decorrentes da Autoridade e alocados às funções da aeronave.

Safety Assessment, em sua totalidade, pode desenvolver-se por meio de um conjunto de avaliações qualitativas e quantitativas, tais como FHA (*Functional Hazard Assessment),* PSSA *(Primary System Safety Assessment) e* SSA *(System Safety Assessment)*, utilizando ferramentas como FTA (*Fault Tree Analysis)* ou DD - *Dependence Diagrams*

[4] A Análise Funcional também será apresentada com mais detalhes no Módulo II.

(as duas têm o mesmo objetivo), FMEA (*Failure Modes, and Effect Analysis*) [5] e *Common Cause Analysis* (CMA). .

No entanto, nem sempre é necessário desenvolver esse cabedal de avaliações e análises, numa *Safety Assessment*. O desenvolvimento *in totum* dessas avaliações vai depender de alguns fatores, como teremos a oportunidade de mostrar no Módulo II.

No que tange às análises quantitativas, onde entram valores de probabilidades de falhas, o leitor vai necessitar de uma base mínima da área do cálculo das probabilidades. Essa base está apresentada no **Apêndice A** deste módulo.

Conforme se pode deduzir das considerações acima deste item, *Safety Assessment* é também uma ferramenta de alocação (inserção) de requisitos de segurança no projeto dos sistemas. Desse modo, *Safety Assessment* pode ser considerada como tendo um duplo objetivo: incorporação de requisitos de segurança nos sistemas, partindo dos requisitos nível aeronave, e demonstração à Autoridade de que esses requisitos estão de fato incorporados no projeto dos sistemas.

> ***Nota**: Por oportuno, assinalamos que, daqui em diante, usaremos simplesmente o termo "requisito", ficando subentendido que se trata de "requisito de segurança".*

7.1 Abrangência do Processo de *Safety Assessment*

De fundamental importância é entender que o foco do *Processo Safety Assessment* está nos sistemas da aeronave, isto é, aquela parte ativa[6] responsável pela geração das funções nível aeronave, que vão ser utilizadas pelo piloto, no comando e controle da aeronave. Nada mais lógico. Deste modo, rigorosamente, o piloto é o foco central. A aeronave, convenhamos, é um corpo inerte, cheio de funções, que, no entanto, só se movimenta sob a batuta de um piloto (tripulação).

Com "parte ativa responsável pela geração das funções da aeronave", queremos dizer que há um bocado de outras coisas da aeronave fora disso. De fato, há mesmo, uma vez que *Safety Assessment* não se aplica a partes estruturais da aeronave (asas, fuselagem, empenagens, superfícies de comando, cabos de controle mecânico de voo, alavancas, berços de motor e elementos estruturais do trem de pouso).

[5] Essas ferramentas estão muito bem apresentadas na ARP 4761.

[6] "Parte ativa" significa meio ativo (sistema) que disponibiliza à tripulação uma função, para o comando e controle da aeronave.

Além de não se aplicar a partes estruturais, também não se aplica aos requisitos de desempenho e de características de voo. Mas, aqui vai a sutileza: *Safety Assessment* aplica-se aos sistemas que realizam as funções que propiciam a incorporação dessas características. Assim, por exemplo, *Safety Assessment* não se aplica às características de *stall* inerentes à aeronave, mas se aplica ao sistema de Alarme de *Stall* (S*tick Pusher) ou* Barreira de *Stall (stall barrier).*

8. PARTICIPAÇÃO DOS SISTEMAS DA AERONAVE NOS ACIDENTES CATASTRÓFICOS[7]

Falamos o tempo todo de sistemas; mas, afinal, qual é a participação dos sistemas da aeronave, nos acidentes catastróficos? Para responder a esta pergunta, devemos nos reportar a um árduo trabalho estatístico, realizado na década de 1970, para determinar a taxa global de acidentes catastróficos de toda a frota de aviões comerciais ocidentais[8]. Esse trabalho mostrou que, nesse período, só 10% dos acidentes catastróficos foram causados por falhas dos sistemas da aeronave. Entre 70% e 75%[9] foram atribuídos a erros da tripulação.

Com relação aos sistemas, constatou-se que a taxa de falhas (probabilidade de falha por hora de voo) daqueles responsáveis por acidentes catastróficos era um pouco menor que 1×10^{-9} (um acidente para cada um bilhão de horas voadas pela frota).

Desse modo, nos parece sensato que quando alguém fosse viajar e rezar para não ocorrer um acidente, deveria fazê-lo focado na tripulação, rogando para que ela estivesse bem treinada, que tivesse tido uma boa noite de sono e que entrasse no avião com a única preocupação de desempenhar bem seu papel.

Mas e os outros 30% ou 25% dos acidentes catastróficos, a quem ou a que atribui-los?

Citamos, de pronto, a manutenção como uma fonte não desprezível dos acidentes.

Aí, devemos considerar também as agressões ambientais externas, como por exemplo, o "bombardeamento" eletromagnético, oriundo dos campos irradiados de alta intensidade (*High Intensity Radiated Fields* – HIRF), originados de transmissores

[7] V. Referência 1.
[8] A adoção da estatística voltada apenas para o mundo ocidental justificava-se porque do lado oriental, pelo menos na época, não havia dados minimamente organizados.
[9] Há controvérsias nesses percentuais, mas não fogem muito desses valores.

instalados principalmente em terra, além de fatores meteorológicos (granizo, vento, chuva). Tudo isso pode fazer com que alguns sensores dos sistemas da aeronave gerem, ao final, informações erradas para a tripulação, em relação ao que de fato estaria ocorrendo no meio exterior à aeronave (*misleading*). Enfatizem-se ainda, nesse agressivo ambiente meteorológico externo, os raios (*lightning*), que podem deixar "malucos" sistemas eletrônicos.

Ainda temos de levar em consideração as falhas do controle de tráfego aéreo, com orientações erradas, além daquelas falhas dos auxílios de rádio à navegação, instalados em terra[10].

Mas, deixemos bem claro que, neste trabalho, estaremos preocupados apenas com os acidentes consequentes de <u>falhas ou mau funcionamento dos sistemas da aeronave, inerentes ao projeto e a agressões ambientais</u>, isto é, só com a parcela de dez por cento das causas dos acidentes catastróficos. Trata-se da parcela sobre a qual temos algum controle. É aí, salientamos, que se concentra o esforço da *Safety Assessment*.

No **Apêndice B** deste módulo, apresentamos um desenvolvimento matemático dos passos que levaram ao valor ($< 10^{-9}$) para a taxa de falha relativa aos acidentes atribuíveis a sistemas da Parte 25, que serviu de base para a Parte 23.

[10] Basta imaginar a perda de um dos equipamentos do sistema ILS (*Localizer, Glide Slope* e *Markers*), instalados nos aeroportos e utilizados pelo piloto, no momento de um pouso por instrumento.

REFERÊNCIAS:

1. *DE FLORIO, Felippo, Airworthiness – An Introduction to Aircraft Certification. Elsevier Ltd., 2nd Ed., MA, EUA, 2011.*
2. *BLANCHARD, Benjamin S. - FABRICKY, Wolter J. Systems Engineering and Analysis. 4. Ed., EUA, 2006.*
3. *MOSS, T.R. and ANDREWS J.D., Reliability Assessment of Mechanical Systems. Proceedings of the Institution of Mechanical Engineers, Part E: Journal of Process Mechanical Engineering, 210 (3), pp. 205-216, (UK), 1996.*
4. *SAE ARP 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment. SAE, EUA, 1996.*
5. *MODARRES, M. Reliability and Risk Analysis. Cincinnati – Ohio (EUA): Marcel Dekker, Inc., 1993.*
6. *O'CONNOR, P.D.T. Practical Reliability Engineering. John Wiley & Sons, Inc., New York (EUA), 1991.*

APÊNDICE A

BASE MATEMÁTICA MÍNIMA PARA O ESTUDO DA *SAFETY ASSESSMENT* – FALIBILIDADE E TAXA DE FALHA

A1 – FALIBILIDADE (*FALLIBILITY* ou *UNRELIABILITY*)

Começamos, tratando da chamada Função de Distribuição Cumulativa de Probabilidades (do Ing.: *Cumulative Distribution Function* – CDF), denominada Falibilidade (*Fallibility* ou *Unreliability*), representada pela letra F, utilizada na área de segurança (*Safety*) de sistemas de aeronaves.

F aponta, para cada intervalo de tempo t, a probabilidade de um item[11] falhar naquele intervalo.

A Falibilidade é uma função complementar da conhecida função Confiabilidade, R, que aponta, para cada intervalo de tempo t, a probabilidade do item não falhar nesse intervalo.

R e F são funções complementares e mutuamente exclusivas. Portanto, obedecem à relação:

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

Essa expressão nos parece óbvia porque a probabilidade de não falhar (R) ou a probabilidade de falhar (F) é 1 (100%), uma vez ser certo que ou a falha ocorre ou não ocorre.

Desse modo, podemos escrever:

$$\mathbf{F = 1 - R} \qquad (2)$$

A função R depende do tipo de sistema (eletrônicos, elétricos e mecânicos).

[11] Estamos seguindo neste Apêndice a nomenclatura adotada pela norma NBR 5462 – Mantenabilidade e Confiabilidade, segundo a qual *Item é qualquer parte, componente, dispositivo, subsistema, unidade funcional, equipamento ou sistema que possa ser considerado individualmente (nota: um item pode ser eventualmente uma pessoa).* Portanto, um avião ou qualquer um de seus equipamentos, por exemplo, é um item; porém, o uso do termo deve ser parcimonioso, para não gerar confusão..

Em se tratando de sistemas puramente eletrônico/elétricos, a função de distribuição de probabilidades denominada Confiabilidade é a chamada exponencial negativa dada por:

$$R = e^{-\lambda t} \qquad (3)$$

Onde λ é uma constante denominada Taxa de Falha.

A figura A1 apresenta as curvas da Confiabilidade e da Falibilidade.

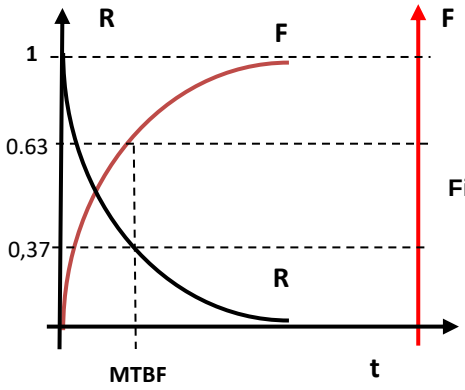

Fig. A1 – Curvas de R e F

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 é 0,37 (37%).

É fácil ver que quando maximizamos F, minimizamos R.

A exponencial negativa tem uma propriedade curiosa e 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 estivesse começando a operar pela primeira vez, ou seja, o item não se "lembra" de ter operado antes.

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

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

$$e^{-\lambda t} = 1 + \frac{(-\lambda t)}{1!} + \frac{(-\lambda t)^2}{2!} + \frac{(-\lambda t)^3}{3!} + \ldots \qquad (4)$$

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

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

Tendo em conta a (2), podemos escrever para a falibilidade:

$F = 1 – (1 - \lambda t) = \lambda t$

Portanto, $\mathbf{F = \lambda t}$ (5)

Trata-se da equação de uma reta com coeficiente angula igual a λ.

Observe que se t = 1, $\mathbf{F = \lambda}$.

Esta equação é fundamental para *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.*

A2 - TAXA DE FALHA

Mostra a prática que a taxa de falha, 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, durante toda ou quase toda a vida operacional do sistema.

As figuras A2 e A3 dão uma ideia da variação da taxa de falha desses dois tipos de itens, numa mesma escala de tempo.

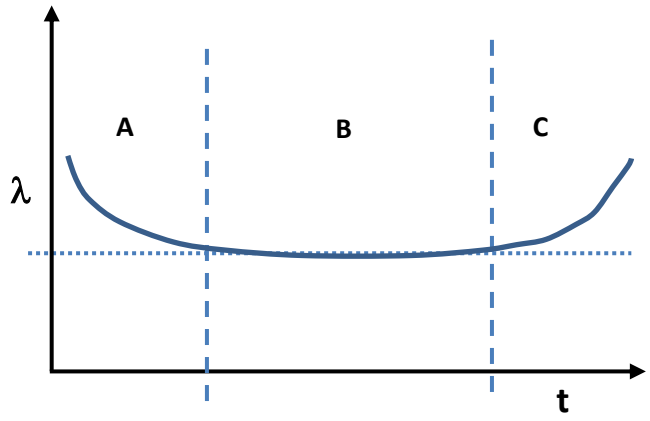

Fig. A2 Taxa de Falha típica de itens eletrônicos/elétricos

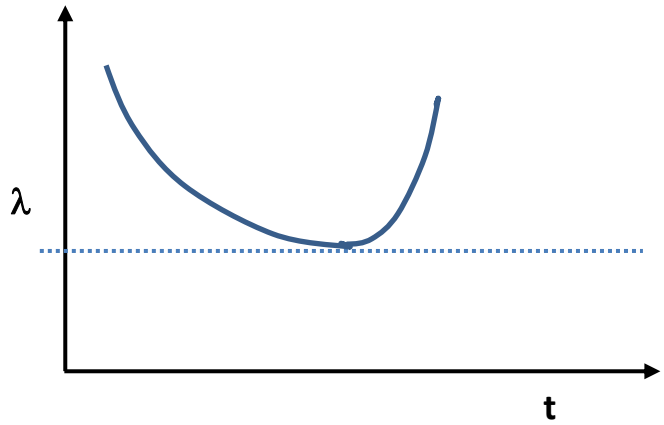

Fig. A3 Taxa de Falha típica de itens mecânicos

Na figura A2, a região denotada por A é denominada Região de *Debugging* ou de Mortalidade Infantil, caracterizada por falhas iniciais atribuídas a defeitos no projeto, fabricação ou construção. A taxa de falha começa alta; mas, depois, as correções de engenharia e de processo de produção vão proporcionando a redução dessa taxa, até o ponto em que ela começa a ficar aproximadamente constante[12]. 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 5. A região C é a região de desgaste (*wearout*), fase em que a taxa de falha assume uma derivada positiva, iso é, com valores crescentes.

Rigorosamente, a equação $F = \lambda t$ só se aplica bem a equipamentos eletrônicos e elétricos, na região de projeto maduro, em virtude de terem esses itens, nessa região, taxa de falha aproximadamente constante.

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

Não é o caso dos sistemas mecânicos[13], como pode ser observado na figura A3, que apresentam uma taxa de falha variável ($\lambda = \lambda(t)$), sendo decrescente na fase inicial, passando por um mínimo, para depois se tornar crescente (fase de desgaste – *wearout*).

Contudo, no cálculo de probabilidades, utiliza-se a mesma equação utilizada para equipamentos eletrônicos ($F = \lambda t$), assumindo-se que a taxa de falha fornecida pelo fabricante seja constante.

Esse procedimento é seguro, desde que a taxa de falha do sistema mecânico, anunciada pelo fabricante, não esteja muito próxima da fase de desgaste (*wearout*), isto é, esteja ainda na fase decrescente. 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*) para o sistema ou para o equipamento responsável pela falha do sistema.

[13] Vide Ref. 2

APÊNDICE B

DEMONSTRAÇÃO ESTATÍSTICA DA PARTICIPAÇÃO DOS SISTEMAS DA AERONAVE, NOS ACIDENTES CATASTRÓFICOS

Na década de 1970 a 1980, um longo trabalho estatístico mostrou, inicialmente, que a taxa global de acidentes catastróficos de toda a frota de aviões comerciais ocidentais[14] era pouco menor que 1×10^{-6} (um acidente em um milhão de horas).

Em números: $\frac{N_C}{10^6} < 1 \times 10^{-6}$, onde N_C é o número total de acidentes catastróficos.

Considerando a grande quantidade de horas envolvidas (10^6), o valor acima pôde ser considerado como a probabilidade de falhar por hora de voo, obtida segundo o conceito empírico de probabilidade, ou seja:

$$P = \lim_{N \to \infty} \frac{n}{N} \ ,$$

onde n é o número de falhas observadas, e N, o número de horas computadas. (Admitindo-se que 10^6 seja um número suficientemente grande de horas)

No entanto, a análise das causas desses acidentes, como já dissemos, evidenciou que apenas 10% resultaram de falhas de sistemas. Em números:

$$\frac{N_C}{10^6} = \frac{N_S + N_O}{10^6} = \frac{0{,}1N_C + 0{,}9N_C}{10^6},$$

onde N_S é o número de acidentes atribuídos a sistemas, e N_O é o número de acidentes atribuídos a outras causas.

Desse modo, a parte atribuída a sistemas foi:

$$\frac{N_S}{10^6} = \frac{0{,}1\ N_C}{10^6} < 0{,}1\ (1 \times 10^{-6}) = 1 \times 10^{-7}.$$

Partindo de uma hipótese arbitrária, mas conservativa, estabeleceu-se que uma aeronave poderia apresentar cerca de 100 potenciais condições de falhas catastróficas atribuíveis a sistemas, em grandes aeronaves comerciais. Desse modo, ter-se-ia um

[14] A adoção da estatística voltada apenas para o mundo ocidental justificava-se porque do lado oriental não havia dados minimamente organizados.

subconjunto de eventos do espaço amostral das condições de falhas catastróficas constituído por 100 eventos, um para cada falha catastrófica atribuível a sistemas. Poder-se-ia então representar tal subconjunto por

$\mathbf{C} = \{C_1 , C_2 , C_3 , \ldots , C_{99} , C_{100}\}$,

onde C_i é um evento catastrófico genérico atribuível a sistemas.

Teríamos então $P(C) = P(C_1) + P(C_2) + P(C_3) + \cdots + P(C_{99}) + P(C_{100}) < 1 \times 10^{-7}$.

Admitindo-se que **C** seja um conjunto equiprovável[15], ou seja, que cada um de seus 100 eventos tenha a mesma probabilidade de ocorrência, teríamos:

$P(C_1) = P(C_2) = P(C_3) = \cdots = P(C_{99}) = P(C_{100}) = P(C_i)$.

Resulta então que $P(C) = P(C_1) + P(C_2) + P(C_3) + \cdots + P(C_{99}) + P(C_{100}) = 100\ P(C_i)$.

Portanto, $100 \times P(C_i) < 1 \times 10^{-7} \Rightarrow P(C_i) < \frac{1 \times 10^{-7}}{10^2}$,

ou $\boxed{\mathbf{P(C_i) < 1 \times 10^{-9}}}$

Esse valor de probabilidade (ou taxa de falha por hora de voo) gerou o requisito de máxima probabilidade de ocorrência aceitável para um acidente catastrófico devido a falhas de um sistema de uma aeronave[16].

Como já apresentado no texto, a aeronave não se precipita apenas em decorrência de falhas de sistemas. A principal causa ainda está no ser humano. Há profissionais dedicados pensando nisso, mas esse notável movimento em curso não se inclui no objetivo deste trabalho. Talvez, tenhamos, num futuro próximo, a oportunidade de comentar esse movimento, mas, sempre nesse ritmo de “comer o boi por bifes”.

E os Veículos Aéreos Não Tripulados (VANT - *Drones*)? Bem, nesse caso, poderiam dizer alguns, os acidentes são devidos somente a falhas de sistemas. Será? E o ser humano que está na estação terrestre, comandando o VANT?

[15] Rigorosamente, isso não é verdade, mas tendo em conta que, para a análise, o interesse está na faixa atribuída a cada severidade, e não no valor exato, podemos considerar um único e genérico valor representativo de probabilidade para cada evento de cada faixa, que, neste caso, é a faixa dos eventos catastróficos.

[16] No Módulo II, trataremos dos requisitos de segurança *(Safety Assessment*) aplicáveis aos sistemas.

Esta é uma situação bem semelhante àquela dos sistemas de controle de tráfego aéreo, como, por exemplo, um radar de vigilância, em que o piloto é “substituído” por um controlador de tráfego aéreo. O controlador não está no radar, como o piloto na aeronave, mas numa sala confortável, recebendo as informações do radar para controlar o tráfego aéreo.