13º WETE
16, 17 e 18 de novembro de 2022
13º Workshop em Engenharia e Tecnologia Espaciais

Uma breve discussão sobre as diferentes abordagens dos conceitos presentes nas técnicas FMEA e FTA

Ana Beatriz Bressan Bertaglia[1], Ângela Antunes Dias de Oliveira[1], Silvio Manea[2], Ana Paula de Sá Santos Rabello[2]

[1]Aluna de Mestrado do curso de Área de Engenharia e Gestão de Sistemas Espaciais – (ETE/CSE).

[2] Instituto Nacional de Pesquisas Espaciais, Divisão de Sistemas Espaciais (DISEP)

anabeatrizbertaglia@gmail.com

eng.angelaantunes@gmail.com

Resumo. *A definição e entendimento de conceitos é uma necessidade que deve ser cumprida na fase inicial dos projetos, uma vez que divergências podem causar impactos negativos, como por exemplo na qualidade dos resultados das análises realizadas através das técnicas FMEA (Failure Mode and Effects Analysis) e FTA (Fault Tree Analysis). Embora os conceitos relacionados a um mesmo assunto sejam muito parecidos, a forma na qual as abordagens são feitas, podem não ser tão semelhantes. Alguns conceitos chaves presentes nas técnicas FMEA e FTA serão apresentados neste artigo a fim de trazer uma visão geral sobre as diferentes abordagens de um mesmo conceito. Para isso, foi realizado um levantamento bibliográfico em diferentes literaturas a fim de comparar os principais conceitos referentes a falhas e como estas são identificadas, avaliadas e mitigadas ao utilizar tais técnicas.*

Palavras-chave: FMEA; FTA; Falha; Falência.

1. Introdução

De acordo com NASA (2002), os métodos para realizar avaliação de risco e confiabilidade foram originados no setor aeroespacial dos Estados Unidos em programas de mísseis no início da década de 1960. A NASA utilizava a técnica FMEA (*Failure Mode and Effects Analysis*) e outros métodos de análise qualitativos para avaliações da segurança dos sistemas. Após o acidente do Challenger em 1986, a importância da técnica FTA (*Fault Tree Analysis*) na análise de risco dos sistemas e a análise de confiabilidade começou a crescer ainda mais. Desde então, a avaliação de riscos e suas técnicas, incluindo a FMEA e FTA, tornou-se uma metodologia útil e respeitada para a avaliação da segurança em sistemas nas áreas de defesa e espaço, e aeronáutica. Em aplicações de segurança, estas técnicas ajudam engenheiros a encontrar as fraquezas operacionais em sistemas complexos de forma sistêmica e então, priorizar as melhorias de segurança.

Então diante da importância das técnicas FMEA e FTA para avaliação de falhas (anomalias), este trabalho tem como objetivo apresentar uma breve discussão sobre as

diferentes abordagens dos conceitos presentes nessas técnicas, uma vez que é de extrema importância que tais conceitos sejam bem claros e definidos já estão diretamente relacionados aos resultados das avaliações.

2. Metodologia

Para atingir o objetivo proposto, foi realizado um levantamento bibliográfico disponível na literatura referente a falhas e como estas são identificadas e avaliadas. Dessa forma, foi feita uma comparação entre diferentes literaturas sobre como as técnicas de análises FMEA e FTA são utilizadas para avaliar e mitigar falhas (anomalias) de produtos (como por exemplo, satélites) em operação ou erros de processos. No trabalho de Dissertação de Mestrado da autora principal, que está em andamento, uma comparação mais detalhada será realizada.

Neste artigo, são utilizados como base os documentos abaixo para a comparação de conceitos importantes para a utilização das técnicas FMEA e FTA.

1. Frequentemente utilizado na área de defesa e espaço:
    a. [FMEA] MIL-STD-1629A (notice 1 e notice 2): Procedures for performing a failure mode, effects and criticality analysis (DOD, 1980)
    b. [FTA] NASA: fault tree handbook with aerospace applications (NASA, 2002)
    c. [FMEA] ECSS-Q-ST-30-02C: Failure modes, effects (and criticality) analysis (FMEA/FMECA) (ECSS, 2009)
    d. [FMEA e FTA] Reliability Modeling: The RIAC guide to reliability prediction, assessment and estimation (DENSON, 2010)
2. Frequentemente utilizado na área aeronáutica:
    a. [FMEA e FTA] ARP4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment (SAE, 1996)
    b. [FTA] ARP4754A: Guidelines for Development of Civil Aircraft and Systems (SAE, 2010)
    c. [FTA] AC 25.1309-1A: System Design and Analysis (FAA, 1988)
    d. [FTA] AC 23.1309-1E: System safety analysis and assessment for Part 23 Airplanes (FAA, 2011)

3. Resultados e Discussão

3.1. Definições de Termos

Os termos *failure* e *fault* são extremamente significativos para a área de gerenciamento de falhas, por essa razão motiva a busca na literatura para a comparação e entendimento.

Nota-se que a FAA (2011), amplamente utilizada na área de gerenciamento de falhas aeronáutica, não inclui o termo *fault* em suas definições. Dessa forma, a tradução do termo *failure* é popularmente utilizada como falha, já o termo *fault* geralmente é motivo de maiores discussões.

Na área de gerenciamento de falhas de defesa e espaço, Pessotta (2018) traz essa discussão mostrando a divergência quanto as definições dos termos *fault* e *failure* mesmo na língua inglesa e demonstra que entre os autores nacionais as divergências têm início na própria tradução dos termos. O autor conclui definindo o termo *failure* como falência e o termo *fault* como falha.

A ECSS (2009) considera o termo *failure* como o evento que resulta em um item não ser mais capaz de desempenhar a função que lhe foi requerida. Já o termo *fault* é o estado de um item caracterizado pela incapacidade de executar sua função. *Failure* é um evento e *fault* é um estado. Ressalta ainda que, uma *fault* pode ser o resultado de uma *failure* do próprio item, portanto uma *fault* pode gerar uma *failure*.

A SAE (1996) considera o termo *failure* como a perda de função ou um mau funcionamento de um sistema ou de uma parte dele. Em contrapartida, o termo *fault* é uma anomalia indesejada em um item ou sistema.

Após as definições dos termos *failure* e *fault* de algumas referências, tanto da área de defesa e espaço e aeronáutica, foram buscados outros termos complementares para o entendimento.

A ECSS (2009) considera *failure mode* (modo de falha) como um mecanismo pelo qual ocorre uma falha, *failure cause* (causa da falha) como causas associadas a um determinado *failure mode*, e *failure effect* como consequência de um *failure mode* de um item sobre sua operação ou função.

O DOD (1980) considera *failure mode* (modo de falha) como a maneira pela qual uma *failure* é observada. Adiciona ainda que, o *failure mode* geralmente descreve a maneira como a *failure* ocorre e seu impacto no funcionamento de um equipamento.

A SAE (1996) considera *failure mode* como a maneira pela qual ocorre a *failure* de um item.

O RIAC (*Reliability and Information Analysis Center*) (DENSON, 2010), através da Tabela 1, apresenta a relação entre causa, modo e efeito em diferentes níveis (sistema, parte montada, item e processo de manufatura de tal item), em uma FMEA.

System	Assembly	Part	Part Manufacturing Process
Effect			
Mode	Effect		
Cause	Mode	Effect	
	Cause	Mode	Effect
		Cause	Mode
			Cause

Tabela 1: Relação entre causa, modo e efeito [DENSON, 2010]

Já a Figura , ilustra como a relação entre causa, modo e efeito escalam para cima ou para baixo na hierarquia do item ou sistema, dependendo do nível hierárquico em que a análise será feita, em uma FTA. Neste exemplo, a *failure cause* é considerada como o nível mais baixo.

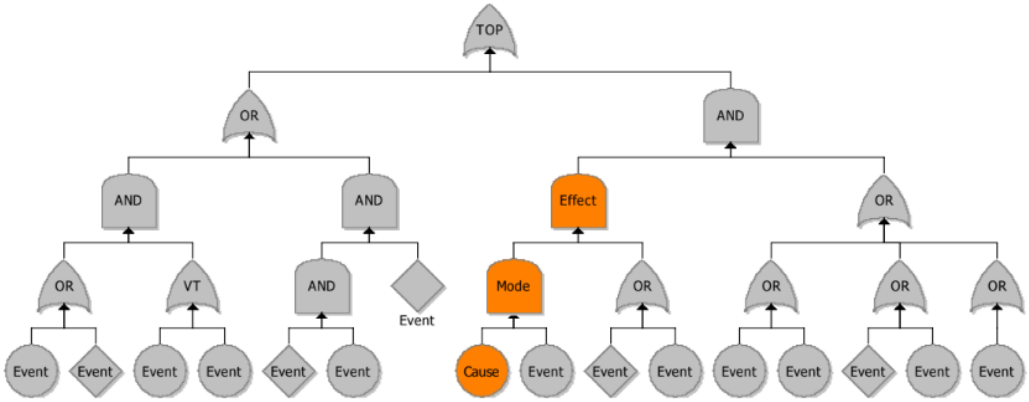

Figura 1: Arvore de falha de um item ou sistema com a causa como nível mais baixo [DENSON, 2010]

O padrão ECSS (2009) agrega neste entendimento ao trazer uma visão que correlaciona a ligação entre causa, modo e efeito com a integração da necessidade de definir termos compatíveis entre os níveis (exemplo: os efeitos da falha no nível subsistema são os modos de falha no nível sistema). Então pode ser observado através da Figura 2 a necessidade de definição de um bom requisito de elaboração da FMEA de um sistema, que é composto de outros subsistemas, e ou equipamentos. Portanto, para garantir essa integração, é necessário que os termos utilizados estejam bem claros e definidos.

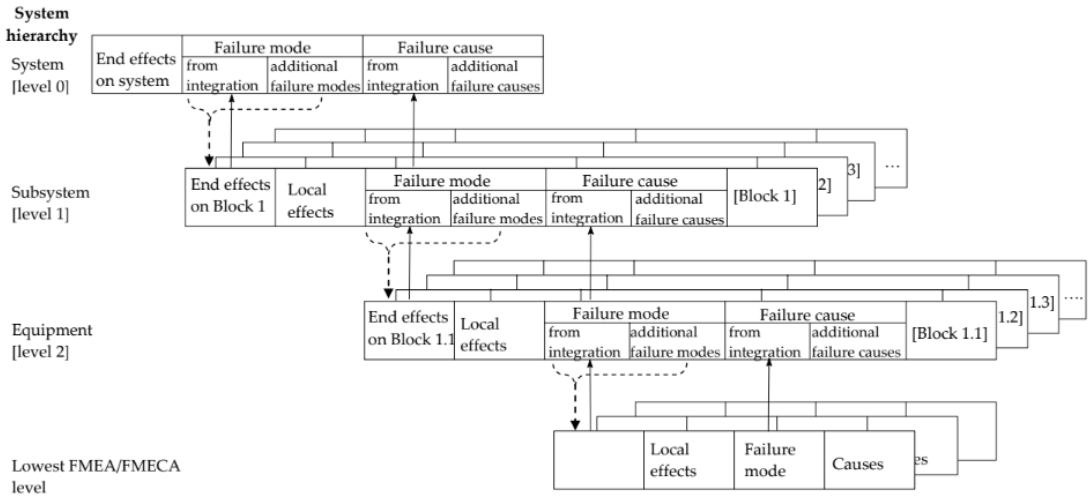

Figura 2: Representação gráfica de integração de requisitos considerando causa, modo e efeito [ECSS, 2009]

Na área de defesa e espaço normalmente a hierarquia considerada é: sistema, subsistema, equipamento e componente. Na área aeronáutica: aeronave, sistema e item (SAE, 2010). Nesse trabalho é considerado a hierarquia adotada na área de defesa e espaço.

3.2. FMEA (*Failure mode and effects analysis*) x FTA (*Fault Tree Analysis*)

De acordo com Denson (2010), o objetivo da disciplina confiabilidade é identificar e mitigar os modos de falhas, verificar como remove-los ou como conviver com eles, implementar as ações corretivas para as falhas conhecidas e aumentar o nível de confiabilidade de tal componente/sistema para o qual ele foi projetado para executar.

Ferramentas como FMEA e FTA são utilizadas para priorizar os casos de falha de acordo com severidade de suas consequências através de análises quantitativas e/ou qualitativas.

3.2.1. Conceitos *Bottom-up* x *Top-down*

A abordagem *botton-up* ou abordagem *top-down* é uma perspectiva de levantamento de dados da análise da falha de forma ordenada. A primeira tem início no nível mais baixo até o nível mais alto no sentido de baixo para cima (*bottom-up*) e a segunda tem início no nível mais alto sendo conduzida até o nível mais baixo no sentido de cima para baixo (*top-down*).

A FMEA (no nível de componentes de um equipamento ou subsistema) é uma técnica *bottom-up* que examina os modos de falha de componentes dentro de um sistema e traça os potenciais efeitos de cada modo de falha de tais componentes no desempenho do sistema.

A FTA utiliza a abordagem *top-down* para resolver problemas. O que significa que é possível ter uma visão de alto nível de um processo ou um produto, identificando a

potencial falha ou evento indesejado que pode levar a tal falha para então entender as potenciais causas do(s) evento(s).

A comparação entre os conceitos *Top-down* e *Bottom-up* é ilustrada na Figura 3.

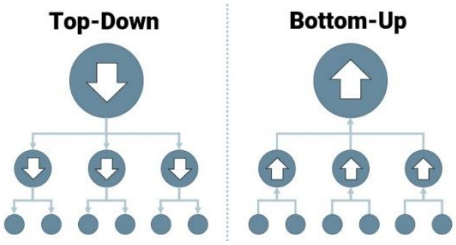

Figura 3: Comparação entre os conceitos *Top-down* e *Bottom-up*

Dessa forma, podemos considerar que a FMEA (*bottom-up*) fornece os inputs necessários para a FTA (*top-down*). Analogamente, a FTA recebe as informações necessárias para sua análise através da FMEA, uma vez que os eventos básicos (mais baixo nível) são os outputs das FMEAs de tais eventos.

Segundo a SAE (1996), a FMEA é uma técnica sistemática, *bottom-up*, para identificar os modos de falha de um sistema, item ou função e determinar os efeitos no nível superior. Ela pode ser desenvolvida em qualquer nível dentro do sistema e tipicamente é usada para tratar os efeitos de falhas resultantes de single failures. A FMEA pode ser usada em conjunto com técnicas probabilísticas como a FTA para produzir uma análise quantitativa e/ou para complementar a FTA, fornecendo uma lista complementar de efeitos de falhas *bottom up*.

3.2.2.*Failure mode and effects analysis* (FMEA)

De acordo com (DENSON, 2010), uma das chaves para a elaboração de uma FMEA eficiente é compreender a relação entre causa, modo e efeito. Em geral, existe um efeito natural de camadas que ocorre em uma FMEA em função do nível do sistema, subsistema, equipamento ou componente, como ilustrado na Tabela 1. Por exemplo, no nível mais básico, o processo de fabricação do componente, pode ser a causa da *failure*, que é uma etapa do desenvolvimento que está fora de controle. O efeito final dessa causa torna-se o *failure mode* no nível do componente, o *failure effect* do componente torna-se o *failure mode* no próximo nível (equipamento), e assim por diante. É muito importante que a causa, o modo e o efeito não sejam confundidos na análise.

Ilustrado pela Figura , as FMEAs de cada nível inferior devem ser integradas em FMEA de nível superior.

De acordo com ECSS (2009), a FMEA deverá fornecer entradas para o cumprimento de requisitos de confiabilidade e *safety* a serem alocadas para implementar os métodos de prevenção e compensação, e para minimizar as *single failures* (falha simples) e os cenários de *critical failures* (falha crítica) identificados. Ainda, acrescenta que os *failure modes* em potencial são classificados de acordo com sua severidade, conforme sugerido pela **Error! Reference source not found.**.

Severity category	Severity level	Description of consequences (failure effects)	
		Dependability effects (as specified in ECSS-Q-ST-30)	Safety effects (as specified in ECSS-Q-ST-40)
Catastrophic	1	Failure propagation (refer to 4.2c)	Loss of life, life-threatening or permanently disabling injury or occupational illness.
			Loss of an interfacing manned flight system.
			Severe detrimental environmental effects.
			Loss of launch site facilities.
			Loss of system.
Critical	2	Loss of mission	Temporarily disabling but not life-threatening injury, or temporary occupational illness.
			Major detrimental environmental effects.
			Major damage to public or private properties.
			Major damage to interfacing flight systems.
			Major damage to ground facilities.
Major	3	Major mission degradation	
Minor or Negligible	4	Minor mission degradation or any other effect	

Tabela 2: Categorias de severidade de acordo com os *failures effects* [ECSS, 2009]

O DOD (1980) apresenta que o objetivo da FMEA é avaliar os efeitos da falha de um item no funcionamento de um sistema. Além disso, a classificação de severidade é atribuída para fornecer uma medida qualitativa das piores consequências potenciais resultantes de erro de projeto ou *failure* de um item. A Figura ilustra que uma classificação de severidade é atribuída a cada modo de falha identificado de acordo com as consequências (efeitos) de tal modo de falha.

a. Category I - Catastrophic - A failure which may cause death or weapon system loss (i.e., aircraft, tank, missile, ship, etc.)

b. Category II - Critical - A failure which may cause severe injury, major property damage, or major system damage which will result in mission loss.

c. Category III - Marginal - A failure which may cause minor injury, minor property damage, or minor system damage which will result in delay or loss of availability or mission degradation.

d. Category IV - Minor - A failure not serious enough to cause injury, property damage, or system damage, but which will result in unscheduled maintenance or repair.

Figura 4: Categorias de severidade de acordo com os *failures effects* [DOD, 1980]

3.2.3. Fault Tree Analysis (FTA)

Segundo a SAE (1996), a FTA é uma análise *top-down* de falha dedutiva que se concentra em um determinado evento indesejável e fornece um método para determinar as causas deste evento.

A FAA (1988) e (2011) ilustra a relação entre a severidade e os efeitos no sistema conforme a Figura 5 e Tabela 3.

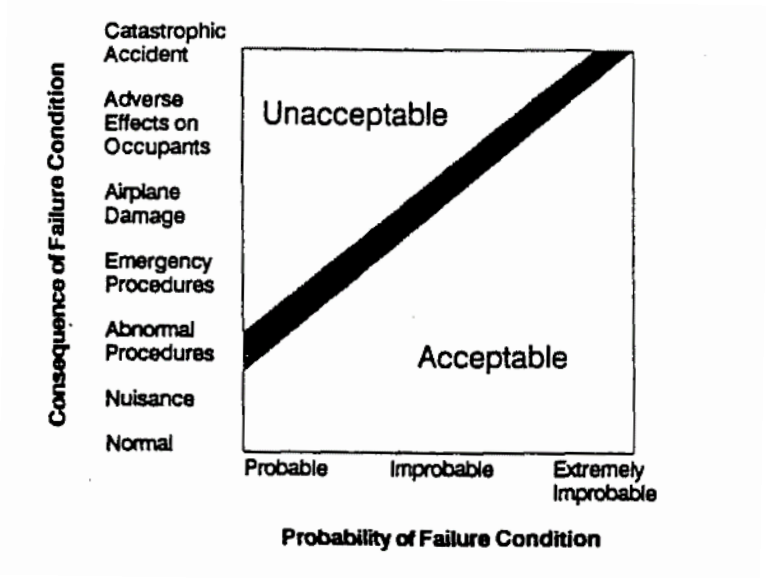

Figura 5: Relação entre probabilidade e severidade de uma condição de falha (evento topo da FTA) [FAA, 1988]

Classification of Failure Conditions	**No Safety Effect**	**<----Minor----->**	**<----Major----->**	**<--Hazardous--->**	**< Catastrophic>**
Allowable Qualitative Probability	**No Probability Requirement**	**Probable**	**Remote**	**Extremely Remote**	**Extremely Improbable**
Effect on Airplane	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with hull loss
Effect on Occupants	Inconvenience for passengers	Physical discomfort for passengers	Physical distress to passengers, possibly including injuries	Serious or fatal injury to an occupant	Multiple fatalities
Effect on Flight Crew	No effect on flight crew	Slight increase in workload or use of emergency procedures	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatal Injury or incapacitation

Tabela 3: Relação entre probabilidade, severidade e efeitos de uma condição de falha (evento topo da FTA) [FAA, 2011]

De acordo com a NASA (2002), a FTA pode ser descrita como uma técnica analítica, onde um estado indesejável do sistema é especificado (geralmente um estado crítico do ponto de

vista de *safety* ou confiabilidade), e o sistema é então analisado no contexto de seu ambiente e operação para encontrar todas as formas realistas nas quais o evento indesejável (evento principal) pode ocorrer. A FTA em si é um modelo gráfico das várias combinações paralelas e sequenciais de falhas que resultarão na ocorrência do evento topo não desejado pré-definido. As falhas podem ser eventos associados a falhas de componentes (hardware), erros humanos, erros de software, ou quaisquer outros eventos pertinentes que possam levar a o evento indesejável. Uma árvore de falhas descreve assim as inter-relações lógicas dos eventos básicos que levam ao evento indesejado, isso é, ao evento topo da árvore de falha.

A definição do evento topo é tão importante que, numa FTA, tal evento da árvore de falhas direciona todo o resto da análise. Se o evento topo for incorretamente selecionado, então a FTA estará totalmente comprometida e pode resultar em tomada de decisões erradas. A relação entre a severidade e os efeitos no sistema pode ser ilustrada como apresentada na Tabela 4.

Fault Category	Effect on system
I	Negligible
IIA	A second fault event causes a transition into Category III (Critical)
IIB	A second fault event causes a transition into Category IV (Catastrophic)
IIC	A system safety problem whose effect depends upon the situation (e.g., the failure of all backup onsite power sources, which is no problem as long as primary, offsite power service remains on)
III	A critical failure and mission must be aborted
IV	A catastrophic failure

Tabela 4: Severidade e efeitos no sistema [NASA, 2002]

4. Conclusão

A luz das motivações mencionadas no capítulo 1, esse trabalho apresentou uma breve discussão sobre as diferentes abordagens dos conceitos presentes nas técnicas FMEA e FTA, utilizados nas áreas de defesa e espaço, e aeronáutica. Com base em referências amplamente utilizadas em tais áreas, foi possível observar a importância da definição, clareza e entendimento de conceitos, abordados neste trabalho, nas fases iniciais do projeto. No trabalho de Dissertação de Mestrado da autora principal, que está em andamento, uma comparação mais detalhada de aplicação das técnicas FMEA e FTA será realizada para avaliar falhas (anomalias) de sistemas espaciais ou processos.

Agradecimentos: *Agradecemos ao Instituto Nacional de Pesquisas Espaciais e nossos orientadores Dra. Ana Paula de Sá Santos Rabello e Dr. Silvio Manea.*

Referências

DENSON, W. Reliability modeling: the RIAC guide to reliability prediction assessment and estimation. Utica, USA: Reliability Information Analysis Center, 2010. 432p. (Technical report OMB No. 0704-0188).

DEPARTMENT OF DEFENSE. Procedures for performing a failure mode, effects, and criticality analysis MIL-STD-1629A (Notice 1 e Notice 2). Washington DC, 1980. 54p.

EUROPEAN COOPERATION FOR SPACE STANDARDIZATION (ECSS). Space product assurance failure modes, effects (and criticality) analysis (FMEA/FMECA). 2.ed. Noordwijk, The Netherlands: ESA Requirements and Standards Division, 2009a. 74p. (ECSS-Q-ST-30-02C).

FEDERAL AVIATION ADMINISTRATION (FAA). System Safety Analysis and Assessment for Airplanes. EUA, 2011. (AC 23.1309-1E). Disponível em: https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_23_1309-1E.pdf. Acesso em: 10 outubro 2022.

FEDERAL AVIATION ADMINISTRATION (FAA). System Safety Analysis and Assessment for Airplanes. EUA, 1988. (AC 25.1309-1A). Disponível em: https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_25_1309-1A.pdf. Acesso em: 10 outubro 2022.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION (NASA). Fault tree handbook with aerospace applications. Washington, USA: NASA, 2002. 218p. Disponível em: http://www.mwftr.com/CS2/Fault%20Tree%20Handbook_NASA.pdf. Acesso em: 22 setembro 2022.

PESSOTTA, FERNANDO ANTONIO. "Uma estratégia para tratamento de falhas sistêmicas (FDIR) em ACDHs de satélites de pequeno e médio porte." Published Version, Instituto Nacional de Pesquisas Espaciais (INPE), 2018.

SAE AEROSPACE STANDARDS. Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment. 1996. 115p. (ARP4761)

SAE AEROSPACE STANDARDS. Guidelines for Development of Civil Aircraft and Systems. 2010. 331p. (ARP4754A)