Relatório Final

Título do projeto de pesquisa:	Revisão sistemática em STPA/ STAMP
Bolsista:	Gabriela Diniz da Silva
Orientador(a):	Carlos Henrique Netto Lahoz
Período a que se refere o relatório:	Março de 2017 a Julho de 2017

Resumo

Systems-Theoretic Process Analysis (sigla STPA) consiste em uma nova técnica de análise de risco desenvolvida para aplicação em áreas como aviação, aeroespacial, automobilística e médica. Técnicas já aplicadas na indústria – como FTA ou FMECA – não consideram relações não-lineares, falhas de projeto, feedbacks vagos e interações inseguras entre os componentes de um sistema, ou seja, tais técnicas não incorporam interações entre humanos, hardware, software. Nesse contexto, a STPA tem por objetivo compreender as interações homem-máquina e regulamentar procedimentos para operação além de oferecer uma nova perspectiva sobre a causa de determinado acidente. A revisão sistemática consiste em uma revisão da literatura disponível em determinada área. No presente trabalho conduziu-se uma revisão sistemática para entender como usuários do novo sistema de segurança desenvolvido (STPA) estão conduzindo suas analises é avaliando o quão eficaz é a técnica quando comparada com as tradicionais.

1. Introdução

O crescente uso de softwares e o crescente papel que esses sistemas tem na sociedade faz com que seja cada vez mais relevante a questão de como construir sistemas que funcionam como esperado e não causam danos.

Esta questão é particularmente importante em todos os sistemas em que um mau funcionamento pode consequências catastróficas, como perda de vidas, danos ao meio ambiente ou danos significativos à propriedade, que podem ocorrer mesmo quando os sistemas funcionam exatamente como projetado e sem falhas de componentes individuais.

Embora as técnicas tradicionais de análise de segurança tenham tido algumas melhorias nos últimos tempos, os sistemas modernos introduziram novos desafios e

problemas que podem ser mais difíceis de serem antecipados, analisados e prevenidos. Os modelos tradicionais se baseiam em uma cadeia de eventos para tentar explicar a causa de acidentes ocorridos em um determinado sistema.

Nesse contexto, surgem novas abordagens para analisar uma ocorrência onde a causa dos acidentes não é vista como uma cadeia de eventos e de falhas ao longo do tempo. Considera-se que as perdas não são eventos finais, mas envolvem um processo complexo.

A STPA é uma nova técnica de análise de riscos, que incorpora o modelo de causalidade do acidente do STAMP, com os mesmos objetivos que qualquer outra técnica de análise de risco, isto é, acumular informações sobre como os perigos podem ocorrer (cenários).

Essas informações podem então serem usadas para eliminar, reduzir e controlar os perigos na concepção, desenvolvimento, fabricação e operações do sistema. No entanto, o STPA é baseado na teoria dos sistemas, enquanto as técnicas tradicionais de análise de perigos possuem teoria da confiabilidade em sua base, permitindo identificar mais fatores causais e cenários perigosos, particularmente aqueles relacionados ao software, design do sistema e comportamento humano.

Enquanto as técnicas tradicionais foram projetadas para evitar acidentes de falha de componentes, o STPA foi projetado também para enfrentar acidentes de interação de componentes cada vez mais comuns, o que pode resultar de falhas de projeto ou interações inseguras entre falhas componentes.

O STAMP (Modelagem e Processos de Aconselhamento Teórico-Teórico) é um modelo de acidente baseado na teoria do sistema, proposto por Nancy Leveson, e baseia-se nos dois principais pares de ideias subjacentes à teoria dos sistemas e ao pensamento sistêmico:

- **Emergência e hierarquia:** nesta nova abordagem, a segurança é tratada como uma propriedade emergente que surge quando os componentes do sistema interagem dentro de um ambiente e são controlados ou aplicados por um conjunto de restrições relacionadas ao comportamento dos componentes do sistema. A causa de um acidente, em vez de ser entendida em termos de uma série de eventos, é vista como resultado da falta de restrições impostas ao projeto de sistemas e às operações. Onde os sistemas são vistos como estruturas hierárquicas, onde cada nível impõe restrições à atividade do nível abaixo dele.

- **Comunicação e controle:** sob este modelo, o sistema é visto como loops de controle interagindo e os acidentes são considerados como resultado da aplicação inadequada de restrições de segurança no design, desenvolvimento e operações. Assim, ocorrem acidentes quando o processo de controle fornece controle inadequado e as restrições de segurança são violadas no comportamento dos componentes de nível inferior. Entre os níveis hierárquicos de cada estrutura de controle, são necessários canais de comunicação efetivos tanto um canal de referência descendente que fornece a informação necessária para impor restrições de segurança ao nível abaixo e um canal de medição para cima para fornecer feedback sobre a eficácia das restrições.

A Figura 1 apresenta um modelo genérico da estrutura de controle, onde o controlador (humano ou automatizado) contém um Algoritmo de Controle para decidir quais as Ações de Controle são fornecidas para garantir que as restrições de segurança sejam mantidas no Processo Controlado. O Algoritmo de Controle usa um Modelo de Processo, com o estado atual do sistema que está controlando, para ajudar a tomar essa decisão. O Feedback é para fornecer as entradas necessárias para manter o Controlador consistente com o estado real do Processo Controlado e fechar o loop.

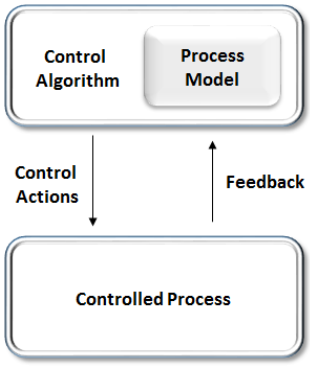

Figura 1 – Estrutura de controle de segurança.

O objetivo principal do STPA é identificar cenários que levem a riscos identificados e, portanto, a perdas para que possam ser eliminadas ou controladas. Ele pode ser usado em qualquer fase do ciclo de vida do sistema, e a análise do processo é dividida em etapas discretas que reduzem a carga analítica sobre os engenheiros de segurança e fornece um processo estruturado para a análise de perigos.

O presente projeto consiste em apresentar uma revisão sistemática para entender como o STAMP/ STPA foi conduzido ou aplicado em diversas áreas. Além disso procura-se verificar as vantagens da técnica em relação às tradicionais.

Em geral, o SR é uma técnica para identificar, avaliar e interpretar pesquisas relevantes em uma área, uma questão de pesquisa ou um fenômeno de interesse específico. Mais especificamente, o SR fornece um resumo conciso das evidências disponíveis sobre uma determinada área [Lahoz e Medeiros, 2015].

Em geral, uma revisão sistemática é uma técnica para identificar, avaliar e interpretar pesquisas relevantes uma área, uma questão de pesquisa ou um fenômeno de interesse específico. Ou seja, a RS fornece um resumo conciso das evidencias disponíveis sobre determinada área [Lahoz e Medeiros, 2015].

A agregação de evidências de pesquisa para orientar o uso do processo STAMP / STPA é um dos principais motivos para desenvolver estudos que resumem a literatura, mas não é o único. As análises sistemáticas são projetadas para serem metódicas, explícitas e replicáveis.

Tais estudos podem ajudar a orientar projetos de desenvolvimento, indicando novas orientações para investigações futuras. Esta pesquisa também é para identificar o que é conhecido e desconhecido, compreender inconsistências entre os achados da pesquisa e discutir possíveis melhorias estratégicas que podem ser realizadas nas próximas versões do STAMP / STPA.

Isso é fundamental para orientar projetos de desenvolvimento, indicando orientações para usos futuros. Esta pesquisa também tem por objetivo determinar o que é conhecido ou não, além de compreender inconsistências entre as aplicações da técnica e discutir possíveis melhoras para as próximas versões do STAMP STPA.

2. Materiais e métodos

Para proceder com a revisão sistemática acerca do STAMP/ STPA foi necessário catalogar os diversos artigos, teses, dissertações publicador a respeito da técnica. Essas publicações são datadas do período de 2012 a 2017 e variam quanto a abordagem em relação à técnica: algumas descrevem aplicações em determinadas áreas outras apenas descrevem.

Esta RS foi conduzida com base nas diretrizes fornecidas por [Kitchenham e Charters 2007]. Dividiu-se em três fases: planejamento, condução e relatórios.

A primeira fase da pesquisa consiste na identificação da necessidade de revisão sistemática relacionada à formulação do problema. Em seguida, baseando-se nisso, são formuladas as questões que guiarão a maior parte do trabalho e direcionarão os critérios de investigação, exclusão e inclusão.

A segunda fase do SR, que conduz a revisão, caracteriza-se pela coleta dos trabalhos do STAMP / STPA (pesquisa de todo o material que abordou o tópico investigado), identificação e seleção de estudos primários.

Esta seleção é de acordo com os critérios de inclusão e exclusão estabelecidos durante a definição do protocolo de revisão, depois que a etapa de extração de dados é realizada para registrar com precisão as pesquisas de informações necessárias para abordar as questões de revisão. Foram utilizadas as plataformas mostradas na tabela a seguir:

Tabela 1 – Fontes utilizadas.

Sigla	Fonte	Link
DSpace	DSpace@MIT	https://dspace.mit.edu
ACM	Association for computing Machinery Digital Library	http://www.acm.org
IEEE Xplore	Institute of Electrical and Electronics Engineers Explore	http://ieeexplore.ieee.org
Google Scholar	Google Scholar	https://scholar.google.com
Citeseer^{X}	Cite Seer^{X} Beta Digital Library	http://citeseerx.ist.psu.edu/index
ScienceDirect	Science Direct	http://www.sciencedirect.com
SpringerLink	Springer Science and Business Media	http://link.springer.com

Além disso, os formulários de coleta de dados devem fornecer informações padrão, incluindo o nome do revisor, o título, os autores, o diário e os detalhes da publicação. Os dados foram compilados

Por último, na terceira fase, o relatório dos resultados de uma revisão sistemática é realizado com as conclusões e instruções para futuras investigações.

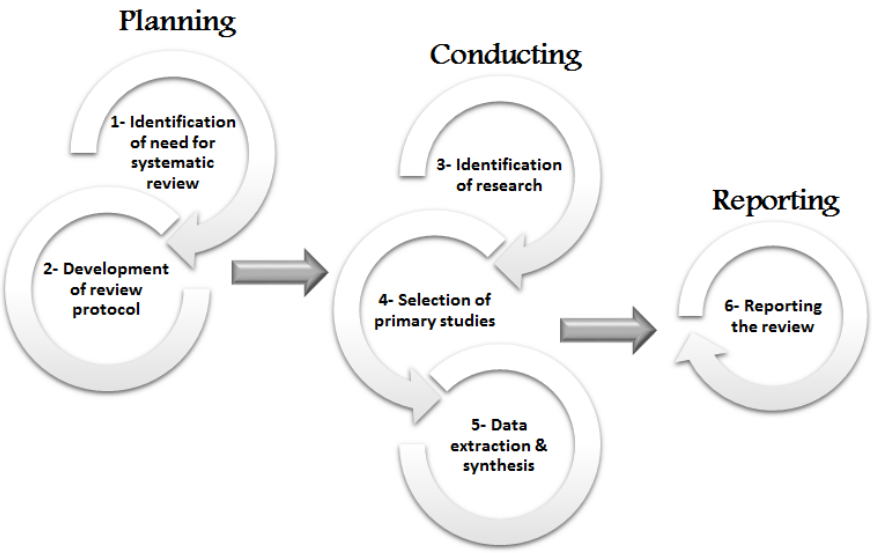

Figura 2 – Método de três passos para a revisão sistemática.

A revisão sistemática pode ajudar a orientar projetos de desenvolvimento, indicando novas orientações para investigações futuras. Assim, o objetivo desta pesquisa é coletar informações sobre casos de estudo onde o STPA foi aplicado, como as pessoas estão usando, o nível de evidências dos resultados e o rigor de como eles usam a metodologia. Além disso, áreas de pesquisa de potencial de identidade para aplicar STPA e melhorias que podem ser realizadas nas próximas versões do STAMP / STPA.

3. Resultados

As questões de pesquisa foram definidas com base em três perspectivas: onde, como e o nível de evidência. A perspectiva "onde" foi usada para identificar onde os estudos foram focados principalmente, áreas como aeronáutica, aeroespacial ou medicina e quais instituições / países estão investindo mais esforços nessa técnica. A perspectiva de "como" foi criada para entender a maneira como os estudos foram utilizados: aplicar STAMP / STPA por si só, de forma complementar ou usar para comparar com outras técnicas. A perspectiva do "nível de evidência" foi utilizada para classificar o rigor científico do estudo e a aplicabilidade em termos de estudo acadêmico ou prático, bem como os resultados apresentados.

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.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?

Os resultados preliminares são dados estatísticos extraídos das publicações catalogadas baseados nas respostas das perguntas acima.

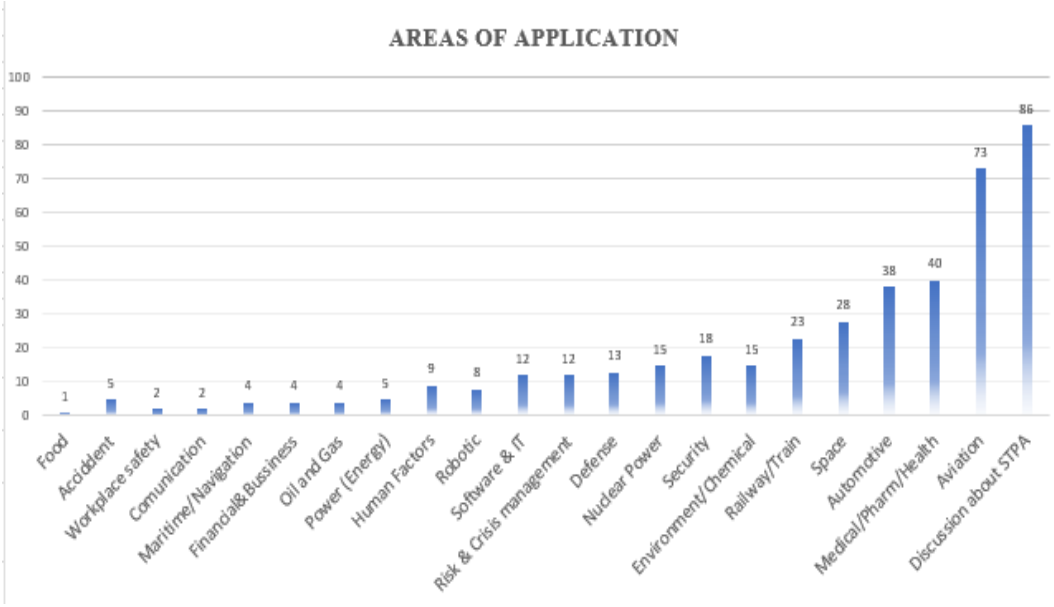

Figura 3 – Áreas de aplicação da STPA.

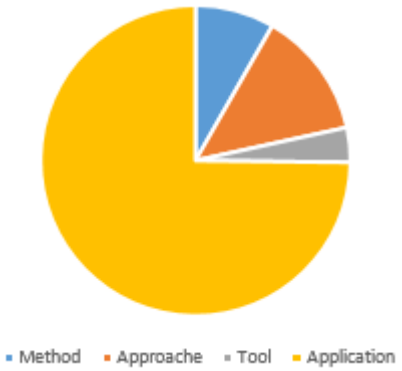

Figure 4 – Formas de utilização da STPA.

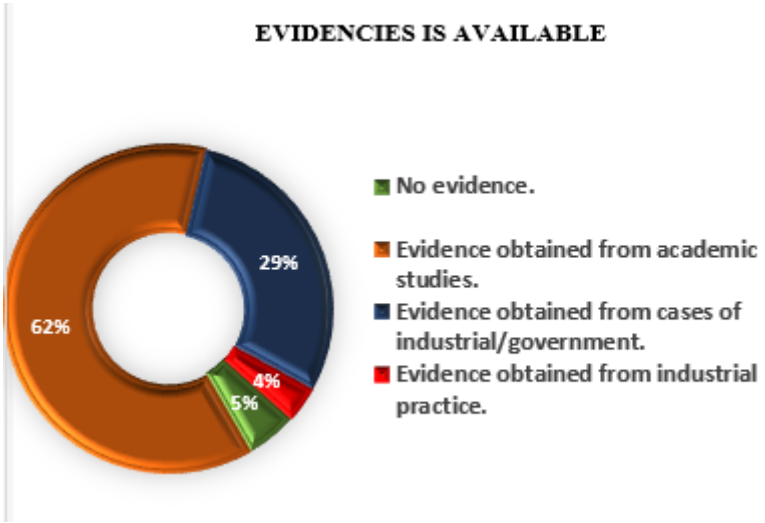

Figure 5 – Evidencias presentes na aplicação da STPA.

4. Próximas Etapas

Uma vez catalogados os artigos publicados na área de STPA/STAMP e feito uma análise preliminar baseado nas áreas de aplicação da técnica, os próximos passos consistem terminar de responder perguntas-chaves que permitam fazer uma revisão sistemática em relação ao tópico estudado.

Tais perguntas serão respondidas analisando-se o conteúdo de cada publicação. As perguntas são respondidas de forma objetiva, através de códigos, para fins estatísticos. A partir dos dados obtidos, que foram mostrados nos gráficos acima, procurar-se-á entender, por exemplo, qual a área mais favorável a aplicação da técnica ou com qual nível de rigor ela está sendo aplicada.

5. Conclusões

A tecnologia e a forma como projetamos e lidamos com sistemas em diversas áreas de engenharia muda rapidamente a cada ano. Dessa forma é fundamental que mude, juntamente com essa evolução, nossa perspectiva sobre como ocorrem as interações dentro de um sistema. As conclusões que inferimos sobre as análises destes nos fornecem ferramentas para lidar e prevenir acidentes.

Sendo essa área – analise de segurança – uma área muito sensível e que exige um alto nível de confiança de seus resultados, é de se esperar que a indústria, por exemplo, não queira arriscar e não aceite com facilidade novos métodos ou novas perspectivas.

A revisão sistemática do STAMP/ STPA é, portanto, fundamental para oferecer uma base de dados confiável que permitam a sua aplicação quando necessária.

Referências

[1] Leveson, N.G. (2012). Engineering a Safer World: Systems Thinking Applied to Safety, MIT. Cambridge.
[2]Lahoz, C H N, Medeiros, S R. Systematic Review on STPA: preliminary results. STAMP Workshop. Cambridge, USA. 2015