Confiabilidade e Segurança (*Safety*): Curiosidades

Berquó, Jolan Eduardo – Eng. Eletrônico (ITA)·.
Certificador de Produto Aeroespacial (DCTA/IFI)
Representante Governamental da Garantia da Qualidade – RGQ (DCTA/IFI)
jberquo@dcabr.org.br

MSC 34 – 12 MAR 2013

Pode um Sistema ser confiável, porém inseguro? Pode um Sistema ser seguro, porém não confiável? Estas questões nos foram colocadas por um amigo. Foi uma oportunidade que tivemos de tratar de coisas "curiosas", no terreno da Confiabilidade e da Segurança. Aliás, nesse terreno há várias coisas "curiosas". A partir dessa colocação, achamos por bem, vez por outra, tratar dessas "curiosidades" neste nosso espaço.

Mas a resposta, de pronto, às perguntas acima é "sim", ou seja, um Sistema pode ser confiável, porém inseguro; ou um Sistema pode ser seguro, porém não confiável. Mas também pode ser confiável e seguro, ou não confiável e inseguro.

Mas, vamos afirmar que a possibilidade acima se deve ao fato de "Segurança" ser um termo relativo. Adiante, mostraremos isso.

Mas, só para deixar claro, vamos nos fixar na tese que queremos demonstrar:

"No terreno da Confiabilidade e Segurança de um Sistema, existe o seguinte conjunto de pares de possibilidades:

$$S = \{(C, S), (C, I), (N, S), (N, I)\} \qquad (1)$$

onde C: Confiável; S: Seguro; N: Não Confiável; e I: Inseguro".

Para demonstrar a tese, temos que conhecer três conceitos: Segurança, Confiabilidade e Severidade de Condições de Falha[1]. Comecemos com a Segurança:

"Segurança (*Safety*) – Ausência daquelas condições que podem causar (um acidente com)[2] morte, ferimentos, doença ocupacional, danos a ou perda de equipamentos ou propriedades, ou danos ao ambiente".

Notem que pessoas, equipamentos, propriedades e ambiente são os "pacientes", ou seja, aqueles que sofrem os efeitos adversos do agente "falha".

As tais "condições" desse conceito são denominadas "Condições de Falha", que caracterizam os possíveis efeitos adversos de uma falha sobre os pacientes.

Observemos ainda que Segurança é um estado, e isso é relativo, ou seja, como na Física ou na Química, há várias configurações para caracterizá-lo, dependendo das condições de falha que o geram.

Vejamos o conceito de Confiabilidade.

"Confiabilidade – Probabilidade que um sistema cumpra com sucesso sua missão, num determinado tempo e em determinadas condições".

De pronto, vemos que a Confiabilidade é um conceito matemático que não representa um estado, mas uma probabilidade de sucesso.

Quando dizemos que um sistema é confiável, significa que há boa probabilidade de cumprimento da missão. Um sistema pode cumprir sua missão, mas durante a mesma pode ocorrer, por exemplo, mortes. Neste caso, para a falha que conduziu pacientes à morte, o sistema é inseguro. Aqui temos então o caso de Sistema confiável, porém inseguro.

Só até aqui, já seria suficiente para perceber que os dois conceitos são bem distintos; não caminham necessariamente na mesma direção e sentido. Mas vamos nos aprofundar mais para demonstrar a tese concretamente.

Vejamos agora o conceito de Severidade:

"Severidade (*Severity*) – É a gravidade dos potenciais efeitos de condições de uma falha".

Como já vimos no MSC 06, as condições de falha são classificadas de acordo com a severidade (gravidade) de seus efeitos.

[1] Condições de Falha – São os efeitos de uma falha obre a aeronave, ocupantes, equipamentos, propriedades e ambiente.
[2] Inserção nossa.

Vamos então considerar a escala de severidade contida na MIL-STD-882 (Ref. 2)[3], apresentada na Tabela 1. Essa tabela também está inserida no documento da FAA: *System Safety Handbook, Capítulo 3 (Principles of System Safety* – Ref. 2).

Tabela 1 - Categorias de Severidade

Descrição	Categoria	Efeitos
Catastrófico	**1**	Morte, perda do sistema e severo impacto ambiental.
Critica	**2**	Ferimento severo, doença ocupacional, danos menores ao Sistema., e impacto ambiental moderado.
Marginal	**3**	Ferimentos leves, doença ocupacional leve, danos menores ao Sistema e ao meio ambiente.
Desprezível	**4**	Quase nenhum efeito sobre as pessoas, sistema e meio ambiente.

Não se pode perder de vista que basta haver a possibilidade de ocorrer pelo menos um dos efeitos de uma determinada categoria, para a condição de falha ser classificada nessa categoria. Assim, se o único possível efeito da falha for "ferimento severo", o acidente se enquadrará na severidade "Crítica", mesmo que não ocorra nenhum dos outros efeitos possíveis enquadrados nessa categoria.

Com essas premissas, podemos dizer que uma boa maneira de validar a tese representada pela expressão (1) está num engenhoso artifício que os engenheiros de segurança pensaram, para estabelecer uma relação entre segurança de sistema e a Confiabilidade. Esse artifício recebeu a denominação de "Análise de Risco". O termo Risco foi assim definido:

"**Risco** – Uma combinação da severidade de uma condição de falha e a probabilidade de ocorrência da falha".

O Risco mede o nível de segurança proporcionado pelo sistema. Risco alto, baixa segurança; risco baixo, alta segurança.

Estamos chegando lá. Vamos continuar.

Vamos apresentar, a seguir, na Tabela 3, a Matriz de Aceitabilidade do Risco, extraída dos documentos referenciados.

Tabela 3 – Matriz de Aceitação do Risco

Severit. / Probab.	Catastr. (1)	Crítical (2)	Marginal (3)	Negligible (4)
Frequent (A)	**High**	**High**	**High**	**Medium**
Probable (B)	**High**	**High**	**Serious**	**Medium**
Occasional (C)	**High**	**Serious**	**Serious**	**Low**
Remote (D)	**Serious**	**Serious**	**Medium**	**Low**
Improbable (E)	**Medium**	**Medium**	**Medium**	**Low**

Na primeira coluna, temos a probabilidade da falha, expressa de modo qualitativo, desde a mais provável até a mais improvável. Existe, contudo, faixas de valores para cada uma delas, mas, para o nosso objetivo, isso é irrelevante.

Notem que não se menciona a Confiabilidade nessa tabela, Contudo, existe uma relação entre a probabilidade de falhar (também chamada de Falibilidade F) e a probabilidade de não falhar (Confiabilidade R), tal que:

$$R = 1 - F \qquad (2)$$

Nas várias células, estão os níveis de risco: **Alto**, **Sério**, **Médio** e **Baixo**, definidos pelo binômio "Falibilidade vs. Severidade".

Essas denominações **Alto**, **Sério**, etc. dependem dos requisitos da Autoridade.

A autoridade pode considerar inaceitáveis os riscos **Alto** e **Sério**, considerando baixa a segurança do Sistema. É o caso do binômio "Catastrófico" e "Remota", apesar da boa confiabilidade. O binômio "Desprezível" e "Frequente" seria considerado seguro, apesar de ter uma confiabilidade baixíssima.

Enfim, vamos então apresentar uma possível configuração aceita pela Autoridade:

(N, I): A1, A2, A3, B1, B2 e B3.
(C, I): C1, C2, C3, D1 e D2.
(N, S): A4 e B4.
(C, S): C4, D3, D4, E1, E2, E3 e E4.

Ou seja, todos os pares de possibilidades contidos na expressão 1.

[3] Não importa se as considerações se refiram a documentos militares ou civis; o que interessa é o conceito.

Cremos então que tenha dado para perceber porque admitimos como “sim” as respostas às perguntas do primeiro parágrafo deste MSC.

Finalizando, podemos dizer que Confiabilidade e Segurança andam juntas, na mesma direção, mas não necessariamente no mesmo sentido.

Paramos por aqui.

Até a próxima.

Referências:

(1) DoD, **MIL-STD-882E, System Safety**. DoD, EUA, 2012.

(2) FAA, **System Safety Handbook**. FAA. EUA, 2000.

(3) DAU (Defense Acquisition University). **Systems Engineering Fundamentals**. Fort Belvoir, VA, EUA. 2000.