11º Workshop em Engenharia e Tecnologia Espaciais
18, 19 e 20 de agosto de 2020

Uma metodologia para refinar os requisitos nas fases preliminares do projeto de sistemas espaciais considerando análises de risco e teste

Larissa dos Santos Martins Bringhenti [1], Dra. Ana Maria Ambrosio [2], Dr. Walter Abrahão dos Santos [2]

[1]Instituto Nacional de Pesquisas Espaciais, São José dos Campos, SP, Brasil

Aluna de Doutorado do curso de Engenharia e Gerenciamento de Sistemas Espaciais - CSE.

[2]Instituto Nacional de Pesquisas Espaciais, São José dos Campos, SP, Brasil

larissa_martinsrj@hotmail.com.br

Resumo. *O presente artigo apresenta conceitos do processo de desenvolvimento de uma missão espacial referente a fase conceitual, com foco na elicitação de requisitos e considerando ferramentas de análise. O objetivo principal do estudo é avaliar a contribuição de técnicas de análise de risco e metodologias de teste nas fases preliminares da missão a fim de se obter melhores requisitos.*

Palavras-chave: Exploração de Conceito; Requisitos; Análises de risco.

1. Introdução

No contexto do desenvolvimento da missão espacial, [Wertz et al, 2018] afirmam que é necessário entender "como" e "por que" o processo de desenvolvimento é feito da maneira que é, com o objetivo de o tornar melhor no futuro.

Sabe-se que o processo é iterativo, o que resulta em maior custo. Dessa forma, desenvolver metodologias, ter um novo entendimento, propor abordagens diferentes nas fases preliminares do projeto podem resultar em redução de custo, que é sempre um fator importante nas missões espaciais.

Por outro lado, os sistemas tem se tornado tão complexos, que a definição e refinamento dos requisitos em fases preliminares não é tarefa fácil.

[Leveson, 2003] discorre sobre acidentes na área espacial que ocorreram no final da década de 90, como, Ariane 501, Mars Climate Orbiter (MCO), Mars Polar Lander (MPL), Titan/Centaur, Milstar, Solar Heliospheric Observatory (SOHO) e conclui que tais acidentes aconteceram por diversos fatores, dentre eles, para o presente artigo, vale destacar:

- Processo inadequado das Engenharias de Sistemas e de Software – Tal processo foi ineficaz na identificação das funções críticas e na escrita dos requisitos. Os requisitos eram tão alto nível que dificultou o desdobramento correto para os subsistemas.
- Especificações pobres ou faltantes – Quase todos os acidentes aeroespaciais relacionados a software foram registrados com requisitos falhos ou mal-entendidos

sobre o que o software deveria fazer. O software funcionou exatamente como foi projetado. Ou seja, a especificação que estava incorreta e não a sua implementação.

Assim, este trabalho foi motivado pela necessidade de melhoria no processo de especificação de requisitos nas fases preliminares para o sucesso de um projeto de missão espacial. A ideia é desenvolver uma metodologia que incorpore análises de risco e questões de teste, visando enriquecer a gama de opções e necessidades que possam indicar relevantes requisitos mais cedo no ciclo de desenvolvimento da missão espacial.

2. Conceitos do Processo de desenvolvimento de uma missão espacial

Essa Seção apresenta conceitos importantes no desenvolvimento do estudo em questão.

O item 2.1 apresenta as fases da missão espacial, destacando para as iniciais Pre-Fase A e Fase A. O item 2.2 apresenta os tipos de requisitos existentes no desenvolvimento da missão espacial. Os itens 2.3, 2.4 e 2.5 apresentam metodologias de análise de risco e teste.

2.1 Pre-Fase A e Fase A - Exploração de Conceito

[Wertz et al, 2018] se baseia na definição da NASA para nomear as fases da missão espacial:

- Pre-Fase A – Estudos de Conceito
- Fase A – Conceito e Desenvolvimento de Tecnologia
- Fase B – *Design* Preliminar e Conclusão de Tecnologia
- Fase C – *Design* Final e Fabricação
- Fase D – Montagem do sistema, Integração & Teste, Lançamento
- Fase E – Operações e Sustentabilidade

Nesse trabalho, o foco principal está nas fases iniciais chamadas de Pre-Fase A e Fase A.

A Pre-Fase A e Fase A são fases iniciais do projeto no qual se tem as necessidades do cliente e a partir desse ponto, as análises começam a ser feitas para desenvolver os requisitos e explorar as possibilidades de solução.

Assim, a exploração de conceito é o ponto de partida de todo o processo da engenharia da missão espacial e pode ser dividida em 4 etapas: Definição dos Objetivos e Restrições da Missão, Definição do Conceito de Missões Alternativas, Análise e Estimativa, Definição da *Baseline* de Requisitos. A Figura 1 ilustra tais etapas destacando os pontos mais relevantes no desenvolvimento de cada uma delas.

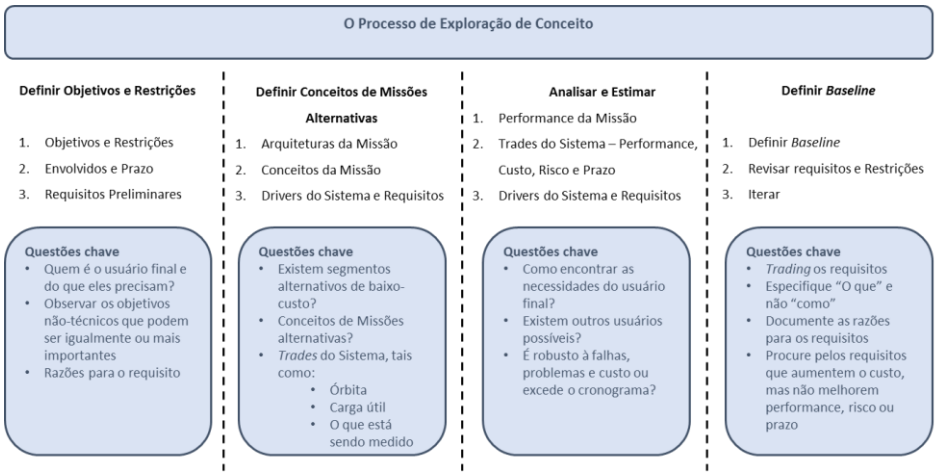

Figura 1: Representação do Processo de Exploração de Conceito [Tradução da Fonte: Wertz et al, 2018]

2.2 Requisitos

Os requisitos devem ser a expressão do que se quer e não de como alcançá-los. Dessa forma, deixa-se aberto diferentes opções de solução que podem reduzir o custo e o risco ou talvez aumentar a performance do sistema com incremento mínimo desses fatores, a fim de obter melhor sistema com o menor custo.

Em [Wertz et al, 2018] são definidos 3 tipos de requisitos: Requisitos funcionais, Requisitos operacionais e Restrições.

Os requisitos funcionais tratam do que o sistema deve fazer. Os requisitos operacionais de como o sistema deve ser usado e as restrições são as limitações impostas.

Apesar dessa literatura apresentar 3 tipos de requisitos, no trabalho de [Viscio et al, 2015] outros tipos de requisitos são apresentados.

[Viscio et al, 2015] apresenta uma metodologia para o projeto de missões espaciais, destacando para o desenvolvimento de requisitos derivados. Segundo os autores, apesar de existirem muitas ferramentas no desenvolvimento de sistemas e missões complexas, não existe um processo rigoroso para o desenvolvimento de requisitos derivados. Assim, são propostas mais categorias de requisitos e quais análises estão relacionadas a eles, conforme mostra a Figura 2.

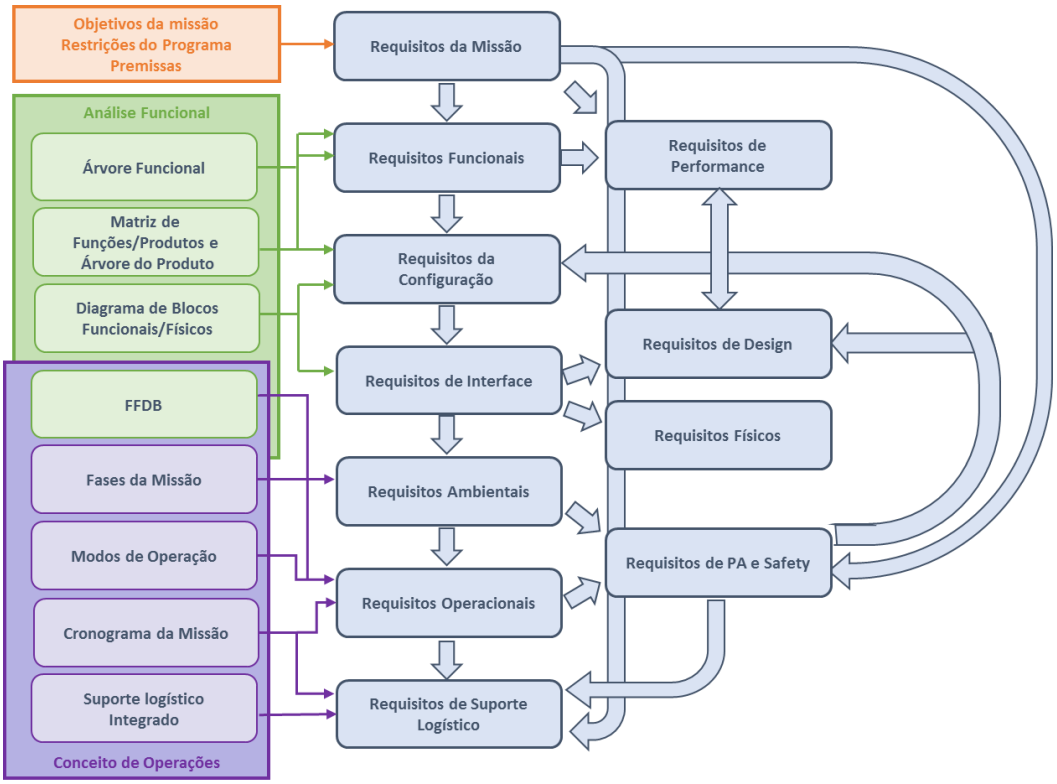

Figura 2: Metodologia da definição de requisitos [Tradução da Fonte: Viscio et al, 2015]

No lado esquerdo do fluxograma, a caixa laranja representa os Objetivos da missão, as restrições do programa e as premissas, nos quais desdobram os requisitos da missão. As caixas verde e roxa são respectivamente, as análises: Análise Funcional e Conceito de Operações. Dentro de cada caixa, estão as ferramentas utilizadas nessas análises.

A Análise Funcional é o processo de identificar, descrever e relacionar as funções do sistema. As ferramentas utilizadas:

- Árvore Funcional: A árvore funcional identifica as funções a serem executadas para desenvolvimento da missão, tendo o topo dela como as funções complexas que vão sendo desdobradas até as funções básicas, ou seja, que não podem mais ser divididas.
- Matriz de Funções/Produto e Árvore do Produto: A matriz de Funções/Produtos identifica os elementos necessários para realizar as funções. Lembrando que o "Produto" pode ser um sistema ou subsistema. A árvore de produto é um agrupamento dos elementos para cada função.
- Diagrama de Blocos Funcionais/Físicos: O Diagrama de blocos Funcionais/Físicos é uma representação no qual identifica o tipo de *link* entre as funções, por exemplo, como as informações trafegam fisicamente, *link* mecânico, elétrico, etc.

O Conceito de Operações permite descrever como o sistema será operado durante o seu ciclo de vida para alcançar os objetivos da missão. As ferramentas utilizadas:

- FFDB (*Functional Flow Block Diagrams):* O FFDB representa o fluxo das funções. A ideia é mostrar uma sequência lógica do "o que" deve acontecer e é proveniente da análise funcional.
- Fases da Missão: São definidas em termos de atividades e ambiente. Cada fase é identificada por um estado do sistema dentro da missão em consideração. O estado do sistema é definido pelo ambiente externo (por exemplo, radiação, calor, vibração) no qual o sistema opera.
- Modos de Operação: Os modos de operação permitem uma visão de quais funções estão disponíveis simultaneamente de acordo com uma certa configuração.
- Cronograma da Missão: Identifica a duração de cada fase da missão.
- Suporte logístico Integrado: Lista as considerações para garantir um suporte econômico e efetivo do sistema durante o seu ciclo de vida.

Cada ferramenta é útil para derivar categorias específicas de requisitos que são representadas nas caixas azuis claras da Figura 2. As categorias do centro são os requisitos "primários" originados da análise funcional, ou seja, considerando as funções que o sistema deve executar. Enquanto as categorias listadas do lado direito, são os requisitos "secundários" estabelecidos através do desempenho dessas funções.

As setas representam as interações. Por exemplo, os requisitos de *Design* recebem entrada dos requisitos de interface, mas também dos requisitos de Performance e de PA (*Product Assurance)* e *Safety*.

2.3 FMEA

O *Failure mode and effect analysis* (FMEA) é definido pela IEC 60812 como um procedimento sistemático para as análises do sistema a fim de identificar os potenciais modos de falha, causas e efeitos no desempenho no sistema.

O FMEA é uma análise gerada para confiabilidade qualitativa, mantenabilidade, segurança e análise logística, que relaciona as causas e os efeitos da falha. Ainda contém informações como severidade, taxa de falha e probabilidade do modo de falha, que indicam a probabilidade de cada modo de falha e seus efeitos na performance do sistema. Para os sistemas complexos, a falha é usualmente associada com muitos componentes. A identificação do componente causa-raiz da falha torna-se um desafio, sendo geralmente, determinado através da experiência humana. É um processo extensivo, que consome tempo, no entanto, uma metodologia clássica que traz um procedimento sistemático conhecido, sendo útil para os requisitos de *safety*.

2.4 Systems-Theoretic Accident Model and Process (STAMP) e STAMP-Based Process Analysis (STPA)

As técnicas tradicionais de análise de risco, como o FMEA, assumem que os acidentes são causados por falhas de componentes. Dessa forma, a técnica consiste em identificar os componentes críticos e prevenir a falha aumentando a integridade do componente e adicionando redundâncias para mitigar os efeitos da falha. Logo, não são considerados nessa análise, erros de software e nem falhas humanas. Fatores cada vez mais presentes no

desenvolvimento de sistemas complexos. Assim, visando endereçar tais eventos, uma nova abordagem foi desenvolvida, chamada *System-Theoretic Accident Model and Processes* (STAMP) e *STAMP-Based Process Analysis* (STPA).

No artigo de [Nan and Liang, 2019], o método STPA é usado como uma nova abordagem de *safety* para um sistema de controle de lançamento.

No processo STPA, o sistema é visto como uma junção de loops de controle. A análise começa identificando os perigos do sistema e transformando-os em *Safety Constraints*. Depois, um modelo com uma estrutura de controle é definido. O diagrama da estrutura de controle descreve os componentes do sistema e os caminhos de controle e feedback. A partir dessa estrutura, são identificadas as ações de controle e elas são avaliadas quanto à contribuição para os perigos, o que servirá para refinar as restrições de segurança do sistema. Um diagrama geral é apresentado na Figura 3.

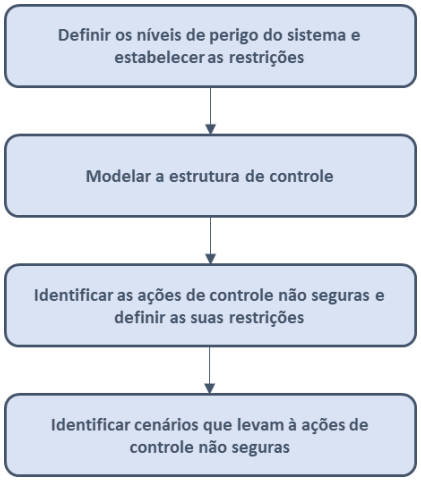

Figura 3: Diagrama do Processo do STPA [Tradução da Fonte: Nan and Liang, 2019]

2.5 Metodologia CoFI

A abordagem CoFI inclui uma metodologia para geração automática de testes e um processo de teste de conformidade, que agregam a técnica de injeção de falhas para validação de software em aplicações espaciais.

O processo de teste define um conjunto de atividades e artefatos necessários para realização dos testes. A metodologia orienta a realização da atividade de criação de casos de teste prevista no processo. [Ambrosio, 2005].

A Figura 4 apresenta uma visão geral da metodologia.

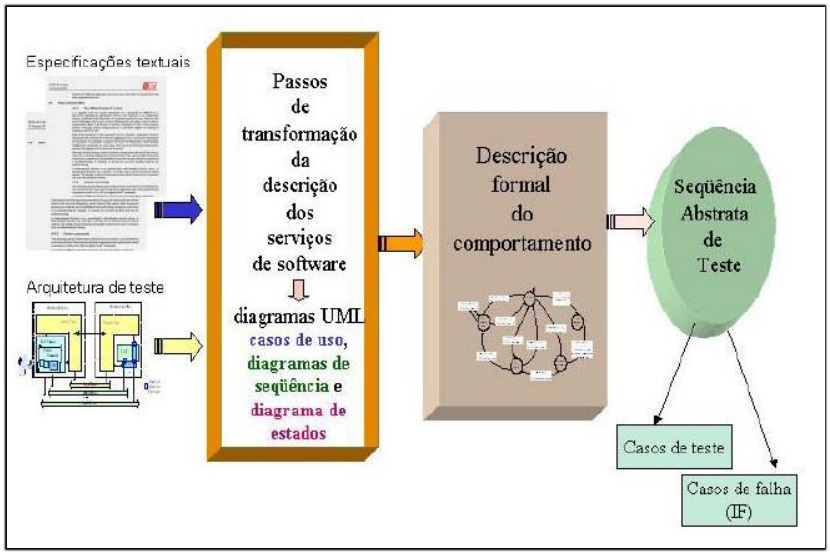

Figura 4: Visão geral da Metodologia CoFI [Fonte: Ambrosio, 2005]

O trabalho de [Pontes, 2018] propõe agregar à metodologias CoFI, duas outras de diferentes áreas:

- *Timed Automata* - usado para verificar a consistência dos modelos em relação às variáveis do sistema (por exemplo, se eles foram declarados corretamente) e comportamento;

- FMEA *(Failure Mode and Effect Analysis)* - auxiliou na avaliação de cada evento de acordo com o estado no qual o sistema estava.

A metodologia CoFI foi usada para desenvolver os modelos de teste de acordo com as especificações e para guiar os desenvolvedores de testes para pensar sobre os eventos que podem perturbar o sistema.

3. Discussão

Nas fases iniciais da missão espacial, Pre-Fase A e Fase A, os requisitos são de alto nível. Nesse início, começam a ser desenvolvidas as análises funcionais do sistema e arquiteturas preliminares são estudadas a fim de encontrar uma melhor solução para ser detalhada. Note que no Final da Figura 1, na qual apresenta a Exploração de Conceito, uma *baseline* de requisitos é gerada, requisitos que foram sendo desdobrados ao decorrer do processo. No entanto, as análises utilizadas não são citadas. O entendimento de diferentes tipos de requisitos e análises associadas é uma das contribuições do trabalho de [Viscio et al, 2015]. Assim, [Viscio et al, 2015] já apresentou uma nova metodologia no qual identifica mais tipos de requisitos do que os três comumente citados (Funcionais, Operacionais, Restrições). Além disso, associou as análises e ferramentas utilizadas, representadas do lado esquerdo do fluxograma da Figura 5.

Nós propomos adicionar mais um tipo de análise, a análise de risco e algumas de suas ferramentas, que são apresentadas nas Seções 2.3, 2.4 e 2.5, respectivamente, FMEA, STAMP, STPA e Metodologia CoFI Porém, aplicado à fase preliminar do projeto – Exploração de Conceito.

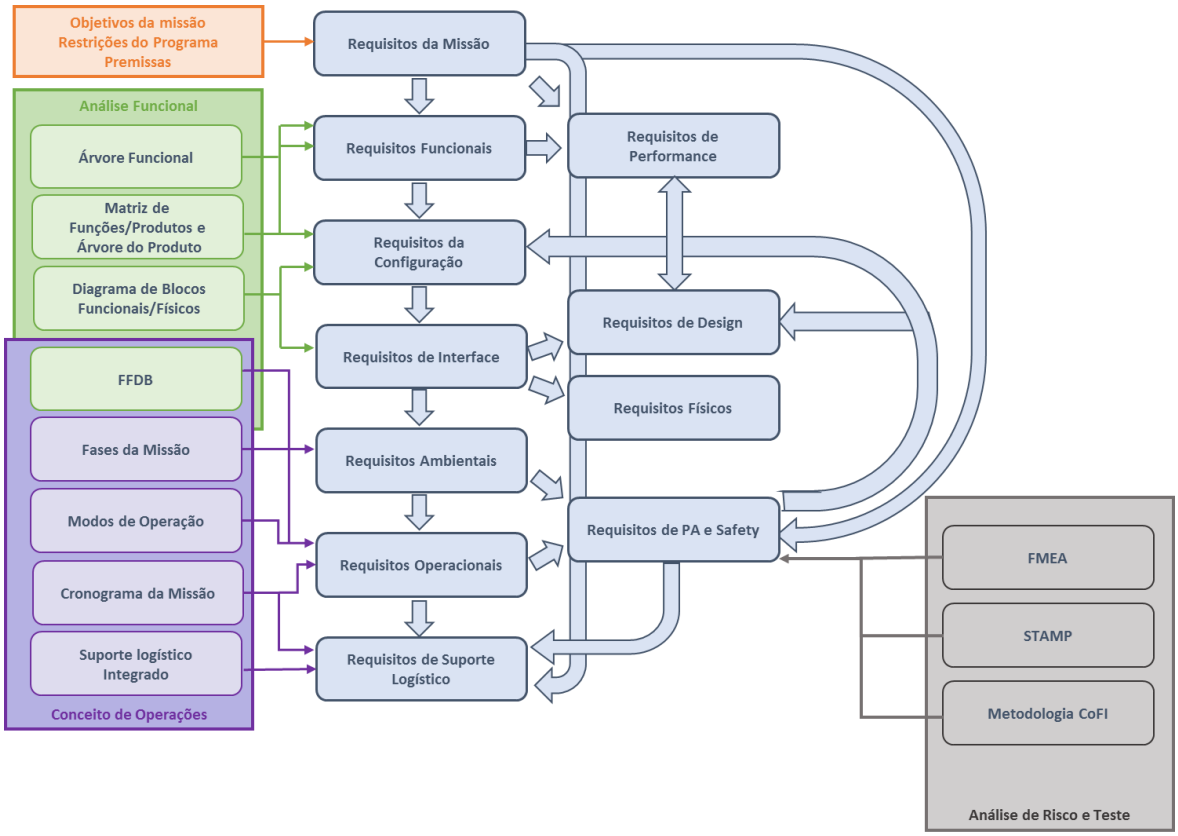

Figura 5: Proposta de estudo

[Wertz et al, 2018] afirmam que se a maior parte do custo do sistema é determinada no final da definição detalhada dos requisitos, então, o processo de definição de requisitos no início do desenvolvimento deve se tornar foco principal na redução de custos.

4. Conclusão

O presente trabalho apresentou uma visão sobre o desenvolvimento de uma metodologia incluindo análises de risco e teste em fases preliminares do projeto a fim de ter requisitos melhores resultando em menores custos e maior confiabilidade na missão.

Referências

Ambrosio, A. M. (2005). CoFI: Uma abordagem combinando teste de conformidade e injeção de falhas para validação de software em aplicações espaciais. Tese (Doutorado em Computação Aplicada) – INPE, São José dos Campos.

INTERNATIONAL STANDARD – IEC60812. (2006). Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA).

Leveson, N. G. (2003). The Role of Software in Spacecraft Accidents – Aeronautics and Astronautics Department – Massachusetts Institute of Technology. Disponível em: http://sunnyday.mit.edu/papers/jsr.pdf

Nan, Q. and Liang, M. (2019). Safety requirements analysis for a launching control system based on STPA. In *International Conference on Mechatronics and Automation*, pages 1201–1205. Proceedings of 2019 IEEE.

Pontes, R.P. (2018). Methodology for the in-process evaluation of software-based process failures in selective laser melting machine tools, Fraunhover Verlag.

Viscio, M. A, et al. (2015). Methodology for requirements definition of complex space missions and systems. In *Acta Astronautica 114,* pages 79-92.

Wertz, J. R, Everett, D. F and Puschell, J. J (2018), Space Mission Engineering: The New SMAD, Microcosm Press, 3th edition.