UNIVERSIDADE FEDERAL DE MINAS GERAIS
ESCOLA DE ENGENHARIA
CURSO DE ENGENHARIA DE SISTEMAS
TRABALHO DE CONCLUSÃO DE CURSO

Thales Pereira Tenebra

FTA E STPA NA ANÁLISE DE RISCOS DO SUBSISTEMA DE COMUNICAÇÃO DE UM CUBESAT

Belo Horizonte
2025

Thales Pereira Tenebra

FTA E STPA NA ANÁLISE DE RISCOS DO SUBSISTEMA DE COMUNICAÇÃO DE UM CUBESAT

Trabalho de Conclusão de Curso apresentado ao Curso de Engenharia de Sistemas da Universidade Federal de Minas Gerais, como requisito parcial para a obtenção do grau de bacharel em Engenharia de Sistemas.

Orientadora: Prof. Dr. Michel Bessani

Coorientador: Eng. João Paulo Brandão Dantas

Belo Horizonte
2025

AGRADECIMENTOS

Dedico este trabalho, antes de tudo, a Deus, que me sustentou nos momentos de incerteza e me deu forças para continuar mesmo quando tudo parecia desmoronar. Foi Ele quem me guiou com propósito, colocou as pessoas certas no caminho e me deu paz em meio à pressão. Sua providência divina foi constante, Ele mostrou que cuida de cada detalhe da nossa jornada. Cada linha deste trabalho carrega não só esforço técnico, mas também oração, fé e gratidão.

À Lucimara, minha mãe, que acreditou em mim quando nem eu mesmo sabia se seria possível trilhar este caminho. Você me incentivou desde quando o como seria minha permanência em Belo Horizonte era incerto e incógnito, oferecendo não apenas apoio, mas verdadeira confiança no meu potencial. À Karina, irmã e companheira de jornada, que foi abrigo nos dias difíceis, apoio nos momentos de cansaço e alegria nos pequenos avanços. Este trabalho é também de vocês.

Agradeço com sinceridade ao meu orientador Michel Bessani e ao coorientador João Dantas que contribuíram com olhar crítico, incentivo e direcionamento em todas as etapas. Um agradecimento especial ao Felipe Turetta da Boeing, por tornar possível a colaboração com um coorientador tão dedicado e presente. Essa parceria foi essencial para o crescimento técnico e intelectual deste trabalho.

E dedico este TCC a mim mesmo, à versão de mim que resistiu. Trabalhar e estudar ao mesmo tempo nunca foi fácil, especialmente em um curso exigente como este. Foram anos de superação, noites mal dormidas, prazos apertados, sabendo que, apesar de tudo, nunca tive dúvida do meu propósito. Mas também foram anos de amadurecimento, de força forjada na dificuldade e de conquistas que carregam mais valor justamente por tudo que custaram. Se cheguei até aqui, foi por inabalável propósito.

"Este é o caminho de quem assume uma missão: atravessar florestas de incertezas, escalar montanhas de complexidade e seguir, mesmo sem saber o que o próximo passo reserva. No fim, não é o poder que vence, mas a clareza de propósito e a integridade de quem não se desviou."

(inspirado na jornada de Frodo e Sam)

RESUMO

Este trabalho apresenta a aplicação integrada da *Fault Tree Analysis* (FTA) e da *System-Theoretic Process Analysis* (STPA) ao subsistema de comunicação do CubeSat PdQSat, demonstrando como a combinação dessas metodologias fornece uma visão mais holística dos riscos do que cada técnica isoladamente. A FTA permitiu identificar conjuntos de corte mínimos relacionados a falhas de *hardware*, destacando vulnerabilidades como a corrupção do micro-SD do Raspberry Pi, a fim de gerar recomendações de robustez, redundância e gestão térmica. A STPA revelou *Unsafe Control Actions* (UCAs) e cenários causais associados, evidenciando riscos gerados por *feedback* inadequado, modelos de processo imprecisos e emissões de radiofrequência fora dos limites regulatórios. A análise de sinergia mostrou que a STPA é mais eficaz nas fases iniciais do ciclo de vida ao orientar requisitos e restrições de segurança, enquanto a FTA complementa a verificação e validação nas fases finais.

Palavras-chave: Análise de risco; FTA; STPA; CubeSat; Integração de metodologias.

ABSTRACT

This work presents the integrated application of Fault Tree Analysis (FTA) and System-Theoretic Process Analysis (STPA) to the communication subsystem of the CubeSat PdQSat, demonstrating how combining these methodologies provides a more holistic view of risks than each technique in isolation. FTA made it possible to identify minimal cut sets related to hardware failures, highlighting vulnerabilities such as corruption of the micro-SD on the Raspberry Pi, in order to generate recommendations for robustness, redundancy, and thermal management. STPA revealed Unsafe Control Actions (UCAs) and associated causal scenarios, evidencing risks caused by inadequate feedback, imprecise process models, and radio-frequency emissions beyond regulatory limits. The synergy analysis showed that STPA is more effective in the early life-cycle phases by guiding safety requirements and constraints, whereas FTA complements verification and validation in the later phases.

Keywords: Risk analysis; FTA; STPA; CubeSat; Methodology Integration.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

COTS	*Commercial Off-The-Shelf*
FHA	*Functional Hazard Assessment*
FTA	*Fault Tree Analysis*
HSI	*Human Systems Integration*
INCOSE	*International Council on Systems Engineering*
LDSE	*Loss-Driven Systems Engineering*
MCC	*Mission Control Center*
RF	Radiofrequência
SDR	*Software Defined Radio*
STPA	*System-Theoretic Process Analysis*
UCA	*Unsafe Control Action*
UFMG	Universidade Federal de Minas Gerais
V&V	*Verification and Validation*
VLS	Veículo Lançador de Satélites

SUMÁRIO

1 INTRODUÇÃO

O contínuo avanço da indústria aeroespacial tem impulsionado a busca por metodologias cada vez mais eficazes para garantir a segurança e a confiabilidade de sistemas espaciais. Nesse contexto, os CubeSats, satélites miniaturizados com grande potencial educacional e científico, destacam-se como plataformas acessíveis para testes tecnológicos e capacitação acadêmica. O PdQSat[1], desenvolvido na Universidade Federal de Minas Gerais (UFMG), é um exemplo desse tipo de iniciativa, voltado à demonstração tecnológica e à formação de estudantes. Dada a criticidade inerente aos sistemas espaciais, torna-se essencial a aplicação de metodologias robustas de análise de risco para assegurar o sucesso da missão.

O presente trabalho foca no subsistema de comunicação do PdQSat, que desempenha o papel de troca de informações entre o satélite e a estação terrestre. Problemas nesse subsistema podem comprometer a missão como um todo, tornando essencial a aplicação de técnicas para prever e mitigar possíveis falhas. Essa criticidade exige abordagens de análise de risco capazes de capturar tanto falhas isoladas quanto interações complexas entre componentes. A integração de abordagens tradicionais e modernas de análise de risco pode oferecer uma estratégia mais eficaz para garantir a robustez do sistema.

A escolha dos métodos STPA e FTA para essa análise permite a identificação de falhas tanto em nível sistêmico quanto na avaliação das probabilidades de eventos raiz resultarem em modos de falha relevantes. A investigação dessas metodologias e sua possível integração contribui para ampliar a compreensão dos desafios envolvidos na mitigação de riscos durante o desenvolvimento de sistemas.

1.1 Justificativa

A análise de riscos é uma etapa essencial no desenvolvimento de sistemas críticos, inclusive aqueles aplicados em missões espaciais, onde falhas podem resultar na perda total da missão. Métodos tradicionais, como a FTA, são amplamente utilizados na engenharia aeroespacial devido à sua abordagem estruturada e quantitativa (Rausand, 2014). No entanto, a crescente complexidade dos sistemas modernos requer metodologias complementares que abordem aspectos sistêmicos e interdependências entre componentes.

A STPA surge como uma alternativa promissora, pois considera de forma holística as interações entre os componentes do sistema, avaliando o cumprimento de restrições de segurança e possíveis ações de controle inseguras (Leveson, 2012). Dessa forma, a integração entre STPA e FTA pode reunir os pontos fortes de ambas as abordagens, proporcionando uma análise mais completa e adequada às particularidades do subsistema de comunicação do PdQSat, ao aliar a estruturação quantitativa da FTA à perspectiva sistêmica da STPA.

[1] https://ufmg.br/comunicacao/noticias/pdqsat-satelite-em-desenvolvimento-na-engenharia-qualifica-mao-de-obra-para-setor-aeroespacial

A importância desse estudo pode ser exemplificada pelo caso do Veículo Lançador de Satélites (VLS)-01, cujo acidente ocorrido em 2003 ilustra as consequências severas de falhas não previstas na análise de risco. O incidente, que resultou na destruição do foguete e na perda de vidas humanas, destaca a necessidade de abordagens mais eficazes para a mitigação de falhas em sistemas espaciais (Nogueira, 2023). Dessa forma, a pesquisa proposta visa contribuir para o aprimoramento das técnicas de análise de risco, garantindo maior confiabilidade às futuras missões de CubeSat, em especial do PdQSat.

1.2 Objetivos

Este trabalho tem como objetivo principal integrar as metodologias STPA e FTA na análise de risco do subsistema de comunicação do PdQSat, buscando compreender suas diferenças, complementaridades e vantagens na identificação e mitigação de riscos. Adicionalmente, busca-se analisar a sinergia entre as metodologias sob a ótica da Engenharia de Sistemas, considerando suas aplicabilidades em diferentes etapas ao longo do ciclo de vida do sistema. Para alcançar tal objetivo, os seguintes objetivos específicos são definidos:

- Realizar uma revisão da literatura sobre metodologias de análise de risco aplicadas a sistemas aeroespaciais, com ênfase em STPA e FTA;
- Caracterizar o subsistema de comunicação do PdQSat como objeto de estudo, com foco na identificação de suas funcionalidades críticas e potenciais falhas;
- Aplicar as metodologias STPA e FTA ao subsistema, avaliando sua eficácia na identificação e mitigação de riscos;
- Explorar a sinergia entre STPA e FTA a partir de conceitos da engenharia de sistemas, como requisitos, arquitetura, *Verification and Validation* (V&V), destacando os etapas em que cada técnica contribui de forma mais efetiva;
- Propor estratégia de integração dos métodos para agregar qualidades e mitigar pontos fracos dos métodos;
- Documentar os procedimentos, análises e conclusões, visando à consolidação de uma contribuição teórica e prática para o projeto do PdQSat.

2 REVISÃO BIBLIOGRÁFICA

A análise de falhas é essencial para garantir a segurança e a confiabilidade de sistemas, especialmente em áreas de alta criticidade, como a aeroespacial. Diversas metodologias são utilizadas para identificar, avaliar e mitigar falhas, sendo a FTA e a STPA algumas das mais proeminentes (Elizebeth *et al.*, 2023). Ambas as abordagens visam analisar a ocorrência de falhas por meio de diferentes paradigmas: a FTA é uma análise probabilística baseada na decomposição de modos de falha em causas descritas em diferentes níveis do sistema; já a STPA adota uma abordagem sistêmica e holística, analisando interações entre componentes, controles, fluxos de informação e condições que tornam ações de controle inseguras. Essa abordagem permite identificar cenários de risco mesmo na ausência de falhas físicas, considerando fatores como erros humanos, falhas organizacionais e influências ambientais durante a etapa de desenvolvimento, gerando requisitos de segurança para o sistema de maneira antecipada à implementação.

A segurança e a confiabilidade de sistemas espaciais são tradicionalmente abordadas por meio de análises probabilísticas, como a FTA, que modela falhas em estruturas hierárquicas para prever eventos críticos (Vesely *et al.*, 2002). A metodologia é amplamente aplicada em diversos setores devido à sua capacidade de quantificar riscos e identificar falhas primárias que podem comprometer o desempenho do sistema. Um estudo realizado na Malásia aplicou a FTA para analisar quedas fatais em trabalhos em altura, evidenciando sua eficácia na priorização de ações corretivas (Zermane *et al.*, 2022).

Entretanto, abordagens como a FTA apresentam limitações ao lidar com sistemas complexos, altamente integrados e influenciados por fatores humanos. Para mitigar essas limitações, foi desenvolvida a STPA (Leveson e Thomas, 2018), método centrado na identificação de *Unsafe Control Action*s (UCAs) e nas condições de controle que podem levar a falhas sistêmicas. Um estudo comparativo entre FTA e STPA em um sistema de *Brake-by-Wire* demonstrou que, enquanto a FTA identificou 93 eventos primários, a STPA revelou 802 fatores causais, destacando sua superioridade em capturar interações sistêmicas e comportamentos inesperados (Elizebeth *et al.*, 2023).

O uso dessas metodologias em sistemas como nanossatélites do tipo CubeSat se torna cada vez mais relevante, à medida que esses dispositivos ganham protagonismo e exigem análises rigorosas para assegurar seu desempenho em condições extremas. Faiella *et al.* (2017) propuseram uma abordagem proativa de avaliação de riscos, combinando dados históricos com testes funcionais e análises probabilísticas, contribuindo para avaliações mais abrangentes em nanossatélites. Langer *et al.* (2017), por sua vez, desenvolveram uma ferramenta de estimativa de confiabilidade aplicada ao CubeSat MOVE-II. A ferramenta combinou dados de falhas com testes em solo, utilizando modelos Bayesianos para determinar o ponto de saturação de testes e apoiar decisões sobre a continuidade das campanhas de validação.

A confiabilidade de CubeSats continua sendo um desafio, dada sua arquitetura com-

pacta e restrições de custo. Estudos indicam que falhas precoces podem ser reduzidas por meio de testes mais rigorosos e da aplicação de metodologias robustas de análise de risco (Bouwmeester, Menicucci e Gill, 2022). A aplicação da FTA no CubeSat Catarina-A1, por exemplo, permitiu a identificação de padrões recorrentes de falhas, reforçando a importância dessa abordagem na mitigação de riscos em pequenos satélites (Bernardes, 2023).

Recentemente, tem-se observado um crescente interesse na integração de metodologias de análise de risco. O estudo de Weglian, Riley e Gibson (2023) propõe a aplicação combinada de STPA e FTA para sistemas aeroespaciais, destacando que a STPA fornece uma visão abrangente das interações e dinâmicas do sistema, enquanto a FTA possibilita a quantificação probabilística dos riscos associados a falhas identificadas. Essa visão está alinhada às boas práticas de Engenharia de Sistemas descritas no *INCOSE Systems Engineering Handbook* (INCOSE, 2023), que reconhece o valor da integração de métodos qualitativos e quantitativos para ampliar a compreensão dos riscos em sistemas complexos.

Adicionalmente, o trabalho de Poth (2024) reforça a relevância dessa integração ao comparar diversas abordagens de análise de risco, como FMEA, FTA, STPA e *Product Quality Risk* (PQR). O autor argumenta que métodos como a STPA são mais eficazes em capturar falhas emergentes e interações sistêmicas, enquanto métodos como a FMEA se mostram úteis na análise detalhada de componentes. A combinação de diferentes abordagens é apontada como estratégia promissora para a construção de diagnósticos mais robustos e completos.

O subsistema de comunicação é um dos componentes mais críticos de um CubeSat, pois viabiliza a transmissão de dados, comandos e telemetria entre o satélite e a estação terrestre. Falhas nesse subsistema podem comprometer a missão por completo, tornando essencial a aplicação de metodologias de análise de risco. Segundo Johnstone *et al.* (2020), os desafios enfrentados pelos subsistemas de comunicação incluem interferências de Radiofrequência (RF), limitações de potência e degradação de componentes em ambiente orbital.

3 ASPECTOS DE HUMANIDADES

O desenvolvimento de CubeSats traz consigo uma série de impactos que vão além do desempenho técnico e das metas de engenharia. Esses impactos incluem considerações ambientais, econômicas e sociais, que são essenciais para avaliar a viabilidade, a sustentabilidade e o valor público desses projetos. Nesta seção, são discutidos os principais aspectos relacionados a esses impactos, subdivididos em impactos ambientais, econômicos e sociotécnicos.

3.1 Impactos Ambientais

Os projetos envolvendo satélites, incluindo os CubeSats, devem considerar os impactos ambientais associados, especialmente em relação ao lixo espacial. Os detritos espaciais (*debris*) e micrometeoritos representam um risco significativo para outros sistemas em órbita, podendo comprometer missões futuras e gerar colisões que aumentam ainda mais a quantidade de lixo espacial. Essa questão é uma preocupação central na sustentabilidade espacial (Gaston *et al.*, 2023).

Para mitigar esses impactos, o desenvolvimento do CubeSat estudado neste trabalho incluirá medidas para evitar que o sistema contribua para o aumento do lixo espacial. Embora o foco principal desta pesquisa seja a análise de risco do subsistema de comunicação, essa análise desempenha um papel importante nesse objetivo, pois falhas nesse subsistema podem comprometer a comunicação com o satélite e impedir o monitoramento adequado de sua condição operacional ao final de sua vida útil. Assim, ao aumentar a confiabilidade do subsistema de comunicação, este trabalho contribui diretamente para a capacidade de acompanhar o status do CubeSat e verificar sua conformidade com as diretrizes internacionais, como a ISO 24113:2019, que recomenda a reentrada atmosférica com destruição completa do sistema. Essa abordagem minimiza os riscos ambientais e alinha o projeto às práticas recomendadas de sustentabilidade espacial.

A consideração desses aspectos ambientais é fundamental para garantir que o projeto esteja em conformidade com as normas internacionais e para promover uma exploração espacial responsável, contribuindo para a manutenção de um ambiente orbital seguro e sustentável.

3.2 Impactos Econômicos

O uso de CubeSats oferece vantagens econômicas significativas em comparação com satélites convencionais, principalmente devido ao seu menor custo de desenvolvimento e lançamento. O projeto do CubeSat abordado neste trabalho utiliza componentes *Commercial Off-The-Shelf* (COTS), reduzindo substancialmente os gastos com *design* e fabricação de *hardware*.

Além disso, o lançamento de CubeSats é geralmente realizado como carga secundária em missões maiores, o que diminui os custos associados a essa fase do ciclo de vida do sistema.

Essa característica torna o CubeSat uma opção viável para projetos acadêmicos e de pesquisa com orçamento limitado, como o explorado neste trabalho.

A adoção do padrão CubeSat também traz benefícios econômicos relacionados à reutilização de *designs* e padrões amplamente aceitos, permitindo economia de recursos durante as fases de projeto e validação. Dessa forma, o desenvolvimento do CubeSat não apenas promove inovação tecnológica, mas também oferece uma solução acessível e eficiente para atender aos objetivos do projeto, maximizando o retorno sobre o investimento limitado em projetos acadêmicos e científicos.

3.3 Impactos Sociotécnicos e Políticos

Além dos aspectos ambientais e econômicos, projetos como o PdQSat possuem implicações sociotécnicas significativas. Ao envolver instituições públicas de ensino, investimento governamental e participação estudantil em tecnologias de fronteira, esse tipo de iniciativa provoca reflexões sobre o papel do Estado no fomento à educação tecnológica e à capacitação nacional em Engenharia de Sistemas.

O sucesso ou a falha desses projetos tem impacto direto na opinião pública e na percepção da sociedade sobre o valor do investimento público em ciência, tecnologia e inovação. Um CubeSat bem-sucedido fortalece a confiança em políticas de incentivo à pesquisa acadêmica aplicada, enquanto fracassos podem ser explorados para questionar a eficácia desses investimentos. Essa dimensão política e comunicacional transcende a engenharia técnica e exige uma postura consciente por parte dos profissionais envolvidos.

É nesse contexto que se destaca o papel do engenheiro de sistemas: atuar como um elo entre o domínio técnico e as expectativas da sociedade, compreendendo que seu trabalho está inserido em um ecossistema mais amplo, que inclui valores públicos, interesses institucionais e repercussões de longo prazo. Projetos como o PdQSat não apenas constroem satélites, como também constroem narrativas públicas sobre soberania tecnológica, responsabilidade ambiental e educação científica transformadora.

4 METODOLOGIA

A metodologia adotada neste trabalho estruturou-se em torno da caracterização do subsistema de comunicação do PdQSat, seguida da aplicação prática e comparativa de duas abordagens de análise de risco: a FTA e a STPA. Ambas as metodologias foram aplicadas de forma independente sobre o mesmo sistema de interesse, permitindo a comparação direta dos riscos identificados, das abordagens analíticas e das respectivas contribuições para a segurança do sistema.

A partir das análises realizadas, foi conduzida uma avaliação crítica da complementaridade entre os métodos, com base em conceitos da Engenharia de Sistemas conforme definidos em (INCOSE, 2023). Essa análise de sinergia buscou compreender como a integração entre FTA e STPA pode fortalecer práticas de engenharia orientada a perdas e ampliar a eficácia da análise de riscos ao longo do ciclo de vida do sistema.

O processo metodológico incluiu desde a pesquisa bibliográfica inicial até a proposição de diretrizes integradas de análise de risco, alinhando os objetivos acadêmicos com as necessidades práticas do projeto PdQSat. A seguir, detalham-se as principais etapas conduzidas:

4.1 Principais Atividades e Métodos

1. **Fundamentação Teórica:** Foi realizada uma pesquisa bibliográfica aprofundada sobre metodologias de análise de risco aplicáveis a sistemas críticos, com ênfase na FTA e STPA. Essa etapa buscou levantar fundamentos conceituais, limitações e casos documentados de aplicação no setor aeroespacial, especialmente em CubeSats. Diretrizes como as de Vesely *et al.* (2002), trabalhos como o de Leveson e Thomas (2018) e Elizebeth *et al.* (2023) foram utilizados como referência.

2. **Caracterização do Sistema de Interesse:** A caracterização técnica do subsistema de comunicação do PdQSat foi realizada com base em documentação interna do projeto, incluindo a decomposição funcional L0–L5 conforme descrito por Arruda (2025, cap. 4). Foram identificadas as funções críticas, os principais componentes envolvidos e suas interfaces, com foco na compreensão dos fluxos de controle e de dados relevantes para a análise de segurança.

3. **Aplicação das Metodologias FTA e STPA:** Ambas as metodologias foram aplicadas de forma prática e independente sobre o sistema de interesse:

    - A FTA foi conduzida seguindo os passos definidos por Vesely *et al.* (2002), com base em eventos de topo definidos a partir da técnica *Functional Hazard Assessment* (FHA).
    - A STPA foi aplicada conforme as diretrizes de Leveson e Thomas (2018), contem-

plando a identificação de perdas, perigos, restrições de segurança, ações de controle inseguras e cenários de perda.

Cada análise utilizou os mesmos dados funcionais e contextuais para garantir consistência comparativa entre os métodos.

4. **Análise Comparativa e de Resultados:** Os resultados de ambas as abordagens foram comparados em termos de abrangência, profundidade da análise, tipos de riscos identificados e aplicabilidade no contexto do PdQSat. A análise incluiu comentários sobre pontos fortes e fracos de cada método, destacando situações em que suas limitações se tornam evidentes.

5. **Análise de Sinergia sob a Ótica da Engenharia de Sistemas:** Foi conduzida uma análise de sinergia entre FTA e STPA com base nos domínios da engenharia de sistemas conforme estabelecidos pelo INCOSE (2023). A análise abordou aspectos como a contribuição para a definição de requisitos, arquitetura do sistema, verificação e validação (V&V), integração homem-sistema (*Human Systems Integration* (HSI)), aplicabilidade ao longo do ciclo de vida, e suporte à engenharia orientada a perdas (*Loss-Driven Systems Engineering* (LDSE)).

6. **Documentação e Consolidação:** Todo o processo metodológico, incluindo artefatos gerados (árvores de falha, tabelas de UCAs, estrutura de controle, etc.), foi documentado de forma sistemática nesta monografia, permitindo rastreabilidade e reprodutibilidade da abordagem. A metodologia contribui assim para fins acadêmicos e para futuras atividades de desenvolvimento no projeto PdQSat.

4.2 Metodologia para FTA

Esta seção descreve a metodologia utilizada para realizar a FTA para o Sistema de Interesse. A condução desta FTA seguirá as etapas preconizadas por Vesely *et al.* (2002), adaptadas ao contexto deste trabalho.

4.2.1 Etapas Fundamentais da FTA

Segundo Vesely *et al.* (2002), para uma FTA de sucesso, as etapas ilustradas na Figura 1 devem ser consideradas.

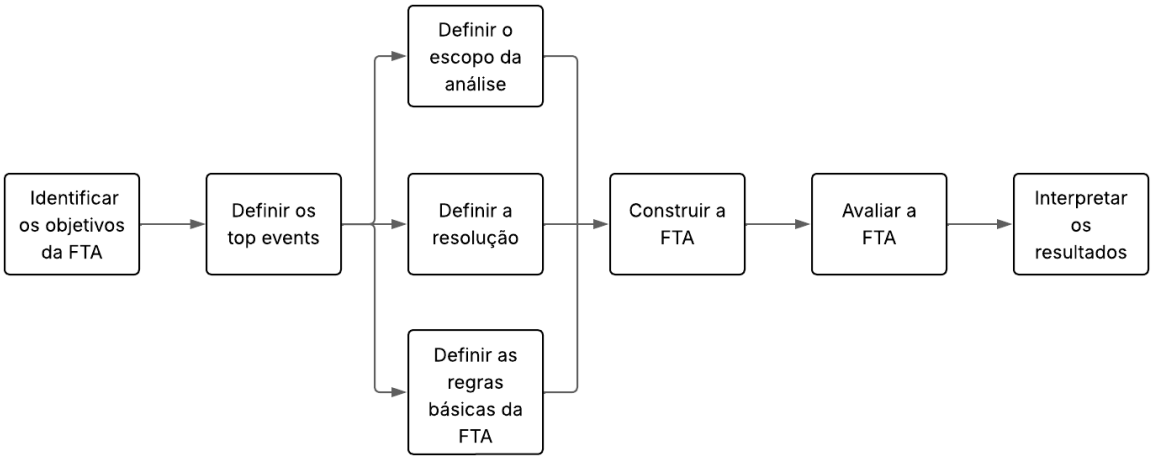


Figura 1: Passos para a árvore de análise de falhas. Fonte: Adaptado de Vesely *et al.* (2002)

Etapa 1: Identificação dos Objetivos da FTA

O primeiro passo é definir o objetivo. Apesar de parecer óbvio, é fundamental. Muitas análises são feitas sem um objetivo bem delimitado e, consequentemente, deixam de agregar valor ao projeto, pois seus resultados não contribuem para as análises dos tomadores de decisão.

Para este trabalho, como as funções do sistema já foram descritas, o objetivo principal da FTA é identificar e analisar as falhas que resultam em perdas de funções do sistema. Essas falhas, caracterizadas como falhas de missão, serão analisadas para que sua ocorrência possa ser mitigada, visando aumentar a confiabilidade do sistema por consequência.

Etapa 2: Definição dos Eventos de Topo

A definição dos eventos de topo, no escopo deste trabalho, será orientada pelo método FHA (Kritzinger, 2017), compreendendo as seguintes atividades:

1. Inventário de Funções: Todas as funções a nível de subsistema (L4) devem ser elencadas a

partir da decomposição funcional proposta por Arruda (2025). As funções desse nível são ideais para a análise proposta, pois elas já estão suficientemente especificadas em termos de arquitetura, evitando a abstração excessiva a nível de elemento (L3), ou o detalhamento em nível de componente (L5).

2. Negação Sistemática: Para cada função elencada no passo anterior, é necessário definir sua respectiva negação formal, caracterizando assim um cenário de falha. Esse passo é fundamental para estruturar os eventos de topo que orientarão a construção das respectivas árvores de falha. Essas funções negadas já podem ser nomeadas como falha, pois representam a incapacidade do sistema em atender um ou mais requisitos funcionais.

3. Classificação de Severidade: As *Failure Conditions* resultantes, que são situações indesejadas que resultam da falha de uma função do sistema, foram categorizadas com base na escala de severidade adaptada do Department of Defense (2012), da SAE International (1996) e da International Electrotechnical Commission (2018). As categorias consideradas para este trabalho foram: *Negligible*, *Marginal*, *Critical* e *Catastrophic*.

4. Seleção dos Eventos de Topo: Com a classificação de todas as funções negadas na atividade 2., selecionou-se os eventos de topo mais representativos com base na severidade e na criticidade de eventos, servindo como ponto de partida para a construção das árvores de falha.

Etapa 3: Definição do Escopo da Análise

Após a definição dos eventos de topo, e em preparação para a construção da árvore, define-se o escopo da FTA. Este passo estabelece quais falhas e fatores serão incluídos ou excluídos da análise. O escopo também deve especificar a versão do projeto e o período histórico considerados, bem como as condições de contorno, que incluem os estados iniciais dos componentes e os insumos assumidos. Assim, a FTA representa um recorte específico do sistema, correspondente a uma determinada configuração.

Etapa 4: Definição da Resolução e das Regras Básicas

Paralelamente à definição do escopo, procede-se com:

1. Definição da Resolução da Análise: Define-se a resolução da FTA, ou seja, o nível de detalhamento até o qual as causas de falha do evento de topo serão desenvolvidas. A resolução pode variar conforme o tipo de falha: falhas funcionais, como falha de operação, são geralmente resolvidas até os principais componentes do sistema; já falhas ambientais exigem modelagem detalhada das causas físicas envolvidas. O nível de detalhamento adotado deve considerar a necessidade de apoiar os tomadores de decisão. Detalhamentos excessivos, além do necessário para a análise de risco, geralmente são evitados.

2. Definição das Regras Básicas (*Ground Rules*): Devem ser definidas as regras básicas para a elaboração da FTA, incluindo os procedimentos e a nomenclatura utilizada na nomeação dos eventos e portas lógicas, de modo a garantir clareza na representação. Também devem ser estabelecidas as regras de modelagem, que orientam como modelar falhas específicas, como falhas de componentes e falhas por causas comuns. Essas regras são essenciais para assegurar a consistência entre diferentes FTAs.

Etapa 5: Construção da Árvore de Falhas (FT)

O passo seguinte às definições prévias é a construção da FTA. A árvore é construída a partir de um evento de topo até os eventos básicos, descendo pelos nós, que descrevem causas que tornam o evento de topo possível. Cada causa vira uma nova caixa de evento; as relações lógicas entre os eventos são representadas por portas lógicas (*gates*). Como E (AND) e OU (OR), que descrevem a combinação de eventos e símbolos de transferência indicam a continuação da árvore em outro local, conforme descritos na Figura 2.

Figura 2: Portas e símbolos de transferência. Fonte: Adaptado de Vesely *et al.* (2002)

A Figura 3 apresenta os principais símbolos utilizados na construção de Árvores de Falhas. Esses símbolos são fundamentais para garantir clareza e padronização na representação

gráfica. Os eventos primários representam condições básicas.

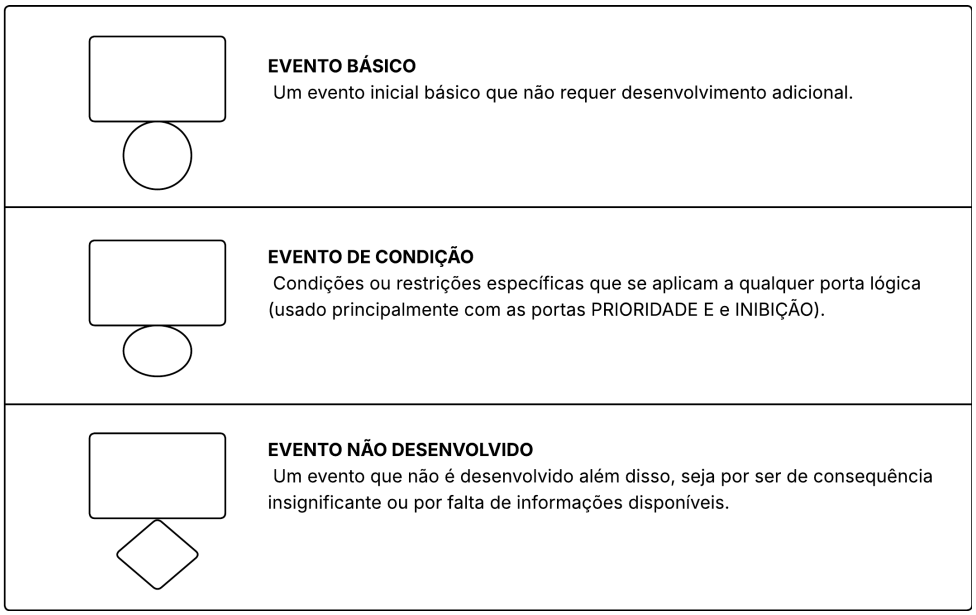


Figura 3: Eventos base presentes na FTA. Fonte: Adaptado de Vesely *et al.* (2002)

O desenvolvimento da árvore continua até que cada ramo culmine em um evento básico (folha), sobre o qual mais decomposições deixam de acrescentar valor à análise. Cada evento deve ser descrito de forma precisa como uma falha, sendo específico com o que falhou e como falhou.

Consideração sobre Falhas Humanas: O desempenho humano é um fator importante na segurança, podendo causar ou mitigar falhas. No entanto, nesta análise de FTA, não consideraremos falhas humanas, pois o sistema analisado é um sistema já implementado, com arquitetura e componentes definidos, e não há planejamento de manutenção ou intervenções complexas previstas. A única interação humana é o envio de comandos e supervisão, ações que, no contexto desta FTA, não configuram riscos significativos ou que justifiquem sua modelagem como falhas. Assim, optou-se por concentrar a FTA exclusivamente nas falhas técnicas e funcionais.

Etapa 6: Avaliação da Árvore de Falhas

Após a construção da árvore de falhas, é realizada a sua avaliação. O principal objetivo desta etapa é verificar se a estrutura está coerente, identificar as relações causais mais importantes e entender como as falhas podem levar ao evento de topo.

Neste trabalho, essa etapa será feita de forma qualitativa, focando na identificação e compreensão dos possíveis cenários de falha e suas consequências. Optou-se por não realizar uma análise quantitativa devido à ausência de dados históricos confiáveis e específicos para o sistema, o que inviabilizaria a atribuição precisa de probabilidades de falha.

Além disso, o foco desta análise é fornecer informações úteis e estruturadas que auxiliem os tomadores de decisão a compreender os principais riscos e definir ações preventivas ou corretivas. Assim, mesmo sem recorrer a cálculos probabilísticos, a avaliação qualitativa já cumpre o papel de destacar pontos críticos e apoiar melhorias no projeto.

Etapa 7: Interpretação dos Resultados

A última etapa consiste em interpretar e apresentar os resultados da análise, transformando a estrutura construída e avaliada em informações claras e úteis para o projeto. Nesta fase, os cenários de falha identificados são discutidos em termos de suas implicações para o sistema, destacando os pontos mais críticos que merecem atenção.

O objetivo é comunicar de forma objetiva os principais achados aos tomadores de decisão, facilitando o entendimento dos riscos e orientando as ações de mitigação ou de melhoria no projeto.

4.3 Metodologia de Análise STPA

Esta seção detalha a metodologia empregada para realizar a análise de segurança do Sistema de Interesse utilizando a técnica STPA. A aplicação seguirá as quatro etapas fundamentais descritas por Leveson e Thomas (2018), adaptadas e detalhadas para o contexto específico deste trabalho e ilustradas na Figura 4.

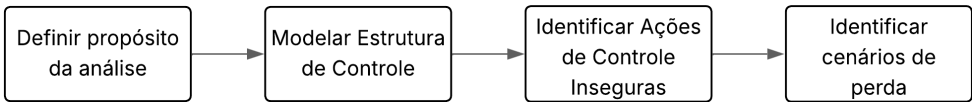


Figura 4: Fluxo das etapas da STPA. Fonte: Adaptado de Leveson e Thomas (2018)

Visando garantir a rastreabilidade e clareza dos artefatos gerados, será adotada uma nomenclatura padronizada para cada item da análise, conforme detalhado na Tabela 1.

Tabela 1: Nomenclatura utilizada na análise STPA.

Elemento	**Abreviação**
Perda	L-#
Perigo	H-#
Ação de Controle Insegura	UCA-#
Cenário de Perda	S-#
Restrição de Segurança	SC-#

4.3.1 Etapas da Análise STPA

A seguir, cada etapa da STPA é detalhada conforme sua aplicação neste trabalho.

Etapa 1: Definição do Propósito da Análise

Conforme Leveson e Thomas (2018), esta etapa será subdividida nas atividades representadas na Figura 5:

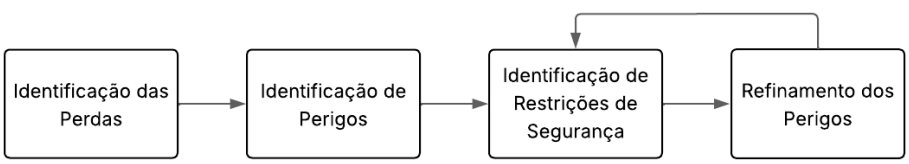


Figura 5: Fluxo da etapa de definição do propósito da análise STPA. Fonte: Adaptado de Leveson e Thomas (2018)

1. Identificação de Perdas (*Losses*): Uma perda é definida como um evento indesejado que resulta em prejuízo a algo de valor para as partes interessadas. Foram identificadas as perdas relevantes para o Sistema de Interesse, como, por exemplo, danos a operadores, perda de funcionalidade, danos ao equipamento e impacto ambiental.

2. Identificação de Perigos (*Hazards*): Um perigo é um estado do sistema ou um conjunto de condições que, em um cenário específico, levará a uma perda. Primeiramente foram listados os perigos em nível de sistema, vinculando cada perigo às perdas identificadas anteriormente.

3. Identificação de Restrições de Segurança: Para cada perigo identificado, foram definidas as restrições de segurança. Essas restrições especificam condições ou comportamentos que devem ser satisfeitos para prevenir os perigos ou mitigar suas consequências.

4. Refinamento dos Perigos: Quando necessário, os perigos identificados foram refinados em sub-perigos para facilitar análises mais detalhadas em etapas posteriores.

Etapa 2: Modelagem da Estrutura de Controle

Nesta etapa, será desenvolvida a estrutura de controle hierárquica do Sistema de Interesse. Esta estrutura, esquematizada na Figura 6, é um modelo funcional composto por *loops* de realimentação (*feedback*) que representam as relações de controle e comunicação entre os componentes do sistema. O modelo identificará:

- **Controladores**: Entidades (humanas, *software*, *hardware*) responsáveis por tomar decisões e emitir ações de controle.
- **Processos Controlados**: As partes do sistema cujo comportamento está sendo gerenciado.
- **Ações de Controle**: Comandos ou sinais emitidos pelos controladores para influenciar os processos controlados.
- ***Feedback***: Informações sobre o estado dos processos controlados que são enviadas de volta aos controladores, permitindo-lhes ajustar suas ações.
- **Modelo do Processo**: Representação interna mantida pelo controlador sobre o estado atual do processo controlado, seu comportamento esperado e as condições do ambiente, utilizada para embasar decisões de controle.
- **Algoritmo de Controle**: Lógica implementada no controlador que determina quais ações de controle devem ser emitidas, com base no modelo do processo e nas entradas recebidas. Define o comportamento do sistema em resposta a diferentes condições operacionais.

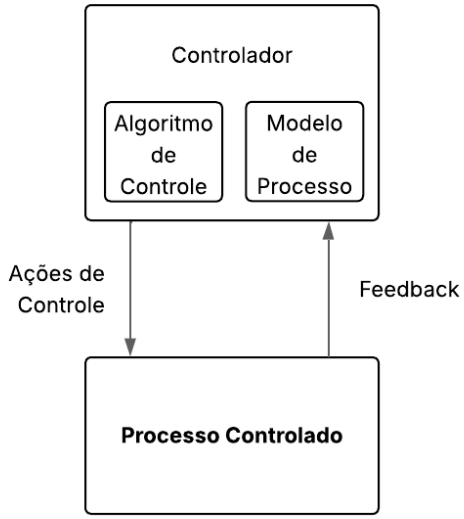


Figura 6: Loop de controle genérico. Fonte: Adaptado de Leveson e Thomas (2018)

A estrutura de controle será desenvolvida com base na documentação técnica do Sistema de Interesse, diagramas existentes e, se necessário, entrevistas com *stakeholders*. A cada controlador identificado na estrutura serão atribuídas responsabilidades relacionadas às restrições de segurança em nível de sistema definidas na Etapa 1. Essas responsabilidades ajudarão a definir as ações de controle e o *feedback* necessário.

Etapa 3: Identificação de Ações de Controle Inseguras

Com a estrutura de controle modelada, cada ação de controle identificada será analisada para determinar como ela poderia se tornar uma UCA. Uma UCA é uma ação de controle que, em um contexto particular e em um cenário de piores condições, leva a um perigo.

Para cada ação de controle, serão investigadas quatro maneiras pelas quais ela pode ser insegura:

1. A não emissão da ação de controle causa um perigo.
2. A emissão da ação de controle causa um perigo (mesmo que emitida corretamente).
3. A ação de controle é emitida muito cedo, muito tarde ou na ordem errada, causando um perigo.
4. A ação de controle, se contínua, é interrompida muito cedo ou aplicada por tempo demais, causando um perigo.

Cada UCA identificada será descrita, incluindo o contexto que a torna insegura, e será vinculada ao perigo correspondente. A partir das UCAs, serão derivadas as Restrições de Controle, que especificam os comportamentos que os controladores devem satisfazer para evitá-las.

Etapa 4: Identificação de Cenários de Perda

A etapa final da STPA consiste em identificar os cenários de perda. Um cenário de perda descreve os fatores causais que podem levar à ocorrência das UCAs identificadas ou explicar por que ações de controle (mesmo que seguras) foram executadas de forma inadequada ou não foram executadas, resultando em perigos.

Serão considerados dois tipos de cenários:

1. Cenários que explicam por que UCAs ocorreram:
    - Falhas no controlador (físicas, de energia, etc.).
    - Algoritmo de controle inadequado (falha na especificação, implementação ou degradação).
    - Modelo do processo inadequado no controlador, devido a:
        - Informação incorreta recebida;
        - Informação correta recebida, mas interpretada incorretamente ou ignorada;
        - Informação não recebida quando necessária (atrasada ou nunca recebida);
        - Informação necessária não existente na estrutura.
    - Análise das causas de *feedback* inadequado, incluindo falhas em sensores ou problemas de transmissão.
2. Cenários que explicam por que ações de controle seguras foram executadas de forma inadequada ou não foram executadas, levando a perigos:
    - Problemas no caminho de controle entre o controlador e o atuador, ou no próprio atuador.
    - Problemas no processo controlado que impedem a ação de controle de ter o efeito desejado distúrbios externos, falhas no processo, interações com outros processos.

Cada cenário de perda será vinculado à UCA correspondente ao perigo resultante.

5 O SISTEMA DE INTERESSE

Para o correto entendimento das análises que serão apresentadas nas seções subsequentes, é indispensável caracterizar o estado atual de desenvolvimento do Segmento Solo do Sistema de Comunicação do PdQSat, que é o Sistema de Interesse. A Figura 7 exibe o diagrama de blocos funcional, destacando as interações entre os subsistemas e seus respectivos componentes, conforme a decomposição arquitetural e as escolhas de componentes documentadas em Arruda (2025).

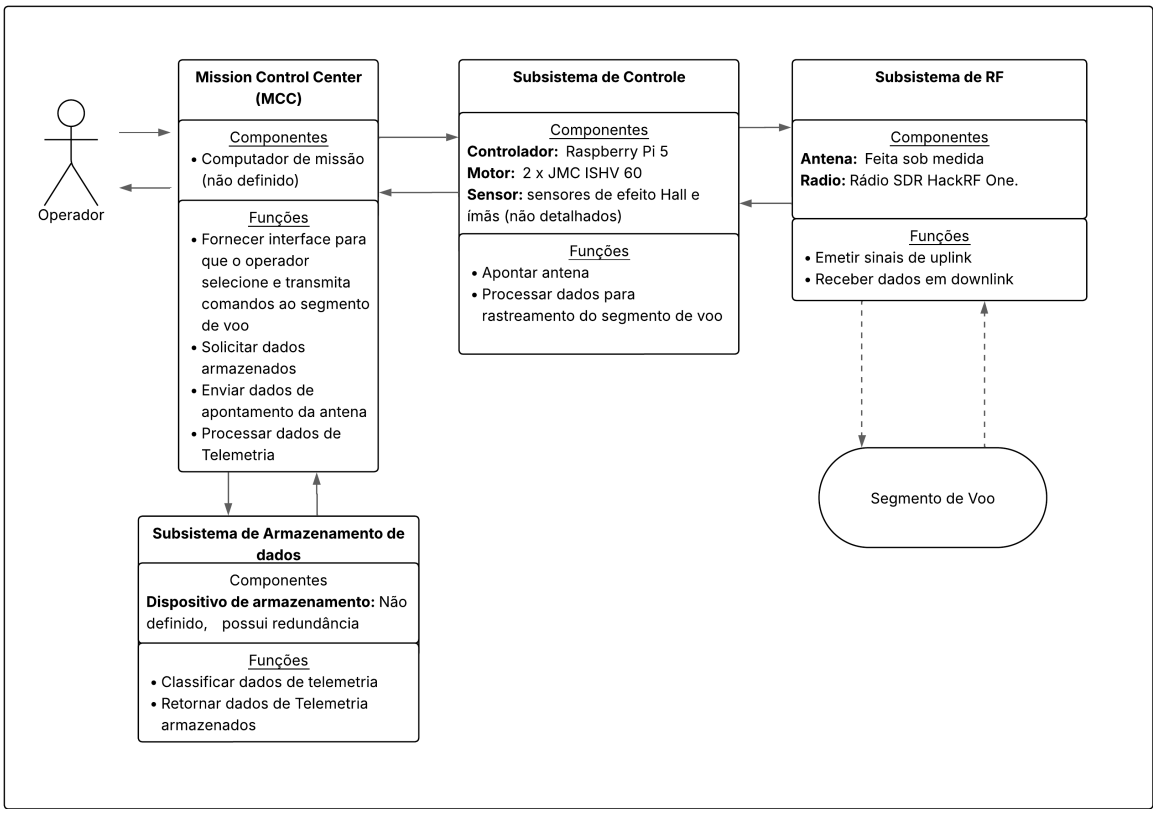


Figura 7: Diagrama de blocos funcional do Segmento Solo do PdQSat.

O operador interage com o *Mission Control Center* (MCC) por meio de um computador (componente não detalhado). O MCC desempenha funções cruciais:

- fornecer interface para que o operador selecione e transmita comandos de *uplink* ao segmento de voo;
- receber dados de *downlink* de telemetria;
- processar os dados de telemetria, extraindo métricas críticas da missão;
- encaminhar os dados processados ao Subsistema de Armazenamento de Dados, que cuida da guarda segura e redundante das informações.

Além disso, o MCC gera os dados de apontamento da antena, calculados a partir da previsão orbital do satélite, e os encaminha ao Subsistema de Controle.

Subsistema de Controle

Implementado em um Raspberry Pi 5, este subsistema executa as seguintes funções:

- calcular em tempo real a posição prevista do satélite para o apontamento preciso da antena;
- enviar comandos ao Subsistema de Radiofrequência;
- receber dados do *Software Defined Radio* (SDR) e repassá-los ao MCC;
- acionar dois motores JMC ISHV 60, um para o movimento em azimute e outro para elevação.

Os motores utilizam *encoders* incrementais, que indicam apenas deslocamentos relativos. Para garantir a referência absoluta após desligamentos, foram adicionados sensores de efeito Hall, possibilitando a recalibração automática da posição inicial.

Subsistema de Armazenamento de Dados

Este subsistema é dedicado exclusivamente ao armazenamento redundante dos dados de telemetria já processados pelo MCC. Embora os dispositivos físicos de armazenamento ainda não tenham sido definidos, para fins desta análise, considera-se a utilização de dispositivos padrão amplamente disponíveis no mercado, como unidades SSD ou HD.

Subsistema de Radiofrequência

É composto por:

- uma antena customizada, otimizada para as necessidades da missão;
- um SDR HackRF One, responsável pela transmissão (*uplink*) de comandos e recepção (*downlink*) de telemetria e demais dados.

A adoção do SDR confere flexibilidade e reconfigurabilidade, permitindo ajustes para diferentes bandas e protocolos de comunicação.

Em resumo, esta caracterização evidencia como os subsistemas do segmento solo do PdQSat se integram para viabilizar a comunicação com o segmento de voo. A compreensão das funções, interações e limitações de cada parte do sistema fundamenta as análises de risco que serão conduzidas nas próximas seções, garantindo que tais avaliações estejam contextualizadas na arquitetura implementada.

6 RESULTADOS FTA

Esta FTA tem como objetivo detectar algumas das combinações de falhas que possam comprometer as capacidades funcionais do Sistema de Interesse, demonstrando a aplicabilidade e os resultados do método.

6.1 Definindo os Eventos de Topo

As funções descritas no nível de subsistema (L4) por Arruda (2025) foram catalogadas, e suas respectivas consequências de falha foram descritas com as classificações de severidade apresentadas na Tabela 2.

Tabela 2: Funções críticas identificadas e as consequências de suas falhas; Nível Subsistema (L4). As categorias de severidade são: CRIT (*Critical*), falha com impacto severo na missão; MARG (*Marginal*), falha com impacto limitado e recuperação possível.

Função	**Consequência da falha**
Rastrear segmento de voo	Antena aponta incorretamente; janela de comunicação perdida (CRIT)
Armazenar dados de telemetria	Dados corrompidos ou não preservados; perda de produto científico (MARG)
Comunicação bidirecional	*Link* interrompido; comandos e dados bloqueados (CRIT)

Priorização para FTA

Neste trabalho, o *Preliminary System Safety Assessment* (PSSA) é conduzido de forma a evitar redundâncias na modelagem, seguindo as diretrizes estabelecidas pela SAE ARP4761 (SAE International, 1996). Para isso, as funções do sistema são agrupadas conforme a similaridade de seus modos de falha, permitindo que cada árvore represente um conjunto funcional coeso e crítico, desta forma definindo os eventos de topo utilizados na análise. Esse agrupamento está detalhado na Tabela 3, que estrutura as funções segundo os critérios adotados para esta análise.

Tabela 3: Eventos de topo para análise de árvores de falhas

Evento de topo	**Severidade**
Perda de Dados Após Recepção	CRIT
Perda da capacidade de comunicação entre segmento solo e segmento voo	CRIT

6.2 Definir o Escopo da Análise e Resolução

Para assegurar que esta análise reflita apenas os riscos pertinentes à missão, o escopo foi restringido aos componentes COTSs que participam diretamente desse fluxo: servomotores de apontamento, Hack RF One, Raspberry Pi 5 e o componente de armazenamento (ainda não especificado); bem como influências ambientais (temperatura, interferências e falha de alimentação). Fatores humanos foram excluídos. É assumido que todos os componentes iniciam em estado nominal, sem degradação prévia. Desta forma, a FTA passa a representar um recorte preciso e rastreável do sistema, alinhado à configuração vigente e às condições operacionais que realmente influenciam o desempenho do Sistema de Interesse.

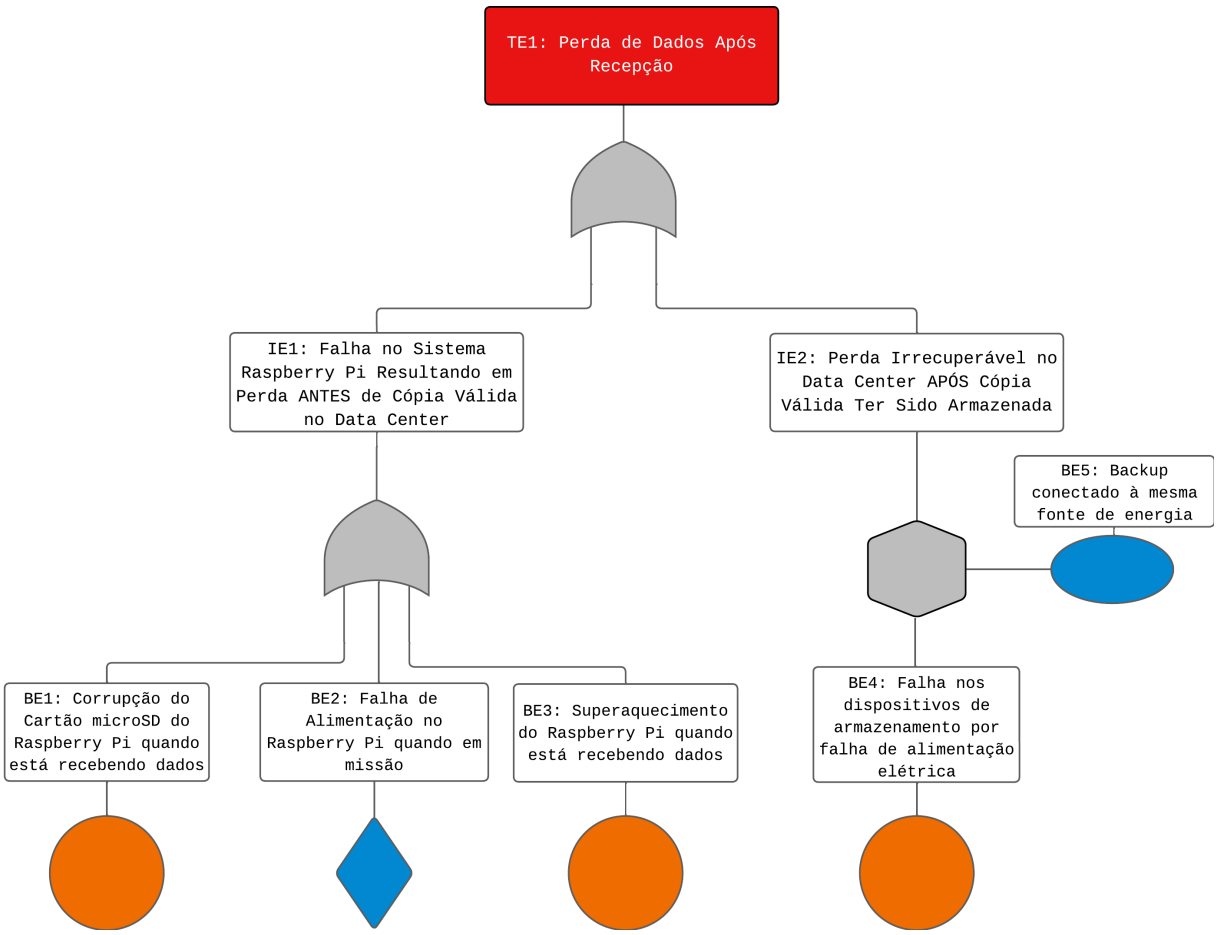
6.3 Definir as Regras Básicas da FTA

A construção das árvores seguiu regras padronizadas para garantir clareza; os eventos foram nomeados com prefixos “TE-” (topo), “IE-” (intermediário) e “BE-” (básico). Usaram-se os símbolos: portas AND, OR, losangos para condições e triângulos para transferências entre figuras. Cada ramo foi desenvolvido até o ponto em que novas divisões não trariam ganho prático, e os eventos básicos incluíram referência a componentes ou eventos possíveis.

6.4 FTA 1: Perda de Dados Após Recepção

A análise para o evento topo TE-1 (Perda de Dados Após Recepção) mostrada na Figura 8 revela duas vias principais e independentes (eventos intermediários IE-1 e IE-2) que conduzem à falha sistêmica. Esta inclui a premissa de que o dispositivo de armazenamento utiliza *backup*.

Figura 8: Árvore de falhas para TE-1



IE-1: Falha no Sistema Raspberry Pi resultando em perda antes de cópia válida no data center

A primeira via para a perda de dados ocorre no sistema Raspberry Pi, antes que uma cópia válida seja consolidada no subsistema de armazenamento. As causas raízes identificadas (BE-1: Corrupção do microSD, BE-2: Falha de alimentação, BE-3: Superaquecimento) são interligadas por uma porta OR, indicando que qualquer uma delas é suficiente para deflagrar a perda de dados nesta fase. O evento BE-2 (Falha de alimentação), representado como um evento não desenvolvido (losango), sugere um ponto que pode merecer investigação, mas que, por possuir uma gama de possibilidades variada (qualidade da fonte, interferências, interrupções de fornecimento de energia), não será decomposto neste trabalho.

IE-2: Perda irrecuperável no data center após cópia válida ter sido armazenada

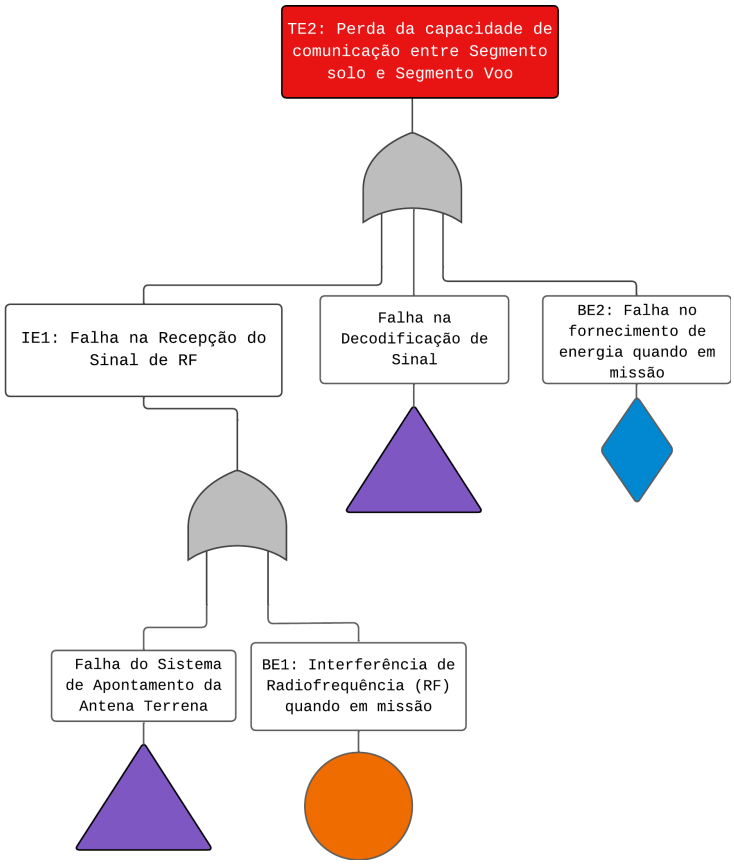
Falhas no subsistema de armazenamento (IE-2): a segunda via crítica aponta para uma perda de dados após sua aparente armazenagem segura. O ponto central desta via é a falha de modo comum na interação entre BE-4 (Falha nos dispositivos de armazenamento por falha

de alimentação elétrica) e BE-5 (*backup* conectado à mesma fonte de energia). Fazendo uso da porta de inibição, a lógica da FTA indica que a falha de alimentação elétrica pode levar a uma perda irrecuperável, precisamente porque a estratégia de *backup* compartilha a mesma vulnerabilidade de alimentação.

6.5 FTA 2: Perda da capacidade de comunicação entre segmento de solo e segmento de voo

A análise para o evento topo TE-2 (Perda da capacidade de comunicação entre segmento solo e segmento voo) está na Figura 9. Esta falha crítica é decomposta em três eventos contribuintes diretos, interligados por uma porta OR: IE-1 (Falha na recepção do sinal de RF), uma transferência de saída Falha na Decodificação de Sinal (detalhada depois) e o evento não desenvolvido BE-2 (Falha no fornecimento de energia quando em missão). A ocorrência de qualquer um desses eventos é suficiente para causar a perda de comunicação.

Figura 9: Árvore de falhas para TE-2

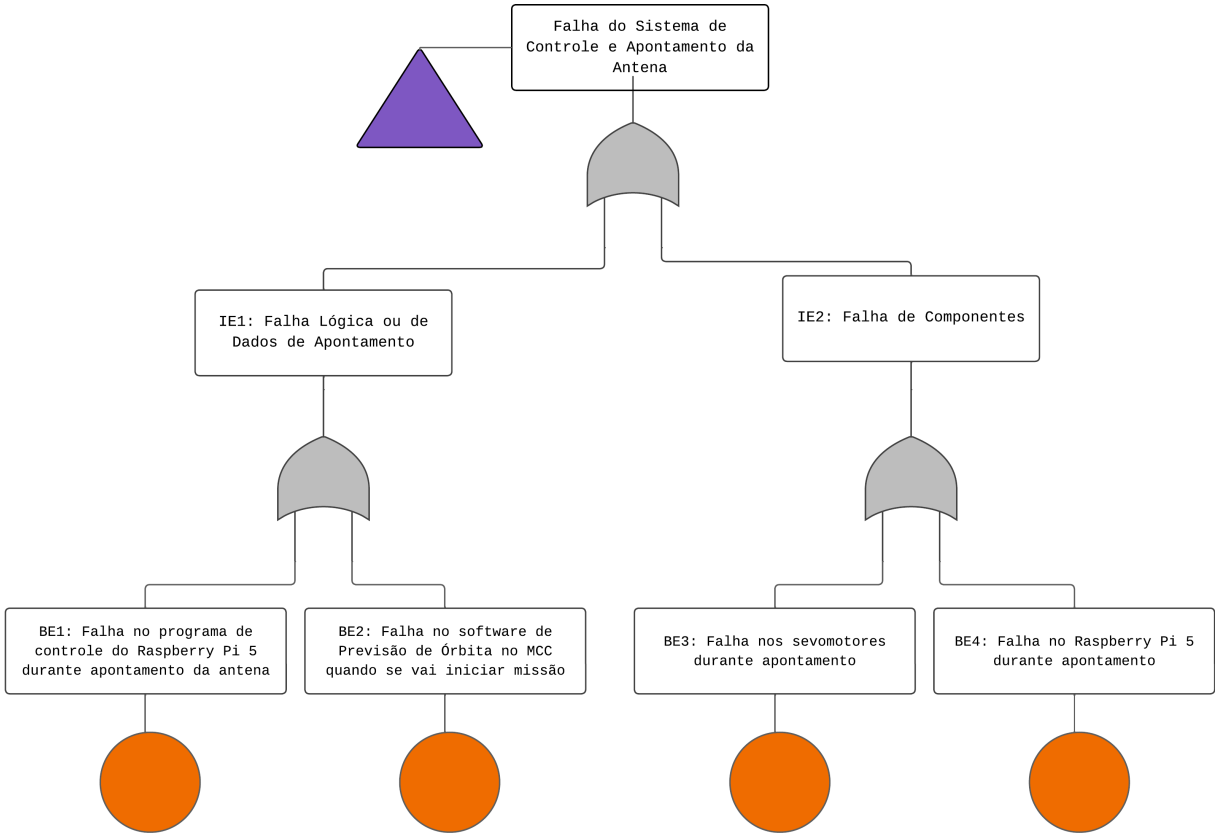


A seguir, detalham-se esses ramos (as figuras correspondentes expandem os eventos intermediários indicados por símbolos de transferência).

1. **IE-1: Falhas na cadeia de recepção de sinal de RF** (ramo IE-1 da Figura 9)

O evento intermediário IE-1 decompõe-se em duas causas principais: (i) o evento básico Interferência de RF quando em missão, possível interferência externa; (ii) o evento intermediário Falha do Sistema de Apontamento da Antena Terrena, cujo detalhamento está na Figura 10.

Figura 10: Falha do Sistema de Controle e Apontamento da Antena, iniciada de um *transfer-out* vindo de TE-2

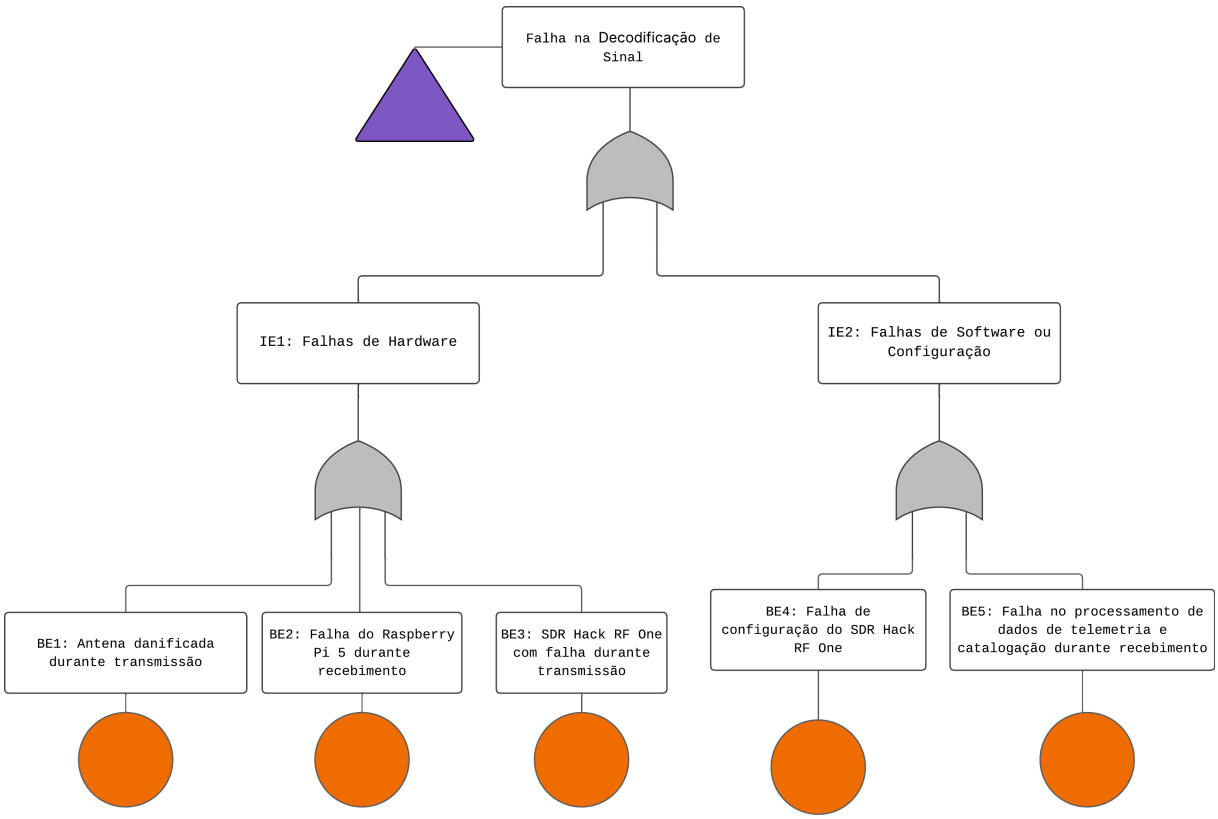


A Figura 10 mostra que a falha pode decorrer de:

- **IE-1: Falhas lógicas ou de dados de apontamento:** falha no programa de controle do Raspberry Pi 5 ou no *software* de previsão de órbita no MCC.
- **IE-2: Falha de componentes:** falha em servomotores ou falha física do Raspberry Pi 5. A interferência de RF (BE-1) também pode degradar o sinal e causar falha de recepção.

2. **Falhas na decodificação do sinal** (transfer-out da Figura 9)

Figura 11: Falha na Decodificação do Sinal, iniciada de um *transfer-out* vindo de TE-2



A Figura 11 revela duas grandes categorias:

- **IE-1: Falhas de hardware:** antena danificada, falha do Raspberry Pi 5 durante recebimento ou SDR Hack RF One com defeito.
- **IE-2: Falhas de software ou configuração:** configuração incorreta do SDR Hack RF One ou falha no processamento de dados de telemetria. A interferência de RF pode, ainda, degradar o sinal.

6.6 Interpretação dos Resultados

A interpretação foca nos *minimal cut sets*, combinações mínimas de falhas básicas que levam ao evento topo. Observou-se que falhas únicas em componentes-chave como o Raspberry Pi, erros de *software* ou configuração e falha de alimentação elétrica podem, isoladamente, levar aos eventos TE-1 ou TE-2. A FTA de TE-1 também evidenciou risco sistêmico em falhas de modo comum no *backup*. Interferência de RF figura entre os fatores ambientais mais críticos.

Principais recomendações:

1. Reforçar robustez e confiabilidade do Raspberry Pi (e.g., micro-SD de alta durabilidade; uso de soluções térmicas).

2. Gerenciar rigorosamente o ciclo de vida de *software* e configurações, por exemplo, testes unitários, testes de integração, testes de ponta a ponta e controle de versão.

3. Monitorar condições ambientais, mitigando interferências e efeitos de variações da temperatura e umidade.

4. Garantir independência da alimentação para sistemas de backup, evitando falhas de modo comum que comprometam a função de contingência em caso de falha de alimentação.

A aplicação destas diretrizes é fundamental para aprimorar a confiabilidade global do sistema.

7 RESULTADOS STPA

De acordo com a metodologia proposta na subseção 4.3, perdas são quaisquer consequências inaceitáveis para os *stakeholders*. A Tabela 4 sintetiza as perdas identificadas neste estudo.

Tabela 4: Perdas identificadas e *stakeholders* afetados

Código	**Descrição**	***Stakeholders* Afetados**
L1	Perda de dados científicos	Equipe Científica
L2	Perda associada à integridade física de operadores	Equipe de Operação
L3	Perda material	Equipe de Projeto
L4	Perda de reputação	Equipe de Projeto / UFMG
L5	Perda de conformidade regulatória	UFMG

Assim, a L1 põe em risco o propósito acadêmico do projeto e compromete o investimento da equipe científica; a L2 reflete a obrigação ética e legal de proteger quem atua no controle e manutenção do sistema; a L3 abrange danos a hardware crítico, impactando cronograma e orçamento da equipe de projeto; a L4 ameaça a confiança institucional na UFMG e na equipe de engenharia envolvida, podendo dificultar futuras colaborações e financiamentos; por fim, a L5 envolve a possibilidade de descumprimento de normas técnicas, legais ou administrativas, o que pode acarretar restrições operacionais e impactos institucionais à universidade.

7.1 Perigos Identificados

Os perigos identificados representam estados críticos que podem levar às perdas previamente definidas. A Tabela 5 apresenta a relação entre perigos e perdas associadas.

Tabela 5: Perigos identificados e perdas associadas

Código	**Descrição**	**Perdas Associadas**
H1	Dados de telemetria não confiáveis	L1, L4
H2	Sinal RF com frequência, potência ou horário não autorizado	L2, L5
H3	Componentes eletrônicos comprometidos	L3
H4	Dados armazenados com falha	L1, L4

A identificação dos perigos apresentados na Tabela 5 permite orientar de forma precisa

as futuras restrições de segurança. A recepção de dados de telemetria não confiáveis (H1) pode comprometer tanto a acurácia dos resultados quanto a credibilidade institucional. A emissão de sinal RF com frequência, potência ou horário não autorizados (H2) representa um risco direto à segurança operacional e ao cumprimento de exigências regulatórias. Componentes eletrônicos comprometidos (H3) podem afetar funções essenciais do sistema, gerando perdas materiais significativas. Dados armazenados com falha (H4) comprometem a integridade das informações científicas e podem afetar a reputação do projeto.

7.2 Restrições de Segurança

As restrições de segurança definidas visam mitigar os perigos identificados e garantir a operação segura do sistema. A Tabela 6 apresenta as principais restrições, orientando o projeto e a operação de acordo com as necessidades de segurança e confiabilidade da missão.

Tabela 6: Restrições de segurança identificadas

Código	**Descrição**
SC1	Os dados de telemetria devem ser confiáveis.
SC2	O sinal RF transmitido deve operar em frequência, potência e horário de funcionamento de acordo com as normas estabelecidas para este tipo de operação.
SC3	Os componentes eletrônicos devem ser utilizados conforme as especificações dos fabricantes e estas devem ser consideradas conforme os requisitos do projeto.
SC4	Os dados armazenados devem ser preservados.

7.3 Estrutura de Controle

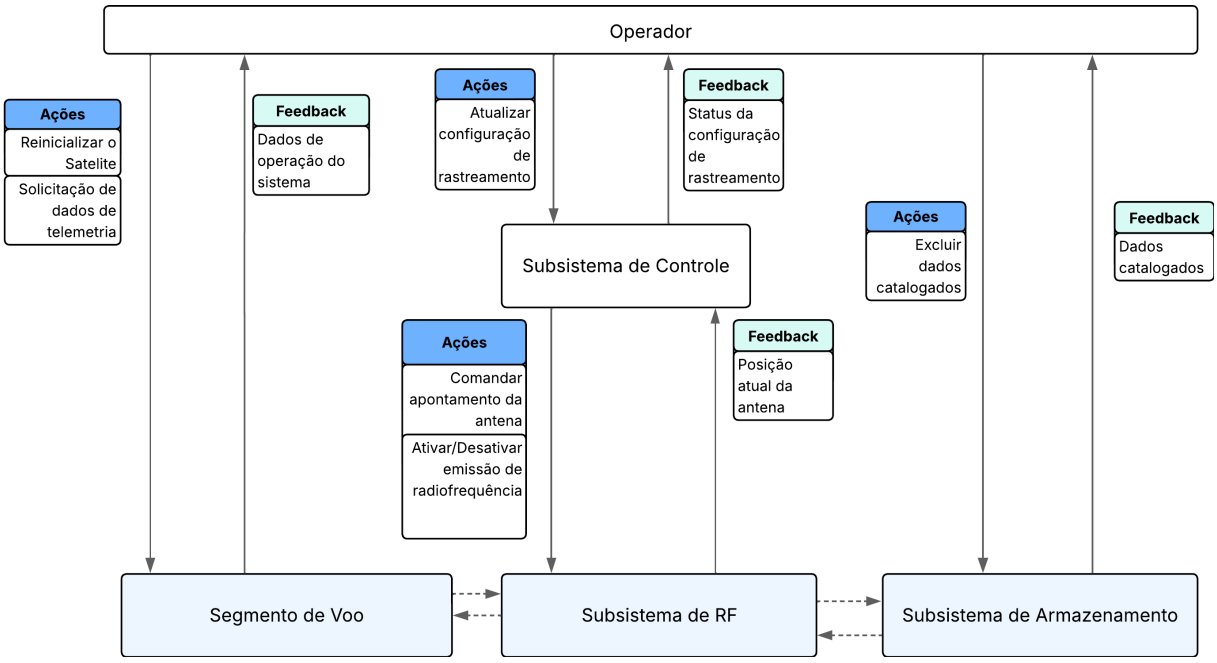


Figura 12: Estrutura de controle para análise STPA.

A Figura 12 ilustra a estrutura de controle hierárquica do Sistema de Interesse. Este diagrama é fundamental para a aplicação da metodologia STPA, pois define os controladores (Operador e Subsistema de Controle), os processos controlados (Segmento de Voo, Subsistema de RF e Subsistema de Armazenamento) e, crucialmente, as ações de controle e os canais de *feedback* entre eles. A Figura 12 ilustra a estrutura de controle hierárquica do Sistema de Interesse. Este diagrama é fundamental para a aplicação da metodologia STPA, pois define os controladores (Operador e Subsistema de Controle), os processos controlados (Segmento de Voo, Subsistema de RF e Subsistema de Armazenamento) e, crucialmente, as ações de controle e os canais de *feedback* entre eles.A Figura 12 ilustra a estrutura de controle hierárquica do Sistema de Interesse. Este diagrama é fundamental para a aplicação da metodologia STPA, pois define os controladores (Operador e Subsistema de Controle), os processos controlados (Segmento de Voo, Subsistema de RF e Subsistema de Armazenamento) e, crucialmente, as ações de controle e os canais de *feedback* entre eles. A Figura 12 ilustra a estrutura de controle hierárquica do Sistema de Interesse. Este diagrama é fundamental para a aplicação da metodologia STPA, pois define os controladores (Operador e Subsistema de Controle), os processos controlados (Segmento de Voo, Subsistema de RF e Subsistema de Armazenamento) e, crucialmente, as ações de controle e os canais de *feedback* entre eles.

7.4 Ações de Controle Inseguras e Cenários de Perda

A Tabela 7 apresenta as ações de controle inseguras identificadas, associando cada uma ao tipo de falha, contexto inseguro e aos perigos relacionados.

Tabela 7: Ações de controle inseguras (UCAs) identificadas

UCA	Descrição
UCA-1	Não prover o comando de reinicializar satélite do operador para o segmento de voo é inseguro quando o segmento de voo está em estado de falha recuperável por reinicialização.
UCA-2	Prover tardiamente o comando de solicitação de dados do operador para o segmento de voo é inseguro quando o armazenamento do segmento está cheio, ocasionando perda de dados por sobrescrita.
UCA-3	Não prover atualização da configuração de rastreamento do operador para o subsistema de controle é inseguro quando os parâmetros estão desatualizados e incapazes de prever a posição do segmento de voo.
UCA-4	Não prover o comando de apontamento da antena do subsistema de controle para o subsistema de RF é inseguro quando o satélite está no campo de visão.
UCA-5	Prover o comando de apontamento da antena do subsistema de controle para o subsistema de RF é inseguro quando a antena não está inicialmente em posição zero no início do apontamento.
UCA-6	Ativar emissão de radiofrequência do subsistema de controle para o subsistema de RF é inseguro quando as configurações estão fora das faixas seguras e permitidas.
UCA-7	Não desativar a emissão de radiofrequência do subsistema de controle para o subsistema de RF é inseguro quando as configurações estão fora das faixas seguras e permitidas.
UCA-8	Não prover ação de excluir dados catalogados do operador para o subsistema de armazenamento é inseguro quando o dispositivo de armazenamento está cheio.

Continuação da Tabela 7

UCA	Descrição
UCA-9	Prover comando de exclusão de dados catalogados do operador para o subsistema de armazenamento é inseguro quando os dados possuem valor para a equipe científica.

A Tabela 8 apresenta os cenários causais identificados na análise, cada um vinculado diretamente à respectiva ação de controle insegura previamente definida. Esses cenários descrevem como falhas nos canais de *feedback* ou nos modelos de processo dos controladores podem levar à ocorrência de condições inseguras no sistema.

Tabela 8: Cenários causais identificados e suas ações de controle inseguras associadas

Cenário	Descrição	UCA Associada
S1	*Feedback* de falha faltante do segmento de voo para o controlador faz com que o operador não tenha consciência de uma possível falha e por isso não forneça o comando de reinicialização.	UCA-1
S2	Processo de tomada de decisão do operador mal estabelecido causa com que o operador não tenha clareza do momento em que a solicitação de dados é necessária por conta do armazenamento cheio, resultando no operador provendo tardiamente o comando de solicitação de dados.	UCA-2
S3	Falta de *feedback* sobre o *status* de armazenamento do segmento de voo leva o operador a enviar o comando de solicitação de dados apenas após a sobrescrita dos dados antigos.	UCA-2
S4	Modelo mental impreciso do operador o leva a acreditar que o subsistema de controle consegue fazer o apontamento sem atualizar os parâmetros de rastreamento, resultando em falha no apontamento da antena.	UCA-3
S5	Modelo de processo impreciso do subsistema de controle faz com que ele acredite que o satélite está fora do campo de visão, mesmo quando visível, resultando em ausência de comando de apontamento.	UCA-4

Continuação da Tabela 8

Cenário	**Descrição**	**UCA Associada**
S6	*Feedback* impreciso da posição da antena enviado pelo subsistema de RF ao subsistema de controle faz com que o comando de apontamento seja enviado antes da antena estar em posição zero.	UCA-5
S7	Falta de *feedback* sobre a configuração atual do transmissor de RF leva o subsistema de controle a assumir que o perfil de transmissão está dentro dos limites permitidos, causando emissões indevidas.	UCA-6
S8	Algoritmo de controle do subsistema de controle mal estabelecido causa o subsistema de controle não considerar as faixas de segurança de emissão de RF, resultando no envio de RF fora de faixas permitidas.	UCA-6
S9	Falta de *feedback* do subsistema de RF impede o subsistema de controle de perceber que o transmissor continua operando, resultando em desgaste e emissões fora das faixas seguras.	UCA-7
S10	Falta de *feedback* do subsistema de RF impede o subsistema de controle de perceber que o transmissor está configurado fora das faixas permitidas, resultando em ativação da emissão de RF fora das faixas seguras.	UCA-7
S11	Falta de *feedback* sobre o nível de ocupação da memória leva o operador a continuar acumulando dados até a sobrescrita de informações importantes.	UCA-8
S12	Processo de tomada de decisão do operador mal estabelecido causa com que o operador não tenha clareza sobre a utilização dos dados, o que leva à exclusão de registros ainda relevantes para a equipe científica.	UCA-9

8 INVESTIGAÇÃO DA SINERGIA ENTRE FTA E STPA

A aplicação individual da FTA (Capítulo 6) e da STPA (Capítulo 7) ao subsistema de comunicação do PdQSat forneceu valiosos *insights* sobre os riscos associados. A FTA concentrou–se na identificação de combinações de falhas de componentes e eventos básicos que poderiam levar aos eventos de topo predefinidos, TE-1: Perda de Dados Após Recepção e TE-2: Perda da capacidade de comunicação entre segmento solo e segmento voo. Por outro lado, a STPA identificou perigos sistêmicos, restrições de segurança e Ações de Controle Inseguras que poderiam levar a esses perigos.

Embora ambas as metodologias busquem compreender os riscos associados ao sistema, elas partem de concepções distintas do que constitui uma falha. A FTA adota uma perspectiva clássica, baseada na decomposição de eventos indesejados em causas físicas, funcionais ou humanas, geralmente modeladas como falhas de componentes, erros de operação ou eventos ambientais. Já a STPA, por sua vez, fundamenta-se no modelo de acidentes STAMP (Zhang *et al.*, 2022), que redefine a falha não como uma quebra ou mau funcionamento de componentes, mas como a ocorrência de interações inseguras no contexto de controle. Assim, mesmo sistemas tecnicamente operacionais podem estar sujeitos a perdas se as decisões de controle forem inadequadas ou mal coordenadas. Essa abordagem permite à STPA capturar perigos sistêmicos que a FTA não contempla.

Esta seção discute os resultados da análise da sinergia entre essas duas metodologias, demonstrando como suas forças se complementam e como sua integração proporciona uma compreensão mais abrangente e profunda dos riscos do subsistema de comunicação do PdQSat, alinhando-se aos objetivos desta pesquisa.

8.1 Complementaridade na Identificação e Análise de Riscos

A principal sinergia observada reside na possibilidade de complementariedade através das naturezas distintas dos cenários identificados por cada método que se propõe a cobrir os aspectos de segurança sob diferentes perspectivas.

A **FTA** foi eficaz em identificar como falhas de *hardware* específicas (e.g., corrupção do microSD e falha nos servomotores) e condições ambientais (e.g., interferência de RF) podem propagar-se e combinar-se para causar os eventos de topo. A FTA do TE-1, por exemplo, destacou a vulnerabilidade a falhas de modo comum relacionadas à alimentação elétrica, um *insight* crucial para a confiabilidade do armazenamento de dados. Essa abordagem é fundamental para direcionar esforços de melhoria na confiabilidade de componentes COTS no *design* do projeto.

A **STPA** identificou UCAs que vão além das falhas de componentes. Por exemplo, UCAs relacionadas ao não envio de comandos adequados, controle incorreto da posição da antena ou falhas no *feedback* para o operador, mesmo que os componentes individuais estejam funcionando conforme especificado. Os cenários de perda associados a essas UCAs frequente-

mente envolvem interações entre o operador, o Subsistema de Controle, o Subsistema de RF e o Segmento de Voo. Esses cenários poderiam não ser detalhados por uma FTA tradicional, que tende a se concentrar nas falhas dos componentes que executam o controle, e não necessariamente na lógica ou no *timing* do controle em si.

A combinação dos resultados da FTA e da STPA oferece uma visão de risco mais completa.

Conforme ilustrado na Figura 13, esse intercâmbio bidirecional materializa a complementaridade discutida nesta seção e sustenta o ciclo iterativo de melhoria da segurança.

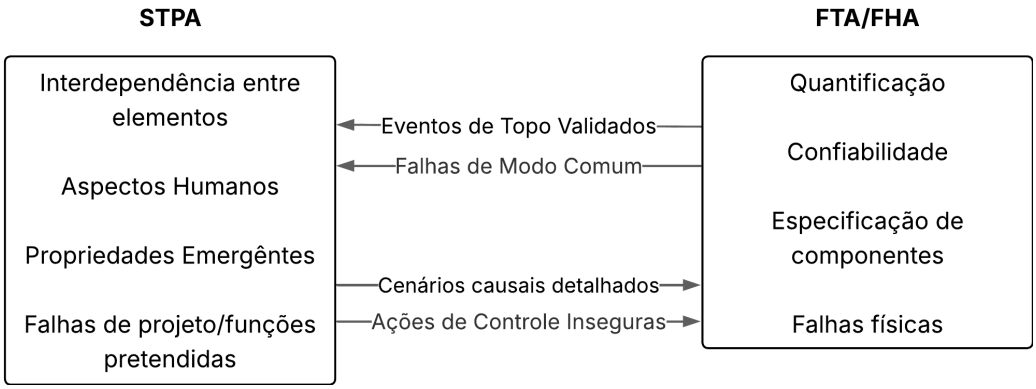


Figura 13: Troca de informações entre STPA e FTA/FHA.

As funções críticas do sistema, identificadas na FHA como ponto de partida para a definição dos eventos de topo da FTA (conforme Tabela 3), atuam como elos fundamentais. A análise dessas funções sob a perspectiva de controle, quem ou o que é responsável por garantir a função, quais ações de controle são necessárias, e quais *feedbacks* são cruciais, são passos essenciais para chegar à estrutura de controle detalhada na STPA (Figura 12). Dessa forma, a análise funcional inicial, mesmo que orientada para a FTA, pode prover insumos valiosos para iniciar a modelagem da estrutura de controle da STPA, evidenciando um fluxo integrado, como ilustrado na Figura 14.

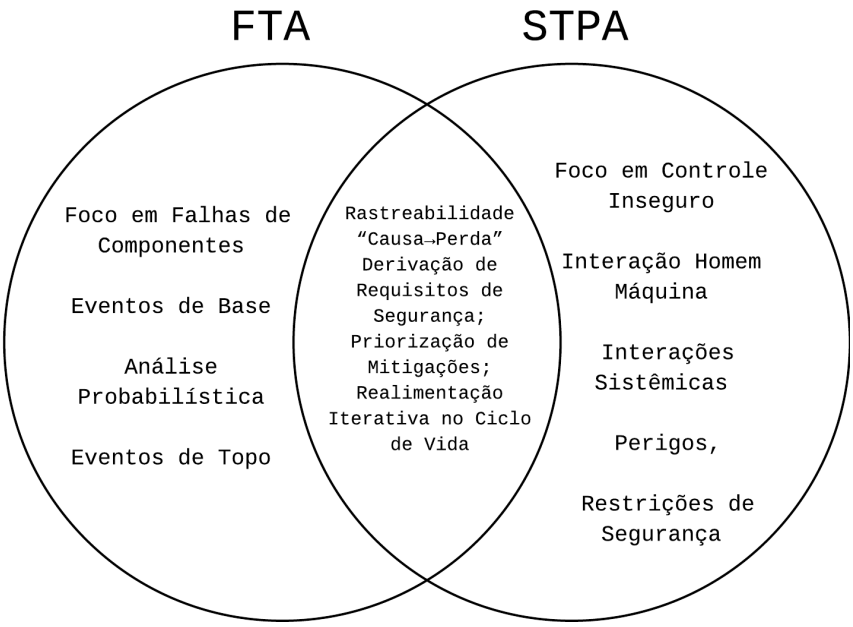


Figura 14: Sobreposição conceitual entre FTA e STPA

A STPA pode identificar a necessidade de um controle de segurança específico. Por exemplo, uma UCA pode ser "Não prover o comando de reinicializar satélite do operador para o segmento de voo é inseguro quando o segmento de voo está com indicativos de falha". A FTA pode então ser usada para analisar a confiabilidade do *hardware* e *software* responsáveis por validar e executar esse comando, ou por fornecer o *feedback* necessário ao operador. Inversamente, uma falha de componente identificada pela FTA, como "Falha no Raspberry Pi 5 durante apontamento da antena", pode estar relacionada a um elemento do *loop* de controle que é responsável por um dos cenários causais para uma UCA identificada na STPA, como "Subsistema de Controle fornece comando de acionamento do motor de forma inadequada, resultando em apontamento incorreto". A STPA ajuda a entender por que essa falha de componente leva a uma perda de controle sistêmico, considerando explicitamente o operador como um controlador e suas potenciais UCAs, o que complementa a modelagem de erro humano mais genérica que poderia ser incluída em uma FTA.

8.2 Orientação para Requisitos e *Design* de Sistema

A complementaridade também se estende à forma como as análises informam os requisitos e estratégias úteis para reduzir riscos através do *design* do sistema.

FTA: Os resultados da FTA, especialmente os conjuntos de *cutsets*, apontam para componentes e combinações de falhas que são críticos para a confiabilidade. Isso pode levar a requisitos de redundância (como a premissa de *backup* para o dispositivo de armazenamento em TE-1, Figura 8), seleção de componentes com maior confiabilidade ou adição de estratégias de proteção específicas para prevenir a propagação de falhas. As recomendações da FTA

focam em reforçar a confiabilidade (redução da probabilidade de falha operando no ambiente pré-estabelecido) dos componentes, fonte de alimentação elétrica, *software* e das configurações.

STPA: A STPA inicialmente gera diretamente restrições de segurança (Tabela 6) que se traduzem em requisitos de alto nível para o comportamento seguro dos controladores e do sistema como um todo. Posteriormente, o método mapeia potenciais cenários que causariam perdas; esses, por sua vez, podem ser contrapostos por requisitos e modelados para cenários de teste. Por exemplo, uma restrição de segurança como "Os dados armazenados devem ser preservados" torna-se um requisito de *design* para o *software* no *Raspberry Pi 5*. As UCAs identificadas na Tabela 7 informam o que o sistema não deve fazer, guiando o *design* da lógica de controle.

Sinergia:

- As restrições de segurança da STPA definem o que o sistema deve fazer para ser seguro em termos de controle e interdependência entre as partes, enquanto a FTA analisa a confiabilidade da arquitetura e dos componentes escolhidos para implementar essas restrições.
- Se a STPA identificar a necessidade de um *feedback* preciso ao operador para evitar uma UCA, a FTA pode analisar os modos de falha dos sensores e interfaces que fornecem esse *feedback*.
- No contexto do PdQSat, a STPA pode levar a requisitos para a interface da controladora ou para a lógica de processamento de telemetria, enquanto a FTA analisa as falhas de *hardware* e *software* que poderiam impedir o cumprimento desses requisitos.

8.3 Contribuições para Verificação e Validação

As duas metodologias, juntas, enriquecem o processo de V&V. As árvores de falhas e os conjuntos de corte mínimos podem ser usados para derivar casos de teste focados na verificação da confiabilidade de componentes específicos ou combinações de falhas. Testes podem ser projetados para simular essas falhas e verificar se o sistema se comporta conforme o esperado (e.g., se um *backup* de armazenamento é ativado).

Os cenários de perda identificados pela STPA (Tópico 7.4) podem ser usados para desenvolver casos de teste de validação que exploram interações complexas e comportamentos emergentes, especialmente aqueles envolvendo *software* e a interface homem-máquina. Para o PdQSat, isso envolve testar o comportamento do sistema em resposta a sequências de comandos do operador ou a condições de *feedback* anormais, não necessariamente ligadas a uma falha de *hardware*.

Sinergia:

- A STPA revela cenários de teste para validar a segurança da lógica de controle e das interações homem-sistema que a FTA, por si só, não identificaria.
- A FTA fornece combinações específicas de falha de *hardware* e *software* para verificar e validar as decisões de projeto relacionados à mitigação de riscos do projeto.
- A combinação de ambas assegura uma cobertura de V&V mais ampla, abordando tanto a "construção correta do sistema" (verificação contra falhas específicas) quanto a "construção do sistema correto" (validação da aderência aos requisitos e da qualidade do projeto).

8.4 Aplicabilidade ao Longo do Ciclo de Vida e Melhoria Contínua

A STPA, por não exigir um *design* detalhado de componentes, pode ser aplicada mais cedo no ciclo de vida para informar a arquitetura e os requisitos de segurança de alto nível. A FTA geralmente requer um conhecimento mais detalhado do *design* do projeto e suas interconexões, sendo mais eficaz em fases posteriores para analisar a confiabilidade do *design* escolhido. Conforme discutido em INCOSE (2023), diferentes estágios do ciclo de vida apresentam oportunidades distintas para a aplicação dessas técnicas.

Um exemplo clássico de modelo sequencial é o **V-Model**, descrito em INCOSE (2023).

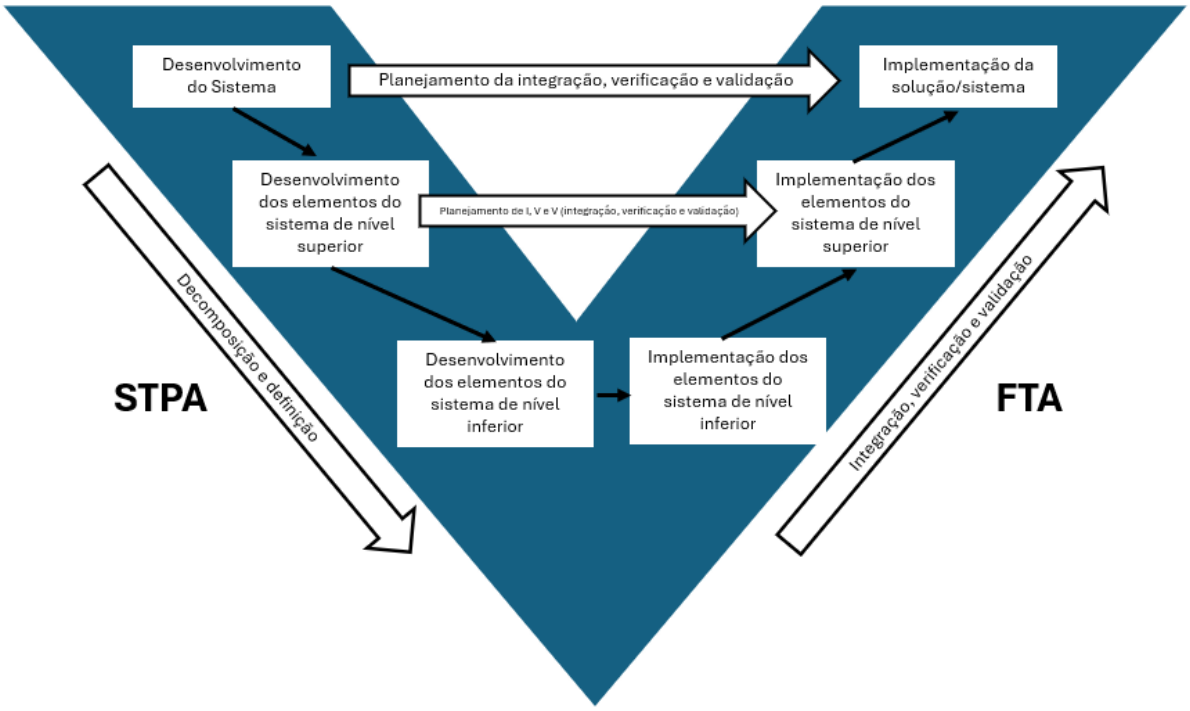


Figura 15: Papel relativo da FTA e da STPA ao longo do V-Model.

A Figura 15 posiciona cada metodologia ao longo do modelo V, mostrando que a STPA se concentra na decomposição e definição de requisitos, ao passo que a FTA fortalece as fases de integração, verificação e validação.

Neste modelo:

- A **STPA** encontra grande aplicabilidade no lado esquerdo do "V", durante as fases de definição de conceito, requisitos e arquitetura, ajudando a embutir a segurança desde o início e a definir restrições de controle para os níveis subsequentes de *design*.
- A **FTA** pode ser empregada tanto no lado esquerdo, para analisar a confiabilidade de conceitos de *design* e arquiteturas preliminares, quanto, e mais intensamente, no lado direito do "V", durante as fases de integração, verificação e validação, o objetivo é analisar falhas de componentes e subsistemas para subsidiar a verificação do atendimento aos requisitos de confiabilidade.

Essa distribuição ilustra como a STPA pode guiar o desenvolvimento seguro do sistema desde as fases iniciais, enquanto a FTA avalia e verifica a robustez do *design* resultante em relação a falhas específicas.

8.5 Implicações para a Engenharia de Sistemas e Recomendações Adicionais

A aplicação combinada de FTA e STPA no subsistema de comunicação do PdQSat demonstra que a integração dessas metodologias oferece uma perspectiva de risco mais holística do que qualquer uma delas isoladamente. A FTA detalha como falhas de componentes podem levar a perdas, enquanto a STPA ilumina como interações complexas e falhas na estrutura de controle podem causar acidentes, mesmo sem falhas de componentes.

Com base nesta análise de sinergia, recomendam-se:

1. **Adotar uma abordagem iterativa e integrada**: iniciar com a STPA nas fases conceituais, usar a FHA como elo para refinar a estrutura de controle, e, conforme o *design* evolui, aplicar a FTA para analisar a confiabilidade dos componentes críticos, iterando entre as duas análises.
2. **Informar testes de V&V de forma abrangente**: Ambas as análises devem ser usadas para guiar o processo de Verificação e Validação. Os cenários da STPA são cruciais para testar a robustez das ações de controle e mitigações, enquanto os conjuntos de corte e eventos básicos da STPA são essenciais para focar os testes na confiabilidade de componentes e na resiliência do sistema a falhas combinadas.
3. **Foco na interface homem-máquina**: usar *insights* da STPA para refinar a interface e procedimentos operacionais; priorizar, com apoio da FTA, a confiabilidade dos sistemas auxiliares que dão suporte direto à operação do usuário.

4. **Gerenciamento de riscos de componentes COTS**: a FTA é utilizada para avaliar falhas conhecidas desses componentes; já a STPA permite analisar como suas limitações de desempenho podem contribuir para as UCAs.

5. **Documentação integrada de riscos**: manter registro consolidado, estruturado, e integrando falhas de componentes (FTA), UCAs (STPA), perigos e perdas de alto nível.

Ao integrar as perspectivas da FTA e da STPA, a equipe do PdQSat alcança uma compreensão mais profunda e multifacetada dos riscos, promovendo um subsistema de comunicação mais seguro e confiável e contribuindo para o sucesso geral da missão de demonstração tecnológica. Adicionalmente, a aplicação das análises ilustradas neste trabalho podem ser adaptadas para outros subsistemas do PdQSat, contribuindo para o sucesso geral da missão.

9 CONCLUSÃO

Este trabalho de conclusão de curso se propôs a investigar sob a ótica da Engenharia de Sistemas, a complementariedade de duas ferramentas de análise de risco no ciclo de vida do subsistema de comunicação do CubeSat PdQSat, um projeto de relevância para a capacitação tecnológica e formação acadêmica na UFMG. A motivação central foi a análise de duas ferramentas que, quando juntas, oferecem uma cobertura robusta ao ciclo de vida do sistema de interesse. Para alcançar tal finalidade, o objetivo principal foi aplicar as duas metodologias, FTA e STPA, a fim de explorar suas complementaridades e a sinergia resultante sob a ótica da Engenharia de Sistemas.

A metodologia adotada partiu da caracterização detalhada do subsistema de comunicação do PdQSat, seguida pela aplicação independente das duas técnicas de análise de risco. A FTA foi conduzida com base na abordagem dedutiva, partindo de eventos de topo indesejados para identificar as combinações de falhas de componentes e eventos básicos que poderiam causá-los. Em paralelo, a STPA foi aplicada com sua abordagem sistêmica, focada na identificação de perigos emergentes de interações de controle inseguras, modelando a estrutura de controle hierárquica e analisando UCAs e seus cenários causais. Por fim, foi realizada uma análise comparativa e de sinergia, avaliando como a integração dos métodos fortalece a identificação de riscos ao longo do ciclo de vida do sistema, conforme preconizado pelo *International Council on Systems Engineering* (INCOSE).

Os resultados demonstraram que a integração da FTA e da STPA proporciona uma visão de risco mais holística e robusta do que cada técnica isoladamente. A análise FTA foi fundamental para identificar vulnerabilidades associadas a falhas de *hardware* e eventos ambientais, como a corrupção do micro-SD do Raspberry Pi e a instabilidade na alimentação, gerando recomendações diretas para o aumento da robustez e redundância de componentes COTS. Por sua vez, a STPA revelou uma classe distinta de riscos, não diretamente ligados a falhas de componentes, mas a deficiências na estrutura de controle, como *feedback* inadequado ao operador, modelos de processo imprecisos e a emissão de radiofrequência fora de parâmetros seguros. Esses cenários, como a falha em atualizar parâmetros de rastreamento (UCA-3) ou a falta de *feedback* sobre o status de armazenamento (S2), dificilmente seriam capturados por uma FTA tradicional. Juntos, os resultados compõem um panorama de risco abrangente, onde as vulnerabilidades de componentes são contextualizadas dentro das falhas de controle sistêmico, oferecendo uma defesa em profundidade contra a perda da missão.

A análise de sinergia evidenciou a complementaridade entre as abordagens, onde as restrições de segurança identificadas pela STPA definem o que o sistema precisa fazer para ser seguro, enquanto a FTA analisa a confiabilidade de como essas restrições são implementadas no *hardware* e *software*. Ficou claro que a STPA é mais eficaz nas fases iniciais do ciclo de vida do sistema, pois pode ser aplicada mesmo com uma arquitetura pouco detalhada para derivar requisitos e restrições de segurança que guiam o projeto. Em contrapartida, a FTA se destaca nas

fases posteriores, especialmente na verificação e validação, onde seus *minimal cut sets* podem ser usados para gerar casos de teste focados na resiliência do sistema a falhas específicas de componentes e suas combinações.

As principais contribuições deste trabalho são, portanto, multifacetadas. Primeiramente, oferece ao projeto PdQSat uma análise de risco detalhada e acionável, com recomendações específicas para mitigar falhas de *hardware* e deficiências sistêmicas no subsistema de comunicação. Em segundo lugar, demonstra de forma prática e documentada como a integração entre FTA e STPA pode ser aplicada em um projeto acadêmico de CubeSat, servindo como um guia metodológico para futuras análises. Por fim, contribui para a área de Engenharia de Sistemas ao explorar a sinergia entre uma técnica tradicional e uma moderna de análise de risco, reforçando a importância de uma abordagem complementar para lidar com a complexidade dos sistemas atuais, alinhando a robustez de componentes com a segurança das interações de controle.

9.1 Trabalhos Futuros

Apesar dos avanços apresentados, este trabalho possui limitações inerentes que abrem espaço para aprofundamentos futuros. Primeiramente, a FTA foi conduzida de forma qualitativa, limitando-se à identificação de cenários críticos sem a estimativa probabilística dos eventos. A ausência de dados confiáveis sobre taxas de falha dos componentes utilizados (em especial os COTS) inviabilizou a modelagem quantitativa. Trabalhos futuros podem buscar essa quantificação por meio de testes de bancada, análise de dados de missões similares ou simulações baseadas em confiabilidade de componentes.

No que diz respeito à STPA, a análise centrou-se nos controladores principais, operadores e subsistemas diretamente ligados à comunicação. Uma possível ampliação seria integrar o lado embarcado do satélite à estrutura de controle, permitindo uma análise ainda mais completa das interações causais, especialmente em cenários onde falhas do subsistema de voo impactam o solo.

Por fim, recomenda-se a aplicação dessa abordagem combinada a outros subsistemas do PdQSat, como o de energia, para avaliar a consistência da sinergia metodológica em diferentes domínios funcionais. A repetição da metodologia em novos contextos pode fortalecer a proposta de integração e contribuir para a consolidação de uma prática mais robusta de análise de risco em pequenos satélites.

REFERÊNCIAS

ARRUDA, D. Andrade de. Trabalho de Conclusão de Curso, *Análise de Segurança no Subsistema de Comunicação do PdQSat: Aplicação da Metodologia STPA*. Belo Horizonte, Brasil: [s.n.], 2025. Orientadora: Profa. Dra. Maria Cecília Pereira de Faria.

BERNARDES, P. v. T. *Gestão da Qualidade em Nanossatélites: Análise Histórica de Missões de Nanossatélites e Análise FTA Preliminar do CubeSat Catarina-A1*. Joinville: [s.n.], 2023. Trabalho de Conclusão de Curso. Curso de Engenharia Aeroespacial, Centro Tecnológico de Joinville.

BOUWMEESTER, J.; MENICUCCI, A.; GILL, E. Improving cubesat reliability: Subsystem redundancy or improved testing? *Reliability Engineering System Safety*, v. 220, p. 108288, 2022. ISSN 0951-8320. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0951832021007584>.

Department of Defense. *MIL-STD-882E: System Safety*. 2012. https://quicksearch.dla.mil/. U.S. Department of Defense Standard Practice.

ELIZEBETH, M. *et al.* Comparison of fta and stpa approaches: A brake-by-wire case study. *SSRN Electronic Journal*, 01 2023.

FAIELLA, G. *et al.* Expanding healthcare failure mode and effect analysis: a composite proactive risk analysis approach. *Reliability Engineering System Safety*, v. 169, 08 2017.

GASTON, K. J. *et al.* Environmental impacts of increasing numbers of artificial space objects. *Frontiers in Ecology and the Environment*, v. 21, n. 6, p. 289–296, 2023. Disponível em: <https://esajournals.onlinelibrary.wiley.com/doi/abs/10.1002/fee.2624>.

INCOSE. *INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*. 5th. ed. Hoboken, NJ: Wiley, 2023. International Council on Systems Engineering.

International Electrotechnical Commission. *IEC 60812:2018 — Failure modes and effects analysis (FMEA and FMECA)*. 2018. https://webstore.iec.ch/publication/65026. IEC Standard, Edition 3.0.

JOHNSTONE, A. *et al.* Cubesat design specification rev. 14 the cubesat program, cal poly slo (no. cp-cds-r14). *Cal Poly, San Luis Obispo, CA*, 2020.

KRITZINGER, D. 3 - functional hazard analysis. In: KRITZINGER, D. (Ed.). *Aircraft System Safety*. Woodhead Publishing, 2017. p. 37–57. ISBN 978-0-08-100889-8. Disponível em: <https://www.sciencedirect.com/science/article/pii/B9780081008898000039>.

LANGER, M. *et al.* A reliability estimation tool for reducing infant mortality in cubesat missions. In: IEEE. *2017 IEEE Aerospace Conference*. [S.l.], 2017. p. 1–9.

LEVESON, N. G. *Engineering a Safer World: Systems Thinking Applied to Safety*. Cambridge, MA: MIT Press, 2012.

LEVESON, N. G.; THOMAS, J. P. *STPA Handbook*. Cambridge, MA, USA, 2018. Versão 1.0. Disponível em: <https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf>.

NOGUEIRA, S. *20 anos após tragédia de Alcântara, Brasil segue longe de ter lançador próprio*. 2023. Disponível em: <https://www1.folha.uol.com.br/ciencia/2023/11/20-anos-apos-tragedia-de-alcantara-brasil-segue-longe-de-ter-lancador-proprio.shtml>.

POTH, A. Product and service quality risks: A survey about evolution and application in different business domains to facilitate quality engineering. *Journal of Software: Evolution and Process*, v. 36, n. 9, p. e2671, 2024. Disponível em: <https://onlinelibrary.wiley.com/doi/abs/10.1002/smr.2671>.

RAUSAND, M. *Reliability of Safety-Critical Systems: Theory and Applications*. Chichester, UK: John Wiley & Sons, 2014. ISBN 978-1-118-11562-3.

SAE International. *ARP4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*. 1996. https://www.sae.org/standards/content/arp4761/. SAE Aerospace Recommended Practice.

VESELY, W. E. *et al. Fault Tree Handbook with Aerospace Applications*. Washington, DC, USA: NASA Office of Safety and Mission Assurance, 2002. NASA Document No. 9821-02. Disponível em: <https://www.nasa.gov/pdf/418878main_Fault_Tree_Handbook_with_Aerospace_Applications.pdf>.

WEGLIAN, J. E.; RILEY, J.; GIBSON, M. Integrating fault tree analysis with system theoretic process analysis. In: IEEE. *2023 Annual reliability and maintainability symposium (RAMS)*. [S.l.], 2023. p. 1–5.

ZERMANE, A. *et al.* Risk assessment of fatal accidents due to work at heights activities using fault tree analysis: Case study in malaysia. *Safety Science*, v. 151, p. 105724, 2022. ISSN 0925-7535. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0925753522000649>.

ZHANG, Y. *et al.* Systems theoretic accident model and process (stamp): A literature review. *Safety Science*, v. 152, p. 105596, 2022. ISSN 0925-7535. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0925753521004367>.