Safety: Há Algo de Novo no Horizonte – II

***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 52 – 03 FEV 2015

Aqui estamos, novamente, falando sobre essa nova metodologia siglada por STPA ("Sistem-Theoretic Process Analysis"), que introduzimos no MSC 51. Consideramos essa metodologia como primordial, nestes tempos em que os sistemas são de extrema complexidade, envolvendo de tal forma a interação ser-humano, sistema e meio ambiente, que não poderíamos deixar de continuar a tratar desse tema. Acreditamos, fortemente, que estamos diante de um novo horizonte na área de segurança ("safety") [1] *. Daremos então continuidade ao tema neste MSC. Outros virão. Acompanhem-nos.*

Quando tratamos de *safety*, defrontamo-nos com dois termos: evento e estado. O evento é algo que ocorre. Tem início e fim, não possuindo reversibilidade. Estado é uma condição que perdura, podendo ou não trazer consequências.

A falha de um sistema é um evento. Quando ele ocorre, surge um estado que pode trazer desde consequências com severidade desprezível, isto é, apenas com um pequeno incômodo para o ser -humano, até consequências indesejáveis, culminando com aquelas ditas catastróficas, afetando severamente o ser-humano e/ou o meio-ambiente. Esse estado com consequências indesejáveis é denominado de "Perigo". Há, pois, uma escala de perigos.

Em *safety*, denominamos Causalidade o conjunto de causas identificáveis por uma análise de perigos (*Hazard Analysis*), que podem gerar esses resultados indesejáveis para um sistema. Seus elementos são denominados causas ou simplesmente perigos. Dependendo da complexidade do sistema, é difícil identificar esse conjunto.

Ao longo desses últimos cinquenta anos, temos lidado com esses conjuntos, mas sempre considerando apenas as falhas de componentes de hardware (e seu software) com seu conjunto causalidade específico. Dito em outras palavras, não inserimos nesses conjuntos as falhas humanas.

Recentemente, surgiu entre nós um novo modelo de causalidade denominado *System-Theoretic Accident Modeling Processes* (STAMP) [2] , incorporando como causas, além das mencionadas falhas de hardware, aquelas atribuídas ao ser-humano, em sua interação com esse hardware (com seu software incorporado) e o meio ambiente.

Um sistema teórico (*System-Theoretic*) poderia ser aquele ainda numa fase de projeto conceitual, isto é, sem uma configuração física definida; com funções conhecidas, mas sem uma arquitetura de hardware (com seu software) definida.

A STPA[3] está fundamentada no modelo STAMP[4]. Trata-se de uma análise de perigos (*Hazard Analysis*), incluindo no específico conjunto de causalidade todas as causas de perigos que possam surgir, incorporando o ser humano como componente do sistema.

[1] Usaremos sempre o termo inglês *Safety*, em vez de Segurança, por ser a maneira usual de profissionais da área se expressarem.

[2] A tradução para o português é um tanto difícil. Arriscamos: "Processos de Modelagem de Acidentes de Sistemas Teóricos".

[3] Aqui adotaríamos a seguinte tradução: "Análise de Processos de Sistemas Teóricos".

[4] Quando nos referimos à STPA, estamos na realidade nos referindo ao binômio STAMP/STPA. Por simplicidade, usamos só a sigla STPA.

De importância fundamental é essa inclusão do ser humano, já que grande parte dos acidentes decorre de ações intempestivas ou equivocadas de indivíduos.

Segundo o modelo STAMP, os acidentes ocorrem em virtude de ações de controle inadequadas. De fato, o ser-humano que está comandando uma aeronave, por exemplo, exerce uma função de controle. Se ele realiza uma ação de controle inadequada ou intempestiva, pode surgir um perigo.

Os adeptos da metodologia alegam que a STPA tem a vantagem enorme de poder ser aplicada quando o projeto do sistema ainda está na fase conceitual, só se conhecendo então as funções do sistema, isto é, quando não existe ainda nenhuma estruturação física do sistema, podendo o mesmo de fato ser chamado de sistema teórico.

Quando usamos análises de segurança do tipo FTA, dizem os adeptos, *o respectivo conjunto causalidade só ficará claro, ao final da fase de desenvolvimento do sistema.*

Bem, neste ponto, gostaríamos, primeiro, de reproduzir um parágrafo do MSC 51: *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.* (grifo introduzido neste MSC).

Acrescentamos mais o seguinte parágrafo do MSC 51: *Contudo, como toda metodologia que se insere, há prós e contras. É a natural reação a mudanças ou à introdução do novo.*

Lembramos ainda que qualquer teoria, em sua infância, tem prós e contras. Sempre recebe críticas de uma ou outra pessoa que a analise. E nós não somos diferentes.

Estamos vendo a STPA como "novo horizonte", sim, mas, bem entendido, sobretudo no caso da interação humana com o hardware, simplesmente porque foi a primeira vez que vimos algo, que felizmente vem se propagando, levando em conta o ser-humano como parte do sistema, na geração de perigos.

A STPA, contudo, não estabelece requisitos probabilísticos, mas restrições (*constraints*) que deverão ser consideradas pelos projetistas.

Diferentemente da STPA, não chamaríamos a FTA de metodologia, mas de uma poderosa ferramenta de uma metodologia denominada *Safety Assessment* [5], sendo empregada na alocação de requisitos, ainda na fase de projeto conceitual (projeto inicial), após uma análise de perigos focada na suposição de perda de funções do sistema.

Ao longo do desenvolvimento do sistema, a FTA continua presente, até que se certifique que o projeto total está em conformidade com os requisitos alocados na fase de projeto conceitual.

Conforme Gloria Steveson, preceptora da STPA, a metodologia se aplica tanto na fase de projeto (*before the fact*)[6] quanto na fase operacional (*after the fact*). Concordamos, mas a FTA também se serve a isso; contudo, isso seria uma discussão para outro MSC, com exemplo prático, isto é, de um fato prático ocorrido.

Bem, isso que estamos dizendo não é só criação nossa. Foi, em boa parte, discutido num fórum que abrimos no grupo de Confiabilidade e Segurança (*Reliability and Safety*), no *site* do Linkedin, tendo a participação de especialistas de algumas partes de nosso planeta.

Abrimos esse fórum com a seguinte indagação: *Hello! I would like to know your opinions about that "new" approach in Hazard Analysis: STPA (System-Theoretic Process Analysis).*

Foi uma enxurrada de opiniões e discussões acaloradas, das quais também participamos e agimos como moderadores porque fomos nós que propusemos o tema (regra do grupo).

A bem da verdade, devemos dizer que a aplicação da STPA não é uma tarefa muito fácil. O aprendizado requer a presença de um instrutor

[5] Vide SAE ARP 4761.

[6] *Before the fact* e *after the fact* são duas expressões inglesas que, em safety, significam, respectivamente, *antes de um acidente* e *depois de um acidente*.

com experiência na prática da STPA e muito estudo.

Numa ocasião oportuna, voltaremos ao assunto.

Obrigado.

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., Engineering a Safer World: Systems Thinking Applied to Safety, MIT Press, January, 2012.