ABORDAGEM DE ANÁLISE DE SEGURANÇA STPA EM PROJETOS DE FOGUETES UNIVERSITÁRIOS

Maria Clara da Silva Oliveira Franco, Maria Clara Vargas Raymundo, Carlos Henrique Netto Lahoz.

Universidade do Vale do Paraíba/Faculdade de Engenharias e Arquitetura FEAU, Avenida Shishima Hifumi, 2911, Urbanova - 12244-000 - São José dos Campos-SP, Brasil
franco.mclra@gmail.com, vargasr.maria@gmail.com, carloslahoz@univap.br

Resumo

Este trabalho apresenta uma proposta de análise de segurança para projetos universitários de foguetes experimentais utilizando a técnica System-Theoretic Process Analysis (STPA). O desenvolvimento aeroespacial acadêmico, exemplificado por equipes como a Bravo Aerospace da Universidade do Vale do Paraíba (UNIVAP), envolve alta complexidade e riscos associados a sistemas propulsivos e às operações de desenvolvimento e lançamento. Metodologias tradicionais de análise de segurança centram-se predominantemente em falhas de componentes e podem apresentar limitações na consideração de interações sistêmicas, software e fatores humanos. A abordagem sugerida sintetiza fases recorrentes do desenvolvimento de projetos universitários de foguetes, integrando a técnica STPA para modelar estruturas de controle e identificar ações de controle inseguras. Espera-se com a aplicação dessa técnica obter um mapeamento proativo de perigos e gerar requisitos operacionais e de projeto mais eficazes. A aplicação da STPA apresenta potencial para apoiar a prevenção de acidentes no solo ou em voo, podendo se consolidar como uma técnica de segurança adequada ao ambiente acadêmico brasileiro.

Palavras-chave: Foguetes universitários. STPA. Segurança de sistemas.

Área do Conhecimento: Engenharia Aeroespacial. Engenharia da Computação.

Introdução

O desenvolvimento de foguetes experimentais por estudantes universitários tem se consolidado no Brasil como uma importante atividade de formação prática e desenvolvimento tecnológico na área aeroespacial. Iniciativas em instituições como o Instituto Tecnológico de Aeronáutica (ITA), a Universidade Federal de Santa Catarina (UFSC) e a Universidade Federal de Minas Gerais (UFMG) desenvolvem projetos de foguetes e participam de competições universitárias nacionais e internacionais. A Agência Espacial Brasileira (AEB) registra a existência de dezenas de equipes distribuídas por universidades brasileiras, dedicadas à construção e ao teste de foguetes e de seus subsistemas, algumas das quais participam de competições e eventos nacionais e internacionais (AEB, 2022). Esses projetos exigem a integração multidisciplinar de conhecimentos de aerodinâmica, propulsão, estruturas, aviônica, telemetria e sistemas de recuperação, proporcionando aos estudantes um ambiente prático de desenvolvimento de sistemas aeroespaciais.

Nesse cenário de crescente fomento tecnológico, destaca-se também a Universidade do Vale do Paraíba (UNIVAP), com a atuação da Bravo Aerospace. A equipe desenvolve atividades relacionadas ao projeto e ao desenvolvimento de foguetes universitários, incluindo trabalhos associados a sistemas propulsivos e ensaios de motores. Projetos dessa natureza podem envolver materiais e sistemas com elevado potencial energético, além de operações de integração, testes e lançamento que demandam critérios sistemáticos de segurança. A consideração desses aspectos é necessária para reduzir a exposição de participantes, espectadores e infraestrutura a condições capazes de resultar em perdas.

No entanto, garantir a segurança de maneira sistemática no ambiente universitário apresenta desafios particulares. A alta rotatividade de membros é uma característica reconhecida das equipes universitárias de foguetes, nas quais o conhecimento técnico é construído ao longo da participação sucessiva de diferentes estudantes, tornando importante sua adequada documentação e transferência entre os integrantes (AEB, 2022). Ademais, metodologias tradicionais de análise de segurança, como a Análise de Modos de Falha e Efeitos (FMEA) e a Análise por Árvore de Falhas (FTA), são

fundamentadas principalmente na identificação de falhas e sequências de eventos. Em sistemas complexos, especialmente aqueles que envolvem software, operadores humanos e múltiplas interações, perdas também podem resultar de interações inseguras entre componentes que individualmente funcionam conforme especificado (Leveson, 2011).

Diante desse contexto técnico e metodológico, o objetivo principal deste trabalho é propor uma estrutura conceitual de análise de segurança para projetos universitários de foguetes experimentais utilizando a técnica System-Theoretic Process Analysis (STPA). Desenvolvida a partir dos trabalhos de Nancy Leveson, professora de Aeronáutica e Astronáutica e de Engenharia de Sistemas no Massachusetts Institute of Technology (MIT), a STPA trata a segurança como um problema de controle do comportamento do sistema, em vez de restringi-la à confiabilidade individual de seus componentes.

Metodologia

A metodologia foi estruturada em duas vertentes complementares. A primeira consistiu na identificação de atividades e marcos recorrentes no desenvolvimento de foguetes em projetos universitários, a partir dos quais foi sintetizado um ciclo de desenvolvimento de referência para esta proposta. A segunda consistiu na proposição da incorporação da STPA a esse ciclo, de modo a integrar a análise de segurança ao processo de desenvolvimento do sistema.

Para a primeira vertente, foram considerados referenciais institucionais de programas e competições universitárias de foguetes. No NASA Student Launch, destinado também a equipes universitárias, o desenvolvimento é conduzido por sucessivas revisões de projeto, incluindo a Revisão Preliminar de Projeto (Preliminary Design Review - PDR), a Revisão Crítica de Projeto (Critical Design Review - CDR), a Revisão de Prontidão para Voo (Flight Readiness Review - FRR) e a Revisão de Prontidão para Lançamento (Launch Readiness Review - LRR), seguidas pelo lançamento e pela Avaliação Pós-Lançamento (Post-Launch Assessment Review - PLAR) (NASA, 2026). A documentação da Latin American Space Challenge (LASC) apresenta, por sua vez, entregáveis e atualizações sucessivas destinados ao acompanhamento progressivo das características técnicas das missões participantes (LASC, 2026). Embora esses referenciais adotem processos e marcos distintos, apresentam atividades recorrentes ao longo do desenvolvimento. A partir dessas convergências, e sem pressupor a existência de um ciclo de vida único e padronizado para foguetes universitários, essas atividades foram sintetizadas nas cinco fases apresentadas na Figura 1.

Figura 1 – Etapas recorrentes no desenvolvimento de foguetes universitários.



Fonte: Elaborado pelos autores com auxílio de IA generativa (2026).

A **Fase A**, definição inicial e requisitos, compreende o estabelecimento dos objetivos da missão e dos principais requisitos e restrições do sistema, como apogeu-alvo, limitações de massa e características gerais da propulsão. A **Fase B**, projeto preliminar e detalhado, abrange o desenvolvimento e o refinamento da solução técnica, incluindo análises aerodinâmicas e de estabilidade, simulações de desempenho, dimensionamento estrutural e definição dos subsistemas do veículo. A **Fase C**, fabricação, integração, testes e verificação, envolve a construção dos componentes, a integração dos subsistemas e a realização de ensaios destinados à verificação do atendimento aos

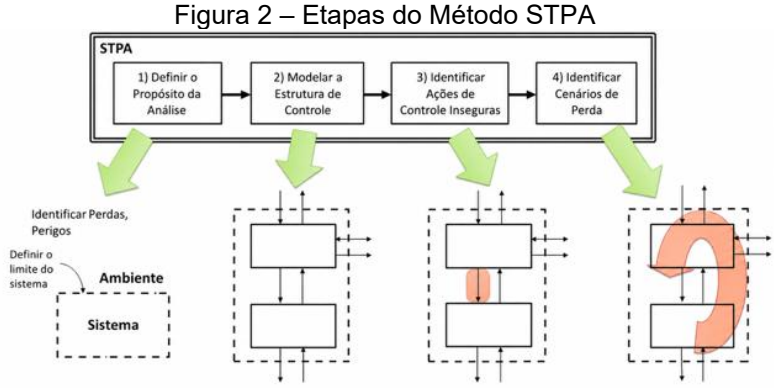
requisitos, incluindo, quando aplicável, ensaios do sistema propulsivo. A **Fase D**, preparação e operações de lançamento, compreende a preparação do veículo e dos sistemas de solo, verificações de prontidão, procedimentos de segurança e operações associadas ao lançamento. Por fim, a **Fase E**, recuperação e avaliação pós-voo, abrange a recuperação do veículo, quando aplicável, a obtenção e análise dos dados de voo e a avaliação do desempenho do sistema após a missão.

Na segunda vertente, apresenta-se a STPA, um método iterativo de análise de perigos fundamentado no modelo sistêmico de causalidade de acidentes STAMP (System-Theoretic Accident Model and Processes), no qual a segurança é tratada como um problema de controle do comportamento do sistema, e não apenas como consequência da confiabilidade individual de seus componentes. A abordagem considera que perdas podem resultar não somente de falhas de componentes, mas também de interações inseguras entre elementos que individualmente funcionam conforme especificado, permitindo incorporar à análise componentes físicos, software, operadores humanos e fatores organizacionais (Leveson; Thomas, 2018).

Essa perspectiva é pertinente ao contexto dos projetos universitários de foguetes, cujo desenvolvimento e operação envolvem a interação entre diferentes subsistemas do veículo, sistemas de solo, procedimentos e operadores ao longo de atividades de projeto, fabricação, testes, preparação, lançamento e recuperação. Além disso, essas atividades podem envolver fontes relevantes de perigo, como sistemas propulsivos e operações de lançamento, demandando a consideração sistemática de condições capazes de conduzir a perdas. A incorporação da STPA desde o desenvolvimento permite identificar perigos e estabelecer restrições de segurança capazes de orientar requisitos, decisões de projeto e procedimentos operacionais ao longo da evolução do sistema (Leveson; Thomas, 2018).

Conforme Leveson e Thomas (2018), a aplicação básica da STPA é estruturada em quatro passos: Definição do Propósito da Análise; Modelagem da Estrutura de Controle; Identificação das Ações de Controle Inseguras; e Identificação dos Cenários de Perda, como representado na Figura 2.

Figura 2 – Etapas do Método STPA



Fonte: Adaptado de Leveson e Thomas (2018).

O Passo 1 consiste na **Definição do Propósito da Análise**. Nessa etapa, são estabelecidas as perdas que se deseja evitar, os perigos associados a essas perdas e as restrições de segurança em nível de sistema. Também são definidos o sistema a ser analisado e sua fronteira, delimitando os elementos e interações considerados na análise. Como exemplo ilustrativo aplicado a uma campanha de lançamento de foguete universitário, uma possível perda seria a ocorrência de lesões ou morte de pessoas, enquanto um perigo associado poderia corresponder à presença de pessoas na área de risco durante uma condição em que o sistema de propulsão possa ser acionado.

O Passo 2 corresponde à **Modelagem da Estrutura de Controle**. Nessa etapa, o sistema é representado por meio das relações funcionais de controle e feedback entre seus componentes. A estrutura é inicialmente constituída em um nível mais abstrato e identifica controladores, processos controlados, ações de controle e feedbacks, podendo ser refinada para explicitar atuadores, sensores, e outros elementos relevantes do sistema. Em uma campanha de lançamento, por exemplo, a estrutura pode representar as relações entre os responsáveis pela autorização e pela execução do lançamento, os elementos do sistema de ignição, o processo de preparação e lançamento do veículo e os feedbacks utilizados para indicar condições de prontidão e segurança.

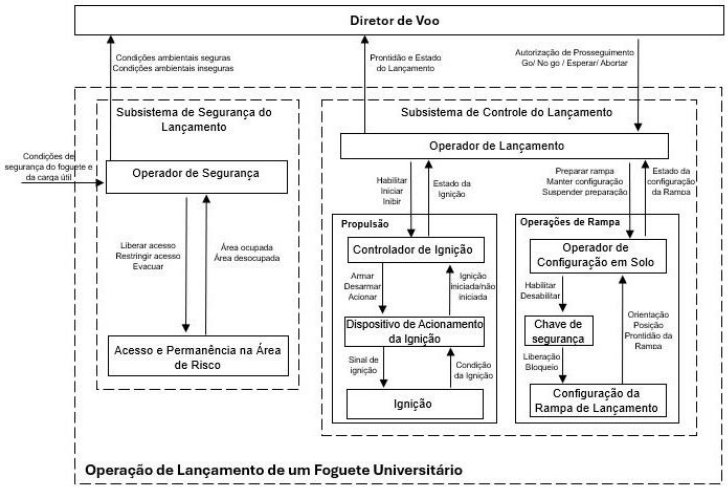
O Passo 3 consiste na **Identificação das Ações de Controle Inseguras** (Unsafe Control Actions - UCAs). Nessa etapa, as ações de controle associadas aos controladores identificados na estrutura são analisadas quanto à possibilidade de conduzirem aos perigos previamente definidos. A identificação das UCAs considera quatro condições gerais: uma ação de controle necessária não é fornecida; uma ação é fornecida quando sua ocorrência é insegura; uma ação é fornecida em momento inadequado, muito cedo, muito tarde ou em sequência incorreta; ou uma ação é aplicada por duração inadequada, sendo interrompida prematuramente ou mantida por tempo excessivo. Como exemplo, a ação de controle de autorizar ou comandar a ignição pode tornar-se insegura caso seja fornecida enquanto uma pessoa ainda se encontre na área de risco associada ao lançamento.

O Passo 4 corresponde à **Identificação dos Cenários de Perda**. Nessa etapa, investigam-se as circunstâncias capazes de produzir as ações de controle inseguras ou de comprometer a execução adequada das ações de controle. A análise considera possíveis inadequações nos processos de controle e feedback, incluindo informações incorretas ou ausentes, inconsistências nos modelos de processo dos controladores, problemas de comunicação, condições ambientais, decisões humanas inadequadas e comportamentos incorretos de componentes ou interfaces. No exemplo da ignição, um cenário de perda poderia envolver a autorização do lançamento com base em uma informação incorreta de que a área de risco se encontra desocupada, decorrente, por exemplo, de falha ou atraso na comunicação entre os responsáveis pela verificação da área e pela autorização da ignição. Esses cenários permitem aprofundar a compreensão dos mecanismos causais capazes de conduzir às perdas identificadas no início da análise.

Para exemplificar a aplicação da STPA no contexto de projetos universitários de foguetes, adotou-se como recorte ilustrativo a campanha de lançamento, etapa em que interagem operadores humanos, sistemas de solo, elementos do veículo e procedimentos operacionais. Em uma estrutura de controle esquemática desse processo, pode ser considerado, em nível superior, um **Diretor de Voo**, responsável por avaliar a prontidão geral para o lançamento e decidir pelo prosseguimento, espera ou aborto da operação. Um **Operador de Segurança** acompanha as condições de segurança da área de risco e do foguete e da carga útil, fornecendo ao **Diretor de Voo** as informações necessárias à decisão. Um Operador de Lançamento coordena a execução operacional da sequência autorizada, articulando as funções de ignição e de configuração em solo. Em níveis inferiores, um **Controlador de Ignição** atua sobre o processo de ignição, enquanto um **Operador de Configuração em Solo** garante a preparação e a manutenção da configuração da rampa de lançamento. No nível de execução, podem ser representados elementos físicos, como **chaves de segurança** e **dispositivos de acionamento**, e o feedback aos controladores pode ocorrer por confirmações visuais, por rádio ou telemetria, indicações de estado, continuidade do circuito e outros sinais de monitoramento disponíveis.

Essa representação, de caráter ilustrativo e não associada à modelagem de uma equipe universitária específica, é apresentada a seguir, na Figura 3.

Figura 3 – Estrutura de Controle Ilustrativa para a Operação de Lançamento de um Foguete Universitário.



Fonte: Os autores

Resultados

Como resultado primordial, objetiva-se a identificação de Ações de Controle Inseguras (UCAs) relacionadas às fases operacionais de montagem, preparação e lançamento de foguetes universitários. Com base nas UCAs identificadas e nos cenários de perda associados, podem ser derivados requisitos e restrições de segurança de projeto e de operação. Por exemplo, a autorização da ignição enquanto a área de risco ainda não estiver confirmada como desocupada pode ser caracterizada como uma UCA, da qual se deriva a restrição de que a ignição somente seja autorizada após a confirmação das condições de segurança da área. A análise dos cenários pode ainda subsidiar recomendações de projeto e decisões de implementação, conforme previsto na aplicação da STPA (Leveson; Thomas, 2018). Como exemplo, uma possível recomendação seria que o sistema de aviônica de solo responsável pela ignição de rampa incorporasse uma chave de segurança mecânica removível, do tipo plug, mantida sob controle do Operador de Rampa durante a preparação, de modo a impedir fisicamente o fechamento do circuito de ignição enquanto as condições necessárias de segurança não estiverem satisfeitas. Adicionalmente, a aplicação do método pode subsidiar a reestruturação e a formalização técnica dos checklists de lançamento, incorporando etapas operacionais e barreiras de segurança relacionadas aos perigos e às ações de controle inseguras identificadas.

Discussão

Os potenciais achados obtidos ao integrar a metodologia STPA ao desenvolvimento de foguetes universitários podem representar uma ampliação significativa da análise proporcionada pelas técnicas tradicionais de engenharia de segurança, como FMEA e FTA. Análises fundamentadas estritamente em falhas ou na confiabilidade de componentes podem não capturar adequadamente riscos decorrentes de software, decisões operacionais e interações entre componentes do sistema, aspectos contemplados pela abordagem sistêmica da STPA (Leveson; Thomas, 2018). Em projetos universitários experimentais, especialmente quando desenvolvidos sob limitações de orçamento e infraestrutura e com componentes manufaturados e testados pelos próprios estudantes em laboratórios acadêmicos, as falhas físicas permanecem uma preocupação importante; entretanto, a análise de segurança também deve considerar falhas de coordenação no controle geral do sistema, decisões operacionais e interfaces organizacionais. A alta rotatividade de alunos que compõem as equipes universitárias representa outro desafio relevante para a continuidade do conhecimento técnico, aspecto reconhecido pela Agência Espacial Brasileira (AEB) no contexto dos projetos nacionais de foguetes. Por meio do mapeamento e da documentação explícita da estrutura de controle, das responsabilidades, das ações de controle, dos perigos e das restrições de segurança, a aplicação da STPA pode contribuir para que o conhecimento operacional crítico deixe de residir exclusivamente em registros informais ou na memória dos integrantes mais experientes da equipe. Essa documentação estruturada pode funcionar como apoio à transferência desse conhecimento e ao treinamento de novos ingressantes. No entanto, deve-se considerar que a STPA demanda uma curva inicial de aprendizagem por parte dos estudantes, que precisam ser instruídos sobre seus fundamentos, conceitos e procedimentos de análise. Esse esforço adicional deve ser considerado em conjunto com os potenciais benefícios da formalização e sistematização das informações de segurança no ambiente universitário.

Conclusão

Conclui-se que a incorporação sistemática da STPA em projetos acadêmicos brasileiros de foguetes experimentais pode constituir um importante mecanismo de apoio à prevenção de acidentes no solo e em voo e ao fortalecimento de uma cultura rigorosa de segurança tecnológica. Sua aplicação às operações de preparação e lançamento pode contribuir para a identificação de ações de controle inseguras, cenários de perda e requisitos de segurança associados, por exemplo, às operações de rampa, ao sistema de ignição, à autorização de lançamento, ao controle de área de risco e à comunicação dos responsáveis pelas etapas críticas da operação.

Além disso, a utilização da STPA no ambiente acadêmico pode proporcionar aos futuros engenheiros aeroespaciais uma formação técnica diferenciada e de alta qualificação, através do contato com uma abordagem de análise voltada a sistemas complexos. Assim, torna-se possível uma aproximação entre sua formação e as práticas de engenharia de segurança empregadas nesse tipo de

sistema. Cabe mencionar também que a Agência Espacial Brasileira (AEB) já promoveu iniciativas como o 1º Workshop de Segurança em Atividades Universitárias de Foguetes Experimentais, realizado em 2021, reforçando a relevância da segurança nesse contexto e fortalecendo a iniciativa aqui apresentada.

Referências

AGÊNCIA ESPACIAL BRASILEIRA (AEB). Foguetes universitários. Brasília, DF: AEB, 2022a. Disponível em: https://www.gov.br/aeb/pt-br/acoes-e-programas/aeb-escola-1/propulsao-academica. Acesso em: 4 set. 2026.

AGÊNCIA ESPACIAL BRASILEIRA (AEB). Relatório de Gestão 2021. Brasília, DF: AEB, 2022b. Disponível em: https://www.gov.br/aeb/pt-br/acesso-a-informacao/auditorias/prestacao-de-contas/Relatorio_de_Gestao_20211.pdf. Acesso em: 4 set. 2026.

LATIN AMERICAN SPACE CHALLENGE (LASC). Event Guidance and Milestones (EGM). 2. ed., rev. 6. Iacanga: LASC, 2026a. Disponível em: https://drive.google.com/file/d/1RKZWne38H3tk7x7DqhLNhRrAQhgeoMWC/view. Acesso em: 4 set. 2026.

LATIN AMERICAN SPACE CHALLENGE (LASC). LASC General Rules (LGR). 1. ed., rev. 1. Iacanga: LASC, 2026b. Disponível em: https://drive.google.com/file/d/1fDEQsoQ36Da3YmeCA9Bnu1X3AhxRkD4j/view. Acesso em: 4 set. 2026.

LEVESON, Nancy G. Engineering a Safer World: Systems Thinking Applied to Safety. Cambridge: MIT Press, 2011.

LEVESON, Nancy G.; THOMAS, John P. STPA Handbook. Cambridge: MIT, 2018.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION (NASA). Student Launch 2026 Handbook & Request for Proposal. Huntsville: NASA Marshall Space Flight Center, 2025. Disponível em: https://www.nasa.gov/wp-content/uploads/2025/08/g-677852-2026-sli-handbook-508-aug-7-optimized.pdf. Acesso em: 4 set. 2026.