Análise de segurança da automação em sistemas sociotécnicos

Sarah Francisca de Souza Borges e Moacyr Machado Cardoso-Junior
Instituto Tecnológico de Aeronáutica - ITA / Grupo de Estudo em Análise de Riscos - GEAR

Resumo — Atualmente, há maior compartilhamento do controle do sistema entre humanos e a automação, conduzindo a novos tipos de erro. Para sistemas sociotécnicos, o método STPA (*System-Theoretic Process Analysis*) se destaca na identificação de UCAs (*Unsafe Control Actions*), respectivos cenários causais e defesas. Contudo, o STPA ainda carece no estudo de fatores humanos e uma implementação nova, segundo especialistas em design de sistemas sociotécnicos, é aplica-lo em conjunto com o método SHERPA (*System Human Error Reduction and Prediction Approach*). Com o SHERPA seria realizado uma descrição das tarefas (abordagem de baixo para cima), e com o STPA a identificação dos perigos e um modelo hierárquico do sistema de controle (abordagem de cima para baixo). Assim, o objetivo deste estudo foi analisar se os métodos SHERPA e STAMP-STPA trariam benefícios ao serem aplicados em conjunto. Como resultado, pelo STPA a identificação foi de 47 UCAs, pelo SHERPA foram 68 modos de erro. Em suma, mostrou-se vantajosa a proposta de usar o SHERPA como complementar, na revisão de resultados do STPA, visando identificar mais modos de erro humano e cenários causais.

I. INTRODUÇÃO

Em sistemas sociotécnicos, a relação entre humanos e automação está cada vez mais complexa. Há maior compartilhamento do controle do sistema, conduzindo a posições em que decisões de alto nível estão a cargo do decisor e a implementação ocorre pela automação. Essas mudanças conduzem a novos tipos de erro humano, como aumento de omissão ou delegação [1].

Nesse cenário, o método STAMP-STPA (*Systems-Theoretic Accident Model and Processes*, *System-Theoretic Process Analysis*) se destaca na identificação de UCAs (*Unsafe Control Actions*), respectivos cenários causais e defesas [2]. Essa nova maneira de visualizar acidentes é resultado de uma demanda por métodos de segurança em engenharia, capazes de lidar com problemas modernos e sistemas complexos. Já demonstrou bons resultados em diversas áreas de atividade, como aeroespacial, defesa, automotiva, medicina e energia [3].

Embora o STPA forneça uma maneira de modelar as interações entre o comportamento humano e a automação, carece na incorporação de fatores humanos (fontes de ações inseguras) para identificação de cenários inseguros específicos [4]. Uma implementação nova, segundo argumentos de especialistas em *design* de sistemas sociotécnicos, seria aplicar o STAMP-STPA em conjunto com o método SHERPA (*System Human Error Reduction and Prediction Approach*) para melhoria dos resultados [5].

Assim, o objetivo deste estudo foi testar esta hipótese, analisar se os métodos STAMP-STPA e SHERPA trariam benefícios ao serem aplicados em conjunto. Em pesquisa na base de dados *Scopus*, *Web of Science* e Google Escolar tal proposta já foi citada em [5], [8], mas não foi aplicada e explorada.

A principal diferença entre os dois métodos é a forma de representação que usam: SHERPA começa com uma descrição das tarefas que estão sendo executadas, enquanto o STAMP-STPA começa com a definição dos perigos do sistema e um modelo hierárquico do sistema de controle. Ou seja, o SHERPA oferece uma abordagem de baixo para cima, enquanto o STAMP-STPA é de cima para baixo [5].

II. Métodos STPA e SHERPA

Entre 2000 e 2004, foi criado pela professora do MIT, Nancy Leveson, a proposta de uma extensão do método STAMP com a análise preventiva de perigos e perdas/acidentes, na ligação entre Engenharia de Segurança e de Sistemas. O objetivo com o STPA, dentro da teoria de controle, não é entender como o ser humano pensa, mas explicar como e por que ele pode violar as restrições de segurança do sistema.

Apresenta 4 passos: 1) Definir a proposta da análise (identificar perdas e perigos); 2) Modelar a Estrutura de Controle; 3) Identificar as ações de controle inseguras (UCAs); 4) Identificar os cenários causais [6].

O SHERPA foi desenvolvido por Embrey, em 1986, com uma taxonomia para identificar modos de falha ou erros associados a atividades humanas. Tendo base na Análise Hierárquica de Tarefas (*Hierarchical Task Analysis*, HTA) [7].

III. PROPOSTA DE INTEGRAÇÃO DOS MÉTODOS SHERPA E STAMP-STPA

O método SHERPA apresenta uma abordagem clássica, reducionista, baseada em tarefas, de predição de erros, enquanto o STAMP-STPA é uma abordagem não reducionista e baseada em sistemas [5], [8].

Apesar destes métodos parecerem, à primeira vista, estar em extremos opostos do aspecto metodológico, no núcleo de ambos existe a taxonomia de erros (SHERPA possui 24 tipos de erros e STAMP-STPA possui 4 tipos de erros). Diante disso, pode-se dizer que o SHERPA possui uma taxonomia de erro mais sofisticada do que o STAMP-STPA [5]. Assim, a proposta é aplicar primeiro o STPA e posteriormente o SHERPA, para verificar se sua taxonomia orientaria para modos de erro não abordados no primeiro método.

IV. RESULTADOS

Antes de aplicar o SHERPA (Figuras 3 e 4), tomou-se como base parte da aplicação do STPA por Megan France, que aborda a interação do motorista (controlador) e a automação (processo controlado), Figura 1, por manobras de estacionamento automáticas (sistema chamado de *Automated Parking Assist* ou APA). Com diferentes tipos de controle, como direção, frenagem, mudança de marcha e aceleração [4].

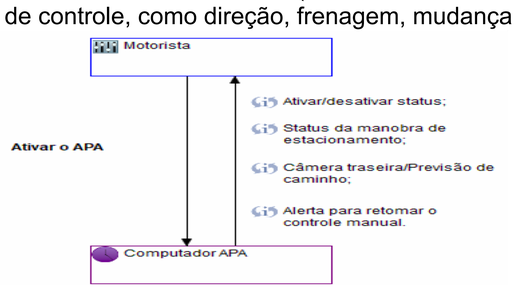

Figura 1 - Estrutura de controle.
Adaptado de [4], software XSTAMP [9].

Tendo como perigos: H1- O veículo não mantém uma distância mínima segura entre si e obstáculos como pedestres, veículos, objetos e terreno. H2- Ocupantes ou carga estão sujeitos a forças repentinas que podem resultar em ferimentos ou danos materiais. H3- O veículo estaciona de forma inadequada, em um espaço inadequado (por exemplo, bloqueando um hidrante) ou violando as diretrizes de estacionamento (por exemplo, excessivamente longe do meio-fio) [4].

Como acidentes: A1- Morte, ferimento ou dano à propriedade resultante de uma colisão com uma pessoa, veículo, objeto ou terreno. A2- Lesões ou danos materiais que ocorrem no veículo, sem colisão. A3- Perda da satisfação do cliente com estacionamento automatizado, sem ferimentos ou danos à propriedade [4].

As Defesas de segurança: 1- O veículo deve manter uma distância mínima segura entre si e obstáculos como pedestres, veículos, objetos e terreno. 2- O veículo não deve frear, acelerar ou girar a velocidades que resultariam em ferimentos ou danos materiais. 3- O veículo deve estacionar em espaços legais válidos e a uma distância adequada do meio-fio [4]. Na sequência, a Figura 2, apresenta 4 UCAs.

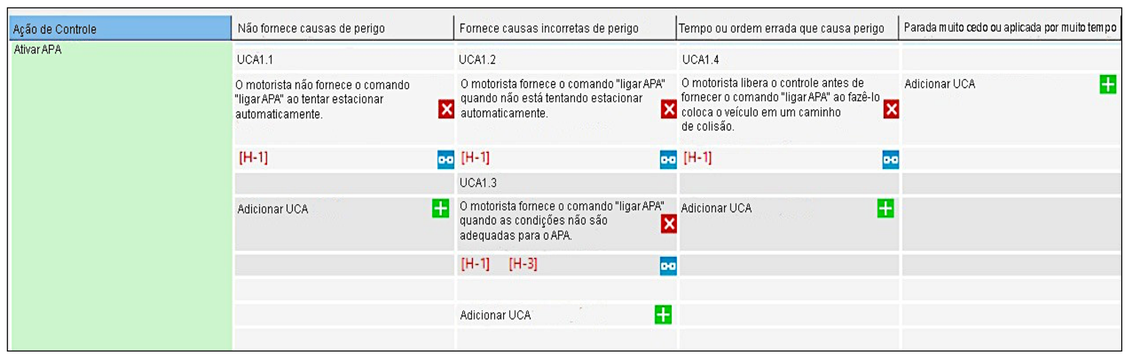

Figura 2 - Definição de UCAs.
Adaptado de [4], software XSTAMP [9].

Tipo de erro	Código	Modo de erro
Erro de ação (*Action*)	A1	Operação muito longa/curta
	A2	Operação realizada no tempo errado
	A3	Operação realizada na direção errada
	A4	Operação muito pequena/grande
	A5	Que sua preparação fracassou
	A6	Operação correta no objeto errado
	A7	Operação errada no objeto correto
	A8	Operação omitida
	A9	Operação incompleta
	A10	Operação errada no objeto errado
Erro de verificação (*check*)	C1	Verificação omitida
	C2	Verificação incompleta
	C3	Verificação correta no objeto errado
	C4	Verificação errada no objeto correto
	C5	Verificação realizada no tempo errado
	C6	Verificação errada no objeto errado
Erro de recuperação (*recovery*)	R1	Informação não obtida
	R2	Informação errada obtida
	R3	Recuperação da informação incompleta
Erro de comunicação (*information*)	I1	Informação não transmitida
	I2	Informação errada transmitida
	I3	Informação transmitida de forma incompleta
Erro de seleção (*selection*)	S1	Seleção omitida
	S2	Seleção errada

Figura 3 - Modos de erro do método SHERPA [6].

SHERPA				
Etapa da tarefa	**Modo de erro**	**Descrição**	**Consequência**	**Recuperação**
1.1 Dar seta	A2, A7, A8, S1, S2	Não dar seta	H1, H3	SC1, SC3
1.2 Ligar APA	A2, A4, A7, A8, C1, R1, R2, S1, S2	Ligar ou não o APA	H1, H3	SC1, SC3
1.3 Desligar APA	A2, A4, A7, A8, C1, R1, R2, S1, S2	Desligar ou não o APA	H1, H3	SC1, SC3
1.4 Direção (computador APA)	A1, A2, A3, A7, A8, A9, R1, R2, I1,I2	Falha na direção pelo computador APA	H1, H3	SC1, SC3
1.5 Direção (motorista)	A3, A7, C1, C3, C4, C5, C6, R1, R2, I1,I2, S1, S2	Falha na direção pelo motorista	H1, H2	SC1, SC2
1.6 Freio (motorista)	A1, A2, A8, A9, C1, S1, S2	Falha ao frear pelo computador APA	H1, H2, H3	SC1, SC2, SC3
1.7 Mudança de marcha (motorista)	A1, A2, A7, A8, C1, S1, S2	Erro na mudança de direção pelo motorista	H1	SC1
1.8 Acelerar (motorista)	A1, A2, A3, A8, A9, C1, S1, S2	Falha ao acelerar muito ou pouco pelo motorista	H1, H3	SC1, SC3

Figura 4 - Aplicação do método SHERPA.

V. CONCLUSÃO

Como resultado, pelo STPA a identificação foi de 47 UCAs, e pelo SHERPA foram 68 modos de erro. As UCAs encontradas no método STPA estavam presentes no SHERPA. Também foi possível verificar que os modos de erro do SHERPA poderiam ser agregados ao STPA na forma de ações de controle e UCAs. Em suma, mostrou-se vantajosa a proposta de usar o SHERPA como complementar, para revisão de resultados do STPA, visando verificar mais fatores humanos e posteriormente cenários causais, e atender a segurança do sistema e operação.

REFERÊNCIAS

1. N. G. Leveson, Engineering a Safer World: Systems Thinking Applied to Safety (Engineering Systems), 1st ed. Cambridge: MIT Press, 2011.
2. N. G. Leveson, “Rasmussen’s legacy: A paradigm change in engineering for safety,” Appl. Ergon., vol. 59, pp. 581–591, 2016.
3. L. S. Campagnaro, “Cubesat Hazard Analysis Using STPA (Trabalho de Graduação),” Instituto Tecnológico de Aeronáutica, São José dos Campos, SP, Brasil, 2016.
4. M. E. France, “Engineering for Humans: A New Extension to Systems Theoretic Process Analysis,” Massachusetts Institute of Technology, 2017.
5. G. Faiella et al., “Expanding healthcare failure mode and effect analysis: A composite proactive risk analysis approach,” Reliab. Eng. Syst. Saf., vol. 169, pp. 117–126, 2018.
6. N. G. Leveson and J. P. Thomas, “STPA Handbook.” p. 188, 2018.
7. C. M. L. Hughes, C. Baber, M. Bienkiewicz, A. Worthington, A. Hazell, and J. Hermsdörfer, “The application of SHERPA (Systematic Human Error Reduction and Prediction Approach) in the development of compensatory cognitive rehabilitation strategies for stroke patients with left and right brain damage,” Ergonomics, vol. 58, no. 1, pp. 75–95, Jan. 2015.
8. T. Bjerga, T. Aven, and E. Zio, “Uncertainty treatment in risk analysis of complex systems: The cases of STAMP and FRAM,” Reliab. Eng. Syst. Saf., vol. 156, pp. 203–209, 2016.
9. A. Abdulkhaleq and S. Wagner, “XSTAMPP: An eXtensible STAMP platform as tool support for safety engineering,” Boston, 2015.