Melhore Seus Conhecimentos (MSC)

O Cerne da SAE ARP 4754A

Eng. Jolan Eduardo Berquó (Instituto Tecnológico de Aeronáutica – 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)*
- *Participação no programa conjunto (Brasil-Itália) de desenvolvimento da aeronave militar caça-bombardeiro AM-X*
- *Experiência de uma década como engenheiro responsável pela manutenção "off aircraft" de sistemas eletrônicos e instrumentos de aeronaves do Parque de Material Aeronáutico de São Paulo.*

jberquo@dcabr.org.br/jberquo@gmail.com

MSC 75 – 15Dez2020

A avalanche dos sistemas aviônicos altamente complexos, que são atualmente instalados nas aeronaves, promoveram, por sua natureza, uma revolução no processo de desenvolvimento de sistemas de uma aeronave, que acabou com uma enorme preocupação da indústria aeronáutica e das autoridades de certificação, ao fazer surgir a ARP 4754A, que descreve esse novo processo para contornar o problema de segurança (safety) desses sistemas. Este é o cerne da ARP 4754A, que será resumida neste MSC.

O que é um sistema complexo? É aquele que, no projeto, não pode ser devidamente analisado, quanto à segurança (*safety*) pelas chamadas análises estruturadas conhecidas, como, por exemplo, a convencional análise FMEA (*Failure Modes and Effects Analysis*). É tal a sofisticação funcional dos sistemas complexos atuais que essas análises convencionais não conseguem detectar erros que possam redundar em graves problemas de segurança.

De fato, a atual proliferação de sistemas altamente complexos, com seus itens (equipamentos ou unidades) contendo circuitos integrados (*chips*) com altíssima densidade de funções [1], torna uma FMEA absolutamente ineficaz para analisar os itens desses sistemas. Mas, esse tipo de análise, assinale-se, continuam se aplicando bem aos sistemas mais simples.

Um exemplo de sistema altamente complexo é o Sistema de Informações Primárias de Voo, que apresenta num display eletrônico, entre outras, informações provenientes de sistemas aviônicos também complexos, como, por exemplo, o ADS (*Air Data System*: altitude, velocidade) e AHRS (*Attitude, Heading Reference Sy*stem: atitude, direção), ambos integrados em um barramento digital, por onde são encaminhadas suas informações ao mencionado display.

Dependendo das condições meteorológicas, um erro no projeto desses sistemas integrados pode trazer conseqüências trágicas para o voo.

Outro exemplo é o sistema aviônico híbrido[2] *Fly-By-Wire* de controle de voo com peças mecânicas (superfícies de comando e atuadores) e o <u>cérebro</u> do sistema, i.e, o computador de controle de voo (*Flight Control Computer* - FCC). A complexidade do sistema é atribuída ao FCC.

O material de orientação apresentado nas DO 178B (projeto *de software*) e DO-254 (projeto de *hardware* eletrônico), com seus rigorosos processos de desenvolvimento de itens desses sistemas, foi reconhecido pela indústria e por várias autoridades regulatórias como suficientes para estabelecer os necessários níveis de confiança de ausência de erros de projeto nesses <u>itens</u> (v. a primeira edição da ARP: ARP 4754).

O fato é que, diante desse incessante crescimento em complexidade dos sistemas, ficou clara a necessidade de se estabelecer níveis de confiança para o projeto, <u>não só de itens</u>, mas para todos os segmentos da aeronave (aeronave, sistemas e itens). Com esse intento, surgiu o chamado **Processo <u>Integral</u> de Garantia Desenvolvimento** da Aeronave, Sistemas e Itens **(PGD)**[3]. <u>Este é o cerne da ARP 4754A.</u>

<u>É importante</u> assinalar que a identificação do nível de garantia de desenvolvimento depende, de início, da classificação das condições de falhas

[1] Sendo comum esses *chips* terem mais de uma centena de entradas e saídas.

[2] A complexidade dos sistemas aumentou, a partir do surgimento dos sistemas aviônicos híbridos.

[3] Por facilidade, assinalaremos, daqui em diante, a sigla PGD para esse processo.

(*failure conditions*) das funções nível aeronave, que são identificadas no Processo de Avaliação de Segurança (Processo de *Safety Assessment* – PSA). Desse modo, o PSA faz parte do PGD.

Devemos ter em conta que uma failure condition pode ser causada por uma ou mais falhas ou por um ou mais erros de projeto. Em relação às falhas e antes do advento da ARP 4754A, o PSA, no caso de sistemas complexos, já exigia do fabricante de sistemas e itens a conter as falhas, por meio de um projeto de garantia de projeto (*Design Assurance Level* - DAL), sugerindo a esses fabricantes o uso das DO-178B e a DO-254A.

Contudo, quando se trata de erros de projeto, a preocupação com os mesmos passa a ser também com o projeto na empresa fabricante da aeronave, nos níveis aeronave e sistemas. O PGD é então um processo com uma parte na empresa fabricante da aeronave e outra com os fabricantes dos sistemas/itens.

Os requisitos de segurança (*safety*) são funcionalmente identificados nos níveis aeronave, sistemas e itens. No nível aeronave, são aqueles gerados na AFHA (*Aircraft Functional Hazard Assessment*), que vão constituir a base para o PGD. No nível aeronave, são aqueles gerados na SFHA, com base nos resultados da AFHA.

A Análise de Causa Comum (*Common Cause Analysis* - CCA) também é parte da PSA e ocorre em cada etapa desse processo, para assegurar a independência entre funções ou aceitar certas dependências, mediante considerações discutidas na análise das mesmas.

Os níveis de garantia de desenvolvimento da aeronave e dos sistemas são caracterizados, no PGD, por meio do *Functional Development Assurance Level* (FDAL), em função da severidade das *failure conditions* nível aeronave. O fato, por exemplo, de existirem *failures conditions* de efeitos catastróficos ou perigosos (*hazardous*), já sugerem fortemente o uso do PGD, a partir do início do desenvolvimento.

A tabela a seguir mostra a caracterização desses níveis, conforme a failure condition:

Failure Condition	FDAL
• Catastrófica (Catastrophic)	A
• Perigosa (Hazardous)	B
• Maior (Major)	C
• Menor (Minor)	D

No que tange aos itens dos sistemas, os níveis de garantia de desenvolvimento são caracterizados em *Item Development Assurance Level* (IDAL), orientando o rigor de projeto do item, conforme previsto nas DO-178C e DO-254A.

A ARP apresenta a maneira de alocar o FDAL para o respectivo sistema que irá realizar a função em análise e, a partir do sistema, a alocação de IDAL para os itens do sistema.

Em nenhum momento, a ARP fala, no PGD, em taxas de falhas, como se faz na PSA, mesmo assim o faz para sistemas mais simples.

Bem, prezados leitores, ficamos por aqui, neste MSC. Nosso objetivo foi apresentar o cerne da ARP 4754A e mostrar sua importância, quando estivermos lidando com segurança (*safety*) de sistemas complexos. Gostaríamos apenas de acrescentar que o estudo da ARP, *in totum*, é uma tarefa árdua. Requer muita concentração, considerações e reconsiderações, até o entendimento correto de cada item e parágrafos.

A propósito, estamos preparando material relativo a essa ARP, que intitulamos "**Interpretando a Visão da Indústria e Autoridades de Aviação na ARP 4754A"**. Trata-se de um trabalho meticuloso, no qual procuraremos esclarecer parágrafo por parágrafo, procurando facilitar o entendimento dos interessados em se familiarizarem com esse importante documento, uma realidade na segurança de projeto.

Por ter sido este MSC desenvolvido no mês de dezembro (2020), encerramos agradecendo e desejando a todos feliz Natal, um próspero ano de 2021 e muita saúde para vocês e todos os seus familiares.

Até uma nova oportunidade.

Referências:

1. ***SAE: ARP 4754*** *– Certification Considerations for Highly-Integrated or Complex Systems, EUA, Nov/1996.*

2. ***SAE: ARP 4754A*** *– Guidelines for Development of Civil Aircraft and Systems, EUA, Dez/2010.*