Revista Científica On-line
Tecnologia – Gestão – Humanismo
ISSN: 2238-5819

REVISÃO SISTEMÁTICA DA TÉCNICA STAMP/STPA EM SISTEMAS AEROESPACIAIS

SYSTEMATIC REVIEW OF THE STAMP/STPA TECHNIQUE IN AEROESPACE SYSTEMS

REVISIÓN SISTEMÁTICA DE LA TÉCNICA STAMP/STPA EN SISTEMAS AEROESPACIALES

Gabrieli Martins de Almeida[1] (martins.gabrieli.07.almeida@gmail.com)
Glauco da Silva[1,2] (glauco.silva@fatec.sp.gov.br)

[1]Faculdade de Tecnologia de Guaratinguetá
[2]Instituto de Aeronáutica e Espaço

Resumo
A revisão sistemática é uma investigação científica que reúne estudos relevantes sobre um conjunto de questões formuladas, com o intuito de identificar tendências de investigação, oportunidades de melhorias e novas orientações para futuras pesquisas e aplicações. Neste trabalho deu-se continuidade ao levantamento de dados relativo a uma revisão sistemática da técnica STPA, abrangente da literatura relacionada à segurança de sistemas aeroespaciais. Esta revisão tem como objetivo levar entendimento aos usuários da técnica de segurança STPA (*System Theoretic Process Analysis*), bem como apresentar a forma como seus utilizadores estão conduzindo suas análises, tornando possível avaliar o quão eficiente é a técnica, em que áreas a técnica está sendo utilizada e o que a diferencia comparada a outras técnicas.
Palavras-chave: Revisão Sistemática, Sistemas Aeroespaciais, STAMP/STPA.

Abstract
A systematic review is a scientific investigation that brings together relevant studies on a set of formulated questions, in order to identify research trends, opportunities for improvement and new directions for future research and applications. In this work, data collection was continued regarding a systematic review of the STPA technique, comprehensive of the literature related to the safety of aerospace systems. This review aims to bring understanding to users of the STPA (System Theoretic Process Analysis) security technique, as well as to present the way in which its users are conducting their analyses, making it possible to evaluate how efficient the technique is, in which areas the technique is being used and what differentiates it compared to other techniques.
Keywords: Systematic Review, Aerospace Systems, STAMP/STPA.

Resumen
Una revisión sistemática es una investigación científica que reúne estudios relevantes sobre un conjunto de preguntas formuladas, con el fin de identificar tendencias de investigación, oportunidades de mejora y nuevas direcciones para futuras investigaciones y aplicaciones. En este trabajo se continuó con la recolección de datos referente a una revisión sistemática de la técnica STPA, comprensiva de la literatura relacionada con la seguridad de los sistemas aeroespaciales. Esta revisión tiene como objetivo brindar comprensión a los usuarios de la técnica de seguridad STPA (System Theoretic Process Analysis), así como presentar la forma en que sus usuarios están realizando sus análisis, lo que permite evaluar qué tan eficiente es la técnica, en qué áreas la técnica que se está utilizando y qué la diferencia frente a otras técnicas.
Palabras clave: Revisión Sistemática, Sistemas Aeroespaciales, STAMP/STPA.

Introdução

O crescimento exponencial da tecnologia da informação e comunicação é de extrema importância na sociedade, e com isso a responsabilidade de se desenvolver sistemas que funcionem conforme o planejado, completando as missões e não introduzindo perigos. Esta é uma questão importante em todos os sistemas, pois um funcionamento inseguro pode ter consequências catastróficas, como danos ambientais, falhas nos componentes eletrônicos e, em casos mais extremos, a perda de vidas. Este comportamento inseguro pode ocorrer mesmo quando o sistema funciona dentro do planejado, pois fatores externos podem influenciar o equipamento em que um software embarcado no sistema está sendo executado, quando este não estiver preparado para certos tipos de ocorrência.

As técnicas tradicionais de análises de perigos têm sido constantemente aperfeiçoadas, com a adoção de novas abordagens e o surgimento de novos desafios. Com isso, novos problemas também surgiram, e muitas vezes é difícil antecipar uma falha. Alguns modelos são baseados em cadeias de eventos, visando identificar a causa de um determinado acidente ocorrido em um sistema.

Dentro da técnica STPA, as perdas decorrentes de perigos não são analisadas como eventos finais, mas envolvem muitos processos complexos. STPA utiliza o modelo de causalidade, isto é, acumula o máximo de informações sobre como os perigos podem ocorrer. As informações coletadas e analisadas podem e devem ser usadas para eliminar ou minimizar os perigos durante todo o projeto e operação do sistema. Entretanto, a técnica é baseada na teoria de sistemas, já as demais técnicas são baseadas na teoria de confiabilidade. Com isso, a STPA permite identificar fatores causais, como por exemplo o comportamento humano, e cenários mais graves, design do sistema e interação insegura com o software.

O STAMP foi uma abordagem proposta pela professora Nancy Leveson do MIT, que derivou em duas técnicas, CAST e STPA, e baseia-se em dois princípios fundamentais:

• Hierarquia: A segurança é tratada como uma prioridade emergencial que surge com a interação dos componentes dentro de um sistema e são controlados por um conjunto de restrições. A causa de um acidente é vista como resultado de falta de restrições que deveriam ter sido feitas no projeto. O sistema é visto como uma estrutura hierárquica, onde os níveis impõem restrições aos níveis abaixo dele.

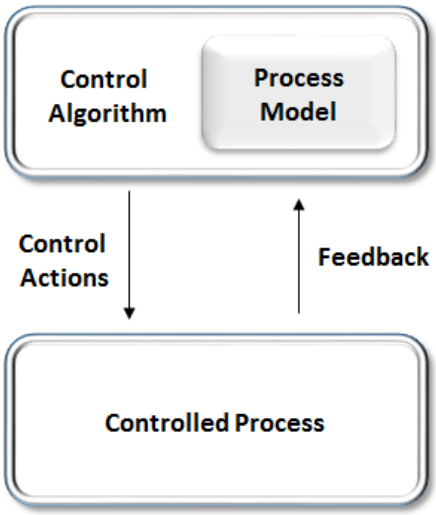
• Controle: O sistema é visto como *loop* de controle interagindo e os acidentes são resultados de ações inadequadas. Os acidentes ocorrem quando o sistema fornece controle inapropriado e as restrições de segurança são violadas.

A Figura 1 apresenta um modelo genérico de estrutura de controle, onde se tem o controlador (humano ou automatizado) e o processo controlado. Com isso o controlador tem um

ISSN: 2238-5819

algoritmo de controle para a tomada de ações de controle, para garantir as restrições de segurança que estão contidas no processo controlado. Este algoritmo utiliza um modelo de processos, com isso ele ajuda o sistema no qual está controlando a tomar as decisões corretas. É muito importante também que o *feedback* forneça as entradas necessárias para manter o controlador informado do que está acontecendo com o processo controlado.

Figura 1 – Estrutura de controle STPA



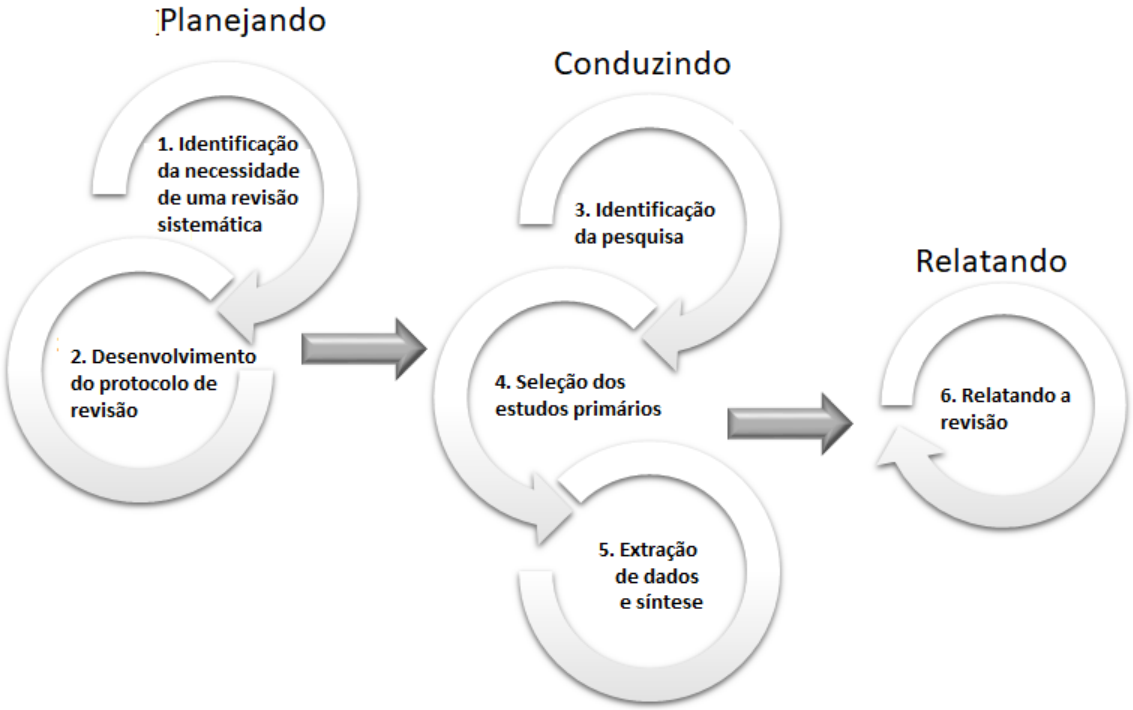
Fonte: LEVESON (2016)

O STPA pode ser usado em qualquer fase do ciclo de vida de um sistema, a análise é dividida em etapas que reduzem a carga analítica sobre os engenheiros de segurança, com isso fornece um processo mais estruturado para analisar de forma ampla os perigos. O STAMP foi um dos principais motivos que levaram a desenvolver estes estudos que resume a literatura do assunto. Acredita-se que este trabalho pode auxiliar a orientar projetos em desenvolvimento, indicando novas direções e recomendações para investigações futuras. Em resumo, este trabalho de pesquisa tem como objetivo finalizar o levantamento abrangente do material desenvolvido e publicado sobre o assunto, além de compreender quais são os pontos fortes e as inconsistências entre as aplicações identificadas.

1 Materiais e Métodos

Para concluir a revisão sistemática, iniciada em 2016 (LAHOZ e MEDEIROS, 2016), foi necessário, além da busca de novos artigos, refazer a catalogação dos diversos artigos, teses, dissertações e publicações a respeito das técnicas datadas do período de 2003 a 2018, utilizando os passos propostos na Figura 2. Elas variam quanto a abordagem: algumas descrevem aplicações do STPA em determinadas áreas, sua combinação com outras técnicas e outras apenas discutem o seu uso.

Figura 2 – Método proposto para a revisão sistemática



Fonte: KITCHENHAM (2004)

A primeira fase da pesquisa foi o planejamento e identificação da necessidade de revisão sistemática relacionada à formulação do problema. Em seguida, são formuladas as questões que guiarão a maior parte do trabalho, avaliando os critérios de investigação. A segunda fase é a condução da revisão, caracteriza-se pela coleta dos trabalhos do STAMP / STPA e seleção de estudos primários, em que foi focado este trabalho, assim como as atividades subsequentes. Além disso, catalogação de dados deve fornecer informações padrão, incluindo o nome do revisor, o título, os autores, o diário e os detalhes da publicação. Por último, na terceira fase, o relato dos resultados de uma revisão sistemática é realizado com a divulgação das conclusões e instruções para futuras investigações, esforço ainda em andamento.

2 Resultados

As questões de pesquisa foram definidas com base em três perspectivas: como, onde e a qualidade do trabalho. A perspectiva *onde* foi usada para identificar a área em que os estudos foram focados, áreas como aeroespaciais, automotiva ou medicina e quais são as instituições e países que estão investindo mais esforços no uso da técnica. A perspectiva *como* foi criada para entender como os estudos foram utilizados: aplicar STAMP/ STPA, como ele foi utilizado, de forma complementar ou mesmo usado para comparar com outras técnicas. A perspectiva *qualidade do trabalho* foi utilizada para classificar as evidências de como foi conduzido o estudo, seu rigor científico e a aplicabilidade em termos de uso acadêmico ou prático.

Além disso, a formulação correta de cada questão de pesquisa é um problema crítico em qualquer SR. Para uma revisão, se você fez a pergunta certa, todo o processo se tornará menos árduo: a pergunta certa significa que é mais fácil encontrar uma resposta correta dentro de um escopo específico e limitado. Foram definidas as seguintes questões de pesquisa (RQ):

RQ.1: Quais são as áreas onde o STPA está sendo aplicado?

RQ.2: Quais são as abordagens e ferramentas que estão sendo aplicadas junto com o STPA?

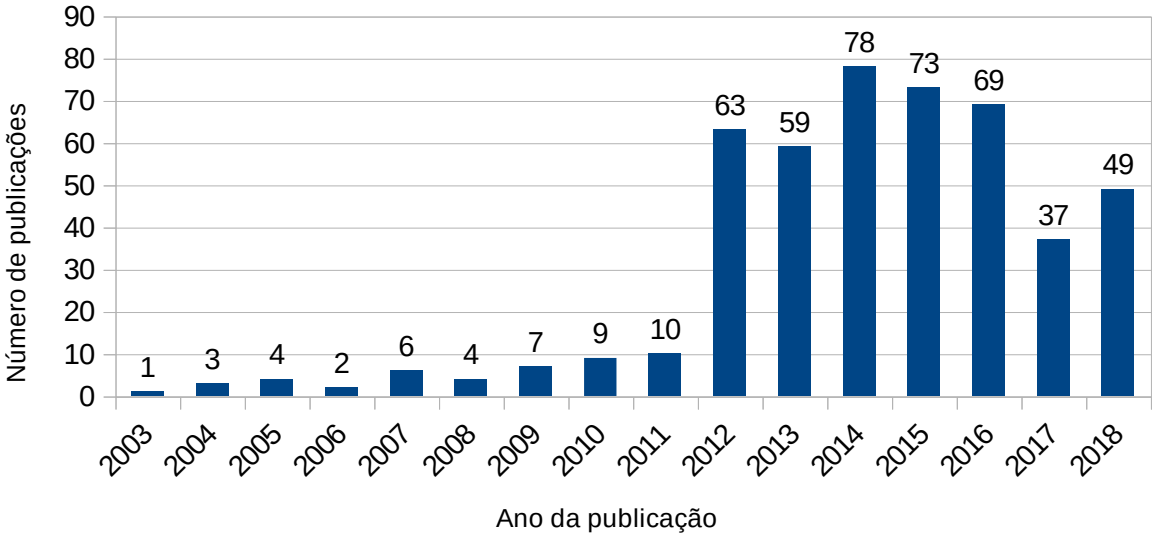
RQ.3: O trabalho discute o STPA com técnicas tradicionais de análise de perigos?

RQ.4: Qual é o nível de evidência disponível em termos de aplicabilidade STPA?

RQ5. Qual o rigor com que o estudo (ou apresentação de workshop) foi conduzido?

A Figura 3 mostra a evolução no número de publicações no período de 2003 até 2018.

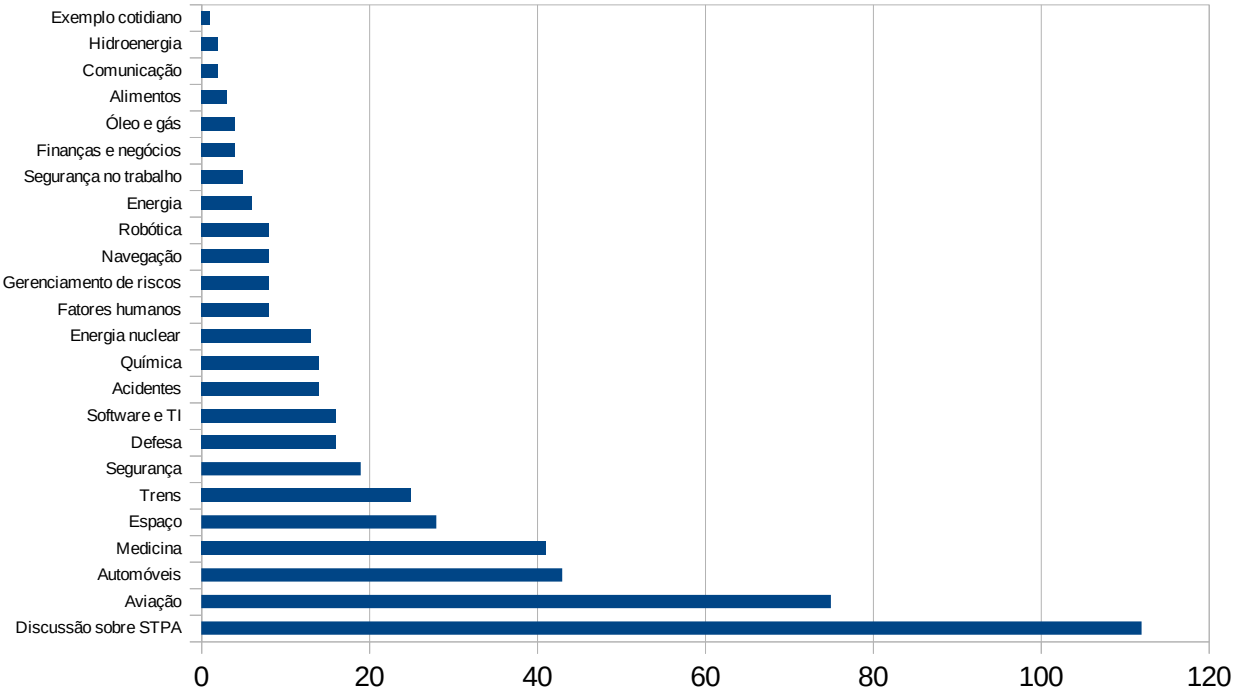
Figura 3 – Evolução no número de publicações



Fonte: Autoria própria

Os resultados preliminares foram extraídos das respostas das RQs elencadas, referentes as análises das publicações já catalogadas e as identificadas recentemente, compondo cerca de 474 trabalhos. A Figura 4, mostra as áreas de aplicação do STPA.

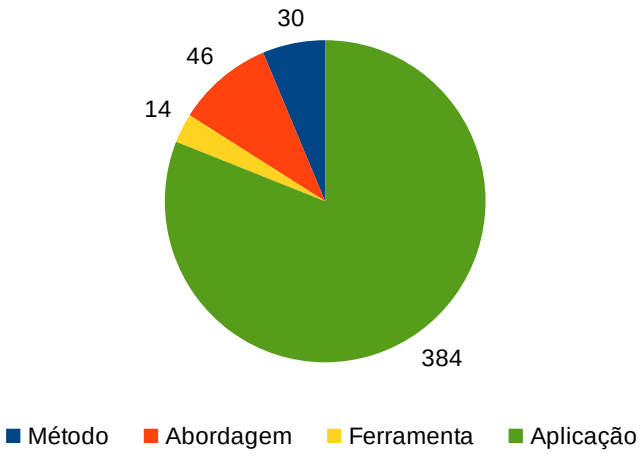
Figura 4 – Áreas de aplicação do STPA



Fonte: Autoria própria

A Figura 5 apresenta os tipos de abordagem dos trabalhos estudados: a combinação da STPA com outras técnicas, como FTA (*Fault Tree Analysis*) ou FMECA (*Failure Mode and Effects Analysis*), por exemplo, seu uso isolado em uma aplicação, ou mesmo o desenvolvimento de ferramenta para sua automação.

Figura 5 – Tipos de abordagem dos trabalhos com STPA



Fonte: Autoria própria

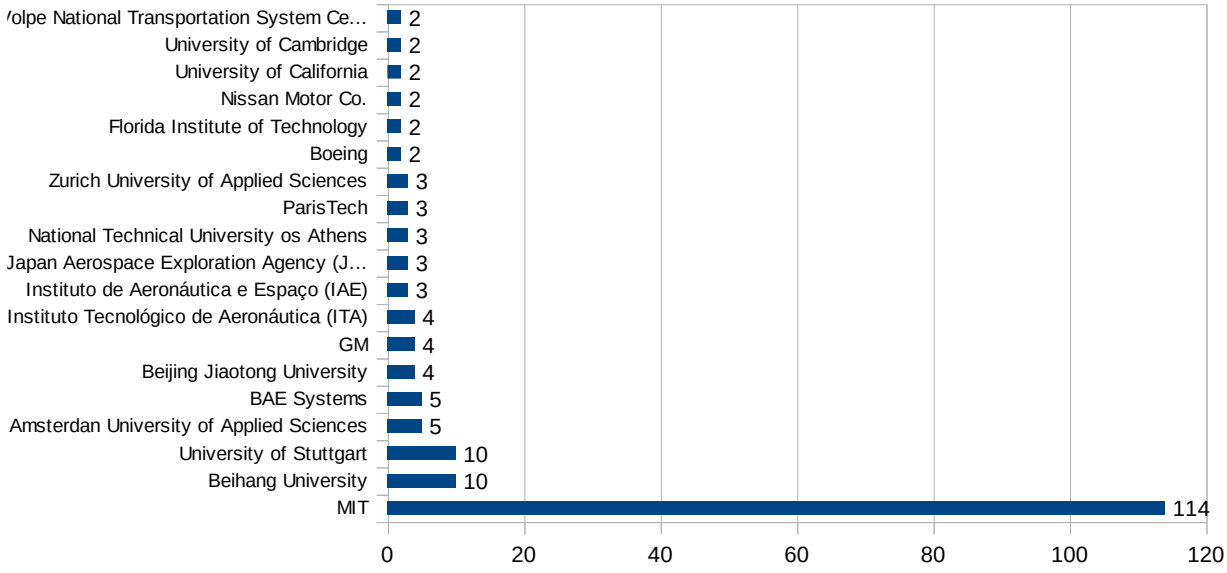
A Figura 6 mostra o nível de evidência dos estudos em termos de uso para propósitos acadêmicos, industriais ou sem nenhuma evidência clara do que o estudo pretendia. Ou seja, se o estudo analisado apresenta resultados que dão indícios de sua aplicação real e prática, ou somente apresenta resultados teóricos.

Figura 6 – Evidências apresentadas nos estudos do STPA

Fonte: Autoria própria

Além dos resultados apresentados na Figura 6, foi feito um levantamento inicial sobre a origem das publicações (Figura 7) quanto à universidade ou empresa de origem dos autores. É importante salientar que nesta Figura estão apresentadas as universidades e/ou empresas que possuem pelo menos duas publicações na área, existem mais instituições que publicaram, porém possuem somente uma publicação.

Figura 7 – Universidades ou empresas que publicaram sobre o STPA



Fonte: Autoria própria

Considerações Finais

Os resultados obtidos forneceram uma base quantitativa e qualitativa sobre as respostas de pesquisa relacionadas a STPA e como os pesquisadores estão utilizando a técnica. Devido à compilação das respostas, pode-se inferir quais as principais áreas em que a técnica está sendo

utilizada, como na área aeroespacial, obviamente por ser objeto de estudo da autora da técnica. Conclui-se que a STPA ainda está sendo utilizada combinada com outras técnicas da área de análise de perigos, provavelmente por ser uma abordagem nova em um ambiente geralmente conservador. Algumas ferramentas de software também foram desenvolvidas e alguns métodos em conjunto com a aplicação.

Há evidências de uso e aplicabilidade, em sua maioria, de estudos acadêmicos, o que significa um primeiro passo para a sua aceitação pela indústria em substituição as abordagens tradicionais. Quando se trata de segurança, a indústria tende a ser mais resistente a novos procedimentos de forma que, quanto mais evidências forem obtidas com aplicações industriais, mais se tenderá a fazer a STPA ser mais aceita neste meio.

Agradecimentos

Ao CNPq pelo auxílio financeiro por meio do Processo 103540/2019-9.

Ao Instituto de Aeronáutica e Espaço (IAE) pela oportunidade de desenvolvimento da pesquisa.

Referências

KITCHENHAM, B. Procedures for performing systematic reviews. **Keele, UK, Keele University**, v. 33, n. 2004, p. 1-26, 2004.

LAHOZ, C. H. N.; MEDEIROS, S. R. G. Systematic review on STPA: final results. In: **STAMP Workshop: MIT Partnership for a Systems Approach to Safety and Security (PSASS)**, Cambridge, MA. 2016.

LEVESON, N. G. **Engineering a safer world**: systems thinking applied to safety. The MIT Press, 2016.