MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS	**PROJETO:** **EQUARS**

EQUARS Preliminary Safety Requirements

DOCUMENTO: EQUARS-3300-TS-001		**ESTADO: APROVADO**
DESCRIÇÃO: Descreve os requisitos de safety para o projeto EQUARS no idioma inglês.		
DATA: 05-09-2019	**EDT:** SEGURANÇA E MISSÃO (SAFETY)	**PÁGINAS:** 15

AUTORES			
NOME	**DIVISÃO**	**DATA**	**ASSINATURA**
Andreia Fatima Sorice Genaro	CGETE/SESEQ	24/9/19	
Alexandre Degasperi	CGETE/SESEQ	19/9/19	

REVISORES			
NOME	**DIVISÃO**	**DATA**	**ASSINATURA**
Cristiane Mariano Zavati Silva	CGCEA	19/9/19	

APROVADO POR			
NOME	**DIVISÃO**	**DATA**	**ASSINATURA**
Inaldo Soares Albuquerque	CGETE/SESEQ	19/9/2019	
Leandro Toss Hoffmann	CGETE/DSS	19/9/2019	

REVISÕES				
REV.	**DATA**	**N. PÁG. / MUDANÇAS**	**AUTOR**	**APROVADO POR**

SUMÁRIO

1 SAFETY

1.1 GENERAL

1.1.1 Objectives

This document defines the safety program and the technical safety requirements that are implemented in order to protect flight hardware and ground personnel, the launch vehicle, associated payloads, ground support equipment, the general public, public and private property, and the environment from hazards associated with EQUARS during its lifecycle.

The safety policy is applied by implementing the EQUARS safety program, supported by risk assessment, which can be summarized as follows.

a) Hazardous characteristics (system and environmental hazards) and functions with potentially hazardous failure effects are identified and progressively evaluated by iteratively performing systematic safety analyses.

b) The potential hazardous consequences associated with satellite system and subsystems characteristics and functional failures are subjected to a hazard reduction sequence whereby:
1) hazards are eliminated from the satellite design and operations;
2) hazards are minimized; and
3) hazard controls are applied and verified.

1.1.2 Reference Documents

The documents listed in this paragraph are applicable to the extent specified in applicable sections.

RD 1 - ECSS-Q-ST-20-07C (01 October 2014) - Space product assurance – Quality and safety assurance for space test centres
RD 2 - ECSS-M-ST-10C Rev. 1 (6 March 2009) - Space project management – Project planning and implementation
RD 3 - ECSS-Q-ST-10C Rev. 1 (15 March 2016) - Space product assurance – Product assurance management
RD 4 - ECSS-Q-ST-40C Rev.1 (15 February 2017) -Space product assurance – Safety
RD 5 - ISO 14620-1: 2018 - Space systems – Safety Requirements - Part 1: System safety
RD 6 - ECSS-Q-ST-40-02C (15 November 2008) - Space product assurance – Hazard Analysis
RD7 – EQUARS-40-MS-001-A - Declaração de Escopo da Missão EQUARS
RD8 – EQUARS-3000-TS-001 – EQUARS Mission Assurance Preliminary Requirements

2 SAFETY PROGRAM

2.1 SCOPE

a) The scope and content of the safety program is to establish a safety management system to implement provisions of this document according to program requirements.
1) The supplier shall establish and maintain a system safety program.
2) The supplier shall ensure that all applicable national or international safety regulations are identified.
3) The system safety program requirements of this document shall be applied.

b) Tailoring shall not diminish the intent to protect flight and ground personnel, the launch vehicle, associated payloads, ground support equipment, the general public, public and private property, and the environment from hazards associated with space systems.

2.2 SAFETY PROGRAM PLAN

2.2.1 Definition

The plan shall define:
a) the safety program tasks to be implemented;
b) the personnel or supplier responsible for the execution of the tasks;
c) the schedule of safety program tasks related to project milestones;
d) safety program activity interface with project engineering and with other product assurance activities; and
e) how the supplier accomplishes the tasks and verifies their satisfactory completion (by reference to internal procedures as appropriate).

2.2.2 Conformance

The plan shall make provisions to ensure safety requirements and regulations applicable to any other facilities and service that are utilized during the course of the project are identified.

2.3 SAFETY ORGANIZATION

2.3.1 Safety Representative

Each supplier shall appoint a safety representative who is qualified by training and experience to perform system safety functions according to national safety regulations and laws.

2.3.2 Reporting Lines

Safety representative shall have reporting lines to the project manager and access to top management that are independent of the hierarchical reporting line within the project.

2.3.3 Safety Integration

Safety shall be integrated in all project activities.

2.4 SAFETY REPRESENTATIVE ACCESS AND AUTHORITY

2.4.1 Access

The safety representative of an organization shall have access to that organization's safety related data relevant to project safety, and shall be at liberty to report freely, and without organizational constraint on any aspect of project safety.

2.4.2 Delegated Authority to Reject – Stop Work

The safety representative of an organization shall have the delegated authority to reject any project document, or to stop/or interrupt any project activity of this organization that does not conform to approved safety requirements or procedures.

2.4.3 Safety Audits

a) The supplier shall perform safety audits or reviews to verify compliance to project safety policy and requirements.

b) The safety audits shall be in accordance with [AD 2] and [AD 3].

c) The customer shall be informed of the audit schedule.

2.4.4 Approval of Reports

The supplier shall only permit project reports that address matters related to safety certification to be issued with signature of the safety representative.

2.4.5 Representation on Boards

Safety should be represented at configuration control boards (CCBs), non-conformance review boards (NRBs), test review board (TRBs), and at qualification, and acceptance reviews, where safety requirements and safety critical functions are involved.

2.5 SAFETY RISK MANAGEMENT

2.5.1 Safety Risks

Risk to human life, flight product, mission and environment shall be managed throughout the project by performing the following activities:

a) allocation of safety requirements;

b) hazard identification;

c) hazard evaluation;

d) hazard prevention, reduction, and control; and

e) hazard close out, including residual risk acceptance.

2.5.2 Hazard Assessment

a) All hazard assessments shall consider primarily the hazard potential and categorize all hazards according to the appropriate severity category.

b) Corresponding controls shall be proposed.

c) The initial design shall be chosen such that the hazard potential and its related consequence severity are minimized.

d) The probability of a hazardous event shall consequently be taken into account whenever hazard consequence severity reduction methods alone are considered insufficient to adequately reduce the risk.

e) The probability of occurrence shall be reduced by considering all areas of design for minimum risk, increasing the reliability of safety devices, providing warning devices, or using procedural controls and training.

2.6 PROJECT PHASES AND SAFETY REVIEW CYCLE

2.6.1 Progress Meetings

The supplier shall hold regular safety progress meetings to review the status of safety program activities as required by this document. The meetings may be attended by the relevant customer and supplier specialists.

2.6.2 Project Reviews

2.6.2.1 General

a) The supplier shall provide a project safety status as required by the customer.
b) A safety data package shall be prepared for each project review.
c) Project Safety status should be presented during the project reviews (e.g.: PDR, CDR, AR)

2.6.2.2 Mission Analysis/Needs Identification – Phase 0

a) The supplier shall prepare a safety analysis to give support to the identification of sources of safety risk as well as the performance of preliminary trade-off analyses between alternative system concepts.

b) During the Phase 0, the supplier shall demonstrate that:
1) Safety requirements and lessons learned from previous projects were analyzed and support was provided to design and operations concept trade-off; and
2) Main system level safety requirements were identified.

2.6.2.3 Feasibility – Phase A

a) Safety analysis shall support trade-off analyses in arriving at the concept that has acceptable safety risk considering the project and mission constraints.

b) The design technology selected and the operational concept to be implemented shall be selected based on the analysis data for the safest system architecture to eliminate or reduce hazards to acceptable levels.

2.6.2.4 Preliminary Definition – Phase B

a) The safety analysis shall support a continued and more detailed safety optimization of the system design and operations and the identification of technical safety requirements and their applicability.

b) The analysis shall also provide inputs to safety risk assessment in support of safety risk evaluation, the identification of risk contributors in the design and in the operational concept.

2.6.2.5 Detailed Definition, Production and Qualification Testing - Phase C/D

a) Safety analysis shall support detailed design, production, qualification, testing.

b) Safety analysis shall also support operational safety optimization, safety requirements implementation evaluation, risk reduction verification, and hazard and risk acceptance.

c) Analysis of operations shall also support the identification of emergency and contingency response planning and training requirements, and the development of procedures.

d) The space test center shall establish a safety program to assure the safety of all space test center personnel, including the customer and visitors, the test specimen, the test facilities and its associated infrastructure, in accordance with [AD 1].

e) Critical tasks, involving a high level of risk, shall be performed after a previous INPE safety representative approval.

2.6.2.6 Utilization – Phase E

a) Safety analysis shall evaluate design and operational changes for impact to safety, assuring that safety margins are maintained and that operations are conducted within accepted risk.

b) The analysis shall also support the evaluation of operational anomalies for impact to safety, and the continued evaluation of risk trends.

2.6.3 Safety Data Package

The supplier shall prepare and deliver the safety data package. The content of the safety data package shall be defined for each project or program by the safety approval authority.

2.7 SAFETY CERTIFICATION

a) All projects shall certify the safety of the flight and ground system products as having reached an acceptable level of risk in conformance to project specific safety requirements.

b) It shall be the responsibility of the project organization to provide to the certification authority all safety related information that is required to enable the statement of safety compliance to be accepted and understood.

2.8 SAFETY TRAINING

2.8.1 Overhall Training

All safety related training of any personnel working - permanently or occasionally - with products that can have hazardous properties has three major aspects:

1) general awareness briefings on safety measures to be taken at a given location or working environment;

2) basic technical training in the required safety techniques and skills (e.g. inspection, test, maintenance or integration), which are mandatory to fulfill the job function under consideration; and

3) product specific training that focuses on the hazards related to the specific product.

2.8.2 Participation

Participation in the general awareness briefing shall be mandatory for all personnel who have access to the area where the product is processed.

2.8.3 Records

Records of personnel having received training shall be maintained.

2.9 ACCIDENT/INCIDENT REPORTING AND INVESTIGATION

The supplier shall report to the responsible entity all accidents and incidents that affect the product and occur during project activities under the control of the supplier or his sub-suppliers.

2.10 SAFETY DOCUMENTATION

2.10.1 General

The supplier shall maintain safety-related data to support reviews and safety certification.

2.10.2 Supplier Review

The supplier shall review project documentation including specifications, drawings, analyses, procedures and reports, non-conformance reports, failure reports, waivers, and documentation changes in order to verify or assess impact on:

a) the implementation of safety requirements and hazard and risk controls;

b) incorporation of hazard and risk controls into the design or the verification program;

c) completion of verification activities;

d) the design and operational safety of the system; and

e) the validity of safety analyses performed and documented.

2.10.3 Safety Deviations and Waivers

The supplier shall identify all deviations and waivers that affect the applicable project safety requirements. The supplier's safety representative for the project shall review these deviations and

waivers to ensure that possible impacts on safety are fully analyzed. Adequate justification for any deviation considered acceptable by the supplier shall be provided.

6.10.4 Lessons-Learned File

Safety lessons learned should consider as a minimum:
1) the impact of newly imposed requirements;
2) assessment of all malfunctions, accidents, anomalies, deviations and waivers;
3) effectiveness of safety strategies of the project;
4) new safety tools and methods which have been developed or demonstrated;
5) effective versus ineffective verifications which have been performed; and
6) changes proposed to safety policy, strategy or technical requirements with rationale.

3 SAFETY ENGINNERING

3.1 SAFETY DESIGN PRINCIPLES

3.1.1 Human Life Consideration

The preservation of personnel safety shall be the most important priority in the development and operation of space systems.

3.1.2 Hazard Detection – Signalling and Safing

Safety monitoring, display, alarm and safing capabilities shall be incorporated for human space flight systems.
These capabilities shall provide the information necessary to allow the flight crew and ground system operators to take actions which are necessary to protect personnel from the consequences of failures within safety critical functions and the failure of hazard control measures.

3.1.3 Safety Risk Reduction and Control

3.1.3.1 Consequence Severity Assessment

The severity of identified hazardous events shall be categorized as shown in Table 1.

Category	Scoring	Severity	Types of consequence	
I	4	Catastrophic	i)	Loss of life, life-threatening or permanently disabling injury or occupational illness, loss of an element of an interfacing manned flight system;
			ii)	Loss of launch site facilities or loss of system;
			iii)	Severe detrimental environmental effects;
II	3	Critical	i)	Temporarily disabling but not life-threatening injury, or temporary occupational illness;
			ii)	Major damage to flight systems or loss or major damage to facilities;
			iii)	Major damage to public or private property;
			iv)	Major detrimental environmental effects.
III	2	Marginal	Minor injury, minor disability, minor occupational illness, or minor system or environmental damage.	
IV	1	Negligible	Less than minor injury, disability, occupational illness, or less than minor system or environmental damage.	

Table 1 (Reference [RD 2])

3.2 FAILURE TOLERANCE REQUIREMENTS

3.2.1 Basic Requirements

Failure tolerance is one of the basic safety requirements that is used to control hazards. The design of the system shall meet the following failure tolerance requirements:

a) No single failure or operator error shall have critical (or catastrophic) consequences.

b) No combination of:
1) two failures, or
2) two operator errors, or
3) one failure and one operator error shall have catastrophic consequences.

3.2.2 Design for Minimum Risk

Hazards related to design for minimum risk areas of design (e.g. mechanisms, structures, pressure vessels, pressurized lines and fittings, pyrotechnic devices, material compatibility and material flammability) shall be controlled by the safety-related properties and characteristics of the design, such as margin or factors of safety. Failure tolerance requirements shall only to be applied to the design process as necessary to ensure that credible failures that can affect the design do not invalidate safety-related properties.

The facilities and tests of space test center shall be in accordance with [AD 1].

3.3 IDENTIFICATION AND CONTROL OF SAFETY CRITICAL FUNCTIONS

A system function that, if lost or degraded, or through incorrect or inadvertent operation, would result in a catastrophic or critical hazardous consequence, shall be identified as safety critical function.
EXAMPLE: A series of operational events that can result in a hazard if they occur inadvertently or are operated out of order.

4 OPERATIONAL SAFETY

4.1 GROUND OPERATIONS

4.1.1 Review and Inspection

Readiness reviews and inspections should include safety review and assessment of facilities, equipment, test articles, operating, test and contingency procedures, access controls, and personnel capabilities for compliance with safety requirements.

4.1.2 Launch and Landing Site Requirements

a) Launch site operations shall be subject to hazard analysis.
b) For ground operations, the analysis shall address:
1) the potential hazardous consequences of human error and procedural deficiencies;
2) the adequacy and maintenance of operational margins;
3) the potential for human exposure to hazards and hazardous effects;
4) the requirements for operator and flight crew training; and
5) the adequacy of information and data provided by the flight hardware, ground support equipment (GSE), or test equipment, as appropriate, to support the performance of the operations in accordance with the applicable safety requirements.

4.1.3 GSE Requirements

Ground support equipment shall be subject to hazard analysis.

5 SAFETY ANALYSIS REQUIREMENTS AND TECHNIQUES

5.1 SAFETY ANALYSIS

5.1.1 General

Safety analysis shall be refined and updated in an iterative manner as the design process proceeds, to ensure that hazards and hazardous events are assessed, and that the relevant detailed design and operational requirements, hazard controls, and verification activities are defined and implemented.

6 SAFETY VERIFICATION

6.1 TRACKING OF HAZARDS

6.1.1 Hazard Reporting System

The supplier shall establish a hazard reporting system for tracking the status of all identified hazards. The system shall be applied for all catastrophic and critical consequences.

Information related to principles, process, implementation and requirements of hazard analysis could be found on [RD 3].

6.2 QUALIFICATION

The safety critical characteristics of all safety critical functions shall be fully qualified by test. Safety critical function qualification testing shall include the determination of performance margins considering worst case combinations of induced and natural environments and operating conditions. Qualification “by similarity” shall be applied only after customer approval on a case by case basis.

6.3 HAZARD CLOSE-OUT

6.3.1 Safety Assurance Verification

In time for acceptance by the customer, and in preparation of transfer to the launch site, safety assurance shall verify that:

a) Hazard close-outs performed so far by the responsible engineer are still valid.

b) There have been no oversights.

c) The verifications reflect the as-built/as-modified status of the hardware.

d) All open verifications at this time are acceptable for transfer to the launch site.

e) All open verifications have been entered into the safety verification tracking log (SVTL), according [RD 1], which now becomes a living document.

6.3.2 Safety Approval Authority

Close out of each hazard requires approval by the safety approval authority. Hazards shall be considered for closure only when:

a) the hazard has been eliminated;

b) the hazard has been minimized and controlled in accordance with the applicable requirement and the associated verification activities have been successfully completed; or

c) the safety approval authority has granted a deviation or waiver.

LISTA DE ITENS *TO BE DEFINED*		
ID	**DESCRIÇÃO**	**STATUS**
LISTA DE ITENS *TO BE CONFIRMED*		
ID	**DESCRIÇÃO**	**STATUS**