Safety: Há Algo de Novo no Horizonte

***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 51 – 15 JAN 2015

No MSC 48, falamos sobre as causas dos acidentes catastróficos da aviação. Colocamos ali o ser humano como o principal responsável por isso. Dissemos, inclusive, que caberia a falhas dos sistemas das aeronaves apenas a parcela de 10% de responsabilidade, e cerca de 80% seriam atribuídos ao ser humano (tripulação). Agora, que estamos com uma espécie de onda de acidentes catastróficos, consideramos oportuno tocar nesse assunto novamente, já que temos novidades alvissareiras,, em nossa opinião, nessa área de prevenção ("Before the fact"), onde o ser humano é o principal foco. Vamos conversar um pouco sobre isso neste MSC.

Sempre nos instigou essa preocupação com a segurança preventiva de aeronaves ou de qualquer outro tipo de sistema. Temos visto metodologias e suas respectivas técnicas de análise trazendo aprimoramentos nessa área, concentrando-se, contudo, apenas nos 10% da reponsabilidade pelos acidentes catastróficos: os sistemas da aeronave.

A mais recente em franca utilização e recomendada pela FAA é aquela contida nas ARP 4754 e, mais especificamente, na ARP 4761. São documentos primorosos, mas referem-se somente aos sistemas das aeronaves. O objetivo é eliminar ou mitigar os efeitos de falhas nesses sistemas. Há técnicas utilizadas na ARP 4761 que estão no foco há mais de 50 anos.

Não que sejamos contra essas técnicas; pelo contrário, são excelentes para os objetivos a que se propõem: riscos decorrentes de falhas dos sistemas das aeronaves. Contudo, o que fica em nossa cabeça é o que fazer com os erros humanos, principalmente da tripulação. Há tempos que pensamos em como atacar esse tipo de problema.

Muito bem, vemos atualmente mais uma metodologia nesse contexto, agora pensando de fato no trinômio ser humano, máquina e meio ambiente. Podemos dizer então que **há algo de novo no horizonte**. Isso nos interessou e nos levou a estudos. Este é, na realidade, o assunto deste MSC.

Conversa vai, conversa vem, em fóruns dedicados ao assunto, informações de colegas que sabem que nos preocupamos com isso, acabamos mergulhando no estudo dessa "nova"[1] metodologia, que de fato se preocupa com esse trinômio e que, de certa forma, já está sendo aplicada por algumas entidades espaciais e aeronáuticas.

Contudo, como toda metodologia que se insere, há prós e contras. É a natural reação a mudanças ou à introdução do novo.

Esquecemos isso e procuramos ver o que traria adicionalmente de bom para preencher essa lacuna, em que o ser humano é o principal protagonista.

Estamos falando da metodologia conhecida pela sigla STPA (*System-Theoretic Process Analysis*).

Até onde tivemos conhecimento, a precursora dessa metodologia é Nancy G. Leveson, professora doutora de Aeronáutica e Astronáutica e Engenharia de Sistemas, no *Massachusetts Institute of Technology* (MIT), nos Estados Unidos.

[1] Na realidade, essa teoria vem sendo desenvolvida há mais ou menos dez anos. Só recentemente, cremos, vem encontrando espaço para se propagar.

Trata-se de uma metodologia que procura decisivamente inserir o ser humano na interação dos processos que o sistema, como um todo, realiza, considerando também o meio ambiente que cerca o sistema, em sua operação. Diríamos que se trata de uma metodologia "de corpo inteiro".

Os que a defendem a consideram como um aperfeiçoamento daquelas que estão entre nós há mais de 50 anos, como a FTA (*Fault Tree Analysis*) e a FMEA (*Failure, Mode and Effect Analysis*). Afirmam que a STPA faz tudo o que essas "velhas" metodologias fazem, com a vantagem de acrescentar o ser-humano no processo. Esta última parte é, sem discussão, uma verdade.

Esclarece que se trata de uma análise de perigos (*Hazard Analysis*) que procura, antes de tudo, identificá-los e desenvolve processos para eliminá-los ou mitigá-los.

Diferentemente do chamado *Safety Assessment (SA)*, ela não parte da perda de funções do sistema, por falhas, para então definir os riscos, incluindo probabilidades de ocorrência. Ela começa identificando os perigos que possam ocorrer na fase operacional, incluindo fortemente o comportamento dos seres humanos, sem inserir probabilidades de ocorrência.

Percebe-se que se trata de uma atividade fortemente voltada para "brainstorming", isto é, com especialistas procurando identificar todos os perigos que possam ocorrer na fase operacional. Isso é fascinante!

É importante frisar que a metodologia já foi testada em alguns sistemas, sendo o mais significativo, em nossa opinião, a espaçonave tripulada japonesa da *Japan Aerospace Exploration Agency*, que deverá ser lançada de *Tanegashima Space Centre* (TNSC), conduzida por um foguete também japonês, e deve voar até a INSS (*International Space Station*).

Os detalhes dessa metodologia, até onde entendemos, ocupariam o espaço de vários MSC. No entanto, o que queremos passar aqui, neste momento, é a existência desse novo horizonte, convidando a todos a estudá-lo. Vamos pelo menos tentar engrenar juntos com essa tendência, fazendo cada um sua pesquisa em cima do tema.

Parte do material de que dispomos neste momento está apresentado na bibliografia deste MSC. Está todo ele na língua inglesa, como não poderia deixar de ser. Consultem também o Google, na Internet, entrando com a sigla "STPA".

Aconselhamos serem pacientes na leitura do material. Leiam e releiam e façam apontamentos, até terem uma razoável familiarização com o assunto. *Safety* é uma disciplina cujo estudo requer muita paciência, muita insistência.

Em MSCs futuros, voltaremos ao assunto, mas aí, certamente, com muitos de nossos leitores já com alguma familiarização sobre o tema.

Vamos tentar não ficar muito atrasados com relação a essa "novidade". Quem sabe, poderemos colaborar com os vários fóruns que acontecem, versando sobre esse assunto. Será bom para todos.

Quem sabe também, num futuro breve, possamos tratar do assunto em seminários no Brasil.

Ficamos por aqui. Obrigado e até breve.

Referências:

1. M.A.B. Alvarenga, P.F. Frutuoso e Melo, R.A. Fonseca. 2014. A critical review of methods and models for evaluating organizational factors in Human Reliability Analysis. *Progress in Nuclear Energy* **75**, 25-41. [CrossRef].

2. Cody Harrison Fleming, Nancy G. Leveson. 2014. Improving Hazard Analysis and Certification of Integrated Modular Avionics. *Journal of Aerospace Information Systems* **11**:6, 397-411. [Abstract] [Full Text] [PDF] [PDF Plus].

3. Leveson, Nancy. G., Enginedering a Safer World: Systems Thinking Applied to Safety, MIT Press, Jamuary, 2012.