Identificação de Requisitos de Segurança para Experimentos Científicos Embarcados

Heuller Aloys Carneiro Procópio[1,3], Luiz Eduardo Galvão Martins[3], Carlos Henrique Netto Lahoz[2]

[1]Instituto de Aeronáutica e Espaço - São José dos Campos - SP - Brasil, [2]Instituto Tecnológico da Aeronáutica - São José dos Campos - SP - Brasil, [3]Universidade Federal de São Paulo - São José dos Campos - SP - Brasil

Abstract. Space flights are risky due to extreme environmental conditions, in addition to the high complexity of rockets, systems and subsystems. Additionally, there are personal and material risks that are due to the rocket launch operation. The cost for the execution of these projects and their respective tests, launching operation and eventual payload recovery, should also being taken in account. The Brazilian Space Agency (AEB) offers the national scientific community opportunities to access space to carry out experiments in a microgravity environment, by launching suborbital rockets. Given that the rate of launches of this type is low, the failures of the payload items cause significant delays in the project development and its constraints, like cost and schedule. This work proposes to apply the STPA technique (System-Theoretic Process Analysis), a method that is a systemic approach to safety analysis, based on the STAMP approach (System-Theoretic Accident Model and Processes), a predictive risk assessment, to analyze scientific experiments onboard on payloads in suborbital rockets. As results, it is expected obtained safety constraints and recommendations that will contribute to the elaboration of safety requirements applicable to space scientific experiments. It is expected that the availability of systematized information to experimenters in the form of requirements, will contribute to the reduction of experiment failures, as well as simplify the validation process, reducing its subjectivity and interpretation problems.

Palavras chave: STPA, STAMP, Payload, Suborbital Rocket, Safety Requirements

1 Introdução

Há décadas a comunidade científica brasileira lança experimentos científicos ao espaço, em sua maioria lançados a bordo de cargas úteis espaciais, impulsionadas por foguetes que propiciam voos espaciais suborbitais. Estas oportunidades são fomentadas pela Agência Espacial Brasileira, e são previstas no Programa Nacional de Atividades Espaciais (PNAE), 2012-2021. Devido aos custos e à alta complexidade das operações de lançamento, os elevados riscos inerentes a este tipo de atividade devem ser

minimizados. O cronograma desse programa é intrinsecamente longo e as oportunidades de lançar os experimentos devem ser bem utilizadas. Para isso, além de se tomar as ações para o sucesso dos dispositivos envolvidos, bem como toda a operação de lançamento, deve-se também mitigar as potenciais falhas relativas aos experimentos propostos pela comunidade técnico-científica.

Para contribuir com o sucesso da missão de lançamento, os requisitos dos experimentos embarcados devem ser concebidos e projetados atendendo às orientações dos especialistas da área. Os experimentadores enviam as propostas à AEB, que seleciona, prioriza, e os financia e após sua seleção, inicia-se a fase de projeto. Durante esta etapa, os especialistas do Instituto de Aeronáutica e Espaço (IAE) são frequentemente consultados para revisões de projeto e detalhamento das necessidades e restrições dos experimentos. Não é incomum, entretanto, que algumas destas necessidades sejam incompatíveis com o voo, infraestruturas do campo de lançamento ou do IAE, e estas informações só são levantadas no decorrer do desenvolvimento do projeto. Atualmente, a identificação das necessidades (que se tornarão requisitos) é realizada por meio da interação entre especialistas do IAE e pesquisadores das universidades. Entretanto, dada a sua subjetividade, constatou-se empiricamente que este processo não tem sido eficaz. O objetivo geral deste trabalho é a sistematização do processo de definição de requisitos e restrições de segurança a fim de otimizar o mecanismo de comunicação entre a comunidade científica e a equipe de projeto da carga útil de veículos suborbitais. O objetivo específico é a definição de parâmetros padronizados para concepção, projeto e desenvolvimento de experimentos científicos, a partir das seguintes premissas: (i) Sistematização, organização e priorização dos requisitos do sistema de forma a obter requisitos obrigatórios relativos à segurança, recomendáveis e indicativos; (ii) Facilitação e ampliação do acesso da comunidade científica ao programa espacial nacional, por meio de disseminação das informações relevantes a segurança; (iii) Mitigação de potenciais falhas dos experimentos tendo como base os históricos de falhas e informações de técnicos da área.

2 Abordagem para identificação de requisitos de segurança

Para elaborar os requisitos e restrições de segurança é necessário utilizar uma abordagem capaz de fornecer resultados que contribuam com a mitigação de perigos do sistema e de forma que os resultados possam ser verificados através de um conjunto de requisitos e restrições factível, claro e suficiente.

Abordagem

Está em execução uma análise de perigos baseada na abordagem STAMP (*System-Theoretic Accident Model and Processes*), tendo em vista mitigar perigos de projeto e de missão no âmbito da carga útil. A abordagem STAMP, desenvolvida por Leveson N. (2011), adota um modelo causal de acidentes baseado na teoria de sistemas. No modelo STAMP não se omitem causas, e o foco passa da prevenção de falhas para imposições de restrições no comportamento do sistema. Assume que acidentes podem decorrer devido a interações inseguras entre componentes do sistema, mesmo que nenhum desses tenha falhado.

As duas técnicas baseadas em STAMP mais amplamente utilizadas são o STPA (*System-Theoretic Process Analysis*) e o CAST (*Causal Analysis based on Systems Theory*) (Leveson e Thomas, 2018). Mais especificamente, STPA trata a análise de segurança como um problema de controle dinâmico ao invés de um problema de prevenção de falhas. É um método de análise proativo que considera as potenciais causas de acidentes durante o desenvolvimento. Desta forma, os perigos podem ser controlados ou eliminados durante a fase inicial. CAST é um método de análise retroativa, que examina um acidente ou incidente ocorrido, e identifica os fatores causais envolvidos. Estas técnicas expandem o tradicional modelo de causalidade para além da cadeia de eventos de falhas diretamente relacionadas ou de componentes, passando a incluir processos mais complexos e interações inseguras entre sistemas e seus componentes. Além da compreensão da dinâmica do sistema estudado, a análise tem como propósito dois pontos principais: (1) Mitigar perigos da propagação de interações disfuncionais dos experimentos e da interação com outros equipamentos; (2) Mitigar perigos advindos de ações inseguras dos próprios experimentos.

A Figura 1 apresenta um modelo para a análise STPA aplicado a experimentos científicos embarcados. Serão utilizados exemplos de algumas partes. Para obtenção dos resultados da análise com o uso da STPA foram seguidos os seguintes passos:

Identificação de quais são as partes interessadas, seus papéis e o respectivo levantamento das perdas potenciais.
Exemplo: Experimentador Científico, IAE, AEB

Modelagem da estrutura de controle.
Exemplo: Conforme apresentado na Figura 1.

Levantamento das ações de controle inseguras UCAs (Unsafe Control Actions).
Exemplo de Ação de controle: Manipulação para preparação para Testes e Voo
Exemplo de UCA-1: O Operador do Experimento não prepara o Experimento nas condições equivalentes às de voo durante o ensaio Ambiental.
Exemplo de UCA-2: O Operador do Experimento executa procedimento de manipulação distinto do validado, tanto durante os testes quanto para a preparação para o Voo.

Identificação dos cenários de perdas.
Exemplo: Cenário 1 para UCA-1. O Ensaio ambiental do experimento é executado sem as condições de voo, sendo assim considerado inválido. Como resultado a amostra do experimento vaza sem que seja possível identificar a falha.
Exemplo: Cenário 1 para UCA-2. O experimento é integrado para voo em condições distintas às de sua qualificação, e assim sujeito a vazamentos sem a possibilidade de identificação da falha.

Identificação das restrições necessárias apara mitigar os perigos.
Exemplo de restrição relativa à UCA-1: Deverá ser utilizado um checklist onde constem os ensaios mínimos, e em que situação que o experimento deva ser submetido.
Exemplo de restrição relativa à UCA-2: O procedimento de manipulação deverá ser vistoriado por equipe responsável pela qualidade.

Dentro do contexto deste trabalho, as partes interessadas foram devidamente identificadas, e a modelagem da estrutura de controle está em processo de revisão. Assim das

restrições identificadas, serão desenvolvidos os requisitos funcionais e não funcionais a fim de atendê-las. Os requisitos serão classificados e ordenados conforme sua importância.

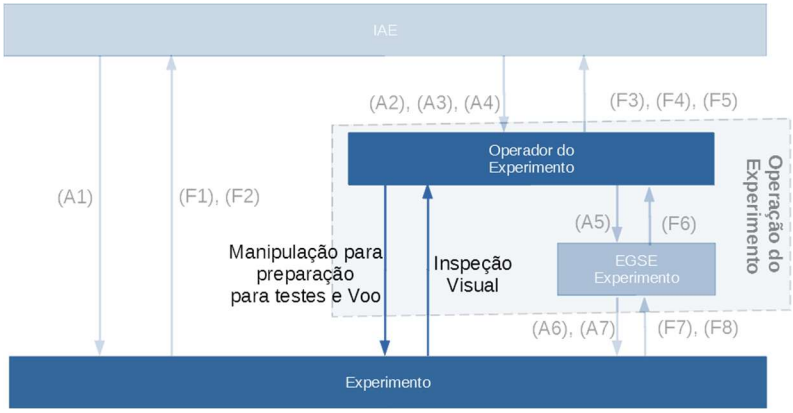

Figura 1: Modelo para a análise STPA aplicado a experimentos científicos embarcados.

Verificação e validação V&V

As restrições e requisitos de segurança que forem identificadas com o apoio da STPA serão verificados e validados, utilizando uma metodologia conhecida e aceita na área de aplicação. Desta forma, serão adotados os trabalhos de Kar P. e Bailey M. (1996), e Halligan R. (2017) para se verificar os requisitos e restrições individualmente e em conjunto. O objetivo é que o processo assegure que os requisitos estão corretos, escritos de forma inequívoca e suficiente. Complementando esta etapa, baseado em Bahill T. e Henderson S. (2004) a verificação se dará através de argumentação lógica e revisão por um corpo de especialistas da área. Assim que elaborado o primeiro conjunto de requisitos e restrições de segurança será iniciada sua verificação e validação V&V. Inicialmente será feita a avaliação lógica, sendo que esta fará parte do trabalho para um melhor entendimento do corpo de especialistas, ao fim desta etapa o conjunto de requisitos será submetido ao corpo de especialistas. Ao final da primeira revisão efetuada pelo corpo de especialistas é avaliado o conjunto de requisitos em forma de questionário com suas respostas graduadas em pontos. Os especialistas deverão confrontar cada um dos requisitos em relação a todos os critérios de verificação, esse também deverá ter a liberdade de questionar cada um dos requisitos em um campo de observações. O valor total da graduação podendo indicar a necessidade de uma nova versão ou se esta pode ser considerada suficiente dentro de um valor limite ainda a ser especificado. Para melhor entendimento do processo a Figura 2 apresenta o fluxograma do processo de V&V

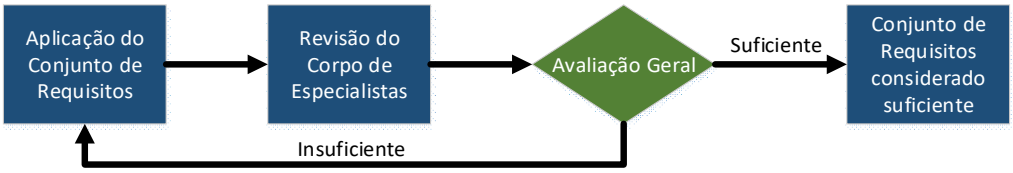

Figura 2: Fluxograma do processo de verificação e validação.

Serão adotados critérios descritos em Kar P. e Bailey M. (1996), e Halligan R. (2017) para o teste de cada requisito ou restrição individualmente. Para efeito de explicação, são utilizados neste artigo dois requisitos que foram definidos pelo IAE como exemplo:
[R 001]: O operador do experimento deve preparar o experimento para o ensaio ambiental com os mesmos materiais e procedimentos previstos para o Voo.
[R 002]: Deverá ser verificado e acompanhado, com o auxílio de um checklist, o procedimento de preparação do experimento para o Voo.
Os critérios, bem como a forma de verificação e validação, são apresentados a seguir:

Capacidade de ser atendido: o requisito deve ser capaz de ser atendido de forma viável e prática.
Argumentação lógica aplicado ao requisito R001: O experimento deverá sofrer o ensaio ambiental nas mesmas condições e com os mesmos procedimentos previstos para Voo. Isto faz com que o ensaio seja representativo e seu procedimento validado, pois a capacidade de contenção da amostra do experimento é testada para as condições de Voo. Questionário do corpo de especialistas aplicado ao requisito R001: O requisito é possível de ser atendido? Possíveis respostas: Completamente (3 pontos); Em grande parte/maioria dos casos (2 pontos); Parcialmente/poucos casos (1 ponto); Não (0 ponto).
Construção padronizada: o requisito dever utilizar apenas termos que previamente foram estabelecidos, dentro de limites e parâmetros aceitáveis a fim de não gerar ambiguidades. Questionário do corpo de especialistas aplicado ao requisito R002: Todos os termos do requisito foram pré-estabelecidos? Possíveis respostas: Todos (3 pontos); Em grande parte/maioria dos termos (2 pontos); Parcialmente/poucos termos (1 ponto); Nenhum (0 ponto).
Verificável: o requisito deve ser capaz de verificação através de um processo de análise, inspeção, demonstração ou teste. Questionário do corpo de especialistas aplicado ao requisito R001: De que forma este requisito pode ser verificado? Possíveis respostas: Análise (3 pontos); Inspeção (3 pontos); Demonstração (3 pontos); Teste (3 pontos); Não pode ser verificado (0 ponto).
Outros critérios serão elaborados e inclusos futuramente, estes são: Correção, Completude, Clareza, Consistência, Não Ambíguo, Conectividade, Singularidade, Capacidade de ser modificado. E em relação conjunto: Orientação funcional.

3 Conclusões e trabalhos futuros

Espera-se que com a disponibilização de informações aos experimentadores, de maneira sistematizada em forma de requisitos, seja possível contribuir com a redução das falhas de experimentos, bem como simplificar o processo de validação, reduzindo também sua subjetividade e problemas de interpretação. A técnica STPA será aplicada para elaborar um conjunto de requisitos e restrições de segurança, tem sido utilizada em diversas análises de missões espaciais e se mostra adequada a este tipo de sistema em diversos níveis de abstração. Será executada uma revisão sistematizada da bibliografia em relação do uso do STAMP e STPA para a aplicação espacial de forma a explorar melhor o uso da técnica e de recomendações já aplicadas em outras análises do setor.

Com o uso dos resultados da análise executada será elaborado um conjunto de requisitos e restrições, e na sequência esse conjunto será verificado conforme parâmetros estabelecidos.

4. Agradecimentos

Este trabalho foi parcialmente apoiado pela Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), processo no. 2019/09396-0.

Bibliografia

1. Palmerio A., Introdução à Tecnologia de Foguetes. 2. ed. São José dos Campos: SindCT, p. 306. 2017.
2. Agência Espacial Brasileira, Programa Nacional de Atividades Espaciais: PNAE: 2012-2021. Ministério da Ciência Tecnologia e Inovação. p. 37. 2012.
3. Leveson N.; Thomas J. STPA Handbook p. 188. 2018. Disponível em: http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf. Acesso em: 27 fev. 2020.
4. Leveson N., Engineering a Safer World: Systems Thinking Applied to Safety. Massachusetts, p. 463. 2011.
5. Kar P., Bailey M., Characteristics of Good Requirements, 1996. Disponível em: http://www.literateprogramming.com/Characteristics%20of%20Good%20Requirements.htm. Acesso em: 09 mar. 2020.
6. Halligan R., Requirements Analysis that Works, Project Performance International: Systems Engineering Key Downloads. p. 6. 2017.
7. Bahill T., Henderson S., Requirements Development, Verification and Validation Exhibited in Famous Failures, Systems Engineering: The Journal of the International Council on Systems Engineering, Published on behalf of the International Council on Systems Engineering (INCOSE). Vol. 8. Issue 1. p. 1-14. 2005.
8. National Aeronautics and Space Administration. NASA Sounding Rockets User Handbook Program Handbook 810-HB-SRP, Goddar Space Flight Center Wallops Flight Facility p. 181. 2015.
9. European Space Agency. European User Guide to Low Gravity Plataforms (UIC-ESA-UM-0001). Issue 3. 1-2 a 1-4. 2014.
10. Agência Espacial Brasileira. Regulamento Geral da Segurança Espacial. Regulamentos de Segurança do Setor Espacial. Vol. 1. p. 11. 2018.
11. Agência Espacial Brasileira, Regulamento Técnico da Segurança para Carga Útil. Regulamentos de Segurança do Setor Espacial. Vol. 2. parte 4. p. 28. 2018.