UNIVERSIDADE FEDERAL DE SÃO PAULO

DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA

PROGRAMA DE MESTRADO PROFISSIONAL EM INOVAÇÃO TECNOLÓGICA

MITIGAÇÃO DE RISCOS DE EXPERIMENTOS CIENTÍFICOS EMBARCADOS EM FOGUETES SUBORBITAIS

HEULLER ALOYS CARNEIRO PROCÓPIO

ORIENTADOR: PROF. DR. LUIZ EDUARDO GALVÃO MARTINS

COORIENTADOR: PROF. DR. CARLOS HENRIQUE NETTO LAHOZ

São José dos Campos - SP
Abril/2022

UNIVERSIDADE FEDERAL DE SÃO PAULO

DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA

PROGRAMA DE MESTRADO PROFISSIONAL EM INOVAÇÃO TECNOLÓGICA

MITIGAÇÃO DE RISCOS DE EXPERIMENTOS CIENTÍFICOS EMBARCADOS EM CARGAS ÚTEIS EM FOGUETES SUBORBITAIS

HEULLER ALOYS CARNEIRO PROCÓPIO

Dissertação apresentada ao Programa de Pós-Graduação Profissional em Inovação Tecnológica da Universidade Federal de São Paulo, como parte dos requisitos para a obtenção do título de Mestre em Inovação Tecnológica, área de concentração: Inovação Tecnológica.
Orientador: Dr. Luiz Eduardo Galvão Martins

São José dos Campos - SP
Abril/2022

Carneiro Procópio, Heuller Aloys
MITIGAÇÃO DE RISCOS DE EXPERIMENTOS CIENTÍFICOS EMBARCADOS EM CARGAS ÚTEIS EM FOGUETES SUBORBITAIS / Heuller Aloys Carneiro Procópio
Orientador(a) Luiz Eduardo Galvão Martins; Coorientador(a) Carlos Henrique Netto Lahoz. - São José dos Campos, 202.
308 p.

Dissertação (Mestrado - Programa de Pós-Graduação em Mestrado Profissional Interdisciplinar em Inovação Tecnológica) - Universidade Federal de São Paulo - Instituto de Ciência e Tecnologia, 202.

1. Requisitos. 2. Cargas Úteis espaciais. 3. Foguetes espaciais. 4. System-Theoretic Process Analysis - STPA. 5. SysML. I. Galvão Martins, Luiz Eduardo, orientador(a). II. Netto Lahoz, Carlos Henrique, coorientador(a). III. , coorientador(a). III. Título.

UNIVERSIDADE FEDERAL DE SÃO PAULO

DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA

PROGRAMA DE MESTRADO PROFISSIONAL EM INOVAÇÃO TECNOLÓGICA

MITIGAÇÃO DE RISCOS DE EXPERIMENTOS CIENTÍFICOS EMBARCADOS EM CARGAS ÚTEIS EM FOGUETES SUBORBITAIS

HEULLER ALOYS CARNEIRO PROCÓPIO

Dissertação apresentada ao Programa de Pós-Graduação Profissional em Inovação Tecnológica da Universidade Federal de São Paulo, como parte dos requisitos para a obtenção do título de Mestre em Inovação Tecnológica, área de concentração: Inovação Tecnológica.

Aprovado em __ de _____ de 2022

Membros da Banca:

Prof. Dr. Johnny Cardoso Marques

(Membro Titular – IEC-ITA)

Dr. Leonardo Ramos Rodrigues

(Membro Titular – Instituto de Aeronáutica e Espaço)

Prof. Dr. Elbert Einstein Nehrer Macau

(Membro Titular – DCT-Unifesp)

São José dos Campos - SP
Abril/2022

Dedico essa dissertação de mestrado à Deus, que iluminou minha mente e possibilitou esta oportunidade, aos meus pais, Luiz e Zeli, minha esposa, Nizia, e meu filho, Davi, por imenso apoio em todas as horas.

AGRADECIMENTOS

Aos meus orientadores Dr. Luiz Eduardo Galvão Martins e Dr. Carlos Henrique Netto Lahoz por toda atenção e paciência recebidas.

A todos os amigos do Instituto de Aeronáutica e Espaço por todo apoio, trocas de informações e produtivas discussões, em especial aos amigos Marco Rizol, Valdir Sebastião (em memória), Allison Maia, Ricardo Franco e Rodrigo Brosler.

Ao Instituto de Aeronáutica e Espaço e Agência Espacial Brasileira por todo suporte e investimento nos projetos de microgravidade.

Aos meus pais, Luiz Procópio e Zeli Procópio, por todo apoio e suporte em minha formação tanto pessoal quanto acadêmica. Muito do que sou e conquistei é devido a dedicação deles.

À minha esposa Nízia Mensch e filho Davi Procópio pelo apoio e carinho em toda essa jornada acadêmica. Graças a este apoio foi possível que eu reunisse forças para concluir este trabalho.

A perfeição não é alcançada quando já não há mais nada para adicionar, mas quando já não há mais nada que se possa retirar

Antoine de Saint Exupery, Airman's Odyssey

RESUMO

Os voos espaciais oferecem riscos devido as condições ambientais extremas, além do alto grau de complexidade da construção e operação dos foguetes, sistemas e subsistemas. Há também, os riscos pessoais e materiais que são devidos a operação de lançamento de foguetes. Os custos para a execução destes projetos, seus respectivos ensaios, operação de lançamento e eventual resgate de carga útil, quando aplicável, também precisam ser considerados. No Brasil, a Agência Espacial Brasileira (AEB) oferece à comunidade científica nacional oportunidades de acesso ao espaço para que se realizem experimentos em ambiente de microgravidade, através de lançamento de foguetes suborbitais. Dado que a cadência de lançamentos deste tipo é baixa, as falhas de experimentos embarcados causam atrasos significativos para as pesquisas que dependem destas oportunidades. Este trabalho propõe aplicar a técnica STPA (*System-Theoretic Process Analysis*), um método de abordagem sistêmica para a análise de segurança do sistema dos experimentos científicos embarcados em cargas úteis espaciais em foguetes suborbitais. Esta técnica é baseada na metodologia STAMP (*System-Theoretic Accident Model and Processes*), a qual faz uma análise de risco preditiva. A aplicação desta metodologia visa a obtenção de restrições de segurança, recomendações e orientações que, por sua vez, contribuam para a elaboração de um conjunto de requisitos aplicáveis a experimentos científicos embarcados em cargas úteis espaciais de foguetes suborbitais. O resultado principal deste trabalho é um conjunto de requisitos de segurança predefinido em forma de *template*, aplicável a experimentos científicos espaciais. Este resultado será disponibilizado aos experimentadores científicos para sua aplicação desde a fase de concepção de seus experimentos. Este conjunto de requisitos será modelado utilizando a abordagem SysML (*Systems Modeling Language*), será então, avaliado através de um corpo técnico. Na sequência será realizado um estudo de caso com o propósito de avaliar a aplicação do conjunto de requisitos em um experimento. Este conjunto de requisitos tem como objetivo final contribuir para a garantia do sucesso da missão dos experimentos e da carga útil.

Palavras-chave: STPA, STAMP, carga útil, foguete suborbital, requisitos de segurança, avaliação.

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 related to the rocket launch operation. The costs for the execution of these projects and their respective tests, launch operation and eventual payload recovery, should also be taken into account. The Brazilian Space Agency (AEB) offers to the national scientific community opportunities to access space to carry out experiments in a microgravity environment, by suborbital rocket launchings. Given that, the rate of launches of this type of launchings is low, the failures of payload items causes significant delays for research that depends on these opportunities. This work proposes to apply the STPA (System-Theoretic Process Analysis) technique, a systemic approach method for the safety analysis of the system of scientific experiments onboard in space payloads in suborbital rockets. This technique is based on the STAMP (System-Theoretic Accident Model and Processes) methodology, which performs a predictive risk analysis. The application of this methodology aims to obtain safety restrictions, recommendations and guidelines, that contributes to the development of a set of requirements applicable to scientific experiments onboard on suborbital rocket space payloads. The main result of this work is a set of predefined safety requirements in template form, applicable to space science experiments. This set of requirements will be modeled using the SysML (Systems Modeling Language) approach, then evaluated by a body of specialists. Next, a case study will be performed with the purpose of evaluating the application of the set of requirements in an experiment. This set of requirements has a goal of contributing to ensure the success of experiments and payload missions.

Keywords: *STPA, STAMP, payload, suborbital rocket, safety requirements, evaluation.*

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

AEB – Agência Espacial Brasileira

CA – *Control Action*

CapSA – *Capability Safety Assessment*

CAST – *Causal Analysis based on Systems Theory*

CG – Centro de Gravidade

CLA – Centro de Lançamento de Alcântara

CLBI – Centro de Lançamento da Barreira do Inferno

COMGAR – Comando Geral de Operações Aéreas

DCTA – Departamento de Ciência e Tecnologia Aeroespacial.

DLR – *Deutsches zentrum für Luft-und Raumfahrt* (Centro Aeroespacial Alemão)

EGSE – *Electrical Ground Support Equipment*

ESMD – *Exploration Systems Mission Directorate*

FAB – Força Aérea Brasileira

FB – *Feedback*

FMEA – *Failure Mode and Effect Analysis*

FMECA – *Failure Mode, Effect, and Criticality Analysis*

FTA – *Fault Tree Analysis*

GPM – *Global Precipitation Measurement*

H – *Hazard*

HTV – H-II *Transfer Vehicle*

IAE – Instituto de Aeronáutica e Espaço

INPE – Instituto Nacional de Pesquisas Espaciais

ISS – *International Space Station*

JAMSS –*Japan Manned Space Systems Corporation*

JAXA – *Japanese Aerospace Exploration Agency*

JPL – *Jet Propulsion Laboratory*

L – *Lost*

LO – *Lift Off* (Decolagem)

MBSE – *Model-Based Systems Engineering*

MR – Módulo de Recuperação

MS – Módulo de Serviços

NASA – *National Aeronautics and Space Administration*

PHA – *Process Hazard Analysis*

PRA – *Probabilistic Hazard Analysis*

PSASS – *Partnership for Systems Approaches to Safety and Security*

R – *Responsability*

REs – Redes Elétricas

RSL – Revisão Sistemática da Literatura

SC – *Safety Constraint*

SMA – Sensor Mecânico Acelerométrico

STAMP – *System-Theoretic Accident Model and Processes*

STECA – *System-Theoretic Early Concept Analysis*

STPA – *System-Theoretic Process Analysis*

UCA – *Unsafe Control Action*

UML – *Unified Modeling Language*

μG – Microgravidade

VS-30 – Veículo de Sondagem – 30

VSB-30 – Veículo de Sondagem *Booster* – 30

V&V – Verificação e Validação

SUMÁRIO

Capítulo 1

INTRODUÇÃO

Neste capítulo é descrito o contexto da pesquisa apontando a relevância do assunto, seguido de seus objetivos a serem alcançados e como o texto está organizado.

1.1 Contextualização

Ao longo do período da exploração espacial, a comunidade científica tem se utilizado de foguetes suborbitais, satélites e, mais recentemente, a estação espacial internacional (ISS – *International Space Station*) para realizar experimentos em ambiente de microgravidade. Ao contrário do que o termo microgravidade sugere, a atração gravitacional ainda está presente neste ambiente; entretanto, este é o único fenômeno atuando sobre o corpo e a sensação de ausência de peso é fruto da ausência da força Normal. O ambiente de microgravidade é criado quando a soma de todas as forças, com exceção da gravidade, atuantes no corpo são nulas ou fortemente reduzidas. (PALMERIO, 2017, p. 55-57). Há diversas formas de se produzir este ambiente, através do emprego dos provedores de microgravidade, conforme apresentado na Tabela 1 pelo autor Plester (2004, p. 2).

As principais diferenças entre os provedores de microgravidade, dizem respeito ao tempo ininterrupto sob a condição em microgravidade e seus respectivos custos. Cada experimento demanda um tempo mínimo de exposição ao ambiente de microgravidade e este que determinará qual o provedor a ser utilizado.

Tabela 1 Características dos provedores de microgravidade.

Provedor de microgravidade	Nível de µG	Tempo de duração	Volume (m^3)	Intervenção Humana	Tempo de preparação
Torres de queda livre	10^{-3} a 10^{-6}	< 5 s	< 1	Indireta	Semanas
Voos parabólicos com aeronaves	10^{-2} a 10^{-3}	20 a 25 s	>10	Direta	Meses
Foguetes suborbitais	10^{-4} a 10^{-5}	5 a 13 min	< 1	Indireta	1 ano
Plataformas orbitais automatizadas (satélites)	Apx. 10^{-5}	Semanas a meses	> 1	Indireta	Anos
Plataformas orbitais tripuladas	10^{-2} a 10^{-5}	Semanas a anos	> 1	Direta	Anos

Fonte: Plester (2004 p. 2)

É possível verificar, na Tabela **1**, que há dois provedores em que a microgravidade é obtida sem a necessidade de se sair da atmosfera terrestre: torres de queda livre e voos parabólicos com aeronaves. Enquanto os demais provedores necessariamente devem sair da atmosfera terrestre e acessar o espaço, sendo estes: foguetes suborbitais, plataformas orbitais automatizadas (satélites) e plataformas orbitais tripuladas.

Os provedores que impulsionam suas cargas úteis até o espaço, elevam-na a altitude de pelo menos 100 km. Não existe uma definição precisa de onde começa o espaço, mas para os especialistas na área de foguetes, o espaço começa a partir dos 100 km de altitude. Para todos os efeitos práticos, admite-se como espaço a área em que as distâncias entre as moléculas e átomos que compõem a atmosfera são tão grandes e a sua resistência ao deslocamento é tão pequena, que é considerada a existência de vácuo (ausência de matéria). A partir desta altitude os sistemas da carga útil podem anular ou reduzir todas as forças que atuam em seu corpo, com exceção da gravidade. (PALMERIO, 2017, p. 42).

Há décadas, a comunidade científica brasileira lança experimentos científicos ao espaço. Em sua grande maioria são lançados a bordo de cargas úteis espaciais, as quais são impulsionadas por foguetes que propiciam voos espaciais suborbitais. Estas oportunidades são fomentadas pela Agência Espacial Brasileira (Experimentos Suborbitais de Microgravidade, 2008) e estão previstas no Programa Nacional de Atividades Espaciais (PNAE), 2012-2021. Devido aos custos e a 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 se lançar os experimentos devem ser bem utilizadas. Para isso, além de se tomar todas as ações para o sucesso dos dispositivos envolvidos, bem como, toda a operação de lançamento, deve-se também mitigar as falhas potenciais relativas aos experimentos propostos pela comunidade técnico-científica.

Para contribuir com o sucesso da missão de lançamento, os requisitos dos experimentos embarcados precisam ser concebidos e projetados atendendo as orientações dos especialistas da área. Os experimentadores enviam as propostas à AEB, a qual seleciona as propostas, prioriza os lançamentos, financia os experimentos e após a fase de 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. É comum, entretanto, que algumas destas necessidades sejam incompatíveis com o voo, infraestruturas do campo de lançamento ou do IAE, estas informações apenas são levantadas no decorrer do desenvolvimento do projeto.

Atualmente, os proponentes recebem informações durante um seminário, então, redigem documentações relativas aos seus experimentos e a enviam à AEB. A AEB usualmente convida especialistas do Instituto de Aeronáutica e Espaço (IAE), do Instituto Nacional de Pesquisas Espaciais (INPE) e de algumas outras instituições, que possam a vir ser necessários a fim de avaliar a viabilidade do experimento. Após estas análises, as informações geradas são enviadas aos proponentes e, então, se inicia a fase de projeto dos experimentos. Durante esta fase, os especialistas do IAE são frequentemente consultados para revisões de projeto e detalhamento das necessidades do experimento. Não é incomum, entretanto, que algumas destas necessidades sejam incompatíveis com o voo, infraestruturas do campo de lançamento ou do IAE, porém estas informações são levantadas apenas no decorrer do projeto.

A identificação das necessidades é realizada por meio da interação entre especialistas do IAE e pesquisadores das universidades. Entretanto, dada a sua subjetividade, constatou-se na prática que é necessário investir na melhoria deste processo.

Este trabalho aplica a técnica STPA (*System-Theoretic Process Analysis*) de Leveson e Thomas (2018), baseada na abordagem STAMP (*System-Theoretic*

Accident Model and Processes) de Leveson (2012), para analisar experimentos científicos embarcados e suas interfaces em cargas úteis espaciais em foguetes suborbitais. Com o uso desta técnica foram obtidas restrições de segurança, que por sua vez contribuíram com a elaboração de um conjunto de requisitos e recomendações de segurança relacionados a experimentos científicos e cargas úteis suborbitais.

Com a identificação dos requisitos de segurança, foi desenvolvido um modelo SysML dos requisitos funcionais e não funcionais. Os requisitos foram classificados e ordenados conforme a responsabilidade e assunto. Este conjunto de requisitos foi submetido a um processo de avaliação por um corpo de especialistas através de um conjunto de questionários.

1.2 Objetivos

O objetivo principal deste trabalho é identificar um conjunto de requisitos, apresentados em forma de *template*, relacionado a experimentos científicos e cargas úteis espaciais. Ao longo desta identificação emergem recomendações de segurança, entretanto não são obrigatórias para o usuário final. Este conjunto de requisitos será disponibilizado aos experimentadores científicos para sua aplicação desde a fase de concepção de seus experimentos. Por sua vez, este conjunto de requisitos visa contribuir para o sucesso da missão dos experimentos e da carga útil.

A identificação dos requisitos, e em segundo plano recomendações, de segurança são baseadas em restrições de segurança, estas fazem parte do desenvolvimento do trabalho. As recomendações de segurança são, em grande parte, ligadas ao projeto, e emergem durante a identificação de requisitos, mas não tem a mesma obrigatoriedade.

Durante o processo de identificação das restrições, requisitos e recomendações de segurança, aplicáveis a experimentos científicos e cargas úteis suborbitais, será estabelecido um modelo deste processo. Este poderá ser utilizado como base em novas identificações de restrições, requisitos, recomendações de segurança e em

análises de experimentos embarcados em e cargas úteis similares. A definição deste processo é um resultado secundário.

1.3 Organização do Texto

Este trabalho de pesquisa está estruturado em 8 capítulos conforme segue:

- **Capítulo 2:** é relacionado à revisão da literatura e discussões detalhadas de tópicos relevantes.
- **Capítulo 3:** é relacionado à metodologia proposta utilizada para a condução deste trabalho.
- **Capítulo 4:** descreve a identificação das restrições de segurança utilizando-se da técnica STPA.
- **Capítulo 5:** descreve a identificação dos requisitos e recomendações de segurança modelados em SysML.
- **Capítulo 6:** descreve a avaliação dos requisitos de segurança por parte do corpo de especialistas.
- **Capítulo 7:** apresenta um estudo de caso na aplicação do grupo de requisitos de segurança.
- **Capítulo 8:** apresenta a conclusão da pesquisa, contribuições e futuras perspectivas.

Capítulo 2

REVISÃO BIBLIOGRÁFICA

Neste capítulo estão descritos a fundamentação teórica a fim de explanar os principais conceitos utilizados nesta pesquisa.

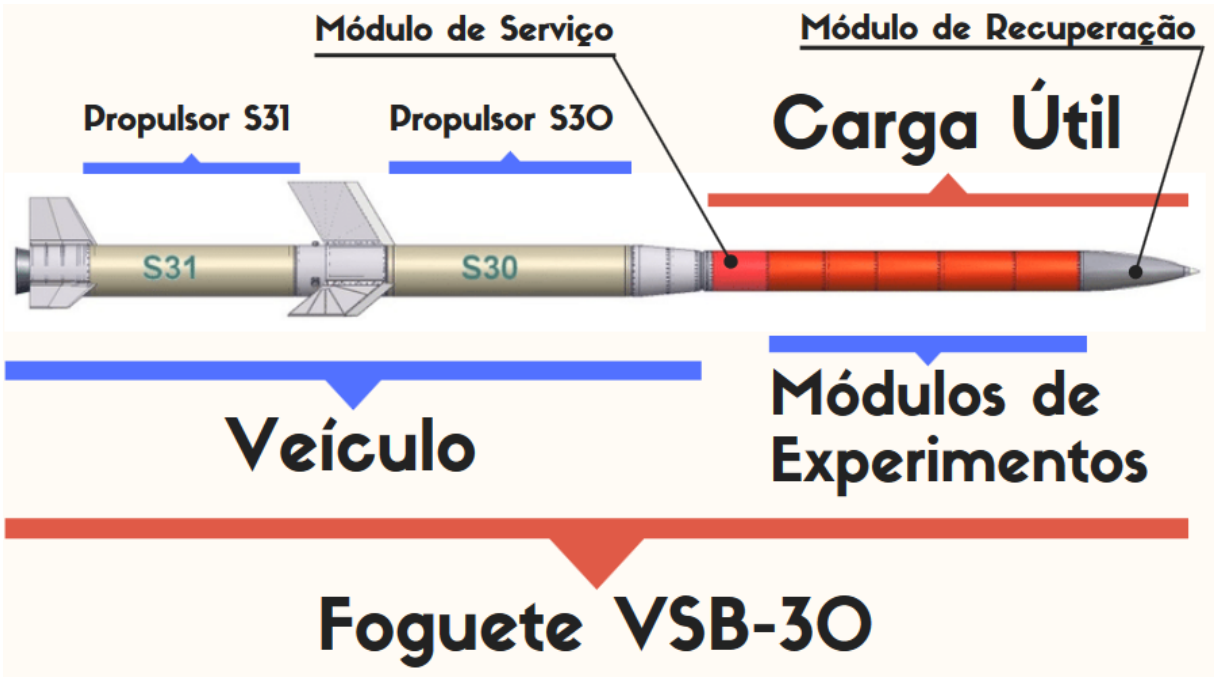
2.1 Fundamentação Teórica

Esta seção tem como objetivo definir e explanar os principais conceitos utilizados nesta pesquisa, como foguetes, cargas úteis, experimentos científicos, missões de lançamento, histórico de falhas, STPA e SysML.

2.1.1 O Foguete e Suas Partes Integrantes

A Figura 1 apresenta o foguete VSB-30 e suas partes integrantes. O foguete VSB-30 pode ser dividido em veículo e carga útil. O veículo contém dois propulsores, o S30 e o S31, os quais provêm o empuxo que impulsiona a carga útil ao espaço, dois módulos porta empenas que contribuem com a estabilização do voo e módulos que comandam os propulsores e os demais serviços do veículo. A carga útil conta com o módulo de serviço, módulo de recuperação, os quais fornecem os serviços aos experimentos científicos e os módulos de experimentos, onde os experimentos científicos são integrados. Uma carga útil pode conter módulos adicionais para prover todos os serviços necessários aos experimentos, como por exemplo, ocorre no caso do VSB-30. Algumas informações não foram explanadas por não serem necessárias para a discussão neste trabalho.

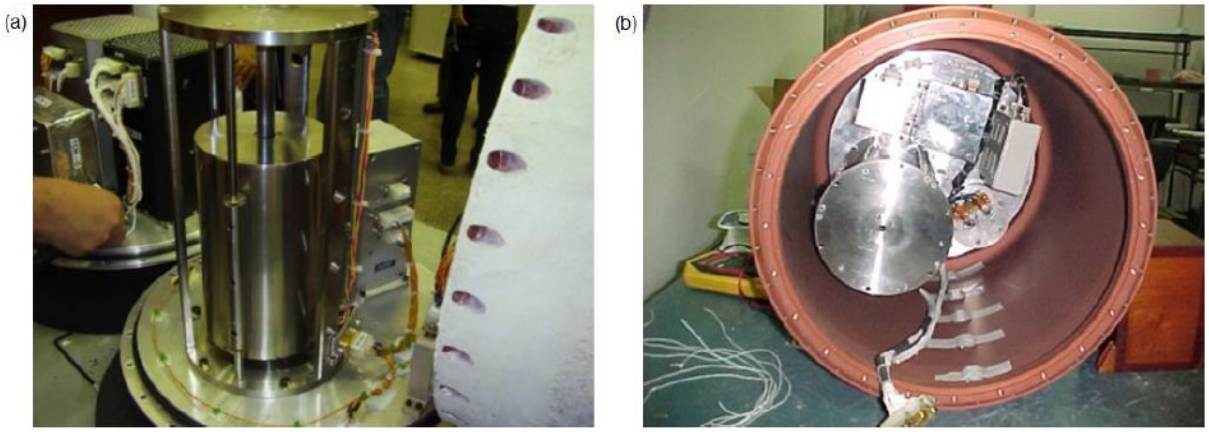
Figura 1 Foguete VSB-30 e suas partes integrantes.



Fonte: Modificado a partir de Lucca (2014, p. 5).

A Figura 2 mostra um experimento integrado a um módulo de experimentos. Este experimento foi desenvolvido no INPE com o propósito de fundir amostras metálicas em solo e solidificá-las em ambiente de microgravidade através de seu resfriamento (TENÓRIO *et al.*, 2019). Para seu funcionamento, este experimento exige que sua integração seja em módulo hermético, o qual é composto por duas tampas que em conjunto com anéis de vedação provêm um ambiente hermético.

Figura 2 (a) experimento integrado na tampa do módulo; (b) experimento integrado no módulo hermético.



Fonte: Tenório *et al.* (2019)

2.1.2 Definições

Para o entendimento do trabalho é importante definir alguns dos termos e conceitos usados na área espacial. Eles são explanados a seguir:

Acesso tardio: Termo utilizado para definir experimentos científicos que inserem suas amostras na carga útil horas antes do voo. As amostras são usualmente acondicionadas em invólucros herméticos e integradas em módulos não herméticos.
Amostras sensíveis: Amostras que se degradam com 3 ou menos ativações, ou cuja amostra tenha tempo viável inferior a 48h.
BCO: Responsável pelo Banco de Controle. Tem como função controlar as atividades dos operadores de EGSEs, bem como de informar aos responsáveis pelo foguete e segurança do campo.
Campo de lançamento: No Brasil há dois campos de lançamentos: o CLA, e CLBI. Entretanto os foguetes VSB-30 e VS-30, bem como seus derivados como VS-30/IO e VS-31/IO, também são lançados em *Esrange Space Center*, localizado na Suécia, *Andøya Space Center* na Noruega e *Woomera* na Austrália.
Carga útil: Neste trabalho refere-se ao conjunto de experimentos embarcados e o conjunto de módulos onde estão instalados, módulo de serviços e módulo de recuperação. A carga útil é a razão pela qual o foguete é lançado.
Casamata: Posto avançado próximo ao lançador (distância de aproximadamente 100 m) onde os sistemas do foguete são operados, neste local os EGSEs e equipes ficam fisicamente alocados. Este local é protegido contra impactos e possui sistemas de ventilação próprios.
Classificação dos experimentos científicos típicos e suas requisições de serviços:
A Tabela 2 apresenta tipos de experimentos típicos em relação aos serviços que demandam.
Exemplo de EX-1: Experimento com amostras biológicas, com aquisições de dados ambientais e enviadas por telemetria.
Exemplo de EX-2: Experimento para análise de comportamento de trocadores de calor durante a microgravidade.
Exemplo de EX-3: Experimento para análise de acelerações, choques e dinâmica de voo.

Exemplo de EX-4: Protótipos de desenvolvimento de novos equipamentos embarcados.

Exemplo de EX-5: Experimento para análises de combinações físico-químicas sob o ambiente de microgravidade.

Exemplo de EX-6: Experimento com amostras biológicas, sem aquisições de dados ambientais enviadas por telemetria.

Exemplo de EX-7: Experimento com amostras susceptíveis a efeitos de grandes altitudes.

Tabela 2 Tipo de experimento x serviço demandado.

Tipo de experimento	Serviço				
	Sinalização	Dados	Potência	Microgravidade	Recuperação
EX-1	X	X	X	X	X
EX-2	X	X	X	X	
EX-3	X	X	X		
EX-4		X	X		
EX-5	X			X	X
EX-6				X	X
EX-7					X

Controle de missão: Sistema que controla as atividades e a cronologia de lançamento de foguetes.

Controle das etapas do ciclo de vida: Função de monitorar e fiscalizar a evolução das etapas do ciclo de vida da carga útil, com base na execução das atividades. A equipe responsável por esta função deve identificar quando é possível evoluir para a próxima etapa do ciclo de vida.

Coordenador das Res: Coordenador de atividades dos operadores dos experimentos, carga útil e veículo. Recebe as orientações, demandas e autorizações da segurança do campo. Frequentemente acumula a função de BCO.

Dinâmica de voo: Equipe responsável pelos cálculos de trajetória do foguete e de fornecer informações à segurança de voo, ao controle de missão e às equipes de recuperação.

EDA: Ensaio Dinâmico de Aceitação. Trata-se de um ensaio ambiental (vide Ensaios Ambientais). É efetuado para a aceitação de um ou mais componentes específicos e

para um sistema completamente integrado. Ou seja, é submetido para a aceitação de um equipamento ou experimento específico e para a aceitação de um ou mais módulos de foguetes ou carga útil completamente integrados.

EGSE: *Electric Ground Support Equipment* ou Equipamento Elétrico de Suporte em Solo. Trata-se do nome particular dos meios de solo aplicado à carga útil e experimentos científicos. Este sistema fornece os serviços necessários aos experimentos durante sua operação em solo e frequentemente auxilia na interpretação de dados embarcados.

Ensaios ambientais: São ensaios que simulam as condições de voo para vibração e choque. Eles são executados em um equipamento conhecido como *shaker* que submete uma determinada amostra a vibrações e choques para que seja possível sua análise. Estes ensaios verificam a capacidade de um sistema suportar esforços a que seja submetido, podendo ser executado em um único equipamento ou em até uma carga útil completa. São executados com os experimentos e equipamentos em funcionamento conforme previsto para o voo, isto para que o ensaio seja representativo e esses possam ser validados para esse ambiente de operação.

Experimentador Chefe: Principal responsável pelo experimento, respondendo por ele junto às demais partes interessadas.

Experimento Científico: Amostras ou processos testados em ambiente espacial. Os experimentos são completamente automatizados, dessa forma não há a necessidade de intervenção durante o voo. Para que desempenhem suas funções requerem serviços fornecidos em bordo.

Falta: Uma falta, ou falta elétrica, é o contato ou arco acidental entre partes vivas sob potenciais elétricos distintos, entre a parte viva e a terra ou entre a parte viva e a massa, em um circuito ou equipamento elétrico energizado.

Foguete: Conjunto da carga útil acrescentado ao veículo.

LO: Sinal de *Lift-Off*, indica que a carga útil está em voo. Inicia com o lançamento do foguete e cessa com o início da sequência de recuperação

Meios de solo: Dispositivos e equipamentos de suporte ao foguete durante todas as fases da missão.

Meteorologia: Responsáveis pelas previsões ambientais que fornecem dados para cálculo de trajetória do foguete e segurança de voo.

Missão: Operação que visa atender ao propósito do lançamento, o qual tem como finalidade cumprir um conjunto de objetivos. Em uma missão com experimentos

científicos os principais objetivos são: lançamento do foguete; voo nominal; recebimento dos dados de experimentos; os objetivos específicos de cada experimento embarcado e, quando aplicável, a recuperação de carga útil e das amostras de experimentos.

Módulo hermético: Módulo onde experimentos ou equipamentos são instalados para o voo. Este modelo de módulo provém um ambiente interno hermético, sendo assim o que estiver instalado em seu interior permanece com pressão próxima a 1 atm., mesmo que a carga útil esteja sujeita ao vácuo. As temperaturas no interior deste módulo sofrem variações mais lentas se comparado a outros tipos de módulos embarcados.

Módulo não hermético: Módulo onde experimentos ou equipamentos são instalados para o voo. Este modelo de módulo sujeita ao que está instalado nele, a mesma pressão externa à carga útil, geralmente vácuo. Este módulo por conter uma solução mecânica mais simples permite seu uso para o acesso tardio.

Módulo de recuperação: Módulo que sequencia e libera os paraquedas nele instalados, este tem a função de desaceleração da carga útil até seu ponto de impacto. Este módulo também envia sinais de RF, que tem como função auxiliar na localização pelas equipes de recuperação.

Módulo de serviços: Módulo que fornece serviços aos experimentos durante o voo. Geralmente fornece potência, sinalizações e canal de comunicação ao experimento. A comunicação é unidirecional sendo que o dado sai do experimento para o módulo de serviços, este por sua vez os envia em formato PCM via RF.

Operador: Responsável por comandar um EGSE.

PCM: *Pulse-Code Modulation* ou modulação por código de pulsos. É um método utilizado para representar digitalmente amostras de sinais.

Pós voo: Fase a qual ocorre após a carga útil ser recuperada, quando aplicável, ou logo ao fim da trajetória desempenhada quando não há recuperação. Nos casos em que o tempo é um fator decisivo para seu sucesso, esta é uma fase crítica para os experimentos que necessitam de acondicionamento de amostra logo após o fim do voo devido a sua degradação. Estes e os demais experimentos tratam dos dados recebidos por telemetria para continuar seus estudos.

Pré-voo: Fase que ocorre nos momentos que antecedem ao voo, em geral poucos minutos antes do lançamento. Nesta fase, todos os sistemas devem estar em estado pronto para voo.

Recuperação: Recuperação da carga útil após do desempenho do voo. Geralmente, equipes específicas são treinadas e destinadas para a execução deste serviço. Alguns experimentos dependem da recuperação de suas amostras para a obtenção de dados de pesquisa.

RF: Rádio Frequência. Este termo é utilizado para quando os dados são transmitidos via rádio frequência.

Segurança do campo: Responsável pela segurança no campo de lançamento.

Serviços: O módulo de serviços, módulo de recuperação, estações de campo e EGSEs fornecem os serviços necessários aos experimentos científicos.

Típicos serviços de bordo requisitados pelos experimentos científicos:

- Sinalização
    - Sinal de uG (microgravidade)
    - Sinal de LO (lançamento)
- Dados enviado via telemetria
- Potência
    - Recebida do módulo de serviço
    - Do próprio experimento
- Microgravidade
- Recuperação

Típicos serviços em solo requisitados pelos experimentos científicos:

- Preparação para voo
- Carga e descarga de baterias
- Informações a respeito do estado funcional do experimento embarcado

Solo: Indica local físico. Equipamentos, foguete, carga útil e qualquer outro item em solo.

Telemetria CLA: Sistema de recepção de dados transmitidos pelo foguete. Este sistema tem a função de receber, decomutar e distribuir os dados de voo às partes interessadas.

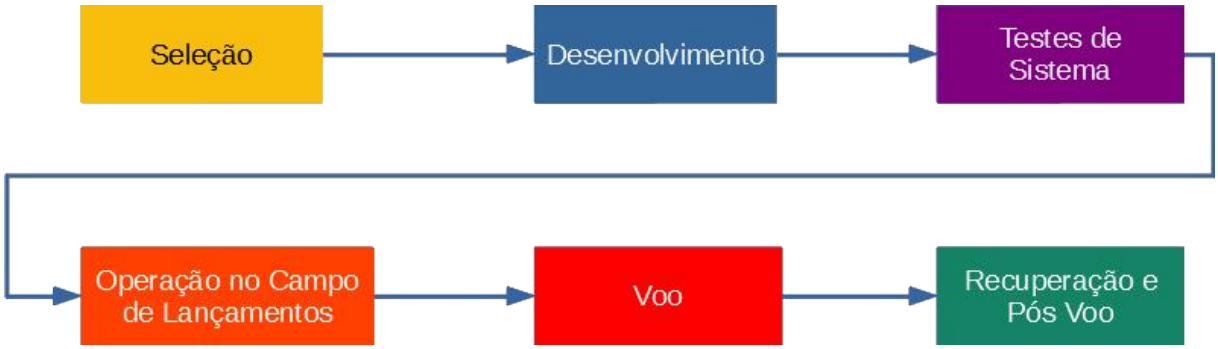
uG: Sinal que indica que a carga útil, bem como todos os experimentos está em ambiente de microgravidade

VEI: Responsável pelo veículo. Tem como função controlar as atividades do BCO, acessos ao foguete, bem como de passar as informações à segurança do campo e controle de missão.
Veículo: Aparato que eleva a carga útil ao espaço.
Voo: Fase pela qual o foguete desempenha o voo, impulsionado pelos propulsores do veículo. Nesta fase, a carga útil provém os serviços aos experimentos científicos a fim de que cumpram seus objetivos.

2.1.3 Ciclo de Vida da Carga Útil

Para um melhor entendimento do processo de desenvolvimento e integração de uma carga útil contendo experimentos, será apresentado o seu ciclo de vida. A Figura 3 apresenta o ciclo de vida da carga útil com suas fases de forma resumida.

Figura 3 Ciclo de vida da carga útil com suas fases de forma resumida.



Fonte: próprio autor

Seleção: Esta fase é de responsabilidade da AEB e seu processo não será abordado neste trabalho.

Desenvolvimento: Esta fase é compreendida de etapas com seus responsáveis indicados e na sequência a seguir:

- Desenvolvimento dos experimentos – Responsabilidade dos Experimentadores.
- Projeto da carga útil – Responsabilidade do IAE.
    - Desenvolvimento do leiaute.
    - Desenvolvimento das redes elétricas.

- Manufatura das conexões elétricas da carga útil, denominada cablagem da carga útil.
- Testes de validação dos experimentos separados e não integrados – Responsabilidade dos Experimentadores e IAE.
    - Aceitação do experimento.
        - Testes funcionais.
        - Testes elétricos.
        - Avaliação dimensional.
    - EDA em operação.

A fase de desenvolvimento inicia-se após da seleção dos experimentos para o voo. Os experimentadores desenvolvem seus experimentos, equipamentos embarcados, equipamentos de apoio em solo e seus procedimentos. Durante o desenvolvimento os experimentadores enviam à AEB a documentação do experimento em duas etapas e, por sua vez, essa documentação é enviada aos responsáveis pela carga útil. A primeira documentação enviada pelos experimentadores apresenta o experimento de forma conceitual e as abordagens planejadas paras as soluções para prover as funcionalidades necessárias. Enquanto a segunda, apresenta o projeto do experimento, EGSE e demais equipamentos de suporte em detalhes. Em cada envio de documentação é efetuada uma revisão por especialistas a fim de verificar a viabilidade das soluções de projeto planejadas ou adotadas pelos experimentadores.

Os responsáveis pela carga útil, munidos da documentação detalhada dos experimentos, projeta as redes elétricas e leiaute da carga útil. Bem como, a agenda, os testes e ensaios com os experimentos, conforme o cronograma de apronto do experimento.

A manufatura das conexões elétricas é iniciada assim que o projeto das redes elétricas e leiaute da carga útil é finalizado, o resultado é denominado de cablagem da carga útil. Ao fim da manufatura, a cablagem é testada e validada para voo.

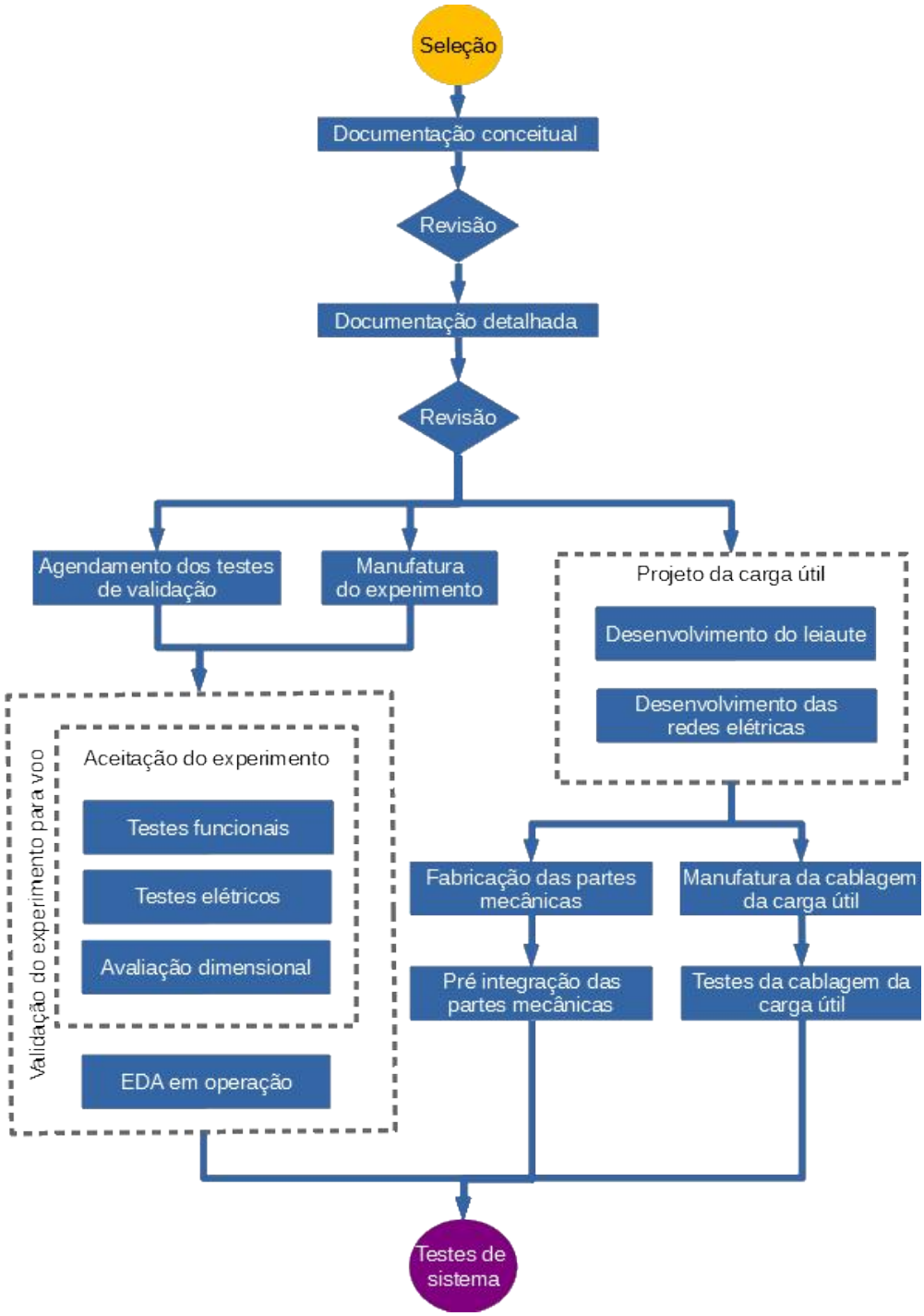
A Figura 4 apresenta as etapas do processo de desenvolvimento do experimento e da carga útil.

Para que seja possível evoluir para os testes de sistema, é necessário que a cablagem da carga útil esteja finalizada e testada, bem como, que os experimentos

tenham sido validados. Para a validação do experimento, ele deve atender satisfatoriamente ao processo de aceitação do experimento e EDA em operação.

Cabe salientar que, frequentemente, a carga útil leva ao espaço mais de um experimento. Como exemplo a carga útil MicroG2, lançada durante a operação Rio Verde em 2016, com 8 experimentos embarcados (Instituto de Aeronáutica e Espaço, 2017).

Figura 4 Desenvolvimento do experimento e da carga útil



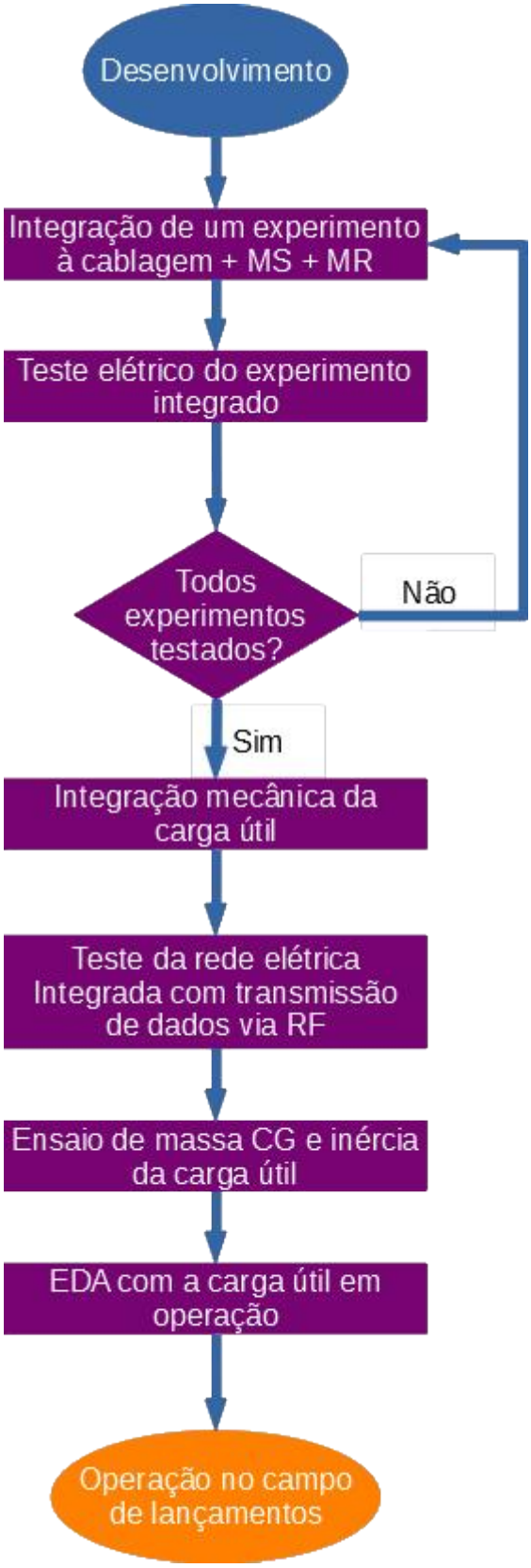
Fonte: próprio autor

Testes de sistema: Após o desenvolvimento da carga útil, segue a fases de testes integrados. As etapas e seus responsáveis são apresentados a seguir:

- Teste de compatibilidade entre experimentos, MS e MR. Os experimentos são eletricamente integrados incrementalmente e se executam testes funcionais em conjunto com o módulo de serviços e módulo de recuperação para verificação de eventuais problemas de compatibilidade. Responsabilidade do IAE, responsável pela carga útil e experimentadores.
- Integração mecânica da carga útil. Os experimentos são mecanicamente integrados à carga útil, bem como a carga útil é mecanicamente integrada. Responsabilidade do IAE.
- Teste de RF da carga útil. São executados testes funcionais com transmissão de dados via RF com a carga útil, suas redes elétricas e partes mecânicas integradas. Responsabilidade do IAE, responsável pela carga.
- Ensaios de massa CG e Inércia. Estes ensaios visam balancear e alimentar, com informações pertinentes, a equipe responsável pela dinâmica de voo. Responsabilidade do IAE.
- Ensaio Dinâmico de Aceitação. Este ensaio é desempenhado com a carga útil integrada em operação, ou seja, com o MS, MR e experimentos desempenhando seus testes funcionais. Responsabilidade do IAE, responsável pela carga útil e experimentadores.

A Figura 5 apresenta as etapas do processo de testes de sistema da carga útil.

Figura 5 Testes de sistema da carga útil



Fonte: próprio autor

Operação no campo de lançamentos: Após os testes de sistema e ensaios dinâmicos de aceitação da carga útil o foguete é transportado e as equipes deslocadas para o campo de lançamento. As fases que envolvem acesso ao veículo ou carga útil no lançador oferecem perigos que são mitigados para evitar a perda de vidas ou lesões. A seguir são apresentadas as fases que ocorrem até o lançamento:

- Transporte para o campo de lançamento – Responsabilidade da FAB;
- Testes e preparação da carga útil no campo de lançamento – Responsabilidade do IAE, DLR e experimentadores;
- Preparação dos experimentos científicos para o voo – Responsabilidade dos experimentadores;
- Treinamento da equipe de recuperação para manipulação de amostras de Experimentos – Responsabilidade da FAB e experimentadores;
- Montagem final da carga útil – Responsabilidade do IAE;
- Transporte da carga útil ao lançador universal – Responsabilidade do IAE e centro de lançamento;
- Instalação dos EGSEs na casamata – Responsabilidade do IAE e experimentadores;
- Testes da carga útil no Lançador – Responsabilidade do IAE, campo de lançamento, DLR e experimentadores;
- Preparação final da operação de recuperação da carga útil – Responsabilidade da FAB;
- Preparação final para voo (Pré-voo) - Responsabilidade do IAE, campo de lançamento, DLR e experimentadores;
- Armação do veículo (retirada das seguranças) – Responsabilidade do IAE e campo de lançamento;
- Lançamento – Responsabilidade do campo de lançamento.

Após o transporte do foguete e das equipes para o campo de lançamento se inicia os testes e preparações para o lançamento. Esta etapa, geralmente, é executada no prazo de duas semanas. Os principais testes executados no campo de lançamento são funcionais e de compatibilidade entre os sistemas embarcados com os do campo de lançamento. Os experimentos que necessitam de trocas de amostras têm seus procedimentos efetuados para que seja possível sua prontidão para o voo.

Ao fim dos testes de preparação, o veículo é transportado ao lançador e, na sequência, a carga útil. Após o foguete ser integrado, novos ensaios funcionais são executados para verificar se as funcionalidades do sistema não foram afetadas pela sua instalação no lançador, assim como todas as operações dos sistemas diretamente conectados a ele, também ocorrem com os EGSEs e equipes na casamata.

Uma vez que o foguete foi integrado e testado no lançador, é realizada uma contagem regressiva simulada, para verificar e validar a cronologia a ser seguida, bem como ajustá-la quando necessário. Há etapas críticas na cronologia, em especial quando ocorrem acesso de equipes ao lançador, durante estes acessos nada no foguete pode estar ativo, ligado ou energizado. Durante a contagem regressiva são integrados à carga útil os experimentos de acesso tardio, esta operação também é considerada de risco. Seguem-se com novos testes funcionais com o foguete na posição horizontal e, finalmente, na vertical. A fase final de preparação ocorre quando restam 30 minutos para o lançamento, nesta fase todos os sistemas são preparados para o lançamento.

Voo: Durante o voo não ocorrem ações na carga útil por parte das equipes que a desenvolveram e prepararam, dado que a plataforma não dispõe de telecomando de serviço. Entretanto, outras atividades de suporte ocorrem simultaneamente ao voo colaborando com o sucesso da missão, conforme segue:

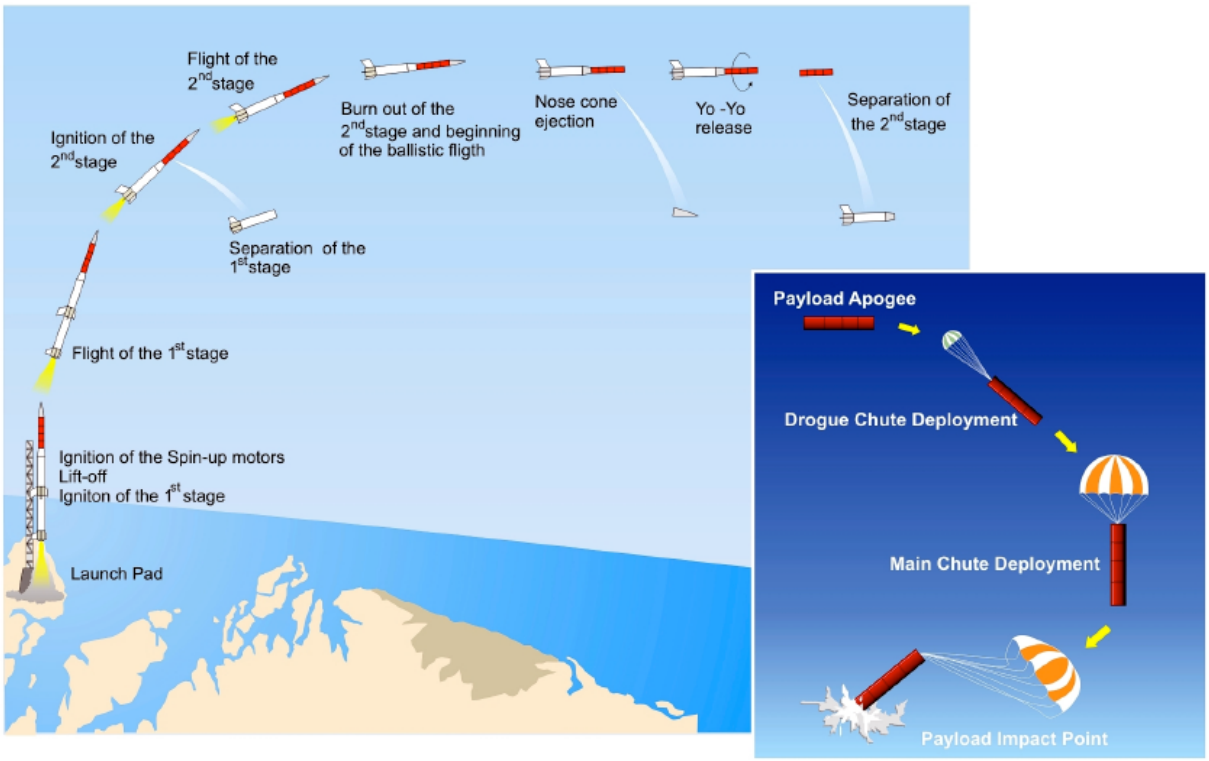
- Envio das informações de posição da carga útil às equipes de recuperação – responsabilidade do DLR e centro de lançamento
- Recepção dos dados enviados pela carga útil via RF e transferência ao DLR – responsabilidade do campo de lançamento
- Transferência das informações de voo aos experimentadores – responsabilidade do DLR
- Início da operação de recuperação da carga útil – Responsabilidade da FAB

Durante esta fase, a relação direta dos experimentos ocorre apenas com a carga útil, pois não há mais nenhuma interface com os operadores. A carga útil sinaliza o início de voo aos experimentos através do sinal LO, então ela é carregada pelo veículo até o momento em que ocorre a separação entre a carga útil e o veículo. A partir deste ponto, inicia-se os procedimentos para se obter a microgravidade (quando aplicável) e liberando o sinal de µG para que os experimentos iniciem seus processos. Esta fase

dura nos voos do VSB-30 aproximadamente 6 minutos. A carga útil continua sua trajetória até que se inicie a reentrada na atmosfera. Nesse momento o sinal de uG é desligado, indicando o fim da microgravidade. O módulo de recuperação da carga útil executa seus processos a fim de reduzir a velocidade de queda e, pouco antes da amerissagem, o módulo de serviço desliga a energia que distribui e se desliga automaticamente.

Durante todo o desempenho do voo, a carga útil transmite seus dados e os recebidos pelos experimentos por RF, enquanto no campo de lançamento, uma ou mais estações de telemetria recebem, tratam e entregam os dados ao EGSE da carga útil. Este separa e distribui os dados a cada um dos EGSEs dos experimentos. Durante o voo, os operadores dos experimentos analisam e gravam os dados recebidos. A Figura 6 apresenta os eventos que ocorrem durante o voo de um foguete VSB-30.

Figura 6 Eventos durante o voo do VSB-30



Fonte: Garcia *et al.* (2011)

Recuperação e pós voo: A carga útil amerissa a centenas de quilômetros da costa e a operação de recuperação oferecem diversos perigos que são mitigados pois podem levar a perda de vidas ou lesões. A sequência de etapas desta fase é apresentada a seguir:

- Abertura de experimentos para acondicionamento das amostras de experimentos conforme treinamento oferecido pelo experimentador – Responsabilidade da FAB
- Transporte da carga útil ao campo de lançamento – Responsabilidade da FAB ou marinha
- Recebimento e abertura da carga útil – Responsabilidade do IAE
- Entrega dos experimentos aos experimentadores – Responsabilidade do IAE
- Tratamento dos experimentos e dados e voo – Responsabilidade dos experimentadores

Dias antes do lançamento, uma base remota é montada para acomodar aeronaves e equipes de recuperação da carga útil. Para esta tarefa são utilizados helicópteros, aviões de patrulha e duas equipes de mergulhadores. O local desta base é estrategicamente escolhido para que a autonomia dos helicópteros e tempo para alcançar a carga útil sejam otimizados, pois o tempo de sua permanência na água é inversamente proporcional à chance de recuperação, bem como a autonomia das aeronaves é limitada.

No momento do lançamento as equipes de resgate decolam em direção ao ponto de impacto previsto pelas equipes da dinâmica de voo e os dados da localização da carga útil são enviados às equipes de recuperação durante o desempenho do voo, para que seu direcionamento possa ser ajustado. Quando as equipes encontram a carga útil, uma das equipes de mergulhadores salta do helicóptero ao mar, iniciando os procedimentos para o içamento, enquanto a outra equipe fica de prontidão. Cabe salientar, que este procedimento é de risco, o qual oferece diversos perigos às equipes envolvidas, bem como aos experimentos que dependem da recuperação para obter os resultados da pesquisa. A carga útil é içada, as equipes retornam ao helicóptero e a aeronave, de acordo com a autonomia, segue até o campo de lançamento ou até a base remota. No primeiro caso, a carga útil é entregue no heliponto do campo de lançamento, onde a carga útil é desmontada e os experimentos que necessitam de intervenção pós voo têm seus procedimentos executados pelos experimentadores. No segundo, ela é parcialmente desmontada, o helicóptero reabastecido e os experimentos que necessitam de intervenção pós voo têm seu procedimento executado na base remota pelas equipes de recuperação, as quais são treinadas

previamente pelos experimentadores, para então ser transportada ao campo de lançamento. Assim que a carga útil chega ao campo de lançamento, é integralmente desmontada e limpa, os experimentos são devolvidos aos experimentadores para que suas análises sejam iniciadas ou complementadas.

2.1.4 Considerações

É possível perceber que o número de etapas aumenta após o transporte do foguete ao campo de lançamento. Isso se deve, não somente, ao número de atividades envolvidas, mas também à sua criticidade. Caso ocorra alguma falha em algum sistema do foguete no campo de lançamento, a possibilidade de reparo cai drasticamente se comparado às fases anteriores.

A análise considerará a etapa de operação de lançamento, devido ser a fase mais complexa e a que oferece perigos com possibilidade de lesões ou perdas de vidas. Considera-se que nas fases anteriores a esta, também ocorrem os mesmos processos, porém de forma parcial.

O veículo, módulo de serviços e módulo de recuperação são sistemas em operação e serão do mesmo modelo para os diversos voos. Os foguetes considerados neste estudo são o VS-30 ou o VSB-30.

Os experimentos podem ou não se utilizarem de todos os serviços fornecidos pelo módulo de serviço.

A atividade de integração de experimento de acesso tardio no lançador oferece perigo às equipes que a executam.

Perigos, em ambiente anterior ao voo, relativos a experimento; à carga útil; ou ao foguete em que a falha não seja identificada, poderão levar a um acidente. Estes serão considerados na análise

A missão de lançamento poderá ser considerada bem sucedida conforme a definição, dada pelos responsáveis pela missão de lançamento, dos objetivos mínimos a serem alcançados.

2.2 Regulamentação da Agência Espacial Brasileira

A agência espacial brasileira, tem como uma de suas funções, regulamentar o setor espacial brasileiro. O documento: Regulamento Geral da Segurança Espacial, estabelece requisitos os gerais de segurança para atividades espaciais comerciais, cuja sua aplicação é obrigatória para qualquer entidade que tenha como intuito desenvolver atividades espaciais nos sítios de lançamento aprovados pela AEB em território brasileiro (Agência Espacial Brasileira, 2020). Este documento também define outros regulamentos específicos a saber:

- Regulamento Técnico Geral da Segurança Espacial;
- Regulamento Técnico da Segurança Ambiental em Atividades Espaciais;
- Regulamento Técnico da Segurança para Lançamento e para Voo;
- Regulamento Técnico da Segurança para Carga Útil;
- Regulamento Técnico da Segurança para Complexo de Lançamento;
- Regulamento Técnico da Segurança para Veículo Lançador;
- Regulamento Técnico da Segurança para Inter-Sítios.

O regulamento geral da segurança espacial prevê que um Certificado de Conformidade para a Segurança da Carga Útil é emitido pelo Organismo de Certificação Espacial para a entidade responsável pelo lançamento espacial, após esta comprovar que a carga útil atende aos requisitos do Regulamento Técnico da Segurança para Carga Útil (Agência Espacial Brasileira, 2020). Dessa forma pode-se dizer que a principal regulamentação pertinente para este estudo é o Regulamento Técnico da Segurança para Carga Útil.

O Regulamento Técnico da Segurança para Carga Útil abrange princípios gerais, regras de projeto, regras operacionais e princípios de submissão. É aplicável a todo trabalho relacionado a cargas úteis, equipamentos de apoio no solo, abrangendo o ciclo de vida completo da carga útil (Agência Espacial Brasileira, 2020).

Este regulamento, Regulamento Técnico da Segurança para Carga Útil, trata das questões gerais relacionadas as cargas úteis e aborda algumas questões de projeto. É possível verificar que o documento aborda as questões em alto nível e tem como objetivo estabelecer parâmetro para as instituições que integram e certificam as

cargas úteis. Dessa forma os campos de lançamentos, CLA e CLBI, instituições que projetam e integram as cargas úteis, IAE, são os principais responsáveis por cumprir as regras estabelecidas neste documento.

Este trabalho abordou de forma mais aprofundada as questões de segurança entre o IAE e experimentadores. Ele é complementar ao Regulamento Técnico da Segurança para Carga Útil, contribuindo para a segurança das cargas úteis espaciais.

2.3 Histórico de Falhas

Ocorreram acidentes e perdas durante o desenvolvimento do programa espacial brasileiro. Serão relacionados os incidentes ocorridos nos últimos 20 anos relacionados a lançamentos dos foguetes VS-30 e VSB-30 no Brasil.

Além dos acidentes com os foguetes e cargas úteis, ocorreram várias perdas nos experimentos. Mesmo que o sucesso seja obtido no voo e na recuperação, não significa necessariamente que os experimentos também serão bem sucedidos.

2.3.1 VS-30

O VS-30 é um foguete suborbital de um único estágio com um propulsor S30 de combustível sólido, lançado por trilho, capaz de transportar cargas úteis entre 260 kg e 330 kg, com uma altitude máxima que varia de 120 km a 160 km. Seu voo pode proporcionar até cinco minutos de um ambiente de microgravidade. O foguete tem aproximadamente oito metros de comprimento e uma massa total de elevação de 1,5 toneladas (PALMERIO, 2017).

Campanhas bem sucedidas do VS-30: Angicos em 2007 (Instituto de Aeronáutica e Espaço, 2010); Brasil-Alemanha em 2011 (Instituto de Aeronáutica e Espaço, 2011); Raposa em 2014 (Instituto de Aeronáutica e Espaço, 2014) e Mutiti em 2018 (Instituto de Aeronáutica e Espaço, 2018).

Sucesso parcial durante a campanha de lançamento Cumã: Este foguete foi lançado em 2002. Ocorreu uma separação intempestiva aos 29s de voo, e a carga útil foi perdida no mar (HARVEY *et al.* ,2010). Deve-se considerar que o sucesso de alguns experimentos depende da recuperação da carga útil e este incidente causou uma perda completa para este tipo de experimento.

2.3.2 VSB-30

O VSB-30 é um foguete de dois estágios suborbital, não guiado, lançado por trilho, constituído por um propulsor de combustível sólido S31, o segundo estágio com mesmo propulsor do VS-30 e uma carga útil com sistemas de recuperação e serviço (GARCIA *et al.*, 2011). Este foguete pode elevar para o espaço uma carga útil de até 400 kg com uma altitude máxima de 260 km, proporcionando aproximadamente 6 minutos de voo ao longo de 100 km; durante este tempo, é possível submeter as experiências a um ambiente de microgravidade. O foguete tem aproximadamente 12 metros de comprimento e tem uma massa total de descolagem de 2,5 toneladas (PALMERIO, 2017).

Campanha bem sucedida do VSB-30: Maracati II em 2010 (Instituto de Aeronáutica e Espaço, 2010).

Sucesso parcial durante a campanha de lançamento Cumã II: Este foguete foi lançado em 2007. Ocorreu um problema com o paraquedas e a carga útil foi perdida no mar (HARVEY *et al.* ,2010). Deve-se considerar que o sucesso de alguns experimentos depende da recuperação da carga útil e este incidente causou uma perda completa para este tipo de experimento.

Sucesso parcial durante a campanha de lançamento Rio Verde: Este foguete foi lançado em 2016. Ocorreu uma separação intempestiva durante o voo, entretanto a carga útil foi recuperada (Instituto de Aeronáutica e Espaço, 2017). Como a carga útil não ultrapassou a altitude de 100 km, todos os experimentos que dependiam do ambiente de microgravidade falharam.

2.4 System-Theoretic Accident Model and Processes – STAMP

System-Theoretic Accident Model and Processes – STAMP é um modelo recente de causas de acidentes e sua principal publicação é de Leveson (2012). É baseado na teoria de sistemas ao invés de confiabilidade e trata acidentes como um problema de controle dinâmico, diferente de outras técnicas que os tratam como um problema de confiabilidade. Essa técnica adota um modelo causal de acidentes baseado na teoria de sistemas. No modelo STAMP não se omitem causas, o foco passa da prevenção de falhas para imposições de restrições no comportamento do sistema. Assume-se que acidentes podem decorrer devido a interações inseguras entre componentes do sistema, mesmo que nenhum desses tenha falhado. Algumas características desta técnica são apresentadas a seguir:

- A análise aborda uma visão do topo para baixo (*top down*), sendo esta apropriada a sistemas de alta complexidade.
- Inclui *softwares*, fatores humanos, organizações e cultura de segurança, entre outros, como fatores causais em acidentes ou qualquer outro tipo de perda sem ser necessário tratar de forma distinta ou separadamente.
- Permite criar ferramentas mais poderosas, tais como STPA, análise de acidentes (CAST), identificação e gerenciamento de principais indicadores de risco crescente, análise de risco organizacional, etc.

De acordo com Leveson e Thomas (2018)

> o STAMP não é um método de análise. Ao invés disso, é um modelo ou conjunto de suposições sobre como os acidentes ocorrem. O STAMP é uma alternativa à cadeia de eventos de falha (ou dominós ou fatias de queijo suíço, todos essencialmente equivalentes) que está subjacente às técnicas tradicionais de análise de segurança (tais como Análise de Árvore de Falhas, Análise de Árvore de Eventos, HAZOP, FMECA e HFACS). Assim como os métodos tradicionais de análise são construídos com base nas suposições sobre por que os acidentes ocorrem em um modelo de cadeia de eventos de falha, novos métodos de análise podem ser construídos usando o STAMP como base. Observe que, como o modelo de eventos em cadeia de falhas é um subconjunto do STAMP, as ferramentas construídas com base no STAMP

> podem incluir como subconjunto todos os resultados derivados usando as técnicas de análise de segurança mais antigas.[1]

As duas técnicas baseadas em STAMP mais amplamente utilizadas são o STPA (*System-Theoretic Process Analysis*) de Leveson e Thomas (2018) e o CAST (*Causal Analysis based on Systems Theory*) de Leveson (2019). 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, então 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.

2.5 System-Theoretic Process Analysis – STPA

A opção pela técnica STPA foi motivada por ser um método que considera que acidentes são resultado de controle inadequado das interações entre componentes do sistema, e não restrito a falhas de componentes ou erro humano. Sua análise é proativa, que considera as potenciais causas de acidentes durante o desenvolvimento. Tendo em vista a complexidade dos sistemas das cargas úteis brasileiras, bem como em seu ciclo de vida a etapa se seu desenvolvimento é relevante, consideramos STPA uma técnica adequada para utilização neste trabalho.

[1]STAMP is not an analysis method. Instead it is a model or set of assumptions about how accidents occur. STAMP is an alternative to the chain-of-failure-events (or dominos or Swiss cheese slices, all of which are essentially equivalent) that underlies the traditional safety analysis techniques (such as Fault Tree Analysis, Event Tree Analysis, HAZOP, FMECA, and HFACS). Just as the traditional analysis methods are constructed on the assumptions about why accidents occur in a chain-of-failure-events model, new analysis methods can be constructed using STAMP as a basis. Note that because the chain-of-failure events model is a subset of STAMP, tools built on STAMP can include as a subset all the results derived using the older safety analysis techniques.

Leveson e Thomas (2018), traduzido pelo autor.

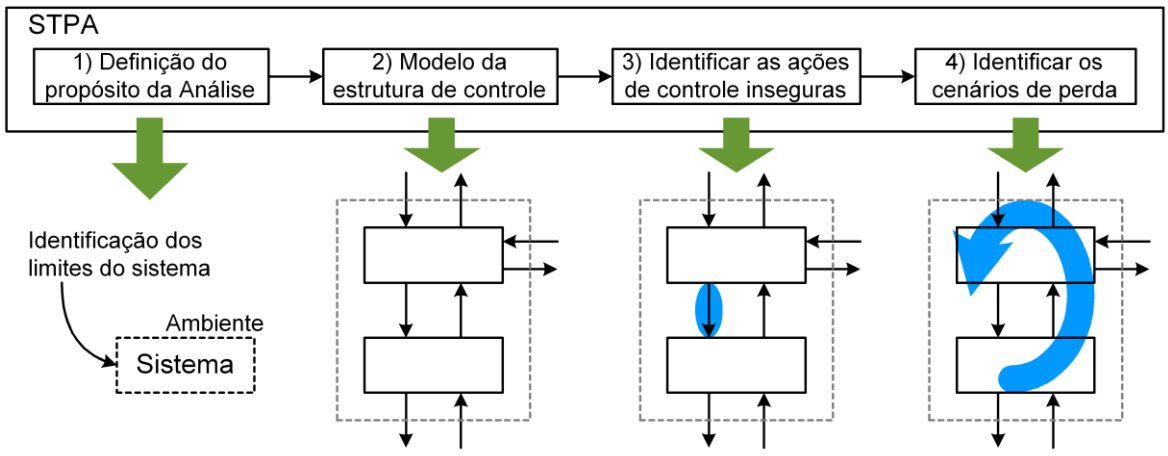
Definir a finalidade da análise é o primeiro passo no STPA. Deve-se elencar quais são os tipos de perdas que a análise visará evitar. Por exemplo, o STPA será aplicado apenas às metas tradicionais de segurança como a prevenção de perda de vidas humanas ou seu escopo será mais amplo como em relação à privacidade, desempenho e outras propriedades do sistema. Deve-se definir o sistema a ser analisado e qual é o seu limite.

A seguir são apresentadas algumas características desta técnica:

- Permite a análise de sistemas de grande complexidade. É possível prever perigos tradicionalmente descobertos apenas durante o início do processo de desenvolvimento, sendo possível mitigá-los ou eliminá-los.
- Pode ser utilizada durante a fase conceitual. Auxilia na identificação de requisitos e restrições de segurança. Estes podem ser utilizadas para projetar a segurança na arquitetura do sistema, reduzindo retrabalho custoso quando falhas são encontradas tardiamente no desenvolvimento ou durante a operação.
- Fornece a documentação da funcionalidade do sistema. É frequente a falta de documentação ou é de difícil rastreamento em sistemas grandes e complexos. STPA pode ser facilmente integrado no processo de engenharia de sistemas e na engenharia baseada em modelo.

Para que seja feita a análise é necessário seguir as etapas que o método pressupõe. Estas etapas são apresentadas na Figura 7.

Figura 7 Visão geral da técnica STPA



Fonte: traduzido de Leveson e Thomas (2018).

O STPA, para ser realizado, pressupõe passos que devem ser desempenhados conforme a sua ordem a seguir:

1 – Definição do propósito da análise
   a. Identificação das perdas inaceitáveis.
   b. Identificação dos perigos em nível de sistema.
   c. Definição das restrições de segurança em nível de sistema
2 - Modelamento da estrutura de controle.
   a. Definição das responsabilidades, ações de controle e realimentações.
3 - Identificação das ações de controle inseguras UCAs (*Unsafe Control Actions*).
4 - Identificação dos cenários de perdas.

2.5.1 Definição do propósito da análise

Identificação das perdas inaceitáveis:

A análise deve servir a um propósito, e para esta ferramenta trata-se de evitar as perdas inaceitáveis. Para isso inicialmente é necessário identificar as perdas inaceitáveis que se tem como objetivo evitar. Uma perda envolve algo de valor para as partes interessadas. Perdas podem incluir ferimentos ou perdas de vidas humanas, danos à propriedade, poluição ambiental, perda de missão, danos à reputação ou qualquer outra perda que seja considerada inaceitável do ponto de vista de uma parte interessada. O objetivo do STPA é contribuir na prevenção de perdas.

Para iniciar a análise STPA as partes interessadas devem apontar quais são as perdas que pretendem evitar. Para isso inicialmente se identificam as partes interessadas, seus valores e objetivos que esperam do sistema, e traduzir estes valores em formas de perdas inaceitáveis. A seguir alguns exemplos de perdas para facilitar o entendimento:

L-1: Perdas de vidas humanas
L-2: Perda ou dano ao veículo

Identificação dos perigos em nível de sistema:

O perigo é um estado do sistema ou um conjunto de condições que, juntamente com um grupo de condições ambientais desfavoráveis, levará a uma perda. Os perigos devem se referir ao sistema de forma geral, e em fatores que podem ser controlados. Os perigos descrevem condições do sistema que devem ser evitadas. O número de perigos a serem considerados durante a análise devem estar entre 7 a 10.

O perigo deve ser identificado, conter as informações do sistema, a condição insegura e sua vinculação com a perda. A seguir alguns exemplos de perigo para facilitar o entendimento:

H-1: Aeronaves violam padrão de separação mínima em voo [L-1, L-2]
H-2: Perda de integridade da fuselagem da aeronave [L-1, L-2]

O perigo H-2 contém todos os elementos conforme citado anteriormente, sendo eles: Identificação (H-2); informações do sistema (fuselagem da aeronave); condição insegura (perda da integridade); vinculação com a perda (L-1, L-2).

Definição das restrições de segurança no nível de sistema:

As restrições no nível de sistema especificam condições ou comportamentos que devem ser satisfeitos para a prevenção de perigos, e consequentemente evitar perdas. A restrição de segurança no nível do sistema deve ser identificada, conter as informações do sistema, a condição a ser aplicada e sua vinculação com o perigo. A seguir alguns exemplos de perigo para facilitar o entendimento:

SC-1: A aeronave deve satisfazer os padrões mínimos de separação [H-1]
SC-2: A fuselagem da aeronave deve manter-se íntegra nas condições de pior caso [H-2]

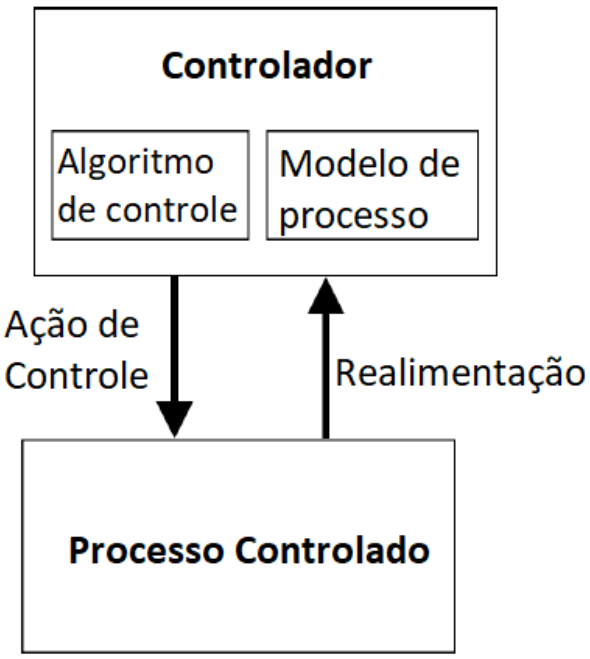
A restrição SC-2 contém todos os elementos conforme citado anteriormente, sendo eles: Identificação (SC-2); informações do sistema (a fuselagem da aeronave); condição a aplicar (manter-se íntegra nas condições de pior caso); vinculação com o perigo (H-2).

Não há uma relação de um para um entre restrições e perigos. Uma única restrição pode evitar mais de um perigo, bem como mais de uma restrição pode estar relacionada a um único perigo.

2.5.2 Modelamento da estrutura de controle

Uma estrutura hierárquica de controle é um modelo de sistema composto por laços de realimentação de controle conforme apresentado na Figura 8. Os controladores oferecem ações de controle como objetivo de controlar um determinado processo e impor restrições no comportamento do processo controlado. O Algoritmo de controle representa o processo de tomada de decisão do controlador, determinando as ações de controle a serem aplicadas. Os controladores também possuem modelos de processo que representam as crenças internas do controlador utilizadas para as tomadas de decisões. Em geral uma estrutura de controle hierárquico contém pelo menos cinco elementos a saber: Controladores, ações de controle, realimentações, processos controlados, outras entradas e saídas de componentes (sem ser ação de controle nem realimentação).

Figura 8 Estrutura hierárquica de controle genérica

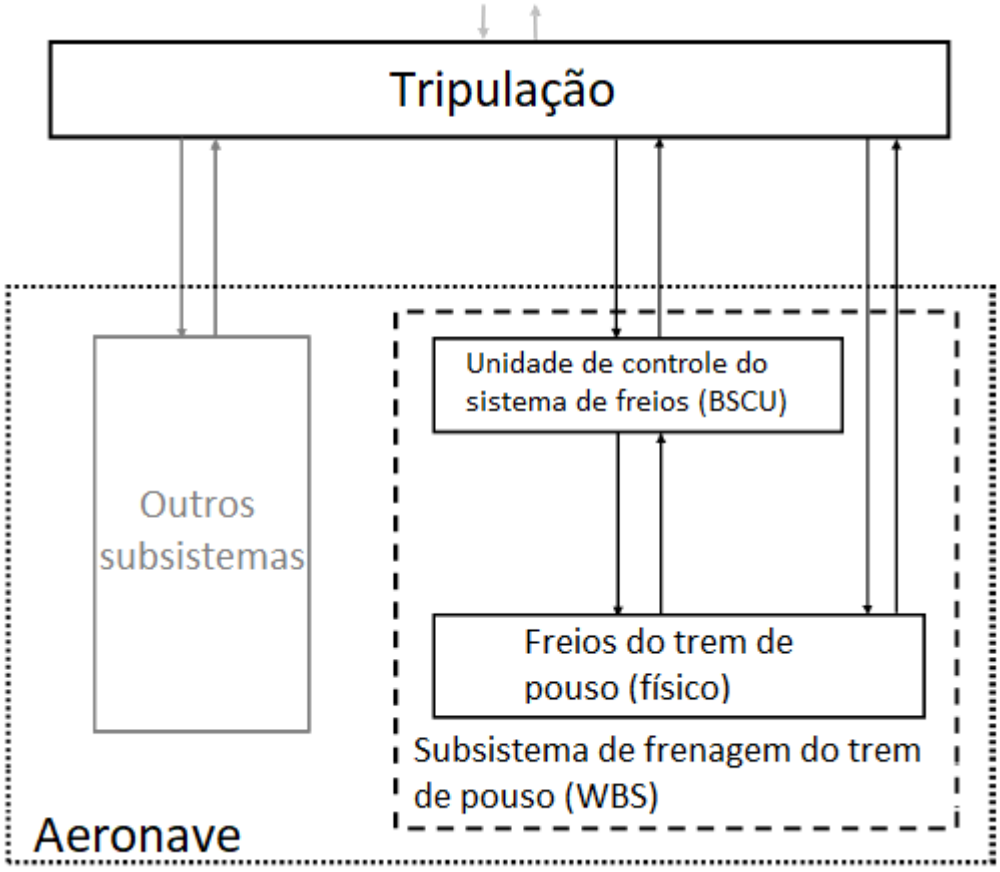


Fonte: traduzido de Leveson e Thomas (2018).

O modelamento do sistema pode ser feito primeiramente uma de alto nível, e posteriormente um detalhamento da parte de interesse. É importante salientar que a

estrutura de controle usada no STPA é um modelo funcional e não físico. Também não se trata de um modelo executável, nem modelo de simulação. Também deve-se considerar que as ações de controle não significam que uma determinada ação enviada por um controlador será necessariamente seguida. O mesmo ocorre com as realimentações, por mais que exista um canal estabelecido para a realimentação não significa que ela seja sempre enviada ou recebida. A Figura 9 apresenta a estrutura de controle detalhada com os controladores de subsistemas incluindo a unidade de controle do sistema de freios (BSCU) dentro do subsistema de frenagem do trem de pouso.

Figura 9 Estrutura de controle detalhada com os controladores de subsistemas



Fonte: traduzido de Leveson e Thomas (2018).

Responsabilidades:

Com os controladores identificados é possível atribuir responsabilidades. As responsabilidades são um refinamento das restrições de segurança, o que cada entidade deve executar para que, juntas, as restrições de segurança sejam aplicadas. A seguir exemplos de responsabilidades relacionadas ao travamento das rodas do trem de pouso.

Freios do trem de pouso (físico):

R-1: Desacelere as rodas quando comandado por BSCU ou tripulação de voo [SC-6]

BSCU:

R-2: Acionar os freios quando solicitado pela tripulação [SC-6]

Tripulação:

R-5: Decidir quando é necessário frear [SC-6]

Ações de controle e realimentações:

A seguir as ações de controle para cada controlador são definidas baseadas nas responsabilidades. Por exemplo, a tripulação deve ser capaz de enviar ações de controle para a frenagem manual para satisfazer R-5.

As realimentações podem ser derivadas das responsabilidades e ações de controle identificando pelo modelo de processo dos controladores utilizam para a tomada de decisão. A seguir um exemplo de realimentação:

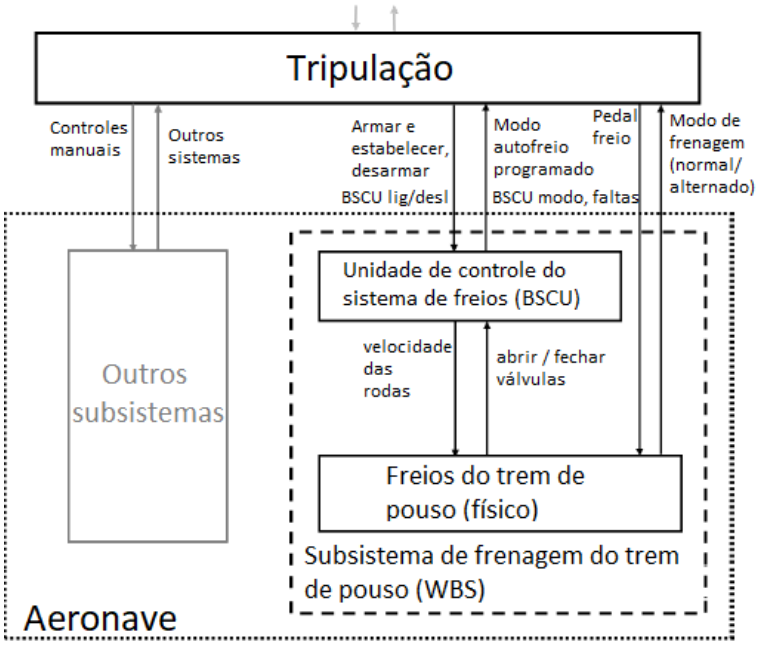
Responsabilidade do BSCU: R-2: Acionar os freios quando solicitado pela tripulação [SC-6].

Modelo do processo: O freio é solicitado pela tripulação.

Realimentação: Pedal de freio acionado.

A estrutura de controle detalhada com as ações de controle e realimentações baseadas nas responsabilidades, apresentada na Figura 10.

Figura 10 Estrutura de controle após o refinamento baseado nas responsabilidades



Fonte: traduzido e simplificado a partir de Leveson e Thomas (2018).

2.5.3 Ações de controle inseguras

Uma ação de controle insegura (UCA) é uma ação de controle, que em um determinado contexto e ambiente desfavorável, pode oferecer um perigo. O foco é identificar os contextos que levem a perdas, a fim de as controlar ou eliminar. Os contextos são estudados através de uma tabela que examina os estados de operação de um determinado sistema em situação perigosa, geradas pelas ações de controle. Esta tabela relaciona uma ação de controle, linha, com as possíveis circunstâncias perigosas, colunas. A Tabela 3 apresenta exemplos de UCAs.

Tabela 3 Exemplos de UCAs para o controlador BSCU

Ação de Controle	Não fornecimento causa perigo	Fornecimento causa perigo	Temporização / Ordem incorreta	Parou muito cedo	Aplicado muito tempo
CA-1	UCA-1:	UCA-2	UCA-3	UCA-4	UCA-4

Fonte: traduzido a partir de Leveson e Thomas (2018).

Legenda da Tabela 3:
CA-1: Freio
UCA-1: Freio automático do BSCU não fornece comando de frenagem durante a aterrisagem quando o BSCU está armado [H-4].
UCA-2: Freio automático do BSCU fornece comando de frenagem durante uma decolagem normal [H-4].
UCA-3: BSCU fornece comando de frenagem muito tarde após o início do pouso [H-4].
UCA-4: Freio automático do BSCU para de comandar a frenagem muito cedo enquanto a aeronave aterrissa [H-4].

Cada UCA pode ser rastreada para um ou mais perigos, e é recomendável documentar a rastreabilidade entre colchetes no fim de cada UCA. Cada UCA deve especificar o contexto no qual a ação de controle não é segura. Cada UCA contém cinco partes a saber: primeira parte é o controlador que pode fornecer a ação de controle; A segunda parte é o tipo de ação de controle inseguro (fornecimento causa perigo, não fornecimento causa perigo, etc.); A terceira parte é o comando em si (da estrutura de controle); A quarta parte é o contexto; e a última parte é o rastreio em relação os perigos.

Para facilitar o entendimento a UCA-2 tem suas partes identificadas: Controlador que pode fornecer a ação de controle (Freio automático do BSCU); tipo de ação de controle inseguro (fornece); Comando em si (comando de frenagem); Contexto (durante uma decolagem normal); rastreio em relação aos perigos (H-4).

2.5.4 Cenários de perdas

Com a identificação das ações de controle inseguras é possível prosseguir com a análise para a identificação dos cenários de perdas. Um cenário de perda descreve os fatores causais que tem potencial para levar a ações de controle inseguras e a perigos.

Identificação de cenários que levam a ações de controle inseguro. Estes tipos de cenários podem ser explorados iniciando-se com uma UCA e verificando o que poderia fazer com que um determinado controlador fornecesse, ou não fornecesse, esta ação de controle. Este tipo de cenário pode ocorrer por falhas relacionadas ao

controlador (falhas físicas como falta de energia, falha do controlador, etc.), algoritmo de controle inadequado, UCA recebido de outro controlador, modelo de processo inadequado, realimentações inadequadas. A seguir é apresentado um exemplo de algoritmo de controle inadequado relacionado ao UCA-3:

Cenário 1 para o UCA-3: A aeronave pousa, entretanto, ocorrem atrasos de processamento da BSCU resultam no atraso do comando de frenagem [UCA-3]. Como resultado, a pode ocorrer desaceleração insuficiente durante o pouso [H-4].

Identificação de cenários que ocorrem por ações de controle executadas indevidamente ou não executadas. Para estes cenários devem ser considerados fatores que afetam o caminho de controle, bem como questões que afetem o processo controlado.

Os cenários podem envolver o caminho de controle neste caso a ação de controle pode não ser executada. Caso a ação de controle seja aplicada ou recebida pelo processo controlado, porém o processo controlado não responde. Caso a ação de controle seja aplicada ou recebida pelo processo controlado, porém responde de forma indevida. Ou a ação de controle não é aplicada ou recebida pelo processo controlado, entretanto o processo responde como se a ação de controle tivesse sido aplicada ou recebida.

Exemplo:
Ação de controle: o controlador BSCU envia o comando de frenagem.
Cenário 6: O BSCU fornece o comando de frenagem, porém os freios não são aplicados devido ao sistema de freio da roda ter sido comandado previamente no modo de frenagem alternativo (ignorando BSCU). Como consequência pode ocorrer desaceleração insuficiente durante o pouso [H-4].

2.6 SysML

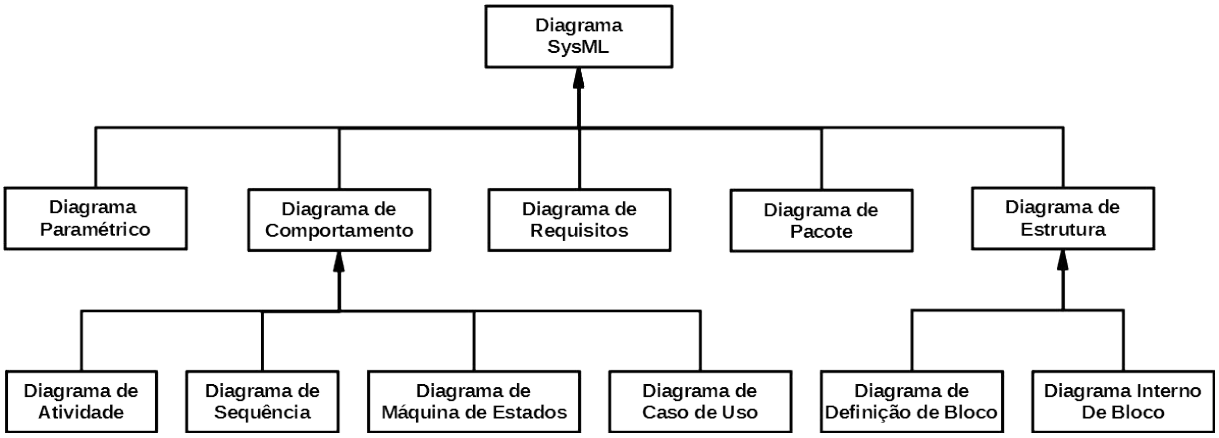
Linguagem de Modelagem de Sistemas, também conhecida por SysML, é uma linguagem de modelagem de uso geral para aplicações de engenharia de sistemas, de acordo com a definição de SYSML.ORG (2003). A SysML evoluiu em seu desenvolvimento ao ponto de ser uma linguagem padrão para a aplicação de Engenharia de Sistemas Baseada em Modelo (MBSE). De acordo com Friedenthal *et al.* (2012), trata-se de uma linguagem de modelagem gráfica de uso geral para apoiar a especificação, análise, projeto, V&V de sistemas complexos. Estes sistemas podem incluir *hardware*, *software*, dados, pessoal, procedimentos, instalações e outros elementos de sistemas. Friedenthal *et al.* (2012) também afirma que uma linguagem de modelo padronizada e robusta pode ser considerada um habilitador crítico para uma abordagem de engenharia de sistemas baseada em modelo e que a linguagem de modelagem de sistemas SysML destina-se a modelar sistemas em uma ampla gama de domínios de indústria, como aeroespacial, automotiva, saúde, entre outros.

O conceito de engenharia de sistemas baseada em modelos deve ser apresentado para a melhor compreensão dos conceitos acerca da linguagem SysML. De acordo com INCOSE (2007), MBSE é “a aplicação formalizada da modelagem para suportar os requisitos do sistema, projeto, análise, verificação e validação das atividades, começando na fase de projeto conceitual e prosseguindo ao longo das fases de desenvolvimento e mais adiantadas do ciclo de vida”.

A elaboração da linguagem SysML deve-se ao esforço de adaptação das práticas de modelagem, bem consolidadas, usadas na engenharia de *software* através da linguagem de modelagem unificada UML (*Unified Modeling Language*) para a Engenharia de Sistemas Baseada em Modelo.

Em Friedenthal *et al.* (2012) são identificados os tipos de diagramas SysML apresentados na Figura 11 e resumidos a seguir.

Figura 11 Taxonomia de diagramas da SysML.



Fonte: Friedenthal *et al.* (2012)

A SysML é apoiada em 5 bases de representação de sistema sendo estes: Estrutura, Comportamento, Requisitos, Paramétrico e Pacote. Nove diagramas possibilitam estas representações de sistema. A seguir, é apresentada uma lista onde em número estão elencados os diagramas principais e nas letras constam os diagramas que os representam:

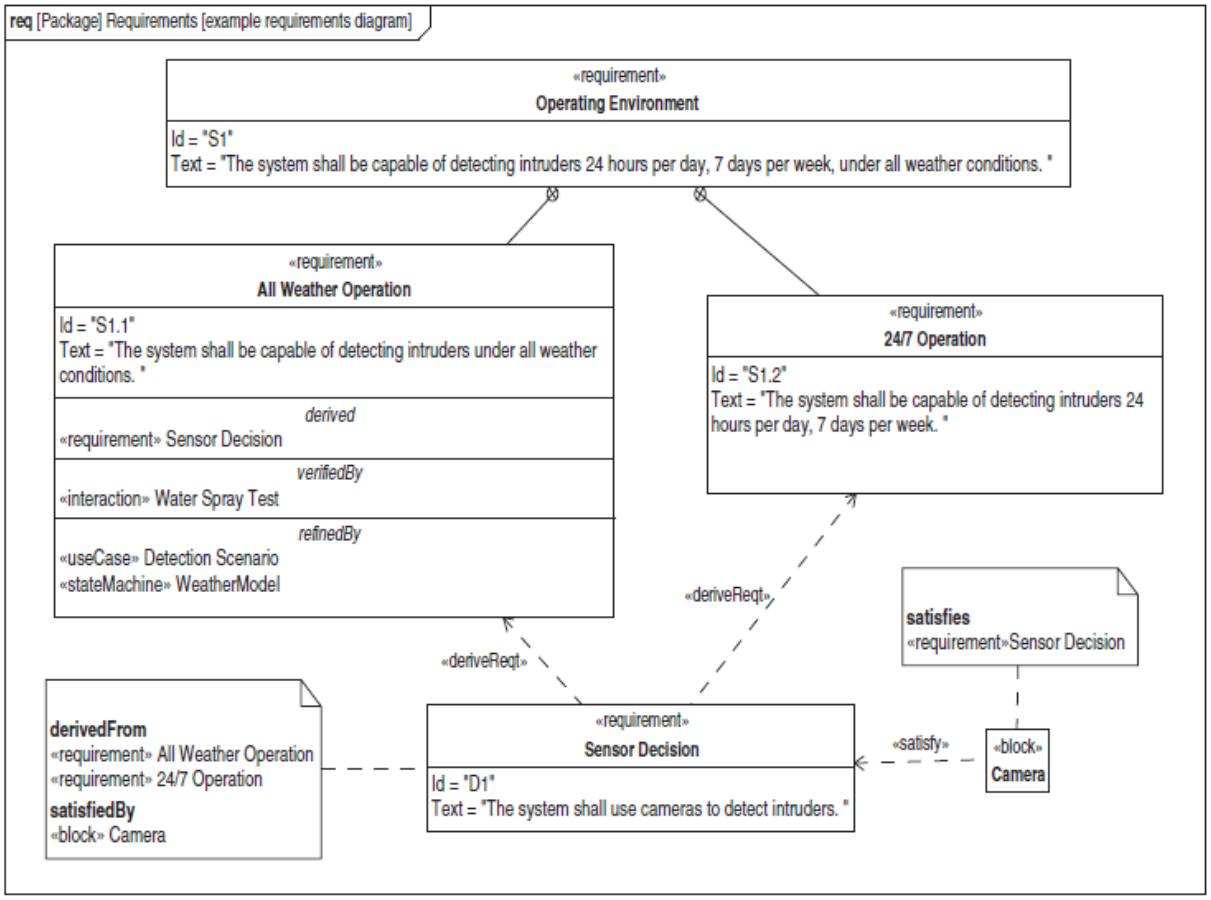
1. Diagramas de representação de Estrutura
    a. Diagrama de definição de bloco
    b. Diagrama interno de bloco
2. Diagramas de representação de Comportamento
    a. Diagrama de atividade
    b. Diagrama de sequência
    c. Diagrama de máquina de estados
    d. Diagrama de caso de uso
3. Diagrama de representação de Requisito
    a. Diagrama de requisito
4. Diagrama de representação Paramétrica
    a. Diagrama paramétrico
5. Diagramas de representação de Pacote
    a. Diagrama de pacote

Este trabalho irá identificar requisitos que serão apresentados em forma de tabelas e em linguagem SysML. Optou-se, portanto, em focar no diagrama de

requisitos, pois este poderá ser utilizado pelos experimentadores científicos na abordagem de Engenharia de Sistemas Baseada em Modelo.

De acordo com Friedenthal *et al*. (2012), o diagrama de requisito representa requisitos (em forma de texto), sua relação com os demais requisitos, com elementos de projeto e com os casos de teste, dando apoio à rastreabilidade de requisitos (não em UML). Os requisitos capturados no SysML podem ser retratados em um diagrama de requisitos, possibilitando a representação gráfica de hierarquias de especificações ou requisitos. Devido a este diagrama poder representar um grande número de relações para um único requisito, auxilia na representação da rastreabilidade de um único requisito para examinar como ele é satisfeito, verificado, refinado e para examinar suas relações derivadas com os demais requisitos. A Figura 12 apresenta um exemplo genérico de um diagrama de requisitos.

Figura 12 Diagrama genérico de requisitos.



Fonte: Friedenthal *et al.* (2012).

A partir das restrições de segurança que serão identificadas neste trabalho, será gerado um conjunto de requisitos de segurança que serão representados por um modelo SysML de requisitos. Este tipo de modelo mostra os vários tipos de relacionamentos entre os diversos requisitos, sendo que o principal objetivo da utilização desta linguagem é a disponibilização das informações de forma mais intuitiva aos experimentadores.

A opção pela modelagem dos requisitos SysML se deu por ser uma linguagem que fornece um tipo de diagrama exclusivo para requisitos. O SysML oferece uma significativa gama de recursos para a modelagem de requisitos e dessa forma se apresentando como uma linguagem apropriada para esta tarefa.

2.7 Trabalhos Correlatos

Foi realizada uma pesquisa para encontrar na literatura trabalhos relacionados a aplicação das técnicas STAMP e STPA em sistemas espaciais. Nenhuma literatura encontrada foi similar a este proposto. Em geral tratavam de sistemas espaciais com requisitos e criticidades distintas, entretanto alguns contam com maior relação com este trabalho e serão descritos a seguir.

O artigo Ishimatsu *et al.* (2014), bem como a dissertação de Ujiie R. (2016), tratam de análises STPA das fases de aproximação e captura do módulo H-II *Transfer Vehicle* da JAXA, também conhecido por HTV, à ISS. As principais diferenças dos sistemas analisados pelos autores em relação ao analisado neste trabalho são descritas a seguir:

Orbital: O sistema analisado por Ishimatsu e por Ujiie envolve módulos orbitais enquanto o nosso trabalho executará análises de cargas úteis suborbitais.

Suporte à vida: O sistema analisado por Ishimatsu e por Ujiie acopla em módulos com suporte à vida humana no espaço, enquanto o nosso trabalho não tem este tipo de necessidade.

Esforços mecânicos: Foguetes orbitais imprimem um nível de aceleração inferior à carga útil se comparado à dos foguetes suborbitais. Isto deve-se à massa superior

dos foguetes orbitais. Os níveis de vibração e choque são distintos entre os lançadores orbitais e suborbitais.

Tempo de duração da missão: Em missões orbitais, o tempo da missão pode variar entre dias a anos, enquanto para sistemas suborbitais este tempo usualmente é de minutos.

Pode-se afirmar que o sistema analisado pelos autores, Ishimatsu e Ujiie, é de maior criticidade se comparado ao sistema a ser analisado neste trabalho. Embora com todas as diferenças entre os sistemas, eles guardam similaridades e a ferramenta STPA pode ser utilizada da mesma forma.

A dissertação de Dunn (2011), o artigo Fleming *et al.* (2011) e no livro de Leveson N. (2012), são apresentadas análises relativas à satélites. As principais diferenças dos sistemas analisados pelos autores em relação ao analisado neste trabalho são descritas a seguir:

Orbital: Os sistemas analisados por Dunn, Fleming e Leveson envolvem módulos orbitais enquanto o este trabalho executará análises de cargas úteis suborbitais.

Esforços mecânicos: Foguetes orbitais imprimem um nível de aceleração inferior à carga útil se comparado a dos foguetes suborbitais. Isto deve-se à massa superior dos foguetes orbitais. Os níveis de vibração e choque são distintos entre os lançadores orbitais e suborbitais. O satélite usualmente recebe níveis amortizados pela própria estrutura do lançador orbital, enquanto os lançamentos suborbitais contam com menor estrutura e por esta razão transferem mais esforços à carga útil.

Tempo de duração da missão: Em missões orbitais o tempo da missão pode variar entre dias a anos, enquanto para sistemas suborbitais este tempo usualmente é de minutos.

Pode-se afirmar que os sistemas analisados pelos autores citados anteriormente, Dunn, Fleming e Leveson N., são de maior criticidade se comparado ao sistema a ser analisado neste trabalho, em especial pela duração da missão. Embora, com todas as diferenças entre os sistemas, eles apresentam similaridades e a ferramenta STPA pode ser utilizada da mesma forma.

No artigo de Rising e Leveson (2018) são descritos oito acidentes ocorridos com sete lançadores distintos e foi pontuado que muitos deles poderiam ter sidos identificados se um sistema de testes apropriado ou análise os identificasse e

priorizassem desde o início. As principais diferenças dos sistemas analisados pelos autores em relação ao analisado neste trabalho são descritas a seguir:

Orbital: O sistema analisado pelo Rising e Leveson envolve módulos orbitais enquanto a proposta deste trabalho é de executar análises de cargas úteis suborbitais.

Esforços mecânicos: Foguetes orbitais imprimem um nível de aceleração inferior à carga útil se comparado a dos foguetes suborbitais. Isto deve-se à massa superior dos foguetes orbitais. Os níveis de vibração e choque são distintos entre os lançadores orbitais e suborbitais.

Momento da Análise: Os autores apresentam análises de acidentes já ocorridos, desta forma a análise é retroativa. Para o trabalho proposto por nós desenvolve uma análise proativa mais adequada.

Pode-se afirmar que os sistemas analisados pelos autores, Rising e Leveson, são de maior criticidade se comparado ao sistema a ser analisado aqui. Embora com todas as diferenças entre os sistemas, eles apresentam similaridades e a metodologia STAMP pode ser utilizada da mesma forma. Este trabalho foca mais em acidentes já ocorridos, cuja análise é executada com a técnica CAST, enquanto estre trabalho se utiliza de STPA.

Capítulo 3

METODOLOGIA

Neste capítulo está a retomada das questões de pesquisa, e as etapas utilizadas para atingir os objetivos desta dissertação.

3.1 Questões de Pesquisa

A questão central deste trabalho é relativa aos requisitos de segurança, para que quando aplicados, contribuam para a segurança dos experimentos científicos espaciais. As recomendações de segurança são identificadas juntamente com os requisitos, entretanto não tem uso obrigatório ao usuário final. Para isto foi pesquisado na literatura, as técnicas de análise de segurança mais recentes, sendo escolhida a STPA, a qual é baseada na metodologia STAMP, para investigar o sistema da carga útil e identificar restrições de segurança.

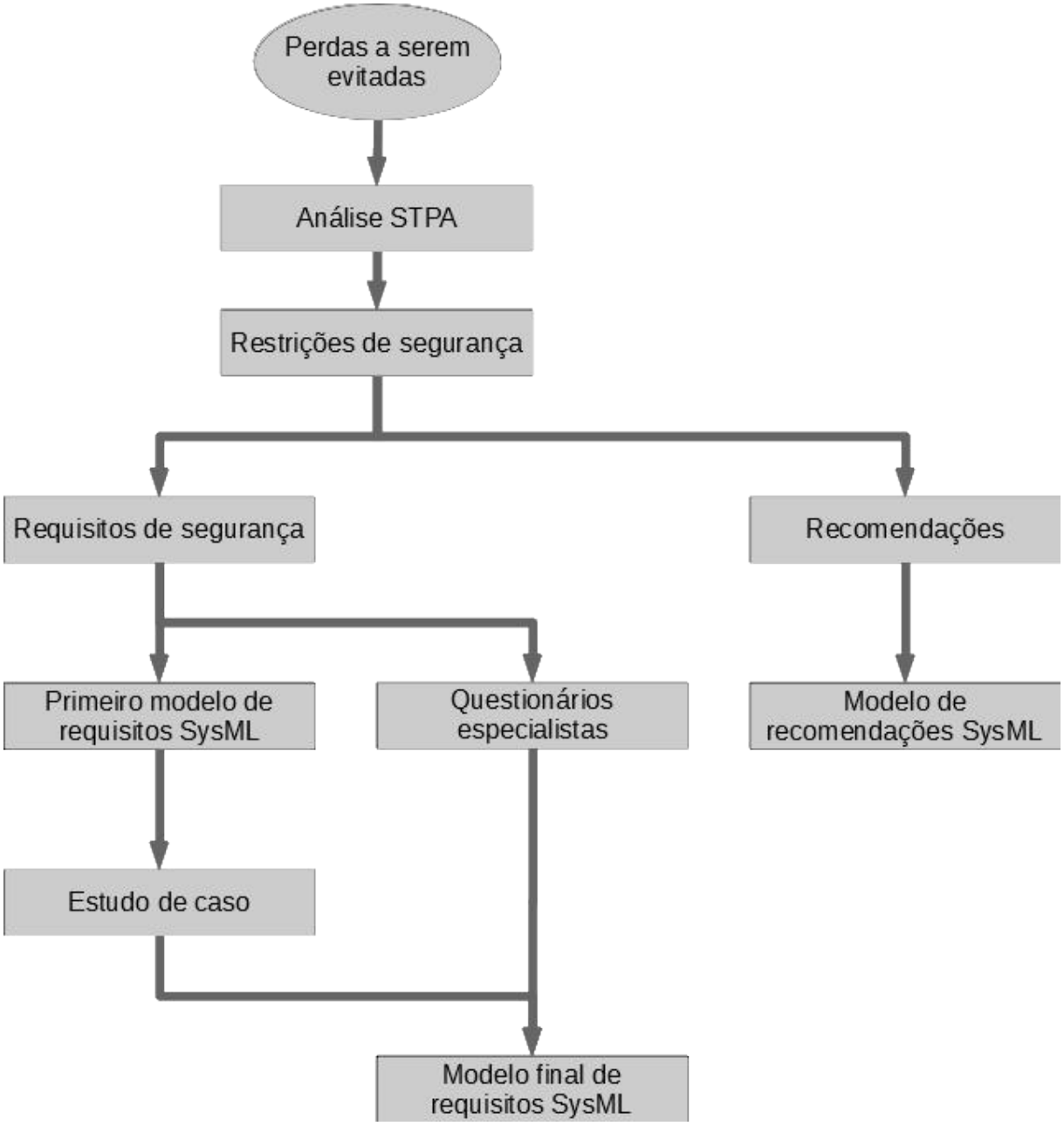
Questão 1: A modelagem SysML aplicada aos requisitos de segurança contribui com a sua organização e elaboração?
Questão 2: Quais os aspectos mais importantes a se considerar na adoção do *template* de requisitos de segurança?
Questão 3: De que forma o uso de STPA auxilia na identificação dos requisitos de segurança?

3.2 Etapas para o Desenvolvimento dos Requisitos de Segurança

Inicialmente foram levantadas as perdas a serem evitadas, e efetuada uma análise de perigos relacionados aos experimentos e cargas úteis espaciais baseada em STPA para a construção de um modelo de requisitos baseado na SysML. Estes

requisitos foram submetidos, a um processo de avaliação através de questionários enviados e respondidos por um corpo de especialistas. Na sequência, foi executado um estudo de caso a fim de verificar a aplicação do conjunto de requisitos de segurança identificados neste trabalho. A sequência destas etapas é apresentada na Figura 13 e detalhadas nos tópicos deste capítulo.

Figura 13 Sequência de etapas de desenvolvimento do modelo de requisitos em SysML



Fonte: próprio autor

3.2.1 Análise com o Uso da Técnica STPA

Foi executada uma análise de perigos, com a técnica STPA, esta é baseada no modelo STAMP (*System-Theoretic Accident Model and Processes*), tendo em vista mitigar perigos de projeto e de missão no âmbito da carga útil.

Além da compreensão da dinâmica do sistema estudado, a análise tem como propósito dois pontos principais.

- Identificar restrições de segurança decorrentes da análise de perigos da propagação de interações disfuncionais dos experimentos e da interação com outros equipamentos.
- Identificar restrições de segurança decorrentes dos perigos advindos de ações inseguras dos próprios experimentos e sua interação tanto com os as partes interessadas (*stakeholders*) como com procedimentos, processos e com o ambiente.

Para esta análise com a técnica STPA, inicialmente, foram levantadas as perdas que se pretende serem evitadas. Uma vez definidas as perdas, os perigos são identificados, que em determinadas condições podem levar a uma perda.

A partir do levantamento das perdas é possível identificar restrições no nível de sistema, que indicam comportamentos ou circunstâncias do sistema que devem ser satisfeitas para evitar os perigos e consequentemente as perdas.

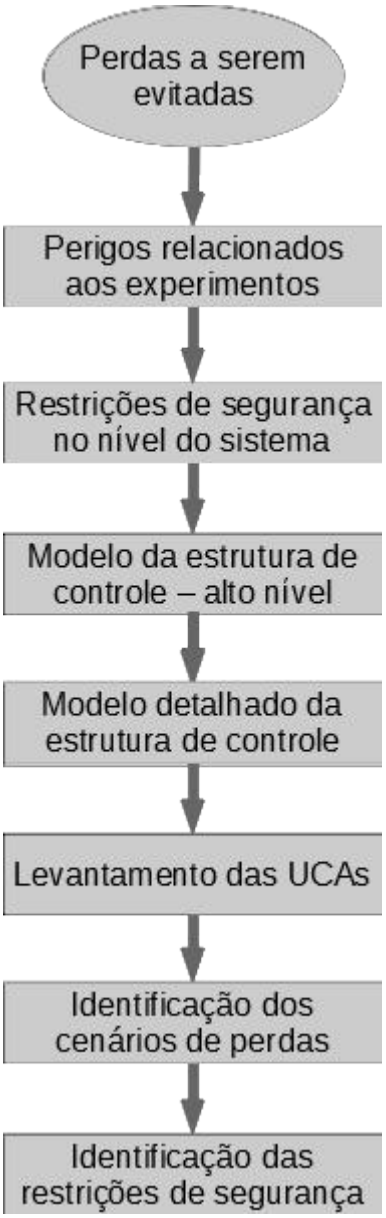
Os próximos passos da análise requerem uma estrutura de controle. Primeiramente, uma de alto nível e, posteriormente, um detalhamento da parte de interesse. É importante salientar que a estrutura de controle usada no STPA é um modelo funcional e não físico. Também não se trata de um modelo executável, nem modelo de simulação. Também deve-se considerar que as ações de controle não significam que uma determinada ação enviada por um controlador será necessariamente seguida. O mesmo ocorre com as realimentações, por mais que exista um canal estabelecido para a realimentação, não significa que ela seja sempre enviada ou recebida.

Com o auxílio do modelo detalhado da parte do sistema estudado foram levantadas as ações de controle inseguras (UCAs). Através da análise das UCAs é possível prosseguir para a identificação dos cenários de perdas. Um cenário de perda descreve os fatores causais que tem potencial para levar a ações de controle

inseguras e a riscos. Por fim, são identificadas as restrições do sistema que evitam ou mitigam os cenários de perda.

A Figura 14 apresenta a sequência dos passos executados, com o uso da técnica STPA, para a identificação das restrições de segurança.

Figura 14 Sequência das etapas executadas para a identificação das restrições de segurança



Fonte: próprio autor

3.2.2 Desenvolvimento dos Requisitos e Modelamento em SysML

Com base nas restrições de segurança identificadas com o uso da ferramenta STPA, foram desenvolvidos requisitos e recomendações de segurança. As restrições

foram utilizadas como ponto de partida, cada uma destas foi detalhada de forma a alcançar ao determinado objetivo. O detalhamento das restrições de segurança foi modelado em forma de requisitos em SysML. Durante o processo de modelagem foi identificado qual parte do detalhamento indicava ações não obrigatórias às partes interessadas, porém recomendáveis, dessa forma foram segregados do conjunto de requisitos e modelados como recomendações de segurança. Foi elaborado um diagrama com estas recomendações, denominado “diagrama de recomendações”.

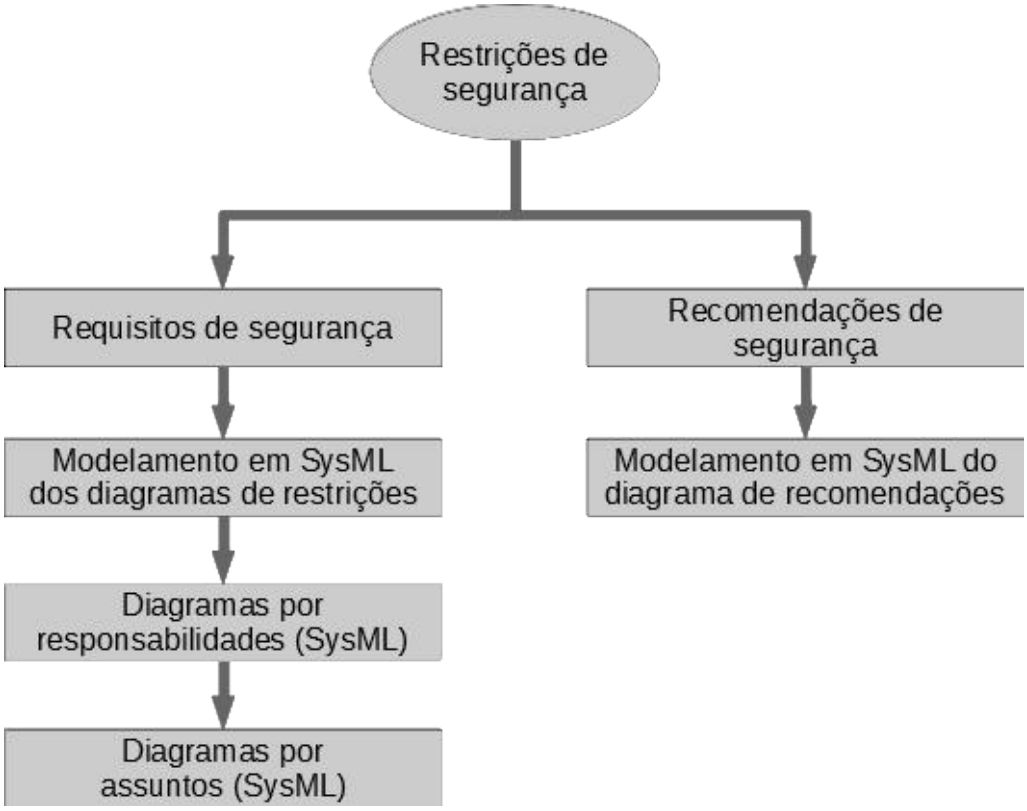
Um diagrama de requisitos e recomendações de segurança elaborado para cada restrição de segurança, apresentando todas suas relações. Estes foram denominados “diagramas de restrições”.

A partir do conjunto de diagramas de restrições, foram desenvolvidos um conjunto denominado “diagramas por responsabilidade”, onde os requisitos de segurança são classificados e apresentados por responsável.

Os requisitos de segurança foram organizados por assunto, novos diagramas foram elaborados e denominados “diagramas por assuntos”.

As etapas seguidas para o modelamento e elaboração dos diagramas de requisitos pode ser visualizado na Figura 15.

Figura 15 Processo de elaboração dos modelos de diagramas de requisitos em SysML



Fonte: próprio autor

3.3 Avaliação dos Requisitos de Segurança

As restrições e requisitos de segurança identificadas com o apoio da abordagem adotada foram avaliados, utilizando uma metodologia conhecida e aceita na área de aplicação. Desta forma, foram adotados os trabalhos de Kar P. e Bailey M. (1996) e Halligan R. (2017) para a avaliação dos requisitos e restrições, tanto individualmente quanto em conjunto. O objetivo é que o processo assegure que os requisitos estão corretos, escritos de forma inequívoca e suficiente.

Foram adotados critérios descritos em Kar P. e Bailey M. (1996) e Halligan R. (2017) para o teste de cada requisito ou restrição individualmente. Estes critérios são: capacidade de ser atendido, construção padronizada, verificável, correção, completude, clareza, consistência, não ambíguo, conectividade, singularidade e capacidade de ser modificado. E em relação ao conjunto: Orientação funcional.

Complementando esta etapa, baseado em Bahill T. e Henderson S. (2004), a verificação se deu 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 foi executada sua avaliação. Inicialmente foi desempenhada uma verificação lógica, sendo que, esta faz parte do trabalho para um melhor entendimento e, ao fim desta etapa, o conjunto de requisitos foi submetido ao corpo de especialistas.

3.3.1 Avaliação por Corpo de Especialistas

A partir da identificação dos requisitos de segurança, sua organização em grupos por assunto e sua verificação lógica, foi desempenhada uma avaliação por um corpo de especialistas. Sua elaboração foi fundamentada nos requisitos de segurança modelados em SysML, com a organização dos diagramas por assunto, suas respostas foram baseadas na escala de Likert (LIKERT, 1932). O Capítulo 6 - apresenta a elaboração e os resultados dos questionários submetidos aos especialistas.

3.3.2 Estudo de Caso

Após a avaliação dos requisitos de segurança um estudo de caso a fim de avaliar seu *template*, bem como sua aplicabilidade. Este estudo de caso foi efetuado através de questionários com a mesma organização proposta para a avaliação pelo corpo de especialistas, porém de forma mais aprofundadas e em conjunto com uma entrevista a um experimentador. Esta entrevista visou coletar as críticas e o parecer a respeito dos grupos de requisitos, fornecendo assim realimentações sobre melhorias que poderiam ser implementadas, bem como possibilidades futuras para a expansão deste trabalho.

Capítulo 4

RESTRIÇÕES DE SEGURANÇA

Este capítulo apresenta o desenvolvimento das restrições de segurança com o uso da técnica STPA.

A primeira etapa da análise é o levantamento das partes interessadas, tanto no desenvolvimento de um veículo espacial (especialistas da área espacial) como de seus usuários (especialistas experimentadores de universidades, centros de pesquisa, entre outros). Tendo em vista que os lançamentos são complexos e envolvem muitas pessoas, pode se dizer que as partes interessadas são numerosas. Apenas para ilustrar a dimensão de uma campanha de lançamento de um Foguete VSB-30, o transporte das equipes do DCTA, baseadas em São José dos Campos, adicionado às equipes de experimentadores para o campo de lançamento conta com aproximadamente uma centena de pessoas. Apenas as partes interessadas abordadas neste estudo serão apresentadas, são elas: AEB, FAB, CLA, CLBI, DCTA, IAE, experimentadores, DLR, COMGAR e a equipe de recuperação.

4.1 Perdas Consideradas Entre as Fases de Testes de Sistema a Pré-voo

O acidente é um evento não programado e indesejável que resulta em uma ou mais perdas. Esta parte da análise considera as fases e etapas compreendidas entre os testes de sistema até o momento da decolagem. Embora a perda possa ocorrer nas fases finais do ciclo de vida da carga útil, as razões podem estar relacionadas a etapas iniciais, como a de desenvolvimento, por exemplo. Perdas podem estar relacionadas a fatores ambientais que não são passíveis de serem controlados. Para esta análise foram levantadas as perdas que se pretendem evitar e são apresentadas a seguir. O identificador “L” indica *Loss*, do inglês, perda.

Perdas:

L-1: Dano material à carga útil

L-2: Dano material ao Experimento

L-3: Perda de informações do Experimento

4.2 Perigos Relacionados ao Experimento

Uma vez levantadas as perdas a serem evitadas a análise segue para a etapa de levantamento de perigos. O perigo é um estado do sistema ou conjunto de condições que, juntamente com um conjunto específico de circunstâncias ambientais, conduzirá a um acidente, e, portanto, à perda. Perigos podem ser controlados através de projeto e planejamento. Devido ao foco deste estudo ser os experimentos científicos e as suas relações, foram estudados os perigos diretos e indiretos, a eles relacionados.

A experiência dos envolvidos com a integração de sistemas das cargas úteis do IAE em conjunto com o direcionamento da análise da técnica STPA permitiu que fossem levantados os perigos apresentados na Tabela 4, nesta tabela o identificador "H" significa *hazard*, do inglês, perigo. A técnica STPA apresenta um roteiro de como a análise deve proceder e dessa forma cada um dos perigos, sob certas circunstâncias, pode levar a uma ou mais das perdas a serem evitadas. A seguir são apresentados dois exemplos de como pode ocorrer uma perda.

Exemplo com o perigo H-1: Ocorre o vazamento de uma amostra líquida de um experimento na carga útil durante a preparação para o lançamento, causando danos ao mesmo (L-2). Esta amostra líquida é corrosiva e vaza sobre os cabos internos de comunicação da carga útil. Como consequência, os cabos perdem a capacidade de transmitir as informações, estas informações são de outros experimentos e de controle da carga útil (L-1 e L-3).

Exemplo com o perigo H-2: Ocorre o vazamento de gás de uma amostra de um determinado experimento durante o voo. O módulo onde o experimento está acondicionado é hermético, em decorrência deste vazamento, ocorre um aumento de pressão deste módulo, acarretando na falha da vedação deste módulo. Quando ocorre

a amerissagem da carga útil este módulo é inundado pela água do mar, que por sua vez, deteriora a flutuabilidade da carga útil. Devido à degradação da flutuabilidade da carga útil, ela não é encontrada pelas equipes de recuperação e como consequência é perdida no mar (L-1, L-2 e L-3).

Tabela 4 Perigos relacionados ao experimento durante a fase de pré-voo.

Perigo	Condição insegura	Perda(s)
H-1	Vazamento de líquido	L-1, L-2, L-3
H-2	Vazamento de gás	L-1, L-2, L-3
H-3	Desprendimento de peças mecânicas	L-1, L-2, L-3
H-4	Superaquecimento	L-1, L-2
H-5	Violação do esquema de aterramento adotado	L-1, L-2, L-3
H-6	Testes insuficientes	L-1, L-2, L-3
H-7	Experimento liberado para voo sem ter obtido desempenho satisfatório durante os testes	L-1, L-2, L-3
H-8	Manipulação fora de especificação durante a preparação para voo	L-1, L-2, L-3
H-9	Ativação indevida	L-1, L-2
H-10	Não prontidão para voo	L-3

Legenda da Tabela 4.

H-1: Vazamento de amostras líquidas ou de outros itens líquidos do experimento.

H-2: Vazamento de amostras gasosas ou de outros itens gasosos do experimento.

H-3: Desprendimento de componentes, peças ou qualquer outra parte do experimento.

H-4: Aquecimento acima do projetado para o experimento.

H-5: Esquema de aterramento do experimento distinto ao da carga útil (foi adotado para as cargas úteis brasileiras o esquema de aterramento IT).

H-6: experimento insuficientemente testado. Pode ocorrer por testes não representativos ou pela não execução de um ou mais testes previstos.

H-7: Autorizada a integração do experimento na carga útil mesmo quando ele não obtém o desempenho suficiente em seus testes.

H-8: Degradação do experimento após manipulações por parte dos experimentadores durante a preparação para voo (Em geral estas manipulações são necessárias para troca ou inclusão de amostras sensíveis ou que se degradam por algum motivo).

H-9: Sequência de atividades incorreta durante a fase de ativação dos experimentos da carga útil e seus componentes integrantes, levando a ativação do experimento em

momento em que não se há permissão para isso (Em diversas fases uma ativação indevida do experimento poderá levar a uma perda).
H-10: Os procedimentos para preparar o experimento para o voo são executados incorretamente, parcialmente, tardiamente ou não executados.

4.3 Restrições de Segurança no Nível de Sistema

As restrições no nível de sistema indicam comportamentos ou circunstâncias do sistema que devem ser satisfeitas para evitar os perigos e consequentemente as perdas. Uma restrição de segurança no nível do sistema especifica condições ou comportamentos do sistema que devem ser satisfeitos a fim de evitar perigos. As restrições elaboradas a partir dos perigos levantados são apresentadas na Tabela 5, nesta tabela o identificador “SC” significa *safety constraint*, ou seja, restrição de segurança no nível do sistema.

Tabela 5 Restrições relacionadas ao Experimento.

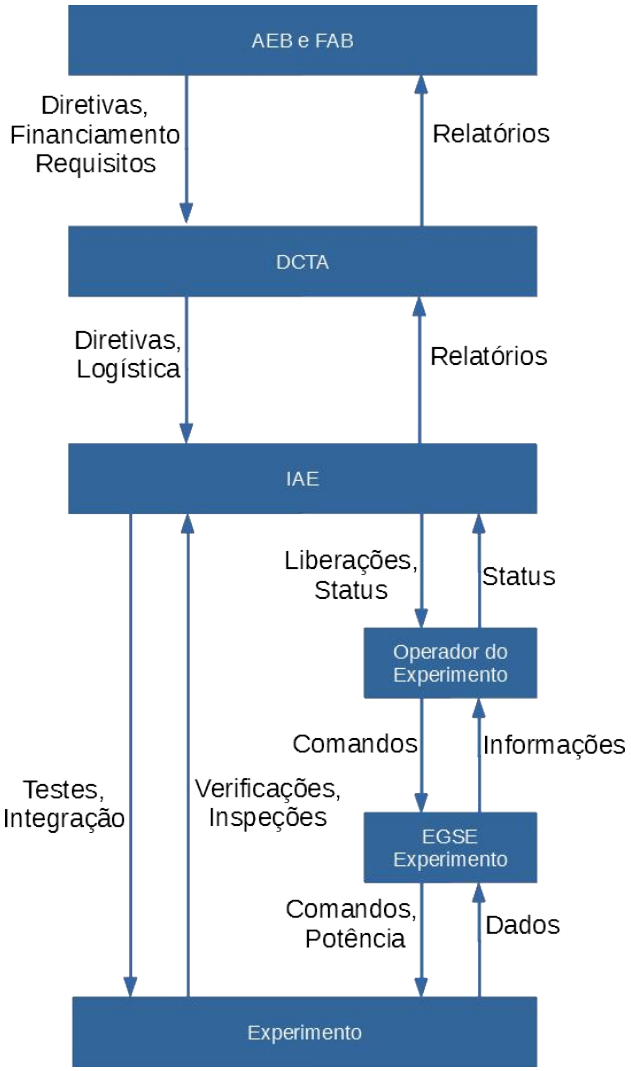
Rest.	Condição a Aplicar	Perigos(s)
SC-1	Não podem ocorrer vazamentos (gases e/ou líquidos) de dentro do experimento	H-1, H-2, H-4, H-5
SC-2	O experimento, durante a fase de voo, não pode alijar ou desprender suas partes mecânicas.	H-3, H-5
SC-3	O experimento deve suportar aos limites de temperatura exigidos pela carga útil sem que haja degradação física ou funcional do mesmo.	H-1, H-2, H-4, H-5
SC-4	O experimento deve contar com proteções contra sobrecorrentes, que atuem em caso de falta.	H-4, H-5
SC-5	O experimento deve respeitar o sistema de aterramento adotado na carga útil, mesmo sob falta simples.	H-4, H-5
SC-6	O experimento deve respeitar o esquema de aterramento e deve ser isolado galvanicamente do restante do sistema (rigidez dielétrica mínima de 250V).	H-5

Rest.	Condição a Aplicar	Perigos(s)
SC-7	O experimento deverá sofrer ensaios ambientais com as mesmas condições de voo (incluindo amostras, procedimentos entre outros).	H-1, H-2, H-3, H-4, H-5, H-6, H-7, H-9
SC-8	O procedimento de manipulação para a preparação para o voo do experimento deverá ser validado (incluindo trocas de amostras)	H-6, H-7
SC-9	O resultado do procedimento que exige manipulação para a preparação para o voo deverá ser inspecionado e validado (incluindo trocas de amostras)	H-6, H-7
SC-10	O experimento deverá desempenhar suas funções dentro de parâmetros nominais em todos os testes para que seja liberado para sua integração na carga útil	H-7
SC-11	A manipulação necessária para preparar o experimento para o voo deverá seguir estritamente o procedimento projetado pelo experimentador	H-1, H-2, H-3, H-4, H-5, H-8
SC-12	O experimento só deve ser ativado quando autorizado pelo Coordenador das REs (IAE)	H-1, H-2, H-4, H-5, H-9
SC-13	Deve haver possibilidade de bloqueio de ativação do experimento, supervisionado pelo coordenador das REs (IAE)	H-1, H-2, H-4, H-5, H-9, H-10
SC-14	Deve ser estabelecido um processo de comunicação entre o coordenador de REs e o operador do experimento	H-9, H-10
SC-15	Devem ser feitas simulações de lançamento com todas as partes envolvidas simultaneamente	H-9, H-10
SC-16	O experimento deverá ser ativado para testes e voo quando solicitado	H-6, H-10
SC-17	Operadores do experimento deverão ser treinados pelo experimentador chefe e IAE.	H-1, H-2, H-3, H-4, H-8, H-9, H-10

4.4 Modelamento da Estrutura de Controle

Os próximos passos da análise requerem que o sistema a ser estudado seja modelado em forma de uma estrutura de controle. Primeiramente uma de alto nível, conforme a **Figura 16** e posteriormente um detalhamento da parte de interesse. É importante salientar que a estrutura de controle usada no STPA é um modelo funcional e não físico. Também não se trata de um modelo executável, nem modelo de simulação. Também deve-se considerar que as ações de controle não significam que uma determinada ação enviada por um controlador será necessariamente seguida. O mesmo ocorre com as realimentações, por mais que exista um canal estabelecido para a realimentação não significa que ela seja sempre enviada ou recebida.

Figura 16 Estrutura de controle de alto nível para o sistema Experimento.



Fonte: próprio autor

O IAE emite relatórios anuais, ou bianuais para o público geral como por exemplo em: Instituto de Aeronáutica e Espaço (2010) e Instituto de Aeronáutica e Espaço (2012), entre outros. Também emite relatórios reservados e mais detalhados ao DCTA, alguns destes assuntos tratados são de cunho patrimoniais, planejamento de atividades, previsões orçamentárias, entre diversos outros. O DCTA envia relatórios à FAB e à AEB, condensando informações de outros institutos e do programa espacial como um todo.

Com os controladores devidamente identificados é possível atribuir suas responsabilidades. As responsabilidades são refinamentos das restrições de segurança, o que cada uma das partes deve fazer para que em conjunto atendam-nas. A seguir são apresentadas as responsabilidades dos controladores, cujo identificar é “R”.

Responsabilidades do controlador IAE:

R-1: Submeter o experimento aos níveis ambientais condizentes aos níveis de voo [SC-7].

R-2: Supervisionar a execução dos procedimentos de manipulações do experimento (troca de amostras) [SC-8, SC-9].

R-3: Autoriza a integração do experimento na carga útil [SC-10].

Responsabilidades do controlador operador do experimento:

R-4: Executar o procedimento para manipulação e troca de amostras do experimento [SC-11].

R-5: Operar o EGSE para preparar e ativar o experimento para os testes e voo [SC-16].

Responsabilidades do controlador EGSE do experimento

R-6: Acionar dispositivos do experimento conforme comandos do operador [SC-16].

R-7: Acionar a potência no experimento quando comandado pelo operador [SC-16].

Responsabilidades do experimento

R-8: Conter líquidos ou gases internos ao experimento, sob todas as condições de operação previstas [SC-1].

R-9: Sua estrutura deve manter os componentes mecânicos no local de sua instalação [SC-2].

R-10: Contenção de partes mecânicas dentro da estrutura mecânica em caso de desprendimento [SC-2].

Observações:

- As responsabilidades R-9 e R-10 são complementares. Há partes do experimento internas a uma estrutura (para R-9), sendo a estrutura também uma carenagem. Há outras partes na região exterior (R-8), regiões onde a estrutura não proporciona a função de carenagem.
- O experimento é passivo em suas responsabilidades em relação à contenção física do experimento. Isto é promovido por outras ações.

As tabelas 5 a 8 apresentam as responsabilidades, modelo de processo e a realimentação para cada um dos controladores.

Tabela 6 Responsabilidades do controlador IAE.

IAE Responsabilidade	Modelo de processo	Realimentação
R-1: Submeter o experimento aos níveis ambientais condizentes aos níveis de voo [SC-7].	Analisar as respostas dos ensaios ambientais e verificar se o experimento comporta o voo.	Dados de sensores obtidos durante o ensaio ambiental e inspeção visual
R-2: Supervisionar a execução dos procedimentos de manipulações do experimento (troca de amostras) [SC-8, SC-9].	Analisar o procedimento de troca de amostra, e se é exequível durante a campanha de lançamento.	Inspeção visual (IAE, e operador do experimento) e/ou informações fornecidas pelo operador do experimento.
R-3: Autoriza a integração do experimento na carga útil.	Analisa as respostas de todos os ensaios ao que o experimento foi submetido e das informações fornecidas pelo experimentador.	Informações relativas à saúde do experimento.

Tabela 7 Responsabilidades do controlador operador do experimento.

Op. Exp. Responsabilidade	Modelo de processo	Realimentação
R-4: Executar o procedimento para manipulação e troca de amostras do experimento [SC-11].	Executar a troca conforme planejado e validado. Executar inspeção visual e/ou analisar as informações apresentadas pelo EGSE do experimento.	Informar ao IAE o resultado da inspeção ou análise após a manipulação.
R-5: Operar o EGSE para preparar e ativar o experimento para os testes e voo [SC-16].	Executar o procedimento dos acionamentos necessários para testes e voo	Resultado da inspeção ou análise após a manipulação (informado ao IAE).

Tabela 8 Responsabilidades do controlador EGSE do experimento.

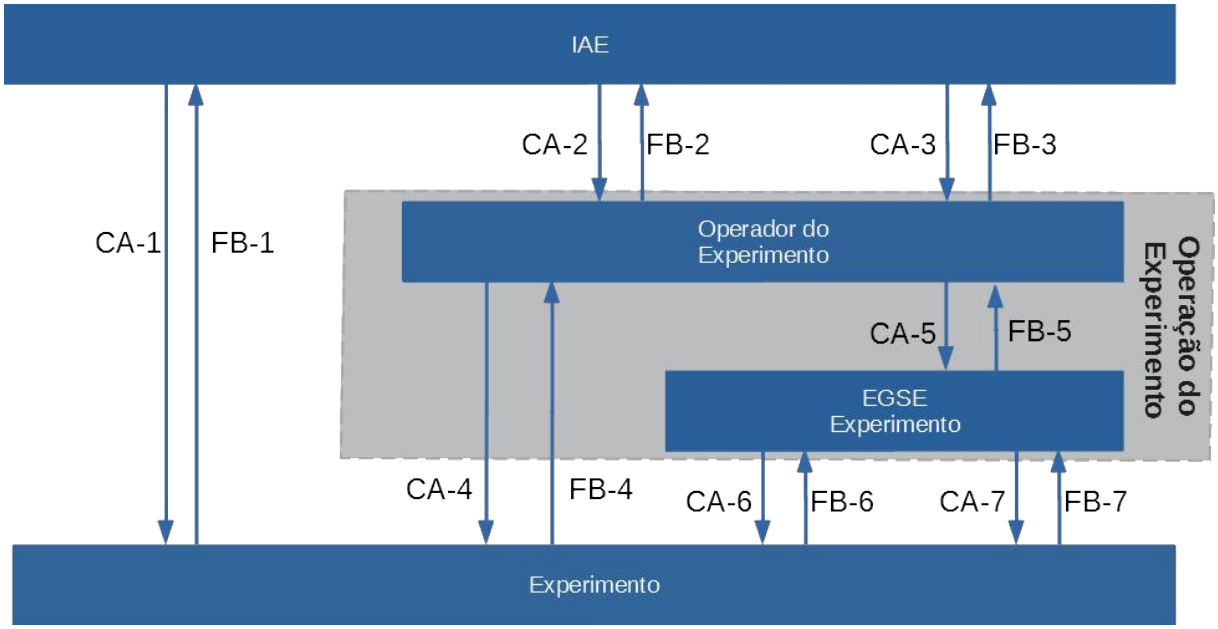
EGSE Exp. Responsabilidade	Modelo de processo	Realimentação
R-6: Acionar dispositivos do experimento conforme comandos do operador [SC-16].	Comanda relés, comandos por interface serial e comandos digitais conforme selecionado pelo operador do experimento.	Dados de estado e sensores do experimento (apresentadas ao operador do experimento).
R-7: Injetar potência externa ou interna à carga útil no experimento quando comandado pelo operador [SC-16].	Injeta potência no experimento quando comandado pelo operador do experimento.	Dados de estado e sensores do experimento (apresentadas ao operador do experimento).

Tabela 9 Responsabilidades do experimento.

Exp. Responsabilidade	Modelo de processo	Realimentação
R-8: Conter líquidos ou gases internos ao experimento, sob todas as condições de operação previstas [SC-1].	A contenção é passiva. Proporcionada pelo projeto e procedimento.	Inspeção visual (operador do experimento, e IAE). Verificação através de análise de sinais de sensores do experimento (operador do experimento).
R-9: Manter os componentes mecânicos no local de sua instalação [SC-2].	A contenção é passiva. Proporcionada pelo projeto e procedimento.	Inspeção visual (operador do experimento e IAE). Verificação através de análise de sinais do ensaio ambiental (IAE).
R-10: Conter as partes mecânicas dentro da estrutura mecânica em caso de desprendimento [SC-2].	A contenção é passiva. Proporcionada pelo projeto e procedimento.	Inspeção visual (operador do experimento e IAE). Verificação através de análise de sinais do ensaio ambiental (IAE).

A partir da definição das responsabilidades é possível refinar a estrutura de controle possibilitando aumentar o nível de detalhes para a análise. As ações de controle para cada controlador podem ser definidas baseadas nas responsabilidades levantadas. A Figura 17 apresenta mais detalhadamente a parte da estrutura de controle que será abordada neste trabalho. Nesta figura o identificador “CA” significa *control action*, ou seja, ação de controle e o identificador “FB” significa *feedback*, ou seja, realimentação.

Figura 17 Detalhe da estrutura de controle do experimento Científico



Fonte: próprio autor

Legenda da Figura 17:

CA-1: Ensaios ambientais.

CA-2: Supervisão e validação dos procedimentos.

CA-3: Autorização para integração.

CA-4: Manipulação para preparação para testes e voo.

CA-5: Procedimento para ativação do experimento.

CA-6: Comandos de acionamento do experimento.

CA-7: Acionamento de potência no experimento.

FB-1: Dados de sensores obtidos durante o ensaio ambiental e inspeção visual.

FB-2: Inspeção visual e relatório do experimentador.

FB-3: Informações referentes à saúde do experimento.

FB-4: Inspeção visual.

FB-5: Informações de estado e saúde do experimento.

FB-6: Dados de estado e de sensores.

FB-7: Dados de estado e de sensores.

Neste trabalho foi optado por explorar apenas questões relacionadas às ações de controle.

4.5 Identificação das Ações de Controle Inseguras (UCAs)

Uma ação de controle insegura (UCA) é uma ação de controle, que em um determinado contexto e ambiente desfavorável, pode oferecer um perigo. O foco é identificar os contextos que levem a perdas, a fim de as controlar ou eliminar. Os contextos são estudados através de uma tabela que examina os estados de operação de um determinado sistema em situação perigosa, geradas pelas ações de controle. As UCAs identificadas são apresentadas nas tabelas 9 a 11.

Tabela 10 Ações de controle inseguras do controlador IAE

Ação de Controle	Não fornecimento causa perigo	Fornecimento causa perigo	Temporização / Ordem incorreta	Parou muito cedo	Aplicado muito tempo
CA-1	UCA-1:	UCA-2	UCA-2 UCA-3	UCA-3	UCA-2
CA-2	UCA-4 UCA-5	UCA-6	UCA-7 UCA-8	UCA-7 UCA-8	
CA-3	UCA-9	UCA-10	UCA-11 UCA-12	UCA-11	UCA-12

Legenda da Tabela 10:
CA-1: Ensaios ambientais (esta ação ocorre apenas durante a fase de testes).
CA-2: Supervisão e validação dos procedimentos.
CA-3: Autorização para integração.

UCA-1: Não execução do ensaio ambiental durante a fase de testes [H-1, H-2, H-3, H-4, H-5, H-6, H-10].
UCA-2: Número de ensaios ambientais excedentes aos previstos durante os testes [H-1, H-2, H-3, H-4, H-5, H-10].
UCA-3: Não testagem do experimento a tempo para sua integração para o voo [H-10].
UCA-4: Validação para voo experimento com procedimento de troca de amostra inviável para sua execução no campo de lançamento [H-1, H-2, H-4, H-5, H-7, H-8, H-10].

UCA-5: Validação dos procedimentos acima dos valores pré-estabelecidos junto ao experimento [H-3, H-4, H-5, H-10].
UCA-6: Validação dos procedimentos ou de ensaios acima dos valores pré-estabelecidos, junto ao experimento [H-3, H-4, H-5, H-10].
UCA-7: Validação do experimento muito tarde para o voo [H-10].
UCA-8: Validação do experimento muito cedo provocando a degradação das amostras [H-1, H-2, H-3, H-4, H-5, H-8, H-10].
UCA-9: Não integração do experimento na carga útil [H-10].
UCA-10: Integração do experimento na carga útil sem validação para voo [H-1, H-2, H-3, H-4, H-5, H-6, H-7].
UCA-11: Autorização e execução da integração do experimento na carga útil muito cedo degradando assim as amostras [H-1, H-2, H-3, H-4, H-5, H-8, H-10].
UCA-12: Autorização da integração do experimento para o voo muito tarde [H-10].

Tabela 11 Ações de controle inseguras do controlador operador do experimento.

Ação de Controle	Não fornecimento causa perigo	Fornecimento causa perigo	Temporização/ Ordem incorreta	Parou muito cedo	Aplicado muito tempo
CA-4	UCA-13 UCA-14	UCA-15 UCA-16	UCA-17 UCA-18	UCA-14 UCA-18	UCA-18
CA-5	UCA-19 UCA-20	UCA-21	UCA-22 UCA-23 UCA-24	UCA-23 UCA-24	UCA-25

Legenda da Tabela 11:
CA-4: Manipulação para preparação para testes e voo.
CA-5: Procedimento para ativação do experimento.

UCA-13: Experimento não preparado nas condições equivalentes às de voo durante o ensaio ambiental [H-1, H-2, H-3, H-4, H-5, H-6].
UCA-14: Experimento não preparado para o voo [H-10].
UCA-15: Experimento sofre procedimento de manipulação diferente do validado, tanto durante os testes quanto para a preparação para o voo [H-1, H-2, H-3, H-4, H-5, H-6, H-8].

UCA-16: Manipulação excessiva do experimento durante a preparação para voo [H-3, H-8, H-10].

UCA-17: Troca de amostra do experimento efetuada muito cedo durante os testes ou preparação para voo, no caso de amostras sensíveis e sujeitas à degradação [H-3, H-6, H-8, H-10].

UCA-18: Manipulação para preparação efetuada muito tarde para o voo [H-3, H-10].

UCA-19: Não ativação do experimento durante os testes [H-1, H-2, H-3, H-4, H-5, H-6, H-7]

UCA-20: Não ativação do experimento para o voo [H-10].

UCA-21: Ocorrência de ativação do experimento quando não autorizado durante a preparação para o voo [H-1, H-2, H-4, H-5, H-9].

UCA-22: Ativação do experimento muito cedo, quando as amostras embarcadas são sensíveis e sujeitas à degradação [H-1, H-2, H-4, H-5, H-9, H-10].

UCA-23: Ativação do experimento de forma incompleta para voo [H-10].

UCA-24: Ativação do experimento de forma incompleta para os testes [H-1, H-2, H-3, H-4, H-5, H-6, H-7].

UCA-25: Ativação do experimento por muito tempo para os testes [H-1, H-2, H-4, H-10].

Tabela 12 Ações de controle inseguras do controlador EGSE do Experimento

Ação de Controle	Não fornecimento causa perigo	Fornecimento causa perigo	Temporização/ Ordem incorreta	Parou muito cedo	Aplicado muito tempo
CA-6	UCA-19 UCA-20	UCA-26	UCA-27 UCA-28	UCA-23 UCA-24	UCA-25 UCA-29
CA-7	UCA-19 UCA-20	UCA-26	UCA-30 UCA-31 UCA-32	UCA-31 UCA-32	UCA-30

Legenda da Tabela 12:

CA-6: Comandos de acionamento do Experimento.

CA-7: Acionamento de potência no Experimento.

UCA-26: Experimento acionado intempestivamente durante testes ou preparação para voo [H-1, H-2, H-4, H-9, H-10].

UCA-27: Comandos de acionamento do experimento ocorrem fora da ordem prevista durante os testes [H-6]
UCA-28: Comandos de acionamento do experimento ocorrem fora da ordem prevista durante a preparação para voo [H-10]
UCA-29: Ativação do experimento durante tempo excessivo na preparação para voo [H-1, H-2, H-4, H-9, H-10].
UCA-30: Ativação das amostras muito cedo provocando aquecimento excessivo durante preparação para voo ou testes (muito cedo) [H-4].
UCA-31: Ativação das amostras por tempo insuficiente durante os testes [H-1, H-2, H-3, H-6].
UCA-32: Ativação das amostras por tempo insuficiente durante preparação para voo [H-10].

4.6 Identificação dos Cenários de Perda

Com a identificação das ações de controle inseguras, apresentado anteriormente, é possível prosseguir com a análise para a identificação dos cenários de perdas. Um cenário de perda descreve os fatores causais que tem potencial para levar a ações de controle inseguras e a perigos. A seguir, serão apresentados alguns exemplos dos cenários de perdas identificados para determinadas UCA. Serão apresentados os cenários de perda para a UCA-6, UCA-25 e UCA-32, para que seja ilustrado o desenvolvimento para UCAs de cada um dos controladores analisados neste estudo. Todos os demais cenários de perdas são apresentados no Apêndice A.

UCA-6: Validação dos procedimentos ou de ensaios acima dos valores pré-estabelecidos, junto ao experimento [H-3, H-4, H-5, H-10].

Cenário 1 para UCA-6: Os ensaios ambientais são executados com níveis estabelecidos muito acima dos padrões nominais e como resultado o experimento não é aprovado para o voo [H-10], mesmo que tenha sido desenvolvido tomando todas as medidas para sua aprovação.

Cenário 2 para UCA-6: Os ensaios ambientais são executados com níveis excessivos e o experimento é aprovado para o voo, porém, sua estrutura sofre degradação sem que seja possível sua identificação.

Neste cenário, durante o voo devido a degradação componentes podem se soltar [H-3], cabos podem romper e provocar curtos-circuitos, incluindo no sistema de aterramento [H-4, H-5]

Cenário 3 para UCA-6: O rigor excessivo oferecido acarreta em alterações desnecessárias de procedimentos e eventualmente em reprojeto do experimento. Neste cenário, como consequência dos reprojetos ocorrem atrasos na entrega do experimento para um novo teste. Desta forma corre o risco de ultrapassar a data de entrega do experimento e ele não ser integrado à carga útil [H-10].

Cenário 4 para UCA-6: O rigor excessivo oferecido limita parte das experiências do experimento causando perda de parte de informações de voo [H-10].

UCA-25: Ativação do experimento por muito tempo para os testes [H-1, H-2, H-4, H-10].

Cenário 1 para UCA-25: O experimento permanece muito tempo com suas amostras ativas causando sua degradação [H-10] e eventual superaquecimento [H-4].
Neste cenário, durante o teste de simulação de voo, o cabo umbilical é desconectado da carga útil com o experimento ativo, conforme planejado, entretanto, o tempo da execução para as diversas etapas da fase de testes nem sempre é exata e pode levar aos experimentos serem ativados por tempo superior ao projetado.

Cenário 2 para UCA-25: O operador do experimento julga que o experimento está em faixa segura de operação, porém permanece muito tempo com suas amostras ativas causando sua degradação [H-10] e eventual superaquecimento [H-4].
Neste cenário, o tempo da execução para as diversas etapas da fase de testes nem sempre é exata e pode levar aos experimentos serem ativados por tempo superior ao projetado. As informações apresentadas pelo EGSE ao operador do experimento são insuficientes, ou indiretas. Podendo acarretar perda do experimento.
Cenário 3 para UCA-25: Ao fim do teste o operador do experimento comanda a desativação do experimento, porém o EGSE não executa os comandos conforme o operador.

Neste cenário, o experimento permanece ativo [H-9] causando seu superaquecimento [H-4], degradação das amostras e as baterias são drenadas além de seu limite, causando assim danos aos conjuntos [H-10].

UCA-32: Ativação das amostras por tempo insuficiente durante preparação para voo [H-10].

Cenário 1 para UCA-32: A cronologia definida não contempla o tempo adicional necessário para a preparação final do experimento para o voo.
Neste cenário, a temperatura da amostra para o voo precisaria de mais tempo para atingir seu valor de prontidão. A manutenção do tempo inferior ao necessário para sua preparação é baseada em um resultado de teste não representativo [H-10].

Cenário 2 para UCA-32: O experimento não é ativado por tempo suficiente durante a preparação final para voo, neste caso trata de aquecimento das amostras.
Neste cenário, o prazo não é estendido e o experimento voa com amostras com temperatura inferior à prevista para o voo, dessa forma o experimento voa com preparação incompleta [H-10], tendo como consequência tempo menor de experimentação, consumo maior de baterias ou seu não funcionamento conforme previsto.

4.7 Relações Entre os Cenários de Perdas e Restrições de Segurança

Através dos passos seguidos da técnica STPA, é possível identificar restrições de segurança para o sistema estudado. A Tabela 13, Tabela 14 e Tabela 15 apresentam as relações entre os cenários de perdas e restrições de segurança deste estudo. Foi adotado o identificador “REST” para as restrições de segurança.

Tabela 13 Relação entre UCAs do controlador IAE, cenários de perdas e restrições de segurança.

UCAs 1 a 12				Restrições
UCA-	1	Cenário	1	REST-001, REST-015, REST-018, REST-019, REST-020
UCA-	1	Cenário	2	REST-001, REST-015, REST-018, REST-019, REST-020
UCA-	2	Cenário	1	REST-001, REST-015, REST-018, REST-019, REST-020
UCA-	2	Cenário	2	REST-002, REST-003, REST-018
UCA-	3	Cenário	1	REST-001, REST-018
UCA-	3	Cenário	2	REST-001, REST-018
UCA-	3	Cenário	3	REST-004, REST-018, REST-020
UCA-	4	Cenário	1	REST-005, REST-018
UCA-	4	Cenário	2	REST-005, REST-006, REST-018
UCA-	5	Cenário	1	REST-001, REST-005, REST-018
UCA-	5	Cenário	2	REST-006, REST-018
UCA-	6	Cenário	1	REST-007, REST-008, REST-011
UCA-	6	Cenário	2	REST-003, REST-009, REST-010
UCA-	6	Cenário	3	REST-007, REST-008, REST-010, REST-018
UCA-	6	Cenário	4	REST-007, REST-008, REST-010
UCA-	7	Cenário	1	REST-001, REST-002, REST-011
UCA-	7	Cenário	2	REST-001, REST-002, REST-011
UCA-	7	Cenário	3	REST-001, REST-002, REST-011
UCA-	8	Cenário	1	REST-001, REST-002, REST-011
UCA-	8	Cenário	2	REST-013, REST-017
UCA-	8	Cenário	3	REST-006, REST-012, REST-013, REST-017
UCA-	8	Cenário	4	REST-006, REST-012, REST-014, REST-017
UCA-	9	Cenário	1	REST-018
UCA-	9	Cenário	2	REST-018
UCA-	10	Cenário	1	REST-001, REST-005, REST-006, REST-019
UCA-	10	Cenário	2	REST-001, REST-005, REST-006, REST-020
UCA-	11	Cenário	1	REST-006, REST-012, REST-017, REST-019, REST-020
UCA-	11	Cenário	2	REST-006, REST-012, REST-017, REST-019, REST-020
UCA-	12	Cenário	1	REST-018, REST-019, REST-020
UCA-	12	Cenário	2	REST-004, REST-018, REST-019, REST-020
UCA-	12	Cenário	3	REST-001, REST-020

Tabela 14 Relação entre UCAs do controlador operador do experimento, cenários de perdas e restrições de segurança.

UCAs 13 a 25				Restrições
UCA-	13	Cenário	1	REST-001, REST-015
UCA-	14	Cenário	1	REST-016, REST-021, REST-022, REST-023, REST-024, REST-025
UCA-	14	Cenário	2	REST-012, REST-014, REST-017, REST-018
UCA-	15	Cenário	1	REST-001, REST-010, REST-015, REST-018
UCA-	15	Cenário	2	REST-001, REST-010, REST-015, REST-018
UCA-	16	Cenário	1	REST-006, REST-012, REST-014, REST-017, REST-018
UCA-	16	Cenário	2	REST-006, REST-012, REST-014, REST-017
UCA-	17	Cenário	1	REST-006, REST-012, REST-017, REST-019
UCA-	17	Cenário	2	REST-012, REST-017, REST-018, REST-019
UCA-	17	Cenário	3	REST-012, REST-017, REST-018, REST-019
UCA-	18	Cenário	1	REST-006, REST-012, REST-017, REST-018, REST-019
UCA-	18	Cenário	2	REST-006, REST-012, REST-017, REST-018, REST-019
UCA-	19	Cenário	1	REST-001, REST-015, REST-016, REST-018, REST-020, REST-021, REST-022
UCA-	19	Cenário	2	REST-015, REST-016, REST-021, REST-022
UCA-	20	Cenário	1	REST-023, REST-024
UCA-	20	Cenário	2	REST-016, REST-021, REST-022
UCA-	20	Cenário	3	REST-025
UCA-	21	Cenário	1	REST-023, REST-024, REST-025, REST-026
UCA-	21	Cenário	2	REST-018, REST-023, REST-024, REST-025, REST-026
UCA-	21	Cenário	3	REST-023, REST-024, REST-026
UCA-	21	Cenário	4	REST-016, REST-021, REST-022, REST-025, REST-026
UCA-	22	Cenário	1	REST-011, REST-012, REST-017, REST-021, REST-027
UCA-	22	Cenário	2	REST-012, REST-017, REST-021, REST-027
UCA-	22	Cenário	3	REST-012, REST-017, REST-021, REST-027
UCA-	22	Cenário	4	REST-012, REST-017, REST-021, REST-022, REST-027
UCA-	23	Cenário	1	REST-016, REST-021, REST-022, REST-025
UCA-	23	Cenário	2	REST-016, REST-021, REST-022, REST-025
UCA-	23	Cenário	3	REST-016, REST-021, REST-022, REST-025, REST-028
UCA-	23	Cenário	4	REST-016, REST-021, REST-022, REST-025
UCA-	24	Cenário	1	REST-001, REST-015, REST-018, REST-020, REST-027
UCA-	24	Cenário	2	REST-001, REST-015, REST-016, REST-018, REST-021, REST-022, REST-025
UCA-	25	Cenário	1	REST-015, REST-018, REST-021, REST-027, REST-028
UCA-	25	Cenário	2	REST-015, REST-016, REST-018, REST-021, REST-027, REST-028
UCA-	25	Cenário	3	REST-015, REST-016, REST-018, REST-021, REST-027, REST-028

Tabela 15 Relação entre UCAs do controlador EGSE do experimento, cenários de perdas e restrições de segurança.

UCAs 26 a 32	Restrições
UCA- 26 Cenário 1	REST-016, REST-021, REST-022, REST-025, REST-026
UCA- 26 Cenário 2	REST-001, REST-015, REST-016, REST-021, REST-022, REST-025
UCA- 27 Cenário 1	REST-001, REST-015, REST-016, REST-021, REST-022, REST-025
UCA- 27 Cenário 2	REST-001, REST-015, REST-016, REST-021, REST-022, REST-025
UCA- 28 Cenário 1	REST-016, REST-021, REST-022, REST-025
UCA- 28 Cenário 2	REST-016, REST-021, REST-022, REST-025
UCA- 29 Cenário 1	REST-012, REST-016, REST-021, REST-022, REST-025, REST-027
UCA- 29 Cenário 2	REST-012, REST-016, REST-021, REST-022, REST-025, REST-027
UCA- 30 Cenário 1	REST-012, REST-016, REST-021, REST-022, REST-025, REST-027
UCA- 31 Cenário 1	REST-001, REST-011, REST-015, REST-027
UCA- 32 Cenário 1	REST-011, REST-015, REST-027
UCA- 32 Cenário 2	REST-011, REST-015, REST-027

4.8 Identificação das Restrições de Segurança

A partir dos cenários foram identificadas mais restrições de segurança, de sistema previamente identificadas em 4.3. A seguir são apresentadas as restrições de segurança (REST) identificadas neste trabalho.

REST-1: A equipe gestora da carga útil não deve permitir que o experimento seja integrado à carga útil sem que tenha atendido completamente à lista de ensaios e validações previstos.

REST-2: O experimentador não deve contar com aprovação imediata da contenção de amostras durante o desenvolvimento.

REST-3: As partes integrantes do experimento não podem degradar quando submetidas ao ensaio dinâmico de aceitação.

REST-4: Deve ser considerada a portabilidade das estruturas de suporte aos testes, permitindo que sua execução seja possível em outras instalações (IAE).

REST-5: A validação do processo de manipulação, ou troca, das amostras deve ser efetuada por equipe competente, com experiência em campo de lançamento e no processo de aceitação de experimentos.

REST-6: As trocas de amostras devem ser acompanhadas pela equipe responsável pela qualidade.

REST-7: Os níveis do ensaio dinâmico de aceitação devem ser previamente estabelecidos e divulgados aos experimentadores.

REST-8: Os ensaios só podem ser executados com equipamentos cuja a calibração esteja dentro da validade.

REST-9: Após o ensaio ambiental o experimento deve ser inspecionado e suas funções verificadas.

REST-10: O rigor exigido relativo aos procedimentos dos experimentos deve ser previamente estabelecido e informado aos experimentadores antes da fase de desenvolvimento.

REST-11: Durante a fase de desenvolvimento todos os procedimentos devem ser testados.

REST-12: As informações a respeito das condições que propiciam a degradação das amostras devem ser precisas.

REST-13: O experimento com amostras sensíveis deve respeitar o cronograma de testes, sem a antecipação de etapas.

REST-14: Para experimentos com amostras sensíveis o tempo de execução do procedimento de manipulação das amostras deve ser conhecido.

REST-15: O experimento deve ser testado no ensaio dinâmico de aceitação nas mesmas condições previstas para o voo.

REST-16: A identificação de cada um dos comandos efetuados no EGSE deve ser clara ao operador do experimento, de forma a permitir seu julgamento a respeito do funcionamento do processo.

REST-17: A degradação das amostras deve ser identificável sem que seja necessária a manipulação do experimento.
Consideração: Esta restrição não é obrigatória para experimentos de acesso tardio.

REST-18: O experimento não pode ser integrado à carga útil caso ofereça perigos não mitigados aos demais experimentos ou sistema da carga útil.

REST-19: As alterações de cronograma devem ser informadas aos experimentadores.

REST-20: Todas as etapas do ciclo de vida da carga útil devem ser controladas com ferramentas de gerenciamento.

REST-21: O operador do experimento deve ser treinado para a operação do EGSE.

REST-22: Os controles do EGSE devem ser de operação simples e inequívocos, permitindo assim clareza para a operação.

REST-23: Deve haver sinalizações relativas às autorizações do coordenador das REs para o operador do experimento de forma simples e inequívoca.

REST-24: Deve haver sinalizações relativas ao estado funcional (*status*) do experimento enviadas pelo operador do experimento, ou seu EGSE, para o coordenador das REs de forma simples e inequívoca.

REST-25: O EGSE deve restringir as possibilidades oferecidas ao operador do experimento de acordo com o procedimento em execução, não sendo possível enviar comandos, ou sequência anômalos ao procedimento.

REST-26: O coordenador das REs deve possuir capacidade para efetuar um bloqueio geral à ativação dos experimentos.

REST-27: Devem ser previstos procedimentos para todas as situações de operação esperadas.

REST-28: O experimento deve inabilitar os sinais de µG e LO, caso seja sensível a eles e possa ter suas amostras degradadas ao recebe-los durante testes.

Capítulo 5

REQUISITOS DE SEGURANÇA

Neste capítulo são apresentados os requisitos e recomendações de segurança e seu modelo SysML.

5.1 Requisitos de Segurança

Os 74 (setenta e quatro) requisitos de segurança apresentados neste capítulo, foram identificados tendo como ponto de partida as restrições de segurança apresentadas no Capítulo 4. Eles definem com mais detalhes as condições a serem atendidas, a fim de contribuir com o atendimento das restrições de segurança. Os requisitos de segurança foram redigidos de acordo com a forma adotada pelo IAE, que por sua vez é baseada na literatura European Cooperation for Space Standardization (2009). Os tipos de requisitos com seus identificadores são apresentados na Tabela 16.

Tabela 16 Identificadores dos tipos de requisitos

Tipo de requisito	Identificação	Tipo de requisito	Identificação
Funcional	FC-XXX	Logístico	LO-XXX
Físico	FS-XXX	Garantia do Produto	GP-XXX
Da Missão	MS-XXX	Projeto	PR-XXX
Ambiental	AM-XXX	Verificação	VR-XXX
Operacional	OP-XXX		

Cada um dos requisitos de segurança está relacionado a ao menos uma restrição de segurança. A Tabela 17 apresenta a lista de requisitos, a identificação de cada um e a qual restrição de segurança está relacionada.

Tabela 17 Lista dos requisitos de segurança e sua relação com as restrições de segurança

Item	Identificação	Restrição		Item	Identificação	Restrição	
1	GP- 001	REST- 001		38	OP- 005	REST- 016	REST- 022
2	VR- 001	REST- 001		39	PR- 012	REST- 016	
3	VR- 002	REST- 001		40	FC- 001	REST- 017	
4	VR- 003	REST- 001		41	GP- 014	REST- 018	
5	VR- 004	REST- 001		42	MS- 002	REST- 019	
6	VR- 005	REST- 001		43	MS- 003	REST- 020	
7	GP- 002	REST- 001		44	OP- 006	REST- 021	
8	PR- 001	REST- 002		45	OP- 007	REST- 021	
9	PR- 002	REST- 002		46	OP- 008	REST- 021	
10	PR- 003	REST- 002		47	OP- 009	REST- 021	
11	FS- 001	REST- 003	REST- 009	48	OP- 010	REST- 021	
12	VR- 006	REST- 003		49	OP- 011	REST- 021	
13	LO- 001	REST- 004		50	OP- 012	REST- 021	
14	OP- 001	REST- 005		51	OP- 013	REST- 022	
15	OP- 002	REST- 005		52	OP- 014	REST- 023	
16	GP- 003	REST- 005		53	OP- 015	REST- 023	
17	GP- 004	REST- 006		54	OP- 016	REST- 023	
18	GP- 005	REST- 006		55	OP- 017	REST- 023	
19	PR- 004	REST- 007	REST- 010	56	OP- 018	REST- 023	
20	GP- 006	REST- 008		57	OP- 019	REST- 023	
21	GP- 007	REST- 008		58	OP- 020	REST- 024	
22	VR- 007	REST- 008		59	OP- 021	REST- 024	
23	VR- 008	REST- 009		60	OP- 022	REST- 024	
24	VR- 009	REST- 009		61	OP- 023	REST- 024	
25	PR- 005	REST- 010		62	OP- 024	REST- 024	
26	VR- 010	REST- 011		63	OP- 025	REST- 024	
27	VR- 011	REST- 011		64	OP- 026	REST- 025	
28	AM- 001	REST- 012		65	OP- 027	REST- 025	
29	GP- 008	REST- 012		66	OP- 028	REST- 025	
30	MS- 001	REST- 012	REST- 014	67	OP- 029	REST- 026	
31	GP- 009	REST- 013		68	PR- 013	REST- 027	
32	GP- 010	REST- 014		69	PR- 014	REST- 027	
33	GP- 011	REST- 015		70	PR- 015	REST- 027	
34	GP- 012	REST- 015		71	GP- 015	REST- 027	
35	GP- 013	REST- 015		72	PR- 016	REST- 028	
36	OP- 003	REST- 016	REST- 022	73	PR- 017	REST- 028	
37	OP- 004	REST- 016	REST- 022	74	PR- 018	REST- 028	

Muitas vezes, há vários responsáveis por uma determinada ação ou função descrita no requisito de segurança. Entretanto, os requisitos de segurança apresentam sempre o principal responsável que foi identificado para esta execução ou controle.

Serão apresentados os requisitos de segurança VR-003, OP-005 e GP-015, apresentados em Quadro 1, Quadro 2 e Quadro 3 respectivamente, para que seja ilustrada sua forma de apresentação e estruturação. Os demais requisitos de segurança são apresentados no Apêndice B.

Quadro 1 Requisito VR-003

Identificação	VR-003
Desempenho	O experimento deve ser submetido à verificação dimensional antes do seu EDA
Título	Verificação dimensional antes do EDA
Justificativa	Impedir que experimentos que não tenham sido aprovados para o voo sejam integrados à carga útil
Tipo	Verificação
Responsabilidade	Gerencial IAE
Relacionado a	REST-001
Tolerância	N/A
Verificação	Relatório de ensaio

Quadro 2 Requisito OP-005

Identificação	OP-005
Desempenho	A sequência de comandos para cada procedimento previsto no EGSE deve estar pré-estabelecida e documentada
Título	Sequência de comandos no EGSE
Justificativa	Evitar operação imprecisa por parte do operador
Tipo	Operacional
Responsabilidade	Técnica do experimentador
Relacionado a	REST-016, REST-022
Tolerância	N/A
Verificação	*Checklist*, análise de documentação, verificação

Quadro 3 Requisito GP-015

Identificação	GP-015
Desempenho	Deve ser enviada uma lista das possíveis situações não nominais passíveis de ocorrência durante a missão aos experimentadores antes do desenvolvimento do experimento
Título	Situações típicas de operação
Justificativa	Munir o experimentador com as informações típicas de operação para que ele possa planejar os procedimentos operacionais
Tipo	Garantia do produto
Responsabilidade	Gerencial IAE
Relacionado a	REST-027
Tolerância	N/A
Verificação	Análise da documentação

5.2 Recomendações de Segurança

Durante o processo de identificação de requisitos também foram identificadas recomendações de segurança, apresentadas e estruturadas da mesma forma. As recomendações de segurança, podem ser consideradas boas práticas, não são obrigatórias e são identificadas conforme a Tabela 16.

Durante o processo também foram identificadas recomendações de implementação, cuja identificação adotada é “RI”. Estas são recomendações de soluções que, usualmente, atendem de forma satisfatória a um ou mais requisitos, mas sua aplicação não é obrigatória, nem mesmo as que apresentam necessariamente um desempenho ótimo para todos os casos. Todas as recomendações são apresentadas no Apêndice C. As recomendações de implementação são baseadas na experiência da equipe de integração de sistemas do IAE, e não são contempladas nas técnicas adotadas deste trabalho.

A seguir um exemplo de cada um dos tipos de recomendações identificadas neste trabalho.

Exemplo de recomendação de segurança

Quadro 4 Recomendação PR-004

Identificação	PR-009
Desempenho	As informações apresentadas pelo EGSE ao operador do experimento devem ter uma área mínima de visualização de 400mm^2. Com a menor dimensão de pelo menos 15 mm
Título	Área de visualização das informações no EGSE
Justificativa	Evitar julgamentos imprecisos por parte do operador
Tipo	Projeto
Responsabilidade	Técnica do experimentador
Relacionado a	REST-016
Tolerância	N/A
Verificação	Inspeção, demonstração, análise de documentação

Exemplo de recomendação de implementação

RI-004: Recomenda-se a substituição dos componentes que receberam estresse durante o desenvolvimento para o seu modelo de aceitação. Recomenda-se a substituição por componentes idênticos, porém novos.

5.3 Modelamento dos Requisitos de Segurança em SysML

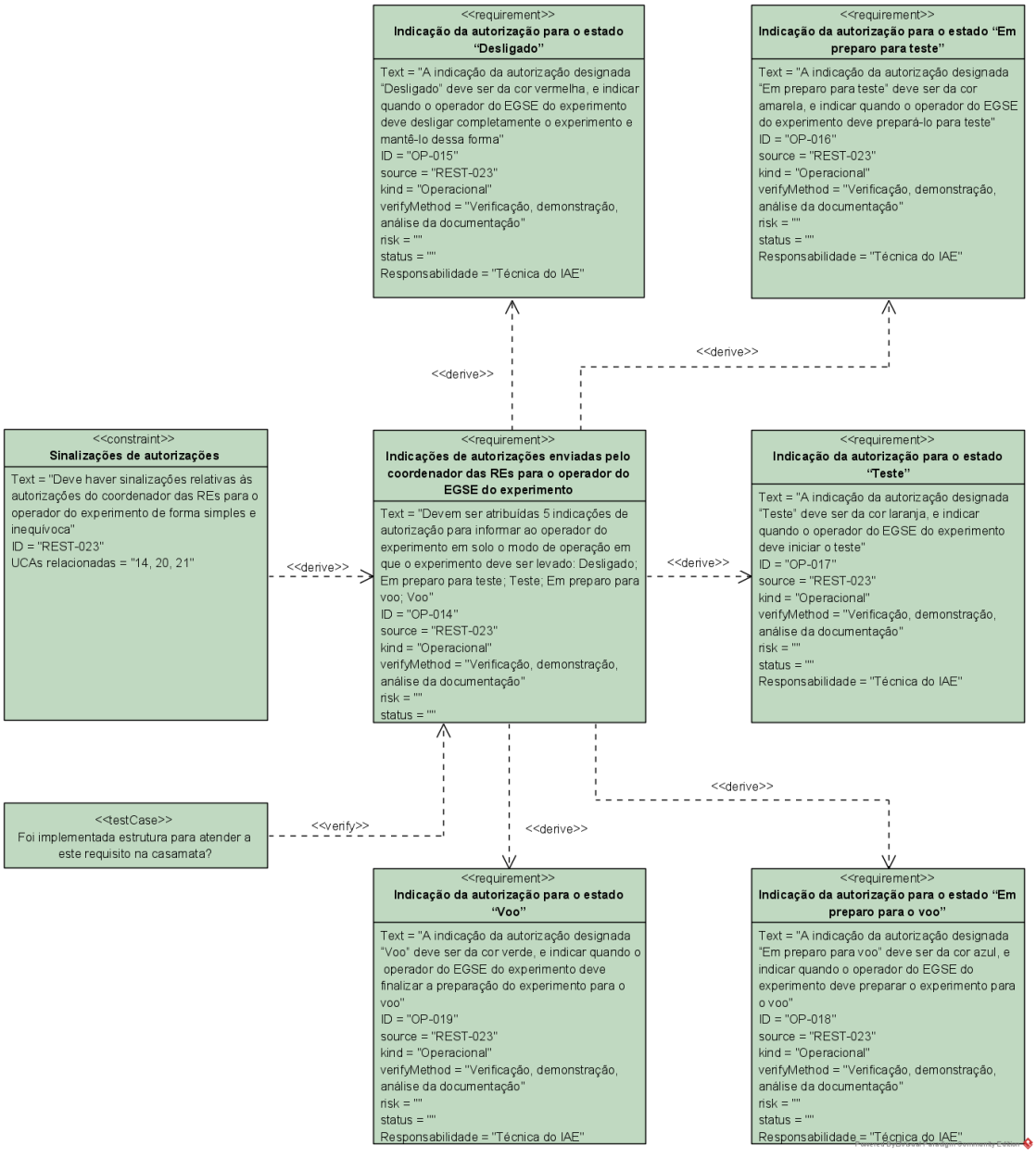
Os requisitos e as recomendações de segurança foram identificados, depois modelados em linguagem SysML, auxiliando na sua rastreabilidade com restrições de segurança. Os diagramas de requisitos SysML foram modelados no *software* “Visual Paragdim” versão 16.2. Foram elaborados 3 tipos de diagramas de requisitos, sendo eles: Diagramas de desenvolvimento; diagramas por responsabilidades; diagramas

por assuntos. Adicionalmente foi elaborado um diagrama de recomendações de segurança. Os tipos de diagramas são descritos a seguir.

5.3.1 Diagramas de Desenvolvimento

Cada um dos diagramas de desenvolvimento apresenta a relação de uma determinada restrição de segurança com os diversos requisitos e restrições de segurança dela derivados. Foram elaborados 28 diagramas deste tipo, um por restrição de segurança. Um exemplo de diagrama de desenvolvimento é apresentado na Figura 18 e todos os diagramas desse tipo podem ser encontrados no Apêndice D.

Figura 18 Diagrama de desenvolvimento da restrição de segurança REST-023.



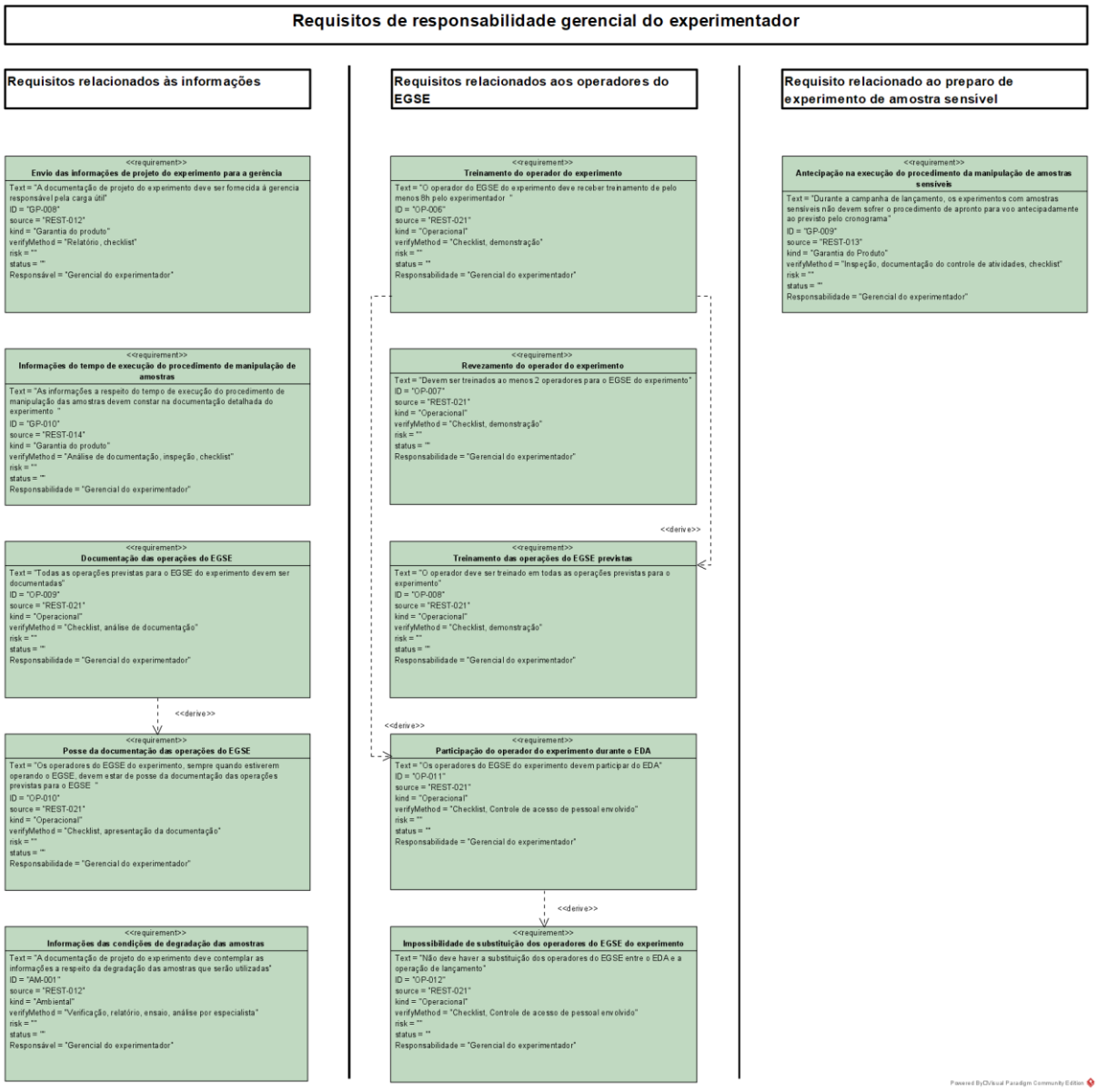
5.3.2 Diagramas por Responsabilidades

Estes diagramas apresentam o mesmo conjunto de requisitos apresentados nos diagramas de desenvolvimento, entretanto foram organizados em quatro grupos divididos por responsabilidades. Ao todo, foram elaborados 5 diagramas de responsabilidades, sendo eles:

- Requisitos de responsabilidade gerencial do IAE.
- Requisitos de responsabilidade técnica do IAE.
- Requisitos de responsabilidade gerencial do experimentador.
- Requisitos de responsabilidade técnica do experimentador - parte 1.
- Requisitos de responsabilidade técnica do experimentador - parte 2.

Um exemplo de diagrama de responsabilidade é apresentado na Figura 19, e todos os diagramas desse tipo podem ser encontrados no Apêndice E.

Figura 19 Diagrama de requisitos de responsabilidade gerencial do experimentador



5.3.3 Diagramas por Assuntos

Estes diagramas apresentam o mesmo conjunto de requisitos apresentados nos diagramas de desenvolvimento, entretanto foram organizados em 8 grupos divididos por assuntos. Ao todo foram elaborados 8 diagramas por assunto, sendo eles:

Grupo 1: Questões relacionadas com as competências e controles exercidos pelo IAE. Este grupo é composto por 14 requisitos, sendo mais relacionado ao IAE e gera impactos indiretos aos experimentos.

Grupo 2: Conteúdo e fluxo das informações entre o IAE e o experimentador. Este grupo é composto por 8 requisitos, o qual visa regular em que momento e quais são as informações que devem ser trocadas entre as equipes de experimentadores e do IAE.

Grupo 3: Questões relacionadas ao operador do EGSE do experimento. Este grupo é composto por 6 requisitos, tratando do treinamento e informações necessárias para o operador do EGSE e a equipe de experimentadores.

Grupo 4: Comunicação entre o coordenador das REs e o operador do EGSE do experimento durante o lançamento. Este grupo é composto por 14 requisitos, que trata das autorizações e indicações utilizadas na casamata durante a operação de lançamento.

Grupo 5: Questões relacionadas às amostras do experimento. Este grupo é composto por 7 requisitos, o qual trata do preparo de experimento com amostras sensíveis, validação de procedimento de manipulação de amostras, verificações do experimento e preparo do experimento para ensaios.

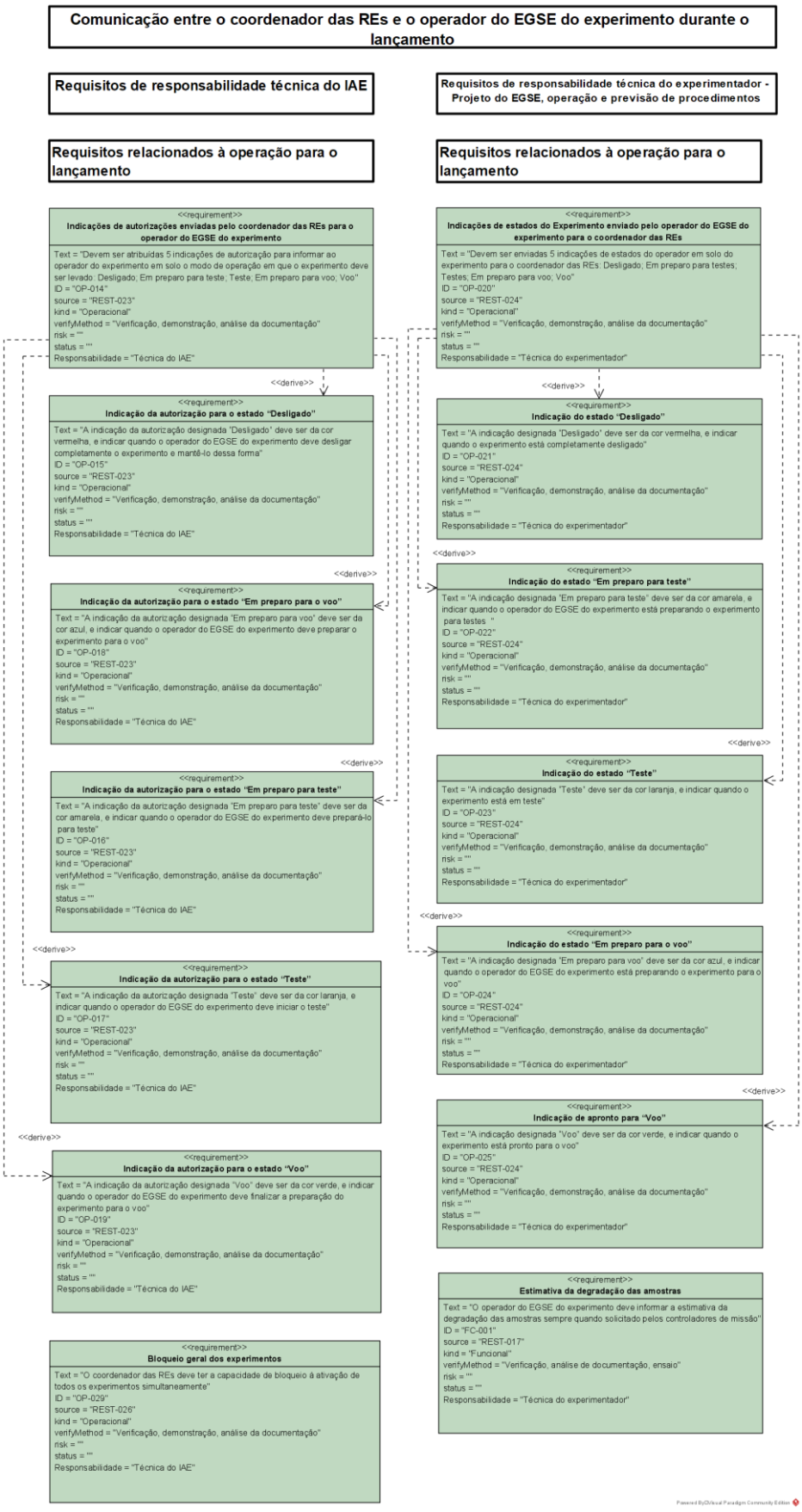
Grupo 6: Parâmetros de projeto para a parte embarcada do experimento. Este grupo é composto por 12 requisitos, o qual trata dos parâmetros para a construção física do experimento, parâmetros de verificações e dos sinais recebidos pelo experimento oriundos da carga útil.

Grupo 7: Procedimentos relacionados ao experimento. Este grupo é composto por 5 requisitos, que trata das verificações dos procedimentos do experimento e da previsão de procedimentos para a campanha de lançamento.

Grupo 8: Parâmetros de projeto e operação para o EGSE do experimento. Este grupo é composto por 8 requisitos, o qual trata de questões relacionadas aos comandos, informações e procedimentos do EGSE do experimento.

Um exemplo de diagrama por assunto é apresentado na Figura 20 e todos os diagramas desse tipo podem ser encontrados no Apêndice F.

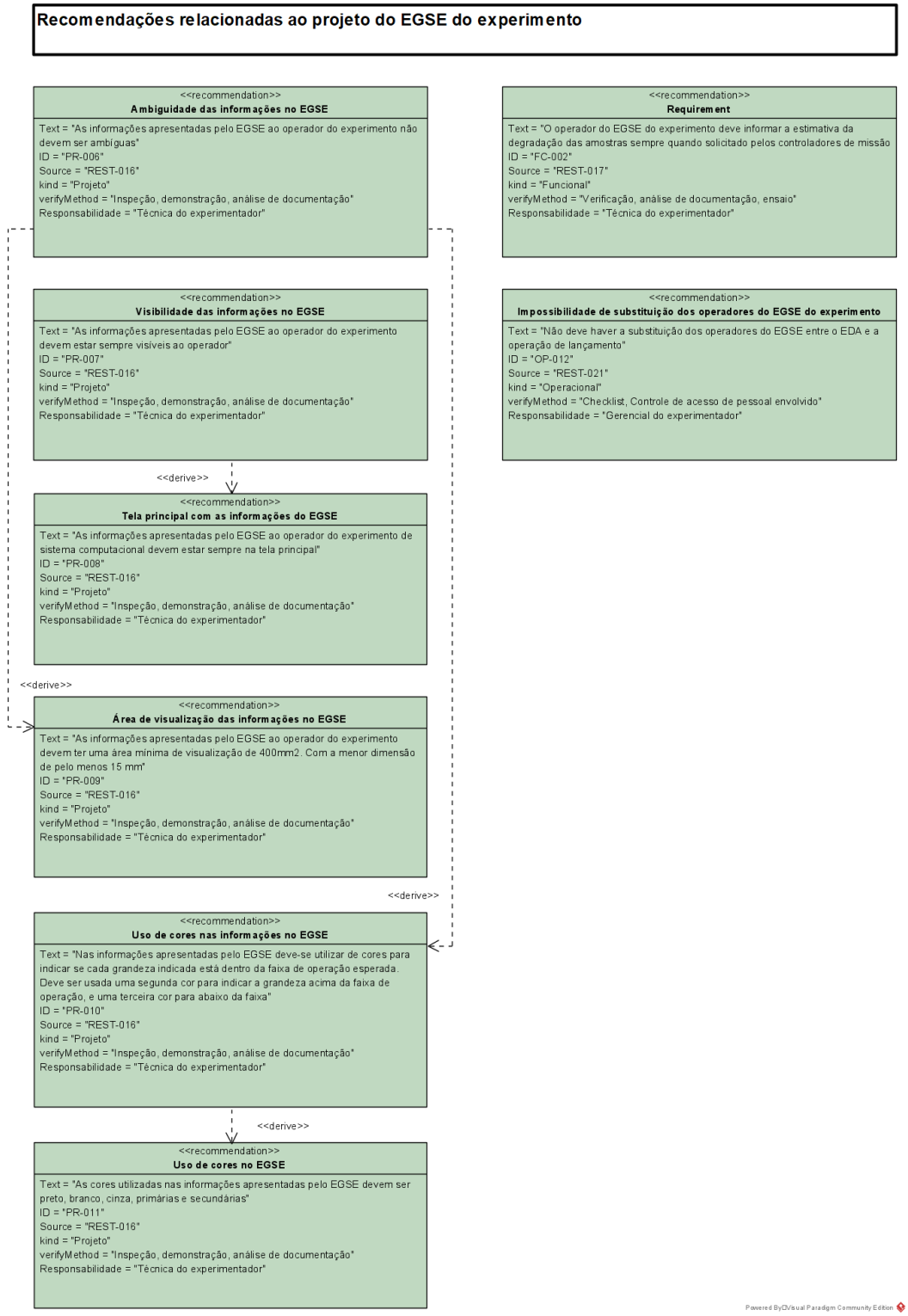
Figura 20 Diagrama por assunto. Grupo 4; comunicação entre o coordenador das REs e o operador do EGSE do experimento durante o lançamento.



5.3.4 Diagrama de Recomendações de Segurança

Este diagrama apresenta todas as recomendações de segurança identificadas neste trabalho e é apresentado na Figura 21.

Figura 21 Diagrama de recomendações de segurança.



Capítulo 6

AVALIAÇÃO DOS REQUISITOS DE SEGURANÇA

O objetivo deste capítulo é apresentar como foi planejada a avaliação dos requisitos de segurança, sua condução e seus resultados.

Após finalizado o modelamento do conjunto de requisitos em SysML e sua organização em 8 grupos, foi proposto um conjunto de perguntas para cada desses grupos.

O primeiro passo deste processo foi a submissão da proposta ao Comitê de Ética em Pesquisa. A seguir o termo de consentimento livre e esclarecido. Estes foram enviados ao Comitê de Ética em Pesquisa da UNIFESP, com os detalhes necessários para conduzir a avaliação. Após sua aprovação, os formulários de avaliação para cada um dos 8 grupos foram elaborados.

Todos os formulários de avaliação podem ser encontrados no Apêndice G.

6.1 Elaboração dos Questionários de Avaliação dos Requisitos de Segurança

Os 8 questionários elaborados, foram baseados na organização por assunto utilizada em 5.3.3, sendo um para cada grupo de requisitos de segurança e possuem todas as perguntas fundamentadas nos requisitos de segurança. Cada questionário está relacionado a um determinado grupo de requisitos como por exemplo; questionário 1 ao grupo 1 de requisitos, questionário 2 ao grupo de requisitos 2 e assim por diante.

As perguntas que analisam os requisitos de forma individual recebem o identificador “Requisito” com um número sequencial. As perguntas que analisam o

conjunto completo dos requisitos apresentados no questionário receberam o identificador “Questão” com um número sequencial. As respostas dos questionários foram baseadas na escala de Likert (LIKERT, 1932), adicionalmente, em cada pergunta também foi incluído um campo opcional para considerações, a fim de dar liberdade ao especialista fazer considerações particulares sobre o tópico tratado. Embora as respostas estejam em forma de texto, correspondem a uma escala de 1 a 5, onde a menor concordância com a afirmativa vale 1 e a maior concordância 5.

Os questionários foram distribuídos a dois grupos distintos de especialistas, o primeiro constituído por profissionais voltados aos experimentos científicos e o segundo por profissionais do IAE.

6.2 Aplicação dos Questionários de Avaliação dos Requisitos de Segurança

Considerando o número elevado da soma total de perguntas dos 8 questionários (96), considerou-se optar por distribuir 2 questionários por especialista. Dessa forma cada participante, dependendo da combinação de questionários recebidos, respondeu entre 18 e 32 perguntas. Os participantes foram divididos em dois grupos, conforme a sua filiação a seguir:

Grupo de especialistas 1: Experimentadores, responsáveis pelos experimentos embarcados. Àqueles cujo envolvimento seja superior a 1 (uma) missão de lançamento; servidores da AEB cujo trabalho é relacionado aos programas de experimentos científicos e pessoas da indústria com experiência em experimentos científicos espaciais.

Grupo de especialistas 2: Desenvolvedores e integradores. Servidores do IAE, da ativa e aposentados, com experiência em foguetes e/ou cargas úteis espaciais. Estes servidores tem experiência nos setores de: Eletrônica; Integração e testes; Projetos de sistemas espaciais e Gerência.

Foram distribuídos questionários a 12 pessoas pertencentes ao grupo de especialistas 1, obteve-se uma adesão total e dessa forma foram respondidos 24 questionários neste grupo. Enquanto no grupo de especialistas 2 foram distribuídos

questionários a 12 pessoas, com uma adesão de 9 e dessa forma foram respondidos 18 questionários neste grupo. A adesão total deste estudo foi de 87,5%, considerada satisfatória pelo autor. Os questionários foram enviados entre 6 e 7/05/2021, com data limite resposta em 21/05/2021. A Tabela 18 apresenta quais questionários cada participante respondeu.

Tabela 18 distribuição dos questionários respondidos pelos grupos de especialistas

Questionário	Participantes do grupo de especialistas 1			Participantes do grupo de especialistas 2		
1	3	6	9	4	9	
2	1	2	10	2	8	9
3	5	7	9	2	6	
4	2	4	10	1	5	
5	1	3	11	4	6	
6	4	8	12	3	7	
7	6	8	12	1	5	8
8	5	7	11	3	7	

Considerou-se como 5 ou mais a quantidade desejável de questionários respondidos para cada tipo e 4 como a quantidade mínima. É possível verificar pela Tabela 19 que foi obtida uma quantidade de respostas considerada como desejável.

Tabela 19 Quantidade de questionários respondidos por tipo, por grupo de especialista, e o total

	Grupo de especialistas 1	Grupo de especialistas 2	Total
Questionário 1	3	2	5
Questionário 2	3	3	6
Questionário 3	3	2	5
Questionário 4	3	2	5
Questionário 5	3	2	5
Questionário 6	3	2	5
Questionário 7	3	3	6
Questionário 8	3	2	5
Total	24	18	42

Para cada questionário as respostas contavam com pesos diferentes dependendo do grupo dos participantes. No questionário em que o assunto é mais relacionado ao experimento, o peso das respostas do Grupo de especialistas 1

(experimentadores) é superior ao do Grupo de especialistas 2 (desenvolvedores e integradores). Enquanto quando o assunto é mais relacionado à carga útil, informações entre as partes interessadas e questões da missão, o peso das respostas do Grupo de especialistas 2 (desenvolvedores e integradores) é superior ao do Grupo de especialistas 1 (experimentadores). A graduação e a quantidade de perguntas por questionário são apresentadas na Tabela 20. Os questionários foram aplicados com o uso do aplicativo *Google Forms*.

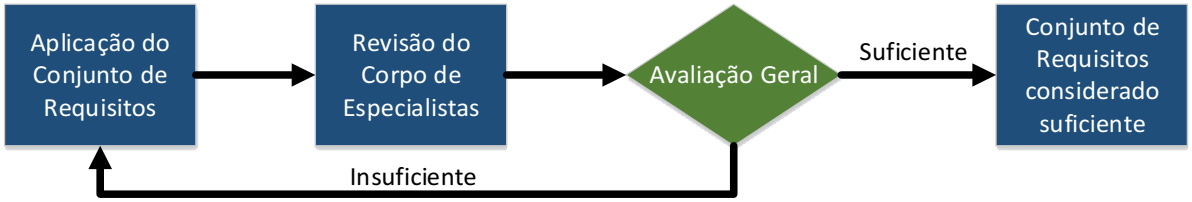
Tabela 20 Peso das respostas dos questionários por grupo

Questionário	Nº de perguntas	Peso aplicado ao grupo de especialistas 1	Peso aplicado ao grupo de especialistas 2
1	16	2	3
2	11	2	3
3	9	3	2
4	17	2	3
5	10	3	2
6	15	3	2
7	7	3	2
8	11	3	2

6.3 Coleta e Processamento das Informações Fornecidas pelos Especialistas

O conjunto de requisitos gerado neste trabalho foi avaliado pelos grupos de especialistas e as informações foram ponderadas conforme a Tabela 20. O conjunto de requisitos é considerado suficiente caso a avaliação geral seja superior a 70%, caso seja inferior, deve passar por uma revisão e ser novamente submetida ao corpo de especialistas, calculada através da Equação 1 e Equação 2. Para melhor entendimento o fluxograma do processo de avaliação é apresentado na Figura 22.

Figura 22 Fluxograma do processo de avaliação



Fonte: próprio autor

Equação 1 Cálculo da avaliação geral

$$Avaliação\ geral = \frac{\left(\left(Meg1\ x \frac{Page1}{5}\right) + \left(Meg2\ x \frac{Page2}{5}\right)\right)}{5} x\ 100$$

Legenda:

Meg1 = Média das notas para o grupo de especialistas 1

Page1 = Peso aplicado ao grupo de especialistas 1

Meg2 = Média das notas para o grupo de especialistas 2

Page2 = Peso aplicado ao grupo de especialistas 2

Equação 2 Cálculo da média das notas dos participantes

$$Meg = \frac{Soma\ das\ notas\ das\ questões}{numero\ de\ questões\ x\ número\ de\ participantes}$$

6.4 Discussão e Resultados

Inicialmente foi levantada a avaliação geral de cada um dos questionários, como o exemplo apresentado na Tabela 21. Todos os cálculos das avaliações gerais dos questionários podem ser encontrados no Apêndice H.

Tabela 21 Cálculo da avaliação geral do questionário 4

	Grupo de Especialistas 1				Grupo de Especialistas 2			
Questões	nota 1	nota 2	nota 3	Media	nota 1	nota 2		Media
1	5	5	5	15,00	5	4		9,00
2	5	5	4	14,00	5	4		9,00
3	5	5	4	14,00	5	3		8,00
4	5	5	4	14,00	5	3		8,00
5	5	5	5	15,00	5	3		8,00
6	5	5	2	12,00	5	4		9,00
7	5	4	2	11,00	5	5		10,00
8	5	5	5	15,00	5	5		10,00
9	5	5	5	15,00	5	4		9,00
10	5	5	5	15,00	5	3		8,00
11	5	5	5	15,00	5	3		8,00
12	5	5	5	15,00	5	3		8,00
13	5	5	5	15,00	5	4		9,00
14	5	5	3	13,00	5	5		10,00
q1	5	5	4	14,00	5	4		9,00
q2	5	4	4	13,00	5	4		9,00
q3	5	5	4	14,00	5	4		9,00
peso	2		media	4,69	peso	3	media	4,41
participantes	3			94%	participantes	2		88%

Avaliação geral	90,4%

O resultado da avaliação geral de cada um dos 8 questionários pode ser verificado na Tabela 22. Todas as avaliações gerais ultrapassaram um valor superior aos 70%. Dessa forma o conjunto de requisitos de cada um dos grupos foi considerado suficiente.

Tabela 22 Avaliação geral dos questionários

	Avaliação geral
Questionário 1	92,8%
Questionário 2	93,2%
Questionário 3	88,9%
Questionário 4	90,4%
Questionário 5	85,6%
Questionário 6	85,9%
Questionário 7	90,3%
Questionário 8	81,8%

As considerações dos campos de observações de cada um dos questionários, foram analisadas, organizadas e classificadas. Todas as 231 considerações podem

ser encontradas no Apêndice I, foram organizadas conforme o questionário e classificadas a seguir:

(1) Considerações relacionadas ao contexto: 9 considerações relacionados à problemas de interpretação do texto do requisito, indicação vaga e falta de contexto. Estas considerações não oferecem informações pertinentes.
(2) Considerações vagas ou imprecisas: 12 considerações com informações vagas ou imprecisas a respeito do assunto tratado. Estas considerações não oferecem informações precisas ou pertinentes.
(3) Considerações de concordância direta ou indireta: 127 considerações que reforçam o conceito do requisito ou questão. Estas considerações reforçam a importância dos requisitos de segurança. Porém, não oferecem novos dados a serem considerados.
(4) Considerações descartadas: 23 considerações baseadas em conceitos distintos ao usualmente aplicados à área tratada neste trabalho, ou cuja análise é parcial em relação ao assunto. Estas considerações não levam em conta a complexidade e os riscos das operações de lançamento ou partem de princípios que não se aplicam a área espacial.
(5) Considerações relacionadas à documentação: Total de 5 considerações relacionadas diretamente à documentação atualmente utilizada. Tratam-se de sugestões de melhorias relacionadas às informações que constam nos documentos, *templates* e distribuição de informações.
(6) Considerações atendidas: 4 considerações atendidas neste trabalho, pois não demandavam maiores discussões.
(7) Considerações de melhorias: 51 considerações que sugerem melhorias nos grupos de requisitos, porém demandam maiores discussões. Tratam em grande parte de assuntos não abordados neste estudo, assuntos que demandam desenvolvimento contando um maior número de especialistas, ou possíveis implementações.

As Considerações (1) relacionadas ao contexto; (2) vagas ou imprecisas e (4) considerações descartadas não necessitam de mais tratamento. Tendo em vista que não propiciam maiores discussões dos temas tratados. Pode-se notar que estas considerações não oferecem oportunidades de melhorias dos requisitos de segurança

e por esta razão foram desconsideradas. A seguir são apresentados 1 exemplo de cada tipo de consideração e uma discussão a respeito de cada:

Consideração (1) relacionada ao contexto, referente ao requisito MS-001: “Não consegui imaginar um contexto”.
Discussão: Não há informação pertinente na declaração. Não traz dados ou fatos novos à discussão.

Consideração (2) vaga ou imprecisa, referente ao requisito AM-001: Requisito parecido com de número 2.
Declaração do requisito AM-001: “*A documentação de projeto do experimento deve contemplar as informações a respeito da degradação das amostras que serão utilizadas.*”.
Declaração do requisito MS-001: “*As informações relacionadas à degradação das amostras dos experimentos, quando aplicável, devem ser utilizadas para o planejamento das atividades para a campanha de lançamento.*”.
Discussão: A declaração se refere às semelhanças dos requisitos AM-001 e MS-001. O requisito AM-001 aborda a necessidade da presença das informações relacionadas à degradação das amostras na documentação do experimento, enquanto o requisito MS-001 aborda a necessidade do uso destas informações para o planejamento das atividades da campanha de lançamento. Embora os requisitos tratem das mesmas informações, um trata na necessidade de ela ser informada, e o outro aborda o seu uso.

Consideração (4) descartada, referente ao requisito OP-002: Nem sempre é necessária uma experiência prévia do campo de lançamento para operar um sistema, pode-se ter um treinamento simulado. Porém o operador deve necessariamente conhecer previamente o sistema em teste e seu processo de aceitação de experimentos.
Declaração do requisito OP-002: “*A validação do procedimento de manipulação de amostras deve ser efetuada por equipe com conhecimento no campo de lançamento e no processo de aceitação de experimentos.*”. Responsabilidade: Técnica do IAE.
Discussão: A experiência requerida é relacionada à equipe de validação do procedimento de manipulação de amostras, esta equipe é formada por profissionais

com experiência no campo de lançamentos. Tal experiência é necessária para julgar se há condições do procedimento ser efetuado no campo de lançamentos.

As Considerações (3) de concordância direta ou indireta reforçam os requisitos de segurança e servem de confirmação da importância dele. Entretanto, não oferecem dados que possibilitem aprimoramentos aos requisitos propostos. Pode-se notar que estas considerações reforçam a necessidade dos requisitos de segurança dos quais se tratam. Todavia não oferecem oportunidades de melhorias, por esta razão não se fazem necessárias maiores discussões a respeito. A seguir são apresentados 3 exemplos e discussões a seu respeito:

Consideração referente ao requisito GP-008: Com toda certeza, estas duas equipes trabalham juntas, da mesma maneira que os experimentadores precisam receber informações, também devem repassar todas as suas informações sobre seu experimento. Estas duas partes devem estar casadas.
Declaração do requisito GP-008: "*A documentação de projeto do experimento deve ser fornecida à gerencia responsável pela carga útil.*".
Discussão: A consideração reforça a importância do requisito apresentando efeitos que se desejam obter com sua adoção: a troca de informações entre as equipes, assim como, a interação entre elas.

Consideração referente ao requisito OP-001: É importantíssimo considerar o ambiente de operação em todas as fases de projeto, desde a montagem, integração e teste, até a operação.
Declaração do requisito OP-001: "*A validação do procedimento de manipulação de amostras deve levar em conta as instalações e facilidades do campo de lançamento.*".
Discussão: A consideração reforça a importância do requisito salientando a questões relacionadas ao ambiente de operação de todas as fases de projeto. Neste caso, o requisito é aplicável à operação no campo de lançamentos, porém deve ser levado em consideração desde a fase de desenvolvimento.

Consideração referente ao requisito VR-010: O procedimento é parte de um conjunto de requisitos. Dessa forma, precisam ser verificados. De que adianta o pesquisador

requisitar uma geladeira capaz de atingir a temperatura de - 50 graus Celsius, se não há como garantir essa condição no transporte do experimento.

Declaração do requisito VR-010: "*O experimento e seu sistema devem ter seus procedimentos operacionais testados na fase de desenvolvimento.*".

Discussão: A consideração salienta a importância dos procedimentos se apresentarem factíveis, reforçando assim a necessidade de testá-los.

As considerações (6) atendidas tratavam de algumas definições necessárias para melhor definir certos aspectos de alguns requisitos. Entretanto, duas delas salientaram que o requisito OP-012 deveria ser reclassificado como uma recomendação, visto que poderia ser um impeditivo para o voo de experimentos sob determinadas circunstâncias e não necessariamente algo que traga riscos à operação ou experimento.

Consideração referente ao requisito OP-012: Esse não deveria ser um requisito. O operador pode ser substituído a qualquer momento, desde que por alguém em condições de operar o experimento. Esse requisito poderia inviabilizar um experimento, o que seria prejudicial ao programa.

Declaração da recomendação OP-012: "*Não deve haver a substituição dos operadores do EGSE entre o EDA e a operação de lançamento*.".

Consideração (3) de concordância direta, referente ao requisito OP-012: O ideal é que sejam os mesmos operadores. Aprende-se muito durante o EDA. Muitos aperfeiçoamentos são feitos após o EDA (na operação do EGSE, não no experimento).

Discussão: A consideração (6) atendida salienta que podem haver substituições de operadores sem que haja prejuízos para o experimento e campanha de lançamentos. Enquanto a consideração (3) de concordância direta, reforça sua importância para o aprimoramento da operação do EGSE. Por este motivo foi considerado pertinente a reclassificação do requisito como recomendação.

As considerações (5) relacionadas à documentação demandam mais discussões e transcendem o escopo deste trabalho. Entretanto, ensejam melhorias no sistema atual de documentação e têm potencial para propiciar uma melhor comunicação entre as partes interessadas. Serão discutidas em trabalhos futuros. A seguir é apresentado um exemplo e uma discussão a seu respeito:

Consideração referente ao requisito GP-008: O responsável pela carga-útil deve receber requisitos básicos/excepcionais das cargas. Muita informação mais atrapalha do que ajuda. Por exemplo: experimento necessita de refrigeração (o gerente precisa saber SEMPRE); o experimento deve ser devolvido ao experimentador tão logo seja recuperado (o gerente precisa saber sempre); O experimento possui duas baterias (essa informação é irrelevante para o gerente).
Discussão: A consideração apresenta necessidade de alteração nos *templates* dos documentos atualmente utilizados, que o escopo deste trabalho não contempla. Trata-se de uma observação pertinente, porém são necessárias discussões com mais profissionais da área pois ensejam alterações na estrutura de documentação atualmente empregada.

As considerações (5) de melhorias tratam do aumento de escopo dos requisitos, como por exemplo: requisitos voltados ao processo de carga e descarga de baterias, transporte, armazenamento, cabos, conectores elétricos, entre outros. Estas considerações também tratam de possíveis implementações para o atendimento dos requisitos. Estas discussões são pertinentes e serão discutidas em trabalhos futuros. A seguir são apresentados 3 exemplos e discussões a seu respeito:

Consideração referente ao requisito GP-006: Se for necessário para garantir a segurança geral. Cada experimento, a princípio, deve ter a calibração dos seus equipamentos de suporte, além da realização dos testes preliminares.
Declaração do requisito GP-006: "*A equipe gerencial do IAE deve verificar os certificados de calibração dos respectivos equipamentos de suporte.*".
Discussão: O requisito é aplicável aos equipamentos de suporte do IAE, entretanto a consideração expande o conceito aos equipamentos dos experimentos. Cabe nesse caso uma discussão mais aprofundada com os experimentadores para expandir este requisito aos experimentos ou oferecer aos experimentadores a mesma declaração como recomendação.

Consideração referente ao requisito PR-004: Os experimentadores precisam apenas do envelope de voo (cargas longitudinais e laterais, níveis de vibração, etc.). O restante, deve ser repassado por meio de um documento de controle de interfaces, para se ter compatibilidade com o sistema. Disponibilizando esses dados, documentos

e lista de testes, o experimentador poderá desenvolver seu experimento de forma a estar compatível com a plataforma.

Declaração do requisito PR-004: "*Todas as informações relativas aos testes, ensaios e procedimentos dos experimentos devem ser disponibilizadas aos experimentadores antes da fase de desenvolvimento.*".

Discussão: A consideração enseja uma possível implementação para a alteração do *template* dos documentos e da estrutura de documentação, cabe salientar que a forma de aplicação dos requisitos não é escopo deste trabalho. As implementações dos requisitos são trabalhos futuros.

Consideração referente ao grupo 6 de requisitos (questão 2 do questionário 6): Acredito que estes 12 requisitos são ainda um conjunto pequeno para classificar como "grande parte". Conectores, comunicação, cablagem, materiais permitidos, proteções para baterias, carga e descarga de bateria, alimentação do experimento via casamata, são alguns dos tópicos importantes que não foram cobertos nos 12 requisitos.

Grupo de requisitos 6: "*Parâmetros de projeto para a parte embarcada do experimento. Este grupo é composto por 12 requisitos e trata dos parâmetros para a construção física do experimento, parâmetros de verificações, e dos sinais recebidos pelo experimento oriundos da carga útil.*".

Questão 1: "*No ponto de vista de segurança da missão e carga útil. O grupo de requisitos (requisitos de 1 a 12) aborda em grande parte as características construtivas, de funcionalidade e de verificação de forma a mitigar os riscos oferecidos pelo experimento para a carga útil?*".

Discussão: A consideração é pertinente e atenta para a necessidade de expansão do conjunto de requisitos. Este estudo não contempla a área eletroeletrônica, materiais, baterias, entre outros. Estes assuntos serão abordados em trabalhos futuros.

Capítulo 7

ESTUDO DE CASO

O objetivo deste capítulo é apresentar como foi planejado o estudo de caso, sua condução e os resultados.

Uma vez que os 8 grupos de requisitos obtiveram avaliações gerais consideradas suficientes, o próximo passo desta pesquisa foi conduzir um estudo de caso com um experimento científico espacial.

Para executar este estudo de caso foi necessário, inicialmente, desenvolver questionários a fim de avaliar os impactos dos grupos de requisitos a um determinado experimento. Na sequência, foi selecionado um experimento e um experimentador experiente na área espacial, para responder aos questionários, tais quais, foram aplicados e respondidos através de entrevistas presenciais. As entrevistas duraram cerca de 10 horas, para que se conseguisse completar os 8 questionários. Por fim, as informações do estudo de caso foram analisadas, discutidas e identificados os aspectos positivos e os pontos referentes a melhorias.

7.1 Protocolo para Estudo de Caso

O protocolo para o estudo de caso foi definido conforme os passos descritos a seguir:

1 – Elaboração dos questionários para a coleta de dados.

2 – Seleção do experimento.

3 – Seleção do experimentador respondente.

4 – Condução das entrevistas e preenchimento dos questionários.

5 – Análise das respostas.

6 – Discussões dos resultados.

7.2 Questionários para o Estudo de Caso

A fim de avaliar a aplicação do conjunto de requisitos foram elaborados 8 questionários baseados nos diagramas por assunto apresentados em 5.3.3 e encontrados integralmente no Apêndice F. Diferente dos questionários do Capítulo 6, foram elaboradas perguntas de forma a obter respostas discursivas. Estes questionários visam obter respostas mais aprofundadas em relação à aplicação dos requisitos em um determinado experimento. Dentro de cada questionário, os requisitos foram organizados em conjuntos, por se tratar do mesmo assunto, focando perguntas específicas para estes conjuntos. Quando o requisito não se enquadrava em um conjunto, as perguntas foram tratadas de forma individual. A Tabela 23 apresenta o número de questões para avaliação de estudo de caso da aplicação dos requisitos em conjunto e individualmente.

Tabela 23 Número de questões por questionário para o estudo de caso

Questionário	Nº questões (conjunto de requisitos)	Nº questões (requisito individual)	Nº questões (total)
1	6	0	6
2	6	0	6
3	0	10	10
4	8	4	12
5	0	25	25
6	7	18	25
7	0	16	16
8	3	17	20

As perguntas dos questionários têm como objetivo identificar a necessidade de alterações físicas dos experimentos, procedimentos, viabilidade e demais impactos que o uso dos requisitos de segurança venham a gerar. As perguntas também têm como objetivo verificar a necessidade de aprimoramento dos requisitos ou de melhorias no contexto de sua aplicação. As informações respondidas pelos experimentadores foram mantidas de forma mais genérica a fim de preservar os

detalhes de projeto. Todos os questionários do estudo de caso estão disponíveis no Apêndice J, as respostas do estudo de caso se encontram no Apêndice K.

A seguir um exemplo das perguntas relacionadas a um conjunto de requisitos (questionário 4):
Perguntas a serem respondidas do ponto de vista do experimento, relacionadas aos requisitos OP-014, OP-015, OP-016, OP-017, OP-018 e OP-019:

- Estas indicações das autorizações enviadas pelo coordenador das REs são claras o suficiente?
- A quantidade de indicações é adequada?
- É possível dessa forma indicar (em grande parte) ao operador do EGSE do experimento quais são os procedimentos que podem ser executados?
- A implementação física destas indicações pode ser executada no EGSE do experimento ou é preferível que seja externo a ele?

A seguir um exemplo das perguntas relacionadas a requisito individual (questionário 5):
Perguntas a serem respondidas pelo ponto de vista do experimento em relação ao requisito OP-002:

- A validação do procedimento de manipulação de amostras pela equipe competente contribui para que o procedimento seja factível e viável no campo de lançamento?
- Quais são os impactos da validação do procedimento de manipulação de amostras para o experimento?
- Quais são os impactos da validação do procedimento de manipulação de amostras para a equipe de experimentadores?

7.3 Seleção do Experimento e Seleção do Experimentador para Responder aos Questionários

O estudo de caso foi efetuado no experimento denominado Estudo da Solidificação de Ligas Metálicas Eutéticas em Ambiente de Microgravidade (SLEM).

Este experimento é descrito em Toledo (2013). Foi convidado um experimentador com 41 anos de experiência na área espacial e que não participou da avaliação dos requisitos de segurança descritos no Capítulo 6 para desempenhar este estudo de caso. A coleta das informações foi efetuada através de entrevistas com o experimentador. Foram efetuadas 3 entrevistas ao todo, cujo tempo total foi de aproximadamente 10h, a fim de conduzir uma análise do experimento, da aplicação dos requisitos e, por fim, responder aos questionários. Foi avaliada a aplicação dos requisitos e respondidas as perguntas dos questionários 1 a 8.

O experimentador selecionado é um profissional pertencente a grupos de experimentadores que participaram do desenvolvimento, operação e lançamento de experimentos e sistemas espaciais.

7.4 Aplicação dos Questionários para Estudo de Caso

Assim que o protocolo de estudo de caso foi considerado pronto para uso, procedeu-se com sua execução. O experimentador foi contatado, os questionários para preenchimento foram entregues.

A seguir são apresentados os resultados do estudo de caso.

7.5 Resultados do Estudo de Caso

Nesta parte do estudo são descritos e discutidos os principais aspectos identificados pelas análises da aplicação dos requisitos de segurança no experimento SLEM. Deve-se levar em consideração que este experimento foi desenvolvido pelo INPE, instituto que tem experiência com artefatos espaciais, dessa forma atende a muitos dos requisitos propostos. Os desenvolvedores têm experiência no desenvolvimento de sistemas críticos, o instituto adota diversas boas práticas que são convergentes com os requisitos de segurança. Todas as respostas às perguntas propostas podem ser encontradas no Apêndice K. A seguir, são apresentados, de

forma resumida, as principais considerações e discussões quanto à adoção dos requisitos de segurança.

Consideração: Controle de ensaios gera maior formalização, considerando que os padrões a serem adotados devem ser preferencialmente os mesmos utilizados pelo IAE.
Origem da consideração: Esta consideração é referente ao Requisito GP-001, resposta da pergunta 1, do questionário 1.
Discussão: A consideração do experimentador e relação à adoção dos padrões de ensaios e de relatórios simplificam a formalização, documentação e padronização dos ensaios. Os padrões de relatórios, documentação e as informações de ensaios devem ser enviadas pelo IAE antes do desenvolvimento do experimento.

Consideração: Em relação ao requisito GP-006, o experimentador aponta que é importante deixar claro ao IAE que o requisito é aplicável. Adicionalmente o experimentador sugere que o mesmo teor deste requisito, pode ser oferecido ao experimentador como uma recomendação. Sugere, também, uma recomendação relacionada à manutenção preventiva dos equipamentos utilizados pelo experimentador.
Origem da consideração: Esta consideração é referente ao Requisito GP-006, resposta da pergunta 9, do questionário 1.
Discussão: O campo de justificativa do requisito GP-006 foi atualizado indicando que é aplicável aos equipamentos do IAE. As demais considerações são pertinentes, mas carecem de maiores discussões e podem levar ao aumento do conjunto de requisitos e recomendações.

Consideração: O experimentador sugere ampliar o assunto do requisito MS-001 para outras especificidades do experimento, não apenas relacionadas à amostra. Como temperatura, baterias, etc.
Origem da consideração: Esta consideração é referente ao Requisito MS-001, resposta da pergunta 2, do questionário 2.
Discussão: Trata do aumento do escopo do requisito. A consideração é válida, entretanto, para tal, se fazem necessárias maiores discussões, podendo dessa forma gerar novos requisitos.

Consideração: O experimentador sugere subdividir a documentação detalhada do experimento para que seja possível apresentar o projeto em etapas.
Origem da consideração: Esta consideração é referente ao Requisito OP-009, resposta da pergunta 7, do questionário 2.
Discussão: Diversas considerações de especialistas apontam para a necessidade de aprimoramento do sistema de documentação atualmente utilizado. Um novo modelo de documentação deve ser estudado a fim de atender melhor as partes interessadas.

Consideração: A equipe técnica responsável pela carga útil deve executar inspeções e análises intermediárias durante o desenvolvimento do experimento. Esta recomendação foi baseada nos processos aplicados aos experimentos durante a Missão Centenário. Durante esta missão os experimentos passaram por duas inspeções dos especialistas responsáveis pela carga útil da missão.
Origem da consideração: Esta se trata de uma consideração adicional que o experimentador ofereceu e não estava prevista em nenhum questionário. Ela foi registrada como consideração geral 3.
Discussão: Esta recomendação exige mudanças no programa de experimentos da AEB. Trata-se de uma recomendação pertinente, entretanto sua implementação exige maiores discussões e possivelmente restruturações no programa de experimentos.

Consideração: O experimento conta com duas barreiras de contenção das amostras, sendo possível verificar a falha da primeira contenção através de medida. As amostras, caso vazem, oferecem riscos ao experimento, mas não ao ambiente.
Origem da consideração: Esta consideração é um resumo das respostas oferecidas para as perguntas 11 a 15 do questionário 6. Estas respostas são relacionadas aos requisitos PR-002 e PR-003.
Discussão: A análise demonstra que o experimento atende aos requisitos PR-002 e PR-003.

Consideração: O percentual de partes passíveis de inspeção visual é de 80% para as partes mecânicas e em torno de 10% dos componentes eletroeletrônicos. Através de inspeções diretas e indiretas é possível inspecionar 90% do experimento.

Origem da consideração: Esta consideração é um resumo das respostas oferecidas para as perguntas 17 a 21 do questionário 6. Estas respostas são relacionadas ao requisito FS-001.
Discussão: A pesar de ser possível inspecionar o experimento de forma direta e indireta em um percentual de 90%, não é possível evidenciar partes soltas não visíveis que permaneçam em funcionamento. A inspeção visual é mais apropriada para avaliações de partes mecânicas. Este requisito auxilia na verificação do experimento, entretanto são necessários requisitos adicionais de verificação para evidenciar a integridade do experimento.

Consideração: A avaliação funcional do experimento pode ser executada pelo operador do EGSE do experimento, entretanto o experimentador é imprescindível para uma avaliação de desempenho.
Origem da consideração: Esta consideração é um resumo das respostas oferecidas para as perguntas 22 a 24 do questionário 6. Estas respostas são relacionadas aos requisitos VR-008, VR-009 e GP-013.
Discussão: O experimentador definiu quais são os responsáveis pela verificação de funcionamento e desempenho de seu experimento.

Consideração: Todos os procedimentos do experimento são passíveis de serem testados e aprovados até o fim do desenvolvimento. O teste dos procedimentos durante o desenvolvimento contribui para o aprimoramento, documentação e maior domínio por parte dos operadores.
Origem da consideração: Esta consideração é um resumo das respostas oferecidas para as perguntas 3 a 5 do questionário 7. Estas respostas são relacionadas ao requisito VR-011.
Discussão: Para atender ao requisito VR-011 gera maiores demandas para o experimentador, entretanto trata-se de uma demanda justificada.

Consideração: Em relação ao requisito PR-013 foi enviada uma lista piloto de possíveis situações passíveis de ocorrência. O requisito GP-015 trata do envio desta lista.
Declaração do requisito PR-013: "*Os procedimentos para a operação do experimento devem ser planejados para as situações de operação esperadas*.".

Declaração do requisito GP-015: “*Deve ser enviada uma lista das possíveis situações não nominais passíveis de ocorrência durante a missão aos experimentadores antes do desenvolvimento do experimento.*”.

A lista apresentada ao experimentador contém 3 itens descritos a seguir:

Item 1: “*O cronograma de ensaios é postergado em 6 meses após a entrega do experimento.*”.

Resposta do item 1: Deve-se devolver o experimento ao experimentador. Mesmo que isso implique na necessidade de uma nova aceitação.

Item 2: “*Ocorrem diversas (mais de 5) ativações da amostra do experimento durante o EDA*.”.

Resposta do item 2 para o EDA do experimento: Necessidade de trocar a amostra.

Resposta do item 2 para o EDA da carga útil: Não há problemas com uma ativação com temperatura mais baixa do que o nominal, usual para este ensaio.

Item 3: “*Necessidade de substituição de amostra no campo de lançamentos.*”.

Resposta do item 3: Não ocorreu antes. Mas são levadas, para a campanha de lançamento, amostras extras para eventual substituição, tendo ao menos, um membro da equipe do experimento capaz de executar o procedimento de troca de amostra.

Origem das considerações: Estas considerações são referentes às respostas oferecidas para as perguntas 6 a 8 do questionário 7 e ponderações adicionais às perguntas. Estas respostas são relacionadas aos requisitos PR-013 e GP-015.

Discussão: O experimentador salienta a importância desta lista ser enviada ao experimentador antes do início do desenvolvimento. Os impactos gerados por este requisito é o aumento da documentação e aumento do número de procedimentos.

Capítulo 8

CONCLUSÃO

Neste capítulo é apresentado um resumo da pesquisa, a retomada das questões de pesquisa, contribuições, a inserção social e perspectivas futuras.

O principal objetivo desta pesquisa foi propor um conjunto de requisitos de segurança que contribuam com a segurança dos experimentos científicos, carga útil, foguete e missão de lançamento. O objetivo secundário foi oferecer um modelo de investigação de requisitos que propicie a ampliação desta pesquisa ou que possa servir como base para a identificação de requisitos de segurança de outros projetos espaciais. As etapas definidas para o desenvolvimento deste trabalho foram atendidas e registradas ao longo desta dissertação.

No Capítulo 2 se descreveu a revisão da literatura desta pesquisa, apresentando os principais conceitos necessários para o desenvolvimento deste trabalho. Este capítulo conta com uma fundamentação teórica que expõe conceitos básicos sobre foguetes, cargas úteis, missão de lançamento e o ciclo de vida. Adicionalmente, mostra um resumo das falhas ocorridas nos últimos 20 anos no programa espacial brasileiro. Exibe uma breve descrição da técnica STPA e dos modelos em SysML, os quais foram utilizados para o desenvolvimento deste trabalho.

No Capítulo 3 se descreveu a metodologia adotada nesta pesquisa, que direciona as etapas conduzidas do trabalho aqui apresentado.

No Capítulo 4 se discorreu a respeito de todas as etapas da análise STPA executada. Como o material é extenso, optou-se por inserir parte dele no Apêndice A.

No Capítulo 5 se apresentou o desenvolvimento dos requisitos de segurança a partir das restrições de segurança do capítulo anterior, bem como sua modelagem na linguagem SysML. Os diagramas SysML foram organizados em 3 formas distintas, sendo que os diagramas por assuntos foram escolhidos para serem utilizados nas demais etapas. Parte do material do deste capítulo foram alocadas nos Apêndices B, C, D, E, F.

No Capítulo 6 se apresentou a avaliação do conjunto de requisitos identificados no Capítulo 5. Inicialmente foi descrita a elaboração dos questionários, a distribuição e aplicação deles para os especialistas. Também foi descrita a coleta e a análise das informações que avaliaram o conjunto de requisitos. Devido à extensão do material, parte dele foi alocado nos Apêndices G, H, I.

No Capítulo 7 foi apresentado um estudo de caso a fim de avaliar a aplicação do conjunto de requisitos nos experimentos científicos. Foi avaliada a aplicação dos requisitos no experimento SLEM do INPE, os principais resultados são apresentados no mesmo capítulo.

8.1 Questões de Pesquisa

Questão 1: A modelagem SysML aplicada aos requisitos de segurança contribui com a sua organização e elaboração?

Inicialmente os requisitos foram modelados em SysML organizados de forma a mapear a relação entre as restrições de segurança e os requisitos de segurança, estes foram denominados diagramas de desenvolvimento. Percebemos que estes diagramas eram úteis para mapear e até mesmo expandir o conjunto de requisitos, contribuindo assim para sua elaboração. Porém para a apresentação para as partes interessadas estes diagramas se demonstraram menos intuitivos se comparados aos demais elaborados ao longo deste trabalho.

Foram elaborados diagramas de requisitos organizados com foco nas partes interessadas, estes foram denominados diagramas por responsabilidades. Estes diagramas tem como objetivo apresentar às partes interessadas os requisitos que são de sua responsabilidade.

Os diagramas por assunto foram organizados de forma a agregar os requisitos que tratam de do mesmo assunto ou de assunto similar. Esta organização se demonstrou útil para a avaliação dos requisitos.

O SysML contribuiu com a organização dos requisitos de forma a atender objetivos específicos neste trabalho.

Questão 2: Quais os aspectos mais importantes a se considerar na adoção do *template* de requisitos de segurança?

A investigação efetuada através da técnica STPA e posterior identificação dos requisitos exige profissionais com experiência na área abordada. É importante estabelecer um canal de comunicação com os profissionais detentores de conhecimentos técnicos específicos da área de fornecimento do serviço, como por exemplo, os profissionais do IAE; usuários do sistema com experiência em campo, como por exemplo, os experimentadores científicos; especialistas na área de regulação e subsídio, como por exemplo, os profissionais da AEB e os profissionais da indústria, como por exemplo, profissionais das diversas empresas ligadas ao programa aeroespacial brasileiro.

Para que a análise com a técnica STPA seja conduzida de forma competente, se faz necessário o domínio da técnica. A fim de se obter um resultado satisfatório para a mitigação dos perigos relacionados ao objeto de análise, deve-se reconhecer quais são as principais perdas que se deseja evitar e, consequentemente, os principais perigos a serem eliminados ou mitigados.

Para a adoção do *template* de requisitos por parte das partes interessadas, se faz necessário ater-se às suas realidades institucionais, para que as exigências do conjunto de requisitos sejam compatíveis para seu atendimento. Por outro lado, deve-se balancear os critérios mínimos para que os riscos sejam devidamente mitigados. Através das considerações do experimentador que respondeu os questionários do estudo de caso, apresentada no Capítulo 7, foi evidenciada a necessidade da distribuição de um material adicional aos experimentadores. Este material deve contribuir na compreensão do contexto da aplicação do conjunto de requisitos em relação aos experimentos. Assim não apenas contribui com o experimentador que possui experiência, como também auxilia os novos experimentadores.

Questão 3: De que forma o uso de STPA auxilia na identificação dos requisitos de segurança?

Para a condução da análise STPA se faz necessário conhecimento da técnica e acesso a profissionais com experiência na área espacial. É ideal que o facilitador da análise tenha experiência na área espacial, pois isto contribui com a comunicação entre as partes e o processo de documentação da análise sejam efetivos. Conciliar as agendas entre o analista que executou a aplicação do STPA com a dos profissionais,

foi uma tarefa que demandou mais tempo do que o previsto e acabou por alongar o cronograma.

É comum que as visões distintas dos profissionais da área espacial apontem para problemas distintos. Foi necessário selecionar quais as perdas e perigos deveriam ser abordados na análise. Estas escolhas foram feitas pelo autor e condutor da análise STPA, sendo baseadas em sua experiência na área espacial. Deve-se ressaltar que os critérios para a seleção não estavam estabelecidos.

Ao conduzir a técnica STPA, se mapeiam os perigos, ações de controle inseguras, cenários de perdas e por fim oferece restrições de segurança. Estas restrições são utilizadas como ponto de partida para a identificação de requisitos de segurança. Os requisitos de segurança detalham e agregam os elementos necessários para que seja possível atender à restrição de segurança. Isto é evidenciado nos Capítulos 4 e 5.

Adicionalmente às questões de pesquisa foram avaliados estes dois quesitos a seguir:
Compreensão dos requisitos de segurança.

É possível avaliar a compreensão dos requisitos de segurança através das respostas dos especialistas apresentadas no Capítulo 6, cuja lista completa pode ser encontrada no Apêndice I. Os especialistas responderam no campo de observações o total de 231 considerações, sendo que destas 9 apresentaram problemas na compreensão da declaração do requisito de segurança. Nesse caso, os problemas de compreensão foram de 9/231, portanto de 3,9%, enquanto a compreensão se demonstrou eficaz em 96,1% das considerações referentes aos requisitos. Este índice de compreensão foi considerado suficiente pelo autor.

Contribuição para a elaboração dos experimentos.

Do total de 231 considerações respondidas no campo de observações pelos especialistas, apresentadas no Capítulo 6 e Apêndice I, 127 delas são de concordância em relação à declaração do requisito de forma direta ou indireta. Foram obtidas 4 considerações, nas respostas dos questionários dos especialistas, que provocaram alterações neste trabalho. Cinco considerações relacionadas ao aprimoramento do sistema de documentação atualmente utilizado. Bem como, obtiveram-se 51 sugestões de melhorias do conjunto de requisitos, sendo que parte dessas tratam da expansão do escopo. Dessa forma, foram contabilizadas 187

considerações que apresentam elementos de concordância com o conjunto de requisitos apresentados, totalizando 80,95% de considerações que lhe dão suporte. Este índice de suporte foi considerado suficiente pelo autor.

8.2 Contribuições

A principal contribuição desta pesquisa é oferecer um conjunto de requisitos de segurança que contribua com a segurança de foguetes suborbitais, cargas úteis, experimentos e da segurança da missão de lançamento. Este conjunto de requisitos tem como objetivo eliminar ou mitigar perdas no âmbito da missão de lançamento como um todo, tanto para os experimentos científicos, quanto para os demais artefatos espaciais.

Outra contribuição é o processo utilizado para a identificação do conjunto de requisitos de segurança, o qual é suficientemente flexível para identificar requisitos para os artefatos espaciais relacionados a voos de foguetes suborbitais em outros projetos. Este processo foi descrito ao longo deste trabalho para que outras análises possam ser executadas a fim de identificar novos conjuntos de requisitos de segurança.

Além do conjunto de requisitos de segurança e o processo para sua identificação, foram estabelecidos processos de avaliação com especialistas e de estudo de caso, a fim de se analisar a aplicação do conjunto de requisitos desenvolvido.

A contextualização inicial deste trabalho, no Capítulo 2, traz informações, que devidamente oferecidas às universidades e institutos de pesquisa, podem incentivar novos experimentadores científicos a participarem de forma satisfatória no programa espacial brasileiro. Este aumento de participação pode gerar novas demandas e, consequentemente, aumentar a frequência de lançamentos no Brasil.

8.3 Inserção Social

Grande parte dos experimentadores científicos são vinculados a universidades, ou a institutos de pesquisa. O experimentador chefe, muitas vezes, tem o perfil acadêmico e coordena diversas atividades, desta forma, nem sempre tem como atribuição o desenvolvimento dos equipamentos e sistemas a serem embarcados na carga útil. É importante que as informações para o desenvolvimento e construção do experimento científico estejam disponíveis a toda sua equipe. Este trabalho vem ao encontro desta demanda, tendo em vista que oferece um conjunto de requisitos de segurança que deve ser distribuído, em conjunto com as documentações necessárias, antes do início do desenvolvimento do experimento.

O IAE oferece ensaios, verifica e integra os experimentos na carga útil, o conjunto de requisitos de segurança, identificado neste trabalho, também é endereçado a estas partes interessadas. Este conjunto de requisitos oferece parâmetros aplicados aos ensaios, verificações e integração dos experimentos, que por sua vez, dão suporte às decisões técnicas e gerenciais, para a gerência responsável pelo lançamento.

Adicionalmente ao IAE e AEB o processo de identificação de requisitos de segurança pode ser utilizado para a sua expansão e aplicado a outros projetos relacionados.

O conjunto de requisitos identificados neste trabalho, também trata da comunicação entre as partes interessadas. Esta comunicação ocorre entre os experimentadores, o IAE e a AEB, a qual estabelece o canal de comunicação entre as partes.

As empresas brasileiras da área espacial podem se beneficiar com este conjunto de requisitos de segurança, uma vez que estes podem assumir o papel de desenvolvedores de equipamentos e sistemas para os experimentadores, AEB e IAE.

8.4 Perspectivas Futuras

Ao longo do desenvolvimento deste trabalho surgiram algumas questões apontadas pelos especialistas apresentados no Capítulo 6 e no estudo de caso do Capítulo 7, que são apresentadas a seguir:

- Expansão do conjunto de requisitos, contando com assuntos ainda não tratados neste trabalho, mas evidenciados como pertinentes pelos especialistas. Como por exemplo, requisitos para baterias elétricas, transporte dos experimentos, manutenção e inspeção dos equipamentos de suporte, entre outros;
- Aprimoramento do sistema de documentação, com um *template* mais adequado a fim de prover uma comunicação mais eficiente entre as partes interessadas;
- Estudos para a adoção de um processo de inspeções periódicas durante o desenvolvimento do experimento;
- Elaboração de material de suporte aos experimentadores iniciantes, a fim de auxiliar na contextualização da aplicação dos requisitos.

A implementação do conjunto de requisitos identificados neste trabalho no contexto prático do desenvolvimento de projetos espaciais irá tratar de forma mais aprofundada os óbices e necessidades para sua adoção. Esta próxima etapa, deverá trazer novos elementos a serem considerados. Pode-se afirmar que esta pesquisa apresenta um conjunto de requisitos de segurança viável para ser implementado no contexto das organizações envolvidas neste domínio do conhecimento, abrindo novas possibilidades e considerações práticas que contribuirão significativamente nos novos projetos de experimentos espaciais no Brasil.

REFERÊNCIAS

Agência Espacial Brasileira. **Programa Nacional de Atividades Espaciais, PNAE: 2012-2021**. Brasília: Agência Espacial Brasileira, 2012.

Agência Espacial Brasileira. **Vol 1 Regulamento Geral da segurança espacial**. Brasília: Agência Espacial Brasileira, 2020. Disponível em: https://www.gov.br/aeb/pt-br/servicos/regulamentos-de-seguranca-do-setor-espacial/documentos/vol_1_regulamento_geral_da_seguranca_espacial.pdf/@@download/file/vol_1_regulamento_geral_da_seguranca_espacial.pdf. Acesso em 18 mai. 2022.

Agência Espacial Brasileira. **Parte 4 Regulamento Técnico da Segurança para Carga Útil**. Brasília: Agência Espacial Brasileira, 2020. Disponível em: https://www.gov.br/aeb/pt-br/servicos/regulamentos-de-seguranca-do-setor-espacial/documentos/parte_4_regulamento_tecnico_da_seguranca_para_carga_util.pdf/@@download/file/parte_4_regulamento_tecnico_da_seguranca_para_carg.pdf. Acesso em 18 mai. 2022.

BAHILL T., HENDERSON S. Requirements Development, Verification and Validation Exhibited in Famous Failures. **The Journal of the International Council on Systems Engineering**, publicado em nome de International Council on Systems Engineering (INCOSE). 8, 1. p. 1-14. 2005.

BALL A. **Identification of Leading Indicators for Producibility Risk in Early-Stage Aerospace Product Development**. Dissertação (Master Business Administration and Master of Science in Aeronautics and Astronautics) – Sloan School of Management and Department of Aeronautics and Astronautics, Massachusetts Institute of Technology, Cambridge, MA, EUA, 2015. Disponível em: https://dspace.mit.edu/bitstream/handle/1721.1/98976/921150418-MIT.pdf?sequence=1&isAllowed=y. Acesso em 20 jun. 2020.

DULAC N. **A Framework for Dynamic Safety and Risk Management Modeling in Complex Engineering Systems**. Tese (Doctor of Philosophy) – Department of Aeronautics and Astronautics, Massachusetts Institute of Technology, Cambridge, MA, EUA, 2007. Disponível em: https://dspace.mit.edu/bitstream/handle/1721.1/42175/228864574-MIT.pdf?sequence=2&isAllowed=y. Acesso em 19 jun. 2020.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY. **Demonstration of a New Dynamic Approach to Risk Analysis for NASA's Constellation Program**, Cambridge, MA, EUA, 2007. Disponível em: sunnyday.mit.edu%2FESMD-Final-Report.pdf&usg=AOvVaw2fmEKNW0yxvMdynPvFe_dL. Acesso em 15 jun. 2020.

DUNN N. **Satellite System Safety Analysis Using STPA**. Dissertação (Master of Science in Aeronautics and Astronautics) – Department of Aeronautics and Astronautics, Massachusetts Institute of Technology, Cambridge, MA, EUA, 2013.

Disponível em: https://dspace.mit.edu/bitstream/handle/1721.1/85777/871340076-MIT.pdf?sequence=2&isAllowed=y. Acesso em 25 jun. 2020.

EUROPEAN COOPERATION FOR SPACE STANDARDIZATION – ECSS. **ECSS-E-ST-10-06C Rev.1**: Space Engineering – Technical requirements specification. 2017. Noordwijk, The Netherlands, 2017.

Agência Espacial Brasileira. **Experimentos Suborbitais de Microgravidade**. Brasília: Agência Espacial Brasileira, 2008. Disponível em: http://portal-antigo.aeb.gov.br/ experimentos-suborbitais-de-microgravidade/. Acesso em: 20 mar. 2020.

FLEMING C., ISHIMATSU T., MIYAMOTO Y., NAKAO H., KATAHIRA M., HOSHINO N., THOMAS J., LEVESON N. Safety-Guided Spacecraft Design using Model-Based-Specifications. *In* International Association for the Advancement of Space Safety Conference, 2011. Versailles, França. [**Anais**]. Versailles, França, 2011. DOI: https://doi.org/10.2514/1.I010164.

FLEMING C.; LEVESON N. Improving Hazard Analysis and Certification of Integrated Modular Avionics. **Journal of Aerospace Information Systems**. Vol. 11, N. 6, p. 397 a 411, 2014. DOI: https://doi.org/10.2514/1.I010164.

FLEMING C. **Safety-Driven Early Concept Analysis and Development**. Tese (Doctor of Philosophy) – Department of Aeronautics and Astronautics, Massachusetts Institute of Technology, Cambridge, MA, EUA, 2015. Disponível em: https://dspace.mit.edu/bitstream/handle/1721.1/97352/910627166-MIT.pdf?sequence=1&isAllowed=y. Acesso em 25 jun. 2020.

FRIEDENTHAL S., MOORE A., STEINER R. **A Practical Guide to SysML**. 3. ed. Amsterdam: Morgan Kaufmann / Object Management Group / Elsevier, 2014. ISBN: 9780128008003.

GARCIA A., YAMANAKA S., BARBOSA A., BIZARRIA F., JUNG W., SCHEUERPFLUG F. VSB-30 sounding rocket: history of flight performance. **Journal of Aerospace Technology and Management**. São José dos Campos, Vol.3, No.3, pp. 325-330. 2011. DOI: 10.5028/jatm.2011.03032211.

HALLIGAN R. **Requirements Analysis that Works**. Melbourne, Australia: Project Performance International. 2017. Disponível em: https://www.ppi-int.com/requirements-analysis-that-works/. Acesso em 30 ago. 2020.

HARVEY B., SMID H., PIRARD T. **Emerging Space Powers**: The New Space Programs of Asia, the Middle East, and South America. Capítulo 10. Praxis, 2010. ISBN: 978-1-4419-0874-2.

HERRING M.; OWENS B.; LEVESON N.; INGHAN M.; WEISS K. **Safety-Driven Model-Based** Part I: Methodology Description. 2007. Disponível em: http://sunnyday.mit.edu/JPL-Part-1.pdf. Acesso em 10 ago. 2020.

INTERNATIONAL COUNCIL ON SYSTEMS ENGINEERING – INCOSE. **INCOSE-TP-2004-004-02**. Systems Engineering Vision 2020. 2007. Seatle, WA, EUA. 2007.

INSTITUTO DE AERONÁUTICA E ESPAÇO. **Relatório de Atividades 2010**. São José dos Campos, SP: DCTA 2011. Disponível em: http://www.iae.cta.br/Arquivos/Relatorio_de_atividadades_2010.pdf. Acesso em: 22 jun. 2020.

INSTITUTO DE AERONÁUTICA E ESPAÇO. **Relatório de Atividades 2011**. São José dos Campos, SP: DCTA 2012. Disponível em: http://www.iae.cta.br/Arquivos/Relatorio_de_atividades_2011.pdf. Acesso em: 22 jun. 2020.

INSTITUTO DE AERONÁUTICA E ESPAÇO. **Relatório de Atividades 2014**. São José dos Campos, SP: DCTA 2015. Disponível em: https://drive.google.com/open?id=0B0aF_L6jHhDReE1LRlpyeWpJTzg. Acesso em: 22 jun. 2020.

INSTITUTO DE AERONÁUTICA E ESPAÇO. **Relatório de Atividades 2016-2017**. São José dos Campos, SP: DCTA 2018. Disponível em: http://www.iae.cta.br/images/relatorios-atividades/Relatorio_de_Atividades_2016-2017.pdf. 2017. Acesso em: 22 jun. 2020.

INSTITUTO DE AERONÁUTICA E ESPAÇO. **Relatório de Atividades 2018**. São José dos Campos, SP: DCTA 2019. Disponível em: http://www.iae.cta.br/images/relatorios-atividades/Relatorio_de_Atividades_2018_Final.pdf. Acesso em: 22 jun. 2020.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC/IEEE 24765:2017(E)**: Systems and software engineering - Vocabulary 2017. ISBN:978-1-5044-4118-6.

ISHIMATSU T., LEVESON N., THOMAS J., KATAHIRA M., MIYAMOTO Y., NAKAO H. Modeling and Hazard Analysis Using STPA. *In* Conference of the International Association for the Advancement of Space Safety, 2010. Huntsville, Alabama, EUA. [**Anais**] 2010. Huntsville, Alabama, EUA, 2011. ISSN 1609-042X.

ISHIMATSU T.; LEVESON N.; THOMAS J.; FLEMING C., KATAHIRA M.; MIYAMOTO Y.; UJIIE R.; NAKAO H.; HOSHINO N. Hazard Analysis of Complex Spacecraft using Systems Theoretic Process Analysis. **Journal of Spacecraft and Rockets** Vol. 51, No. 2, 2014. DOI: https://doi.org/10.2514/1.A32449.

KAR P., BAILEY M. Characteristics of Good Requirements. *In* INCOSE International Symposium 6, 1, 1996. Boston, MA, EUA [**Anais**]. Boston, MA, EUA, 1996. DOI:10.1002/J.2334-5837.1996.TB02142.X

LAHOZ C, MEDEIROS S. Systematic Review on STPA: Final Results. *In* MIT STAMP Workshop, 2016. Cambridge, MA, EUA [**Anais**]. Cambridge, MA, EUA, 2016. Disponível em: http://psas.scripts.mit.edu/home/wp-content/uploads/2016/01/30-LahozMedeiros-W2016.pdf. Acesso em: 10 jul. 2020.

LEVESON N. **CAST Handbook**: How to Learn More from Incidents and Accidents. Cambridge, MA, EUA, 2019. Disponível em: http://psas.scripts.mit.edu/home/get_file4.php?name=CAST_handbook.pdf. 2019. Acesso em: 26 jun. 2020.

LEVESON N.; DULAC N.; BARRET B.; CAROLL J.; CUTCHER-GERSHENFELD J.; FRIEDENTHAL S. **Risk Analysis of NASA Independent Technical Authority.** 2005. Disponível em: http://sunnyday.mit.edu/ITA-Risk-Analysis.doc. Acesso em 12 ago. 2020.

LEVESON N. **Engineering a Safer World**: Systems Thinking Applied to Safety. Massachusetts, EUA: The MIT Press, 2012. Disponível em: http://psas.scripts.mit.edu/home/get_file4.php?name=CAST_handbook.pdf. 2019. Acesso em: 26 jun. 2020. ISBN 10: 0262016621

LEVESON N.; THOMAS J. **STPA HANDBOOK**. Cambridge, MA, EUA, 2018. Disponível em: http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf. 2018. Acesso em: 27 fev. 2020.

LIKERT R. A Technique for the measurement of attitudes. **Archives of psychology** N$_o$ 140. NY, New York, 1932. p. 5-55.

LUCCA E. The Brazilian Sounding Rocket VSB-30: Meeting the Brazilian Space Program and COPUOS objectives. *In* Committee on the Peaceful Uses of Outer Space – UNOOSA Conference 2014. United Nations, Vienna, Austria [**Anais**]. Vienna, Austria, 2014. Disponível em: http://www.unoosa.org/pdf/pres/stsc2014/tech-44E.pdf. Acesso em: 11 jun. 2020.

NAKAO H.; KATAHIRA M.; MIYAMOTO Y.; LEVESON N. Safety Guided Design of Crew Return Vehicle in Concept Design Phase Using STAMP/STPA. *In* 5th IAASS conference 'A safer space for a safer world' 2011. Versailles, França [**Anais**]. ISBN: 9789290922636 929092263X.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION. **NASA SP-2016-6105** Rev2. NASA Systems Engineering Handbook 2007. Disponível em: https://nasa.gov/sites/default/files/atoms/files/nasa_systems_engineering_handbook_0.pdf. Acesso em: 21 fev. 2020. ISBN: 9781680920918.

OWENS B.; Crocker A. SimSup's loop: a control theory approach to spacecraft operator training. *In* IEEE Aerospace Conference Proceedings, 2015. MT, EUA [**Anais**]. MT, EUA, 2015. DOI:10.1109/AERO.2015.7118921.

OWENS B.; HERRING M.; DULAC N.; LEVESON N. Application of a Safety-Driven Design Methodology to an Outer Planet Exploration Mission. *In* IEEE Aerospace Conference, 2008. Big Sky, Montana [**Anais**]. Big Sky, Montana, 2008. Disponível em: https://drive.google.com/file/d/1XmoT8a4YjRbjMzRzfYysFHGtfq_1p1pZ/view. Acesso em: 09 set. 2021.

OWENS B.; HERRING M.; LEVESON N.; INGHAN M.; WEISS K. **Safety-Driven Model-Based** Part II: Application of the Methodology to an Outer Planet Exploration Mission. 2007. Disponível em: sunnyday.mit.edu/JPL-Part-2.doc. Acesso em: 10 ago. 2020.

PALMERIO A. **Introdução à Tecnologia de Foguetes** 2. ed. São José dos Campos: SindCT, 2017.

PEREIRA S.; LEE G.; HOWARD J. A system-theretic hazard analysis methodology for a non-advocate safety assessment of the ballistic missile defense system. *In* AIAA Missile Sciences Conference, 2006. Monterey, CA, EUA [**Anais**]. Monterey, CA, EUA 2006. Disponível em: http://sunnyday.mit.edu/papers/BMDS.pdf. Acesso em: 22 set. 2020.

PLESTSER V. Short duration microgravity experiments in physical and life sciences during parabolic flights: the first 30 ESA campaigns. **Acta Astronautica Journal** 55, 10, 2004. p. 829-854. DOI: https://doi.org/10.1016/j.actaastro.2004.04.006.

PARTNERSHIP FOR SYSTEMS APPROACHES TO SAFETY AND SECURITY - PSASS. **A new sorted list of STAMP-related publications**, 2018. Disponível em: http://psas.scripts.mit.edu/home/wp-content/uploads/2019/05/STAMP-publications-sorted-v2.pdf. Acesso em: 05/05/2020.

SILVA R.; YAMADA Y.; GUIMARÃES DA SILVA M. Sensor Mecânico Acelerométrico. *In* Workshop em Engenharia e Tecnologia Espaciais, 9., 2018. São José dos Campos, [**Anais**]. São José dos Campos: INPE, 2018. ISSN: 2177-3114. Disponível em: http://urlib.net/ibi/8JMKD3MGPDW34R/3S2EGDS. Acesso em: 15/06/2021.

RISING J.; LEVESON N. Systems-Theoretic Process Analysis of space launch vehicles. **Journal of Space Safety Engineering** 5, 3-4. p. 153 a 183, 2018. https://doi.org/10.1016/j.jsse.2018.06.004. Disponível em: https://dspace.mit.edu/bitstream/handle/1721.1/122988/JSSE-40-proofs.pdf?sequence=2&isAllowed=y. Acesso em: 13/10/2019.

SYSML.ORG. **SysML Open-Source Specification Project**. sysml.org, 2003. Disponível em: http://sysml.org/. Acesso em: 02 jul. 2020.

TENÓRIO P., MINEIRO S., BANDEIRA I., TOLEDO R., YING NA C. Simulador das rotações do voo ascendente de um foguete de sondagem em centrifugas. *In* Workshop em Engenharia e Tecnologias Espaciais, 10., 2019. São José dos Campos, [**Anais**]. São José dos Campos: INPE, 2019. ISSN: 2177-3114. Disponível em: http://mtc-m16d.sid.inpe.br/rep/8JMKD3MGPDW34R/3TTABDB. Acesso em: 12/06/2021.

TOLEDO R. **Estudo da Solidificação de Ligas Metálicas Eutéticas em Ambiente de Microgravidade**. Tese (Doutorado) Curso de pós graduação em ETE/Ciência e Tecnologia de Materiais e Sensores, Instituto Nacional de Pesquisas Espaciais. São José dos Campos, 2013. Disponível em: mtc-m16d.sid.inpe.br/col/sid.inpe.br/mtc-m19/2013/02.21.12.26/doc/publicacao.pdf. Acesso em 22 fev. 2021.

UJIIE R. **Safety-Guided Design Analysis in Multi-Purposed Japanese Unmanned Transfer Vehicle**. Dissertação (Master of Science in Engineering and Management), Massachusetts Institute of Technology, Cambridge, MA, EUA, 2016. Disponível em: https://dspace.mit.edu/bitstream/handle/1721.1/107593/974710088-MIT.pdf?sequence=1&isAllowed=y. Acesso em 26 jun. 2020.

Apêndice A

CENÁRIOS DE PERDAS

Nesta parte são apresentados todos os cenários de perdas identificados.

UCA-1: Não execução do ensaio ambiental durante a fase de testes [H-1, H-2, H-3, H-4, H-5, H-6, H-10].

Cenário 1 para UCA-1: O experimento é integrado à Carga Útil sem ter passado pelo ensaio ambiental. Este tipo de cenário pode ocorrer devido à pressão de cronograma e não conferência das atividades previstas. Dessa forma não há como verificar a capacidade do experimento conter suas amostras ou partes integrantes [H-6] durante os ensaios ambientais. A não verificação pode ocultar potenciais vazamentos líquidos [H-1], gasosos [H-2] e desprendimento de suas partes [H-3]. Podem, também, ocultar fragilidades nas redes elétricas, levando a curtos-circuitos [H-4, H-5], durante o voo.

Cenário 2 para UCA-1: A não execução do ensaio na fase de testes. Este tipo de cenário pode causar pressão para que seja postergada a campanha de lançamento. Em caso de atrasos na campanha, pode se perder a oportunidade de lançamento gerando atrasos ao programa como um todo [H-10].

Consideração referente ao cenário 2 para UCA-1: A prática comum, em relação a lançamentos de foguetes de sondagem, é a priorização do êxito da missão como um todo em detrimento do prazo.

UCA-2: Quantidade de ensaios ambientais excedentes aos previstos durante os testes [H-1, H-2, H-3, H-4, H-5, H-10].

Cenário 1 para UCA-2: O experimento apresenta problemas de contenção das amostras durante os testes ou até mesmo durante o desenvolvimento. Neste tipo de cenário, o experimento é ensaiado múltiplas vezes até que sejam sanados os problemas. Estes ensaios adicionais podem degradar a estrutura do experimento [H-3], podendo levar, também, a vazamentos de amostras líquidas [H-1] e gasosas [H-2]

durante os ensaios ambientais ou voo. Podem, também, ocorrer danos às redes elétricas levando a curtos-circuitos [H-4] e ao sistema de aterramento durante o voo [H-5].

Consideração referente à recomendação 3: Esta recomendação é útil em caso de falhas do experimento durante a campanha. Também é útil em caso de processo longo e complexo de substituição de amostras, sendo possível, assim, facilitar a administração do preparo do experimento, com amostras sensíveis, para novas tentativas.

Cenário 2 para UCA-2: Os ensaios excedentes degradam a estrutura do equipamento durante os testes [H-3] e não há peças sobressalentes disponíveis para substituição, impossibilitando sua integração na carga útil [H-10].

UCA-3: Não testagem do experimento a tempo para sua integração para o voo [H-10].
Cenário 1 para UCA-3: O experimento apresenta problemas nos testes, sendo necessário sua repetição. Neste cenário, a sequência de testes é mantida e outros experimentos são priorizados, a repetição dos testes para o experimento que apresentou problemas fica para o final. Devido a prorrogação e não alteração do cronograma de lançamento o experimento não é testado a tempo para sua integração na carga útil [H-10].

Cenário 2 para UCA-3: O experimento não é disponibilizado a tempo para os testes, e não ocorre prorrogação de prazo. Neste cenário, o experimento não é integrado na carga útil [H-10].

Cenário 3 para UCA-3: Estrutura de suporte aos testes não disponível, dentro do previsto, para sua execução. Neste cenário, caso não ocorra prorrogação da campanha de lançamento o experimento não é testado nem integrado na carga útil [H-10].

UCA-4: Validação para voo experimento com procedimento de troca de amostra inviável para sua execução no campo de lançamentos [H-1, H-2, H-4, H-5, H-7, H-8, H-10].

Cenário 1 para UCA-4: O procedimento de troca de amostras do experimento é validado sem considerar os óbices que a estrutura do campo oferece [H-7] e seu voo poderá ser impossibilitado, caso seja necessária a manipulação ou troca da amostra [H-10].

Cenário 2 para UCA-4: O procedimento de troca de amostras do experimento é validado sem considerar os óbices que a estrutura do campo oferece [H-7]. Neste cenário, opta-se por um procedimento de manipulação ou troca, de amostras da forma não prevista [H-8]. Dessa forma caso seja optado pela liberação para voo do experimento nestas condições, podem ocorrer vazamentos [H-1, H-2], que, por sua vez podem levar a danos das redes elétricas levando a curtos-circuitos [H-4] e ao sistema de aterramento [H-5] durante o voo.

UCA-5: Não validação do procedimento para manipulação ou troca de amostras [H-5, H-6, H-8].
Cenário 1 para UCA-5: O procedimento de troca de amostras do experimento não é validado durante a fase de testes. Neste cenário, o experimento é validado com um procedimento ineficaz para a contenção das amostras durante o voo [H-6]. As amostras podem vazar [H-1, H-2], e por sua vez podem levar a danos das redes elétricas levando a curtos-circuitos [H-4] e ao sistema de aterramento [H-5] durante o voo.

Cenário 2 para UCA-5: O procedimento de troca de amostras é executado durante a preparação para voo, porém por uma equipe diferente da que participou da fase de testes, sem que ocorra a verificação. Neste cenário, o procedimento executado é diferente do validado [H-8] e dessa forma há riscos de vazamento as amostras [H-1, H-2], que por sua vez podem levar a danos das redes elétricas levando a curtos-circuitos [H-4] e ao sistema de aterramento [H-5] durante o voo.

UCA-6: Validação dos procedimentos ou de ensaios acima dos valores pré-estabelecidos, junto ao experimento [H-3, H-4, H-5, H-10].
Cenário 1 para UCA-6: Os ensaios ambientais são executados com níveis estabelecidos muito acima dos padrões nominais e como resultado o experimento não

é aprovado para o voo [H-10], mesmo que tenha sido desenvolvido tomando todas as medidas para sua aprovação.

Cenário 2 para UCA-6: Os ensaios ambientais são executados com níveis excessivos e o experimento é aprovado para o voo, porém sua estrutura sofre degradação sem que seja possível sua identificação.
Neste cenário, durante o voo devido a degradação componentes podem se soltar [H-3], cabos podem romper e provocar curtos-circuitos, incluindo no sistema de aterramento [H-4, H-5]

Cenário 3 para UCA-6: O rigor excessivo oferecido acarreta em alterações desnecessárias de procedimentos e eventualmente em reprojeto do experimento. Neste cenário, como consequência dos reprojetos ocorrem atrasos na entrega do experimento para um novo teste. Desta forma corre o risco de ultrapassar a data de entrega do experimento e ele não ser integrado à carga útil [H-10].

Cenário 4 para UCA-6: O rigor excessivo oferecido limita parte das experiências do experimento causando perda de parte de informações de voo [H-10].

UCA-7: Validação do experimento muito tarde para o voo [H-10].
Cenário 1 para UCA-7: A validação do experimento atrasa devido a necessidade de repetição de testes, e com a manutenção do cronograma de lançamento faz com que sua integração na carga útil não seja possível [H-10].

Consideração referente ao cenário 1 para UCA-7: A escolha da manutenção do cronograma é gerencial, usualmente prioriza o êxito da carga útil como um todo. Caso muitos experimentos estejam nesta situação é provável que os gestores estejam inclinados a postergar a campanha de lançamentos. Caso seja apenas um é possível que os gestores optem por realocar este experimento para outro lançamento (gerando a necessidade de substituição por massa *dummy*, gerando custo, retrabalho e possível atraso).

Cenário 2 para UCA-7: O experimento é disponibilizado em atraso para os testes, e com a manutenção do cronograma de lançamento faz com que sua integração na

carga útil não seja possível [H-10] (gerando a necessidade de substituição por massa *dummy*, gerando custo, retrabalho e possível atraso).

Cenário 3 para UCA-7: A necessidade de revisão de procedimentos faz com que ocorram atrasos na validação do experimento e com a manutenção do cronograma de lançamento faz com que sua integração na carga útil não seja possível [H-10] (gerando a necessidade de substituição por massa *dummy*, gerando custo, retrabalho e possível atraso).

UCA-8: Validação do experimento muito cedo provocando a degradação das amostras [H-1, H-2, H-3, H-4, H-5, H-8, H-10].
Cenário 1 para UCA-8: A validação do experimento é efetuada no momento previsto, porém o cronograma de lançamento é postergado.
Neste cenário, um experimento cujas amostras são sensíveis as tem degradadas e por esta razão são substituídas. O procedimento de troca de amostras pode ser executado de forma distinta à validada [H-8], podendo acarretar em vazamentos de amostras [H-1, H-2], por sua vez, podem levar a danos das redes elétricas [H-4] e ao sistema de aterramento [H-5] durante o voo.

Consideração referente ao cenário 1 para UCA-8: O conhecimento da dinâmica da degradação das amostras, bem como, as condições para que ocorra contribui para identificar e adotar as medidas a fim de mitigar a degradação.

Cenário 2 para UCA-8: A validação do experimento é adiantada, devido à antecipação da entrega do experimento para os testes, com a manutenção do cronograma de lançamento.
Neste cenário, um experimento cujas amostras são sensíveis as tem degradadas e por esta razão são substituídas. O procedimento de troca de amostras pode ser executado de forma distinta à validada [H-8], podendo acarretar em vazamentos de amostras [H-1, H-2], por sua vez, podem levar a danos das redes elétricas [H-4] e ao sistema de aterramento [H-5] durante o voo.

Cenário 3 para UCA-8: A validação do experimento ocorre muito cedo, pelo apresentado no cenário 1 ou 2 da UCA-8, as amostras degradam e são substituídas.

Neste cenário, durante o procedimento ocorre quebra de componente devido à manipulação, sem que esteja disponível peças sobressalentes [H-3]. Dessa forma o experimento é integrado à carga útil de forma degradada ou inativa [H-10].

Cenário 4 para UCA-8: O experimento utiliza amostras sensíveis que degradam em questão de horas.
Neste cenário, o procedimento de troca de amostras é iniciado com poucas horas antes do lançamento, porém, não é finalizado a tempo do lançamento, inviabilizando assim sua reintegração à carga útil [H-10].

UCA-9: Não integração do experimento na carga útil [H-10].
As razões para que o experimento não seja integrado na carga útil são diversas e são demonstradas em diversos cenários neste documento (gerando a necessidade de substituição por massa *dummy*, gerando custo, retrabalho e possível atraso).
Cenário 1 para UCA-9: O experimento não é liberado para ser integrado à carga útil, devido à falta do ensaio ambiental [H-10].

Cenário 2 para UCA-9: O experimento oferecer riscos a outros experimentos e à carga útil sem ações para mitigação [H-10].

UCA-10: Integração do experimento na carga útil sem validação para voo [H-1, H-2, H-3, H-4, H-5, H-6, H-7].
Cenário 1 para UCA-10: Pressões para a execução do lançamento podem antecipar o cronograma de lançamento e acarretar em integração de experimento sem validação [H-7].
Neste cenário, pode se ocultar problemas na capacidade do experimento conter suas amostras ou partes integrantes [H-6], tendo como potenciais vazamentos líquidos [H-1], gasosos [H-2] e desprendimento de suas partes [H-3]. Podem, também, ocorrer danos às redes elétricas levando a curtos-circuitos [H-4], e ao sistema de aterramento [H-5] devido aos vazamentos de amostras durante o voo.

Cenário 2 para UCA-10: Controle gerencial ineficaz das validações pendentes dos experimentos, aceitando, erroneamente, como validado um determinado experimento [H-7].

Neste cenário, pode-se ocultar problemas na capacidade do experimento conter suas amostras ou partes integrantes [H-6], tendo como potenciais vazamentos líquidos [H-1], gasosos [H-2], e desprendimento de suas partes [H-3]. Podem também ocorrer danos às redes elétricas levando a curtos-circuitos [H-4] e ao sistema de aterramento [H-5] devido aos vazamentos de amostras durante o voo.

UCA-11: Autorização e execução da integração do experimento na carga útil muito cedo degradando assim as amostras [H-1, H-2, H-3, H-4, H-5, H-8, H-10].
Cenário 1 para UCA-11: A integração do experimento é executada conforme programado, porém o cronograma é alterado posteriormente. O experimento contém amostras que degradam com decorrer do tempo, devido a esta situação faz-se necessária a substituição das amostras. O procedimento de troca de amostras pode ser executado de forma distinta à validada [H-8], podendo acarretar em vazamentos de amostras [H-1, H-2], por sua vez podem levar a danos das redes elétricas [H-4] e ao sistema de aterramento [H-5] durante o voo.

Cenário 2 para UCA-11: Controle gerencial ineficaz do momento oportuno para a integração do experimento, acabando por antecipar a etapa.
Neste cenário, o experimento contém amostras que degradam com o decorrer do tempo, devido a esta faz se necessária a substituição das amostras. Durante o procedimento de troca de amostras ocorre quebra de componente, sem que estejam disponíveis peças sobressalentes [H-3]. Dessa forma o experimento é integrado à carga útil de forma degradada ou inativa [H-10].

UCA-12: Autorização da integração do experimento para o voo muito tarde [H-10].
Cenário 1 para UCA-12: Controle gerencial ineficaz para garantir que todas as etapas que precedem a autorização ocorram de acordo com o programado.
Neste cenário, com a manutenção do cronograma de lançamento faz com que sua integração na carga útil não seja possível [H-10].

Cenário 2 para UCA-12: Estrutura para os testes dos experimentos sobrecarregada ou indisponível para as etapas que precedem a autorização da integração do experimento.

Neste cenário, com a manutenção do cronograma de lançamento faz com que sua integração na carga útil não seja possível [H-10].

Cenário 3 para UCA-12: Entrega tardia do experimento para os testes, ou necessidade de reprojeto do experimento.
Neste cenário, a autorização é atrasada para que todas as etapas que precedem a autorização para integração sejam desempenhadas, porém, esta ultrapassa a data limite para que a integração do experimento na carga útil seja possível [H-10].

UCA-13: Experimento não preparado nas condições equivalentes às de voo durante o ensaio ambiental [H-1, H-2, H-3, H-4, H-5, H-6].
Cenário 1 para UCA-13: Durante os ensaios ambientais as amostras instaladas no experimento não são iguais às previstas para o voo.
Neste cenário, os ensaios ambientais não são representativos [H-6], podendo acarretar em vazamentos de amostras [H-1, H-2], por sua vez podem levar a danos das redes elétricas [H-4] e ao sistema de aterramento [H-5] durante o voo.

Consideração referente ao cenário 1 para UCA-13: Por mais que as amostras que serão utilizadas para o voo sejam dispendiosas, elas devem ser utilizadas também para a validação e ensaios ambientais do experimento. Ao utilizar outros tipos de amostras para os testes corre-se o risco de suas propriedades físico-químicas não serem representativas e invalidar o ensaio ou até mesmo sujeitar a carga útil a acidentes.

UCA-14: Experimento não preparado para o voo [H-10].
Cenário 1 para UCA-14: Durante a preparação final para o voo (minutos que antecedem o voo) o experimento não recebe os comandos para sua preparação final.
Neste cenário, o experimento voa parcialmente ativo ou inativo [H-10].

Cenário 2 para UCA-14: Durante a preparação para o voo (dias ou horas que antecedem o voo) o experimento necessita de troca de amostra e não a recebe. Neste cenário, o experimento voa degradado ou inativo [H-10].

UCA-15: Experimento sofre procedimento de manipulação diferente do validado, tanto durante os testes quanto para a preparação para o voo [H-1, H-2, H-3, H-4, H-5, H-6, H-8].

Cenário 1 para UCA-15: Durante os testes o procedimento de troca de amostras executado é diferente do validado.

Neste cenário, por razões exploradas em cenários anteriores, a configuração testada é distinta da validade [H-6] e, portanto, os testes não são representativos [H-7].

Cenário 2 para UCA-15: Durante a preparação para voo o procedimento de troca de amostras executado é diferente do validado [H-8].

Neste cenário, a configuração testada é distinta da validade [H-6], os testes não são representativos [H-7]. Esta situação pode ocultar vazamentos de amostras [H-1, H-2], e por sua vez podem levar a danos das redes elétricas [H-4] e ao sistema de aterramento [H-5] durante o voo.

UCA-16: Manipulação excessiva do experimento durante a preparação para voo [H-3, H-8, H-10].

Cenário 1 para UCA-16: Durante a campanha de lançamento ocorrem diversas tentativas de lançamento, podendo ocorrer quebra de componente durante o procedimento de manipulação, sem que esteja disponível peças sobressalentes [H-3], podendo o experimento ser integrado à carga útil de forma degradada ou inativa [H-10].

Neste cenário, o experimento contém amostras sensíveis que são viáveis apenas por horas, desta forma cada tentativa de lançamento requer uma nova manipulação para seu preparo, podendo ser necessária a troca de amostras. Não é incomum que durante esta etapa o descanso das equipes esteja comprometido.

Cenário 2 para UCA-16: Durante uma tentativa de lançamento ocorrem diversas paradas e retrocessos na contagem regressiva e o experimento tem amostras que suportam um número máximo de ativações.

Neste cenário, durante a contagem regressiva o número de ativações é excedido [H-10], sendo necessária uma troca de amostras ou manipulação do experimento. Não é incomum que durante esta etapa o descanso das equipes esteja comprometido,

podendo contribuir para que a manipulação do experimento não ocorra conforme a especificação [H-8].

Consideração referente ao cenário 2 para UCA-16: O experimentador cujo experimento necessite constantes trocas de amostras pode considerar as soluções existentes de acesso tardio. Estas soluções permitem trocas mais rápidas de amostras, com um experimento muito mais acessível. Entretanto este tipo de alternativa tem outras considerações que devem também ser analisadas, como por exemplo a necessidade de o experimento ser hermético haja vista que neste caso é instalado em módulo não hermético.

UCA-17: Troca de amostra do experimento efetuada muito cedo durante os testes ou preparação para voo, no caso de amostras sensíveis e sujeitas à degradação [H-3, H-6, H-8, H-10].
Cenário 1 para UCA-17: O experimento tem as amostras trocadas para os testes, entretanto o cronograma é alterado e os testes são postergados.
Neste cenário, o experimento necessitará de uma nova troca de amostras, podendo contribuir para a quebra de componente durante o procedimento de manipulação [H-3], caso não estejam disponíveis peças sobressalentes o experimento voa inerte [H-10].

Cenário 2 para UCA-17: O experimento tem as amostras trocadas para os testes, entretanto o cronograma é alterado e os testes são postergados.
Neste cenário, as amostras do experimento degradam, alterando assim suas características, porém não são substituídas [H-8]. O teste é executado desta forma, entretanto não é representativo [H-6].

Cenário 3 para UCA-17: O experimento tem as amostras trocadas logo após os testes, ou segue com as mesmas amostras dos testes.
Neste cenário, as amostras sofrem degradação, porém não são substituídas [H-8], dessa forma o experimento voa degradado [H-10].

UCA-18: Manipulação para preparação efetuada muito tarde para o voo [H-3, H-10].

Cenário 1 para UCA-18: O tempo para a execução do procedimento de troca de amostras (manipulação) no campo de lançamento demora mais do que o previsto e não é finalizado a tempo para a integração do experimento na carga útil [H-10].

Cenário 2 para UCA-18: O tempo para a execução do procedimento de troca de amostras no campo de lançamento demora mais do que o previsto e causa exaustão da equipe de experimentadores.
Neste cenário, durante a manipulação ocorre a quebra de componente sendo necessário o reparo [H-3], caso não estejam disponíveis peças sobressalentes o experimento voa inerte [H-10].

UCA-19: Não ativação do experimento durante os testes [H-1, H-2, H-3, H-4, H-5, H-6, H-7]
Cenário 1 para UCA-19: O experimento não é ativado durante os testes, dessa forma os testes não são representativos, entretanto a condição da ativação não estava prevista na lista de conferência gerencial e o experimento é liberado para voo [H-7].
Neste cenário, falhas podem estar ocultas e o teste não revela a capacidade do experimento conter suas amostras ou partes integrantes [H-6], tendo como potenciais vazamentos líquidos [H-1], gasosos [H-2] e desprendimento de suas partes [H-3]. Podem também ocorrer danos às redes elétricas levando a curtos-circuitos [H-4] e ao sistema de aterramento [H-5] devido aos vazamentos de amostras durante o voo.

Cenário 2 para UCA-19: O operador do experimento comanda o EGSE da forma prevista para sua ativação, porém o experimento não recebe os comandos do EGSE ou recebe-os em ordem errônea.
Neste cenário, como consequência o experimento não é ativado de forma apropriada para os testes e, portanto, não podem ser considerados representativos [H-6], ocultando assim possíveis falhas.

UCA-20: Não ativação do experimento para o voo [H-10].
Cenário 1 para UCA-20: O experimento não é ativado durante a preparação final para voo por problemas de comunicação entre o coordenador das REs e o operador do experimento.

Neste cenário, as autorizações do Coordenador das REs não são seguidas pelo operador do experimento. Dessa forma o experimento não é ativado e voa desativado, parcialmente ou completamente [H-10].

Cenário 2 para UCA-20: O procedimento de ativação é complexo e com poucas realimentações, causando confusão ao operador.
Neste cenário, o operador julga que o experimento está ativo, entretanto a ativação não foi executada completamente ou em ordem correta. Dessa forma o experimento não é ativado para o voo, de forma parcial ou completa [H-10].

Cenário 3 para UCA-20: Embora o operador do experimento comande o EGSE da forma prevista para sua ativação, o experimento não recebe os comandos do EGSE ou recebe-os em ordem errônea.
Neste cenário, como consequência, o experimento não é ativado de forma apropriada para o voo, dessa forma voa inativo ou com operação degradada [H-10].

UCA-21: Ocorrência de ativação do experimento quando não autorizado durante a preparação para o voo [H-1, H-2, H-4, H-5, H-9]
Cenário 1 para UCA-21: O experimento é ativado durante a preparação para o voo, quando não autorizado pelo coordenador das REs. O experimento permanece ativado enquanto equipes acessam o lançador [H-9] colocando-as sob risco.

Cenário 2 para UCA-21: O experimento é ativado durante a preparação para o voo, quando não autorizado pelo coordenador das REs [H-9].
Neste cenário, o experimento aquece durante sua atividade, aquecendo o módulo de experimentos. O módulo inicia o voo com temperatura superior à prevista, causando superaquecimento no experimento em seu entorno [H-4], este sobreaquecimento pode gerar vazamentos [H-1, H-2], e danos às redes elétricas [H-5].

Cenário 3 para UCA-21: O experimento mantém se ativo após um teste durante a preparação para o voo, o coordenador das REs solicita o desligamento dos experimentos.

Neste cenário, a comunicação entre o coordenador das REs e operador do experimento é ineficiente e a desativação não ocorre [H-9].

Cenário 4 para UCA-21: O experimento mantém se ativo após o experimentador comandar sua desativação.
Neste cenário, a visualização da informação da realimentação é indireta ou confusa para o operador do experimento, desta forma o experimento permanece ativo, enquanto o operador acredita estar desativado [H-9].

UCA-22: Ativação do experimento muito cedo, quando as amostras embarcadas são sensíveis e sujeitas à degradação [H-1, H-2, H-4, H-5, H-9, H-10].
Cenário 1 para UCA-22: O experimento é ativado após a autorização do coordenador das REs durante a preparação final para o voo.
Neste cenário, ocorre uma parada na contagem regressiva fazendo com que se alongue o lançamento, dessa forma o experimento permanece muito tempo com suas amostras ativas causando sua degradação [H-10] e eventualmente superaquecimento [H-4].

Cenário 2 para UCA-22: O experimento é ativado após a autorização do coordenador das REs durante a preparação final para o voo.
Neste cenário, ocorre uma parada na contagem regressiva momentos antes do voo (poucos minutos ou segundos) fazendo com que se alongue o lançamento. O coordenador das REs solicita a desativação dos experimentos, entretanto a interrupção da ativação do experimento faz com que seja necessário retrabalho. O experimento é desativado e voa inerte [H-10].

Consideração a respeito do cenário 2 para a UCA-22: Este cenário é válido para experimentos com processos de ativação irreversíveis. Como por exemplo rompimento de selo para promover o contato entre duas amostras químicas para o estudo relacionado a reações químicas em ambiente de voo. Para este caso é necessária a abertura do experimento para manipulação das amostras e substituição do selo.

Cenário 3 para UCA-22: O experimento é ativado após a autorização do coordenador das REs durante a preparação final para o voo.
Neste cenário, ocorre uma parada na contagem regressiva momentos antes do voo (poucos minutos ou segundos) fazendo com que se alongue o lançamento. O coordenador das REs solicita a desativação dos experimentos, entretanto a interrupção da ativação do experimento faz com que seja necessário que sofra retrabalho. O experimento é mantido ativo com o consentimento do coordenador das REs [H-9], podendo levar a superaquecimento [H-4].

Consideração a respeito do cenário 3 para a UCA-22: Se a situação é esperada e anteriormente planejada, este cenário pode ser mitigado. O ponto de partida para a análise deste cenário é que foi executada a análise e esta forma de mitigação foi avaliada e aprovada pela equipe que gerencia os riscos da operação de lançamento.

Cenário 4 para UCA-22: As amostras do experimento têm um limite de vezes para sua ativação, ao exceder ocorre degradação.
Neste cenário, durante as tentativas de lançamento ocorrem diversas paradas na contagem regressiva em momento posterior à ativação do experimento, ocorrendo assim a degradação das amostras [H-10]. As tentativas de lançamento são exaustivas para as equipes envolvidas e o gerenciamento fica prejudicado, dessa forma a condição da degradação da amostra não é percebida e o experimento sofre vazamento [H-1, H-2], tendo que suas amostras são condutivas, corrosivas e deterioram as redes elétricas [H-5].

UCA-23: Ativação do experimento de forma incompleta para voo [H-10].
Cenário 1 para UCA-23: O operador comanda a ativação do experimento, entretanto a interface e o processo são complexos, exigindo comandos de preparação final para o voo segundos antes do lançamento.
Neste cenário, o operador se confunde e não envia um comando ou inverte a ordem, e o experimento voa com a ativação incompleta [H-10].

Cenário 2 para UCA-23: Enquanto o operador executa os comandos de preparação final para o voo ocorre problemas na interface entre as partes do EGSE, o operador

não obtém êxito em restaurar a conexão e o experimento voa com sua ativação incompleta [H-10].

Neste cenário, o EGSE do experimento é dividido em duas partes, a primeira faz interface com o experimentador, a segunda é mais próxima ao foguete e consequentemente ao experimento. As partes do EGSE comunicam-se através de interface serial, sendo que o ambiente em que passa as conexões elétricas desta comunicação pode ser considerado ruidoso.

Cenário 3 para UCA-23: A inabilitação das ativações decorrentes dos sinais de µG e LO não ocorre, o experimento é ativado de forma irreversível e para sua reversão necessita de nova manipulação [H-10], interrompendo assim a contagem regressiva, ou correndo o risco de voar inativo.

Neste cenário, durante os testes que ocorrem durante a contagem regressiva ocorrem simulações de voo, onde os sinais de µG e LO são enviados aos experimentos. Os experimentos que recebem estes sinais são responsáveis por inabilitar suas ativações que são decorrentes destes, em caso de as ativações serem irreversíveis.

Cenário 4 para UCA-23: O operador comanda o EGSE para ativar o experimento durante a preparação para o voo, porém parte dos comandos não são enviados ao experimento por parte do EGSE.

Neste cenário, como consequência o experimento não é ativado de forma apropriada, o operador do experimento julga que o experimento está propriamente ativado para o voo. Entretanto o experimento voa de forma inativa ou com ativação degradada [H-10].

UCA-24: Ativação do experimento de forma incompleta para os testes [H-1, H-2, H-3, H-4, H-5, H-6, H-7].

Cenário 1 para UCA-24: Assume-se erroneamente que a ativação completa do experimento durante os testes não é necessária, dessa forma os testes não são representativos. Entretanto, a condição da ativação não estava prevista na lista de conferência gerencial e o experimento é liberado para voo [H-7].

Neste cenário, falhas podem estar ocultas e o teste não revela a capacidade do experimento conter suas amostras ou partes integrantes [H-6], tendo como potenciais vazamentos líquidos [H-1], gasosos [H-2] e desprendimento de suas partes [H-3].

Podem também ocorrer danos às redes elétricas levando a curtos-circuitos [H-4] e ao sistema de aterramento [H-5] devido aos vazamentos de amostras durante o voo.

Cenário 2 para UCA-24: O operador comanda o EGSE para ativar o experimento para os testes, porém parte dos comandos não são enviados ao experimento por parte do EGSE.
Neste cenário, como consequência o experimento não é ativado de forma apropriada para os testes e, portanto, não podem ser considerados representativos [H-6]. O operador do experimento julga que o experimento desempenhou conforme o previsto e transmite esta informação às equipes gerenciais. Dessa forma o experimento é liberado para voo com um o teste não representativo [H-7]

UCA-25: Ativação do experimento por muito tempo para os testes [H-1, H-2, H-4, H-10].
Cenário 1 para UCA-25: O experimento permanece muito tempo com suas amostras ativas causando sua degradação [H-10] e eventual superaquecimento [H-4].
Neste cenário, durante o teste de simulação de voo o cabo umbilical é desconectado da carga útil com o experimento ativo, conforme planejado, entretanto o tempo da execução para as diversas etapas da fase de testes nem sempre é exata, podendo levar aos experimentos serem ativados por tempo superior ao projetado.

Cenário 2 para UCA-25: O operador do experimento julga que o experimento está em faixa segura de operação, porém, permanece muito tempo com suas amostras ativas causando sua degradação [H-10] e eventual superaquecimento [H-4].
Neste cenário, o tempo da execução para as diversas etapas da fase de testes nem sempre é exata, o que pode levar aos experimentos serem ativados por tempo superior ao projetado. As informações apresentadas pelo EGSE ao operador do experimento são insuficientes, ou indiretas. Podendo acarretar perda do experimento.

Cenário 3 para UCA-25: Ao fim do teste o operador do experimento comanda a desativação do experimento, porém o EGSE não executa os comandos conforme o operador.

Neste cenário, o experimento permanece ativo [H-9] causando seu superaquecimento [H-4], degradação das amostras e as baterias são drenadas além de seu limite, causando assim danos aos conjuntos [H-10].

UCA-26: Experimento acionado intempestivamente durante testes ou preparação para voo [H-1, H-2, H-4, H-9, H-10].
Cenário 1 para UCA-26: Durante a preparação para o voo o experimento é ativado pelos comandos enviados pelo EGSE enquanto o operador do experimento comanda outras funções.
Neste cenário, o operador do experimento é levado a acreditar que o experimento não está ativo [H-9] devido a não o ter comandado dessa forma.

Cenário 2 para UCA-26: Durante os testes o experimento é ativado pelos comandos enviados pelo EGSE enquanto o operador do experimento comanda outras funções.
Neste cenário, o operador do experimento é levado a acreditar que o experimento não está ativo [H-9] devido a não o ter comandado dessa forma. O experimento permanece ativo por tempo superior ao programado e sofre degradações nas amostras, fazendo que os testes não sejam representativos [H-6].

UCA-27: Comandos de acionamento do experimento ocorrem fora da ordem prevista durante os testes [H-6, H-7].
Cenário 1 para UCA-27: O EGSE não provém informações claras de funcionamento e seus comandos são complexos, o operador do experimento
envia comandos em ordem incorreta durante os testes.
Neste cenário, o experimento é testado de forma distinta à prevista para o voo e dessa forma o teste não é considerado válido [H-6]. O operador do experimento julga que o experimento desempenhou conforme o previsto e transmite esta informação às equipes. Dessa forma o experimento é liberado para voo com um o teste não representativo [H-7].

Cenário 2 para UCA-27: O operador envia comandos na ordem correta ao EGSE, porém este muda a ordem dos comandos.
Neste cenário, o experimento é testado de forma distinta à prevista para o voo, e dessa forma o teste não é considerado válido [H-6]. O operador do experimento julga que o

experimento desempenhou conforme o previsto e transmite às equipes gerenciais a informação de que o experimento desempenhou conforme o esperado. Dessa forma o experimento é liberado para voo com um o teste não representativo [H-7].

UCA-28: Comandos de acionamento do experimento ocorrem fora da ordem prevista durante a preparação para voo [H-10]

Cenário 1 para UCA-28: O EGSE não provém informações claras de funcionamento e seus comandos são complexos, o operador do experimento envia ordens em ordem incorreta durante a preparação para o voo.

Neste cenário, o operador do experimento julga que o experimento está propriamente ativado para o voo, entretanto o experimento voa de forma inativa ou com ativação degradada [H-10].

Cenário 2 para UCA-28: O operador envia comandos na ordem correta ao EGSE, porém este muda a ordem dos comandos.

Neste cenário, o operador do experimento julga que o experimento está propriamente ativado para o voo, entretanto o experimento voa de forma inativa ou com ativação degradada [H-10].

UCA-29: Ativação do experimento durante tempo excessivo durante a preparação para voo [H-1, H-2, H-4, H-9, H-10].

Cenário 1 para UCA-29:

O experimento permanece ativo por tempo superior ao programado e sofre superaquecimento [H-4].

Neste caso, por razões exploradas em outros cenários, pode ser propiciado o vazamento de amostras [H-1, H-2], possíveis danos à rede elétrica [H-5], degradações nas amostras e consumo superior da bateria embarcada, podendo assim comprometer seu funcionamento pleno durante o voo [H-10].

Cenário 2 para UCA-29: Um experimento necessita de tempo adicional para sua ativação completa, dessa forma a cronologia é alterada de forma a contemplar este experimento.

Neste cenário, durante este tempo adicional outros experimentos são acionados por tempo demasiado levando ao seu superaquecimento [H-4], degradações nas

amostras e consumo superior da bateria embarcada, podendo assim comprometer seu funcionamento pleno durante o voo [H-10].

UCA-30: Ativação das amostras muito cedo provocando aquecimento excessivo durante preparação para voo ou testes (muito cedo) [H-4].
Cenário 1 para UCA-30: O experimento é acionado dentro do tempo permitido para sua ativação, porém o tempo necessário para sua ativação é inferior ao tempo total autorizado.
Neste cenário, o operador do experimento ativa o experimento assim que autorizado, e o experimento atinge a condição para o voo em menor tempo que o total disponível para esta operação, durante o tempo excedente o experimento acumula calor e acresce a temperatura do módulo onde está instalado, fazendo com que a temperatura inicial de voo seja superior ao usual. Durante o voo o módulo alcança níveis superiores ao previsto provocando um nível superior de stress aos experimentos embarcados no mesmo módulo [H-4].

UCA-31: Ativação das amostras por tempo insuficiente durante os testes [H-1, H-2, H-3, H-6].
Cenário 1 para UCA-31: O experimento é ativado pelo tempo programado durante os testes, porém o experimento não alcança as condições necessárias para sua completa ativação, neste caso temperatura de experimentação das amostras.
Neste cenário, o experimento é testado de forma distinta à prevista para o voo, dessa forma o teste não é considerado válido [H-6]. A equipe gerencial assume o teste como válido devido ao tempo decorrido e libera o experimento dessa forma [H-7].

UCA-32: Ativação das amostras por tempo insuficiente durante preparação para voo [H-10].
Cenário 1 para UCA-32: A cronologia definida não contempla o tempo adicional necessário para a preparação final do experimento para o voo.
Neste cenário, a temperatura da amostra para o voo precisaria de mais tempo para atingir seu valor de prontidão. A manutenção do tempo inferior ao necessário para sua preparação é baseada em um resultado de teste não representativo [H-10].

Cenário 2 para UCA-32: O experimento não é ativado por tempo suficiente durante a preparação final para voo, neste caso trata de aquecimento das amostras.

Neste cenário, o prazo não é estendido e o experimento voa com amostras com temperatura inferior à prevista para o voo, dessa forma o experimento voa com preparação incompleta [H-10], tendo como consequência tempo menor de experimentação, consumo maior de baterias ou seu não funcionamento conforme previsto.

Apêndice B

REQUISITOS DE SEGURANÇA

Nesta parte são apresentados todos os requisitos de segurança identificados neste trabalho.

Identificação	GP-001
Desempenho	Os ensaios aplicados aos experimentos devem ser controlados e validados por membros da equipe gerencial da carga útil
Título	Controle de validações de ensaios
Justificativa	Dar à equipe de gestão subsídios para a permissão para a integração do experimento à carga útil
Tipo	Garantia do produto
Responsabilidade	Gerencial IAE
Relacionado a	REST-001
Tolerância	N/A
Verificação	Inspeção e *Checklist*

Identificação	VR-001
Desempenho	O experimento não deve ser liberado para o voo sem ter sido aprovado no ensaio dinâmico de aceitação
Título	Liberação para voo
Justificativa	Impedir que experimentos que não tenham sido aprovados para o voo sejam integrados à carga útil
Tipo	Verificação
Responsabilidade	Gerencial IAE
Relacionado a	REST-001
Tolerância	N/A
Verificação	Relatório de teste, *Checklist*

Identificação	VR-002
Desempenho	O experimento deve ser submetido a um teste funcional, validado por equipe técnica do IAE, antes do seu ensaio dinâmico de aceitação.
Título	Teste funcional antes do EDA
Justificativa	Garantir que
Tipo	Verificação
Responsabilidade	Gerencial IAE
Relacionado a	REST-001
Tolerância	N/A
Verificação	Relatório de ensaio

Identificação	VR-003
Desempenho	O experimento deve ser submetido à verificação dimensional antes do seu EDA
Título	Verificação dimensional antes do EDA
Justificativa	Impedir que experimentos que não tenham sido aprovados para o voo sejam integrados à carga útil
Tipo	Verificação
Responsabilidade	Gerencial IAE
Relacionado a	REST-001
Tolerância	N/A
Verificação	Relatório de ensaio

Identificação	VR-004
Desempenho	O experimento deve apresentar variação inferior a ± 0,5 mm de suas dimensões externas (LxAxC) em relação ao que consta no projeto
Título	Variações nas dimensões do experimento
Justificativa	Garantir que não ocorram interferências mecânicas no módulo em que o experimento é integrado
Tipo	Verificação
Responsabilidade	Técnica do experimentador
Relacionado a	REST-001
Tolerância	± 0,5 mm
Verificação	Relatório de ensaio, análise de documentação

Identificação	VR-005
Desempenho	O experimento deve apresentar variação inferior a ± 0,2 mm na posição de suas furações de fixação relação ao que consta no projeto
Título	Variação da fixação
Justificativa	Impedir que experimentos que não tenham sido aprovados para o voo sejam integrados à carga útil
Tipo	Técnica do experimentador
Responsabilidade	Técnica do experimentador
Relacionado a	REST-001
Tolerância	± 0,2 mm
Verificação	Relatório de ensaio, análise de documentação

Identificação	GP-002
Desempenho	O experimento deve ser integrado à carga útil com validação do procedimento de manipulação, ou troca, de amostras
Título	Integração do experimento na carga útil sem validação de procedimento
Justificativa	Garantir que o experimento seja integrado apenas com o processo de troca de amostras validado
Tipo	Garantia do produto
Responsabilidade	Gerencial do IAE
Relacionado a	REST-001
Tolerância	N/A
Verificação	Inspeção, *checklist*

Identificação	PR-001
Desempenho	As vedações aplicadas aos recipientes de vedação de gases devem prover estanqueidade de modo que o vazamento seja inferior a 50 ppm de gás/hora
Título	Contenção de amostra gasosa
Justificativa	Garantir limites de degasagem nos experimentos
Tipo	Projeto
Responsabilidade	Técnica do experimentador
Relacionado a	REST-002
Tolerância	O limite, de 50 ppm / hora, pode ser alterado conforme o gás utilizado, dependendo de análise de equipe de especialistas.
Verificação	Análise de projeto

Identificação	PR-002
Desempenho	Experimento com amostra liquida não deve apresentar vazamento superior a 0,1% do volume por hora
Título	Contenção de amostra líquida
Justificativa	Garantir limites de vazamento nos experimentos
Tipo	Projeto
Responsabilidade	Técnica do experimentador
Relacionado a	REST-002
Tolerância	O limite, de 0,1 % do volume / hora, pode ser alterado conforme o líquido utilizado, dependendo da análise da equipe de especialistas.
Verificação	Inspeção visual, medida, e/ou superfícies úmidas

Identificação	PR-003
Desempenho	Experimento com amostra liquida não deve apresentar vazamento superior a 1% do volume após a realização de cada ensaio dinâmico
Título	Contenção de amostra líquida sob ensaio
Justificativa	Garantir limites de vazamento nos experimentos
Tipo	Projeto
Responsabilidade	Técnica do experimentador
Relacionado a	REST-002
Tolerância	O limite, de 1 % do volume por teste, pode ser alterado conforme o líquido utilizado, dependendo de análise de equipe de especialistas.
Verificação	Inspeção visual, medida, e/ou superfícies úmidas

Identificação	FS-001
Desempenho	O experimento, após EDA, não deve apresentar avarias aparentes em suas partes integrantes
Título	Degradação das partes integrantes
Justificativa	Assegurar a integridade física do experimento
Tipo	Físico
Responsabilidade	Técnica do experimentador
Relacionado a	REST-003, REST-009
Tolerância	N/A
Verificação	Inspeção visual

Identificação	VR-006
Desempenho	A contenção de amostra deve ser inspecionada após submissão ao EDA
Título	Inspeção da contenção da amostra no desenvolvimento
Justificativa	Garantir limites de vazamento nos experimentos
Tipo	Verificação
Responsabilidade	Técnica do experimentador
Relacionado a	REST-003
Tolerância	N/A
Verificação	Inspeção visual, medida, e/ou superfícies úmidas

Identificação	LO-001
Desempenho	Deve haver redundância na estrutura para os testes dos experimentos
Título	Estrutura para testes
Justificativa	Garantir a execução dos testes necessários aos experimentos
Tipo	Logístico
Responsabilidade	Gerencial do IAE
Relacionado a	REST-004
Tolerância	N/A
Verificação	Inspeção e *Checklist*

Identificação	OP-001
Desempenho	A validação do procedimento de manipulação de amostras deve levar em conta as instalações e facilidades do campo de lançamento
Título	Considerações para a validação da manipulação de amostras
Justificativa	Garantir a validação de procedimentos de manipulação ou troca de amostras viáveis de serem executados no campo de lançamento
Tipo	Operacional
Responsabilidade	Técnica do IAE
Relacionado a	REST-005
Tolerância	N/A
Verificação	Inspeção e *Checklist*

Identificação	OP-002
Desempenho	A validação do procedimento de manipulação de amostras deve ser efetuada por equipe com conhecimento no campo de lançamento e no processo de aceitação de experimentos
Título	Equipe para a validação da manipulação de amostras
Justificativa	Garantir que a validação do procedimento de toca de amostras seja efetuada por equipe competente
Tipo	Operacional
Responsabilidade	Técnica do IAE
Relacionado a	REST-005
Tolerância	N/A
Verificação	Inspeção, *Checklist*, análise de equipe responsável

Identificação	GP-003
Desempenho	O procedimento de manipulação de amostras deve ser acompanhado pela equipe responsável por esta validação durante os testes de desenvolvimento
Título	Acompanhamento da validação da manipulação de amostras
Justificativa	Garantir que a manipulação de amostras seja acompanhada por equipe competente durante a fase de desenvolvimento
Tipo	Garantia do produto
Responsabilidade	Técnica do IAE
Relacionado a	REST-005
Tolerância	N/A
Verificação	Inspeção e *Checklist*

Identificação	GP-004
Desempenho	A equipe de qualidade do IAE deve acompanhar o procedimento de manipulação de amostra para todas as vezes que for executado após sua validação
Título	Acompanhamento da manipulação de amostras
Justificativa	Garantir que a validação do procedimento de toca de amostras seja efetuada por equipe competente
Tipo	Garantia do produto
Responsabilidade	Gerencial do IAE
Relacionado a	REST-006
Tolerância	N/A
Verificação	Inspeção e *Checklist*

Identificação	GP-005
Desempenho	A equipe de qualidade deve informar à gerência responsável pelo lançamento os resultados do procedimento de manipulação de amostra executado
Título	Indicador do resultado da manipulação de amostras
Justificativa	Garantir que que o procedimento executado seja executado conforme o previsto
Tipo	Garantia do produto
Responsabilidade	Gerencial do IAE
Relacionado a	REST-006
Tolerância	N/A
Verificação	Inspeção, c*hecklist*, e relatório

Identificação	PR-004
Desempenho	Todas as informações relativas aos testes, ensaios e procedimentos dos experimentos devem ser disponibilizadas aos experimentadores antes da fase de desenvolvimento
Título	Informações sobre os ensaios
Justificativa	Garantir que todas as informações pertinentes sejam disponibilizadas aos experimentadores antes da fase de desenvolvimento
Tipo	Projeto
Responsabilidade	Gerencial IAE
Relacionado a	REST-007, REST-010
Tolerância	N/A

Identificação	GP-006
Desempenho	A equipe gerencial do IAE deve verificar os certificados de calibração dos respectivos equipamentos de suporte
Título	Certificados de calibração de equipamentos
Justificativa	Garantir que os equipamentos utilizados pelo IAE estejam calibrados
Tipo	Garantia do produto
Responsabilidade	Gerencial do IAE
Relacionado a	REST-008
Tolerância	Aplicável aos equipamentos do IAE
Verificação	Inspeção, e c*hecklist*

Identificação	GP-007
Desempenho	Os ensaios dinâmicos de aceitação devem ser efetuados com calibração validada de seus equipamentos de suporte (IAE)
Título	Calibração de equipamentos
Justificativa	Garantir que os equipamentos utilizados estejam calibrados
Tipo	Garantia do produto
Responsabilidade	Gerencial do IAE
Relacionado a	REST-008
Tolerância	N/A
Verificação	Inspeção, e c*hecklist*

Identificação	VR-007
Desempenho	Os sensores de realimentação do *shaker* devem ter sua instalação e operação de forma a fornecer informações confiáveis ao sistema de controle do equipamento
Título	Instalação dos sensores do shaker
Justificativa	Garantir que os níveis de ensaio sejam aplicados aos experimentos
Tipo	Verificação
Responsabilidade	Técnica do IAE
Relacionado a	REST-008
Tolerância	N/A
Verificação	Análise de especialista

Identificação	VR-008
Desempenho	O experimento deve sofrer testes funcionais e de desempenho após o ensaio dinâmico de aceitação
Título	Testes funcionais após EDA do experimento
Justificativa	Garantir a execução dos testes funcionais do experimento após EDA
Tipo	Verificação
Responsabilidade	Técnica do experimentador
Relacionado a	REST-009
Tolerância	N/A
Verificação	Inspeção, *Checklist*

Identificação	VR-009
Desempenho	O experimento deve apresentar as mesmas funcionalidades antes e após sofrer o EDA
Título	Funcionalidades do Experimentos após EDA
Justificativa	Garantir que as funcionalidades do experimento sejam preservadas
Tipo	Verificação
Responsabilidade	Técnica do experimentador
Relacionado a	REST-009
Tolerância	N/A
Verificação	Inspeção, análise de relatório do experimento

Identificação	PR-005
Desempenho	Todos as verificações relativas aos procedimentos dos experimentos devem ser estabelecidas antes do seu desenvolvimento
Título	Verificações dos procedimentos relativos aos experimentos
Justificativa	Garantir que as verificações relativas aos procedimentos sejam estabelecidas antes da fase de desenvolvimento
Tipo	Projeto
Responsabilidade	Técnica do IAE
Relacionado a	REST-010
Tolerância	N/A
Verificação	Verificação, *Checklist*, confirmação de recebimento

Identificação	VR-010
Desempenho	O experimento e seu sistema devem ter seus procedimentos operacionais testados na fase de desenvolvimento
Título	Testes dos procedimentos durante o desenvolvimento
Justificativa	Contribuir para estimativa de tempo para execução dos procedimentos mais precisa, bem como de promover uma avaliação acerca da complexidade dos procedimentos
Tipo	Verificação
Responsabilidade	Técnica do experimentador
Relacionado a	REST-011
Tolerância	N/A
Verificação	Verificação, *Checklist*

Identificação	VR-011
Desempenho	O sistema do experimento deve ter sido aprovado em todos os testes de seus procedimentos até o fim da etapa de desenvolvimento
Título	Êxito nos procedimentos do experimento durante o desenvolvimento
Justificativa	Garantir que todos os procedimentos planejados sejam exequíveis
Tipo	Verificação
Responsabilidade	Técnica do experimentador
Relacionado a	REST-011
Tolerância	N/A
Verificação	Verificação, demonstração, análise de documentação

Identificação	AM-001
Desempenho	A documentação de projeto do experimento deve contemplar as informações a respeito da degradação das amostras que serão utilizadas
Título	Informações das condições de degradação das amostras
Justificativa	Garantir que as informações que promovam a degradação das amostras sejam levantadas e informadas às equipes responsáveis pela operação e lançamento
Tipo	Ambientais
Responsabilidade	Gerencial do experimentador
Relacionado a	REST-012
Tolerância	N/A
Verificação	Verificação, relatório, ensaio, análise por especialista

Identificação	GP-008
Desempenho	A documentação de projeto do experimento deve ser fornecida à gerencia responsável pela carga útil
Título	Envio das informações de projeto do experimento para a gerência
Justificativa	Garantir que as informações que promovam a degradação das amostras sejam acessíveis à gerência responsável pelo lançamento
Tipo	Garantia do produto
Responsabilidade	Gerencial do experimentador
Relacionado a	REST-012
Tolerância	N/A
Verificação	Relatório, *checklist*

Identificação	MS-001
Desempenho	As informações relacionadas à degradação das amostras dos experimentos, quando aplicável, devem ser utilizadas para o planejamento das atividades para a campanha de lançamento
Título	Informações de experimentos para o planejamento de atividades da campanha de lançamento
Justificativa	Garantir que o planejamento das atividades de campanha de lançamento considere as informações acerca dos experimentos
Tipo	Da missão
Responsabilidade	Gerencial do IAE
Relacionado a	REST-012, REST-014
Tolerância	N/A
Verificação	Relatório, análise de especialistas

Identificação	GP-009
Desempenho	Durante a campanha de lançamento, os experimentos com amostras sensíveis não devem sofrer o procedimento de apronto para voo antecipadamente ao previsto pelo cronograma
Título	Antecipação na execução do procedimento da manipulação de amostras sensíveis
Justificativa	Garantir que o as amostras não se deteriorem antes da data para o lançamento
Tipo	Garantia do produto
Responsabilidade	Gerencial do experimentador
Relacionado a	REST-013
Tolerância	N/A
Verificação	Inspeção, documentação do controle de atividades, *checklist*

Identificação	GP-010
Desempenho	As informações a respeito do tempo de execução do procedimento de manipulação das amostras devem constar na documentação detalhada do experimento
Título	Informações do tempo de execução do procedimento de manipulação de amostras
Justificativa	Evitar atrasos na cronologia
Tipo	Garantia do produto
Responsabilidade	Gerencial do experimentador
Relacionado a	REST-014
Tolerância	N/A
Verificação	Análise de documentação, inspeção, *checklist*

Identificação	GP-011
Desempenho	O experimento deve ser preparado pelo experimentador para ensaio dinâmico de aceitação conforme procedimento de manipulação de amostras validado
Título	Preparação das amostras para o EDA
Justificativa	Executar ensaio mais representativo em relação às condições de preparação e voo
Tipo	Garantia do produto
Responsabilidade	Técnica do experimentador
Relacionado a	REST-015
Tolerância	N/A
Verificação	Inspeção, verificação, *checklist*

Identificação	GP-012
Desempenho	O experimento deve ser preparado para o ensaio dinâmico de aceitação com os mesmos tipos de materiais previstos para o voo
Título	Materiais utilizados no experimento para o EDA
Justificativa	Executar ensaio mais representativo em relação às condições de preparação e voo
Tipo	Garantia do produto
Responsabilidade	Técnica do experimentador
Relacionado a	REST-015
Tolerância	N/A
Verificação	Inspeção, verificação, *checklist*

Identificação	GP-013
Desempenho	O experimento deve apresentar funcionamento conforme o previsto através de ensaio funcional durante sua etapa de aceitação
Título	Ensaio funcional do experimento durante aceitação
Justificativa	Apresentar a funcionalidade do experimento durante a aceitação
Tipo	Garantia do produto
Responsabilidade	Técnica do experimentador
Relacionado a	REST-015
Tolerância	N/A
Verificação	Verificação, demonstração

Identificação	OP-003
Desempenho	Os níveis das ativações do EGSE devem ser pré definidos (tensão, corrente, temperatura, etc.)
Título	Níveis das ativações do EGSE
Justificativa	Evitar operação imprecisa por parte do operador
Tipo	Operacional
Responsabilidade	Técnica do experimentador
Relacionado a	REST-016, REST-022
Tolerância	N/A
Verificação	*Checklist*, análise de documentação, verificação

Identificação	OP-004
Desempenho	Os comandos no EGSE devem ser do tipo liga/desliga, ou de forma similar
Título	Tipo dos comandos do EGSE
Justificativa	Evitar operação imprecisa por parte do operador
Tipo	Operacional
Responsabilidade	Técnica do experimentador
Relacionado a	REST-016, REST-022
Tolerância	N/A
Verificação	*Checklist*, análise de documentação, verificação

Identificação	OP-005
Desempenho	A sequência de comandos para cada procedimento previsto no EGSE deve estar pré-estabelecida e documentada
Título	Sequência de comandos no EGSE
Justificativa	Evitar operação imprecisa por parte do operador
Tipo	Operacional
Responsabilidade	Técnica do experimentador
Relacionado a	REST-016, REST-022
Tolerância	N/A
Verificação	*Checklist*, análise de documentação, verificação

Identificação	PR-012
Desempenho	As informações de status no EGSE devem permitir que o operador e o Coordenador RE possam verificar o correto funcionamento do experimento
Título	Informações suficientes no EGSE
Justificativa	Garantir que o EGSE forneça informações suficientes a seu operador e coordenador das REs
Tipo	Projeto
Responsabilidade	Técnica do experimentador
Relacionado a	REST-016
Tolerância	N/A
Verificação	*Checklist*, análise de documentação, demonstração

Identificação	FC-001
Desempenho	Deve haver controle da estimativa da degradação das amostras do experimento no EGSE do experimento.
Título	Estimativa da degradação das amostras
Justificativa	Monitorar a degradação da amostra via EGSE
Tipo	Funcional
Responsabilidade	Técnica do experimentador
Relacionado a	REST-017
Tolerância	Este requisito não é obrigatório para experimentos de acesso tardio (pois não possuem EGSE)
Verificação	Verificação, análise de documentação, ensaio

Identificação	GP-014
Desempenho	A retirada de um experimento, não deve implicar em alteração das propriedades de massa, CG e inércia da carga útil
Título	Retirada de experimento da carga útil
Justificativa	Manter as propriedades físicas da carga útil
Tipo	Garantia do produto
Responsabilidade	Gerencial do IAE
Relacionado a	REST-018
Tolerância	N/A
Verificação	Inspeção visual, *Checklist*, teste

Identificação	MS-002
Desempenho	O cronograma de apronto da missão deve ser disponibilizado a todas as partes interessadas sempre que sofrer alterações
Título	Alterações de cronograma
Justificativa	Garantir que todas as partes interessadas estejam cientes das informações acerca do cronograma da missão
Tipo	Da missão
Responsabilidade	Gerencial do IAE
Relacionado a	REST-019
Tolerância	N/A
Verificação	*Checklist*, confirmação de recebimento

Identificação	MS-003
Desempenho	Deve haver controle das etapas do ciclo de vida da carga útil por parte das equipes gerenciais responsáveis pela missão de lançamento
Título	Controle do ciclo de vida da carga útil
Justificativa	Garantir o gerenciamento das etapas do ciclo de vida da carga útil
Tipo	Da missão
Responsabilidade	Gerencial do IAE
Relacionado a	REST-020
Tolerância	N/A
Verificação	*Checklist*, inspeção

Identificação	OP-006
Desempenho	O operador do EGSE do experimento deve receber treinamento de pelo menos 8h pelo experimentador
Título	Treinamento do operador do experimento
Justificativa	Garantir que o operador do EGSE receba treinamento efetivo
Tipo	Operacional
Responsabilidade	Gerencial do experimentador
Relacionado a	REST-021
Tolerância	N/A
Verificação	*Checklist*, demonstração

Identificação	OP-007
Desempenho	Devem ser treinados ao menos 2 operadores para o EGSE do experimento
Título	Revezamento do operador do experimento
Justificativa	Garantir capacidade de revezamento dos operadores durante a campanha de lançamento
Tipo	Operacional
Responsabilidade	Gerencial do experimentador
Relacionado a	REST-021
Tolerância	N/A
Verificação	*Checklist*, demonstração

Identificação	OP-008
Desempenho	O operador deve ser treinado em todas as operações previstas para o experimento
Título	Treinamento das operações do EGSE previstas
Justificativa	Garantir que todas as operações previstas sejam de conhecimento dos operadores
Tipo	Operacional
Responsabilidade	Gerencial do experimentador
Relacionado a	REST-021
Tolerância	N/A
Verificação	*Checklist*, demonstração

Identificação	OP-009
Desempenho	Todas as operações previstas para o EGSE do experimento devem ser documentadas
Título	Documentação das operações do EGSE
Justificativa	Garantir que todas as operações previstas sejam documentações
Tipo	Operacional
Responsabilidade	Gerencial do experimentador
Relacionado a	REST-021
Tolerância	N/A
Verificação	*Checklist*, análise de documentação

Identificação	OP-010
Desempenho	Os operadores do EGSE do experimento, sempre quando estiverem operando o EGSE, devem estar de posse da documentação das operações previstas para o EGSE
Título	Posse da documentação das operações do EGSE
Justificativa	Garantir que o operador esteja em posse da documentação das operações previstas do EGSE do experimento
Tipo	Operacional
Responsabilidade	Gerencial do experimentador
Relacionado a	REST-021
Tolerância	N/A
Verificação	*Checklist*, apresentação da documentação

Identificação	OP-011
Desempenho	Os operadores do EGSE do experimento devem participar do EDA
Título	Participação do operador do experimento durante o EDA
Justificativa	Garantir que o operador do EGSE demonstre seu domínio da operação do EGSE durante o EDA
Tipo	Operacional
Responsabilidade	Gerencial do experimentador
Relacionado a	REST-021
Tolerância	N/A
Verificação	*Checklist*, Controle de acesso de pessoal envolvido

Identificação	OP-013
Desempenho	Cada comando do EGSE do experimento deve contar com ao menos uma proteção para inibir comandos indevidos ou intempestivos
Título	Proteção contra comandos não intencionais do EGSE do experimento
Justificativa	Aumentar a segurança contra comandos intempestivos no EGSE do experimento
Tipo	Operacional
Responsabilidade	Técnica do experimentador
Relacionado a	REST-022
Tolerância	N/A
Verificação	Verificação, demonstração, análise da documentação

Identificação	OP-014
Desempenho	Devem ser atribuídas 5 indicações de autorização para informar ao operador do experimento em solo o modo de operação em que o experimento deve ser levado: Desligado; Em preparo para teste; Teste; Em preparo para voo; Voo
Título	Indicações de autorizações enviado pelo coordenador das REs para o operador do EGSE do experimento
Justificativa	Dar objetividade à comunicação entre o coordenador das REs e operador do experimento durante a operação de lançamento
Tipo	Operacional
Responsabilidade	Técnica do IAE
Relacionado a	REST-023
Tolerância	N/A
Verificação	Verificação, demonstração, análise da documentação

Identificação	OP-015
Desempenho	A indicação da autorização designada “Desligado” deve ser da cor vermelha, e indicar quando o operador do EGSE do experimento deve desligar completamente o experimento e mantê-lo dessa forma
Título	Indicação da autorização para o estado “Desligado”
Justificativa	Indicar ao operador do EGSE do experimento que o experimento deve ser desligado e mantido assim
Tipo	Operacional
Responsabilidade	Técnica do IAE
Relacionado a	REST-023
Tolerância	N/A
Verificação	Verificação, demonstração, análise da documentação

Identificação	OP-016
Desempenho	A indicação da autorização designada “Em preparo para teste” deve ser da cor amarela, e indicar quando o operador do EGSE do experimento deve prepará-lo para teste
Título	Indicação da autorização para o estado “Em preparo para teste”
Justificativa	Indicar ao operador do EGSE do experimento que o experimento deve ser preparado para testes
Tipo	Operacional
Responsabilidade	Técnica do IAE
Relacionado a	REST-023
Tolerância	N/A
Verificação	Verificação, demonstração, análise da documentação

Identificação	OP-017
Desempenho	A indicação da autorização designada “Teste” deve ser da cor laranja, e indicar quando o operador do EGSE do experimento deve iniciar o teste
Título	Indicação da autorização para o estado “Teste”
Justificativa	Indicar ao operador do EGSE do experimento que o experimento deve ser testado
Tipo	Operacional
Responsabilidade	Técnica do IAE
Relacionado a	REST-023
Tolerância	N/A
Verificação	Verificação, demonstração, análise da documentação

Identificação	OP-018
Desempenho	A indicação da autorização designada “Em preparo para voo” deve ser da cor azul, e indicar quando o operador do EGSE do experimento deve preparar o experimento para o voo
Título	Indicação da autorização para o estado “Em preparo para o voo”
Justificativa	Indicar ao operador do EGSE do experimento que o experimento deve ser preparado para o voo
Tipo	Operacional
Responsabilidade	Técnica do IAE
Relacionado a	REST-023
Tolerância	N/A
Verificação	Verificação, demonstração, análise da documentação

Identificação	OP-019
Desempenho	A indicação da autorização designada “Voo” deve ser da cor verde, e indicar quando o operador do EGSE do experimento deve finalizar a preparação do experimento para o voo
Título	Indicação da autorização para o estado “Voo”
Justificativa	Indicar ao operador do EGSE do experimento que o experimento deve ser aprontado para o voo
Tipo	Operacional
Responsabilidade	Técnica do IAE
Relacionado a	REST-023
Tolerância	N/A
Verificação	Verificação, demonstração, análise da documentação

Identificação	OP-020
Desempenho	Devem ser enviadas 5 indicações de estados do operador em solo do experimento para o coordenador das REs: Desligado; Em preparo para testes; Testes; Em preparo para voo; Voo
Título	Indicações de estados do Experimento enviado pelo operador do EGSE do experimento para o coordenador das REs
Justificativa	Dar objetividade à comunicação entre o operador do experimento e o coordenador das REs durante a operação de lançamento
Tipo	Operacional
Responsabilidade	Técnica do experimentador
Relacionado a	REST-024
Tolerância	N/A
Verificação	Verificação, demonstração, análise da documentação

Identificação	OP-021
Desempenho	A indicação designada “Desligado” deve ser da cor vermelha, e indicar quando o experimento está completamente desligado
Título	Indicação do estado “Desligado”
Justificativa	Informar ao coordenador das REs o estado de operacional do experimento
Tipo	Operacional
Responsabilidade	Técnica do experimentador
Relacionado a	REST-024
Tolerância	N/A
Verificação	Verificação, demonstração, análise da documentação

Identificação	OP-022
Desempenho	A indicação designada “Em preparo para teste” deve ser da cor amarela, e indicar quando o operador do EGSE do experimento está preparando o experimento para testes
Título	Indicação do estado “Em preparo para teste”
Justificativa	Informar ao coordenador das REs o estado de operacional do experimento
Tipo	Operacional
Responsabilidade	Técnica do experimentador
Relacionado a	REST-024
Tolerância	N/A
Verificação	Verificação, demonstração, análise da documentação

Identificação	OP-023
Desempenho	A indicação designada “Teste” deve ser da cor laranja, e indicar quando o experimento está em teste
Título	Indicação do estado “Teste”
Justificativa	Informar ao coordenador das REs o estado de operacional do experimento
Tipo	Operacional
Responsabilidade	Técnica do experimentador
Relacionado a	REST-024
Tolerância	N/A
Verificação	Verificação, demonstração, análise da documentação

Identificação	OP-024
Desempenho	A indicação designada “Em preparo para voo” deve ser da cor azul, e indicar quando o operador do EGSE do experimento está preparando o experimento para o voo
Título	Indicação do estado “Em preparo para o voo”
Justificativa	Informar ao coordenador das REs o estado de operacional do experimento
Tipo	Operacional
Responsabilidade	Técnica do experimentador
Relacionado a	REST-024
Tolerância	N/A
Verificação	Verificação, demonstração, análise da documentação

Identificação	OP-025
Desempenho	A indicação designada “Voo” deve ser da cor verde, e indicar quando o experimento está pronto para o voo
Título	Indicação de apronto para “Voo”
Justificativa	Informar ao coordenador das REs o estado de operacional do experimento
Tipo	Operacional
Responsabilidade	Técnica do experimentador
Relacionado a	REST-024
Tolerância	N/A
Verificação	Verificação, demonstração, análise da documentação

Identificação	OP-026
Desempenho	O operador do EGSE do experimento deve poder escolher qual o procedimento que será executado no EGSE
Título	Operações no EGSE
Justificativa	Possibilitar ao operador do EGSE do experimento a execução dos procedimentos previstos
Tipo	Operacional
Responsabilidade	Técnica do experimentador
Relacionado a	REST-025
Tolerância	N/A
Verificação	Verificação, demonstração, análise da documentação

Identificação	OP-027
Desempenho	A execução de procedimentos pelo EGSE não deve permitir comandos fora da sequência conforme definido previamente
Título	Limitações de sequência dos comandos no EGSE
Justificativa	Não permitir alterações na sequência da operação do EGSE
Tipo	Operacional
Responsabilidade	Técnica do experimentador
Relacionado a	REST-025
Tolerância	N/A
Verificação	Verificação, demonstração, análise da documentação

Identificação	OP-028
Desempenho	A execução de procedimentos pelo EGSE não deve permitir comandos não previstos, conforme definido previamente
Título	Limitações de comandos das operações no EGSE
Justificativa	Não permitir comandos não previstos no procedimento executado
Tipo	Operacional
Responsabilidade	Técnica do experimentador
Relacionado a	REST-025
Tolerância	N/A
Verificação	Verificação, demonstração, análise da documentação

Identificação	OP-029
Desempenho	O coordenador das REs deve ter a capacidade de bloqueio à ativação de todos os experimentos simultaneamente.
Título	Bloqueio geral dos experimentos
Justificativa	Dar capacidade do coordenador das REs bloquear as ativações dos experimentos em situações de emergência
Tipo	Operacional
Responsabilidade	Técnica do IAE
Relacionado a	REST-026
Tolerância	N/A
Verificação	Verificação, demonstração, análise da documentação

Identificação	PR-013
Desempenho	Os procedimentos para a operação do experimento devem ser planejados para as situações de operação esperadas
Título	Previsão para os procedimentos das situações esperadas
Justificativa	Ter planejados procedimentos para todas as situações esperadas durante a operação
Tipo	Projeto
Responsabilidade	Técnica do experimentador
Relacionado a	REST-027
Tolerância	N/A
Verificação	Análise da documentação, demonstração

Identificação	PR-014
Desempenho	Os procedimentos para a operação do experimento devem ser planejados prevendo possível adiamento da operação de lançamento
Título	Previsão para os procedimentos para adiamento da operação de lançamento
Justificativa	Ter planejados procedimentos para todas as situações esperadas durante a operação
Tipo	Projeto
Responsabilidade	Técnica do experimentador
Relacionado a	REST-027
Tolerância	N/A
Verificação	Análise da documentação, demonstração

Identificação	PR-015
Desempenho	Os procedimentos para a operação do experimento devem ser planejados prevendo possível cancelamento da operação de lançamento
Título	Previsão para os procedimentos para o cancelamento da operação de lançamento
Justificativa	Ter planejados procedimentos para todas as situações esperadas durante a operação
Tipo	Projeto
Responsabilidade	Técnica do experimentador
Relacionado a	REST-027
Tolerância	N/A
Verificação	Análise da documentação, demonstração

Identificação	GP-015
Desempenho	Deve ser enviada uma lista das possíveis situações não nominais passíveis de ocorrência durante a missão aos experimentadores antes do desenvolvimento do experimento
Título	Situações típicas de operação
Justificativa	Munir o experimentador com as informações típicas de operação para que ele possa planejar os procedimentos operacionais
Tipo	Garantia do produto
Responsabilidade	Gerencial IAE
Relacionado a	REST-027
Tolerância	N/A
Verificação	Análise da documentação

Identificação	PR-016
Desempenho	O experimento deve possuir comando que ignore os sinais de μG e LO, quando sofrer ações devido a estes sinais
Título	Inibição dos sinais de μG e LO
Justificativa	É comum que durante o teste funcional da carga útil os sinais de uG e LO sejam enviados aos experimentos.
Tipo	Projeto
Responsabilidade	Técnica do experimentador
Relacionado a	REST-028
Tolerância	N/A
Verificação	Demonstração, análise da documentação

Identificação	PR-017
Desempenho	O comando para ignorar os sinais de μG e LO deve ser enviado pelo EGSE do experimento
Título	Comando de inibição dos sinais de μG e LO
Justificativa	É comum que durante o teste funcional da carga útil os sinais de uG e LO sejam enviados aos experimentos.
Tipo	Projeto
Responsabilidade	Técnica do experimentador
Relacionado a	REST-028
Tolerância	N/A
Verificação	Demonstração, análise da documentação

Identificação	PR-018
Desempenho	O comando para ignorar os sinais de µG e LO deve conter bloqueio que impeça seu envio ao experimento durante a preparação final para o voo
Título	Bloqueio do comando de inibição dos sinais de µG e LO
Justificativa	O envio do comando em questão pode fazer com que o experimento voe inativo, ou degradado. Por esta razão deve ser bloqueado quando em preparação para o voo
Tipo	Projeto
Responsabilidade	Técnica do experimentador
Relacionado a	REST-028
Tolerância	N/A
Verificação	Demonstração, análise da documentação

Apêndice C

RECOMENDAÇÕES DE SEGURANÇA

Nesta parte são apresentadas todos as recomendações de segurança identificados neste trabalho, bem como recomendações de implementação.

Recomendações de segurança:

Identificação	FC-002
Desempenho	O operador do EGSE do experimento deve informar a estimativa da degradação das amostras sempre quando solicitado pelos controladores de missão
Título	Estimativa da degradação das amostras
Justificativa	Monitorar a degradação da amostra via EGSE
Tipo	Funcional
Responsabilidade	Técnica do experimentador
Relacionado a	REST-017
Tolerância	N/A
Verificação	Verificação, análise de documentação, ensaio

Identificação	PR-006
Desempenho	As informações apresentadas pelo EGSE ao operador do experimento não devem ser ambíguas
Título	Ambiguidade das informações no EGSE
Justificativa	Evitar julgamentos imprecisos por parte do operador
Tipo	Projeto
Responsabilidade	Técnica do experimentador
Relacionado a	REST-016
Tolerância	N/A
Verificação	Inspeção, demonstração, análise de documentação

Identificação	PR-007
Desempenho	As informações apresentadas pelo EGSE ao operador do experimento devem estar sempre visíveis ao operador
Título	Visibilidade das informações no EGSE
Justificativa	Evitar julgamentos imprecisos por parte do operador
Tipo	Projeto
Responsabilidade	Técnica do experimentador
Relacionado a	REST-016
Tolerância	N/A
Verificação	Inspeção, demonstração, análise de documentação

Identificação	PR-008
Desempenho	As informações apresentadas pelo EGSE ao operador do experimento de sistema computacional devem estar sempre na tela principal
Título	Tela principal com as informações do EGSE
Justificativa	Evitar julgamentos imprecisos por parte do operador
Tipo	Projeto
Responsabilidade	Técnica do experimentador
Relacionado a	REST-016
Tolerância	N/A
Verificação	Inspeção, demonstração, análise de documentação

Identificação	PR-009
Desempenho	As informações apresentadas pelo EGSE ao operador do experimento devem ter uma área mínima de visualização de 400mm^2. Com a menor dimensão de pelo menos 15 mm
Título	Área de visualização das informações no EGSE
Justificativa	Evitar julgamentos imprecisos por parte do operador
Tipo	Projeto
Responsabilidade	Técnica do experimentador
Relacionado a	REST-016
Tolerância	N/A
Verificação	Inspeção, demonstração, análise de documentação

Identificação	PR-010
Desempenho	Nas informações apresentadas pelo EGSE deve-se utilizar de cores para indicar se cada grandeza indicada está dentro da faixa de operação esperada. Deve ser usada uma segunda cor para indicar a grandeza acima da faixa de operação, e uma terceira cor para abaixo da faixa.
Título	Uso de cores nas informações no EGSE
Justificativa	Evitar julgamentos imprecisos por parte do operador
Tipo	Projeto
Responsabilidade	Técnica do experimentador
Relacionado a	REST-016
Tolerância	N/A
Verificação	Inspeção, demonstração, análise de documentação

Identificação	PR-011
Desempenho	As cores utilizadas nas informações apresentadas pelo EGSE devem ser preto, branco, cinza, primárias e secundárias
Título	Uso de cores no EGSE
Justificativa	Evitar julgamentos imprecisos por parte do operador
Tipo	Projeto
Responsabilidade	Técnica do experimentador
Relacionado a	REST-016
Tolerância	N/A
Verificação	Inspeção, demonstração, análise de documentação

Identificação	OP-012
Desempenho	Não deve haver a substituição dos operadores do EGSE entre o EDA e a operação de lançamento
Título	Impossibilidade de substituição dos operadores do EGSE do experimento
Justificativa	Garantir que não sejam efetuadas trocas nas equipes dos operadores do EGSE
Tipo	Operacional
Responsabilidade	Gerencial do experimentador
Relacionado a	REST-021
Tolerância	N/A
Verificação	*Checklist*, Controle de acesso de pessoal envolvido

Recomendações de implementação:

RI-001: O gerenciamento do requisito de segurança GP-001 pode ser apoiado por um checklist.

RI-002: É sugerido que os experimentos disponham de partes sobressalentes, para pronta substituição caso se faça necessário.

RI-003: É possível optar por um experimento completo, sobressalente e aceito, para sua substituição. Isto é recomendável para todos os experimentadores, mas em especial para os que executam troca de amostra no campo de lançamentos.

RI-004: Recomenda-se a substituição dos componentes que receberam estresse durante o desenvolvimento para o seu modelo de aceitação. Recomenda-se a substituição por componentes idênticos, porém novos.

RI-005: Recomenda-se o uso de checklist contando as facilidades e instalações do campo de lançamento para apoiar o trabalho da equipe de validação da manipulação de amostras, aplicável ao requisito GP-003.

RI-006: Recomenda-se o uso de checklist, aplicável ao requisito VR-010, contendo cada um dos testes e itens a serem verificados.

RI-007: Planejar, durante o desenvolvimento, planos de contingências para a simplificação do experimento, a fim de obter sua viabilização. Mesmo que com menos funcionalidades, ou com a experimentação incompleta. Não é incomum a ocorrência desta necessidade.

RI-008: Concepção de experimento modular, onde atenha-se inicialmente no essencial para a experimentação. Os demais módulos podem ser acrescidos dentro das possibilidades. O intuito é dar foco inicialmente ao essencial para o funcionamento do experimento e desempenho da experiência. Caso o prazo disponível permita, podem ser acrescidos módulos que incrementem a funcionalidade do experimento.

RI-009: Em caso de adoção de um projeto modular deve-se priorizar o controle de interfaces, dessa forma equipes distintas podem trabalhar de forma paralela.

RI-010: Para experimentos com amostras sensíveis, é recomendável considerar a utilização das soluções aplicadas a experimentos com acesso tardio.

RI-010: A implementação dos requisitos OP-014 a OP-019 por meio de um painel com 5 sinais luminosos, um por autorização. Uma unidade para cada EGSE de experimento.

RI-011: A implementação dos requisitos OP-020 a OP-025 por meio de um painel com 5 sinais luminosos, um por autorização. Uma unidade para que concentra as informações de todos os experimentos.

RI-012: Priorizar projeto com interfaces e sinais simples entre as partes que compõe o EGSE que são alocadas fisicamente distantes entre si, como por exemplo uma unidade na casamata e outra no abrigo próximo ao lançador. Fazer uso de comandos de contato seco, ao invés de comunicações de dados, por exemplo.

RI-012: A duração do voo dos foguetes VS-30 e VSB-30 alcançam até pretas 15 minutos. Recomenda-se a implementação de auto desligamento, do experimento, após o experimento completar sua experiência em voo. É preferível que este evento seja temporizado a partir do sinal de LO e o tempo para o auto desligamento deve ser acordo com a orientação do coordenador das REs.

Apêndice D

DIAGRAMAS DE DESENVOLVIMENTO

Nesta parte são apresentados todos os diagramas de desenvolvimento modelados na linguagem SysML.

Figura 23 Diagrama de desenvolvimento da restrição de segurança REST-001.

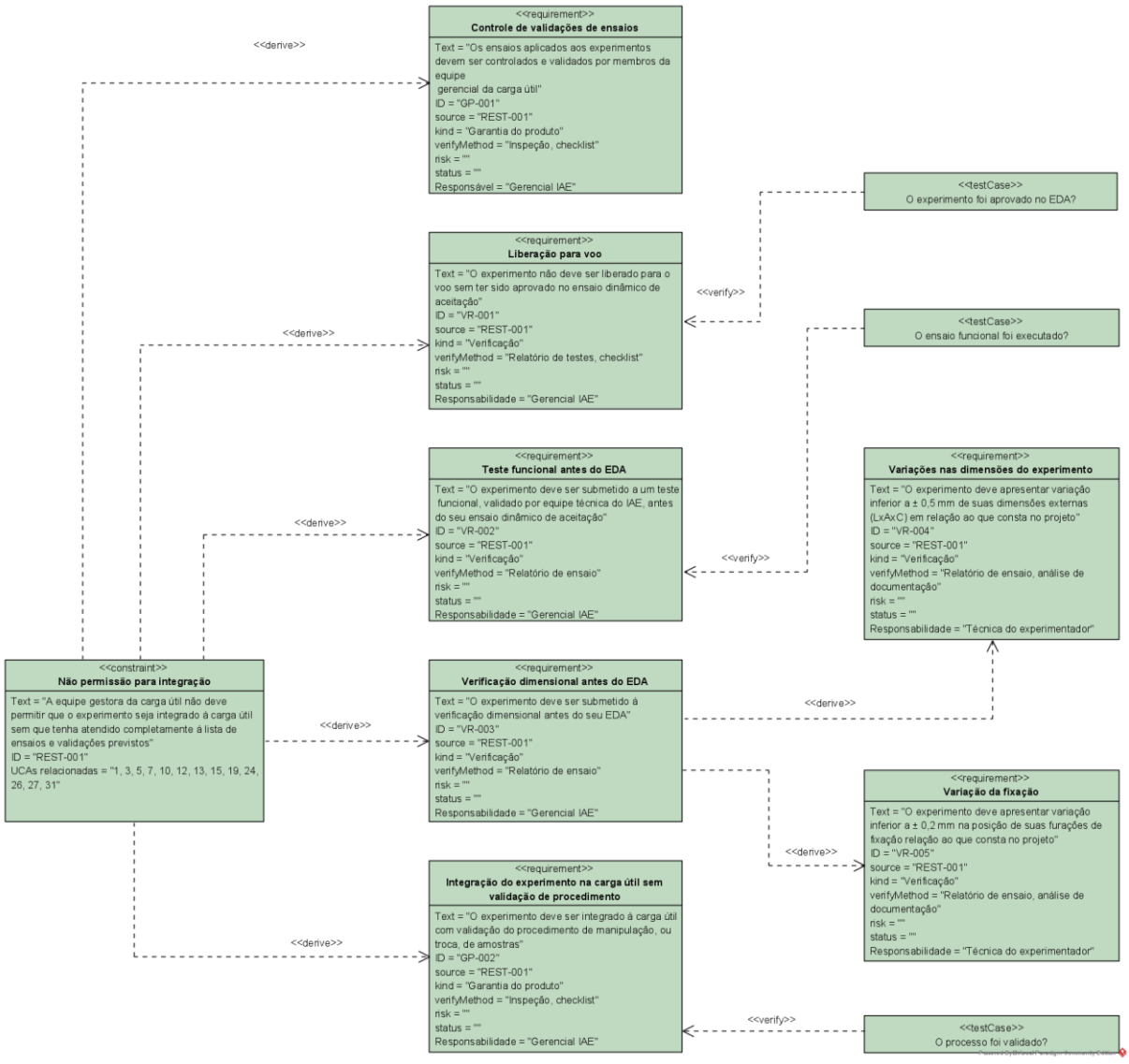


Figura 24 Diagrama de desenvolvimento da restrição de segurança REST-002.

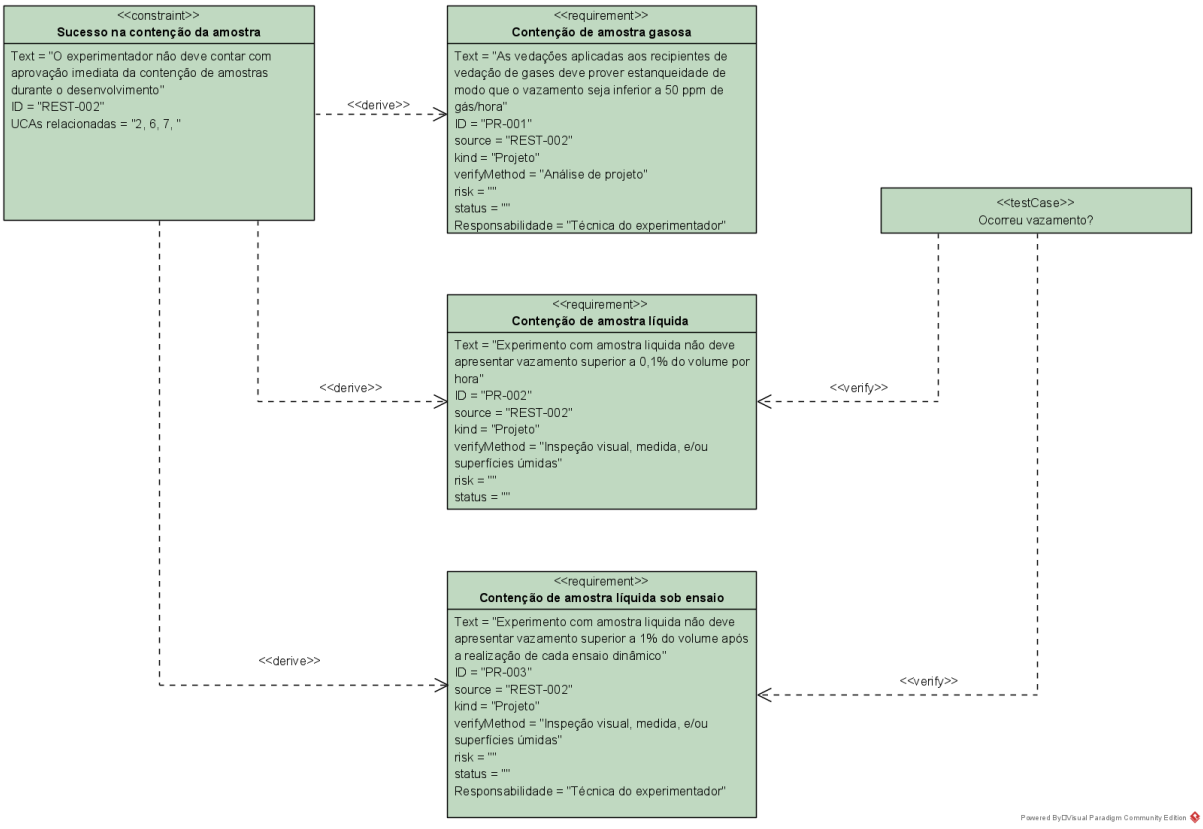


Figura 25 Diagrama de desenvolvimento da restrição de segurança REST-003.

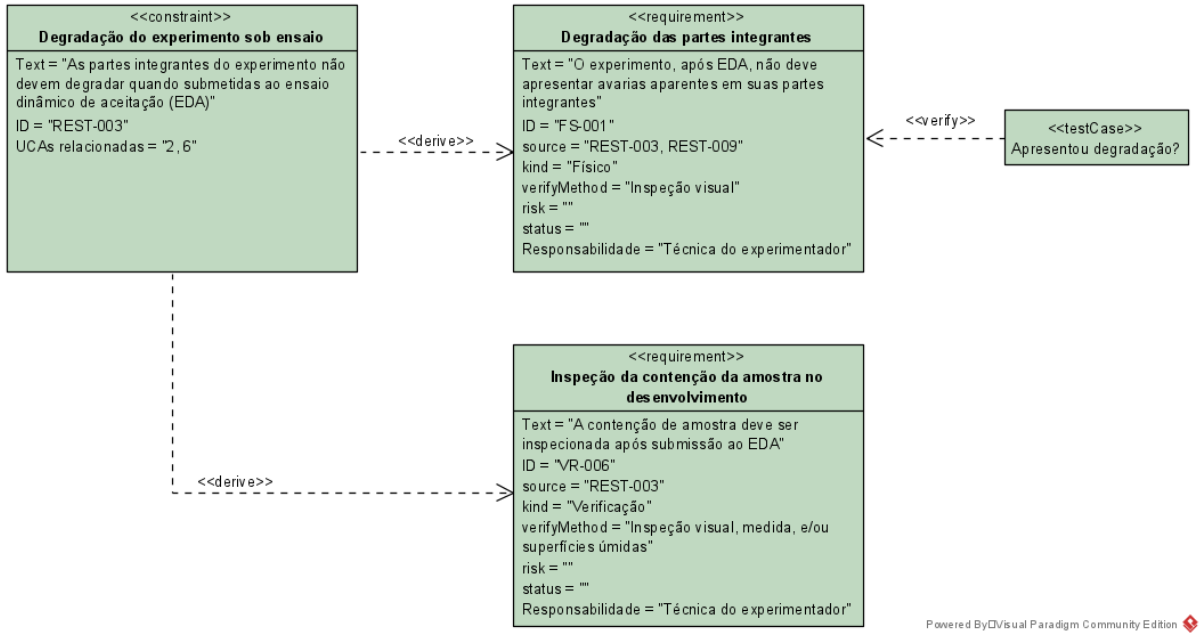


Figura 26 Diagrama de desenvolvimento da restrição de segurança REST-004.

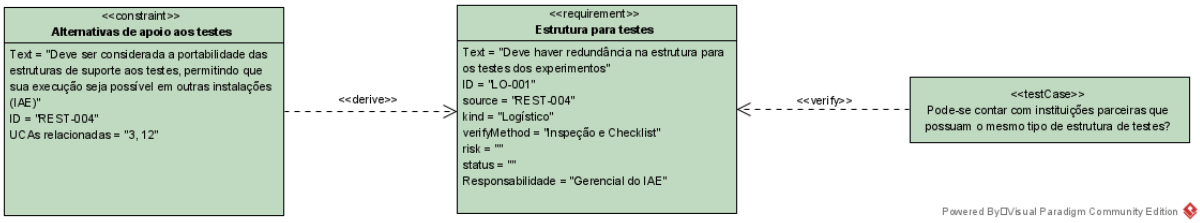


Figura 27 Diagrama de desenvolvimento da restrição de segurança REST-005.

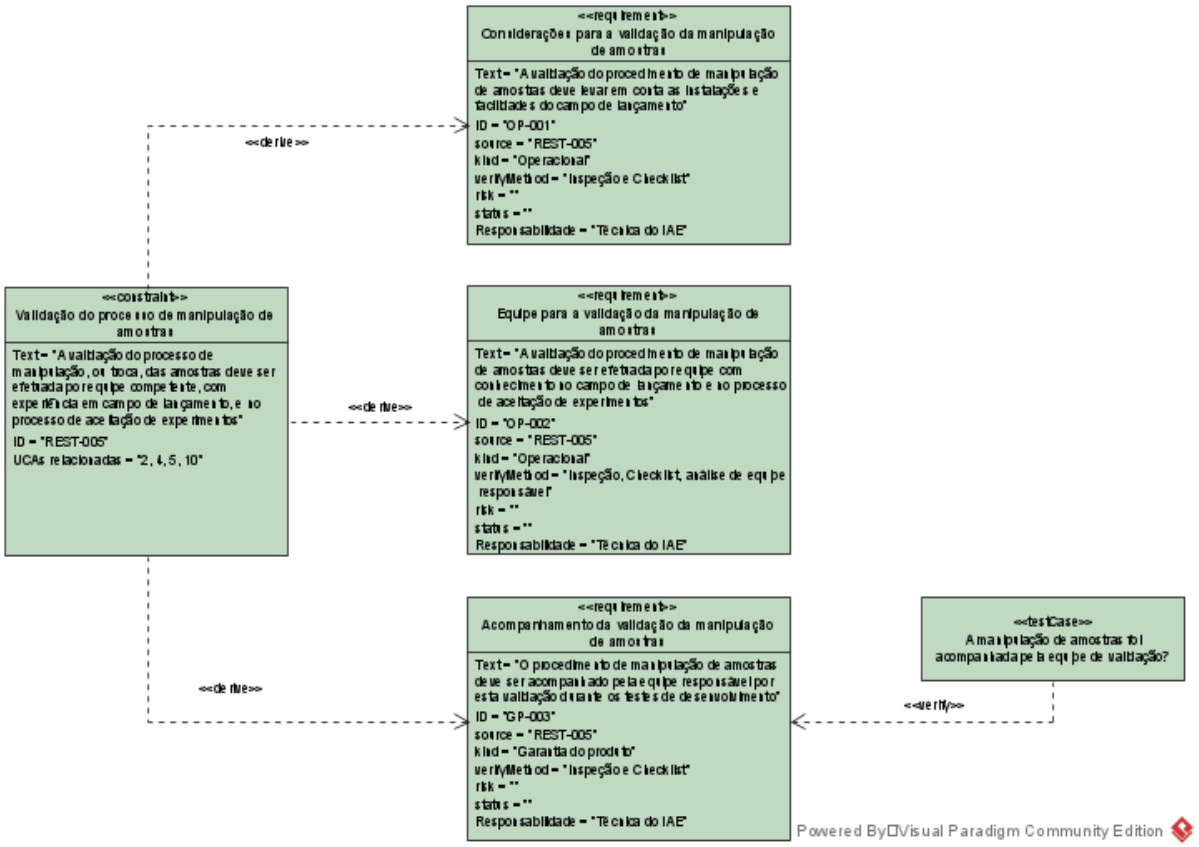


Figura 28 Diagrama de desenvolvimento da restrição de segurança REST-006.

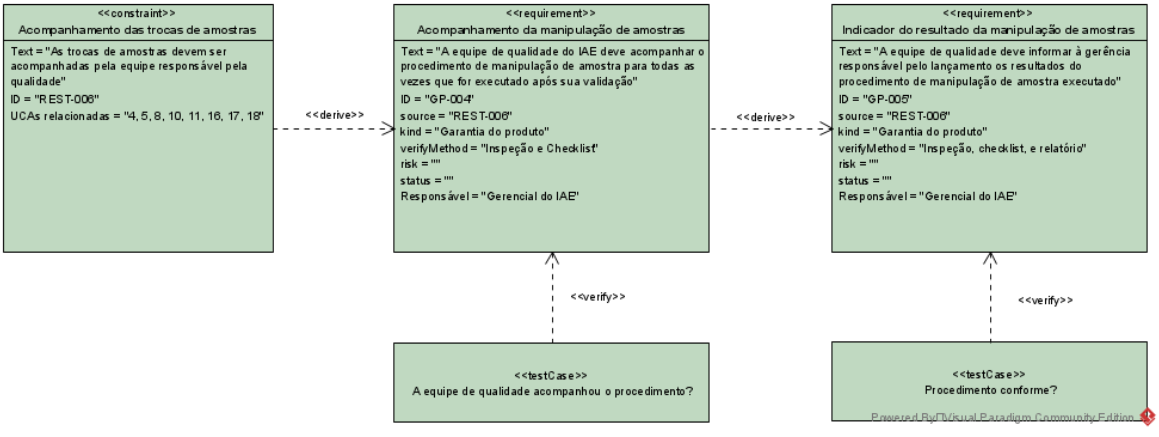


Figura 29 Diagrama de desenvolvimento da restrição de segurança REST-007.

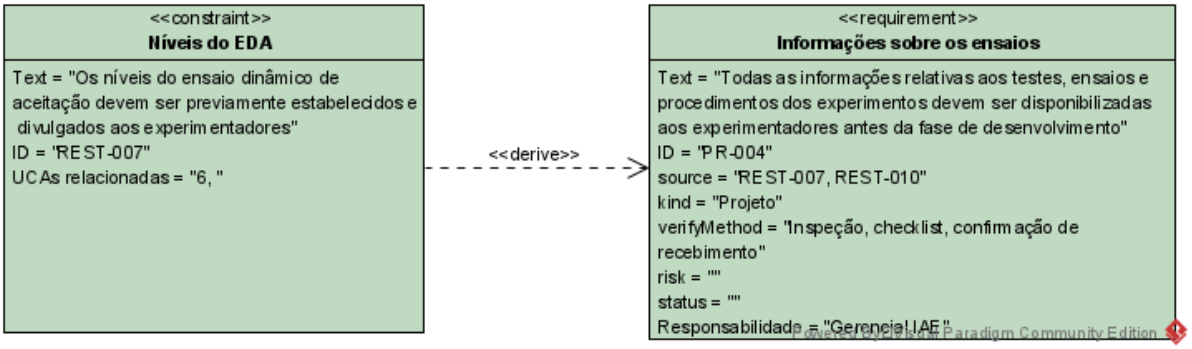


Figura 30 Diagrama de desenvolvimento da restrição de segurança REST-008.

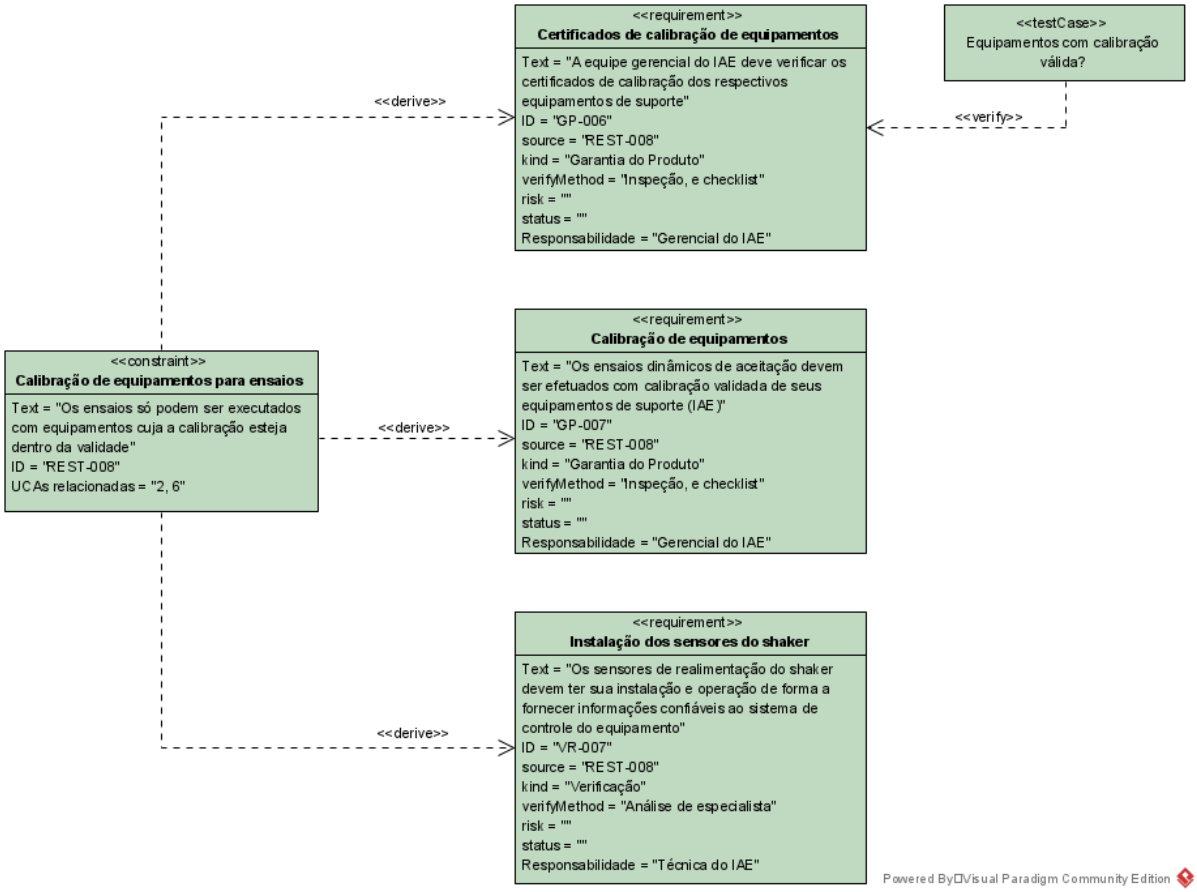


Figura 31 Diagrama de desenvolvimento da restrição de segurança REST-009.

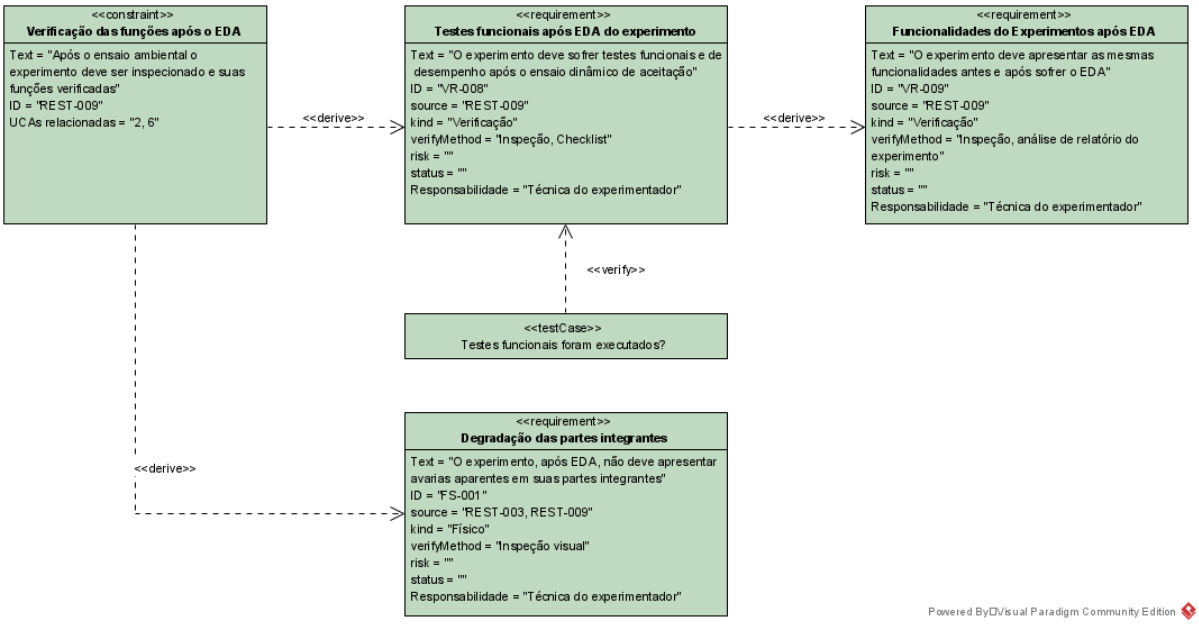


Figura 32 Diagrama de desenvolvimento da restrição de segurança REST-010.

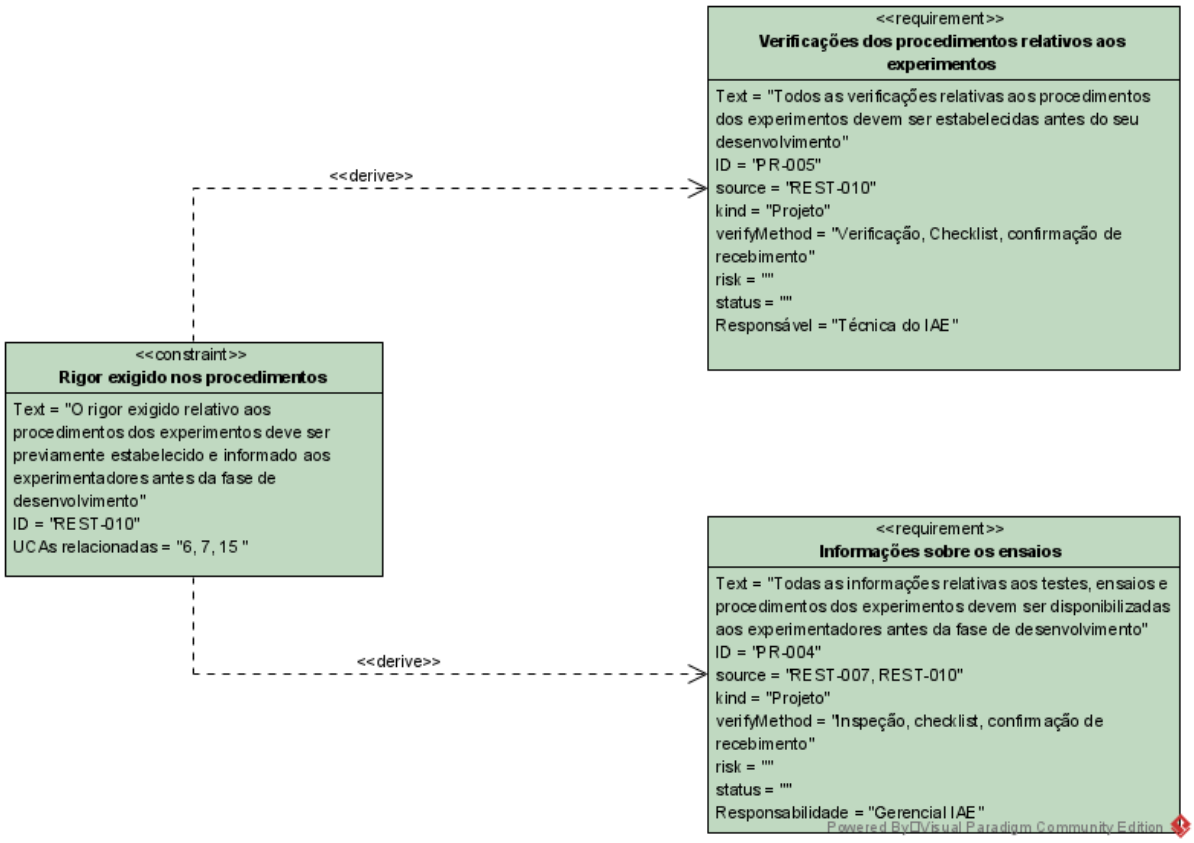


Figura 33 Diagrama de desenvolvimento da restrição de segurança REST-011.

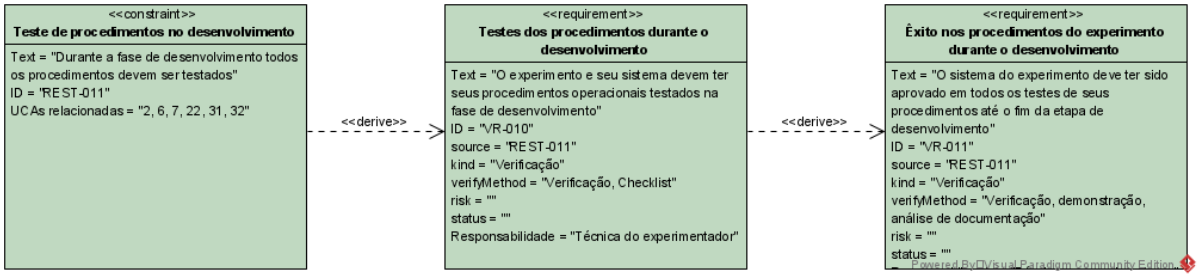


Figura 34 Diagrama de desenvolvimento da restrição de segurança REST-012.

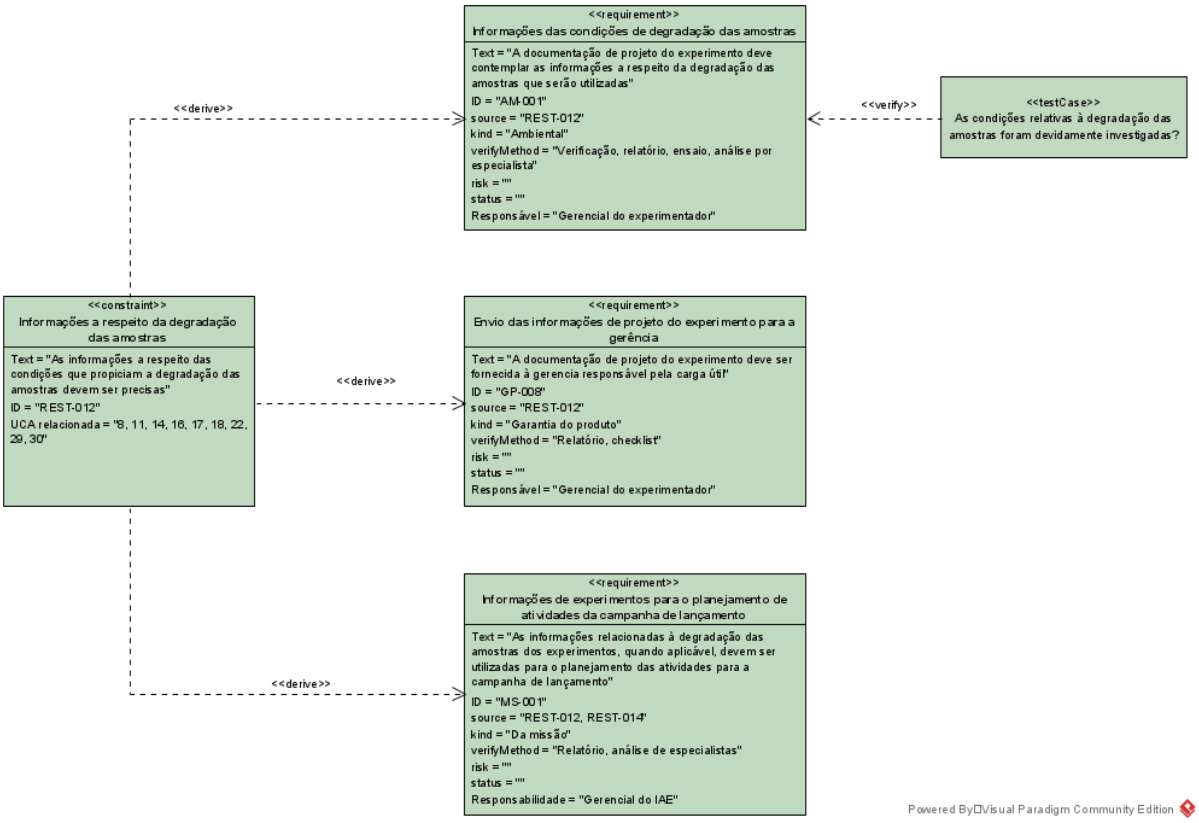


Figura 35 Diagrama de desenvolvimento da restrição de segurança REST-013.

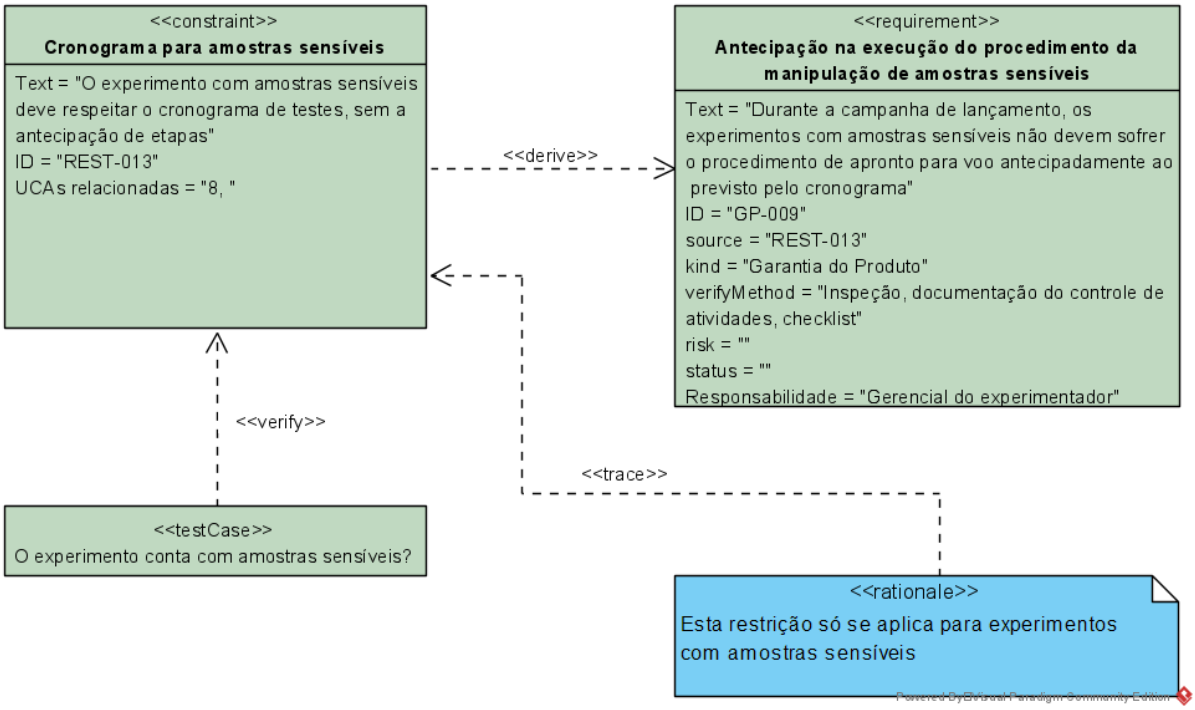


Figura 36 Diagrama de desenvolvimento da restrição de segurança REST-014.

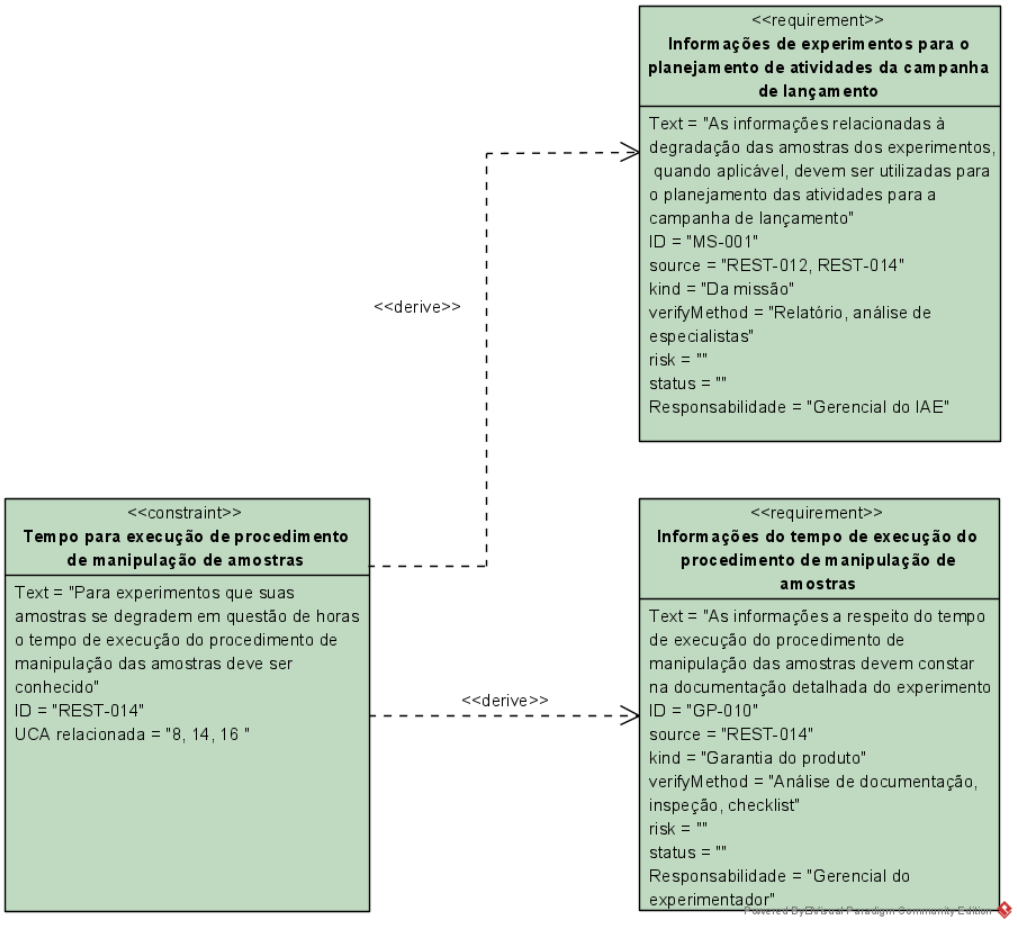


Figura 37 Diagrama de desenvolvimento da restrição de segurança REST-015.

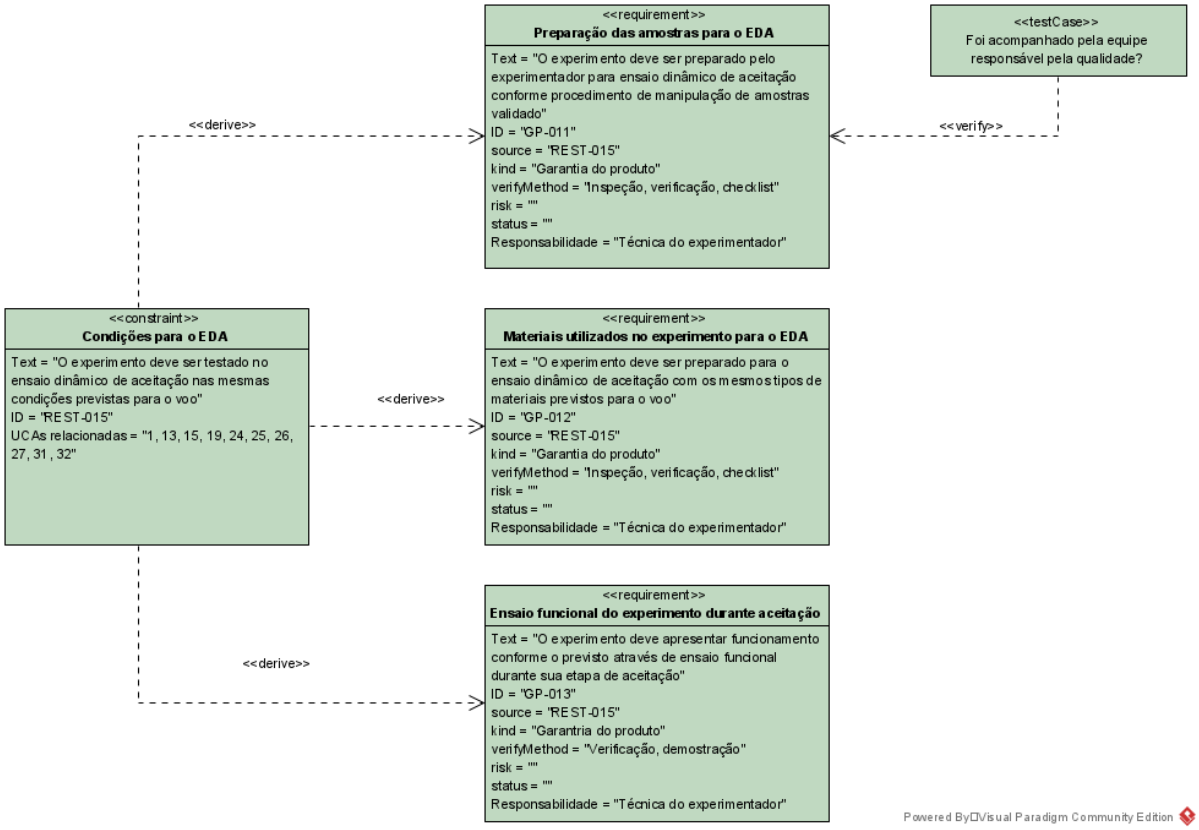


Figura 38 Diagrama de desenvolvimento da restrição de segurança REST-016.

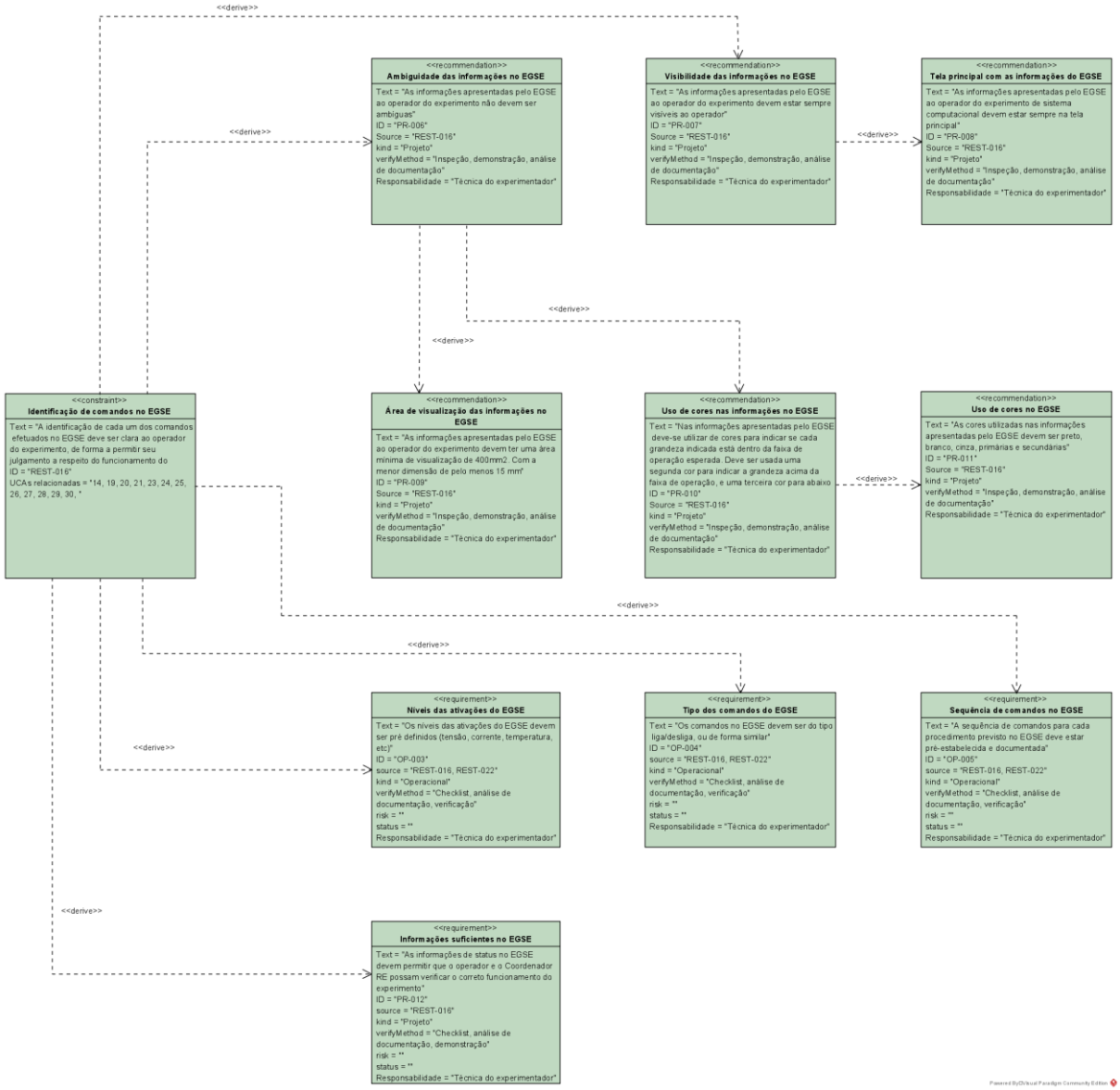


Figura 39 Diagrama de desenvolvimento da restrição de segurança REST-017.

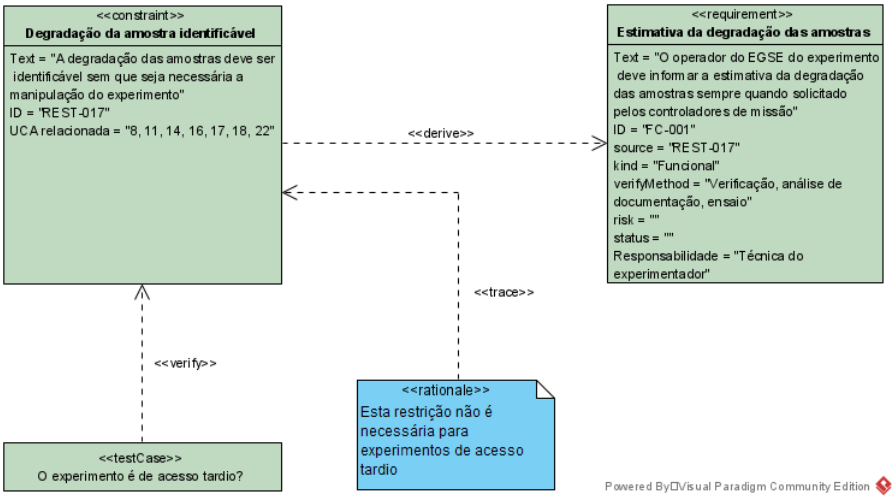


Figura 40 Diagrama de desenvolvimento da restrição de segurança REST-018.

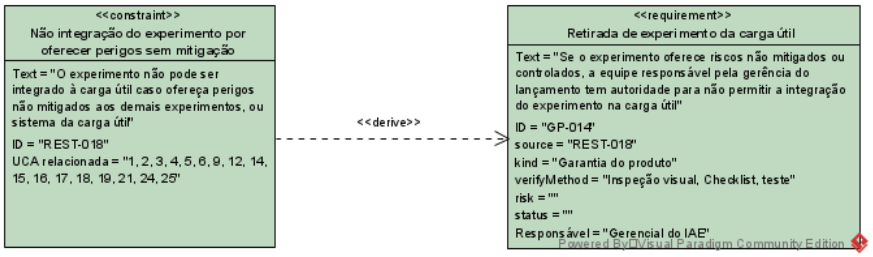


Figura 41 Diagrama de desenvolvimento da restrição de segurança REST-019.

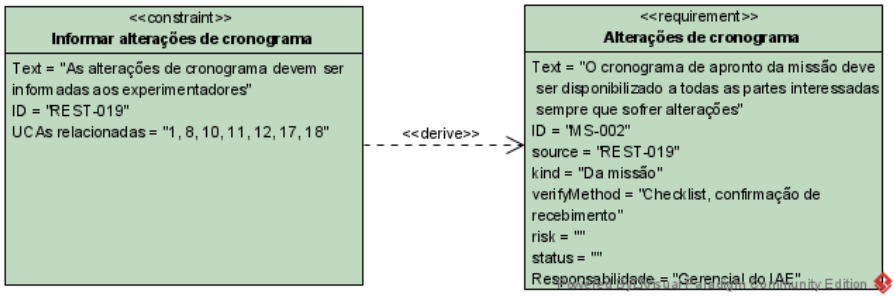


Figura 42 Diagrama de desenvolvimento da restrição de segurança REST-020.

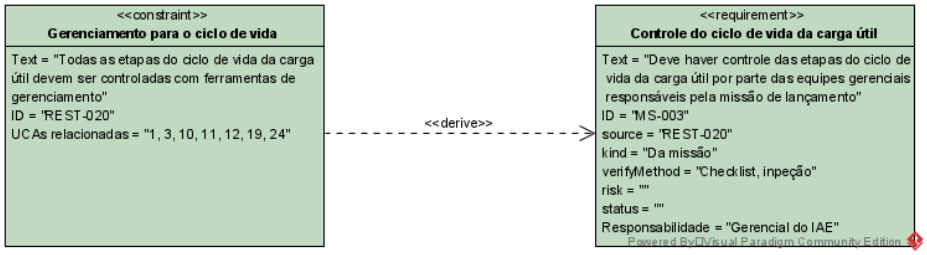


Figura 43 Diagrama de desenvolvimento da restrição de segurança REST-021.

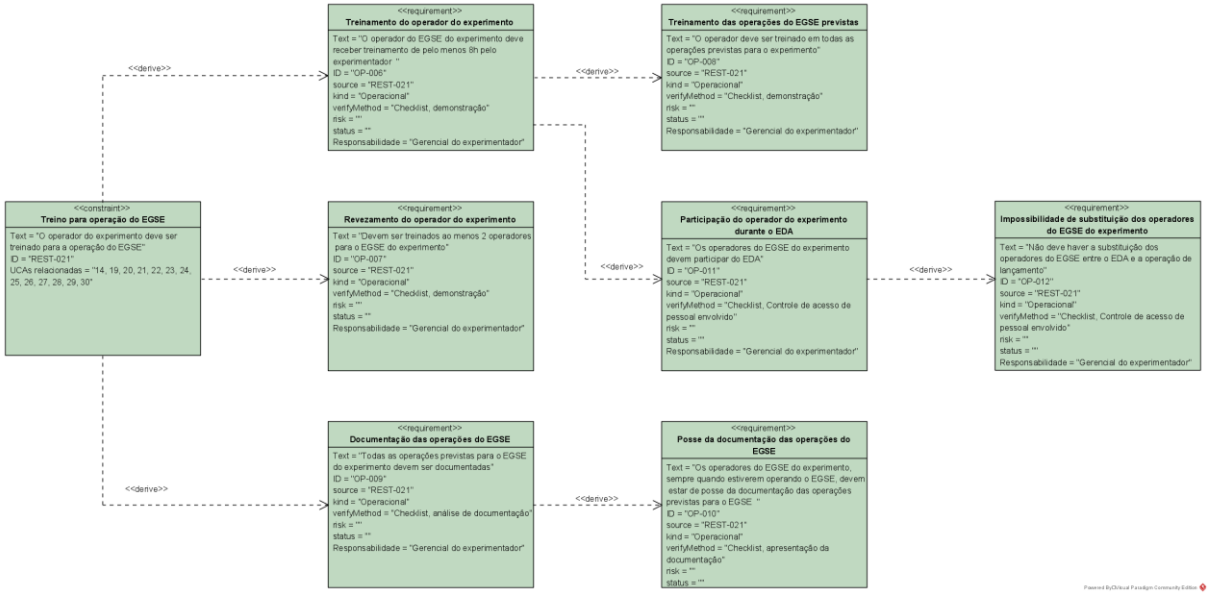


Figura 44 Diagrama de desenvolvimento da restrição de segurança REST-022.

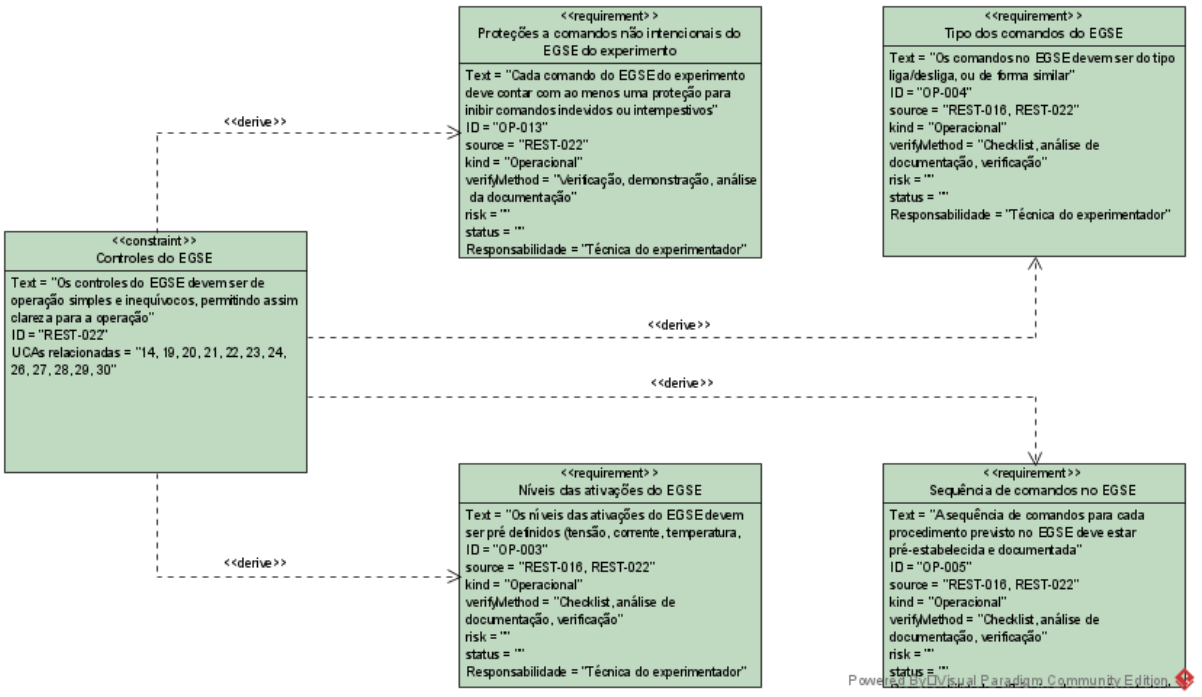


Figura 45 Diagrama de desenvolvimento da restrição de segurança REST-023.

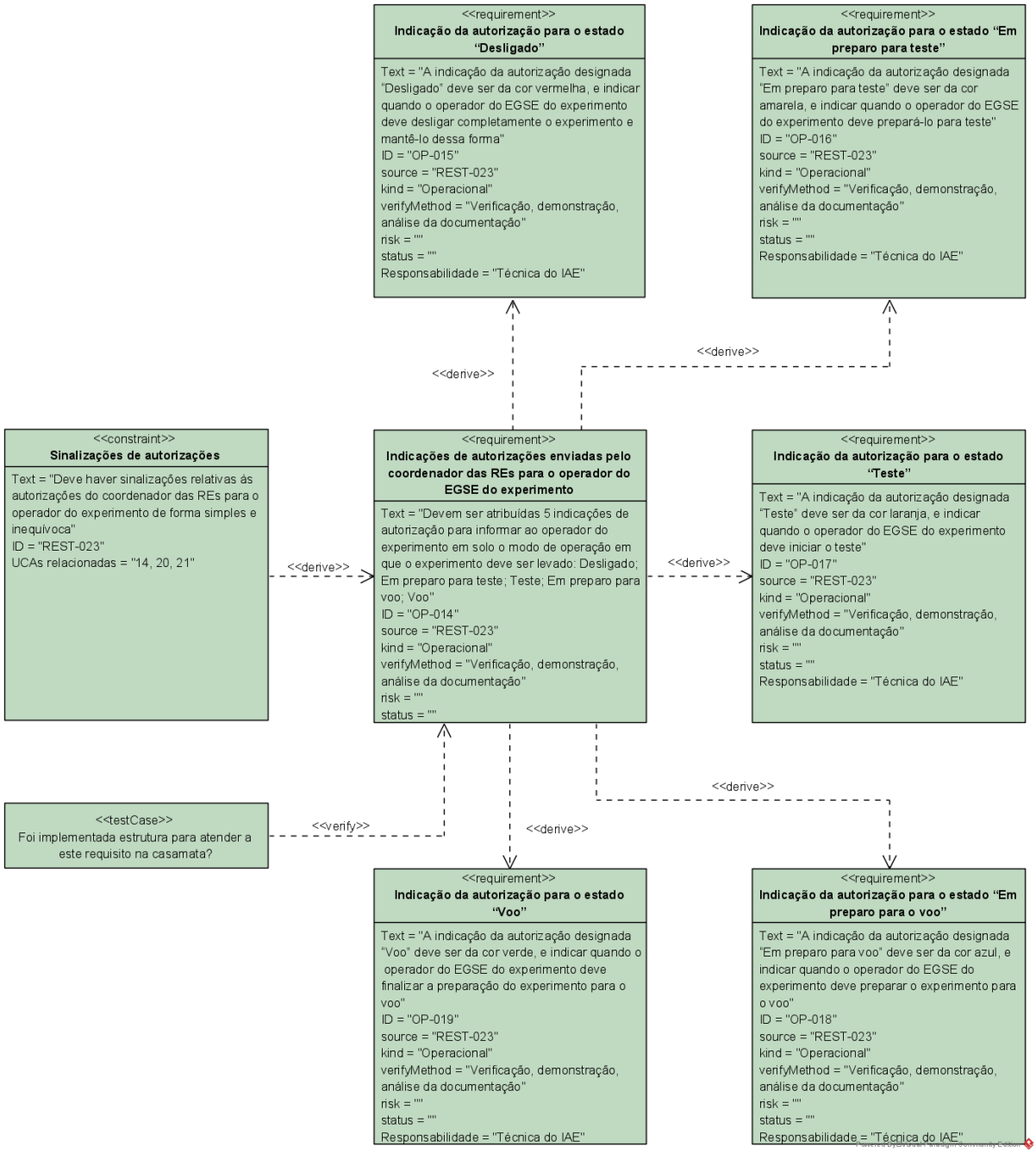


Figura 46 Diagrama de desenvolvimento da restrição de segurança REST-024.

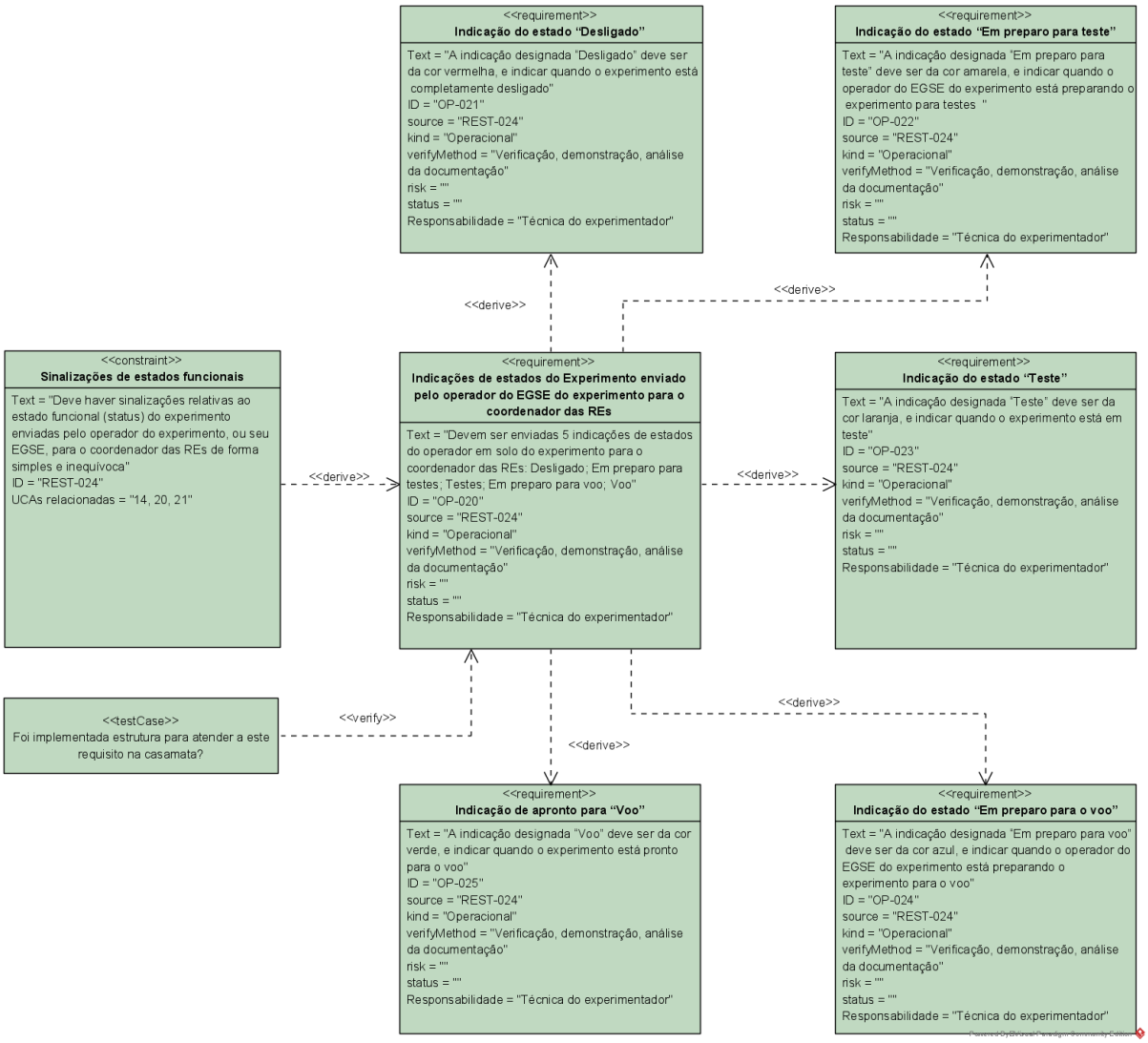


Figura 47 Diagrama de desenvolvimento da restrição de segurança REST-025.

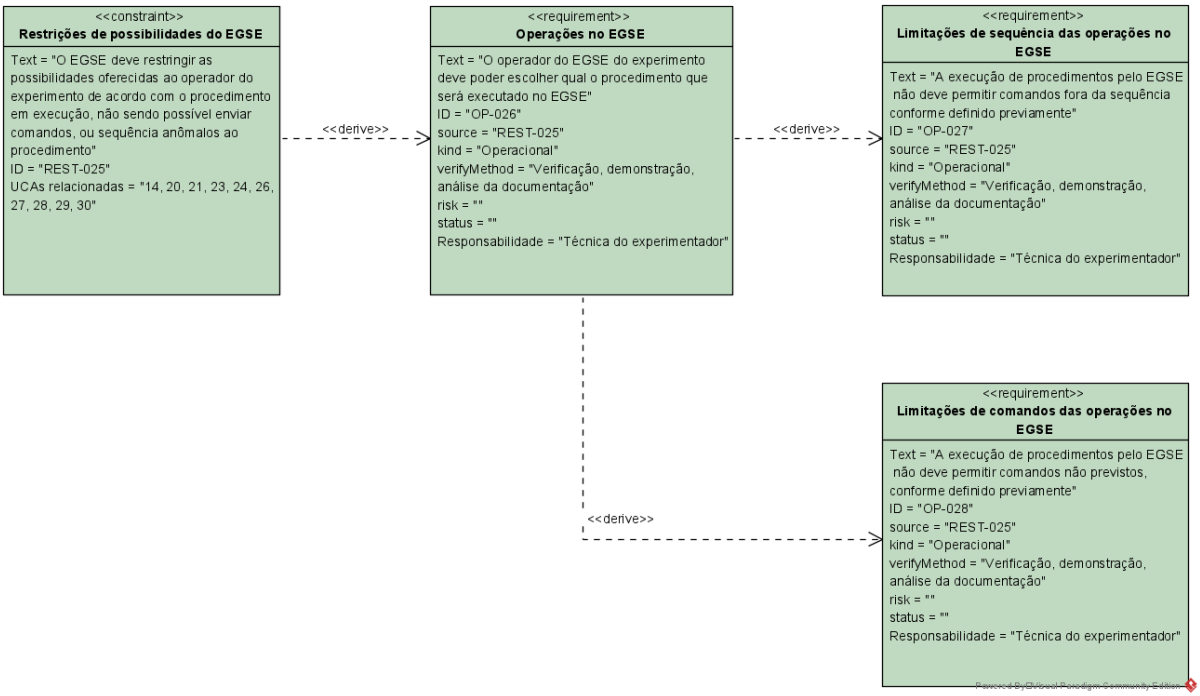


Figura 48 Diagrama de desenvolvimento da restrição de segurança REST-026.

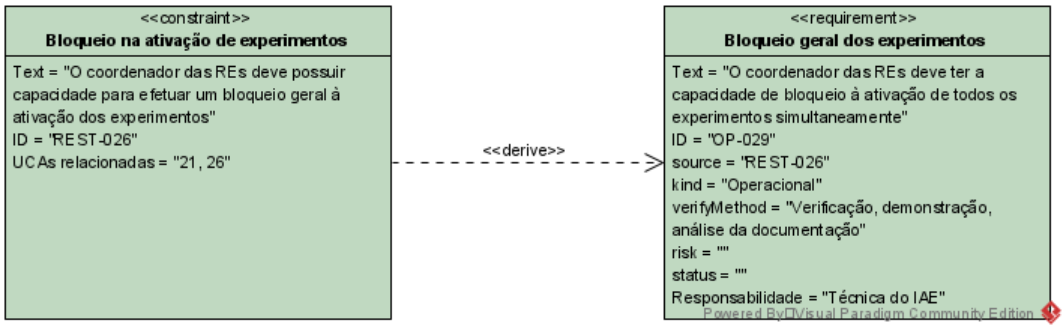


Figura 49 Diagrama de desenvolvimento da restrição de segurança REST-027.

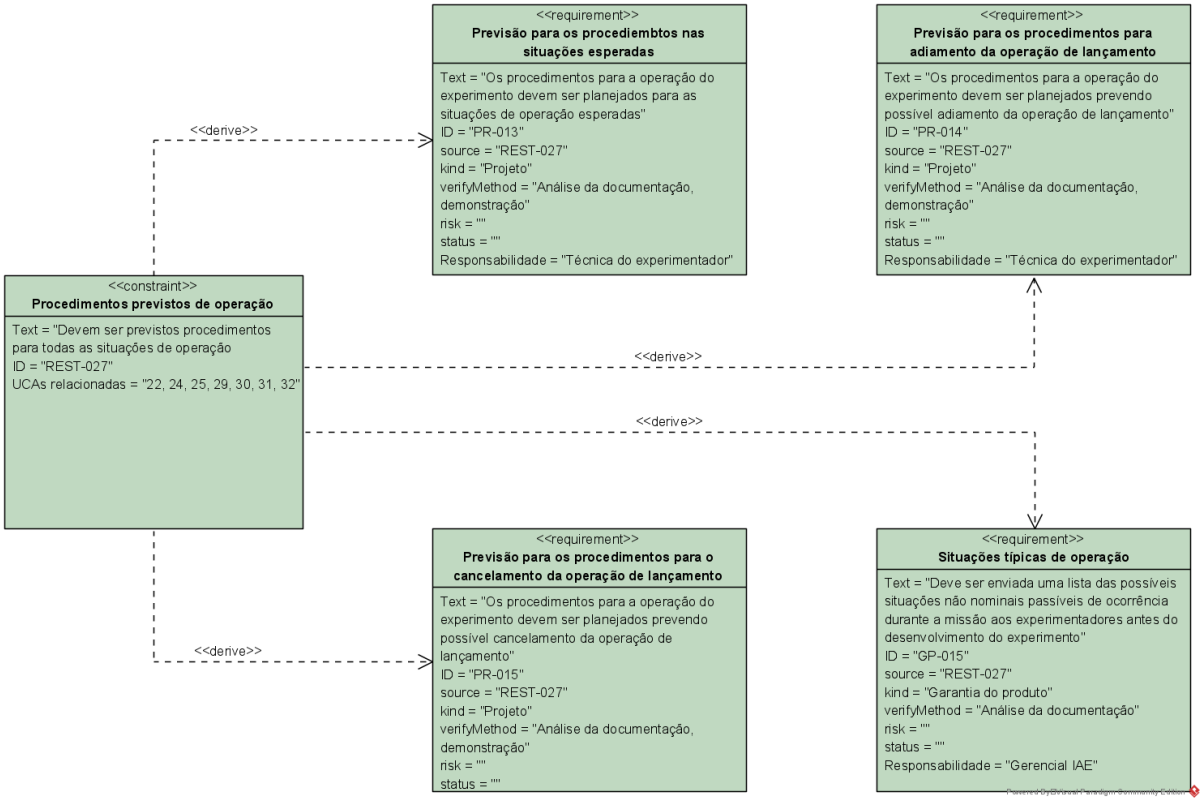
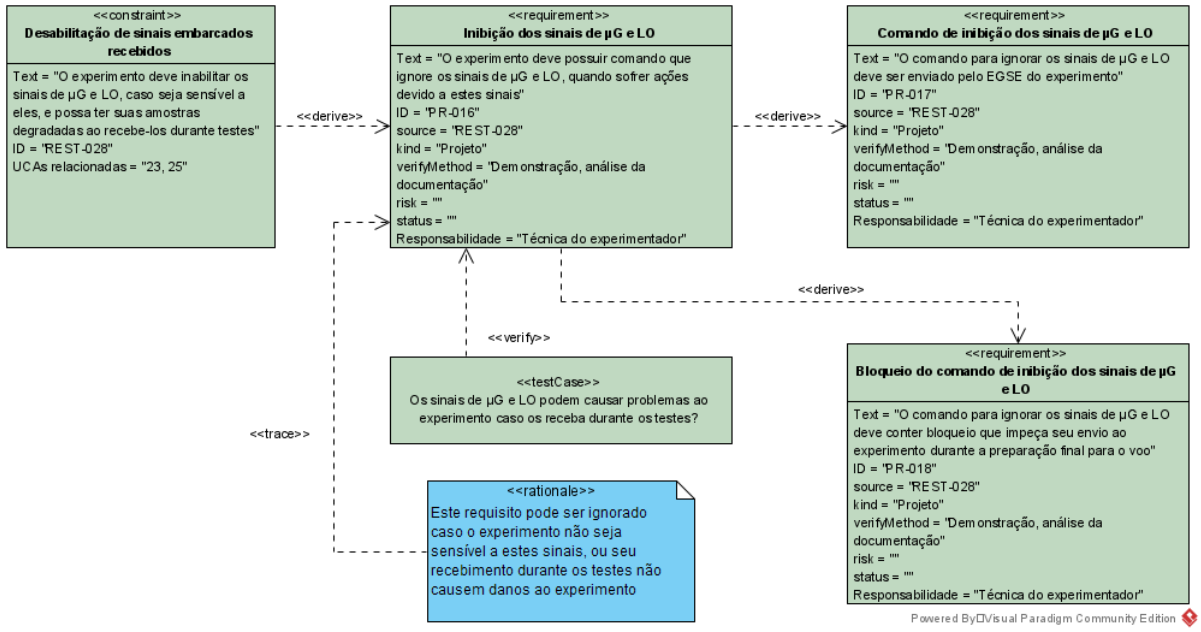


Figura 50 Diagrama de desenvolvimento da restrição de segurança REST-028.



Apêndice E

DIAGRAMAS POR RESPONSABILIDADES

Nesta parte são apresentados todos os diagramas por responsabilidades modelados na linguagem SysML.

Figura 51 Requisitos de responsabilidade gerencial do IAE.

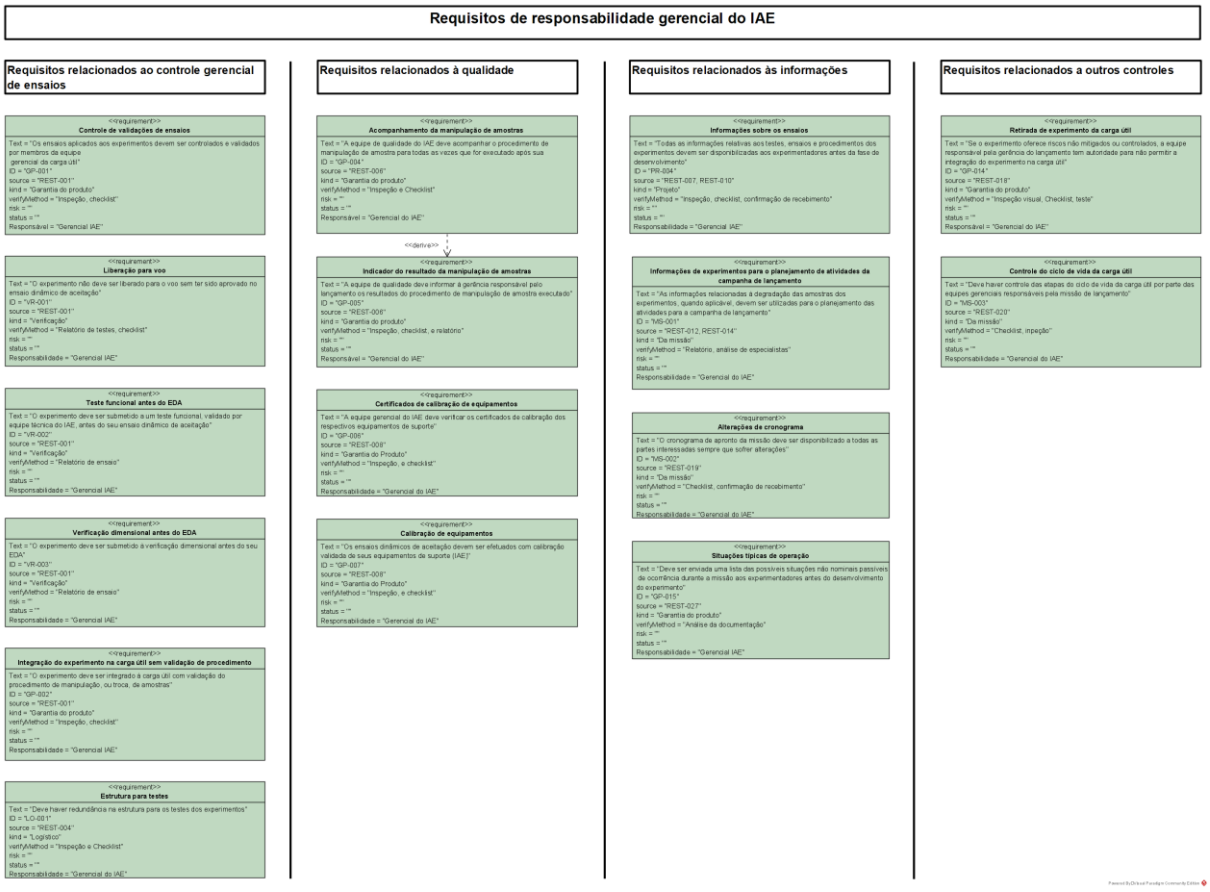


Figura 52 Requisitos de responsabilidade técnica do IAE.

Figura 53 Requisitos de responsabilidade gerencial do experimentador.

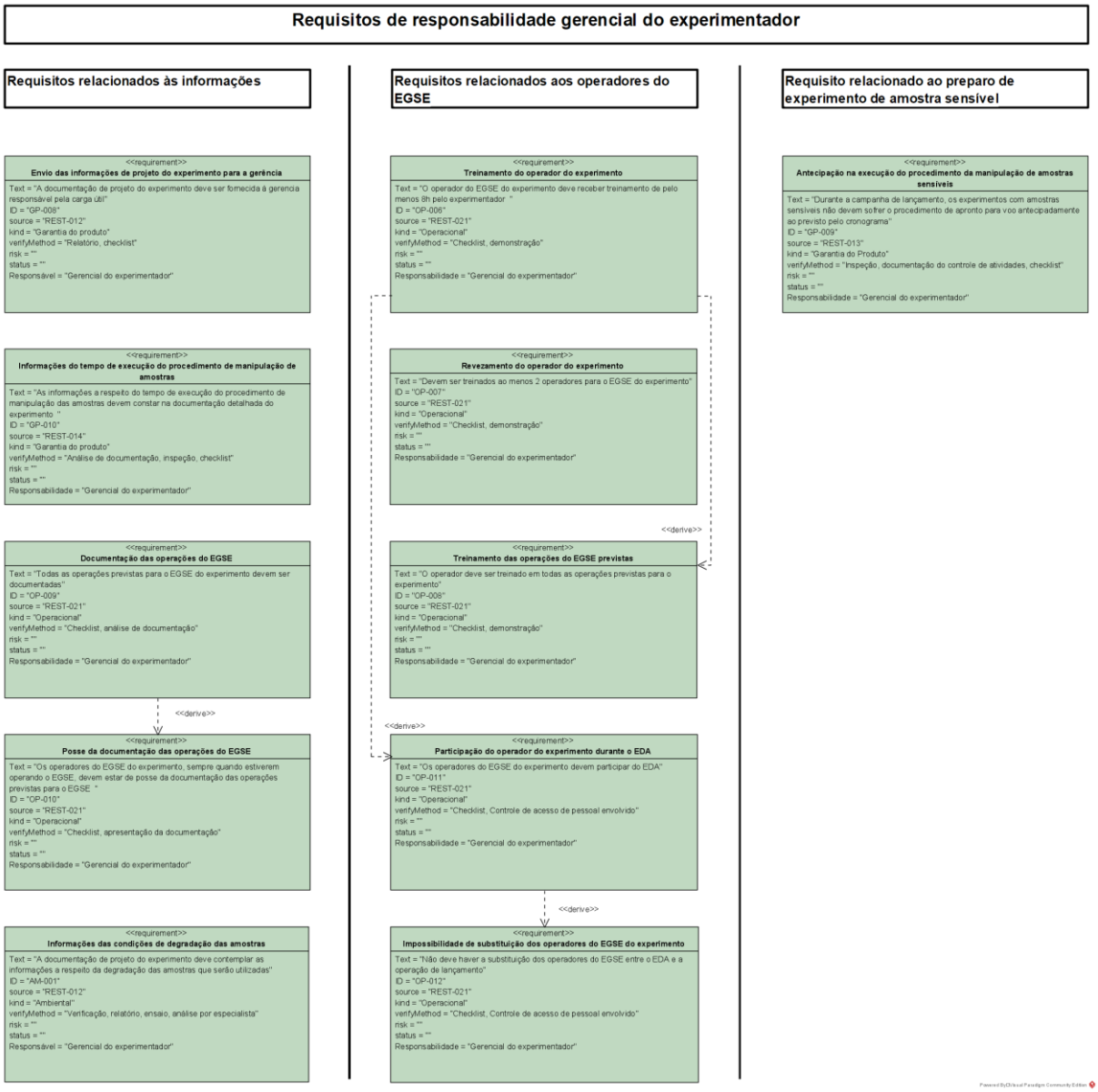


Figura 54 Requisitos de responsabilidade técnica do experimentador, parte 1.

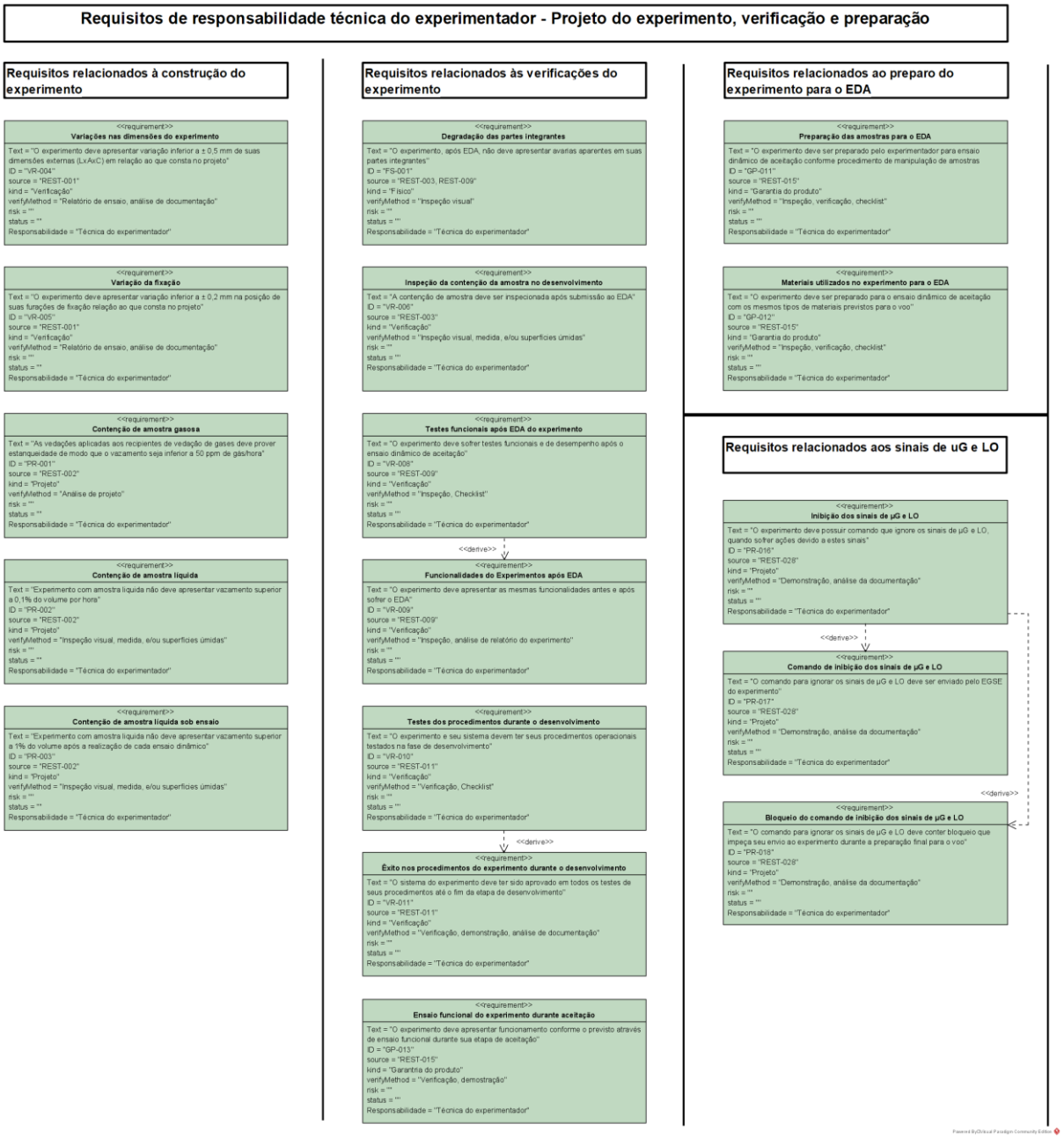
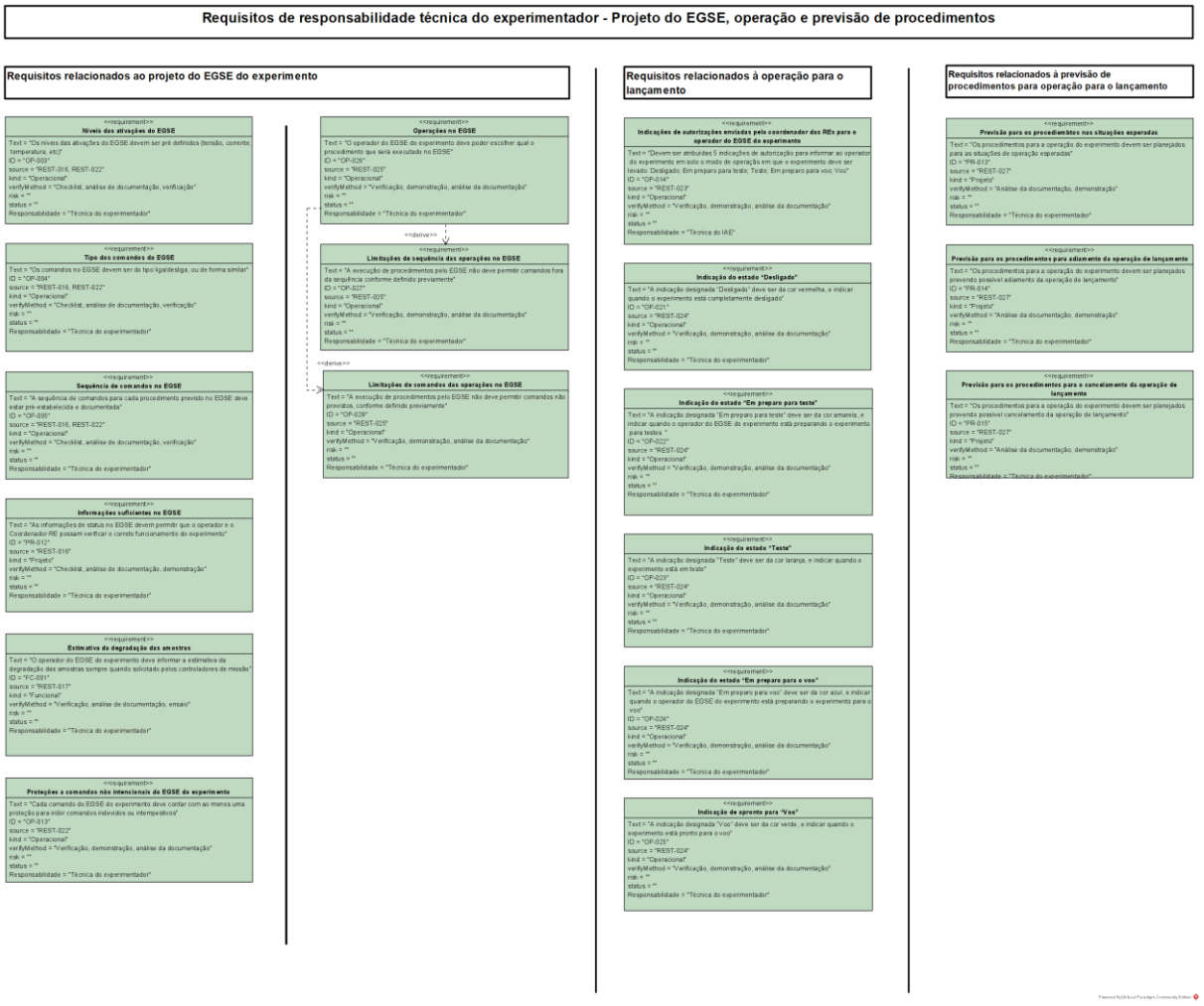


Figura 55 Requisitos de responsabilidade técnica do experimentador, parte 2.



Apêndice F

DIAGRAMAS POR ASSUNTOS

Nesta parte são apresentados todos os diagramas por assuntos modelados na linguagem SysML.

Figura 56 Grupo 1; Questões relacionadas com as competências e controles exercidos pelo IAE.

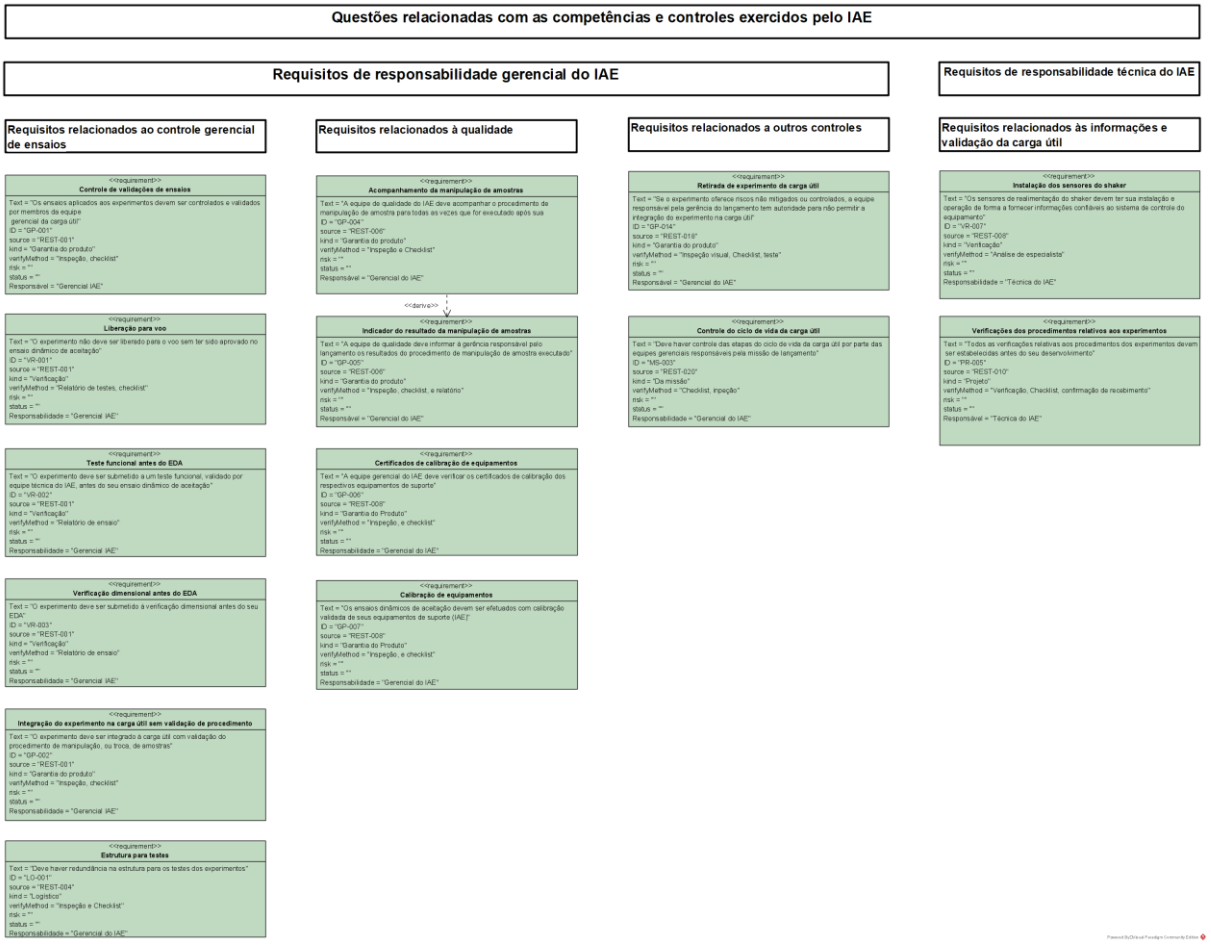


Figura 57 Grupo 2; Conteúdo e fluxo das informações entre o IAE e o experimentador.

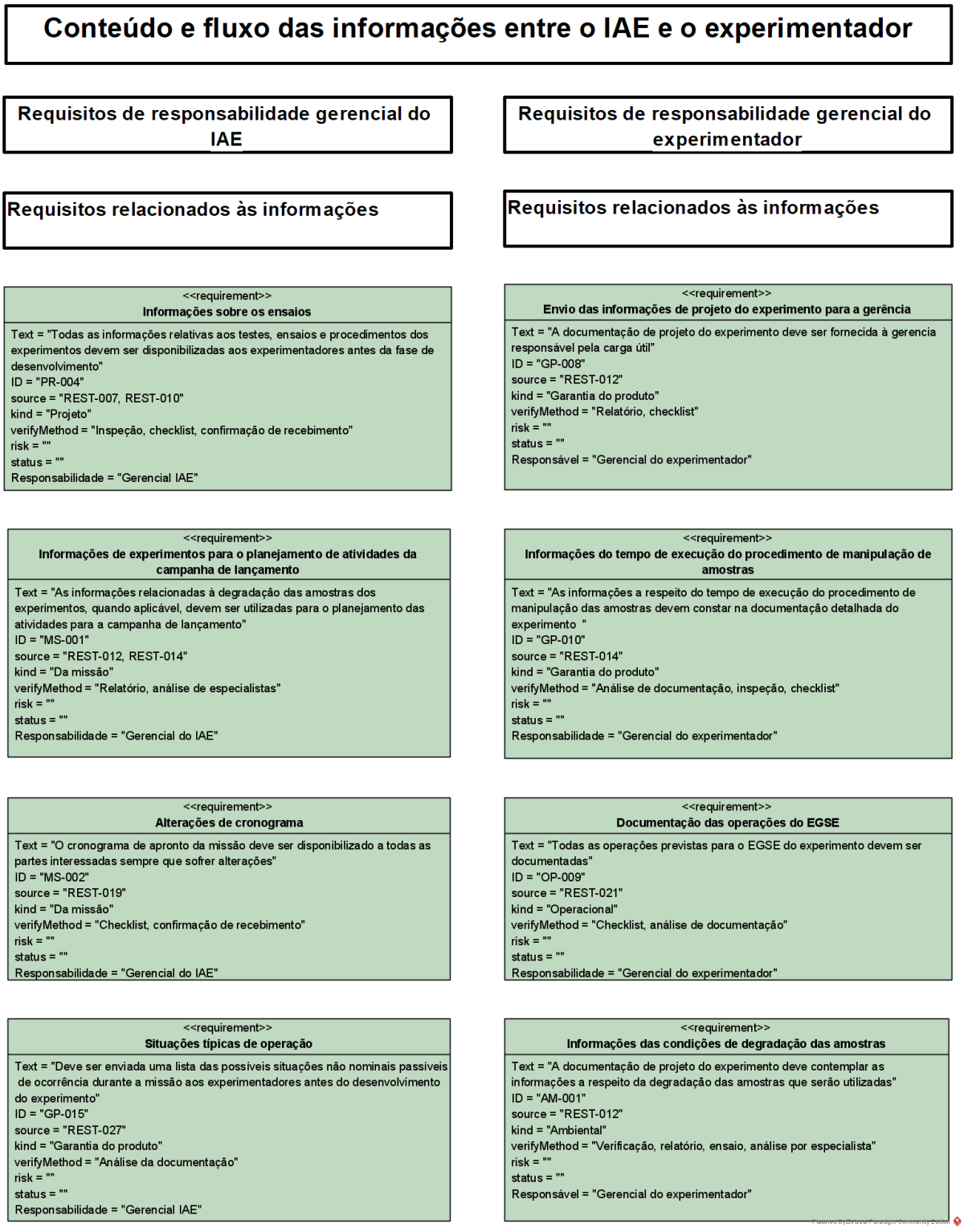


Figura 58 Grupo 3; Questões relacionadas ao operador do EGSE do experimento.

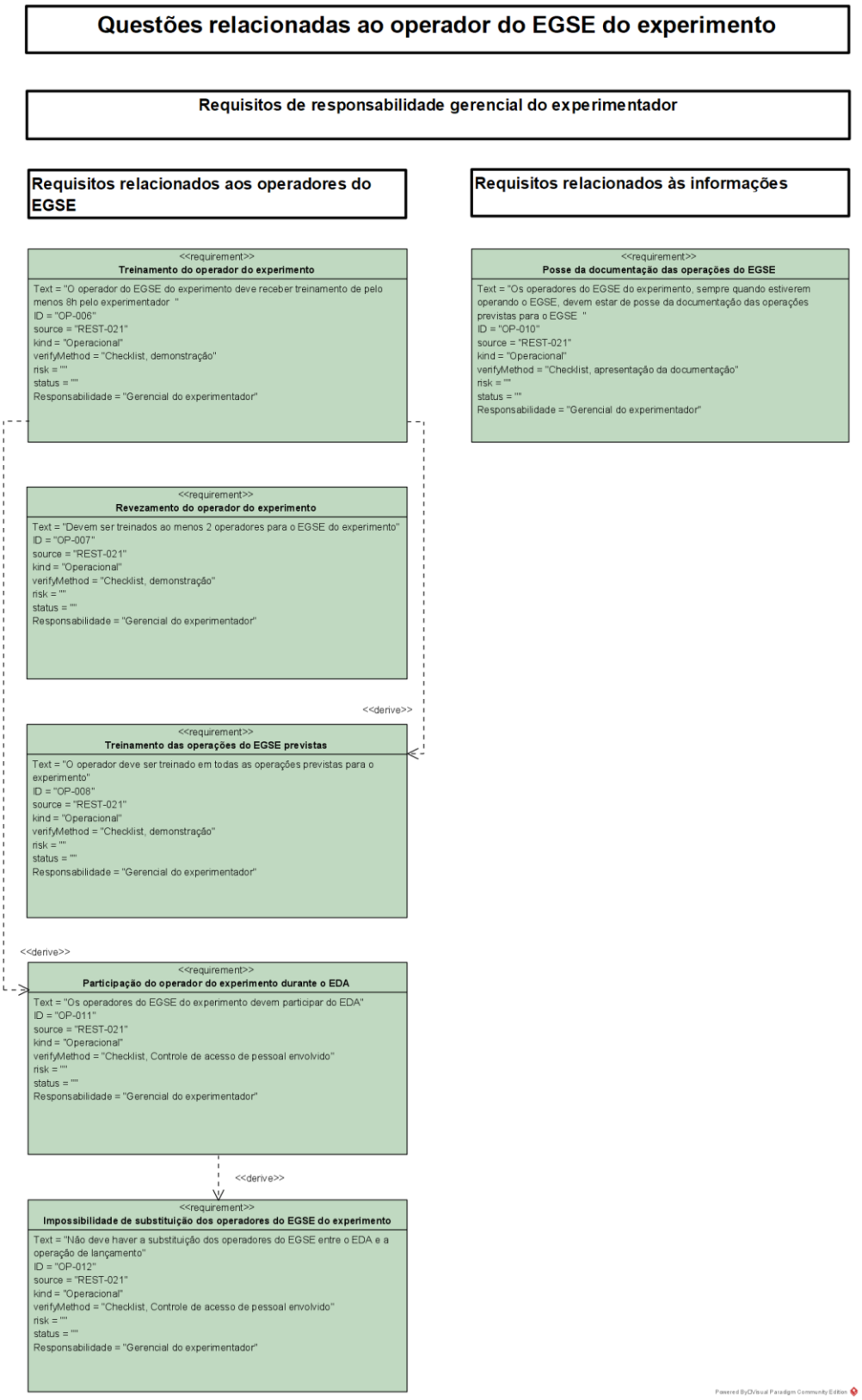


Figura 59 Diagrama por assunto. Grupo 4; comunicação entre o coordenador das REs e o operador do EGSE do experimento durante o lançamento.

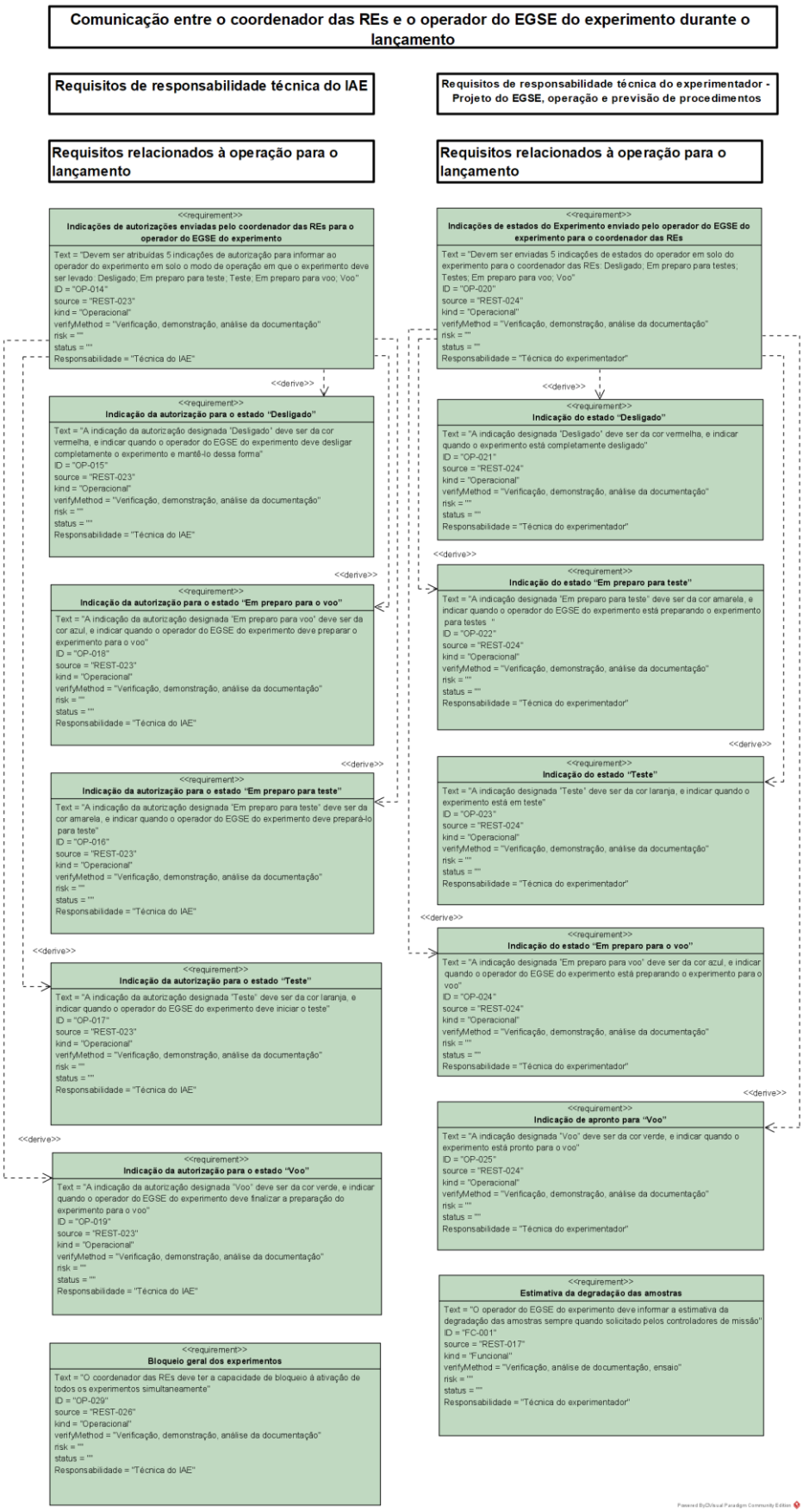


Figura 60 Grupo 5; Questões relacionadas às amostras do experimento.

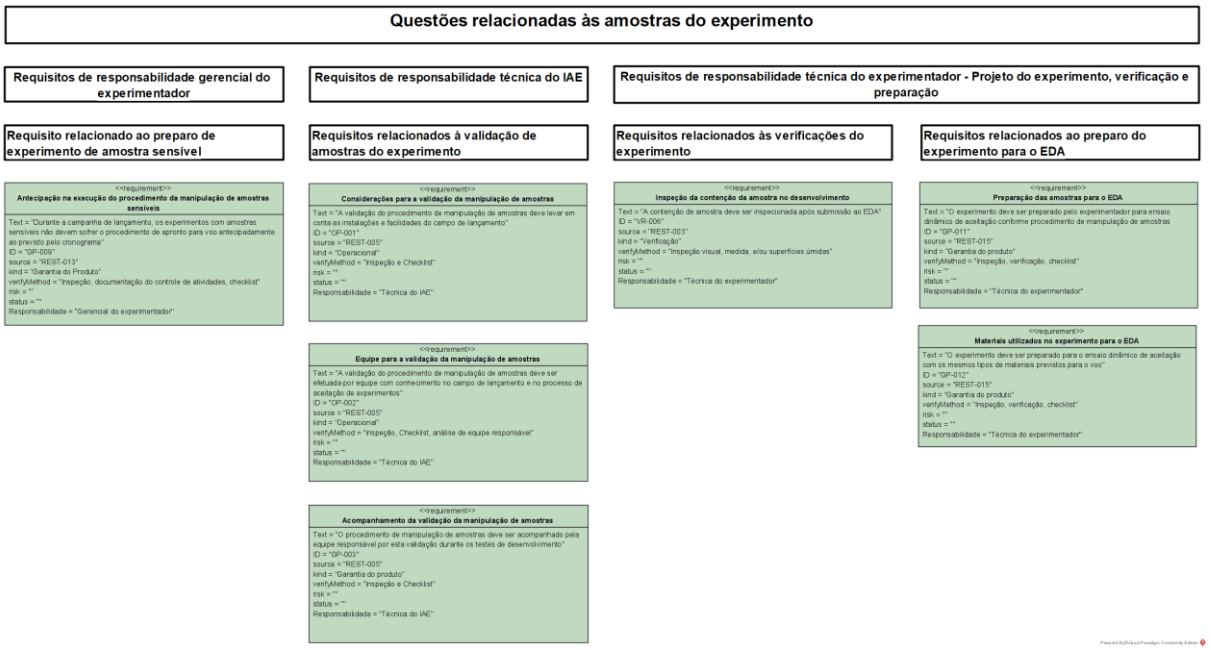


Figura 61 Grupo 6; Parâmetros de projeto para a parte embarcada do experimento.

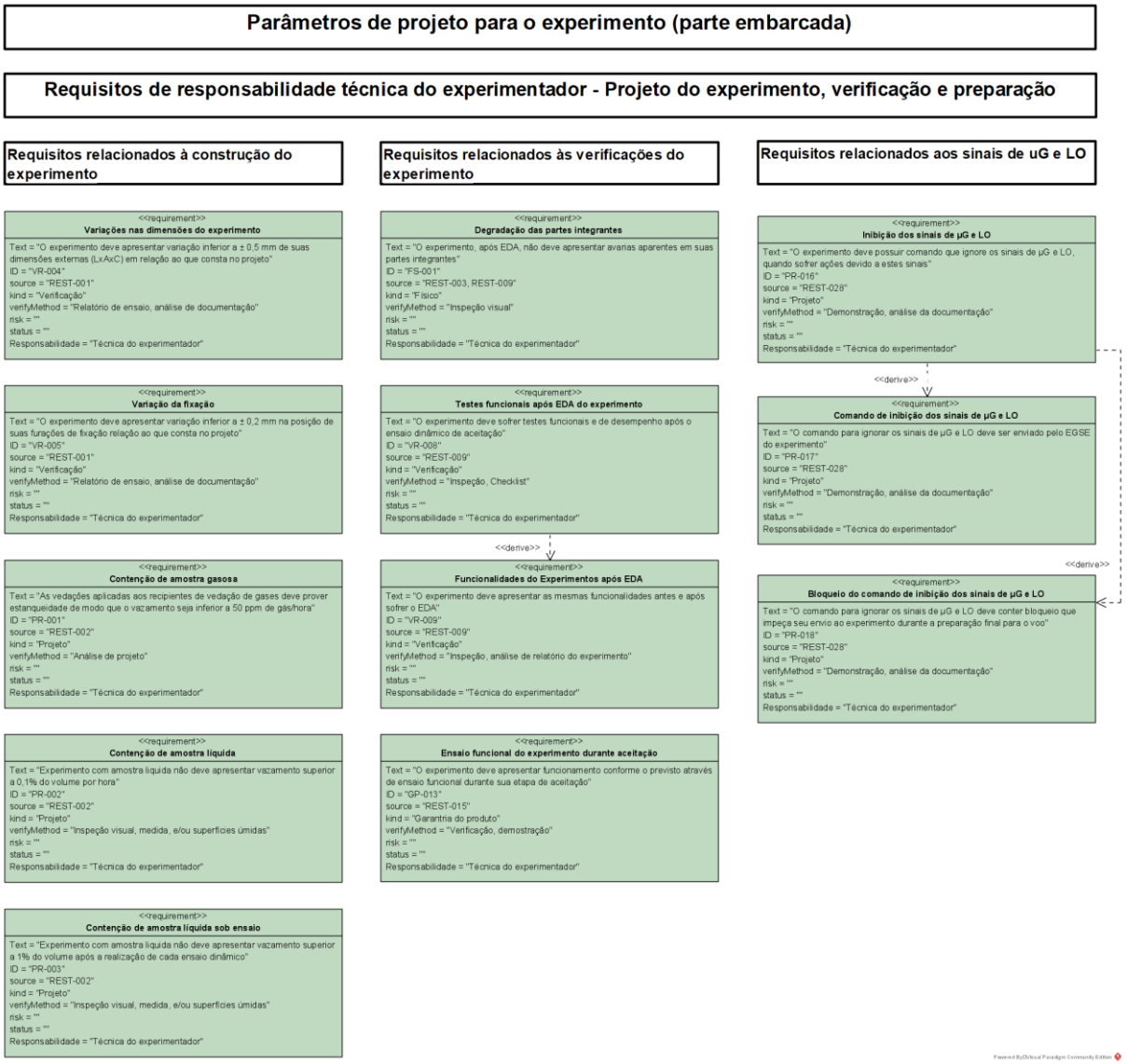


Figura 62 Grupo 7; Procedimentos relacionados ao experimento.

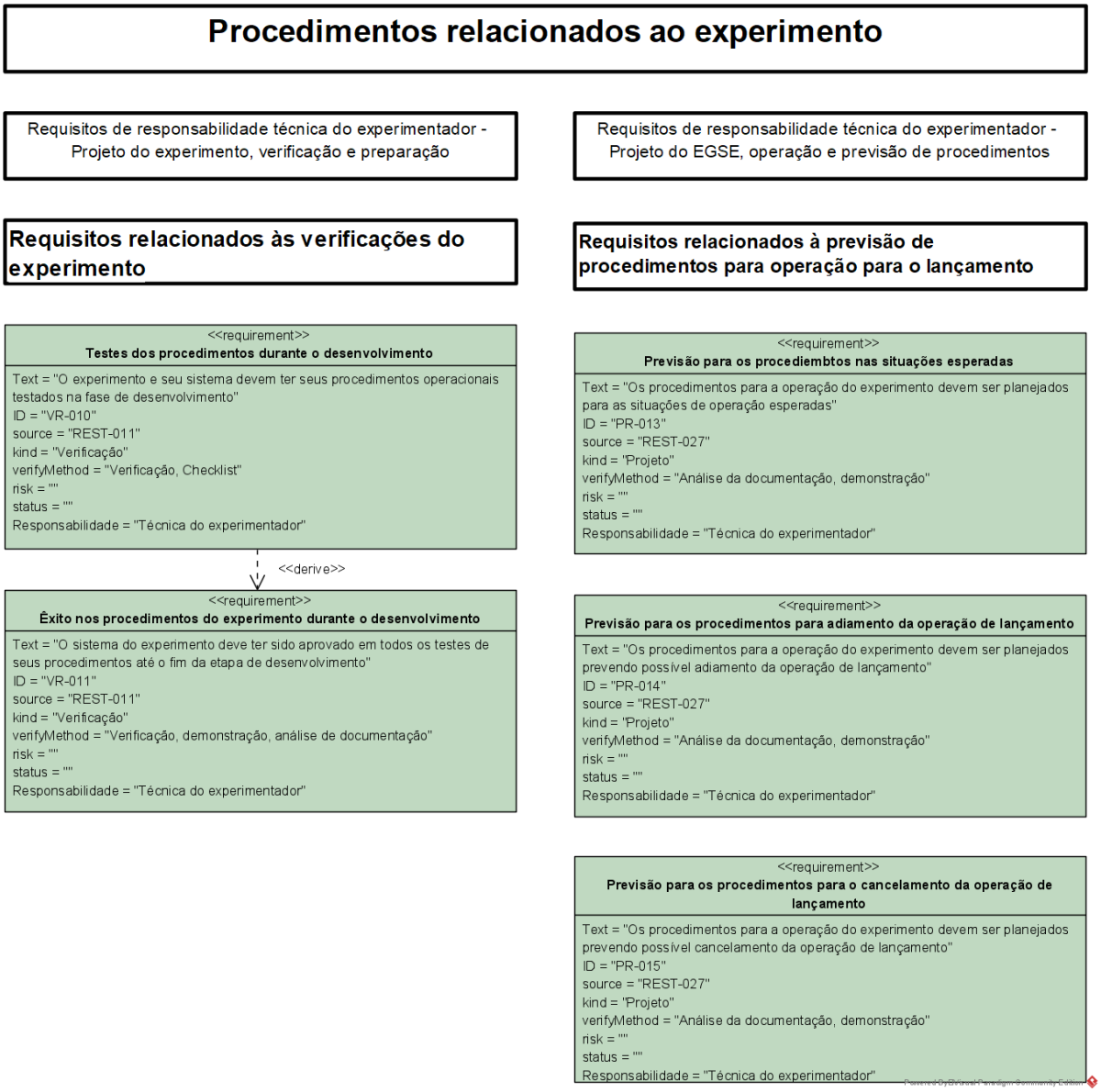
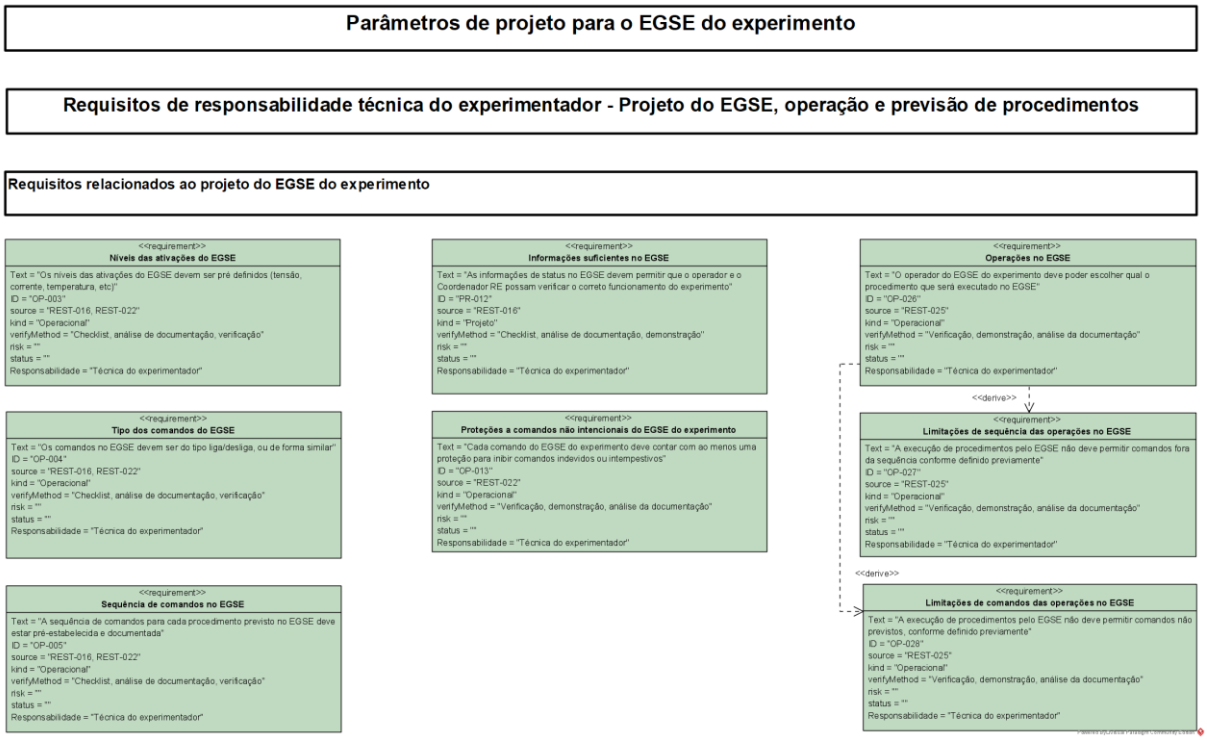


Figura 63 Grupo 8; Parâmetros de projeto e operação para o EGSE do experimento.



Apêndice G

QUESTIONÁRIOS APLICADOS AO CORPO DE ESPECIALISTAS

Nesta parte são apresentados todos os aplicados ao corpo de especialistas.

O cabeçalho de todos os questionários é idêntico, por esta razão será apresentado apenas uma única vez.

Sou aluno de Mestrado Profissional em Inovação Tecnológica pela Universidade Federal de São Paulo e esta PESQUISA fará parte da consolidação dos resultados obtidos com minha pesquisa, voltado para a área de requisitos de segurança aplicados às cargas úteis espaciais de foguetes de sondagem. Os resultados obtidos com sua participação terão impacto positivo nos novos requisitos relacionados à segurança na missão, carga útil, lançamento e dos experimentos nas missões espaciais brasileiras.

O questionário levará aproximadamente 15 minutos, suas respostas são totalmente anônimas. Se você tiver alguma dúvida sobre o questionário, envie-nos um e-mail para: Heuller.procopio@gmail.com. Pode entrar em contato também pelo telefone (12) 3947 4953.
Agradecemos sua colaboração!

Gostaria de saber de sua opinião a respeito dos requisitos declarados no início de cada item deste questionário. Ao final, responda mais algumas questões relativas aos requisitos como um todo.

As definições a seguir são necessárias para responder ao questionário:

EGSE: Electric Ground Support Equipment, ou Equipamento Elétrico de Suporte em Solo. Sistema fornece os serviços necessários aos experimentos durante sua operação em solo, fornecendo dados pela sua interface ao seu operador.
REs: Redes Elétricas. Conjunto de linhas e outros equipamentos ou instalações elétricas, ligados entre si, permitindo o movimento de energia elétrica.

Análise do Grupo de Requisitos 1

Requisito 1: “Os ensaios aplicados aos experimentos devem ser controlados e validados por membros da equipe”.

- ☐ Sempre
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 1 (opcional)

Requisito 2: “O experimento não deve ser liberado para o voo sem ter sido aprovado no ensaio dinâmico de aceitação”.

- ☐ Concordo, obrigatório
- ☐ Concordo, na maioria dos casos
- ☐ Concordo, só em alguns casos
- ☐ Excepcionalmente pode ser liberado
- ☐ Sempre pode ser liberado

Comentário relacionado ao requisito 2 (opcional)

Requisito 3: “O experimento deve ser submetido a um teste funcional, validado por equipe técnica do IAE, antes do seu ensaio dinâmico de aceitação”

- ☐ Submissão obrigatória
- ☐ Submissão na maioria dos casos
- ☐ Submissão apenas em alguns casos
- ☐ Submissão não obrigatória
- ☐ Não precisa ser submetido

Comentário relacionado ao requisito 3 (opcional)

Requisito 4: “O experimento deve ser submetido à verificação dimensional antes do seu EDA ".

- ☐ Submissão obrigatória
- ☐ Submissão na maioria dos casos
- ☐ Submissão apenas em alguns casos
- ☐ Submissão não obrigatória
- ☐ Não precisa ser submetido

Comentário relacionado ao requisito 4 (opcional)

Requisito 5: “O experimento deve ser integrado à carga útil com validação do procedimento de manipulação, ou troca, de amostras”.

- ☐ Validação obrigatória
- ☐ Validação na maioria dos casos
- ☐ Validação apenas em alguns casos
- ☐ Validação não obrigatória
- ☐ Não precisa ser validado

Comentário relacionado ao requisito 5 (opcional)

Requisito 6:” Deve haver redundância na estrutura para os testes dos experimentos”.

- ☐ Concordo, redundância obrigatória
- ☐ Concordo, redundância na maioria dos casos
- ☐ Concordo, mas redundância só em alguns casos
- ☐ Excepcionalmente pode ser executado sem redundância
- ☐ Sempre pode ser executado sem redundância

Comentário relacionado ao requisito 6 (opcional)

Requisito 7: "A equipe de qualidade do IAE deve acompanhar o procedimento de manipulação de amostra para todas as vezes que for executado após sua validação".

- ☐ Sempre
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 7 (opcional)

Requisito 8:" A equipe de qualidade deve informar à gerência responsável pelo lançamento os resultados do procedimento de manipulação de amostra executado".

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 8 (opcional)

Requisito 9: "A equipe gerencial do IAE deve verificar os certificados de calibração dos respectivos equipamentos de suporte".

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 9 (opcional)

Requisito 10: "Os ensaios dinâmicos de aceitação devem ser efetuados com calibração validada de seus equipamentos de suporte (IAE)".

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 10 (opcional)

Requisito 11: "Se o experimento oferece riscos não mitigados ou controlados, a equipe responsável pela gerência do lançamento tem autoridade para não permitir a integração do experimento na carga útil".

- ☐ Autoridade total
- ☐ Autoridade parcial
- ☐ Autoridade em alguns casos
- ☐ Autoridade eventual
- ☐ Não deve ter autoridade

Comentário relacionado ao requisito 11 (opcional)

Requisito 12: "Deve haver controle das etapas do ciclo de vida da carga útil por parte das equipes gerenciais responsáveis pela missão de lançamento".

- ☐ Controle total
- ☐ Controle parcial
- ☐ Controle em alguns casos
- ☐ Controle eventual
- ☐ Não deve ter controle

Comentário relacionado ao requisito 12 (opcional)

Requisito 13: "Os sensores de realimentação do shaker devem ter sua instalação e operação de forma a fornecer informações confiáveis ao sistema de controle do equipamento"

- ☐ Concordo, alta confiança conforme definição do especialista responsável pela missão
- ☐ Concordo, confiável na maioria dos casos
- ☐ Concordo, mas podem ser confiáveis só em alguns casos
- ☐ Excepcionalmente podem ser usados sem confiança
- ☐ Sempre podem ser usados sem confiança

Comentário relacionado ao requisito 13 (opcional)

Requisito 14: "Todos as verificações relativas aos procedimentos dos experimentos devem ser estabelecidas antes do seu desenvolvimento".

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 14 (opcional)

Questão 1) No ponto de vista de segurança da missão e carga útil. O conjunto de requisitos apresentados (requisitos 1 a 14) abordam em grande parte as questões relacionadas às atribuições gerenciais do IAE e o controle que deve exercer na validação dos experimentos?

- ☐ Concordo totalmente
- ☐ Concordo em grande parte
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte
- ☐ Discordo

Comentário relacionado à questão 1 (opcional)

Questão 2) O conjunto de requisitos apresentados (requisitos 1 a 14) é completo e consistente?

- ☐ Concordo totalmente
- ☐ Concordo em grande parte
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte
- ☐ Discordo

Comentário relacionado à questão 2 (opcional)

Análise do Grupo de Requisitos 2

Requisito 1: “Todas as informações relativas aos testes, ensaios e procedimentos dos experimentos devem ser disponibilizadas aos experimentadores antes da fase de desenvolvimento”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 1 (opcional)

Requisito 2: “As informações relacionadas à degradação das amostras dos experimentos, quando aplicável, devem ser utilizadas para o planejamento das atividades para a campanha de lançamento”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 2 (opcional)

Requisito 3: “O cronograma de apronto da missão deve ser disponibilizado a todas as partes interessadas sempre que sofrer alterações”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 3 (opcional)

Requisito 4: “Deve ser enviada uma lista das possíveis situações não nominais passíveis de ocorrência durante a missão aos experimentadores antes do desenvolvimento do experimento".

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 4 (opcional)

Requisito 5: “A documentação de projeto do experimento deve ser fornecida à gerência responsável pela carga útil”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 5 (opcional)

Requisito 6:” As informações a respeito do tempo de execução do procedimento de manipulação das amostras devem constar na documentação detalhada do experimento”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 6 (opcional)

Requisito 7: "Todas as operações previstas para o EGSE do experimento devem ser documentadas”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 7 (opcional)

Requisito 8: "A documentação de projeto do experimento deve conter contemplar as informações a respeito da degradação das amostras que serão utilizadas ".

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 8 (opcional)

Questão 1) O conjunto de requisitos apresentados (requisitos 1 a 8) aborda suficientemente quais são as informações que deve transitar entre as partes interessadas?

- ☐ Concordo totalmente
- ☐ Concordo em grande parte
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte
- ☐ Discordo

Comentário relacionado à questão 1 (opcional)

Questão 2) O conjunto de requisitos apresentados (requisitos 1 a 8) trata devidamente do fluxo de informações entre as partes interessadas?

- ☐ Concordo totalmente
- ☐ Concordo em grande parte
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte
- ☐ Discordo

Comentário relacionado à questão 2 (opcional)

Questão 3) O conjunto de requisitos apresentados (requisitos 1 a 8) é completo e consistente?

- ☐ Concordo totalmente
- ☐ Concordo em grande parte
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte
- ☐ Discordo

Comentário relacionado à questão 3 (opcional)

Análise do Grupo de Requisitos 3

Requisito 1: “O operador do EGSE do experimento deve receber treinamento de pelo menos 8h pelo experimentador”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 1 (opcional)

Requisito2: “Devem ser treinados ao menos 2 operadores para o EGSE do experimento”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 2 (opcional)

Requisito 3: “O operador deve ser treinado em todas as operações previstas para o experimento”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 3 (opcional)

Requisito 4: “Os operadores do EGSE do experimento devem participar do EDA.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 4 (opcional)

Requisito 5: “Não deve haver a substituição dos operadores do EGSE entre o EDA e a operação de lançamento”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 5 (opcional)

Requisito 6: “Os operadores do EGSE do experimento, sempre que estiverem operando o EGSE, devem estar de posse da documentação das operações previstas para o EGSE”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 6 (opcional)

Questão 1) No ponto de vista de segurança da missão e carga útil. Os requisitos (requisitos 1 a 6) abordam em grande parte as questões de treinamento e restrições para os operadores do EGSE?

- ☐ Concordo totalmente
- ☐ Concordo em grande parte
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte
- ☐ Discordo

Comentário relacionado à questão 1 (opcional)

Questão 2) No ponto de vista de segurança do operador do EGSE e experimento. Os requisitos (requisitos 1 a 6) não restringem a operação do experimento a ponto de inviabilizar a execução da experiência?

- ☐ Concordo totalmente
- ☐ Concordo em grande parte
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte
- ☐ Discordo

Comentário relacionado à questão 2 (opcional)

Questão 3) O conjunto de requisitos apresentados (requisitos 1 a 8) é completo e consistente?

- ☐ Concordo totalmente
- ☐ Concordo em grande parte
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte
- ☐ Discordo

Comentário relacionado à questão 3 (opcional)

Análise do Grupo de Requisitos 4

Requisito 1: “Devem ser atribuídas 5 indicações de autorização para informar ao operador do experimento em solo o modo de operação em que o experimento deve ser levado: Desligado; Em preparo para teste; Teste; Em preparo para voo; Voo”.

- ☐ Concordo totalmente
- ☐ Concordo em grande parte
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte
- ☐ Discordo

Comentário relacionado ao requisito 1 (opcional)

Requisito 2: “A indicação da autorização designada “Desligado” deve ser da cor vermelha, e indicar quando o operador do EGSE do experimento deve desligar completamente o experimento e mantê-lo dessa forma”.

- ☐ Concordo totalmente, indicação clara e inequívoca
- ☐ Concordo em grande parte, parcialmente clara e inequívoca
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte, declaração equivocada
- ☐ Discordo, declaração equivocada

Comentário relacionado ao requisito 2 (opcional)

Requisito 3: “A indicação da autorização designada “Em preparo para teste” deve ser da cor amarela, e indicar quando o operador do EGSE do experimento deve prepará-lo para teste”.

- ☐ Concordo totalmente, indicação clara e inequívoca
- ☐ Concordo em grande parte, parcialmente clara e inequívoca
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte, declaração equivocada
- ☐ Discordo, declaração equivocada

Comentário relacionado ao requisito 3 (opcional)

Requisito 4: “A indicação da autorização designada “Teste” deve ser da cor laranja, e indicar quando o operador do EGSE do experimento deve iniciar o teste”.

- ☐ Concordo totalmente, indicação clara e inequívoca
- ☐ Concordo em grande parte, parcialmente clara e inequívoca
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte, declaração equivocada
- ☐ Discordo, declaração equivocada

Comentário relacionado ao requisito 4 (opcional)

Requisito 5: “A indicação da autorização designada “Em preparo para voo” deve ser da cor azul, e indicar quando o operador do EGSE do experimento deve preparar o experimento para o voo”.

- ☐ Concordo totalmente, indicação clara e inequívoca
- ☐ Concordo em grande parte, parcialmente clara e inequívoca
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte, declaração equivocada
- ☐ Discordo, declaração equivocada

Comentário relacionado ao requisito 5 (opcional)

Requisito 6: “A indicação da autorização designada “Voo” deve ser da cor verde, e indicar quando o operador do EGSE do experimento deve finalizar a preparação do experimento para o voo”.

- ☐ Concordo totalmente, indicação clara e inequívoca
- ☐ Concordo em grande parte, parcialmente clara e inequívoca
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte, declaração equivocada
- ☐ Discordo, declaração equivocada

Comentário relacionado ao requisito 6 (opcional)

Requisito 7: “O coordenador das REs deve ter a capacidade de bloqueio à ativação de todos os experimentos simultaneamente”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 7 (opcional)

Requisito 8: “Devem ser enviadas 5 indicações de estados do operador em solo do experimento para o coordenador das REs: Desligado; Em preparo para testes; Testes; Em preparo para voo; Voo”.

- ☐ Concordo totalmente, indicação clara e inequívoca
- ☐ Concordo em grande parte, parcialmente clara e inequívoca
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte, declaração equivocada
- ☐ Discordo, declaração equivocada

Comentário relacionado ao requisito 8 (opcional)

Requisito 9: “A indicação designada “Desligado” deve ser da cor vermelha, e indicar quando o experimento está completamente desligado”.

- ☐ Concordo totalmente, indicação clara e inequívoca
- ☐ Concordo em grande parte, parcialmente clara e inequívoca
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte, declaração equivocada
- ☐ Discordo, declaração equivocada

Comentário relacionado ao requisito 9 (opcional)

Requisito 10: “A indicação designada “Em preparo para teste” deve ser da cor amarela, e indicar quando o operador do EGSE do experimento está preparando o experimento para testes”.

- ☐ Concordo totalmente, indicação clara e inequívoca
- ☐ Concordo em grande parte, parcialmente clara e inequívoca
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte, declaração equivocada
- ☐ Discordo, declaração equivocada

Comentário relacionado ao requisito 10 (opcional)

Requisito 11: “A indicação designada “Teste” deve ser da cor laranja, e indicar quando o experimento está em teste”.

- ☐ Concordo totalmente, indicação clara e inequívoca
- ☐ Concordo em grande parte, parcialmente clara e inequívoca
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte, declaração equivocada
- ☐ Discordo, declaração equivocada

Comentário relacionado ao requisito 11 (opcional)

Requisito 12: “A indicação designada “Em preparo para voo” deve ser da cor azul, e indicar quando o operador do EGSE do experimento está preparando o experimento para o voo”.

- ☐ Concordo totalmente, indicação clara e inequívoca
- ☐ Concordo em grande parte, parcialmente clara e inequívoca
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte, declaração equivocada
- ☐ Discordo, declaração equivocada

Comentário relacionado ao requisito 12 (opcional)

Requisito 13: “A indicação designada “Voo” deve ser da cor verde, e indicar quando o experimento está pronto para o voo”.

- ☐ Concordo totalmente, indicação clara e inequívoca
- ☐ Concordo em grande parte, parcialmente clara e inequívoca
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte, declaração equivocada
- ☐ Discordo, declaração equivocada

Comentário relacionado ao requisito 13 (opcional)

Requisito 14: “O operador do EGSE do experimento deve informar a estimativa da degradação das amostras sempre quando solicitado pelos controladores de missão”.

- ☐ Concordo totalmente, indicação clara e inequívoca
- ☐ Concordo em grande parte, parcialmente clara e inequívoca
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte, declaração equivocada
- ☐ Discordo, declaração equivocada

Comentário relacionado ao requisito 14 (opcional)

Questão 1) Os requisitos (requisitos 1 a 6, e 8 a 13) apresentam indicações claras e suficientes de autorizações e de estado de operação do experimento?

- ☐ Concordo totalmente
- ☐ Concordo em grande parte
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte
- ☐ Discordo

Comentário relacionado à questão 1 (opcional)

Questão 2) O conjunto de requisitos apresentados (requisitos 1 a 14) é completo e consistente?

- ☐ Concordo totalmente
- ☐ Concordo em grande parte
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte
- ☐ Discordo

Comentário relacionado à questão 2 (opcional)

Questão 3) A implementação do conjunto de requisitos apresentados (requisitos 1 a 14) é viável?

- ☐ Concordo totalmente
- ☐ Concordo em grande parte
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte
- ☐ Discordo

Comentário relacionado à questão 3 (opcional)

Análise do Grupo de Requisitos 5

Requisito 1: “Durante a campanha de lançamento, os experimentos com amostras sensíveis não devem sofrer o procedimento de apronto para voo antecipadamente ao previsto pelo cronograma”.

- ☐ Concordo para todos os casos
- ☐ Concordo na maioria dos casos
- ☐ Concordo em casos excepcionais
- ☐ Indiferente
- ☐ Não concordo

Comentário relacionado à questão 1 (opcional)

Requisito 2: “A validação do procedimento de manipulação de amostras deve levar em conta as instalações e facilidades do campo de lançamento”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 2 (opcional)

Requisito 3: “A validação do procedimento de manipulação de amostras deve ser efetuada por equipe com conhecimento no campo de lançamento e no processo de aceitação de experimentos”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 3 (opcional)

Requisito 4: “O procedimento de manipulação de amostras deve ser acompanhado pela equipe responsável por esta validação durante os testes de desenvolvimento ".

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 4 (opcional)

Requisito 5: “A contenção de amostra deve ser inspecionada após submissão ao EDA”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 5 (opcional)

Requisito 6: “O experimento deve ser preparado pelo experimentador para ensaio dinâmico de aceitação conforme procedimento de manipulação de amostras validado”.

- ☐ Sempre
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 7 (opcional)

Requisito 7: “O experimento deve ser preparado para o ensaio dinâmico de aceitação com os mesmos tipos de materiais previstos para o voo”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 7 (opcional)

Questão 1) No ponto de vista de segurança da missão e carga útil. Os requisitos (requisitos 1 a 7) abordam em grande parte o tratamento das amostras dos experimentos de forma a mitigar os riscos delas para a carga útil?

- ☐ Concordo totalmente
- ☐ Concordo em grande parte
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte
- ☐ Discordo

Comentário relacionado à questão 1 (opcional)

Questão 2) No ponto de vista de viabilidade do experimento. Os requisitos (requisitos 1 a 7) não restringem o projeto e a operação do experimento a ponto de inviabilizar a execução da experiência?

- ☐ Concordo totalmente
- ☐ Concordo em grande parte
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte
- ☐ Discordo

Comentário relacionado à questão 2 (opcional)

Questão 3) O conjunto de requisitos apresentados (requisitos 1 a 7) é completo e consistente?

- ☐ Concordo totalmente
- ☐ Concordo em grande parte
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte
- ☐ Discordo

Comentário relacionado à questão 3 (opcional)

Análise do Grupo de Requisitos 6

Requisito 1: “O experimento deve apresentar variação inferior a ± 0,5 mm de suas dimensões externas (LxAxC) em relação ao que consta no projeto”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 1 (opcional)

Requisito 2: “O experimento deve apresentar variação inferior a ± 0,2 mm na posição de suas furações de fixação relação ao que consta no projeto”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 2 (opcional)

Requisito 3: “As vedações aplicadas aos recipientes de vedação de gases deve prover estanqueidade de modo que o vazamento seja inferior a 50 ppm de gás/hora”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 3 (opcional)

Requisito 4: “Experimento com amostra liquida não deve apresentar vazamento superior a 0,1% do volume por hora”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 4 (opcional)

Requisito 5: “Experimento com amostra liquida não deve apresentar vazamento superior a 1% do volume após a realização de cada ensaio dinâmico”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 5 (opcional)

Requisito 6: “O experimento, após EDA, não deve apresentar avarias aparentes em suas partes integrantes”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 6 (opcional)

Requisito 7: “O experimento deve sofrer testes funcionais e de desempenho após o ensaio dinâmico de aceitação”

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 7 (opcional)

Requisito 8: “O experimento deve apresentar as mesmas funcionalidades antes e após sofrer o EDA".

- Obrigatoriamente
- Na maioria das vezes
- Em alguns casos
- Excepcionalmente
- Nunca

Comentário relacionado ao requisito 8 (opcional)

Requisito 9: “O experimento deve apresentar funcionamento conforme o previsto através de ensaio funcional durante sua etapa de aceitação".

- Obrigatoriamente
- Na maioria das vezes
- Em alguns casos
- Excepcionalmente
- Nunca

Comentário relacionado ao requisito 9 (opcional)

Requisito 10: “O experimento deve possuir comando que ignore os sinais de µG e LO, quando sofrer ações devido a estes sinais”.

- Obrigatoriamente
- Na maioria das vezes
- Em alguns casos
- Excepcionalmente
- Nunca

Comentário relacionado ao requisito 10 (opcional)

Requisito 11: “O comando para ignorar os sinais de µG e LO deve ser enviado pelo EGSE do experimento”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 11 (opcional)

Requisito 12: “O comando para ignorar os sinais de µG e LO deve conter bloqueio que impeça seu envio ao experimento durante a preparação final para o voo”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 12 (opcional)

Questão 1) No ponto de vista de segurança da missão e carga útil. O grupo de requisitos (requisitos de 1 a 12) aborda em grande parte as características construtivas, de funcionalidade e de verificação de forma a mitigar os riscos oferecidos pelo experimento para a carga útil?

- ☐ Concordo totalmente
- ☐ Concordo em grande parte
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte
- ☐ Discordo

Comentário relacionado à questão 1 (opcional)

Questão 2) No ponto de vista de viabilidade do experimento. O grupo de requisitos (requisitos de 1 a 12) não restringem o projeto e a operação do experimento a ponto de inviabilizar a execução da experiência?

- ☐ Concordo totalmente
- ☐ Concordo em grande parte
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte
- ☐ Discordo

Comentário relacionado à questão 2 (opcional)

Questão 3) O conjunto de requisitos apresentados (requisitos de 1 a 12) é completo e consistente?

- ☐ Concordo totalmente
- ☐ Concordo em grande parte
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte
- ☐ Discordo

Comentário relacionado à questão 3 (opcional)

Análise do Grupo de Requisitos 7

Requisito 1: “O experimento e seu sistema devem ter seus procedimentos operacionais testados na fase de desenvolvimento”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 1 (opcional)

Requisito 2: “O sistema do experimento deve ter sido aprovado em todos os testes de seus procedimentos até o fim da etapa de desenvolvimento”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 2 (opcional)

Requisito 3: “Os procedimentos para a operação do experimento devem ser planejados para as situações de operação esperadas”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 3 (opcional)

Requisito 4: “Os procedimentos para a operação do experimento devem ser planejados prevendo possível adiamento da operação de lançamento”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 4 (opcional)

Requisito 5: “Os procedimentos para a operação do experimento devem ser planejados prevendo possível cancelamento da operação de lançamento”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 5 (opcional)

Questão 1) O conjunto de requisitos (requisitos 1 a 5) trata adequadamente da previsão dos procedimentos para as situações esperadas, bem como de sua verificação?

- ☐ Concordo totalmente
- ☐ Concordo em grande parte
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte
- ☐ Discordo

Comentário relacionado à questão 1 (opcional)

Questão 2) O conjunto de requisitos apresentados (requisitos 1 a 5) é completo e consistente?

- ☐ Concordo totalmente
- ☐ Concordo em grande parte
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte
- ☐ Discordo

Comentário relacionado à questão 2 (opcional)

Análise do Grupo de Requisitos 8

Requisito 1: “Os níveis das ativações do EGSE devem ser pré-definidos (tensão, corrente, temperatura, etc.)”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 1 (opcional)

Requisito 2: “Os comandos no EGSE devem ser do tipo liga/desliga, ou de forma similar”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 2 (opcional)

Requisito 3: “A sequência de comandos para cada procedimento previsto no EGSE deve estar pré-estabelecida e documentada”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 3 (opcional)

Requisito 4: “As informações de status no EGSE devem permitir que o operador e o Coordenador RE possam verificar o correto funcionamento do experimento”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 4 (opcional)

Requisito 5: “Cada comando do EGSE do experimento deve contar com ao menos uma proteção para inibir comandos indevidos ou intempestivos”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 5 (opcional)

Requisito 6: “O operador do EGSE do experimento deve poder escolher qual o procedimento que será executado no EGSE”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 6 (opcional)

Requisito 7: “A execução de procedimentos pelo EGSE não deve permitir comandos fora da sequência conforme definido previamente”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 7 (opcional)

Requisito 8: “A execução de procedimentos pelo EGSE não deve permitir comandos não previstos, conforme definido previamente”.

- ☐ Obrigatoriamente
- ☐ Na maioria das vezes
- ☐ Em alguns casos
- ☐ Excepcionalmente
- ☐ Nunca

Comentário relacionado ao requisito 8 (opcional)

Questão 1) No ponto de vista de segurança da missão e carga útil. O grupo de requisitos (requisitos 1 a 8) aborda em grande parte as características necessárias ao EGSE e que venham a contribuir com a operação segura do experimento, mitigando assim riscos à carga útil?

- ☐ Concordo totalmente
- ☐ Concordo em grande parte
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte
- ☐ Discordo

Comentário relacionado à questão 1 (opcional)

Questão 2) No ponto de vista de viabilidade do experimento. O grupo de requisitos (requisitos 1 a 8) não restringem o projeto do EGSE do experimento a ponto de inviabilizar a execução da experiência?

- ☐ Concordo totalmente
- ☐ Concordo em grande parte
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte
- ☐ Discordo

Comentário relacionado à questão 2 (opcional)

Questão 3) O conjunto de requisitos apresentados (requisitos 1 a 8) é completo e consistente?

- ☐ Concordo totalmente
- ☐ Concordo em grande parte
- ☐ Não concordo nem discordo
- ☐ Discordo em grande parte
- ☐ Discordo

Comentário relacionado à questão 3 (opcional)

Apêndice H

CÁLCULOS DAS AVALIAÇÕES GERAIS DOS QUESTIONÁRIOS

Nesta parte são apresentados todos os cálculos de avaliação geral dos questionários.

Tabela 24 Cálculo da avaliação geral do questionário 1

	Grupo de Especialistas 1				Grupo de Especialistas 2			
Questões	nota 1	nota 2	nota 3	Media	nota 1	nota 2		Media
1	5	4	4	13,00	5	3		8,00
2	5	5	5	15,00	5	5		10,00
3	5	5	5	15,00	5	5		10,00
4	5	5	4	14,00	5	4		9,00
5	5	5	5	15,00	5	5		10,00
6	5	3	2	10,00	5	4		9,00
7	5	5	2	12,00	5	5		10,00
8	5	4	4	13,00	5	5		10,00
9	5	5	3	13,00	5	4		9,00
10	5	4	4	13,00	5	5		10,00
11	5	5	5	15,00	5	5		10,00
12	5	3	3	11,00	5	4		9,00
13	5	5	5	15,00	5	5		10,00
14	5	5	3	13,00	5	5		10,00
q1	5	5	4	14,00	5	4		9,00
q2	5	5	4	14,00	5	4		9,00
peso	2		media	4,48	peso	3	media	4,75
particip	3		%	90%	particip	2	%	95%

Avaliação geral | 92,8% |

Tabela 25 Cálculo da avaliação geral do questionário 2

	Grupo de Especialistas 1				Grupo de Especialistas 2			
Questões	nota 1	nota 2	nota 3	Media	nota 1	nota 2	nota 3	Media
1	5	5	5	15,00	5	5	4	14,00
2	5	5	3	13,00	5	5	5	15,00
3	5	5	5	15,00	5	5	5	15,00
4	5	5	3	13,00	5	5	4	14,00
5	5	5	5	15,00	5	5	2	12,00
6	5	5	4	14,00	5	5	5	15,00
7	5	5	5	15,00	5	5	5	15,00
8	5	5	3	13,00	5	5	5	15,00
q1	5	5	2	12,00	5	5	4	14,00
q2	5	5	2	12,00	5	5	4	14,00
q3	5	5	2	12,00	5	5	4	14,00
peso	2		media	4,52	peso	3	media	4,76
particip	3		%	90%	particip	3	%	95%

Avaliação geral | 93,2% |

Tabela 26 Cálculo da avaliação geral do questionário 3

	Grupo de Especialistas 1				Grupo de Especialistas 2			
Questões	nota 1	nota 2	nota 3	Media	nota 1	nota 2		Media
1	5	5	5	15,00	5	5		10,00
2	5	5	5	15,00	5	2		7,00
3	5	5	5	15,00	5	5		10,00
4	5	3	3	11,00	5	4		9,00
5	5	4	2	11,00	5	1		6,00
6	5	5	5	15,00	5	3		8,00
q1	5	4	4	13,00	5	4		9,00
q2	5	5	4	14,00	5	4		9,00
q3	5	5	4	14,00	5	4		9,00
peso	3		media	4,56	peso	2	media	4,28
particip	3		%	91%	particip	2	%	86%

Avaliação geral | 88,9% |

Tabela 27 Cálculo da avaliação geral do questionário 4

	Grupo de Especialistas 1				Grupo de Especialistas 2			
Questões	nota 1	nota 2	nota 3	Media	nota 1	nota 2		Media
1	5	5	5	15,00	5	4		9,00
2	5	5	4	14,00	5	4		9,00
3	5	5	4	14,00	5	3		8,00
4	5	5	4	14,00	5	3		8,00
5	5	5	5	15,00	5	3		8,00
6	5	5	2	12,00	5	4		9,00
7	5	4	2	11,00	5	5		10,00
8	5	5	5	15,00	5	5		10,00
9	5	5	5	15,00	5	4		9,00
10	5	5	5	15,00	5	3		8,00
11	5	5	5	15,00	5	3		8,00
12	5	5	5	15,00	5	3		8,00
13	5	5	5	15,00	5	4		9,00
14	5	5	3	13,00	5	5		10,00
q1	5	5	4	14,00	5	4		9,00
q2	5	4	4	13,00	5	4		9,00
q3	5	5	4	14,00	5	4		9,00
peso	2		media	4,69	peso	3	media	4,41
participantes	3			94%	participantes	2		88%

Avaliação geral | 90,4% |

Tabela 28 Cálculo da avaliação geral do questionário 5

	Grupo de Especialistas 1				Grupo de Especialistas 2			
Questões	nota 1	nota 2	nota 3	Media	nota 1	nota 2		Media
1	5	5	1	11,00	4	3		7,00
2	5	5	5	15,00	5	5		10,00
3	5	5	4	14,00	5	1		6,00
4	5	5	4	14,00	5	3		8,00
5	5	5	5	15,00	5	4		9,00
6	5	5	5	15,00	5	5		10,00
7	5	5	4	14,00	4	3		7,00
q1	5	5	3	13,00	4	4		8,00
q2	5	3	1	9,00	5	4		9,00
q3	5	4	3	12,00	4	4		8,00
peso	3		media	4,40	peso	2	media	4,10
particip	3		%	88%	particip	2	%	82%

Avaliação geral | 85,6% |

Tabela 29 Cálculo da avaliação geral do questionário 6

	Grupo de Especialistas 1				Grupo de Especialistas 2			
Questões	nota 1	nota 2	nota 3	Media	nota 1	nota 2		Media
1	5	4	4	13,00	5	5		10,00
2	5	5	4	14,00	5	5		10,00
3	4	4	3	11,00	5	4		9,00
4	5	4	4	13,00	5	4		9,00
5	4	4	3	11,00	5	4		9,00
6	5	5	4	14,00	5	4		9,00
7	5	5	4	14,00	5	3		8,00
8	5	4	4	13,00	5	5		10,00
9	5	5	3	13,00	5	4		9,00
10	5	3	3	11,00	3	2		5,00
11	5	4	3	12,00	5	3		8,00
12	5	5	3	13,00	5	5		10,00
q1	4	4	4	12,00	4	4		8,00
q2	5	5	4	14,00	5	5		10,00
q3	4	4	3	11,00	5	4		9,00
peso	3		media	4,20	peso	2	media	4,43
particip	3		%	84%	particip	2	%	89%

Avaliação geral | 85,9% |

Tabela 30 Cálculo da avaliação geral do questionário 7

	Grupo de Especialistas 1				Grupo de Especialistas 2			
Questões	nota 1	nota 2	nota 3	Media	nota 1	nota 2	nota 3	Media
1	5	5	4	14,00	5	5	5	15,00
2	5	4	4	13,00	5	4	1	10,00
3	5	4	4	13,00	5	5	4	14,00
4	5	5	5	15,00	5	5	5	15,00
5	5	5	5	15,00	5	5	4	14,00
q1	5	5	4	14,00	5	4	4	13,00
q2	5	4	3	12,00	4	4	4	12,00
peso	3		media	4,57	peso	2	media	4,43
particip	3		%	91%	particip	3	%	89%

Avaliação geral | 90,3% |

Tabela 31 Cálculo da avaliação geral do questionário 8

	Grupo de Especialistas 1				Grupo de Especialistas 2			
Questões	nota 1	nota 2	nota 3	Media	nota 1	nota 2	nota 3	Media
1	5	5	4	14,00	5	5		10,00
2	5	4	4	13,00	4	4		8,00
3	5	5	5	15,00	5	5		10,00
4	5	4	4	13,00	5	5		10,00
5	5	4	3	12,00	4	4		8,00
6	5	2	2	9,00	4	3		7,00
7	4	3	2	9,00	4	4		8,00
8	5	4	2	11,00	4	4		8,00
q1	4	4	4	12,00	5	4		9,00
q2	4	4	3	11,00	5	4		9,00
q3	4	4	3	11,00	4	4		8,00
peso	3		media	3,94	peso	2	media	4,32
particip	3		%	79%	particip	2	%	86%

Avaliação geral | 81,8% |

Apêndice I

CONSIDERAÇÕES DOS QUESTIONÁRIOS DOS ESPECIALISTAS

Nesta parte são apresentadas todas as considerações do campo opcional dos questionários respondidos pelo corpo de especialistas.

Legenda para as Tabelas 31 a 54.

Quest.: Questionário, identifica em qual questionário foi recebido o comentário.

Req.: Requisito, identificador do requisito ao qual o comentário é relacionado.

Esp.: Grupo de especialistas, podendo ser 1 ou 2.

Comentário: Texto do comentário do especialista.

Discussão: Resposta do autor em relação ao comentário (quando aplicável).

Tabela 32 Considerações relacionadas ao contexto.

Quest.	Req.	Esp.	Consideração
2	MS-001	1	Não consegui imaginar um contexto.
2	GP-010	1	Não consegui imaginar um contexto.
4	FC-002	1	Não consigo imaginar um contexto.
4	Questão 1	1	Requisito 6: "A indicação da autorização designada "Voo" deve ser da cor verde, e indicar quando o operador do EGSE do experimento deve finalizar a preparação do experimento para o voo". Não achei claro quem dá liberação.
4	Questão 1	1	Requisito 6: "A indicação da autorização designada "Voo" deve ser da cor verde, e indicar quando o operador do EGSE do experimento deve finalizar a preparação do experimento para o voo". * Não achei claro.
5	Questão 1	1	Faltam informações técnicas para análise.
5	Questão 2	1	Faltam informações técnicas para análise.
5	Questão 3	1	Faltam informações técnicas para análise.
8	OP-026	1	Desde que o procedimento não interfira no experimento

Tabela 33 Considerações vagas ou imprecisas.

Quest.	Req.	Esp.	Consideração
1	Questão 2	2	Requisitos sempre podem ser melhorados
2	MS-001	2	Requisito parecido com de número 8.
2	AM-001	2	Requisito parecido com de número 2.
2	GP-015	1	Espera-se, sempre, que o experimento voe em situações nominais. Situações adversas possivelmente irão atrapalhar os resultados e, por consequência, o experimento deverá ser realizado novamente. O experimentador não deve ficar preocupado com situações não adversas. Deve se garantir a situação planejada inicialmente.
3	Questão 3	2	As questões relacionadas à segurança poderiam ser melhor exploradas.
3	Questão 3	2	Neste formulário os requisitos apresentados são de 1 a 6. Ao final são levantadas duas questões que abordam definições de abrangência dos requisitos (1 a 6) comentados acima.
4	OP-029	1	É uma necessidade? Se sim, sim. Se não, não. Depende da necessidade.
5	Questão 3	1	Podem haver experimentos que demandem requisitos diferentes dos apresentados.
7	VR-011	2	Esta seria a condição ideal, mas não se for aplicada com este rigor, não haverá voo no Brasil.
7	PR-015	2	As operações de lançamento no Brasil se tornaram tão raras, que incluir este item nos procedimentos seria desestimulante para os experimentadores. Cancelamento da operação, se ocorrida no centro de lançamento, equivale ao retorno de fim de missão.
7	Questão 1	2	Não ficou claro nas perguntas anteriores como serão validados todos os requisitos
8	Questão 3	1	Sempre dá pra melhorar, mas precisa de um começo.

Tabela 34 Considerações em concordância, com o texto da questão, referentes ao questionário 1.

Req.	Esp.	Consideração
GP-001	1	A participação dos autores dos experimentos é sempre importante
GP-001	1	É possível ser controlado e validado por outras pessoas que forem devidamente treinadas
VR-001	1	Sem qualificação, pode haver falhas e comprometer outros experimentos.
VR-002	1	Isto garante a maior segurança na integração do experimento ao veículo lançador.
VR-002	2	Deve se ter certeza do correto funcionamento do experimento antes de submetê-lo a EDA, possibilitando assim perceber os efeitos reais da vibração
VR-003	1	Para poder ser integrado fisicamente ao módulo de experimentos sem problemas.
GP-002	1	Alguns experimentos podem necessitar da realização de troca de amostras, com os devidos procedimentos.
GP-002	2	Todo manuseio deve possuir procedimento validado pois uma carga útil faz parte de um sistema bastante complexo (lançador, veículo, meios de solo, etc.)
LO-001	1	Para não comprometer o andamento dos testes para os demais experimentos.
GP-004	1	Garante a maior segurança geral.
GP-004	2	Situação mandatória
GP-005	2	Manter a equipe gerencial a par de todas as atividades e primordial pois essa equipe é responsável pela “saúde” do sistema
GP-006	2	Para os equipamentos passíveis de calibração
GP-007	1	Os equipamentos de suporte do IAE devem possuir a calibração para garantir a confiabilidade dos resultados dos testes.
GP-007	2	A calibração permite ao usuário conhecer a incerteza dos equipamentos
GP-014	1	Caso contrário pode comprometer a segurança do voo e a realização dos experimentos.
GP-014	2	Se o risco de determinado experimento pôr em risco a “saúde” do sistema a equipe gerencial de lançamento deve ter autonomia para decisão de não o incluir na carga útil
VR-007	2	Somente com precisão nesta informação o ensaio pode ser validado
PR-005	1	Muitas vezes os procedimentos são aperfeiçoados após o desenvolvimento do experimento.
PR-005	2	As regras devem ser estabelecidas antes do início do desenvolvimento, pois elas geram requisitos para eles
Questão 2	1	A participação efetiva de grupos como o IAE é essencial para o sucesso de qualquer missão de microgravidade e/ou espacial neste país! O trabalho feito pela equipe é notável apesar de todas as dificuldades que representa levar adiante um programa espacial no Brasil!

Tabela 35 Considerações em concordância, com o texto da questão, referentes ao questionário 2.

Req.	Esp.	Consideração
PR-004	1	Pois estas informações são importantes para todo o planejamento dos experimentadores e durante a fase de desenvolvimento, é possível pensar em alternativas para contornar possíveis problemas.
PR-004	2	Informações necessárias para definir o contexto técnico ambiental para testes e validação dos experimentos antes do voo real.
PR-004	2	Muitas vezes o aprendizado dos técnicos do IAE em relação ao experimento ocorre ao longo do tempo, o mesmo sendo válido para os experimentadores em relação aos requisitos do IAE e do CLA.
MS-001	1	Pois dependendo do experimento esta informação é importante tanto para o experimentador como para todo o planejamento do que pode ser realizado para ser evitado ou reduzido no planejamento da campanha de lançamento
MS-001	2	Não faz sentido desenvolver um experimento que demanda anos de trabalho, sem que as partes saibam dessa possibilidade.
MS-002	1	Se for um experimento principalmente biológico é de extrema importância. Mas é importante ressaltar que cada experimento tem suas características e peculiaridades. Devemos trabalhar juntos, sendo assim importante sabermos de possíveis alterações.
MS-002	1	É mandatório.
GP-015	1	Pois com isso os experimentadores sabem como será provavelmente o lançamento, e como o foguete se comporta e com essas informações podem melhor planejar seus experimentos.
GP-008	1	Com toda certeza, estas duas equipes trabalham juntas, da mesma maneira que os experimentadores precisam receber informações, também devem repassar todas as suas informações sobre seu experimento. Estas duas partes devem estar casadas.
GP-008	1	Mandatório.
GP-010	1	Sim, é importante que os experimentadores forneçam uma estimativa, pois essas informações podem ser importantes para a campanha de lançamento.
OP-009	1	É uma parte burocrática, mas é uma maneira de termos todas informações de ambos os lados, e é uma segurança tanto para os experimentadores como para todos envolvidos na campanha de lançamento.
OP-009	1	Mandatório, uma vez que o EGSE é responsável por toda a interface com o experimento em solo.
AM-001	1	Informação de extrema valia, assim a campanha de lançamento sabe todas essas informações e se algo modificar já pode avisar o experimentador.
Questão 2	2	A COMUNICAÇÃO é fundamental, mas não se deve tornar esse requisito em um ato meramente burocrático, o que muitas é o caso.

Tabela 36 Considerações em concordância, com o texto da questão, referentes ao questionário 3.

Req.	Esp.	Consideração
OP-006	1	Dessa forma pode auxiliar nas correções quando surgir resultados inesperados.
OP-006	1	Carga horária adequada. 8h pode ser muito para determinado experimento.
OP-007	1	Imprevistos podem ocorrer é aconselhável mais de uma pessoa treinada para operar
OP-007	2	Não deveria ser um requisito, mas uma recomendação. Nem todos os grupos de pesquisa, terão 2 operadores disponíveis para serem treinados.
OP-008	1	É importante conhecer cada operação
OP-008	1	"Se algo pode dar errado, vai dar errado". Com base nessa premissa, tem que estar preparado pra tudo.
OP-008	2	Particularidade de cada experimento, com por exemplo: troca de amostras, deverá definir se necessário operadores especializados e diferenciados em cada tarefas, ou não.
OP-008	2	O operador deve estar preparado para operar o sistema em todas as situações previstas, de ensaio e preparação para voo.
OP-010	1	Eu ainda incluiria que os projetistas do EGSE devem ter um representante presente no EDA, ou até mesmo ser um dos operadores.
OP-011	1	Sempre que realizei o EDA, o EGSE foi utilizado plenamente para verificar online o experimento.
OP-011	2	É indispensável a participação do experimentador ou de um responsável pelo experimento na EDA, não necessariamente, um operador de EGSE específico.
OP-012	1	O ideal é que seja (m) os mesmos. Aprende-se muito durante o EDA. Muitos aperfeiçoamentos são feitos após o EDA (na operação do EGSE, não no experimento).
OP-012	2	Atendidos os requisitos, anteriores de 1 a 4, de treinamento de operadores titular e reserva este requisito será cumprido adequadamente.
OP-010	1	Duvidas e/ou imprevistos podem ocorrer
Questão 1	1	Concordo
Questão 2	1	Concordo
Questão 3	1	Concordo
Questão 3	1	Minha opinião: quem propõe o experimento e o executa (o caso da PAANDA ou do E-MEMS por exemplo) os requisitos devem ser até mais rígidos: quem PROJETOU o EGSE deve estar presente nos testes, nas qualificações, nos ensaios, no lançamento na recuperação dos dados, e tudo mais. Pelo menos UM representante, sendo ideal DOIS. Quando o experimento é operado pelo experimentador, mas o projeto dos sistemas foi feito por terceiros, a documentação é importante, mas o TREINAMENTO e compreensão total da operação é mais importante. Como se treina operação? Operando! Oportunidade para aprender: durante o EDA.

Tabela 37 Considerações em concordância, com o texto da questão, referentes ao questionário 4.

Req.	Esp.	Consideração
OP-014	1	É uma boa forma de detalhar as funcionalidades e modos de operação do experimento ao operador.
OP-015	2	É inequívoca quando se adota a filosofia "Verde = Preparado para voo e Vermelho = Não preparado para voo", o que difere da filosofia "Verde=Seguro e Vermelho=inseguro". E o operador entende as duas filosofias e quando cada uma é aplicada.
OP-019	2	É inequívoca quando se adota a filosofia "Verde = Preparado para voo e Vermelho = Não preparado para voo", o que difere da filosofia "Verde=Seguro e Vermelho=inseguro". E o operador entende as duas filosofias e quando cada uma é aplicada.
OP-029	2	Dado que é o coordenador das REs reúne as informações das Redes Elétricas e a ele cabe a decisão do prosseguimento ou não da cronologia de lançamento concordo totalmente com este requisito.
OP-020	2	Dado que o requisito 1 é valido, acredito que o coordenador das REs deve saber o modo de operação de todos os experimentos em qualquer momento da cronologia, independente de quantos modos houver.
OP-021	2	É inequívoca quando se adota a filosofia "Verde = Preparado para voo e Vermelho = Não preparado para voo", o que difere da filosofia "Verde=Seguro e Vermelho=inseguro". E o operador entende as duas filosofias e quando cada uma é aplicada.
OP-025	2	É inequívoca quando se adota a filosofia "Verde = Preparado para voo e Vermelho = Não preparado para voo", o que difere da filosofia "Verde=Seguro e Vermelho=inseguro". E o operador entende as duas filosofias e quando cada uma é aplicada.
Questão 2	2	Concordo que são completos e consistentes
Questão 3	2	Acredito que sejam viáveis

Tabela 38 Considerações em concordância, com o texto da questão, referentes ao questionário 5.

Req.	Esp.	Consideração
GP-002	1	Cada experimento tem sua característica, assim deve ser apresentado no início do planejamento da missão para todos terem ciência e adequar o melhor momento durante a missão de lançamento.
GP-002	1	Os experimentos com amostras devem ser preservados o melhor possível.
OP-001	1	De extrema importância para o planejamento do experimento, uma coisa é no laboratório e outra coisa é no local, e os experimentadores devem ter o conhecimento do local e das possibilidades, para que possam se adequar das reais situações na campanha de lançamento.
OP-001	1	É importantíssimo considerar o ambiente de operação em todas as fases de projeto, desde a montagem, integração e teste, até a operação.
OP-001	2	Os recursos disponibilizados são requisitos para o desenvolvimento dos procedimentos e de suas verificações
OP-002	2	No mínimo
OP-003	1	É importante ter sempre na equipe um responsável pelo experimento que conheça a manipulação de amostras.
OP-003	2	Isso possibilita um bom entendimento do processo
VR-006	1	Porque no momento da campanha de lançamento, o que conta serão todos os experimentos que estão na carga útil, e um experimento não deve afetar os demais.
VR-006	1	As fases do projeto devem ser acompanhadas por inspeções frequentes do processo.
VR-006	2	Sempre que possível
VR-006	2	É necessário que o experimentador verifique e confirme a integridade de seu experimento após a EDA.
GP-011	1	Pois auxilia o experimentador a testar todas as possibilidades que podem ocorrer, e com isso estes testes auxiliam no sucesso durante a missão de lançamento.
GP-011	1	experimentador é o responsável pelo experimento, e deve acompanhar as fases do projeto.
GP-011	2	Serve inclusive como treinamento
GP-012	1	O teste ajuda a simular a situação, assim os materiais devem ser os mesmos.
Questão 1	2	O risco para o ensaio também é abordado
Questão 2	2	As recomendações, aparentemente, são viáveis

Tabela 39 Considerações em concordância, com o texto da questão, referentes ao questionário 6.

Req.	Esp.	Consideração
VR-004	1	A tolerância proposta é factível, e caso seja maior do que isso, dificulta o processo de integração.
VR-004	2	Projetos mecânicos geralmente contam com tolerância de +- 0,1 mm, de modo que o requisito apresentado não deve ter impacto no custo.
VR-005	1	Importante para a fixação dos experimentos pratos de equipamento, evitando retrabalho nos mesmos (quando possível).
VR-005	2	Projetos mecânicos geralmente contam com tolerância de +- 0,1 mm, de modo que o requisito apresentado não deve ter impacto no custo.
VR-008	1	Para garantir a funcionalidade do mesmo.
PR-016	1	Acho importante para verificações em solo.
PR-016	1	A experiência deve ter modos de operação que irão tratar estes sinais de diferentes formas.
PR-016	2	Entendo que o requisito existe para facilitar os testes, no entanto como depende do tipo de experimento talvez não deva ser mandatório.
PR-017	1	Caso haja um caso de verificação da carga útil durante campanha de lançamento, é importante que o experimento não seja acionado durante alguma verificação.
PR-017	1	O EGSE deve enviar comandos para mudar o estado da experiência. A experiência deve lidar com os sinais de uG e LO de forma automática.
PR-017	2	Quanto o requisito 10 existir, o 11 deve ser mandatório.
PR-018	1	Em se tratando de um EGSE que envia comandos para atuadores e relês, sim. Idealmente a experiência deveria lidar com estes comandos de forma automática, dependendo do seu estado de operação.
PR-018	2	Quanto o requisito 10 existir, o 12 deve ser mandatório.
Questão 2	1	Talvez esses requisitos possam inviabilizar alguns experimentos, mas considero importante para a integridade geral da carga útil e demais experimentos.

Tabela 40 Considerações em concordância, com o texto da questão, referentes ao questionário 7.

Req.	Esp.	Consideração
VR-010	1	Importante para a aceitação do experimento.
VR-010	2	A experiência mostra que a cada execução de procedimento operacional, identificam-se melhorias operacionais a serem realizadas. Outro fato que contribui para a obrigatoriedade deste requisito é o de que os operadores devem estar muito bem treinados quanto aos procedimentos operacionais.
VR-010	2	O procedimento é parte de um conjunto de requisitos. Dessa forma, precisam ser verificados. De que adianta o pesquisador requisitar uma geladeira capaz de atingir a temperatura de - 50 graus Celsius se não há como garantir essa condição no transporte do experimento.
PR-013	1	Também deve ser considerado os procedimentos para algumas situações inesperadas, se for relevante. Cada experiência deve ter a sua própria relação de procedimentos para as situações consideradas pertinentes.
PR-013	1	Na maioria das vezes, mas também deve haver planejamento para situações não nominais
PR-013	2	Sim, para toda situação de operação deve haver um procedimento planejado previamente, pois uma operação de lançamento envolve diversas equipes e diversas situações, há varias condições que podem ocorrer durante toda uma campanha de lançamento e devem ser planejadas previamente de modo a aumentar as chances de sucesso de missão e segurança para as equipes e instalações.
PR-013	2	Remete ao Requisito 1.
PR-013	Req 1	A experiência mostra que a cada execução de procedimento operacional, identificam-se melhorias operacionais a serem realizadas. Outro fato que contribui para a obrigatoriedade deste requisito é o de que os operadores devem estar muito bem treinados quanto aos procedimentos operacionais.
PR-014	2	É bem comum em uma operação de lançamento haver adiamento. Este adiamento pode ocorrer devido à diversos fatos com diferentes probabilidades de ocorrerem: problemas de sistemas, mau-tempo, problemas operacionais, entre outros.
PR-014	2	O adiamento de um voo é previsível em qualquer lugar do mundo.
PR-015	2	Existe a possibilidade de cancelamento da missão e a desmobilização deve ser feita de modo a garantir a segurança de todos os envolvidos e também das instalações.

Tabela 41 Considerações em concordância, com o texto da questão, referentes ao questionário 8.

eq.	Esp.	Consideração
OP-003	1	Sempre que possível
OP-004	1	Evitaria falhas de interpretações
OP-005	1	É fundamental a especificação de um EGSE em um Procedimento de Teste, assim como a suas interfaces e a sequência de operação.
OP-005	1	Haveria necessidade de maior número de simulações para "ajustar/revisar" a sequência ideal de comandos
PR-012	1	Em alguns casos nem todas as informações do funcionamento do experimento são possíveis de colocar em um EGSE. Por exemplo, a decodificação de frames de dados pode dificultar a implementação de um EGSE visual. No entanto todo estimulo em teste deve ser capaz de ter um respostar a ser observada.
PR-012	1	Concordo
OP-013	1	Normalmente são utilizados mecanismos de inibição de comando para proteção contra falhas em sistemas com alto impacto ou alto risco de acidente, como propulsão ou fontes de alimentação (baterias e painel solares).
OP-013	1	Sempre que possível
OP-013	1	vai depender muito do tipo do EGSE. Pode ser que a proteção seja uma trava no botão ou pode ser um código de liberação, mas é necessário sim.
OP-026	1	O objetivo do teste e a metodologia aplicada no processo de Verificação deve ser estabelecida na fase de planejamento do desenvolvimento do projeto. Excepcionalmente o operador pode realimentar o planejamento ou mesmo do procedimento, sem colocar em risco os testes do sistema.
OP-026	1	Desde que o procedimento não interfira no experimento
OP-026	1	Acho importante ter liberdade pra isso sim desde que haja também responsabilidade.
OP-027	1	Somente em casos de correções de falhas não previstas anteriormente
Questão 1	1	No meu ponto de vista, faltaram algumas abordagens nos requisitos, como, (1) Treinamento do Operador, (2) referência as especificações do EGSE, (3) diagramas ou descrições da Configuração do EGSE, (4) Planejamento de revisão do Procedimento.
Questão 1	1	Concordo
Questão 1	1	É um grande esforço. Conheço a rebeldia dos experimentadores.
Questão 2	1	Concordo
Questão 2	1	Imprevistos acontecem. Congelar demais as operações podem inviabilizar alguns experimentos, principalmente os novatos (ou os teimosos).
Questão 3	1	A estrutura do requisito deve atender a missão, e nem sempre é necessário um detalhamento dos requisitos. No entanto é importante que o requisito seja a referência aos objetivos, os métodos de verificação e as métricas de critérios de sucesso.
Questão 3	1	Concordo

Tabela 42 Considerações descartadas referentes aos questionários 1 a 3.

Quest.	Req.	Esp.	Consideração	Discussão
1	GP-005	1	Se for necessário para garantir a segurança geral.	Deve ser feita uma análise pela equipe responsável pela segurança da missão em caso de procedimento não conforme o validado. Necessidade para a segurança da missão.
2	MS-002	2	Ainda que no caso do IAE isso seja utópico, uma vez que os cronogramas jamais são seguidos.	É de conhecimento do autor, mas deve-se trabalhar com a informação oficial
3	OP-011	1	Somente em experimentos que requerem uma atenção especial	Isto é importante para o treinamento das equipes envolvidas
3	OP-010	2	É recomendável que o experimentador acompanhe o funcionamento de seu experimento e tenha suas anotações a respeito, mas não poderia ser obrigatório.	Obrigatório. É necessária a posse da documentação para caso de necessidade de procedimento em situação não nominal

Tabela 43 Considerações descartadas referentes ao questionário 4.

Req.	Esp.	Consideração	Discussão
OP-014	2	Entendo que "Desligado", "Teste" e "Voo" são essenciais, porém não vejo prejuízo à segurança da missão haver mais dois modos de operação: "Em preparo para teste" e "em preparo para voo".	Necessários para experimentos com processo mais lento de preparação para testes e preparação para voo. Processos mais lentos pode ser entendido como superiores a 5 minutos.
OP-016, OP-017, OP-018, OP-022, OP-023, OP-024	2	Acredito que quanto mais simples melhor, muitos códigos de cores durante a cronologia final podem levar à confusão. Porém se houver algum motivo no qual esta indicação leva a uma maior segurança para a missão não acho errado que se mantenha este requisito.	Necessários para experimentos com processo mais lento de preparação para testes e preparação para voo. Processos mais lentos pode ser entendido como superiores a 5 minutos.
OP-015	1	Há casos em que a experiência não pode ser desligada.	Caso excepcional. Via de regra todos os experimentos devem ser desligados para acesso das equipes ao foguete
OP-019	1	O voo não pode ser iniciado sem que o experimento esteja preparado. Quem dá o Verde, na sequência, é o experimento. Depois, pode-se alterar para o status Voo.	O "pronto para voo" é descrito em OP-024
OP-029	1	Quanto mais pessoas tem essa capacidade, maior a chance de erro. O coordenador deve ter ciência do estado das experiências, mas não a capacidade de mudar seus respectivos estados. O papel dele é coordenar e não operar, o que deve ser delegado exclusivamente ao pesquisador.	Várias razões para esta implementação. A principal é garantir a segurança das equipes durante o acesso ao foguete.

Tabela 44 Considerações descartadas referentes aos questionários 5 a 7.

Quest.	Req.	Esp.	Consideração	Discussão
5	OP-002	1	Nem sempre é necessária uma experiência prévia do campo de lançamento para operar um sistema, pode-se ter um treinamento simulado. Porém o operador deve necessariamente conhecer previamente o sistema em teste e seu processo de aceitação de experimentos.	A equipe de análise é do IAE, não do experimentador
6	VR-005	1	Dependendo do dispositivo de fixação, uma variação um pouco maior pode não comprometer severamente o posicionamento do experimento.	Comentário válido, porém, uma regra geral deve ser abordada nesse assunto
6	FS-001	1	Caso a avaria não comprometa o funcionamento ou outra parte qualquer do módulo, não necessariamente o experimento precisa ser reprovado no ensaio.	Comentário válido, porém, uma regra geral deve ser abordada nesse assunto
6	VR-009	1	Talvez possa ocorrer variações, principalmente em experimentos com amostras líquidas.	Funcionalidade deve ser a mesma, o funcionamento pode variar.
7	VR-011	1	Talvez a reprovação em alguma etapa possa ser aceita, desde que seja realizada uma análise do risco que isso possa representar para a carga útil e demais experimentos, e esse risco possa ser mitigado.	Comentário válido, porém uma regra geral deve ser abordada nesse assunto
7	VR-011	2	Durante o desenvolvimento, são encontradas diversas falhas de procedimento e do sistema. "O sistema do experimento deve ter sido aprovado nos testes de verificação e validação", nos testes de desenvolvimento é natural que sejam encontradas falhas do sistema e falhas de processos operacionais.	A aprovação de todos os procedimentos é um dos indicadores do fim do desenvolvimento
7	Questão 1	2	Concordo com a ressalva do que foi já descrito como comentário no requisito 2.	A aprovação de todos os procedimentos é um dos indicadores do fim do desenvolvimento

Tabela 45 Considerações descartadas referentes ao questionário 8.

Req.	Esp.	Consideração	Discussão
OP-003	1	Acho importante uma padronização, mas antes é necessária uma prospecção com os experimentadores. Exemplo: mudar de 12 para 5V ou de 5V para 3.3V é fácil, mas, se o experimentador possui um sistema de aquecimento ou refrigeração e precisa de 48 V ou 127 VAC complica.	Há níveis pré-estabelecidos para as interfaces com a plataforma. Os demais são definidos pelo experimentador, mas devem ser definidos!
OP-027	1	Esta restrição de operação não necessários mais em casos de sistemas críticos.	Os experimentos são definidos como parte de um sistema crítico

Tabela 46 Considerações referentes a melhorias na documentação.

Req.	Esp.	Comentário	Discussão
GP-008	2	O responsável pela carga-útil deve receber requisitos básicos/excepcionais das cargas. Muita informação mais atrapalha do que ajuda. Por exemplo: experimento necessita de refrigeração (o gerente precisa saber SEMPRE); o experimento deve ser devolvido ao experimentador tão logo seja recuperado (o gerente precisa saber sempre); O experimento possui duas baterias (essa informação é irrelevante para o gerente).	Alteração na documentação.
GP-010	2	Além disso, a equipe de recuperação da carga-útil precisa ser informada desses procedimentos.	Nova distribuição de documentação
Questão 1	2	Eu creio que o processo de seleção dos experimentos já deveria contemplar alguns desses requisitos. Muitas vezes os experimentadores candidatam-se aos recursos para realização dos experimentos, sem que tenham conhecimento detalhado de como se dá o processo inteiro.	Alteração na documentação.
Questão 2	1	Há uma pequena lista de itens das relações entre experimentadores e stakeholders. Ainda há muito o que ser inserido. Deve-se criar uma situação de contexto para cada momento do ciclo de vida (experimento em solo, experimento em desenvolvimento, experimento em integração, experimento em voo, experimento pós voo), analisar os stakeholders e suas atribuições.	Alteração na documentação.
Questão 3	2	Maior aprofundamento dos requisitos. Deve ser tratado oportunamente no detalhamento das discussões das informações solicitadas e apresentadas nos documentos.	Nova documentação

Tabela 47 Considerações que foram tratadas na dissertação.

Quest	Req.	Esp	Consideração	Discussão
1	MS-003	2	Gostaria de uma melhor definição de “controle” neste caso	Incluir definição no texto.
1	Questão 1	2	Incluem também atribuição dos experimentadores e das equipes envolvidas nos ensaios e lançamentos. Em sistemas complexos as fronteiras das atribuições nem sempre são passíveis de serem binariamente determinadas	O principal responsável é identificado no requisito, e nos diagramas de responsabilidade. Deixar esta informação clara.
3	OP-012	2	Esse não deveria ser um requisito. O operador pode ser substituído a qualquer momento, desde que por alguém em condições de operar o experimento. Esse requisito poderia inviabilizar um experimento, o que seria prejudicial ao programa.	Alteração deste requisito para Recomendação
3	Questão 2	2	Verificar principalmente, o comentário do requisito 5.	Alteração deste requisito para Recomendação
3	Questão 2	req 5	Esse não deveria ser um requisito. O operador pode ser substituído a qualquer momento, desde que por alguém em condições de operar o experimento. Esse requisito poderia inviabilizar um experimento, o que seria prejudicial ao programa.	Alteração deste requisito para Recomendação

Tabela 48 Considerações de melhorias relacionadas ao questionário 1.

Req.	Esp.	Consideração	Discussão
GP-001	2	Cada item a ser ensaiado tem características peculiares e o procedimento para ensaio deve ser avaliado individualmente	Complementa o requisito.
VR-001	2	Levando em consideração que uma versão do experimento tenha passado por ensaio de qualificação e, portanto, não poderá voar	Ensaios de qualificação não são aplicados em experimentos. Há uma discussão para passar a aplicar dessa forma.
VR-003	2	Alguma verificação dimensional deve ser feita, porém não necessariamente de todo o experimento (pode ser feita apenas nos pontos mais relevantes) e as tolerâncias devem ser devidamente dimensionadas para evitar *waivers* excessivas	Complementa o requisito.
LO-001	2	Desde de que seja viável economicamente	Complementa o requisito.
GP-006	1	Se for necessário para garantir a segurança geral. Cada experimento, a princípio, deve ter a calibração dos seus equipamentos de suporte, além da realização dos testes preliminares.	Concordância. Este requisito é relacionado aos equipamentos do IAE. No caso do experimento se trata de uma recomendação
MS-003	1	Em caso de adiamentos de longa espera (meses), as cargas das baterias devem ser monitoradas, de preferência, pelos próprios responsáveis pelo experimento. Se for necessário, a equipe gerencial pode realizar este controle. Para os casos envolvendo materiais perecíveis ou degradáveis, principalmente se forem sensíveis a variação das condições ambientais (tempo, temperatura, umidade, pressão), há necessidade de uma monitoração mais rigorosa.	Complementa o requisito.

Tabela 49 Considerações de melhorias relacionadas ao questionário 2.

Req.	Esp.	Consideração	Discussão
PR-004	1	Os experimentadores precisam apenas do envelope de voo (cargas longitudinais e laterais, níveis de vibração, etc.). O restante, deve ser repassado por meio de um documento de controle de interfaces, para se ter compatibilidade com o sistema. Disponibilizando esses dados, documentos e lista de testes, o experimentador poderá desenvolver seu experimento de forma a estar compatível com a plataforma.	Direciona uma possível implementação
GP-015	2	Este requisito/pergunta é bastante vago. Não está claro que são situações não nominais.	Estas situações devem ser enviadas em momento oportuno
Questão 1	1	Há uma pequena lista de itens das relações entre experimentadores e stakeholders. Ainda há muito o que ser inserido. Deve-se criar uma situação de contexto para cada momento do ciclo de vida (experimento em solo, experimento em desenvolvimento, experimento em integração, experimento em voo, experimento pós-voo), analisar os stakeholders e suas atribuições.	Complementa proposta dos requisitos

Tabela 50 Considerações de melhorias relacionadas ao questionário 3.

Req.	Esp.	Comentário	Discussão
OP-006	2	O tempo definido de 8 horas como mínimo dependerá da complexidade do procedimento.	Complementa o requisito.
OP-006	2	Em geral, o operador do EGSE é o próprio experimentador ou alguém do seu grupo de trabalho, portanto familiarizado com o experimento, portanto, esse requisito só se aplicaria em casos específicos. Além disso, na minha opinião, o tempo mínimo de treinamento dependente da complexidade do EGSE e do experimento como um todo.	O requisito é aplicável da mesma forma. Em relação ao tempo é um comentário complementar
OP-012	1	Somente deve haver caso o substituto passou por os treinamentos.	Complementa o requisito.
OP-012	1	Mas há de ser realizado novo treinamento.	Complementa o requisito.
Questão 1	2	Aparentemente, as questões abordam pouco os requisitos relacionados à "segurança", principalmente, se levarmos em consideração experimentos de alto risco.	Complementa proposta dos requisitos

Tabela 51 Considerações de melhorias relacionadas ao questionário 4.

Req.	Esp.	Consideração	Discussão
Questão 1	2	Indicam modos de operação e não estado do experimento, talvez possa haver, a depender do experimento estados de operação que não são dependentes do modo de operação. A exemplo da degradação da amostra.	Complementa o requisito.
Questão 2	2	Os requisitos devem ser mais claros em relação à maneira como as indicações serão disponibilizadas para o responsável pelas redes elétricas.	Complementa o requisito.
Questão 3	2	Acredito que a implementação seja possível, mas para definir a complexidade entendo ser necessário definir como ocorrerá a comunicação entre os EGSEs dos experimentos e o Responsável pelas redes elétricas	Complementa o requisito.

Tabela 52 Considerações de melhorias relacionadas ao questionário 5.

Req.	Esp.	Consideração	Discussão
GP-002	2	Sempre deve ser feita uma análise individual	Comentário válido, porém, uma regra geral deve ser abordada nesse assunto
GP-002	2	Casos como esse devem ser tratados de forma excepcional e em conjunto com a coordenação do Veículo.	Complementa o requisito. Porém uma regra geral deve ser abordada nesse assunto
OP-001	2	Além da necessidade de estarem descritos em detalhes no DOC 200, os procedimentos para manipulação e resgate dos experimentos devem ser discutidos com o os demais envolvidos.	Complementa o requisito. Porém uma regra geral deve ser abordada nesse assunto
OP-002	2	Existe um Coordenador de Experimentos responsável por essa análise, cabe a ele, portanto, a decisão quanto a necessidade de instituir um grupo ou equipe para análise.	Comentário válido, porém, uma regra geral deve ser abordada nesse assunto
OP-003	2	Cabe ao Coordenador de Experimentos a decisão quanto a esse acompanhamento.	Comentário válido, porém, uma regra geral deve ser abordada nesse assunto
GP-011	2	Todos os procedimentos devem ser descritos e avaliados pelo Coordenador de Experimentos.	Complementa o requisito.
GP-012	1	Em muitos casos pode-se utilizar Dummies que representam fisicamente ou simulem o experimento sem influenciar os resultados dos testes.	Comentário válido, porém, uma regra geral deve ser abordada nesse assunto
GP-012	2	Exceto quando o risco exceda o aceitável para o local da EDA	Complementa o requisito.
GP-012	2	Podem ser utilizados materiais compatíveis, mas não necessariamente idênticos ao de voo.	Complementa o requisito.
Questão 1	2	Experimentos que degradam precisam de tratamento especial e serem tratados caso a caso.	Complementa o requisito.
Questão 2	2	Deve se ter sempre a possibilidade de avaliação dos casos não previstos através de RID	Complementa o requisito.
Questão 3	2	Os requisitos devem direcionar o processo/produto, mas uma abertura para avaliação deve sempre existir	Complementa o requisito.
Questão 3	2	Deveriam ser vistos como recomendações e não requisitos, uma vez que cada experimento, pode necessitar de uma abordagem específica.	Complementa o requisito.

Tabela 53 Considerações de melhorias relacionadas ao questionário 6.

Req.	Esp.	Consideração	Discussão
VR-004	1	Essa não é uma tolerância apertada para uma fabricação mecânica, mas entendo que alguns experimentos possam apresentar algumas variações construtivas, ainda mais para experimentos tenho alguma transformação observada durante ambiente de microG.	Complementa o requisito.
PR-001	1	Acho que isso depende do tipo de gás e do tempo na qual o gás ficará vazando dentro do veículo.	Complementa o requisito.
PR-001	2	Atentar para o método de verificação do requisito: se teste, quanto à disponibilidade e custos. O requisito deve valer para todos os tipos de gases?	Complementa o requisito.
PR-002	1	De novo, acredito que isso dependa do tipo de líquido e onde a experiência foi alocada. Dependendo do local vazamento algum é aceitável.	Complementa o requisito.
PR-003	1	Entendo que vazamentos maiores do que o volume propostos podem danificar experimentos de um mesmo módulo, ou até comprometer a cablagem. No entanto, se o volume total for muito pequeno, 1% pode ser irrelevante, e um vazamento superior a este poderia ser aceitável.	Complementa o requisito.
PR-003	1	De novo, acredito que isso dependa do tipo de líquido e onde a experiência foi alocada. Dependendo do local vazamento algum é aceitável.	Complementa o requisito.
Questão 1	1	Talvez possam ser observados alguns requisitos referentes a parte elétrica dos experimentos, como proteção de curto circuitos, por exemplo. A carga útil também precisa estar preparada para alguma ocorrência nesse sentido. Os ensaios funcionais têm uma função importante para tentar evitar esse tipo de situação.	Complementa o requisito.
Questão 1	1	Acredito que estes 12 requisitos são ainda um conjunto pequeno para classificar como "grande parte". Conectores, comunicação, cablagem, materiais permitidos, proteções para baterias, carga e descarga de bateria, alimentação do experimento via casamata, são alguns dos tópicos importantes que não foram cobertos nos 12 requisitos	Complementa proposta dos requisitos
Questão 1	2	Quanto à segurança, verifique a possibilidade de incluir requisito para bateria, se houver no experimento.	Complementa proposta dos requisitos
Questão 3	1	Não considero completo, mas são consistentes	Complementa proposta dos requisitos

Tabela 54 Considerações de melhorias relacionadas ao questionário 7.

Req.	Esp.	Consideração	Discussão
PR-013	2	Entendo que situações inesperadas devam ser avaliadas e as possíveis ações listadas, entretanto isto pode ser concluído até o fim dos testes da rede elétrica.	Complementa proposta dos requisitos
Questão 2	1	Este conjunto é muito pequeno para ser considerado "grande parte", mas está consistente	Complementa proposta dos requisitos
Questão 2	2	Sugiro acrescentar a necessidade de haver procedimentos de transporte, se não foi considerado que fazem parte dos procedimentos operacionais. Considero o conjunto de requisitos consistentes.	Complementa proposta dos requisitos

Tabela 55 Considerações de melhorias relacionadas ao questionário 8.

Req.	Esp.	Comentário	Discussão
OP-003	1	Em alguns casos os níveis das ativações de um EGSE podem ser variáveis, no entanto mesmo nestes casos, um nível inicial deve ser pré-definido no Procedimento de Teste.	Complementa o requisito.
OP-004	1	Estímulos de um processo utilizando um EGSE nem sempre são binários, muitas vezes tem informações acompanhando ao estimulo, seja comando digital ou analógico. Além do fato que em alguns casos de teste ou simulações comandos de um EGSE podem vir de malhas de realimentação dos sensores e atuadores, os chamados Testes de "Hardware In the Looping".	Complementa o requisito.
OP-004	1	Acho que faltou uma definição aqui: liga/desliga ou liga/desliga do tipo LATCH? Note que faz toda diferença, principalmente quando tem um cabo que pode ser desconectado, por exemplo.	Complementa o requisito.
PR-012	1	ou "possuir comandos específicos para que o coordenador possa checar o correto funcionamento"	Complementa proposta dos requisitos
OP-026	2	Deverá depender da fase: e.g. se testes em bancada ou já na carga útil.	Complementa o requisito.
OP-027	1	Pode até obrigar, mas não vai dar certo de primeira. As coisas travam, principalmente nos primeiros testes. Se for obrigatório, deve-se pensar em ensaios de preparação.	Complementa proposta dos requisitos
OP-027	2	Pode haver exceção para "debug", no entanto este requisito pode ser mantido e neste caso o experimentador pode (i) fazer um outro programa exclusivo para debug sem travas; ou (ii) adicionar um modo de operação do EGSE que permita executa comandos fora da sequência desde que com autorização.	Complementa proposta dos requisitos
Questão 2	1	Faltam informações técnicas para avaliar.	Complementa proposta dos requisitos

Apêndice J

QUESTIONÁRIOS PARA O ESTUDO DE CASO

Nesta parte são apresentados todos os questionários aplicados no estudo de caso.

Grupo de Requisitos 1

Este é um grupo de requisitos relacionado às competências e controles exercidos pelo IAE. É esperado que os impactos gerados por este grupo de requisitos aos experimentos sejam indiretos, na maior parte dos casos. Solicito uma análise dos impactos, positivos ou negativos, da aplicação destes requisitos.

As perguntas são relacionadas ao conjunto de requisitos: GP-001; VR-001; VR-002; VR-003; GP-002; LO-001; GP-004; GP-005; GP-006; GP-007; GP-014; MS-003; VR-007; e, PR-005.

Perguntas para análise do ponto de vista do experimento:

- Há, neste grupo, requisitos quem provocam prejuízos no desenvolvimento ou viabilidade do experimento?
- Se sim, quais requisitos, quais prejuízos e quais seriam os motivos?
- Com a aplicação deste conjunto de requisitos, haveriam necessidades de alterações de *hardware* ou *software* no experimento?
- Se sim, qual requisito, quais alterações e quais seriam os motivos?
- Devido a este conjunto de requisitos, haveriam alterações de procedimentos aplicados ao experimento?
- Se sim, qual requisito, quais alterações, e quais seriam os motivos?

Grupo de Requisitos 2

Este é um grupo de requisitos relacionado ao fluxo de informações entre o IAE e os experimentadores. Este grupo deve regular em que momento e quais são as informações que devem ser trocadas entre as equipes de experimentadores e do IAE. Solicito uma análise dos impactos, positivos ou negativos, da aplicação destes requisitos.

As perguntas são relacionadas ao conjunto de requisitos: PR-004; MS-001; MS-002; GP-015; GP-008; GP-010; GP-009; OP-010; e, AM-001.

Perguntas para análise do ponto de vista do experimento:

- Há, neste grupo, requisitos quem provocam prejuízos no desenvolvimento ou viabilidade do experimento?
- Se sim, quais requisitos, quais prejuízos e quais seriam os motivos?
- Com a aplicação deste conjunto de requisitos, haveriam necessidades de alterações de *hardware* ou *software* no experimento?
- Se sim, qual requisito, quais alterações e quais seriam os motivos?
- Devido a este conjunto de requisitos, haveriam alterações de procedimentos aplicados ao experimento?
- Se sim, qual requisito, quais alterações e quais seriam os motivos?

Grupo de Requisitos 3

Este é um grupo de requisitos relacionado ao operador do EGSE do experimento. Trata do treinamento e informações necessárias para o operador/equipe. Solicito uma análise dos impactos, positivos ou negativos, da aplicação de cada um dos requisitos. Neste caso a análise deve ser individual para cada requisito.

Requisito OP-007:

Do ponto de vista da equipe do experimento e em relação ao OP-007.

- É possível de atender a este requisito?
- Quais são os impactos para a equipe para que sejam treinados 2 ou mais operadores?

Requisito OP-008:

- Do ponto de vista da equipe do experimento e em relação ao OP-008.
- É factível treinar o operador em todas as operações previstas?
- Há limitações no treinamento do operador?

Requisito OP-009:

Do ponto de vista da equipe do experimento e em relação ao OP-009.

- É possível documentar todas as operações previstas para o EGSE assim do encerramento do desenvolvimento do experimento?
- Qual seria o impacto de gerar esta documentação?

Requisito OP-010:

Do ponto de vista da equipe do experimento e em relação ao OP-010.

- Qual seria o impacto para os operadores estarem de posse da documentação enquanto operam o EGSE?

Requisito OP-011:

Do ponto de vista da equipe do experimento e em relação ao OP-011.

- Quais são os impactos para a equipe se os operadores participarem do EDA em tempo integral do ensaio?

Requisito OP-012:

Do ponto de vista da equipe do experimento e em relação ao OP-012.

- Quais seriam os óbices para que este requisito seja atendido?
- Este requisito poderia inviabilizar a participação do experimento e/ou da sua equipe durante a campanha de lançamento? Qual seria o motivo?

Grupo de Requisitos 4

Este é um grupo de requisitos relacionado a comunicação entre o responsável das REs e o operador do EGSE do Experimento durante o Lançamento. Solicito uma análise dos impactos, viabilidade, da aplicação de requisitos individuais e de conjuntos.

Perguntas para análise do ponto de vista do experimento:

Relacionadas aos requisitos OP-014; OP-015; OP-016; OP-017; OP-018; e, OP-019.

- Estas indicações das autorizações enviadas pelo coordenador das REs são claras o suficiente?
- O número de indicações é adequado?
- É possível dessa forma indicar (em grande parte) ao operador do EGSE do experimento quais são os procedimentos que podem ser executados?
- A implementação física destas indicações pode ser executada no EGSE do experimento, ou é preferível que seja externo a ele?

Relacionadas aos requisitos OP-014; OP-015; OP-016; OP-017; OP-018; e, OP-019.

- Estas indicações do estado do experimento enviadas pelo operador do EGSE do experimento são claras o suficiente?
- O número de indicações é adequado?
- É possível dessa forma indicar (em grande parte) ao coordenador das REs qual é o estado em que o experimento se encontra?
- A implementação física destas indicações pode ser executada no EGSE do experimento, ou é preferível que seja externo a ele?

Perguntas relacionadas ao requisito OP-029.

- O bloqueio da ativação do experimento por parte do coordenador das REs pode danificar ou inviabilizar o experimento?
- É possível sua implementação no experimento ou em seu EGSE?
- Como seria esta implementação?
- Quais seriam seus impactos?

Grupo de Requisitos 5

Este é um grupo de requisitos relacionado às questões relacionadas às amostras do experimento. Trata do preparo de experimento com amostras sensíveis, validação de procedimento de manipulação de amostras, verificações do experimento e preparo do experimento para ensaio. Solicito uma análise dos impactos, positivos ou negativos, da aplicação de cada um dos requisitos. Neste caso a análise deve ser individual para cada requisito.

Requisito GP-009:

OBS: O requisito GP-009 é aplicável apenas a experimento com amostras sensíveis. A amostra é considerada sensível quando degrada com 3 ou menos ativações ou cuja amostra tenha tempo viável inferior a 48h.

Do ponto de vista do experimento em relação ao requisito GP-009.

- Este requisito é aplicável?
- Quais são os impactos para a equipe para que este requisito seja atendido?
- Quais são os impactos para o planejamento de lançamento do experimento para que este requisito seja atendido?
- Este requisito inviabiliza o lançamento do experimento?

Requisito OP-001:

Do ponto de vista do experimento em relação ao requisito OP-001.

- O procedimento de manipulação de amostras pode ser impactado pelas instalações, facilidades e equipamentos do campo de lançamento? Quais impactos?

- Em caso de o campo de lançamentos não prover infraestrutura, nem equipamentos necessários para a manipulação de amostras do experimento, é possível que o experimentador elabore um plano e forneça equipamentos a fim de viabilizar o lançamento do experimento?
- Qual seria o plano e equipamentos para viabilizar o lançamento?

Requisito OP-002:

Do ponto de vista do experimento em relação ao requisito OP-002.

- A validação do procedimento de manipulação de amostras por equipe competente contribui para que o procedimento seja factível e viável no campo de lançamento?
- Quais são os impactos da validação do procedimento de manipulação de amostras para o experimento?
- Quais são os impactos da validação do procedimento de manipulação de amostras para a equipe de experimentadores?

Requisito GP-003:

Do ponto de vista do experimento em relação ao requisito GP-003.

- Quais são os impactos da validação do procedimento de manipulação de amostras para o desenvolvimento do experimento?
- Quais são os impactos da validação do procedimento de manipulação de amostras para o experimento?
- Quais são os impactos da validação do procedimento de manipulação de amostras para a equipe de experimentadores?

Requisito VR-006:

Do ponto de vista do experimento em relação ao requisito VR-006.

- É possível inspecionar a amostra do experimento?
- Qual é o processo para a inspeção da amostra?
- Quais são os impactos no experimento para que este requisito seja atendido?
- Quais são os impactos nos procedimentos relacionados ao experimento para que este requisito seja atendido?

Requisito GP-011:

Do ponto de vista do experimento em relação ao requisito GP-011.

- As amostras sofrem degradação durante a preparação do experimento se executada conforme o procedimento de manipulação de amostras validado?
- A execução do procedimento de manipulação de amostras validado prejudica de alguma forma a integridade do experimento?

Requisito GP-012:

Do ponto de vista do experimento em relação ao requisito GP-012.

- Quais são os riscos que as amostras oferecem ao ambiente de ensaios?
- Há materiais substitutos que representem a amostra de forma fidedigna para a execução do ensaio, sem oferecer riscos ao ambiente de ensaios?
- Qual são os motivos para a degradação das amostras devido ao ensaio?
- Qual são os motivos para a degradação das amostras devido ao armazenamento do experimento após o ensaio?
- Há necessidade de manipulação da amostra após o ensaio de EDA?

Grupo de Requisitos 6

Este é um grupo de requisitos relacionado ao projeto da parte embarcada do experimento. Trata dos parâmetros para a construção física do experimento, parâmetros de verificações e dos sinais recebidos pela carga útil. Solicito uma análise dos impactos, positivos ou negativos e da aplicação de cada um dos requisitos. Neste caso a análise deve ser individualmente e em grupos selecionados conforme indicado.

Requisitos VR-004 e VR-005:

Do ponto de vista do experimento em relação aos requisitos VR-004 e VR-005.

- As tolerâncias das dimensões apresentadas do requisito são possíveis de serem obtidas?
- Para atingir estas tolerâncias, o método designado para a fabricação das partes mecânicas do experimento é adequado?
- Caso seja necessário qual seria o plano para o atendimento deste requisito?

Requisito PR-001:

Do ponto de vista do experimento em relação ao requisito PR-001.

- Este experimento conta com amostra gasosa ou amostra que entre em ebulição durante a missão?
- É possível evidenciar vazamento inferior aos limites que o requisito apresenta através de teste? Se sim, como pode ser efetuado este teste?
- Caso o teste de contenção não seja viável, as informações da documentação permitem através de análise chegar à conclusão que o limite de vazamento é respeitado?
- Os limites do requisito são adequados ao projeto do experimento? Se não, qual seria o limite adequado?
- A amostra oferece riscos à carga útil ou aos ensaios?

Requisitos PR-002 e PR-003:

Do ponto de vista do experimento em relação aos requisitos PR-002 e PR-003.

- Este experimento costa com amostra líquida, ou amostra que se torne líquida durante a missão?
- Como pode ser evidenciado o vazamento das amostras?
- O projeto da contenção da amostra demonstra que atende aos requisitos?
- Os limites do requisito são muito rigorosos para o projeto do experimento? Se não, qual seria o limite adequado?
- A amostra oferece riscos à carga útil, ou aos ensaios?

Requisito FS-001:

Do ponto de vista do experimento em relação ao requisito FS-001.

- O experimento contém partes integrantes que não são visíveis?
- Se sim, qual é o percentual de partes que são passíveis de serem inspecionadas através de inspeção visual?
- É possível evidenciar eventuais avarias em partes integrantes não visíveis?
- Através de inspeções diretas e indiretas, qual é percentual de peças inspecionáveis?

Requisitos VR-008, VR-009 e GP-013:

Do ponto de vista do experimento em relação aos requisitos VR-008, VR-009 e GP-013.

- Os procedimentos de testes funcionais devem ser acompanhados pelo experimentador ou apenas pelo operador do EGSE do experimento?
- A avaliação do desempenho do experimento pode ser executada apenas pelo experimentador ou o operador do EGSE do experimento também possui tal competência?
- Qual é a forma utilizada para a conferência das funcionalidades do experimento?

Requisitos PR-016, PR-017 e PR-018:

Do ponto de vista do experimento em relação aos requisitos PR-016, PR-017 e PR-018.

Durante o EDA, e testes antes do voo a carga útil envia os sinais de µG e LO a todos os experimentos.

- O experimento é suscetível aos sinais de µG e LO?

OBS: entende-se como experimento suscetível aos sinais de µG e LO quando o experimento dispara processos quando do recebimento de pelo menos um destes sinais.

- O conjunto de requisitos define uma proteção ao recebimento dos sinais de µG e LO, tendo isso em vista, como é efetuada sua implementação?
- Quais são os impactos no experimento e seu EGSE para o atendimento deste conjunto de requisitos?

Grupo de Requisitos 7

Este é um grupo de requisitos relacionado aos procedimentos relacionados ao experimento. Trata das verificações dos procedimentos do experimento e da previsão de procedimentos para a campanha de lançamento. Solicito uma análise dos impactos, positivos ou negativos, da aplicação de cada um dos requisitos. Neste caso a análise deve ser individual para cada requisito.

Requisito VR-010:

Do ponto de vista do experimento em relação ao requisito VR-010.

- Quais são os impactos dos testes dos procedimentos operacionais do experimento durante o desenvolvimento?
- Há procedimentos operacionais que não são possíveis de serem testados durante o desenvolvimento?

Requisito VR-010:

Do ponto de vista do experimento em relação ao requisito VR-011.

- Há procedimentos que não são possíveis de serem testados e aprovados até o fim do desenvolvimento?
- Quais são os impactos que o atendimento deste requisito gera para a documentação?
- Testar os procedimentos durante o desenvolvimento pode contribuir com a simplificação, aprimoramento, e melhor domínio dos procedimentos operacionais?

Requisito PR-013:

OBS: Adicionalmente deve ser observado o requisito GP-015: *"Deve ser enviada uma lista das possíveis situações não nominais passíveis de ocorrência durante a missão aos experimentadores antes do desenvolvimento do experimento".*

Lista piloto:

1 - O cronograma de ensaios é postergado em 6 meses após a entrega do experimento. Aceitou o experimento, EDA etc.

2 - Ocorrem diversas (mais de 5) ativações da amostra do experimento durante o EDA.

3 - Necessidade de substituição de amostra no campo de lançamentos.

Do ponto de vista do experimento em relação ao requisito PR-013.

- O planejamento dos procedimentos para as situações esperadas contribui para a documentação dos procedimentos do experimento? Quais são os impactos na documentação?
- O planejamento dos procedimentos para as situações esperadas contribui para o treinamento do operador do EGSE? Quais são os impactos no treinamento?
- Para atender este requisito se faz necessário ampliar a quantidade de procedimentos atualmente definidos? Quais são estes procedimentos?

Requisito PR-014:

Do ponto de vista do experimento em relação ao requisito PR-014.

- Este requisito contribui para a elaboração de um plano de contingência em caso de adiamento do lançamento?
- Este plano de contingência contribui com a segurança do experimento?
- Quais são os procedimentos para o adiamento da operação de lançamento?

Requisito PR-015:

Do ponto de vista do experimento em relação ao requisito PR-015.

- Este requisito contribui para a elaboração de um plano de desmobilização em caso de cancelamento do lançamento?
- Este plano de desmobilização contribui com a segurança do experimento?
- Quais são os procedimentos para o cancelamento da operação de lançamento?

Grupo de Requisitos 8

Este é um grupo de requisitos relacionado aos parâmetros para o projeto e operação do EGSE do experimento. Solicito uma análise dos impactos, positivos ou negativos e da aplicação de cada um dos requisitos. Neste caso a análise deve ser individualmente e em grupos selecionados conforme indicado.

Requisito OP-003:

Do ponto de vista do experimento em relação ao requisito OP-003.

- Os níveis de ativações podem ser definidos durante a fase de desenvolvimento?
- Como podem ser definidos?
- Caso sejam necessários ajustes é possível alterar os níveis após a fase de desenvolvimento?

Requisito OP-004:

Do ponto de vista do experimento em relação ao requisito OP-004.

- Todos os comandos no EGSE atendem ao requisito?
- Como este tipo de comando é implementado?
- Os comandos que não atendem a este requisito, como são executados?
- Este requisito pode inviabilizar o experimento?

Requisito OP-005:

Do ponto de vista do experimento em relação ao requisito OP-005.

Há previsão de procedimentos, bem como sua sequência para as situações esperadas nominais atendendo os requisitos PR-013, PR-014, PR-015 e GP-015?

PR-013: *"Devem ser planejados os procedimentos para a operação de experimentos para as situações de operação esperadas"*.
PR-014: *"Devem ser planejados os procedimentos para a operação de experimentos caso ocorra o adiamento da operação de lançamento"*.
PR-015: *"Devem ser planejados os procedimentos para a operação de experimentos caso ocorra o cancelamento da operação de lançamento"*.
GP-015: *"Deve ser enviada uma lista das possíveis situações não nominais passíveis de ocorrência durante a missão aos experimentadores antes do desenvolvimento do experimento".*

Lista do GP-015:

1. O cronograma de ensaios é postergado em 6 meses após a entrega do experimento.
2. Ocorrem diversas (mais de 5) ativações da amostra do experimento durante o EDA.
3. Necessidade de substituição de amostra no campo de lançamentos.

- Quais são os procedimentos?

Requisito PR-012:

Do ponto de vista do experimento em relação ao requisito PR-012.

- Qual é o conjunto mínimo de informações que evidencia o correto funcionamento do experimento?

- Este conjunto de informações está disponível na interface do EGSE?

Requisito PR-013:

Do ponto de vista do experimento em relação ao requisito OP-013.

- É possível atender este requisito de forma integral no experimento?
- Quais são os comandos que atendem a este requisito?
- Qual é a forma de proteção para cada um destes comandos?
- Quais são os comandos que não atendem a este requisito?
- Qual é a forma de obter proteção para estes comandos?
- Este requisito pode inviabilizar este experimento?

Requisitos PR-026, PR-027 e PR-028:

Do ponto de vista do experimento em relação aos requisitos OP-026, OP-027 e OP-028.

- De que forma as limitações previstas neste grupo de requisitos podem ser implementadas no EGSE do experimento?
- O atendimento deste grupo de requisitos pode contribuir com a operação do EGSE durante os ensaios e lançamento?
- Há algum impeditivo para o atendimento deste grupo de requisitos?

Apêndice K

ESTUDO DE CASO

Nesta parte são apresentadas todas as respostas do experimentador relacionadas ao experimento SLEM do estudo de caso.

Considerações gerais do experimentador:

1- Fazer um diagrama para explicar em que fase (e sub fase) cada requisito se aplica. Tipo “linha do tempo”.
2- *Focal point*. É necessário um coordenador responsável pelos experimentos no IAE. Deve ser ativo e de perfil adequado.
3- Na missão Centenário, os russos visitaram os experimentos e experimentadores por duas vezes durante o desenvolvimento. Serviu para corrigir diversas questões do experimento de forma antecipada. É interessante se aplicar o mesmo processo para este programa.
4- Inspeções intermediárias durante o desenvolvimento.

Respostas para o grupo de requisitos 1:

GP-001:

- Se comparado ao aplicado, atualmente, há aumento de formalização documental, incluindo os ensaios intermediários (entre fases, não os ensaios de entrega ou finais).
- O experimentador, atualmente, já controla os ensaios e vê de forma positiva o aumento da formalização.
- De acordo com o experimentador é interessante adotar, preferencialmente, padrões já utilizados pelo IAE.

VR-001:

- Este experimento sofreu o EDA no LIT, ao invés de ser no IAE. Neste caso, foi necessário desenvolver e construir um cabo umbilical para o ensaio do experimento.
- Quando o EDA é efetuado fora do IAE podem ocorrer demandas adicionais para o experimentador.

VR-002:

- Se comparado ao aplicado atualmente há aumento de formalização documental.

VR-003: Sem Impactos.

GP-002:

- Se comparado ao aplicado atualmente, há aumento de formalização documental.
- Necessidade de maior treinamento de equipe.
- Necessidade de apresentação do procedimento de manipulação de amostras.

LO-001: Sem Impactos.

- O experimentador aponta que é importante deixar claro que se trata da estrutura de testes do IAE.

GP-004: Sem Impactos.

GP-005: Sem Impactos.

GP-006: Sem Impactos.

- O experimentador aponta que é importante deixar claro que se trata dos equipamentos do IAE.
- Sugere uma recomendação de igual teor ao experimentador (GP-006).
- Sugere uma recomendação relacionada à manutenção preventiva nos equipamentos utilizados pelo experimentador (quando aplicável).

GP-007: Sem Impactos.

GP-014: Sem Impactos.

- Necessário discutir a responsabilidade da fabricação da massa *dummy*.

MS-003: Sem Impactos.

VR-007: Sem Impactos.

PR-005: Sem Impactos.

- Sugestão de envio das informações, relacionadas ao PR-005, antes do desenvolvimento do experimento.

Respostas para o grupo de requisitos 2:

PR-001: Concorda. Responde à sugestão do PR-005.

MS-001: Sem Impactos.

- Sugestão para ampliar o requisito para outras especificidades do experimento, não apenas limitado à amostra. Por exemplo: temperatura, baterias, etc.

MS-001: Sem Impactos.

GP-015: Sem Impactos.

GP-008: Sem Impactos.

- Sugestão para indicar quando deve ocorrer este evento. A indicação é que seja ao fim da fase de desenvolvimento do experimento. Pois, nesse caso ainda não ocorreu, necessariamente, a fabricação do experimento, mas a solução está desenvolvida.

GP-010: Sem Impactos.

- Sugestão para definir documentação detalhada.

OP-009: Sem Impactos.

- Sugestão para definir OP-009 como evento ligado à documentação detalhada.
- Sugestão para subdividir a documentação detalhada, para que seja possível apresentar o projeto em etapas.
- Sugestão de elaboração de um *template* de documentação mais adequado se comparado ao atual.

OP-010: Sem Impactos.

- Sugestão alterar para procedimentos ao invés de operações. Para aumentar a abrangência do requisito.

AM-001: Sem Impactos.

Respostas para o grupo de requisitos 3:

OP-007: Sem Impactos.

- Sem impactos para treinar 2 ou mais operadores.
- É possível atender a este requisito integralmente.

OP-008: Sem Impactos.

- Sugestão do experimentador, expandir o conceito de operação para procedimento.
- É factível treinar o operador em todas as operações previstas.
- Não há limitações no treinamento do operador.

OP-009: Sem Impactos.

- É possível documentar todas as operações previstas para o EGSE assim do encerramento do desenvolvimento do experimento.

OP-010: Sem Impactos.

- A questão de os operadores estarem de posse da documentação, não impacta na operação do EGSE.

OP-011: Sem Impactos.

- Não há impactos para a equipe se os operadores participarem do EDA em tempo integral do ensaio.

OP-012:

- É importante que as informações, de quando ocorrerão os eventos, sejam bem ajustadas, para que não ocorram óbices para o atendimento deste requisito.
- Deve-se observar o OP-007 e treinar mais os operadores.
- Deve-se deixar claro que se trata do EDA da carga útil.

- O requisito é desejável, mas pode ter impactos para a equipe. É importante o experimentador planejar para atender ao requisito.

Respostas para o grupo de requisitos 4:

OP-014 a OP-025: Sem Impactos.

Em relação ao conjunto OP-014 a OP-025:

- As indicações das autorizações enviadas pelo coordenador das REs são claras o suficiente.
- As indicações do estado do experimento enviadas pelo operador do EGSE do experimento são claras o suficiente.
- O número de indicações é adequado para este experimento.
- É possível dessa forma indicar (em grande parte) ao coordenador das REs qual é o estado em que o experimento se encontra.
- A implementação física destas indicações externas ao EGSE, ou seja, visual. Pois não há, hoje, como automatizar este processo.
- Sugestão para todos os estados: um *led* junto à chave para confirmar o estado ou autorização enviado.

OP-029: Sem Impactos.

- O bloqueio da ativação do experimento por parte do coordenador das REs não danifica ou inviabiliza o experimento.
- É possível sua implementação no experimento ou no EGSE.

Respostas para o grupo de requisitos 5:

GP-009: Sem Impactos, as amostras utilizadas não são sensíveis.

OP-001: Sem Impactos.

- Caso se faça necessária a substituição de amostra, serão levadas para a campanha reservas já devidamente acondicionadas e prontas para instalação no experimento.
- Em caso de o campo de lançamentos não prover infraestrutura, nem equipamentos necessários para a manipulação de amostras do experimento, o experimentador conta com um plano para o fornecimento equipamentos a fim de viabilizar o lançamento do experimento.

OP-002:

- O requisito gera impactos na documentação, acréscimo de documentação.
- Não há impactos no atendimento deste requisito à equipe de experimentadores.
- Sugestão de indicar na linha do tempo quando este evento ocorre.

GP-003: Sem Impactos.

- Não há impactos no atendimento deste requisito para o desenvolvimento do experimento.
- Não há impactos no atendimento deste requisito para o experimento.

- Não há impactos no atendimento deste requisito à equipe de experimentadores.

VR-006:

- É possível verificar a contenção da amostra através de medida, não de forma visual.
- Para esta verificação se executa um procedimento de aquecimento e posterior resfriamento da amostra.

GP-011: Sem Impactos.

- As amostras não sofrem degradação durante a preparação do experimento se executada conforme o procedimento de manipulação de amostras validado.
- A execução do procedimento de manipulação de amostras validado não prejudica a integridade do experimento

GP-012: Sem Impactos.

- As amostras não oferecem riscos ao ambiente de ensaios, considerando seu volume, e a dupla camada de contenção.
- Não há necessidade de se utilizar materiais substitutos às amostras para uso nos ensaios.
- Pode ocorrer degradação da amostra durante os ensaios pelo rompimento da contenção, entretanto isso não ocorreu em diversos ensaios. Adicionalmente caso ocorra é possível identificar o problema através de medida.
- Não há motivos para degradação da amostra durante o armazenamento após o ensaio.
- Em geral não há necessidade de substituição de amostra após o EDA, caso ocorra o rompimento da contenção, condição não nominal, é efetuada a troca da amostra.

Respostas para o grupo de requisitos 6:

VR-004: Sem Impactos.

VR-005: Sem Impactos.

Respostas relacionadas ao VR-004 e VR-005

- O experimento já atende a estes requisitos.
- As tolerâncias das dimensões apresentadas do requisito são possíveis de serem obtidas.
- Para atingir estas tolerâncias, o método designado para a fabricação das partes mecânicas do experimento é adequado.

PR-001: Não aplicável.

PR-002:

PR-003:

Respostas relacionadas aos requisitos PR-002 e PR-003

- Este experimento conta com duas barreiras de proteção, na falha da primeira ocorre a contenção pela segunda.

- Este experimento inicia o voo com suas amostras líquidas, que se solidificam durante a microgravidade.
- O vazamento pode ser detectado através de medida.
- A contenção das amostras ocorre por meio de ampolas de vidro, dessa forma a equipe de experimentadores considera que os vazamentos admissíveis para este experimento devem ser nulos.
- As amostras oferecem riscos ao experimento, não ao seu ambiente.

FS-001:

- O experimento contém partes integrantes que não são visíveis.
- O experimento contém em torno de 80% das partes mecânicas visíveis. E em torno de 10% de eletroeletrônica (cabos, conexões, conectores e motor).
- Podem ser evidenciada avarias, pelo menos parcialmente, através de testes eletroeletrônicos.
- Através de inspeções diretas e indiretas em torno de 90% do experimento é inspecionável. Apenas não é possível para ocorrência de partes soltas, as não visíveis, e que permaneçam em funcionamento.

VR-008: Sem impactos.

VR-009: Sem impactos.

GP-013: Sem impactos.

Respostas relacionadas aos requisitos VR-008, VR-009 e GP-013.

- Os procedimentos de testes funcionais podem ser acompanhados apenas pelo operador do EGSE do experimento.
- A avaliação do desempenho do experimento deve ser executada pelo experimentador e pelo operador do EGSE do experimento (ambos).
- As formas utilizadas para a conferência das funcionalidades do experimento são testes eletroeletrônicos e *checklist*.

PR-016, PR-017 e PR-018: Já possui.

Respostas relacionadas aos requisitos PR-016, PR-017 e PR-018.

- O experimento é suscetível ao sinal de µG. Não recebe, nem necessita do sinal de LO.
- A implementação foi feita através de uma chave, normalmente, aberta na parte do EGSE da casamata. É seguro intrinsicamente (porta “E” antes do umbilical). Ocorre desbloqueio assim que ocorre a desconexão do umbilical. O bloqueio funciona somente com o umbilical conectado.
- O experimento já atende a este conjunto de requisitos.

Respostas para o grupo de requisitos 7:

VR-010: Sem Impactos.

- O experimentador atende a este requisito atualmente.
- Não há impactos dos testes durante o desenvolvimento.
- Todos os procedimentos são testados individualmente, durante a etapa de desenvolvimento.

VR-011: Sem Impactos.

- Todos os procedimentos são passíveis de serem testados e aprovados até o fim do desenvolvimento.
- Todos os testes são atualmente documentados, dessa forma não há impactos na documentação.
- Testar os procedimentos durante o desenvolvimento pode contribuir com a simplificação, aprimoramento, e melhor domínio dos procedimentos operacionais.

PR-013:

Conforme a lista enviada ao experimentador. Abaixo segue uma lista piloto a fim de exercitar esta questão. O requisito GP-015 trata do envio da lista.

Respostas relacionada à lista:

Item 1: O cronograma de ensaios é postergado em 6 meses após a entrega do experimento.

Resposta: Deve-se devolver o experimento ao experimentador. Mesmo que isso implique na necessidade de uma nova aceitação.

Item 2: Ocorrem diversas (mais de 5) ativações da amostra do experimento durante o EDA.

Resposta: Para o EDA do experimento, necessidade de trocar a amostra.

Resposta: Para o EDA da carga útil não há problemas com uma ativação com temperatura mais baixa do que o nominal, usual para este ensaio.

Item 3: Necessidade de substituição de amostra no campo de lançamentos.

Resposta: Não ocorreu antes. Mas são levadas, para a campanha de lançamento, amostras extras para eventual substituição e ao menos um membro da equipe do experimento é capaz de executar o procedimento de troca de amostra.

Respostas relacionadas ao PR-013:

- O planejamento dos procedimentos para as situações esperadas contribui para elaboração de planos para as situações descritas na lista.
- Para atender ao requisito ocorre alteração na documentação (aumento da documentação).
- O planejamento dos procedimentos para as situações esperadas aumenta a quantidade de procedimentos a serem treinados pelo operador do EGSE.

- Para atender este requisito se faz necessário incluir o procedimento de troca de amostras no campo de lançamento na documentação e treinamento.

PR-014:

- Necessário que seja informado o cronograma de adiamento e em qual situação. O experimentador irá elaborar um plano para cada tipo de atraso.
- Este requisito contribui para a elaboração de planos de contingência, em caso de adiamento do lançamento, bem como, com a segurança do experimento.
- O procedimento para adiamento inferior a 2 hr. durante o lançamento é de resfriamento parcial da amostra. O experimento é mantido ligado.
- O procedimento para adiamento superior a 2 hr. durante o lançamento é de resfriamento completo da amostra. O experimento é desligado.

PR-015:

- Este requisito contribui com o plano de desmobilização em caso de cancelamento do lançamento, bem como, com a segurança do experimento.
- Neste caso, o experimento deve retirado da carga útil, acondicionado nas caixas de transporte e devolvido ao experimentador.

Respostas para o grupo de requisitos 8:

OP-003: Sem Impactos.

- Os níveis de ativação são definidos durante a fase de desenvolvimento.
- Estes níveis são definidos através de testes.
- É possível ajustar os níveis após o desenvolvimento, caso se faça necessário.

OP-004: Sem Impactos.

- Todos os comandos atendem a este requisito.
- A temperatura a ser induzida nas amostras é pré-definida. Os demais comandos são tipo chaves (liga/desliga).
- Este requisito não inviabiliza o experimento.

OP-005:

A sequência de comandos para cada procedimento está documentada.

Para estudo de caso foi aplicada a mesma lista utilizada em GP-015.

- Para o atendimento deste requisito os procedimentos identificados em GP-015 devem ser detalhados.
- Demais procedimentos operacionais estão detalhados.

PR-012: Sem Impactos.

- O conjunto mínimo de informações que evidencia o correto funcionamento do experimento são indicações de estado e indicação de temperatura do forno.

PR-012: Sem Impactos.

- Atualmente todos os comandos contam com proteção.
- Comandos que atendem a este requisito:
    - Liga
    - Desliga
    - Sobe forno
    - Desce forno
    - Inibe μG
    - Reajuste de temperatura
- No caso do comando de reajuste de temperatura a segurança é intrínseca, pois o processo exige uma série de confirmações.
- O experimento atende este requisito de forma integral.

OP-026, OP-027 e OP-028:

Respostas relacionadas aos requisitos OP-026, OP-027 e OP-028.

- O EGSE é analógico, desta forma o operador escolhe e executa conforme a documentação que acompanha o EGSE.
- Não é possível fazer a inibição de comandos, visto que o EGSE é analógico.
- Pode ser acompanhado por *checklist*.
- Caso o *checklist* não seja suficiente seria necessária efetuar a automação do EGSE.
- O atendimento destes requisitos contribui com o treinamento do operador do EGSE.

Não há impeditivos para o atendimento destes requisitos. Mas deve ser definido se o EGSE deve, necessariamente, ser automatizado.