MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS	**PROJECT:** **EQUARS**

Mission Assurance Preliminary Requirements

DOCUMENT: EQUARS-3000-TS-001	**STATUS:** APROVADO	
DESCRIPTION: This document establishes the mission assurance preliminary requirements applicable for the EQUARS mission.		
DATE: 13-09-2019	**EDT:** 3000 – GARANTIA DE MISSÃO	**PAGES:** 15

AUTORS			
NAME	**DIVISION**	**DATE**	**SIGNATURE**
Cristiane Mariano Zavati Silva	CGCEA		
Andreia Fátima Sorice Genaro	CGETE/SESEQ		
Ana Paula de Sá Santos Rabello	CGETE/SESEQ		
Lucas Lopes Costa	CGETE/SESEQ		
Silvio Manea	CGETE/SESEQ		
Sergio Itami	CGETE/SESEQ		

REVIEWERS			
NAME	**DIVISION**	**DATE**	**SIGNATURE**
Renato Henrique Ferreira Branco	CGCEA		

APPROVED BY			
NAME	**DIVISION**	**DATE**	**SIGNATURE**
Leandro Toss Hoffmann	CGETE/DIDSS		
Inaldo Soares de Albuquerque	CGETE/SESEQ		

REVISIONS				
REV.	**DATE**	**CHANGES/ PAGES N.**	**AUTOR**	**APPROVED BY**

SUMMARY

LIST OF TABLES

1 INTRODUCTION

1.1 SCOPE

This document establishes the mission assurance preliminary requirements applicable for the EQUARS mission.
The requirements document is the highest level document that specifies the activities to be performed by INPE, their suppliers, and subcontractors to assure the quality and safety of all segments of EQUARS mission during all the phases of the project life cycle.
The EQUARS mission includes: the satellite (platform and payload modules), also known as space segment and the ground and application segments.

1.2 APPLICABILITY

All requirements described in this document and its applicable documents (such as ECSS standards) apply to the whole system and the EQUARS mission lower-levels products or components.

1.3 APPLICABLE DOCUMENTS AND REFERENCES

1.3.1 Applicable Documents

The following documents contain provisions that are considered as part of this document. For dated references, subsequent amendments to, or revision of any of these publications do not apply. For undated references, the latest edition of the publication referred to applies.

AD01 EQUARS-0000-MS-001-A - Declaração do Escopo da Missão EQUARS.

AD02 EQUARS-2000-TS-001-A - Especificação Preliminar de Requisitos Técnicos da Missão EQUARS.

Conflicts among documents must be reported to INPE that shall establish precedence.

1.3.2 Reference Documents

The following documents contain information that develop, add, or clarify concepts described herein. For dated references, subsequent amendments to, or revision of any of these publications do not apply. For undated references, the latest edition of the publication referred to applies.

RD01 ECSS-M-ST-10-01C – Space management: organization and conduct of reviews

RD02 ECSS-M-ST-10C - Space project management: project planning and implementation

RD03 ECSS-E-ST-10C - Space Engineering: system engineering general requirements

RD04 ECSS-S-ST-00-01C - ECSS system - Glossary of terms

RD05 TOR-2007(8546)-6018 Rev B - Mission Assurance Guide

RD06 TOR-2010(8591)-18 Rev Jun, 2010 - Mission Assurance Program Framework

RD07 EXP-RQMT-0003 Rev. A - SMall EXplorers (SMEX) - Mission Assurance Requirements (MAR)

RD08 ECSS-S-ST-00C - ECSS System Description, implementation and general requirements

Conflicts among documents must be reported to INPE that shall establish precedence

1.4 ACRONYMS AND DEFINITIONS

1.4.1 Acronyms List

AD *Applicable Document*

FTA *Fault Tree Analysis*

INPE *National Institute for Space Reasearch*

MA *Mission Assurance*

MS *Mission Success*

RD *Reference document*

RM *Risk Management*

SE *System Engineering*

SEQ *Quality Engineering Service*

TBC *To Be Confirmed*

TBD *To Be Defined*

1.4.2 Definition

Mission Success (MS)	acquired system (or system of systems) singularly or in combination meeting not only specified performance requirements but also the expectations of the users and operators in terms of safety, operability, suitability, and supportability. MS is typically evaluated after operational turnover and according to program specific timelines and criteria, such as key performance parameters. MS assessments include operational assessments and user community feedback [RD05].
Mission Assurance (MA)	disciplined enforcement of proven quality and program management principles towards the goal of achieving mission success. MA follows a general systems engineering (SE) framework and uses risk management (RM) and independent assessment as cornerstones throughout the program life cycle [adapted from RD05].
Customer-Supplier Model ECSS [RD08]	The production of space systems calls for the cooperation of several organizations that share the common objective of providing a product that satisfies the customer's needs (performance within cost and schedule constraints). All space project actors are either a customer or a supplier, or both. In its simplest form, a project can comprise one customer with just one

supplier; however, most space projects comprise a number of hierarchical levels, where:

- the actor at the top level of the hierarchy is the top level customer;
- the actors at intermediate levels of the hierarchy are both supplier and customer; and
- the actors at the lowest level of the hierarchy are suppliers only.

Customer [RD04].

organization or person that receives a **product** as part of a **business agreement.**
NOTE: customer can be internal or external to the supplier organization.

Supplier [RD04].

organization or person that provides a **product** as part of a **business agrement.**
NOTE: supplier can be internal or external to the customer organization.

2 REQUIREMENTS

This Mission Assurance Requirements (MAR) document is a Class C MAR in accordance with mission management decision, as a Class C mission.

2.1 SYSTEMS SAFETY AND MISSION ASSURANCE PROGRAM

The supplier shall prepare, document, and implement a Mission Assurance Plan (MAP).

The MAP shall cover:

a. Flight hardware and software that is designed, built, or provided by the developer and its subcontractors or furnished by INPE/AEB, from project initiation through launch and mission operations

b. The ground support equipment that interfaces with flight items to the extent necessary to assure the integrity and safety of flight items

c. The ground data system to the extent necessary to assure performance as required by the Statement of Work

The mission assurance requirements compliance matrix shall be maintained and submitted to approval in design reviews.

Note: All changes between draft MAP/compliance matrix and final MAP/compliance matrix will need to be highlighted and supported with rationale.

2.2 MANAGEMENT

The supplier shall designate a manager for assurance activities. The assurance manager shall not be responsible for project costs and schedules other than those pertaining to assurance activities. The manager shall have direct access to management that is independent of project management and the functional freedom and authority to interact with all elements of the project.

2.3 REQUIREMENTS FLOWDOWN

The supplier shall apply system safety and mission assurance requirements to subcontractors and suppliers to the extent necessary to ensure the delivered product meets performance requirements and this MAR. The developer MAP needs to include specifics of the subcontractor requirements flowdown and oversight process in support of this project. Developer shall provide sub-tier component suppliers' MAP/Compliance Matrix response to the government.

2.4 SUSPENSION OF WORK ACTIVITIES

The supplier shall direct the suspension of any work activity that presents a hazard, imminent danger, or future hazard to personnel, property, or mission operations resulting from unsafe acts or conditions that are identified by inspection, test, or analysis.

2.5 USE OF INHERITED PRODUCTS

For inherited products, defined as those that were previously developed and exist (e.g., spares), will be build-to-print (BTP), or are available as commercial-off-the-shelf (COTS), the developer may follow

an inherited items review process. With this process the INPE/AEB reviews risk for using the product that is based on established prior history, changes in design, environment or operations, and information regarding the processes used to develop the product and data supplied by developer. The INPE/AEB evaluates if developer's risks are acceptable.

The supplier shall assume ownership and responsibility for risk mitigation.

Use of this process does not relieve the developer from meeting contractual performance and functional requirements.

2.6 MISSION ASSURANCE DISCIPLINES

The mission assurance supporting disciplines are listed in Table 1.

Table 1: Mission Assurance Supporting Disciplines

1	Risk Assessment and Management
2	Dependability Engineering
3	Configuration Management
4	Parts, Materials and Processes
5	EEE Parts
6	Quality Assurance
7	System Safety Assurance
8	Software Assurance

2.7 MISSION ASSURANCE REQUIREMENTS

2.7.1 Risk Assessment and Management

2.7.1.1 The mission shall identify and mitigate events and situations that are possible, but not yet materialized, and that can carry adverse consequences for a program or mission.

2.7.1.2 The mission shall ensure independent assessment and identification of remaining program risks through the examination of work products, processes, and program milestone events. Independent technical reviews validate processes, techniques, and results.

2.7.1.3 The mission shall ensure that the communication processes and issues scaling processes will be planned, executed, and managed.

2.7.1.4 The mission shall ensure that all the management processes and tools are integrated in order to allow the stated and approved communication flow and risk management, including all the independent areas that will manage risks.

Note 1: Program Risk Management: Ensure all risks are identified, mitigation plans established, and funding, schedule, and resources are adequate to mitigate; Capture technical, cost, and schedule risks; Monitor and track risks until they are either accepted or retired.

Note 2: Besides the formal program risk management process, many organizations have an independent, less formal risk identification and management process that frequently is executed by the Mission Assurance or similar organization.

Note 3: This additional risk process provides the following: Independent path for risk reporting; Independently identify risks to program; Monitor program risk resolution; Big Picture of risk in mitigation and cumulative "residual" risk; Focus is on all risk with cost and schedule imposing constraints; Collecting and integration of risks from the Mission Assurance Disciplines; MA risks are integrated into the program risk list as appropriate; Captures early program decisions that contribute to overall risk posture, e.g., accepted single point failures.

Note 4: Risk management is used as a communication tool to ensure common understanding of a program's current project risk posture. The risk management process is managed and monitored separately from issue tracking.

2.7.1 Dependability (Reliability, Availability, and Maintainability)

2.7.1.1 Dependability Program

The Dependability mission organization shall plan, document, implement and maintain a dependability (reliability, availability, and maintainability) program for all mission phases, according the appropriate responsibility level (eg. Mission, Segment, Subsystem, Equipment), that interacts effectively with other project disciplines (e.g. engineering, hardware design, software reliability, systems safety, mission assurance).

2.7.1.1.1 Dependability Mission Plan

The Dependability Mission Plan shall include how the developer will be performing the analyses specified in the section 2.7.1.1.2 to evaluate mission risks and when additional reliability analysis techniques (e.g., RBD/prediction, FMEA (Functional, Design, or Process), PSA, and/or WCA) will be used to supplement these when needed.

Nota 1: The Dependability Mission Plan can be included in the Mission Assurance Programme Plan document.

Nota 2: The Dependability Mission Plan shall be documented, implemented and maintained.

2.7.1.1.2 Fault Tree Analysis (FTA)

Dependability mission organization shall perform qualitative fault tree analyses (FTA) to address mission failure and degraded modes of operation. The fault tree analyses shall address both hardware and software contributions to loss of mission scenarios.

The FTA is meant to be a living document that is updated throughout the development life cycle to address the latest design and any changes to corresponding faults, fault consequences, fault logic, and/or fault propagation scenarios.

The FTA shall analyze critical items to assess risk and where there is an opportunity to influence design or process (i.e., manufacturing, measurement, inspection, and/or test), recommend corresponding mitigation strategies.

The FTA shall analyze where there is a potential to damage other items/elements across an interface (e.g., power surges, excessive thermal dissipation, inadvertent grounding, erroneous control commands) having safety or significant mission success implications.

Nota 1: The FTA shall be documented, implemented and maintained.

2.7.2 Configuration Management

2.7.2.1 The mission shall establish and maintain consistency and accurate knowledge of a product's performance, functional, and physical attributes with its requirements, design, and operational information throughout its life.

Note 1: The activities that are performed within the configuration management processes are as follows: Configuration Management Planning; Configuration Identification; Configuration Control; Configuration Status Accounting; Configuration Verification; and Audit of the Configuration Management System.

Note 2: The CM program operating plan normally includes or references the following topics: Purpose and scope of CM; Description of CM Management: organization, responsibilities, policies, directives, procedures and security; Activities and procedures for each major CM function; Interface control; Supplier control; Technical data management; Description of Information/Documentation management: Information identification; Data formats; Processes; Information systems; Information status reporting; Schedules and resources.

2.7.3 Parts, Materials, and Processes

2.7.3.1 The mission shall ensure that parts, materials, and processes used in deliverable products and GSEs will function and perform in accordance with the mission requirements of their intended application.

Note: PMP activities include but are not limited to: Verification of all subcontractor's performance to assure that delivered products contractually satisfy flowed down requirements; Regularly scheduled PMP meetings to resolve issues; Validation of materials, manly regarding contamination, outgassing, resistance; Qualification of process; Validation of mechanical part; and Verification of degradation limits of critical parameters for worse case design, considering extreme temperatures; micro-meteoroid and space debris; and other natural space environments such as atomic oxygen and extreme ultraviolet (EUV) effects.

2.7.4 EEE Parts

2.7.4.1 The mission shall ensure that's Electrical, Electronic and Electro-mechanical (EEE) parts are sufficiently robust to endure the environmental and application stress they encounter during the mission.

NOTE 1: These assurance activities include, but are not limited to:
1) define environmental requirements;
2) consider these requirements in the design and implementation of the system;
3) support environmental testing and assessment;
4) assure the traceability EEE parts since their origin;
5) support the environmental response assessment after launch.

NOTE 2: Environmental aspects to be analyzed: contamination, outgassing; EMI/EMC/magnetics; verification of worst-case circuit analysis; validation of piece part failure rates; loads and acceleration; pressure, vacuum, and venting; radiation; shock, vibration, and acoustics; extreme temperatures; micro-meteoroid and space debris; and other natural space environments such as atomic oxygen and extreme ultraviolet (EUV) effects.

2.7.5 Product Assurance and Quality Assurance

2.7.5.1 The mission shall ensure that supplied products used in deliverable products, and ground support equipment, meet the quality requirements for their intended application

2.7.5.2 The mission shall ensure that hardware products used in deliverable products and GSEs meet the quality requirements for their intended application.

2.7.5.3 The mission shall assure that systemic issues or defects are identified and appropriate corrective and preventive actions are implemented.

2.7.5.4 The mission shall ensure that for each level of assembly, the functional performance, design, construction, and interface requirements are properly executed.

2.7.5.5 The mission shall ensure that a complete and optimal set of requirements is established based on analysis of mission needs

2.7.5.6 The mission shall ensure that each source requirement is properly decomposed into derived requirements, and mapped to its implementation, verification method and verification results

2.7.6 System Safety Assurance

2.7.6.1 The mission shall ensure that all safety risks associated with the design, development, production and operations of space hardware and software are adequately identified, assessed, minimized, controlled and finally accepted through the implementation of safety assurance program.

2.7.6.2 The mission shall ensure the identification and control of potential hazards to personnel, environmental, flight hardware and facilities and address all of them to achieve acceptable levels of risk.

Note 1: Significant activities include the following: Provide safety requirements checklists for the project; tailoring consistent with mission requirements and determination of compliance position; Perform hazard analyses and risk assessments, create preliminary hazard analysis, Safety requirements/criteria analysis, Subsystem hazard analysis, System hazard analysis , and operating and support hazard analysis; Monitor safety-critical activities; Investigate and formally report mishaps and safety-related failures; Provide input to the Safety Data Package, Safety Analysis Reports (SAR), etc.

Note 2: System Safety interfaces with the Environmental, Health and Safety department on issues relating to compliance with the Occupational Safety and Health Legislation; the Environmental Protection Legislation); and other federal, state, and local legislations.

2.7.7 Software Assurance

2.7.7.1 The mission shall ensure that delivered software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its lifecycle, and that the software functions in the intended manner.

2.7.7.2 The mission shall ensure that processes, procedures, and products used to produce and sustain the software conform to all requirements and standards specified, including the required quality, dependability, reliability, maintainability, availability, safety, security, supportability, and usability.

LIST OF ITEMS *TO BE DEFINED*		
ID	**DESCRIPTION**	**STATUS**
TBD-1		
LIST OF ITEMS *TO BE CONFIRMED*		
ID	**DESCRIPTION**	**STATUS**
TBC-1		\