II Congresso Aeroespacial Brasileiro
De 16 a 19 de setembro

GERENCIAMENTO DE RISCOS E GARANTIA DA SEGURANÇA DE SISTEMAS APLICADOS A PROJETOS DE SATÉLITES

Barroso, B.F.C.[a]; Genaro, A. F. S.[b]; Perondi. L.F.[c] , Maia, G. F. S [a]
[a] Mestranda em Engenharia e Tecnologia Espaciais - Instituto Nacional de Pesquisas Espaciais (INPE), Av. dos Astronautas, 1.758 - Jardim da Granja, São José dos Campos - SP, 12227-010.
[b] Dra em Engenharia e Tecnologia Espaciais - Instituto Nacional de Pesquisas Espaciais (INPE)
[c] Dr em Física Teórica - (Universidade de Oxford). Instituto Nacional de Pesquisas Espaciais (INPE)

Resumo: *Os riscos inerentes ao ambiente espacial somado a complexidade das missões espaciais mostram a importância e a necessidade de haver um esforço no sentido de assegurar o sucesso de uma missão espacial, ou seja, é indispensável haver uma gestão de riscos e garantia de segurança bem delineados e eficaz. O presente artigo aborda a temática de Safety sendo parte de uma pesquisa de mestrado em andamento apresentando o surgimento do conceito de segurança na área espacial e sua importância acidentes que marcaram e sustentaram a evolução deste conceito, além de abordar a relação entre gestão de risco e garantia da segurança com o intuito de garantir a integridade da vida humana e de todos os recursos físicos envolvidos.*

Palavras-chave: *Safety, Gestão de Risco, Projetos.*

1. INTRODUÇÃO

O conceito de sistemas de segurança nasceu no final dos anos de 1940 com a indústria bélica e depois evoluiu para indústria aeronáutica. Na área espacial tal conceito surge com a guerra fria onde o foco eram voos tripulados e desenvolvimento de foguetes, assim surge a necessidade de assegurar que não haja danos em relação à vida humana em projetos espaciais. No contexto histórico compreendido entre o final da década de 1950 e início da década de 1960 nasce a disciplina de segurança de sistemas espaciais.

Em 1958 a *National Aeronautics and Space Administration* (NASA) iniciou o primeiro programa para enviar o homem para o espaço o projeto Mercury que tinha por objetivo verificar a capacidade do homem sobreviver no espaço. Em seguida, teve início o programa Gemini e todos os esforços para voos espaciais tripulados se estendeu até a missão Apollo que culminou com a chegada do homem na Lua. É importante ressaltar que a NASA gerenciou programas de sucesso, mas muitas falhas ocorreram levando a acidentes envolvendo a perda de vidas humanas, tais como os acidentes da Apollo 1, Challenger e Columbia. As investigações de tais acidentes ajudaram a NASA a evoluir por meio da implementação de técnicas melhorias de projetos e programas de segurança adequados, construindo uma cultura de safety que hoje está profundamente enraizada no dia a dia da organização, sendo utilizadas como referência em projetos espaciais de outros países.

A disciplina de Garantia da Segurança (*Safety*) em projetos da área espacial objetiva, de forma sintética, garantir a integridade da vida humana e dos recursos físicos gerais envolvidos em projetos espaciais. Tal disciplina relaciona-se com a de Gestão de Riscos, na medida em que ambas buscam identificar riscos e desenvolver estratégias para a sua mitigação.

O exercício das atividades de gestão de riscos e de garantia da segurança em programas espaciais de referência, como os da NASA e *European Space Agency* (ESA), encontra-se já bem consolidado, dado o volume e complexidade das missões desenvolvidas e a necessidade de garantia de preservação da integridade da vida humana em missões tripuladas.

Bruna Barroso: ninabruna01@gmail.com

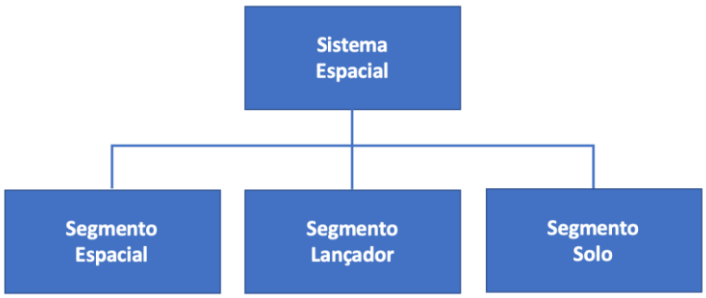
2. REVISÃO DA LITERATURA

A seção a seguir apresentará uma breve revisão de conceitos e está dividida em seis partes. Na primeira parte define-se um sistema espacial; na segunda apresenta- se as fases do ciclo de vida de um projeto espacial; na terceira define-se o conceito de segurança em sistemas espaciais; na quarta apresenta-se um breve histórico de acidentes ocorridos na área espacial; na quinta define-se o conceito de gestão de riscos e na sexta parte apresenta-se a relação entre gestão de riscos, garantia da segurança e engenharia de sistemas.

2.1 Sistema Espacial

O padrão *European Cooperation For Space Standarization* (ECSS) define sistema espacial como sendo um sistema que contém pelo menos um segmento espacial, um segmento solo e lançador. Geralmente, um sistema espacial é composto de todos os três segmentos e por um segmento de suporte (ECSS, 2012). A Figura 1 ilustra a hierarquia de um sistema espacial.

Figura 1: Hierarquia de um sistema espacial: Adaptado de ECSS, (2012)



Segmento Solo: É a Parte de um sistema espacial, localizado no solo, que monitora e controla os elementos do segmento espacial.
Segmento Espacial: É a Parte de um sistema espacial, colocada no espaço, para cumprir os objetivos da missão espacial.
Segmento Lançador: É a parte de um sistema espacial que é usada para transportar elementos para o espaço.

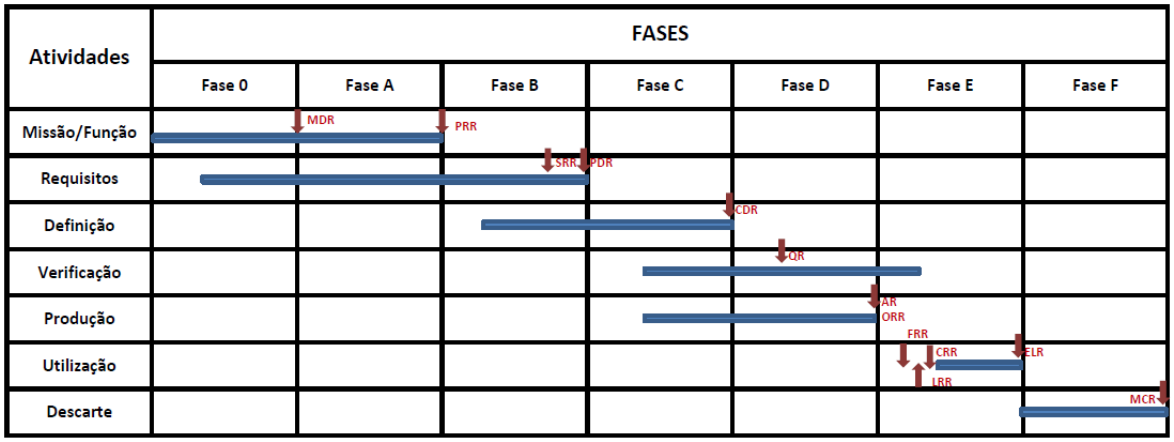
2.2 Projetos Espaciais

Segundo a ECCS, o planejamento e implementação do projeto engloba todos os processos realizados para planejar e executar um projeto espacial desde a iniciação até a conclusão, em todos os níveis da cadeia, recebendo insumos de todas as disciplinas e envolvendo cooperação próxima entre os domínios do projeto. (ECSS, 2009b). O ciclo de vida de projetos espaciais, proposto pela ECSS, apresentado na Figura 2, é tipicamente dividido em 7 fases:

- Fase 0 - Análise da missão / identificação de necessidades;
- Fase A - Viabilidade do Projeto;
- Fase B - Definição Preliminar;
- Fase C - Definição Detalhada;
- Fase D - Qualificação e Produção;
- Fase E - Operações;

- Fase F - Descarte.

Figura 2: Ciclo de vida de um projeto/ produto espacial: Adaptado de ESA, (2009)



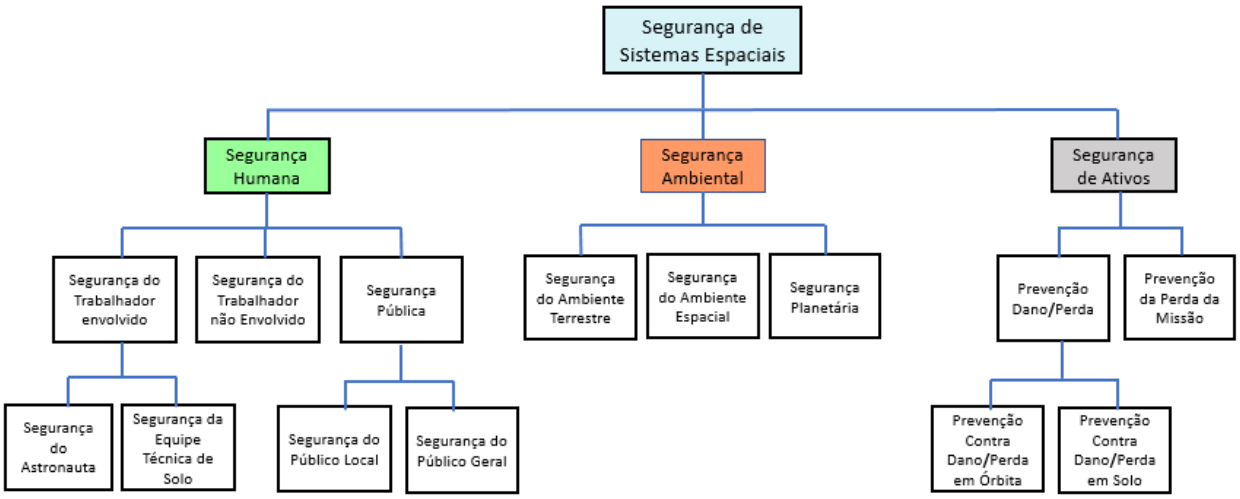
O padrão ECSS ainda determina que as Fases 0, A e B são focadas principalmente na elaboração de requisitos funcionais e técnicos do sistema e identificação dos conceitos do sistema para cumprir a declaração da missão, tendo em conta as restrições técnicas e programáticas identificados, a identificação de todas as atividades e recursos a serem usados para desenvolver segmentos espaciais e segmento solo do projeto, as avaliações iniciais de risco técnico e programático, e o início de atividades de pré-desenvolvimento. As Fases C e D compreendem todas as atividades a serem executadas para desenvolver e qualificar o segmento espacial e segmento solo e seus produtos. A Fase E compreende todas as atividades a serem executadas para lançamento, comissionamento, utilizar e manter os elementos orbitais do segmento espacial e utilizar e manter o segmento solo associado. A Fase F compreende todas as atividades a serem executadas para eliminar com segurança produtos lançados no espaço, bem como segmento solo. (ECSS, 2009b)

2.3 Segurança em projetos espaciais

A segurança é uma parte integrante de todas as atividades de engenharia e garantia de produto de um projeto. O sucesso de todos os trabalhos relacionados à engenharia de segurança deve basear-se na garantia de que o sistema seja projetado, qualificado, fabricado e operado de acordo com os requisitos de garantia do produto. (ISO, 2018)

Segundo a MIL-STD-882D, a segurança é estar livre daquelas condições que podem causar danos ou perda de equipamento ou propriedade, ou danos ao meio ambiente, incluindo danos a vida humana, ou seja, de trabalhadores direto e indiretamente envolvidos nas interações do sistema, os trabalhadores não diretamente envolvidos com o sistema, bem como membros do público em geral (NASA, 2011), conforme apresentado na figura 3.

Figura 3 : Populações Impactadas dentro do escopo de segurança: Adaptado de NASA, (2011)



Segundo a NASA, a segurança do sistema é a aplicação de princípios, critérios e técnicas de engenharia e gerenciamento com o objetivo de otimizar a segurança dentro das limitações de eficácia operacional, tempo e custo em todas as fases do ciclo de vida do sistema (NASA, 2011).

Segundo a norma ECSS-Q-ST-40C o objetivo da garantia da segurança é garantir que todos os riscos de segurança associado ao projeto, desenvolvimento, produção e operação do produto espacial sejam adequadamente identificados, avaliados, minimizados, controlados e finalmente aceitos por meio da implementação de um programa para garantia da segurança. (ECSS, 2017)

Conforme padrões de projetos na área espacial, a gestão de riscos e as ações de garantia de segurança são fundamentais para o sucesso de projetos, principalmente no que tange ao cumprimento dos requisitos de missão, de prazo, de custo e de segurança de pessoas e infraestrutura.

2.4 Acidentes na área Espacial

Neste tópico serão apresentados alguns acidentes na área espacial em que houve perda de vida humana, demonstrando assim a importância das normas de segurança espacial assim como a necessidade de um programa de garantia da segurança bem eficaz.

2.4.1 Foguete VLS-1 v3

Em 2003 o Brasil entrou para a triste estatística de acidentes da área espacial envolvendo vítimas fatais, quando do trágico acidente ocorrido na base de lançamento de foguetes de Alcântara, no Maranhão, que causou a morte de 21 técnicos e engenheiros do DCTA (Departamento de Ciência e Tecnologia Aeroespacial) devido a um incêndio ocorrido no VLS – (Veículo Lançador de Satélites), por conta do acionamento intempestivo de um dos motores do primeiro estágio do foguete (WINTER, 2007; PALMERIO, 2016). O relatório oficial que avaliou as causas daquele acidente aponta que, caso as normas mínimas de segurança tivessem sido observadas, ou o acidente poderia ter sido evitado, ou ao menos não teria ceifado tantas vidas (MINISTERIO DA DEFESA, 2004).

2.4.2 Apollo 1

No dia 27 de Janeiro de 1967, houve um acidente na torre de lançamento no Cabo Canaveral durante um ensaio pré voo. Um incêndio no *cockpit* levou a morte de três astronautas durante o teste de sistemas e procedimentos operacionais na configuração de lançamento. A missão era para ter sido o primeiro voo tripulado da Apollo e estava com lançamento programado para 21 de fevereiro de 1967.

2.4.3 Challenger

Os sete astronautas que estavam a bordo do ônibus espacial Challenger morreram tragicamente na explosão que ocorreu durante o lançamento no Cabo Canaveral por volta das 11h40 do dia 28 de janeiro de 1986. A explosão ocorreu 73 segundos após o lançamento devido a uma falha no anel de vedação em um dos *boosters* do foguete de propelente sólido que incendiou o tanque de propelente líquido principal.

Garantir a segurança de um sistema espacial é uma atividade de extrema importância durante a fabricação de qualquer dispositivo que será colocado em órbita da Terra, incluindo seu meio de transporte (foguetes lançadores) e seus meios de operação/comunicação (estações terrenas, centros de controle), pois, caso um equipamento crítico para a segurança venha a falhar ou operar fora das especificações, poderá causar acidentes levando inclusive a perdas de vidas de trabalhadores. (Genaro, 2019)

2.5 Gestão de riscos

Os riscos são uma ameaça ao sucesso do projeto porque têm efeitos negativos no custo, cronograma e desempenho técnico do projeto, mas as práticas apropriadas de controle de riscos também podem apresentar novas oportunidades com impacto positivo. (ISO, 2018)

Segundo o padrão ECSS-M-ST-80C o objetivo do gerenciamento de riscos do projeto é identificar, avaliar, reduzir, aceitar e controlar os riscos do projeto espacial de maneira sistemática, proativa, abrangente e econômica, levando em consideração as restrições técnicas e programáticas do projeto. (ECSS, 2008)

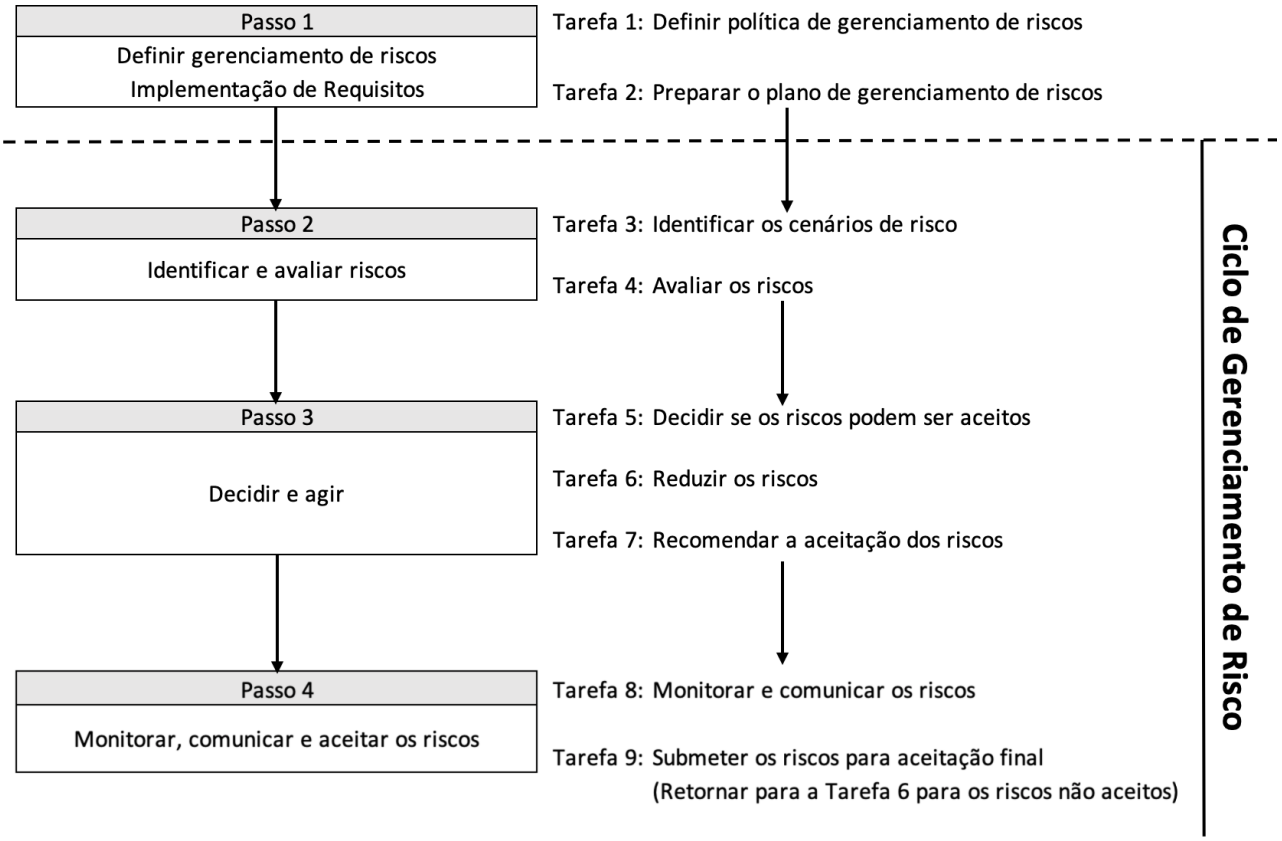
O *Project Management Body of Knowledge* (PMBOK) define que a gestão dos riscos de um projeto inclui a identificação, análise, planejamento de resposta e controle do risco, na seguinte ordem de processos a saber:

1. Planejar o gerenciamento de riscos
2. Identificar Riscos
3. Realizar Análise qualitativa de risco
4. Realizar análise quantitativa de risco
5. Planejar resposta ao risco
6. Controle dos Riscos

Ainda de acordo com o PMBOK, o processo de planejar o gerenciamento de risco deve obter como saída a categorização dos riscos do projeto onde busca-se agrupar as possíveis causas de risco em categorias, além de uma lista de riscos identificados onde esses são descritos com tantos detalhes quanto razoáveis.

Os riscos para o projeto podem ser categorizados por fontes de risco, a área do projeto afetada ou outras categorias, os riscos também podem ser categorizados por causas básicas comuns. Esta técnica ajuda determinar pacotes de trabalho, atividades, fases do projeto ou mesmo funções no projeto, o que pode levar ao desenvolvimento de respostas de risco efetivas, conforme apresentada na Figura 4.

Figura 4: Tarefas associadas às etapas do processo de gerenciamento de riscos dentro do ciclo de gerenciamento de riscos: [Adaptado de PMBOK, 2013]



A NASA define que o risco é o potencial para deficiências de desempenho que podem estar relacionadas a qualquer um ou mais dos seguintes domínios de execução de missão: Segurança, técnico, custo e cronograma. A abordagem de Gestão de Risco é aplicada em situações em que os valores fundamentais da NASA nos domínios de segurança e realização técnica devem ser equilibrados com as realidades programáticas nos domínios de cronograma e custo.

2.5.1 Gestão de Riscos de Safety

O risco de segurança (por vezes referido como "risco de desempenho de segurança") é o potencial para deficiências em relação aos requisitos de desempenho de segurança. O risco de segurança só surge na medida em que existe incerteza se o desempenho de segurança do sistema atende aos requisitos (NASA, 2014).

A ECSS, (2017) cita que o objetivo da garantia de segurança é certificar que todos os riscos de segurança associados ao projeto, desenvolvimento, produção e operações do produto espacial sejam adequadamente identificados, avaliados, minimizados, controlados e finalmente aceitos por meio da implementação de um programa de garantia de segurança. A identificação, redução e controle de riscos de segurança devem fazer parte do processo de gerenciamento de riscos do projeto e deve ser um processo contínuo e interativo durante todo o ciclo de vida do projeto, englobando as seguintes atividades:

1. atribuição de requisitos de segurança;
2. identificação de risco e segurança;
3. avaliação (incluindo categorização) da gravidade da consequência;
4. redução e controle do risco de segurança;
5. encerramento e aceitação de risco residual.

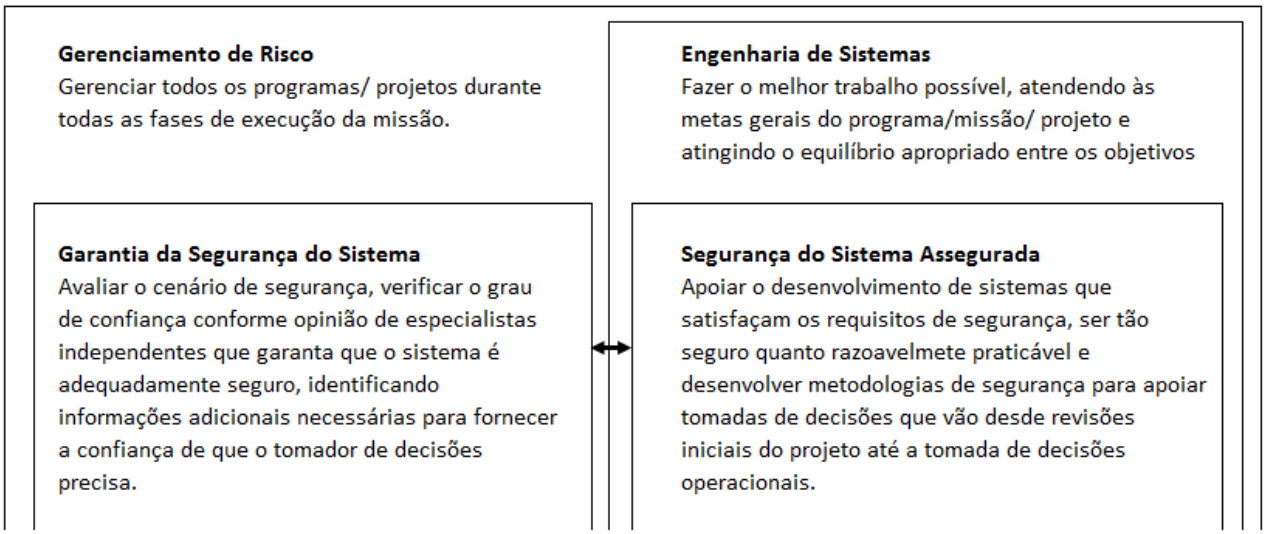
De acordo com (ECSS, 2017) a avaliação do risco de segurança deve ser iniciada no início do projeto e executada em etapas progressivas durante a implementação do programa de segurança e deve:

1. compreender a identificação, classificação e classificação dos riscos de segurança e seus contribuintes;
2. basear-se na análise determinística dos riscos, combinando a gravidade das consequências e a probabilidade de ocorrência das consequências;
3. ser usado para facilitar a redução e controle efetivo e eficiente de riscos de segurança;
4. apoiar a gestão de riscos do projeto, conforme definido na ECSS-M-ST-80;
5. avaliar a conformidade com metas de segurança probabilísticas.

2.6 Relação entre Engenharia de Sistemas, Garantia da segurança e Gestão de risco.

A NASA em seu *Systems Safety Handbook* possui uma abordagem de segurança que reconhece a substancial sobreposição entre engenharia de sistemas, gerenciamento de riscos e segurança do sistema. Gestão de riscos e engenharia de sistemas se preocupam com a realização de objetivos definidos. De um modo geral, a engenharia de sistemas é o modo pelo qual os objetivos são alcançados, assim como o papel da gestão de risco é o de fornecer uma função de controle para a engenharia de sistemas de forma a assegurar que o desenvolvimento esteja no caminho certo, em todos os domínios de execução da missão (NASA, 2014). Essa relação está ilustrada na Figura 5.

Figura 5: Relação entre gerenciamento de riscos, engenharia de sistemas e segurança de sistemas em um projeto: Adaptado de NASA, (2014)



A segurança do sistema é uma entrada para a engenharia de sistemas e gerenciamento de riscos. Considerando que o desempenho de segurança de um sistema é uma preocupação das partes interessadas, da mesma forma que o desempenho técnico, são preocupações das partes interessadas, a segurança de sistemas é

parte integrante dos esforços de engenharia de sistemas para desenvolver um sistema que satisfaça os objetivos das partes interessadas. através dos domínios de segurança, técnico, custo e cronograma A garantia de segurança do sistema é uma atividade de avaliação que mantém a independência funcional da engenharia de sistemas para ser mais eficaz no fornecimento de confiança de que o sistema é de fato adequadamente seguro. (NASA, 2014)

3. Discussão

Os acidentes apresentados na seção 2.4 nos mostram a importância que um programa de garantia de segurança tem dentro de uma organização da área espacial para garantir que não haja nenhum tipo de dano que leve a comprometer a missão ou o projeto.

No sentido de que a gestão de risco busca identificar e tratar os riscos de forma que eles não se tornem uma ameaça ao sucesso do projeto, fica evidente que se os riscos de safety não forem considerados na gestão de riscos do projeto, acidentes podem acontecer danificando instalações e recursos físicos ou até mesmo levar a perda de vida humana. Caso qualquer um desses danos ocorram, consequentemente podem causar um prejuízo em qualquer domínio de um projeto, seja ele domínio técnico, desempenho, custo ou cronograma.

Sendo assim, na fase de identificação dos potenciais riscos de um projeto espacial os riscos relacionados à segurança também devem ser levantados e analisados como uma categoria de riscos a ser trabalhada. Uma vez identificados os riscos de segurança, programam-se ações que objetivam minimizar tais riscos de forma efetiva, em termos técnicos e de custo.

4. Conclusão

O presente trabalho apresentou uma visão sobre a importância da garantia da segurança em projetos espaciais e a relação existente entre garantia de segurança e gestão de risco Observou-se, existir grande intersecção entre a gestão de riscos e a garantia de segurança, principalmente pelo fato de que os riscos que afetam a segurança, como acima definidos, constituem-se em um subgrupo dos riscos que ameaçam o sucesso do projeto como um todo. Sendo assim para obter uma gestão de risco efetiva em projetos espaciais é imprescindível haver um programa de safety bem definido.

5. REFERÊNCIAS

DEPARTMENT OF DEFENSE STANDARD PRACTICE FOR SYSTEM SAFETY- MIL-STD-882D. 10 February 2000.

EUROPEAN COOPERATION FOR SPACE STANDARDIZATION - ECSS. Glossary of terms. (ECSS-S-ST-00-01C) - Noordwijk, The Netherlands. 2012. 63 p.

EUROPEAN COOPERATION FOR SPACE STANDARDIZATION - ECSS. Space Management – Risk Management. (ECSS-M-ST-80C). Noordwijk, The Netherlands. 2008a.

EUROPEAN COOPERATION FOR SPACE STANDARDIZATION – ECSS Space Product Assurance – Safety. (ECSS-Q-ST-40C) Noordwijk, The Netherlands: *ESA Requirements & Standards Division*, 2017.

EUROPEAN COOPERATION FOR SPACE STANDARDIZATION – ECSS. Space Project Management, project planning and implementation. (ECSS-MST-10C) - Noordwijk, The Netherlands. 2009b. 50 p

GENARO, A. F. S. Levantamento e implementação de requisitos de segurança de sistemas espaciais durante o ciclo de vida de projetos de satélites, São Paulo, 2019.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO 14620-1:2018 Space Systems – Safety Requirements – Part 1: Systems Safety. Switzerland. 2018.

MINISTÉRIO DA DEFESA. Relatório de Investigação do acidente ocorrido com o VLS-1 V03, em 22 de agosto de 2003, em Alcântara, Maranhão. Brasília, 2004.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION. NASA System Safety Handbook – Volume 1 – System Safety Framework and Concepts for Implementation. Washington DC. 2011. 120 p.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION. NASA System Safety Handbook – Volume 2 – System Safety Concepts Guidelines and Implementation Examples. Washington DC. 2014. 216 p.

PALMERIO, A. F. Introdução à tecnologia de foguetes. 2ª Edição. São José dos Campos, São Paulo, SindCT, 2016. 304 p.

PROJECT MANAGEMENT INSTITUTE. Um Guia do Conjunto de Conhecimento em Gerenciamento de Projetos (Guia PMBOK), 2013. 5a edição. Four Campus Boulevard, 2013.

WINTER, O. C.; Prado, A. F. B. A. A conquista do espaço: do Sputinik à Missão Centenário. São Paulo, Editora Livraria da Física, 2007.