**Melhore Seus Conhecimentos (MSC)**

# *Interpretando os termos Fault e Failure, no Processo de Safety Assessment*

*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@gmail.com*

*MSC 70 – 04MAR2019*

Há pouco, um de nossos leitores questionou-nos sobre o termo *fault* usado para a FTA (*Fault Tree Analysis*), inserido no manual **NUREG 0492 – *Fault Tree Handbook***, considerado o melhor trabalho já realizado sobre a FTA. Já tratamos do assunto alhures, mas resolvemos voltar ao mesmo, procurando deixá-lo mais claro. A dúvida dos leitores está no fato de a FTA ser apresentada também, por um ou outro autor, como sigla de *Failure Tree Analysis,* em vez do original *Fault Tree Analysis* do NUREG 0492.

Nosso objetivo neste MSC, como o próprio título indica, é apresentar nossa interpretação no emprego dos termos *failure* e *fault,* principalmente no processo de *Safety Assessment*, bem como a relevância de usar um ou outro termo no mencionado processo.

Já nos é familiar o termo *failure*, cuja tradução é incontestavelmente falha. O nó está no termo *fault.* O que nos interessa agora é então buscar um conceito que nos dê um entendimento firme desse termo, mais acentuadamente no processo de *Safety Assessment*.

Assinalamos, de pronto, que as AC 23.1309-1E: *System Safety Analysis and Assessment* ou AC 25.1309-1A *System Design and Analysis*, ambas da FAA, não incluem no roll de definições o termo *fault*. Apenas apresentam o significado da sigla FTA, qual seja: *Fault Tree Analysis*, sem entrar em detalhes em relação ao mencionado termo.

Consideraremos básicos para nosso raciocínio os seguintes documentos:

(1) NBR ABNT 5462 – Confiabilidade e Mantenabilidade[1];
(2) NUREG 0492 – *Fault Tree Handbook*;
(3) AC 23.1309-1E: *System Safety Analysis and Assessment For* ou AC 25.1309-1A *System Design and Analysis*, ambos da FAA (principalmente a AC 23.1309-1E, por ser mais recente e rica sobre o assunto).

E nos referiremos aos mesmos, no texto, pelos marcadores (1), (2) e (3) a eles atribuídos.

Comecemos então com o documento (1). Ele apresenta em seu item 2.4.1 a seguinte definição de *failure*: "Término da capacidade de um item para realizar sua função", e faz a seguinte observação: "A falha é um evento; diferente de pane, que é um estado".

Mais adiante, em seu item 2.5.1 vem a definição de pane: "Estado de um item caracterizado pela incapacidade de desempenhar a função requerida, excetuando-se o tempo de parada para manutenção preventiva".

Até este ponto, parece-nos claro que, segundo o documento (1), após uma falha, o item entra no estado denominado pane.

Por outro lado, no Anexo C do documento encontramos a tradução de pane; para o inglês: *fault*; e para o francês: *panne*.

Com essa tradução, cremos que o documento nos passa o entendimento do que vigora na área da manutenção. Seria algo assim: "Quando ocorre a falha de um item, o mesmo entra no estado de pane, ou seja, o item ingressa em estado de *fault,* que para nós é o mesmo que dizer inoperante"[2].

Este é, pois, o conceito que, de fato, vigora na manutenção.

Vejamos agora o que nos diz o documento (2), precursor do termo *fault*.

Já no item 1 do capítulo V encontramos uma distinção entre *failure* e *fault.* Começamos com uma expressão do autor:

[1] Tradução do Cap. 1 do padrão internacional "Electrotechnical Vocabulary – Cap 191", da IEC (International Electrotechnical Commission).

[2] Atuamos por uma década na área de manutenção, podendo afirmar que de fato é esse o conceito usado nessa área para o termo pane.

"Toda *failure* é uma *fault*, mas nem toda *fault* é uma *failure*". Cremos ser essa a frase mais lapidar para nossa interpretação. Continuemos.

O autor começa com um exemplo, em que se inserem o termo *failure* e *fault.*

Cita a operação de um relé de um sistema elétrico genérico. Quando esse relé fecha seus contatos, no momento em que tem uma tensão elétrica ou voltagem aplicada a seus terminais. Diz-se, neste caso, que a operação do relé foi um sucesso. Mas, se nessa operação o relé falha, diz-se que o relé falhou ou que teve uma falha (*failure*).

Por outro lado, prossegue, se o relé fecha o circuito, porém num momento errado, i. e, inadvertidamente, devido a uma falha ou mau funcionamento de algum outro componente do sistema, dizemos que não houve falha do relé, mas que o sistema entrou num estado de operação insatisfatória, em virtude de uma *fault*.

**Considerações iniciai:**

De fato, não houve falha do relé, mas do sistema, ou seja, o sistema como um todo falha, tanto por uma falha do relé quanto por falha ou mau funcionamento num ou noutro componente. No entanto, o que interessa aos analistas do processo de *Safety Assessment* é que o sistema, como um todo, falha. Prevalece então como causa uma falha do sistema, não necessariamente do relé. E tem mais: queremos saber qual é a *failure rate* (taxa de falha: probabilidade de falhar por hora de voo) do sistema, e não uma *fault rate*. Aliás, em nenhum dos dois documentos se fala em *fault rate.*

Na verdade, a frase "Todas as *failures* são *faults*, mas nem todas as *faults* são *failures"*, nos sugere que *faults* incluem falhas ou mau funcionamento de algum componente do sistema, ou, diríamos, até mesmo devido ao acionamento de um eventual circuito oculto (CC) no sistema.

De passagem, o circuito oculto, num sistema eletrônico, é devido a algum erro cometido no projeto, ou na manutenção, o qual, em certas circunstâncias de operação do sistema, pode surgir, produzindo tensões elétricas ou voltagens não previstas no projeto, podendo então trazer resultados nefastos (catastróficos), como já ocorreu em muitas ocasiões, inclusive em projetos de sistemas espaciais. Trata-se de um capítulo à parte da análise de segurança *(Safety Analysis)*.

Voltando, cremos que já dá para entender a frase "Toda *failure* é uma *fault*, mas nem toda *fault* é uma *failure".* Podemos até recorrer à teoria dos conjuntos e dizer que em qualquer sistema o conjunto das *failures* é subconjunto do conjunto de *faults*.

**Considerações finais.**

Tudo o que foi apresentado, parece-nos fazer sentido; mas, vejamos como utilizamos a FTA, na área de *safety* pertinente à aviação. Ela é usada mais intensamente em duas situações:

(a) na atividade de certificação de projeto de aeronaves; e
(b) na análise de acidentes aeronáuticos.

Na certificação, ela aparece no processo de *Safety Assessment,* para a empresa fabricante de aeronaves demonstrar que possíveis acidentes ou situações desconfortáveis em vôo, em decorrência de falhas ou maus funcionamentos em seus sistemas, têm probabilidade de ocorrer enquadrada na faixa de probabilidades aceitável pela Autoridade Aeronáutica (FAA, EASA, ANAC, etc.).

Aqui então *fault* é uma falha, mas o termo não é mencionado na análise. Mesmo sabendo que falha é *fault*, o analista usa o termo falha porque ele precisa saber qual é a probabilidade de uma condição de falha (e não de uma condição de *fault*), sendo esse termo utilizado para os efeitos de uma falha (Catastrófica, Perigosa, Maior e Menor), considerando-se então comum considerar a FTA também como sigla de *Failure Tree Analysis*. Tudo bem considerar assim, mas não perdendo de vista que *failure* é uma *fault*.

Por outro lado, nos acidentes, quando se procura as causas mais prováveis do acidente, não se fala em probabilidades, mas em fatalidades; procuram-se então as *faults,* que possam ter decorrido de falhas, maus funcionamentos do sistema, agressões ambientais (tempestades, HIRF[3]) ou ações equivocadas ou intempestivas da tripulação. Aqui, o uso de *fault* é bem evidente, justificando-se plenamente a denominação *Fault Tree Analysis* para a FTA.

É bom lembrar que o NUREG 0492 foi escrito no ambiente da energia nuclear, considerando os perigos existentes nessas instalações.

Só para concluir. A etapa final de um processo de *Safety Assessment*, em se tratando de um sistema,

[3] HIRF: *High Intensity Radio Frequency.*

em termos de análise para verificar se o sistema atende aos requisitos da Autoridade (probabilidade de falha do sistema), é realizada pelo fabricante do sistema com o concurso de uma FMECA[4] (*Failure Mode, Effects, and Criticality Analysis*) aplicada aos blocos funcionais do sistema.

O fabricante do sistema procura, por meio dessa análise, verificar se a probabilidade de falha do sistema como um todo se enquadra no intervalo de probabilidade de falha estabelecido pela análise *Functional Hazard Analysis* (FHA), realizada *a priori* pela equipe de *Safety Assessment* do fabricante da aeronave, na qual vai ser instalado esse sistema. Notem que aqui a preocupação é com as condições de falha do sistema, isto é, o tipo de *fault* dessa análise é *falha*.

Bem, caros leitores, já nos alongamos muito para um MSC. Esperamos ter trazido alguma luz para essa discussão.

Até uma próxima oportunidade.

Referências


1. *Veseley, W. E.; Goldberg, F.F.; Roberts, N.H.; Haasi, D.F. NUREG 0492: Fault Tree Handbook; U.S. Nuclear Regulatory Commission. EUA, 1981.*
2. *FAA: AC 25.1309-1A; System Design and Analysis. EUA, 1988.*
3. *ABNT. NBR 5462; Confiabilidade e Mantenabilidade. Associação Brasileira de Normas Técnicas (ABNT). Brasil, 1994.*
4. *FAA: AC 23.1309-1E, System Safety Analysis and Assessment for Airplanes. EUA, 2011.*


[4] Exceto se o sistema for complexo, situação em que se usam outros recursos.(v. Ref, 2),