Breve discussão sobre as diferentes abordagens de utilização das técnicas FMEA e FTA em processos aplicados nas indústrias espacial e aeronáutica

Ana Beatriz Bressan Bertaglia[1], Graziela Fernanda de Souza Maia[1], Silvio Manea[1], Ana Paula de Sá Santos Rabello[1]

[1]Instituto Nacional de Pesquisas Espaciais, Divisão de Sistemas Espaciais (DISEP), São José dos Campos/SP – Brasil

***Resumo*—Produtos que atendem elevados níveis de confiabilidade estão presentes nos projetos de engenharia de sistemas espaciais e aeronáuticos. Uma das formas de garantir a confiabilidade desses sistemas é através da identificação e avaliação de eventos adversos e, para tal, podem ser aplicadas técnicas como a FMEA (Análise dos Modos de Falha e seus Efeitos) e a FTA (Análise da Árvore de Falhas), amplamente conhecidas e utilizadas em ambas as indústrias. No entanto, ainda há necessidade de maiores esforços para se estabelecer um procedimento de escolha e de utilização dessas técnicas. Alguns conceitos chaves presentes na literatura a respeito das técnicas FMEA e FTA serão apresentados neste artigo a fim de trazer uma visão geral sobre as diferentes abordagens de utilização. Para isso, foram estudados e comparados os principais conceitos referentes a falhas, como estas são identificadas, avaliadas e mitigadas ao utilizar tais técnicas, seja empregando apenas uma ou combinando ambas.**

***Palavras-Chave*—Sistemas espaciais, Falhas, Técnicas.**

I. INTRODUÇÃO

Os métodos para realizar avaliação de risco e confiabilidade foram originados no setor de sistemas espaciais dos Estados Unidos em programas de mísseis no início da década de 1960 [1]. A NASA utilizava a técnica FMEA (Análise de Modos e Efeitos de Falha) e outros métodos de análise qualitativos para avaliações da segurança dos sistemas. Após o acidente do *Challenger* em 1986, a importância da técnica FTA (Análise de Árvore de Falhas) na análise de risco dos sistemas e na análise de confiabilidade começou a crescer ainda mais. Desde então, a avaliação de riscos com suas técnicas, incluindo a FMEA e FTA, tornou-se útil e respeitada para a avaliação da segurança e eventos não desejados em produtos das áreas de 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.

De acordo com [2], o fator contribuinte mais importante para que uma avaliação de confiabilidade seja bem-sucedida é a definição inequívoca do objetivo específico a ser alcançado na avaliação. Somente conhecendo o objetivo de uma avaliação é possível selecionar uma metodologia adequada. Se o objetivo não estiver claro, há pouca chance de que a avaliação seja bem-sucedida. Na opinião do autor, essa definição pouco clara do objetivo é a principal causa de muitas das controvérsias encontradas na disciplina de Confiabilidade. Uma avaliação bem-sucedida aproveitará os pontos fortes de metodologias específicas para atingir os objetivos específicos da avaliação em questão. Também, é possível observar em alguns trabalhos recentes na literatura, como por exemplo o trabalho de [3], onde os autores relatam que a preocupação com a utilização da FTA está cada vez mais ampla na indústria de sistemas espaciais.

Então, diante da importância das técnicas FMEA e FTA para avaliação de falhas, este trabalho tem como objetivo apresentar uma breve discussão sobre as diferentes abordagens da utilização dessas técnicas, uma vez que é de extrema importância que os conceitos estejam bem claros e definidos já que estão diretamente relacionados aos resultados das avaliações. Nesse trabalho será apresentada uma parte das FMEAs de um processo da área espacial e também da aeronáutica, e os resultados de uma parte da FTA de um processo aeronáutico.

II. METODOLOGIA

Para atingir o objetivo proposto, foi realizado um levantamento bibliográfico disponível na literatura referente a falhas e como estas são identificadas, avaliadas e mitigadas ao utilizar as técnicas FMEA e FTA. Dessa forma, foi feita uma comparação entre diferentes literaturas sobre como tais técnicas são aplicadas. No trabalho de Dissertação de Mestrado da autora principal, que está em andamento, uma comparação mais detalhada está sendo realizada.

III. DISCUSSÕES

A. Definições de termos

Os termos *failure* e *fault* são extremamente significativos para a área de engenharia de sistemas no que tange ao gerenciamento de falhas, por essa razão motiva a busca na literatura para a comparação e entendimento.

Nota-se que [4], 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 empregada como falha, já o termo *fault* geralmente é motivo de maiores discussões.

Referência [5] 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*. Ainda, considera *failure mode* (modo de falha) como um mecanismo pelo qual ocorre uma falha, *failure cause* (causa da falha) como uma causa associada a um determinado *failure mode*; e *failure effect* (efeito da falha) como uma consequência de um *failure mode* de um item sobre sua operação ou função. Referência [2], através da Tabela I, apresenta a relação entre causa, modo e efeito em diferentes níveis, em uma FMEA.

Tabela I: RELAÇÃO ENTRE CAUSA, MODO E EFEITO [2]

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

Já a Fig. 1, 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.

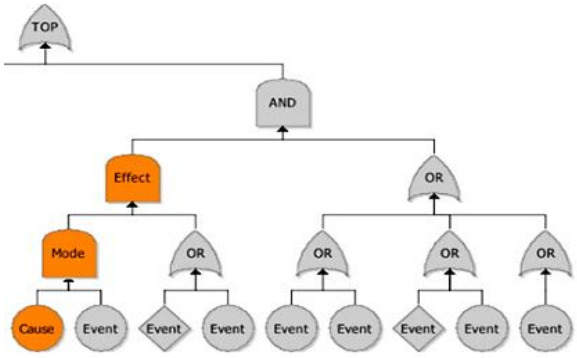

Fig. 1: Árvore de Falhas de um item ou sistema com a causa como nível mais baixo (adaptado [2])

Referência [5] 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, há uma 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.

Na área de sistemas espaciais normalmente a hierarquia considerada é: sistema, subsistema, equipamento e componente. Na área de sistemas aeronáuticos: aeronave, sistema e item [6]. Nesse trabalho é considerado a hierarquia adotada para sistemas espaciais.

B. *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 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 avaliar os problemas (eventos indesejados). 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 Fig. 2.

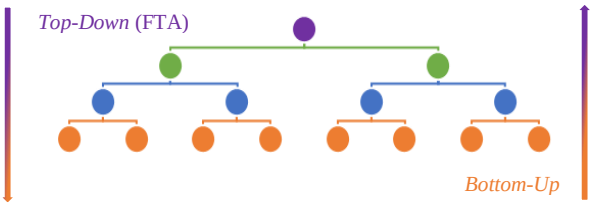

Fig. 2: Comparação entre os conceitos *Top-down* e *Bottom-up*

Dessa forma, podemos considerar que a FMEA (*bottom-up*) pode fornecer os *inputs* necessários para a FTA (*top-down*). Em outras palavras, a FTA pode receber 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, tudo isso é dependente do nível (sistema, subsistema, equipamento e componente) de aplicação das técnicas.

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

Referência [7] apresenta a seguinte definição para FMEA (tradução nossa): “Uma FMEA é uma técnica de avaliação de confiabilidade e revisão de projeto que examina os modos de falha em potencial dentro de um sistema ou nível inferior, para determinar os efeitos das falhas no desempenho do equipamento ou do sistema. Cada modo de falha de *hardware* ou *software* é classificado de acordo com seu impacto no sucesso operacional do sistema e na segurança do pessoal. A FMEA usa lógica indutiva (um processo de busca de explicações) em uma análise de sistema "*bottom-up*”, de baixo para cima. De modo geral, essa abordagem começa no nível mais baixo da hierarquia do sistema e percorre toda sua hierarquia para determinar o efeito final no desempenho do sistema. O benefício máximo da conclusão de uma FMEA é obtido a partir de uma aplicação inicial no ciclo de vida do sistema, ao invés de uma aplicação depois que o projeto do sistema é finalizado.”

D. *Fault Tree Analysis (FTA)*

Referência [7] apresenta a seguinte definição para FTA (tradução nossa): “A FTA é uma técnica sistemática e dedutiva para definir um único evento indesejável específico e determinar todos os possíveis motivos (falhas) que poderiam causar a ocorrência desse evento. O evento indesejado constitui o evento principal em um diagrama de Árvore de Falhas e geralmente representa uma falha completa ou catastrófica do produto. A FTA concentra-se em um subconjunto selecionado de todas as possíveis falhas do sistema, especificamente aquelas que podem causar um "evento principal" catastrófico. Quando aplicada adequadamente, a FTA é extremamente útil durante as fases iniciais do projeto do produto como uma ferramenta de avaliação para conduzir as modificações preliminares do projeto. Depois que um produto estiver disponível no mercado, os resultados da FTA poderão ser usados como uma ferramenta de solução de problemas. Por meio de uma FTA, um produto pode ser avaliado tanto do ponto de vista da confiabilidade quanto da probabilidade de falha. Do ponto de vista da confiabilidade, a FTA pode estimar se um produto atenderá ou não aos requisitos de desempenho de confiabilidade. Por meio da avaliação probabilística, a ênfase da FTA muda para a probabilidade de ocorrência do evento indesejado, o que é benéfico para quantificar o risco em relação aos possíveis perigos de segurança que poderiam resultar do evento indesejado.”

IV. APLICAÇÕES

A. *Aplicações das técnicas conforme a literatura*

De acordo com [8], uma das aplicações mais importantes da FMEA é auxiliar no gerenciamento de riscos, já que é uma ferramenta que pode contribuir para prevenção de falhas no projeto do produto (sistema /subsistema /equipamento /componente) e seus processos.

Conforme [5], existem dois tipos de FMEA: de projeto ou DFMEA (*Design FMEA*), e de processo ou PFMEA (*Process FMEA*), sendo que personalizações adicionais acrescentadas à FMEA podem ser favoráveis ao desempenho desta ferramenta em uma determinada organização, por levar em consideração características particulares e exclusivas de um determinado projeto. A FMEA de projeto utiliza o método analítico onde são estudados cada detalhe do projeto. Este acompanhamento identifica os possíveis modos de falha e, assim, os prevenir, com base na experiência da equipe. Este método sistemático, formalizado e documentado, possibilita o acompanhamento do projeto do início ao fim. Já a FMEA de processo tem como principais objetivos assegurar que as atividades sejam realizadas conforme designadas e identificar as possíveis falhas, prevenindo então tais falhas potenciais do processo. É uma técnica de método analítico utilizada para garantir que os modos potenciais de falha não gerem problemas no processo. Todas as etapas do processo são detalhadas e analisadas para identificar os potenciais eventos adversos.

De acordo com [1], a FTA é uma ferramenta que auxilia na busca por melhorias e informações, auxiliando na determinação quantitativa de riscos em eventos inesperados via avaliações sistemáticas, analisando cada ocorrência associada em uma razão especifica, podendo sua implementação ser baseada na prevenção ou correção de erros. Ainda segundo [1], uma FTA também pode ser construída para um sistema que está sendo projetado, assim como para um sistema que está sendo implementado e operando. Embora os princípios gerais usados na construção desses dois tipos diferentes de árvores de falha sejam os mesmos, existem diferenças nas estratégias usadas, no escopo das FTAs, e no nível de resolução delas. Quando uma FTA é construída para um sistema implementado e operacional, o projeto detalhado e as informações operacionais estão geralmente disponíveis. Neste caso, o objetivo na realização da FTA é muitas vezes melhorar o sistema ou diagnosticar problemas dentro do sistema. A FTA também pode ser construída para monitorar o desempenho de segurança ou confiabilidade do sistema, nesse caso, a árvore é desenvolvida até um nível que contém os contribuintes de interesse e para o qual os dados estão disponíveis. Isto frequentemente significa construir a FTA até o nível do componente principal, por exemplo, até o nível de uma válvula, bomba e módulo de controle. Devido a suas baixas probabilidades de falha, as tubulações e fiação não são geralmente modeladas a menos que o objetivo seja especificamente ir a este nível de detalhe ou se houver suspeita de que efeitos globais, tais como envelhecimento ou desgaste, tenham aumentado as probabilidades de falha.

A comunidade científica discute acerca da similaridade entre as técnicas, podendo ser aplicadas de forma complementar ou simultânea.

B. *Comparação entre as duas técnicas*

De acordo com [2], o objetivo da disciplina de Confiabilidade é identificar e mitigar os modos de falhas, verificar como removê-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 a criticalidade de suas consequências através de análises quantitativas e/ou qualitativas.

Referência [9] apresenta a seguinte ideia para diferenciar as técnicas FTA e FMEA (nossa tradução): É possível notar as semelhanças que a FTA compartilha com a FMEA, especialmente em relação à identificação de partes críticas que influenciam seriamente a confiabilidade do sistema. Isso pode levar alguém a questionar as diferenças entre as duas técnicas. O fator de distinção é a abordagem geral adotada por cada ferramenta. A FTA é uma abordagem dedutiva, no sentido de que pressupõe um evento específico de nível superior e considera as possíveis combinações de eventos de nível inferior que podem causar sua ocorrência. A análise "*top-down*" da FTA difere completamente da abordagem "*bottom-up*" de uma FMEA. O processo da FMEA, de propor algum evento inicial e determinar como isso afeta o sistema geral, é considerado uma abordagem indutiva. Portanto, embora apresentem resultados semelhantes, essas duas técnicas de análise de confiabilidade utilizam metodologias completamente diferentes. O consenso é que a melhor prática de confiabilidade é empregar as duas técnicas, com a mentalidade de que elas se complementam e evitam que o analista perca algum detalhe crítico.

Considerando que, na indústria de sistemas aeronáuticos, a FMEA e a FTA são normalmente aplicadas em diferentes níveis (FMEA para equipamentos e/ou componentes e FTA para sistemas e/ou subsistemas) e, corroborando com [6], amplamente utilizada na indústria aeronáutica, quando a FMEA é realizada, deve-se fazer uma comparação para garantir que todos os efeitos significativos identificados estejam na FTA como eventos básicos. Os eventos básicos da FTA obtêm suas taxas de falha das FMEAs.

Referência [10] afirma que a FTA e a FMEA podem ser combinadas em uma análise de falhas para obter os benefícios individuais de ambas as técnicas. Duas opções podem ser identificadas: (1) realizar uma FMEA e uma FTA separadamente ou (2) usar uma abordagem mista. Quanto à primeira opção, alguns autores defendem a utilização da FTA e FMEA complementares entre si, pois isso pode expandir o número de modos de falha encontrados devido aos diferentes pontos de partida de ambos os métodos: *bottom-up* na FMEA *versus top-down* na FTA. No entanto, realizar ambas as análises levariam bastante tempo, e pode levar à perda de foco nas partes mais críticas do sistema, que a análise de falhas normalmente visa identificar. Alternativamente, pode-se decidir usar uma abordagem mista que seja uma combinação de FTA e FMEA. Ambas as técnicas consomem muito tempo para serem aplicadas completamente, e é por isso que muitas vezes isso não é feito. No entanto, isso significa que possíveis modos de falha podem não ser identificados. Em [7], os autores propõem um método estruturado que leva menos tempo quando comparado ao tempo de aplicação completa das técnicas (ou seja, é mais eficiente), e também permite que seus usuários encontrem todos os modos de falha relevantes (ou seja, é eficaz). É entendido que a ideia principal dos autores é aplicar as técnicas FTA e FMEA de maneira recursiva: primeiro, é realizada uma FTA em nível de sistema, o que resulta em um conjunto de modos de falha. Usando a FMEA, a criticidade dos modos de falha é avaliada a fim de selecionar apenas os modos de falha críticos no nível do sistema. Para cada um deles, é realizada uma FTA de nível de

função, seguida de uma FMEA sobre esses modos de falha. Finalmente, uma FTA e FMEA em nível de componente são realizadas considerando os modos de falha em nível de função crítica. Vale ressaltar que a FMEA pode ser estendida a uma FMECA (Análise dos Modos de Falha, seus Efeitos e Criticidade) adicionando uma análise de criticidade. Desta forma, a FMEA puramente qualitativa pode ser feita com base numa análise também quantitativa.

Referência [2] traz a ideia da complementação da utilização de ambas as técnicas para um melhor resultado. O autor afirma que a tarefa de identificar as causas de falhas é uma atividade muito desestruturada, e que a intenção dessa tarefa é identificar todas as possíveis causas que poderiam resultar num modo de falha. As causas geralmente são mais complexas do que a identificação de um único mecanismo de falha e, portanto, descrevê-las em algumas frases na FMEA pode ser problemática. Uma causa de falha geralmente é o resultado de subcausas e pode ser detalhada cada vez mais até que o fenômeno físico da falha seja identificado. Por esse motivo, uma alternativa é realizar uma análise de FTA para cada modo de falha. Isso permite a decomposição das causas de falha em qualquer nível de detalhe.

C. *Deficiências das técnicas quando utilizadas unicamente*

Referência [10] afirma que para a análise de falhas de um sistema recentemente desenvolvido e altamente complexo, a escolha mais óbvia é usar um FMEA padrão ou um FTA padrão para a análise completa. No entanto, isso leva a algumas dificuldades, como já citado, o tempo despendido e a probabilidade de modos de falha não serem identificados. Os autores começam discutindo o uso apenas da FMEA, que é mais eficaz quando usada em sessões com diversas equipes e quando os membros da equipe têm experiência com a operação do item em questão. Porém, para a análise de um sistema novo e complexo isso oferece uma série de desafios, são eles: em primeiro lugar, o comportamento de falha de um sistema novo não é conhecido na prática, e em segundo lugar, este tipo de sistema é tipicamente grande e complexo. Isso significa que em um ambiente não estruturado, pode ser difícil definir um ponto de partida e manter uma concentração nas falhas mais críticas. Além disso, a abordagem *bottom-up* da FMEA pode tornar ainda mais difícil determinar "onde procurar modos de falha" quando há falta de experiência prática. Por último, quando a FMEA é aplicada a um sistema completo, pode ser difícil alcançar profundidade de análise suficiente para obter uma compreensão completa do comportamento da falha.

Referência [10], cita que a FTA dedutiva e estruturada pode ser utilizada como método único para analisar o comportamento da falha. Embora a FTA tenha algumas vantagens sobre a FMEA, ela ainda apresenta algumas desvantagens na análise de sistemas complexos. São vantagens: em primeiro lugar, a abordagem estruturada da FTA é uma vantagem quando um sistema completamente novo é analisado e há pouca experiência prática com falhas de sistema no campo (devido ao raciocínio estruturado e dedutivo implícito na FTA, ela depende menos da experiência prática do especialista do que a FMEA); em segundo lugar, a FTA é uma técnica gráfica mais fácil de interpretar e de identificar as interrelações em comparação com a FMEA; em terceiro lugar, a complexidade do sistema em análise implica que seria difícil realizar uma FMEA em todo o sistema com profundidade de análise suficiente (este também é o caso da FTA, mas o analista pode optar por aprofundar-se apenas em partes ou ramos específicos da árvore, o que torna a FTA uma abordagem mais controlável. Se o analista decidir não se aprofundar em um ramo específico da Árvore de Falhas, ele poderá usar o evento não desenvolvido que representa que o ramo não é mais analisado. No entanto, não existem diretrizes rigorosas para decidir sobre a utilização de um evento não desenvolvido e esta decisão é muitas vezes tomada de forma arbitrária ou baseada no parecer de peritos).

Corroborando com a ideia de que ambas as técnicas são ótimas, mas deficientes quando utilizadas unicamente, tem-se em [3] que a FTA é uma análise que começa com uma falha total do sistema e vai descendo, explorando cada possível causa até que o nível do componente seja alcançado. Isto é útil para analisar os efeitos combinados das falhas, mas é pobre para esclarecer todas as suas possíveis causas. Já a FMEA é uma abordagem ascendente, que começa com cada componente e explora como os efeitos de uma falha se propagam através de um sistema. Esta técnica é muito eficaz para descrever a maioria das causas de falhas em um sistema, mas se esforça para explorar como seus efeitos podem se combinar. Ainda, afirmam que é comum aplicar em conjunto tanto a FTA como a FMEA em vários sistemas, dado que cada uma é eficaz no reforço das fraquezas da outra.

V. RESULTADOS E DISCUSSÕES

Para aplicação das técnicas, na prática, foram selecionados dois processos. O primeiro, relacionado à indústria de sistemas espaciais, referente à soldagem de interconectores em células solares estudado por Graziela Maia em sua Dissertação de Mestrado [11]. O segundo, relacionado à indústria aeronáutica e amplamente utilizado, referente ao FHA (*Failure Hazard Analysis*). Até o presente momento, para o desenvolvimento da Dissertação de Mestrado da autora principal, a FMEA foi aplicada em ambos os processos por algumas vezes, amadurecendo a cada nova revisão. Já a FTA, até o momento foi aplicada apenas no processo relacionado à indústria aeronáutica. Portanto, neste artigo, será apresentada apenas uma pequena parte para representar a aplicação da técnica em cada processo (FMEA para ambos e FTA para o FHA).

A. *FMEA aplicada ao processo de um sistema espacial*

O desenvolvimento de um painel solar de satélite pode ser descrito por um processo genérico. Tal processo, compreende os níveis de processo, subprocesso, atividade e tarefa. Estão representadas pela Fig. 3 as tarefas de uma determinada atividade pertencente a esse processo.

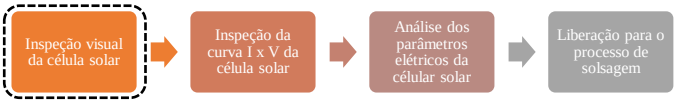

Fig. 3: Tarefas de uma determinada atividade no processo genérico de desenvolvimento do painel solar de satélite

A FMEA será exemplificada parcialmente pela análise da tarefa "Inspeção visual da célula solar" (em destaque na Fig. 3), conforme apresentada na Tabela II.

Tabela II: FMEA PARCIAL DA TAREFA “INSPEÇÃO VISUAL DA CÉLULA SOLAR”

Etapa do processo	Modos de falha	Causa da Falha	Efeito da Falha			Classificação de Severidade		Métodos de Detecção	Provisão Compensatória	Recomendações
			Efeito Local (Célula solar)	Efeito no próximo nível superior (SCA)	Efeito final (Painel Solar)	(Célula solar)	(Painel Solar)			
Inspeção visual da célula solar	Célula solar apresentando riscos / arranhões	Falta de inspeção de recebimento, manuseio incorreto.	A eficiência da célula solar não será conforme esperado	O SCA com nível de eficiência degradada	Painel solar irá produzir menos energia do que é capaz	Maior	Negligenciável	Inspeção ao receber o produto	A pessoa responsável pelo armazenamento deve ser informada sobre como deve ser o procedimento de inspeção de recebimento e manuseio.	Treinamento do pessoal
	Microfissuras não visíveis a olho nu	Pressão sob as caixas de armazenamento, falta de cuidado ao transportar, manuseio incorreto.	Degradação da eficiência da célula solar	O SCA com nível de eficiência degradada	Painel solar irá produzir menos energia do que é capaz	Negligenciável	Negligenciável	Inspeção da eficiência da célula solar	Ter o máximo de cuidado durante o transporte e armazenamento das células	Conscientização dos envolvidos

B. *FMEA aplicada ao processo de um sistema aeronáutico*

O processo de FHA pode ser dividido em dois subprocessos: FHA de aeronave (AFHA) e FHA de sistemas (SFHA). Para este trabalho foi selecionado o SFHA. As atividades do subprocesso escolhido podem ser descritas genericamente conforme representado pela Fig. 4.

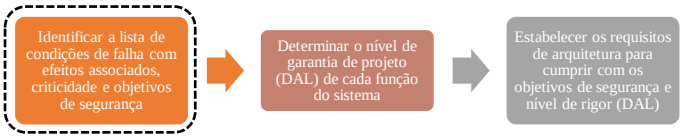

Fig. 4: Atividades do subprocesso genérico de SFHA

A atividade “Identificar a lista...” (em destaque na Fig. 4) é detalhada no nível de tarefas, através da Fig. 5.

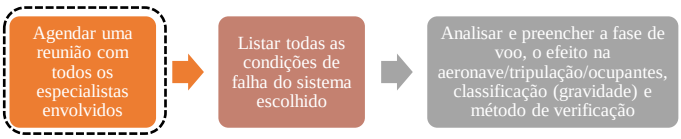

Fig. 5: Tarefas da atividade “Identificar a lista...” do subprocesso SFHA

Para este artigo, a FMEA será apresentada apenas parcialmente para a tarefa “Agendar uma reunião com todos os especialistas envolvidos” (tarefa em destaque na Fig. 5) representada pela Tabela III.

Tabela III: FMEA PARCIAL DA TAREFA “AGENDAR UMA REUNIÃO...”

Etapa do processo	Modos de falha	Causa da Falha	Efeito da Falha			Classificação de Severidade		Métodos de Detecção	Provisão Compensatória	Recomendações
			Efeito Local (na tarefa)	Efeito no próximo nível (na atividade)	Efeito final (no processo SFHA)	Técnica	Gerencial			
Agendar (enviar convite) reunião com todos os especialistas envolvidos	Convite não enviado para nenhum dos convocados	Falha de internet/servidor	Não haverá a reunião	A lista de condições não será elaborada nessa ocasião	O processo SFHA não será realizado nessa ocasião	Sem efeito	Menor	Nenhuma resposta será enviada ao organizador da reunião	Utilizar a ferramenta de convocação de reunião para confirmar a presença de todos os envolvidos	Solicitar resposta dos convocados ao aceitarem a reunião
		Esquecimento do envio do convite por parte do organizador								
	Convite enviado para apenas alguns dos especialistas	Falha de internet/servidor	Não haverá a reunião	A lista de condições não será elaborada nessa ocasião	O processo SFHA não será realizado nessa ocasião	Sem efeito	Menor	Verificar no início da reunião se todos os envolvidos estão presentes	Criar uma lista padrão dos especialistas necessários por Departamento e fazer a conferência dos especialistas presentes antes de iniciar a reunião	Solicitar resposta dos convocados ao aceitarem a reunião
		Esquecimento/erro na seleção completa de destinatários por parte do organizador								
		Falta de experiência por parte do organizador								
		Falha no processo na definição dos especialistas necessários								
	Convite enviado para mais especialistas do que o necessário	Falta de organização por parte do organizador	Pessoas que não são da área serão deslocadas para uma atividade que não poderão desenvolver/ cooperar.	A lista de condições de falha poderá contemplar cenários incoerentes.	O processo não terá eficiência máxima.	Menor	Maior	Verificar no início da reunião se há mais especialistas do que o necessário	Criar uma lista padrão dos especialistas necessários por Departamento	Fazer a conferência dos especialistas presentes antes de iniciar a reunião
		Falta de experiência por parte do organizador								

C. *FTA aplicada ao processo de um sistema aeronáutico*

Durante o exercício de aplicação da técnica FTA, o evento topo considerado foi a falha da atividade “Identificar a lista de condições de falha com efeitos associados, criticidade e objetivos de segurança” (em destaque na Fig. 4), que gerou uma árvore com 483 eventos. Desta forma, observou-se que alguns eventos (intermediário de segundo nível) que compõem o evento topo, exigiram mais desenvolvimento do que outros. Por exemplo, abaixo do evento topo foram consideradas três falhas, uma para cada tarefa da atividade em questão (conforme Fig. 5). Considerando a análise da tarefa “Agendar uma reunião com todos os especialistas envolvidos”, tem-se que essa possui 273 eventos (56% do total de eventos da FTA completa); a tarefa “Listar todas as condições de falha do sistema escolhido”, possui 190 eventos (39% do total de eventos da FTA completa); e a tarefa “Analisar e preencher a fase de voo, o efeito na aeronave/tripulação/ocupantes, classificação (gravidade) e método de verificação”, possui 20 eventos (5% do

total de eventos da FTA completa).

D. *Resultados após aplicação parcial das técnicas*

Após a aplicação das técnicas, foi observado que os efeitos que são de outra natureza (natureza: técnica, gerencial, programática), ou estão em outro nível, podem ser considerados na análise através da técnica FTA, o que não seria possível com a aplicação da FMEA, que determina e define com rigor as camadas dos efeitos da falha a serem desenvolvidos. Tem-se como exemplo a tarefa "Agendar uma reunião com todos os especialistas envolvidos" (em destaque na Fig. 5), avaliada tanto na FMEA quanto na FTA. Pode-se observar através deste exemplo, que na FMEA os modos, causas e efeitos das falhas foram listados exaustivamente, no entanto respeitando o limite dos níveis pré-estabelecidos. Em contrapartida, após a aplicação da mesma tarefa na FTA, foi observado que os eventos que levam a tal falha (não agendar reunião com todos os especialistas) podem ser extrapolados até o nível em que os especialistas acreditam ser necessário e relevante para a análise, não havendo um limite de nível para chegar ao evento básico. Portanto, após a aplicação parcial das técnicas FTA e FMEA, podemos já concluir que FMEA possui uma característica positiva que é listar de modo exaustivo todos os modos de falha conhecidos pelos especialistas e, consequentemente, suas causas e efeitos. Já a FTA possui uma característica positiva no que tange a listar todos os eventos contribuintes para uma determinada falha com vasta amplitude de níveis e diferente natureza.

VI. OBSERVAÇÕES FINAIS

Corroborando com o explanado nesse trabalho, para [12], a FTA não é como uma FMEA. A FMEA é uma análise de baixo para cima (*bottom-up)* de todos os modos de falha do item, enquanto a FTA é uma análise de cima para baixo (*top-down)*. Além disso, a FTA inclui apenas as falhas pertinentes ao evento indesejado, enquanto a FMEA traz uma análise exaustiva de todos os modos de falha e seus efeitos. De acordo com [13], as técnicas se complementam, e combinadas são mais claras e razoáveis para revelar a relação entre falhas de componentes e falhas do sistema. Dessa forma, é possível constatar com maior precisão quais são os componentes mais importantes e de maiores efeitos para o sistema. Podemos perceber que muito se encontra na literatura sobre os conceitos e padrões das técnicas de análise FMEA e FTA, mas pouco se encontra sobre o "passo a passo" de suas aplicações, quais os "melhores caminhos" e "dicas" para resultados mais eficientes. Por isso, no trabalho de Dissertação de Mestrado da autora principal, que está em andamento, está sendo realizado um estudo a fim de analisar, registrar e otimizar as diferentes visões que se encontram nas literaturas apresentadas nas seções anteriores, que diz respeito à utilização das técnicas. Foram selecionadas as três abordagens abaixo para tal estudo:

- Teoria e Análise: estudo das boas práticas presentes na literatura e comparação com a prática utilizada na indústria;
- Modelagem e Simulação: diversos exercícios da aplicação das técnicas; e
- Observação e Experimentação: registro de todo o passo a passo dos exercícios realizados para aplicação das técnicas.

Com relação a aplicação das técnicas, vale ressaltar que é um processo interativo, com diversas repetições de análise. A cada aplicação o grupo se reúne para discutir as dificuldades e possíveis melhorias a serem utilizadas na aplicação seguinte. Esse processo está sendo repetido até que, no entendimento do grupo, haja amadurecimento da aplicação das técnicas com registros sólidos e maduros para que uma conclusão da interação das técnicas de FMEA e FTA seja possível.

VII. CONCLUSÃO

A luz das discussões apresentadas nas seções anteriores, esse trabalho apresentou uma breve discussão sobre as diferentes abordagens da utilização das técnicas de análise FMEA e FTA, utilizadas nas áreas espacial e aeronáutica, uma vez que é de extrema importância que tais conceitos sejam bem claros e definidos já que estão diretamente relacionados aos resultados das avaliações. Com base em referências amplamente utilizadas em tais áreas, foi possível observar a importância da definição, clareza e entendimento de conceitos, para então entender melhor o que pode ser considerado como vantagens e desvantagens na aplicação de ambas as técnicas, em ambas as áreas.

REFERÊNCIAS

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

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

[3] TIMPERLEY, Louis & Berthoud, Lucy. (2022). Reliability Analysis and Failure Mitigation Strategies for the PROVE Pathfinder CubeSat Payload. Disponível em: https://www.researchgate.net/publication/362626203_Reliability_Analysis_and_Failure_Mitigation_Strategies_for_the_PROVE_Pathfinder_CubeSat_Payload/citations. Acesso em: 24 abril 2024.

[4] 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.

[5] EUROPEAN COOPERATION FOR SPACE STANDARDIZATION (ECSS). Space product assurance failure modes, effects (and criticality) analysis (FMEA/FMECA). 2. ed., 2009a. 74 p. (ECSS-Q-ST-30-02C).

[6] SAE AEROSPACE STANDARDS. Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment. 1996. 115 p. (ARP4761)

[7] DEPARTMENT OF DEFENSE. Guide for Achieving Reliability, Availability, and Maintainability. Washington DC, 2005. 266 p.

[8] DAILEY, K. W. The FMEA Pocket Handbook. DW Publishing Co. 2004. 40p.

[9] ROSE, D; MACDIARMID A.; LEIN, P. Mechanical analysis and other specialized techniques for enhancing reliability (MASTER). Quanterion Solutions Incorporated, 2012. 611 p.

[10] J.F.W. Peeters, R.J.I. Basten, T. Tinga, Improving failure analysis efficiency by combining FTA and FMEA in a recursive manner, Reliability Engineering & System Safety, Volume 172, 2018, Pages 36-44, ISSN 0951-8320.

[11] MAIA, G. F. S., Estudo e otimização do processo de soldagem de interconectores às células de painéis solares empregados em satélites artificiais aplicando projeto e análise de experimentos. São José dos Campos: INPE, 2021. Disponível em: http://mtc-m21c.sid.inpe.br/col/sid.inpe.br/mtc-m21c/2021/05.04.16.16/doc /doc/publicacao.pdf. Acesso em: 6 fev. 2024.

[12] ERICSON II, C.A. Introduction to Fault Tree Analysis, 2014, slides. Disponível em: http://ndl.ethernet.edu.et/bitstream/123456789/87809/12/FTA.pdf. Acesso em 20 jun 2024.

[13] Y. YANG, S. Yan, L. Xie and J. Wu, "Failure analysis of deployment mechanism of a satellite solar array," The Proceedings of 2011 9th International Conference on Reliability, Maintainability and Safety, Guiyang, China, 2011, pp. 931-937, doi: 10.1109/ICRMS.2011.5979419.