Melhore Seus Conhecimentos (MSC)

Safety Assessment: Conversando com Requerentes e Certificadores – I

***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 54 – 13 JUL 2015

Quando éramos alunos do curso de engenharia eletrônica do ITA (São José dos Campos), nos idos da década de 70, tivemos a oportunidade de ouvir de um grande mestre daquela instituição algumas frases que consideramos lapidares. Uma delas, dita no curso básico (os dois primeiros anos), dizia: "Neste mundo, só as coisas simples têm importância". É com esse espírito que temos tentado escrever nossos MSC; mas; neste, em especial, pela complicação como o assunto tem sido apresentado por outrem, estamos muito mais ligados a esse ensinamento.

Alguns poderiam estar pensando: "mas o que *Safety Assessment* (SA) tem a ver com a frase acima? Resposta: muito a ver, não só com *SA,* mas com tudo que se apresenta em nossa vida profissional e, quiçá, no cotidiano de nossa vida familiar e social. Contudo, queremos demonstrar aqui, tanto quanto pudermos, que a SA não é essa complicação que vemos, no cotidiano das atividades de segurança de sistemas.

De pronto, devemos apresentar o que entendemos pelos termos *Assessment* e *Analysis*, para que nos sirva de "norte", no desenrolar deste MSC.

Nosso entendimento, que comunga com aquele da AC 25-1309-1A (Ref. 1) ou 23-1309-1E (Ref. 2), da FAA (*Federal Aviation Administration*), é que *Assessment* é um conjunto de análises, que, neste contexto, nos permite avaliar a segurança do projeto de um sistema. Ora, quando se fala em "conjunto", sob o ponto de vista matemático, convenhamos, significa que este ente pode conter um ou mais elementos. No caso especial de um só elemento, estaremos diante do chamado conjunto unitário; aí, apesar de conter uma só análise, ela poderá ser chamada de *Assessment*.

Agora, vamos ao assunto propriamente dito.

O termo *Safety Assessment* não impõe uma determinada metodologia, mas uma filosofia pertinente à segurança de sistemas. Cabe aos que se proponham desenvolvê-la e concretizá-la, fazê-lo da melhor maneira que puderem. Sugestões do Universo[1], é claro, sempre serão muito bem-vindas, mas sua modelação final depende de cada área que se disponha a desenvolvê-la.

Uma coisa é certa: qualquer que seja a metodologia para realizar uma *safety assessment*, ela começa necessariamente com um binômio de análises, quais sejam: *Hazard Analysis* (HA) e *Risk Analysis* (RA*)*, que, em seu conjunto, chamamos de *Risk Assessment* (Avaliação de Risco). Não há como fugir disso. Entender isso, acreditem, é superar o primeiro marco ou obstáculo de uma SA.

De fato, perguntamo-nos: o que procuramos fazer, o tempo todo, em nossa vida, em termos de segurança? Procuramos, cremos, consciente ou inconscientemente, identificar os perigos e avaliar os riscos decorrentes (consequências), como por exemplo: morte, ferimentos leves ou

[1] Consideramos o termo Universo como sendo aquele ambiente, aquele espaço compartilhado, visando um mesmo objetivo. "Ouvir o Universo" significaria: discutir as proposta de soluções de problemas com os colegas de trabalho e partir então para a solidão da decisão".

mais ou menos graves, levando ou não a incapacidades físicas, etc.

Pois bem, ao procurar identificar o nível dessas consequências, estaremos procurando prever a severidade das mesmas. É ou não é simples assim? No entanto, se quisermos complicar, isso é fácil.

Saibam então que quando alguém lhes disser que vai realizar uma *Safety Assessment* de um sistema qualquer, forçosamente terá que realizar primeiro uma avaliação de risco (HA e RA). Isso é ponto pacífico.

Como fazer isso? Bem, aí é outro discurso. Dissemos, até aqui, "o que tem de ser feito"; agora, falaremos sobre "como tem de ser feito".

Com esse propósito, vamos considerar uma aeronave, por ser, para nós, mais familiar; contudo, a discussão, acentuamos, pode ser estendida para qualquer sistema, com as devidas adequações da área a que se refere, o que precisa ser muito bem feito, repetimos: muito bem feito, para evitar dificuldades no desenvolvimento da avaliação.

Pois bem, sabemos que para uma aeronave decolar e chegar a um destino com segurança, ela tem que estar sob a batuta de um piloto, que a comanda e controla. Isso é simples, porém fundamental: comando e controle de um piloto, eis o ponto focal.

É com esse foco que uma aeronave é projetada, isto é, com sistemas propiciando aos pilotos meios ativos para comandá-la e controlá-la. Esses meios são as funções[2] da aeronave. Só para citar uma, apresentamos, pela sua simplicidade, a que mais temos considerado em nossos MSC: "Apresentar aos pilotos sua orientação espacial", ou "Indicar ao piloto a atitude da aeronave".

Há, no entanto, muitas outras funções, sempre dentro desse conceito inarredável de dar aos pilotos meios de comando e controle da aeronave.

Outro fato importante é que, no caso de uma aeronave, os pilotos convivem com ela, ou seja, estão em seu interior, sendo então parte integrante dela. Qualquer descuido – na atitude de comando e controle, que possa levar a um acidente, eles sabem, terá reflexos neles próprios, o que nos permite afirmar que, sendo eles parte dos alvos, a preocupação deles com os riscos certamente é enorme.

Dito isso, vamos nos concentrar neste nosso primeiro quadro: funções de uma aeronave. Há várias funções e que se repetem, numa determinada classe de aeronaves; contudo, cada projeto é um projeto. Desse modo, a primeira preocupação do analista de segurança é identificar com clareza cada função.

Isso é feito com o concurso da área de Engenharia de Sistemas. É uma tarefa que tem de ser exaustiva, ou seja, ao final, não pode haver dúvida de terem sido identificadas todas as funções. Enfatizamos: não se pode ir adiante sem que essa tarefa esteja perfeitamente realizada.

Depois de cumprida, meticulosamente, a tarefa de identificação das funções da aeronave, o analista de segurança faz a seguinte pergunta, válida para todas as funções: "O que pode dar errado, caso se perca esta função ou a tenhamos distorcida, em virtude de uma falha[3]"? Nesse momento, o analista está iniciando a busca de perigos.

Pois bem, interrompemos por aqui, mas vamos continuar no próximo MSC. Queremos ser cautelosos, buscando o máximo de simplicidade que nossa capacidade e competência permitam nesse mister.

Obrigado e até o próximo MSC.

Referências:

(1) **FAA**: AC 25.1309-1A, System Design and Analysis, EUA, 21/06/1988..

(2) **FAA**: AC 23.1309-1E, System Safety Analysis and Assessment for Part 23 Airplanes, EUA, 17/11/2011.

[2] Função é uma ação. Desse modo, rigorosamente é expressa por um verbo no infinito impessoal. Contudo, pode-se usar uma expressão substantivada, dando uma denominação à função; ex.: "Indicação de atitude da aeronave"..

[3] Falha é um evento que acarreta a perda de uma função ou um mau funcionamento (o resultado obtido é diferente do esperado, ou seja, ocorre um resultado distorcido em relação ao esperado).