https://doi.org/10.1590/jatm.v16.1351 ORIGINAL PAPER

Safety Requirements Identification in Suborbital Payload Experiments

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

1. Departamento de Ciência e Tecnologia Aeroespacial – Instituto de Aeronáutica e Espaço – Divisão de Eletrônica – São José dos Campos/SP – Brasil.
2. Universidade Federal de São Paulo – Instituto de Ciência e Tecnologia – Departamento de Ciência e Tecnologia – São José dos Campos/SP – Brazil.
3. Departamento de Ciência e Tecnologia Aeroespacial – Instituto Tecnológico de Aeronáutica – Divisão de Sistemas Espaciais – São José dos Campos/SP – Brazil.

*Correspondence author: heullerhacp@fab.mil.br

ABSTRACT

In the concept, design, and development phases of suborbital payload scientific experiments, designers tend to focus on what will be tested using automation and procedures that support the vehicle and space environment. Although tests are the focus, safety is one of the primary areas that may contribute to a successful mission. This paper presents the typical Brazilian suborbital payloads and rockets, and then reviews some losses during the launching campaigns. The system-theoretic process analysis (STPA), which is based on the system-theoretic accident model and process (STAMP) approach, was used to identify 32 unsafe control actions (UCAs), 77 loss scenarios, and 28 safety constraints. These safety constraints were the basis for establishing 74 safety requirements modeled in systems modeling language (SysML). A group of experts in space systems evaluated these safety requirements, and a case study was performed to test the requirement set. The results may contribute to mitigating or eliminating hazards related to these space systems and launch mission safety.

Keywords: Payload; Rocket; Experiments; STPA; SysML; Requirements.

INTRODUCTION

The Brazilian Space Program develops various space systems such as satellites, payloads, and rockets (Palmerio 2017). Safety is one of the core features needed in these systems; therefore, a proper and thorough safety analysis technique must be carried out. During the design phase of the system, it is common to use some component failure-based analyses, such as fault tree analysis (FTA) and failure mode and effect analysis (FMEA), as hazard analysis methods. However, these techniques are not very suitable for identifying hazards when the causes are unrelated to a component, which may lead to an incomplete investigation of hazards and their further mitigation.

Brazil has experienced accidents and losses during the development of its space program. Introducing a new hazard analysis technique called system-theoretic process analysis (STPA) may help prevent accidents. STPA focuses on control problems, not component failures, and can identify hazards that arise due to unsafe and unintended interactions among the system components without component failures.

The Brazilian scientific community has been launching several experiments into space over the last decades (IAE 2010; 2011; 2014; 2017; 2018). Most of them were launched on suborbital payloads using the rockets VSB-30 and VS-30 (Garcia *et al.* 2011). These opportunities are promoted by the Brazilian Space Agency (AEB 2008) and are planned in the National Space Activities

Received: Jul. 31, 2024 | **Accepted:** Set. 27, 2024
Section editor: Adam Cumming
Peer Review History: Single Blind Peer Review.

Program (AEB 2012). Due to the costs and high complexity of launch operations, the increased risks inherent to this activity should be minimized (Brazilian Space 2010). The schedule for this program is intrinsically long, and the opportunities to launch the experiments must be optimized. All efforts to achieve the success of the involved devices must be made, including during the launch operation, and the risks related to the experiments proposed by the technical-scientific community must be mitigated as well.

This work proposes applying the STPA technique (Leveson and Thomas 2020), based on the system-theoretic accident model and process (STAMP) (Leveson 2012), to analyze onboard scientific experiments and their interfaces in suborbital rocket payloads. This technique aims to identify safety constraints, recommendations, and guidelines that will contribute to developing a set of requirements applicable to scientific experiments onboard suborbital rocket space payloads. This set of requirements was verified and validated by logical assessment and subsequently reviewed by experts.

METHODOLOGY

The main objective of this work is to identify a set of safety constraints, requirements, and recommendations presented in a template form related to scientific experiments and space payloads. In order to achieve the objective, a method was defined to conduct this study.

Initially, we identified the losses that need to be prevented. The losses were used to identify the hazards. Based on these hazards, system-level constraints were found, indicating system behaviors or circumstances that must be satisfied to avoid the hazards and losses. The following steps in the analysis require a control structure. First, a high-level control structure, followed by a detailed model for the part of interest. It is important to note that the control structure used in the STPA is a functional model, not a physical one. It is also not an executable model nor a simulation model. It should also be considered that control actions do not necessarily mean that a certain action sent by a controller will be followed. The same goes for feedback. As much as there is an established channel for feedback, it does not mean that it will always be sent or received. With the help of the detailed model of the part of the system under study, unsafe control actions (UCAs) were found. Through the analysis of the UCAs, it is possible to proceed to the identification of loss scenarios. A loss scenario describes the causal factors that have the potential to lead to UCAs and risks. These scenarios help identify safety constraints that may prevent or mitigate the losses.

The safety constraints were the basis for identifying safety requirements and recommendations. We built a requirements model based on SysML. These requirements were submitted to an evaluation process through questionnaires answered by experts. The answers were analyzed, and a case study was performed to verify the application of the safety requirements identified in this work. The sequence of these steps is presented in Fig. 1.

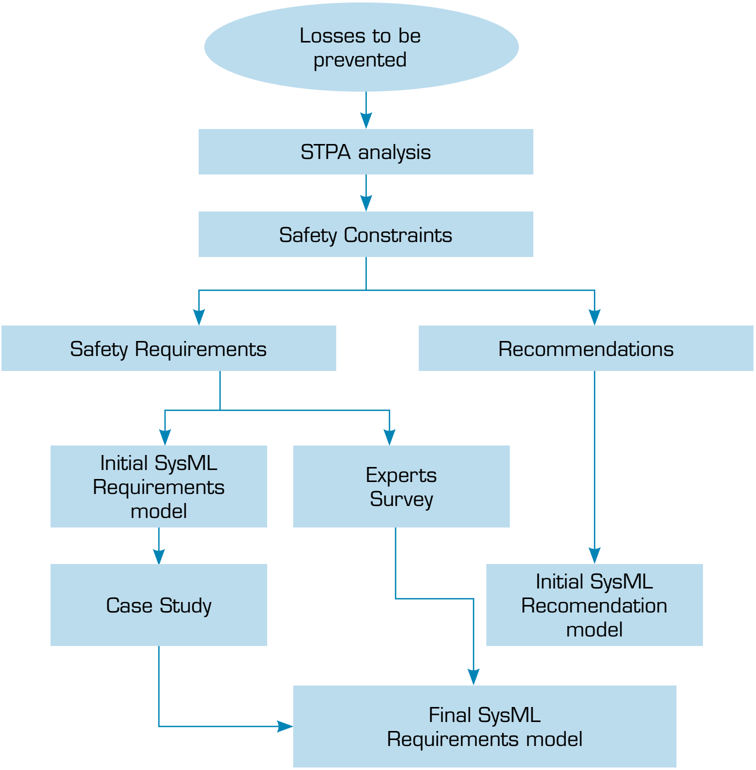
System-theoretic accident model and process (STAMP)/system-theoretic process analysis (STPA)

Traditional hazard analysis techniques need a completed design before the analysis can begin, assuming that component failures cause accidents. Component failure was considered the primary cause of accidents in the past. The hazard analysis and safety design techniques focused on identifying critical components and preventing failures (based on component reliability) or investing in redundant systems to mitigate failure effects.

During the experiment testing and launching phases, it is necessary to apply an analysis that is not restricted to component failure. Many of the hazards involved are related to the interaction between teams, operators, equipment, or systems.

The STAMP/STPA technique, developed by Leveson (2012), adopts a causal model of accidents based on system theory. It assumes that accidents can occur due to unsafe interactions between components of the system, even if none of them has failed. Some characteristics of this technique are suitable for the development of this work: (i) the top-down view analysis is appropriate for highly complex systems; (ii) it includes software, human factors, organizations, and safety culture, among others, as causal factors in accidents or any other type of loss without having to treat them separately.

The two most widely used STAMP-based techniques are STPA (Leveson and Thomas 2020) and causal analysis based on systems theory (CAST) (Leveson 2019). Specifically, STPA treats safety analysis as a dynamic control problem rather than a failure prevention problem. It is a proactive analysis method that considers the potential causes of accidents during development. This way,



Source: Elaborated by the authors.

Figure 1. Methodology steps.

hazards can be controlled or eliminated during the initial phase. CAST is a retroactive analysis method, which examines an accident or incident that has occurred and identifies the causal factors involved. These techniques expand the traditional causality model beyond the directly related or component failure event chain to include more complex processes and unsafe interactions between systems and their components (Fugivara *et al.* 2021; Nakao *et al.* 2011).

System-theoretic process analysis (STPA) analysis of scientific experiments

Since this work focuses on requirements identification based on safety constraints, the most appropriate method to be used is STPA. STPA was applied to analyze onboard scientific experiments and their interfaces in suborbital rocket payloads. This methodology aims to obtain safety constraints, recommendations, and guidelines. They contributed to the development of a set of requirements applicable to scientific experiments in suborbital rocket payloads.

Besides understanding the dynamics of the studied system, the analysis has two primary purposes: a) mitigate the dangers of the propagation of dysfunctional interactions of the experiments and their interaction with other equipment; b) mitigate dangers that emerge from UCAs of the experiments.

The control structure of this STPA analysis is presented in Fig. 2. In this figure, CA means Control Action, and FB means Feedback.

The STPA steps, with the results and examples of the analysis, are presented below.

Identification of stakeholders, their roles, and the respective mapping of potential losses

Examples of stakeholders: scientific experimenter, Aeronautics and Space Institute (IAE), AEB.

In this analysis, the losses that are intended to be avoided are presented below.

L-1: material damage to the payload

L-2: material damage to the experiment

L-3: loss of information from the experiment

Hazards are system states or a set of conditions that, combined with specific circumstances, will lead to an accident and loss. With the experience of those involved in the systems integration of IAE payloads combined with the STPA technique, 10 system-level hazards were identified and are presented below.

H-1: leakage of liquid samples or other liquid items from the experiment

H-2: leakage of gaseous samples or other gaseous items from the experiment

H-3: attachment of components or any other part of the experiment

H-4: overheat

H-5: violation of the grounding system

H-6: inadequate testing

H-7: experiment allowed to fly without achieving satisfactory performance during testing

H-8: out-of-specification handling of the experiment during flight preparation

H-9: improper activation

H-10: not flight-ready

The hazards were identified based on the system-level constraints. The system-level constraints indicate system behaviors or circumstances that must be satisfied to avoid hazards and consequential losses. Seventeen system-level safety constraints were identified. They specify system conditions or behaviors that must be met to prevent hazards. There are three examples below.

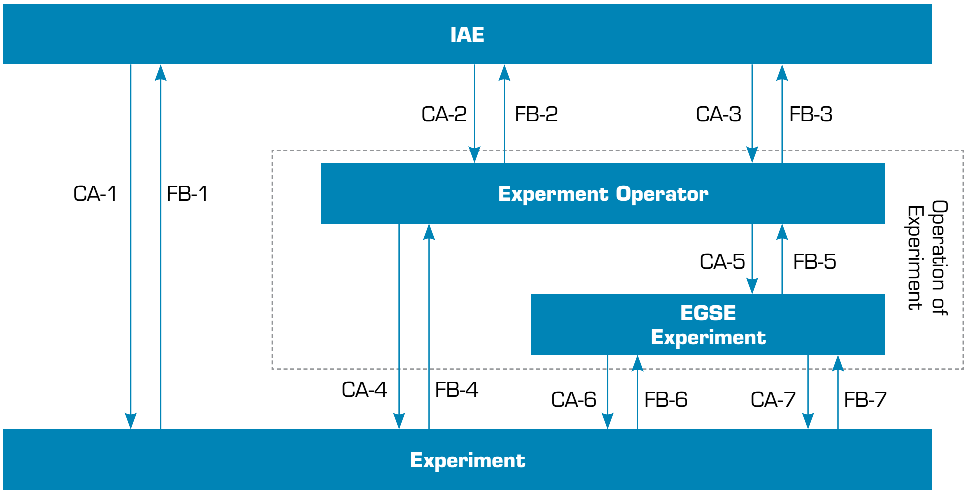
SC-1: no leaks (gases or liquids) can occur from the experiment (H-1, H-2, H-4, H-5).

SC-11: the manipulation necessary to prepare the experiment for the flight shall strictly follow the procedure designed by the experimenter (H-1, H-2, H-3, H-4, H-5, H-8).

SC-14: a communication process between the electric network coordinator and the experiment operator shall be established (H-9, H-10).

Modeling the control structure

The analysis requires models in the form of a control structure of the studied system. A high-level model and a detailed view of the parts of interest are shown in Fig. 2.



Source: Elaborated by the authors.

Figure 2. STPA experiment control structure.

Identification of unsafe control actions (UCAs)

An UCA is a control action in a specific context and unfavorable environment and may offer a hazard. Thirty-two UCAs were identified based on the control actions shown in Fig. 2.

Two examples of the analysis related to CA-4 are shown below.

CA-4: preparation for tests and flight

FB-4: visual inspection

Example UCA-15 (based on CA-4): the experiment was not prepared with the same procedure validated during the tests or preparation for flight (H-1, H-2, H-3, H-4, H-5, H-6, H-8).

Example UCA-17 (based on CA-4): change of experiment sample carried out too early during testing or preparation for flight, in the case of degradation-prone samples (H-3, H-6, H-8, H-10).

Identification of loss scenarios

A loss scenario describes causal factors that have the potential to lead to UCAs and hazards. Seventy-seven loss scenarios were identified based on the 32 UCAs. Two examples are presented below.

Example scenario 1 of UCA-15: the sample exchange procedure performed differs from the validated one during the tests. In this scenario, the tested configuration is different from the validated one; therefore, the tests are not representative. This way, it may hide possible sample leaks, which might damage the electrical networks and the grounding system during flight.

Example scenario 2 of UCA-17: the experiment has the samples replaced for testing. However, the schedule is changed, and testing is postponed. In this scenario, the samples in the experiment degrade, thus changing their characteristics, but are not replaced (H-8). The test runs in this way. However, it is not representative (H-6).

Identification of the necessary safety constraints to mitigate the hazards

The steps followed in the STPA technique make it possible to identify safety constraints to minimize the UCAs for the studied system. Twenty-eight safety constraints were identified based on the 77 loss scenarios.

Example – Safety constraint REST-001 referring to UCA-15: the payload management team must not allow the integration of the experiment into the payload until it has fully met the expected list of tests and validations.

Example – Safety constraint REST-012 referring to UCA-17: the information about the conditions that lead to the degradation of the samples must be accurate.

Example – Safety constraint REST-015 referring to UCA-15: the experiment must be tested in the dynamic acceptance test under the same conditions as the flight.

Example – Safety constraint REST-019 referring to UCA-17: the schedule changes must be communicated to the experimenters.

Safety requirements identification and SysML model

As a starting point, 74 safety requirements were identified based on the 28 safety constraints. They define the conditions to be met to contribute to achieving the safety constraints. The safety requirements have been written in the form adopted by IAE, based on European Cooperation for Space Standardization (ECSS 2009). Each of the safety requirements is related to at least one safety constraint. The requirements were classified based on ECSS (2009), and their classes are shown in Table 1.

Table 1. Requirements classes and their identifications.

Requirement class	Identification
Functional	FC-XXX
Physical	FS-XXX
Mission	MS-XXX
Environmental	AM-XXX
Operational	OP-XXX
Logistic support	LO-XXX
Product assurance	GP-XXX
Design	PR-XXX
Verification	VR-XXX

Source: Elaborated by the authors.

Several stakeholders are described in the safety requirement, often for a particular action or function. However, safety requirements always present the primarily responsible stakeholder identified for this execution or control.

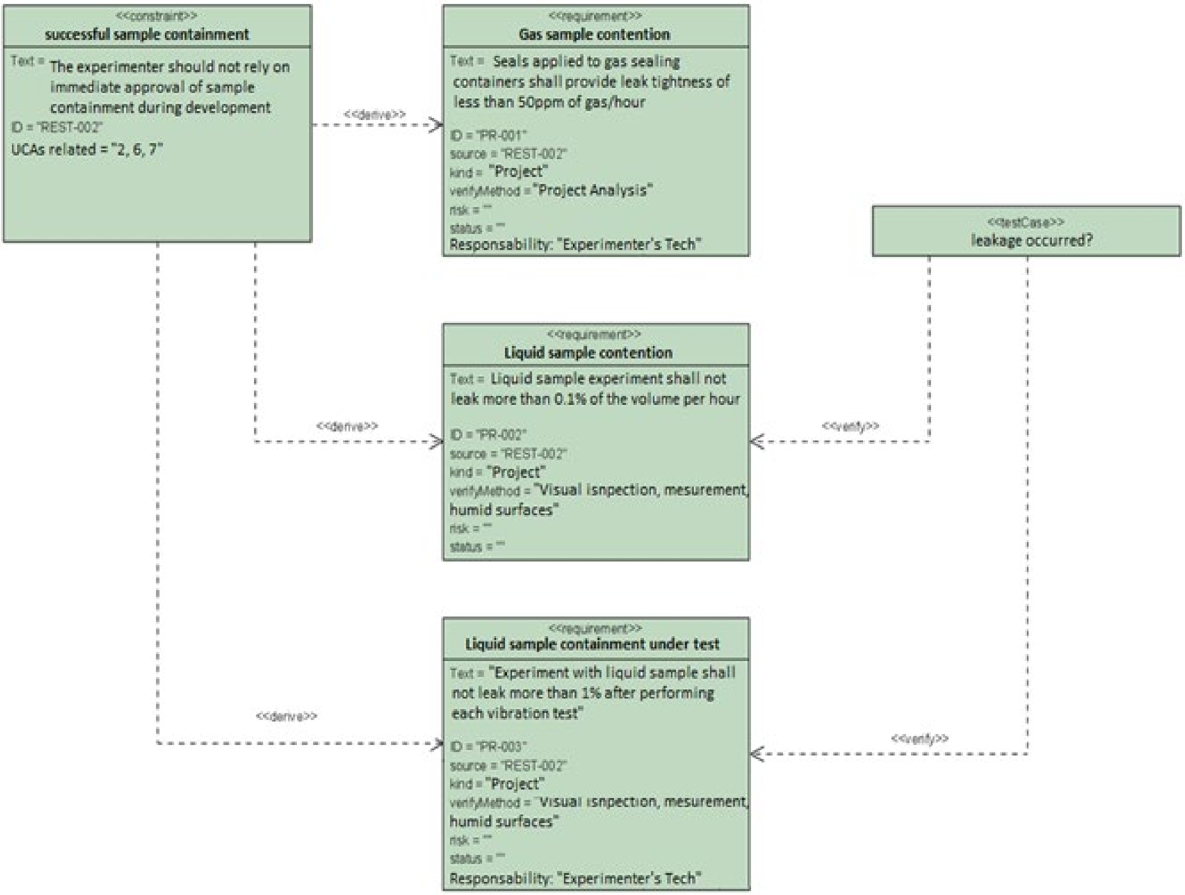
Requirements identification

The safety requirements and recommendations were identified and modeled in SysML language to aid their traceability with safety constraints. The SysML requirements diagrams were modeled in Visual Paradigm software version 16.2. Three types of requirements diagrams were developed: development diagrams, diagrams by responsibilities, and diagrams by subject. Additionally, a safety recommendations diagram was built. The types of diagrams are described below.

Development diagrams – Each development diagram shows the relationship of a given safety constraint to the various safety requirements and constraints derived from it. These diagrams were built to show the traceability of the safety constraints and requirements. As an example, the REST-002 development diagram is presented in Fig. 3.

Diagrams by responsibilities – These diagrams present the same requirements as the development diagrams; however, they have been organized into four groups divided by responsibilities. The responsibilities are IAE technical team/staff/area, IAE management, experimenter technical team/staff/area, and experimenter management. As an example, the experimenter's management responsibility diagram is presented in Fig. 4.

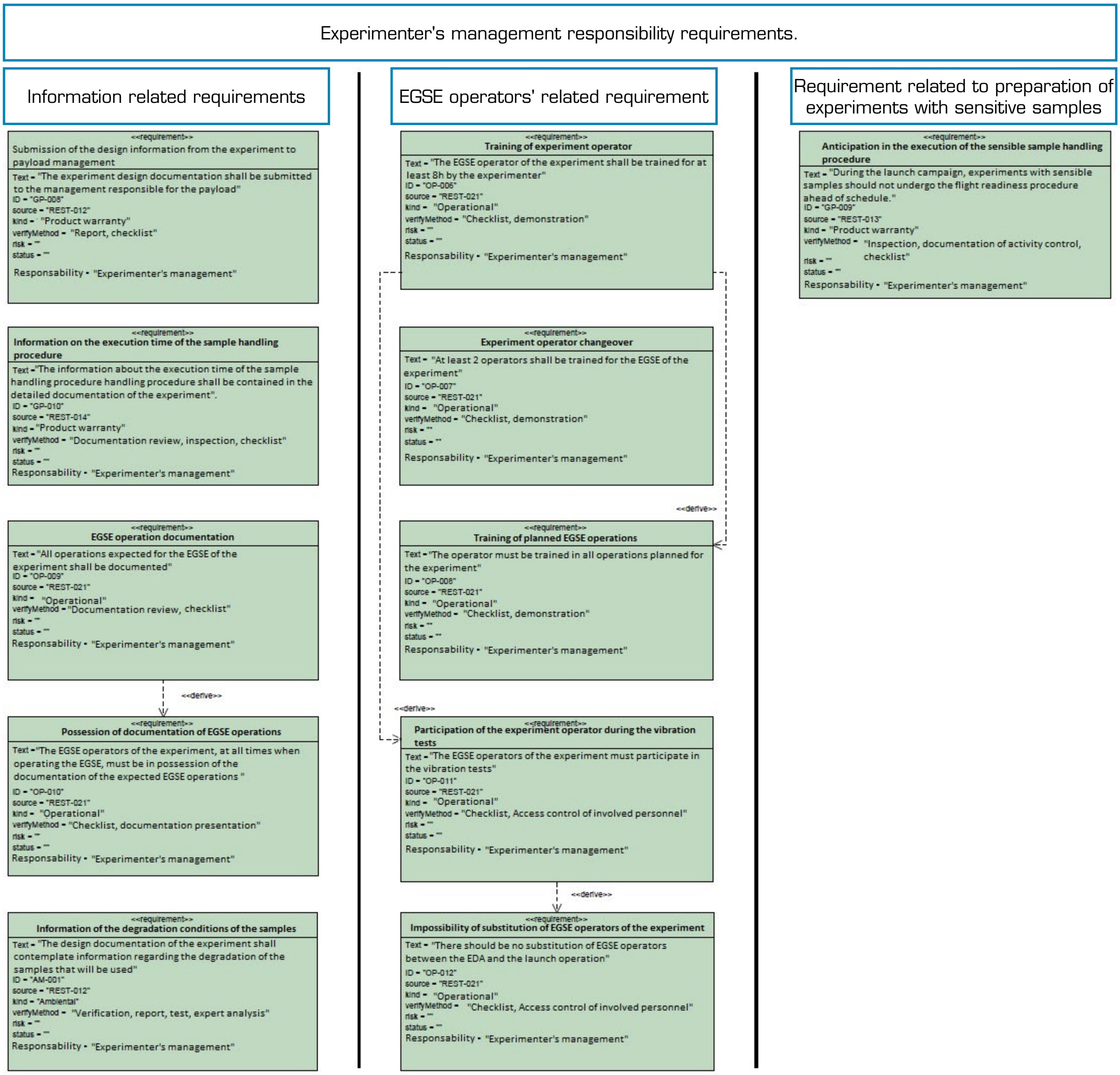
Diagrams by subject – These diagrams present the same requirements as the development diagrams. As an example, the Group 4 diagram is presented in Fig. 5.



<<constraint>>
successful sample containment
Text = The experimenter should not rely on immediate approval of sample containment during development
ID = "REST-002"
UCAs related = "2, 6, 7"
<<derive>>
<<requirement>>
Gas sample contention
Text = Seals applied to gas sealing containers shall provide leak tightness of less than 50ppm of gas/hour
ID = "PR-001"
source = "REST-002"
kind = "Project"
verifyMethod = "Project Analysis"
risk = ""
status = ""
Responsability: "Experimenter's Tech"
<<testCase>>
leakage occurred?
<<derive>>
<<requirement>>
Liquid sample contention
Text = Liquid sample experiment shall not leak more than 0.1% of the volume per hour
ID = "PR-002"
source = "REST-002"
kind = "Project"
verifyMethod = "Visual isnpection, mesurement, humid surfaces"
risk = ""
status = ""
<<verify>>
<<derive>>
<<requirement>>
Liquid sample containment under test
Text = "Experiment with liquid sample shall not leak more than 1% after performing each vibration test"
ID = "PR-003"
source = "REST-002"
kind = "Project"
verifyMethod = "Visual isnpection, mesurement, humid surfaces"
risk = ""
status = ""
Responsability: "Experimenter's Tech"
<<verify>>

Source: Elaborated by the authors.

Figure 3. Safety constraint REST-002 development diagram.



Experimenter's management responsibility requirements.

Information related requirements

Submission of the design information from the experiment to payload management
Text - "The experiment design documentation shall be submitted to the management responsible for the payload"
ID - "GP-008"
source - "REST-012"
kind - "Product warranty"
verifyMethod - "Report, checklist"
risk - ""
status - ""
Responsability - "Experimenter's management"

Information on the execution time of the sample handling procedure
Text -"The information about the execution time of the sample handling procedure handling procedure shall be contained in the detailed documentation of the experiment".
ID - "GP-010"
source - "REST-014"
kind - "Product warranty"
verifyMethod - "Documentation review, inspection, checklist"
risk - ""
status - ""
Responsability - "Experimenter's management"

EGSE operation documentation
Text - "All operations expected for the EGSE of the experiment shall be documented"
ID - "OP-009"
source - "REST-021"
kind - "Operational"
verifyMethod - "Documentation review, checklist"
risk - ""
status - ""
Responsability - "Experimenter's management"

Possession of documentation of EGSE operations
Text -"The EGSE operators of the experiment, at all times when operating the EGSE, must be in possession of the documentation of the expected EGSE operations "
ID - "OP-010"
source - "REST-021"
kind - "Operational"
verifyMethod - "Checklist, documentation presentation"
risk - ""
status - ""
Responsability - "Experimenter's management"

Information of the degradation conditions of the samples
Text - "The design documentation of the experiment shall contemplate information regarding the degradation of the samples that will be used"
ID - "AM-001"
source - "REST-012"
kind - "Ambiental"
verifyMethod - "Verification, report, test, expert analysis"
risk - ""
status - ""
Responsability - "Experimenter's management"

EGSE operators' related requirement

Training of experiment operator
Text - "The EGSE operator of the experiment shall be trained for at least 8h by the experimenter"
ID - "OP-006"
source - "REST-021"
kind - "Operational"
verifyMethod - "Checklist, demonstration"
risk - ""
status - ""
Responsability - "Experimenter's management"

Experiment operator changeover
Text - "At least 2 operators shall be trained for the EGSE of the experiment"
ID - "OP-007"
source - "REST-021"
kind - "Operational"
verifyMethod - "Checklist, demonstration"
risk - ""
status - ""
Responsability - "Experimenter's management"

Training of planned EGSE operations
Text -"The operator must be trained in all operations planned for the experiment"
ID - "OP-008"
source - "REST-021"
kind - "Operational"
verifyMethod - "Checklist, demonstration"
risk - ""
status - ""
Responsability - "Experimenter's management"

Participation of the experiment operator during the vibration tests
Text -"The EGSE operators of the experiment must participate in the vibration tests"
ID - "OP-011"
source - "REST-021"
kind - "Operational"
verifyMethod - "Checklist, Access control of involved personnel"
risk - ""
status - ""
Responsability - "Experimenter's management"

Impossibility of substitution of EGSE operators of the experiment
Text - "There should be no substitution of EGSE operators between the EDA and the launch operation"
ID - "OP-012"
source - "REST-021"
kind - "Operational"
verifyMethod - "Checklist, Access control of involved personnel"
risk - ""
status - ""
Responsability - "Experimenter's management"

Requirement related to preparation of experiments with sensitive samples

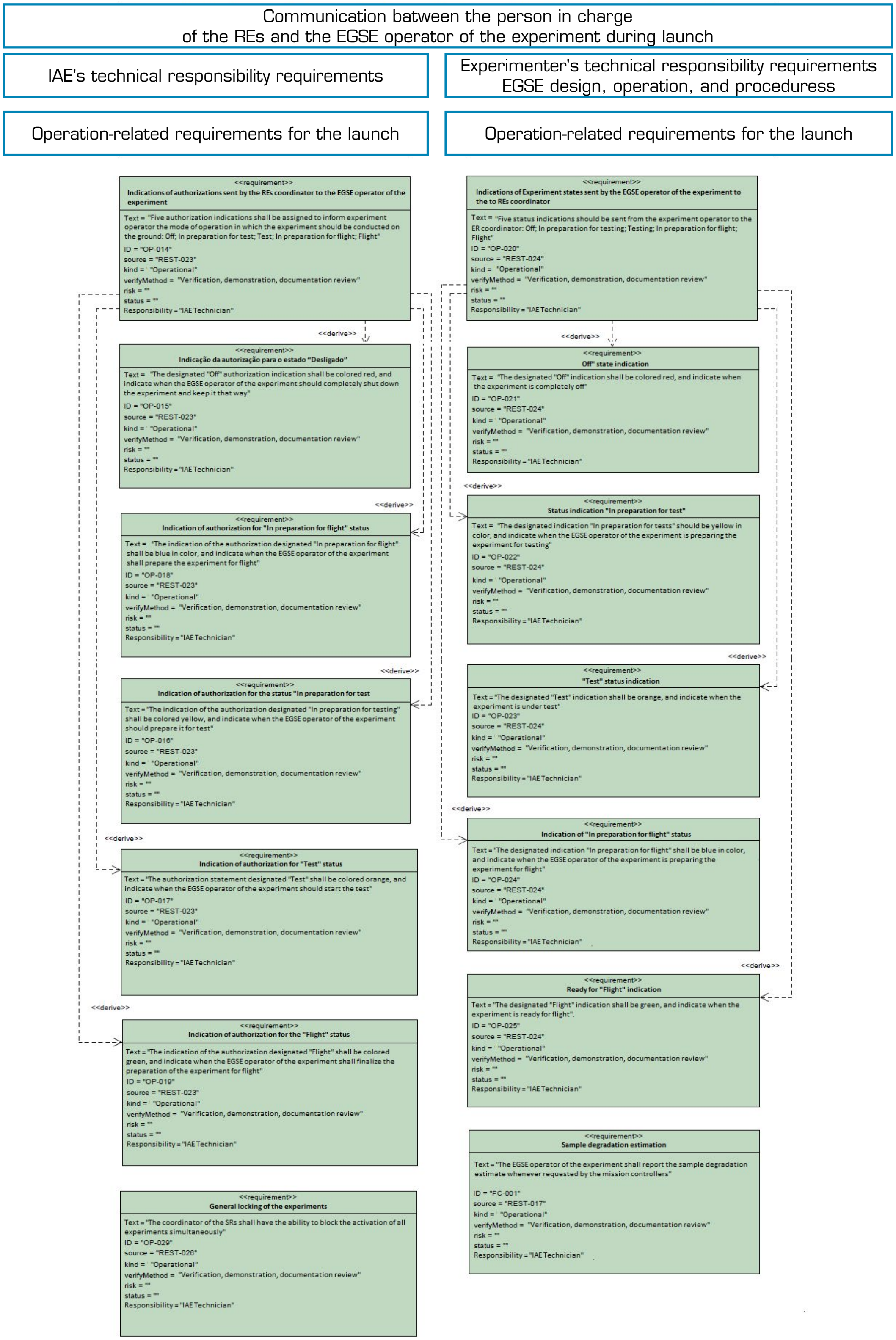
Anticipation in the execution of the sensible sample handling procedure
Text - "During the launch campaign, experiments with sensible samples should not undergo the flight readiness procedure ahead of schedule."
ID - "GP-009"
source - "REST-013"
kind - "Product warranty"
verifyMethod - "Inspection, documentation of activity control, checklist"
risk - ""
status - ""
Responsability - "Experimenter's management"

Source: Elaborated by the authors.

Figure 4. Experimenter's management responsibility diagram.

The requirements were organized into eight groups divided by subject. These groups are:

- Group 1: issues related to the competencies and controls exercised by IAE.
- Group 2: content and flow of information between IAE and the experimenter.
- Group 3: issues related to the experiment's electric ground support equipment operator.
- Group 4: communication between the coordinator of the electrical network and the electric ground support equipment operator of the experiment during deployment.
- Group 5: issues related to the experiment samples.
- Group 6: design parameters for the onboard part of the experiment.
- Group 7: procedures related to the experiment.



Communication batween the person in charge
of the REs and the EGSE operator of the experiment during launch

IAE's technical responsibility requirements

Experimenter's technical responsibility requirements
EGSE design, operation, and proceduress

Operation-related requirements for the launch

Operation-related requirements for the launch

<<requirement>>
Indications of authorizations sent by the REs coordinator to the EGSE operator of the experiment
Text = "Five authorization indications shall be assigned to inform experiment operator the mode of operation in which the experiment should be conducted on the ground: Off; In preparation for test; Test; In preparation for flight; Flight"
ID = "OP-014"
source = "REST-023"
kind = "Operational"
verifyMethod = "Verification, demonstration, documentation review"
risk = ""
status = ""
Responsibility = "IAE Technician"

<<requirement>>
Indicação da autorização para o estado "Desligado"
Text = "The designated "Off" authorization indication shall be colored red, and indicate when the EGSE operator of the experiment should completely shut down the experiment and keep it that way"
ID = "OP-015"
source = "REST-023"
kind = "Operational"
verifyMethod = "Verification, demonstration, documentation review"
risk = ""
status = ""
Responsibility = "IAE Technician"

<<requirement>>
Indication of authorization for "In preparation for flight" status
Text = "The indication of the authorization designated "In preparation for flight" shall be blue in color, and indicate when the EGSE operator of the experiment shall prepare the experiment for flight"
ID = "OP-018"
source = "REST-023"
kind = "Operational"
verifyMethod = "Verification, demonstration, documentation review"
risk = ""
status = ""
Responsibility = "IAE Technician"

<<requirement>>
Indication of authorization for the status "In preparation for test
Text = "The indication of the authorization designated "In preparation for testing" shall be colored yellow, and indicate when the EGSE operator of the experiment should prepare it for test"
ID = "OP-016"
source = "REST-023"
kind = "Operational"
verifyMethod = "Verification, demonstration, documentation review"
risk = ""
status = ""
Responsibility = "IAE Technician"

<<requirement>>
Indication of authorization for "Test" status
Text = "The authorization statement designated "Test" shall be colored orange, and indicate when the EGSE operator of the experiment should start the test"
ID = "OP-017"
source = "REST-023"
kind = "Operational"
verifyMethod = "Verification, demonstration, documentation review"
risk = ""
status = ""
Responsibility = "IAE Technician"

<<requirement>>
Indication of authorization for the "Flight" status
Text = "The indication of the authorization designated "Flight" shall be colored green, and indicate when the EGSE operator of the experiment shall finalize the preparation of the experiment for flight"
ID = "OP-019"
source = "REST-023"
kind = "Operational"
verifyMethod = "Verification, demonstration, documentation review"
risk = ""
status = ""
Responsibility = "IAE Technician"

<<requirement>>
General locking of the experiments
Text = "The coordinator of the SRs shall have the ability to block the activation of all experiments simultaneously"
ID = "OP-029"
source = "REST-026"
kind = "Operational"
verifyMethod = "Verification, demonstration, documentation review"
risk = ""
status = ""
Responsibility = "IAE Technician"

<<requirement>>
Indications of Experiment states sent by the EGSE operator of the experiment to the to REs coordinator
Text = "Five status indications should be sent from the experiment operator to the ER coordinator: Off; In preparation for testing; Testing; In preparation for flight; Flight"
ID = "OP-020"
source = "REST-024"
kind = "Operational"
verifyMethod = "Verification, demonstration, documentation review"
risk = ""
status = ""
Responsibility = "IAE Technician"

<<requirement>>
Off" state indication
Text = "The designated "Off" indication shall be colored red, and indicate when the experiment is completely off"
ID = "OP-021"
source = "REST-024"
kind = "Operational"
verifyMethod = "Verification, demonstration, documentation review"
risk = ""
status = ""
Responsibility = "IAE Technician"

<<requirement>>
Status indication "In preparation for test"
Text = "The designated indication "In preparation for tests" should be yellow in color, and indicate when the EGSE operator of the experiment is preparing the experiment for testing"
ID = "OP-022"
source = "REST-024"
kind = "Operational"
verifyMethod = "Verification, demonstration, documentation review"
risk = ""
status = ""
Responsibility = "IAE Technician"

<<requirement>>
"Test" status indication
Text = "The designated "Test" indication shall be orange, and indicate when the experiment is under test"
ID = "OP-023"
source = "REST-024"
kind = "Operational"
verifyMethod = "Verification, demonstration, documentation review"
risk = ""
status = ""
Responsibility = "IAE Technician"

<<requirement>>
Indication of "In preparation for flight" status
Text = "The designated indication "In preparation for flight" shall be blue in color, and indicate when the EGSE operator of the experiment is preparing the experiment for flight"
ID = "OP-024"
source = "REST-024"
kind = "Operational"
verifyMethod = "Verification, demonstration, documentation review"
risk = ""
status = ""
Responsibility = "IAE Technician"

<<requirement>>
Ready for "Flight" indication
Text = "The designated "Flight" indication shall be green, and indicate when the experiment is ready for flight".
ID = "OP-025"
source = "REST-024"
kind = "Operational"
verifyMethod = "Verification, demonstration, documentation review"
risk = ""
status = ""
Responsibility = "IAE Technician"

<<requirement>>
Sample degradation estimation
Text = "The EGSE operator of the experiment shall report the sample degradation estimate whenever requested by the mission controllers"
ID = "FC-001"
source = "REST-017"
kind = "Operational"
verifyMethod = "Verification, demonstration, documentation review"
risk = ""
status = ""
Responsibility = "IAE Technician"

Source: The authors

Figure 5. Group 4 SysML diagram.

- Group 8: design and operation parameters for the experiment's electric ground support equipment.

During the requirements identification process, safety recommendations were also identified, presented, and structured in the same way. The safety recommendations may be considered best practices and are not mandatory. During the process, implementation recommendations were also identified. These are recommendations for solutions that usually meet satisfactorily one or more requirements, but their application is not mandatory, even if they present an optimal performance for all cases.

Evaluation of safety requirements

After modeling the safety requirements in SysML, we proposed a set of questions and organized the diagrams by subject. The eight questionnaires developed were based on the SysML diagrams by subject (eight groups), one for each group of safety requirements, and all the questions were based on the safety requirements. Each questionnaire is related to a specific group of requirements, such as questionnaire 1 to requirements Group 1, questionnaire 2 to requirements Group 2, and so on.

Questions that analyze requirements were individually identified as "Requirement" followed by a sequential number. Questions that explore the complete requirements presented in the questionnaire were identified as "Question" with a sequential number. The answers in the questionnaires were based on the Likert (1932) scale, in text form, where the lowest agreement with the statement is 1, and the highest agreement is 5. Additionally, each question included an optional field for considerations to offer the expert the opportunity to make particular remarks about the topic.

Two groups of experts were invited to answer these questionnaires. Group 1 is composed of experimenters responsible for the onboard experiments, whose involvement includes more than one launch mission is; AEB experts whose work is related to the scientific experiment programs; and industry professionals with experience in space scientific experiments. Group 2 is composed of developers and integrators, active and retired IAE personnel with expertise in rockets or space payloads. These employees have experience in electronics, space systems design, integration and testing, and management. Each expert received two out of the eight questionnaires to answer.

The questionnaires were distributed to 12 people belonging to expert Group 1, with total adherence, and thus 24 questionnaires were answered in this group. While in the expert Group 2, questionnaires were distributed to 12 people, with adherence from nine, and thus, 18 questionnaires were answered. The total adherence of this study was 87.5%.

We considered five or more as the desired number of answered questionnaires for each type and four as the minimum number. It is possible to verify in Table 2 that several desirable answers were obtained.

Table 2. Number of answered questionnaires by type, group of experts, and total.

Questionnaire	Expert Group 1	Expert Group 2	Total
1	3	2	5
2	3	3	6
3	3	2	5
4	3	2	5
5	3	2	5
6	3	2	5
7	3	3	6
8	3	2	5
Total	24	18	42

Source: Elaborated by the authors.

For each questionnaire, the answers had different weights depending on the group of participants. In the questionnaire where the subject is more related to the experiment, the importance of expert Group 1 (experimenters) is higher than that of expert Group 2 (developers and integrators). When the issue is more related to the payload, information among stakeholders, and mission issues, the weight of expert Group 2 (developers and integrators) is higher than that of expert Group 1(experimenters). The weight and number of questions per survey are presented in Table 3.

Table 3. Weight of the answers by the expert group and the number of questions.

Questionnaire	Questions (n)	Weight Expert Group 1	Weight Expert Group 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

Source: Elaborated by the authors.

The experts answered a total of 42 questionnaires, and the general evaluation of each one achieved 70% or more, so each set of requirements was considered sufficient. The calculation of the general evaluation was according to Eqs. 1 and 2.

$$GE = \frac{\left(Meg1\ x\frac{Page1}{5}\right)+\left(Meg2\ x\frac{Page2}{5}\right)}{5} * 100 \tag{1}$$

where GE is the general evaluation, Meg1 is the average grades for the expert group 1, Page1 is the group weight for experts' group 1, Meg2 is the average grades for the expert group 2, and Page2 is the group weight for experts' group 2.

$$Meg = \frac{Sum\ of\ value\ of\ the\ answers}{number\ of\ questions\ x\ number\ of\ experts} \tag{2}$$

The result of the general evaluation of each of the eight questionnaires is presented in Table 4. All the general evaluations obtained a value above 70%. In this way, the set of requirements for each of the groups was considered sufficient.

Table 4. General evaluations.

Questionnaire	General evaluation (%)
1	92.8
2	93.2
3	88.9
4	90.4
5	85.6
6	85.9
7	90.3
8	81.8

Source: Elaborated by the authors.

The considerations from the observation fields of each of the questionnaires were analyzed, organized, and classified. There were 231 considerations, and they were organized according to the questionnaire and classified as follows:

Lack of context considerations: considerations that have problems interpreting the text of the requirement, vague indication, and lack of context (nine in total).

Vague or inaccurate considerations: considerations with incomplete or inaccurate information regarding the subject matter (12 in total).

Excluded considerations: considerations based on concepts different from those usually applied to the area of this work or whose analysis is partial concerning the subject. These considerations do not take into account the complexity and risks of launching operations or are based on principles that do not apply to the space area (23 in total).

Direct or indirect concordance considerations: considerations that reinforce the concept of the requirement or question. These considerations reinforce the importance of safety requirements. However, they do not provide new data to be considered (127 in total).

Documentation considerations: considerations directly related to the documentation currently used. These are suggestions for improvements related to the information in the documents, templates, and distribution of information (five in total).

Accepted considerations: considerations that were promptly accepted and the modifications were performed in this work (four in total).

Improvement considerations: considerations that suggest improvements in the groups of requirements, although they demand further discussions. They mainly address issues not covered in this study, issues that require development with a more significant number of experts, or possible implementations (51 in total).

Considerations related to lack of context, vague or inaccurate, and excluded considerations need no further treatment. Since they do not provide a good basis for further discussion of the issues addressed, these considerations do not offer opportunities to improve the safety requirements, and for this reason, they were disregarded. An example of one vague or inaccurate consideration and a discussion is presented below.

Example of vague or imprecise consideration

Requirement AM-001 is similar to Requirement MS-001.

Requirement AM-001 Statement: "The design documentation for the experiment shall include information regarding the degradation of the samples that will be used."

Requirement MS-001 Statement: "Information related to the degradation of the experiment samples, when applicable, shall be used for planning the activities of the launching campaign."

Discussion: the statement refers to the similarities between AM-001 and MS-001. Requirement AM-001 addresses the need for the presence of the information related to sample degradation in the experiment documentation, while Requirement MS-001 addresses the need to use this information for planning activities for the launching campaign. Although the requirements address the same information, one addresses the need for it to be reported, and the other addresses its use.

The direct or indirect concordance considerations reinforce the safety requirements and confirm their importance. However, they do not provide data that allow improvements to the proposed requirements. Two examples of concordance considerations and a discussion are presented below.

Example 1 of concordance consideration (GP-008)

Certainly, these two teams work together. Just as the experimenters need to receive information, they must also communicate all the information about their experiment. These stakeholders must be paired.

Requirement GP-008 Statement: "The experiment design documentation shall be provided to the management responsible for the payload."

Discussion: the consideration reinforces the importance of the requirement by presenting the desired effects of its adoption, the exchange of information between teams and the interaction between them.

Example 2 of concordance consideration (OP-001)

It is essential to consider the operating environment in all design phases, from assembly, integration, and testing, to operation.

Statement from Requirement OP-001: "Validation of the sample handling procedure should take into account the facilities of the launch field."

Discussion: the consideration reinforces the importance of the requirement by highlighting issues related to the operating environment of all design phases. In this case, the requirement applies to the launch site operation; however, it should be considered from the development phase.

The documentation considerations require further discussion and are beyond the scope of this work. However, they call for improvements in the current documentation system and have the potential to lead to better communication between the stakeholders. They may be discussed in future papers.

The accepted considerations dealt with some definitions needed to provide a better understanding of certain aspects of some requirements. However, two of them pointed out that Requirement OP-012 should be reclassified as a recommendation since it could impede flying experiments under certain circumstances and is not necessarily something that brings risks to the operation or experiment.

Example of accepted consideration (OP-012)

This should not be a requirement. The operator may be replaced at any time, as long as by someone who can operate the experiment. This requirement could make an experiment unfeasible, which would be detrimental to the program.

Recommendation OP-012 Statement: “There should be no substitution of EGSE operators between the vibration tests and the launch operation.”

Direct concordance consideration (OP-012): ideally, it should be the same operators. The operator obtains knowledge and experience during the vibration tests. Many improvements are made after the vibration tests (in the electrical ground support equipment [EGSE] operation, not the experiment).

Discussion: the accepted consideration points out that there may be substitutions of operators without detriment to the experiment and launching campaign. At the same time, the direct concordance reinforces its importance for improving the EGSE operation. For this reason, it was considered pertinent to reclassify the former requirement as a recommendation.

The improvement considerations deal with the increase in the scope of the requirements, for example, requirements related to charging and discharging batteries, transportation, storage, cables, and electrical connectors, among others. These considerations also deal with possible implementations to meet the requirements. These discussions are pertinent and may be discussed in future works. Two examples of improvement considerations and a discussion are presented below.

Example 1 of improvement consideration (PR-004)

The experimenters only need the flight envelope (longitudinal and lateral loads, vibration levels, etc.). Other information must be passed on through an interface control document to ensure/allow/provide compatibility with the system. By making these data, documents, and test lists available, the experimenter can develop the experiment in a way that is compatible with the platform.

Requirement PR-004 Statement: “All information regarding tests, trials, and experiment procedures must be made available to the experimenters before the development phase.”

Discussion: the consideration suggests a possible implementation for changing the template of the documents and the documentation structure; this is not the scope of this work. Implementations of the requirements may be discussed in the future.

Example 2 (requirements group 6) question

“From the point of view of mission and payload safety, does the group of requirements (requirements 1 through 12) largely address the construction, functionality, and verification characteristics to mitigate the risks offered by the experiment to the payload?”

Expert answer: these 12 requirements are still a small set to classify as a “large part.” Connectors, communication, wiring, allowable materials, protections for batteries, battery charging and discharging, and powering the experiment via the bunkhouse, are some of the critical topics that were not covered in the 12 requirements.

Requirements group 6: “Design parameters for the onboard part of the experiment. This group consists of 12 requirements and deals with the parameters for the physical construction of the experiment, parameters for checks, and the signals received by the experiment from the payload.”

Discussion: the consideration is pertinent and addresses the need to expand the set of requirements. This study does not address electronics, materials, batteries, and other subjects. These issues may be addressed in the future.

Case study

Once the eight groups of requirements obtained overall evaluations considered sufficient, the next step in this research was to conduct a case study. The main objective of this part of the study was to test the requirement set in real experiments to verify if they were feasible to be applied. This case study was performed in an experiment defined in (Toledo 2013). To perform this case study, first, it was necessary to develop questionnaires to evaluate the impacts of the requirement groups on a specific experiment. As a second step, the experiment was selected to perform this case study. The third step was to select the expert to answer the questionnaires. The expert involved during the development of this experiment has 41 years of space science experience and was not involved in the evaluation described in the Conclusion section. The questionnaires were answered during 10 hours of interviews with the selected expert. The answers were analyzed, and the results were discussed.

The questionnaires were based on the eight groups defined on the SysML diagrams by subject. Within each questionnaire, the requirements were organized into sets, according to the subjects they relate to, focusing on specific questions for these sets. When the requirement did not fit into a set, the questions were addressed individually. The questions were designed to elicit discursive answers. Table 5 shows the number of questions on the eight questionnaires.

Table 5. Number of questions of the questionnaires.

Questionnaire	Questions - requirements set (n)	Questions - requirements individually (n)	Total questions (n)
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

Source: Elaborated by the authors.

Examples of questions related to a set of requirements and individually addressed are presented below.

Example of questions of a group of requirements of the case study questionnaire 4

Requirement OP-014 Statement: "Five authorization indications must be designated to inform the ground experiment operator of the operating mode in which the experiment should be conducted: Off; In test preparation; Test; In preparation for flight; Flight."

Requirement OP-015 Statement: "The designated authorization indication "Off" shall be colored red and indicate when the EGSE operator of the experiment shall completely turn it off and keep it in this state."

Requirement OP-016 Statement: "The designated authorization indication 'In preparation for test' shall be colored yellow and indicate when the EGSE operator of the experiment shall prepare it for the test."

Requirement OP-017 Statement: "The designated authorization indication 'Test' shall be colored orange and indicate when the EGSE operator of the experiment should start the test."

Requirement OP-018 Statement: "The designated authorization indication 'In preparation for flight' shall be colored blue and indicate when the EGSE operator of the experiment should prepare the experiment for flight."

Requirement OP-019 Statement: "The designated authorization indication 'Flight' shall be colored green and indicate when the EGSE operator of the experiment should finish the preparation of the experiment for flight."

From the point of view of the experiment related to requirements OP-014, OP-015, OP-016, OP-017, OP-018, and OP-019:

Question 1: Are these indications of the authorizations sent by the coordinator of the electrical networks clear enough?

Answer 1: The indications of the authorizations sent by the coordinator of the electrical networks are clear enough.

Question 2: Is the number of indications adequate?

Answer 2: The number of indications is adequate for this experiment.

Question 3: Is it possible to indicate (most of the time) to the EGSE operator of the experiment which procedures can be performed?

Answer 3: It is possible in this way to indicate (in most situations) the electrical network coordinator's status of the experiment.

Question 4: May the physical implementation of these indications be implemented in the EGSE of the experiment, or is it preferable to be external to it?

Answer 4: The physical implementation of these indications should be external to the EGSE (visual). It is not feasible to automate this process at the moment.

Extra consideration from the expert: for all the five states, implement lights next to the keys to confirm the state or authorization sent. It is an implementation consideration.

Example of questions from individual requirements of the case study questionnaire 5

Requirement OP-002 Statement: "Validation of the sample handling procedure must be performed by a team with knowledge of the launch site and the experiment acceptance process."

From the point of view of the experiment concerning requirement OP-002:

Question 1: Does a competent team's validation of the sample handling procedure contribute to the procedure being feasible and viable at the launching site?

Answer 1: The requirement impacts documentation, increasing it.

Question 2: What are the impacts of the validation of the sample handling procedure for the experiment?

Answer 2: There are no impacts on the team of experimenters in meeting this requirement.

Question 3: What impacts validate the experimenter team's sample handling procedure?

Answer 3: There are no impacts.

Extra consideration from the expert: indicate the schedule when this event (OP-002) occurs.

Some case study results

This part of the study describes and discusses the main aspects identified by the analyses of the application of the safety requirements in the solidification of eutectic alloys in microgravity (SLEM) experiment. It should be taken into account that this experiment was developed by the National Institute for Space Research (Instituto Nacional de Pesquisas Espaciais – INPE), an institute with experience in space artifacts, thus meeting many of the proposed requirements. The developers have experience in the development of critical systems. The institute adopts several good practices that are convergent with the safety requirements. Next, some primary considerations and discussions regarding the adoption of the safety requirements are briefly presented.

Consideration: test control generates more formalization, considering that the standards to be adopted should preferably be the same as those used by IAE.

Origin of the consideration: this consideration is related to Requirement GP-001, answer to question 1, from questionnaire 1.

Discussion: the experimenter's consideration about the adoption of testing and reporting standards simplifies the formalization, documentation, and standardization of testing. Reporting standards, documentation, and assay information must be submitted to IAE before the development of the experiment.

Consideration: regarding requirement GP-006, the experimenter points out that it is essential to make it clear to IAE that the requirement is applicable. Additionally, the experimenter suggests that the same content of this requirement can be offered to the experimenter as a recommendation. He also suggests a recommendation related to the preventive maintenance of the equipment used by the experimenter.

Origin of the consideration: this consideration is related to Requirement GP-006, answer to question 9, from questionnaire 1.

Discussion: the justification field of Requirement GP-006 has been updated, indicating that it applies to IAE equipment. The other considerations are pertinent but need further discussion and may lead to an increase in the set of requirements and recommendations.

Consideration: the experimenter suggests extending the subject of Requirement MS-001 to other specifications of the experiment, not just related to the sample, such as temperature, batteries, etc.

Origin of consideration: this consideration is related to the Requirement MS-001, answer to question 2 from questionnaire 2.

Discussion: it deals with the increase of the requirement scope. The consideration is valid. However, further discussions are needed, which may generate new requirements.

Consideration: the experimenter suggests subdividing the detailed documentation of the experiment, allowing the project presentation in stages.

Origin of the consideration: this consideration is related to Requirement OP-009, answer to question 7, from questionnaire 2.

Discussion: several expert considerations point to the need to improve the current documentation system. A new documentation model should be studied to better serve the stakeholders.

Consideration: the technical team responsible for the payload should perform inspections and intermediate analyses during the development of the experiment. This recommendation was based on the processes applied to the experiments during the Centennial Mission. During this mission, the experiments underwent two inspections by the experts responsible for the mission payload.

Origin of the consideration: this is an additional consideration offered by the experimenter that was not foreseen in any questionnaire. It has been recorded as general consideration 3.

Discussion: this recommendation requires changes in the AEB experiment program. It is a pertinent recommendation. However, its implementation requires further discussion and possibly restructuring the experiment program.

Consideration: the experiment has two sample containment barriers, and the failure of the first barrier can be verified by measurement. The accidental leakage of the samples poses risks to the experiment but not to the environment.

Origin of consideration: this consideration summarizes the answers provided for questions 11 to 15 in questionnaire 6. These answers are related to Requirements PR-002 and PR-003.

Discussion: the analysis demonstrates that the experiment meets Requirements PR-002 and PR-003.

CONCLUSION

System-theoretic process analysis (STPA) guided the research to identify 28 safety constraints used to propose 74 safety requirements. Professionals in the space sector may use the STPA process to conduct new investigations to expand safety constraints and requirements sets. The technique steps guided the research and made it easier to delimit the research scope.

The SysML development diagrams were used to review the safety requirements after the evaluation and may be used to aid in tracing and expanding the requirements set. The SysML diagrams by responsibilities may be used presently by those responsible for the requirements. The SysML diagrams by subjects may be used to distribute and present the safety requirements to the stakeholders.

It is possible to evaluate the understanding of the safety requirements through the experts' answers presented in Case study section. The experts answered 231 considerations in the comments field and nine presented problems in understanding the safety requirement statement. In this case, the comprehension problems were 9/231 (3.9%), while the comprehension proved effective in 96.1% of the requirements considerations. This rate of understanding was considered sufficient by the author.

Of the total of 231 considerations answered by the experts in the comments field, 127 of them are directly or indirectly in concordance with the requirement statement. Four considerations were obtained from the experts' questionnaires answers, which provoked changes in this work. Five considerations were related to improving the current documentation system. In addition, 51 suggestions were obtained for improving the requirements, part of which deals with expanding the scope. Thus, 187 considerations were accounted for, presenting elements of concordance with the set of requirements, totaling 80.95% of considerations that support it. This support index was considered sufficient by the author. The organization of the SysML diagrams by subjects was used to evaluate, execute the case study, and present the requirements to the stakeholders.

The STPA analysis performed in this work and subsequent identification of requirements demand professionals with experience in space systems. It is crucial to establish a communication channel with professionals with specific technical knowledge, such as

IAE professionals, system users with experience, such as scientific experimenters, experts in the area of regulation and subsidy, such as AEB professionals, and industry professionals, such as those professionals from the various companies involved in the Brazilian aerospace program.

For the stakeholders' adoption of the requirements template, the set of requirements should be compatible with the institutional realities. At the same time, the minimum criteria must be balanced so that the risks are appropriately mitigated. Through the considerations of the case study expert, the need for the distribution of additional material to the experimenters, not only the requirements set, was evidenced.

The main contribution of this research was providing a set of safety requirements that contribute to the safety of suborbital rockets, payloads, experiments, and the safety of the launch mission. This set of requirements is intended to eliminate or mitigate losses within the launch mission as a whole for both the scientific experiments and the other space artifacts. Another contribution is the process used for identifying the set of safety requirements, which is flexible enough to identify requirements for space artifacts related to suborbital rocket flights in other projects. This process has been described throughout this paper so that further analyses can be performed to identify new safety requirements. In addition to the set of safety requirements and the process for identifying them, evaluation processes have been established with case study experts to analyze the application of the developed requirements.

CONFLICT OF INTEREST

Nothing to declare.

AUTHORS' CONTRIBUTION

Conceptualization: Procópio HAC; **Methodology:** Martins LEG; **Software:** Procópio HAC; **Validation:** Martins LEG and Lahoz CHN; **Investigation:** Procópio HAC; **Resources:** Procópio HAC; **Data Curation:** Procópio HAC; **Writing - Original Draft:** Procópio HAC; **Writing - Review & Editing:** Procópio HAC and Martins LEG; **Supervision:** Martins LEG and Lahoz CHN; **Project administration:** Martins LEG; **Final approval:** Procópio HAC.

DATA AVAILABILITY STATEMENT

The data will be available upon request.

FUNDING

Not applicable.

ACKNOWLEDGMENTS

Not applicable.

REFERENCES

[AEB] Brazilian Space Agency (2008) Experimentos suborbitais de microgravidade [accessed Sep 25 2024] https://www.gov.br/aeb/pt-br/centrais-de-conteudo/publicacoes/institucional/revistas-pdf/004revista-peb-abr-mai-jun-2008.pdf/

[AEB] Brazilian Space Agency (2012) National Program of Space Activities. PNAE: 2012-2021. Brasília: Ministério da Ciência Tecnologia e Inovação; p. 37.

[ECSS] European Cooperation for Space Standardization (2009) ECSS-E-ST-10-06C: Space Engineering – Technical requirements specification [accessed Sep 25 2024]. https://ecss.nl/standard/ecss-e-st-10-06c-technical-requirements-specification/

[IAE] Aeronautics and Space Institute (2010) Activity report 2010 https://www.academia.edu/75829678/Relat%C3%B3rio_de_Atividades_do_Instituto_de_Aeron%C3%A1utica_e_Espa%C3%A7o

[IAE] Aeronautics and Space Institute (2011) Activity report 2011 https://www.academia.edu/51170681/Relat%C3%B3rio_de_Atividades_do_Instituto_de_Aeron%C3%A1utica_e_Espa%C3%A7o

[IAE] Aeronautics and Space Institute (2014) Activity report 2014 https://www.academia.edu/124140800/Instituto_de_Aeron%C3%A1utica_e_Espa%C3%A7o_Relat%C3%B3rio_de_Atividades_2014

[IAE] Aeronautics and Space Institute (2017) Activity report (2016-2017) https://www.academia.edu/124140889/Instituto_de_Aeron%C3%A1utica_e_Espa%C3%A7o_Relat%C3%B3rio_de_Atividades_2016_e_2017

[IAE] Aeronautics and Space Institute (2018) Activity report 2018 https://www.academia.edu/124140933/Instituto_de_Aeron%C3%A1utica_e_Espa%C3%A7o_Relat%C3%B3rio_de_Atividades_2018

Brazilian Space (2010) Operação Maracati II [accessed Sep 25 2024]. https://brazilianspace.blogspot.com/2010/12/opera%C3%A7%C3%A3o-maracati-ii.html

Fugivara S, Merladet AVD, Lahoz CHN (2021) STPA analysis of Brazilian sounding rockets launching operations. Microgravity Sci Technol 33:43. Available in: https://www.scielo.br/j/jatm/a/nT8RX4jBxnGVDKB3yXcrnVy/

Garcia A, Yamanaka S, Barbosa A, Bizarria F, Jung W, Scheuerpflug F (2011) VSB-30 sounding rocket: history of flight performance. J Aerosp Technol Manag 3(3):325-330. https://doi.org/10.5028/jatm.2011.03032211

Leveson N (2012) Engineering a safer world: systems thinking applied to safety. Massachusetts: The MIT Press.

Leveson N (2019) CAST handbook: How to learn more from incidents and accidents [accessed Sep 25 2024]. https://psas.scripts.mit.edu/home/get_file4.php?name=CAST_handbook.pdf

Leveson N, Thomas J (2020) STPA handbook [accessed Sep 25 2024]. https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

Likert R (1932) A technique for the measurement of attitudes. Arch Psychol 140:55.

Nakao H, Katahira M, Miyamoto Y, Leveson N (2011) Safety guided design of crew return vehicle in concept design phase using STAMP/STPA. Versailles: International Association for the Advancement of Space Safety.

Palmerio A (2017) Introduction to rocket technology. 2nd ed. São José dos Campos: SindCT.

Toledo R (2013) Estudo da solidificação de ligas metálicas eutéticas em ambiente de microgravidade (doctoral dissertation). São José dos Campos: Instituto Nacional de Pesquisas Espaciais. In Portuguese. Available in; http://urlib.net/sid.inpe.br/mtc-m19/2013/02.21.12.26