System Safety Assessment: Ciência ou Arte?

Berquó, Jolan Eduardo – Eng. Eletrônico (ITA)

Certificador de produto Aeroespacial (DCTA/IFI)

Representante Governamental da Garantia da Qualidade – RGQ (DCTA/IFI)

Pós-graduado em Engenharia de Confiabilidade e em Engenharia de Segurança de Sistemas (ITA)

Especialização em Engenharia e Análise de Sistemas (Itália)

jberquo@dcabr.org.br/jberquo@uol.com.br

MSC 62 – 10Jun2017

Aqui estamos, novamente; desta feita, martelando na Avaliação de Segurança de Sistemas (System Safety Assessment), assunto que recentemente, diríamos, exploramos com alguma profundidade, nos três módulos do PDC-01 – “Interpretando a Visão da Autoridade de Aviação Civil, no Processo de Safety Assessment”. Por ser um tema continuamente controverso entre os que se postam como analistas nessa área, resolvemos explorar um pouco mais o assunto, procurando aguçar o entendimento de todos que se interessam pelo tema. Tentaremos responder à pergunta que sustenta o título deste MSC: “Afinal, como classificaríamos o Processo de Safety Assessment: Ciência ou Arte?”.

O tema pode parecer irrelevante; mas, não o consideramos assim. É importante para os que resolverem entrar nessa área, ou até mesmo para os que já estão nela, terem uma visão mais pragmática do processo de SSA, evitando, talvez, possíveis frustrações.

Primeiramente, um pouco de história da SSA. Antes da década de 1960, a SSA era realizada por meio da já lendária FMEA (*Failure Modes and Effect Analysis*). O panorama da SSA, no entanto, mudou, quando em 1965 surgiu o projeto Concorde, com entrada em serviço em 1978.

Nesse desenvolvimento, ficou evidenciado que uma nova concepção de SSA estava presente, decorrente de uma grande interação funcional entre os sistemas das aeronaves de grande porte, i. e, passou a haver sistemas cujas funções dependiam claramente das funções de outros sistemas. Surgia então, inevitavelmente, o enfoque funcional da atual SSA. Descortinava-se, enfim, uma nova era.

Contudo, a FMEA não saiu de cena; antes, praticamente única, no processo de *Safety Assessment*, ela passou a fazer parte de uma das etapas do novo processo.

Procurando ser didáticos, vamos assinalar, neste ponto, o objetivo da SSA, como se depreende dos atuais regulamentos das Autoridades de Aeronavegabilidade (FAA, EASA e ANAC). É objetivo da SSA:

“Demonstrar à Autoridade que os sistemas da aeronave e seus equipamentos, considerados separadamente e em relação aos outros sistemas, sejam projetados de maneira que:

- (1) qualquer *Catastrophic Failure Condition*¹
 - a. seja extremamente improvável; e
 - b. não resulte de uma falha simples (*singular failure*).
- (2) qualquer *Hazardous Failure Condition* seja extremamente remota; e
- (3) qualquer *Major Failure Condition* seja remota”.

Parece muito simples; contudo, quando se esmiúça o processo da SSA, para atingir esse objetivo, vão surgindo as dúvidas; por exemplo: “O que significa Extremamente Improvável, Extremamente Remota ou apenas Remota”? Se a Autoridade simplesmente deixasse esses requisitos de segurança de sistemas assim expressos, provavelmente surgiria uma avalanche de questionamentos, quanto à subjetividade da interpretação de um e de outro analista.

¹ *Failure Condition* (Condição de Falha): Potencial efeito de uma falha ou mau funcionamento de um sistema.

Parece-nos então razoável acreditar que tenha sido por essa razão que vieram à tona os requisitos quantitativos, isto é, que tenham sido inseridos valores numéricos, ou melhor, faixas de valores de probabilidades, com limites máximos de permissividade para a severidade de cada *Failure Condition*².

Essa inserção de faixas de probabilidades, configurando os requisitos quantitativos, como já tivemos a oportunidade de discutir, em MSC's anteriores e, recentemente, no PDC-01, foi baseada na análise estatística dos acidentes catastróficos, desenvolvida na década dos anos 70, com a conclusão de que os sistemas eram responsáveis por apenas 10% desses acidentes.

A subjetividade então parou por aí? Parou nada. De posse dos requisitos qualitativos e quantitativos, os analistas dos Aplicantes (ou Requerentes), mui naturalmente, cremos, devem ter questionado: "E aí, como fazemos para demonstrar isso?".

Veio então o desejável socorro da Autoridade, por meio de sugestões aos Aplicantes, para a demonstração de conformidade dos sistemas de suas aeronaves com os requisitos qualitativos/quantitativos de *safety*. Esse auxílio veio por meio das *Advisory Circulars* do FAA, ou dos documentos análogos das demais Autoridades.

Tais documentos propuseram uma metodologia, isto é, um processo, a título de sugestão, sobre "o que fazer", para realizar uma avaliação de segurança (*Safety Assessment*).

No entanto, não satisfeita com o conteúdo desses documentos, para a etapa seguinte do "como fazer", a Comunidade Aeronáutica se debruçou no assunto e com o auxílio da *SAE Aerospace* constituiu os comitês S-18 e WG-63 (*Working Group 63*), para desenvolver, respectivamente, os documentos SAE ARP 4754 (Ref. 1) e SAE ARP 4761 (Ref. 2).

A propósito, o desenvolvimento da ARP 4754 contou com a presença de três membros brasileiros (ANAC, Embraer e CTA-IFI). O desenvolvimento da ARP 4761, infelizmente, não teve a presença de brasileiros.

Esses documentos, embora muito bem intencionados, em nossa opinião não aliviaram muito as dificuldades dos Aplicantes. As controvérsias, nas interpretações do assunto, continuaram e assim ocorrem até hoje. É difícil encontrar dois analistas de *Safety Assessment* sequer proximamente com a mesma interpretação. Essa dificuldade é gerada, em nossa opinião, pela subjetividade na interpretação do processo de SSA.

Diante desse quadro, decidimos seguir a linha de nos concentrar nas AC's da FAA e documentos análogos de outras Autoridades, contando, no entanto, como coadjuvantes, as mencionadas ARP's.

Essa dificuldade de harmonizar posições de vários analistas levou-nos, claramente, a **considerar a SSA mais como arte do que ciência**³. Ficou-nos patente que as metodologias sugeridas não levavam a práticas de eficácia inequívoca. Em grande parte, assim concluímos, ficaria o trabalho ao sabor da habilidade (*skill*) ou genialidade do Analista, restando, ao final, o inevitável e inapelável crivo ou julgamento da Autoridade.

O que de fato está bem estabelecido é o encadeamento das etapas do processo, isto é, a metodologia do processo, e aí entra a parte mais ligada ao aspecto científico. Esse processo ficou claro nos documentos SAE 4754 e 4761, compreendendo a seguinte sequência de avaliações: FHA (*Functional Hazard Assessment*) nível aeronave, FHA nível sistemas, PSSA (*Preliminary System Safety Assessment*), SSA (*System Safety Assessment*) e CCA (*Common Cause Analysis*).

Mas, novamente, a maneira como deveriam ser realizadas (como fazer) essas avaliações continuavam, claramente, dependendo da habilidade do analista. Uns omitindo considerações importantes, enquanto outros se excedendo nos detalhes, tornando o processo até mesmo enfadonho.

Esta é a nossa interpretação, caro leitor. Não obstante, fique à vontade para contrariá-la. A nós, creia, agradaria muito conhecer os argumentos de outros pontos de vista.

² Por exemplo: $F < 10^{-9}$ /(hora de voo), para *Failure Conditions* com potencial catastrófico.

³ Os dois conceitos estão presentes na SSA; mas, numa análise pessoal crítica, diríamos que prevalece a "arte".

Por importante, informamos que essa discussão fará parte do curso que ministraremos sobre o PDC-01, na DCA-BR, em julho do corrente ano.

Um abraço a todos.

Referências:

- (1) *SAE ARP 4754A Guidelines for Development of Civil Aircraft and Systems*, EUA, 2010
- (2) *SAE ARP 4761 - Guidelines and Method for Conduction the Safety Assessment Process on Civil Airborne Systems and Equipment*, EUA, 1996.
- (3) *FAA: AC 25.1309-1A, System Design and Analysis*, EUA, 21/06/1988.
- (4) *FAA: AC 23.1309-1E, System Safety Analysis and Assessment for Part 23 Airplanes*, EUA, 2011.