Hazard Analysis, Risk Anaslysis e *Safety Assessment*

***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 50 – 29 OUT 2014

Hazard (Perigo), Risk (Risco), Hazard Analysis (Análise de Perigo), Risk Analysis (Análise de Risco) e Safety Assessment (Avaliação de Segurança): Afinal, o que significa cada um desses termos? Neste MSC, vamos tentar responder a essa pergunta.

Há pouco tempo, um dileto amigo nos perguntou qual seria a diferença entre esses termos. Trata-se de uma pergunta muito pertinente, uma vez que, como em toda disciplina, os conceitos e definições que constituem o arcabouço da disciplina têm de estar perfeitamente entendidos, sob pena de se ter um entendimento distorcido da disciplina. É imperioso, pois, que isso seja evitado.

Vamos aqui conservar os termos em inglês, já que os profissionais da área sempre os usam nessa língua.

Os termos que vamos apresentar aqui estão definidos, por exemplo, nos CFR 14 Parts 23 e 23.1309. A propósito, antes de prosseguir, gostaríamos de expressar aqui o que entendemos por definição e conceito. Rigorosamente, definições são difíceis de serem formuladas, e quando o fazemos, quase sempre são imprecisas. Uma vez definido algo, dificilmente alguém conseguirá mudar. Diríamos então que definições são praticamente definitivas. Por exemplo: "Circunferência é o lugar geométrico dos pontos equidistantes de outro ponto chamado centro". Trata-se realmente de uma definição; jamais foi modificada.

O conceito, por sua vez, é o que se sabe ou se pensa, num certo momento, sobre alguma coisa. Com o passar do tempo e com novas informações, pode ser modificado, como amiúde ocorre.

No entanto, nos regulamentos da certificação, o termo utilizado é sempre "Definição" (*Definitions*), isto é, não se fala em conceitos. Por que isso? Exatamente porque um requerente de uma certificação de seu produto, quando se dirigir à Autoridade de Aeronavegabilidade (FAA, EASA, ANAC), para certificar seu produto, terá que usar aqueles termos com o significado que está expresso nos regulamentos pertinentes. Neste caso, e só para aquela finalidade, faz realmente sentido chamar os termos de "definições".

Pois bem, comecemos tratando do termo *Hazard* (perigo). Esse termo é utilizado para qualquer condição que possa produzir um efeito considerado adverso (perda de vida ou ferimentos de pessoas ou de exemplares da flora e da fauna; perda ou danos de bens públicos ou propriedades privadas).

Exemplo da área aeronáutica de condição que constitui um perigo: "perda da referência de atitude da aeronave, num ambiente sem visibilidade".

Devemos ter em mente que um perigo pode advir de uma falha de componentes de um sistema ou de agressões ambientais (vibrações, raios, interferência eletromagnética, etc.), que

podem mudar o comportamento do sistema, levando-o a não realizar uma ou mais funções que deveria realizar.

O perigo advém sempre da perda ou modificação de uma função do sistema.

O termo *Risk* (risco) expressa o potencial do provável efeito adverso decorrente da exposição ao perigo (*hazard*).

No caso do exemplo anterior, a exposição ao perigo pode levar ao efeito adverso de um acidente catastrófico (perda de vidas, ferimentos, perdas de exemplares da fauna, flora, etc.) ou a efeitos menos graves, mas ainda assim adversos.

É então de todo importante que conheçamos, tanto quanto possível, os perigos existentes, num projeto de um sistema, que podem levar à falência de funções desse sistema, bem como os riscos associados a cada um desses perigos.

Surge então, de forma natural, a necessidade de serem feitas análises de perigo (*Hazard Analyses*), complementando-as com as análises de risco (*Risk Analyses*). Deve-se no entanto ter em mente que a *Hazard Analysis* e a *Risk Analysis* constituem um binômio, no sentido de essas análises não poderem ser dissociadas, ou seja, só faz sentido fazer uma *Hazard Analysis* se, em seguida, for feita a respectiva *Risk Analysis* e, reciprocamente, não é possível fazer uma *Risk Analysis* sem ter sido feita a respectiva *Hazard Analysis*.

Cada área (aeroespacial – aeronáutica e espacial, nuclear, automotiva, etc.) tem sua metodologia para fazer isso, mas o conceito é sempre o mesmo, qualquer que seja a área. Nossa preocupação, entretanto, concentra-se na área aeroespacial.

Não se pode deixar para fazer essas análises no fim do desenvolvimento de um sistema. Elas têm de ser iniciadas já na fase de concepção do projeto e têm de ser atualizado, o tempo todo, à medida que o desenvolvimento do sistema prossegue.

Esse é o conceito do *Safety Assessment*, isto é, da metodologia de acesso para avaliação de um projeto, por meio de um conjunto de análises, que incluem as análises mencionadas, de modo a se certificar de que o projeto está em conformidade com os requisitos de segurança (*safety*) estabelecidos no CFR 14 Parts 23, 25, 27, 29.1309, obtendo-se então a certificação de projeto de tipo por parte da Autoridade de Aeronavegabilidade (FAA, EASA, ANAC).

Essa é a metodologia sugerida pelo documento SAE ARP 4754, desenvolvida no SAE ARP 4761. Trata-se de metodologia aceita e recomendada pelas autoridades de aeronavegabilidade. Já tratamos, numa outra oportunidade (MSC 37) dessa metodologia, ainda que de maneira breve.

Encerramos por aqui

Obrigado pela atenção.

Referências:

1. **M. Modarres**, What Every Engineer should Know about Reliability and Risk Analysis. Marcel Dekker, Inc., EUA, 1993.
2. **SAE**: ARP 4754, Guidelines for Development of Civil Aircraft and Systems, EUA, 2010 (Rev.).
3. **SAE**: ARP 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, EUA, 1996.