SAE ARP 4761: Excelência de Procedimento para a Avaliação de Segurança (*Safety Assessment*)

***Berquó**, Jolan Eduardo – Eng. Eletrônico (ITA)·.*
Certificador de Produto Aeroespacial (DCTA/IFI)
Representante Governamental da Garantia da Qualidade – RGQ (DCTA/IFI)
jberquo@dcabr.org.br

MSC 37 – 04 JUN 2013

Vamos apresentar, neste MSC, uma análise sobre a importância da ARP 4761, documento desenvolvido pelo Comitê S-18, instalado na *SAE Aerospace*, um grupo da *SAE International*, documento este voltado para a realização de Avaliação de Segurança (*Safety Assessment*) para aeronaves civis de grande porte, e considerado pela FAA como uma metodologia aceitável para demonstrar a conformidade com os requisitos de segurança do CFR 14 Part 25.1309 (FAR 25.1309). Concluiremos com um desafio aos analistas de segurança que nos leem.

Já tratamos da ARP 4761, nos MSC 09, 10 e 11, que versam sobre a Avaliação de Segurança, documento que está atrelado à ARP 4754 (*Guidelines for Development of Civil Aircraft and Systems*), mas não nos aprofundamos, naquela ocasião, nos motivos pelos quais imaginamos que teriam levado a SAE a criar o S-18 para elaborar a ARP 4761.

Começamos, assinalando que a AC (*Advisory Circular*) 25-1309-1A, que, como todas as AC, foi elaborada como uma tentativa de ajudar o requerente de certificação, no caso, na avaliação de segurança, visando os requisitos (b), (c) e (d), do FAR 25.1309, não é um documento de fácil entendimento, em termos de sequenciamento lógico do processo que propõe.

Trata-se de um documento muito bem intencionado, mas seus parágrafos, em nossa opinião, não são por si só concludentes. Trata, por exemplo, de uma determinada tarefa, num parágrafo, relacionando-a com várias outras, em outros parágrafos, adiante ou já tratadas algures, trazendo, nesse vai e vem, razoável dificuldade para o analista.

Quem pretenda resumir a AC, tentando torná-la mais palatável, terá uma árdua tarefa pela frente, digna, quem sabe, de uma monografia. Sabemos bem disso porque já realizamos esse trabalho.

Por isso, acreditamos que não foi nenhuma surpresa que uma entidade do calibre da SAE organizasse um comitê (S-18), que propusesse a metodologia registrada na ARP 4761. A lógica do processo ali contido é cristalina, embora seja um tanto complexa, mas só e somente só em virtude das intermináveis iterações, ao longo do processo. Ela, sem dúvida, é muito mais iterativa que sequencial.

Mas a ideia contida na 4761 de desenvolver a Avaliação de Segurança, partindo das funções da aeronave, por meio da FHA (*Functional Hazard Assessment*), num processo "top-down", foi simplesmente genial. Aliás, nesse contexto, não podemos deixar de parafrasear o grande e estimado professor brasileiro Francisco Antonio Lacaz Neto, que foi inclusive reitor de nosso Instituto Tecnológico de Aeronáutica (ITA), de São José dos Campos (SP). Disse-nos ele, numa certa ocasião: "As grandes ideias são simples".

Acreditamos então que até foi muito bom ter surgido a AC 25.1309-1A, tentando ajudar os requerentes de certificação, porque ela motivou a comunidade aeronáutica americana, por meio da SAE, a desenvolver um processo decididamente voltado para simplificar a sugestão contida nessa AC. Se ela, a AC, fosse simples, convenhamos, não seria necessário elaborar a 4761.

O mais interessante é que a ideia contida nas ARP 4754 e 4761 já existia latente na Engenharia e Análise de Sistemas (EAS). Mas a SAE, sem fugir da metodologia da EAS, introduziu um processo deveras mais claro e simplificador.

Como dissemos, ela é complexa, mas apenas pelo seu intenso ritmo iterativo; mas o importante está na simplicidade da lógica do processo que nos propõe, não nos deixando matutando, tanto quanto o fazemos, quando

resolvemos seguir estritamente a AC 25.1309-1A.

Vamos interpretar agora o raciocínio da ARP. "Uma aeronave é uma coisa que foi feita para voar. Para isso, ela necessita de outra coisa chamada sistema moto-propulsor. Ela não levantaria voo se não tivesse sido pensado em alguma coisa que lhe propiciasse correr numa pista até chegar a uma velocidade que a permitisse decolar e aterrissar: o trem de pouso. Outra coisa fundamental também para decolar, aterrissar e controlar atitudes de voo são aquelas coisas chamadas superfícies de comando de voo. Para se orientar no ar, quando voando, é necessária outra coisa que promova essa orientação. E assim vai, de coisa em coisa. Mas a coisa mais importante é a coisa falível chamada piloto".

O fato é que cada coisa tem sua função. Pode-se identificar então uma série de funções da aeronave. Várias são absolutamente críticas, se faltarem. São aquelas cuja falta pode conduzir a acidentes catastróficos; a falta de outras, sem serem catastróficas, pode, no entanto, levar a situações de intenso trabalho para a tripulação e desconforto a passageiros, enquanto a falta de outras não conduzem a consequências maiores.

Pensamos então, de maneira natural, que seja fácil perceber que devêssemos iniciar nosso trabalho de Avaliação de Segurança, avaliando as consequências da perda das funções da aeronave. Contudo, pode parecer simples identificar todas as funções que deverão estar presentes numa aeronave, mas o fato é que, dependendo da complexidade da aeronave, essa identificação é difícil, requerendo capacidade e experiência, por parte dos engenheiros envolvidos nessa labuta. Imaginemos a quantidade de funções de uma aeronave como as do Boeing 787 ou as do Airbus 380.

Tanto é assim que a ARP 4761, sabiamente, admite que a primeira identificação das funções da aeronave deva ser considerada como preliminar. No desenvolvimento posterior dos sistemas e de sua arquitetura, podem surgir mais funções. Aí é que está um dos motivos da intensa iteratividade da ARP.

Bem, mas o fato é que, uma vez identificadas preliminarmente as funções da aeronave, o processo segue com a alocação dos requisitos de segurança a cada função identificada. São requisitos provenientes do FAR 25.1309, já mencionados, requisitos dos potenciais clientes e requisitos da própria empresa.

É notável a utilização da técnica da *Fault Tree Analysis* (FTA), nessa alocação de requisitos de segurança às funções da aeronave, e, posteriormente, às funções dos sistemas. Outras técnicas são sugeridas na 4761, mas a FTA é, de longe, a mais utilizada. É um tipo de análise que usa os axiomas e propriedades do Cálculo das probabilidades, associados com a Álgebra de Boole, em sua "Teoria dos Conjuntos" da Matemática.

É só um pulo sair das funções da aeronave e prosseguir na identificação das funções dos sistemas necessários à realização das funções da aeronave, e realizar as respectivas alocações de requisitos de segurança a esses sistemas.

Nesse momento, como dissemos, podem surgir novas funções para a aeronave ou novas funções para os sistemas. A realidade é que o processo é extremamente iterativo, bem mais iterativo que sequencial.

Definidos os sistemas, com seus requisitos alocados, passa-se à identificação dos itens (principalmente equipamentos) que vão constituir esses sistemas. Nessa fase, os projetistas arquitetam a interligação dos itens, desenvolvendo então processos de instalação na aeronave.

Conceitualmente, é esse o processo, mas para desenvolvê-lo, como já mencionamos, são consideradas outras técnicas de análise, além da FTA.

O grande mérito da 4761, enfim, é apresentar um processo que pode ser uma excelente alternativa à AC 25-1309-1A e que tem a anuência da Autoridade de Aeronavegabilidade (FAA e nossa ANAC). O processo também pode ser aplicado para a demonstração de conformidade com os requisitos do FAR 23.1309, tendo em conta apenas as observações de cautela contidas na AC-23.1309-1E.

Mas atentem para o seguinte: após conhecerem bem a 4761, e sabendo do propósito da AC 25.1309-1A (ou da 23.1309-1E), o analista pode estabelecer seu próprio procedimento, tomando como base a 4761. Isso é possível porque, como registram as AC mencionadas, não há uma única maneira para comprovar a conformidade com os requisitos de segurança do FAR 25.1309 ou do FAR 23.1309.

Aliás, colocamos, para terminar, um excelente desafio para os analistas de segurança: "Desenvolvam seu próprio procedimento, para suas empresas, a partir da 4761, procurando reduzir a intensa iteratividade contida no documento (este seria o grande desafio). No mínimo, teriam a oportunidade de se aprofundarem no assunto".

Há algum tempo, estamos desenvolvendo um trabalho dessa natureza, já em fase adiantada. Pretendemos, a partir desse trabalho, desenvolver um curso. É fascinante. Desenvolvam o trabalho de vocês, mas, vejam bem, tenham paciência. Podemos fazer qualquer coisa, desde que tenhamos dedicação e paciência.

Ficamos por aqui. Até a próxima.

Referências:

(1) **SAE**: ARP 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, EUA, 01/12/1996.

(2) **FAA**: CFR 14 Part 25 § 1309, Equipment, Systems, and Installations, Amendment 25-123, EUA, 8/11/2007.

(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, 17/11/2011.