- Segurança (*Safety*) de Sistemas: Enfoques Civil e Militar –

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 20 – 03 OUT 2012

Já tratamos do assunto, em linhas gerais, no MSC 15, mas com um enfoque filosófico. Desta feita, vamos procurar fazer uma análise mais de perto do tratamento civil e militar do tema, que assimilamos, e continuamos assimilando, com a prática e com o estudo continuado.

Logo de início, é de todo prudente tratar do significado do termo "Segurança".

Quando falamos de segurança, em português, temos de deixar claro se estamos falando daquela segurança decorrente de perigos em sistemas (aeronaves), ou seja, efeitos falhas não intencionais, ou se estamos tratando daqueles perigos provocados intencionalmente, como por exemplo os atos terroristas.

A língua inglesa tem uma palavra para cada significado acima: *Safety*, para o primeiro caso, e *Security*, para o segundo.

Generalizando, o termo *Security* está ligado a qualquer perigo de ataques, visando desestabilizar o estado de segurança de pessoas e de instalações.

Mas trataremos aqui apenas do termo segurança voltado para efeitos de falhas não intencionais. Esse é o termo tratado pela Autoridade de Aeronavegabilidade Civil e pelas autoridades militares da área de risco.

Fala-se de segurança preventiva, procurando evitar ou minimizar a ocorrência de acidentes (*before the fact*), atuando diretamente no projeto, nas fases de desenvolvimento e operacional, e segurança corretiva, procurando evitar que o acidente ocorra novamente ou minimizar sua probabilidade de ocorrência (*after the fact*).

Desta última atividade podem surgir modificações de requisitos ou introdução de novos requisitos na regulamentação da Autoridade Civil ou nos contratos de aquisição da aviação militar.

Consideramos aqui apenas o primeiro caso. O segundo enfoque é tratado, no Brasil, pelo CENIPA (Centro de Investigação e Prevenção de Acidentes Aeronáuticos), órgão diretamente subordinado ao Comandante da Aeronáutica.

Comecemos pela área civil. Até há pouco tempo, a Autoridade civil se preocupava quase que somente com a segurança do projeto de desenvolvimento de uma aeronave (Certificação de Tipo - CT) ou com a segurança voltada para o projeto de instalação de um equipamento numa aeronave certificada, ou seja, Certificação Suplementar de Tipo (CST).

Recentemente, a Autoridade Civil começou a se preocupar com a segurança também na fase operacional, surgindo então a atividade que se intitula *Safety Management System*, ao pé da letra em português: "Sistema de Gerenciamento de Segurança", mas a tradução para o português parece ter se consagrado como "Sistema de Gerenciamento de Segurança Operacional (SGSO)", bem colocada porque explicita que se trata de um sistema aplicado na fase operacional da aeronave. Detalhes do SGSO podem ser encontrados na Ref. 1, uma tradução realizada pela DCA-BR.

Do lado militar, temos a norma MIL-STD-882E (Ref. 2). Desde a primeira versão dessa norma (versão A), ela vem se preocupando com a segurança, mas, enfatize-se, ao longo de todo o ciclo de vida do sistema. A primeira versão foi lançada em julho de 1969. A versão E apareceu em maio de 2012, sendo portanto recentíssima.

Quando essa norma é inserida no contrato, sem especificar as partes da mesma que deverão ser levadas em conta pelo contratado, só os capítulos 3 ("Siglas e Definições")e 4 ("Requisitos Gerais") são obrigatórios.

Vamos então nos concentrar no Capítulo 4.

Vemos ali que existem várias diferenças entre essa norma e aqueles regulamentos voltados para a aviação civil. Mas existem também pontos comuns. Por exemplo, ambas trabalham com o binômio "Severidade-Probabilidade" (S&P).

Os regulamentos 14 CFR Parte 25§1309 – para grandes aeronaves – e o 14 CFR Part 23§1309 –

para pequenas aeronaves (mais popularmente conhecidos com FAR 25.1309 e FAR 23.1309) classificam as severidades, pela ordem da mais grave para a menos grave, da seguinte maneira: **Catastrófica** (*Catastrophic*), **Maior Severa** (*Severe Major*) ou **Perigosa** (*Hazardous*, no 23.1309), **Maior** (*Major*) e **Menor** (*Minor*).

Já a MIL-STD-882E, apresenta a seguinte classificação: **Catastrófica** (*Catastrophic*), **Crítica** (*Critical*), **Marginal** (*Marginal*) e **Desprezível** (*Negligible*).

Já tratamos da escala de severidade na aviação civil, por exemplo no MSC 06. Vimos ali que a severidade da falha é medida considerando os efeitos adversos na tripulação e passageiros.

A severidade na aviação militar inclui ainda os efeitos adversos de doença ocupacional, perda de equipamentos, danos à propriedade, danos ao meio ambiente e perda financeira.

Uma diferença acentuada entre as normas civis e a militar está na inclusão, por parte da militar, de valores financeiros nas quatro severidades.

Assim, se o efeito da falha for tal que a perda seja igual ou exceda US$ 10 milhões, ela deve ser enquadrada como catastrófica, com ou sem perda de vidas humanas.

No caso da Crítica, o enquadramento financeiro admite um intervalo entre 10 milhões e 1 milhão. No caso da menos severa (Desprezível), a perda não pode ultrapassar 100 mil dólares.

Por outro lado, no caso da probabilidade da falha (perigo), admitem-se, na área militar, requisitos qualitativos, quando for difícil atender a requisitos quantitativos.

Os requisitos qualitativos enquadram-se nos seguintes níveis: **Frequente** (esperado ocorrer amiúde), **Provável** (esperado ocorrer várias vezes), **Ocasional** (esperado ocorrer alguma vez), **Remoto** (pouco provável, mas pode ocorrer), **Improvável** (muito difícil ocorrer) e **Eliminado** (não se espera ocorrer). Este último nível aplica-se a riscos que foram identificados, mas em seguida eliminados com modificações do projeto ou com medidas mitigadoras.

O Anexo A da norma Mil apresenta uma tabela como exemplo de requisitos quantitativos. A norma deixa a entender que o requisito para o nível **Improvável** é $P<10^{-6}$. Os demais níveis podem se enquadrar em faixas baseadas em lições aprendidas ou em outros critérios estabelecidos em contrato pelas autoridades militares competentes.

A norma reconhece a dificuldade de se ter valores de probabilidade quantitativos no início do Programa, mas uma vez que sejam considerados esses requisitos, estes passam a ser alocados ao projeto, à semelhança do que se faz na Aviação Civil, onde tal alocação é feita, já na fase inicial do projeto, para as funções da aeronave – na *Functional Hazard Assessment (FHA)*, propagando-se depois para os sistemas e, finalmente, para os equipamentos.

É no mínimo curioso que na área militar a faixa de probabilidade mais restrita seja $Pr<10^{-6}$ (um milionésimo), enquanto que na civil seja $Pr<10^{-9}$ (um bilionésimo), isto é, 1.000 vezes mais restrita. Entretanto, pode-se explicar isso, não perdendo de vista que as operações militares, mesmo no tempo de paz, tem mais risco, sendo irrealística uma faixa semelhante à civil.

Com esses dados, obtidos para cada condição de falha, passa-se para a chamada Matriz de Aceitação do Risco, como a mostrada na tabela abaixo.

Matriz de Aceitação do Risco				
Severid. / Probab.	**Catastr.**	**Crítico**	**Marg.**	**Desprez.**
Provável (B)	**Alto**	**Alto**	**Sério**	**Médio**
Frequente (A)	**Alto**	**Alto**	**Sério**	**Médio**
Ocasional (C)	**Alto**	**Sério**	**Médio**	**Baixo**
Remoto (D)	**Sério**	**Médio**	**Médio**	**Baixo**
Improvável (E)	**Médio**	**Médio**	**Médio**	**Baixo**
Eliminado (F)	**Eliminado (não pode ocorrer)**			

A responsabilidade pela aceitação desses riscos é definida pelo escalão competente do órgão militar, e nos parece lógico que essa responsabilidade seja inserida no contrato de aquisição.

A norma sugere que a responsabilidade de aceitação do Risco Alto (RA) seja da autoridade que conduz programas de aquisição; que o Risco Sério (RS) seja de responsabilidade do executivo dedicado àquele programa específico;

que a responsabilidade pelo Risco Médio (RM) seja atribuída ao Gerente de Programa; e que o Risco Baixo (RB) seja automaticamente aceito, isto é, sem submissão a qualquer nível de autoridade.

Ficamos por aqui.

Referências:

(1) Stolzer, Alan J.; Halford, Carl D.; Goglia, John J. Sistemas de Gerenciamento da Segurança Operacional na Aviação. (Tradução Equipe DCA-BR). São José dos Campos (SP): DCA-BR – Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica, 2011.

(2) DoD: MIL-STD-882E, System Safety. EUA, maio 2012.

(3) FAA: CFR 14 Part 23 § 1309, Equipment, Systems, and Installations, Emenda 23-49, EUA, janeiro 1996.

(4) FAA: CFR 14 Part 25 § 1309-1A, Equipment, Systems, and Installations, Emenda 25-123, EUA, novembro 2007.